Objectworld

Unified Communications Server ®

Standard Edition

Planning and Deployment Guide

Version 4.4

Part No. CAO-1011-009-v4.4

Table of Contents

1 Objectworld UC Server Planning and Deployment Overview

1.1 About this Guide

This document provides guidelines, recommendations and best practices for all activities that comprise a UC Server installation project, beginning with pre-sales work, and ending with contract closure and customer transition to maintenance and support services. This document additionally provides information on all the steps to complete the UC Server installation.

This guide is divided into the following chapters:

- Chapter 1, “Objectworld UC Server Planning and Deployment Overview”
- Chapter 2, “Planning for UC Server”
- Chapter 3, “Deploying UC Server”

For the latest version of this document, check Objectworld’s support area at www.objectworld.com/support.

This guide is accompanied by the Planning and Deployment Worksheet, which is a Microsoft Excel spreadsheet that can guide sales and implementation specialists. It is available on the installation media or on Objectworld’s support area at (www.objectworld.com/support/).

1.2 Who this Guide Is Written for

This guide is intended for use by certified Objectworld Technical Professionals, Objectworld Authorized Resellers and end users responsible for the sale, project management, installation, and configuration of a UC Server solution.

To receive information about Objectworld Certification Programs contact your Objectworld Account Executive.

1.3 UC Server Overview

This section provides a technical overview of the main components of Objectworld UC Server and the system environment that it integrates with. The following subsections describe the UC Server architecture, and the hardware and software components required to support the rich features of an Objectworld UC Server IT Telephony solution.

The UC Server system environment depends upon the licensed Edition of Objectworld UC Server that you are employing. UC Server is shipped as a single software distribution that is licensed to provide different capabilities. Objectworld UC Server is available in the following three licensed Editions, each of which provides a different set of capabilities:

- UC Server—SIP Edition
- UC Server—Standard Edition
- UC Server—CEBP Edition (Communications Enabled Business Processes)

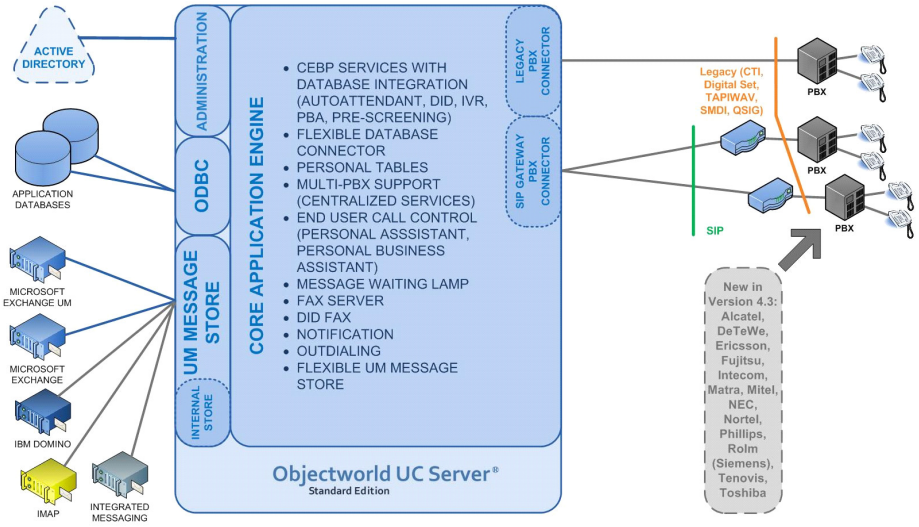
Each Edition is made available in license bundles that accommodate different market segments and different size systems, and which may be expanded and customized to different requirements by using expansion licenses.

In addition, the licenses for one UC Server SIP Edition bundle and one Standard Edition bundle may be combined to economically support external PBXs on UC Server SIP Edition.

The following diagrams illustrate the system configurations supported by each Edition of UC Server.

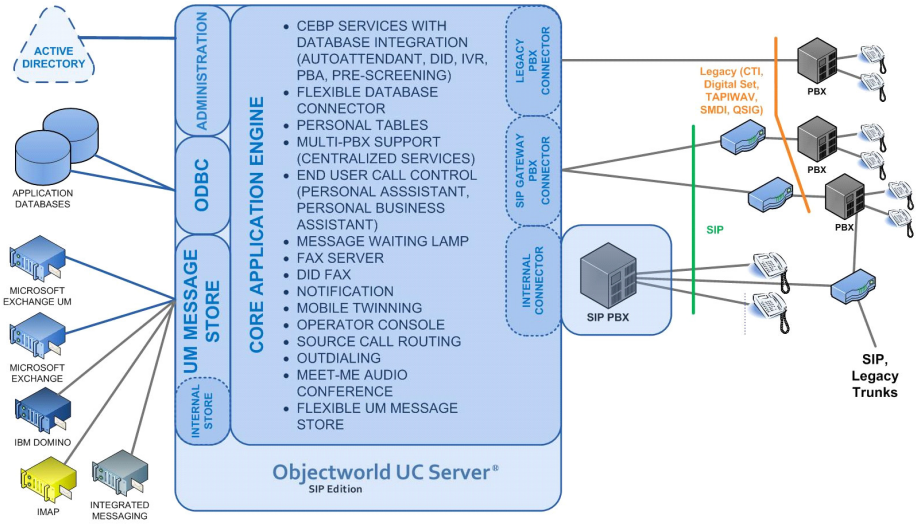
UC Server—Standard Edition

UC Server—Standard Edition provides unified communications capabilities for one or more external PBXs.



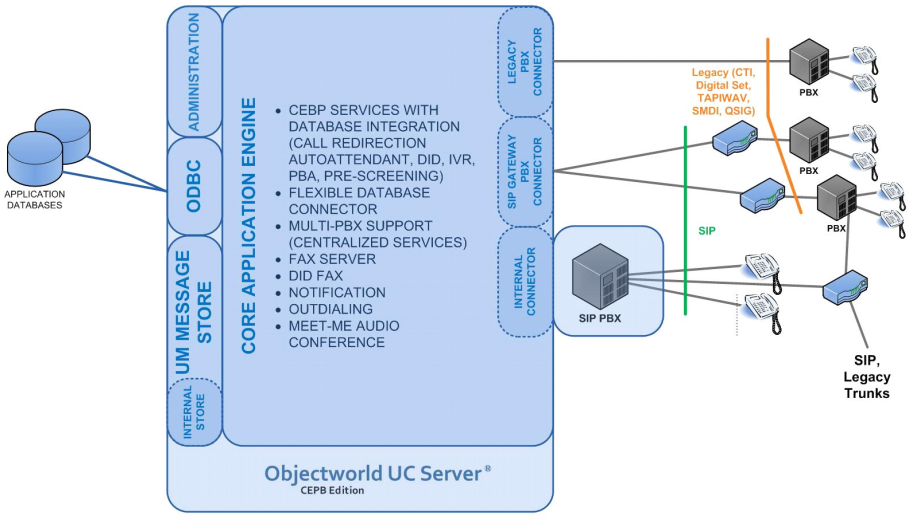
UC Server—SIP Edition

UC Server—SIP Edition includes a fully featured SIP PBX in addition to the capabilities of UC Server Standard Edition.



UC Server—CEBP Edition

UC Server—CEBP Edition is an application server that provides outbound dialing capabilities as well as inbound IVR, call redirection, fax, paging, and conferencing solutions.



UC Server Capabilities

Objectworld UC Server is a single software application that supports a rich set of unified communications and communications enabled business processes. Objectworld UC Server supports the following high-level capabilities:

Support for external PBXs

UC Server provides unified communications and communications enabled business processes for PBXs (private branch exchanges) and IP-PBXs using a variety of integration methods that depend on the capabilities of the PBX. UC Server can support all of its UC functionality for most PBXs. Consult with the Objectworld PBX interoperability guides or Objectworld if your PBX is not listed to determine the features that UC Server can provide for a specific PBX.

Application services

UC Server provides a services environment that allows you to build custom communications services for automated attendants, IVR (integrated voice response), outbound notification, call screening, and Personal Business Assistants. Services can be built quickly and easily using predefined service elements in a drag and drop service editor. Application services can access and manipulate multimedia data in any corporate ODBC-compliant database or application, or using UC Server's built-in multimedia tables which are accessible by either an administrator or personally by each user. The services environment allows you to quickly build custom telecommunications services that allow callers to interact with corporate data.

Fax server

UC Server provides a fax server that allows you to transmit fax messages from any Windows desktop application using its fax printer driver. You may also send faxes from any application service, which can retrieve fax content from TIFF files, UC Server's built-in tables, and ODBC-compliant databases. Faxes can be received into any user's mailbox or copied into any ODBC database or built-in table. The fax server also includes a cover page editor, allows for scheduled transmission and bulk transmission of faxes.

Unified messaging

UC Server provides unified messaging for voice and fax messages using the following mail servers (referred to as message stores by UC Server): Microsoft Exchange Server, Local Message Store, Integrated messaging client (with Local Message Store), Lotus Domino (IMAP4) and other IMAP4 compatible servers such as Novell GroupWise and Google Gmail. Message waiting lights on any telephone assigned to a user can be synchronized when Local Message Store, Microsoft Exchange Server or Lotus Domino are used as the user's message store. UC Server's UC Client provides voice and fax plug-ins for both Microsoft Outlook and IBM Lotus Notes e-mail clients.

UC Client

UC Server includes a UC Client desktop client that allows users to access and control their unified communications. UC Client operates in one of two modes: Personal Assistant and Personal Business Assistant.

Personal Assistant (PA) mode provides a simple user interface that allows you to:

- Manage greetings.
- Access and manage voice and fax mail when using UC Server's internal message store.
- Send faxes from any Microsoft application.
- Create fax cover pages and fax documents.
- Use your Microsoft Outlook contacts.

- Create and manage One-time Messages.
- Selectively get notified by a voice server when you have a message, using Active Message Delivery.
- Selectively transfer calls when you don't answer.
- Selectively get notified by Pager Notification when you have a message.
- Selectively get notified by E-mail Notification.
- Create and manage voicemail distribution lists.
- View voice and fax mail in Outlook and Lotus Notes using viewer plug-ins.

Personal Business Assistant (PBA) mode provides similar functionality to PA mode but additionally provides access to the Service Editor so you can create and manage custom personal services that run when you do not answer a call. PBA mode also enables personal built-in tables in UC Client, allowing you to manage personal information that can be provided to callers or used to determine the actions to be taken dependant on the caller and the options selected by the caller.

Telephone user interface (TUI)

UC Server provides a telephony user interface so that users can access their messages and control their unified communications from any telephone.

System Components

Objectworld UC Server operates in both simple and complex network and IT environments. UC Server integrates and interacts with the following system components:

Existing PBXs and IP-PBXs

UC Server provides unified communications for existing PBXs.

A PBX (private branch exchange) is used to make connections between telephones within an office and provide internal telephones with a connection to the PSTN via trunk lines. PBX development has evolved from PBXs supporting analog and TDM telephones to IP-PBXs which support VoIP and VoIP telephones. Some PBXs that support both VoIP and older analog/TDM telephones are referred to as Hybrid-PBXs. Many legacy PBX have been evolved into Hybrid-PBXs by their manufacturers to extend the useful life of their existing products and installed base. IP-PBXs use the Internet Protocol to carry calls. The integration type used by UC Server to connect to a PBX varies dependent upon the capabilities of the PBX.

UC Server integrates with PBXs using one of the following techniques:

- Analog-In-band DTMF
- Digital Set Emulation
- T1-CAS (channel associated signaling)
- SMDI (simplified message desk interface) with separate media integration

- T1/E1 PRI
- T1/E1 Q.SIG
- TAPI/Analog
- TAPI/Wave
- Direct SIP Connection

Although UC Server will integrate with any PBX, the following capabilities which affect the services that can be offered by UC Server may not be supported by your PBX or may only be supported by certain types of integrations with your PBX: calling party number, calling party identification, call reason, and turn message waiting indicators on and off. Consult with the Objectworld PBX interoperability guides or Objectworld if your PBX is not listed to determine which integration applies to a specific PBX.

LANs/WANs

VoIP transmits and receives voice communication using the same data networks that computers use. Within an office, voice traffic is carried over the LAN (local area network). Interoffice voice traffic is carried over the WAN (wide area network). Additional consideration is required to ensure the WAN architecture meets the real-time requirements necessary for voice traffic. In many cases, the WAN connectivity between corporate offices is conducted over a Virtual Private Network (VPN) on the Internet.

1.4 Protocols and APIs

A communication protocol is a set of rules for data representation, signaling, authentication, and error detection required to send information over a network. An API (application programming interface) is a set of declarations of the functions (or procedures) that an operating system, library or service provides to support requests made by one computer program to another. The standardization of communication protocols and APIs allows products of different hardware and software manufacturers to communicate with each other because they follow the same rules and have compatible interfaces. UC Server makes use of many communication protocols and APIs to integrate SIP communications devices (telephones, gateways, ALGs and IP-PBXs), other software programs (operating systems, mail servers, databases and server based applications), and IP network and IT data center infrastructures such as Microsoft Windows Server System.

SIP (Session Initiation Protocol), RFC3261

SIP (session initiation protocol) is used to create, modify and terminate communication sessions with one or more participants. It provides signaling and call setup between SIP endpoints, including SIP telephones, SIP PSTN gateways, and SIP services. SIP uses an open architecture, which allows customers to take advantage of the wide range of communications manufacturers and their various capabilities. SIP is used by UC Server to provide real-time communication of voice, fax, and video. SIP is a naturally scalable VoIP protocol that is only used for signaling. After a call is established, RTP (real-time transport protocol) is used between the SIP endpoints.

Message Stores

- **Internet Message Access Protocol Version 4 (IMAP4)**—is an application layer protocol that allows e-mail programs to access new and saved messages on a remote server without having to download them to the user's desktop. UC Server integrates with most mail servers (such as Lotus Domino, Google Gmail, Novell GroupWise, etc.) using IMAP4.
- **Messaging Application Programming Interface (MAPI)**—is a messaging architecture for Microsoft Exchange Server. Messaging clients like Microsoft Outlook use MAPI to communicate with Microsoft Exchange Server. UC Server integrates with Microsoft Exchange Server using MAPI.
- **Simple Mail Transfer Protocol (SMTP)**—is an application layer protocol that is the standard for e-mail transmission across the Internet. SMTP is a text-based protocol where recipients are identified and the message content is transferred. UC Server can be configured to use SMTP for e-mail transmission.

Databases and Applications

Open Database Connectivity (ODBC)—is a standard software API method for accessing databases. UC Server's service environment uses ODBC to extract, modify and add information to most databases and server based applications such as CRM, ERP and SCM applications.

1.5 Microsoft Environment

UC Server leverages the following components of the Microsoft IT infrastructure:

- Operating system (e.g. Microsoft Windows Server 2008, Microsoft Windows Server 2003, Microsoft Windows 2003 Small Business Server, or Microsoft Windows XP Professional)
- Administration (e.g. Active Directory integration)
- Security (e.g. global policies, authorization and permissions, single user sign-on)
- Desktop environment (e.g. Microsoft Outlook, Objectworld fax printer driver)
- Database (e.g. SQL server, Microsoft Dynamics applications)
- Messaging and Communications (e.g. Microsoft Exchange Server, Office Communications Server)
- Applications (e.g. Outlook contact, Objectworld UC Client, ucCompanion)
- Backup utilities

UC Server software installs on the host platform as Windows services that require a Windows service account. The UC Server service account can be either a locally managed account or, in the case of Microsoft Domain deployments, an Active Directory user account. UC Server requires a service account for the following purposes:

- File permissions for UC Server installation directory
- File permissions for FTP file path and IIS (Internet Information Services) file path
- Microsoft Exchange Server integration
- Roles-based authentication and administration
- Active Directory access (read access, optionally: write access to integrate telephone extension information back into Active Directory)

Active Directory

Active Directory, though not mandatory, can play an integral role within UC Server. Benefits include Active Directory-based administration, single sign-on, delegation of control, and role-based permissions. UC Server integration with Active Directory does not modify or extend the Active Directory schema.

UC Server uses Windows Active Directory for a variety of functions, including the following:

- **MMC plug-in to the Active Directory for Users and Computers application**—enables Windows IT Administrators to configure all aspects of a Windows user from a single location. Just as the IT Administrator can add and configure a Microsoft Exchange Server mailbox, they can configure a UC Server capability.

When IT Administrators disable an Active Directory user, the UC Server account is also automatically disabled. Disabled Active Directory users can no longer access customer resources, file shares, remote access or voice, fax or e-mail messages from their telephone.

- **Importing users from Active Directory**—during the UC Server Configuration Wizard, UC Server can import users from Active Directory to configure users' internal telephone numbers for use with SIP telephony. The UC Server administrator can run the wizard again later to import more users.
- **Single sign-on**—when users are created, they can be associated with Active Directory users. When users log into any Windows workstation using their Windows username and password, they can also manage their UC Server profile without having to separately log into UC Server. Their UC Server credentials and Windows credentials are the same.
- **Delegation of control**—the UC Server Administrator can delegate control of a user's profile to other users. The user's UC Client can access a different tab for each delegated user profile.
- **Role-based authorization**—the UC Server Administrator can associate a user with a specific role, which allows the administrator to delegate permissions based on their position in the organization. Some examples of roles that can be associated with a user are Standard User, Administrator, Executive Assistant and Read-only Administrator.
- **Service Connection Points (SCP)**—A Service Connection Point (SCP) object class can be defined in Active Directory to make it easy for a service to publish server-specific data in the directory. Clients of the service can use the data in the SCP to locate, connect to, and authenticate an instance of the service. An object class is a category of objects such as users, printers or application programs, which share a common set of characteristics.

  Using the defined UC Server SCP, UC Client users can automatically discover UC Servers deployed in a customer network. After an SCP has been established, users can connect directly to any one of the UC Servers without having to know the specific name or IP address of the server.
- Populating the Active Directory field with telephone number information.

Microsoft Exchange Server

Integration with Microsoft Exchange Server allows voice and fax messages to be stored in mailboxes on a Microsoft Exchange server. It also allows users to retrieve voice, fax and e-mail messages over the telephone from any location.

UC Server integrates with Microsoft Exchange Server using an Active Directory service account, Microsoft Exchange Server mailbox, and special permissions on the Microsoft Exchange server. UC Server can automatically locate the correct Microsoft Exchange server by using information stored in Active Directory. UC Server permissions are managed through Microsoft Exchange System Manager allowing appropriate permissions to the message store server objects. This management ensures the integration can fit into any organizational category by explicitly assigning permissions for the UC Server service account on a Microsoft Exchange message store server object. UC Server can then deposit the end user messages into the user's appropriate message store.

2 Planning for UC Server

2.1 Overview

This chapter outlines the steps and considerations that are necessary and recommended to ensure a well-planned UC Server deployment that satisfies the customer's needs and expectations.

The key to a successful implementation is to plan all aspects of the installation. Planning must take into account the existing PSTN connection, details of the customer's business, the existing IT environment and the network. The planning phase also involves finding out as much detail as possible about the customer's business needs and how they intend to use UC Server and its associated features. Customer expectations about existing functions that should be preserved, or existing limitations that need to be addressed, must also be understood and documented during the planning phase.

Another key to a successful implementation is to consolidate all the planning information that is gathered from the customer. The Planning and Deployment Worksheet is a Microsoft Excel spreadsheet that accompanies this guide, and allows you to record the information. It is available as part of the product documentation which can be found on the UC Server installation media or in the Objectworld support area at www.objectworld.com/support/

Planning for successful UC Server implementations will include the following:

- UC Server System Requirements
- Assessing the Organization Size
- Assessing Deployment Options
- Assessing the Network
- Assessing the IT Environment
- Assessing Voice Requirements
- Assessing Application Requirements
- Assessing Call Routing and Numbering

2.2 UC Server System Requirements

This section describes the operating systems and hardware required for server and client components of UC Server.

Server Requirements

Operating system

The server components of UC Server support the following Microsoft® Windows™ operating systems:

- Microsoft® Windows Small Business Server 2008 (x64)—UC Server should be deployed on the additional Windows Server 2008 license that is part of the Premium Edition of Windows Small Business Server 2008. UC Server can also be installed on the Windows Small Business Server 2008 platform with suitable hardware.
- Microsoft® Windows Essential Business Server 2008 (x86, x64)—UC Server should be deployed on the additional Window Server 2008 license that is part of the Premium Edition of Windows Essential Business Server. Do not install UC Server on the Security Server. It is not recommended to install UC Server on either the Management Server or the Messaging Server.
- Microsoft® Windows™ Server 2008 (x86, x64)—Deployment on Server Core or Hyper-V is not supported.
- Microsoft® Windows™ Small Business Server 2008 (x64)
- Microsoft® Windows™ Server 2003 R2 SP1, SP2 (x86)
- Microsoft® Windows™ Server 2003 SP1, SP2 (x86)
- Microsoft® Windows™ Small Business Server 2003 SP1 (x86)
- Microsoft® Windows™ XP SP2 (Professional) (x86)

Other operating systems are not supported.

Objectworld recommends using a server operating system for all installations of UC Server. While the client platforms mentioned above (such as Microsoft® Windows™ XP SP2) are supported, they are designed by Microsoft for desktop use, not server use.

Generally speaking, UC Server is considered a dedicated application server providing unified communications. Using the server for a combined purpose must be undertaken with caution.

Platform

The following table lists the minimum recommended server platforms based on the number of users. The platform also requires a 100/1000 MBits/s Ethernet NIC.

Table 2–1: UC Server—Standard Edition minimum server platform recommendations

Users	OS	Processor	RAM	Storage
Integrated with Microsoft Windows XP Professional				
5 to 15	Windows XP Pro	1 x Pentium Dual-core E2140	2G 667 MHz	No Raid, 80G, 7200 RPM
Integrated with Microsoft Small Business Server 2003				
5 to 10	Windows SBS	1 x Pentium Dual-core E2140	4G 667 MHz	No Raid, 80G, 7200 RPM
15 to 25	Windows SBS	1 x Quad-core E5310	4G 667 MHz	Raid 1, 2x80G, 7200 RPM
25 to 75	Windows SBS	2 x Quad-core E5310	4G 667 MHz	Raid 5, 3x160G, 7200 RPM
Integrated with Microsoft Small Business Server 2008				
5 to 10	Windows SBS	1 x Pentium Dual-core E2140	6G 667 MHz	No Raid, 80G, 7200 RPM
15 to 25	Windows SBS	1 x Quad-core E5310	6G 667 MHz	Raid 1, 2x80G, 7200 RPM
25 to 75	Windows SBS	2 x Quad-core E5310	6G 667 MHz	Raid 5, 3x160G, 7200 RPM
Integrated with Windows Server 2003 or Windows Server 2008				
100 to 200	Windows Server	1 x Quad-core Xeon E5310	2G 667 MHz	Raid 1, 2x80G, 7200 RPM
200 to 400	Windows Server	2 x Quad-core Xeon E5310	2G 667 MHz	Raid 5, 3x160G, 7200 RPM
400 to 600	Windows Server	1 x Quad-core Xeon E5450	2G 667 MHz	Raid 5, 4x146G, 15k RPM
600 to 1200	Windows Server	2 x Quad-core Xeon E5450	4G 667 MHz	Raid 5, 4 x 146G, 15k RPM
1200 to 2000	Windows Server	4 x Quad-core Xeon 7110M	4G 667 MHz	Raid 5, 4 x 146G, 15k RPM

Client Operating System Requirements

UC Server provides advanced communications that can be realized to its full potential when UC Client is installed.

UC Client software includes the following capabilities:

- User management of greetings, notification services and transferring callers
- Voice and fax plug-ins for Microsoft Outlook
- Voice and fax plug-ins for Lotus Notes
- Fax print driver
- Plug-in for Active Directory management console

Operating system

The client components of UC Server (UC Client and ucCompanion—Live Attendant) are supported on the following Microsoft® Windows™ operating systems:

- Microsoft® Windows™ Vista (Business, Ultimate or Enterprise Edition) (x86, x64)
- Microsoft® Windows™ Server 2008 (x86, x64)
- Microsoft® Windows™ Server 2003 R2, SP2
- Microsoft® Windows™ Server 2003 SP1, SP2
- Microsoft® Windows™ XP SP2 (Professional or Tablet PC Edition)

Other operating systems are not supported.

Platform

To install UC client, the platform must meet the minimum requirements for the Microsoft Windows operating system listed below.

Table 2–2: UC Client minimum platform recommendations

OS	Processor	RAM	Storage
XP SP2, Server 2003	x86 compatible processor 600 MHz or higher	256 MB	500 MB
Vista, Server 2008	x86 or x64 compatible processor 1 GHz	1 GB	500 MB

2.3 Assessing the Organization Size

The size of the organization and the desired deployment option are important in determining what pieces of hardware are needed and the associated specifications of that hardware.

UC Server is targeted towards companies ranging in size from approximately 15 to 2000 employees. For UC Server planning, the organization size is divided into three categories.

- Small business market—5 to 75 users
- Mid market—100 to 500 users
- Enterprise market—400 to 2000 users

The number of users also includes utility phones and integrated fax services (these topics are covered in "Assessing Voice Requirements" on page 43).

Another consideration when discussing the organization size with the customer is the organization's near and midterm growth projections. This is important if there is planned growth that might put the organization into a different category of hardware requirements.

For information about server platform recommendations, see "Server Requirements" on page 14.

2.4 Assessing Deployment Options

The deployment options vary with the Edition of UC Server, and determine how it will connect with outside callers.

PBX Integration Options

UC Server can integrate with a PBX using one of the following methods:

- Integrated Intel Dialogic Card installed in the UC Server computer
  - Analog telephone emulation
  - Digital telephone emulation
  - TAPI with Analog Dialogic Card
- PBX integration using Dialogic Media Gateways (SIP Integration)
  - Analog station with Inband DTMF
  - Analog station with serial interface (SMDI, MCI, Proprietary)
  - Digital telephone emulation
  - T1-CAS (Channel Associated signaling)
  - T1-SMDI
  - T1/E1 PRI
  - T1/E1 QSIG
- Direct SIP connection
- TAPI/Wave

The following must be considered when planning to integrate with UC Server:

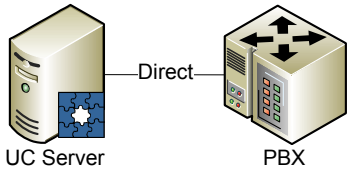
- **PBX integration hardware**—The PBX capacity may need to be expanded to integrate with UC Server. Additional capacity can be added by adding a card or in some cases an additional peripheral cabinet.
- **Power**—Additional power outlets and backup power will be required for each Dialogic Media Gateway.
- **Network Cables**—Additional network connections will be required for each Dialogic Media Gateway.
- **PBX licenses**—Additional PBX vendor licenses may be required to perform the integration.

For a list of PBXs and integration techniques that are supported, see Objectworld's PBX integration guides available on the installation media or in the Objectworld's Web site in the support area (www.objectworld.com/support/)

Document the PBX manufacturer, model and version and any other pertinent details related to the installed system. The information about the existing system helps determine the additional parts and services that are required to integrate the PBX with UC Server.

Direct PBX integration

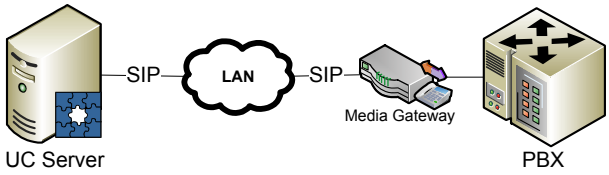
A direct PBX integration uses Dialogic hardware installed in the UC Server computer. The Dialogic hardware emulates station interfaces such as analog telephones or digital telephones. Some PBX integrations require an additional CTI (Computer Telephony Integration) interface - such as TAPI, TSAPI - to provide the complete feature set of UC Server.



Integration through a SIP media gateway

SIP (RFC 3261 - SIP: Session Initiation Protocol) media gateways provide a complete range of integration techniques. The SIP media gateway integrates directly with UC Server. SIP media gateways can be combined to provide the capacity required. The SIP media gateway is placed on the customer's network and the telecom interfaces connect to the PBX. The SIP media gateway used for PBX integration must support the SIP extensions as described in the following section on "Direct SIP connection".

.



Direct SIP connection

UC Server can provide unified communications services to PBXs using a direct SIP (RFC 3261 - SIP: Session Initiation Protocol) connection with extensions for the following capabilities:

- **Diversion Header**—Allows UC Server to determine if the call has been redirected to voicemail. The diversion header must be implemented as defined in RFC 3326 - "The Reason Header Field for the Session Initiation Protocol (SIP)."

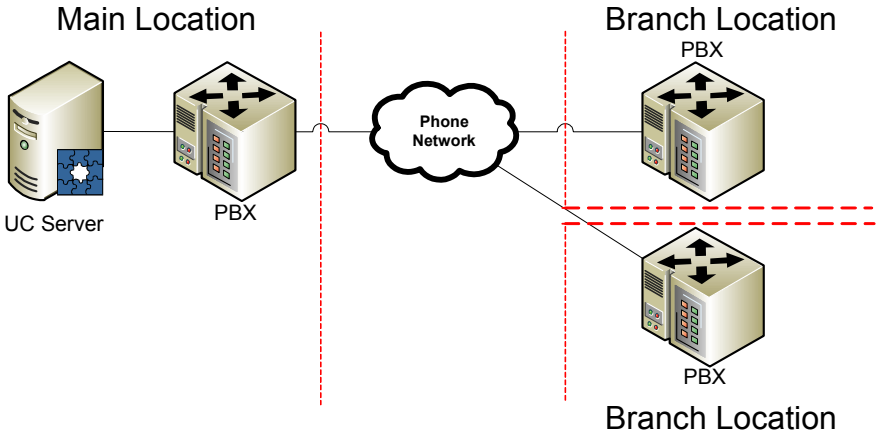
- **Supervised Transfer Extension**—Allows calls to be transferred eliminating the need for calls to be hair pinned through UC Server. When a gateway is employed, this reduces the number of channels that are required for connection to the PBX. This is also useful but less so for PBXs that support SIP directly. The supervised transfer extension must be implemented as defined in draft-ietf-sipping-cc-transfer-05 - "Session Initiation Protocol Call Control - Transfer."
- **Message Waiting Indicator Control**—Enables UC Server to control the message waiting indicators on the PBX phones. The Message Waiting Indicator Control must be implemented as defined in RFC 3842 - "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol."

Centralized PBX integration with distributed networked PBXs

UC Server can also exploit PBX network capabilities to provide a centralized unified communications solution. This capability leverages one of the aforementioned integration techniques. The network of distributed PBXs must be capable of private network signaling. A common inter-working technique is proprietary private networking signaling if the PBXs are from the same manufacturer. If different PBX manufacturers are part of the same customer PBX network, signaling systems such as Q.SIG provide transparent networking between PBXs.

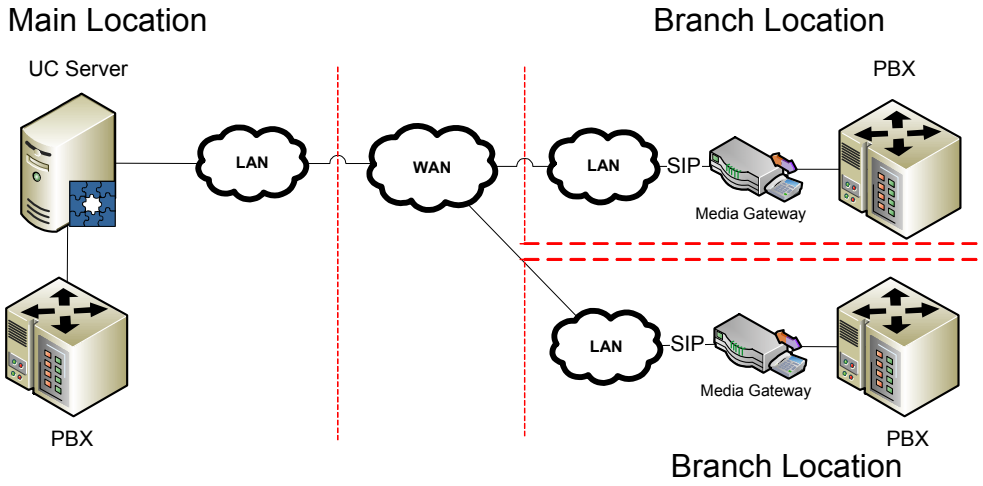
The PBX that is directly connected to UC Server must provide the following capabilities for proper operation:

- Call forwarded calls from any PBX must behave as if the call has been forwarded from the connected PBX.
- Message waiting light requests must be relayed to the target PBX to toggle the message waiting light on the associated extension.



Centralized PBX integration with distributed SIP media gateways

UC Server can also provide centralized services by deploying SIP media gateways at each location. SIP media gateways are deployed at the locations of the PBXs that are to be integrated. The different locations must be part of the same network. The WAN must be capable of supporting voice networks. The WAN must be highly reliable, provide adequate bandwidth and have low latency.



2.5 Assessing the Network

Assessing the network ensures the customer's network is ready for voice traffic. The following topics related to the network assessment are discussed in this section.

- Bandwidth Requirements
- QoS (Quality of Service)
- Internet Connectivity
- Network Engineering
- Backup Power - UPS (Uninterruptible Power Supply)

Bandwidth Requirements

Special attention to bandwidth is required for any real-time network traffic that is not considered part of the corporate LAN. This includes remote PBX support. Bandwidth requirements for voice traffic as well as data traffic must be characterized.

Voice requirements

Sampling voice

Human speech is digitized (converted from analog to digital) by sampling the audio frequencies. Traditional telecommunications equipment samples the analog speech within a frequency range of 300 Hz to 3400 Hz. This is the basis for many of the VoIP narrowband codecs. Some phone vendors have introduced wideband codecs that digitally encode higher frequencies (e.g. 7 kHz). Narrowband codecs sample the audio at 8 kHz which produces a PCM (pulse code modulation) digital audio source that requires 64 kbps of bandwidth.

VoIP (voice over IP)

VoIP (voice over IP) bundles PCM voice information into IP (Internet protocol) packets and sends them over an IP network.

In addition, the PCM "stream" needs to be "packetized", so that there is a sample rate. Taking a continuous 64kbps stream and sampling it down to 20 ms of 'sampled' audio, allows 50 packets per second to be sent to maintain the 64kbps of voice data. The smaller the packetization interval, the more packets that will be placed onto the network which in turn includes more network signaling overhead.

Compression algorithms

Standardized compression algorithms have been developed for use in voice applications. Data compression is the process of encoding information using fewer bits than an un-encoded representation would use, through use of specific encoding schemes. The most popular compression algorithms are G.723 (6 kbps every 30 ms), G.729 (8 kbps every 20 ms), and uncompressed G.711 (64 kbps every 20 ms). These algorithms differ in packet size, voice quality and complexity.

Calculating VoIP bandwidth

The bandwidth allocation for a SIP phone or UC Server is dependent on the codec or compression type used for the VoIP encoders. For VoIP using G.723 compression, a minimum bandwidth of at least 32 kbps is required, while G.729 compression requires between 30 and 40 kbps of bandwidth depending on the sampling rate (30 or 20 ms).

These calculations are:

- Voice packet size = transport header + IP/UDP/RTP header + voice payload size
- Voice packet size in bits = voice packet size * 8 [bits per byte]
- Voice packets per second = codec bit rate / voice payload size
- Bandwidth per call = voice packet size * voice packets per second

Here is a practical application of these formulas, assuming the use of the G.711 codec:

- Voice packet size (214 bytes) = MAC header (14 bytes) + IP/UDP/RTP header (40 bytes) + voice payload (160 bytes)
- Voice packet size in bits (1712) = voice packet size (214) x bits per byte (8)
- Voice packets per second (50) = codec bit rate (64 Kbps) / voice payload size (1280 bits)
- Bandwidth per call (85.6 Kbps) = voice packet size in bits (1712) x voice packets per second (50)

VoIP's impact on the network can be estimated by taking the bandwidth per call and extrapolating with the number of concurrent calls that are expected during peak hours of calling, as previously calculated. Such estimates are usually made with the largest amount of bandwidth required by a codec, which is currently G.711.

Table 2–3: Summary throughput for VoIP codecs

Codec (sample rate)	Single direction bandwidth
G.723 (30 ms)	~30 kbps
G.729 (30 ms)	~30 kbps
G.729 (20 ms)	~40 kbps
G.711 (20 ms)	~90 kbps

NOTE: SIP calls to the application server (e.g. voice mail and auto-attendants), including PBX integration using Dialogic media gateways, only use the G.711 codec.

Once all of the call flows, call volumes and available network bandwidth are determined, calculate the bandwidth that is required to support the expected VoIP traffic.

Additional VoIP bandwidth requirements using VPN

IPsec (IP security) is one common method for encryption. IPsec is a standard for securing IP communications by encrypting and/or authenticating all IP packets. IPsec provides security at the network layer. These additional cryptographic protocols add approximately 10% overhead to the voice traffic over a VPN tunnel.

Table 2–4: Summary throughput for VoIP codecs using VPN with IPsec

Codec (sample rate)	Single direction bandwidth
G.723 (30 ms)	~33 kbps
G.729 (30 ms)	~33 kbps
G.729 (20 ms)	~44 kbps
G.711 (20 ms)	~99 kbps

VoIP performance requirements

VoIP has three specific performance requirements that must be met to provide quality voice: latency, jitter and packet loss.

Latency

If you have ever tried a long distance conversation using a satellite link, you might have experienced how excessive latency impacts voice quality. The long delays make it difficult for callers to have a natural speech pattern in their conversation because it is difficult to determine when the other person is finished talking. How much latency is too much? Typically, one-way latency should not exceed 150 milliseconds. 150-millisecond delays are noticeable but tolerable. However, when latency exceeds 250 milliseconds having a conversation becomes too difficult. Latency is not an issue on the PSTN, but delays on IP networks can cause latency to exceed 150 milliseconds because of data congestion.

End-to-end latency is the sum of encoding/decoding latency and transmission latency. The encoding/decoding latency introduced is proportional to the level of compression provided by the codec. For example, G.711 performs no compression and adds negligible latency while G.729 codecs compress voice to 8 kbps and add a one-way delay of about 25 ms of latency. Transmission latency can cause more significant delays when voice packets are transmitted across a network, including LANs and WANs. Because voice and data share the same network, it is possible for the voice packets to be delayed behind data packets sent over various WAN link types and link speeds.

Even when voice packets are not delayed by data packets, they are subject to serialization delay, which is the amount of time that it takes to clock the bits into a serial link. Again, this delay is determined by packet size and link speed. Reductions in packet size result in less serialization delay and therefore, lower end-to-end latency. The adjustment in the sample rate adjusts the packet size, but sending more packets to the network increases the overhead added to each conversation.

Latency also increases when IP traffic is encrypted over a WAN connection between office locations. When VPN or IPsec tunnels are created, they are typically encrypted. Encryption delay will affect the end-to-end latency.

Jitter

Jitter is the amount of variation in the packet arrival rate for real-time audio. VoIP devices recover from jitter encountered on an IP network by buffering incoming audio packets. Excessive jitter can disrupt conversations. The PSTN has virtually no latency and therefore no jitter, but enterprise IP networks are subject to jitter caused by:

- Congestion on LANs and WANs
- Packet buffering in routers and other network devices
- Packet re-ordering caused by packets taking different routes through the Internet

Packet loss

The third metric is packet loss. Because VoIP is a real-time audio service that uses UDP transport protocols, there is no way to recover lost packets. Packet loss can result in a metallic sound or dropouts in conversations that can be frustrating to users. The PSTN experiences virtually no loss of digitized voice, but IP networks routinely experience packet loss. The packet loss can happen for a variety of reasons, but the primary cause is congestion.

Minimizing latency, jitter and packet loss

To minimize latency, jitter and packet loss, ensure reliable network connectivity by planning and deploying a network with no points of congestion and adequate bandwidth throughout the network. Networks that are deployed as flat as possible with enough bandwidth to ensure proper data and voice communications have the best performance. Some best practices to keep latency, jitter and packet loss within tolerable limits include the following:

- Avoid putting multiple Layer 2 switches together in a long serial chain, because the higher up the chain that traffic travels, the more congested the final up-link becomes.
- Deploy a number of Quality of Service (QoS) techniques to ensure the best prioritization of voice and data.
- Calculate the bandwidth requirements of the voice and data at all common points of convergence.

QoS (Quality of Service)

QoS (quality of service) is a method of prioritizing network traffic. Current business-quality routers and switches provide a variety of technology that ensure that real-time network requirements are met.

The use of QoS is recommended in the following situations:

- When the customer cannot predict the amount of bandwidth that is being used over the network.
- When quantity of data traffic is high enough to interfere with voice communications.

Some common techniques to explore for ensuring real-time performance over the LAN are:

- VLAN tagging (802.1q)
- Priority tagging (802.1p)
- Differentiated services (DiffServ)
- Increased bandwidth - switching from 100MB to 1000MB

Some techniques to explore for ensuring real-time performance over the WAN are:

- Traffic shaping

- Service level agreements with ISP (Internet service provider)
- Increased bandwidth

LAN QoS options

QoS must be seen as a system approach to network engineering.

VLAN tagging (802.1q)

The VLAN is a virtual LAN that is used to separate the voice and data traffic and, in combination with QoS, to ensure voice has a higher priority over data. Consider VLANs only when the data traffic is high enough to interfere with the voice traffic, which typically happen for enterprises that have more than 50 users.

Priority tagging (802.1p)

Priority tagging is a technique of assigning a priority to each packet as it is inserted onto the LAN. Priority tags must be understood by all switches and routers across the network.

Differentiated services (DiffServ)

Differentiated services (DiffServ) is a technique for classifying and managing network traffic, and for providing QoS guarantees.

WAN QoS options

The Internet is intended as a “Best Effort” network without concerns for reliability and latency. The following techniques should be considered in order to increase the QoS for applications that require real-time network traffic that traverses a broadband connection.

Traffic shaping

Traffic shaping or packet shaping prioritizes network traffic by delaying packets, in order to optimize or guarantee performance, low latency, and/or bandwidth. Traffic shaping deals with the concepts of packet classification, queue discipline, policy enforcement, congestion management, QoS and fairness.

Some security products incorporate a traffic shaper (or QoS module). They can prioritize and do bandwidth limitation for different traffic types based on either the source or the destination IP address, type of service, packet size, and TOS/DSCP markup. This ensures VoIP traffic has primary use of the available bandwidth.

Traffic shaping methods will not guarantee QoS over the public Internet.

Service level agreements with ISP (Internet service provider)

An ISP (Internet service provider) can offer an SLA (service level agreement). The SLA guarantees bandwidth, quality and reliability, which helps to ensure network performance. Typically, an ISP will be able to guarantee network bandwidth for equipment that they own. An SLA may be an option if you are providing a multi-site deployment with each location served by the same ISP.

Increased bandwidth

Increasing the amount of bandwidth for a customer's broadband connection is also an acceptable strategy for increasing QoS.

Internet Connectivity

Internet and WAN connections are required to connect to:

- Multiple offices
- Remote PBX using SIP media gateways

ISP (Internet service provider) services

An ISP (Internet service provider) is a business or organization that provides consumers and businesses access to the Internet and related services. In addition to access to the Internet using various technologies such as dial-up and DSL, ISPs may provide a combination of services including Internet transit, domain name registration and hosting, web hosting, and other Internet services.

ISPs employ a range of technologies to enable consumers to connect to their network. For "home users", the most popular options include dial-up, DSL (typically ADSL), cable modem, and ISDN (typically BRI). Medium-to-large businesses with more demanding requirements use DSL (often SDSL, VHSDSL or SHDSL), Ethernet, Metro Ethernet, Gigabit Ethernet, Frame Relay, ISDN (BRI or PRI), ATM, and SONET.

It is also possible for service providers to provide an enterprise point-to-point network connection between two office campuses. The WAN connection serves as a private interoffice network for voice and data transfer. When measuring or calculating bandwidth availability, ensure that both upload and download characteristics are included.

NOTE: If the connection to the Internet is asymmetrical - different speeds for upload and download - ensure that the slowest speed is factored in the bandwidth calculations.

Typical home user connection

- Dial-up (56 kb/s)
- DSL (up to 3 Mb/s)
- Cable modem (up to 5 Mb/s)

Typical enterprise connection

- DSL (up to 3 Mb/s)
- SHDSL (up to 3 Mb/s)
- T1/ISDN (1.54 Mb/s)
- Ethernet technologies (up to 10 Mb/s)
- Frame Relay (varies)
- ATM
- SONET

CAUTION: Objectworld does not recommend using ADSL services for more than small 2-person offices. ADSL provides asymmetric upload and download speeds. Upload speeds vary widely.

When determining the appropriate Internet connectivity needed for any small/home office or enterprise office, the decision is based completely on bandwidth utilization for both data and voice. There are few solutions to ensure QoS or the priority of voice communication over data communications on the physical connection between the office and the ISP. The solution must ensure that at a minimum there is adequate bandwidth for voice communications.

Analysis of the data communication requirements is needed. Web hosting, multimedia, e-mail hosting, FTP hosting, VPN requirements, and more are all factors in determining data communication bandwidth requirements. Voice communications is another bandwidth calculation that is added to the data communications.

Network Engineering

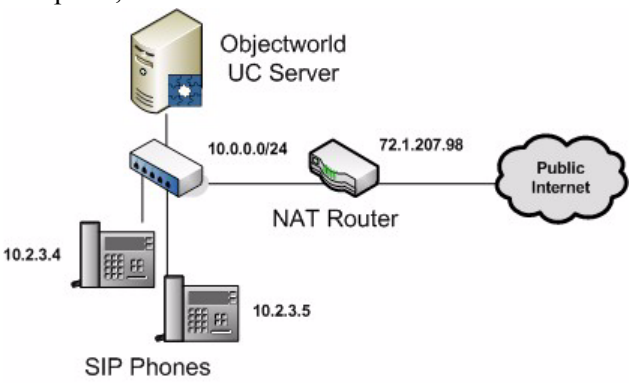
This section contains information on the following network engineering considerations.

- NAT (network address translation)
- VPN (virtual private networks)
- Firewall considerations

NAT (network address translation)

A firewall provides NAT (network address translation), which allows businesses to have a single public IP address on the WAN with multiple private IP addresses for all the workstations, servers, and other IP equipment within the LAN. The router running NAT must never advertise the LAN network addresses to the WAN network backbone. Only the networks with global addresses may be known outside the router. However, global information that NAT receives from the border router can be advertised in the LAN network. Typical or traditional firewalls apply NAT to the IP protocol at the network layers.

NAT's basic operation is illustrated below. The network addresses inside a private domain can be reused by any other private domain. For example, a single Class A address can be used by many private domains. NAT is installed at each exit point between a private domain and the public WAN backbone. If there is more than one exit point, each NAT must have the same translation table.



Typical firewalls cannot apply NAT to the SIP protocol because SIP is a protocol that resides in the application layer. SIP traffic cannot effectively traverse traditional enterprise or home firewalls and NAT devices, and as a result, the firewall/NAT device blocks all SIP traffic, including VoIP. Thus when a SIP phone call attempts to traverse a typical firewall, although the TCP/IP addressing NAT is correct, the IP addresses within the SIP protocol information are not properly corrected. As a result, when a far end WAN device receives a SIP request, the SIP addresses are the private IP addresses of the SIP device behind the typical firewall.

The Ingate, and similar “SIP-aware” firewalls, contain SIP ALG (application layer gateway) functionality above the typical firewall NAT capabilities. This SIP ALG component allows the traversal of the IP addresses within the SIP protocol. The Ingate firewall allows the network traversal of SIP trunking calls to various service providers from UC Server. The firewall controls both incoming and outgoing SIP communications and routes the SIP communication to the intended users and devices. The advantage of the Ingate firewall is that it allows all voice traffic as well as data traffic to traverse the enterprise firewall/NAT/ALG. A NAT firewall with ALGs enables enterprises to utilize SIP trunks to ITSPs while continuing to manage data traffic.

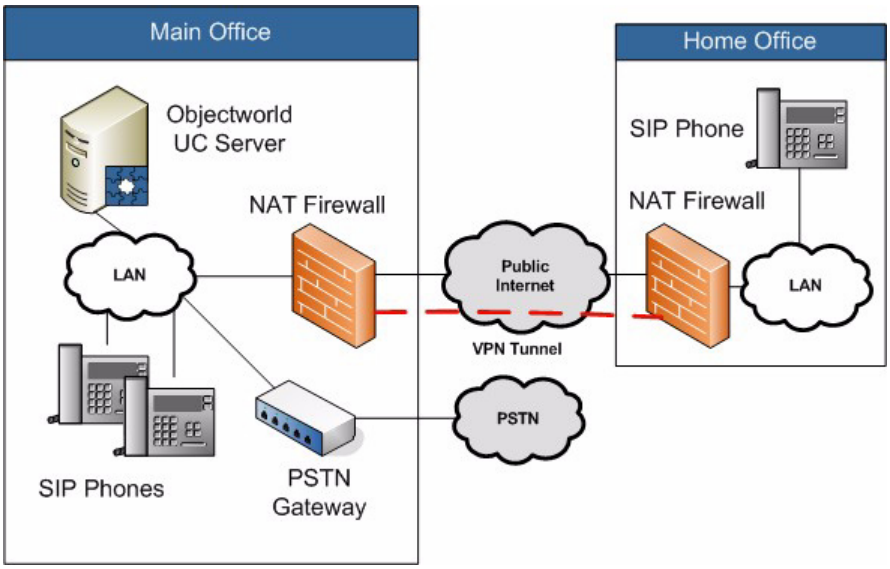
For SIP trunking or teleworker solutions, Objectworld recommends the Ingate Firewall/SIParator for NAT traversal of the SIP protocol.

VPN (virtual private network)

A VPN (virtual private network) is a communications network tunneled through another network, and dedicated to a specific network. One common application is secure communications through the public Internet. VPNs, for example, can be used to separate the traffic of a remote office community over the public Internet network while applying security features.

A VPN is useful for providing employees with remote access to the company network without compromising security. However, encryption can have a negative impact on call quality, as the overhead on the network connection is increased. For example, IPSec, one common type of encryption, adds approximately 10% overhead to the voice traffic over a VPN tunnel.

Ensure that VPN devices are selected that can automatically reconnect in the event of a disconnect. Disconnects and lockouts can occasionally occur.



Firewall considerations

A firewall is a dedicated appliance, or software that runs on another computer. A firewall inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Proper configuration of a firewall is required to ensure network security. Standard security practices dictate a “default-deny” firewall rule set, in which the only network connections allowed are the ones that have been explicitly allowed. Unfortunately, such a configuration requires detailed understanding of the network applications and the endpoints required for the organization's day-to-day operations.

Microsoft Windows Firewall

The Microsoft Windows operating system contains the Windows Firewall application within the security center of the control panel. UC Server automatically configures and uses of the following ports on the Microsoft Windows operating system:

Default UC Server TCP/IP UDP and TCP Settings

- Default Server Port = 5746 (TCP)
- Default FTP Server Port = 5747 (TCP)
- Default Audio Streaming Server Port = 5749 (TCP)

UC Server SIP Ports (Application Server)

- Application Server SIP Port = 5080 (TCP or UDP, depending on your configuration)
- Application Server RTP Ports = 7000-7999 (UDP)

Firewall appliance

A firewall is needed at the edge of the network to protect the private network from the public Internet. One of the main uses of a firewall appliance is Network Address Translation (NAT). The hosts are protected behind a firewall and commonly have addresses in the private address range. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited amount of IPv4 routable addresses that could be used or assigned to companies or individuals, as well as reduce both the amount and cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against malicious hackers and software.

The following information provides some guidelines regarding firewall installation and integration.

- **Microsoft Windows Firewall**—Allow the UC Server application to configure its default settings with the Windows Firewall. Do not attempt to install other applications with conflicting port assignments.
- **Network security**—At all times there must be a firewall appliance providing network security for the enterprise network. This firewall allows VPN access to outside users, if necessary.

Backup Power - UPS (Uninterruptible Power Supply)

A UPS (uninterruptible power supply), also known as an uninterruptible power source, or a battery backup, is a device which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available. There are two distinct types of UPS: off-line and line-interactive (also called on-line).

An off-line UPS remains idle until a power failure occurs, and then switches from utility power to its own power source, almost instantaneously. An on-line UPS continuously powers the protected load from its reserves (usually lead acid batteries), while simultaneously replenishing the reserves from utility power.

While not limited to safeguarding any particular type of equipment, a UPS is typically used to protect computers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption, or data loss. UPS units come in sizes ranging from units that back up a single computer without monitor (around 200 VA) to units that power entire data centers or buildings (several megawatts). Larger UPS units typically work in conjunction with generators.

There are two key factors to consider when choosing a UPS unit. The first is the load rating, expressed as both volt amps (VA) and watts (W). Both the ratings represent the maximum amount of load that the UPS can support. The connected load typically should not exceed 80% of either rating.

The second factor is the amount of runtime the unit can provide when the power fails. This number varies with the load amount that is plugged into the UPS. For example, a unit may run a single computer for 30 minutes, but with two computers it generally lasts less than half that time. Larger units typically can provide more runtime for the same load than smaller units. However, that is not always the case. Some UPS units are designed to provide extended runtime or can have external battery packs connected.

Another factor is the anticipated usage. If the UPS is only intended to provide enough power to gracefully shut down the computers, serial or USB ports on the UPS and support software are essential. If the purpose of the UPS is to provide power until a standby generator kicks in (typically under a minute), the UPS input capabilities should be matched to the generator outputs. If the purpose of the UPS is to provide power until utility power is restored, the UPS input capabilities must match the total consumption over the duration of the outage.

As UC Server is a critical communications server, at a minimum the UPS should provide enough power to gracefully shut down the UC Server platform via serial or USB ports on the UPS and supporting software. Check the volt amps (VA) and watts (W) of the UC Server platform. If there is no power outage survivability requirement, no UPS is required.

If the requirement is to maintain communication services until utility power is restored, a UPS deployment plan must include all of the solution components. These include

- UC Server computer platform
- Ethernet switches and routers (all network equipment that interconnects communications equipment)
- Gateways

When connecting remote offices using a WAN connection, the following must be included:

- Firewall
- WAN modem
- ISP equipment

2.6 Assessing the IT Environment

The purpose of the IT environment assessment is to establish key details of the customer's infrastructure. This information helps determine which steps to follow during the installation phase, due to the differing network scenarios and variation of planning steps for each one. The IT environment information also helps determine what functionality and features are available to the customer based on their specific network, and the availability of UC Server features in the different environments.

UC Server Messaging Feature Sets

UC Server's feature set is available in its entirety when it is integrated in a Windows Server, Active Directory with Microsoft Exchange Server environment. However, this environment is not required for a UC Server installation. UC Server can integrate with Lotus Notes or other standard IMAP4 mail servers and provide unified messaging, even in a non-Microsoft environment. UC Server's flexibility can accommodate any customer IT infrastructure.

The following tables summarize the feature sets that are available with various server and message store environments that might comprise a customer's IT infrastructure.

Table 2–5: UC Server messaging feature sets

IT infrastructure	Unified messaging	Listen to voice mail on computer over speakers	Listen to voice mail on computer over phone handset	Fax feature set	Toggle Message Waiting Indicators on phone from computer	UC Client available	Contact support via caching on server
Outlook Client on Windows with Exchange and Active Directory	✓	✓	✓	✓	✓	✓	N/A

Table 2–5: UC Server messaging feature sets

IT infrastructure	Unified messaging	Listen to voice mail on computer over speakers	Listen to voice mail on computer over phone handset	Fax feature set	Toggle Message Waiting Indicators on phone from computer	UC Client available	Contact support via caching on server
Notes Client on Windows	✓	✓	✓	✓	✓	✓	
Notes Client on Unix or Linux	✓	✓		Partial			
Outlook Client on Windows with IMAP4 mail server	✓	✓	✓	✓		✓	✓
Other mail client on Windows with IMAP4 mail server	✓	✓		Partial		✓	
Other mail client on other operating system with IMAP4 mail server	✓	✓		Partial			

Table 2–6: UC Server messaging feature sets

E-mail server	Messaging client			Voice message playback options		
		Unified messaging	Integrated forms [1]	Device speakers	Telephone handset	Message Waiting Light sync.
Microsoft Exchange Server	Microsoft Outlook	✓	✓	✓	✓	✓
Microsoft Exchange Server	Outlook Web Access	✓		✓		✓[2]
Microsoft Exchange Server	RIM BlackBerry	✓		✓		✓[2]
Microsoft Exchange Server	Windows Mobile Device	✓		✓		✓[2]
Lotus Domino	Lotus Notes Client (Windows)	✓	✓	✓	✓	✓
Lotus Domino	Lotus Notes Client (Other OS)	✓		✓		

Table 2–6: UC Server messaging feature sets

E-mail server	Messaging client			Voice message playback options		
		Unified messaging	Integrated forms [1]	Device speakers	Telephone handset	Message Waiting Light sync.
Lotus Domino	Web Client	✓		✓		
IMAP4 Server	IMAP E-mail client	✓		✓		
Novell Groupwise	Groupwise Client	✓		✓		
Google Mail (gmail)	Web Client	✓		✓		
POP3 Server	Any e-mail client	No, Forwarded copy only		✓		
HTTP Mail Server (web mail)	Web Browser	No, Forwarded copy only		✓		
None	UC Client	Visual Messaging	✓	✓	✓	✓

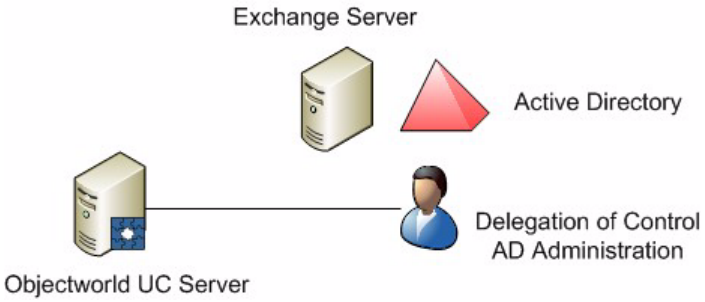
[1] UC Client forms, which provide visual representations of voice and fax messages, are included with the UC Client installation.

[2] This capability requires Exchange Mailbox Monitoring feature enabled

Completing this assessment gives an understanding and record of the customer's security environment, account management system, message store, and server type.

User Authentication

UC Server uses two methods for user authentication: Active Directory single sign-on or local user accounts created within UC Server. It is possible to combine both authentication schemes in a single implementation. However, locally managed users do not receive the benefits of Active Directory integration.



Active Directory integration

Upon deployment of the UC Server and during the UC Server Configuration Wizard, the Microsoft Windows Domain needs to be identified to allow the UC Server to import the list of active users. This step speeds up the overall configuration and allows for single management of all users on the system.

Active Directory integration provide the following benefits:

- UC Server automatically uses the Microsoft Exchange Server message store configuration from Active Directory.
- User authentication is tied to Active Directory.
- Single sign-on. The user only has to login to a computer to get all the capabilities that have been delegated to the user.
- When an employee leaves the company, the AD administrator can disable the user account and be assured that all communication services are also disabled.

The **Active Directory for Users and Computers** plug-in enables Windows IT administrators to configure all aspects of a Windows user from a single location. Just as an IT administrate can add and configure a Microsoft Exchange Server mailbox, they can configure the UC Server capability.

Managing local users

Local users can be created for standalone implementations, integrations where Microsoft Active Directory is not deployed, or for specific users within an active directory that do not require an Active Directory user. Local users can only be managed from within UC Server Administration and cannot be managed through the Active Directory plug-in. Local users will have to enter their username and password to manage their personal data in UC Client.

Message Store Requirements

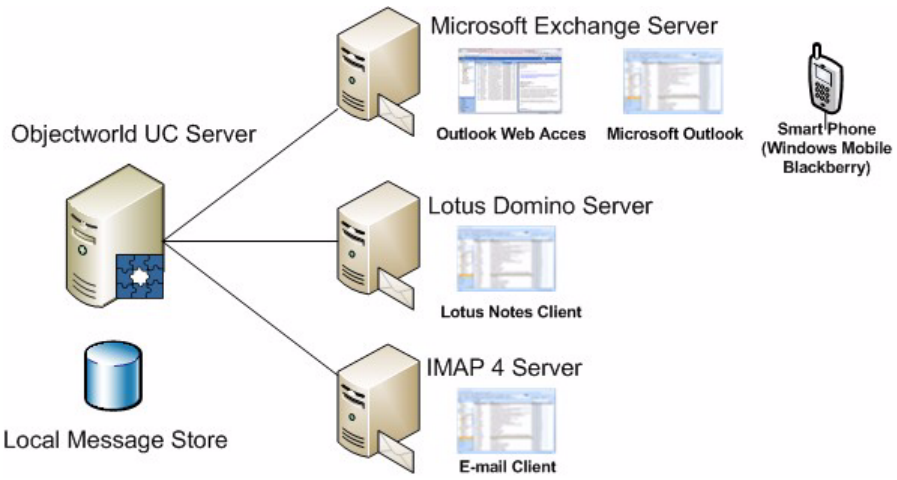
A message store is the physical repository where voice, fax messages and, in the case of unified messaging applications, e-mail messages are stored.

UC Server can support multiple message stores simultaneously. It is possible to create users with Microsoft Exchange Server as the message store and other users with Lotus Notes, IMAP or local message store. It is possible to combine at least one Microsoft Exchange Server and any number of Lotus Notes, IMAP or local message stores. If a customer has a combination of message stores, the details need to be understood and the users that are using each message store need to be recorded. A good example of this is in environments where there are a number of facility or lobby phones. Those extensions can be added to the UC Server as Local Message Store and do not require an entry in the Active Directory environment.

UC Server can integrate with the following message stores.

- Microsoft Exchange Server with Outlook Client
- Lotus Domino Server with Lotus Notes Client

- Industry standard IMAP4 mail server with Outlook or other mail client
  - Google Mail using IMAP4
  - Novell Groupwise



Refer to the appropriate section below that matches the customer's message store.

Microsoft Exchange Server

The following versions of Microsoft Exchange Server are compatible with UC Server.

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2003 SP1 or later
- Microsoft Exchange Server 2000 Service Pack 2 or later

Microsoft Exchange MAPI Connector

Integration with Microsoft® Exchange Server requires a MAPI connector to be installed on the UC Server platform.

The supported MAPI connectors, of which only one should be installed on the server platform, are the following:

- "Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1

This is available for download free of charge from: http://www.microsoft.com/downloads/details.aspx?familyid=e17e7f31-079a-43a9-bff2-0a110307611e&displaylang=en

[Version: 6.5.8069.0, 2009-Feb-16 - older versions are not be compatible with all platforms]

- "Microsoft® Outlook™ 2003 SP3

WARNING: Failure to use SP3 with Microsoft® Outlook™ 2003 will cause unreliability of the integration with Microsoft® Exchange™ Server and may cause system outages.

- "Microsoft® Outlook™ 2007 SP1 (SP2 is not Supported)

WARNING: Outlook 2007 SP2 is not compatible as a server MAPI connector with UC Server and installing it will cause UC Server to be unable to connect to Exchange Server.

Objectworld recommends the use of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 instead of Microsoft Outlook.The benefits of doing this are as follows:

- No Outlook license is required for the UC Server system. The MAPI/CDO software package is available at no charge.
- The MAPI/CDO package is a minimal installation that requires fewer Microsoft Updates.
- This component is designed and provided by Microsoft explicitly for the purpose of allowing applications such as UC Server to access Microsoft Exchange Server.

Requirements

The following requirements must be satisfied for UC Server to integrate with Microsoft Exchange Server. The customer needs to be aware of, and comply with, each of these items.

- An account must be allocated for the UC Server service account in the Microsoft Exchange Server forest.
- A new Exchange account must be created with privileges granted to it for UC Server to integrate with Microsoft Exchange Server. Further details are provided in the *UC Server Configuration Guide*.
- All messages (voice, fax, and e-mail) for all Microsoft Exchange Server-integrated UC Server users are stored in the user’s mailbox on the Microsoft Exchange server.

- Each UC Server integrates directly with only one Microsoft Exchange Server. However, it is possible to access mailboxes on other Microsoft Exchange Servers, provided they are within the same Microsoft Exchange Server forest and have the proper permissions for the UC Server service account. The Microsoft Exchange server proxies the requests from the UC Server mailbox to other Microsoft Exchange servers.
- It is strongly recommended that the customer use an appropriate e-mail archiving strategy. E-mail server search performance is directly proportional to the number of messages in individual user mailboxes. Slow performance increases latency when managing messages over the telephone.

NOTE: For more detailed information on UC Server's Microsoft Exchange Server integration technique, network bandwidth requirements or information on remote Microsoft Exchange Server connectivity refer to TN108, "Best Practices for Integrating UC Server with Microsoft Exchange Server" which is available from the Objectworld Web site support area at www.objectworld.com/support/

Mailbox monitoring

Mailbox monitoring is a method of synchronizing message waiting lights on phones by using Microsoft Exchange Server to monitor when messages arrive, are read, and so on. Using mailbox monitoring also enables the synchronization of message waiting lights when messages are accessed through Microsoft Outlook, Microsoft Outlook Web Access (OWA), or through a mobile device that synchronizes with Microsoft Exchange Server (e.g. Blackberry and Windows mobile devices).

CAUTION: Performance issues may arise when mailbox monitoring is enabled. On systems with more than 100 users, system design and engineering must consider the increased load that keeping open large numbers of mailboxes will have on Microsoft Exchange Server. Enabling monitoring of more than 500 mailboxes requires careful consideration and probably should not be done without a slow roll-out procedure to validate the performance of both Microsoft Exchange Server and UC Server in the specific customer environment. If Microsoft Exchange Server is at or near capacity, consider disabling mailbox monitoring.

Mailbox monitoring can be enabled or disabled at the system level when adding or configuring Microsoft Exchange Server. The default mailbox monitoring setting for users can either be on or off. When you add or configure users, either the server default can be chosen or individual users can have a specific mailbox monitoring configuration.

NOTE: For more information see the *UC Server Administrator Manual*, in the product documentation available from the Objectworld Web site support area at www.objectworld.com/support/

Lotus Notes

UC Server can integrate with IBM Lotus Domino Server and Lotus Notes clients. Message waiting light synchronization is supported in Lotus Notes integration. This feature uses an embedded voice and fax form with Lotus Notes.

The following versions of IBM Lotus Domino Server and Lotus Notes clients are compatible with UC Server.

- IBM Domino Server 6.0.x
- IBM Domino Server 6.5.x
- IBM Domino Server 7.0
- IBM Domino Server 8.0

Requirements

The following requirements must be satisfied for UC Server to integrate with Lotus Notes. The customer needs to be aware of, and comply with, each of these items.

- All UC Server users must have their account configured as an IMAP mailbox in Lotus Notes.
- The Mail template file needs to be modified on the Lotus Notes server to include new forms for displaying voice and fax messages. Further details are provided in *TN014 - Lotus Domino and Notes Integration Guide* (available on the UC Server installation media and the Objectworld support Web site).
- The voice and fax form needs to be modified to support message waiting light synchronization and thus allow true unified messaging integration.
- All messages (voice, fax and e-mail) for all Notes integrated UC Server users are stored in their mailbox on the Lotus Notes server.
- It is recommended that each user's mailboxes must be fully text indexed in order to access voice, fax and e-mail messages from the Lotus Domino Server. If full text indexing is not possible, UC Server will still be able to retrieve the mailbox contents with a slight performance degradation and delay in retrieving mailbox statistics.
- It is strongly recommended that the customer uses an appropriate e-mail archiving strategy. E-mail server search performance is directly proportional to the number of messages in individual user mailboxes. Slow performance increases latency when managing messages over the telephone.

IMAP4

UC Server can integrate with other IMAP4 mail servers.

NOTE: Message waiting light synchronization is not supported in IMAP4 integration.

The following versions of IMAP4 Servers are compatible with UC Server. The specific version used by the customer needs to be recorded.

- University of Washington IMAPd
- Google's GMail using stunnel integration. Refer to *TN100 - IMAP Integration with Google Mail* for specific instructions on how to integrate with Google Mail.
- Any 100% compliant IMAP4rev1 (RFC3501) message store (must correctly support searching of message headers, otherwise users will be unable to play voice messages over the phone)

Requirements

The following requirements must be satisfied for UC Server to integrate with IMAP4 mail servers. The customer needs to be aware of, and comply with, each of these items.

- All UC Server users must have their account configured as an IMAP mailbox in the client.
- All messages (voice, fax and e-mail) for all IMAP4 integrated UC Server users are stored in their mailbox on the IMAP4 server.
- It is strongly recommended that the customer uses an appropriate e-mail archiving strategy. E-mail server search performance is directly proportional to the number of messages in individual user mailboxes. Slow performance increases latency when managing messages over the telephone.

Local message store

If a customer is using local message store, all voice and fax messages are stored on the UC Server. The following items are characteristics of using local message store.

- Voice and fax messages are stored on UC Server.
- No unified messaging. Users cannot listen to their e-mails using text-to-speech using the telephone handset.
- Voice and fax messages do not appear directly in the user's e-mail inbox.
- Voice and fax messages can be viewed in the UC Server Integrated Message Client, if there is a LAN connection from the client PC to UC Server.
- A copy of the messages can be forwarded to the user's e-mail account using E-mail Notification, if a LAN connection and an SMTP mail server are available to UC Server. UC Server does not support eSMTP authentication.

2.7 Assessing Voice Requirements

Use the voice requirements assessment to collect sufficient information about the number and type of users to determine licensing requirements.

Users

All UC Server users have the following:

- User profile
- Identity (extension)
- Authentication (Active Directory authentication or local authentication)
- User type (basic or advanced)

User profile

Each UC Server user needs a profile to access unified communications services. A user profile includes information that describes the user (for example, their name), information on the message store they are using (for example, the server and mailbox), and information on the user's authentications and identities. The user profile also contains a time zone setting that indicates in which time zone the user is typically located. The time zone setting affects the time and dates that appear on voice, fax and e-mail messages when users access their mailbox using the telephone user interface. For workers who travel or are relocating to another site for a period of time, the time zone setting can be changed. Time zone settings also need to be changed for remote users and remote offices that are using the same UC Server but are in a different time zone.

Identity

An identity is the address of a user on some device. Identities also include the concept of a “trunk”. A user can have zero or more identities. Each identity can have a separate set of behaviors, but messages are saved in the message store that is associated with the user profile.

Authentication

An authentication determines whether someone is allowed to have access to the system. For example, an authentication might correspond to a login name and password. It might also correspond to a Windows user. A Windows user that attempts to log in to any of the UC Client applications automatically gains access if that user corresponds to an authentication; this is called single sign-on.

The administrator can also grant other users the ability to manage aspects of the system. Some examples of roles where this is particularly useful are executive assistants and team managers.

If Windows authentication is enabled, it is possible to assign a role to a Windows user. Users can be added or removed from specific roles. If a custom authorization store has been created, the following roles are available. If there is no custom store, all Windows authentications are assigned the 'Administrator' role as defined below.

- **Administrator**—authentications have full access. Administrators are able to manage system objects, and they can create, change and delete objects in shared folders.
- **Read Only Administrator**—authentications are the same as Administrator, except they cannot create, change or delete system objects.
- **Restricted User**—authentications with capabilities typically associated with Personal Assistant or Personal Business Assistant users, except they cannot create or delete announcements, and services can only be read.
- **Standard User**—authentications with capabilities typically associated with Personal Assistant and Personal Business Assistant users.
- **Executive Assistant**—authentications are the same as Standard Users, but can also manage objects that belong to other profiles to which they have access. For other profiles, their authorization does not allow them to create or delete announcements, and allows them to only read services.
- **Restricted Executive Assistant**—authentications that have Restricted User capabilities for their own profile, and the same authorization for other profiles to which they have access.
- **Power User**—authentications similar in capability to Executive Assistant, except that they can also create or delete announcements for other profiles, and have full authorization for services.

User type

There are two user types that can be purchased with the system, basic and advanced. Depending on the customer's operational environment and user needs, they can choose from a variety of bundles to accommodate those requirements. The following table shows the features that are included with each user type.

Table 2–7: Features available to basic and advanced users

Feature	Basic user	Advanced user
PA (Personal Assistant) client	✓	✓
PBA (Personal Business Assistant) client		✓
Internal message store for messages	✓	✓

Table 2–7: Features available to basic and advanced users

Feature	Basic user	Advanced user
Integrated messaging client	✓	✓
Unified messaging		✓
Telephone access to messages	✓	✓
Fax integration	✓	✓
Message waiting light integration	✓	✓

Different options for supporting these different types of employees should be explored with the customer. Different UC Server offerings have different capabilities designed to match the customer's requirements.

All SIP users can have two associated identities. Highly mobile employees might require additional identities (i.e. for their home office or satellite office). Additional SIP expansion pack licenses are available.

As shown in the above table, a basic user can be configured with PA (Personal Assistant). An advanced user can be configured with either PA or PBA (Personal Business Assistant).

PA (Personal Assistant)

PA (Personal Assistant) is the default user setting. The PA user setting provides the most commonly used unified communications features. They can:

- Manage personalized greetings and delivery features
- Access voice, fax and e-mail from a single inbox
- Use a local or remote telephone to log on to the system, and retrieve voice messages and e-mail

A user is set to PA in the User Configuration Wizard on the *Call Answering* screen. It is possible to edit this setting for an existing user by opening the user profile. Under the **General** tab, the *Call Answering* section has the choice of **PA** or **PBA**.

PBA (Personal Business Assistant)

The PBA (Personal Business Assistant) user settings provide all the features of PA, but also the opportunity for the user to design auto attendant services and to record customized announcements. To provision PBA users, there must be adequate licensing in place (each PBA user requires a license).

A user is set to PBA in the User Configuration Wizard on the *Call Answering* screen. Edit this setting for an existing user by opening the user profile. Under the **General** tab, the *Call Answering* section has the choice of **PA** or **PBA**.

The number of employees requiring the PBA application needs to be established to determine if a PBA Expansion pack is necessary. Discuss the differences between a PA and PBA user with the client to assist in this process.

Administrator

If users log in as the UC Server Administrator they have access to the admin profile and can perform numerous administrative functions. If a user's authentication includes the 'admin' user in the accessible user profiles, they can make changes to UC Server.

Some of the functions that the Administrator can perform are the following.

- Manage user profiles, identities and authentications
- Add and configure communications systems and SIP phones
- Configure ports, auto attendant services, IVRs and announcements

All the functions of the Administrator profile can be done from any Windows-based PC that connects to UC Server via TCP/IP and has the UC Client application loaded on it, or from the UC Server platform itself.

It is necessary to ensure that the appropriate personnel's authentication includes the system profile ('admin') as an accessible user profile so they can manage the day-to-day maintenance and administration of UC Server.

2.8 Assessing Application Requirements

There are a number of applications supported by UC Server that a customer may want to take advantage of that require planning to determine the exact number and type of additional licenses.

Auto Attendants

An auto attendant does not have to be provisioned on UC Server. However, most customers want at least some basic auto attendant functionality, even if it is only used to provide after hours service.

There are many ways to develop an auto attendant design. Generally, a “white board” or brainstorming session is a productive way to plan the auto attendant with the customer. Keep the following points in mind:

- A solid understanding of the available service elements to build the auto attendant is mandatory to assist the customer in understanding all the options available. Complete details of the available service elements are provided in the *Administrator Guide* or in the help menu within the service creation environment.
- A solid understanding of the customer's “wish list” is important to ensure that their needs and expectations are addressed in the auto attendant design.
- A pre-determined person, either from the client location or the reseller's business, may be required to review the auto attendant requests and be available for any potential audio recordings. Pay close attention to language requirements when selecting this person.

Database Integration

Database integration can be used for inbound and outbound IVR services. UC Server supports the creation and maintenance of data sources. Data sources are set up similar to tables; each row corresponds to a data row and each column is a field. This data can be used by service elements in the service creation environment to provide information to a caller or to determine appropriate call routing. There are two types of data sources: user data sources and external data sources. For user data sources, the data is managed by UC Server and users have their own copy of the data. For external data sources, the data is managed by another server or process and is shared by UC Server users and others. External data is accessed using Microsoft's ODBC (Open Database Connectivity). External data sources are often called ODBC database sources. Complete details of the UC Server data source capabilities are provided in the *Administrator Guide*.

It must be established during the planning phase if a customer needs database integration because the data source feature is only available if database integration is licensed.

Unified Messaging

Unified messaging allows users to manage all message types from one central storage location. Unified messaging provides a single inbox for voice, e-mail and fax messages that is accessible by both telephone and computer. UC Server provides a unified messaging solution that allows a user to receive all their messages in Outlook.

One aspect of unified messaging is the text-to-speech (TTS) engine. The TTS engine reads back e-mail messages over the phone when users call in to review their messages.

Text-to-speech licenses can be purchased either as part of the initial purchase or at any time after installation. TTS licenses are not based on user count, but based on usage count. The number of TTS licenses available determines the number of simultaneous users using TTS. For example, if a customer purchases four TTS licenses, up to four people can use the TTS engine at any one time. If a fifth person tries to access the TTS engine, they would be unable to do so until one of the TTS licenses is released.

During the planning phase, the customer's requirement for TTS needs to be discussed and the license requirements calculated. A small office with 20 people may require only one or two TTS licenses to facilitate their demand. Larger offices need more TTS licenses to reduce the number of people wanting to access TTS but being unable to do so and to reduce the wait times for a license to be released.

Contact Integration with Outlook

Contact integration allows users to access their contact lists for all their messaging, including phone calls, e-mails and faxes. Contact integration requires UC Server to use Outlook or Outlook Express for the contact manager.

Contact integration provides the following capabilities:

- Incoming calling telephone numbers can be matched with a user's personal contacts.
- The subject line includes a contact-matched name for voice and fax messages.
- Management of mailbox contact information.
- The ability to locate personal contact names, telephone numbers and address information when retrieving or managing messages.
- Retrieval of contact information over the phone from a user's personal contacts.
- Connection to a telephone number in a user's personal contacts.
- Notification services can apply individual rules based on who is calling. Applies to active message delivery, pager notification, e-mail notification and transfer of callers.
- One-time-messages, which deliver a personal message to a caller when they reach a user's mailbox. The individual message is recorded for a specific personal contact.

Faxing

If a customer wants to leave their current fax services unchanged, no further planning is required beyond understanding what trunks must be preserved for the fax machines. However, if there is a desire to integrate fax services with UC Server, more in depth planning is required to understand the level of fax integration that is most appropriate.

Using the UC Server fax services can be approached in a variety of ways. For planning purposes, the method of implementing fax services and the level of fax integration that best suits the customer's needs must be understood.

- Incoming faxes can be received in a general mailbox that is monitored by an office administrator, who then uses e-mail to distribute the faxes to user mailboxes.
- A DID line can be assigned to a specific user so that faxes arriving on that line go directly to that user's mailbox. In this case, specific configurations are required on the gateway to ensure calls are sent to the proper identity.
- A fax attendant identity can be created for a user. Faxes are received in the user's mailbox. This is an extra identity and may require additional licensing and further gateway configuration.
- A single voice and fax number can be assigned to a user. This involved pre-answering each assigned voice and fax number before ringing the telephone.
- Appropriate service elements can be used to receive faxes. In this case the caller is prompted to select the extension of the user for whom the fax is intended.
- Fax-on-demand can be implemented in an auto attendant menu. This allows callers to submit their fax number to have pre-defined information faxed to them.
- Users can send faxes from their computer and fax cover pages can be managed in UC Server.

Complete details of the UC Server fax service capabilities are provided in the *Administrator Guide*.

If the customer wants desktop fax capability and/or fax-on-demand service, ensure that the appropriate number of simultaneous fax licenses are provisioned with the system.

Advanced Applications

Advanced applications on UC Server include any customized applications for a variety of vertical markets. For an example of a vertical market application, view the real estate service demonstration that is available with UC Server. Part of the voice requirements assessment is to understand if the customer has an immediate need for this type of service and, if so, to discuss what their needs are and how they would like to see the application developed. UC Server includes a powerful service creation environment that allows a customer to create advanced service applications with the potential of supporting their existing business processes.

Many of these advanced applications require media channels. All license bundles come with a limited number of media channels. If the particular license bundle that best meets the customer's needs does not have an adequate number of media channels, application media channel expansion licenses can be purchased.

2.9 Assessing Call Routing and Numbering

Application Server Dialing Rules

The UC Server application server provides an additional level of dialing rule flexibility. For unified communications services, such as transferring calls to external numbers, active message delivery, pager notification, outgoing faxing, fax-on-demand and outbound notification services, additional dialing rules can be created. They are separate from the PBX dialing rules so that outgoing calls can be routed differently then other callers.

Defining a numbering plan based on geographical location

It must be determined whether it is required to dial a 7-digit or 10-digit numbering sequence for a local number. It can also be determined what dialing patterns are treated as long distance calls. Prefixes can be independently assigned for local and long distance calls. For example, if users are accustomed to dialing 9 to reach an outside line, an outgoing dialing prefix 9 can be added to each outgoing local and long distance call.

Working with account codes

Some organizations use account codes to allow certain calling patterns to override the PBX system defaults or to track calls for accounting purposes. For example, long distance calls can require the caller to enter a personal account code before the call is placed.

3 Deploying UC Server

This chapter covers the complete deployment of the UC Server. All the steps required to install, configure and verify UC Server are discussed, and references to more detailed documentation are provided.

Before beginning the deployment, complete the Planning and Deployment Worksheet.

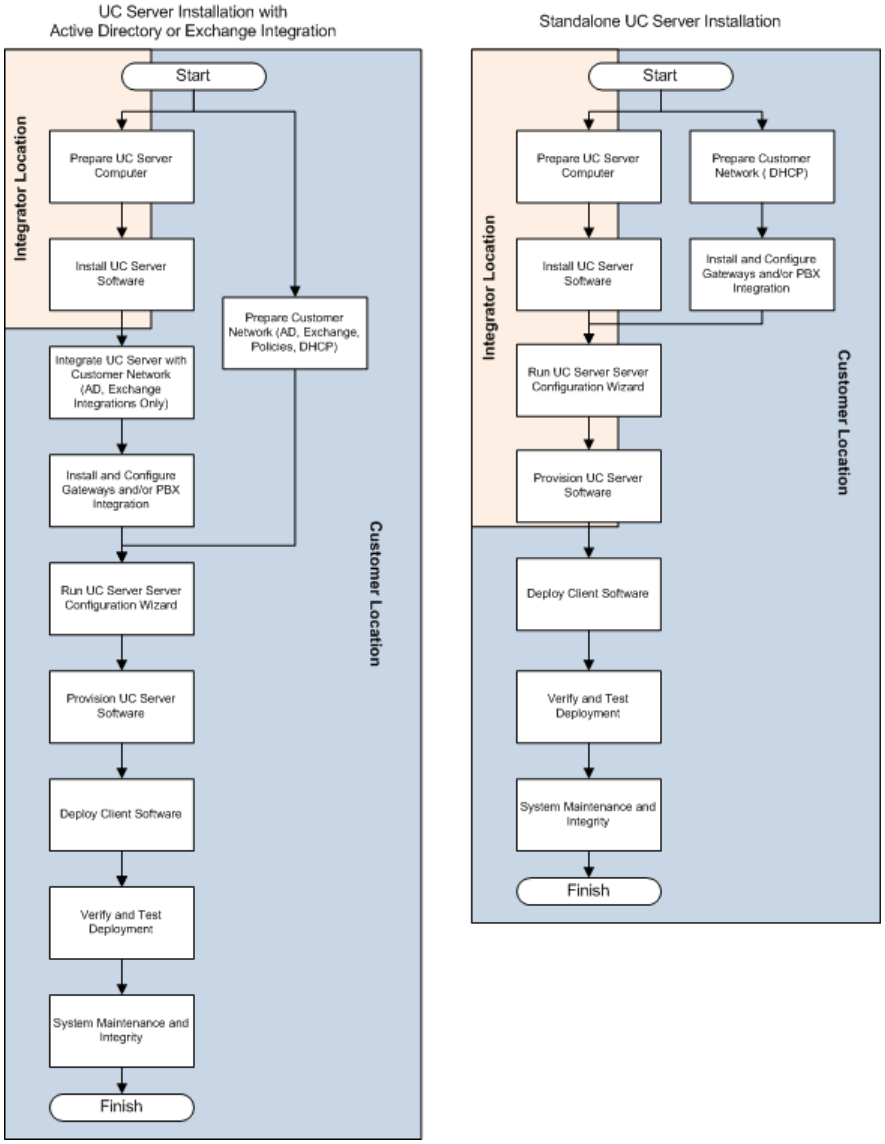
The following steps are involved in the deploying UC Server.

1. Preparing the Customer's Network
2. Preparing the UC Server Computer
3. Installing UC Server Software
4. Integrating UC Server with the Customer's Network
5. Configuring PBX Integration
6. Running the UC Server Configuration Wizard
7. Provisioning UC Server
8. Deploying UC Client
9. Verifying the UC Server Deployment
10. Maintaining System Integrity

If problems occur during the installation and/or provisioning of UC Server, see Troubleshooting.

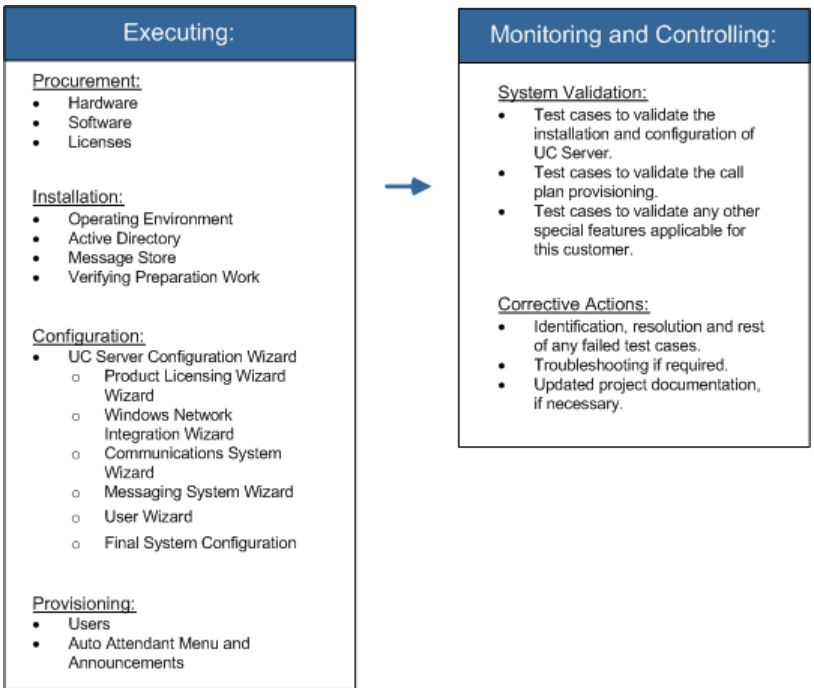
Objectworld customer support may require remote access to the customer's UC Server system. To configure remote access, see Configuring Remote Access.

The steps are meant to be accomplished in the order. However, some tasks can be accomplished independent of others, performed at the integrator's location or at the customer's location. The following illustration shows the deployment steps for both a UC Server deployment integrated with Microsoft Active Directory or Microsoft Exchange Server and a stand-alone UC Server deployment. The steps that exist in both the integrator location and the customer location can be performed at either the integrator's location or the customer's location.



The final section of this chapter documents troubleshooting the most common problems encountered during UC Server installation and provisioning.

The following diagram provides a more detailed view of the activities that must happen during these phases. Note that the specific activities need to be adapted to fit each individual project's needs.



3.1 Planning and Deployment Worksheet

The Planning and Deployment Worksheet is a Microsoft Excel spreadsheet that accompanies this guide, and is available to record the information. It is available as part of the product documentation which can be found on the UC Server installation media or in the Objectworld support area at www.objectworld.com/support/.

The Planning and Deployment Worksheet guides the deployment activities and assists in coordinating information that is required for various steps. It provides a summary of all the steps that need to be performed to successfully complete the UC Server deployment. This worksheet provides space for recording information that is required for various configuration steps (for example, server names and IP addresses) to assist in having that information organized and available. The worksheet also serves as a checklist for the deployment process, enabling the user to document when the steps are completed.

There are several key pieces of information that must be provided as input to the UC Server Configuration Wizard. The worksheet provides space for recording this information so that it is organized and readily available. By completing this worksheet prior to running the wizard, any missing information can be identified and obtained ahead of time. This facilitates a more efficient UC Server configuration.

With preparation, you can minimize the time it takes to add users to the system. The most time consuming installation tasks are adding users and associating SIP telephones to users. To assist you, the Planning and Deployment Worksheet:

- Imports user names, Microsoft Exchange Server mailbox information, and Active Directory information.
- Allows you to configure extension numbers for users. If extension numbers are also included in Active Directory, the worksheet allows you to automatically assign extension numbers to users from Active Directory.

The worksheet runs on a computer that is at the customer's location and can be used as a communication vehicle with the customer. Either you or the customer can modify the worksheet before the installation to remove extraneous users, modify the extension number, and configure SIP telephones.

When the changes to the worksheet are complete, the data can be exported to a format (tab separated file) that can be used directly with the UC Server Configuration Wizard.

3.2 Preparing the Customer's Network

Preparing the customer's network can be done at any point in the deployment process. Depending on the type of deployment, much of this can be done in advance by the customer's IT department.

The following steps must be performed on the customer's network:

- Creating an Active Directory User Account for UC Server
- Preparing the Message Store

Creating an Active Directory User Account for UC Server

You can skip this step if you are not planning to integrate with Active Directory or Microsoft Exchange Server. You can also skip this step if you will log in as a user with the appropriate administrative privileges to the domain, before you run the UC Server Configuration Wizard. In this case, the wizard will automatically create the UC Server service account.

An Active Directory user account must be created for the UC Server service account, and must be done for every UC Server being deployed. The name of the service account needs to be recorded as this information is used by the UC Server Configuration Wizard. The wizard performs the following actions with the service account:

- The UC Server service account is granted the logon right on the Objectworld Application Server service on the UC Server platform.
- The UC Server service account is granted full control on the file system for the directories in which UC Server was installed. By default, the installation path is C:\Program Files\Objectworld.

To manually create an Active Directory user account for UC Server

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. In the left pane, click **Users > Action > New > User**.
3. In the *New User* window, enter the required user account information.

   The *Logon Name* can be **UCServer** or **UCServer1**, or any other name that you choose.
4. Click **Next**.
5. Enter the user password information.
6. Select the **Password Never Expires** option and click **Next**.

7 If you also plan to integrate with the Microsoft Exchange Server, select the **Create an Exchange Mailbox** check box.

This option appears only if the Microsoft Exchange System Manager software is installed on the same platform that is running the Active Directory Users and Computers program.

8 Click **Next**, and then click **Finish**.

Preparing the Message Store

The following message stores are supported by UC Server:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2003 SP1 or later
- Microsoft Exchange Server 2000 Service Pack 2 or later
- IBM Domino Server 6.0.x
- IBM Domino Server 6.5.x
- IBM Domino Server 7.0
- IBM Domino Server 8.0
- University of Washington IMAPd
- Any 100%-compliant IMAP4rev1 (RFC3501) message store (must correctly support searching of message headers otherwise users will be unable to play voice messages over the phone)
- Integrated Messaging
- Local Message Store

The following subsections describe how to prepare each specific message store for UC Server integration. Refer to the section that is applicable to your project.

Microsoft Exchange Server

If the customer's mail server is Microsoft Exchange Server, the following criteria must be satisfied before installing UC Server.

- All UC Servers have a mailbox created on Microsoft Exchange Server for the UC Server service account.
- An Exchange account has been created with privileges granted to it for UC Server to integrate with Microsoft Exchange Server.
- UC Server and Microsoft Exchange Server are in the same Active Directory.
- Each UC Server is integrating directly with only one Microsoft Exchange Server.

Integrating with Microsoft Exchange Server requires user accounts with permissions to access specific folders or mailboxes and carry out particular actions. If the user installing/configuring the software has administrative privileges to the Microsoft Exchange Server, the UC Server Configuration Wizard automatically creates the user accounts, and no additional action is required. It is recommended to complete the following steps prior to using the wizard:

- Creating a Microsoft Exchange Server mailbox for the UC Server service account
- Modifying permissions on Microsoft Exchange Server

NOTE: For more detailed information on UC Server's Microsoft Exchange Server integration technique, network bandwidth requirements or information on remote Microsoft Exchange Server connectivity refer to TN108, "Best Practices for Integrating UC Server with Microsoft Exchange Server" which is available from the Objectworld Web site support area at www.objectworld.com/support/

Creating a Microsoft Exchange Server mailbox for the UC Server service account

Skip this step if you have already created a Microsoft Exchange Server mailbox for the UC Server service account in a previous step.

To create a Microsoft Exchange Server mailbox for an existing account using Windows 2003

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. In the left pane, click **Domain**.
3. Select the **Users** folder.
4. In the right pane, right-click the UC Server account.
5. Select **Exchange Tasks** to start the Exchange Tasks Wizard.
6. From the list of tasks, select **Create Mailbox**.
7. Click **Next**, and then click **Finish**.

Modifying permissions on Microsoft Exchange Server

The UC Server service account uses a separate security context that does not require administrative permissions on the local computer or in the Domain Administrator's Active Directory group.

The UC Server account's administrative privileges are limited to Microsoft Exchange Server mailboxes. The account must access Microsoft Exchange Server user mailboxes in an administrative capacity because it uses them to store and retrieve messages.

To manually set rights and privileges using Microsoft Exchange Server 2007

1. Click **Start > Programs > Exchange Server 2007 > Exchange Management Console**.
2. Navigate to **Microsoft Exchange > Recipient Configuration**.
3. Right-click **Mailbox** and select **New Mailbox**.
4. Select **User Mailbox** and then click **Next**.
5. Select **New user** and then click **Next**.
6. Enter the information for the new user, disable the option **User must change password at next logon**, and then click **Next**.
7. Click **Next** again, and then click **New**.

NOTE: To integrate with Exchange Server 2007, A Microsoft Exchange Server MAPI client be installed on the UC Server platform to permit connection. Objectworld recommends using Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2. Microsoft Outlook 2007 SP2 is not supported.

To run a script if required to grant permissions to the Microsoft Exchange Server 2007 message store from the UC Server service account

NOTE: If you are using Microsoft Exchange Server 2007, then additional steps may be required. If you do not have access to a Windows account with “Server Data Permissions” and Exchange Administrator, then run the script outlined below on the Microsoft Exchange Server 2007 console. The script is required to grant permissions to the Microsoft Exchange Server 2007 message store from the UC Server service account.

- From the Microsoft Exchange Server 2007 console, type the following script replacing `<SERVICE_ACCOUNT>` with the UC Server service account name.

```
Get-MailboxServer | Add-ADPermission -User
<SERVICE_ACCOUNT> -AccessRights GenericRead, GenericWrite -
ExtendedRights Send-As, Receive-As, ms-Exch-Store-Admin
```

To manually set rights and privileges using Microsoft Exchange Server 2003 or Microsoft Exchange Server 2000

1. Click **Start > Programs > Microsoft Exchange > System Manager**.
2. In the left pane of the *Exchange System Manager* window, select the Microsoft Exchange Server that you want to integrate with.
3. Click **Action > Properties** to open the **Exchange Server Properties** window.
4. Click the **Security** tab and then click **Add** to open the *Select Users, Computer or Groups* window.
5. From the **Look In** list box, select each of the following:
   - The Domain name
   - The UC Server account name
6. Click **Add** and then click **OK**.
7. From the **Permissions: Allow Deny** list box, select **Full control and Send As** for the account you just added.
8. Make sure that the **Allow inheritable permissions from parent to propagate to this object** check box is enabled.
9. Click **OK** and then close the *Exchange System Manager* window.

Lotus Notes/IMAP4

If the customer's mail server is Lotus Notes or another IMAP4 mail server, the following criteria must be satisfied before installing UC Server.

- All UC Servers must have an account configured as an IMAP mailbox in Lotus Notes.
- The Mail template file must be modified on the Lotus Notes server to include new forms for displaying voice and fax messages.

Integrated messaging

If the customer is using integrated messaging, there is no further action required to prepare the message store. Integrated messaging requires a user license, and the capability of using integrated messaging must be associated with a user.

Local message store

If the customer is using local message store, there is no further action required to prepare the message store.

3.3 Preparing the UC Server Computer

This section provides an overview of the steps that need to be executed to install and prepare the operating environment for UC Server. The complete operating environment installation involves the installation, upgrade, and/or configuration of the following components:

- Installing and Preparing the Operating System
- Installing the Windows 2003 Server Administration Tools Pack
- Installing MAPI Client for Microsoft Exchange Server Integration
- Disabling 'Install updates automatically'
- Disabling the Indexing Service

The installation and preparation of the UC Server computer can be done either on or off customer premises. From a technical perspective, there are no advantages or disadvantages to either location. However, from a scope management perspective, there are advantages to performing this step away from the customer's premises.

Installing and Preparing the Operating System

You must install UC Server on one of the supported Microsoft operating systems and use a computer platform that meets the requirements for the applications that are to be deployed. For more information, see “Server Requirements” on page 14.

To validate that minimum server OS, service packs/patches and hardware requirements are satisfied

1. Click **Start > Settings > Control Panel > System**.
2. Verify the OS version and service pack level (recommended Windows XP SP2, or Windows 2003 SP1 and above).
3. Verify CPU and memory requirements in accordance to system capacity guidelines. Refer to “Server Requirements” on page 14 for recommended platform configurations.

Limitations and restrictions

This section details the operational limitations of server hardware and software configurations.

- Limitations of using Microsoft Exchange Server and mailbox monitoring
- Do not install UC Client on the same platform as Microsoft Exchange Server and Microsoft Outlook
- Do not change the recovery setting for the Objectworld UC Server Application Service

Limitations of using Microsoft Exchange Server and mailbox monitoring

Mailbox monitoring is a method of synchronizing message waiting lights on phones using Exchange Server to monitor when messages arrive, are read and so on. Using mailbox monitoring enables the synchronization of message waiting lights when messages are accessed through Microsoft Outlook Web Access or through a mobile device.

CAUTION: Performance issues may arise when mailbox monitoring is enabled. On systems with more than 100 users, system design and engineering must consider the increased load that keeping open large numbers of mailboxes will have on the Exchange Server. Enabling monitoring of more than 500 mailboxes requires careful consideration and probably should not be done without a slow roll-out procedure to validate the performance of both Exchange Server and UC Server in the specific customer environment. If your Exchange Server is at or near capacity, then you may want to disable mailbox monitoring.

You can enable or disable mailbox monitoring at the system level when you add or configure Microsoft Exchange Server. You can also set the default for mailbox monitoring for users to on or off. When you add or configure users, you can choose to use the server default, or you can enable or disable mailbox monitoring for individual users.

NOTE: For more information see the *UC Server Administrator Guide*, available from the Objectworld Web site in the support area at www.objectworld.com/support.

Do not install UC Client on the same platform as Microsoft Exchange Server and Microsoft Outlook

The Objectworld voice and fax forms, included as part of the UC Client software installation, do not operate correctly when Microsoft Outlook is installed on the same computer as Microsoft Exchange Server or on a computer that has Microsoft Exchange 2007 Tools. This is a result of a conflict between the Microsoft Exchange and Microsoft Outlook MAPI drivers. Do not install the UC Client software on the following platforms:

- Any platform running both Microsoft Exchange Server and Microsoft Outlook.
- Windows Small Business Server (which includes Exchange Server and Microsoft Outlook).
- Any operating system on which both Terminal services and Microsoft Exchange Server services are operating.

Do not change the recovery setting for the Objectworld UC Server Application Service

The recovery settings for the Objectworld UC Server Application Service must be set to “Take no Action”. Modifying this setting hinders diagnosis of any startup issues, and might result in unnecessary entries being added to the system or application event logs. The other services are set to restart on failure.

Installing the Windows 2003 Server Administration Tools Pack

The Windows 2003 Server Administration Tools Pack allows administrators to install the Windows Server 2003 management tools onto a Windows XP Professional or Windows Server 2003 family of servers to perform remote server management functions. The Windows Server 2003 Administration Tools Pack is required for Active Directory integration and user rights delegation in UC Server. Windows 2003 Server and Windows 2003 Small Business Server automatically include the Windows Administration tools, but Windows XP Professional does not.

If UC Server is installed on a Microsoft Windows XP platform, the Microsoft Administration Pack is installed as part of the UC Server Installation Wizard, provided the wizard can access Microsoft's web site on the Internet.

The Windows 2003 Server Administration Tools pack is only available on Microsoft's web site.

If there is a problem with installing the Windows 2003 Server Administration Tools Pack, you can download it manually. For installation instructions see the *UC Server Installation Guide* available from the Objectworld web site at www.objectworld.com/support.

For more information about the Microsoft Windows Admin Pack, see http://support.microsoft.com/kb/304718 for Microsoft Knowledge base article KB304718.

Installing MAPI Client for Microsoft Exchange Server Integration

If UC Server is integrating with Microsoft Exchange Server, A Microsoft Exchange Server MAPI connector must be installed. Refer to “Microsoft Exchange Server” on page 38 for a list of applicable Microsoft Exchange Server MAPI Connectors that are required to be installed on the UC Server computer.

If UC Server is not integrating with Microsoft Exchange Server you can skip this section.

Disabling 'Install updates automatically'

Objectworld recommends that the Windows operating system have the latest Microsoft Service packs and security patches applied. Objectworld recommends the use of Microsoft Update, which includes updates for all Microsoft products. For instructions on verifying that the latest Microsoft Windows updates have been applied, see the *UC Server Installation Guide* available from the Objectworld web site at www.objectworld.com/support.

Although Objectworld recommends that the UC Server computer platform accept Microsoft updates, it is recommended that automatic Windows Updates be disabled. Some Microsoft Windows updates require a computer restart and temporarily incapacitate UC Server. Updates should instead be scheduled as part of a regular Microsoft Update task to be performed on a regular basis.

To turn off Windows automatic updates

1. Click **Start > Settings > Control Panel > Automatic Updates**.
2. Choose either **Download updates…**, **Notify me…** or **Never check for updates**.

Disabling the Indexing Service

Default installations of Windows Server 2008, Windows Server 2003 and Windows XP enable the Indexing Service. This service is used to improve search speeds on the local system by continually monitoring and indexing files. This can consume a moderate amount of CPU resources. This service is not required or used by UC Server and it therefore should be disabled to improve system performance. Failure to disable the Indexing Service will result in intermittent reduction of system performance.

To turn off the Indexing Service

1. Double-click **My Computer** or open Explorer.
2. Right-click **C:** (do this for all the drives in the system) and select **Properties**.
3. On the **General** Tab, clear the **Allow Indexing Service to index this disk for fast file searching** check box.
4. Click **OK**.
5. Select **Apply changes to C:\, subfolders and files**.
6. Click **OK**.

3.4 Installing UC Server Software

Before running the UC Server Configuration Wizard, ensure that the UC Server platform is connected to a network that can connect to the Internet. An Internet connection is required to install some Microsoft components that are part of the UC Server installation media.

Install the UC Server software by running the UC Server Configuration Wizard. Detailed instructions can be found in the *UC Server Installation Guide*. Running the wizard also allows UC Server to automatically detect the Microsoft Windows minimum requirements, such as service packs and updates.

All the previously described activities involved in installing and preparing the operating environment should be finished prior to starting the UC Server software installation.

NOTE: You can continue to run the UC Server Configuration Wizard only if you have completed the customer network integration.

The following steps are required when integrating UC Server at a customer's location. Many of the steps can be done only at the customer site.

- Incorporating UC Server into the Windows Domain
- Configuring the date and time
- Preparing for domain policies

3.5 Integrating UC Server with the Customer's Network

The UC Server computer platform must be installed on the customer's network. This includes changing the networking information and creating a computer account on the customer's network.

The following steps must be performed:

- Changing the Networking Properties
- Connecting to the Internet
- Configuring the Date and Time

The following steps are conditionally required:

- If integrating UC Server with Active Directory or Microsoft Exchange Server, Incorporating the UC Server Platform into the Windows Domain
- If the domain administrator has created firewall policies, Configuring Windows Firewall Settings
- If certain domain policies exist, Configuring Local Computer Policies

Changing the Networking Properties

You must change the networking properties of the UC Server computer to integrate with the customer's network.

This includes assigning an IP address and computer name. The IP address can be configured as a static IP address or as a DHCP reservation. It is preferred to configure the UC Server computer to use DHCP reservation that reserves a specific IP address on the DHCP server for the UC Server computer.

Ensure that the computer name and DNS server names are configured correctly.

Connecting to the Internet

A public Internet connection is required to retrieve Windows software components, and this connection must be established and verified before UC Server installation begins.

Configuring the Date and Time

Change the date and time according to the UC Server platform's local region.

To change the UC Server platform date and time

1. Click **Start > Control Panel** > **Date and Time**.
2. Change the Date and Time according to the customer's specifications.
3. Change the Time Zone according to the customer's specifications.

Incorporating the UC Server Platform into the Windows Domain

If integrating UC Server with Active Directory or Microsoft Exchange Server, the UC Server platform must be a participating member of a Windows domain to take advantage of Active Directory (single sign-on) and Microsoft Exchange Server integration.

NOTE: You can skip this step if you are not intending to integrate UC Server with Active Directory or Microsoft Exchange Server.

To incorporate the UC Server platform into the Windows domain

1. Click **Start > Control Panel** > **System**.
2. Select the **Computer Name** tab.
3. Click the **Network ID** button.
4. Follow the steps until you have incorporated the UC Server platform successfully.

NOTE: You will be required to enter the username and password of a Windows user that has the ability to create a computer account on the customer's network. Typically this is the domain administrator. Ensure that the Windows Administrator is available to complete this task.

Configuring Windows Firewall Settings

Extra considerations regarding the Windows Firewall settings are only necessary when the domain administrator has created firewall policies on participating computers in Microsoft Windows Active Directory.

UC Server supports the use of the Windows integrated firewall to comply with corporate security and firewall policies. Windows Firewall must be configured appropriately to support the following network applications:

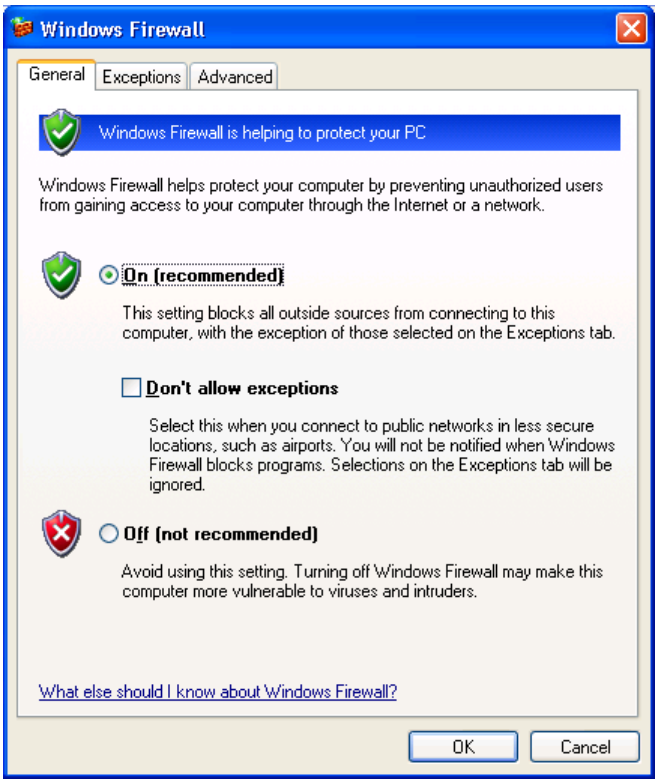
- Automatic discovery and configuration of SIP devices (FTP, TFTP and HTTP)
- General SIP telephony
- Unified communications
- UC Client connections

When configuring the Windows Firewall settings, the current settings must first be verified.

To verify your Windows Firewall settings

1 Click **Start > Control Panel** > **Windows Security Center**.

2 Click **Windows Firewall**.



3 Verify that the **General** tab has one of the following options selected:

- The Windows Firewall is **On**, and **Don't allow exceptions** is disabled.

OR

- The Windows Firewall is **Off**.

4 If the settings in Step 3 are correct for this installation's requirements, continue with this procedure. If the settings in Step 3 are incorrect, select the appropriate setting and then continue with this procedure. If the firewall settings cannot be reconfigured and they need to be, go to step 7.

5 If Windows Firewall is on and exceptions are allowed, then Objectworld UC Server will automatically configure the firewall exceptions.

6 If Windows Firewall is off, no further configuration of Windows Firewall is required.

7 If Windows Firewall cannot be reconfigured (fields are disabled and cannot be changed), you must verify Windows network policies that might prohibit you from changing the Windows Firewall settings. Refer to Validating domain policies for Windows Firewall for information about how to change the Windows Firewall configuration if there is a domain policy restricting the changing of Windows Firewall.

Validating domain policies for Windows Firewall

NOTE: The procedures in this section are only required if it is not possible to configure the Windows Firewall settings.

To verify if the UC Server platform is able to manage the Windows Firewall configuration

1 On the UC Server platform, click **Start > Run**.

2 Type **CMD** to start a Windows command shell.

3 Type **GRPRESULT /Z** to get a list of local policies for the user or computer.

4 With the results from Step 3, ensure the following policy does not exist: `GPO: Restricted Firewall`.

The following excerpt is an example of a computer policy that enforces Windows Firewall behavior and requires corrective action for proper operation of SIP Telephony.

```
Microsoft (R) Windows (R) Operating System Group Policy Result
tool v2.0

Copyright (C) Microsoft Corp. 1981-2001<sections removed for
brevity>

    Resultant Set Of Policies for Computer

    ---------------------------------------

<sections removed for brevity>

    Administrative Templates

    ------------------------

    GPO: Restricted Firewall

    KeyName:
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Enab
leFirewall

    Value:       1, 0, 0, 0

    State:       Enabled

    GPO: Restricted Firewall
```

```
    KeyName:
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\DoNo
tAllowExceptions
                Value:       1, 0, 0, 0
                State:       Enabled
```

NOTE: If the computer has a "GPO: Restricted Firewall" limitation, do the following. If no policy exists, proceed to the next section.

To find the domain policy and values

1. Click **Start > Run**.
2. Type **gpedit.msc** to launch the Group Policy management application.
3. Navigate to **Computer Configuration > Administrative Templates > Network > Windows Firewall > Domain Profile**

   The value of the following policy objects should be:

   - Windows Firewall: **Protect all network connections** set to **Enabled**
   - Change the Windows Firewall: **Do not allow exceptions** set to **Disabled**
   - All other settings for the Windows Firewall set to **Not Configured**
   - **Password must meet complexity requirements** set to **Disabled**
4. If the firewall rules cannot be changed, follow the instructions on how to create group policy exceptions for UC Server in "Configuring Local Computer Policies" on page 72. Re-verify the domain policies once the local computer policies have been modified.

Adding Windows Firewall rules using Windows NETSH

The UC Server Configuration Wizard adjusts Windows Firewall rules automatically.

NOTE: The instructions in this section are only required if you choose to manually configure the Windows Firewall rules.

The following NETSH scripts allow control of the Windows Firewall to be installed on the UC Server platform.

To configure the firewall

1. Click **Start > Run**.
2. Type **CMS** to start a Windows command shell.

3 Copy the following firewall configuration parameters into the Windows Clipboard and paste them into the Windows CMD shell application.

NOTE: The NETSH script below assumes a default UC Server installation path. If the installation path is different for the UC Server platform, change the path to meet your specific requirements.

```
netsh firewall add allowedprogram "C:\Program
Files\Objectworld\UC Server\bin\CAServer.exe" "Objectworld
UC Server Application Services" ENABLE ALL
```

Configuring Local Computer Policies

This section is only required for the following conditions:

- A domain policy exists that prohibits changing the firewall exceptions required for normal operation of UC Server.

If none of these conditions apply, you can skip this section.

If UC Server is being installed on a workstation or domain member server, configure local computer policies by following the instructions below.

- Creating group policy exceptions for UC Server
- Moving UC Server to another organization unit
- Changing the policy for UC Server
- Activating new group policy objects on UC Server

If UC Server is being installed on the same platform as Active Directory Server or Microsoft Windows Small Business Server, configure the Windows Firewall domain policy for UC Server by following the instructions below.

- Changing the Windows Firewall domain policy for UC Server when installed on the same platform as Active Directory Server or Windows SBS

Creating group policy exceptions for UC Server

To create an exception for the UC Server policies

1 Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

2 Right-click the Domain object, select **New > Organizational Unit**.

3 Create a new name for the organizational name (e.g., UC Server Exceptions).

4 Right-click the new organizational unit that you created in the previous step, and select **Properties**.

5 Select the **Group Policy** tab and configure a New Group policy object (e.g., NonComplexPassword).

6 Select **Edit** to change the options.

7 Go to the appropriate group policy object and change the setting to the appropriate value. For the policy to take effect, you might have to enable the "Block Policy Inheritance" option in the Security Policy Management Interface.

Moving UC Server to another organization unit

To move the UC Server platform Windows computer account from the initial Active Directory container

1 Log in as a user with privileges to manage Active Directory.

2 Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

3 Go to the computer account in Active Directory Users and Computers.

4 Right-click the computer name and select **Move**.

5 From the list, select the Organizational unit container that you created in Creating group policy exceptions for UC Server.

Changing the policy for UC Server

Follow the instructions in this section to implement domain policy exceptions.

To change the Windows Firewall domain policy for UC Server

1 Click **Start > Run**.

2 Type **gpedit.msc** to launch the Group Policy management application.

3 Navigate to **Computer Configuration > Administrative Templates > Network > Windows Firewall > Domain Profile**

The value of the following policy objects should be:

- Windows Firewall: **Protect all network connections** set to **Enabled**
- Change the Windows Firewall: **Do not allow exceptions** set to **Disabled**
- All other settings for the Windows Firewall set to **Not Configured**

Activating new group policy objects on UC Server

Group policy objects are replicated automatically. The following instructions allow the domain group policy object to be activated immediately.

To activate the group policy for the UC Server platform

1. Click **Start > Run**.
2. Type **CMD** to start a Windows command shell.
3. Type **GPUPDATE /force** to copy the Domain group policies to the local computer.

Changing the Windows Firewall domain policy for UC Server when installed on the same platform as Active Directory Server or Windows SBS

Follow the instructions in this section when UC Server is installed on the same platform as Active Directory Server or Microsoft Small Business Server. In this case, the local computer policy dictates the policies for the domain.

Make sure that these instructions are applied to the “local computer policy” for the Active Directory or the Windows Small Business Server.

To change the Windows Firewall domain policy for UC Server

1. Click **Start > Run**.
2. Type **gpedit.msc** to launch the Group Policy management application.
3. Navigate to **Computer Configuration > Administrative Templates > Network > Windows Firewall > Domain Profile**

   The value of the following policy objects should be:

   - Windows Firewall: **Protect all network connection**s set to **Enabled**
   - Change the Windows Firewall: **Do not allow exceptions** set to **Disabled**
   - All other settings for the Windows Firewall set to **Not Configured**

3.6 Configuring PBX Integration

If UC Server is integrating with an existing PBX, the correct integration hardware and software must be available for installation. See the applicable PBX integration note for the specific details of installation and configuration available from the Objectworld Support Center.

Refer to the planning section of the list of hardware and software components to integrate with your PBX.

PBX integration can be accomplished by the following methods:

- Dialogic card installed in UC Server
- Dialogic Media Gateway
- TAPI/Wave integration
- Direct SIP connection

Dialogic Card Installed in UC Server

You will require the following references to integrate UC Server with a PBX

- Objectworld PBX Integration Technical Note
- Objectworld UC Server Installation Guide for Dialogic Components

The *UC Server Installation Guide* provides detailed instructions on how to install and configure Dialogic hardware and software components.

The PBX Integration guides can be found with the Objectworld UC Server installation media or available on the support area of our Web site: www.objectworld.com/support/.

The general approach for installation and configuration is as follows:

- Install the Dialogic hardware
- Install and configure the Dialogic software
- Connect the cables between the Dialogic cards and the PBX
- Verify the integration
- This may also require a PBX CTI interface such as TAPI or TSAPI

Dialogic Media Gateway

Dialogic Media Gateways are standalone gateways that interface with PBXs through a variety of techniques.

You will require the following references to integrate Dialogic Media Gateways with a PBX:

- *TN088 - Dialogic Media Gateway Configuration Guide*
- The Dialogic Media Gateway Integration notes for the specific PBX

The TN088 is available with the Objectworld UC Server installation media or available on the support area of our Web site: www.objectworld.com/support/. The Dialogic installation notes area available from the Dialogic Web site (www.dialogic.com)

The general approach for installation and configuration is as follows:

- Install and configure the Dialogic Media Gateway
- Connect the cables between the Dialogic Media Gateway and the PBX
- Verify the integration

TAPI/Wave Integration

TAPI/Wave integration is available for some Avaya IP Office and Cisco CallManager.

You will require the following references to integrate Objectworld UC Server with a PBX:

- The Objectworld Technical Integration Guide for the PBX that you want to integration with TAPI/Wave
- The PBX vendor's installation instructions for the TAPI/Wave driver.

The PBX Integration guides can be found with the Objectworld UC Server installation media or available on the support area of our Web site: www.objectworld.com/support/.

The general approach for installation and configuration is as follows:

- Install and configure the vendor's TAPI/Wave software
- Verify the integration

Direct SIP Connection

The direct SIP connection integration applies to Cisco CallManager.

You will require the following references to integrate Objectworld UC Server with a PBX:

- *TN092 - Cisco CallManager Integration Guide using SIP*
- Cisco documentation for integrating Cisco CallManager with Exchange 2007 Unified Messaging.

The general approach for installation and configuration is as follows:

- Configure Cisco CallManager to support SIP based messaging support
- Verify the integration

3.7 Running the UC Server Configuration Wizard

Verifying the Preparation Work

After all the procedures described in this chapter are complete, it is recommended that you perform some simple verification tests to confirm that everything is set up as required for starting the UC Server Configuration Wizard. If everything is properly configured, the wizard steps run smoothly and efficiently.

NOTE: This verification step is particularly important if the person who is running the UC Server Configuration Wizard is different from the person who performed the preceding preparation work. If the person running the wizard also performed the preparation work, this step is optional.

Before running the UC Server Configuration Wizard, verify that the UC Server platform is connected to the network and has a valid IP address. Complete the Planning and Deployment Worksheet with all the relevant information.

Verification Checklist

Verify the following before optionally creating an authorization store, and then running the UC Server Configuration Wizard.

- ☐ Verify that the UC Server has a valid IP address and DNS server
- ☐ Verify that the UC Server computer can access the Internet
- ☐ If integrating with Active Directory or Microsoft Exchange Server, verify that a service account has been configured
- ☐ If integrating with Microsoft Exchange Server, verify the Exchange mailbox has been created and that the UC Server service account has permission granted to the Microsoft Exchange Server store
- ☐ Verify the domain policies for Windows Firewall configuration

Creating an Authorization Store to Enable Active Directory Roles

Creating an authorization store is an optional step that applies to UC Server installations that are integrated with Active Directory. You can skip this step if you are configuring UC Server as stand-alone.

The authorization store is typically created prior to running the UC Server Configuration Wizard.

The following conditions must be satisfied in order to create an authorization store:

- The UC Server computer platform must be integrated with customer’s network.

- The UC Server Active Directory account must already be created on the customer's domain.
- The user creating the authorization must be authenticated with the domain.

If users were already created prior to creating an authorization, the administrator must assign a role to each configured Windows user. Users added after the authorization store is created have a default role "Standard User" assigned to their user profile.

To create an authorization store

1. Log in to the UC Server computer as a domain administrator.
2. Click **Start > Run**.
3. Type **CMD** to launch a CMD window.
4. Navigate to the UC Server installation directory **\Objectworld\UC Server\bin**
5. Type **manageazman +createxmlstore +admin <DOMAIN>\<UC SERVER SERVICE ACCOUNT>**.
6. Stop and restart the UC Server application service.
   a. Open the service control panel application.
   b. Restart the service named **Objectworld UC Server Application Services**.

NOTE: You can create the customer authorization store at any time; before, during or after installation. However, any Active Directory users and their associated authentications will have to be modified to include a role from the role list. Consult the *UC Server Administrator Guide* for details on how to change the authentication role for individual user authentications.

Running the UC Server Configuration Wizard

There are eight steps to the UC Server Configuration Wizard, each of which must be run in order. Subsequent wizard steps become available only after the previous wizard(s) are successfully completed.

1. Product Licensing Wizard
2. Windows Network Integration Wizard
3. Communication Systems Wizard
4. Phone Types Wizard
5. Gateway Wizard
6. Messaging Systems Wizard
7. User Wizard

8 Final System Configuration

For detailed instructions about completing the UC Server Configuration Wizard in your specific environment, refer to the *UC Server Configuration Guide*, available on the installation media or on the support area of our Web site: www.objectworld.com/support/.

3.8 Provisioning UC Server

After you successfully run the UC Server Configuration Wizard, the functioning UC Server system is able to process incoming and outgoing calls. You will next provision UC Server with users and auto attendants.

The following sections provide basic information about the steps that you need to do and guidance for implementing these steps. Complete, detailed UC Server administration procedures are provided in the *UC Server Administrator Guide*, available from Objectworld's support area at www.objectworld.com/support. The specific procedures depend on the customer's system design and vary for each installation.

Users

Users include administrators, utility phones, hunt groups and ring groups. For an installation that is integrating with Active Directory and Microsoft Exchange Server, accounts for all users on the system should be imported from a text file, Active Directory or Microsoft Exchange Server when UC Server is configured. If the accounts were successfully imported, user accounts and profiles do not need to be setup again unless there is a new user being added to the system. To add additional users manually you can use UC Client or Active Directory plug-in.

Auto Attendants

Auto attendants are created using services within the service environment in UC Client.

There are six general steps to create auto attendant services.

1. Defining behavior for services
2. Creating custom folders and shared folders
3. Recording announcements
4. Configuring database data sources
5. Building the service
6. Activating and associating a service to an identity

Basic details about each of these steps are provided in the following subsections. Detailed information can be found in the *UC Server Administration Guide*.

Defining behavior for services

The most critical part of the auto attendant menu is defining the purpose and behavior of the service. You will want to include a high-level menu tree definition and actions when somebody makes a selection. When defining the service you must also ensure that you address all possible failure conditions.

A thorough understanding of the service environment and the capabilities of the service environment will allow you to model an existing behavior or even come up with some new ideas on how to improve incoming call handling and improve the customer's business operations.

UC Server provides many default service samples that you can modify and customize.

Creating custom folders and shared folders

Create a folder for the services in the Services Editor and create a folder for the announcements in the Announcements Editor. Opening each new folder and then creating the new services and announcements allow for the services and announcements to be populated with the custom data defined for the customer's system.

Additionally, you will want to set up shared folders, which are an effective way of sharing services, announcements and corporate templates, such as fax cover pages. The administrator can manage the information in the shared folder and regular users can access that information. However, regular users cannot edit information contained in the shared folder.

Recording announcements

Announcements are the outgoing messages that callers hear when they call into an auto attendant. These announcements typically initiate the call flow in a service and guide the caller through the call process. The system administrator is usually responsible for managing announcements and incorporating them into the services assigned to identities.

Before recording announcements it is always a good idea to write down the script for the announcement. This reduces the amount of time it takes to record an announcement.

The customer has to choose whether they want the announcements to be professionally recorded, assign someone internally to record the announcements or have the integrator record the announcements. Announcements can be recorded using either the computer microphone (provided the computer being used has a sound card) or an associated telephone.

Audio can be recorded when creating a service, or can be recorded in advance and then imported. Professionally recorded announcements are imported using the Import/Export Wizard that is explained in the *UC Server Administrator Guide*.

Configuring database data sources

If you are planning to use databases in a service, you must define the data sources before using them in a service. If the data source is an ODBC database, you must also define the ODBC data source on the UC Server computer platform in advance.

You can define a data source as either a personal table or as an ODBC data source.

Building the service

Services are made up of elements that are linked together to create the call flow that was designed with the customer during planning. The service can be simple with as little as one or two elements, or it can contain many elements.

While building the service it is important to verify the behavior of the service. Pay particular attention to failure conditions to ensure that the service does not accidentally hang-up on a caller. The service can be associated with test identity to allow testing and verification.

The elements are available on the tool palette of the Service Editor. They are divided into three categories: standard, advanced, and database. The standard and advanced elements are always available. The database elements are available only if the system is licensed for database integration. The elements that are available are summarized in the following tables.

Table 3–1: Standard elements

Element name	Description
Hang Up	Terminates the call.
Play One Time Message	Allows you to leave a personalized message for a specific caller.
Play Announcement	Plays a pre-recorded announcement to callers.
Menu	Allows callers to make a selection using the telephone keypad.
Flow Control	Controls the call flow according to phone number or time and day conditions.
Dial by Extension	Allows callers to select an extension and be transferred to it.
Dial by Name	Allows callers to dial and be transferred to a user's extension by entering the user's name on the telephone keypad.
Voice Mail	Provides basic voice mail service.
Deliver Messages	Delivers voice or fax messages from a selected mailbox to a specified number.
Transfer Call	Transfers the call to another number or extension.
Assisted Transfer	Allows call transfer recipients to accept or deny calls based on the caller's recorded name.
Notify Pager	Enables you to send a message to a pager number.
Send E-mail	Allows you to be notified by e-mail when a caller moves successfully through the Send E-mail element.
Send Fax	Allows you to send a list of faxes.
Receive Fax	Receives a fax and places it in a mailbox.
Fax-on-demand	Captures a caller's number and faxes the selected document to the caller.

Table 3–2: Advanced elements

Element name	Description
Select Extension	Waits for callers to enter an extension number using the telephone keypad; can be used for selecting mailboxes.
Record Announcement	Allows callers with user accounts to record over an existing announcement using a remote telephone.
Take Message	Triggers the recording of an incoming message for storage to a mailbox.
Advanced Menu	Allows callers to make a selection using the telephone keypad.
Manage Mailbox	Allows callers to retrieve messages remotely.
Change Mailbox Password	Allows users to change their mailbox password.
Verify Password	Allows the service to request a password from callers and ensure that a given password matches a specified one or the password for a particular mailbox.
Loop Counter	Allows you to limit the number of times the call flow executes a path in the call flow.
Text to Speech	Reads text to the caller.
Gather Digits	Allows users to keep track of information that is entered by callers.
Compare Data	Allows users to compare patterns of data and directs call flow accordingly.
Create Log Entry	Allows users to capture and export detailed call log entry information.

Table 3–3: Database elements

Element name	Description
Fetch Data	Accesses the specified data source and fetches the required data.
Dial for Data	Accesses the specified data source and fetches the data specified by the caller.
Add Data	Allows a caller to add data to a specified data source.
Delete Data	Allows a caller to delete data from a specified data source.
Update Data	Updates the data contained in a specified data source.
Move Current Row	Allows callers to modify which row is the current row in a multi-row set, retrieved by either Fetch Data or Dial for Data elements.
Prompt for Current Row	Using a series of prompts, allows callers to use the keypad to select which row becomes the current row.

After you build a service, it is recommended that you validate it. The Service Editor inspects the service for errors. If problems are found with the service design, the element will be highlighted and a a message box appear describing the nature of the error.

Activating and associating a service to an identity

Once the service has been built and tested, the service can be activated by associating it to one or more identities.

3.9 Deploying UC Client

UC Client facilitates unified communications, and must be installed for:

- Viewing messages with Microsoft Outlook
- Viewing messages with Lotus Notes
- Managing voice and fax messages with the integrated messaging client
- Allowing users to customize their UC Client environment

UC Client can be deployed by installing it on each client from the UC Server installation media. It can also be deployed using Active Directory, once UC Server has been established as an Active Directory user with the appropriate permissions. Copy UC Client software to a shared directory. Users can then install or upgrade the software from the shared directory, or you can use a group policy to deploy the software.

Copying UC Client Software to a Shared Directory

To copy UC Client software to a shared directory

1. Create a directory and copy the contents of the installation media to that directory.
2. Set the file and directory permissions to allow users to install the software.
3. Share the directory to the users and/or groups to whom you want the software distributed.

Using the Shared Directory

To have users install UC Client software from the shared directory

- Notify the users to install or upgrade UC Client by accessing the file share.

Using a Group Policy

To create a group policy

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Ensure that you are connected to the domain where you want to create the new policy. If you are not connected to the correct domain, follow the steps below.
   a. Right-click **Active Directory Users and Computers**.
   b. Select **Connect to Domain**.
   c. Enter the name of the domain where you want to distribute the client software and click **OK**.
3. Right-click the domain and select **Properties**.
4. Select the **Group Policy** tab.
5. Click **New** and enter the name for the new policy (i.e. **Objectworld Client Distribution**) and press **Enter**.
6. Click **Edit**.

   The *Group Policy Object Editor* window opens. Use **Computer Configuration** to set the policy for all computers in the group, regardless of who is logged in. This approach is typically used. Alternately, you can use **User Configuration** to set the policy for all users in the group, regardless of what computer they are using.
7. Expand **Computer Configuration > Software Settings**.
8. Right-click **Software Installation** and select **New > Package**.
9. Browse to the directory you created in Copying UC Client Software to a Shared Directory.

   When browsing for the client .msi file, the path to the .msi file must be represented as a UNC path (for example, "\\server1\clientsoftware\Objectworld Unified Communications Client.msi"). You must not select the file while browsing the local machine. Clients attempting to reference a local path will get an error, because the file does not exist locally.
10. Select the .msi file for the client software and click **Open**.
11. Select **Advanced** and click **OK**.
12. Once the next window appears, select the **Deployment** tab.
13. Under *Deployment Type*, select **Assigned**. This option is already selected by default, but must be reselected to enable the *Install this application at logon* check box.

14 Select the **Install this application at logon** check box and click **OK**.

This saves the changes and returns you to the *Group Policy* tab of the *Domain Policy Properties* window.

To apply the group policy

1 Select the policy.

2 Click **Properties**. The *Distribution Properties* window opens.

3 Select the **Security** tab.

4 Select a group, user, or computer that you want to apply the policy to. If the group that you want to apply the policy to is not in the list, click **Add** and follow the instructions to add the new group.

5 Select the **Read** and **Apply Group Policy** check boxes.

6 Click **Apply** to save the changes and click **OK** to close the policy *Distribution Properties* window.

7 Click **OK** again to save the changes and return to the Active Directory Users and Computers console.

3.10 Verifying the UC Server Deployment

After the UC Server installation, configuration, and provisioning activities are complete, the execution phase of the UC Server implementation project is finished. The final step in the project, prior to beginning the closure activities, is to verify the UC Server deployment.

The deployment verification involves a number of test cases designed to validate the UC Server installation and configuration, and the call plan provisioning. The results of these tests provide the necessary information to establish that the project deliverables satisfy the acceptance criteria agreed upon with the customer.

During these test cases, any found issues must be resolved and the test case done again.

The details of each suite of test cases must be tailored to meet the unique requirements of each UC Server project and the specific acceptance criteria established with each individual customer. The primary goal of the deployment verification testing is to gather sufficient data to demonstrate to the customer that the installed system meets their requirements and expectations. These test results are important input for securing customer acceptance and sign-off on the project deliverables. At a minimum, there needs to be a one-to-one mapping of test case and acceptance criterion.

The following list provides some examples of areas that might require validation testing.

- Are all incoming DID numbers routed as expected?
- Can outbound calls be placed?
- Do extensions work properly?
- Do toll restrictions work as designed?
- Does the entire auto attendant menu function exactly as designed?
- Have time of day conditions been correctly set?
- Are emergency calls routed properly?
- Can e-mails be retrieved using a phone?
- Are voice mail messages appearing properly in e-mail inboxes?
- Are faxes being sent and received properly?
- Do dial-by-name and dial-by-extension work properly?
- Do hunt groups and/or ring groups function properly?
- Does call queuing function properly?
- Can teleworkers access the network?

Verifying the Message Store

Microsoft Exchange Server

If the message store is Microsoft Exchange Server, confirm that the message store is configured properly by verifying that Microsoft Outlook is installed and that the service account can access Microsoft Exchange Server mailboxes.

To verify the Microsoft Outlook installation

1. Log onto the UC Server system with the service account.
2. Start Microsoft Outlook.

   If Outlook has not been run on this server before, you must follow the instructions to create a profile.
3. Send a message to the service account mailbox and verify that it is received.

To verify that the service account can access Microsoft Exchange Server mailboxes

1. Log onto the UC Server system with the service account.
2. Start Microsoft Outlook.

   If Outlook has not been run on this server before, you must follow the instructions to create a profile.
3. Access another user's mailbox by doing the following from the Outlook toolbar.
   a. In the **File** menu, click **Open > Open Other User's Folder**.
   b. Select **Inbox** and any user's Inbox from the menu.
4. View the content of the user's inbox. This confirms that the service account has permission to access mailboxes on Microsoft Exchange Server.

Lotus Notes or IMAP4

If the message store is Lotus Notes or IMAP4, confirm that the message store is configured properly by testing the IMAP4 connection with Lotus Notes, verifying the username and password, listing the mail directories, and then logging out.

To test the IMAP4 connection with Lotus Notes

1. Log in to the UC Server computer as a domain administrator.
2. Click **Start > Run**.
3. Type **CMD** to launch a CMD window.

4 Type **Telnet <LOTUS NOTES SERVER> 143**.

The IMAP4 server should respond with:

```
* OK Domino IMAP4 Server Release 7.0 ready Tue, 24 May 2005
14:21:25-0400
```

NOTE: IMAP servers treat the backspace key as a valid ASCII character. If you make a mistake during the following steps, start a new line number and type more carefully. Each interaction with the IMAP server must begin with a unique identifier. In this example, sequential numbers starting from 1 are used.

5 Type **1 login "<LOTUS NOTES USERNAME>" <INTERNET PASSWORD>**.

The IMAP4 server should respond with:

```
1 OK LOGIN completed.
```

If the server responds with the following error message, you entered the wrong username and/or password. Verify the information on the Lotus Notes server and repeat this step.

```
NO LOGIN invalid username or password
```

6 Type **2 list "*"**.

The IMAP4 server should respond with a list of mail directories on the Lotus Notes server:

```
*LIST (\HasNoChildren) "\\" Drafts
*LIST (\Noinferiors\HasNoChildren) "\\" "Sent Items"
*LIST (\Noinferiors\HasNoChildren) "\\" Trash
2 OK LIST completed
```

7 Type **3 logout**.

The IMAP4 server should respond with:

```
*BYE logging out
3 OK LOGOUT completed
```

3.11 Maintaining System Integrity

Antivirus Software

If it is necessary due to corporate policy to have antivirus software on the UC Server platform, make sure that it is configured to not interfere with the regular operation of UC Server.

CAUTION: Objectworld has observed that third-party firewall and antivirus products can cause problems with the proper operation of UC Server. If a problem occurs, Objectworld Technical Support advises that third-party products be removed from the system prior to contacting Technical Support.

Excluding folders from antivirus scanning

For performance reasons, the following UC Server folders must be excluded from antivirus software scanning. The default folder locations for new installations are listed below. Note that the folder locations may differ on your installation if they were not saved to the default locations:

The default location of the application:

- C:\Program Files\Objectworld

The default location of the software log files:

- C:\OWLogs

The default location of the database folder:

- C:\Program Files\Microsoft SQL Server

NOTE: UC Server is tested with Microsoft security products, such as Windows Firewall and Windows Defender.

Backup and Restore Procedures

Overview

Backup and restore procedures protect UC Server data. The key objectives are to minimize downtime and provide the quickest possible data recovery in the event of a database corruption, system crash, or other forms of data loss.

Protecting the UC Server databases requires careful thought and planning to meet the availability needs of the Service Level Agreements (SLAs) in your company and its budget.

Regarding data protection, the higher the requirement for availability, the higher the cost to achieve data protection. Availability solutions rely on data protection, and choosing a reliable backup product must be thought out carefully.

Below are some basic backup and restore procedures using the built in backup utilities that come with Microsoft Windows Server 2008, Microsoft Windows Server 2003, and the included scripts. If you are currently using or planning to use different backup software, make sure that it supports Microsoft Volume Shadow Copy Services (VSS) to back up open files and is capable of backing up the databases live.

It is also important to note that the Windows Server 2003 backup procedure in this document demonstrates how to back up and restore UC Server data only. You must have a full backup and restore plan in the event of a server failure. In the case of complete data loss on a server, you can reinstall UC Server on another server and restore the latest available UC Server data, as mentioned in the restoration procedures below.

Regardless of your established backup and restore plan for failure recovery, it should be thoroughly tested and documented in a simulated environment using production backups. Testing helps to ensure that you have the required backups to recover from various failures, and that your procedures can be executed smoothly and quickly if a real failure occurs.

CAUTION: Use of the UC Server platform as a backup server is not recommended due to the risk that the backup server may consume all available disk storage, resulting in the loss of UC Server data and the possibility of an unrecoverable failure of UC Server.

Backups using Other Applications

If you are planning to use another application to back up UC Server data, make sure that the backup software supports the following features:

- Ability to back up open files and/or support Microsoft VSS (Volume Shadow Copy Services)
- Ability to back up file permissions, service account permissions, and system state information
- Ability to back up the database live

Below are the specific UC Server data components and related items to back up in addition to your regular scheduled backups:

- Folders
  - C:\Program Files\Objectworld\UC Server\Data
- Database
  - All databases on the %computername%\OBJECTWORLD SQL Server instance.

If your backup procedures involve stopping the SQL Server (OBJECTWORLD) service, the following services are dependent on it, and will be stopped as well.

- Objectworld UC Server SIP Service Manager
- Objectworld UC Server SIP Management Server
- Objectworld UC Server SIP Back-to-Back User Agent
- Objectworld UC Server SIP Media Relay
- Objectworld UC Server SIP Call Router
- Objectworld UC Server Database Access

These services are required for proper operation of UC Server SIP Edition, and will need to be started after the procedure in addition to SQL Server (OBJECTWORLD) in order for UC Server to function properly.

Backup Procedures

Accessing the Backup Scripts

1. Locate the **Utility\Scripts** folder.
2. Create the folder **C:\Backup** if it does not already exist on the UC Server machine.
3. Copy the **Backup** and **Restore** folders into the **Backup** folder created in the previous step.

The following sections describe how to perform a full UC Server backup for the various supported Windows operating systems. Follow the steps in the section that corresponds to the operating system for the UC Server machine.

- Windows Server 2008
- Windows Server 2003

Windows Server 2008

The backup utility included with Windows Server 2008 is significantly different from the *ntbackup* utility used with previous versions. It no longer has the ability to backup specific files and folders, only entire volumes. Because of this, the backup destination must be a second hard drive, either internal or external, or a network location with enough storage space. To prevent potential capacity problems, the hard drive used should be dedicated to storing the backup.

1. If the backup utility has not yet been installed, follow the lettered steps.

   If it has been installed, proceed to step 2.

   a. Open a command prompt.
   b. Type **servermanagercmd.exe -install Backup-Features**
   c. Click **OK** then wait until it is finished.

2. Open a text editor.
   a. To store the backup on a network share type:
   wbadmin start Backup -backupTarget:\\remotestorageserver\Backup\ -include:c: -vssFull -quiet
   b. To store the backup to a internal hard, external hard or DVD drive, type:
   wbadmin start Backup -backupTarget:e: -include:c: -vssFull -quiet

CAUTION: If you save a backup to a remote shared folder, that backup will be overwritten if you use the same folder to back up the same computer again. In addition, if the backup operation fails, you may end up with no backup because the older backup will be overwritten, but the newer backup will not be usable. To avoid this, you can copy the backup files to another location such as a DVD or a different network location.

NOTE: Backups on DVDs can only be used for complete volume restoration.

NOTE: If you are using any other backup solution in addition to this, remove "-vssFull" as it can interfere with other backup solutions.

NOTE: Replace "c:" with the volume containing UC Server.

TIP: It is recommended that the backup not be written to an internal hard drive. A removable hard drive or a network share is a more reliable solution.

3. Save the file as a batch file named **backup<Volume being backed up>to<destination>.bat**; make a note of where you saved it.

   Example: BackupCtoE.bat

4. Click **Start > Administrative Tools > Task Scheduler**.
5. Click **Create Basic Task**.
6. Create a name and description and then click **Next**.
7. Select the type of schedule that meets your backup needs and then click **Next**.
8. Configure the schedule to meet you backup needs and then click **Next**.

NOTE: It is best to schedule it to run when the system is unlikely to be used, such as the early morning hours as the backup process consumes enough system resources to reduce service quality, depending on the server configuration.

9. Select **Start a program** and then click **Next**.
10. Click **Browse**, navigate to the location of the batch file, select it, click **Open**, and then click **Next**.

11 Click **Finish**.

Windows Server 2003

Backing up UC Server Files

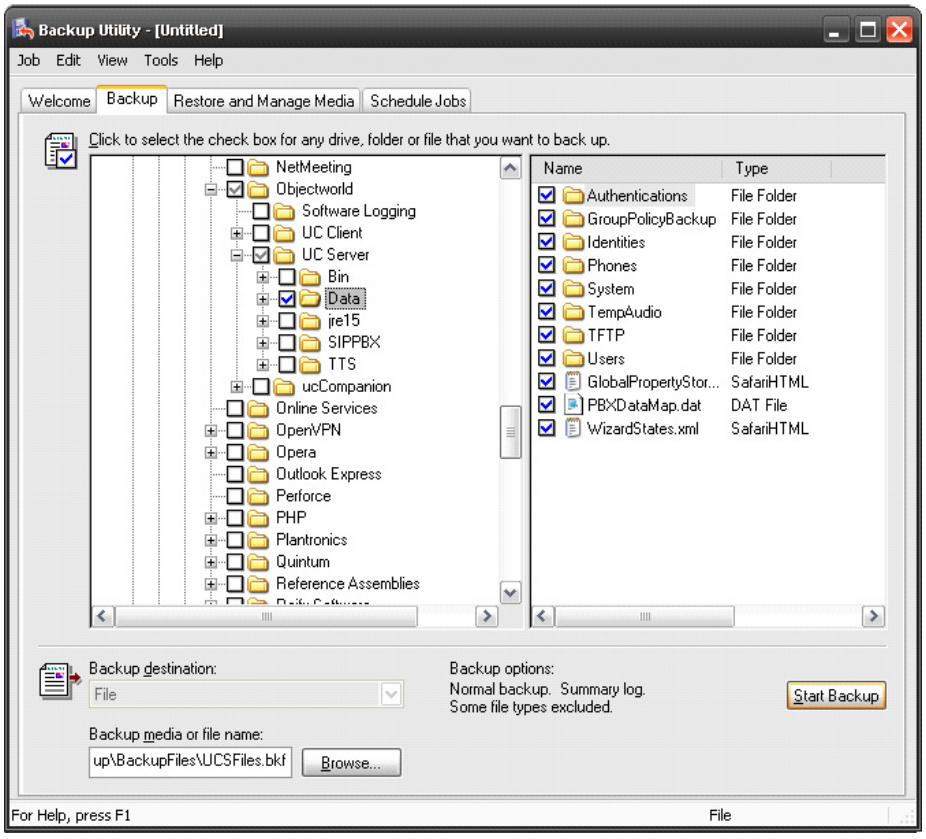
All versions of Microsoft Windows Server 2003 and Microsoft Windows XP Professional include a backup utility called *ntbackup* that you can use to back up your UC Server.

To launch the backup program

1 Click **Start > Programs > Accessories > Systems Tools > Backup**. If this is the first time you are running the Backup utility, the backup wizard automatically launches.

2 Click **Advanced Mode**, and then select the **Backup** tab.

Depending on your company backup policy and SLA agreement, you may want to perform a full backup of UC Server weekly in addition to a daily incremental backup.



3 Select the folders.

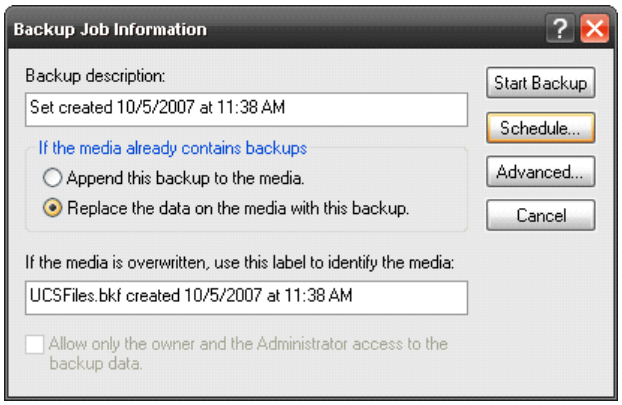
- **C:\Inetpub\ftproot**
- **C:\Program Files\Objectworld\UC Server\Data**

NOTE: If you installed UC Server to a different directory other than the default location, select the appropriate directory.

4 Click the **Browse** button to select the location where you want to save the backup file.

5 Enter the name of the backup file and click **Save**.

6 Click **Start Backup**.



NOTE: The UC Server files should be written to reliable online storage on another server or removable media on the UC Server platform that is removed after each backup.

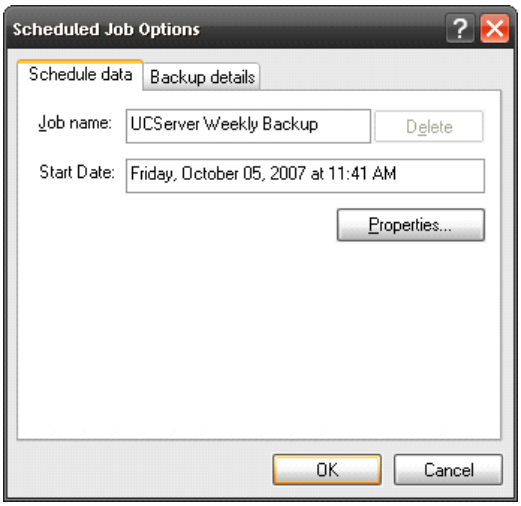
NOTE: The Microsoft Backup tool does not support backing up directly to a CD/DVD burner. To back up to a CD/DVD drive, you must first back up to another location and write the file to a CD/DVD using the software that came with the drive. For instructions about how to write to a CD/DVD drive, refer to the user's guide that came with your drive.

7 Decide whether you want *ntbackup* to append the backup to an existing file, or to replace the previous backup and click **Schedule**.

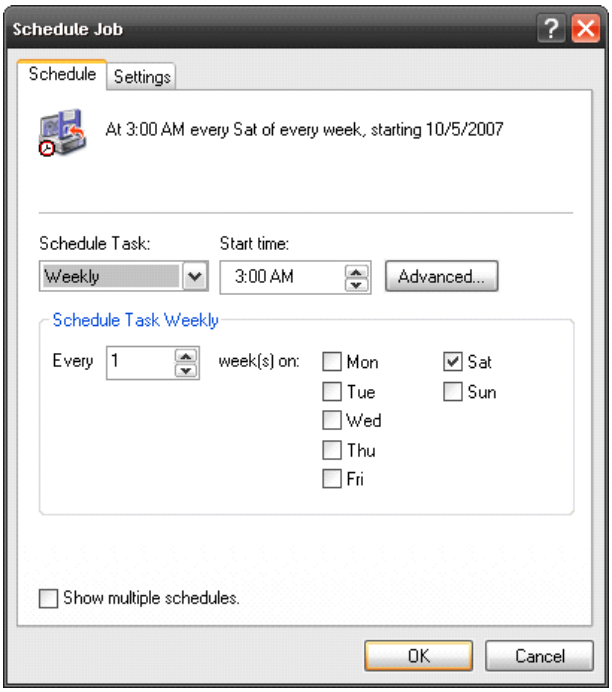
NOTE: If you want to use a backup type other than "Normal", click **Advanced** and select another type of backup.

8 When *ntbackup* prompts you to save your current selections, click **yes**. Name and save the file. When prompted for account information, insert the user name and password of an account with appropriate permissions to read and write the files to the backup location.

9 Enter a job name, and then click **Properties**.



10 Set up the schedule to meet your backup needs, and then click **OK**.



NOTE: A weekly schedule provides a low level of protection, and any changes made after the backup are lost if the backup is used. Daily backups provide more protection, but require more space if multiple backups are kept. To reduce the space required, a weekly "Normal" backup and daily "incremental" backups can be used. The level of protection needed varies greatly between companies, so it is best to follow your company's backup policy.

11 In the *Scheduled Job Options* window, click **OK**. The job is now scheduled and can be viewed and tested from the "Scheduled Tasks" folder, which can be accessed from the Control Panel. To test the job, right-click it and select **Run**. This produces a backup file immediately so you do not have to wait for the first occurrence of the schedule.

Backing up the UC Server Database

1 Click **Start > Control Panel**.

2 Open the **Scheduled Tasks** folder.

3 Right click, select **New > Scheduled Task** and name the new task.

4 Double-click the new scheduled task.

5 In the **Run** box, enter: **cmd /C Backup_Objectworld_Database.bat "C:\Backup\BackupFiles\"**

NOTE: The database backup files should be written to reliable online storage on another server or removable media on the UC Server platform that is removed after each backup.

6 In the **Start in** box, enter: **"C:\Backup\"**

Where "C:\Backup\" is the location where **Backup_Objectworld_Database.bat** and **BackupObjectworldDatabase.sql** are.

7 Select the **Schedule** tab.

8 Configure the schedule to match that of the file backup.

9 Click **OK**.

10 Enter a user name and password that have appropriate permissions to run the backup batch file and sqlcmd command, and then click **OK**.

11 In the Scheduled Tasks folder right-click the task you have just created and select run. The database backup files will be created.

Restore Procedures

The following sections describe how to restore UC Server for the various supported Windows operating systems. Follow the steps in the section that corresponds to the operating system for the UC Server machine.

- Windows Server 2008
- Windows Server 2003

Windows Server 2008

File or Database Corruption

If announcements, services, dial plans, identities, users, and so on are corrupted, accidently deleted or modified, then you can restore UC server and its database to its previous condition by following these steps.

1. Ensure the media the backup data is stored on is accessible by the server.
2. Click **Start > Run** and type **C:\Program files\Objectworld\UC Server\StopAllUCServerServices.bat**.

NOTE: If UC Server is on a different drive, change C: accordingly.

3. Click **Start > Administrative Tools > Server Manager**.
4. Select **Windows Server Backup**, under **Storage** on the left.
5. Select **Recover** on the right.
6. Select **This server(servername)** and click **Next**.
7. Select the backup date and time to restore the data from and click **Next**.
8. Select **Files and folders** and click **Next**.
9. Navigate to and select the Program files folder in the section on the left.
10. In the section on the right, click the **Microsoft SQL Server** folder, then hold **Ctrl** and click the **Objectworld** folder.
11. Click **Next**.
12. Select **Original location, Overwrite existing files with recovered files, Restore security settings**, and click **Next**.
13. Click **Recover**.
14. Once it is finished, click **Close**.
15. Click **Start > Run** and type **C:\Program files\Objectworld\UC Server\StartAllUCServerServices.bat**.

Total Server Reconstruction

If the computer UC Server resides upon has ceased to work completely, such as a drive failure, a serious operating system error, or theft, these steps will restore UC Server as well as the operating system.

If you are restoring to a new drive, it must be at least as large as the capacity of the media the backup is stored upon. For example, if 45GB of backup data was on an 80GB portable hard drive, the new hard drive must be at least 80GB in size or larger.

Note: To restore to different server hardware, you must contact Objectworld Technical Support to obtain a new license key for your new installation. Also, if a different MAC address is being used, change the settings in the DHCP server to ensure the new server has the same IP address as the old server.

1. Place the Windows Server 2008 startup disk into the CD or DVD drive and boot the computer.
2. Select the appropriate language settings and click **Next**.
3. Click **Repair your computer** in the bottom left of the window.
4. If you are restoring to the original drive, it will be displayed here. Click **Next**.

NOTE: You may need to click Load Drivers to load the appropriate drivers depending on the server's configuration.

NOTE: If you are restoring to a new drive, click Next.

5. Select **Windows Complete PC Restore**.
6. To restore from a backup stored on an internal or external hard drive:
   - Select **Use the latest available backup** and click **Next** or
   - Select **Restore a different backup**, click **Next**, and follow the prompts until asked to **Choose how to restore the backup**.
7. To restore from a backup stored on a network store:
   a. Select **Restore a different backup** and click **Next**.
   b. Click **Advanced**.
   c. Click **Search for a backup on the network**.
   d. Enter the complete path to the folder holding the backup files and click **OK**. Example: \\StorageServer\BackupFiles\20080924\
   e. Enter your login information and click **OK**.
   f. Select the location that has appeared in the list and click **Next**.
   g. Select the backup to restore and click **Next**.
8. If there are any disks that you do not want to have reformatted, click **Exclude disks**, select the drive to exclude and click **OK**.
9. Check that everything is correct. If it is not, click **Back** until you reach the right page to correct it.
10. When it is correct, navigate forward to the final page, and click **Finish**.
11. Confirm the actions and click **OK**.

12 If the restoration was performed on different server hardware, you will need to provide the new license key obtained from Objectworld Technical Support to UC Server.

   a Open UC Client using credentials with access to the Admin account.
   b Click **Help > License Information**.
   c Click **Modify License**, enter the new license and click **OK**.
   d Close UC Client.
   e Click **Start > Run**, type **c:\Program Files\Objectworld\UC Server\RestartAllUCServerServices.bat**, and click **OK**.

Windows Server 2003

The following procedures assume that your UC Server data is corrupted; however, if there is a complete data loss or corruption in UC Server, you must perform one of the following steps before proceeding to restore UC Server data in Restoring UC Server Files and then Restoring the UC Server Database.

NOTE: If you are restoring on a new server, it is required that the new server have the same version of Windows as the old server.

NOTE: To restore to different server hardware, you must contact Objectworld Technical Support to obtain a new license key for your new installation.

A) Restore the server operating system and UC Server application from your backup tapes. After restoring the server, go to Restoring UC Server Files to restore the most recent UC Server data.

or

B) Install the server operating system and the same version and build of UC Server that was previously installed, including the presence components if they were installed previously. After installing the server, follow the Configuration wizard. Add just one user, and finish the wizard. Go to Restoring UC Server Files to restore the most recent UC Server data.

Accessing the Restore Scripts

1 Locate the **Utility\Scripts** folder.

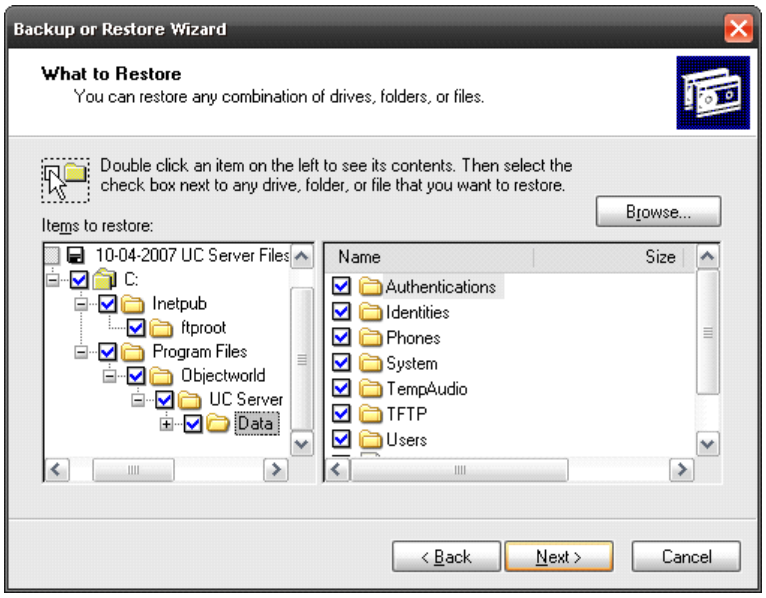
2 Create the folder **C:\Restore** if it does not already exist on the UC Server machine.

3 Copy the **Backup** and **Restore** folders into the **Restore** folder created in the previous step.

   The scripts for the restore procedures are in the Restore folder.

Restoring UC Server Files

1. Click **Start > Programs > Accessories > Systems Tools > Backup** to launch the Backup utility from Microsoft.
2. Click **Next**.
3. Select **Restore Files and Settings**, and click **Next**.
4. A list of backup histories displays. If the backup file is not listed, click **Browse** and find the backup file. Select the desired backup data to restore and click **Next**.



5 If *Existing files* says *Do not replace*, click **Advanced** and then **Next**, and then select the **Replace existing files** radio button. Click **Next**. *Existing files* now says *Always replace*. Click **Finish**.

6 Contact Objectworld Technical Support to obtain a new license key if you are restoring to different server hardware than the existing server. Refer to UC Server Configuration documentation to install your new license key.

Restoring the UC Server Database

1 Click **Start > Run**.

2 Enter **cmd** and click **OK**.

3 Navigate to where **RestoreDatabases.bat** is located.

4 Enter **RestoreDatabases.bat "C:\Backup\BackupFiles\"**

Where "C:\Backup\BackupFiles\" is the folder where the database backup files are located.

3.12 Troubleshooting

This section provides some information and guidance for the most common problems that are encountered during the installation and provisioning of UC Server.

NOTE: It is recommended that, if problems arise during the installation and/or provisioning of UC Server, this section be referred to first to determine if the problem and solution are documented here prior to seeking additional technical support.

Microsoft Exchange Server Problems and Solutions

Server log error

Problem: If you receive the following error in the Server log, the mailbox you are attempting to connect to is either hidden from the Global Address List or the UC Server application service account does not have permissions to access the mailbox.

```
2006-11-28 11:55:17.733 0000094c:00000758 CAServer ?ExchMgr
DEBUG_TRACE (M?ExchangeManager::UpdateMAPIProfile) After
?ConfigureMsgService(), hRes=0x81002746
```

Solution: Follow the steps listed below.

To get the <UCSERVER_SERVICE> account

1. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services** > **Objectworld UC Server Application**.
2. Click the **Logon** tab.
3. Note the entry in **This Account.**

To get the <EXCHANGE_MAILBOX> mailbox display name

1. Open UC Server client.
2. Navigate to **Servers**.
3. Right-click the configured Exchange Server and select **Open**.
4. Note the entry in **Mailbox Name**.

To check that the mailbox display name is correct

1. Navigate to **Active Directory Users and Computers** > **<YOUR DOMAIN>** > **Users**.
2. Right-click **User <EXCHANGE_MAILBOX>** and select **Properties**.
3. Click the **General** tab.

4 Ensure the **Display Name** matches <EXCHANGE_MAILBOX>.

To check that the mailbox is not hidden

1 Navigate to **Active Directory Users and Computers** > **<YOUR DOMAIN>** > **Users**.

2 Right-click **User <EXCHANGE_MAILBOX>** and select **Properties**.

3 Click the **Exchange Advanced** tab.

4 Clear the **Hide from Exchange address lists** check box.

5 Click **OK**.

To check the application service account has the appropriate rights to the Account

1 Navigate to **Active Directory Users and Computers** > **<YOUR DOMAIN>** > **Users**.

2 Right-click **User <EXCHANGE_MAILBOX>** and select **Properties**.

3 Click the **Security** tab.

4 Select the **<UCSERVER_SERVICE>** account from the *Name* window.

5 Under **Permissions**, give **Allow access** to the **Read**, **Write**, **Receive As** and **Send As** entries.

To check that the Exchange Global Address is updated with the <EXCHANGE_MAILBOX>

1 On any client computer, open Outlook with any user connected to Exchange Server.

2 Navigate to **Action** > **New Message**.

3 In the *To:* box, type the name **<EXCHANGE_MAILBOX>**.

4 Click the **Check Names** icon.

To check that the profile on the UC Server has the correct mailbox (with Outlook installed)

1 Click **Start** > **Control Panel** > **Mail**.

2 Click **Show Profiles**.

3 Select **MS Exchange Settings**.

4 Click **Properties**.

5 Click **E-mail Accounts**.

6 Select **View or Change Existing Accounts**.

7 Click **Next**.

8 Select **Microsoft Exchange Server**.

9 Click **Change**.

10 Ensure the **User Name** matches <EXCHANGE_MAILBOX>.

To check that the profile on the UC Server has the correct mailbox (without Outlook installed)

1 Log on to the UC Server Windows computer with the <UCSERVER_SERVICE> account.

2 Click **Start > Run**.

3 Type **regedit**.

4 Navigate to **HKEY_CURRENT_USER\Software\Microsoft\Windows NT\?CurrentVersion\Windows Message Subsystem\profiles\Outlook**.

Application log error - A?DsOpenObject

Problem: If you see the following message in the Application log, an error has been generated with A?DsOpenObject:

```
0x8007203A maps to ERROR_DS_SERVER_DOWN constant.
```

```
2007-06-28 17:41:30.704 000014e8:00001564 CAServer
?ActiveDirSearch DEBUG_TRACE (?SearchActiveDirectory) Domain
'kml.local'. searchPath . filter
'(&(objectclass=User)(|(name=ucAdmin)(userPrincipalName=ucAdmi
n)(displayName=ucAdmin)(cn=ucAdmin)(sAM?AccountName=ucAdmin)))
'. 2007-06-28 17:41:31.747 000014e8:00001564 CAServer
?ActiveDirSearch DEBUG_HIGH (GetGCSearch) A?DsOpenObject for
Global Catalogue failed (domain 'k'): 0x8007203a
```

An error can be caused by several reasons:

- The LDAP server is down.
- The DC server is too busy to respond to the call and causes a timeout which the client may interpret as the server not being available.
- There are DNS name resolution errors, which means a name is not resolvable using DNS.

Solution: Try connecting to port 389 on the Domain Controller for that computer. Replace <DNSNAMEOFDOMAINCONTROLLER> with the DNS name of the intended domain controller.

- Type **telnet <DNSNAMEOFDOMAINCONTROLLER> 389**.

Application log error - Loss of Microsoft Exchange Server connections

Problem: Finding loss of Microsoft Exchange Server connections within the Application log.

Solution: Within the log, the verification process proceeds as follows during a failure (note that the error code may vary).

```
CAServer MsgMgrThread      DEBUG_HIGH (Process) Performing
periodic operation

CAServer      ExchMgr     DEBUG_TRACE
(MExchangeManager::VerifyConnection) Entering

CAServer      ExchMgr         WARNING
(PrepareAddressBookTableForQuery) Failed to set restriction on
table, hr=0x80040115, ignoring and continueing

CAServer      ExchMgr         WARNING
(MExchangeManager::CanReadFromAddressBook) Unable to retrieve
rows from the address book (hr=0x80040115)

CAServer      ExchMgr         WARNING
(MExchangeManager::VerifyConnection) Failed to read from
address book
```

A failed verification results in a reattempt to connect to the Exchange Server, as indicated by the following log message.

```
CAServer      ExchMgr     DEBUG_TRACE
(MExchangeManager::Connect) Entered
```

A successful connection results in the following log message.

```
CAServer      ExchMgr     INFORMATION
(MExchangeManager::ReconnectMailSystem) Reconnected to
Exchange server
```

3.13 Configuring Remote Access

Objectworld's support organization requires that remote access to UC Server be available to help provide technical support after the customer has transitioned to managed services.

Windows XP Professional and Windows 2003 Server include a built-in Remote Desktop application that allows connectivity to the computer on which they reside. Remote access is preferable through a TCP/IP connection, but can also be made using a modem connection.

Use the following sections to help you configure either remote access through the public Internet or a modem.

Allowing Remote Desktop Connection to UC Server

To enable UC Server as a Remote Desktop host

1. Right-click **My Computer** on the desktop and select **Properties**.
2. Select the **Remote** tab.
3. Enable the **Allow users to connect remotely to this computer** check box.

   A warning message appears about the configuration of Internet connection sharing and/or a personal firewall, which must be configured to allow such Remote Desktop connections.

   If you use a router to connect to the Internet, and the UC Server platform is behind a firewall, you might need to configure the firewall to allow the Remote Desktop connection to the server: you need to forward Remote Desktop Port 3389 to your UC Server platform.

   If Windows XP Service Pack 2 (SP2) is installed on the server and you enable Remote Desktop, Windows Firewall is automatically configured to allow Remote Desktop connections to your computer. However, Remote Desktop does not work if you have Windows Firewall configured to allow no exceptions.

To allow exceptions in Windows Firewall

1. Click **Start > Control Panel > Security Center > Windows Firewall**.
2. Clear the **Don't allow exceptions** check box.

Allowing Incoming Connections to UC Server via Modem

Follow these steps if you have a modem connected to an external analog telephone line. Follow the modem manufacturer's instructions to install the modem software.

To configure UC Server to accept incoming connections

1. Click **Start > Control Panel > Network and Internet Connections > Network Connections**.
2. In the **Network Tasks** section, click **Create a new connection** to start the New Connections Wizard.

   The first time you start the New Connections Wizard, the *Location Information* window appears, requesting country or region, area code and, if necessary, a carrier code and an outside access number. You also need to indicate whether your phone system uses tone or pulse dialing. After entering this information, click **OK**.
3. Click **Next**.
4. On the *Network Connection Type* window, select **Set up an advanced connection**, and then click **Next**.
5. On the *Advanced Connection Options* page, select **Accept incoming connections**, and then click **Next**.

   This allows other computers to connect to your Windows XP Professional-based computer through the Internet, a phone line, or a direct cable connection.
6. On the *Devices for Incoming Connections* page, select your modem to use for incoming connections, and then click **Next**.
7. On the *Incoming Virtual Private Connection* page, select **Allow virtual private connections**, and then click **Next**.

   This enables a virtual private connection so that another computer can use the Internet or another public network to access your computer. For this to work, your computer must have a known name or an IP address on the Internet.
8. On the *User Permissions* page, enable the **Administrator** check box, or click **Add** for each new user you want to add.
9. Click **Next**, which specifies the name of each user you permit to access your computer.
10. On the *Networking Software* page, enable the check box for each type of networking software that you want to enable for incoming connections.

    All is selected by default.
11. Click **Next**, and then click **Finish**.

Remote Access Considerations for WAVE Audio Devices

CAUTION: Mapping remote computer sound to local computer when using Windows Remote Desktop may cause WAVE audio devices to stop working.

UC Server can integrate with existing communications systems using TAPI/Wave audio devices. Ensure that the remote audio mapping is disabled for a client computer that wishes to manage UC Server using a Windows Remote Desktop connection.

To configure Remote Desktop connections to leave sound at remote computer

1. Launch remote desktop connection using Start > All Programs > Accessories > Remote Desktop Connection.
2. Click Options.
3. Select the Local Resources tab.
4. Change the Remote computer sound configuration is set to Leave at remote computer.

4 Index

Numerics

A

B

C

D

E

F

G

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Objectworld™

308 Legget Drive
Ottawa, Ontario
K2K 1Y6 Canada

Voice: (613) 599-9698
Fax: (613) 599-7457