



MITEL

# UNIFIED COMMUNICATOR ADVANCED

**ADMINISTRATOR GUIDE  
ISSUE 6.0 SP1  
NOVEMBER 2013**

### Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

### Trademarks

Mitel® is a registered trademark of Mitel Networks Corporation.

Inter-Tel® is a registered trademark of Inter-Tel (Delaware), Incorporated.

VMware, VMware vMotion, VMware vCloud, VMware vSphere, VMware Horizon View, ESX, and ESXi are trademarks of VMware Incorporated.

All other trademarks mentioned in this document are the property of their respective owners, including Mitel Networks Corporation. All rights reserved.

®, ™ Trademark of Mitel Networks Corporation  
© Copyright 2013, Mitel Networks Corporation  
All rights reserved

## Emergency Call Services Support Legal Disclaimers

When used in a remote location, UC Advanced with the embedded softphone is not suitable for providing reliable access to call for emergency services (for example, 911, 999 or 112). See the following warnings.

---

**WARNING: FAILURE OF A SERVER RESULTS IN THE INABILITY OF THAT SERVER'S UC ADVANCED SOFTPHONES TO OPERATE AND PLACE CALLS, INCLUDING EMERGENCY CALLS. A SERVER FAILURE WOULD NOT AFFECT THE FUNCTIONALITIES OF A DESK PHONE.**

---

### English

---

**WARNING: MITEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT THE SOFTWARE WILL PERMIT OR ALLOW YOU ACCESS TO EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES (IN THE APPLICABLE TERRITORY WHERE THE SOFTWARE IS USED). MITEL FURTHER DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT, IN THE EVENT SUCH ACCESS IS AVAILABLE, THE SOFTWARE WILL RELAY ACCURATELY OR AT ALL, THE DEVICE IDENTIFICATION NUMBER OR PHONE NUMBER (ALSO KNOWN AS AN AUTOMATIC NUMBER IDENTIFICATION (ANI) OR CALLBACK) OR THE LOCATION (ALSO KNOWN AS AUTOMATIC LOCATION INFORMATION (ALI)) YOU ARE CALLING FROM, TO THE APPROPRIATE EMERGENCY RESPONSE CENTER (ALSO KNOWN AS A PUBLIC SAFETY ANSWERING POINT (PSAP)). MITEL RECOMMENDS THAT THE SOFTWARE NOT BE USED IN CONNECTION WITH OR TO UTILIZE EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES.**

---

### Dutch

---

**WAARSCHUWING: MITEL WIJST ALLE EXPLICIETE EN IMPLICIETE GARANTIES EN VERKLARINGEN AF DAT DEZE SOFTWARE GESCHIKT IS VOOR HET VERKRIJGEN VAN TOEGANG TOT TELEFONISCHE HULPDIENTEN ALS 911, 999 EN 112 OF SOORTGELIJKE TELEFONISCHE HULPDIENTEN (AANWEZIG IN HET GEBIED WAAR DEZE SOFTWARE WORDT GEBRUIKT). MITEL WIJST VOORTS ELKE EXPLICIETE OF IMPLICIETE GARANTIE OF VERKLARING AF DAT WANNEER DERGELIJKE TOEGANG WEL WORDT VERKREGEN HET IDENTIFICATIENUMMER VAN HET TOESTEL OF HET TELEFOONNUMMER (OOK BEKEND ALS AUTOMATIC NUMBER IDENTIFICATION (ANI) OF TERUGBELNUMMER) OF DE LOCATIE WAAR VANDAAN U BELT (OOK BEKEND ALS AUTOMATIC LOCATION INFORMATION (ALI)) CORRECT EN IN ALLE GEVALLEN WORDT DOORGEGEVEN AAN HET JUISTE HULPDIENTSCENTRUM (OOK BEKEND ALS OPENBAAR ALARMNUMMER (PSAP)). MITEL RAADT U AAN DE SOFTWARE NIET TE GEBRUIKEN VOOR VERBINDINGEN MET HULPDIENTEN ALS 911, 999 OF 112 OF SOORTGELIJKE TELEFONISCHE HULPDIENTEN.**

---

## French (Canadian)

---

**AVERTISSEMENT : MITEL DÉCLINE TOUTE AUTRE GARANTIE EXPRESSE OU IMPLICITE OU REPRÉSENTATION QUE LE LOGICIEL PERMETTRA L'ACCÈS AUX APPELS DE SERVICES D'URGENCE, COMME LE 911/999/112 OU AUTRES SERVICES D'APPELS D'URGENCE SIMILAIRES (DANS LE TERRITOIRE APPLICABLE OÙ LE LOGICIEL EST UTILISÉ). MITEL DÉCLINE ÉGALEMENT TOUTE AUTRE GARANTIE EXPRESSE OU IMPLICITE OU REPRÉSENTATION QUE, DANS LE CAS OÙ L'ACCÈS À CES SERVICES SERAIT DISPONIBLE, LE LOGICIEL TRANSMETTRA PRÉCISÉMENT, S'IL LES TRANSMET, LE NUMÉRO D'IDENTIFICATION DE L'APPAREIL OU LE NUMÉRO DE TÉLÉPHONE (ÉGALEMENT CONNU SOUS LE NOM D'ENREGISTREMENT AUTOMATIQUE DU NUMÉRO [ANI] OU RECOMPOSITION AUTOMATIQUE) ET L'EMPLACEMENT D'OÙ VOUS APPELEZ (ÉGALEMENT CONNU SOUS LE NOM D'ENREGISTREMENT AUTOMATIQUE DE L'EMPLACEMENT [ALI]) AU CENTRE D'INTERVENTIONS D'URGENCE APPROPRIÉ (ÉGALEMENT CONNU SOUS LE NOM DE POINT DE RÉPONSE DE SÉCURITÉ PUBLIQUE [PSAP]). MITEL RECOMMANDE DE NE PAS UTILISER CE LOGICIEL POUR RECOURIR À DES SERVICES D'APPELS D'URGENCE TEL QUE 911/999/112 OU À TOUT AUTRE SERVICE D'URGENCE SIMILAIRE.**

---

## French (European)

---

**AVERTISSEMENT : MITEL NE VOUS GARANTIT AUCUNEMENT, DE FAÇON EXPRESSE OU TACITE, NI NE DECLARE QUE LE LOGICIEL VOUS PERMETTRA OU VOUS AUTORISERA A ACCEDER A DES SERVICES D'APPEL D'URGENCE, TELS LE 911/999/112 OU SERVICES D'APPEL D'URGENCE SIMILAIRES (PROPRES AU TERRITOIRE SUR LEQUEL LE LOGICIEL EST UTILISE). MITEL NE VOUS GARANTIT EN OUTRE EN AUCUN CAS, DE FAÇON EXPRESSE OU TACITE, NI NE DECLARE, QUE MEME DANS L'EVENTUALITE OÙ UN TEL ACCÈS SERAIT POSSIBLE, LE LOGICIEL RETRANSMETTRA PRECISEMENT OU INTEGRALEMENT LE NUMERO D'IDENTIFICATION DE L'APPAREIL OU LE NUMERO DE TELEPHONE (FONCTION DITE D'IDENTIFICATION AUTOMATIQUE DU NUMERO (EAN) OU DE RAPPEL) OU LE SITE A PARTIR DUQUEL VOUS APPELEZ (IDENTIFICATION AUTOMATIQUE DU SITE), AU CENTRE DE REPONSE D'URGENCE CONCERNE. MITEL VOUS RECOMMANDE DE NE PAS UTILISER LE LOGICIEL DANS LE CADRE DE OU POUR APPELER DES SERVICES D'URGENCE, TELS LE 911/999/112 OU SERVICES D'APPEL D'URGENCE SIMILAIRES.**

---

## German

---

**WARNUNG: MITEL SCHLIESST ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEEN AUS UND BEHAUPTET NICHT, DASS DIE SOFTWARE DEN ZUGRIFF AUF NOTRUFDIENSTE WIE 911/999/112 ODER ENTSPRECHENDE NOTRUFDIENSTE (JE NACH VERWENDUNGSGEBIET DER SOFTWARE) ERMÖGLICHT. WEITERHIN SCHLIESST MITEL SÄMTLICHE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEEN AUS UND BEHAUPTET NICHT, DASS DIE SOFTWARE IM FALLE EINES MÖGLICHEN ZUGRIFFS DIE GERÄTEIDENTIFIKATIONSNUMMER ODER TELEFONNUMMER (AUCH BEZEICHNET ALS „AUTOMATISCHE RUFNUMMERNIDENTIFIZIERUNG“ (ANI) ODER „RÜCKRUF“) ODER DEN STANDORT DES ANRUFERS (AUCH BEZEICHNET ALS „AUTOMATIC LOCATION INFORMATION“ (ALI)) EXAKT ODER ÜBERHAUPT AN DIE ENTSPRECHENDE NOTRUF-ZENTRALE ÜBERMITTELN WIRD. MITEL EMPFIEHLT, DIE SOFTWARE NICHT IN VERBINDUNG MIT ODER FÜR NOTRUFDIENSTE WIE 911/999/112 ODER ÄHNLICHE NOTRUFDIENSTE ZU VERWENDEN.**

---

## Italian

---

**AVVERTENZA: IN NESSUN CASO, MITEL SARÀ RESPONSABILE PER LA VIOLAZIONE DI QUALSIASI GARANZIA O CONDIZIONE ESPRESSA DEI SERVIZI DI EMERGENZA AI QUALI IL SOFTWARE CONSENTIRÀ DI ACCEDERE, AD ESEMPIO 113/112/118 O SERVIZI SIMILI PER CHIAMATE DI EMERGENZA (ALL'INTERNO DEL TERRITORIO IN CUI VIENE UTILIZZATO IL SOFTWARE). INOLTRE, MITEL NON FORNISCE ALCUNA GARANZIA CHE, IN CASO DI TALI ACCESSI, IL SOFTWARE TRASMETTA CORRETTAMENTE IL NUMERO DI IDENTIFICAZIONE DEL DISPOSITIVO O IL NUMERO DI TELEFONO ANI (AUTOMATIC NUMBER IDENTIFICATION, IDENTIFICAZIONE AUTOMATICA DEL NUMERO O RICHIAMATA) O LA POSIZIONE ALI (AUTOMATIC LOCATION INFORMATION, IDENTIFICAZIONE AUTOMATICA POSIZIONE) DALLA QUALE SI STA CHIAMANDO AL CENTRO DI RISPOSTA EMERGENZE (PUBLIC SAFETY ANSWERING POINT, PUNTO PSAP). MITEL CONSIGLIA DI NON UTILIZZARE IL SOFTWARE CON CONNESSIONI A SERVIZI PER CHIAMATE DI EMERGENZA, AD ESEMPIO 112/113/118 O SERVIZI PER CHIAMATE DI EMERGENZA SIMILI.**

---

## Portuguese

---

**AVISO: A MITEL NÃO OFERECE NENHUMA GARANTIA OU REPRESENTAÇÃO, EXPRESSA OU IMPLÍCITA, DE QUE O SOFTWARE IRÁ PERMITIR O ACESSO A SERVIÇOS DE CHAMADA DE EMERGÊNCIA COMO O 911/999/112 OU OUTROS SERVIÇOS DE CHAMADA DE EMERGÊNCIA SEMELHANTES (NO TERRITÓRIO APLICÁVEL ONDE O SOFTWARE É UTILIZADO). A MITEL TAMBÉM NÃO OFERECE NENHUMA GARANTIA OU REPRESENTAÇÃO, EXPRESSA OU IMPLÍCITA, DE QUE, NO CASO DE TAL ACESSO ESTAR DISPONÍVEL, O SOFTWARE IRÁ TRANSMITIR, OU FAZÊ-LO DE FORMA PRECISA, O NÚMERO DE IDENTIFICAÇÃO DO DISPOSITIVO OU NÚMERO DE TELEFONE (TAMBÉM DESIGNADO POR IDENTIFICAÇÃO AUTOMÁTICA DE NÚMERO (ANI: AUTOMATIC NUMBER IDENTIFICATION) OU CHAMADA DE RETORNO) OU A LOCALIZAÇÃO (TAMBÉM DESIGNADA POR INFORMAÇÃO AUTOMÁTICA DE LOCALIZAÇÃO (ALI: AUTOMATIC LOCATION INFORMATION)) DE ONDE ESTÁ A LIGAR, PARA O CENTRO DE RESPOSTA DE EMERGÊNCIA APROPRIADO (TAMBÉM DESIGNADO POR PONTO DE ATENDIMENTO DE SEGURANÇA PÚBLICA (PSAP: PUBLIC SAFETY ANSWERING POINT)). A MITEL RECOMENDA QUE O SOFTWARE NÃO SEJA UTILIZADO EM LIGAÇÃO COM OU PARA UTILIZAR SERVIÇOS DE CHAMADA DE EMERGÊNCIA, TAIS COMO O 911/999/112 OU SERVIÇOS DE CHAMADA DE EMERGÊNCIA SEMELHANTES.**

---

## Spanish (Latin American)

---

**ADVERTENCIA: MITEL RECHAZA TODA GARANTÍA EXPRESA O IMPLÍCITA O REPRESENTACIÓN DE QUE EL SOFTWARE AUTORIZARÁ O LE PERMITIRÁ TENER ACCESO A SERVICIOS DE LLAMADAS DE EMERGENCIA, COMO 911/999/112 O SERVICIOS DE LLAMADA DE EMERGENCIA SIMILARES (EN EL TERRITORIO CORRESPONDIENTE DONDE SE UTILIZA EL SOFTWARE). MITEL TAMBIÉN RECHAZA TODA GARANTÍA EXPRESA O IMPLÍCITA O REPRESENTACIÓN QUE, EN CASO QUE DICHO ACCESO ESTÉ DISPONIBLE, EL SOFTWARE TRANSMITIRÁ EN FORMA EXACTA O POR COMPLETO EL NÚMERO DE IDENTIFICACIÓN DEL DISPOSITIVO O NÚMERO TELEFÓNICO (TAMBIÉN CONOCIDO COMO IDENTIFICACIÓN AUTOMÁTICA DE NÚMERO (ANI) O DEVOLUCIÓN DE LLAMADA) O LA UBICACIÓN (TAMBIÉN CONOCIDA COMO INFORMACIÓN AUTOMÁTICA DE UBICACIÓN (ALI)) DESDE DONDE USTED REALIZA LA LLAMADA AL CENTRO DE RESPUESTA DE EMERGENCIA CORRESPONDIENTE (TAMBIÉN CONOCIDO COMO PUNTO DE CONTESTACIÓN DE SEGURIDAD PÚBLICA (PSAP)). MITEL RECOMIENDA QUE EL SOFTWARE NO SE UTILICE JUNTO CON NI PARA USAR SERVICIOS DE LLAMADAS DE EMERGENCIA, COMO 911/999/112 O SERVICIOS DE LLAMADAS DE EMERGENCIA SIMILARES.**

---

## Spanish (European)

---

**ADVERTENCIA: MITEL SE EXIME DE TODA RESPONSABILIDAD O REPRESENTACION EXPRESA O IMPLICITA ACERCA DE QUE EL SOFTWARE LE PERMITA ACCEDER A SERVICIOS DE LLAMADAS DE EMERGENCIA, COMO LAS 911/999/112 O SIMILARES (EN EL TERRITORIO EN CUESTION EN EL QUE SE UTILICE DICHO SOFTWARE). ASIMISMO, MITEL SE EXIME DE TODA RESPONSABILIDAD O REPRESENTACION EXPRESA O IMPLICITA ACERCA DE QUE, EN EL CASO DE QUE ESTE ACCESO ESTE DISPONIBLE, EL SOFTWARE BRINDE CON NINGUN GRADO DE FIABILIDAD, EL NUMERO DE IDENTIFICACION DEL DISPOSITIVO O NUMERO DE TELEFONO (TAMBIEN LLAMADO IDENTIFICACION AUTOMATICA DEL NUMERO, ANI, O DE DEVOLUCION DE LLAMADA), O LA UBICACION (TAMBIEN LLAMADA INFORMACION AUTOMATICA DE UBICACION, ALI) DESDE LA QUE LLAMA, AL CENTRO DE RESPUESTA DE EMERGENCIAS CORRESPONDIENTE (TAMBIEN CONOCIDO COMO PUNTO DE RESPUESTA DE SEGURIDAD, PSAP). MITEL RECOMIENDA QUE NO UTILICE EL SOFTWARE JUNTO CON O PARA UTILIZAR SERVICIOS DE LLAMADAS DE EMERGENCIA, COMO LAS DE 911/999/112 O SIMILARES.**

---





Emergency Call Services Support Legal Disclaimers. . . . .	iii
English . . . . .	iii
Dutch . . . . .	iii
French (Canadian) . . . . .	iv
French (European) . . . . .	iv
German . . . . .	v
Italian . . . . .	v
Portuguese . . . . .	vi
Spanish (Latin American) . . . . .	vi
Spanish (European) . . . . .	vii

## Chapter 1: Overview

Introduction . . . . .	3
About This Guide . . . . .	3
Audience . . . . .	3
Terminology . . . . .	4
Features, Enhancements, and Changes . . . . .	5
MiVoice for Lync . . . . .	5
Google Integration . . . . .	6
Basic Unified Communication (UC) Client . . . . .	6
UC Advanced Mobile for iPad and iPhone enhancements . . . . .	6
UC Advanced Mobile for Android enhancements . . . . .	6
UC Advanced Mobile for BlackBerry enhancements . . . . .	6
Web Portal Enhancements . . . . .	6
UC Server Changes . . . . .	7
Server and Client Components. . . . .	8
UC Server . . . . .	8
Desktop Client . . . . .	10
MiVoice for Lync Client . . . . .	11
Web Portal . . . . .	12
UC Advanced Mobile for BlackBerry . . . . .	13
UC Advanced Mobile for Android . . . . .	14
UC Advanced Mobile for iPad . . . . .	15
UC Advanced Mobile for iPhone . . . . .	15

Supported Communication Platforms (PBXs) . . . . .	16
Mitel Integrated Applications . . . . .	16
Optional Third-Party Integrated Applications . . . . .	17
Documentation . . . . .	18

## Chapter 2: Features

Introduction . . . . .	23
Server-Level Features . . . . .	27
Federation . . . . .	27
Peering . . . . .	29
Client Interface Features . . . . .	32
Desktop Client Features . . . . .	32
MiVoice for Lync Features . . . . .	37
Web Portal Features . . . . .	37
UC Advanced Mobile for BlackBerry Features . . . . .	39
UC Advanced Mobile for Android Features . . . . .	40
UC Advanced Mobile for iPad Features . . . . .	42
UC Advanced Mobile for iPhone Features . . . . .	43
Communication Platform Features . . . . .	44
MCD Features . . . . .	44
Mitel 5000 Communication Platform Features . . . . .	50
Inter-Tel Axxess Features . . . . .	53
About Account Synchronization . . . . .	57
About Presence . . . . .	58
Presence Server . . . . .	58
Presence Modes . . . . .	58
Types of Presence . . . . .	59
Dynamic Status . . . . .	61
About Collaboration . . . . .	62
About SIP . . . . .	63
About OfficeLink . . . . .	64

PBX Software Requirements .....	64
Supported Device Types .....	65
OfficeLink Functionality .....	66
Basic UC Client .....	68
Teamwork Mode .....	69
UC Advanced for VMware Horizon View .....	71

## Chapter 3: Specifications

Introduction .....	77
System Requirements .....	77
PBX Requirements .....	77
UC Server Requirements .....	79
About Virtualization .....	80
Mitel Integrated Application Requirements .....	81
Desktop Client Requirements .....	82
MiVoice for Lync Requirements .....	84
Optional Third-Party Client Components .....	84
Web Portal Requirements .....	84
UCA Mobile for BlackBerry Requirements .....	85
UCA Mobile for Android Requirements .....	85
UCA Mobile for iPad Requirements .....	85
UCA Mobile for iPhone Requirements .....	85
PBX Node Environments .....	86

## Chapter 4: Installation and Configuration

Introduction .....	89
Planning Considerations .....	89
High Level Installation and Configuration Procedures .....	90
Configure the PBX .....	91
MCD PBX .....	91
User Configuration Form .....	92
License and Option Selection Form .....	92
Class of Service Options Form .....	92

Personal Ring Group Assignment Form .....	93
SIP Softphone settings .....	93
Mitel 5000 PBX .....	94
Software License .....	96
System – Devices and Feature Codes – Assistants .....	96
System – Devices and Feature Codes – Phones .....	96
System – IP-Related Information – Call Configuration (Softphones Only) .....	97
System – Sockets .....	97
Users .....	97
Inter-Tel Axxess PBX .....	98
Software License .....	100
System – Devices and Feature Codes – Stations .....	100
System – Sockets .....	100
Configure Integrated Applications. ....	101
NuPoint UM Configuration .....	101
Visual Voice Mail for Peered UC Servers .....	101
NuPoint Configuration Options .....	102
FCOS Options .....	102
Port Utilization .....	102
Other Voice Mail Systems .....	103
MCA Configuration .....	103
MBG and Remote Proxy Services Configuration .....	104
Configure UC Advanced Mobile for Smart Devices .....	107
Install and Configure MSL and UC Server .....	108
Software Installation Options .....	108
Install the MSL Operating System .....	109
Configure MSL .....	109
Install the UC Server Blade .....	111
Verify UC Server Licensing .....	113
Install the UC Advanced Virtual Appliance .....	114
Install and Configure UCA Softphone for VMware Horizon View .....	116
Configure User Options UCA for VMware Horizon View .....	118
Access the UC Server Administration Page .....	121
Provision UC Advanced .....	122
Install the Desktop Client .....	124
Software Distribution Point .....	124
User Installation Permissions .....	124

Client Firewalls .....	125
Welcome E-mail Message .....	125
Microsoft .NET Framework .....	127
Installation Procedure .....	128
Custom Installation Options .....	131
IntelliMirror .....	131
Logon Script .....	132
SMS .....	132
Group Policy .....	132
Citrix Deployments .....	133
Installer Transforms .....	133
Creating a Transform .....	134
Installer Properties .....	135
Install MiVoice for Lync Client. ....	137
Install the Mobile Client. ....	138
Remote User Configuration .....	141
MCD PBX Configuration for Remote Users .....	142
Desktop Client Softphone and Teleworker Settings .....	142
MBG Device Configuration .....	144
Mitel 5000/Inter-Tel Axxess PBX Configuration for Remote Users .....	148
Softphone (SIP-based) specific considerations .....	149
Softphone Configuration - Desktop client .....	153
Softphone Configuration - Android client .....	158
Softphone Configuration - iPad client .....	164
Softphone Configuration - iPhone client .....	169
Teamwork Mode .....	174
Server Admin portal impacts and considerations .....	174
Google Calendar Integration. ....	176
Authentication and access to Google Calendar .....	176
Changes to Clients .....	184
Google Contacts Integration. ....	187
Authentication and access to Google Contacts .....	187

## Chapter 5: Maintenance

About Software Upgrades. ....	193
UC Advanced Software Upgrades .....	193

Upgrade UC Server version 4.0, 4.1, 5.0 or 5.1 to version 6.0 SP1 .....	194
Upgrade UC Server version 6.0 to version 6.0 SP1 .....	194
Upgrade virtual UC Server (vUCA) version 4.0 or higher to version 6.0 or higher .....	195
Upgrade the UC Advanced Desktop Clients .....	196
Upgrades from v5.x .....	196
Upgrade MiVoice for Lync Client .....	197
Upgrade the UC Advanced Mobile for BlackBerry Clients .....	198
Client Only Delivery .....	199
User Upgrades (Stand-alone to Integrated) .....	201
MSL Server Administration .....	202
UC Server Administration .....	202
Configuration .....	202
Status .....	203
Diagnostics .....	204
Reinitialize System .....	212
Desktop Client Maintenance .....	212
Install Custom Options .....	212
Repair the Desktop Client .....	217
Uninstall the Desktop Client .....	219
PBX Configuration Changes .....	220

## Chapter 6: Troubleshooting

Server Troubleshooting .....	223
Installation Problems .....	223
Server Synchronization Error Messages .....	223
UC Server Synchronization Messages .....	224
AD/LDAP Synchronization Error Messages .....	224
PBX Node Synchronization Error Messages .....	225
Collaboration Server Synchronization Message .....	226
Alarms/Events .....	227
SIP Connection Event Messages .....	227
Presence Event Messages .....	228
SIP Registrar Event Messages .....	228
Watchdog Messages .....	229
MiTAI Error Codes .....	229

Server Log Files .....	230
AD/LDAP Synchronization Log File .....	232
Domain Synchronization Summary .....	233
Account Totals .....	234
License and PBX Changes .....	235
Account Reactivation Following License Changes .....	236
Calendar Integration Troubleshooting .....	238
Failure to successfully connect to the Exchange Server .....	238
Google calendar integration error after database backup and restore or MSL upgrade ..	239
Desktop Client Troubleshooting .....	240
Problem Reporting Tool .....	240
Additional Client Log Files and Troubleshooting Tools .....	243
Desktop Client Troubleshooting Table .....	244
Desktop Client Error and Warning Messages .....	247
Initialization Messages .....	248
Configuration Change Messages .....	249
Teleworker Setup Message .....	250
File Sending Message .....	250
ACD Messages .....	250
PIM Integration Messages .....	251
Audio Problems .....	252
Video Problems .....	254
Device Error .....	254
MiVoice for Lync Troubleshooting .....	255
Web Portal Troubleshooting .....	255
Android Device Troubleshooting .....	256
BlackBerry Device Troubleshooting .....	257
UCA Mobile for BlackBerry Secure Connections .....	257
Access Point Name Settings .....	259
Transport Layer Security Settings .....	259
UCA for VMware Horizon View Troubleshooting .....	261
MCA Collaboration Troubleshooting .....	262





# CHAPTER 1

## OVERVIEW



## Introduction

Mitel® Unified Communicator® (UC) Advanced is a product that converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration, to simplify and enhance communications.

As a UC Advanced Administrator, you will be accessing the **Unified Communications (UC) Server** to configure and manage UC Advanced. The UC Server provisions users with UC Advanced features and provides communication paths to the Private Branch Exchange (PBX) telephone system, voice mail, collaboration server, and other integrated applications.

Users can access UC Advanced features from the following interfaces:

- Desktop Client
- MiVoice for Lync™
- Web Portal
- Mobile for BlackBerry®
- Mobile for Android™
- Mobile for iPad™
- Mobile for iPhone™



**Note:** UC Advanced functionality described in documentation refers to **enterprise as a single company entity**. In scenarios where multiple server domains are created, it is understood to be within a single company environment where multiple UC servers or mixed PBX nodes are required to manage the solution.

## About This Guide

This administrator guide contains information about configuring UC Advanced on a Mitel communications platform, and is organized as follows:

- [Overview](#)
- [Features](#)
- [Specifications](#)
- [Installation and Configuration](#)
- [Maintenance](#)
- [Troubleshooting](#)

## Audience

This document is intended for UC Advanced and network administrators. This administrator guide assumes that you are familiar with the system administration interfaces for the PBX

platform you are connecting to. It also assumes that your UC Advanced site has already purchased UC Advanced and the necessary UC Advanced, PBX, and integrated application hardware, software, and licenses. Review the Release Notes before installing UC Advanced.

This document is intended for UC Advanced standalone installations; if you are working with UC Advanced integrated into the Mitel Applications Suite (MAS), refer to the MAS documentation suite.



**Note:** This document assumes that the UC Advanced administrator and the MSL administrator are the same person.

## Terminology

The following terms are used throughout this guide:

- The term **PBX** (Private Branch Exchange) refers to the communication platform that UC Advanced is connected to. See [page 16](#) for more information about supported Mitel PBXs.
- The term **PIM** (Personal Information Manager) refers to a supported PIM application (for example, Google® Contacts, Microsoft® Outlook® or IBM® Lotus Notes®). See [page 17](#) for a list of supported PIMs.
- The term **softphone** refers to the software-based IP or SIP phone that is available with the UC Advanced Desktop Client or Mobile Clients.
- The term **desk phone** refers to the physical phone on the user's desk that is controlled by UC Advanced.
- The term **peering** refers to the server configuration where UC Server is connected to and communicating with another UC Server and contacts for both servers are visible in the respective Desktop Client applications. Contact-related features are accessible to all peered servers.
- The term **federation** refers to the server configuration where the UC Server Extensible Messaging and Presence Protocol (XMPP) server is connected to and communicating with an external Instant Messaging (IM) XMPP server for the purposes of sharing IM presence and providing IM features.
- The product names **VMware View** and **VMware Horizon View** are used interchangeably throughout this guide. These are trademarks of VMware Incorporated.

## Features, Enhancements, and Changes

This Mitel Unified Communicator Advanced Administrator Guide was last published as Issue 6.0. This section provides information about the features, enhancements and changes included in the UC Advanced 6.0 SP1 release.

Version 6.0 SP1 includes the following enhancements:

- Microsoft Exchange 2010 SP3 support.
- Server Diagnostic improvement: A new Clients option was added under Unified Communications Server Diagnostics (See Clients on [page 205](#)).
- Support of iPad mini and iOS 7.0.
- UC Advanced client and Server Compatibility:
  - The UCA 6.0 SP1 desktop client will work with the following servers: UCA 6.0 SP1, UCA 6.0 and UCA 5.1.

Version 6.0 includes the following features, enhancements, and changes:

- MiVoice for Lync (supported on MAS deployed UCA only)
- Google Calendar Integration
- Google Contacts Integration
- Basic Unified Communication (UC) Client
- Forward Compatibility of UC Advanced 5.1 Mobile client running on a 6.0 server
- MSL 10 support
- MAS 5.0 support
- MBG 8.0 support (also see [“TCP/TLS to UDP Connector” on page 141](#))
- Windows 8 support
- Teleworker: the Desktop client Teleworker menu under Configuration has been removed. The Teleworker for Softphone has been moved to Softphone Settings menu along with the Teleworker Gateway address setting.

### MiVoice for Lync

UC Advanced 6.0 introduces the support of the MiVoice for Lync seamless integration with Microsoft Lync 2010 and 2013 clients and allows MS Lync users to use Mitel telephony features through its feature rich UCA infrastructure. **Requires Desktop client SDK license.**



**Note:** MiVoice for Lync is supported on MAS deployed UCA only.

### Google Integration

- **Google Calendar Integration:** UC Advanced 6.0 now provides users with the option to integrate with Google calendar. This feature is an alternative to the Exchange calendar integration and is supported on the Desktop Client See [“Google Calendar Integration” on page 176](#)
- **Google Contacts Integration:** From a Personal Information Manager standpoint, UC Advanced 6.0 now supports Google contacts. See [“Google Contacts Integration” on page 187](#)

### Basic Unified Communication (UC) Client

UC Advanced 6.0 offers Basic UC functionality to the desktop and web client. This basic client offers non-licensable features. See [“Basic UC Client” on page 68](#) for additional details and feature listing.

### UC Advanced Mobile for iPad and iPhone enhancements

Mitel® Unified Communicator® Advanced Mobile for iPad™ and iPhone™ client application (UCA Mobile for iPad and iPhone) provides Dynamic Status updates based on time or geographical. location. In addition, UCA Mobile provides an integrated environment in which you can communicate utilizing the UCA Softphone, and access and manage visual voice mail and call history.

**iPad mini** is supported on release 6.0 SP1.

### UC Advanced Mobile for Android enhancements

UC Advanced Mobile for Android™ is a stand-alone mobile client application that provides Dynamic Status updates based on time, GPS location, and Wi-Fi/Bluetooth connection options. In addition, UCA Mobile provides an integrated environment in which users can communicate utilizing the UCA Softphone, and access and manage visual voice mail and call history. Shortcuts and widgets provide customization options.

### UC Advanced Mobile for BlackBerry enhancements

UCA Mobile for BlackBerry is a stand-alone mobile client that provides automatic Dynamic Status updates based on the user's current location. In addition, the client provides access to UC Advanced call logs, messages, Corporate Contacts, and OfficeLink calling capabilities. The client requires the BlackBerry mobile operating system v5.x, v6.x or v7.x.

### Web Portal Enhancements

As part of UC Advanced 6.0, Web Portal now supports:

- **Basic UC Client:** see Basic Unified Communication Client on [page 68](#).

## UC Server Changes

The following enhancements and additions are supported on v6.0 SP1:

A new **Client** option was added under Server **Diagnostics** showing client specific data supported by this server. Information such as total number of connected clients, bridge info, login ID, connection URL and connection duration.

UC Advanced 6.0 SP1 supports **Exchange 2010 SP3**.

The following enhancements and additions are supported on v6.0:

**Google Calendar Integration:** UC Advanced 6.0 now provides users with the option to integrate with Google calendar. This feature is an alternative to the Exchange calendar integration. Once enabled and configured, the Google Calendar information will provide presence information and be presented to UCA users as dynamic statuses. UCA users may have multiple calendars, however UCA will only integrate with one of them, as configured by the user. See [“Google Calendar Integration” on page 176](#)

Google Federation is also supported. In addition, for UC Advanced v6.0, federation with MBG in the network path between UCA server and the federated server (OCS, IBM Sametime or Google server) is supported. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0. See UC Advanced engineering guidelines for further details.

UC Advanced 6.0 supports Exchange 2010 SP2.

**Features Tab:** The Features Tab has been simplified as per of UCA 6.0 in support of Basic UC Client functionality. The default profile can only contain non-licensable features. The Licensed Feature Usage has been modified to display only the licensable features.

**Integrated Directory Services (IDS) Password Monitoring:** This server level feature allows password monitoring when UC Advanced is operating in MAS integrated mode. See **Integrated Directory Services (IDS) Auth Cache** on [page 210](#).

## Server and Client Components

The UC Server communicates with the phone system (see [page 16](#)) and other integrated applications (see [page 16](#)) to provide UC Advanced features and functionality to the user interfaces.

The UC Advanced product includes the UC Server components and user interfaces described in this section.

### UC Server

The UC Server software can reside as a stand-alone application on an MSL v10.0 or later approved hardware platform or as part of an integrated system with MAS, either on the physical server or on VMware. The UC Advanced virtual appliance (vUCA) can be deployed in a VMware environment running vSphere 4.1 or higher (for more information see <http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf>).

UC Server software components include:

- **ADEPM:** Manages Active Directory communication for account synchronization.
- **DSM:** Analyzes accounts in the PBX database or Active Directory and maintains the account representation in the UC Server.
- **EPM:** Manages MiXML-based communication with the MCD PBX for account synchronization.
- **FEDERATIONGW:** Handles the XMPP federation with third-party systems such as Microsoft Office Communicator Server (OCS), Microsoft Lync, Google or IBM Lotus Sametime Server.
- **IM:** Handles Instant Messaging between Desktop Clients and provides page mode, conversation mode, and conference mode instant messages.
- **JBoss:** Provides the various administrator features and Web services.
- **PbxProxy:** Maintains MiTAI connections and receives call and feature events from the MCD PBX. Publishes the events on the UC Server internal message bus.
- **Proxy5k:** Maintains OAI connections and receives call and feature events from the Mitel 5000 PBX. Publishes the events to the UC Server internal message bus.
- **Presence:** Handles subscriptions and notifications for presence, calls, message waiting etc.
- **RPS:** Includes the server component for the UC Server peered connection. This component “listens” on TCP port 36009 for incoming connection requests from the RTC component on a peered UC Server.
- **RTC:** Includes the client component for the UC Server peered connection. This component connects to the RPS component on a peered UC Server.
- **SEE:** Provides the advanced call processing services such as preferential contact call routing.



- **SIPProxy**: Receives SIP messages from the network and routes them to the corresponding UC components, such as the SIP Registrar, Presence and IM.
- **SIPRegistrar**: Manages the SIP registrations from the UC Advanced Desktop Client and notifies other UC Advanced components whenever registration is added or removed.
- **Watchdog**: Maintains and monitors other UC Server components.
- **WSP**: Web Socket Proxy handles the connections from the UCA mobile clients for real-time notifications.

Administrators can provision, maintain, and troubleshoot UC Advanced from the Mitel Unified Communications Server Administration interface.

The UC Server software blade includes the client software for UC Advanced. The following user interfaces provide access to UC Advanced features:

- [“Desktop Client” on page 10](#)
- [“MiVoice for Lync Client” on page 11](#)
- [“Web Portal” on page 12](#)
- [“UC Advanced Mobile for BlackBerry” on page 13](#)
- [“UC Advanced Mobile for Android” on page 14](#)
- [“UC Advanced Mobile for iPad” on page 15](#)
- [“UC Advanced Mobile for iPhone” on page 15](#)

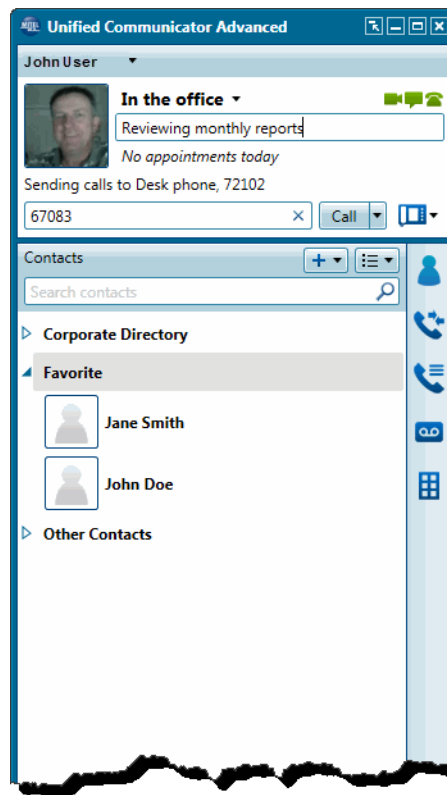


Some UC Advanced features require specific PBX software versions as detailed in the Notes column for the end-user feature tables starting on [page 32](#).

## Desktop Client

The UC Advanced Desktop Client is an application that is installed on the user's computer (see [Figure 1](#)). The Desktop Client allows users to control their desk phone and associated devices from their computer. The Desktop Client includes an embedded softphone, providing users with two devices, if both are configured on the PBX. The softphone requires a separate license (see Table 1 on [page 23](#).)

The Desktop Client requires the Microsoft.NET Framework (see [page 82](#)). This component must be installed on the user's computer prior to the installation of the Desktop Client.



**Figure 1: UC Advanced Desktop Client Interface**

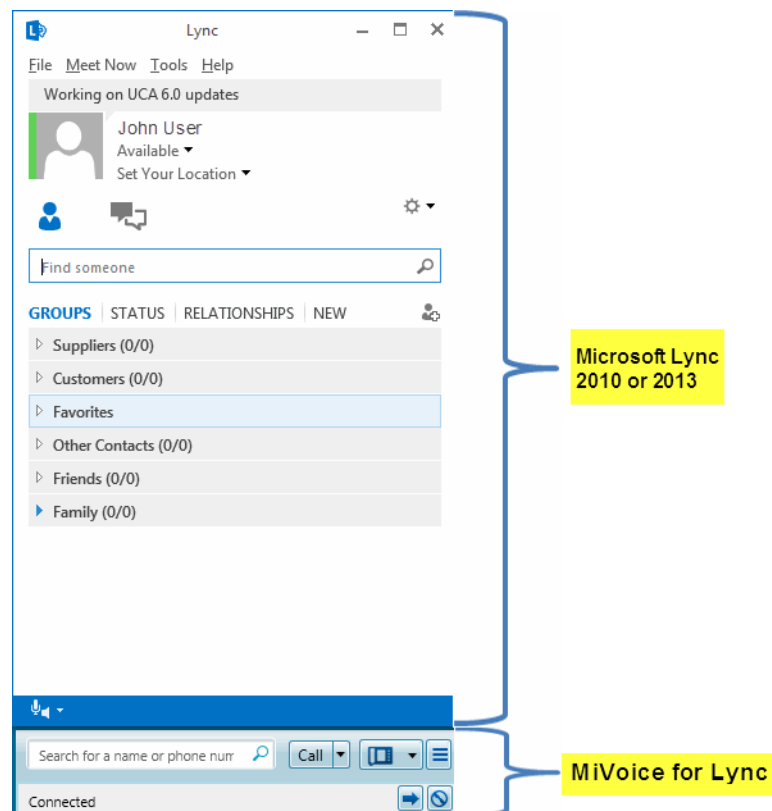
See [page 32](#) for a list of Desktop Client features.

## MiVoice for Lync Client

MiVoice for Lync is an application that is installed on the user's computer (see [Figure 2](#)) and integrates seamlessly with Microsoft Lync 2010 and 2013 clients. It allows MS Lync users to use Mitel telephony features through its feature rich UCA infrastructure.



**Note:** MiVoice for Lync is supported on MAS deployed UCA only.



**Figure 2: MiVoice for Lync Interface**

## Web Portal

The UC Advanced Web Portal interface provides remote access to a subset of UC Advanced features from a Web browser on a computer or mobile device.

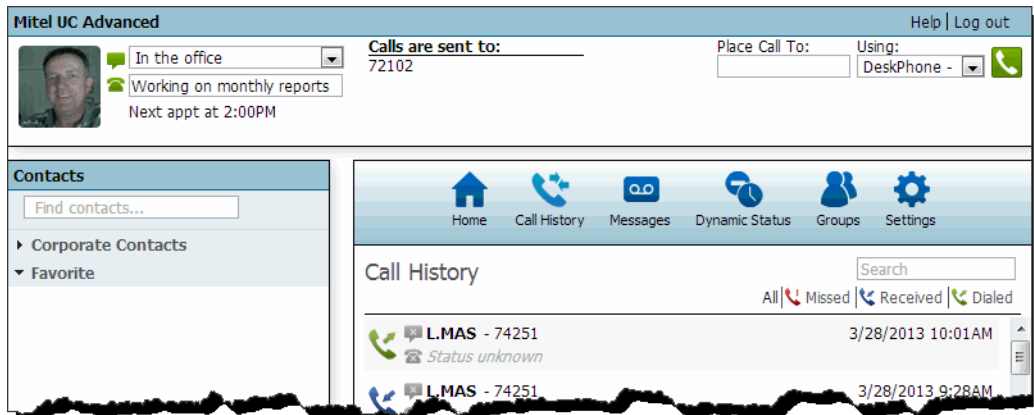


Figure 3: UC Advanced Web Portal Interface

See [page 37](#) for a list of Web Portal features.

## UC Advanced Mobile for BlackBerry

UCA Mobile for BlackBerry is a stand-alone client that users install on their BlackBerry mobile device (see [Figure 4](#)). The client provides automatic Dynamic Status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, Corporate Contacts, and OfficeLink calling capabilities. To install and use UC Advanced Mobile for BlackBerry, users must have a mobile device that meets the documented requirements (see “UCA Mobile for BlackBerry Requirements” on [page 85](#)) and be licensed for this feature.

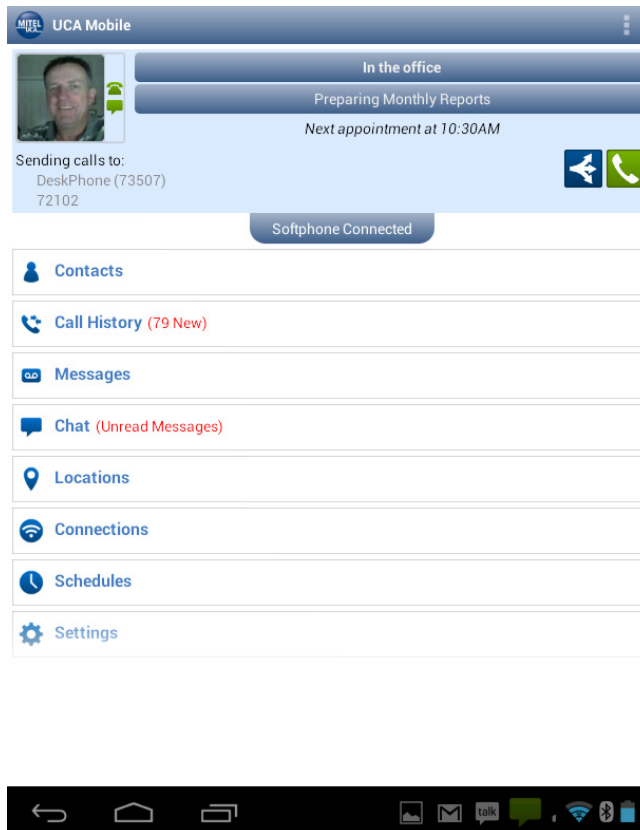


**Figure 4: UCA Mobile for BlackBerry Interface**

See [page 39](#) for a list of UCA Mobile for BlackBerry features.

## UC Advanced Mobile for Android

UCA Mobile for Android is a stand-alone client that users install on their Android mobile device. The client provides automatic Dynamic Status updates based on the user's current location. Location options include GPS and Bluetooth. In addition, the client provides access to call logs, messages, Corporate Contacts, a Softphone and OfficeLink calling capabilities. To install and use UC Advanced Mobile for Android, users must have a mobile device that meets the documented requirements and be licensed for this feature.

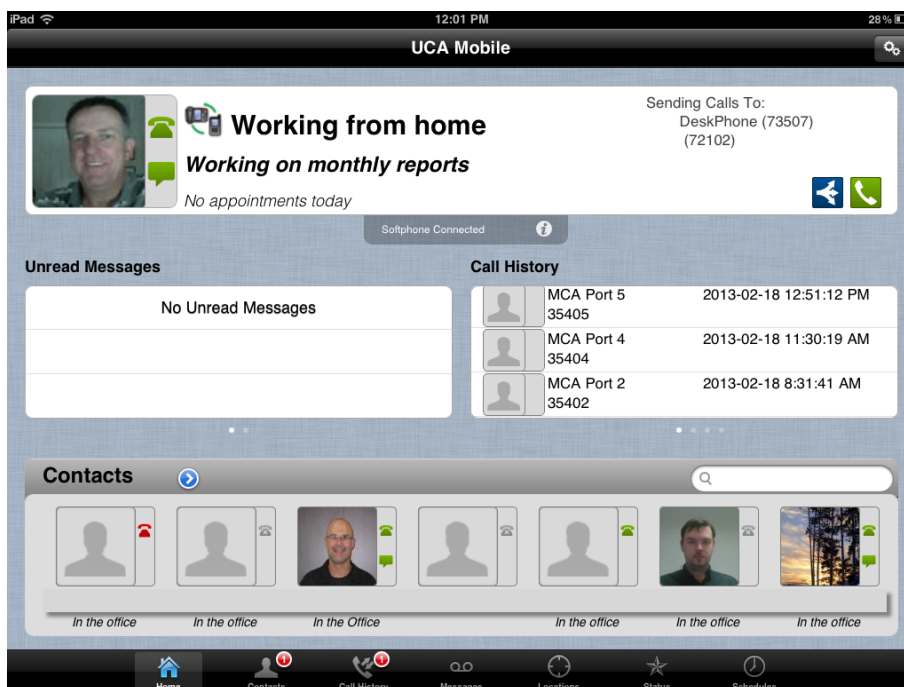


**Figure 5: UCA Mobile for Android Interface**

See [page 40](#) for a list of UCA Mobile for Android features.

## UC Advanced Mobile for iPad

UCA Mobile for iPad is a stand-alone client that users install on their iPad mobile device. The client provides automatic Dynamic Status updates based on the user's current location. In addition, the client provides access to call logs, messages, Corporate Contacts and Softphone calling capabilities. To install and use UC Advanced Mobile for iPad, users must have a mobile device that meets the documented requirements and be licensed for this feature.



**Figure 6: UCA Mobile for iPad Interface**

See [page 42](#) for a list of UCA Mobile for iPad features.

## UC Advanced Mobile for iPhone

UCA Mobile for iPhone is a stand-alone client that users install on their iPhone mobile device. The client provides automatic Dynamic Status updates based on the user's current location. In addition, the client provides access to call logs, messages, Corporate Contacts and Softphone calling capabilities. To install and use UC Advanced Mobile for iPhone, users must have a mobile device that meets the documented requirements and be licensed for this feature.

See [page 43](#) for a list of UCA Mobile for iPhone features.



**Note:** Mitel recommends setting up the softphone as a part of a ring group to avoid missing incoming calls due to the following condition:

Due to Apple iOS application management, the UCA application for iPhone and iPad may stop running while in the background (consistent with IOS behavior on other IOS Apps). The result is that a UCA application user may be unaware that the UCA application has stopped receiving incoming softphone calls and chat messages.

## Supported Communication Platforms (PBXs)

The following Mitel communication platforms provide call control for UC Advanced desk phones and softphones:

- **Mitel Communications Director (MCD) v4.2 and later:** Formerly known as Mitel 3300 IP Communications Platform (ICP), the MCD call processing software is configured through the MCD Administration Tool. **MCD v5.0 SP2 is required for UCA SIP softphone functionality.**
- **Mitel 5000 Communications Platform (CP) v3.2 and later:** The Mitel 5000 call processing software is configured through the Mitel 5000 Database Programming interface. **5000 v5.0 or later is required for UCA SIP softphone functionality.**
- **Inter-Tel Axxess Converged Communications Platform (CCP) v11.017 and later:** The Inter-Tel Axxess call processing software is configured through the Inter-Tel Axxess Database Programming interface.

Users can access and use the communication system features provided by the communications platform from the UC Advanced interfaces (see [page 44](#)). Note that some features may not be supported on the user's desk phone or softphone.

## Mitel Integrated Applications

The following Mitel application components and versions are integrated with UC Advanced:

- **Mitel Collaboration Advanced (MCA)** - formerly known as Audio and Web Conferencing (AWC): Access to MCA is integrated within UC Advanced. If users are licensed for MCA, they can use collaboration features (see [page 62](#)) such as video calls, audio conferencing, Web conferencing, annotation, chat, file transfer, and desktop sharing.



**Note:** UC Advanced v6.0 requires MCA 5.0 or later. MCA 5.0 is not compatible with any earlier versions of UCA.

- **NuPoint Unified Messaging (UM):** Provides access to Visual Voice Mail (NuPoint UM voice mail and FAX messages) from the UC Advanced client interfaces.
- **Mitel Border Gateway (MBG):** MBG provides a secure communications path for remote UC Advanced users to the UC Server. This product is supported for MCD communication systems only. **MBG v7.1 and later is required.**
- **Mitel Remote Proxy Services:** Remote Proxy Services provide a secure communications path for remote UC Advanced Web Portal users. This product is supported for MCD communication systems only.
- **Mitel Mobile Extension/UC Mobile:** UC Mobile, (formerly branded as Mobile Extension), provides twinning between your desk phone and another internal or external phone. For example, you can configure your mobile device as a twinned device for your desk phone. Incoming calls ring your desk phone and mobile phone simultaneously, allowing you to answer either device. This product is supported for MCD communication systems only.



## Optional Third-Party Integrated Applications

UC Advanced includes support for the following third-party integrated applications:

- **Personal Information Manager (PIM)s:** PIMs allow users to easily import personal contacts into UC Advanced. Supported PIMs include:
  - Microsoft Outlook 2003, 2007, and 2010 (32-bit and 64 bit)
  - IBM Lotus Notes Server and Client 7.0, 8.0, 8.5, 8.5.1, 8.5.2 and the Fix Packs
  - Sage® Software Act!® 2006, 2007, 2008, and 2011
  - Google Contacts version 3
- **Instant Messaging Clients:** UC Advanced includes its own integrated chat component. It also supports launching the following Instant Messaging clients when they are installed and running on the user's computer:
  - Windows Live Messenger 8.5, 2009, and 2011
  - Microsoft Office Communicator 2005, 2007, and Lync 2010
- **Federation Servers:** Federation provides a communication path between a single UC Server and one or more external IM servers to provide UC Advanced users with presence and chat features for external IM contacts (see [page 27](#)). UC Advanced supports IM and presence federation with the following servers:
  - Microsoft Office Communicator Server (OCS) 2007 R2
  - Microsoft Lync 2010 Server
  - IBM Lotus Sametime® Server 7.0, 8.0.x, 8.5, 8.5.1, and 8.5.2 and Fix Packs
  - Google Server
- **Exchange Server:** Exchange server integration enables users to integrate their dynamic status with their calendars whether or not they are logged into their PIM. This feature can be used with Microsoft Exchange 2007, Exchange 2007 SP1, Exchange 2010, Exchange 2010 SP1, Exchange 2010 SP2 and Exchange 2010 SP3.
- **Google Server:** Google server integration enables users to integrate their dynamic status with their Google calendars.

## Documentation

Documentation for UC Advanced includes the following:

- Administrator documentation includes:
  - **UC Advanced Engineering Guidelines:** The *UC Advanced Engineering Guidelines*, part number 835.3288, provides system requirements, configuration information, network diagrams, virtualization information, performance recommendations, system capacities, etc. for sites installing the UC Advanced product.
  - **UC Advanced Administrator Guide:** This *Mitel Unified Communicator Advanced Administrator Guide*, part number 835.3246, includes PBX configuration information, Unified Communications specifications and hardware configuration information, and configuration information for integrated applications.
  - **Unified Communications Administrator Online Help:** Embedded in the UC Server Administrator Interface, this help system provides a high-level overview of the provisioning process with links to task-related instructions. The task-related instructions provide detailed descriptions for fields and options. To open the help, access the Mitel UC Server Configuration Web pages and click the help icon.
- End-user documentation includes:
  - **UC Advanced Quick Reference Guide:** Provides basic feature and usage information for the Desktop Client, Web Portal and Mobile for BlackBerry. In addition, the quick reference guide provides basic installation instructions for the Desktop Client and Mobile for BlackBerry. A link to the [Mitel Unified Communicator Advanced Quick Reference Guide](http://edocs.mitel.com/UG/UCA_QRG.pdf) ([http://edocs.mitel.com/UG/UCA\\_QRG.pdf](http://edocs.mitel.com/UG/UCA_QRG.pdf)) on the Mitel eDocs Web site is included in the Welcome e-mail message generated from the UC Server.
  - **Online Help:** Embedded in the user interface, the following help systems focus on interface elements, supported features, and task-related instructions:
    - *UC Advanced Desktop Client Help:* To open the online help, select **Help** from the main menu or press the F1 function key on your keyboard.
    - *UC Advanced Web Portal Help:* To open the Help, click the **Help** link at the top of the page.
    - *MiVoice for Lync Help:* To open the Help, click the menu icon and select **Help**.
    - *UC Advanced Mobile for Android Help:* To open the Help, click the help icon at the top of the page.
    - *UC Advanced Mobile for Blackberry Help:* To open the Help, click the help icon at the top of the page.
    - *UC Advanced Mobile for iPad Help:* To open the Help, click the Settings icon at the top of the page and choose Help for Mitel UCA for iPad.
    - *UC Advanced Mobile for iPhone Help:* To open the Help, click the More (...) icon at the bottom of the page. Choose Settings, then choose Help for UCA Mobile.

User documentation for UC Advanced is available in the following languages:

- Dutch
- English (US)
- French (Canadian)

- French (European)
- Italian
- Portuguese (Brazilian)
- Spanish (European)
- Spanish (Latin America)



**Note:** The user interface supports the following languages:

Chinese (Simplified), Chinese (Traditional), Dutch, English (US), English (UK), French (Canadian), French (European), German, Italian, Portuguese (Brazilian), Spanish (European), Spanish (Latin American).



**Note:** MiVoice for Lync documentation and user interface is supported in the English (US) language only.

- **UC Advanced SDK Programmers Guide:** The *UC Advanced Software Developers Kit and SDK Programmers Guide*, part number 835.3246, are optional components for software developers designing third-party applications that integrate with UC Advanced. Refer to the [Mitel Solutions Alliance \(MSA\) Web page](http://www.mitel.com/DocController?documentId=9971) for more information (<http://www.mitel.com/DocController?documentId=9971>).

Documentation for the following Mitel integrated applications is available on the [Mitel eDocs Web site](http://edocs.mitel.com) (<http://edocs.mitel.com>):

- Mitel Standard Linux® (MSL)
- Mitel Application Suite (MAS)
- Mitel Collaboration Advanced (MCA)
- NuPoint Unified Messaging (UM)
- Mitel Border Gateway (MBG) and Remote Proxy Services
- Virtual Appliance Deployment
- VMware Horizon View Support



# CHAPTER 2

## FEATURES



## Introduction

This chapter provides information about UC Advanced features.

There are a total of 29 licensed features for UC Advanced. Two of the features are server-level licensed features ([“Federation” on page 27](#), and [“Peering” on page 29](#)), and are considered to be “in use” at all times.

The remaining 27 licensed features are user-level licensed features (see [page 32](#)), and are allocated to a specified user. These types of features are considered to be “in use” when you assign them to the user, regardless of whether or not the user is actually using the feature.

[Table 1](#) describes the UC Advanced licensed features.

**Table 1: UC Advanced Licensed Features**

Feature Name	Description
Auto Answer <sup>1</sup>	Incoming calls are answered at the first ring by the selected device. Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client.
Call Forwarding	<p>The Call Forwarding feature allows users to:</p> <ul style="list-style-type: none"> <li>• forward to any non-Personal Ring Group (PRG) destinations.</li> <li>• add preferential contacts.</li> <li>• send calls to dynamic extensions.</li> </ul> <p>When users are not licensed for Call Forwarding, they can still send calls to their desk phones, softphones, and voice mail. In addition, users can set Do-Not-Disturb and Auto Answer options.</p>
Chat	Users can participate in online chat sessions with other users also licensed for chat. Users access the Chat submenu option when they right-click a contact from the Contacts view.
Collaboration Integration	<p>Users can access Collaboration features including the Collaboration submenu (available from the main menu) and the Start Collaboration option when the user right-clicks one or more contacts.</p> <p>See <a href="#">“Server-Level Features” on page 27</a> for more information about collaboration.</p>
Compact Mode	Users can switch between the full mode and Compact mode Desktop Client interfaces.
Console Option <sup>2</sup>	Users have access to the Console view from the main menu. The Console view provides access to attendant functions such as answer, transfer, hold, and the ability to view and change another user's status.
Desk Phone	Users' desk phone extensions, as programmed on the PBX, are integrated with UC Advanced.
Desktop client SDK	<p>This license is required for MiVoice for Lync (Lync PlugIn) feature.</p> <p><b>Note:</b> MiVoice for Lync Deskphone only users: those users only require the <b>Desktop client SDK</b> feature.</p> <p>MiVoice for Lync Softphone only users OR those users with a Softphone and an associated Deskphone will require the <b>Softphone</b> feature in addition to the <b>Desktop client SDK</b> feature.</p>

Table 1: UC Advanced Licensed Features (continued)

Feature Name	Description
Do-Not-Disturb (DND)	Users can enable and disable DND to override current Dynamic Status settings. When DND is enabled, callers receive a busy tone and a Do-Not-Disturb message and incoming calls are not logged in the call log.
Dynamic Status	<p>Users can manually change their Dynamic Status at any time using the UC Advanced interface, which is then communicated to other UC Advanced users. In addition, Dynamic Status can also be configured to be automatically updated in response to many events, such as a user's Calendar availability. Users can also add statuses and configure the following Dynamic Status elements:</p> <ul style="list-style-type: none"> <li>• Status Message (for example, In the office or Gone for the day)</li> <li>• Optional custom text (for example, Reviewing reports or Back on Thursday)</li> <li>• Instant Message and Video Call availability</li> <li>• Preferential Contacts</li> <li>• Phone Settings (Busy/no answer routing, DND, Auto Answer)</li> </ul> <p>When users are not licensed for Dynamic Status, they have only one status. This status provides call forwarding capabilities as long as the user is licensed and configured to use the Call Forwarding feature.</p>
External Dial	Users can dial an external number from an integrated application such as Microsoft Word, Outlook, Internet Explorer®, and IBM Lotus Notes. The user may need to complete some configuration in the application to enable external dialing.
Federation	<p>The Federation feature provides UC Advanced users with expanded IM capabilities. When the UC Server is licensed for this feature, you can configure federation from the Federation Tab, and users can view IM presence and chat with federated IM contacts using the Desktop Client's Chat window.</p> <p>See <a href="#">“Server-Level Features” on page 27</a> for more information about federation.</p>
Knowledge Management	Users can index computer files and documents associated with a contact. When the user receives an incoming call, the Knowledge Management popup window appears presenting the user with a list of files associated with the caller including e-mail messages, contact entries, and documents (Microsoft Word, Excel®, PowerPoint®, Outlook and Adobe® Portable Document Format).
Launchpad	Users can access the Launchpad view, which provides quick access to frequently completed actions, from their Desktop Client. Actions include dialing a number, browsing to a URL, running a program, and exploring a folder.
Mobile Handoff	<p>Users on Mobile device can use the Call Handoff feature (ability to push a call to other devices within the Personal Ring Group).</p> <p>NOTE: Handoff Feature Code: As a prerequisite, the MCD Feature Code for Handoff must be programmed. If this feature is added to an existing server, the PBX need to be synchronized with UCA before the feature can be used.</p>
Mobile SIP Softphone	<p>Allows users to have SIP-Based Softphone on Desktop, Android and iOS clients. (You must have the “UC Advanced Mobile for Smart Devices” license enabled before you can enable the “Mobile SIP Softphone” license).</p> <p>This feature is supported on 5000 and MCD systems only (MCD 5.0 SP2 and later release is required or 5000 running 5.1 or later release is recommended).</p>
Office Communicator Integration	Users can send and receive instant messages using the Office Communicator IM client, from the UC Advanced interface. Similar to the Chat feature, users can access the Office Communicator submenu when they right-click a contact from the Contacts view.



**Table 1: UC Advanced Licensed Features (continued)**

Feature Name	Description
Peering	The Peering licensed feature allows you to configure communication paths with other UC Servers for the purposes of sharing presence information and providing communication features between multiple UC servers. See <a href="#">“Peering” on page 29</a> for more information about peering.
Phone Button Programming	Users can configure the buttons on their 5312, 5320, 5324, 5330, 5340, or 5360 IP phone from the Desktop Client. This feature is limited to users on MCD communication platforms only.
Presence	The Presence Server provides the following types of presence for UC Advanced users: <ul style="list-style-type: none"> <li>• Dynamic Status</li> <li>• Telephony presence</li> <li>• UC Advanced chat presence</li> <li>• IM presence</li> <li>• Video presence</li> </ul> See <a href="#">“About Presence” on page 58</a> for more information about presence.
Presence on Mitel Sets	Users can configure presence information for speed call keys on their 5320, 5330, 5340, or 5360 IP phone from the Desktop Client. This feature is limited to users on MCD communication platforms only.
RSS Window	Users have access to the RSS window (Rich Site Summary), located at the bottom of the Desktop Client UI. Typically, RSS feeds provide syndicated content such as events listings, news stories, headlines, excerpts from discussion forums, or corporate information to the user.
Softphone	Users' softphone extensions, as programmed on the PBX, is integrated with UC Advanced. UCA Softphones are <b>not</b> available on the Inter-Tel Axxess PBX.
Stand-alone Mobile Web Portal	The Mobile Web Portal provides users with remote access to a subset of UC Advanced features. This interface allows users to configure and change their Dynamic Status, access call history data, view corporate contacts, access voice mail messages, and configure account options.
Stand-alone Web Portal	The Web Portal provides users with remote access to a subset of UC Advanced features. This interface allows users to configure and change their Dynamic Status, access call history data, view corporate contacts, access voice mail messages, and configure account options.
UC Advanced Mobile for Smart Devices	Users can install and use the UC Advanced Mobile client application on their Android, BlackBerry, iPad, or iPhone mobile device. Depending on the device, the UCA mobile client application provides Dynamic status updates based on location, time, WiFi and/or Bluetooth. The UCA mobile client provides an integrated environment in which users can manage Dynamic Status, communicate with corporate contacts, and access visual voice mail and call history. Depending on the device, shortcuts and widgets provide customization options for users. When using the Mitel Unified Communication Server Configuration interface to assign licenses, this feature will appear as “UC Advanced Mobile for Smart Devices” and will represent a consolidated license count for the Android, BlackBerry, iPad, and iPhone licenses. The <b>UC Advanced Mobile for Smart Devices</b> was previously known as the <b>Locator</b> .
Page 3 of 4	

Table 1: UC Advanced Licensed Features (continued)

Feature Name	Description
Video Calls	Users have access to video presence for Corporate Contacts and can participate in point-to-point and multi-party video sessions. Video services for the UC Advanced Desktop Client are provided by Mitel MCA (formerly known as AWC). Refer to the MAS and MCA documentation, available on <a href="#">Mitel eDocs</a> Web site, for additional licensing information for MCA.
Visual Voice Mail	Users have access to the following NuPoint Unified Messaging (UM) voice mail features from the Visual Voice Mail view: <ul style="list-style-type: none"><li>• Receive message waiting indications</li><li>• Play, forward, and delete voice mail messages</li><li>• View, forward, and delete fax messages</li><li>• Change the voice mail PIN</li></ul> Supported on systems with NuPoint UM voice mail only.
WLM Integration	Users can send and receive instant messages using the Windows Live Messenger (WLM) IM client, from the Desktop Client interface. Similar to the Chat feature, users can access the WLM submenu when they right-click a contact from the Contacts view.
Page 4 of 4	

1. The Auto Answer feature conflicts with the Mitel 5000 Dynamic Extension Express feature.

2. SIP softphone should not be used with UC Advanced console.

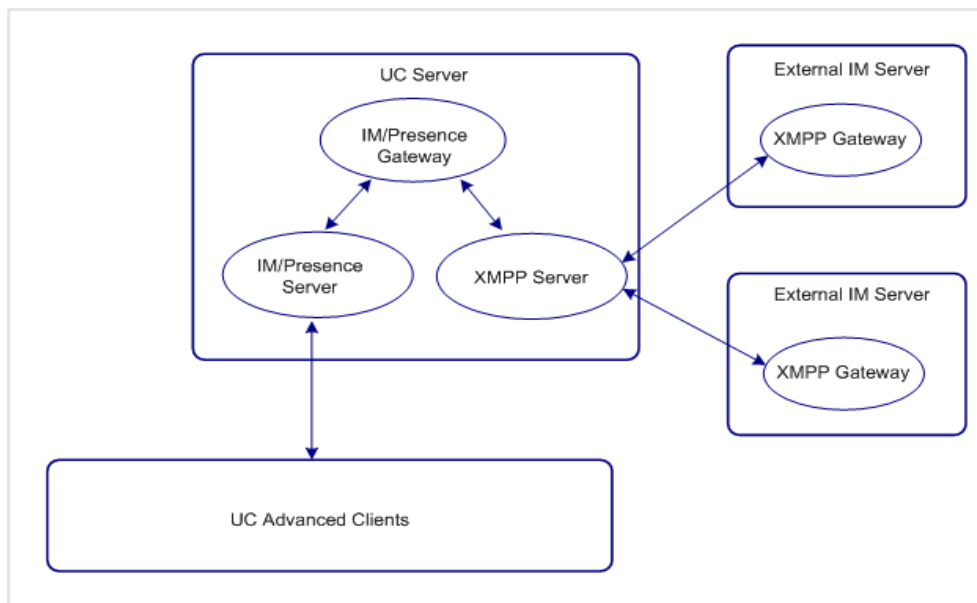
## Server-Level Features

Server-level licensed features include:

- [Federation](#), below
- [“Peering”](#) on page 29

### Federation

Federation provides a communication path between a single UC Server and one or more external IM servers to provide UC Advanced users with presence and chat features for external IM contacts. The communication path between the UC Server and the external IM server uses the Extensible Messaging and Presence Protocol (XMPP). [Figure 7](#) provides a basic federation configuration diagram.



**Figure 7: Federated Servers**



**Note:** For v6.0, external IM server support is limited to Microsoft Office Communicator Server (OCS) 2007 R2, Microsoft Lync 2010, Google and IBM Lotus® Sametime® Server 8.5, 8.5.1, and 8.5.2.

UC Server federation capabilities are provided by the following services:

- **Subscription Federation service:** Creates subscriptions for local UC Advanced users to external presence servers.
- **Presence Gateway service:** Sends presence information to/from the UC Presence Server (see [page 58](#)) and the external IM presence server. This service translates information from SIP to XMPP, and vice versa. The Presence Gateway service allows Desktop Client users to view and refresh IM presence information for external IM contacts. UC Advanced account presence (Dynamic Status) and telephony presence is not available through this service.

- **Instant Messaging (IM) service:** Allows Desktop Client users to chat (point-to-point) with external IM contacts using the Desktop Client Chat window. Federated chat sessions are page-mode conversations, similar to a two-way pager device or Short Message Service (SMS), where a small number of independent messages are exchanged between two participants and are perceived as part of the same conversation. Page mode does not support multi-party chat or file transfer.

There are two options you can use to configure Federation using the UC Server Administrator interface:

- Configure an external IM server and perform an AD/LDAP synchronization with the server from the Peer Server Details page. After synchronization, the IM server contacts are imported to the UC Server database (visible from the Corporate Directory Tab, see Figure 10 on [page 30](#)) and federation is automatically enabled. When you configure federation this way, federated contacts are displayed in a separate list in the user's corporate directory from the Desktop Client's Contacts View, similar to peered contacts (see Figure 10 on [page 30](#)).
- Enable Federation and configure the federated server domain from the Federation Tab. When you configure federation this way, instruct users to manually add the federated contacts. Users should create a new personal contact, and then add the IM login information for the contact using the **UC Advanced Login** option.

Refer to the UC Server Administrator interface online help for information and instructions about configuring federation for UC Server.

Note the following guidelines for Federation:

- The site must purchase the Federation license for UC Server (see Table 1 on [page 23](#)).
- The external IM server must be installed and the IM server's XMPP gateway must be deployed before you can configure federation for UC Server. Refer to the IM server's documentation for information about configuring federation for the IM server.



**Note: Google Federation specific:** Google Apps server hostname domain must be different from the UCA server hostname domain for the federation to work. In addition, the UCA server hostname domain should not have the same root parent domain as the Google Apps server.

For example, Google Federation will not work if UCA server hostname is `usmas12.company.com` and Google Apps server hostname is `google.company.com`.

See UC Advanced Engineering Guidelines for further details.

- Presence for federated contacts is limited to IM presence only. UC Advanced account and telephony status is not provided.
- Chat for federated contacts is limited to point-to-point only. Multi-party chat and file transfer is not available.

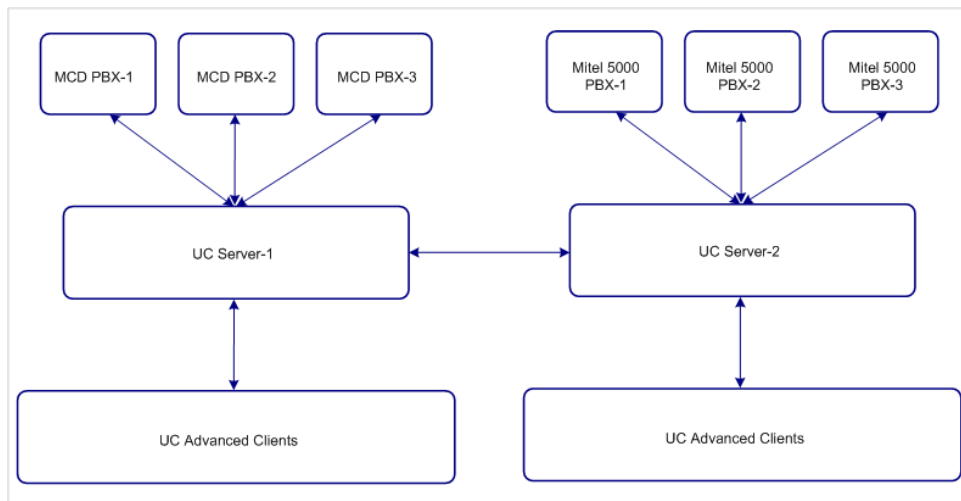


**Note:** Federation with MBG in the network path between UCA server and the federated server (OCS, Lync, IBM Sametime or Google server) is supported as of UC Advanced 6.0. This is accomplished by adding MBG connector for TCP port 5269 in MBG v8.0.

## Peering

UC Server Peering configures a communication path between a local UC Server and one or more peered UC Servers within the same company or between different companies on the same server. Peering UC Servers provides greater scalability for the UC Advanced product. UC Server peering supports a combined maximum of 10,000 clients in the configuration.

It is possible to peer a UC Server connected to multi-node MCD system with a UC Server connected to a multi-node Mitel 5000 system (see [Figure 8](#)).



**Figure 8: Peered UC Servers**

To configure UC Server peering, add one or more UC Servers from the Peering Tab – **Peer Server Details** page in the UC Server Administrator interface (see [Figure 9](#)).



**Note:** The enterprise domain should be unique for each UC Server peer. Refer to the UC Server Administrator interface online help for details.

### Peer Server Details

**Add New Peer Server**

**<< Settings**

Peer type:

UC Server

Description:

IP address / hostname:

Peer enterprise ID:

[Select Enterprise](#)

Peer dialing prefix:

Create

Cancel

**Figure 9: Peer Server Details Page-UC Server Administrator Interface**

In addition to peering with UC Servers, you can configure Federation with an external IM server from the Peer Server Details page by adding the external server and performing an AD/LDAP synchronization with the server. See [page 27](#) for details about Federation configuration.

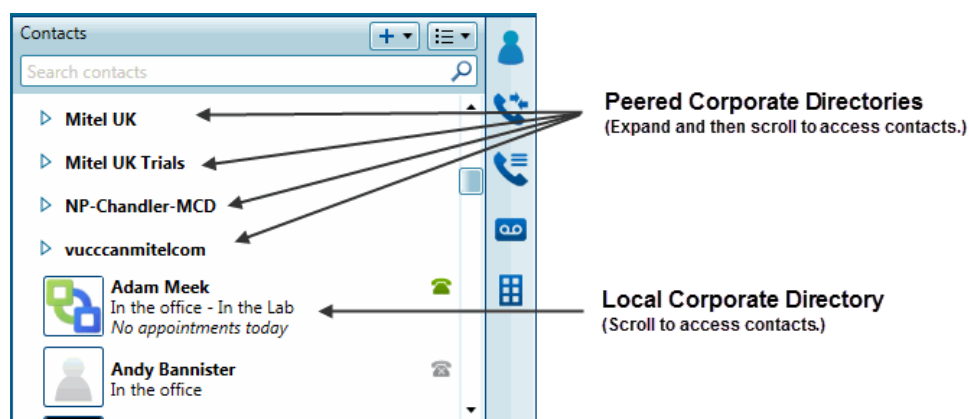
Refer to the UC Server Administrator interface online help for information and instructions about configuring peering for UC Server.

After peering has been established and a synchronization performed, peered contacts are displayed on the Corporate Directory tab in the UC Server Administrator interface. Peered corporate directories appear as sub-folders to the top-level local Corporate Directory (see [Figure 10](#)). For each peered server, the directory tree structure displayed under the local Corporate Directory folder mirrors the corporate directory structure on the peer server itself.

**Figure 10: Peered Corporate Directories-UC Server Administrator Interface**

Peered contacts are located in the Desktop Client Contacts view, and are organized within the expanding peered server corporate directory (see [Figure 11](#)). Desktop Client users can view presence information for peered contacts and can use UC Advanced communication features such as chat, video, and collaboration with peered contacts.

Users can expand each peered server corporate directory to access peered contacts. Local corporate contacts appear below the peered corporate directories.

**Figure 11: Peered Corporate Contacts-Desktop Client**

Note the following guidelines for peered UC Servers:

- All peered UC Servers must be running identical versions of UC Advanced v4.0 or later software.
- To peer with another UC Server, a site must purchase the Peering license (see Table 1 on [page 23](#)). The Peering license controls the connection initiated by the local UC server and not the connection established from the peer UC Server.
- Each UC Server in a peered configuration operates independently and is maintained and managed by the administrator assigned to that server. If a UC Server in a peered configuration is unavailable, the other servers in the configuration are not affected.
- If contacts are hidden from the corporate directory on the local UC Server, they will also be hidden on a peered UC server.
- Call routing rules must be configured properly in the PBX to route calls properly to the peered server. The Peer Server Details page includes a field called **Peer Dialing Prefix**. The value you enter for the Peer Dialing Prefix corresponds with the dialing prefix (not including the outgoing call digit) that PBX users must dial to call an extension on the networked PBX. The Peer Dialing Prefix is only required for PBX-to-PBX calls where the networked PBXs are not configured for transparent extension dialing.
- When UC Servers are peered, the voice mail systems between the servers must be networked and configured properly so that users are able to forward voice mail messages to users on other servers.

## Client Interface Features

UC Advanced includes the following interfaces, which provide access to user-level features:

- Desktop Client (see Table 2 [Desktop Client UI Features](#))
- MiVoice for Lync Client (see Table 3 [MiVoice for Lync UI Features](#))
- Web Portals (see Table 4 [Web Portal UI Features](#))
- UCA Mobile for BlackBerry Client (see Table 5 [UCA Mobile for BlackBerry UI Features](#))
- UCA Mobile for Android Client (see Table 6 [UCA Mobile for Android UI Features](#))
- UCA Mobile for iPad Client (see Table 7 [UCA Mobile for iPad UI Features](#))
- UCA Mobile for iPhone Client (see Table 8 [UCA Mobile for iPhone UI Features](#))

This section describes the main features provided by the end-user interfaces.

### Desktop Client Features

Table 2 provides descriptions for the main features accessed from the Desktop Client UI.

**Table 2: Desktop Client UI Features**

Feature Name	Description	Notes
Account Options	The My Account dialog box provides configuration options that the user can set for his or her account. Options include uploading a photo, changing password and log in options, and adding phone, e-mail, and IM contact information for publication and routing purposes.	
ACD	The Desktop Client provides the ACD view for ACD hunt group agents using the communication system ACD features. UC Advanced supports the following types of ACD: <ul style="list-style-type: none"> <li>• ACD traditional agents (MCD communication system)</li> <li>• ACD Hunt Groups (Mitel 5000 and Inter-Tel Axxess communication system)</li> </ul> The ACD view is an optional component for UC Advanced.	
Auto Answer	When the Auto Answer feature is enabled, incoming calls are answered at the first ring by the selected device (Desk Phone or Softphone). Users enable and disable this feature from the Dynamic Status dialog box on the Desktop Client.	
Calendar Integration	Calendar integration provides Dynamic Status updates based on the user's Busy and Out of Office settings in their Google Calendar, Outlook, Lotus Notes, or Exchange calendar.	
Page 1 of 5		



Table 2: Desktop Client UI Features (continued)

Feature Name	Description	Notes
Call Annotation	Call Annotation features are displayed in the Call Window when you are on an active call and include: <ul style="list-style-type: none"> <li>• <b>Notes:</b> Provides a text box to add notes about the call.</li> <li>• <b>Recorder<sup>1</sup>:</b> Records the current call.</li> </ul>	The recorder function is provided by the UC Advanced embedded softphone, which is a licensed feature (see Table 1 on <a href="#">page 23</a> ).
Call Control	Call Control features are displayed in the Call Window and provide one-click access to the following call control features: <ul style="list-style-type: none"> <li>• <b>Call Me Back (MCD systems):</b> Provides call me back notifications for internal calls only.</li> <li>• <b>Leave Station Message (Mitel 5000 systems):</b> Delivers a station message (flashing LED indicator) on the internal destination device.</li> <li>• <b>Hold/Retrieve Held:</b> Places/retrieves a call on hold.</li> <li>• <b>End Call:</b> Ends the call.</li> <li>• <b>Transfer, Conference:</b> Allows the user to complete a transfer or conference. Includes the complete, cancel, or consult associated actions.</li> <li>• <b>Split:</b> Places the party that joined the call last on hold. This feature is not supported by the Mitel 5000 communication system.</li> <li>• <b>Trade:</b> During a consult call or a split call, this control places the active party on hold, and makes the other party active.</li> </ul>	Call Me Back and Split are supported on MCD systems only.  Leave Station Message is supported on Mitel 5000 systems only.
Call Forwarding	The Call Forwarding feature allows users to forward calls to non-Personal Ring Group (PRG) destinations and dynamic extensions. In addition, users can configure forwarding for preferential contacts.	
Call Handoff	The Call Handoff feature allows users to either push an active call to another device or pull in a call to a selected device.	Requires a 3300 system running 10.3 and higher as well as MCD 4.2.
Call History	Provides a list of missed, received, and dialed calls that includes caller ID and presence information for known contacts.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file transfer, chat history, and user configurable chat alert sounds.	
Collaboration	Collaboration is an optional component that provides extended conferencing functions as well as provide annotation, file transfer, application sharing, desktop sharing, and video capabilities from a Mitel integrated conferencing product.	
Compact Mode	Compact Mode provides access to frequently-used UC Advanced features from a minimized interface that can be moved to any area of your desktop.	

Table 2: Desktop Client UI Features (continued)

Feature Name	Description	Notes
Configuration Options	Configuration options allow the user to customize the following features for the Desktop Client: <ul style="list-style-type: none"> <li>• Appearance</li> <li>• Calendar Integration</li> <li>• Call Notification</li> <li>• Chat Settings</li> <li>• Knowledge Management</li> <li>• Login Notification</li> <li>• PIM Integration</li> <li>• RSS Window</li> <li>• Teleworker</li> <li>• Softphone Settings</li> <li>• Contacts View</li> </ul>	
Console <sup>2</sup>	The UC Advanced Console is an optional component that provides attendant call handling functions such as answer, transfer, hold, and conference. When a user is licensed for the console, it is available from the Desktop Client main menu and Dynamic Status view.	Split Conference is supported on MCD systems only. Transfer to Hold is supported on Mitel 5000 systems only.
Contact Management	Corporate contacts are provided by the UC Advanced corporate directory. Users can view detailed information (including uploaded photos) for each corporate contact, as well as presence information. Users can import personal contacts from their PIMs, or create them manually, and then organize them into groups.	
Dynamic Status	Dynamic Status provides customized call routing, IM and video presence, and calendar integration for UC Advanced users. In addition to displaying the user's current Dynamic Status, the Dynamic Status view includes communication notification icons, which indicate new messages and missed calls.	
External Dialing	UC Advanced provides external dialing functionality for the following applications: <ul style="list-style-type: none"> <li>• <b>Microsoft Word and Excel:</b> Users must configure Smart Tags/Actions for external dialing from Word and Excel.</li> <li>• <b>Microsoft Outlook:</b> Users must configure Smart Tags/Actions for external dialing from Outlook, or use the TAPI service provider (TSP) that is automatically installed for Outlook PIM users.</li> <li>• <b>IBM Lotus Notes:</b> The Lotus Notes Toolbar provides external dialing from Lotus Notes.</li> <li>• <b>Microsoft Internet Explorer:</b> The UC Advanced Dialing Helper Add-On provides external dialing in IE.</li> </ul>	
Favorites	Favorites include the list of corporate and personal contacts that the user has assigned as a Favorite.	
Page 3 of 5		

Table 2: Desktop Client UI Features (continued)

Feature Name	Description	Notes
Hot Desking	Provides the ability to Hot Desk in and Hot Desk out of supported systems by a simple right-click operation.	This feature is limited to users on MCD communications platform only.
IM Client Integration	Users licensed for Window Live Messenger or Office Communicator Integration can launch an IM session from the Desktop Client with any contact who has a corresponding login for the application and is currently logged in to the application.	
Knowledge Management	Provides indexing and search functions to correlate files and e-mail messages with users' contacts.	
Launchpad	Provides easy access to frequently-performed tasks. Launchpad items are associated with actions (Dial a number, Browse to a URL, Run a program, and Explore a folder) and appear on the Launchpad as buttons.	
Notifications	Popup windows (incoming call, call me back, chat invitation, collaboration invitation, and login notification) and auditory alerts (new chat, chat received, knowledge management window, and login notification) provide users with notification when events occur.	
Phone Button Programming	Buttons can be configured by users on their 5312, 5320, 5324, 5330, 5340, or 5360 IP phone from the Desktop Client.	This feature is limited to users on MCD communication platforms only.
PIM Integration	Creates a connection between UC Advanced and the contacts in the user's PIM. Supported PIMs include Microsoft Outlook, IBM Lotus Notes, and Sage Software ACT!	
Presence	Presence information (telephony, video, UC chat, integrated IM) for corporate contacts uses <b>Dynamic Presence</b> (replacement for Universal Presence and On-Demand Presence).	
Presence on Mitel Sets	Users can configure presence information for multiple contacts on their 5320, 5330, 5340, or 5360 IP phone from the Desktop Client.	This feature is limited to users on MCD communication platforms only.
RSS Content	The RSS window provides access to scrolling Rich Site Summary (RSS) content such as news headlines, excerpts from discussion forums, or corporate information displayed in the RSS Window. The RSS window provides links to Web content and additional RSS feeds, as well as navigation capabilities.	
SIP-Based Softphone	Provides a SIP-Based Softphone to the Desktop Client	This feature is supported on MCD systems running 5.0 SP2 or 5000 running 5.1 or later release.
Page 4 of 5		

**Table 2: Desktop Client UI Features (continued)**

Feature Name	Description	Notes
Softphone	The Desktop Client provides an embedded softphone that users can use with a USB headset or handset to place and receive calls. The softphone extension must be configured on the PBX.	The UCA Softphone is not supported on the Inter-Tel Axxess systems. See Table 21 on <a href="#">page 83</a> for supported headsets and handsets.
Teamwork Mode	Teamwork Mode provides the ability for a desktop user to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status and chat are supported.	
Teleworker	Teleworker mode allows MCD users to connect to and access their MCD voice network through the UC Advanced softphone or IP desk phone from a remote location. In Teleworker mode, the remote UC Advanced client uses a secure SSL connection with the Mitel Border Gateway (MBG) for all communication between the client and the UC Server.	Supported on MCD systems with an MBG installed on site.
Tray Icon and Menu	Provides a visual indication of the user's telephony presence, message waiting indication, and menus for frequently-used features such as Set Status, Voice Mail, Missed Calls, and Do-Not-Disturb.	
Video Call/Presence	A video call includes an audio call established by the PBX and a video broadcast established by MCA. The user can configure video presence for each Dynamic Status to indicate if he or she is available for video calls. The Video Contacts view provides a list of contacts available for video calls.	Requires MCA 4.0 or later.
Visual Voice Mail	Provides access to the following voice mail features: <ul style="list-style-type: none"> <li>• Receive message waiting indications</li> <li>• Play, forward, and delete voice mail messages</li> <li>• View, forward, and delete fax messages</li> <li>• Change the voice mail PIN</li> </ul>	Visual Voice Mail is only available on systems with NuPoint UM voice mail.
Page 5 of 5		

1. The embedded softphone records and saves call recordings to the user's computer. It does not save the recordings in the user's voice mailbox like the PBX Record-A-Call (RAC) feature. Note that users cannot use the Recorder option in the Desktop Client and PBX RAC feature simultaneously. To use the UC Advanced record feature, the user must be provisioned with the Softphone licensed feature (see Table 1 on [page 23](#)).
2. SIP softphone should not be used with UC Advanced console.

## MiVoice for Lync Features

Table 3 provides descriptions for the main features accessed from MiVoice for Lync UI.

**Table 3: MiVoice for Lync UI Features**

Feature Name	Description	Notes
Auto Answer	When the Auto Answer feature is enabled, incoming calls are answered at the first ring by the selected device (Deskphone or Softphone).	
Conference	Allows the user to add a third-party to the call.	
Call Forwarding	The Call Forwarding feature allows users to forward calls using Call Forward Always, Call Forward No answer or Call Forward Busy options.	
Call History	Provides a list of missed, received, and dialed calls that includes caller ID (if available).	
Do Not Disturb	Users can enable and disable Do Not Disturb (DND). When DND is enabled, callers receive a busy tone or go to Voicemail (if programmed).	
Transfer	Allows the user to transfer the call (supervised and unsupervised transfers are supported).	

## Web Portal Features

Table 4 provides descriptions for the main features accessed from the UC Advanced Web-Portal.

**Table 4: Web Portal UI Features**

Feature Name	Description	Notes
Account Options	Provides a way for users to edit their Dynamic Extensions, update their password, and change their time zone.	
Call History	Provides call history information for missed, received, and placed calls.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file, chat history, and user configurable chat alert sounds.	
Contacts	Provides a list of corporate contacts, a search function, and a way to view contact details. With UCA 5.0 you can also group contacts.	
Dynamic Status	Displays users' current status and allows them to change, add, edit, and delete Dynamic Statuses.	
Messages	Provides a list of users' current voice mail and FAX messages, access to initialize and change the voice mail PIN, and a way to download them to the device.	

**Table 4: Web Portal UI Features (continued)**

Feature Name	Description	Notes
OfficeLink	Allows users to place calls from the Web and Mobile Portals using one of the devices configured for their UC Advanced account. You must have Personal Ring Groups (PRG) configured to use OfficeLink.	See <a href="#">page 66</a> for OfficeLink information.
Teamwork Mode	Teamwork Mode provides the ability for a Web-based client to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status and chat are supported.	

## UC Advanced Mobile for BlackBerry Features

Table 5 provides descriptions for the main features accessed from the UC Advanced Mobile for BlackBerry client.

**Table 5: UCA Mobile for BlackBerry UI Features**

Feature Name	Description	Notes
Call History	The user can access call history for missed, received, and dialed calls.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file transfer, chat history, and user configurable chat alert sounds.	
Calendar Integration	Integrates UC Advanced with your Exchange Server. Regardless of whether or not you are logged into Microsoft Outlook, your UC Advanced Dynamic Status can access your calendar availability information directly from the server and update your Dynamic Status appropriately.	
Configuration	After the application is installed, the user must run the <b>Setup Wizard</b> to configure basic UC Advanced options. The user can access credentials and settings at any time from the Settings – Options menu.	
Corporate Contacts	Allows the user to access all corporate contact information stored on the UC Server.	
Dynamic Status	This screen allows users to view and change Dynamic Status and add custom text to their Dynamic Status. The <b>Update Status</b> option in the main menu allows users to update their status based on the current GPS or Bluetooth location.	
Location Manager	The Location Manager allows users to associate a Dynamic Status with each of their saved locations. Selecting <b>Current Location</b> from the main menu allows the user to configure and save locations based on associated GPS and Bluetooth defined locations.	
Messages	The user can call voice mail, view, and play received messages.	
OfficeLink	Allows users to place calls from the mobile client using one of the devices configured for their UC Advanced account.	See <a href="#">page 66</a> for OfficeLink information.
Scheduler	Configures GPS and Bluetooth search intervals and time-out options to conserve battery power on your mobile device.	
Teamwork Mode	Teamwork Mode provides the ability for a BlackBerry user to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status and chat are supported.	

## UC Advanced Mobile for Android Features

[Table 6](#) provides descriptions for the main features accessed from the UC Advanced Mobile for Android client.

**Table 6: UCA Mobile for Android UI Features**

Feature Name	Description	Notes
Call History	The user can access call history for missed, received, and dialed calls.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file transfer, chat history, and user configurable chat alert sounds.	
Calendar Integration	Integrates UC Advanced with either your Google or Exchange Server. Regardless of whether or not you are logged into Google Calendar or Microsoft Outlook, your UC Advanced Dynamic Status can access your calendar information directly from the server and update your Dynamic Status appropriately.	
Configuration	After the application is installed, the user must run the <b>Setup Wizard</b> to configure basic UC Advanced options. The user can access credentials and settings at any time from the Settings – Options menu.	
Corporate Contacts	Allows the user to access all corporate contact information stored on the UC Server.	
Dynamic Status	This screen allows users to view and change Dynamic Status and add custom text to their Dynamic Status. The <b>Update Status</b> option in the main menu allows users to update their status based on the current GPS or Bluetooth location.	
Location Manager	The Location Manager allows users to associate a Dynamic Status with each of their saved locations. Selecting <b>Current Location</b> from the main menu allows the user to configure and save locations based on associated GPS and Bluetooth defined locations.	
Messages	The user can call voice mail, view, and play received messages.	
OfficeLink	Allows users to place calls from the mobile client using one of the devices configured for their UC Advanced account.	See <a href="#">page 66</a> for OfficeLink information.
Presence	Telephony, Instant Messaging and dynamic status presence.	
Scheduler	Configures GPS and Bluetooth search intervals and time-out options to conserve battery power on your mobile device.	
Softphone (SIP-Based)	Provides Softphone functionality to Android Client.	This feature is supported on 5000 and MCD systems only (MCD 5.0 SP2 and later release).



**Table 6: UCA Mobile for Android UI Features (continued)**

Feature Name	Description	Notes
Teamwork Mode	Teamwork Mode provides the ability for an Android user to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status, and chat are supported.	

## UC Advanced Mobile for iPad Features

[Table 7](#) provides descriptions for the main features accessed from the UC Advanced Mobile for iPad client.

**Table 7: UCA Mobile for iPad UI Features**

Feature Name	Description	Notes
Call History	The user can access call history for missed, received, and dialed calls.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file transfer, chat history, and user configurable chat alert sounds.	
Configuration	The user can download the application from the Apple Apps store or from iTunes.	
Corporate Contacts	Allows the user to access all corporate contact information stored on the UC Server.	
Dynamic Status	This screen allows users to view and change Dynamic Status and add custom text to their Dynamic Status. The <b>Update Status</b> option in the main menu allows users to update their status based on their current location.	
Location Manager	The Location Manager allows users to associate a Dynamic Status with each of their saved locations. Selecting <b>Current Location</b> from the main menu allows the user to configure and save locations based on their location settings.	
Messages	The user can access voice mail, view, and play received messages.	
OfficeLink	Allows users to place calls from the mobile client using one of the devices configured for their UC Advanced account.	See <a href="#">page 66</a> for OfficeLink information.
Presence	Telephony, Instant Messaging and dynamic status presence.	
Schedules	Configures search intervals and time-out options to conserve battery power on your mobile device.	
Softphone (SIP-Based)	Provides Softphone functionality to iPad Client.	This feature is supported on 5000 and MCD systems only (MCD 5.0 SP2 and later release).
Teamwork Mode	Teamwork Mode provides the ability for an iPad user to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status, and chat are supported.	

## UC Advanced Mobile for iPhone Features

Table 8 provides descriptions for the main features accessed from the UC Advanced Mobile for iPhone client.

**Table 8: UCA Mobile for iPhone UI Features**

Feature Name	Description	Notes
Call History	The user can access call history for missed, received, and dialed calls.	
Chat	Provides multi-party chat functionality for corporate contacts. Chat features include emoticons, timestamp, file transfer, chat history, and user configurable chat alert sounds.	
Configuration	The user can download the application from the Apple Apps store or from iTunes.	
Corporate Contacts	Allows the user to access all corporate contact information stored on the UC Server.	
Dynamic Status	This screen allows users to view and change Dynamic Status and add custom text to their Dynamic Status. The <b>Update Status</b> option in the main menu allows users to update their status based on the current location.	
Location Manager	The Location Manager allows users to associate a Dynamic Status with each of their saved locations. Selecting <b>Current Location</b> from the main menu allows the user to configure and save locations based on defined locations.	
Messages	The user can call voice mail, view, and play received messages.	
OfficeLink	Allows users to place calls from the mobile client using one of the devices configured for their UC Advanced account or from the phone itself.	See <a href="#">page 66</a> for OfficeLink information.
Presence	Telephony, Instant Messaging and dynamic status presence.	
Schedules	Configures search intervals and time-out options to conserve battery power on your mobile device.	
Softphone (SIP-Based)	Provides Softphone functionality to iPhone Client.	This feature is supported on 5000 and MCD systems only (MCD 5.0 SP2 and later release).
Teamwork Mode	Teamwork Mode provides the ability for an iPhone user to have certain UC Advanced functions without having a Mitel phone (without being tied to a PBX). Non-telephony based features such as contact grouping, presence, dynamic status, and chat are supported.	

## Communication Platform Features

In addition to the licensed features provided by UC Advanced (see Table 1 on [page 23](#)), users can access and use the features provided by the following supported communication platforms:

- [MCD Features](#), below
- [“Mitel 5000 Communication Platform Features”](#) on [page 50](#)
- [“Inter-Tel Axxess Features”](#) on [page 53](#)

Some PBX features may not be supported on the user’s desk phone or softphone. In the following tables, supported features are indicated by ✓ and features not supported are indicated by ✕.

### MCD Features

[Table 9](#) provides the MCD PBX feature matrix.

**Table 9: MCD PBX Feature Matrix**

Features	UC Advanced	
	Desk Phone	Softphone
Ability to work offline	✓	✓
Account Codes <sup>1</sup> – Default	✓	✓
Account Codes – System	✓	✓
Account Codes – Verified and Non-verified	Non-verified <sup>2</sup>	Non-verified <sup>2</sup>
ACD Support	✓	✓
Add Held	✓	✓
Advisory Message	✓	✓
Auditory Alerts (accessibility/disability)	✓	✓
Auto Answer	✓	✓
Auto-Answer	✓	✓
Auto-Hold	✓	✓
Broker’s Call	✕	✕
Calculator	✕	✕
Call Duration Display	✓	✓
Call Forward	✓	✓
Call Forward – Cancel All	✓ <sup>2</sup>	✓ <sup>2</sup>
Call Forward – Delay	✓ <sup>2</sup>	✓ <sup>2</sup>
Call Forward – Follow Me – End Chaining	✓	✕
Page 1 of 5		

**Table 9: MCD PBX Feature Matrix (continued)**

Features	UC Advanced	
	Desk Phone	Softphone
Call Forward – Follow Me – Reroute when Busy	✓	✗
Call Forward – Forced	✓	✓
Call Forward – Override	✓ <sup>2</sup>	✓ <sup>2</sup>
Call Forward profiles	✓	✓
Call Handoff	✓	✓
Call History	✓	✓
Call history / logs – local	✓	✓
Call history / logs – server-based	✓	✓
Call Me Back	✓	✓
Call Park	✗	✗
Call Park Retrieve	✗	✗
Call Pickup (Dialed, Directed, Clustered)	✓ <sup>2</sup>	✓ <sup>2</sup>
Call Privacy	✗	✗
Call timer and annotation tools	✓	✓
Call Waiting – Swap Automatic	✗	✗
Callback	✓	✓
Caller ID-based call routing	✓	✓
Camp-on	✗	✗
Clear All Features	✗	✗
Compression Support	✓	✓
Conference	✓	✓
Conference Application (controls Conference Unit)	✗	✗
Conference Split	✓ <sup>2</sup>	✓ <sup>2</sup>
Conference Unit Support (5305/5310)	✗	✗
Contact sync from Outlook to UC Advanced	✓	✓
Corporate Directory	✓ <sup>2</sup>	✓ <sup>2</sup>
Corporate Directory – LDAP sync (inc. Active Directory)	✓	✓
Corporate Directory – sync to MCD directory	✓	✓
Destination-based Call Display	✗	✗
Dial from PIM – Outlook 2003, 2007, 2010 (32 and 64 bit), Lotus Notes 8.0 and 8.5	✓	✓
Dial Tone – Outgoing Calls	✓	✓
Dialed Number Editing	✓	✓
Page 2 of 5		

Table 9: MCD PBX Feature Matrix (continued)

Features	UC Advanced	
	Desk Phone	Softphone
Direct Outward Dialing (DOD)	✓	✓
Direct Page – Initiate	✓ <sup>2</sup>	✓ <sup>2</sup>
Direct Page – Receive	✗	✗
Do Not Disturb	✓	✓
Drag-and-drop conference calls	✓	✓
Favorites menu	✓	✓
Feature Keys	✗	✗
Flash – Calibrated	✗	✗
Flash – Switchhook	✗	✗
Flash – Trunk	✗	✗
Flexible Answer Point	✓	✓
Gigabit Ethernet Stand Support	✓	✓
Group Listen	✗	✗
Group Page – Initiate	✗	✗
Group Page – Receive	✗	✗
Handset Receiver Volume Control	✓	✓
Handsfree Answerback	✗	✗
Handsfree Operation	✓	✓
Headset Mute Switch	✓	✓
Headset Operation	✓	✓
Hold	✓	✓
Hold Key Retrieves Last Held Call	✓ <sup>2</sup>	✓ <sup>2</sup>
Hold on Hold	✓	✓
Hot Desking	✓	✓
Hot Line	✗	✗
In-call control window allowing transfer, conference, hold and hang up	✓	✓
Knowledge Management	✓	✓
Language Change	✓	✓
Launch of UC Advanced at computer start	✓	✓
LCS integration	✓	✓
Licensing through the Mitel AMC	✓	✓
Line Interface Module Support	✗	✗

**Table 9: MCD PBX Feature Matrix (continued)**

Features	UC Advanced	
	Desk Phone	Softphone
Line Types and Appearances	✓	✓
Meet Me Answer	✗	✗
Messaging – Advisory	✓ <sup>2</sup>	✓ <sup>2</sup>
Messaging – Callback	✗	✗
Messaging – Dialed	✓	✓
Mobile Extension	✓	✗
Multiple Message Waiting Indicator	✗	✗
Music	✓	✗
Mute Key	✓	✓
Off-Hook Voice Announce	✗	✗
Override	✗	✗
Override Security	✗	✗
PC Programming Application Support (Desktop Tool)	✓ <sup>2</sup>	✓ <sup>2</sup>
Personal Directory	✓	✓
Phonebook	✓	✓
PIM Integration – ACT!	✓	✓
PIM Integration – Lotus Notes	✓	✓
PIM Integration – Outlook	✓	✓
PKM Support	✗	✗
Presence Indicator – Busy Lamp Field (BLF)	✓	✓
Presence Indicator – Computer	✓	✓
Privacy Release	✗	✗
Record a Call	✗	✓
Redial	✓ <sup>2</sup>	✓ <sup>2</sup>
Redial – Saved Number	✓ <sup>2</sup>	✓ <sup>2</sup>
Release	✓ <sup>2</sup>	✓ <sup>2</sup>
Reminder	✗	✗
Resiliency Support	✓	✓ <sup>3</sup>
Ringer Control (Pitch and Volume)	✗	✓
Ringing Line Select	✗	✗
RSS Window	✓	✓
Screen-pops on calls with ability to forward, send to voice mail	✓	✓
Secure instant messaging (chat) with file transfer	✓	✓
Page 4 of 5		

Table 9: MCD PBX Feature Matrix (continued)

Features	UC Advanced	
	Desk Phone	Softphone
Silent Monitor	✗	✗
Simplified Account Code Entry	✗	✗
SIP Support	✗	✗
Softkey Support	✗	✗
Speaker Volume Control	✓	✓
Speed Call – Pause	✗	✗
Speed Call – Personal	✓ <sup>2</sup>	✓ <sup>2</sup>
Speed Call – System	✗	✗
Speed Call Keys	✓ <sup>2</sup>	✓ <sup>2</sup>
Station-to-Station Dialing	✓	✓
SuperKey	✗	✗
Swap	✓	✓
System tray status icon	✓	✓
Tag Call (Malicious Call Trace)	✗	✗
Teleworker Support	✓	✓
Tone Demonstration	✗	✗
Transfer	✓	✓
Trunk Access	✗	✗
Trunk Answer From Any Station (TAFAS)	✗	✗
Visual Voice Mail	✓	✓
Voice Mail	✓	✓
Web browser	✓ <sup>2</sup>	✓ <sup>2</sup>
Wireless LAN Stand Support	✓	✓
WLM Integration	✓	✗

Page 5 of 5

1. Account code dialing is not supported on SIP softphone.

2. Functionality is limited or provided in a way different from a non-UC Advanced desk phone.

3. Resiliency is supported for Minet softphone using a 5020 IP set type.

Resiliency for SIP softphone is NOT supported.

For MCD communication systems, any number dialed from the Desktop Client that exceeds the Extension Length configured for the communication system will be automatically prefixed with the Dialing Prefix. To dial a number “as is,” start the number with a hyphen (-) character.

Table 10 provides the MCD Feature Access Codes (FACs).



Table 10: MCD Supported Feature Access Codes

Feature Number	Feature Name	Desk Phone	Softphone
2	ACD Silent Monitor	✓	✗
3	ACD Agent Login	✓	✗
4	ACD Agent Logout	✓	✗
5	Make Busy Setup	✓	✗
6	Make Busy Cancel	✓	✗
10	Call Forwarding – Busy – External Only	✗	✓
11	Call Forwarding – Busy – External and Internal	✗	✓
12	Call Forwarding – Follow Me	✓	✓
13	Cancel Call Forwarding – Busy – External and Internal	✗	✓
16	Call Forwarding – Follow Me	✓	✓
17	Cancel Call Forwarding – Follow Me	✓	✓
21	Call Forwarding – I Am Here	✓	✓
22	Call Forwarding – No Answer – External Only	✓	✓
23	Call Forwarding – No Answer – External and Internal	✓	✓
24	Call Forwarding – No Answer – Internal Only	✓	✓
25	Cancel Call Forwarding – No Answer – External and Internal	✓	✓
27	Cancel All Forwarding	✓	✓
29	Call Hold – Remote Retrieve	✓	✓
32	Call Pickup – Dialed	✓	✓
33	Call Pickup – Directed	✓	✓
40	Do Not Disturb	✓	✓
41	Do Not Disturb – Cancel	✓	✓
42	Do Not Disturb – Cancel Remote	✓	✓
43	Do Not Disturb – Remote	✓	✓
47	Last Number Re-dial	✓	✓
48	Message Waiting – Activate	✓	✓
49	Message Waiting – Deactivate	✓	✓
50	Message Waiting – Inquire	✓	✓

## Mitel 5000 Communication Platform Features

Table 11 provides the Mitel 5000 CP feature matrix.

**Table 11: Mitel 5000 CP PBX Feature Matrix**

Feature Name	Code	UC Advanced	
		Desk Phone	Softphone
Account Code <sup>1</sup> – All Calls Following	391	✓	✓
Account Code – Optional	390	✓	✓
ACD Agent Login	326	✓	✓
ACD Agent Logout	327		
ACD Agent Login/Logout Toggle	328		
ACD Agent Wrap-Up Terminate	329	✓	✓
Activate Door Relay <sup>2</sup>	332	✓	✓
Agent Help	375	✗	✗
Agent Help Reject	376	✓	✓
Answer (Ringing Call)	351	✓	✓
Audio Diagnostics	320	✗	✗
Automatic CO Access On/Off	360	✓	✗
Automatic IC Access On/Off	361	✓	✗
Automatic Trunk Answer	350	✓	✗
Background Music On/Off	313	✓	✓
Barge-In	386	✗	✗
Call Forward All Calls	355	✓	✓
Call Forward If Busy	357	✓	✓
Call Forward If No Answer	356	✓	✓
Call Forward If No Answer/Busy	358	✓	✓
Call Logging	333	✓	✓
Change Language	301	✓	✗
CO Hookflash	330	✓	✓
Conference	5	✓	✓
Data	340	✓	✗
Default Phone	394	✓	✗
Directories	307	✓	✗
Display Outside Party Name On/Off	379	✓	✗
Page 1 of 3			

Table 11: Mitel 5000 CP PBX Feature Matrix

Feature Name	Code	UC Advanced	
		Desk Phone	Softphone
Display Time/Date (ITP) Show IP Address (SIP)	300	✓	✗
Do-Not-Disturb Do-Not-Disturb Cancel Do-Not-Disturb On/Off	370 371 372	✓	✓
Do-Not-Disturb Override	373	✗	✗
Dynamic Extension Express On Dynamic Extension Express Off Dynamic Extension Express On/Off	363 362 364	✓	✓
Dynamic Extension Express – Handoff	388	✓	✓
Enhanced Speakerphone Enable	310	✗	✗
Feature Key Default	395	✓	✗
Group Listen	312	✗	✗
Handsfree On/Off	319	✓	✓
Headset Enable Headset Disable Headset On/Off	315 316 317	✓	✗
Hold – Individual	336	✓	✓
Hold – System	335	✗	✗
Hot Desk On/Off <sup>3</sup>	348	✓	✗
Hunt Group Remove Hunt Group Replace Hunt Group Remove/Replace	322 323 324	✓	✓
LCD Contrast Adjustment	303 <sup>4</sup>	✓	✗
Message	365	✓	✗
Message – Cancel	366	✓	✓
Message – Cancel Current	368	✓	✓
Message – Silent	367	✓	✓
Mute On/Off	314	✓	✓
Page	7	✓	✓
Page On/Off	325	✓	✗
Program Buttons	397 <sup>4</sup>	✓	✗
Program Phone Password	392	✓	✗
Queue Request	6	✓	✓
Record-A-Call	385	✓	✓
Redial	380	✓	✓

Table 11: Mitel 5000 CP PBX Feature Matrix

Feature Name	Code	UC Advanced	
		Desk Phone	Softphone
Redirect Call	331	✓	✓
Reminder Message	305	✓	✗
Reminder Message Cancel	306		
Remote Configuration – Disable	343	✓	✓
Remote Configuration – Display License Key	347	✓	✗
Remote Configuration – Enable	342	✓	✓
Remote Configuration – Reset	344	✓	✓
Remote Programming	359	✓	✗
Reverse Transfer (Call Pick-Up)	4	✓	✓
Review Keys	396 <sup>4</sup>	✓	✗
Ring Intercom Always On/Off	377	✓	✓
Ring Tone Selection	398	✓	✗
Routing Off	304	✓	✓
Station Monitor	321	✓	✓
Station Speed Dial	382	✓	✗
Station Speed Dial Programming	383	✓	✗
Steal	387	✗	✗
Switch Keymap	399	✓	✗
System Forward Enable	352	✓	✓
System Forward Disable	353		
System Forward On/Off	354		
System Speed Dial	381	✓	✓
Transfer to Hold	346	✗	✗
Transfer to Ring	345	✓	✓

Page 3 of 3

1. Account code dialing is not supported on SIP softphone.
2. This feature requires an HX Controller and Mitel 5000 v4.0 software.
3. This feature requires Mitel 5000 v5.0 software.
4. This feature must be completed on the phone.

Note the following for Mitel 5000 systems:

- Any number dialed from the Desktop Client that is not equal to the Extension Length configured for the communication system will be automatically prefixed with the Dialing Prefix. To dial a number “as is,” start the number with a hyphen (-) character.
- When entering feature codes in the Desktop Client using the Quick Connector, users should enter the hyphen character (-) before the digits to indicate to the UC Server that the digits are a feature code.

Also, some feature codes require additional digits to complete the feature. If users need to add digits following the feature code, they should first insert the hyphen character before entering the digits. For example, to use Station Monitor to monitor extension 1000, users would enter

-321-1000 in the Quick Connector.

- When entering feature codes using the Dial Pad, users can use the Special button to enter feature codes for on-call features. On call features include:
  - Agent help
  - Audio diagnostics
  - Barge in
  - Do-not-disturb override
  - Group Listen
  - System Hold
  - Steal
  - Transfer to hold

## Inter-Tel Axxess Features

Table 12 provides the Inter-Tel Axxess PBX feature matrix.



**Note:** The UC Advanced Softphone is not available with an Inter-Tel Axxess PBX.

**Table 12: Inter-Tel Axxess CCP PBX Feature Matrix**

Feature Name	Code	UC Advanced Desk Phone
Account Code – All Calls Following	391	✓
Account Code – Optional	390	✓
ACD Agent Login	326	✓
ACD Agent Logout	327	
ACD Agent Login/Logout Toggle	328	
ACD Agent Wrap-Up Terminate	329	✓
Agent Help	375	✗
Agent Help Reject	376	✓
Answer (Ringing Call)	351	✓
Audio Diagnostics	320	✗
Automatic CO Access On/Off	360	✓
Automatic IC Access On/Off	361	✓
Automatic Trunk Answer	350	✓

Page 1 of 3

Table 12: Inter-Tel Axxess CCP PBX Feature Matrix (continued)

Feature Name	Code	UC Advanced Desk Phone
Background Music On/Off	313	✓
Barge-In	386	✗
Call Forward All Calls	355	✓
Call Forward If Busy	357	✓
Call Forward If No Answer	356	✓
Call Forward If No Answer/Busy	358	✓
Call Logging	333	✓
Change Language	301	✓
CO Hookflash	330	✓
Conference	5	✓
Data	340	✓
Default Phone	394	✓
Directories	307	✓
Display Outside Party Name On/Off	379	✓
Display Time/Date (ITP) Show IP Address (SIP)	300	✓
Do-Not-Disturb	370	✓
Do-Not-Disturb Cancel	371	
Do-Not-Disturb On/Off	372	
Do-Not-Disturb Override	373	✗
Enhanced Speakerphone Enable	310	✗
Feature Key Default	395	✓
Group Listen	312	✗
Handsfree On/Off	319	✓
Headset Enable	315	✓
Headset Disable	316	
Headset On/Off	317	
Hold – Individual	336	✓
Hold – System	335	✗
Hunt Group Remove	322	✓
Hunt Group Replace	323	
Hunt Group Remove/Replace	324	
LCD Contrast Adjustment	303 <sup>1</sup>	✓
Message	365	✓
Message – Cancel	366	✓
Message – Cancel Current	368	✓
Message – Silent	367	✓

**Table 12: Inter-Tel Axxess CCP PBX Feature Matrix (continued)**

Feature Name	Code	UC Advanced Desk Phone
Mute On/Off	314	✓
Page	7	✓
Page On/Off	325	✓
Program Buttons	397 <sup>1</sup>	✓
Program Phone Password	392	✓
Queue Request	6	✓
Record-A-Call	385	✓
Redial	380	✓
Redirect Call	331	✓
Reminder Message	305	✓
Reminder Message Cancel	306	
Remote Programming	359	✓
Reverse Transfer (Call Pick-Up)	4	✓
Review Keys	396 <sup>1</sup>	✓
Ring Intercom Always On/Off	377	✓
Ring Tone Selection	398	✓
Routing Off	304	✓
Station Monitor	321	✓
Station Speed Dial	382	✓
Station Speed Dial Programming	383	✓
Steal	387	✗
Switch Keymap	399	✓
System Forward Enable	352	✓
System Forward Disable	353	
System Forward On/Off	354	
System Speed Dial	381	✓
Transfer to Hold	346	✗
Transfer to Ring	345	✓
Page 3 of 3		

<sup>1</sup>. This feature must be completed on the phone.

Note the following for Inter-Tel Axxess systems:

- Any number dialed from the Desktop Client that is not equal to the Extension Length configured for the communication system will be automatically prefixed with the Dialing Prefix. To dial a number “as is,” start the number with a hyphen (-) character.
- When entering feature codes in the Desktop Client using the Quick Connector, users should enter the hyphen character (-) before the digits to indicate to the UC Server that the digits are a feature code.

Also, some feature codes require additional digits to complete the feature. If users need to add digits following the feature code, they should first insert the hyphen character before entering the digits. For example, to use Station Monitor to monitor extension 1000, users would enter

-321-1000 in the Quick Connector.

- When entering feature codes using the Dial Pad, users can use the Special button to enter feature codes for on-call features. On call features include:
  - Agent help
  - Audio diagnostics
  - Barge in
  - Do-not-disturb override
  - Group Listen
  - System Hold
  - Steal
  - Transfer to hold



## About Account Synchronization

UC Advanced supports two types of synchronization to quickly populate the UC Advanced accounts list based on your existing PBX node, Active Directory (AD), or Lightweight Directory Access Protocol (LDAP) corporate directory. Synchronizer types include:

- **AD/LDAP Synchronizer:** Using this option you can populate the UC Advanced accounts database using the corporate AD or LDAP directory. The UC Server can integrate with single or multiple LDAP v3-enabled directory servers to import accounts. If you intend to use AD/LDAP synchronization to import accounts into UC Advanced, make sure your directory server supports LDAP v3. The Microsoft 2003 Server LDAP/AD server supports LDAP v3.



**Note:** Refer to the following topics in the UC Server Administrator online help for detailed information about AD/LDAP Corporate Directory Synchronizers:

- Synchronization Tab
  - Adding and Editing AD/LDAP Synchronizers
- **PBX Node Synchronizer:** Select this option if you want to populate the UC Advanced accounts database using the user/extension information programmed for the MCD, Mitel 5000 PBX, or Inter-Tel Axxess PBX node database.

To provide ongoing synchronization between UC Advanced and the AD/LDAP or PBX node directories, you can schedule automatic synchronizations. You can also complete manual synchronizations for either type of synchronizer.

In addition to synchronization, you can also populate the UC Advanced accounts list by manually creating accounts. Accounts that are created manually will automatically be configured with the default account settings.

## About Presence

The UC Advanced presence feature allows users to monitor other users on the system.

### Presence Server

Presence is provided by the Presence Server component on UC Server and consists of the following components which provide presence for UC Advanced users.

- **SIP Proxy:** A SIP-compliant proxy server that routes all the incoming SIP requests to the correct components in UC Server.
- **SIP Subscription Manager:** Abstracts the SIP SUBSCRIBE/NOTIFY semantics from the application and implements the application-specific logic.
- **IM Server:** Maintains state information for offline IM messages and conferences. The IM server uses the SIP Subscription Manager to track incoming SIP SUBSCRIBE requests for offline IM and conference states. The SIP Subscription Manager also sends the corresponding SIP NOTIFY requests to subscribers when it receives state changes from the IM Server.

### Presence Modes

UC Advanced utilizes **Dynamic Presence** which means the desktop client will automatically display presence for the contacts in the current view.



**Note:** When the user is filtering or scrolling the contact list there may be a brief delay between when the contact is displayed and when the presence for the contact is displayed. This delay is the amount of time it takes for the client to request the presence from the server and for the server to respond with the presence updates. This delay is minimal, however there are certain conditions like server load which may increase this delay.



**Note:** Users who are licensed for the Console Option will work in much the same way as the main contact list. The client will only subscribe to presence for contacts that are visible. Refer console users to the **Contacts Context Menu** topic in the Desktop Client online help for instructions about showing and hiding presence for contacts.








## Types of Presence

When the Presence licensed feature is enabled for a user, the following information is displayed in the Desktop Client Contacts view for UC Advanced contacts:

- **Dynamic Status:** Incorporates the following elements to provide status and availability information for UC Advanced users:
  - *Dynamic Status Name:* Provides a simple description for the Dynamic Status.
  - *Default message/custom text:* Provides additional information for the selected Dynamic Status.
  - *Calendar advisory text:* Provides advisory messages that indicate a user's calendar availability timing summary based on their Google, Outlook, Lotus Notes or Exchange calendar entries (for example, "In appointment until 2:30 PM", "Free until 11 AM").








**Note:** By default, all users who log in to UC Advanced are provided with a list of default Dynamic Statuses. The **Status unknown** message indicates that the contact has not logged in to UC Advanced.

- **Telephony presence:** The following icons indicate telephony presence for UC Advanced corporate and peered contacts:
  -  Indicates that the contact's phone is idle.
  -  Indicates the contact's phone is ringing.
  -  Indicates that the contact is on hold.
  -  Indicates that the contact's phone is busy or has enabled Do-Not-disturb.
  -  Indicates that the contact's telephony presence is offline.
- **UC Advanced chat presence:** The following icons indicate chat presence for corporate and federated contacts:
  -  Indicates that the contact is online and available for chat.
  -  Indicates that the contact is away from his or her computer.
  - No icon is present when the contact is offline.



**Note:** The icons above are also used to display IM presence for federated contacts (see [page 27](#)).

- **Instant Message presence:** If you are licensed to use the Windows Live Messenger or Office Communicator Integration features, UC Advanced displays presence icons for contacts who have Windows Live Messenger or Office Communicator logins.
  -  Indicates that the contact is online for his or her Windows Live Messenger account.
  -  Indicates that the contact is offline for his or her Windows Live Messenger account.
  -  Indicates that the contact is online for his or her Office Communicator account.
  -  Indicates that the contact is offline for his or her Office Communicator account.
- **Video presence:** UC Advanced displays presence icons for corporate contacts who are configured to engage in video calls:
  -  Indicates that the contact is currently accepting video calls.

- No icon indicates that the contact is offline for video.

## Dynamic Status

Dynamic Status provides a way for the user to control and communicate their presence and availability, and customize their call routing. UC Advanced provides default Dynamic Statuses as per Table 13 [Dynamic Status defaults](#). The user can add, edit, and delete Dynamic Statuses as needed on their individual clients (for example, see Manage Statuses on Desktop Client).

**Table 13: Dynamic Status defaults**

Phone Configuration	In the office	Mobile	Working from home	Do not Disturb	Gone for the day
Deskphone and no Voicemail number	X				
Deskphone and has Voicemail number	X			X	X
Deskphone, softphone and no Voicemail	X		X		
EHDU Deskphone and no Voicemail number	X	X			
Deskphone, Softphone and Voicemail number	X		X	X	X
Deskphone, Softphone, EHDU number and Voicemail (need PRG)		X	X	X	X
Deskphone1, Deskphone2, EHDU and Voicemail (need PRG)	X	X	X	X	X
Deskphone1, Deskphone2 and Voicemail	X		X	X	X



**Note:** Softphone or deskphone 2 is treated as Home IP phone.



**Note:** Additional EHDU numbers (after the first one) are not taken into account in the setting of dynamic statuses.



**Note:** The above logic is executed only when the account has no account statuses defined in the account status table in UCA server. The account will be in this default state of 'no statuses' until the user connects to UCA server from one of the UCA clients, the very first time.



**Note:** If account has 1 or more valid account status, changes in account's phone numbers or adding voicemail number later will not create additional statuses.



**Note:** The web service call to create the default account statuses will also create the favorites and loginNotify group for that account. The loginNotify group is created if it did not exist before. The favorites group is created if no user defined groups exists for that account.

## About Collaboration

Mitel supports the Mitel Collaboration Advanced (MCA) - formerly known as Audio and Web Conferencing (AWC) product to provide integrated collaboration features to UC Advanced users. MCA collaboration features include video calls, audio conferences, web conferences, and other tools such as desktop and application sharing, whiteboarding, and annotation.

The collaboration server is the central hub for all conference sessions. Conferences require a server where the conference sessions are hosted, and all conference information flows through the server before being distributed to the UC Advanced Desktop Client.

MCA is packaged on the Mitel Applications Suite (MAS) server, which is connected to the IP network. The MAS server provides access to a Web-based administrator interface for configuring MCA, scheduling conferences, viewing conference calls, and administering collaboration controls. Users can access all interfaces through either HTTP or HTTPS.

For product information for MCA, refer to the *Mitel Collaboration Advanced Configuration and Maintenance Manual* on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

Note the following when implementing collaboration integration for UC Advanced:

- To use collaboration features users must be licensed for the Collaboration Integration feature (see Table 1 on [page 23](#)).
- If users receive a licensing error message when attempting to use collaboration features, you may need to increase the number of collaboration port licenses for the MCA collaboration server.
- The UC Server does not control the user limit for the collaboration servers. This is handled by the MCA collaboration server.
- You can configure only one default MCA server. If more than one Collaboration server is in use at the site, you must specify which MCA server should be used on a per-account basis in the UC Server Administrator interface (see [page 123](#)).
- UC Advanced v6.0 requires MCA 5.0 or later. Earlier versions of MCA or AWC are not compatible with UC Advanced v6.0.

## About SIP

UC Advanced supports SIP - Session Initiation Protocol. UCA Desktop client as well as Mobile Clients (Android, iPad and iPhone) all support a SIP softphone and can operate with UC360 devices and MCA (Mitel Collaboration Advanced). In addition, UCA is capable of operating with a number of third party SIP Servers and SIP end points such as SIP phones, Audio Conference Units and Video Conference Units.

Mitel maintains a SIP Centre of Excellence (SIP CoE); the CoE performs interoperability testing between third party devices and Mitel SIP devices. The CoE generates documents that cover the results of the interoperability tests and how the devices should be configured for successful interoperation.

For the complete list of devices that can interoperate with please refer to Knowledge Base article called the SIP Technical Reference Guide 08-5159-00014. This Reference Guide can be found on Mitel On-Line under 'Support' and then under 'Mitel Knowledge Base'.

## About OfficeLink

UC Advanced 3.2 and later includes the OfficeLink feature. Using this feature, users can place calls from the devices configured for them on the PBX from the following UC Advanced interfaces:

- Web Portal
- UCA Mobile for BlackBerry client interface
- UCA Mobile for Android client interface
- UCA Mobile for iPad client interface
- UCA Mobile for iPhone client interface

## PBX Software Requirements

Supported device types and OfficeLink functionality are determined by the following factors:

- The PBX that is connected to the UC Server
- The software version running on the PBX

At a minimum, the UC Advanced OfficeLink feature requires the following PBX system software:

- Mitel Communications Director (MCD) v4.2 or later
- Mitel 5000 v4.0 or later
- Inter-Tel Axxess v11.017 or later

Devices must be configured as follows in the PBX programming application to be available for use with the UC Advanced OfficeLink feature:

- **Mitel Communications Director (MCD) System Administration Tool:** UC Advanced users can use devices configured in the user's Personal Ring Group (PRG) for the OfficeLink and Multi-Device User Group (MDUG) features.



**Note:** Multi-Device User Groups are supported for MCD 5.0 and later ONLY.

PRGs are an association of two or more devices for a single user under a common Directory Number (DN). Complete the following programming from the v4.0 or later MCD System Administration Tool for the OfficeLink feature:

- Configure PRGs using the Personal Ring Group Assignment form. See [page 93](#) for details.
- If required, define a DN to be used as the prime member of the PRG using the Multiline IP Set Configuration form. See [page 92](#) for details.
- Complete these same fields from the 5.0 or later MCD system Administration Tool for the OfficeLink feature for either PRG or MDUG. See [page 92](#) for details.



- **Mitel 5000 Database Programming:** UC Advanced users can use devices configured as the user's Associated Destinations for the OfficeLink feature. Associated Destinations provide advanced call routing capabilities for the PBX and UC Advanced. Complete the following programming from Mitel 5000 DB Programming for the OfficeLink feature:
  - Configure the fields and options for the user in the Users folder (Users -<User>). See [page 97](#) for details.
  - For Mitel 5000 v5.0 and later systems, configure the OfficeLink Assistant (System -Devices and Feature Codes - **Assistants**). See [page 96](#) for details.



**Note:** The Inter-Tel Axxess system supports basic OfficeLink functionality with desk phones only (see [page 67](#)). No special programming is required for the OfficeLink feature.

If you are using PBX synchronization to populate the UC Advanced account database, after programming the PBX as described above you will need to complete a manual PBX synchronization from the UC Server Administrator interface (PBX Nodes tab) to provide OfficeLink functionality to UC Advanced accounts.

## Supported Device Types

Depending on the PBX and the software version running on the PBX, the following device types can be used with the UC Advanced OfficeLink feature:

- **Desk phones:** Includes the list of supported desk phones (see Table 17 on [page 77](#)) for the following PBXs:
  - MCD v4.2 and later
  - Mitel 5000 v3.2 and later
  - Inter-Tel Axxess v11.017 and later
- **Softphones:** Includes the UC Advanced softphone for the following PBXs:
  - MCD v4.2 and later (5.0 SP2 required for SIP softphones)
  - Mitel 5000 v3.2 and later (5.1 or later for SIP softphones)



**Note:** The UC Advanced softphone is not supported for the Inter-Tel Axxess PBX.

- **External Devices:** Includes external devices (for example, mobile devices) that meet the following requirements:
  - *MCD v4.1 and later:* OfficeLink calls are allowed from external devices that are logged in to the user's External Hot Desk User (EHDU) extension.
  - *Mitel 5000 v5.0 and later:* OfficeLink calls are allowed from external devices programmed as a user's Associated Destination.



**Note:** The OfficeLink feature is not supported for external devices in the MCD v4.0, Mitel 5000 v4.0, and Inter-Tel Axxess v11.017 PBXs.

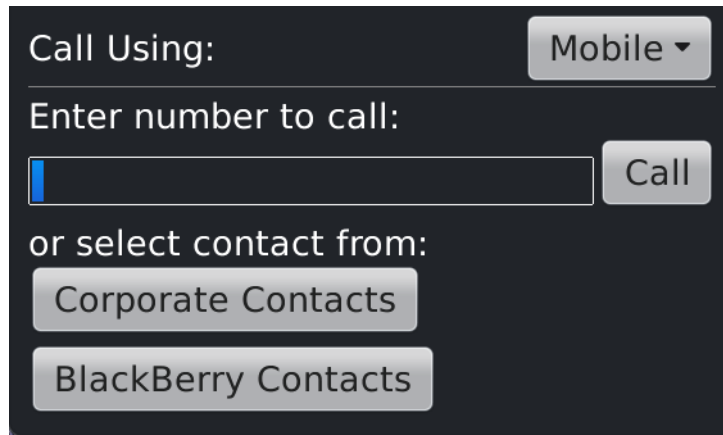
- **SIP Devices:** Includes SIP devices connected to an MCD 5.0 SP2 or later system.



**Note:** The OfficeLink feature is not supported for Mitel 5000 or Inter-Tel Axxess SIP devices.

## OfficeLink Functionality

When users access the OfficeLink feature , the **Place OfficeLink Call** dialog box appears. The example below shows the **Place OfficeLink Call** dialog box from the BlackBerry.



**Figure 12: BlackBerry Place OfficeLink Call Dialog Box**

From the **Place OfficeLink Call** dialog box, users must specify the following:

- The number to call
- The device to place the call from

When users activate the OfficeLink feature, the response from the PBX varies based on the software version running on the PBX and the device the user has selected.

Table 14 [PBX Response to OfficeLink Feature](#) provides the PBX responses which include:

- **Click to Call:** The PBX immediately places a call to the specified number from the specified device. This behavior is also known as Click to Call.
- **Remote Click to Call:** The PBX places a call to the device the user selected. After the user answers the call on the device, the PBX immediately places a call to the specified number. This behavior is also known as Remote Click to Call.

Table 14: PBX Response to OfficeLink Feature

PBX	Software Version	Device			
		Desk Phone	Softphone	External Device	SIP Device
MCD	4.0	Click to Call	Click to Call	N/A	N/A
	4.1 and later	Click to Call	Click to Call	Remote Click to Call	Remote Click to Call
Mitel 5000	4.0	Click to Call	Click to Call	N/A	N/A
	5.0 and later	Click to Call	Click to Call	Remote Click to Call	N/A
Inter-Tel Axxess	11.017 and later	Click to Call	N/A	N/A	N/A



Devices marked as Not Applicable (N/A) are not supported OfficeLink device types for the PBX software version.

## Basic UC Client

As part of UC Advanced 6.0, the Desktop and Web client can be configured as a basic client using the default UCA profile.

### *Admin Portal Changes*

To accommodate the Basic UC client feature, the UCA admin portal features tab was simplified in UCA 6.0. See Feature Tab under Admin Portal help.

On the UCA server, if an account is assigned the Default Profile, it will be treated as a Basic UC account. In other words, users will only have access to the allowed features list below.

### *Desktop and Web Client impact*

Only default profile features listed below are supported.

### *Licensing*

No impact.

### *Allowed features*

UCA server will pass the following list of allowed features to the desktop or web client on login:

Allowed Features	Desktop Client	Web Client
Blind Transfer	X	X
Call Forwarding	X	
Compact Mode	X	
Contact Groups	X	X
Corporate Contact	X	X
External Dial	X	
Missed Call Logs	X	X
Make and Receive Call	X	X
Office Communicator Integration	X	
Phone Button Programming	X	
RSS Window	X	
Visual Voice Mail	X	X
WLM Integration	X	

## Teamwork Mode

Teamwork Mode provides the ability for a user to have certain UC Advanced functions without having a Mitel phone. In other words, a user will still be able to use certain non-telephony based features within the client even though the user does not have a desk phone or softphone.



**Note:** Prior to release 5.1, a UC Advanced user without any devices online and a hot desk user that was not logged in would go into offline mode. However, as of UC Advanced 5.1 if the user has no devices associated with their account, they automatically go into **Teamwork Mode**.

### *Licensing*

There are no new or additional licenses required specific to the Teamwork Mode feature. Licenses for individual features such as Chat, Visual Voicemail, etc...are still required.

### *Client Impacts*

Since Teamwork Mode users have no devices associated with their account, telephony specific features will be hidden or not available on the following clients:

- Desktop client
- Android client
- BlackBerry client
- iPad/iPhone clients
- Web client

However, features such as contact grouping, presence, dynamic status and chat are supported.

### *User Interface*

Teamwork Mode is not something the user can change and therefore there will be no indication that the user is running in Teamwork Mode. A user in Teamwork Mode will still appear in the contact list of other UCA clients but without telephony presence. In addition, a user in Teamwork Mode will still be able to see the telephony presence of other contacts if these are available.

### *Routing Information*

The main screen on all mobile and web clients displays routing information for the user's current status. This section will be hidden for users in Teamwork Mode.

### *OfficeLink*

OfficeLink functionality will be hidden from the user in Teamwork Mode. However, native dialing will still be available from the various clients, for example a BlackBerry user is still able to use the BlackBerry Smart Dialing feature to call other UC Advanced users from the Company Directory.

### *Call History*

The Call History feature will be hidden for Teamwork Mode users.

## UC Advanced for VMware Horizon View

Unified Communicator Advanced (UCA) version 5.0 introduced support for VMware Horizon View. UC Advanced for VMware Horizon View now enables a UCA softphone to function as a plug-in to VMware View virtual desktops. For the vUCA 6.0 client, VMware View 5.0, View 5.1 and View 5.2 are supported (see Table 15 on [page 72](#)). For more information, also see VMware Horizon View support documentation.

The following are the supported VMware Horizon View configuration attributes:

- Linked-Clone virtual desktop pools
- Dedicated-Assignment desktop pools
- Floating-Assignment desktop pools
- Full VM desktop
- View Persona Management



**Note:** Floating-Assignment desktop **with** View Persona Management is **strongly recommended**. However, there are situations where View Persona Management is not desirable, for example, where the administrator want all data to be wiped clean between sessions (eg. kiosk, guest access).



**Note:** Local mode and Windows Roaming Profile are **NOT** supported.

### *UCA Direct Media*

With UCA Direct Media architecture, the real-time sensitive media path flows directly between any two endpoints. It does not need to be processed in the VDI (Virtual Desktop Infrastructure) back end or traverse the WAN/Internet paths between the endpoints and the backend. This architecture prevents “tromboning” which has scalability issues resulting from a topology requiring extensive VDI backend use.

Referring to Figure 13 on [page 73](#), the basic system consists of:

- A collection of View virtual desktops, managed by the View Connection Server
- VMware Horizon View Connection Server - this manages the View sessions
- A collection of physical endpoints (Thin Clients / PC's running View Client), used to present the virtual desktop to the end user
- VMware Horizon View Agent software
- VMware Horizon View Client software
- Mitel Call Director (MCD)
- UCA Server
- UCA Client in the View environment, this resides in the virtual desktop

- UCA Client Plugin, installed in the physical endpoint in the View environment, this contains the media portion of the UCA Client and handles the actual media streaming.

**Note:** The version of UCA Client Plugin installed in the physical endpoint device must align with the version of the UCA Client installed in the virtual desktop for correct functioning of UCA on VMware Horizon View. For more information, refer to the UCA Release Notes.

The View media services API, running over the PCoIP side channel to the View client, is used to control media functions of the UC Client Plugin in the physical client device.

Table 15 and Table 16 provide VMware Horizon view version and feature support in UCA environment.

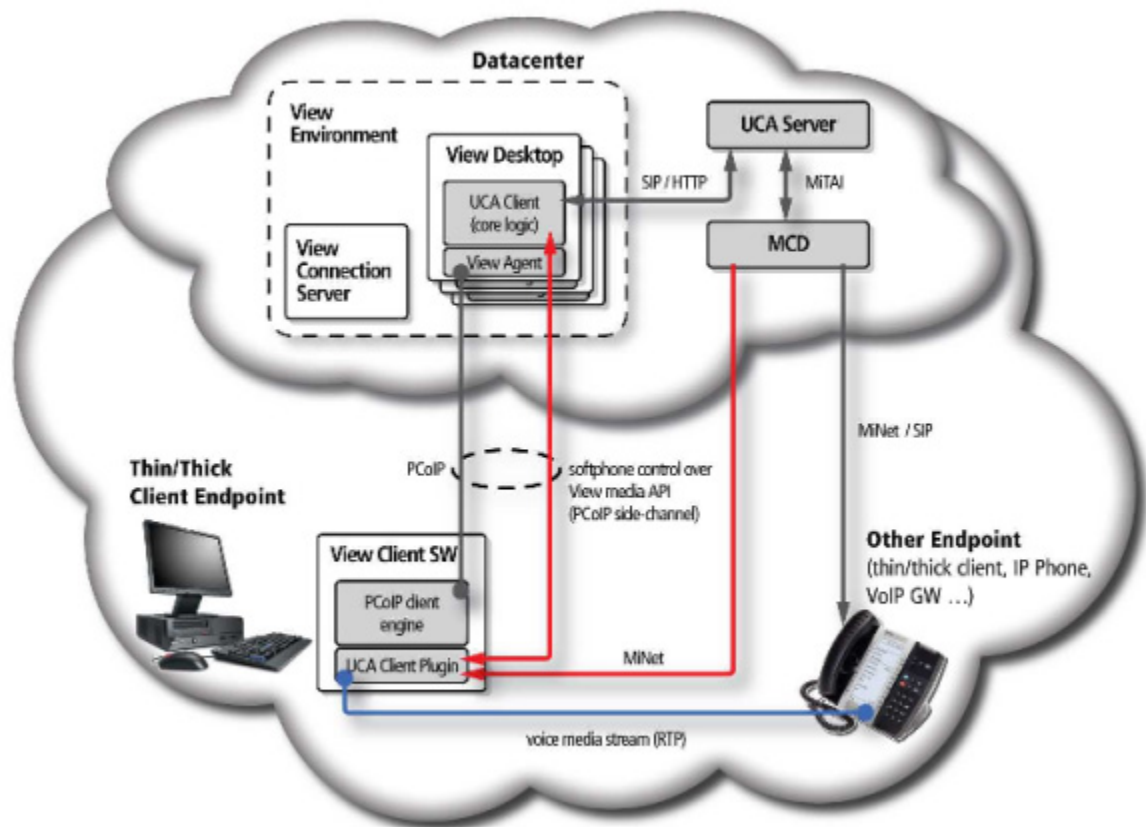
**Table 15: vUCA / VMware Horizon View version support**

UCA product release	View 4.6	View 5.0	View 5.1	View 5.2
vUCA 6.0	No	Yes	Yes	Yes
vUCA 5.1 (Includes softphone with direct media)	No	Yes	Yes	No
vUCA 5.1 (desk phone only)	Yes	Yes	Yes	No
vUCA 5.0 SP1 (Includes softphone with direct media)	No	Yes	Yes	No
vUCA 5.0 (desk phone only)	Yes	Yes	Yes	No

**Table 16: vUCA / VMware Horizon View feature support**

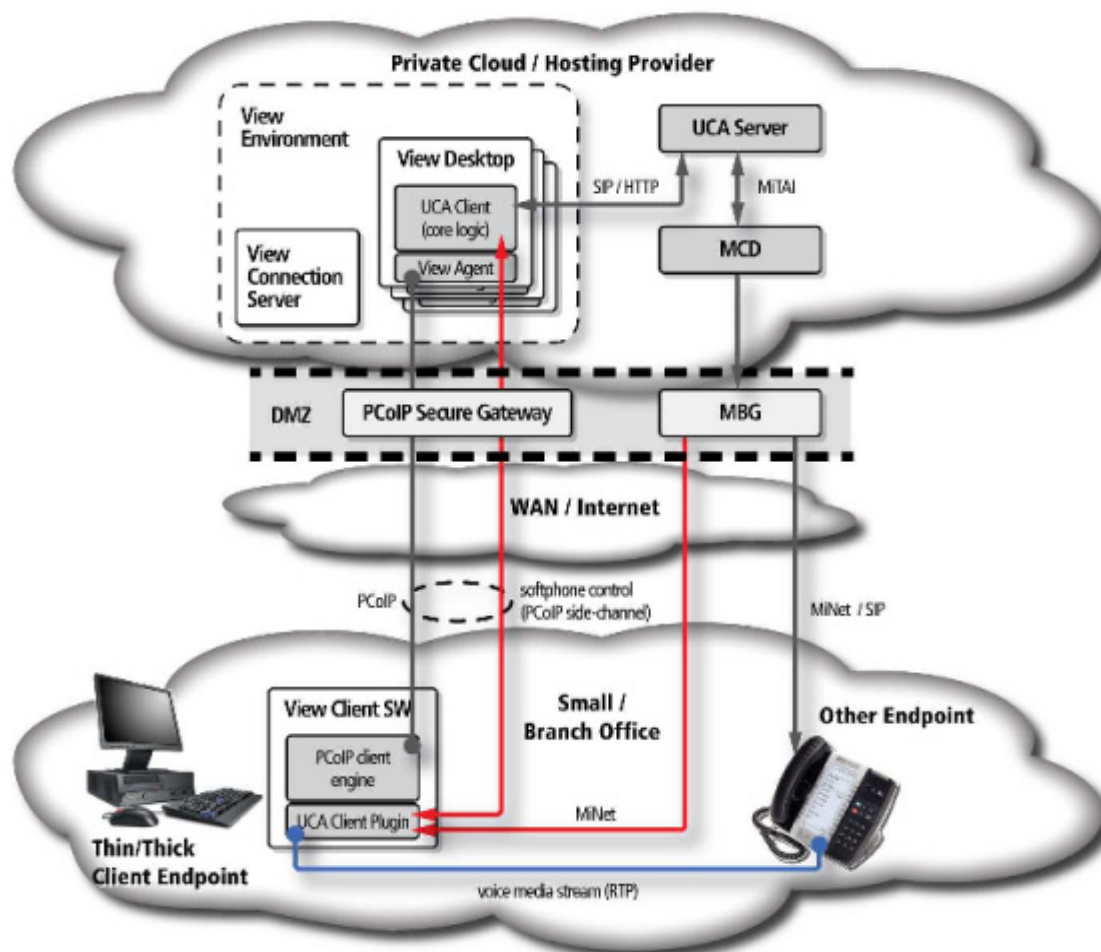
	Display Protocol		View 5 feature						
	PCoIP	RDP	Full VM	Linked Clone VM	Dedicated Desktop	Floating Desktop	View Persona Management	Local Mode	Windows Roaming Profile
vUCA6.0 (desk phone)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
vUCA 6.0 (softphone)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No
vUCA 5.0 SP1 (softphone)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No
vUCA 5.1 (desk phone)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
vUCA 5.1 (softphone)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No
vUCA 5.0 (desk phone)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No





**Figure 13: Flat Network Topology**

In a more complex architecture shown in Figure 14 on [page 74](#) below, Mitel Border Gateways (MBG) can be used to include remote users such as a branch or small office into the VMware Horizon view solution. A network DMZ configuration is used to contain the PCoIP Secure Gateway (also known as Security Server) and MBG components.



**Figure 14: Remote Office / Hosted Office Topology**

More complex configurations are possible. For more information, refer to the UCA Engineering Guidelines.

# CHAPTER 3

## SPECIFICATIONS



## Introduction

This chapter provides system hardware and software requirements, capacities, and network guidelines for UC Advanced installations.

## System Requirements

This section provides the system hardware and software requirements for UC Advanced.

### PBX Requirements

To use UC Advanced, integrated users must have either a desk phone, softphone or both configured on one of the following Mitel communication platforms and versions:

- Mitel Communications Director (MCD) v4.2 or later (5.0 SP2 is required for SIP softphone)
- Mitel 5000 Communications Platform (CP) v3.2 or later (5.1 is required for SIP softphone)
- Inter-Tel Axxess Converged Communications Platform (CCP) v11.017 or later

This guide assumes that you are familiar with the programming interface for the PBX installed on site. UC Advanced requires certain fields and options be programmed correctly for the PBX to provide integration with the communication platform. Programming interfaces include:

- MCD System Administration Tool
- Mitel 5000 Database (DB) Programming
- Inter-Tel Axxess Database (DB) Programming

Table 17 [Supported Mitel Phones](#) provides the list of supported desk phones for UC Advanced. In the following table, supported phones are indicated by ✓ and phones not supported are indicated by ✕.

**Table 17: Supported Mitel Phones**

Mitel Phone Model	MCD PBX	Mitel 5000 PBX	Inter-Tel Axxess PBX
4015 Digital Telephone	✓	✕	✕
4025 Digital Telephone	✓	✕	✕
4150 Digital Telephone	✓	✕	✕
5005 IP Phone	✓	✕	✕
5010 IP Phone	✓	✕	✕
5020 IP Phone	✓	✕	✕
5140 Digital Telephone	✓	✕	✕
5212 IP Phone	✓	✕	✕
5215 IP Phone	✓	✕	✕

Page 1 of 2

Table 17: Supported Mitel Phones (continued)

Mitel Phone Model	MCD PBX	Mitel 5000 PBX	Inter-Tel Axxess PBX
5220 IP Phone	✓	✗	✗
5224 IP Phone	✓	✗	✗
5304 IP Phone	✓	✓	✗
5312 IP Phone	✓	✓	✗
5320 IP Phone	✓	✓	✗
5324 IP Phone	✓	✓	✗
5330 IP Phone	✓	✓	✗
5340 IP Phone	✓	✓	✗
5360 IP Phone	✓	✓	✗
5602 SIP Phone	✓	✗	✗
5603 SIP Phone	✓	✓	✗
5604 SIP Phone	✓	✓	✗
5606 SIP Phone	✓	✗	✗
5607 SIP Phone	✓	✓	✗
5610 SIP Phone	✓	✓	✗
8520 Digital Telephone	✗	✓	✗
8528 Digital Telephone	✗	✓	✗
8560 Digital Telephone	✗	✓	✗
8568 Digital Telephone	✗	✓	✗
8620-2 IP Phone	✗	✗	✓
8622 IP Phone	✗	✓	✗
8660 IP Phone	✗	✗	✓
8662 IP Phone	✗	✓	✓
IP Plus	✗	✗	✓
IPSLA	✗	✗	✓
Navigator IP Phone	✓	✗	✗
Turret	✓	✗	✗

Page 2 of 2



**Note:** SIP phones support a limited PBX feature set.

## UC Server Requirements

UC Advanced provides two options for the UC Server component:

- **UC Advanced Software:** Includes the UC Server software blade. This option requires the customer to:
  - Purchase and install a Mitel Standard Linux® (MSL) approved hardware platform.
  - Download, install, and configure the MSL operating system on the hardware platform.
  - Download, install, and configure the UC Advanced software blade on the hardware platform.
- **UC Advanced Virtual Appliance:** Includes the packaged MSL operating system and UC Server software in an Open Virtualization Format (OVA) file. This option requires the customer to purchase a virtualization license and install the virtual appliance in a pre-established VMware environment. Note that the UC Advanced application is also included as part of the MAS virtual appliance as of MAS version 3.0.

Requirements for the standalone UC Server virtual appliance are listed in Table 18 [UC Advanced Virtual Appliance Requirements](#).

**Table 18: UC Advanced Virtual Appliance Requirements**

Component	Requirement	Version
Environment	An established VMware virtual environment.	Refer to the VMware documentation available on the <a href="http://www.vmware.com">VMware Web site</a> ( <a href="http://www.vmware.com">http://www.vmware.com</a> ).
Server	A Nehalem based server with <a href="#">Mitel BIOS settings</a> .	
Hard Disk Space	30 GB disk space	
CPUs	2 virtual CPUs	
Memory	2 GB Memory	
VMware Software	VMware® ESX or ESXi™	v4.1 or higher. <sup>1</sup>
	VMware vSphere™	
	vSphere Client	
Virtualization License		

<sup>1</sup> See Virtual Appliance Deployment Guide <http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf>

See [page 80](#) for additional virtualization information.

### About Virtualization

UC Server is provided in virtual appliance form for customers who have an established VMware environment in place. The virtual appliance includes the MSL operating system and the UC Server software blade. Running the UC Server within a VMware environment requires a license that allows usage in a virtualized environment ((for more information see <http://edocs.mitel.com/TechDocs/Solutions-Guides/BP-Virtualization.pdf>).

The vSphere virtual environment supports the following VMware infrastructure capabilities with UC Server:

- Virtual machine management tools, including:
  - Virtual Appliance Deployment (Import)
  - Export OVA
  - Power On
  - Shutdown
  - Reset/Restart
  - Cold Migration
  - Snapshot (Powered Off)
  - Cloning
  - Health Monitoring
  - Performance reports
- vMotion



**Note:** UC Advanced virtual appliance may experience service degradations during a vMotion operation, but will recover upon completion of the operation.

- Storage vMotion
- High Availability
- Distributed Resource Scheduler
- Distributed Power Management
- VMware vStorage APIs
- Data Recovery



**Note:** UC Advanced virtual appliance supports VMware Data Recovery operation only during off-hours or in a maintenance window where disk I/O activities are limited.

- Site Recovery Manager (SRM)



UC Advanced virtual appliance requires application-specific configuration to support the VMware SRM operation. During your SRM planning phase, contact the [Mitel Professional Services group](#) to assist with the deployment of UC Advanced virtual appliance.

For additional information about the VMware vSphere infrastructure, ESX, and ESXi, refer to the VMware documentation available on the [VMware Web site](http://www.vmware.com) (<http://www.vmware.com>).



## Mitel Integrated Application Requirements

The following Mitel applications can be integrated with the UC Advanced installation:

- NuPoint UM Voice Mail application, v4.0 or later (MCD and Mitel 5000 only)
- Mitel Collaboration Advanced (MCA - formerly known as Audio and Web Conferencing) Collaboration application, v4.0 or later
- Mitel Border Gateway (MBG), v7.1 or later (MCD only)
- Mitel UC Mobile, v1.7 or later (MCD only)

Basic server requirements for the integrated Mitel applications are listed in Table 19 [Mitel Integrated Applications Server Requirements](#).

**Table 19: Mitel Integrated Applications Server Requirements**

Component	Requirement	Version
Hardware Platform	An approved MSL hardware platform.	Refer to the <a href="#">Application/MSL Matrix</a> available on Mitel Online for a list of approved hardware platforms.
Operating System	MSL	v10.0

Most of the Mitel applications listed above are integrated components of Mitel Application Suite (MAS). Each application may include application-specific client and server requirements. Refer to the individual application documentation for application-specific requirements. All Mitel applications are licensed through the Mitel Application Management Center (AMC).

Documentation for MSL, Mitel Applications Suite (MAS), and the integrated applications listed above is available on the [Mitel eDocs](#) Web site (<http://edocs.mitel.com>).

## Desktop Client Requirements

The Desktop Client is installed on users' computers at the site. Table 20 [Desktop Client Requirements](#) provides the computer hardware and software requirements for the Desktop Client.

**Table 20: Desktop Client Requirements**

Component	Requirement	Version
Central Processing Unit (CPU)	1.6 GHz or faster	Dual Core
Available Hard Disk Space	100 MB free hard disk space	
Random Access Memory (RAM)	2 GB RAM minimum (4 GB or more recommended)	
Network Interface Card (NIC)	Full duplex 10/100/1000 Mbps (100 Mbps full duplex recommended)	
Sound Card	Full duplex	
Operating System (OS)	Microsoft Windows® XP	Professional Service Pack 3 32- or 64-bit
	Microsoft Windows Vista®	Business/ Enterprise/Ultimate Service Pack 2 32 or 64-bit
	Microsoft Windows 7	Professional/Enterprise/Ultimate 32 or 64-bit
	Microsoft Windows 8	Desktop mode only 32 or 64-bit
Thin Clients <sup>1</sup>	Citrix® XenApp® Client	6.0 or 6.5 (Requires Citrix Presentation™ Server 6.0 or Citrix XenApp Server 6.5) 32- or 64-bit
	Remote Desktop Services (formerly Windows Terminal Services)	v6.1 (Installed as part of Windows Server 2008 R2)
	VMware Horizon View	4.6, 5.0 <sup>2</sup> , 5.1 or 5.2
Digital Media Player	Windows Media® Player	6 or later
Microsoft Add-on	Microsoft.NET™ Framework	4.0

<sup>1</sup> - The embedded softphone and video call features will not function in the Thin Client environment.

<sup>2</sup> - VMware Horizon View 4.6 and later are supported for desktop phone operation. VMware Horizon View 5.0 and later supports softphone operation.

The Desktop Client includes an embedded softphone (**not available on an Inter-Tel Axxess PBX**). The user requires the following to use the embedded softphone:

- The softphone license provisioned for the user's account (see Table 1 on [page 23](#))
- A programmed extension for the user on the PBX (see [page 91](#))
- A supported headset or handset (see Table 21 [Supported Headsets and Handsets](#), below)

Table 21 [Supported Headsets and Handsets](#) provides the list of USB/Bluetooth headsets and handsets that have been tested with the UC Advanced softphone.

**Table 21: Supported Headsets and Handsets**

Headsets	Handsets
Jabra® GN 2000 USB <sup>1</sup>	VoipVoice® Cyberphone 654
Jabra GN 2100 USB <sup>2</sup>	
Plantronics® CS50-USB	
Plantronics Blackwire C610 <sup>3</sup>	

<sup>1</sup>. Limitations:

- a) **Mute** button is not functional even if configured.
- b) While on an active call, the **Audio** does not automatically recover if the headset is unplugged and plugged back in.

<sup>2</sup>. Limitation: **Mute** button is not functional even if configured.

<sup>3</sup>. Limitation: **Mute** button is not functional even if configured.



**Note:** Supported Headsets and Handsets were tested with the UCA product. However, there are known limitations - see [Table 21](#) footnotes.

## MiVoice for Lync Requirements

MiVoice for Lync is installed on users' computers. Table 22 [MiVoice for Lync Requirements](#) provides the computer hardware and software requirements.

**Table 22: MiVoice for Lync Requirements**

Component	Requirement	Version
Central Processing Unit (CPU)	1.6 GHz or faster	Dual Core
Available Hard Disk Space	100 MB free hard disk space	
Random Access Memory (RAM)	2 GB RAM minimum (4 GB or more recommended)	
Network Interface Card (NIC)	Full duplex 10/100/1000 Mbps (100 Mbps full duplex recommended)	
Operating System (OS)	Microsoft Windows® XP	Professional Service Pack 3 32- or 64-bit
	Microsoft Windows Vista®	Business/ Enterprise/Ultimate Service Pack 2 32 or 64 bit
	Microsoft Windows 7	Professional/Enterprise/Ultimate 32 or 64 bit
	Microsoft Windows 8	Desktop Mode only 32 or 64 bit
Microsoft Add-on	Microsoft.NET Framework	4.0
Microsoft Application	Microsoft Lync	2010 or 2013

## Optional Third-Party Client Components

See [“Optional Third-Party Integrated Applications”](#) on page 17.

## Web Portal Requirements

The UC Advanced Web Portal provides remote access to a subset of UC Advanced features from one of the following supported computer Web browsers:

- Microsoft Internet Explorer® (IE) 10 or later (see note)
- Mozilla® Firefox® 14 or later
- Apple® Safari 5.6, 6.0 or later
- Google Chrome™ 21 or later



**Note:** IE8 or IE9 users could use the Google Chrome Frame plug-in to get real-time data and have chat, presence and call control functionality. However, the plug-in will no longer be updated and supported effective Jan 2014. The plug-in will continue to work if you already have it installed otherwise upgrade to IE10 or later to get all the functionality.

## UCA Mobile for BlackBerry Requirements

UC Advanced Mobile for BlackBerry is a stand-alone client that users install on their BlackBerry mobile device. The client provides automatic Dynamic Status updates based on the user's current location. UCA Mobile for BlackBerry and Mobile Portal requires a BlackBerry mobile device running mobile OS 5.x, 6.x or 7.x.

## UCA Mobile for Android Requirements

UC Advanced Mobile for Android is a stand-alone client that users install on their Android mobile device. The client provides automatic Dynamic Status updates based on the user's current location. UCA Mobile for Android requires an Android mobile device running version 2.3 or later.



**Note:** The minimum hardware requirements for the Android client if you intend to use the SIP softphone:

Processor = Dual core, 1000 MHz, ARM Cortex-A9

Memory = 1024 MB RAM

## UCA Mobile for iPad Requirements

Mitel® Unified Communicator® Advanced Mobile for iPad™ client application (UCA Mobile) provides Dynamic Status updates based on time or geographical location. In addition, UCA Mobile provides an integrated environment in which you can communicate with corporate contacts, and access and manage visual voice mail and call history.

UCA Mobile operates on all Apple® iPad models (some features are specific to certain models). iOS version 5.0 or later is required. iPad mini is not officially supported in this release.

## UCA Mobile for iPhone Requirements

Mitel® Unified Communicator® Advanced Mobile for iPhone client application (UCA Mobile) provides Dynamic Status updates based on time and GPS location. In addition, UCA Mobile provides an integrated environment in which you can communicate with corporate contacts, and access and manage visual voice mail and call history.

UCA Mobile operates on the Apple iPhone platform. iOS version 5.0 or later is supported. iPhone version 3GS and later versions are supported.

## PBX Node Environments

The UC Advanced site's PBX provides call control for UC Advanced local and remote users. The following PBX configurations are supported for UC Advanced:

- Single MCD/ Mitel 5000/Inter-Tel Axxess PBX Node
- Multiple MCD/ Mitel 5000/Inter-Tel Axxess PBX Nodes
- Multiple mixed MCD/Mitel 5000/Inter-Tel Axxess PBX Nodes

UC Server is capable of communicating with multiple PBXs to provide a global view for the UC Advanced clients. Call commands from the UC client interface to the server are directed to the respective PBX by the UC server based on which PBX the account resides.

A single UC Server can support MCD, Mitel 5000, and Inter-Tel Axxess PBX nodes. However, in the UC Server Administrator Interface, a single enterprise can be configured with just one PBX type.

Multiple mixed PBX type environments are only supported within the same company and require a separate enterprise per PBX type.



**Note:** The UC Server Administrator Interface does *not* distinguish between a Mitel 5000 PBX type and an Inter-Tel Axxess PBX type when an enterprise is configured. Therefore, a Mitel 5000 and an Inter-Tel Axxess are considered the same PBX type and can be on the same enterprise.

# CHAPTER 4

## INSTALLATION AND CONFIGURATION





## Introduction

This chapter describes how to install and configure UC Advanced.

## Planning Considerations

Before implementing the UC Advanced installation, make sure the site has the required hardware, software, licensing (AMC Application Record), and virtualized environment (if the virtual appliance option is used).

Also, determine the following:

- Which communications platform (see [page 16](#)) are you connecting to (MCD, Mitel 5000, or Inter-Tel Axxess)?
- Which type of synchronization (see [page 57](#)) do you want to use to create accounts (PBX node or AD/LDAP)? You can also manually create accounts.



**Note:** The UC Server can integrate with single or multiple LDAP v3-enabled directory servers to import accounts. If you intend to use AD/LDAP synchronization to import accounts into UC Advanced, make sure your directory server supports LDAP v3.

- How will remote users connect to the UC Server? Options include:
  - Teleworker mode (MBG and Remote Proxy Services) for MCD users (see [page 104](#)).
  - Firewall ports for Mitel 5000 and Inter-Tel Axxess users (see the *Mitel UC Advanced Engineering Guidelines* for details).
  - Virtual Private Network (VPN) connection.
- Which Mitel applications will be integrated with UC Advanced (e.g., NuPoint UM, MCA, MBG, etc.)? Several features (Video Calls, Collaboration, Visual Voice Mail, UC Server Peering, Federation, etc.) require you to configure the associated servers.

Do the following for all integrated applications:

- Make sure that you have downloaded all of the documentation for each product. The individual application documentation includes detailed hardware, software, and licensing requirements as well as installation and configuration instructions.
- Make sure that you have completed the required configuration for each server *before* starting the UC Advanced installation.
- Review all of the planning information, including the detailed port diagrams, provided in the *Mitel UC Advanced Engineering Guidelines*.
- Which UC Advanced licensed features does the customer want to purchase and activate in the AMC? Make sure all licenses are purchased before you begin the UC Advanced installation.



**Note:** All the UCA clients - desktop, web and mobile - use secure connection for signalling and need valid certificates on the UCA server.

## High Level Installation and Configuration Procedures

The high-level procedure for installing and configuring UC Advanced is provided below. This procedure applies to installations and to upgrades from UC Advanced 2.0 and Your Assistant 5.1.



**Note:** The installation and configuration information in this chapter is UC Advanced-specific. It does not include complete installation and configuration information for MSL, MAS, and the Mitel applications that can be integrated with UC Advanced. For product-specific documentation, refer to the appropriate documentation on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

*To install and configure UC Advanced, complete the following high-level steps:*

1. Configure the PBX for UC Advanced using one of the following programming interfaces:
  - System Administration Tool for the MCD PBX (see [page 91](#)).
  - DB Programming for the Mitel 5000 PBX (see [page 94](#)).
  - DB Programming for the Inter-Tel Axxess PBX (see [page 98](#)).
2. Install and configure the integrated Mitel applications:
  - *If required*, install and configure NuPoint UM, MCA, and UC Mobile (see [page 101](#)).
  - *If required*, install and configure MBG and Remote Proxy Services (see [page 104](#)).
3. Install and configure MSL and UC Server (see [page 108](#)).
4. Access the UC Server Administration page (see [page 121](#)).
5. Provision UC Advanced as documented in the UC Server Administrator online help (see [page 122](#)).
6. Install UC Advanced Desktop Clients (see [page 124](#)).
7. Install MiVoice for Lync Clients (see [page 137](#)).
8. Install the UC Advanced Mobile Clients (see [page 138](#)).
9. Configure access for remote users. Configuration procedures differ based on PBX:
  - For remote users connected to the MCD PBX, see “[MCD PBX Configuration for Remote Users](#)” on [page 142](#).
  - For remote users connected to a Mitel 5000 or Inter-Tel Axxess PBX, see “[Mitel 5000/Inter-Tel Axxess PBX Configuration for Remote Users](#)” on [page 148](#).
10. See “[Softphone \(SIP-based\) specific considerations](#)” on [page 149](#). Individual client configuration and testing instructions can be found:
  - “[Softphone Configuration - Desktop client](#)” on [page 153](#)
  - “[Softphone Configuration - Android client](#)” on [page 158](#)
  - “[Softphone Configuration - iPad client](#)” on [page 164](#)
  - “[Softphone Configuration - iPhone client](#)” on [page 169](#)

## Configure the PBX

This section describes how to configure the MCD, Mitel 5000, and Inter-Tel Axxess PBXs for UC Advanced.

This section assumes that you are familiar with the programming interface for the PBX installed on site. UC Advanced requires certain fields and options be programmed correctly for the PBX to provide integration with the communication platform. Programming interfaces include:

- MCD System Administration Tool
- Mitel 5000 Database (DB) Programming
- Inter-Tel Axxess Database (DB) Programming

For additional PBX programming documentation, refer to the PBX programming interface online help and the supplemental PBX documentation on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

### MCD PBX

All the required configuration to support UC Advanced for the MCD PBX is completed using the Mitel Communications Director System Administration Tool. The information in this section provides guidelines for UC Advanced -specific configuration only.

The following MCD System Administrator Tool forms include UC Advanced-specific fields and options:

- “User Configuration Form” on page 92
- “License and Option Selection Form” on page 92
- “Class of Service Options Form” on page 92
- “Personal Ring Group Assignment Form” on page 93

Note the following for MCD PBXs:

- For sites that intend to use ACD PBX features in UC Advanced, UC Advanced supports ACD traditional agents only.
- For sites that intend to use the PBX node synchronization method for creating accounts in UC Advanced, special programming may be required if multiple directory number (DN) records with the same name exist on the PBX. Typically, when UC Advanced encounters multiple records with the same name during a synchronization with the MCD PBX, only the highest directory number (DN) is brought over to UC Advanced. To ensure that all records are included during a synchronization, DNs that share the same name require a unique entry in the **Department** or **Location** fields. Refer to the **User Configuration** and **Device Configuration** forms online help topics for details.
- The MCD system must be running system software v4.2 or later for remote click to call OfficeLink functionality (see Table 14 on [page 67](#)).

- The MCD must be running v5.0 SP2 or later for SIP softphone functionality.
- When you make changes to the PBX configuration, you will need to complete a manual synchronization from the UC Server Administrator interface to import those changes to UC Advanced (see [page 235](#)).

### NOTICE

Only Mitel MCD-certified personnel can configure the MCD PBX.

## User Configuration Form

The UC Advanced Minet softphone must be programmed correctly in the MCD system. In the User Configuration form (MCD v4.1 or later), in order to have **resiliency the UCA Minet softphone must be programmed on the MCD as 5020 IP set type**.

## License and Option Selection Form

In the License and Option Selection form, set the MiTAI/Tapi Computer Integration option to **Yes**.

TAPI enables Windows applications to share telephony devices with each other and provides a common means of handling different media (voice, data, fax, video, and so on) on a wide range of hardware platforms.

A TAPI service provider (TSP) is a driver that allows TAPI applications to communicate with different types of TAPI hardware. When using telephony hardware other than modems, such as PBXs, voice processing cards, and so on, you will typically use a TSP provided by the hardware vendor. The TSP provided by Mitel allows users to make calls from other applications. There is no direct interaction with UC Advanced and the TSP; UC Advanced monitors only the events from MiTAI that occur due to actions performed by the TSP on the PBX, e.g. Dialing from Outlook.

## Class of Service Options Form

UC Advanced desk phones and softphones can have different Classes of Service (COS) as long as the COS options below are properly set.

Configure the following fields and options on the Class of Service Options form:

- Group Presence Control: Set to **Yes**
- Group Presence Third Party Control: Set to **Yes**
- HCI/CTI/TAPI Call Control Allowed: Set to **Yes**
- HCI/CTI/TAPI Monitor Allowed: Set to **Yes**
- Voice Mail Softkey Allowed: Set to **No**<sup>1</sup>

---

1. If set to Yes, users will not be able to hang up from their voice mailbox when using UC Advanced.

## Personal Ring Group Assignment Form

UC Advanced users can use devices configured in the user's Personal Ring Group (PRG) for the OfficeLink and Multi-Device User Group (MDUG) features. PRGs are an association of two or more devices for a single user under a common Directory Number (DN).



**Note:** Multi-Device User Groups are supported for MCD 5.0 and later ONLY.



**Note:** For multiple devices support also see Synchronization Rules (under Synchronization Tab) on Admin portal online help.  
Mitel recommends using Multi-Device User Group for Softphone deployments.



**Note:** Personal Ring Group (PRG) prime device must be an IP device and can not be a DNIC device.

Use the Personal Ring Group Assignment form to configure PRG devices for UC Advanced users. You will need to define a DN to be used as the prime member of the PRG using the Multiline IP Set Configuration form.

## SIP Softphone settings

MCD specific settings: To ensure proper functionality, **there are two critical changes that MUST be made on MCD when configuring a UC Advanced SIP Softphone:**

- a. First, you must select a Device Type of **UC Endpoint**.

The screenshot shows the 'User and Device Configuration' form for App29. The left sidebar contains a navigation tree with categories like Licenses, LAN/WAN Configuration, Voice Network, System Properties, Hardware, Trunks, and Users and Devices. The main area is titled 'User and Device Configuration on App29'. It includes a search bar with 'Search Scope' set to 'App29' and a search result for 'Number: 29408, Name: Denis L, Hot Desking User: No, Device Type: UC Endpoint'. Below this, there are tabs for 'Profile', 'Device Details', 'Service Details', 'Access and Authentication', 'Phone Applications', and 'Keys'. The 'Profile' tab is active, showing fields for 'User Profile' (Last Name: L, First Name: Denis, Department, Location, Role: No Role, Language: English, Email, IDS-Manageable: checked) and 'Service Profile' (Number: 29408, Directory Name: L\_Denis, Hot Desking User: unchecked, Device Type: UC Endpoint (highlighted with a red circle), Service Level: Full, Local-only DN: unchecked, ACD Enabled: unchecked, Prime Name: No, Privacy: No, Home Element: App29, Secondary Element: Not Assigned).

- b. Second, you must add at least one additional line. This is accomplished by adding a key with a Line Type of Multicall, a Button Dir. Number matching the number of the device, and Ring Type of Ring.

App29

View by Category SOS Share

User and Device Configuration on **App29** DN to search Show form on Not Accessible Go

User and Device Configuration Search:

Search Scope: ☒ App29 ☐ Admin Group

Find a field named: Number that has a value of: 29408 Search

Add Change Copy Delete Print... Import... Export... Data Refresh

Number: 29408 Name: Denis L Hot Desking User: No Device Type: UC Endpoint Apply Save Cancel

Profile Device Details Service Details Access and Authentication Phone Applications Keys

Copy Keys Clear All Keys Clear Key

Button Number	Label	Line Type	URL	Button Directory Number	Ring Type	MIXML Application Feature	Phone Application Feature
2		Multicall		29408	Ring	Not Assigned	
3		Not Assigned				Not Assigned	
4		Not Assigned				Not Assigned	
5		Not Assigned				Not Assigned	
6		Not Assigned				Not Assigned	
7		Not Assigned				Not Assigned	
8		Not Assigned				Not Assigned	

## Mitel 5000 PBX

All configuration changes for Mitel 5000 CP are completed using the Mitel 5000 DB Programming interface. The information in this section provides guidelines for UC Advanced-specific configuration only.

The following Mitel 5000 DB Programming folders include UC Advanced-specific fields and options:

- “Software License” on page 96
- “System – Devices and Feature Codes – Assistants” on page 96
- “System – Devices and Feature Codes – Phones” on page 96
- “System – IP-Related Information – Call Configuration (Softphones Only)” on page 97
- “System – Sockets” on page 97
- “Users” on page 97

Note the following for Mitel 5000 PBXs:

- The Mitel 5000 system must be running system software v5.0 or later and the system must be programmed correctly to support full remote click to call OfficeLink functionality (see Table 14 on page 67).
- When you make changes to the PBX configuration, you will need to complete a manual synchronization from the UC Server Administrator interface to import those changes to UC Advanced (see page 235).

- For sites that intend to use the PBX node synchronization method for creating accounts in UC Advanced, the UC Server retrieves user and/or phone extension information configured in DB Programming to create accounts via the OAI stream for the PBX node synchronization type.

It is important that the information in the **Users** and/or **Phones**<sup>1</sup> folders in DB Programming is configured correctly to avoid the creation of unwanted accounts on the UC Server if using PBX synchronization. PBX synchronization looks to the **Users** folder first and then the **Phones** folder to create accounts during the initial synchronization.

- Before you run a PBX Node Synchronization from the **Synchronization** tab, it is recommended that you set the Default feature profile field to the Default Feature Profile. The Default Feature Profile does not apply any features and licenses, so the system will not run out of licenses if there are more phones/accounts than available licenses. Instead, assign phones/accounts with the required licensed features from the UC Server **Features** tab after performing the synchronization.

If the **Synchronize Dynamic Extension only** option in the Synchronization tab is enabled, only the extensions listed under Users will be synchronized. This option limits the number of accounts created.

- For sites synchronizing multiple Mitel 5000 PBX nodes, all nodes must be entered under PBX Nodes. If using a CT Gateway, all 5000 nodes and the CT Gateway are entered under **PBX Nodes**. See the UC Server Online Help for additional details.



**Note:** The CT Gateway must be programmed to monitor all nodes programmed under PBX Nodes.

Adhere to the following guidelines when using a CT Gateway to synchronize multiple Mitel 5000 nodes:

- When using a CT Gateway to communicate with multiple Mitel 5000 nodes, each node's session manager must have a DB programming account with the same password that matches the password set at the single PBX node representing the cluster on the UC Server.
- The CT Gateway must be running software version 4.4.01 or higher.
- All nodes configured on the CT Gateway must be communicating (up and working) so that the PBX synchronizer will synchronize all of the accounts. If one or more of the Mitel 5000 nodes are not communicating with the CT Gateway, the node will not be synchronized as indicated by the message that is generated under the PBX Nodes tab.
- The PBX Node for CT Gateway must have a Voice Mail system pilot number programmed. You must choose a Voice Mail application number from one of the Mitel 5000 nodes. This will not impact phone/account voice mail set for each PBX.
- All nodes connected to the CT Gateway must be using OAI protocol version 10.0 or later (Mitel 5000 v3.2). Node connections to the CT Gateway that are not running protocol version 10.0 or later must be removed from the CT Gateway, or the nodes must be upgraded to v3.2.

---

<sup>1</sup> Prior to Mitel 5000 v4.0, this folder in DB Programming was named Endpoints.



- It is recommended that all duplicate extensions between nodes be removed before installing the CT Gateway. If this is not done, one of the accounts with the duplicate extension information will be deleted during the synchronization.

Refer to Mitel Knowledge Base article number [4376](#) for additional Mitel 5000 configuration information.

### NOTICE

Only Mitel 5000-certified personnel can configure the Mitel 5000 PBX.

## Software License

The **Software License** folder in DB Programming displays the licenses currently uploaded to the system. The features common to all licenses are displayed in this folder along with the value for each feature according to the current software license. This folder is read-only.

The following Mitel 5000 system software licenses must be enabled to provide full integration with UC Advanced:

- **Dynamic Extension Express:** Dynamic Extension Express provides Ring Group options for UC Advanced users in the Desktop Client. Ring Groups provide call routing options for user's Dynamic Statuses.
- **System OAI 3rd Party Call Control:** Provides call control capabilities from the PBX to UC Advanced so that users connected to the PBX can access system call features. System OAI 3rd Party Call Control is required to support the Dynamic Extension Express PBX feature.
- **System OAI Events:** Allows UC Advanced to monitor the devices on the PBX to provide advanced presence. System OAI Events are required to support the Dynamic Extension Express PBX feature.

## System – Devices and Feature Codes – Assistants

For Mitel 5000 v5.0 and later systems, configure the OfficeLink Assistant to provide full OfficeLink functionality for UC Advanced users.

Adding an OfficeLink Assistant allows UC Advanced users to place OfficeLink calls from any of their ring group devices (including Mobile). If the OfficeLink Assistant is not present (or if using software older than 5000 v5.0), then UC Advanced users can only place OfficeLink calls from their desk phone and UC Advanced softphone.

See [page 66](#) for more information about the OfficeLink feature.

## System – Devices and Feature Codes – Phones

The UC Server retrieves information programmed in the **Users** and/or **Phones** folders to create UC Advanced accounts.



If the **Phones** information is configured for the Mitel 5000, but the **Users** information is not, the UC Advanced PBX node synchronizer retrieves the following information from the **Phones** folder in DB Programming to create UC Advanced accounts:

- **System – Devices and Feature Codes – Phones – Extension:** The value configured in the **Extension** field becomes the desk phone extension for the UC Advanced account after synchronization.
- **System – Devices and Feature Codes – Phones – Description:** The value configured in the **Description** field becomes the account name for the UC Advanced account after synchronization. Note the following for the Description field:
  - Configure the user's name in Last name, First Name format for the Description field. This is the format used by the PBX node synchronizer for the account name in UC Advanced.
  - The Tilde character (~) before the Description and a blank Description field excludes the account from the synchronization.



**Note:** If you create both a desk phone and a UC Advanced Softphone in DB Programming for a single user, two separate accounts are created in UC Advanced for the extensions during the PBX node synchronization.

### System – IP-Related Information – Call Configuration (*Softphones Only*)

Mitel recommends that you configure audio settings specific to the UC Advanced Softphone to ensure good audio quality.

Under System – IP-Related Information – Call Configuration, configure the Audio Frames/IP Packet with a value of **2**.

### System – Sockets

To support UC Advanced, select System – Sockets, and set the System OAI Level 2 option to **Yes**.

### Users

The UC Server retrieves information programmed in the **Users** and/or **Phones** folders to create UC Advanced accounts. See Synchronization on [page 57](#).

If the **Users** information is configured for the Mitel 5000, but the **Phones** information is not, the UC Advanced PBX node synchronizer retrieves the following information from the **Users** folder in DB Programming to create UC Advanced accounts:

- **Users:** Configure the **First Name** and **Last Name** fields. These fields provide the value for the account name on the UC Server.

Note the following:

- To exclude a UC Advanced account from being created during synchronization, insert the Tilde character (~) before the **First Name** or **Last Name**.



**Note:** If there is a phone programmed with the same extension under the Phones folder and the **Description** does not include a tilde, the phone will be included in the synchronization.

- If the **First Name** and **Last Name** fields are blank in DB Programming, UC Advanced will create an account with no name.



**Note:** If there is a phone programmed with the same extension under the Phones folder and the Phones **Extension** field matches the User **Main Extension** field, then the name from the Phones **Description** field is used for the synchronization.

- If both Phones and Users is programmed in DB Programming, if the Phones **Extension** fields and Users **Main Extension** field match, then only one account is created.
- Users – **<user>**: Configure the following for each user:
  - The value configured for the **Main Extension** field becomes the desk phone or soft-phone extension for the UC Advanced account after synchronization. UC Advanced softphones are allowed as the Main Extension.
  - The **Yes** value configured for the **Enable Dynamic Extension Express** field instructs the PBX node synchronizer to use the programmed Associated Destinations fields when configuring Ring Group devices. In addition, this value instructs AD/LDAP synchronizers to synchronize Dynamic Express Extension information from the PBX.
- **Associated Destinations:** Configure the values for the Associated Destinations sub folder. UC Advanced users can use devices configured as the user's Associated Destinations for the OfficeLink feature (see [page 66](#)). These values populate the **My Ring Group** devices in the UC Advanced account after synchronization:
  - Desk, Desk 2
  - Voice Mail
  - Home, Home 2
  - Home IP, Home IP 2
  - Mobile, Mobile 2
  - Softphone, Softphone 2



**Note:** Associated Destinations must be set to **Active** to be included in the PBX node synchronization.

## Inter-Tel Axxess PBX

All configuration changes for the Inter-Tel Axxess are completed using the Inter-Tel Axxess DB Programming interface. The information in this section provides guidelines for UC Advanced -specific configuration only.

The following Inter-Tel Axxess DB Programming folders include UC Advanced-specific fields and options:

- “[Software License](#)” on [page 100](#)

- [“System – Devices and Feature Codes – Stations” on page 100](#)
- [“System – Sockets” on page 100](#)

Note the following for Inter-Tel Axxess PBXs:

- For sites that intend to use the PBX node synchronization method for creating accounts in UC Advanced, the UC Server retrieves phone (station) extension information configured in DB Programming to create accounts via the OAI stream for the PBX node synchronization type.

It is important that the information in the **Station** folders in DB Programming is configured correctly to avoid the creation of unwanted accounts on the UC Server.

- Before you run a PBX Node Synchronization from the **Synchronization** tab, it is recommended that you set the Default feature profile field to the Default Feature Profile. The Default Feature Profile does not apply any features and licenses, so the system will not run out of licenses if there are more phones/accounts than available licenses. Instead, assign phones/accounts with the required licensed features from the UC Server **Features** tab after performing the synchronization.

If the **Synchronize Dynamic Extension only** option in the Synchronization tab is enabled, only the extensions listed under Users will be synchronized. This option limits the number of accounts created.

- For sites synchronizing multiple Axxess PBX nodes, all nodes must be entered under PBX Nodes. If using a CT Gateway, all Axxess nodes and the CT Gateway are entered under PBX Nodes. See the UC Server Administrator interface online help for additional details.



**Note:** The CT Gateway must be programmed to monitor all nodes programmed under PBX Nodes.

Adhere to the following guidelines when using a CT Gateway to synchronize multiple Inter-Tel Axxess nodes:

- When using a CT Gateway to communicate with multiple Inter-Tel Axxess nodes, each node's session manager must have a DB programming account with the same password that matches the password set at the single PBX node representing the cluster on the UC Server.
- The CT Gateway must be running software version 4.4.01 or higher.
- All nodes configured on the CT Gateway must be communicating (up and working) so that the PBX synchronizer will synchronize all of the accounts. If one or more of the Inter-Tel Axxess nodes are not communicating with the CT Gateway, the node will not be synchronized as indicated by the message that is generated under the PBX Nodes tab.
- The PBX Node for CT Gateway must have a Voice Mail system pilot number programmed. You must choose a Voice Mail application number from one of the Inter-Tel Axxess nodes. This will not impact phone/account voice mail set for each PBX.
- All nodes connected to the CT Gateway must be using OAI protocol version 10.0 or later (Inter-Tel Axxess v11.017). Node connections to the CT Gateway that are not

running protocol version 10.0 or later must be removed from the CT Gateway, or the nodes must be upgraded to v11.0.17.

- It is recommended that all duplicate extensions between nodes be removed before installing the CT Gateway. If this is not done, one of the accounts with the duplicate extension information will be deleted during the synchronization.

### NOTICE

Only Mitel Inter-Tel Axxess certified personnel can configure the Inter-Tel Axxess PBX.

## Software License

The **Software License** folder in DB Programming displays the licenses currently uploaded to the system. The features common to all licenses are displayed in this folder along with the value for each feature according to the current software license. This folder is read-only.

The following Inter-Tel Axxess system software licenses must be enabled to provide full integration with UC Advanced:

- **System OAI 3rd Party Call Control:** Provides call control capabilities from the PBX to UC Advanced so that users connected to the PBX can access system call features.
- **System OAI Events:** Allows UC Advanced to monitor the devices on the PBX to provide advanced presence.

## System – Devices and Feature Codes – Stations

The UC Server retrieves information programmed in the Stations folders to create UC Advanced accounts. The UC Advanced PBX node synchronizer retrieves the following information from the Stations folder in DB Programming to create UC Advanced accounts:

- **System – Devices and Feature Codes – Stations – Extension:** The value configured in the **Extension** field becomes the desk phone extension for the UC Advanced account after synchronization.
- **System – Devices and Feature Codes – Stations – Description:** The value configured in the **Description** field becomes the account name for the UC Advanced account after synchronization. Note the following for the Description field:
  - Configure the user's name in Last name, First Name format for the Description field. This is the format used by the PBX node synchronizer for the account name in UC Advanced.
  - The Tilde character (~) before the Description and a blank Description field excludes the account from the synchronization.

## System – Sockets

To support UC Advanced, select System – Sockets, and set the System OAI Level 2 option to **Yes**.

## Configure Integrated Applications

To install and configure the Mitel applications you want to integrate with your UC Advanced installation, refer to the documentation that was provided with the application. Documentation is also available on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

Mitel integrated applications/products include:

- NuPoint Unified Messaging (UM) v4.0 or later
- Mitel Collaboration Advanced (formerly known as Audio and Web Conferencing) 4.0 or later
- Mitel Border Gateway (MBG) v7.1 or later

This section describes basic UC Advanced configuration requirements for Mitel integrated applications. You may also need to configure integrated third-party application servers and components for use with UC Advanced. For configuration guidelines for third-party products, refer to the product documentation.

### NuPoint UM Configuration

UC Advanced includes a Visual Voice Mail view in the Desktop Client that provides access to NuPoint UM voice mail and FAX messages. Other Mitel and third-party voice mail systems are not supported by UC Advanced.

To provide visual voice mail features, the NuPoint UM server must be configured properly as described in the following sections:

- [Visual Voice Mail for Peered UC Servers](#), below
- [NuPoint Configuration Options](#), below
- [“FCOS Options” on page 102](#)
- [“Port Utilization” on page 102](#)



**Note:** NuPoint UM is not supported on the Inter-Tel Axxess PBX. See [“Other Voice Mail Systems” on page 103](#) for additional information.

### Visual Voice Mail for Peered UC Servers

When UC Servers are peered, the NuPoint UM voice mail servers must be networked in the peered configuration for the voice mail forwarding and transfer to voice mail features to function. UC Advanced does not support multiple NuPoint UM voice mail systems for peered UC Servers.

If UC Servers are peered and each server is configured with a different voice mail system, the following UC Advanced voice mail features will not function between the servers:

- A Desktop Client user on UC Server A cannot forward a voice mail message to a peered contact on UC Server B.
- A Desktop Client console user on UC Server A cannot use the Transfer to Voice Mail feature to transfer a call to a voice mailbox on UC Server B.

### NuPoint Configuration Options

The **Dialer (Pager)** and a **Pager Line Group** must be configured for NuPoint under System Configuration to enable the “Request playback call” function in the UC Advanced Desktop Client Visual Voice Mail view. It is not necessary to enable the dialer or pager on each mailbox under Message Waiting.



**Note:** If your NuPoint UM application is running on a MAS server, Mitel recommends upgrading to MAS software version R2.0.1.106 or later, which includes several NuPoint UM Dialer updates.

### FCOS Options

The following NuPoint UM feature (FCOS) options are required for UC Advanced Desktop client to control voice mail calls within the application:

- FCOS 289 Enable UM-SMTP
- FCOS 290 Enable UM-Web
- FCOS 295 Enable UM Pro

The following features are required for Caller ID to appear in the UC Advanced Desktop Client:

- FCOS 262 Store Caller Line ID as Phone Number
- FCOS 263 Store Caller Line ID as Phone or Mailbox Number
- FCOS 264 Play outside caller user interface (With FCOS bit 280)
- FCOS 280 Enable CLI Outside Caller interface (with FCOS bit 264)

### Port Utilization

From the Visual Voice Mail view, users can listen to voice mail messages from the Desktop Client as follows:

- Direct the voice mail system to place a call to their desk phones and play the message using the “Request playback call” function.
- Play the message on their computer using the default media player.

When users direct the voice mail system to place a call to their desk phone, UC Advanced consumes outgoing NuPoint UM ports, for the duration of the voice mail message. When users play voice mail messages using their media player, no outgoing ports are consumed.

Be sure you have configured sufficient outgoing NuPoint UM ports for UC Advanced. If users regularly receive a busy signal when directing the voice mail system to call their desk phone and play voice mail messages, NuPoint UM may not have sufficient outgoing ports configured. Refer to the **NuPoint UM Port Utilization Report** to capture port utilization details.



**Note:** Like the UC Advanced server, the NuPoint UM server needs to have a publicly-resolvable hostname. This hostname is used by the UC Advanced Desktop Client and the Web Portal when users listen to voice mail messages using the media player installed on their computer. If users cannot access the NuPoint UM server from their computers, voice mail message playback is limited to the “Request playback call” option from the Desktop Client.

## Other Voice Mail Systems

The MCD, Mitel 5000, and Inter-Tel Axxess PBXs support embedded legacy and third-party voice mail systems. If the PBX is connected to a voice mail system other than NuPoint UM, the Visual Voice Mail feature will not function. Because the PBX provides call routing to voice mail, only the **Call Voice Mail** and **Send to Voice Mail** features will function in UC Advanced when the PBX is connected to non-NuPoint voice mail systems.

When the PBX is connected to a non-NuPoint UM voice mail system, note the following configuration information:

- The PBX node must be configured on the PBX Node tab and it must be synchronized with UC Advanced.
- Some legacy voice mail systems have a different pilot number for the message retrieval application versus the voice mail application. To ensure that UC Advanced users reach the Message Retrieval application instead of the Voice Mail application when they use the Call Voice Mail function, the UC Advanced Administrator can configure the Voice Mail Number field on the PBX Details page with the Message Retrieval application extension.
- If UC Advanced Desktop Clients are open when the administrator makes changes to the PBX configuration in the UC Server Administrator interface, they must be closed and re-opened for configuration changes to take effect.

After the voice mail systems are configured on the UC server, the Call Voice Mail and Send to Voice Mail features are functional.

## MCA Configuration

MCA provides collaboration features and video calls for UC Advanced Desktop Client users.

To provide access to audio conferencing, Web conferencing, collaboration features and video calls, verify the following for MCA:

- The MCA server has sufficient ports and licenses configured for all users – including UC Advanced users.
- If you know the URL for the MCA server, you can synchronize the UCA Server with the MCA Server during system provisioning (see [page 122](#)).

## MBG and Remote Proxy Services Configuration

### NOTICE

Only MBG/Remote Proxy-certified personnel can configure the MBG.

If the customer site is using an MCD PBX and has remote users, you must configure the MBG and Remote Proxy Services for use with UC Advanced as described in this section. Additional configuration for the MBG is required after the Desktop Clients are installed (see [page 143](#)).

MBG provides a secure communications path from remote UC Advanced Desktop Clients, Mobile Clients as well as softphones and IP desk phones running on the MCD PBX to the UC Server. Remote Proxy Services provide a secure communications path for remote UC Advanced Web Portal users.



**Note:** If the customer is using Mitel Border Gateway (MBG) in a perimeter network (DMZ), the firewall that the MBG is connected to may have Session Initiation Protocol (SIP) application layer gateway (ALG) functionality turned ON, which may interfere with SIP messaging on UC Advanced. Mitel recommends that you disable the firewall's SIP ALG for this type of configuration.



**Note:** Starting in UCA v5.1, when teleworker mode is enabled in the UCA desktop clients and mobile clients, the SIP softphone and Minet softphone route the signaling and media traffic through the MBG even when the clients are used in the corporate LAN.

### *To configure MBG for use with UC Advanced:*

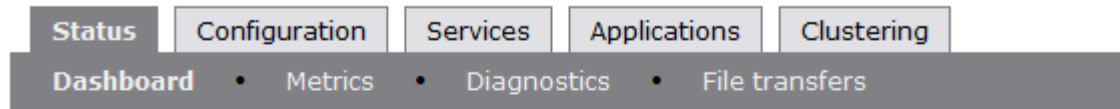


**Note:** Refer to the appropriate version of MBG documentation on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>) for updated information and images.

1. Open a Web browser and navigate to the MSL Server Manager URL (for example, `https://<MSL_server_FQDN>/server-manager`) where the MBG/Remote Proxy Services are installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The Welcome to the Server Manager page appears.
3. Under Applications, click **Mitel Border Gateway**.



## Manage Mitel Border Gateway



» Location: Dashboard

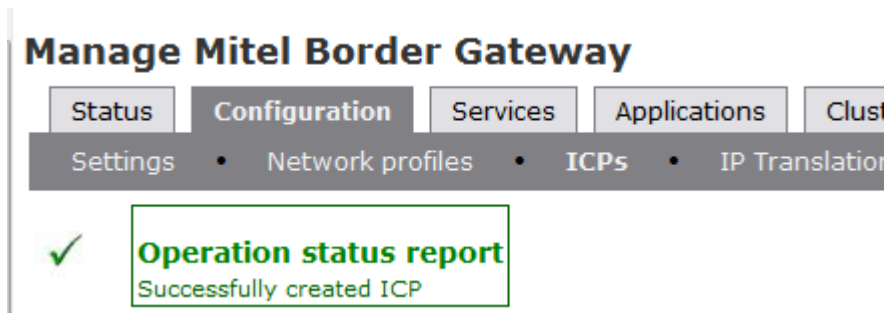
Welcome to the MBG administrative interface. From here you can manage all aspects of the MBG of the system. If at any time you require more information, click the Help icon in the upper-right

On this page you will find controls for managing the status of your Mitel Border Gateway server.

MBG status as of 14 February 2012 14:25:34.

<b>MBG status</b>	Enabled
<b>Start or stop MBG</b>	<input type="button" value="Start"/> <input type="button" value="Stop"/> Courtesy down? <input checked="" type="checkbox"/>
<b>Node ID</b>	uca-vmas05.inter-tel.com_1
<b>Network profile</b>	Gateway mode
<b>Security profile</b>	Legacy mode
<b>WAN IPs</b>	172.16.4.55
<b>LAN IPs</b>	192.168.77.88

4. Click the **Configuration** tab. Click the **ICPs** tab.
5. On the ICP tab, click **Add ICP** to add the MCD PBX (3300 ICP).
6. Program the ICP settings as described in the online Help.
7. Click **Save**. The Successfully created ICP message appears.



8. Click the **Applications** tab. The Manage Connectors data is displayed.  
Select **UC Advanced** on the Connectors page, and then click **Edit**.
9. Modify the UC Advanced connector as follows:
  - Ensure the UC Advanced connector is enabled.
  - Type the IP address or hostname for the UC Server in the following fields:
    - UC Advanced server hostname or IP address
    - Collaboration server hostname or IP address

- Type the IP address or hostname for the NuPoint UM voice mail server in the **NuPoint voicemail hostname or IP address** field.
- Click **Save**.

## Manage Mitel Border Gateway

Status	Configuration	Services	<b>Applications</b>	Clustering
<b>Application integration</b> • Show all connectors				
» Location: <a href="#">Manage connectors</a> / UC Advanced support				
Welcome to the MBG administrative interface. From here you can manage all aspects of the system. If at any time you require more information, click the Help icon in the upper right corner.				
Summary				
UC Advanced				
Here is shown the current status of the server's UC Advanced support. Click the "Edit" button to modify the settings.				
<b>UC Advanced connector</b> Disabled				
<b>UC Advanced server hostname or IP address</b>				
<b>NuPoint voicemail hostname or IP address</b>				
<b>Collaboration server hostname or IP address</b>				
<input type="button" value="Edit"/>				

### *To configure Remote Proxy Services for use with UC Advanced:*

The external DNS entry for the UC Server needs to resolve to the Remote Proxy Services server so that users outside of the internal LAN can use the Remote Proxy Services to access the UC Server.

1. Open a Web browser and navigate to the MSL Server Manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the MBG/Remote Proxy Services are installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The Welcome to the Server Manager page appears.
3. Under Applications, click **Remote Proxy Services**.
4. Click **Add new proxied domain**, and create a new proxied domain for the UC Server.

## Configure Web Proxy & Remote Management Service

**Domain list**

Users

Supported applications

» Location: Domain list

Welcome to the Remote proxy services administrative interface. From here you can manage all aspects of the service. For more information, click the Help icon in the upper-right corner of the page.

This page outlines any existing domains, and provides the means to manage them. These rules define traffic received on TCP port 443 to the LAN server.

*Note that unencrypted HTTP traffic is not proxied at this time.*

[Add new proxied domain](#)

There are currently no domains defined.

**Licensing information**

**Web proxy Remote management**

False

False

## Configure UC Advanced Mobile for Smart Devices

UC Advanced mobile clients make use of a websocket connection to the UC Server to support real-time notifications of missed calls and other events. To enable this functionality, a persistent connection is made from the device via TCP port 36008 to the UC Server.



**Note:** This procedure is applicable only if you are running MBG version 7.0 or earlier. It is not applicable if you are running MBG version 7.1 or higher.

If you are using an MBG version 7.0 server in server/gateway mode to proxy UCA traffic, a port-forwarding entry must be manually configured on the MBG server using the “Port forwarding” panel under Security on the Server Manager interface using the following parameters:

- Protocol: TCP
- Source Port(s): 36008
- Destination Host IP Address: <IP address of UC Server>
- Destination Port(s): 36008
- SNAT: Yes

If you are using an MBG server in a DMZ configuration, you must configure the edge firewall to forward traffic arriving on TCP port 36008 to TCP port 36008 on the MBG.



**Note:** MBG 7.1 does not have these limitations.

## Install and Configure MSL and UC Server

UC Advanced includes two options for the UC Server component: UC Advanced Software and UC Advanced Virtual Appliance (see [page 79](#) for details).

If UC Advanced is being installed as application on MAS, see the MAS Installation and Maintenance Guide: [http://edocs.mitel.com/default.htm#MAS\\_anchor](http://edocs.mitel.com/default.htm#MAS_anchor)

High-level installation and configuration steps are provided for each deployment option, below:

- **UC Advanced Software:** High-level installation and configuration steps include:
  - “Install the MSL Operating System” on [page 109](#).
  - “Configure MSL” on [page 109](#).
  - “Install the UC Server Blade” on [page 111](#).
  - “Verify UC Server Licensing” on [page 113](#).
- **UC Advanced Virtual Appliance:** High-level installation and configuration steps include:
  - “Install the UC Advanced Virtual Appliance” on [page 114](#).
  - “Configure MSL” on [page 109](#).
  - “Verify UC Server Licensing” on [page 113](#).



**Note:** This document assumes that the UC Advanced administrator and the MSL administrator are the same person.

## Software Installation Options

The UC Server software includes both the server and client software for UC Advanced. Before beginning a software installation for UC Advanced, review the release notes and the Engineering Guidelines for a comprehensive list of requirements.

There are two methods you can use to install UC Advanced software:

- Download and install the software blade directly from the AMC using the Server Manager interface.
- Download the ISO software image from Mitel Online, create a software CD, and install from CD.

*To download and install software directly from the AMC:*

1. Open a Web browser and navigate to the MSL server manager URL where the UC Server is installed (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)). The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. In the left navigation pane under ServiceLink, click **Blades**. The available list of blades is displayed.

4. Install the software blade as detailed in the Service Manager online help.

*To download an ISO software image, build a CD, and install from CD:*

1. Log on to [Mitel Online](#).
2. Select Support, and then click **Software Downloads**.
3. Click Unified Communicator – **Unified Communicator Advanced Software Download**.
4. Click the appropriate links to download the software.
5. Agree to the download disclaimer.
6. Save the file to a location on your maintenance computer.
7. Insert a CD into the CD/DVD ROM drive of your maintenance computer.
8. Navigate to the stored UC Server software ISO image and burn the image to CD.
9. Insert the CD in the hardware platform's CD ROM drive and install the software.

## Install the MSL Operating System

UC Advanced runs on MSL as a stand-alone application. This section describes the high-level MSL installation steps.



**Note:** The procedure in this section applies to the **UC Advanced Software** server deployment type. It does **not** apply to UC Advanced Virtual Appliance.

For detailed installation instructions for MSL, refer to the *MSL Installation and Administration Manual* on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

*To install the MSL Server:*

1. Install the hardware platform as described in the *MSL Installation and Administration Manual*.
2. Install the MSL v10.0 operating system as described in the *MSL Installation and Administration Manual*.

## Configure MSL

This section describes the high-level MSL configuration steps.



**Note:** The procedure in this section applies to both server deployment types:

- UC Advanced Software
- UC Advanced Virtual Appliance

For detailed MSL configuration instructions, refer to the *MSL Installation and Administration Manual* on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>).

*To configure MSL:*

1. Configure the MSL server settings. The following table lists the information you will need to enter during the MSL configuration process.

MSL Setting	Description
Administrator Password	For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters.
Domain Name	Names must start with a letter; can contain letters, numbers, and hyphens.
System Name	
Local Network Adapters	MSL automatically detects your system's Ethernet adapters and displays them (eth0, eth1) so you can configure a "Local" adapter (for LAN mode) or a "Local" AND a "WAN" adapter (for Network Edge mode). When configuring UC Server, only the first local adapter should be configured (for LAN mode).
Local Networking Parameters	The local IP address and subnet mask for the server.
WAN Adapters	This setting is not applicable for UC Server configuration.
External Interface Connection	This setting is not applicable for UC Server configuration.
Gateway IP Address	The IP address that UC Server will use to access the network.
DNS Server IP Address	The IP address of your corporate DNS server. Note the following: <ul style="list-style-type: none"> <li>• If you specify a Corporate DNS server, you must also configure the server's domains to Use Corporate DNS Servers under Configuration – <b>Domains</b> in Server Manager.</li> <li>• If DNS is supplied by your ISP, leave this setting blank.</li> </ul>
IPv6 Configuration	N/A. IPv6 is not currently supported by UC Server.

2. Using the Application Record ID you received from the AMC, register the server with the AMC and download licensing information.

`https://<MSL_server_FQDN>/server-manager`



**Note:** MSL provides two methods of completing offline synchronizations with the AMC for servers with no direct Internet connection. Refer to the *Mitel Standard Linux Installation and Administration Guide* for instructions.

3. Log into the MSL server manager interface. The **Welcome to the Server Manager** page appears.
4. In the left navigation pane under **Configuration**, click **E-mail Settings**. The **E-mail configuration** page appears.
5. Click **Change** for the **Forwarding address for administrative email** field.

## E-mail configuration

**Server to use for outbound SMTP** (delivered direct via DNS lookup)

Change

**SMTP email injection restrictions** localhost only

Change

**Forwarding address for administrative email** (delivered to 'admin' mailbox)

Change

**E-mail sent for events:** critical, major

Change

6. Enter your e-mail address in the box and then click **Save**.



**Note:** You must configure this field so that e-mail messages generated by the Desktop Client Problem Reporting Tool (see [page 240](#)) are routed to your e-mail address.

## Install the UC Server Blade

The UC Server blade contains the server and client software for UC Advanced. *If required*, install the UC Server blade.



**Note:** The procedure in this section applies to the **UC Advanced Software** server deployment type. It does **not** apply to UC Advanced Virtual Appliance.

### *To install the UC Server software blade:*

1. Open a Web browser and navigate to the MSL server manager URL where the UC Server is installed (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)). The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. *If you are installing the blade from CD*, insert the CD in your CD ROM drive.  
*If you are installing the blade directly from the AMC*, proceed to the next step.
4. In the left navigation pane under ServiceLink, click **Blades**. The available list of blades is displayed.



5. If you are downloading the software directly from the AMC, click **Update List** to ensure an up-to-date listing.

Skip this step if you are installing from CD.



**Note:** If the AMC sync process is disabled, the blades list will not be refreshed. The listing will show only installed blades, blades from CD, and entries from the last sync.

6. Click the **Install** link beside the blade you want to install. The licenses page appears displaying the licensing information for the UC Server software blade.
7. Review all of the licensing information.
8. Scroll to the bottom of the page and click **Accept All Licenses**. The installation process for the Unified Communications blade begins. The installation screen provides installation **Progress Overview** and **Progress Details** information.

### Installation of Mitel UC Server V3.2.12.0 blade

The blade is being installed in the background. This page should refresh every 5 seconds; otherwise, click [here](#) to update the page.

#### Progress Overview

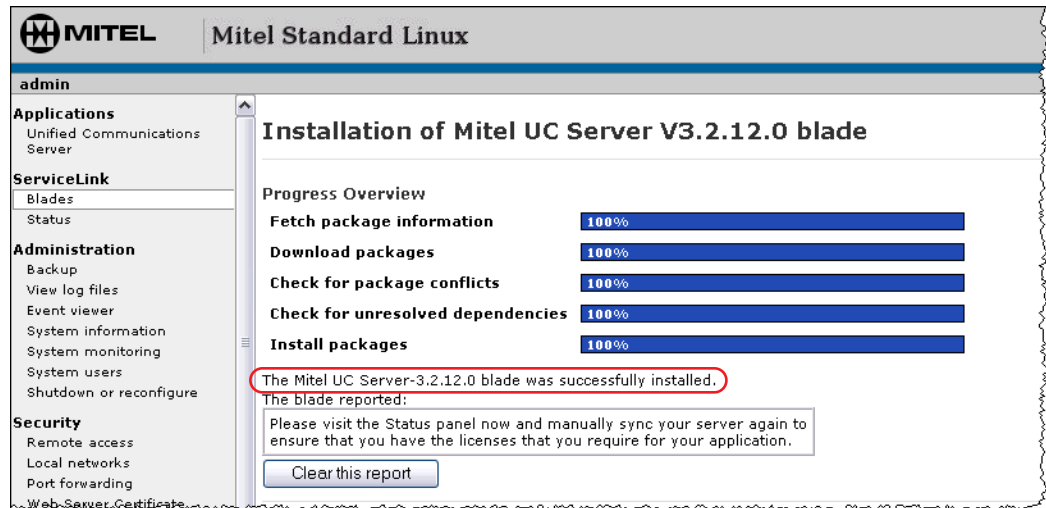
Fetch package information	100%
Download packages	3%
Check for package conflicts	0%
Check for unresolved dependencies	0%
Install packages	0%

#### Progress Details

Fetch package information	Completed successfully		
Download packages	In progress...		
	Blade-Mitel_UC_Server-3.0.12.0-01.noarch.rpm	0/7837 bytes downloaded	0% compl
	ace-tao-5.5.1-1.el4.i386.rpm	0/34561020 bytes downloaded	0% compl

When the blade is completely installed, the following message appears on the screen.





9. Click **Clear this report.**

After the UC Server blade installation is complete, the UC server automatically starts.

## Verify UC Server Licensing

Follow the steps below to verify that the required licensing information is available for the UC Server.



**Note:** The procedure in this section applies to both server deployment types:

- UC Advanced Software
- UC Advanced Virtual Appliance

*To verify UC Server licensing:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the UC Server is installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. Under Service Link, click **Status**. The current ServiceLink Status information is displayed.

## ServiceLink Status Information

This web panel provides updated ServiceLink status information for this server. Status part of the synchronization protocol.

The display includes information about your ServiceLink account, the latest synchronor subscribed. The display also includes the expiration date for each service and, if app

If you wish to deactivate your ServiceLink account, please click [here](#).

Your service account ID is: **00340010**

Your descriptive server name is: **uca-vmas05**

The last sync completed successfully at: **Wed Nov 23 21:42:02 2011**

### *Current ServiceLink subscription listing*

Service	Status	Expires	Messages
Audio and Web Conferencing	Subscribed	No expiry	None
Mitel Applications Suite	Subscribed	No expiry	None
Server activation and synchronization	Subscribed	No expiry	None
Mitel Border Gateway (MBG)	Subscribed	No expiry	None
NuPoint Messenger	Subscribed	No expiry	None

4. Click **Sync** in the bottom right hand corner to download the UC Advanced license information from the AMC to the UC Server. The sync completed successfully message appears.

## Install the UC Advanced Virtual Appliance

The UC Advanced virtual appliance allows you to install MSL and the UC Server in an existing virtual environment.

This section describes the installation and configuration steps to deploy the UC Advanced virtual appliance. For other UC Advanced deployments, see the options listed on [page 108](#).

For more detailed information on virtualization, refer to the *Virtual Appliance Deployment* solutions guide, part number 58013669, available on <http://edocs.mitel.com>.



**Note:** The procedure in this section applies to the **UC Advanced virtual appliance (vUCA)** deployment type. It does **not** apply to UC Advanced Software.



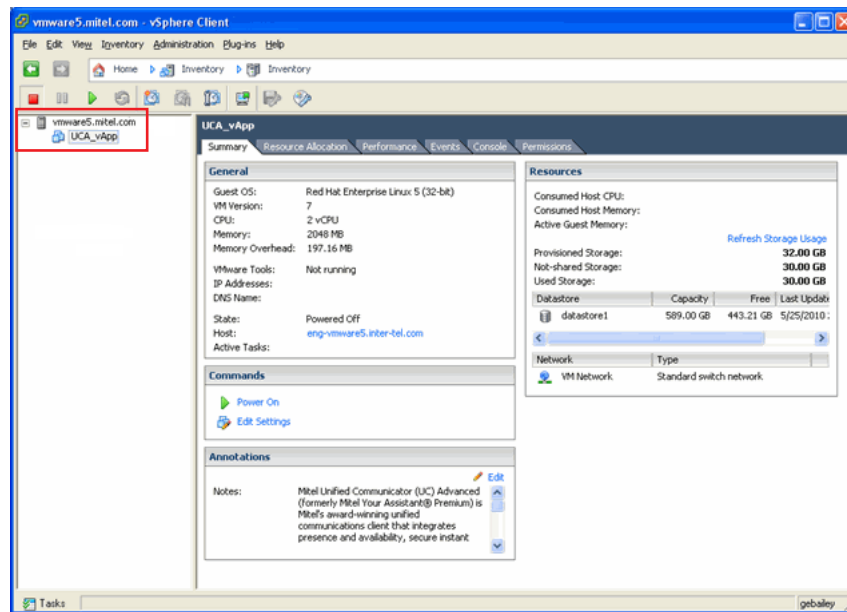
**Note:** vUCA must be installed in the vSphere environment using Thick provisioning. Thin provisioning can cause voice quality issues due to disk sharing.

The VMware vSphere Client must be installed on the local machine before deploying the UC Advanced virtual appliance.

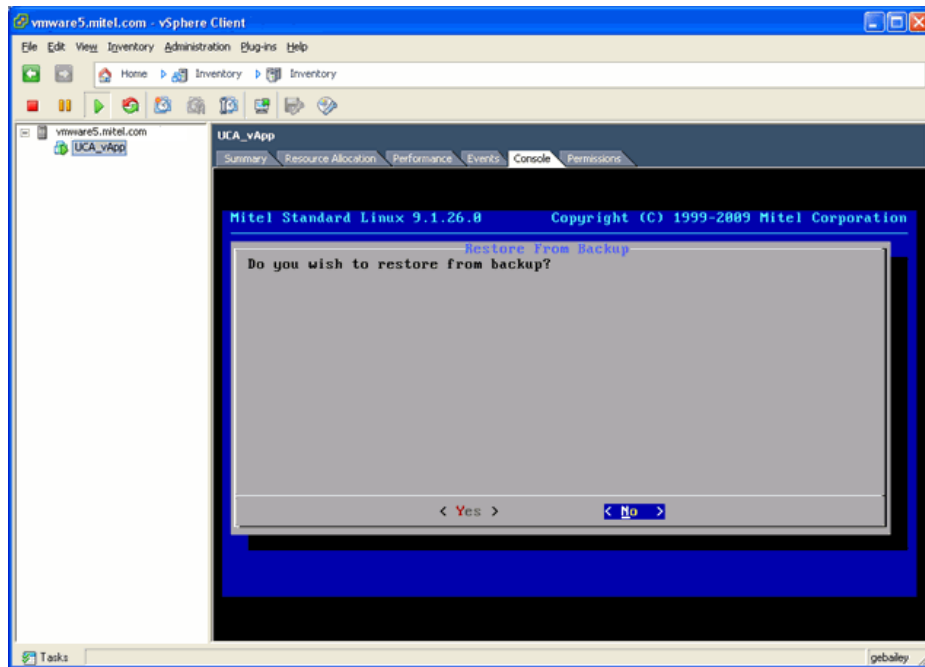
### *To install the UC Advanced virtual appliance:*

1. Download the virtual appliance file (.ova) from Mitel OnLine and save it on your local machine.

2. Start the vSphere Client, and then select File – **Deploy OVF Template....**
3. Select **Deploy from file** and then browse to the location on your machine where you saved the file.
4. Click **Next**. The OVF Template Details page appears.
5. Click **Next**. The End User License Agreement page appears.
6. Click **Accept**, and then click **Next**. The Name and Location page appears.
7. Type a name for virtual server, and then click **Next**. Deployment settings for the virtual appliance are shown.
8. Confirm the settings, and then click **Finish** to deploy the file. A dialog box shows the progress of the files being deployed.
9. When the deployment completes successfully click **Close** to continue.
10. In the vSphere client window, expand the VMware host view to show the newly created virtual machine.



11. Click the Console tab. Click the green arrow to power on the virtual machine.
12. After the virtual machine has booted, the Console Tab shows the MSL installation window.



To complete the configuration for the UC Advanced virtual appliance:

- “Configure MSL” on page 109.
- “Verify UC Server Licensing” on page 113.

## Install and Configure UCA Softphone for VMware Horizon View

This section describes how to install and configure UC Advanced for VMware Horizon View.

### Requirements

UCA for VMware Horizon View requires the following:

- The UCA Client Plugin - the installer for this is called UnifiedCommunicatorAdvancedVMwareViewplugin.msi and can be found on Mitel Online in the 6.0 Software Downloads folder in the UCA folder.
- View 5.0, View 5.1, View 5.2 and vSphere 5.0



**Note:** Versions prior to 5.0 are NOT supported.

- Windows 7 virtual desktop



**Note:** UCA for VMware Horizon View is **NOT** supported on the following products: Windows Vista or XP, Apple, Android or Linux.

It is assumed that the required VMware and Windows components are set up. These can be obtained through VMware and [www.Microsoft.com](http://www.Microsoft.com) respectively.

### Installation

Use the following procedure to install UC Advanced with VMware Horizon View:

1. Install and configure VMware Horizon View and the virtual desktops following the instructions provided by VMware.
2. **It is strongly recommended that the protocol is set to PCoIP and that other protocols are disallowed.** Failure to do so will result in inconsistent or non-existence audio for users. Perform the following steps:
  - a. In VMware View administration, go to **Inventory>Pools**.
  - b. In **Settings**, go to the **Pool Settings** tab.
  - c. Under Remote Display Protocol, choose **PCoIP** for **Default Display Protocol**. Choose **No** for **Allow Users to Change Protocol**. Click **OK** to save your changes.
3. Install and configure the UCA 6.0 server.
4. Install UCA Client on each virtual desktop (in View backend).
  - a. Install the UCA Client (which is downloaded from the UCA server) using the instructions found in the Welcome email.

**NOTE:** Virtual clients look exactly like regular desktops, but they exist in the View backend.

5. Install the VMware View Client on each physical desktop (the physical Thin Client or Thick Client/repurposed PC).
  - a. Point your browser to the address of the View Connection Server.
  - b. Ensure that you select the correct version (32-bit or 64-bit) for your physical desktop.

**NOTE:** Local mode is *not* required.

  - c. Double click the installer.exe file after it downloads and follow the instructions provided.

Thin Client devices normally come with the View client already installed. If this is not the case for your Thin Client, follow the vendor-specific instructions provided with your Thin Client.

6. Install the UCA Client Plugin on each physical desktop. The Plugin is the media driver software that runs on the physical device. This Plugin ensures that voice streams locally through the physical device.
  - a. For the PC/Thick Client - doubleclick the .msi file. A brief progress dialog appears. You do not have to do anything but monitor the progress. Click **Done** when the installation has completed.
  - b. For the Thin Client, perform the following steps:
    - Log in as Administrator (refer to the Thin Client documentation to determine how to log in as Administrator. The default password is vendor-specific.
    - Unlock the device. Refer to your vendor documentation to determine the location of the lock application. **The device will reboot when you unlock it.**

- Log in as Administrator again.
- Download and install the correct version of the .msi file.
- Relock the device by performing a reverse of the procedure in substep 2). **The device will reboot when you lock it.**



**Note:** Automated methods for mass deployment of the Plugin to Thin Client is possible using vendor-specific tools (for example, Wyse Device Manager or HP Device Manager). Procedures for using these tools to perform mass deployment are being developed.



**Note:** Ensure the Thin Client is set to operate in LAN mode (not Wireless mode).

## Configure User Options UCA for VMware Horizon View

Once the component parts (UCA Server, UCA Client, VMware Horizon View, and the UCA Client Plugin) have been installed, the following user configuration steps must be completed for UCA VMware Horizon View to function properly.

### *Teleworker Configuration*

In UCA for VMware Horizon View, the teleworker options enable you to properly configure the UCA software to interact with the VMware Horizon View virtual desktops.

This section outlines how to configure the Teleworker options specifically for use with UCA for VMware Horizon View. These steps do NOT configure normal Teleworker mode. For information on configuring Teleworker mode in the traditional setup, refer to UCA Desktop Client online help, Teleworker topic.

When UC Advanced starts it will always try to connect directly to the Unified Communications server. If UC Advanced is unable to connect directly to the server, it will start in Teleworker mode if you have a valid Teleworker certificate or in VMware Horizon View mode if you have the .msi file installed. If UC Advanced is unable to determine if you have a valid certificate OR if it does not detect a valid VMware Horizon View installation, it will start in Offline mode.

To configure the Teleworker options in UCA for VMware Horizon View, go to the Configuration Screen in the Desktop Client and set the following options:

**Directory Number:** Type your remote Softphone or IP desk phone extension in the box. This must be a number ranging from 1 to 99999999.

**Teleworker Gateway IP:** Type the IP address of the MBG. The IP address should be in the form of xxx.xxx.xxx.xxx.

If there are any leading zeros in the IP address, do not enter those (for example, if the IP address is 074.xxx.xxx.yyy, enter 74.xxx.xxx.yyy).

For UCA VMware Horizon View purposes only, you do not need to enable Teleworker mode, nor configure any of the other Teleworker options. You also do not need to have a valid Teleworker certificate. All these options are greyed out.

### Device Configuration

After you have configured UCA for VMware Horizon View, you must configure the devices (headsets) that work when your client is operating in VMware Horizon View mode. Once the UCA Client Plugin has been installed, you must configure the UCA Client and your virtual desktop to work properly with the endpoint device (Thin or Thick Client).

Use the Softphone Settings in the Configuration menu on the UCA Client to configure these devices.

Ensure that you have chosen either Bluetooth or USB audio device as your default audio device for both Playback and Recording. **ONLY** these options work correctly with UCA for VMware Horizon View:

1. On the physical device, go to Start>Control Panel>Sound.
2. Under both the Playback and Recording tabs, ensure that the default device is the Bluetooth or USB audio device. Click on the proper device. Click on **Set Default** and choose **Default**. Under Properties, ensure **Use this device** is chosen. Confirm all choices.



**Note:** Do not use USB redirection for your audio devices (on the View Client, the option is under Connect USB Device at the top of the screen). Using USB redirection causes audio to flow through the virtual desktop, and results in poor or nonexistent audio.

### Headsets

UCA VMware Horizon View supports several headsets for audio (see Table 21 on [page 83](#) for supported headsets).

### Softphone Settings

Configuring the softphone settings for UCA for VMware Horizon View on the Desktop client is very similar to configuring devices for the thick client version. However, there are now additional options specifically for UCA VMware Horizon View.

In the UCA Client Configuration menu, Softphone Settings, you can choose either Local (to your machine) or View (for UCA VMware Horizon View) options for both the Microphone and the Speaker settings. If you choose local, but no devices are available on your machine, UCA switches automatically to the VMware Horizon View options.

The image shows a screenshot of the 'UCA Configuration' window, specifically the 'Softphone Settings' tab. The window has a blue header with the title 'UCA Configuration' and a close button. On the left is a sidebar with various configuration categories: Appearance, Calendar Integration, Call Notification, Chat Settings, Knowledge Management, Login Notification, PIM Integration, RSS Window, Softphone Settings (which is highlighted), and Contacts View. The main area of the window contains the following settings:

- ☒ Enable SIP soft phone
  - SIP soft phone DN: 72102 (dropdown menu)
  - SIP Connection: Default (dropdown menu)
- ☒ This number is used on multiple devices. (72102)
- Soft phone will use the following devices:
  - Microphone: System Default (dropdown menu)
  - Speaker: System Default (dropdown menu)
  - Alerts: System Default (dropdown menu)
  - Call Control: None (dropdown menu) with a 'Configure' button next to it.
  - Video Camera: Integrated Webcam (dropdown menu) with a 'Configure' button and a video rate dropdown set to 'HD (1600 kbps)'.
- Ringtone:
  - Default (selected radio button) and System Default (radio button) are shown.
  - There is a 'Play' button and a small icon to the right of the radio buttons.
- ☒ Use Teleworker for soft phone
  - Teleworker Gateway: xxx.xxx.xxx.xxx (text input field with a red border)

At the bottom right of the window are three buttons: 'OK', 'Apply', and 'Cancel'.

### Expected Behavior

The UCA Desktop Client operates in one of two modes, namely:

- Local softphone (meaning on the same machine at the Desktop Client itself)
- View softphone (meaning as a plug-in to VMware Horizon View).

In order to switch between softphones, UCA must deregister the current softphone to bring the new active softphone online. This switchover causes a delay - no more than five to ten seconds.

The UI does not directly indicate which mode of softphone is active.



## Access the UC Server Administration Page

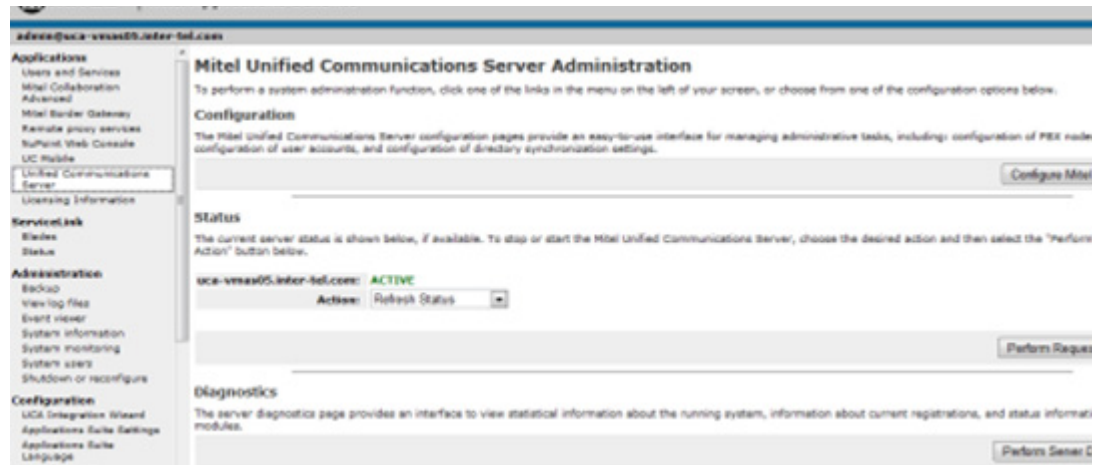
The MSL server manager interface provides access to the Mitel UC Server Administration page. From this page you can:

- access the Unified Communications configuration interface to provision UC Advanced (see [page 122](#)).
- view and refresh the server status, and start and stop the server (see [page 203](#)).
- generate diagnostics information (see [page 204](#)).
- reinitialize the server (see [page 212](#)).

*To access the UC Server Administration page:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, `https://<MSL_server_FQDN>/server-manager`) where the UC Server is installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. Under Applications, click **Unified Communications Server**. The Mitel UC Server Administration page appears.

The page may show a status of **STARTING** while the server is being started. The status changes to **ACTIVE** when the server is operational.




## Provision UC Advanced

Provision UC Advanced as documented in the UC Server Administrator interface online help. Refer to the **Provisioning UC Advanced** help topic, which includes the high-level provisioning procedure, with links to detailed instructions and field descriptions.

*To access the UC Server administrator interface and online help:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the UC Server is installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. In the left navigation pane under Applications, click **Unified Communications Server**. The Mitel UC Server Administration page appears.
4. Click **Configure Mitel UC Server**. The **Enterprise** tab appears.

The screenshot shows the 'Mitel Unified Communications Server Configuration' interface with the 'Enterprise' tab selected. The page contains enterprise-wide configuration settings. A 'Settings for' dropdown is set to 'Documentation testing'. Below this, there is a 'Settings' section with various fields: Enterprise ID (test), Description (Documentation testing), Enterprise domain (47.100.100.100), Voice mail server, Administrator e-mail, Switch type (Mitel Communications Director), Collaboration server type ([None]), Language (English (US)), and Time zone (U.S.A. - Arizona (GMT-07:00)). There are also links for 'Add New Enterprise' and 'Delete This Enterprise'.

5. Click the help icon  to open the online help. The About Unified Communications Server topic appears.
6. In the Help table of contents, click the **Administrator Tasks** link, and then click the **Provisioning UC Advanced** link. The Provisioning UC Advanced topic appears, which includes the high-level steps you should follow to provision the system.

High-level provisioning steps include:

- a. Create an enterprise.
- b. Add Feature Profiles.
- c. Add PBX nodes.
- d. Add collaboration servers (*optional*).

- e. Configure the enterprise fields and options.
- f. Add user accounts using one of the following methods:
  - Add user accounts automatically, by configuring a an Active Directory/Lightweight Directory Access Protocol (AD/LDAP) Corporate Directory Synchronizer, and then completing a manual synchronization.



**Note:** Refer to the following topics in the UC Server Administrator online help for detailed information about AD/LDAP Corporate Directory Synchronizers:

- Synchronization Tab
  - Adding and Editing AD/LDAP Synchronizers
- Add user accounts automatically, by configuring a Private Branch Exchange (PBX) Node Corporate Directory Synchronizer, and then completing a manual synchronization.
  - Add user accounts manually. Accounts that you create manually are not affected if you later configure a Corporate Directory Synchronizer and complete an AD/LDAP or PBX node synchronization.
- g. Configure Automatic Call Distribution (ACD) settings (*optional*).
  - h. Configure Peering with other UC or external servers (*optional*).
  - i. Configure IM and presence Federation (*optional*). Configuration options include:
    - **Peering tab:** Add an external IM server and perform an AD/LDAP synchronization with the server. After synchronization, the IM server contacts are imported to the UC Server database (visible from the Corporate Directory tab) and federation is automatically enabled.
    - **Federation tab:** Configure federation from the Federation tab in the UC Server Administrator Interface.



**Note:** Federation must be fully-configured on the IM server before you configure federation for the UC Server (see [page 27](#)).

- j. Send the Welcome E-mail Message to UC Advanced users (see [page 125](#)).

## Install the Desktop Client

The UC Advanced client installer ships as a Windows Installer package. You can use a file server on your network as a software distribution point for the UC Advanced client. When you complete the system configuration, send the Welcome E-mail to users, which includes a link to the software location on the server.

### Software Distribution Point

A Software Distribution Point uses Active Directory Group Policy objects to deploy UCA using Active Directory Group Policy objects. This enables UCA to be run from a single location and appear to be installed on every user's desktop.

Installing UC Advanced using a distribution point is done with an administrative install of the installer package to a network share. The share point must be accessible to all users who will install UC Advanced. The command for the administrative installation is:

```
%>msiexec /a UnifiedCommunicatorAdvanced.msi
```

The administrative installation wizard prompts you to enter a location for the administrative image. Users can be instructed to install UC Advanced from this folder via the network share. The users can run the installation wizard by clicking the file and entering the UC Server FQDN when prompted.

Alternatively, a transform file (see [page 134](#)), or the Explorer shortcut that includes the IP property in the command parameters, could be provided:

```
%>msiexec /i UnifiedCommunicatorAdvanced.msi  
UC_SERVER_HOSTNAME="192.168.1.66"
```

In this example, UC\_SERVER\_HOSTNAME property is set to the IP address of the UC Server.

Suppressing the installation wizard dialogs can further customize the installation by using the /qn flag. More customization options can be found in the Windows Installer SDK documentation at <http://msdn2.microsoft.com/en-us/library/aa367988.aspx>.

### User Installation Permissions

Installing UC Advanced requires administrator permissions on the user's computer. In Windows XP, the user must be logged in with Windows administrative permissions to install the client. In Windows Vista/7, the user is prompted to provide User Account Control credentials (standard user) or confirmation (administrator) to install the client. Running the client does not require administrative privileges.

All data files that are modified (logs, config, contact database, recorded calls, etc.) when settings are updated (call forwarding profile, startup mode, etc.) are located in one of the following folders or subfolders:

- **XP:** C:\Documents and Settings\- **Vista/Windows 7:** C:\Users\

## Client Firewalls

A client computer that uses a firewall, such as Windows Firewall or a third-party firewall, must specify UCA.exe and UCASoftphoneManager.exe as exceptions in the firewall's configuration settings. This allows UCA.exe and UCASoftphoneManager.exe to accept network traffic through the firewall. The UC Advanced 6.0 client installer adds these exceptions automatically.

## Welcome E-mail Message

After you configure the system, you can send the users a Welcome E-mail Message that provides users with the following information and links:

- **The UC Server Fully Qualified Domain Name (FQDN):** Required when installing the UC Advanced Desktop Client, UCA Mobile for BlackBerry and MiVoice for Lync software.
- **UC Advanced Login ID and Password:** Used to log in to the UC Advanced Desktop Client, Web Portal, UCA Mobile for BlackBerry and MiVoice for Lync.
- Softphone and Desk phone extensions.
- **A link to the UC Advanced URL:** Provides access to the Web Portal.
- **A link to the Quick Reference Guide:** Provides installation instructions and a brief overview of the UC Advanced product.
- **A secure link to the Desktop Client Software:** Provides access to the Desktop Client software .msi file.
- **A secure link to the UCA Mobile for BlackBerry Software:** Provides access to the UCA Mobile for BlackBerry software.
- **A secure link to the UCA Mobile for Android Software:** Provides access to the UCA Mobile for Android software.
- **A secure link to the UCA Mobile for iPhone and iPad Software:** Provides access to the UCA Mobile for iPhone and iPad software.
- **A secure link to MiVoice for Lync Software:** Provides access to MiVoice for Lync software.



**Note:** To configure a secure connection to the UC Server from a BlackBerry mobile device, users are required to know the key store password on their device to accept the UC Server SSL certificate.

Dear user,

This e-mail message contains your Mitel Unified Communicator Advanced credentials:

Unified Communications Server (Fully Qualified Domain Name): test.com

Login ID: userABC@test.com

Password: password

Desk Phone: 12345

Soft Phone: 67890

Click the following link to access the UC Advanced Web/Mobile Portal from your computer or mobile device. Log in using the Login ID and Password provided above.  
Link to Web/Mobile Portal Login\*: <https://test.com/ucs/webclient>

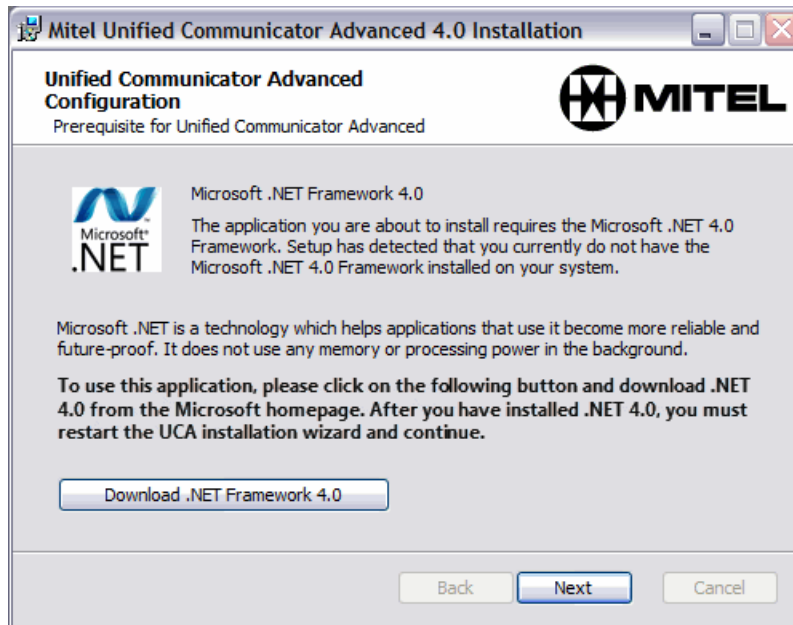
Click the following link to download a PDF of the UC Advanced Quick Reference Guide, which provides basic usage information for UC Advanced.  
Link to Quick Reference Guide: [http://edocs.mitel.com/UG/UCA\\_QRG.pdf](http://edocs.mitel.com/UG/UCA_QRG.pdf)

Click the following link to download the Desktop Client software. Refer to the UC Advanced Quick Reference Guide for installation and log in instructions.  
Link to download client software:

**Figure 15: Welcome E-mail Message Example**

## Microsoft .NET Framework

The UC Advanced Desktop Client requires the installation of the Microsoft .NET Framework v4.0 prior to installing the Desktop Client. When the user attempts to install the Desktop Client, if the v4.0 .NET framework is not detected, he or she will be prompted to download and install it.



**Figure 16: Microsoft .NET Framework 4.0 Download Prerequisite**

After the user installs the .NET framework, he or she will need to restart the UC Advanced Desktop Client installation. You can download the [Microsoft .NET Framework v4.0](http://www.microsoft.com/downloads) from the Microsoft Web site ([www.microsoft.com/downloads](http://www.microsoft.com/downloads)).

## Installation Procedure

This section describes the procedure used to complete a typical installation for the UC Advanced Desktop Client from a computer that has administrator permissions and access to the software. For custom installation options, see [page 212](#).

The installation wizard requires the user to provide just one parameter during installation: the FQDN of the UC Server. The FQDN is provided in the Welcome E-mail message (see [page 125](#)) that you generate at the end of the provisioning process.



**Note:** For user level step-by-step basic installation instructions for desktop and mobile clients, go to “[UC Advanced Client Considerations:](#)” on [page 151](#)



**Note:** The "Run Setup Wizard" command previously in the Desktop Client Main menu is no longer required and was removed in UC Advanced 5.1.

### *To install the UC Advanced Desktop Client:*

1. Close all Windows applications on the computer.
2. Install the Microsoft .NET Framework on the user's computer (see [page 127](#)).
3. Click the link provided in the Welcome E-mail message to access the client software.
4. In the File Download dialog box, click **Run** to launch the client download.
5. In the Security Warning dialog box, click **Run** to launch the client installer. The Welcome dialog box appears.
6. Click **Next**.

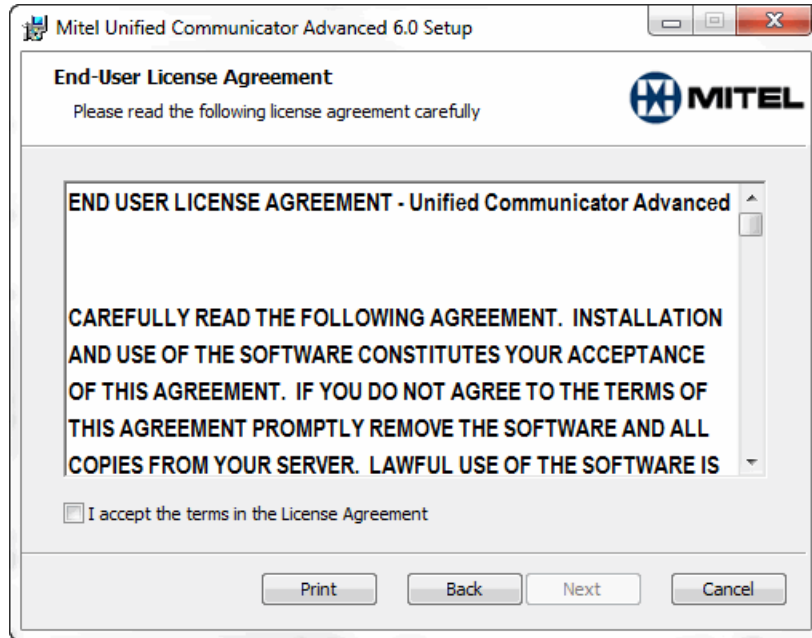




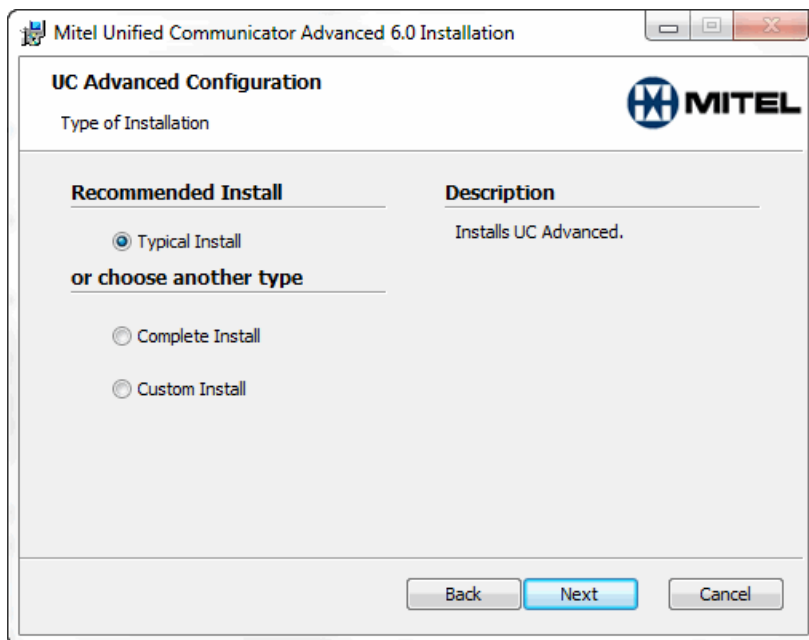


**Note:** If the v4.0 Microsoft .NET Framework is not detected on the computer, you are prompted to download and install it (see [page 127](#)). You must restart the Desktop Client installation following the installation of the .NET Framework.

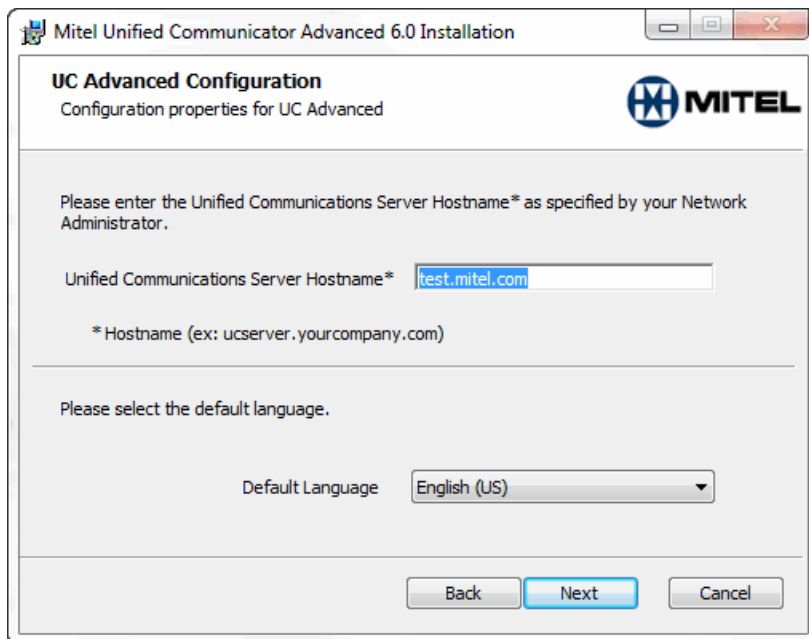
7. Select **I accept the terms of the License Agreement**, and then click **Next**.



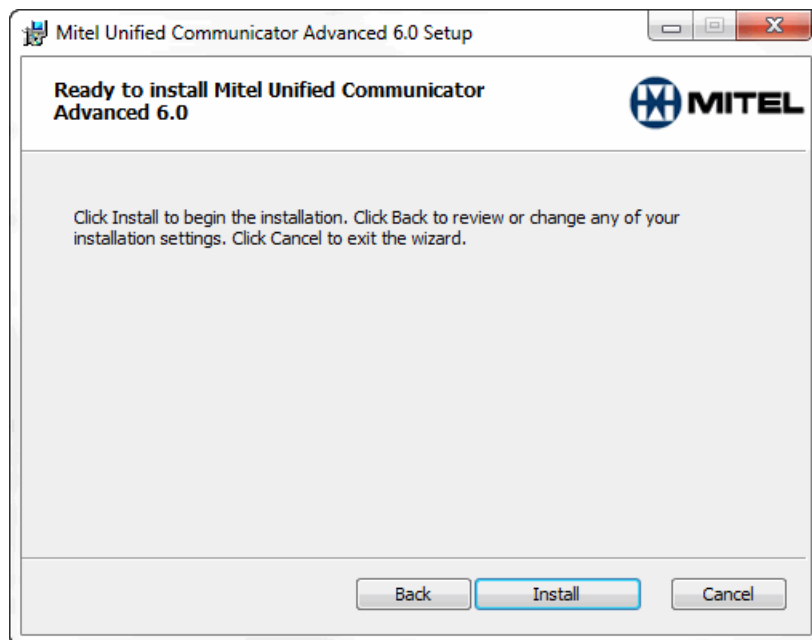
8. Select an installation type and then click **Next**. Options include:
  - **Typical Install:** Includes the Desktop Client, Dial From IE, and the PIM extensions for the PIMs that are installed on the user's computer (Outlook, Lotus Notes, or ACT!), the Google OR Microsoft Exchange Server information for the user.
  - **Complete Install:** Includes all of the Typical Install components and the UC Advanced SDK.
  - **Custom Install:** Installs the Desktop Client and allows the user to deselect or select optional components (see [page 212](#)).



9. Type the Fully Qualified Domain Name for the UC Server in the box. The FQDN is provided in the Welcome E-mail message (see [page 125](#)).
10. Select a Default Language, and then click **Next**.



11. Click **Install**.



The Desktop Client software is installed on the computer.

**12.** Click **Finish** to complete the installation process.

By default the Desktop Client launches automatically.

## Custom Installation Options

If you do not want to use a software distribution point for the client software, the following options are available for UC Advanced client installation:

- [IntelliMirror](#) below
- [“Logon Script”](#) on page 132
- [“SMS”](#) on page 132
- [“Group Policy”](#) on page 132
- [“Citrix Deployments”](#) on page 133

### IntelliMirror

Microsoft® IntelliMirror® management technologies can be used with Windows Installer to deploy and manage the installation of Mitel UC Advanced client. Two policies must be addressed when deploying UC Advanced for IntelliMirror:

- User Data Management
- Software Installation and Maintenance.

UC Advanced persists user settings such as window settings, the call log, history, personal contacts, and favorites. These settings are saved in the user's Application Data folder.

For deployment, UC Advanced should be assigned to users such that when a UC Advanced user logs in to a computer that does not have UC Advanced installed, UC Advanced gets installed.



**Note:** If the site prevents software installations to be performed by the user, automatic upgrades of the UC Advanced client deployed by IntelliMirror will fail during the process. Instead, use your current installation mechanism to deploy any client upgrades.

The UC Advanced IP property should be set using an installer transform (see [“Creating a Transform” on page 134](#)).

For more information refer to the [Step-by-Step Guide to Software Installation and Maintenance](http://technet.microsoft.com/en-us/windowsserver) (<http://technet.microsoft.com/en-us/windowsserver>).

### Logon Script

The Windows Script Host can also be used to create a logon script for deploying UC Advanced. Logon scripts use the same installation techniques as the software distribution point, except the mechanism used to run the installer is a script rather than an Explorer shortcut. The logon script is set through an Active Directory Group Policy. An example of a logon script that will install UC Advanced might be

```
Set oShell = CreateObject("Wscript.Shell")
oShell.Run msixec /i /q UnifiedCommunicatorAdvanced.msi
```

See the [Windows Management Instrumentation](http://msdn2.microsoft.com/en-us/library/aa286547.aspx) site (<http://msdn2.microsoft.com/en-us/library/aa286547.aspx>) for more information on scripting.

### SMS

Where scheduling, inventory, status, reporting, and support for deployment across a wide area network is required, Microsoft recommends using Systems Management Server 2003 (SMS).

Again, refer to the syntax shown for Software Distribution Point to create the installer command that SMS will run to install UC Advanced on the client computer. See [Systems Management Server Home](http://www.microsoft.com/smsserver/) (<http://www.microsoft.com/smsserver/>) for more information on SMS.

### Group Policy

You can create a Group Policy object to deploy UC Advanced clients. For a network install, the installer can be assigned to users with a Group Policy object (GPO). The GPO should install the software from an administrative image installed on a network share. For a detailed explanation on how to install software using an Active Directory Group Policy, see [Step-by-Step Guide to Software Installation and Maintenance](http://technet.microsoft.com/en-us/windowsserver) (<http://technet.microsoft.com/en-us/windowsserver>).

## Citrix Deployments

The UC Advanced client can be deployed using the Citrix delivery system. UC Advanced supports both Desktop mode and Web mode for the following Citrix versions:

- Citrix® XenApp® Client v6.0 (Requires Citrix Presentation™ Server 6.0, 32- or 64-bit)
- Citrix XenApp Client v6.5 (Requires Citrix XenApp Server 6.5, 32- or 64-bit)

The following restrictions apply when the client is running on a Citrix server:

- **No softphone:** UC Advanced acts as a desk phone controller under Citrix Presentation Server. The Softphone option is not available to the user at client startup, nor does the Configuration dialog box provide the **Softphone Settings** option. Softphone features such as call recording and Teleworker are not available.
- **No collaboration:** The Collaboration feature is not available under Citrix. The Collab menu does not appear in the main window and collaboration invitations sent to a user running UC Advanced under Citrix do not cause an invitation pop-up to display. In addition, video calls are not supported for Citrix deployments.
- **Access to Citrix-based resources only:** UC Advanced cannot access resources that reside on the client workstation. This includes the local file system, PIMs, and instant messaging clients. To be accessible to UC Advanced, these resources must reside on the Citrix server:
  - *PIM integration:* UC Advanced integrates normally with PIMs that are running on the Citrix server.
  - *Exchange Server integration:* UC Advanced integrates normally with the Microsoft Exchange server.
  - *Knowledge Management:* The Knowledge Management feature works the same on Citrix, provided the indexed Outlook folders and file paths are on the Citrix server.
  - *Instant Messaging:* UC Advanced integrates normally with Microsoft Messenger and Microsoft Office Communicator (LCS) clients that are running on the Citrix server.

For information about setting up Citrix servers to run UC Advanced, refer to the Citrix product documentation.

## Installer Transforms

Windows Installer packages can be customized with installer transforms. Installer Transforms are files that, when run with the installer package, modify certain installation properties and application features.

The UC Advanced installer package requires that the UC Server IP property be set at install time. If the installer package is executed without any command-line parameters setting this property, the installer package prompts the user for it.

Alternatively, a transform can be created that will set this property. The transform can be specified in the command string used to install UC Advanced or it can be specified when installing software using an Active Directory Group Policy.

If the server IP property is set in this way, the installer can be run with reduced or “silent” user interaction. More customization options can be found in the [Windows Installer SDK](http://msdn2.microsoft.com/en-us/library/aa367988.aspx) documentation (<http://msdn2.microsoft.com/en-us/library/aa367988.aspx>).

### Creating a Transform

You can use third-party tools to create a transform. These tools are usually bundled with MSI authoring tools. However, the transform is simple and can be created with a simple script using COM components deployed on platforms supported by UC Advanced. The following script will create a transform called **transform.mst**.



**Note:** The following script is an example based on documentation provided by Microsoft. It is not a Mitel supported script and is provided for information only.

```
Option Explicit

Dim wi, basedb, db, fs, sh, infile, ip, sql, view

Const msiTransformValidationLanguage = 1

Const msiTransformErrorNone = 0

Const msiOpenDatabaseModeReadOnly = 0

Const msiOpenDatabaseModeTransact = 1

Set sh = CreateObject("WScript.Shell")

If WScript.Arguments.Count < 2 Then

    WScript.Echo "Usage: maketransform.vbs <input file> <ya server ip>"

    WScript.Quit

End If

Set fs = CreateObject("Scripting.FileSystemObject")

Set wi = CreateObject("WindowsInstaller.Installer")

infile = WScript.Arguments(0)

ip = WScript.Arguments(1)

fs.CopyFile infile, "tmp.msi"

Set basedb = wi.opendatabase(infile, msiOpenDatabaseModeReadOnly)

Set db = wi.opendatabase ("tmp.msi", msiOpenDatabaseModeTransact)

sql = "INSERT INTO Property (Property.Property, Property.Value) VALUES" & _

    "('UC_SERVER_HOSTNAME', '" & ip & "')"

Set view = db.OpenView(sql)
```

```

view.Execute

db.Commit

db.GenerateTransform basedb, "transform.mst"

db.CreateTransformSummaryInfo basedb, "transform.mst", _
    msiTransformErrorNone, msiTransformValidationLanguage

Set view = Nothing

Set db = Nothing

Set wi = Nothing

Set sh = Nothing

fs.DeleteFile "tmp.msi"

Set fs = Nothing

```

The output is **transform.mst** and this transform file can be used to modify a UC Advanced installation.

## Installer Properties

The following table lists the UC Advanced installer properties that may be modified to create custom deployments.

**Table 23: Modifiable Installer Properties**

Property	Valid Values	Description
UC_SERVER_HOSTNAME	A valid IP address or computer name.	The PC running the UC Advanced management software where the user's account is configured.
UC_LANGUAGE	en-US North American English en-GB British English nl-NL Dutch fr-CA Canada French de-DE German pt-BR Brazilian Portuguese it-IT Italian es-MX Latin American Spanish fr-FR European French es-ES European Spanish zh-CN Simplified Chinese zh-TW Traditional Chinese	This is the language UC Advanced will use on its first startup.

**Table 23: Modifiable Installer Properties (continued)**

Property	Valid Values	Description
<p>The following properties are associated with Teleworker and are optional. With the exception of UC_DEF_TW_DN and UC_DEF_TW_GATEWAYIP, the default values are acceptable for most configurations.</p> <p>All of these values are configurable in the UC Advanced client's Teleworker Configuration panel and are provided in the installer as a convenience to administrators that may use a deployment mechanism like SMS or Active Directory Group Policies.</p>		
UC_DEF_TW_DN	A numeric value 3 to 7 digits long. The default is blank.	The directory number of the Teleworker softphone that is being configured.
UC_DEF_TW_ENABLED	"True" or "False". The default is "False".	Whether or not Teleworker is enabled. If enabled, the user will still be required to get the certificate through the Teleworker configuration panel.
UC_DEF_TW_GATEWAYIP	A valid IP address (xxx.xxx.xxx.xxx). The default is blank.	The IP address of the Teleworker gateway. This must be an IP address, not a computer name.
UC_DEF_TW_YASERVERPORT	A numeric value between 1 and 65535. The default is 2114.	The port of the PC running the UC Server component of the UC Advanced Management Software.
UC_DEF_TW_TELEPHONYSERVERPORT	A numeric value between 1 and 65535. The default is 2116.	The port of the PC running the UC Advanced Telephony Server component of the UC Advanced Management Software.
UC_DEF_TW_PRESENCESERVERPORT	A numeric value between 1 and 65535. The default is 35000.	The port of the PC running the UC Server component of the UC Advanced Management Software.
UC_DEF_TW_COLLABSERVERPORT	A numeric value between 1 and 65535. The default is 37000.	The port of the PC running the Your Assistant Collaboration Server (if available).



## Install MiVoice for Lync Client

Lync deployment is supported in various options as seen in the table below. MiVoice for Lync is a Lync PlugIn which integrates seamlessly with Microsoft Lync application.



**Note:**

MiVoice for Lync is supported on MAS deployed UCA only.

MiVoice for Lync Deskphone only users: those users only require the **Desktop client SDK** feature.

MiVoice for Lync Softphone only users OR those users with a Softphone and an associated Deskphone will require the **Softphone** feature in addition to the **Desktop client SDK** feature (see [Table 1](#)).

**Table 24: Lync Deployment Options**

Lync Server	MCD	UCA Server	Supported (Yes/No)
Local	Local	local	Yes
Local	Cloud	Cloud	Yes
Cloud (Office 365)	Local	Local	Yes
Cloud (Office 365)	Cloud	Cloud	Yes

### Information email



**Note:** Microsoft Lync 2010 or 2013 should be installed prior to installing MiVoice for Lync.

Once the MiVoice for Lync account is created on the UCA server, the user will receive a Welcome email with the following information:

- User client Login ID (Login ID is driven from Active Directory - AD) and password
- Link to download the MiVoice for Lync plug-in software installer
- The Server Fully Qualified Domain Name - FQDN (host name)
- User account information (desk phone, softphone, voice mail, etc...)
- Teleworker (MBG) IP Address.

### MiVoice for Lync (Lync Plug-in) installer

The following components will be installed on the user's computer (may vary if 2010 or 2013 clients) - the following are major components only and not the complete component list:

- Mitel Lync Plug-in executable file (also known as MiVoice for Lync)
- Mitel UCA and Lync client Software Development Kit - SDK components (as .dll files)
- Mitel UCA headless client
- Mitel Lync Plug-in service

- Configuration settings (like setting to indicate that UCA client shall run without a UI)

### *Installation wizard*

- All the components of MiVoice for Lync will be installed mandatorily and user will not be able to select/deselect Plug-in components for installation.
- Installer will prompt user to enter configuration options like UCA server FQDN etc.
- There will be no desktop/start menu icon specific for MiVoice for Lync client installed on the computer as this application will be launched via Microsoft Lync.
- User can re-run the installation wizard. This will allow user to change configuration options like UCA server FQDN or repair the damaged installation.



**Note:** In the event that another version of UCA client (or MiVoice for Lync) is already installed on the user's computer, the user will be prompted to remove the earlier installation of the client.



**Note:** Ideally MiVoice for Lync installation shall be done after the installation of MS Lync 2010 or 2013 client only. Installing the MS Lync client after plug-in installation may override settings/configuration files of plugin and is not recommended. User should re-install the MiVoice for Lync if problem are encountered in this scenario.



**Note:** The user must have installation permissions on the computer or provide the administrator credentials when prompted.

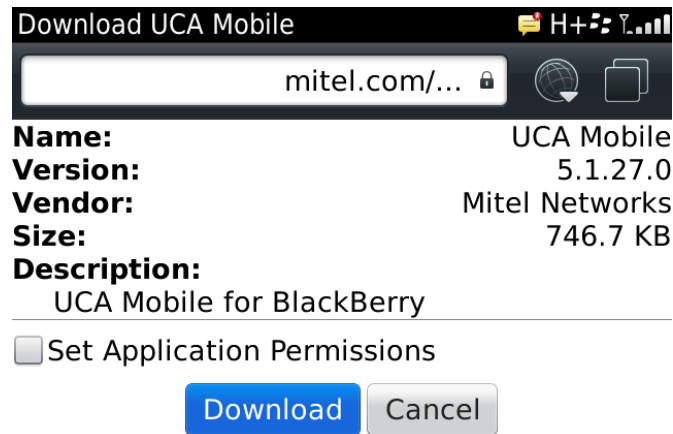
## Install the Mobile Client

This section describes the procedure used to complete a typical installation for the UC Advanced Mobile for BlackBerry client from a mobile device running a supported BlackBerry mobile operating system (see [page 85](#)).

The Welcome e-mail message (see [page 125](#)) provides the user with the information that they need to download and install the software, and connect to the UC Server.

### *To install and configure the UCA Mobile for BlackBerry client:*

1. Close all other applications on the BlackBerry device.
2. Open the Welcome E-mail message using the BlackBerry e-mail client.
3. Click the link provided in the Welcome E-mail message to access the client software. The BlackBerry Web browser opens and the UCA Mobile downloads page appears.



4. Select **Download**. The software is downloaded to the mobile device and automatically installed. A message indicates that the application was successfully installed.
5. Select **Run** to launch the UCA Mobile client.



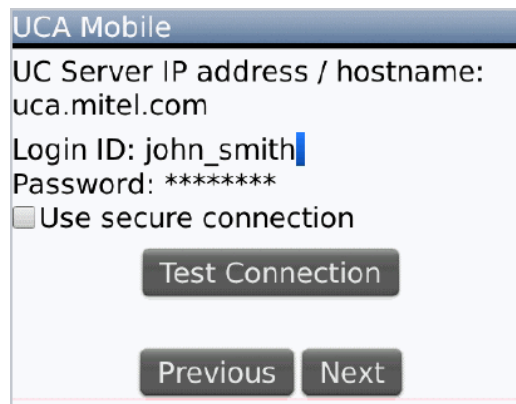
**Note:** If you are prompted to reboot, select **Reboot** to complete the upgrade. The mobile device powers off and then on again. Launch the UCA Mobile client by selecting the UCA Mobile icon in the Downloads folder.

6. Select **I agree** for the End User License Agreement (EULA). The UCA Mobile setup wizard welcome page appears.

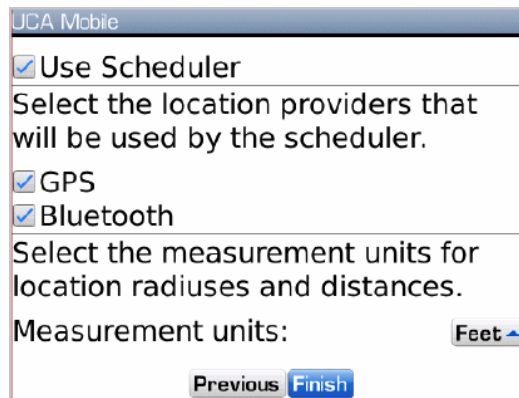


**Note:** If the mobile device is configured for a language that is not supported by UC Advanced, you are prompted to select a supported language (see [page 3](#)).

7. From the welcome page, select **Next**.
8. Type the following information (provided by the UC Advanced welcome e-mail message, see [page 125](#)) in the appropriate fields:
  - UC Server IP address/hostname (FQDN)
  - Login ID
  - Password



9. If you have configured a secure connection for mobile clients, instruct users to select the **Use secure connection** option.
10. Select **Test Connection** to verify that you can connect to the UC Server with the entered credentials. The connection status appears.
11. Select **Next**.
12. Configure the following:
  - Enable the **Use Scheduler** option (*optional*).
  - Select a location provider (**GPS**, **Bluetooth**, or both).
  - Select a measurement unit.



The image shows a screenshot of the 'UCA Mobile' configuration window. It has a title bar with the text 'UCA Mobile'. The main content area contains the following elements:

- A checkbox labeled 'Use Scheduler' which is checked.
- Text: 'Select the location providers that will be used by the scheduler.'
- Two checkboxes: 'GPS' and 'Bluetooth', both of which are checked.
- Text: 'Select the measurement units for location radiuses and distances.'
- A label 'Measurement units:' followed by a dropdown menu currently showing 'Feet'.
- At the bottom, there are two buttons: 'Previous' and 'Finish'.

13. Select **Finish**.



By default, following the installation, the UCA Mobile icon is saved to the Downloads folder on the device. Users can move the icon to their home page for easier access to the application.

## Remote User Configuration

After the Desktop Client is installed on a computer that resides outside of the local network, you must configure remote user access to UC Advanced. Configuration procedures differ for each PBX. See the configuration information that applies to the site's PBX:

- [“MCD PBX Configuration for Remote Users”](#) below
- [“Mitel 5000/Inter-Tel Axxess PBX Configuration for Remote Users”](#) on page 148

### *TCP/TLS to UDP Connector*

The TCP/TLS to UDP connector is a feature introduced in MBG 7.1 SP2 as part of MAS 4.0 SP2. This feature is also available in MBG 8.0 as part of MAS 5.0. This connector enables UCA desktop and mobile clients to configure the SIP softphone to use TCP or TLS protocol when connected to MBG. MBG will convert the TCP or TLS protocol to UDP when communicating to the MCD or the 5000 PBX. Using the TCP/TLS protocol for SIP softphone eliminates many of the Network Address Translation issues encountered when using UDP for SIP signalling.

This connector is supported in the MBG in server gateway mode and in DMZ setup ([“MBG and Remote Proxy Services Configuration”](#) on page 104). This connector is automatically enabled or disabled when UCA support on MBG is enabled or disabled.



**Note:** This connector is supported only for UCA SIP softphones and there is no support for any 3rd party SIP phones. The UCA clients must enable teleworker mode for the SIP softphone to use this connector on the MBG when the signalling protocol is set to TCP or TLS.

MCD supports TCP and TLS for SIP in MCD 6.0 and later versions. The default SIP protocol used by different UCA clients are shown below:

- Desktop UCA client version 6.0: defaults to TCP when connecting to MCD directly. Defaults to UDP in teleworker mode. Defaults to UDP when connecting to 5k PBX.
- iOS (iPad and iPhone) and Android UCA clients version 5.1: defaults to UDP in all modes.

For 5000 PBX this connector on MBG has to be used when TCP or TLS protocol is enabled in the SIP softphone configuration in the UCA clients. 5000 PBX does not support SIP over TCP or TLS.



**Note:** Mitel recommends that users always set the iOS (iPad and iPhone) clients in teleworker mode and set the protocol to TCP or TLS when using MBG 7.1 SP2 or later with TCP to UDP connector enabled. Otherwise, if the SIP protocol is set to UDP, the iOS operating system will not wake up the UCA client application during an incoming call (while UCA client application is in the background).

## MCD PBX Configuration for Remote Users

This section describes the required configuration for remote users connected to an MCD PBX. Remote User Configuration includes:

- “Desktop Client Softphone and Teleworker Settings” below
- “MBG Device Configuration” on page 144

For additional port information, see the *Mitel UC Advanced Engineering Guidelines*.

### Desktop Client Softphone and Teleworker Settings

Before users can use UC Advanced softphone features from Desktop Client, they must configure as per options under: Main menu – Configuration – **Softphone Settings**.

The screenshot shows the 'UCA Configuration' window with the 'Softphone Settings' tab selected. The left sidebar lists various configuration categories, with 'Softphone Settings' highlighted. The main area contains the following settings:

- ☒ **Enable SIP soft phone**
  - SIP soft phone DN: 72102
  - SIP Connection: Default
- ☒ **This number is used on multiple devices. (72102)**
  - Soft phone will use the following devices:
    - Microphone: System Default
    - Speaker: System Default
    - Alerts: System Default
    - Call Control: None (with a 'Configure' button)
    - Video Camera: Integrated Webcam (with a 'Configure' button and 'HD (1600 kbps)' dropdown)
  - Ringtone:
    - ☒ Default
    - ☐ System Default
    - ... (button)
    - ▶ Play (button)
- ☒ **Use Teleworker for soft phone**
  - Teleworker Gateway: xxx.xxx.xxx.xxx

At the bottom right, there are 'OK', 'Apply', and 'Cancel' buttons.

Additionally, in Teleworker mode, the remote UC Advanced client uses a secure SSL connection with the Mitel Border Gateway (MBG) for all communication between the client and the UC Server.

Make sure that you provide the information in Table 25 [Desktop Client Softphone Settings](#) to users so that they can configure the Teleworker fields. Refer users to the online help for instructions.

**Table 25: Desktop Client Softphone Settings**

Field	Description
Enable SIP softphone	Enable this option if you wish to use the SIP softphone on this desktop client
SIP softphone DN	Select SIP softphone extension (Directory Number) to use from pull-down menu.
SIP Connection	Options: Default, TCP, UDP and TLS. Leave at Default. Note: When connected to either 5000 or MCD PBX, TCP and TLS protocols are only supported when the Use Teleworker for soft phone is enabled. SIP TCP and SIP TLS are supported for endpoints (not trunks) as of MCD 6.0. (Also see <a href="#">"TCP/TLS to UDP Connector"</a> on page 141).
This number is used on multiple devices	This feature allows the user to use their SIP extension on other devices such as an iPad, iPhone or Android devices. With this option selected, they can register their SIP softphone extension from another device if licensed to do so
Microphone, Speaker, Alerts, Call control	Users can leave at default or select desired devices to suit their needs.
Video Camera	This option will appear only if Enable SIP softphone (above) is set. Select which camera to use from the pull-down menu. Select the video data rate or leave at default based on the camera selected.
Ringtones	Use system default or browse to desired ringtone, click play to test.
Use Teleworker for softphone	If this flag is enabled, the Minet or SIP Softphone will always connect to the MBG.
Teleworker Gateway IP	Mitel Border Gateway (MBG) IP or FQDN Address is mandatory if <b>Use Teleworker for softphone</b> is set. The IP address should be in the form of xxx.xxx.xxx.xxx.



**Note:** Teleworkers equipped with both a Mitel deskphone and a Mitel softphone will use two teleworker licenses.



**Note:** A MiNet Softphone and SIP Softphone cannot be active at the same time.

## MBG Device Configuration

To provide access to remote users accessing the UC Server through the MBG, you must add or enable a device for each remote user:

- “To add or enable MiNet devices in the MBG for remote MCD users:” below
- “To add or enable SIP devices in the MBG for remote MCD users:” on page 147



**Note:** Verify that SIP support is enabled on the MBG (it is disabled by default). Go to Configuration Settings, under SIP Options.

### *To add or enable MiNet devices in the MBG for remote MCD users:*

1. Open a Web browser and navigate to the MSL Server Manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the MBG/Remote Proxy Services are installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. Under Applications, click **Mitel Border Gateway**.
4. Click **Services > MiNet Devices**.

### Manage Mitel Border Gateway

Status
Configuration
Services
Applications
Clustering

MiNet devices
Device settings by DN
SIP devices
SIP trunking
Recording status

» Location: Minet device settings

Welcome to the MBG administrative interface. From here you can manage all aspects of the MBG's behaviour. Above are various tabs for different parts of the system. If at any time you require more information, click the Help icon in the upper-right corner of the page.

Below is a list of devices for this MBG server. You may change the number of devices displayed in each page by using the pulldown menu view a device in detail, or edit its settings, click on the Device ID.

The "Filter" field may be used to filter the result set displayed in this page. Some of the most common filters are provided in the pull-down below the filter field.

To apply a supported operation to the current result set en masse, select the "Bulk modify" button and pick an operation.

See the online help for more information.

Devices per page 20 Refresh

Filter listing

Canned filters (select and apply)

Modify current list in bulk

[Add a MiNet device](#)

Device Information							
Enabled	Device ID ↑	Device DN(s)	Current ICP	Configured ICP	Description	Device Type	Timezone

5. Add or enable the softphone and desk phones that need to connect to the UC Server through the MBG.

You must configure a **Device ID** on the MBG for each MiNet Directory Number.





**Note:** The Device ID is a network MAC address consisting of 6 hexadecimal numbers separated by colons. It starts with **a1:21:00** and contains the Directory Number within the digits. The **0** (zero) digit is replaced by the letter **a**, the **\*** symbol corresponds to the letter **b** and the **#** corresponds to the letter **c**. For example, a Directory Number of 71\*0#8 would have a Device ID of a1:21:00:71:ba:c8

## Manage Mitel Border Gateway

Status	Configuration	Services	Applications	Clustering
MiNet devices • Device settings by DN • SIP devices • SIP				
» Location: <a href="#">Minet device settings</a> / Create				
Welcome to the MBG administrative interface. From here you can manage all aspects different parts of the system. If at any time you require more information, click the H				
The following is a form for creating a device entry. You may edit this information as y done.				
Device ID:		<input type="text"/>		
Description:		<input type="text"/>		
Enabled:		<input type="checkbox"/>		
Configured ICP:		<input type="text"/>		
G.729 transcoding:		Use master setting ▼		
Set-side codec:		Use master setting ▼		
Local streaming:		Use master setting ▼		
Call recording:		Use master setting ▼		

To add a device:

- Click **Add MiNet Device** to add a device to the MBG. Configure the device as described in the online Help.
- Click **Save**.

## Manage Mitel Border Gateway

StatusConfigurationServicesApplicationsClustering

MiNet devices • Device settings by DN • SIP devices • SIP

» Location: [Minet device settings](#) / Create

Welcome to the MBG administrative interface. From here you can manage all aspects different parts of the system. If at any time you require more information, click the H  
The following is a form for creating a device entry. You may edit this information as y done.

Device ID:

Description:

Enabled: ☐

Configured ICP: ----- ▾

G.729 transcoding: Use master setting ▾

Set-side codec: Use master setting ▾

Local streaming: Use master setting ▾

Call recording: Use master setting ▾

Log Verbosity: Use master setting ▾

To enable a device:

- a. Click the device ID. The device details page appears.
- b. Click **Edit**.
- c. Select the Enabled option and then click **Save**.

*To add or enable SIP devices in the MBG for remote MCD users:*

1. Open a Web browser and navigate to the MSL Server Manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the MBG/Remote Proxy Services are installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. Under Applications, click **Mitel Border Gateway**.
4. Click **Services > SIP Devices**.

The screenshot shows the 'Manage Mitel Border Gateway' web interface. At the top, there are tabs for 'Status', 'Configuration', 'Services' (which is active), 'Applications', and 'Clustering'. Below these are sub-tabs: 'MiNet devices', 'Device settings by DN', 'SIP devices' (selected), 'SIP trunking', and 'Recording status'. The main content area has a heading '» Location: Sip device settings'. Below this is a welcome message and instructions. There are controls for 'Devices per page' (set to 20) and a 'Refresh' button. A 'Filter listing' section includes an input field, 'Apply' and 'Clear' buttons, and a dropdown for 'Canned filters (select)'. A 'Bulk modify' button is also present. At the bottom, there is a link 'Add a SIP device' and a table header for 'Device Information' with columns: 'Enabled', 'Set-side username', 'ICP-side username', 'Device DN(s)', 'Current ICP', and 'Configured ICP'.

5. Add or enable the SIP softphone that need to connect to the UC Server through the MBG. Every unique SIP softphone number used for UC Advanced Mobile and Desktop clients will need to be added to the MBG SIP device services.
6. To add and enable a SIP device:
  - a. Click **Add a SIP Device** to add a device to the MBG. Configure the device as described in the online Help.
  - b. Select the **Enabled** option and then click **Save**.

**Manage Mitel Border Gateway**

Status Configuration **Services** Applications Clustering

• MiNet devices • Device settings by DN • **SIP devices** • SIP trunking •

» Location: [Sip device settings](#) / Create

Welcome to the MBG administrative interface. From here you can manage all aspects of the MBG's behavior. If you require more information, click the Help icon in the upper-right corner of the page.

The following is a form for creating a device entry. You may edit this information as you wish, and click the Save button to create the device.

Set-side username:	<input type="text"/>
Set-side password:	<input type="password"/>
Confirm set-side password:	<input type="password"/>
Icp-side username:	<input type="text"/>
Icp-side password:	<input type="password"/>
Confirm icp-side password:	<input type="password"/>
PRACK support:	Use master setting ▼
Options keepalives:	Use master setting ▼
Heartbeat interval:	<input type="text"/>
Challenge methods:	Use master setting <input type="button" value="Override"/>
Description:	<input type="text"/>
Enabled:	<input type="checkbox"/>
Configured ICP:	----- ▼
Local streaming:	Use master setting ▼

## Mitel 5000/Inter-Tel Axxess PBX Configuration for Remote Users

Remote UC Advanced users connected to a Mitel 5000 or Inter-Tel Axxess PBX access the UC Server through the site's firewall ports. Configure the firewall ports to provide access to the UC Server and the integrated Mitel applications as documented in the *Mitel UC Advanced Engineering Guidelines*.

## Softphone (SIP-based) specific considerations

### *To configure softphone (SIP-based):*

#### 1. Licensing requirements (for Desktop, iOS and Android clients):

For the desktop client, the existing “**Softphone**” license will cover both the Minet softphone and the new SIP-based softphone.

The mobile clients must have the “**Mobile SIP Softphone**” license in order to configure and use the SIP softphone.



**Note:** On the UC Advanced server: you must first select “**UC Advanced Mobile for Smart Devices**” license then select “**Mobile SIP Softphone**”.



**Note:** The **UC Advanced Mobile for Smart Devices** was previously known as the **Locator**.

#### 2. Quality of Service (QoS):

The softphone supports L3 quality of service (QoS) values as per the Table below. These values are used for audio, SIP signaling, and video streaming.

These values are not accessible on the Desktop client but do appear on the Android and iOS clients under Softphone Advanced Settings at their default values.

Service Class	L3 Values
Telephony (Voice)	46 (EF)
Signaling	24 (CS3)
Multimedia Streaming (Video)	34 (CS4)

#### 3. Admin Considerations:

Before a UCA client can use a SIP Softphone, it must be configured on the **PBX, MBG, UCA sever, and UCA client**. For all UCA clients, the softphone will be available for use once UCA is launched and running.

Also see “[High Level Installation and Configuration Procedures](#)” on page 90

#### 4. PBX Considerations:



**Note:** MCD 5.0 SP2 or newer release is required.

5000 running 5.1 or later release is required.

The account code dialing is not supported for SIP softphone on MCD or 5000 PBX.

5000 specific: On the 5000 provisioning system, the admin can create a SIP device and assign it to the user. This is necessary to support the softphone on desktop client and mobile devices.



**Note:** By default, a UCA SIP softphone on a 5000 will only allow one incoming call at a time. To handle multiple incoming calls on the 5000, go to the SIP phone group, On-line monitor, Maximum number of calls, then set to **two**.

MCD specific: To ensure proper functionality, **there are two critical changes that MUST be made on MCD when configuring a UC Advanced SIP Softphone:**

a. First, you must select a Device Type of **UC Endpoint**.

The screenshot shows the 'User and Device Configuration' window for 'App29'. The 'Device Details' tab is active. The 'Device Type' is set to 'UC Endpoint'. The 'Service Profile' section shows 'Number: 29408', 'Hot Desking User: No', 'Service Level: Full', and 'ACD Enabled: No'. The 'User Profile' section shows 'Last Name: L', 'First Name: Denis', 'Role: No Role', 'Language: English', 'Department: ', 'Email: ', 'Location: ', and 'IDS-Manageable: Yes'.

b. Second, you must add at least one additional line. This is accomplished by adding a key with a Line Type of Multicall, a Button Dir. Number matching the number of the device, and Ring Type of Ring.

The screenshot shows the 'Keys' tab in the 'User and Device Configuration' window. A table lists keys with columns: Button Number, Label, Line Type, URL, Button Directory Number, Ring Type, MIXML Application Feature, and Phone Application Feature. A new key is added with Button Number '2', Label '2', Line Type 'Multicall', URL '29408', Button Directory Number '29408', Ring Type 'Ring', MIXML Application Feature 'Not Assigned', and Phone Application Feature 'Not Assigned'.

5. MBG and Teleworker Considerations:

Softphone users outside of the PBX/UCA network will require a connection through an MBG for both data and audio/video real-time streaming.

See “[MBG and Teleworker Considerations:](#)” on page 152,  
 “[MBG and Remote Proxy Services Configuration](#)” on page 104  
 “[Remote User Configuration](#)” on page 141.

## 6. UC Server Considerations:

Under Accounts tab: select **Phone Numbers**, add **SIP Softphone** type, **Number** and **Video Capable** (if supported).



**Note:** Step 5 is only required if the account was not synchronized, i.e. in the event the account(s) was created manually in UCA server for 6.0.

## 7. UC Advanced Client Considerations:

Follow the procedures for the installation, configuration and testing of the UC Advanced Softphone for each client as listed below. For additional assistance on feature, go to each client online Help or <http://edocs.mitel.com/default.htm>

Desktop client - see “[Softphone Configuration - Desktop client](#)” on page 153

Android client - see “[Softphone Configuration - Android client](#)” on page 158

iPad client - see “[Softphone Configuration - iPad client](#)” on page 164

iPhone client - see “[Softphone Configuration - iPhone client](#)” on page 169



**Note:** On the desktop client, in order to use SIP-based video calls, enable the availability for video calls under Dynamic status (Manage Statuses).



**Note:** A new checkbox has been added in the Teleworker settings screen on each client that indicates “Prefer Teleworker Connection”. This flag will alert the client to always attempt to connect the softphone through the TW.



**Note:** Mitel recommends setting up the softphone as a part of a ring group to avoid missing incoming calls due to the following condition:  
 Due to Apple iOS application management, the UCA application for iPhone and iPad may stop running while in the background (consistent with iOS behavior on other iOS Apps). The result is that a UCA application user may be unaware that the UCA application has stopped receiving incoming softphone calls and chat messages.

Participation in a Ring Group will accommodate missed calls but not missed chat messages.

Also see MCD “[Personal Ring Group Assignment Form](#)” on page 93 and 5000 “[Users](#)” on page 97.

## *Migration from Minet Softphone on Desktop Client*

A few scenarios to consider:

- a. **Minet Softphone:** The desktop client will automatically use the Minet softphone when the user has the “Softphone” license, a Minet softphone DN, and no SIP DN.
- b. **SIP Softphone:** The desktop client will use the SIP softphone when the user has the “Softphone” license, a SIP DN, and no Minet softphone DN. Note that in this case, the

user must configure and enable the SIP softphone in the desktop client (i.e., on first startup, the desktop client will not automatically start the SIP softphone).

**Minet or SIP Softphone** (depending on user configuration): When the user has the “Softphone” license, a Minet softphone DN, and a SIP DN, the softphone used by the desktop client depends on whether or not the user has configured the desktop client to use the SIP softphone. On first startup, the desktop client will use the Minet softphone. If the user wants to use the SIP softphone, the user must configure and enable the SIP softphone (note that a restart of the client may be necessary). After the SIP softphone has been configured and enabled, the SIP softphone will automatically be used by the desktop client on subsequent restarts. If the user wants to switch back to the Minet softphone, he must disable the SIP softphone and restart the client.

### *MBG and Teleworker Considerations:*

Softphone users outside of the PBX/UCA network will require a connection through an MBG for both data and audio/video real-time streaming. It is expected that the normal setup for such a configuration involves configuring the fully-qualified domain name (FQDN) of both the PBX and the UCA server to resolve to the IP address of the MBG when outside the corporate network. However, since an FQDN may not be used on the PBX or MBG in all cases, the clients need to support both an internal and external address/hostname for connection.

The clients will always attempt to connect to the local address first and then subsequently try the remote address unless the client is configured to only use the remote address.

The MBG IP/hostname and username/password is configurable at the client level.

The SIP softphone should be configured as a normal SIP teleworker device on the MBG.



**Note:** UC Advanced client profile can have different credentials for Teleworker mode and non-Teleworker mode. It is strongly recommended that the credentials be more secure when connecting to an MBG.



## Softphone Configuration - Desktop client

The following step-by-step procedure will guide you through installing the Unified Communicator Advanced (UCA) software application onto your Desktop device and testing basic softphone call functionality. For the purpose of this exercise, a SIP softphone will be used (softphone definition, see Note 1 page 157).

### Requirements:

- **Wifi** or **Data** connectivity established for your computer.
- **Mitel Unified Communicator Advanced Account Credentials** e-mail from your system administrator (also known as Welcome e-mail).

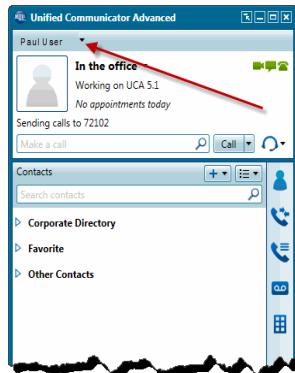
### Installing the UC Advanced client application

1. From your Desktop device, follow the instructions from your Welcome e-mail to download the Desktop Client software. A link has been provided, for example: <https://<your server>/ucs/dl/UnifiedCommunicatorAdvanced.msi>.
2. In the File Download dialog box, click **Run** to launch the client download.
3. In the Security Warning dialog box, click **Run** to launch the client installer. The welcome dialog box appears. Then click **Next** (see Note 2 page 157 if Microsoft.NET Framework is not detected on your computer).
4. Select **I accept the terms of the License Agreement**, and then click **Next**.
5. Select **Typical Install** and then click **Next**.
6. Type the **Fully Qualified Domain Name** for the **Unified Communications Server Hostname** in the box as provided in your Welcome E-mail.
7. Select a Default Language, and then click **Next**. On the next screen, click **Install**.
8. The Desktop Client software is installed on your computer. Click **Finish** to complete the installation process. By default the Desktop Client launches automatically.
9. Next you will be prompted to login.
10. Enter your **Credentials** as per your Welcome e-mail then click Log in:
  - Login ID
  - Password

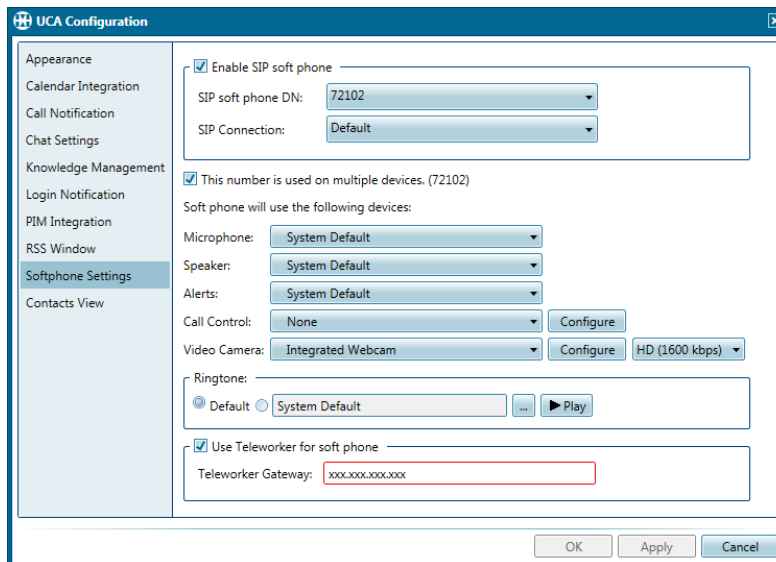
## Enabling your softphone

11. The **Unified Communicator Advanced** main screen will appear.

Go to the **Main Menu** by selecting the drop-down symbol next to the name.



12. Select **Configuration**, and then select **Softphone Settings**.

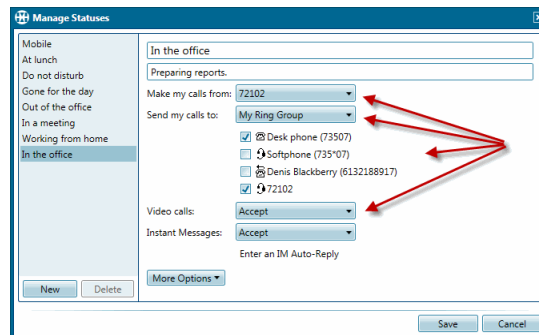


There are several fields to consider that are unique to your particular configuration.

- Click **Enable SIP soft phone**.
- **SIP soft phone DN**: select SIP softphone extension (Directory Number) to use from pull-down menu.
- **SIP Connection** Options: Default, TCP, UDP and TLS. Leave at Default unless advised otherwise by your system administrator.
- **This number is used on multiple devices (xxxxx)** is **OFF** (unchecked) by default. Tap the check box if you plan to use this softphone number on more than just your Desktop. For example if you plan to use this number on another client such as your iPhone, iPad or Android client.
- Other options such as **Microphone**, **Speaker**, **Alerts**, **Call Control** and **Ringtone** can be left at default (or can be modified later).
- **Video Camera**: will only appear if **Enable SIP softphone** is checked. Select one camera device if you plan to use video with your softphone.

- **Use Teleworker for softphone:** enable this option if you plan to use your Desktop client softphone off your corporate network. If enabled, enter the Teleworker Gateway IP address or FQDN as provided by your system administrator. See note 3 [page 157](#).
- Click **OK**.

13. Go to the **Main Menu** and then select **Manage Statuses**.

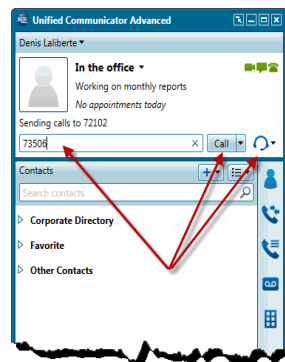


See Note 4 [page 157](#) for more information on these fields.

- From the pull-down menu **Make my calls from**: select your softphone number.
- From the pull-down menu **Send my calls to**: select My Ring Group or leave at default.
- From the pull-down menu **Video calls**: select **Accept** if you plan to use collaboration (Mitel Collaboration Advanced) or your softphone for Video calls.
- Click **Save**.

### Testing your softphone

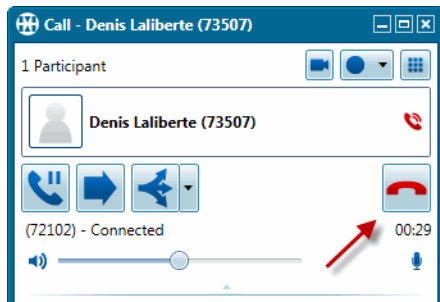
14. From the Home screen.



- Select the softphone from the pull-down menu to originate your call. As a test, enter an extension number and select Call. A Call screen will be displayed for the duration of the call.

15. Answer the call at the far-end.

- Test to ensure that you have 2-way audio and tap **End Call**.



16. Have the far-end call you at your Softphone number, answer the call and test for 2-way audio.

Having problems making or receiving a call, see Note [5 page 157](#).

Tap **End call**.

**You are done!**

**To leverage all the functionality of Unified Communicator Advanced or need Help, press F1 or select Help from the Main Menu or go to <http://edocs.mitel.com/default.htm>**

-----

**Notes:**



1. **SIP softphone definition:** The UC Advanced for Mobile devices (such as iPad, iPhone and Android) use a SIP-based softphone. SIP stands for **Session Initiation Protocol**, which is an industry-wide standard offering a feature-rich experience and new functionality to your Mobile device. The Desktop client can be configured with a Mitel softphone or a SIP-based softphone. **In this exercise, a SIP-based softphone will be used.**



2. If the v4.0 **Microsoft.NET Framework** is not detected on the computer, you are prompted to download and install it. You must restart the Desktop Client installation following the installation of the .NET Framework.




3. **Teleworker definition:** remote or off-premise worker who needs connectivity to the office. Internet connectivity is often accomplished by the use of the public network internet. **If you plan to use your Desktop Client softphone outside of your company's corporate network, you must configure Teleworker Settings.** When the Teleworker Settings are configured and enabled, the softphone will connect and register to the Teleworker server regardless if you are inside or outside your corporate network.  
**Non-Teleworker:** Connecting via VPN from outside is considered being on the corporate LAN. **"Most Desktop users will not be Teleworkers".**



4. **Manage Statuses** (part of Dynamic Status feature) allows you to customize call handling based on your particular UCA status. For example, you may choose to make and receive calls using a certain number while **In the Office** but utilizing a different profile while **Working from Home**. This is just one of the many features of **Unified Communicator Advanced**.



5. Several issues may arise preventing you from making or receiving a call, such as:
  - Lost network connectivity - a message trying to reconnect will appear.
  - Softphone de-activated or registration taken by another device. A notification pop-up will appear near the top of the screen, bring cursor over the notification and click Connect to re-activate your softphone.
  - Dialing a valid number / extension? If dialing an external number, is the prefix (i.e. 8 or 9) for external calls being automatically inserted by your system, try with and without the prefix.
  - Try exiting and re-launching the UCA application (Main Menu, Exit Unified Communicator Advanced), double click on the UCA icon from your desktop.  

  - Still having issues, you may need to contact your system or network administrator for assistance.



## Softphone Configuration - Android client

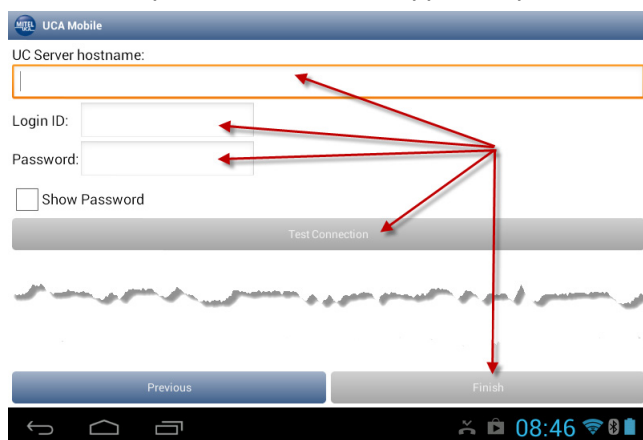
The following step-by-step procedure will guide you through installing the UC Advanced software application onto your Android device and testing basic softphone call functionality (softphone definition [page 162](#)).

### Requirements:

- **Wifi** or **Data** connectivity established for your Android device.
- **Mitel Unified Communicator Advanced Account Credentials** e-mail from your system administrator (also known as Welcome e-mail).



### Installing the UC Advanced client application

1. On your Android, go to <http://market.android.com/apps/> (as per your Welcome e-mail).
2. Enter Mitel UC in the search field, tap , tap **Install**, tap **Accept & download**.
3. The UCA Application will be automatically installed.
4. Once installation is complete, go to your apps and tap **Mitel UCA** icon .
5. The License agreement will be displayed, tap **Agree**.
6. The Setup Wizard screen will appear, tap **Next**.



7. Enter your **Login Credentials** provided as part of your Welcome e-mail:
  - UC Server hostname (Unified Communications Server)
  - Login ID
  - Password
8. Tap **Test Connection** button.
  - Tap **Finish** if **Connection is successful**, be patient and the screen will update automatically.
  - If **Unsuccessful**, see Note [1 page 163](#).

### Enabling your softphone

9. Tap  **Settings** (alternatively use  Menu to access Settings).
  - Tap **Softphone Settings**.
  - Set **Configure Softphone** checkbox (it is unchecked by default).

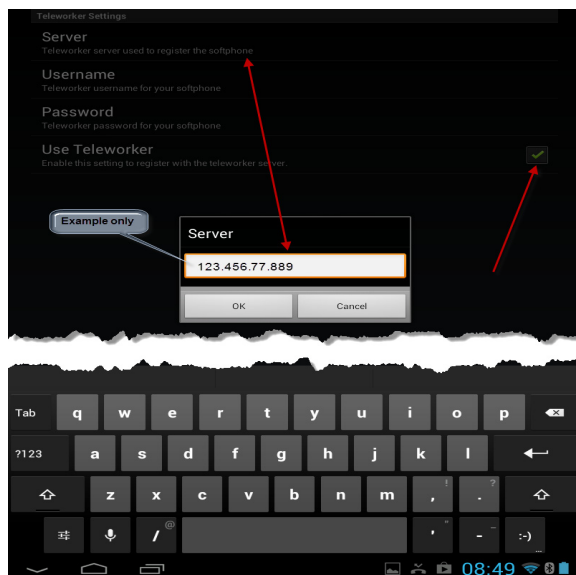


The following fields will appear automatically:

- **Number** (pull down list should have your softphone extension number pre-selected or pick a number if you were given more than one device).
- **Password** (as programmed on the telephone system by your administrator).
- Set **Used on Multiple Devices**, it is unchecked by default. **Check** this box if you plan to use this softphone number on more than just your Android device. For example if you plan to use this number on another client such as your Desktop, iPad or iPhone client.

**10. Tap Teleworker Settings.**

Skip this step if you are not a **Teleworker**, see Note 2 page 163.



There are three fields to enter. This information should have been provided to you by your system administrator.

- **Server:** tap on server to enter the IP address (do not enter leading zeros in the IP address, for example 074.xxx.xxx.yyy must be entered as 74.xxx.xxx.yyy)
- **Username** (as provided by your system administrator)
- **Password** (as provided by your system administrator)
- Set **Use Teleworker** checkbox. See Note 2 page 163 for more information.

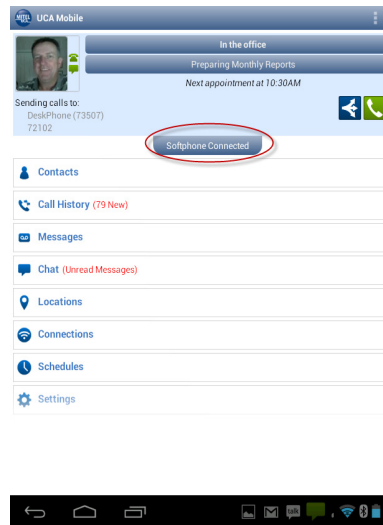
**11. Tap back arrow to return to Softphone Settings.**

Tap **Advanced Settings**. Advanced Settings should be left at default unless instructed otherwise by your system administrator. The **WiFi Only** flag is checked by default. Therefore, the softphone will only be connected when the device is connected to a WiFi network.

- 12.** On the UCA Home screen you will notice a grey rectangle that reads **Softphone Off**. Tap on the rectangle to reveal a switch and then tap to the “on” position. If all credentials and connectivity are properly set, the Android client will automatically register and connect to the server. As per the example below, the display will show **Softphone Connected**. You are now ready to test your softphone.



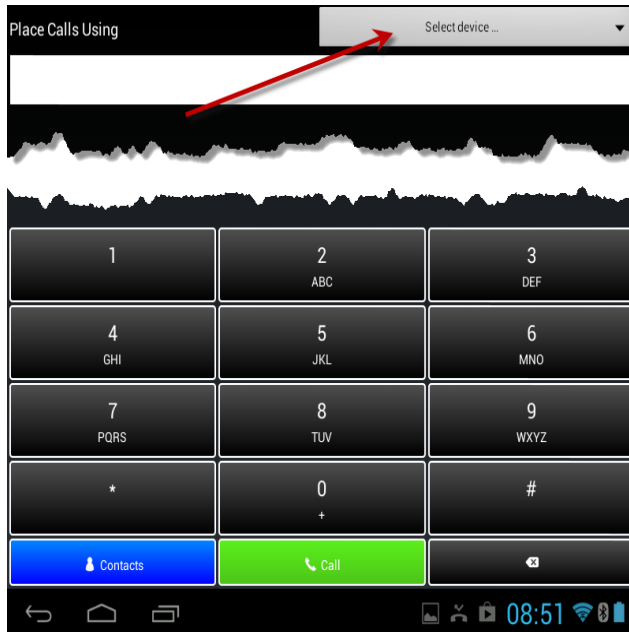
Not connecting or other possible statuses, see [Note 3 page 163](#).



### Testing your softphone

13. Tap the **Call** button , a dialpad screen will appear.

14. **Select a Device** (pull-down menu) to make the call. Select your **softphone number** then dial a number, then tap **Call**.



- Need more information on **Selecting device to place call**, see **Place Call Using** option Note 4 page 163.

15. The dialpad screen will automatically switch to a call screen offering several options depending on your configuration. Answer the call at the far-end.

16. Test to ensure that you have 2-way audio and tap **End Call**.

17. Have the far-end call you at the Softphone number and test for 2-way audio, then tap **End call**.

### You are done!

Go to UCA Help or go to <http://edocs.mitel.com/default.htm> to leverage all the functionality of Unified Communicator Advanced.

To access UCA Help or Exiting UCA on the Android, go to more options as per diagram below:



**SIP definition:** The UC Advanced for Mobile devices (such as iPad, iPhone and Android) use a SIP-based softphone. SIP stands for Session Initiation Protocol, which is an industry-wide standard offering a feature-rich experience and new functionality to your Mobile device.

**Notes:**

1. If Test Connection is **unsuccessful**, possible errors are:  
“**UC Server login failure**”. Possible cause: incorrect Login ID or Password  
“**Unable to connect to IP address**”. Possible cause: invalid UC Server Hostname.  
Try re-entering your credentials. If still unsuccessful, you probably have a network, system or server issue. Contact your system administrator for further assistance.



2. **Teleworker definition:** remote or off-premise worker who needs connectivity to the office. Internet connectivity is often accomplished by the use of the public network internet. **If you plan to use the softphone outside of your company's corporate network, you must configure Teleworker Settings.** When the Teleworker Settings are configured and enabled, the softphone will connect and register to the Teleworker server regardless if you are inside or outside your corporate network.”  
**Most Android users will be Teleworkers.**  
**Non-Teleworker:** Skip [step 8](#) if you are connected to your company's network at all times and do not plan to use this device off premises.



3. The Softphone may show different statuses such as **Connected, Off, No WiFi, Disconnected, Timeout, Unauthorized, No Service or Failure**. You can tap the **Softphone** button at anytime to reveal the switch and manually turn the Softphone “**ON**” or “**OFF**”. This can be useful in troubleshooting or re-enabling the softphone after making a network change. Contact your system administrator if unable to connect after several attempts.



4. **Place Call Using** option can be modified by tapping **Settings** followed by **Call Settings**. By default, **Prompt** will be selected. In other words, you will be prompted to choose a device every time you place a call. You have the option to select which device to use when making a call thus eliminating the prompting step.


### Softphone Configuration - iPad client

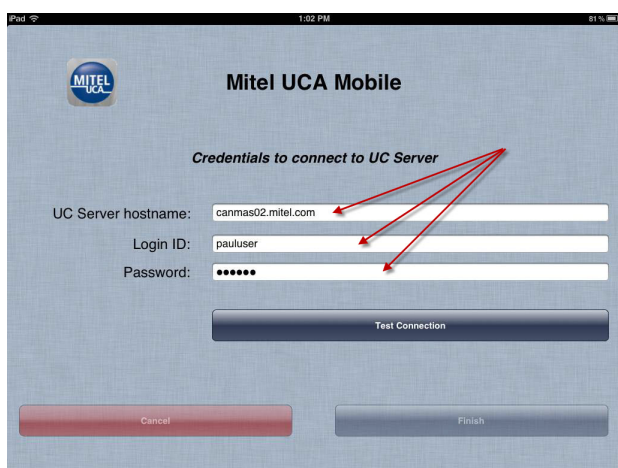
The following step-by-step procedure will guide you through installing the UC Advanced software application onto your iPad device and testing basic softphone call functionality (softphone definition [page 167](#)).

#### Requirements:

- **Wifi** or **Data** connectivity established for your iPad device.
- **Mitel Unified Communicator Advanced Account Credentials** e-mail from your system administrator (also known as Welcome e-mail).

#### Installing the UC Advanced client application

1. On your iPad, go to the App Store and enter **Mitel UCA** in the Search field.
2. Under iPad Apps, tap **INSTALL**. Enter your **Apple ID** when prompted.
3. The **Mitel UCA** Application will be automatically installed.
4. Once the installation is complete, tap **Mitel UCA** icon 

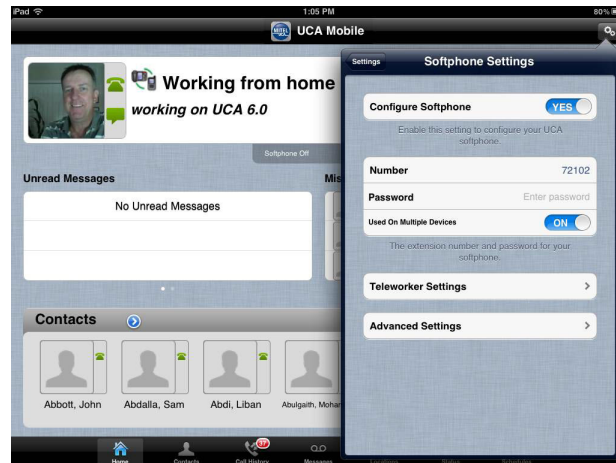


5. Enter your **Credentials to connect to UC Server** as per your Welcome e-mail:
  - UC Server hostname (Unified Communications Server)
  - Login ID
  - Password
6. Tap **Test Connection** button.
  - If **Test Connection** is **successful**, tap **Finish**.  
If **Unsuccessful**, see Note 1 [page 168](#).
  - The **End User License Agreement** (EULA) will be displayed, tap **Accept**.
  - Be patient, the screen will update automatically.

## Enabling your softphone

### 7. Tap **Settings**

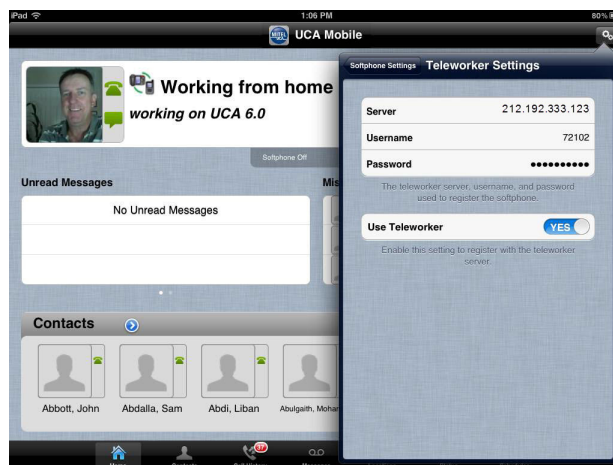
- Tap **Softphone Settings**.
- Set **Configure Softphone** to **YES**.



- The following fields will appear automatically and should be pre-filled:
  - **Number** (will either display your softphone extension number or **Pick a number** if you were given more than one device).
  - **Password** (as programmed on the telephone system by your administrator including an empty or blank password).
  - **Used on Multiple Devices** is **OFF** by default. Tap to the **ON** position if you plan to use this softphone number on more than just your iPad. For example if you plan to use this number on another client such as your Desktop, iPhone or Android client.

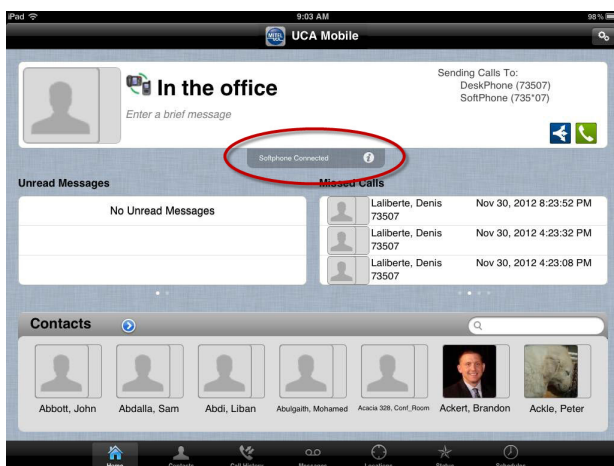
### 8. Tap **Teleworker Settings**.

Skip this step if you are not a **Teleworker**, see Note 2 page 168.




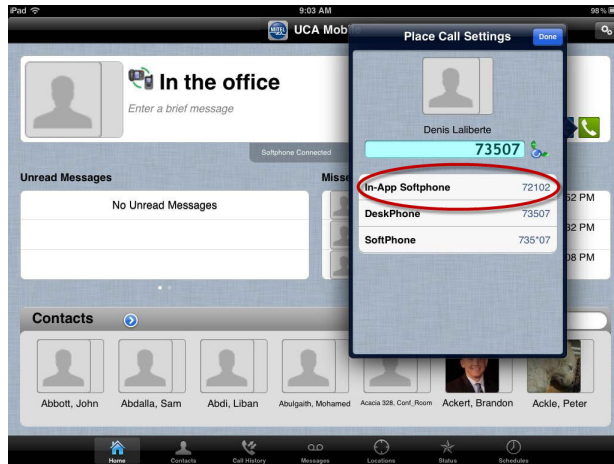
There are three fields to complete. This information should have been provided to you by your system administrator.

- **Server:** enter the IP address (do not enter leading zeros in the IP address, for example 074.xxx.xxx.yyy must be entered as 74.xxx.xxx.yyy)
  - **Username** (as provided by your system administrator)
  - **Password** (as provided by your system administrator)
  - Set **Use Teleworker** to **YES**. See Note 2 page 168 for more information.
9. **Advanced Settings** options should be left at default unless instructed otherwise by your system administrator. The **WiFi Only** flag is ON by default. Therefore, the softphone will only be connected when the device is connected to a WiFi network.
10. Tap **Home** (bottom left of your screen).
11. On the UCA Home screen you will notice a grey rectangle that reads **Softphone Off** followed by the letter “i” (Info button). If you tap the “i” the rectangle will flip to an “on-off” switch. Tap to the “on” position. If all credentials and connectivity are properly set, the iPad client will automatically register and connect to the server. As per the example below, the display will show **Softphone Connected**. You are now ready to test your softphone. Not connecting or other possible statuses, see Note 3 page 168.




*Testing your softphone*

12. Tap the **Call** button  , a dialpad screen will appear, dial an extension number, then tap **Call**.



13. Tap **In-App Softphone**. Need more information about **Place Call Settings** option, see Note 4 page 168.
14. The dialpad screen will automatically switch to a call screen. Answer the call at the far-end.  
See Notes 3 and 5 page 168 in the event of a call failure or audio quality issues.
15. Test to ensure that you have 2-way audio and tap **End Call**.
16. Have the far-end call you at your Softphone number and test for 2-way audio, then tap **End call**. You are done!

Go to UCA Help under Settings  or go to <http://edocs.mitel.com/default.htm> to leverage all the functionality of Unified Communicator Advanced.

**SIP definition:** The UC Advanced for Mobile devices (such as iPad, iPhone and Android) use a SIP-based softphone. SIP stands for Session Initiation Protocol, which is an industry-wide standard offering a feature-rich experience and new functionality to your Mobile device.

**Notes:**

1. If Test Connection is **unsuccessful**, possible errors are:  
**“UC Server login failure”**. Possible cause: incorrect Login ID or Password  
**“Unable to connect to IP address”**. Possible cause: invalid UC Server Hostname.  
 Try re-entering your credentials. If still unsuccessful, you probably have a network, system or server issue. Contact your system administrator for further assistance.



2. **Teleworker definition:** remote or off-premise worker who needs connectivity to the office. Internet connectivity is often accomplished by the use of the public network internet. **If you plan to use the softphone outside of your company's corporate network, you must configure Teleworker Settings.** When the Teleworker Settings are configured and enabled, the softphone will connect and register to the Teleworker server regardless if you are inside or outside your corporate network.”  
**Most iPad users will be Teleworkers.**  
**Non-Teleworker:** Skip [step 8](#) if you are connected to your company's network at all times and do not plan to use this device off premises.



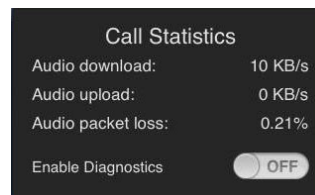
3. The Softphone may show different statuses such as **Connected, Connecting, Off, On or Time-out**. You can tap the “i” (Info button) at anytime to reveal the switch and manually turn the Softphone “**ON**” or “**OFF**”. This can be useful in troubleshooting or re-enabling the softphone after making a network change. Contact your system administrator if unable to connect after several attempts.



4. **Place Call Settings** option can be modified by tapping **Settings** followed by **Call Settings**. By default, **Prompt** will be selected. In other words, you will be prompted to choose a device every time you place a call. You have the option to select which device to use when making a call thus eliminating the prompting step.



5. **If you are experiencing audio quality issues.** You can send **Call diagnostics** by selecting the icon on the active call view (see example below). Set **Enable diagnostics** to **ON** will capture and send diagnostics via e-mail upon call termination (see example below).





## Softphone Configuration - iPhone client

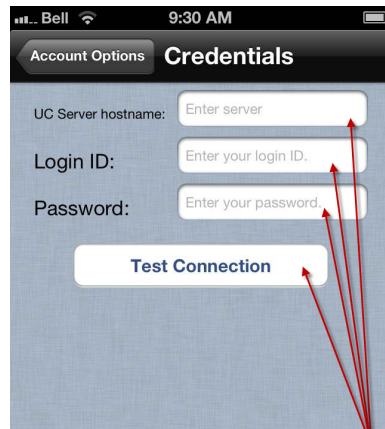
The following step-by-step procedure will guide you through installing the UC Advanced software application onto your iPhone device and testing basic softphone call functionality (softphone definition [page 172](#)).

### Requirements:

- **Wifi** or **Data** connectivity established for your iPhone device.
- **Mitel Unified Communicator Advanced Account Credentials** e-mail from your system administrator (also known as Welcome e-mail).


### Installing the UC Advanced client application

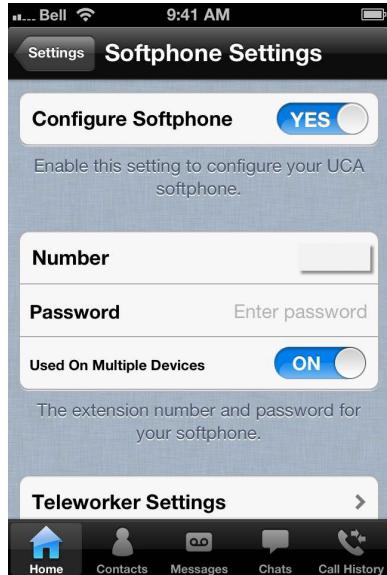
1. On your iPhone, go to the App Store and enter **Mitel UCA** in the Search field.
2. Tap **INSTALL**. Enter your **Apple ID** when prompted.
3. The **Mitel UCA** Application will be automatically installed.
4. Once installation is complete, tap **OPEN**. The **End User License Agreement** (EULA) will be displayed, tap **Accept**.
5. The Setup Wizard screen will appear, tap **Next**.



6. Enter your **Credentials** as per your Welcome e-mail:
  - UC Server hostname (Unified Communications Server)
  - Login ID
  - Password
7. Tap **Test Connection** button.
  - If **Test Connection is successful**, be patient and the screen will update automatically. If **Unsuccessful**, see Note 1 [page 173](#).

### Enabling your softphone

8. Once UCA mobile home screen appears, tap  **Settings**.
9. Tap **Softphone Settings**.
  - Set **Configure Softphone** to **YES**.



The following fields will appear automatically:

- **Number** (will either display your softphone extension number or **Select a number** if you were given more than one number).
- **Password** (as programmed on the telephone system by your administrator including an empty or blank password).
- **Used on Multiple Devices** is **OFF** by default. Tap to the **ON** position if you plan to use this softphone number on more than just your iPhone. For example if you plan to use this number on another client such as your Desktop, iPad or Android client.

10. Tap **Teleworker Settings**.

Skip this step if you are not a **Teleworker**, see Note [2](#) page [173](#).



There are three fields to complete. This information should have been provided to you by your system administrator.

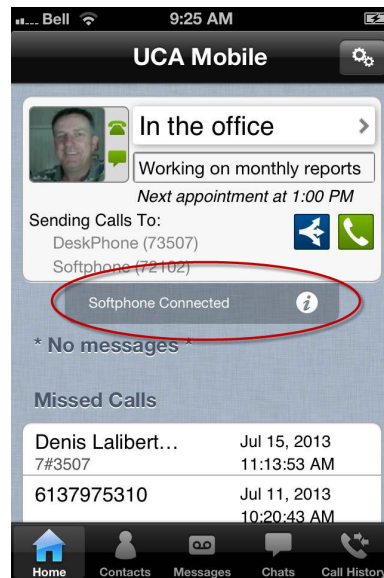
- **Server:** enter the IP address (do not enter leading zeros in the IP address, for example 074.xxx.xxx.yyy must be entered as 74.xxx.xxx.yyy)
- **Username** (as provided by your system administrator)
- **Password** (as provided by your system administrator)
- Set **Use Teleworker** to **YES**. See Note [2 page 173](#) for more information.

**11. Advanced Settings** option will be revealed by scrolling down.

**Advanced Settings** should be left at default unless instructed otherwise by your system administrator. The **WiFi Only** flag is **ON** by default. Therefore, the softphone will only be connected when the device is connected to a WiFi network.

**12. Tap Home** (bottom left of your screen).

**13.** On the UCA Home screen you will notice a grey rectangle that reads **Softphone Off** followed by the letter “i” (Info button). If you tap the “i” the rectangle will flip to an “on-off” switch. Tap to the “on” position. If all credentials and connectivity are properly set, the iPhone client will automatically register and connect to the server. As per the example below, the display will show **Softphone Connected**. You are now ready to test your softphone. Not connecting or other possible statuses, see Note [3 page 173](#).



### Testing your softphone

14. Tap the Call button.

A dialpad screen will appear as well as **Place Calls Using: Select device**, tap on drop-down list (top left corner), tap (xxxxx) your softphone number. Need more information about **Place Calls Using** option, see Note 4 page 173.



15. As a test, dial an extension number, then tap **Call**.

16. The dialpad screen will automatically switch to a call screen. Answer the call at the far-end.

See Notes 3 and 5 page 173 in the event of a call failure or audio quality issues.

17. Test to ensure that you have 2-way audio and tap **End Call**.

18. Have the far-end call you at the Softphone number and test for 2-way audio, then tap **End call. You are done!**

**Go to UCA Help (tap More then Settings) or go to <http://edocs.mitel.com/default.htm> to leverage all the functionality of Unified Communicator Advanced.**

**SIP softphone definition:** The UC Advanced for Mobile devices (such as iPad, iPhone and Android) use a SIP-based softphone. SIP stands for Session Initiation Protocol, which is an industry-wide standard offering a feature-rich experience and new functionality to your Mobile device.

**Notes:**



1. If Test Connection is **unsuccessful**, possible errors are:  
 “UC Server login failure”. Possible cause: incorrect Login ID or Password  
 “Unable to connect to IP address”. Possible cause: invalid UC Server Hostname.  
 Try re-entering your credentials. If still unsuccessful, you probably have a network, system or server issue. Contact your system administrator for further assistance.



2. **Teleworker definition:** remote or off-premise worker who needs connectivity to the office. Internet connectivity is often accomplished by the use of the public network internet. **If you plan to use the softphone outside of your company's corporate network, you must configure Teleworker Settings.** When the Teleworker Settings are configured and enabled, the softphone will connect and register to the Teleworker server regardless if you are inside or outside your corporate network.”  
**Most iPhone users will be Teleworkers.**  
**Non-Teleworker:** Skip [step 10](#) if you are connected to your company's network at all times and do not plan to use this device off premises.



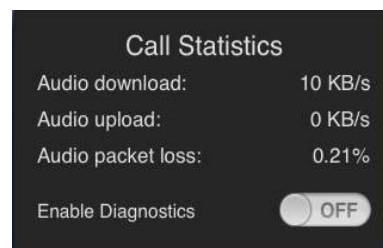
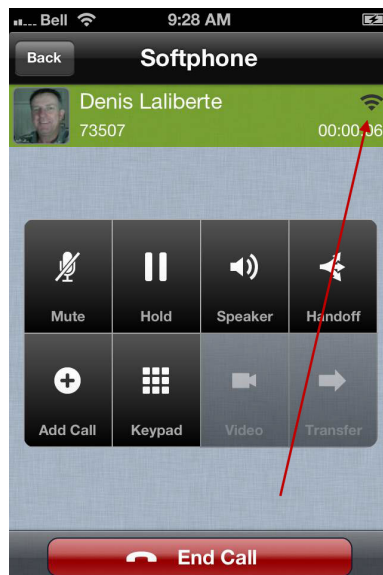
3. The Softphone may show different statuses such as **Connected, Connecting, Off, On** or **Time-out**. You can tap the “i” (Info button) at anytime to reveal the switch and manually turn the Softphone “**ON**” or “**OFF**”. This can be useful in troubleshooting or re-enabling the softphone after making a network change. Contact your system administrator if unable to connect after several attempts.



4. **Place call using** option can be modified by tapping **More** followed by **Call Settings**. By default, **Prompt** will be selected. In other words, you will be prompted to choose a device every time you place a call. You have the option to select which device to use when making a call thus eliminating the prompting step.



5. **If you are experiencing audio quality issues.** You can send **Call diagnostics** by selecting the icon on the active call view (see example below). Set **Enable diagnostics** to **ON** will capture and send diagnostics via e-mail upon call termination (see example below).



## Teamwork Mode

To support Teamwork Mode functionality, accounts that do not have a desk phone or a softphone will by default operate in Teamwork Mode. See [“Teamwork Mode” on page 69](#).



**Note:** Prior to UC Advanced 5.1, a UCA user was required to have either a desk phone or a softphone. This requirement would in turn force a UCA account to be associated with a PBX node, this is no longer the case in UCA 5.1.

### Server Admin portal impacts and considerations

In order to support Teamwork Mode, it is possible to have a group of user accounts with no real PBX nodes. By the same token, it is possible to have some accounts operate in Teamwork Mode (without a desk phone or softphone) while other users operate in a traditional mode with either a desk phone, softphone, or both assigned.

The following UC Server areas are impacted to support Teamwork Mode:

#### *Enterprise Tab*

There are no specific actions required on the Enterprise Tab for Teamwork Mode. However, note that the “Switch type” field is still mandatory. When creating a new enterprise that will not have any PBX nodes and only have Teamwork Mode accounts, the switch type can be left at the default value of “Mitel Communications Director” (the value will be ignored). Otherwise, choose the switch type of your enterprise as usual.

#### *Account Tab*

The Account tab displays a PBX Node column for every account. If a user is not assigned to a PBX node or PBX Node is [None] (i.e. the user does not have a desk phone or a softphone), this column will be blank. **Therefore, any account with a PBX Node column blank is considered to be in Teamwork Mode.**

A Teamwork Mode account that has a PBX Node value of [None] can be later moved to a real PBX node if they get assigned a phone on that PBX. However, an account that is assigned to a real PBX node cannot be moved back to Teamwork Mode.



**Note:** When adding an account manually the PBX node must be set to 'None' for account to be in teamwork mode.

When using Active directory sync (see [Synchronization](#) for more information), the PBX node value in active directory should be set to **<enterpriseld>.local** and no desk phone or softphone number must be assigned to the user account in active directory.

#### *Account Details Page*

To add a user in Teamwork Mode, in creating an account leave the “PBX node” field set to [None]. See [“Synchronization”](#) for more information.



**Note:** Prior to UCA 5.1, the admin was required to select a PBX node when creating an account. If there were no PBX nodes, the admin could not create accounts.

## Features

There are no specific features related to Teamwork Mode. You can select any feature for a Teamwork Mode account, however any phone or call control related features (such as Desk phone or Softphone) will be ignored. Also note that licenses for individual features such as Chat, Visual Voicemail, etc... are still required.

## Synchronization

UC Advanced Teamwork Mode accounts (i.e. those accounts with no desk phone or softphone) can be created manually in Server Admin portal or via AD/LDAP synchronization as explained below:

### ☐ **Server Admin portal Teamwork Mode account creation:**

1. From Accounts tab, select **Add Account**.
2. In the new Account Details page, select **[None]** for the PBX Node field.
3. Fill out other fields as you would normally fill them out (if they are available).
4. Select **Create** to create a new Account.
5. On the newly created Account Details page, fill out any other available information if necessary, such as Contact Information or Account Settings.



**Note:** You should not add any numbers under Phone Numbers since Teamwork Mode accounts shouldn't have a desk phone or softphone and cannot do call control.

6. Select **Save** when finished.

### ☐ **AD/LDAP Synchronization Teamwork Mode account creation:**

1. Fill out all fields as you would for a regular account except for the following:
  - Set PBX node value to **<enterpriseld>.local**, where <enterpriseld> is the ID of the enterprise being created and can be found on **Enterprise Tab**.
  - Do not fill out fields for desk phone and softphone.
2. Perform AD/LDAP synchronization as usual. Newly created Teamwork Mode account should show **[None]** for PBX Node and no desk phone and softphone numbers on that account's Account Details page.

## Default Account Statuses

The first time a user logs into a UCA client, the UC server creates the following list of default set of Dynamic Statuses for a Teamwork Mode user:

- In the office
- Do not disturb
- Gone for the day.

## Google Calendar Integration

UC Advanced provides users with the option to integrate with Google calendar.

### *Licensing*

This feature is available by default and no specific UC Advanced license is necessary.

### *Admin Portal*

UC Advanced can support connection to **one Google** enterprise domain. At the enterprise level, the Administrator must select between Exchange Integration and Google Calendar Integration. This selection is accomplished by selecting Calendar Integration option under the Enterprise Tab on the Admin Portal. In addition, the Advanced Calendar Integration Settings can also be found at this same location.



**Note:** UCA 6.0 release has support for Google calendar integration. If UCA 5.1 mobile clients try to connect to a UCA 6.0 server which has Google calendar integration enabled, then the calendar integration feature will not be configurable from the clients. The calendar integration configuration screen on the clients may display a message to this effect: "Calendar integration is not enabled on the server". To make use of Google calendar integration, the clients need to be upgraded to UCA 6.0 or later software.

## Authentication and access to Google Calendar

To provide the calendar integration feature, UCA server will access Google calendars belonging to a specific Google Apps domain. UCA uses OAuth 2.0 to access Google calendars. One of the strengths of OAuth is that UCA does not need to know your Google Account credentials, and you can grant and revoke access permissions to UCA at anytime. UCA administrator should setup this access as described below.



**Note:** Calendars with no sharing (Google users can control sharing on their individual calendars) will not publish free/busy information and hence their calendar availability information cannot be accessed by UCA. UCA administrators should ensure that users who want to make use of the Calendar Integration feature have shared their calendars.



**Note:** The following sequence of steps will grant UCA server the permission to access free/busy information from calendars belonging to the enterprise's Google Apps domain (subject to sharing constraints as described above). This access privilege can be revoked at anytime (this feature will stop working if privileges are revoked) by logging into Google at:  
<https://accounts.google.com/b/0/IssuedAuthSubTokens>  
For more information, please refer to:  
<https://developers.google.com/accounts/docs/OAuth2WebServer#tokenrevoke>

The process for granting Google calendar access to applications is described in <https://developers.google.com/accounts/docs/OAuth2ForDevices>. Below are the sequence of



steps that need to be performed by the UCA administrator. For the latest information, please refer to the google URL for OAuth2ForDevices (stated above).

### 1. Login to Google console

From a browser, navigate to <https://code.google.com/apis/console#access> and login using your Google Apps credentials.

You can login as the Google Apps domain SuperAdmin or as a Google Apps domain user. Each of these can affect how much information UCA can access from Google calendars:

- Login as SuperAdmin – This will allow UCA to access calendar free/busy information even when individual users have not shared their calendars.
- Login as a user – This will allow UCA to access calendar free/busy information for all the calendars that have been shared at least within your Google Apps domain.



**Note:** In either of the above cases, UCA will only present the calendar free/busy information (the start and end times of events). Other details (such as Event subject, content, participant list, etc.) will not be visible to UCA users even if UCA is able to access such information from Google calendar.

### 2. Register UCA as a Google application

Once you are logged in, click on “Create Project”. If you hadn’t registered any applications before, you will see a splash screen as shown below with a “CreateProject” link:

**Start using the Google APIs console**  
to manage your API usage

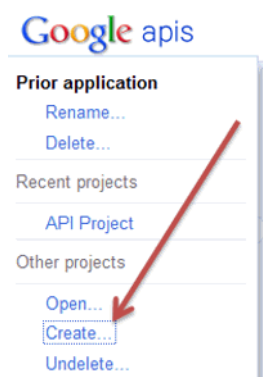


Creating an **APIs** project will let you:

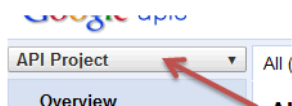
- Use Google APIs **beyond anonymous limits**.
- Monitor API usage and control API access.
- Share API management with a team.

**Create project...**

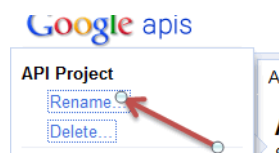
If you have other applications associated with your Google account, then go to the left-hand menu, click on your prior application name, and then select “Create”.



Google now creates a new application project named “API project”.



If you wish to rename this to something relevant, click on the “API Project” link from the left-hand menu and select “Rename”, then enter a new name and save.



### 3. Enable Google Calendar API access

From the Services menu, if the Calendar API Status shows as OFF, then click the OFF button and toggle it to ON position:

The screenshot shows the Google Cloud Platform 'All services' page. The left sidebar has a menu with 'Overview', 'Services', 'Team', and 'API Access'. The 'Services' menu item is highlighted with a red arrow. The main content area shows a list of services with their status. The 'Calendar API' is highlighted with a red arrow pointing to its 'OFF' status toggle.

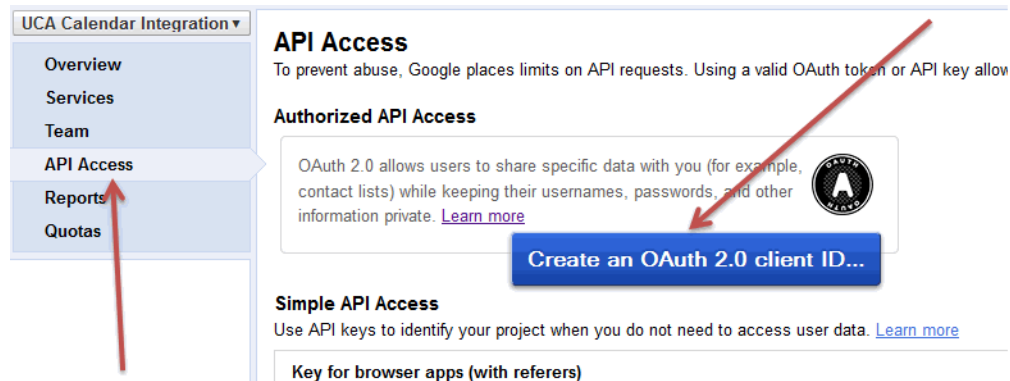
Service	Status	Notes
Ad Exchange Buyer API	OFF	Courtesy limit: 1,000 queries/day
AdSense Host API	<a href="#">Request access...</a>	Courtesy limit: 100,000 queries/day
AdSense Management API	OFF	Courtesy limit: 10,000 queries/day
Analytics API	OFF	Courtesy limit: 50,000 queries/day
Audit API	OFF	Courtesy limit: 10,000 queries/day
Blogger API	<a href="#">Request access...</a>	Courtesy limit: 1,000 queries/day
Books API	OFF	Courtesy limit: 1,000 queries/day
Calendar API	OFF	Courtesy limit: 10,000 queries/day
Custom Search API	OFF	<a href="#">Pricing</a> • Courtesy limit: 100 queries/d
Freebase API	OFF	Courtesy limit: 100,000 queries/day

Google will present some agreements. Please read them and accept. After acceptance, Google Calendar API is enabled for use by applications registered with your Google account.

#### 4. Create a Client ID

Once you successfully registered UCA as a Google application and enabled Calendar API, it is time to create **client\_id** and **client\_secret**. These pieces of information are required by Google to track the number of calendar access requests made on behalf of your Google Apps domain, and to throttle/limit the requests and protect the Google Apps infrastructure from overload.

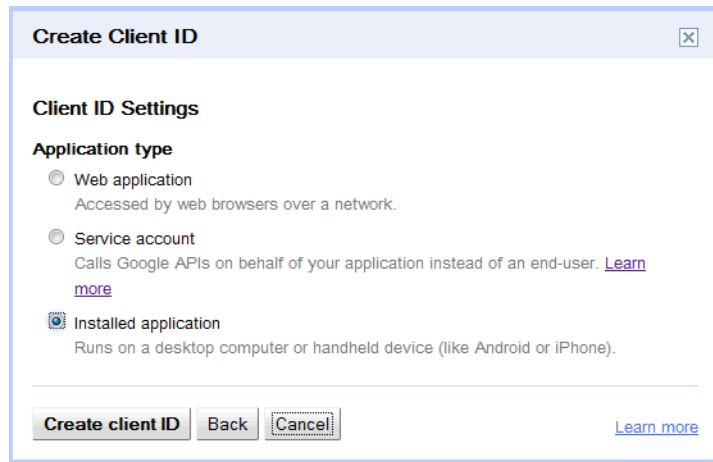
From the left-hand menu, select “API Access” and click on “Create an OAuth 2.0 client ID”.



You will see a form to fill in some information. For branding information, provide a name and the logo can be ignored or supplied as per your preference. Since end users will not use UCA calendar integration directly as a web application, the Product Name and Logo supplied here will not be visible to users. Click Next.

A screenshot of the 'Create Client ID' form. The 'Branding Information' section is visible, with the following fields: 'Product name' (UCA Calendar Integration), 'Google account' (example@test12.com - you), and 'Product logo' (a placeholder box). There is an 'Update' button next to the logo field. At the bottom, there are 'Next' and 'Cancel' buttons, and a 'Learn more' link.

Select the “Installed application” option and click on “Create Client ID”:



**Create Client ID**

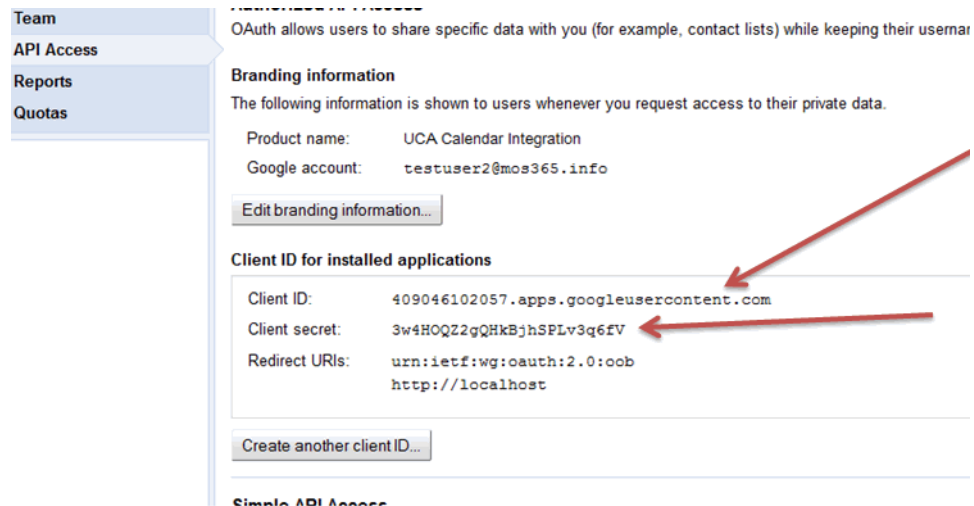
**Client ID Settings**

**Application type**

- ☐ Web application  
Accessed by web browsers over a network.
- ☐ Service account  
Calls Google APIs on behalf of your application instead of an end-user. [Learn more](#)
- ☒ Installed application  
Runs on a desktop computer or handheld device (like Android or iPhone).

**Create client ID** **Back** **Cancel** [Learn more](#)

Now, Google will create Client ID and Client secret, which should be visible in the “API Access” tab:



**Team**  
**API Access**  
**Reports**  
**Quotas**

OAuth allows users to share specific data with you (for example, contact lists) while keeping their usermar

**Branding information**  
The following information is shown to users whenever you request access to their private data.

Product name: UCA Calendar Integration  
Google account: testuser2@mos365.info

[Edit branding information...](#)

**Client ID for installed applications**

Client ID: 409046102057.apps.googleusercontent.com  
Client secret: 3w4HQZ22gQHkBJhSPLv3q6fV  
Redirect URIs: urn:ietf:wg:oauth:2.0:oob  
http://localhost

[Create another client ID...](#)

**Simple API Access**

### 5. Provide Client ID and Client secret to MSL

Copy-paste the Client ID and Client secret from the previous step into the fields on MSL server-manager (Login to server-manager -> Google Apps -> OAuth 2 Config. On that page you will see fields to accept client ID and client Secret. The product name can be left blank) as shown below:

The screenshot shows the Google OAuth 2.0 configuration page. At the top, there is a warning: "Applications relying upon this token will not be able to access Google APIs until you have added the user authorization process below." Below this, there are three input fields: "Product Name" (empty), "Client ID" (containing "1961741482714.apps.googleusercontent.com"), and "Client Secret" (containing "TGA8YsbqufoJAGKmbdAKI2d8"). A "Save and Generate Authorization Code" button is located at the bottom right. Two red arrows are overlaid on the image: one pointing to the "Client ID" field and another pointing to the "Client Secret" field.

Click on "Save and Generate Authorization Code" button, MSL will now communicate with Google to obtain consent URI. If the information you entered was incorrect (for example, due to some error in copy-pasting), the MSL page will display a brief error message. If this happens, make sure to copy the information from Google console correctly and try again.

## 6. Enter Code, Login to Google and provide access to UCA

If the client ID and client Secret were valid, MSL communicates with Google and obtains an authorization code (displayed in bold), and a link to Google, as shown below:

### Step 3: Provide the Authorization Code to Google

Access tokens cannot be granted until you click on the link below and enter the authorization code displayed in bold. Google may ask you to log into the admin account for your site. By entering the displayed code when queried for it you will be authorizing applications on this server access using OAuth 2.0 to a set of Google APIs that you selected in Step 1.

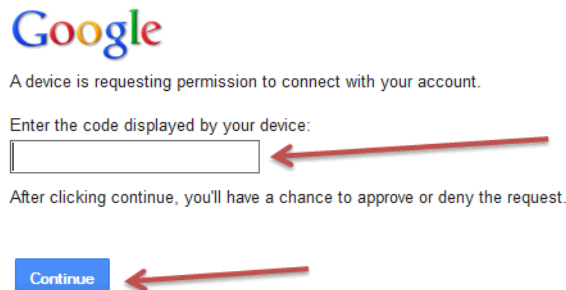
Here is your authorization code: **ijt9ammz**

This code is valid until: Mon Nov 12 10:53:42 2012

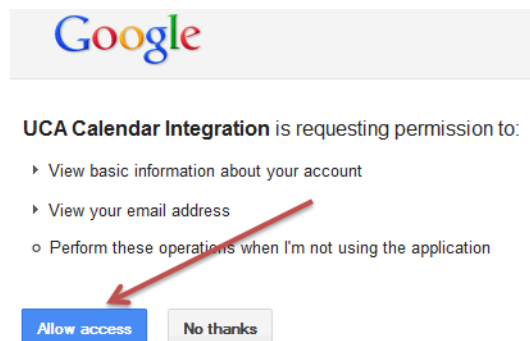
Please click on the following link and enter the above code when requested.

<http://www.google.com/device>

Copy the authorization code, browse to the URL displayed. If prompted by Google, login to your Google account (use the same Google account with which the client\_id was generated). The newly loaded web page will look similar to the one below. Copy-paste the code shown in the server-manager into the field and click Continue.



You will now be presented with a form to allow UCA to access your Google calendar. Click on "Allow Access".



Once you allow access, within a minute or so, MSL will poll Google and obtain OAuth2 access token. Once this operation is successfully completed, you may logout of your Google account and return to UCA server-manager.

When these steps are complete, to verify whether UCA has access to the tokens, go to Server-Manager -> Unified Communications Server -> Perform Server Diagnostics ->

Calstatus. At the bottom of that page, UCA lists the recent OAuth2 events that it received. See screenshot below for an example:

```

o 2012-11-12 10:29:13: Token: <null> Additional Info: ErrorCode: <authorization_pending> Additional Info: Missing props in OAuth2 keys: accessToken, validUntil,
o 2012-11-12 10:29:34: Token: <null> Additional Info: ErrorCode: <authorization_pending> Additional Info: Missing props in OAuth2 keys: accessToken, validUntil,
o 2012-11-12 10:29:54: Token: <null> Additional Info: ErrorCode: <authorization_pending> Additional Info: Missing props in OAuth2 keys: accessToken, validUntil,
o 2012-11-12 10:30:15: Token: <null> Additional Info: ErrorCode: <authorization_pending> Additional Info: Missing props in OAuth2 keys: accessToken, validUntil,
o 2012-11-12 10:30:38: Token: <Bearer ya29.AHES6ZTwRfoYHhF9_W5qoDsylaU1oRNaZAgKraXrvylxbsa8bUD9gA> Valid Until 2012-11-12 11:30:38 ErrorCode: <>

```

As can be seen from the screenshot, the first few OAuth2 notifications to UCA didn't contain all the information (because we were still in the process of setting up OAuth2 configuration). The last update shows the bearer token and no error. This means that UCA received the OAuth2 token and is now ready to access Google calendars using that token.

To enable Google **Calendar Integration** on the server:

1. select the desired enterprise
2. under Calendar Integration, select **Google** from drop down Calendar Type list
3. click the **Enable calendar integration** checkbox
4. click **Test Connection**.

« Calendar Integration

Calendar Type:

☒ Enable calendar integration

[\[Advanced Calendar Integration Settings\]](#)

Connection successful. Click Apply to save the calendar integration settings.

Once the connection is successful, apply changes and save the enterprise details. Now the UCA users in that enterprise can enable Google calendar integration by providing their calendar ID from their respective UCA clients.

## Changes to Clients

### Google Calendar setting

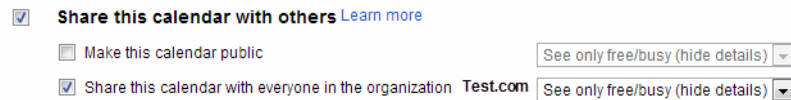


**Note:** Google calendar has some options to control which events are displayed in the calendar and which are not. These options can be accessed from Google calendar's settings webpage. These options include (but are not limited to) "Show events you have declined", "Only show invitations to which I have responded", etc. While these options control some aspects of how events are displayed in your Google calendar, UCA's Google calendar integration status may not be controlled by them. More specifically, UCA reflects your Google calendar's Free/Busy status only, and does not necessarily correspond to what events are visibly "shown" to you in your Google calendar. Even though some events are hidden from your view in the Google calendar (in order to reduce clutter, etc.) if those events influence the calendar's free/busy status (by default, events will mark your calendar as busy for the duration of the event unless they are declined, or are marked explicitly as "Available"), then UCA will reflect that status.



Calendar whose availability information is needed must be shared at least within the Google Apps domain. The calendars can be public, or shared with all event details visible, or shared with only free/busy information visible.

This setting can be accessed on Google calendar under “My calendars” -> <Calendar Name> -> Click on the down arrow on the right -> Calendar settings -> Share this calendar -> Share this calendar with others. The image below shows a calendar that has shared its free/busy information.

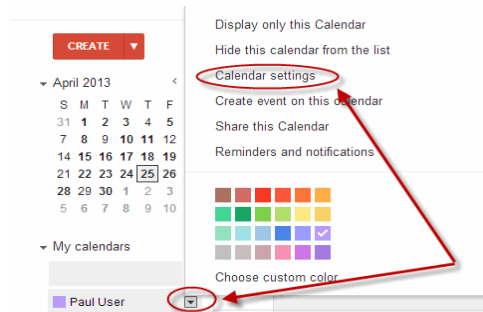


### Calendar ID

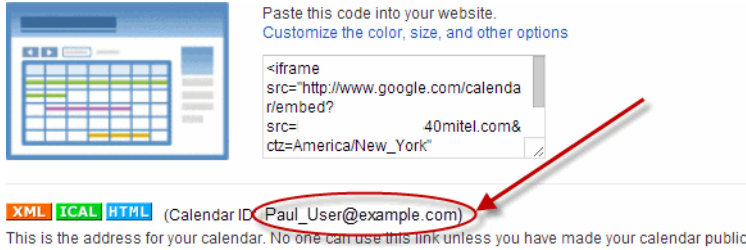
The clients should collect user's Google calendar ID and provide the information to the server. The server will then poll that calendar.

User can find the calendar's ID as follows:

Login to Google account at <https://www.google.com/calendar>. From the menu on the left-side, under My Calendars, hover on your calendar name. To the right of the calendar name, you will see a drop-down arrow. Click that and select “Calendar settings”.



The “Calendar settings” page shows the Calendar ID. Provide this ID to the UCA client.



The screenshot shows the Google Calendar settings page. On the left is a calendar view. On the right, there's a section titled "Paste this code into your website. Customize the color, size, and other options" with an `<iframe>` code block. Below this, there are three buttons: XML, ICAL, and HTML. To the right of these buttons is the text "(Calendar ID: Paul\_User@example.com)". A red circle highlights the email address, and a red arrow points from the code block's `src` attribute to it. Below the buttons, a line of text reads: "This is the address for your calendar. No one can use this link unless you have made your calendar public."



**Note:** Google calendar has a relatively new feature called appointment slots. They can be created from the same UI as creating calendar events, but by choosing Appointment slots instead of Event. For this release of UCA (v6.0), Appointment Slots created in Google calendar will not be reflected as UCA dynamic status. This is because Google APIs do not yet have the capability to retrieve appointment slots. This affects appointment slots created by a user and also slots accepted by someone. Neither type will be read by UCA. Normal events in the Google calendar will be processed and will be used to reflect UCA dynamic status.

## Google Contacts Integration

UC Advanced provides users with the option to integrate with Google Contacts.

### Licensing

This feature is available by default and no specific UC Advanced license is necessary.

### Authentication and access to Google Contacts

To provide the contacts integration feature, UCA uses OAuth 2.0 to access Google Contacts.

The process for granting Google Contacts access to applications is described in <https://developers.google.com/accounts/docs/OAuth2ForDevices>. Below are the sequence of steps that need to be performed by the UCA administrator. For the latest information, please refer to the google URL for OAuth2ForDevices (stated above). Login to Google console.



**Note:** Google Contacts only requires the Client ID and Client Secret on the UCA Server Manager (using OAuth 2.0 form). Unlike Google Calendar, the authorization code to acquire the access token of the user's contacts is done at the client level (not at the server level) as per [step 4](#).

#### 1. Access Google APIs

From a browser, navigate to <https://code.google.com/apis/console#access> and login using your Google Apps credentials.

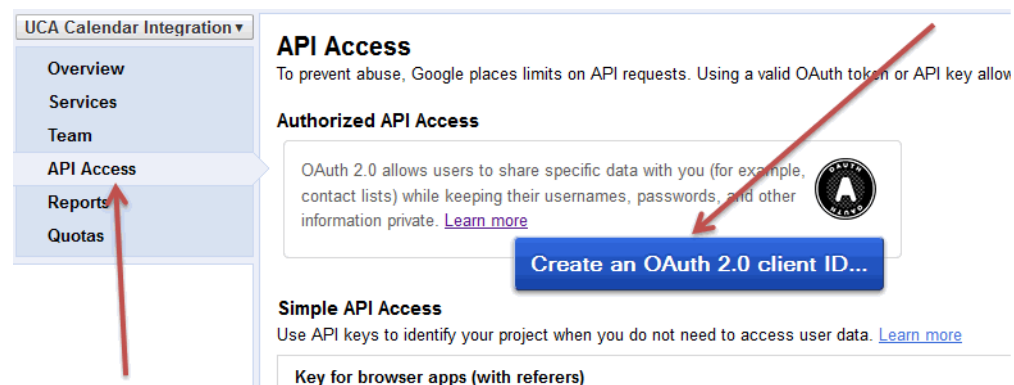


**Note:** When you create the Google API, the Contacts is not listed as an option that you can select. The Contacts is the most basic feature for Google API (i.e. having Google API account means having Google Contacts enabled -- unlike Google Calendar which is a selectable item).

#### 2. Create a Client ID

Create **client\_id** and **client\_secret**. These pieces of information are required by Google.

From the left-hand menu, select "API Access" and click on "Create an OAuth 2.0 client ID".



Now, Google will create Client ID and Client secret, which should be visible in the “API Access” tab:

The screenshot shows the Google API Access console interface. On the left, a sidebar contains links for Team, API Access (selected), Reports, and Quotas. The main content area is titled 'API Access' and includes a description of OAuth. Below this, there is a 'Branding information' section with fields for Product name (UCA Contacts Integration) and Google account (testuser2@mos365.info). A 'Client ID for installed applications' section follows, displaying the Client ID (409046102057.apps.googleusercontent.com), Client secret (3w4HOQZ2gQHkBJhSPLv3q6fV), and Redirect URIs (urn:ietf:wg:oauth:2.0:oob and http://localhost). Red arrows point to the Client ID and Client secret fields. At the bottom, there is a 'Create another client ID...' button.

### 3. Provide Client ID and Client secret to MSL

Copy-paste the Client ID and Client secret from the previous step into the fields on MSL server-manager (Login to server-manager -> Google Apps -> OAuth 2 Config. On that page you will see fields to accept client ID and client Secret. The product name can be left blank) as shown below:

The screenshot shows the MSL server-manager OAuth 2 Config page. It features a warning message at the top: 'Applications relying upon this token will not be able to access Google APIs until you have added the user authorization process below.' Below the warning, there are three input fields: Product Name (empty), Client ID (1961741482714.apps.googleusercontent.com), and Client Secret (TGA8YsbqufoJAGKmbdAKI2d8). A 'Save and Generate Authorization Code' button is located at the bottom right. Red arrows point to the Client ID and Client Secret fields.

Click on “Save and Generate Authorization Code” button. If the information you entered was incorrect (for example, due to some error in copy-pasting), the MSL page will display a brief error message. If this happens, make sure to copy the information from Google console correctly and try again.

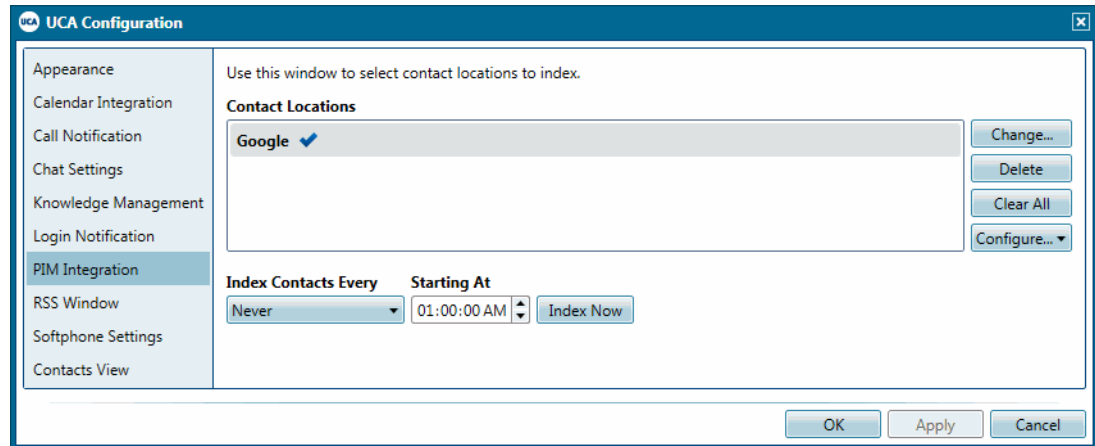
### 4. UCA clients will need to Configure Google

Desktop clients are now ready to use Google Contacts as part of UC Advanced. Desktop Clients will need to access PIM Integration window (from Configuration under Main Menu) and click on "Configure..." drop down button will have a new "Google" item.



**Note:** The "Google" item is available whether or not Google calendar integration is enabled on the server. If there are no other PIMs, the button will not be a drop down, it will just appear as "Configure Google".

See Desktop Client Help for details on how to **Configure Google** and **Import Contacts**.



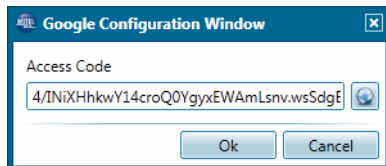
Once the user selects Google, a Google configuration window will appear and the Google website will automatically be launched. Select **Allow access** when prompted by Google.

**UCA Calendar Integration** is requesting permission to:

▸ Manage your contacts

**Allow access** No thanks

A Google Configuration Window will appear displaying an Access Code, click OK.



If you have multiple Google Accounts, you will be prompted to select one account.

If Google Contacts was successfully configured, you are now ready to **Import Contacts** to the client. See Desktop client help to Import Contacts.



# CHAPTER 5

## MAINTENANCE





## About Software Upgrades

The UC Server software includes both the server and client software for UC Advanced. UC Advanced software upgrades may require additional upgrades to the MSL operating system and/or integrated application software.

Before beginning a software upgrade, review the release notes and the Engineering Guidelines for a comprehensive list of upgrade requirements.



**Note:** "Client Only Delivery" functionality is applicable to the following clients: Desktop, Android, BlackBerry and Web clients. See [Client Only Delivery on page 199](#).

## UC Advanced Software Upgrades

The upgrade to UC Advanced 6.0 SP1 requires an upgrade to the following components:

- **UC Server v6.0:** Includes v6.0 server and client software. The client software must be deployed to each user to complete the upgrade.
- **MSL v10.0:** Includes the Mitel Standard Linux operating system and Server Manager interface.



**Note:** You must be running UC Server version 4.0 or higher before attempting to upgrade to UC Server version 6.0. If you are running UC Server version 3.2 or earlier, first upgrade to UC Server version 4.0.



**Note:** UC Server version 6.0 requires MSL version 10.0 or later. It will not run on MSL 9.4 or earlier. The upgrade from MSL 9.4 or earlier to MSL 10.0 or later on physical servers requires a backup, reinstall, and restore of the operating system and application data.

See the following sections for software upgrades:

- [Upgrade UC Server version 4.0, 4.1, 5.0 or 5.1 to version 6.0 SP1 on page 194](#)
- [Upgrade UC Server version 6.0 to version 6.0 SP1 on page 194](#)
- [Upgrade virtual UC Server \(vUCA\) version 4.0 or higher to version 6.0 or higher on page 195](#)
- [Upgrade the UC Advanced Desktop Clients on page 196](#)
- [Upgrade MiVoice for Lync Client on page 197](#)
- [Upgrade the UC Advanced Mobile for BlackBerry Clients on page 198](#)



**Note:** Upgrades specific to the UC Advanced Mobile for Android, iPad and iPhone clients:  
You will be automatically notified of a new version of software available for your clients. Simply follow the on-screen instructions to perform the upgrade.

## Upgrade UC Server version 4.0, 4.1, 5.0 or 5.1 to version 6.0 SP1

Follow one of the 2 scenarios:

*Scenario 1: Upgrade UC Server version 4.0, 4.1, 5.0 or 5.1 (physical server) to version 6.0 SP1 (physical server) using software downloaded from the AMC*

1. Perform an MSL backup of the UC Server.
2. Download the MSL 10.0 CD image from Mitel OnLine and burn it to a recordable CD.
3. Install MSL 10.0 (see [Install the MSL Operating System on page 109](#)).
4. When prompted if a restore operation should be performed, select "Yes".
5. Restore from either removable media, or from a network location (see MSL Installation & Administration Guide).
6. Use the "Blades" panel to install the UC Server version 6.0 SP1 software.

*Scenario 2: Upgrade UC Server version 4.0, 4.1, 5.0 or 5.1 (physical server) to version 6.0 SP1 (physical server) using downloaded CD images*

1. Perform an MSL backup of the UC Server.
2. Download the MSL 10.0 CD image from Mitel OnLine and burn it to a recordable CD.
3. Download the UC Server version 6.0 SP1 software from Mitel OnLine and burn it to a recordable CD.
4. Install MSL 10.0 (see [Install the MSL Operating System on page 109](#)).
5. When prompted if a restore operation should be performed, select "Yes".
6. Restore from either removable media, or from a network location (see MSL Installation & Administration Guide).
7. Insert the recordable CD produced in step 3 above into the CD-ROM tray.
8. Use the "Blades" panel to install the UC Server version 6.0 SP1 software.

## Upgrade UC Server version 6.0 to version 6.0 SP1

Follow one of the 2 scenarios:

*Scenario 1: Upgrade UC Server version 6.0 (physical server) to version 6.0 SP1 (physical server) using software downloaded from the AMC*

1. Perform an MSL backup of the UC Server.
2. Use the "Blades" panel to install the UC Server version 6.0 SP1 software.

*Scenario 2: Upgrade UC Server version 6.0 (physical server) to version 6.0 SP1 (physical server) using downloaded CD images*

1. Perform an MSL backup of the UC Server.

2. Download the UC Server version 6.0 SP1 software from Mitel OnLine and burn it to a recordable CD.
3. Insert the recordable CD produced in step 2 above into the CD-ROM tray.
4. Use the “Blades” panel to install the UC Server version 6.0 SP1 software.

### Upgrade virtual UC Server (vUCA) version 4.0 or higher to version 6.0 or higher

1. Backup your existing UC Advanced virtual appliance. Select **Backup**. Select a location to place the backup file. Click **Perform**.
2. Copy your vUCA database backup file to a USB device or a shared directory on the network file server. Note that back up to a USB device is available only with vSphere 4.1 and later.
3. Shut down the existing UCA server, using the MSL **Shutdown or reconfigure** option.
4. Download the new virtual appliance file (.ova) from Mitel OnLine and save it on your local machine.
5. Start the vSphere Client, and then select File – **Deploy OVF Template....**
6. Select **Deploy from file** and then browse to the location on your machine where you saved the new .ova file.
7. Click **Next**. The OVF Template Details page appears.
8. Click **Next**. The End User License Agreement page appears.
9. Click **Accept**, and then click **Next**. The Name and Location page appears.
10. Type a name for virtual server, and then click **Next**. Deployment settings for the virtual appliance are shown.
11. Confirm the settings, and then click **Finish** to deploy the file. A dialog box shows the progress of the files being deployed.
12. When the deployment completes successfully click **Close** to continue.
13. In the vSphere client window, expand the VMware host view to show the newly created virtual machine.
14. Click the Console tab. Click the green arrow to power on the virtual machine.
15. After the virtual machine has booted, the Console Tab shows the MSL installation window.
16. Choose your preferred keyboard from the list (the default is us) and click **Next**.
17. MSL prompts you by asking if you want to restore from backup. Enter **Yes**.
18. Select **Restore from USB** and insert your USB key when prompted OR **Select Restore from Network Server** (depending on where you placed your backup at the beginning of this procedure). Follow the prompts to specify the location of the backup file and start the restore process.

## Upgrade the UC Advanced Desktop Clients

When you upgrade the UC Server software blade, a Desktop Client installer is included in the software blade and the UC Server property file is updated with the latest software version information.



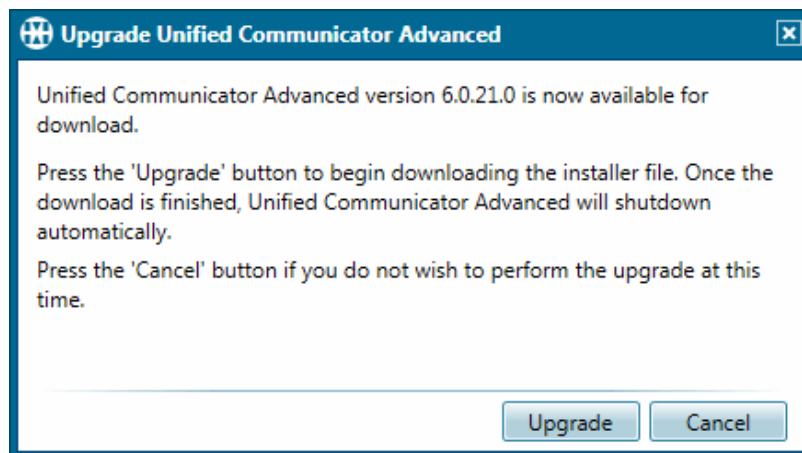
**Note:** The UC Advanced Desktop Client requires the installation of the Microsoft.NET Framework v4.0 (see [page 127](#)) prior to installing the Desktop Client.

### Upgrades from v5.x

After you upgrade the UC server to v6.x, the 5.x Desktop Client polls the UC Server property file and determines that a client installer is available.

The Desktop Client notifies the user that the 6.x software is available as follows:

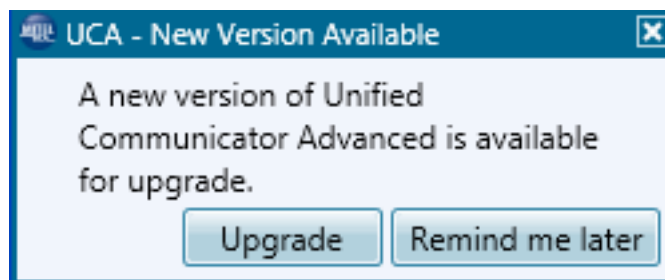
- If the user is logged off the Desktop Client when the upgrade becomes available, the Upgrade Product notification dialog box appears when he or she attempts to log in.



**Figure 17: Upgrade Notification Dialog Box**

The user can click **Upgrade** to start the upgrade process. If the user clicks **Cancel**, the UC Advanced version popup window (see [Figure 18](#)) appears after the user logs in.

- If the user is logged in to the Desktop Client when the upgrade becomes available, the UC Advanced version popup window appears



**Figure 18: Version Popup Window**

The user can click **Upgrade** to start the upgrade process. If the user clicks **Remind me later**, this popup window reappears each following day until the user upgrades to the latest version.

Users should-close all Windows applications before initiating the upgrade.

After the client upgrade process is initiated, the software is downloaded to the user's computer. When the download is complete, the installation wizard appears prompting the user to install. The user can then run the installation wizard (see [page 128](#)) to install the upgraded client. When completing upgrades, the Installation wizard auto-populates the **UC Server FQDN** and **Default Language** fields based on the previous software version's settings.

Following an upgrade, the Desktop Client restarts automatically and the following client components are migrated to the upgrade version:

- User-specific configuration settings
- Detailed call history
- Personal contacts

## Upgrade MiVoice for Lync Client

In the first release of MiVoice for Lync (UCA 6.0), the UCA server will not automatically notify the user about the availability of upgraded versions.



**Note:** The upgrade notification process will be manual (not automated) in the first release of MiVoice for Lync.

The administrator will need to inform the user(s) of a new MiVoice for Lync software version being available with a link (URL) to download the new .msi file.

Before executing manually, the user has to explicitly close MS Lync client and then upgrade the Mitel Lync plug-in. To perform the upgrade, the user must have installation permissions on the computer or provide the administrator credentials when prompted. It is not required to uninstall the previous software version prior to performing an upgrade.

Once the upgrade is complete, the Mitel Lync plug-in and MS Lync client will be restarted. The existing settings will be preserved throughout an upgrade.

## Upgrade the UC Advanced Mobile for BlackBerry Clients

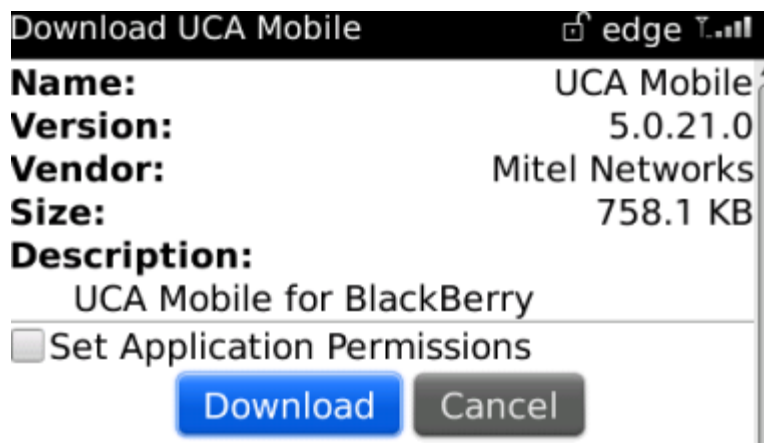
When you upgrade the UC Server software blade, mobile client software is included in the software blade. Users are prompted to download the upgrade when they restart the client after the server upgrade if they are running version 4.0.20.0 or earlier.

**Note:** If you are running an OS less than 5.0 with the UC Advanced server running version 4.1, you will download version 4.0.21.0 only. Even if there is a higher version than 4.0.21.0 available, you will not receive a prompt to upgrade if you are running an OS less than 5.0.

If they do not install the upgrade at that time, the next time they start the application, they will be prompted again to upgrade.

*To upgrade the UC Advanced Mobile client:*

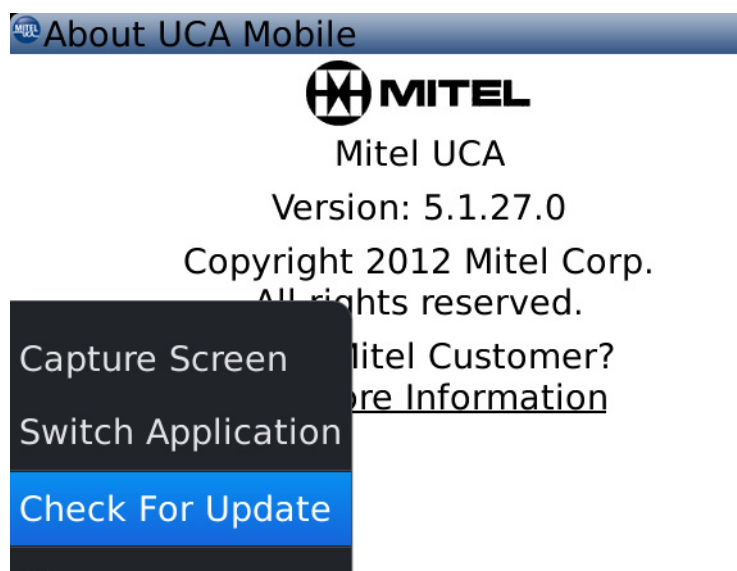
1. Select **Yes** for the version popup window. The download page appears.



2. Select **Download**. The following prompt appears:  
The Application UCA Mobile already exists. Replace version <x.x.x.x> with version <y.y.y.y>?
3. Select **Replace**. The software is downloaded and installed automatically. The reboot prompt appears.
4. Do one of the following:
  - Select **Reboot** to complete the upgrade now. The mobile device powers off and then on again.
  - Select **Later** to complete the upgrade later. If you select **Later**, you must remember to reboot the device at a later time to complete the upgrade process. The upgraded software will not run until after you reboot the device.

Following an upgrade you must accept the End User License Agreement (EULA) again.

Users can also check for upgrades at any time from the UC Advanced Mobile About page by selecting the **Check For Update** option.



**Figure 19: UC Advanced Mobile About Page**

The client queries the server and prompts the user to upgrade if a software version is available.



**Note:** Users should consult their mobile service provider for BlackBerry mobile operating system upgrades. After a major OS upgrade, it may be necessary for users to re-enter their UC Advanced credentials and settings. Locations are stored in the device's file system and are restored if the OS upgrade is done properly using BlackBerry Desktop Manager.

## Client Only Delivery

**Client Only Delivery** functionality delivers Windows Desktop Client and mobile clients software without having to upgrade the UCA server version.

Supported clients: Desktop, Android, BlackBerry and Web clients.

A new Administration web user interface has been introduced to support this activity. A "Client Versions" section was added to this page to allow the administration of these upgrades. Example below shows the page using Chrome browser. The page will display **Browse** instead of **Choose File** using other browsers such as IE or Firefox.

### Mitel Unified Communications Server Administration



To perform a system administration function, click one of the links in the menu on the left of your screen, or choose from one of the configuration options below.

#### Configuration

The Mitel Unified Communications Server configuration pages provide an easy-to-use interface for managing administrative tasks, including: configuration of PBX nodes, configuration of user accounts, and configuration of directory synchronization settings.

Configure Mitel UC Server

#### Status

The current server status is shown below, if available. To stop or start the Mitel Unified Communications Server, choose the desired action and then select the "Perform Requested Action" button below.

uca-vmas02.mitel.com: **ACTIVE**

Action: Refresh Status

Perform Requested Action

#### Client Versions

This table shows the UC Advanced client software versions currently available on this server. To make a newer version of UC Advanced client software available for users, specify the package to upload and then select the "Upload UC Advanced Client" button below.

UC Advanced Desktop Client:	6.0.21.0
UC Advanced Mobile for Android:	5.1.34.20408
UC Advanced Mobile for BlackBerry:	5.1.27.0
UC Advanced Web Client:	6.0.21.20722

New Client Package: Choose File No file chosen

Upload UC Advanced Client

#### Diagnostics

The server diagnostics page provides an interface to view statistical information about the running system, information about current registrations, and status information of running modules.

Perform Server Diagnostics

Using the Administration web interface you will be able to install, upgrade, or downgrade selected components of the UC Server blade by specifying a local client package and clicking the "Upload UC Advanced Client" link.

An "Operation status report" displays either a successful client software package installation or an error message indicating a validation step has failed. Several validation steps are performed to prevent user from:

- uploading files that are not valid client packages
- replacing a system or UC Server level component
- uploading a corrupted client file



**Note:** There is no ability or mechanism to remove any individual UC Advanced software clients.



## User Upgrades (Stand-alone to Integrated)

UC Advanced provides two options for users: Integrated and Stand-alone:

- **Integrated UC Advanced users:** Users who are licensed for the Desk Phone or Softphone features and **not** the Stand-alone Web Portal feature have access to the integrated suite of UC Advanced interfaces including the Desktop Client, Web Portal, and Mobile Portal.
- **Stand-alone UC Advanced users:** Users who are licensed for the Stand-alone Web Portal and **not** the Desk Phone or Softphone features can access UC Advanced features from the corresponding portal only. They do not have access to the Desktop Client application.

*UC Advanced provides an upgrade process to upgrade stand-alone users to integrated.*

### To upgrade Stand-alone Web Portal users to Integrated:

1. Purchase the desired number of Desk Phone and/or Softphone licenses from the AMC. A Desk Phone or Softphone license is required for integrated users (see Table 1 on [page 23](#)).
2. From the MSL Server Manager interface, synchronize the UC Server with the AMC to verify that the server has the appropriate licenses for each user (see [page 113](#)).
3. From the UC Server Administrator interface, complete the following tasks:
  - Do one of the following to apply the Desk Phone or Softphone license to the users you want to upgrade (Accounts Tab – <user> – Account Details page – **Licensed Features**):
    - For each user, select a feature profile that includes the Desk Phone or Softphone licensed features.



**Note:** If required, configure a feature profile that includes the Desk Phone and/or Softphone licensed features (Features Tab – **Add Profile**).

- For each user, select the **Desk Phone** or **Softphone** Add-On feature.
- If other account -specific changes are required, reconfigure those fields and options on the Account Details page for each user.
- Resend the Welcome e-mail message to each upgraded user.



**Note:** Refer to the Online Help for information about the following topics:

- Stand-alone vs. integrated user settings
- Feature profiles
- Welcome E-mail message

4. Do one of the following:
  - Instruct the user to install the Desktop Client using the client software URL provided in the Welcome E-mail message.
  - Install the Desktop Client on the user's PC (see [page 124](#)).

## MSL Server Administration

The MSL Server Manager provides menus for performing MSL-related administrative tasks. These tasks are not related to UC Advanced administrator tasks (see [page 202](#)). However, they may be helpful for UC Server diagnostic purposes such as gathering log files (see [page 230](#)).

For information about MSL administrator tasks, refer to the MSL Server Manager online help or the *MSL Installation and Administration Guide* available on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>) for details and instructions.

## UC Server Administration

The main UC Server Administration page provides access to several options.

**Mitel Unified Communications Server Administration**

To perform a system administration function, click one of the links in the menu on the left of your screen, or choose from one of the configuration options below.

**Configuration**

The Mitel Unified Communications Server configuration pages provide an easy-to-use interface for managing administrative tasks, including: configuration of PBX nodes, configuration of user accounts, and configuration of directory synchronization settings.

[Configure Mitel UC Server](#)

**Status**

The current server status is shown below, if available. To stop or start the Mitel Unified Communications Server, choose the desired action and then select the "Perform Requested Action" button below.

ucsm92.mitel.com: **ACTIVE**

Action: Refresh Status

[Perform Requested Action](#)

**Client Versions**

This table shows the UC Advanced client software versions currently available on this server. To make a newer version of UC Advanced client software available for users, specify the package to upload and then select the "Upload UC Advanced Client" button below.

UC Advanced Desktop Client:	6.0.21.0
UC Advanced Mobile for Android:	5.1.34.20408
UC Advanced Mobile for BlackBerry:	5.1.27.0
UC Advanced Web Client:	6.0.21.20722

New Client Package: [Choose File](#) No file chosen

[Upload UC Advanced Client](#)

**Diagnostics**

The server diagnostic page provides an interface to view statistical information about the running system, information about current registrations, and status information of running modules.

[Perform Server Diagnostics](#)

**Import Data**

You may import Unified Communications Server data using the form below. Use this form if you have a backup file generated on a Mitel UC Server, and you wish to restore the UC Server data contained in the backup file on this system. MSL configuration information (regions information, hostname, etc.) contained in the backup file will be ignored. **Note that selecting this option will overwrite all Mitel Unified Communications Server configuration information and reinitialize the Mitel Unified Communications Server database to the values stored in the specified backup file.** Once started, the import process will take several minutes to complete.

Import Data File: [Choose File](#) No file chosen

[Import Mitel UC Server Data](#)


**Reinitialize System**

You may reinitialize the configuration of the Mitel Unified Communications Server by selecting the "Reinitialize Mitel UC Server Configuration" button below. **Note that selecting this option will remove all Mitel Unified Communications Server configuration information and reinitialize the Mitel Unified Communications Server database.** Once started, the reinitialization process will take several minutes to complete.

[Reinitialize Mitel UC Server Configuration](#)

Mitel Standard Linux 10.0.20.0  
Copyright 1999-2013 Mitel Corporation  
All rights reserved.

## Configuration

The Configuration section of the page provides access to the UC Server Configuration tabs where you can provision the system (see [page 122](#)). Click **Configure Mitel UC Server**. The configuration pages open to the Enterprise tab. Refer to the online Help  for tab-specific information and instructions.

## Status

The Status section of the Mitel UC Server Administration page provides the name and current status for the UC Server. Statuses include:

- **Active:** The server is online and operational.
- **Becoming Active:** The server is in the process of coming online.
- **Idle:** The server is offline and not operational.

*To start, stop, or refresh the server:*

1. Select an action from the list box. Options include:
  - Start Mitel UC Server
  - Stop Mitel UC Server
  - Refresh Status
2. Click **Perform Requested Action**.



**Note:** If the UC Server is stopped using the “Stop Mitel UC Server” selection, then the UC Server will remain stopped until it is explicitly started using the “Start Mitel UC Server” selection, even across system reboot operations.

## Diagnostics

The Diagnostics section of the page provides access to diagnostics tools. Click **Perform Server Diagnostics** to access diagnostics tools.



**Notes:** Do not use the Mitel UC Server Diagnostic tools unless you are instructed to do so by Mitel technical support personnel.

Name	Uptime	Restarts	Status	Status Operations	Debug Level	Set Debug Level
ACCTPRES	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
ADEPM	4 days 23h:35m:02s	1	IN_SERVICE	Start   Stop   Restart	4	1 Set
ALARMD	4 days 23h:35m:02s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
AMC_AGENT	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
DB_CHECK	4 days 23h:35m:02s	1	READY_FOR_CALL	Start   Stop   Restart	2	1 Set
DSM	4 days 23h:35m:02s	1	IN_SERVICE	Start   Stop   Restart	2	1 Set
EP3300	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	3	1 Set
ERRLOG	4 days 23h:35m:01s	1	UNKNOWN. (not watched)	Start   Stop   Restart	1	1 Set
FEDERATIONGW	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
FEDERATION_SERVICE	4 days 23h:35m:54s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
GNM	4 days 23h:35m:36s	1	IN_SERVICE	Start   Stop   Restart	2	1 Set
IMEVENTS	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set
JBOS	4 days 23h:35m:02s	1	UNKNOWN. (not watched)	Start   Stop   Restart	1	1 Set
JBOS_CHECKER	4 days 23h:35m:02s	1	UNKNOWN. (not watched)	Start   Stop   Restart	1	1 Set
MailNotif	4 days 23h:35m:02s	1	UNKNOWN. (not watched)	Start   Stop   Restart	1	1 Set
NOTIFY_SERVICE	4 days 23h:35m:54s	1	UNKNOWN. (not watched)	Start   Stop   Restart	1	1 Set
NOTIF_MANAGER	4 days 23h:35m:01s	1	IN_SERVICE	Start   Stop   Restart	1	1 Set

**Figure 20: Server Diagnostics Tools**

The tabs on the Mitel UC Server Diagnostics page include:

- **Modules:** Displays the following information for all of the modules running on the system:
  - *Name:* Displays the name of the module running.
  - *Uptime:* Displays how long the module has been running for.
  - *Restarts:* Displays how many times the module has been stopped and restarted. This helps you determine if a module stopped unexpectedly. If a module was not restarted manually and the module indicates it has been restarted, this indicates an error condition.
  - *Status:* Displays the state of a module. IN\_SERVICE indicates a module is operating correctly. Many modules have custom strings like READY\_FOR\_CALL, etc. A module shows SHUTDOWN if it is turned off by clicking **Stop**. Unwatched modules show UNKNOWN (not watched), because they are not monitored by a watchdog component. A monitored module should not display UNKNOWN.
  - *Status Operations:* Modules that are monitored by a watchdog component can be started, stopped, or restarted from here. You may need to refresh the view by clicking the Modules tab.

- *Debug Level*: Indicates the debug level at which the module is currently running. The debug level for a module can be anywhere between 1 and 5. The higher the debug level, the more information that is generated by the module and printed in the associated logs.
- *Set Debug Level*: Configure the debug level for a module here by selecting the level from the list and then clicking **Set**. After the page is refreshed, the Debug Level reflects the level you configured.
- **Clients**: Provides information about currently connected clients in the system. The first line of the page indicates the number of connected clients on the system. You can search for a specific Login ID, or for a specific client type by modifying the appropriate form fields provided and then clicking the Search button. If no values are supplied on the search form, pressing the Search button will display a listing of all connected clients. The following information is displayed for each client:
  - Bridge ID
  - Login ID
  - Client Info (the type of client that the user is using)
  - Connection (the IP address of the connecting client)
  - Connected Since (the time that the client connected).
- **Registrations**: Provides information about currently registered phones in the system. The first line of the page indicates the number of registered phones on the system. By default, no phone is selected. You can search for a specific phone by selecting a **Tenant** from the list, typing the **Login ID** for the user, and then clicking **Search**. You can also search for all registered phones by typing the % character in the **Login ID** field. The following information is displayed for each user:
  - Tenant ID
  - *Alias ID* (an alternate name for the user on the server)
  - *Address ID* (usually the user's public number)
  - *Expiration Date* (the time when the user's registration expires)
  - *Device ID* (the type of device/and Desktop Client version that the user is using)
  - *User Agent* (additional information about the user's Desktop Client)
  - *Resource ID* (the registered SIP address where the server sends SIP requests)
- **TDC**: Indicates information about the following modules on the system:
  - *ACCTPRES*, *IM EVENTS*, *PRES*, *SIP PROXY*, *SIP REG*: These modules show SIP statistics and include the following information:
    - The tabs show **Incoming** and **Outgoing** SIP requests and responses.
    - The request columns are further divided into **Register**, **Subscribe** and **Notify** which are types of SIP messages.
    - The Responses are broken down into 1xx, 2xx, 3xx, 4xx, 5xx, 6xx and unknown columns. 2xx responses are success messages, while unknown, 1xx, 3xx, 4xx, 5xx, and 6xx responses are error responses.
    - The Errors column reports any anomalies for the module.

- **CALL SERVICES:** This area indicates the feature usage for the server. Hourly values for each day for Place call, Answer, Hangup, Hold, Retrieve, Deflect, Transfer and Conference are reported.
- **VISUAL VOICEMAIL:** This page shows the session success and error codes for the Visual Voice Mail feature provided by the Web services. Hourly statistics for VM Session Success, VM Session Fail, Make Call, Forward Message, Delete Message, Set VM Pin and Send Fax are shown.

You can view logs for each day by selecting a day from the list.

- **Subscriptions:** Indicates the subscription events in use by the system. The information is shown in the tabular format with the first column indicating the Event ID and the next column showing the number of each subscription events in use. You can view detailed information for each subscription by selecting a **Tenant** from the list, typing the **Login ID** for the user, and then clicking **Search**. You can also search all subscriptions by typing the % character in the **Login ID** field. The following information is displayed for each user:
  - Subscription ID
  - *EVENT\_ID* (which event the user is subscribing to)
  - *WATCHER\_ID* (the user subscribing to the event)
  - *WATCHED\_USER*
  - *EXPIRES* (the time when the user's subscription expires)
  - *ROUTE\_SET* (the route that future SIP NOTIFYs from the server should take to reach the client)
- **Calstatus:** Provides a set of diagnostic functions that can be used for troubleshooting. Although some of the diagnostic information is valid for all types of Calendar Integration, the Calstatus diagnostics are geared towards Microsoft Exchange and Google Calendar Integration.



**Note:** Some operations with Calstatus diagnostics can cause issues with Calendar and Google or Exchange Integration. Use caution when reviewing Calstatus values and work in conjunction with your Google or Exchange server administrator and Mitel Technical Support if necessary when handling problems.

The following is a description of the information that can be accessed through these diagnostics:

- **Enterprises and Advanced Configuration:** This page under the Calstatus diagnostics tab lists all the enterprises available on the UCA Server.
  - **Enterprise Details:** If any of the enterprises have either a Google or Exchange Server configured and enabled for Calendar Integration, those are listed under the Calendar Integration column. If Google and Exchange Integration is disabled for an enterprise, then the Details link is not displayed. Clicking on the Details link displays the Calendar Integration details for that enterprise.
  - **Advanced Configuration:** Below the list of enterprises, the page shows Advanced Configuration for the Calendar Integration. For more information about these fields, changing them, and the effects of such changes, refer to the UCA Administrator Online Help system.
  - List of recent OAuth 2.0 Data Updates is also displayed on this page. See

screenshot below as an example:

List of recent OAuth 2.0 Data Updates (applies across all enterprises):

```

• 2013-02-04 00:40:45: Token: <Bearer ya29.AHES6ZRT5xaWBHA4gCRuVuvvMy2ZTeMBYyximB3Srm_IHA4U4g> Valid Until 2013-02-04 01:40:45 Error: <>
• 2013-02-04 01:31:05: Token: <Bearer ya29.AHES6ZSfQ9QF8PC22oeTW6QJtex4YqUtLddivY32EuUSMuIw> Valid Until 2013-02-04 02:31:05 Error: <>
• 2013-02-04 02:21:06: Token: <Bearer ya29.AHES6ZQwYAvyb2STeAxiTGKsLc3NI6WM41tPeoeRN5pWoGYy7w> Valid Until 2013-02-04 03:21:06 Error: <>
• 2013-02-04 03:11:28: Token: <Bearer ya29.AHES6ZTT8QE5niefmKIpLefhsO5ISdw2036-YYMbDSzSKOxYfw> Valid Until 2013-02-04 04:11:28 Error: <>
• 2013-02-04 04:01:49: Token: <Bearer ya29.AHES6ZRPX356tFTPIKfV0RVq1y1ymxTk3C-iCSOZRQ4wQs28w> Valid Until 2013-02-04 05:01:49 Error: <>
• 2013-02-04 04:52:09: Token: <Bearer ya29.AHES6ZTh74e2mNwGrd71OurcskHCSYGvviZp_4dvKUY3LayLcw> Valid Until 2013-02-04 05:52:09 Error: <>
• 2013-02-04 05:42:10: Token: <Bearer ya29.AHES6ZRXPMIN7qwlKpg-vwS1NWoS6b262gteCOWQP8jyoTXRMw> Valid Until 2013-02-04 06:42:10 Error: <>
• 2013-02-04 06:32:31: Token: <Bearer ya29.AHES6ZT-uORHTEvzD3k_CLN3GTE6tRf9ROSE2qsFCxG1JSmcrv> Valid Until 2013-02-04 07:32:31 Error: <>
• 2013-02-04 07:22:52: Token: <Bearer ya29.AHES6ZTqNSogbcUIR1fAtvdMAkkPw9zyrGKtBVgIaUo2NI8xAA> Valid Until 2013-02-04 08:22:52 Error: <>
• 2013-02-04 08:13:13: Token: <Bearer ya29.AHES6ZRHxtEOb4kOoyOpScjs-gMeuiwATUdHFFvFvMvviCR5yQ> Valid Until 2013-02-04 09:13:13 Error: <>
• 2013-02-04 09:03:35: Token: <Bearer ya29.AHES6ZSVGDhy7S5i9Vlu0o0nQoO5CJIC9XnnW88YLS4ZJlaBw> Valid Until 2013-02-04 10:03:35 Error: <>

```

- **Enterprise Details:** This page shows the detailed Google or Exchange Integration configuration information for a specific enterprise.
  - **Enterprise Name:** UCA enterprise name
  - **Calendar Integration Type:** Google or MS Exchange
  - **Enterprise's calendar integration active?:** Indicates whether or not the Google or Exchange Integration is active and enabled for this enterprise. If there are any permanent errors associated with this calendar integration, this flag shows "No". If error details are available, those details are shown at the bottom of the page.
  - **Is Temporarily Disabled?:** Indicates whether communication with Google or Exchange server has been temporarily disabled. If details are available, they are shown below this flag, along with a time stamp of when the communication will be retried. For this retry to happen, no action needs to be taken by the Administrator. UCA will continue to retry until the error is resolved.
  - **Exchange Access URL:** The Exchange Web Services (EWS) URL on the Exchange server. UCA retrieves user calendar information from this URL.
  - **Exchange Impersonation Enabled?:** Indicates whether or not UCA Exchange integration is configured to use impersonation.
  - **Exchange Server Access Username:** Displays the Exchange username that is used to retrieve calendar information.
  - **Exchange Access Credentials Valid?:** Indicates whether or not the Exchange access username and password are valid.
  - **Exchange Version:** Displays the Exchange server version.
  - **Subscription URL:** Displays the Subscription URL (applicable to Exchange Integration only).
  - **Users List:** The lists displayed are categorized according to users' status and are based on error conditions, if any exist:
  - **Number of Valid Users:** Lists users who have Google or Exchange Integration configured. If a user has another type of Calendar Integration configured (such as Outlook or Lotus Notes), then that user does not show up in this list.
  - **Active Users:** Lists a subset of valid users and contains only those users whose Google or Exchange Integration is active. Users who have configured either Google or Exchange Integration but have disabled it or those who have been deactivated because of errors do not show up in this list.
  - **Deactivated: various errors:** see list below.
  - **Deactivated: temporarily disabled.**
  - **Deactivated due to impersonation error:** If impersonation is not configured correctly on the Exchange server, Exchange Integration can be deactivated for the affected users. Once impersonation is configured correctly, you can click on "Reactivate Users" to reactivate Exchange Integration for the affected users.

The other lists pertain to various error conditions.

- **User Lists:** Select a user from the list or enter the user's UCA login ID and click Show User Details. This takes you to either the user's Google or Exchange Integration details page.
- **User Details:** This page displays details about the user's Google or Exchange Integration configuration and status. Most of the settings shown here are configured by the user from a UCA client.
  - **Calendar Type:** Indicates the type of Calendar Integration chosen by the user. This can be Google, MS Exchange, Outlook, or Lotus Notes based on the configuration. Most of the information on the User Details page is grayed out unless the Integration is with Google or Exchange, because the remaining types (such as Outlook/Notes) are managed by UCA clients, and not by UCA server.
  - **UCA User ID:** Displays the user's UCA Enterprise ID and user ID.
  - **User's Calserver Credentials Valid:** Indicates whether or not the user's credentials are valid.
  - **User's Calendar integration Valid:** Indicates whether or not the user has configured Calendar Integration.
  - **CalServer Primary Email Address:** Displays the user's Exchange primary email address.
  - **CalServer Username** (specific to Exchange Integration): Shows the user's Exchange username. The "Dissociate Credentials" option clears out the user's Exchange credentials that are cached on the UCA server and immediately disables the user's Exchange Integration. **Use with caution.**
  - **Google Calendar ID:** Shows the user's Google Calendar ID. The "Dissociate Credentials" option clears out the user's Google credentials that are cached on the UCA server and immediately disables the user's Google Integration. **Use with caution.**
  - **User's Calendar integration Active:** Indicates whether or not the user's Calendar Integration is active. A user's Calendar Integration could be inactive if the user has disabled Calendar Integration or as a result of other errors, usually with user configuration. Therefore these errors are specific to that user and do not affect Calendar Integration for the entire enterprise. If errors details are available, they are displayed in this field, as shown in the examples below. In the first example, a user has disabled Calendar Integration from the client. In the second example, the Exchange server has returned an error that the Exchange email address entered by the user has no mailbox associated with it (this is most likely a result of entering the email address incorrectly). Even if user's calendar integration settings are all correct, there could be other problems (such as network connectivity issues, or incorrect calendar integration settings at the Enterprise level. In such cases, calendar integration will be disabled for that entire enterprise. Such problems are not specific to a user. However, to indicate the presence of a problem, those problems are also shown in the user details page.
  - In the example shown below, the communication with Exchange server has been temporarily disabled. The error details indicate that the UCA Administrator can act on it. Since this is not a user-specific error, the user cannot do much apart from notifying the Administrator of the error. Not correcting the error but trying to reactivate this user alone will not help, because the user will encounter the same



error once again and will get disabled.

User's calendar  
integration  
Active? **No**

**Reason  
Inactive**

**Server is temporarily disabled: java.net.UnknownHostException wrong.hostname.mitel.com - The server's hostname is not resolvable. Please check the URL or the Name Server settings.: Calstatus: node99(c0ffca7e-1dd1-11b2-aa14-e63830356130) - Communication with this calendar server will be disabled temporarily. This error may be actionable by UCA Administrator. If no action is taken, an error recovery attempt will be made at 2012-08-01 11:04:26**

Reactivate User

User's calendar  
integration  
Active? **No**

**Reason  
Inactive**

**USER\_DISABLED: User's calendar integration has been disabled**

Reactivate User

User's calendar  
integration Active? **No**

**Reason  
Inactive**

**UNCATEGORIZED\_ERROR: Server returned 500 Internal Server Error: The following error message was received from Exchange server. For details on error codes, see <http://msdn.microsoft.com/en-us/library/bb402172%28v=exchg.140%29.aspx> ErrorCode=ErrorNonExistentMailbox ErrorMessage=The SMTP address has no mailbox associated with it.**

Reactivate User

- After correcting the error conditions, you can click on “Reactivate User” to have UCA reinitiate the user’s Calendar Integration. If the error condition persists or another error is displayed, the user is deactivated again.



**Note:** In most cases, user reactivation should be done by the user correcting the incorrect configuration parameters, NOT by administrative action. The “Reactivate User” button is provided as an additional mechanism for you to troubleshoot problems.

- **Calendar Integration Enabled?:** Indicates whether the user has enabled/disabled Calendar Integration from the client.
- **Advisory Message Enabled?:** Indicates whether the user has enabled/disabled Calendar Advisory. If advisory is disabled, Calendar Integration continues to work, but UCA clients do not display advisory messages such as “In a meeting until 11:30 AM”.
- **Status Transition Settings:** Lists the UCA status transitions configured by the user. These UCA status transitions are triggered based on the user’s calendar status.

- **Calendar Event Subscription** (specific to Exchange Integration): The UCA server subscribes to event notifications with the Exchange server. If an Exchange user's calendar is updated, then the Exchange server notifies the UCA server of this update through the subscription mechanism. The times at which the last few subscriptions occurred, the times at which the Exchange server sent the notifications, and so on can be helpful in troubleshooting problems. The UCA server initiates subscriptions based on the configured interval (see Exchange Integration Advanced Settings in the UCA Administrator Online Help). Clicking on "Force Resubscription" causes the UCA server to immediately try to initiate a subscription for this user.
- **Calendar Event Polling**: The UCA server periodically polls the Google and Exchange server to fetch users' calendar information. The times at which the polling occurred and the next scheduled poll time can be useful in troubleshooting problems. The "Force Event Poll Now" button causes the UCA server to immediately initiate an event poll for this user.
- **Last few UCA status changes triggered by calendar availability**: This is a list of the last few UCA dynamic status changes caused by either Google or Exchange Integration. If the UCA dynamic status changes for any reason other than Google or Exchange Integration, that change is not shown here. For each status change, the time of change, the previous status, the next status, calendar advisory (if any), and status names and IDs are displayed.
- **Integrated Directory Services (IDS) Auth Cache**: When UCA is operating in MAS integrated mode, the administrator can setup Integrated Directory Services (MAS IDS) to authenticate UCA users. In that configuration, IDS will authenticate UCA users' login passwords with a configured LDAP server (in most deployments, an Active Directory server). The password can change on the ActiveDir server (for example, due to a password expiry policy). When this happens, UCA users should not be allowed to login with their old passwords, for the sake of security. To accomplish this, UCA server periodically validates passwords with IDS (which in turn validates it with the ActiveDir).  
In most cases there is no special configuration needed to use this feature. However, there are some parameters which can be tweaked if necessary. They are described in the following sections.  
When UCA detects that the password has changed on ActiveDir and the password previously entered by the UCA user is no longer valid, the user will be logged out of the UCA clients (if they are logged in at that time). The user will have to re-login with the new password.
- **How to enable UCA IDS Password monitoring**: The administrator does not need to do anything explicit to enable this. When UCA is operating in MAS-integrated mode, the monitoring will turn itself on.
- **ServerStatus**:
  - **Server Mode**: This field indicates whether UCA is operating in MAS-Colocated or

This server has accumulated 3 permanent/unrecoverable errors.

**Last Error:** 2012-02-16 10:01:18 : Server returned 401 Unauthorized. Your authentication credentials are incorrect.: Calstatus: 5ksystem(75b8c3a0-1dd2-11b2-9727-b06539393430) - Disabling this server due to unrecoverable error. Please update the configuration from server manager and try again.

MAS-Integrated mode. The password monitoring is disabled in Co-located mode, and only works in integrated mode.

- **Number of Subscribers being monitored:** Indicates how many UCA users' passwords are being monitored. All the users on the UCA system may not be monitored. Specifically, if a UCA user has never logged in through a UCA client, that user will not be monitored. Once the user logs in for the first time, monitoring will start for that user.
- **State of server:** Indicates whether the password monitoring is initializing or is fully up and running.
- **Last password validation occurred at:** Shows the timestamp of the last validation. This does not necessarily mean that the password was valid, but it is only the time when the validation attempt was made.
- **Configuration Parameter:** In most cases these parameters do not need to be changed and the default values work fine.
  - **Subscriber Load Retry Delay:** During the initialization phase of the password monitoring, if there are any errors in loading the subscribers, server will wait for some time and retry. This parameter controls the duration of that wait.
  - **MAS Mode Retry Delay:** UCA server checks periodically whether it is in integrated mode or not. This parameter controls how often UCA checks for the mode. The monitoring only starts when UCA is in integrated mode.
  - **Poll Loop Delay:** When in integrated mode, UCA server periodically checks whether any subscriber is eligible for password monitoring right now. This parameter controls how often that check is made.
  - **Password Validation Interval:** When in integrated mode, UCA server periodically validates each user's password. This parameter controls how often each user's password is validated. By default the parameter is set to 6 hours. That means once a user's password is changed in ActiveDir, within 6 hours (3 hours on average because the users are uniformly distributed in that time interval) the UCA will detect it and notify the user. The minimum parameter value is 4 hours (this is to prevent overloading the IDS and ActiveDir server with frequent requests) and maximum is 24 hours.
- **Last few Errors:** This section shows some errors that occurred in the past. Invalid user password is not an error condition. Errors are listed if there are any problems contacting the ActiveDir server and other such issues. For example, the following screenshot shows a MAS server that couldn't connect to the ActiveDir server to validate password. When errors like this occur, the UCA user's password is not immediately invalidated. UCA server will periodically keep retrying until it can successfully contact the ActiveDir server determine whether the password is correct or not.

#### Last Few Errors

© 2013-04-25 11:02:04.867: PasswordUpdateManager: Error authenticating user <>org.jboss.ws.core.WSTimeoutException: Timeout after: 15000ms

- **User Details:** This section shows the password monitoring details for a particular user. For troubleshooting, you can force the UCA server to immediately re-validate a user's password. To do this, enter the loginID and click "Validate User's password now". It can take about 10-30 seconds for ActiveDir to respond. After that time, click on "Show User Details" again to check whether user's password was valid or not. Once the user's

password is determined to be incorrect, all the logged in UCA clients for that user will be logged out. User will need to enter the new password and log back in.

## Reinitialize System

The **Reinitialize System** section of the Mitel UC Server Administration page provides a mechanism to default the system database.

---

### CAUTION

**Loss of Data:** Reinitializing the system defaults the system database, which deletes all of the values that you have configured for the system. Do not reinitialize the system unless you are instructed to do so by a Mitel Product Support Specialist. After you complete this task, you will need to reconfigure the entire system.

---

*To reinitialize the system:*

1. Click **Reinitialize Mitel UC Server Configuration**. A dialog box prompting you to confirm your actions appears.
2. Do one of the following:
  - Click **OK** to reinitialize the system. This may take several minutes to complete.
  - Click **Cancel** to cancel the action.

## Desktop Client Maintenance

This section describes how to install custom options, repair an installation, and uninstall the Desktop Client.

### Install Custom Options

During a typical installation of UC Advanced, the installer detects the PIMs that are installed on the user's computer and installs the associated extensions by default. However, in the case where a custom installation was performed and an extension was not installed, or in the case where a PIM was installed after UC Advanced was installed, UC Advanced prompts the user to install the PIM extension on startup. Users can install PIM extensions and other custom options using the Custom Install option available in the installation wizard.

Custom options include:

- **ACT! Integration:** Includes the ACT! PIM extension, which provides contact integration between ACT! and UC Advanced.
- **Dial from IE:** Allows users to dial an external number from Internet Explorer using UC Advanced.
- **Lotus Notes Integration:** Includes the Lotus Notes PIM extension, which provides contact integration between Lotus Notes and UC Advanced and provides dialing from Lotus Notes.

- **Outlook Extensions:** Includes the Outlook PIM extension, which provides contact integration between Outlook and UC Advanced and provides dialing from Outlook.
- **UCA Office Smart Tag:** Adds Smart Tags/Actions to Microsoft Office Applications, allowing users to dial external numbers from the applications using UC Advanced. Users must complete additional configuration in the application to enable Smart Tags/Actions.
- **Unified Communicator SDK:** The Software Development Kit (SDK) includes additional software and tools to integrate third-party applications with UC Advanced. This component is used strictly by Software Developers and typical UC Advanced users should not install it.

## NOTICE

The UC Advanced SDK is supported by the [Mitel Solutions Alliance \(MSA\) Developers and Integrators Program](http://www.mitel.com/DocController?documentId=9971) (<http://www.mitel.com/DocController?documentId=9971>).

For UC Advanced SDK technical support (requires Technical Support ID), contact the MSA program at [MSASupport@mitel.com](mailto:MSASupport@mitel.com) or one of the following numbers:

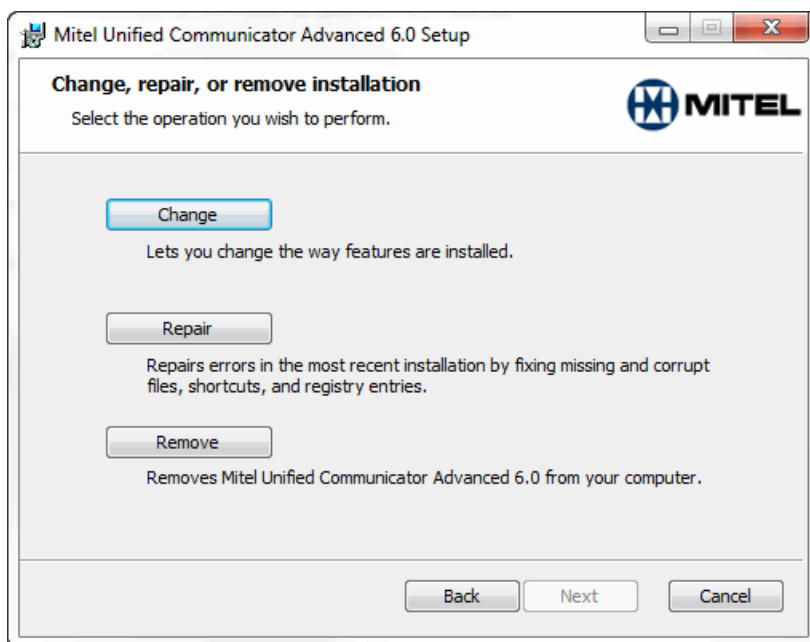
- North America: 1-800-267-6244 (8 a.m. to 5 p.m. Monday to Friday, EST)
- EMEA / AP: +44 (0) 1291 436888 (8 a.m. to 6 p.m. Monday to Friday GMT)

### *To install custom options for the UC Advanced Desktop Client:*

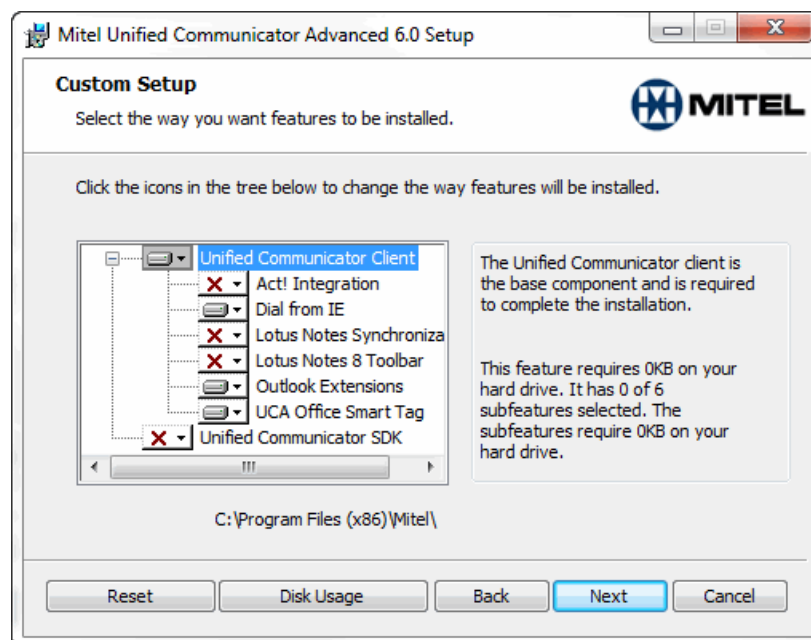
1. Exit the Desktop Client.
2. Close the user's PIM application, Internet Explorer, and all Microsoft Office applications.
3. Do one of the following:
  - For XP: Select Start – Control Panel – **Add or Remove Programs**.
  - For Vista/Windows 7: Select Start – Control Panel – **Programs and Features**.
4. Highlight Mitel Unified Communicator Advanced in the list of programs.
5. Click **Change**. The UC Advanced Installation Wizard Welcome screen appears.



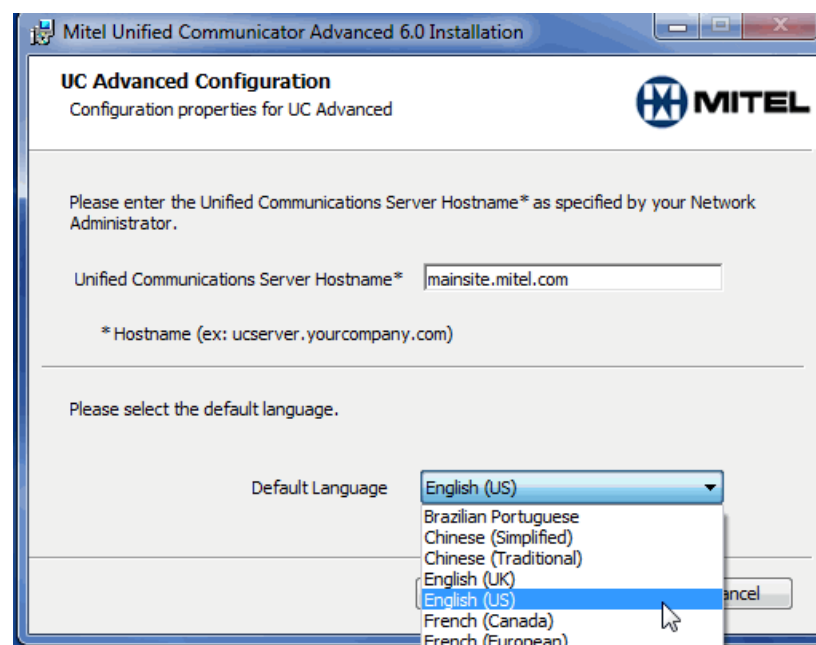
6. Click **Next**. The Change, Repair, and Remove options are displayed.



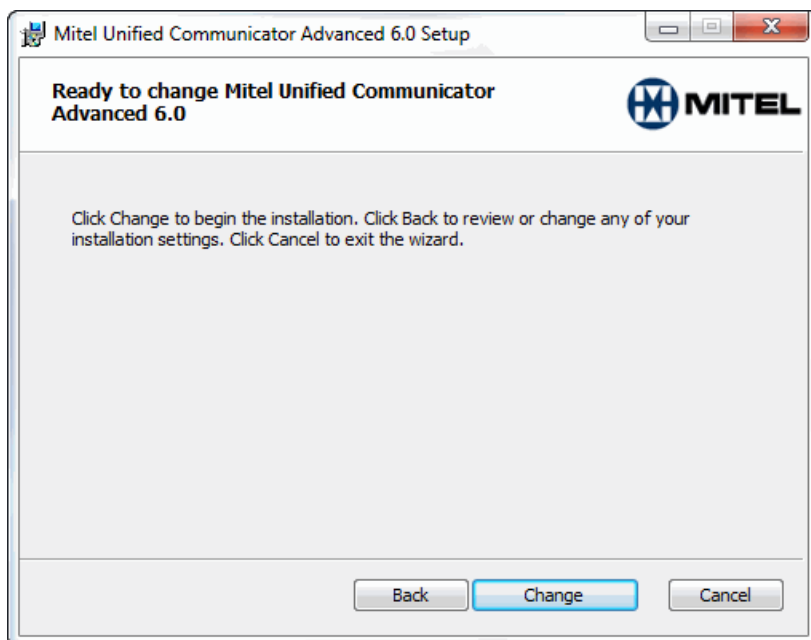
7. Click **Change**. The Custom Setup screen appears. A red **X** indicates that a component is currently not installed.



8. Do the following for each component you want to install:
  - Click the down arrow next to the uninstalled component.
  - Select **Will be installed on local hard drive**.
9. Click **Next**. The UC Advanced Configuration dialog box appears.

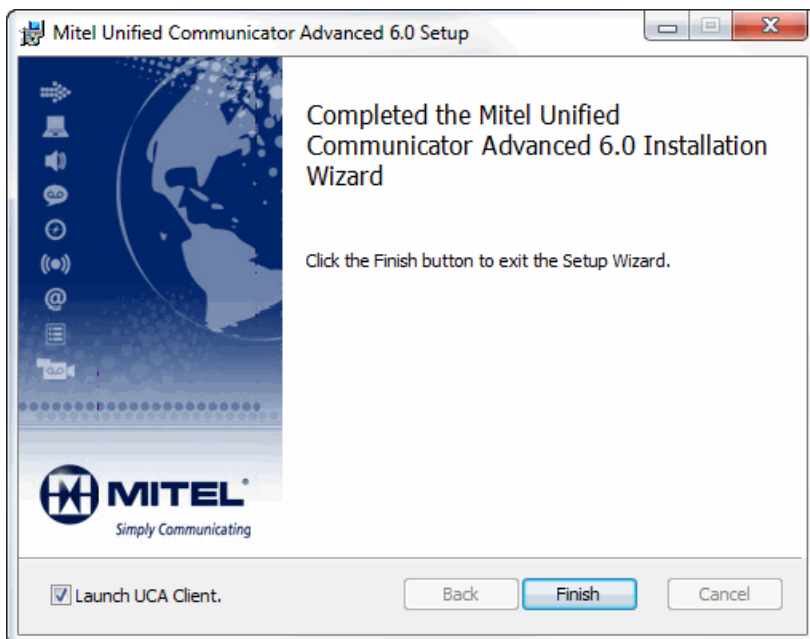


10. Verify that the Fully Qualified Domain Name field is accurate. The FQDN is provided in the Welcome E-mail message (see [page 125](#)).
11. Select a Default Language, and then click **Next**. The Ready to change dialog box appears.



12. Click **Change** to begin the installation. The components you selected are installed.

13. Click **Finish** to complete the installation process.



14. Do one of the following at the restart prompt:

- Click **Yes** to automatically restart your computer now.
- Click **No** if you want to restart your computer later.



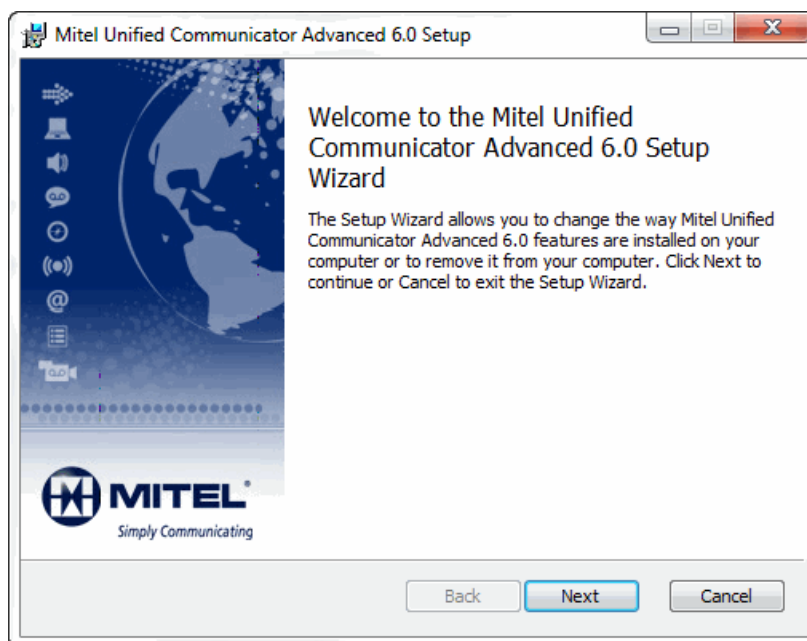
## Repair the Desktop Client

If the client installation becomes corrupt, a repair is required. Although this event is unlikely, it can occur if the user inadvertently deletes one or more application files.

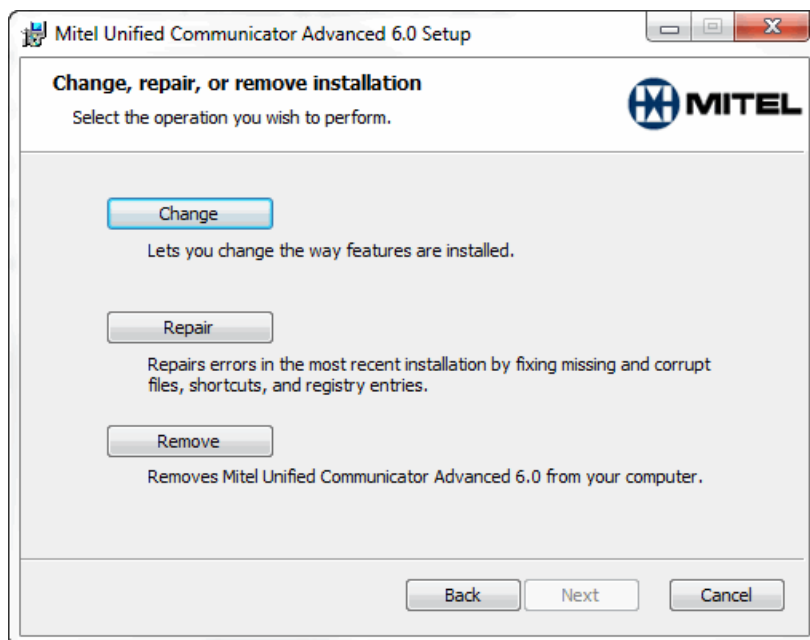
In addition, if you have contacted Mitel Technical Support regarding a problem, the support associate may request that you run a repair to ensure that the installation is valid before proceeding to diagnose an issue.

### *To repair the UC Advanced Desktop Client installation:*

1. Exit the Desktop Client.
2. Close the user's PIM application, Internet Explorer, and all Microsoft Office applications.
3. Do one of the following:
  - For XP: Select Start – Control Panel – **Add or Remove Programs**.
  - For Vista/Windows 7: Select Start – Control Panel – **Programs and Features**.
4. Highlight Mitel Unified Communicator Advanced in the list of programs.
5. Click **Change**. The UC Advanced Installation Wizard Welcome screen appears.



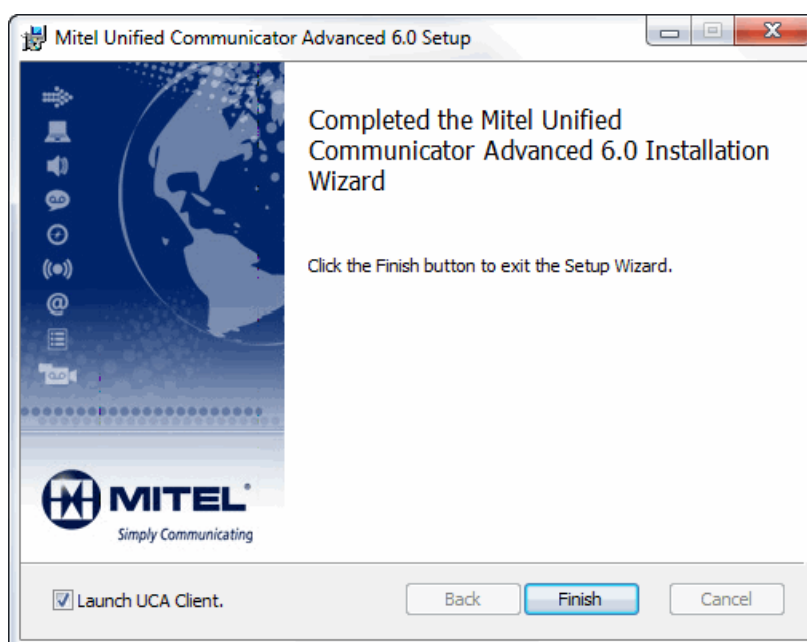
6. Click **Next**. The Change, Repair, and Remove options are displayed.



7. Click **Repair**. The Repair screen appears.



8. Click **Repair**. UC Advanced repairs the installation.
9. Click **Finish** to complete the installation process.



## Uninstall the Desktop Client

Although users can safely upgrade by installing the latest UC Advanced version, they may prefer to uninstall the previous version before installing the latest version.

To uninstall the Desktop Client, remove the application using the Windows **Add or Remove Programs** function.

User-specific files including configuration files, log files, license files, and databases, are not removed. To remove the older data, settings, and logs, rename or delete the following folders:

- Windows Vista/Windows 7/Windows 8
  - C:\Users\username\AppData\Roaming\Mitel\UC
  - C:\Users\username\AppData\Local\Mitel\UC
- Windows XP Pro
  - C:\Documents and Settings\username\Application Data\Mitel\UC
  - C:\Documents and Settings\<username>\Local Settings\Application Data\Mitel\UCA.exe<Windows generated folder name>\x.x.x.x



**Note:** The “Application Data” or “AppData” folders may be hidden by default in the system. To view these folders, click on ‘Show hidden files and folders’ from the Folder View Options menu in Windows.

## PBX Configuration Changes

This information applies to sites that have configured a PBX Node Synchronizer in the Unified Communications Administrator Interface to create UC Advanced accounts.

After you complete phone extension configuration changes (add, delete, move, change) on the PBX, perform a manual synchronization (click the **Sync Now** button on the Synchronization tab in the UC Server Administrator interface) to *immediately* update the affected UC Advanced accounts. If you do not perform a manual synchronization, the affected UC Advanced accounts will be updated at the next scheduled synchronization.

In addition, for those UC Advanced users whose extensions are affected by the configuration changes you make on the PBX, instruct the users to exit and then restart their UC Advanced Desktop Clients to refresh extension information.

# CHAPTER 6

## TROUBLESHOOTING



# Server Troubleshooting

This section provides troubleshooting information for the UC Server.

## Installation Problems

Table 26 [UC Advanced Installation Problems](#) provides troubleshooting information for server installation problems.

**Table 26: UC Advanced Installation Problems**

Problem or Error	Probable Cause	Corrective Action
The MSL server is showing the <b>Service Temporarily Unavailable</b> or <b>Bad Gateway</b> message when you are trying to install the Mitel Unified Communications Server.	This can occur if the status page is refreshed (reloaded) automatically at the same time that the Web server is restarted.	To clear the message, click the <b>Blades</b> link under ServiceLink.
The MSL server is showing the <b>Service Temporarily Unavailable</b> message when you are trying to provision the UC Server.	This may occur if the JBoss application server is starting at the same time that the configuration page is loaded (for example, if you click <b>Configure Mitel UC Server</b> immediately after the UC Server is configured or started).	Wait a couple of minutes and then try the request again.

## Server Synchronization Error Messages

This section provides error messages for the following situations:

- [UC Server Synchronization Messages](#) below
- [“AD/LDAP Synchronization Error Messages”](#) on page 224
- [“PBX Node Synchronization Error Messages”](#) on page 225
- [“Collaboration Server Synchronization Message”](#) on page 226

## UC Server Synchronization Messages

Table 27 [UC Server Synchronization Error Messages](#) lists the Unified Communications (UC) server error messages that may appear in the UC Server Administration interface during the synchronization process.

**Table 27: UC Server Synchronization Error Messages**

Error Message	Probable Cause	Corrective Action
System Busy.	System is in maintenance mode, or system in start up mode.	Wait until system is in service mode or wait until system is fully started.
License exceeded.	Exceeded customer purchased license feature.	Purchase additional license.
Too many primary aliases exists.	Too many aliases exists.	Remove user/account alias.
Invalid alias ID.	Alias ID is invalid.	Validate user/account alias.
Invalid voice mail system.	The provisioned VM is invalid.	Provision a valid VM system.
Authentication failed.	Invalid user name or password.	Try user's valid user name and password.
Password too short.	User's password is too short.	Change to a longer password.

## AD/LDAP Synchronization Error Messages

Table 28 [AD/LDAP Synchronization Error Messages](#) lists the AD/LDAP synchronization errors that may appear in the UC Server Administration interface when you complete this type of synchronization. The actual error message may vary depending on the LDAP server. Use the error messages below as guidelines.

**Table 28: AD/LDAP Synchronization Error Messages**

Error Message	Probable Cause	Corrective Action
Error establishing LDAP Context for url ldap://<ldap server IP>:<ldap port>.	Invalid LDAP URL (Wrong IP/Port, etc.).	From the UC Server administrator interface, set the correct LDAP url and try the synchronization again.
[LDAP: error code 32 - 0000208D: NameErr: DSID-031001CD, problem 2001 (NO_OBJECT), data 0, best match of: 'OU=EPMTest,DC=pvuc,DC=inter-tel,DC=com'].	Invalid LDAP search context.	From the UC Server administrator interface, either remove the search context or set the correct search context and try again.
Invalid User query - The error message varies based on the actual error in the user query.	LDAP user query is wrong.	From the UC Server administrator interface, either remove the user query or correct the user query and try the synchronization again.
Error establishing LDAP Context for url ldap://<ldap server IP>:<ldap port>: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 525, vece].	Invalid username/password.	From the UC Server administrator interface, set the correct username/password and try the synchronization again.



**Table 28: AD/LDAP Synchronization Error Messages (continued)**

Error Message	Probable Cause	Corrective Action
[LDAP: error code 12 - Unavailable Critical Extension]	The LDAP server does not support paged results and the Server <b>supports paging results</b> option is selected on the Synchronizer Details page in the UC Server Administrator interface.	Deselect the <b>Server supports paging results</b> flag on the Synchronizer Details page, save the change, and try the synchronization again.
Page 2 of 2		



**Note:** See “[AD/LDAP Synchronization Log File](#)” on page 232 for more information about the AD/LDAP Synchronization log file.

## PBX Node Synchronization Error Messages

Table 29 [PBX Node Synchronization Error Messages](#) lists the PBX node synchronization errors that may appear in the UC Server Administration interface when you complete this type of synchronization.

**Table 29: PBX Node Synchronization Error Messages**

Error Message	Probable Cause	Corrective Action
AuthData Sign failed.	UC Server security certificate is invalid.	Upgrade MCD and the UC Server to compatible versions.
Authenticate request failed.	Verify that the UC Server is compatible with MCD.	Upgrade MCD and the UC Server to compatible versions.
Authentication error.	Verify that the UC Server is compatible with MCD.	Upgrade MCD and the UC Server to compatible versions.
Invalid number of fields. NTuples failed.	MCD and the UC Server versions are incompatible.	Upgrade MCD and the UC Server to compatible versions.
Search first failed with invalid number of fields.	Verify that the UC Server is compatible with MCD.	Upgrade MCD and the UC Server to compatible versions.
Search next failed with invalid number of fields.	MCD became non-operational during sync.	Retry sync after 5 minutes.
Search NextTuples failed.	MCD became non-operational during sync.	Retry sync after 5 minutes.
Search NTuples failed.	MCD became non-operational during sync.	Retry sync after 5 minutes.
Server returned Error. NextNTuples failed.	MCD became non-operational during sync.	Retry sync after 5 minutes.
Server returned Error. NTuples failed.	MCD became non-operational during sync.	Retry sync after 5 minutes.
Server returned failure.	View the EPM logs to determine error code.	Corrective action based on the error code.
Soap client context setup error.	Internal UC Server error.	Restart the UC Server.
Page 1 of 2		

**Table 29: PBX Node Synchronization Error Messages (continued)**

Error Message	Probable Cause	Corrective Action
Soap login failed.	Node IP/Password is incorrect.	Set the correct IP/Password for the node and sync again.
Soap login rejected.	Node IP/Password is incorrect.	Set the correct IP/Password for the node and sync again.
Version request failed.	The UC Server is not compatible with MCD version.	Upgrade MCD and the UC Server to compatible versions.
Version fetch failed.	The UC Server is not compatible with MCD version.	Upgrade MCD and the UC Server to compatible versions.
DSM internal error.	UC Server internal error.	Capture the UC Server dsm.log and contact support.
Node not found.	The UC Server is not connected to 5k PBX.	Check the IP, Port and password set for the node. Correct the information and try the sync again.
INVALID Password.	The UC Server is not connected to 5k PBX.	Check the IP, Port and password set for the node. Correct the information and try the sync again.
Node connection terminated.	The UC Server connection to 5k got lost during sync.	Retry sync after 5k PBX becomes operational.
Connection not established.	The UC Server connection to 5k is not valid.	Retry sync after 5k PBX becomes operational.

Page 2 of 2

## Collaboration Server Synchronization Message

Table 30 [Collaboration Server Synchronization Error Message](#) lists the collaboration server error message that may appear in the UC Server Administration interface during a collaboration server synchronization.

**Table 30: Collaboration Server Synchronization Error Message**

Error Message	Probable Cause	Corrective Action
Unknown host exception.	This error message may appear in the UC Server Administrator interface on the Collaboration Server Details page when you click <b>Sync Now</b> . This error message indicates that the UC Server cannot resolve the hostname for the collaboration server.	Restart UC Server, and then attempt the synchronization with the collaboration server again.

## Alarms/Events

This section describes the Alarms/Events available from the **Event Viewer** option in the MSL Server Manager Administration menu (see [page 202](#)).

Alarms/Event include:

- [SIP Connection Event Messages](#) below
- “Presence Event Messages” on [page 228](#)
- “SIP Registrar Event Messages” on [page 228](#)
- “Watchdog Messages” on [page 229](#)

### SIP Connection Event Messages

Table 31 [SIP Connection Event Messages](#) provides information about SIP Connection Event Messages.

**Table 31: SIP Connection Event Messages**

Alarm/Event Description	Probable Cause	Corrective Action
Failed to create listen socket for IP/Host.	Unable to open a socket for the IP and port specified in the event.	Check if port specified is already in use.
Active SIP Connection of type [1] established with [IP port].	The Severity Cleared means the connection established with the specified IP/Port has been removed.	Either UC Client has closed the connection or could happen due to network issues.
Passive SIP Connection of type [1] established with [IP port].	The Severity Cleared means the connection established by the specified IP/Port has been removed.	Either UC Client has closed the connection or could happen due to network issues.
<number> connections received from <ip> in last second. Total connections <number>. Max Allowed Connections <number>.	The specified IP is trying to open more connections per second than allowed.	Check if the IP is trying to DNS attack. If it is a trusted node like MBG then add it in the trusted list on admin portal.
<number> connections were received from <ip>. Max Allowed Connections are <number>.	The specified IP is trying to establish more connections than allowed.	Check if IP is trying DNS attack. If it is a trusted node like MBG then add it in a trusted list on admin portal.

## Presence Event Messages

Table 32 [Presence Event Messages](#) provides information about Presence Event Messages.

**Table 32: Presence Event Messages**

Alarm/Event Description	Probable Cause	Corrective Action
Max. Session Limit Reached.	Total number of presence sessions allowed has reached the limit allowed in the UC Server.	Check the number of presence sessions using the Administrator interface. Shut down some UC Clients or restart ACCTPRES module/ softswitch if you believe that the number of UC Clients should be much smaller than reported.
Queue size has reached size <i>&lt;number&gt;</i> for Presence Notification Queue.	Total number of pending Notifications is exceeding the threshold.	The presence server gaps the notifications at some preconfigured rate in order to prevent server/client overload. Check CPU/IO usage and re-configure the gapping rate if needed. This event is not an error but just an indication of presence server load.
Rejecting SIP message.	Invalid SIP message was received.	Check the client that sent the message about validity of the SIP message.
Queue size has reached size <i>&lt;number&gt;</i> for <i>&lt;subscription&gt;</i> .	Total notification pending for a subscriptions are more than the subscriber can consume.	This can indicate a slow client or a large number of notifications for a specific subscription. This is just an indication and not an error condition.
Account Presence Subscription <i>&lt;subscription id&gt;</i> from <i>&lt;subscriber&gt;</i> to <i>&lt;presentity&gt;</i> terminated. Reason - <i>&lt;reason description&gt;</i>	UC Server's presence subscription was terminated for the reason specified.	This is a diagnostic alarm raised whenever the presence subscription is terminated on UC Server. It is used for troubleshooting presence issues on the server.

## SIP Registrar Event Messages

Table 33 [Registrar Event Messages](#) provides information about Registrar Event Messages.

**Table 33: Registrar Event Messages**

Alarm/Event Description	Probable Cause	Corrective Action
Registration for [ <i>&lt;account information&gt;</i> ] with resource [ <i>&lt;registration&gt;</i> ] from device [ <i>&lt;device&gt;</i> ] userAgent [ <i>&lt;user agent&gt;</i> ] callId [ <i>&lt;SIP call id&gt;</i> ] expired.	UC Client has shut down or network issues are occurring.	Restart the UC Client or check if network connectivity between the client and server is working.
Total [ <i>&lt;number&gt;</i> ] Registrations expired.	A specified number of registrations expired at the same time.	Check if there are any network issues occurring that may prevent clients from registering with the server.

## Watchdog Messages

Table 34 [Watchdog Messages](#) provides information about Watchdog Messages.

**Table 34: Watchdog Messages**

Alarm/Event Description	Probable Cause	Corrective Action
Congestion update from module DB_CHECK, congestion type cpu, congestion level 1, description cpu_yellow, details cpu_average.	UC Server has CPU congestion which is indicated by level of RED (85% cpu), ORANGE (70%), YELLOW (50%), GREEN (0%) in order of severity. The levels can be configured on the UC server manually if needed.	These notifications do not indicate a problem but rather load on the server, and are helpful when troubleshooting server issues.
Resource usage capacity exceeded for resource cpu, resource type cpu, resource description cpu_yellow, capacity <capacity %> .	The resource CPU has exceeded capacity (specified in alarm) utilization.	These notifications include pre-configured thresholds (50, 70, 85) raised by the server whenever the CPU exceeds the threshold. These notifications do not indicate a problem but rather load on the server, and are helpful when troubleshooting server issues.
Current server congestion level 2, description CONG_ORANGE, DebugLevel: 0, BlockProvisioning: 0, BlockSIPRegistration: 0, PercentInboundDrops: 0, PercentOutboundDrops: 0, reason cpu	UC Server has taken the specified actions on server congestion level specified in the alarm (for example, Debug level has been set to 0 (WARNING).	This alarm indicates that actions have been taken by UC Server based on the congestion level.

## MiTAI Error Codes

Table 35 [MiTAI Error Codes](#) provides troubleshooting information about MiTAI error codes. These error codes appear in the PBX\_Proxy log file (see [page 204](#)).

**Table 35: MiTAI Error Codes**

MiTAI Error Code	Description	Probable Cause
SXERR_DEVICE_ALREADY_MONITORED	An attempt was made to monitor the same device more than once.	UC Advanced has attempted to monitor the same device more than once. This error should be treated more as a warning.
SXERR_FEATURE_NOT_ALLOWED	A MiTAI call processing service invocation failed because the device was in a state in which the service could not be completed.	A switch configuration is preventing the completion of an operation on a call.
SXERR_INVALID_CALL_ID	The specified call-ID is not valid. The call-ID can change at the device before the application invokes a call manipulation routine or the call-ID was never valid.	A race condition.

Table 35: MiTAI Error Codes (continued)

MiTAI Error Code	Description	Probable Cause
SXERR_INVALID_PBX_HANDLE	An hPbxObject supplied to a MiTAI routine was not valid. The ICP was previously closed or never opened.	Internal UC Advanced error resulting from a race condition.
SXERR_INVALID_DN	A specified SX_DN is not valid.	UC Advanced is attempting to monitor an invalid extension. The extension no longer exists on the switch.
SXERR_NO_CALL_TO_CLEAR	A MiTAI call manipulation routine attempted to clear a call when none was present at the specified device.	A race condition occurred when both parties hung up at the same time.
SXERR_NO_CALL_TO_ANSWER	A MiTAI call manipulation routine attempted to answer a call. No active call existed, possibly because the call had cleared before the routine took effect.	A race condition occurred when the caller hung up at the same time the call was answered.
SXERR_PRIVILEGE_VIOLATION	The invoker of the MiTAI service does not have sufficient privileges.	UC Advanced is attempting to perform an operation that is not allowed by the device's class of service.
SXERR_UNSPECIFIED	An error of unknown origin.	A GPF occurred within the MiTAI library as a result of passing bad data to it. This is a UC Advanced internal error.
Page 2 of 2		

## Server Log Files

The following server log files are located in the `/opt/intertel/log` directory on the UC server and provide valuable information when diagnosing UC Advanced problems:

- **pbxProxy.log**: Provides MiTAI command and event related information for the MCD PBX.
- **Proxy5k.log** and **5kCmdEvts.log**: Provides OAI command and event related information for the Mitel 5000 PBX.
- **jboss.log**: Provides information for:
  - The UC Server Administrator interface
  - Web services for client presence status updates
  - MCA collaboration interaction
  - Web portal features
  - Call control commands received by the UC server from the desktop and Web clients
- **sipregistrar.log**: Provides information about SIP registration for the Desktop Client.
- **sipbaccountpresence.log**: Provides information for telephony and account presence features.
- **imevents.log**: Provides information for chat-related features.

- **proxy.log**: Contains the SIP messages sent from and received by UC Server.
- **rps.log**: Includes server side information related to peering such as which UC server connected and what information was requested.
- **rtc.log**: Includes peering related information on accounts synchronized from UC server that this UC Server connects to.
- **federationgw.log**: Includes log entries related to XMPP-based IM/Presence federation with third-party systems such as Microsoft OCS.
- **/var/log/prosody/prosody.log**: Includes the XMPP messages and other XMPP server details for IM/Presence federation with third party systems.

Log files can be viewed or downloaded from the server using the MSL Server Manager **View log files** function.

Logs in the `/opt/intertel/log` directory appear as `uc_server/<file name>` (for example, `uc_server/pbxProxy.log.1`).

### *To use the Server Manager View Log Files function:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, `https://<MSL_server_FQDN>/server-manager`) where the UC Server is installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. In the left navigation pane under Administration, click **View Log Files**.
4. Select a log file from the list provided by the **Choose a log file to view** field.

For information about MSL administrator tasks, refer to the MSL Server Manager online help or the MSL Installation and Administration Guide available on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>) for details and instructions.

For specific problems gather the log files noted below:

- For UC Server Administrator interface problems, review the `jboss.log*` file.
- For account synchronization problems, log files include:
  - `epm3300.log.*`
  - `adepm.log.*`
  - `dsm.log.*`
  - `jboss.log.*`
- For chat problems, log files include:
  - `sipims.log.*`
  - `imevents.log.*`
- For IM problems, log files include:
  - `imevents.log.*`
  - `proxy.log.*`

- For call, presence, and offline client problems, log files include:
  - pbxProxy.log.\* (MCD PBXs)
  - Proxy5k.log.\* (Mitel 5000 PBX)
  - 5kCmdEvts.log.\*(Mitel 5000 PBX)
  - sipbaccountpresence.log.\*
  - jboss.log.\*
  - acctpres.evts.\*
  - proxy.log.\*
  - sipregistrar.log.\*

\* Includes all log files with this file name.

## AD/LDAP Synchronization Log File

The AD/LDAP synchronization module is known as ADEpm. This module creates a log file named `adepm.log`, which can be used to debug AD/LDAP synchronization errors (see Table 28 on [page 224](#)).

*To access the `adepm.log` file:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, `https://<MSL_server_FQDN>/server-manager`) where the UC Server is installed. The server manager log in page appears.
2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. In the left navigation pane under Administration, click **View Log Files**.
4. Select `uc_server/adepm.log` from the **Choose a log file to view** list.
5. Click **Next**. Server Manager displays the `adepm.log` file.

The synchronization summary appears at the bottom of the `adepm.log` file between the SUMMARY BEGIN and SUMMARY END tags in the file and includes:

- “Domain Synchronization Summary” on [page 233](#)
- “Account Totals” on [page 234](#)





- **2 accounts were rejected because: PBX Node IP is not set.** This indicates that these 2 accounts did not have a valid PBX Node IP attribute populated and were therefore rejected (PBX Node IP is a mandatory parameter for AD/LDAP sync). This can happen because the field mapping is incorrect (pointing to an invalid LDAP attribute name) or the accounts did not have any value for that attribute.
- **Other Errors:** Describes other problems, which can be due to incorrect configuration or incorrectly populated account details on the LDAP server. For example, **14 accounts were rejected because: Neither Deskphone nor Softphone attributes are set.**
- **Account Names:** Lists the account names of the accounts in each category. This list allows you to focus on one account and examine why it was or was not rejected. For example, **Accounts for which PBX Node IP is not set: CN=John D. Smith|CN=John Doe|.**

```
Domain: california_branch :
2 accounts were sent for account creation
2 accounts were rejected because: PBX Node IP is not set.
14 accounts were rejected because: Neither Deskphone nor Softphone attributes are set.
0 accounts were rejected because: LDAP Guid is not set.
Account which were Successfully processed: CN=Fname Lname27,OU=3_2test|CN=Fname Lname28,OU=3_2test|
Accounts for which PBX Node IP is not set: CN=John D. Smith|CN=John Doe|
Accounts for which Neither Deskphone nor Softphone attributes are set: CN=Valid PhotoUser97|CN=Valid
Accounts for which LDAP Guid is not set:
```

**Figure 22: Domain Synchronization Summary Example**

## Account Totals

Account totals are displayed just before the SUMMARY END tag.

Account totals (see [Figure 23](#)) provide account counts for the various processing categories. Account totals should add up to the category counts from all the domains.

Account totals include the following information:

- **Accounts pulled from LDAP server:** This is the total number of accounts retrieved from the LDAP server. Currently, UC Advanced can retrieve a maximum of 9000 eligible accounts from the LDAP server. If the LDAP server contains more than 9000 eligible accounts, those accounts in excess of the 9000 account maximum will not be retrieved.

If no accounts were pulled from the LDAP server, one of the following may have occurred:

- The synchronizer configuration did not contain any eligible accounts. Note that an overly restrictive LDAP query can cause this.
- A synchronization error occurred. Synchronization errors are displayed at the top of the domain summary. For example:

```
Error: Error establishing LDAP Context for url
ldap://127.0.0.1:389/DC=test,DC=mitel,DC=com: [LDAP: error code 49 -
80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error,
data 52e, vece
```

- **Accounts sent for account creation:** This is the total number of accounts that should be created on UC Server if the synchronization is successful.

If you do not see this many accounts on your UC server, the following issues may be the cause:

- **Synchronization incomplete:** The synchronization process may not be complete yet. Refresh the Synchronization tab on the UC Server Administrator interface to show the status of the synchronization.
- **Insufficient licenses:** UC Server may not have a sufficient number of licenses available to create all of the accounts. View the `dsm.log.*` and `jboss.log.*` files for further details.
- **Incorrect PBX Node IP address:** Accounts may not have their PBX Node IP address set to one of the configured PBX Nodes in the UC Server Administrator interface.



UC Server does not convert IP addresses to hostnames and vice versa. For example, if the PBX Node has been configured as an IP address on UC Server, then the accounts being synchronized should also include an IP address in the PBX Node IP field. View the `dsm.log.*` file for further details.

- **Accounts rejected:** This is the total number of accounts that were rejected when the synchronization occurred due to invalid, missing, or incorrectly mapped LDAP attributes.

```
ACCOUNT TOTALS ACROSS ALL DOMAINS:
-----
23 Accounts were pulled from LDAP server
2 Accounts were sent for account creation
21 Accounts were rejected
```

Figure 23: Account Totals Example

## License and PBX Changes

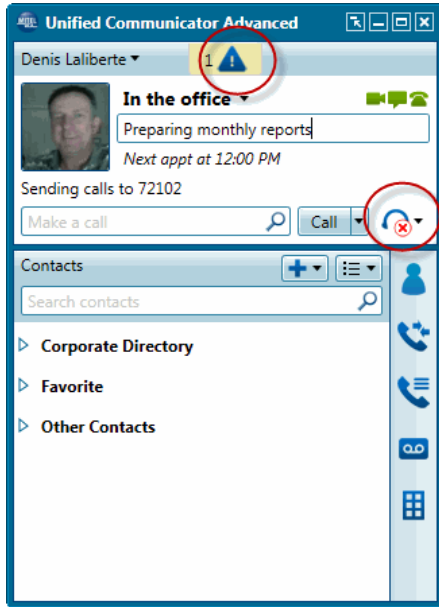
Follow these guidelines about which action to perform on the UC Server administrator interface for license and PBX changes. Refer to the online help for instructions.

- **Licensing changes:** Adding a licensed feature to your installation requires you to perform a synchronization with the AMC from the MSL Server Manager interface. After the license synch with AMC, you may have to wait up to 15 minutes for the `AMC_AGENT` module in UC server to update the UC server database with the license information. If after 15 minutes, it does not appear that the license is enabled, restart the UC Server.
- **Changing a Directory Number (DN) on the PBX:** Changing line configuration requires you to complete a line monitor refresh (MCD only) for the node using the Administrator interface. No restart is required.
- **Adding a DN on the PBX:** Adding a DN requires you to complete a manual synchronization for the PBX node if the DN needs to be pulled into the UC Server database. No restart is required.
- **Deleting an Existing DN:** Deleting a DN from the UC Server database requires you to complete a manual synchronization for the PBX node. No restart is required.
- **Changing Voice Mail:** Changing voice mail numbers does not require a UC Server restart.

## Account Reactivation Following License Changes

After making licensing changes to UC Advanced such as restoring a license or installing a license, you may need to reactivate accounts in the Unified Communications Administrator interface.

When a license is revoked, the user will be unable to use the feature or device in the Desktop Client. In the example in [Figure 24](#), the user's softphone license has been revoked, and the device is showing offline.



**Figure 24: Desk Phone and Softphone Offline**

To properly provision licensed features to UC Advanced users, you must do all of the following

- Verify UC Advanced licenses from the AMC (see [page 113](#)).
- Sync the UC Server with the AMC to update licenses (see [page 114](#)).
- Provision the features to users in the Unified Communications Administrator interface:
  - Create a Feature Profile by selecting the licensed features for the profile.
  - Assign the Feature Profile to accounts.

Refer to the UC Server Administrator interface online help for details.

The following procedure describes how to reactivate accounts after making licensing changes.

### *To reactivate licensed features:*

1. Open a Web browser and navigate to the MSL server manager URL (for example, [https://<MSL\\_server\\_FQDN>/server-manager](https://<MSL_server_FQDN>/server-manager)) where the UC Server is installed. The server manager log in page appears.

2. Log in to the MSL server manager interface. The **Welcome to the Server Manager** page appears.
3. Under ServiceLink, click **Status**. The ServiceLink Status Information page appears.

### ServiceLink Status Information

This web panel provides updated ServiceLink status information for this server. Status information is downloaded from the of the synchronization protocol.

The display includes information about your ServiceLink account, the latest synchronization event status, and a list of services subscribed. The display also includes the expiration date for each service and, if applicable, any error notice for that service.

If you wish to deactivate your ServiceLink account, please click [here](#).

Your service account ID is: **00160000**  
 Your descriptive server name is: **02**  
 The last sync completed successfully at: **Thu Dec 6 11:03:24 2012**

#### Current ServiceLink subscription listing

Service	Status	Expires	Messages
Unified Communicator	Subscribed	No expiry	None
Server activation and synchronization	Subscribed	No expiry	None

**Online sync disabled**  
 The process that automatically performs online sync operations with the AMC has been disabled. Online syncs are disabled generate an offline license request click Sync. To enable the automated online sync process check the box below and click Sync.

Enable automatic online sync: ☐

Mitel Standard Linux 10.0.29.0  
 Copyright 1999-2013 Mitel Corporation

4. Verify that the status and expiration for the Mitel UC Server subscription is valid and active.
5. Under Applications, click **Unified Communications Server**.
6. Click **Configure Mitel UC Server**.
7. Click the **Accounts** tab. The Accounts tab displays an Active column when at least one account is inactive.
8. Select the accounts to activate and click **Activate**.

**Mitel Standard Linux**

admin@xyzcompany.mitel.com
 Logout

**Applications**  
 Unified Communications Server

**ServiceLink**  
 Blades  
 Status

**Administration**  
 Backup  
 View log files  
 Event viewer  
 System information  
 System monitoring  
 System users  
 Shutdown or reconfigure

**Security**  
 Remote access  
 Local networks  
 Port forwarding  
 Web Server Certificate  
 Certificate Management

**Configuration**  
 Clustering  
 E-mail settings  
 DHCP

### Mitel Unified Communications Server Configuration

Enterprise
 Synchronization
 PBX Nodes
 **Accounts**
 Corporate Directory
 ACD Settings
 Collaboration
 Features
 Peering
 Federation

This page displays the list of accounts on the Mitel Unified Communications Server.

[\[Add Account\]](#)
[\[Delete Account\]](#)
[\[Send Welcome E-mail\]](#)
[\[Activate\]](#)

Accounts for: ucteam 1 - 1 of 1 (1 selected) Search accounts: 4321 Search Clear

Active	Type	PRG	Last Name	First Name	Desk Phone	Soft Phone	PBX Node
<input checked="" type="checkbox"/>	No	No	dragon	douled		4321	172.16.15.241

Refresh

9. When prompted to confirm the activation, click **OK**.

## Calendar Integration Troubleshooting

This section provides troubleshooting information for Calendar Integration on UCA.

### Failure to successfully connect to the Exchange Server

When configuring the Exchange server from the Enterprise Tab of the UCA Administration Tool, the following error can be encountered when testing the connection:

Invalid calendar server credentials

If this error is encountered, perform the following steps:

1. Re-enter the credentials and click the Test Connection button again to rule out spelling errors.
2. Ensure that no one in your organization has changed the password for the account being used for UCA-Exchange integration.
3. Verify that the IIS Webserver on the Exchange server has enabled at least one of Basic or Digest authentication mechanism. UCA server does not support NTLM authentication mechanism (also known as Windows Authentication) and will fail authentication if that is the only type of authentication enabled on Exchange server. To verify this, do the following:
  - a. PuTTY onto the UCA server and run the following command. **Replace the Exchange URL and user/password with one reflecting your configuration**. If you have enabled only digest authentication on the Exchange server, then change the `--basic` to `--digest` in the curl command options:

```
curl -v --insecure --basic -u 'administrator:password' -d ''  
https://exchange.mitel.com/ews/exchange.asmx
```

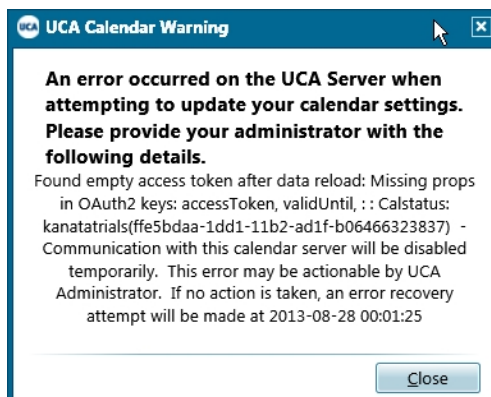
- b. This command should NOT return 401/403 response codes. If it does, then you may need to enable Basic/Digest authentication on the Exchange server. More specifically, look at the HTTP headers shown in the curl response. The WWW-Authenticate headers should contain Basic and/or Digest (for example, `WWW-Authenticate: Digest qop="auth",...` OR `WWW-Authenticate: Basic realm="10.101..."`). If the response has only NTLM header (such as `WWW-Authenticate: NTLM`), then your Exchange server is configured for only NTLM.
4. To enable Basic/Digest authentication (this applies for Windows Server 2003 R2 – your exact steps may vary):
    - a. Start IIS Manager: **Start -> All programs -> Administrative Tools -> Internet Information Services (IIS) Manager**.
    - b. Navigate to EWS: (**Local computer -> Web Sites -> Default Web Site -> EWS**).
    - c. Right click -> **Properties -> Directory Security -> Authentication and access control -> Edit**.
    - d. Check **Digest**, **Basic**, or both. **Apply** and **Save**.

- e. From the DOS prompt, enter: `iisreset.exe /RESTART`
- f. Attempt the **curl** command again. The curl command may show a 500 response, which is acceptable. It should not show a 401/403 response.

## Google calendar integration error after database backup and restore or MSL upgrade

When MSL is upgraded (or after database backup and restore), the Google OAuth2 tokens are lost (this is due to security reasons, so that the refresh token may not be read from a DB backup). Therefore, the Google OAuth2 configuration has to be redone. Until that configuration is complete, the UCA will disable Google calendar integration and will retry every 15 minutes (with default configuration) to re-read the OAuth2 tokens. When UCA tries to read the tokens and fails it raises an alarm and sends error notifications to UCA clients (to the effect that the access token is empty).

The UCA clients will receive these error popups (see below) every 15 minutes until the OAuth2 configuration is complete. To minimize this impact, you should re-configure OAuth2 as soon as the DB restore or MSL upgrade is done.



# Desktop Client Troubleshooting

This section provides troubleshooting information for the UC Advanced Desktop Client.

## Problem Reporting Tool

The Problem Reporting tool, available from the Desktop Client, allows users to create a problem report and send it to you. Users can access the tool from the Desktop Client main menu.

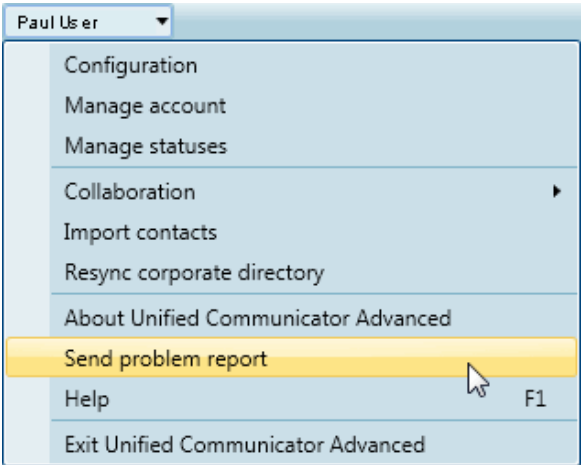


Figure 25: Desktop Client Send Problem Report Option

In addition, if an exception occurs that forces a client shut down, the error message generated includes the option to report the problem. This option is selected by default.

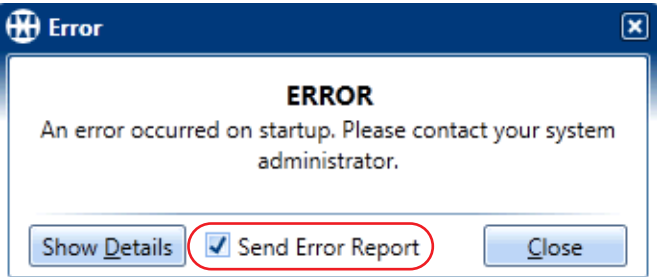


Figure 26: Desktop Client Error Message Example



The Problem Reporting Tool dialog box prompts the user to provide both a brief and detailed description of the problem.

**Figure 27: UC Advanced Problem Reporting Tool Description Dialog Box**

By default, the Desktop Client attaches the following compressed log files to the report:

- ucc.log.<sup>1</sup>
- SipSubscriber<sup>1</sup>
- uca.dmp (if available)
- SoftphoneManager.log

After the user sends the report, the log files sent by the Desktop Client are combined with server log files into a single ZIP file. You receive an e-mail message notifying you that a problem report has been generated, the name of the ZIP file, and the log files that are included. The e-mail message provides the descriptions that the user entered in the Problem Reporting Tool dialog box. An example of an e-mail message generated from a problem report is shown in Figure 28 on [page 242](#).



**Note:** The report is sent to the e-mail address configured in the MSL Server Manager interface under Configuration – E-mail settings – **Forwarding address for administrative e-mail** (see [page 110](#)). It is assumed that the UC Advanced administrator and the MSL administrator are the same person.

The compressed log file included with the report is stored on the UC Server in the `/var/log/feedback` directory. The file includes a timestamp that indicates when it was generated. The timestamp includes year, month, calendar date, hour, minute, and second.

1. Includes all logs with this file name (see [page 243](#)).

Client log files sent to the server can be retrieved using the MSL Server Manager **View log files** function (see [page 223](#)). After 30 days client log files are automatically deleted from the server.

For information about MSL administrator tasks, refer to the MSL Server Manager online help or the *MSL Installation and Administration Guide* available on the [Mitel eDocs](http://edocs.mitel.com) Web site (<http://edocs.mitel.com>) for details and instructions.

```
-----Original Message-----
From: Mitel Unified Communicator Advanced
[mailto:uca.no.reply@uca_server.xyzcompany.com]
Sent: Wednesday, February 24, 2010 4:38 PM
To: Administrator, Joe
Subject: Mitel@ Unified Communicator Advanced Problem Report Submission

A Mitel Unified Communicator Advanced user has submitted a problem report.

User ID: sally_user@Enterprise X.uca_server.xyzcompany.com

Product: Unified Communicator Advanced 4.0
Version: 4.0.16.0

Summary: Incoming call popup window did not close.

Description:
John from Sales called me and the Incoming call popup window appeared, but did not
close when I answered the call.

Files attached to the problem report:
feedback/20100224163806-sallyuser/ucc.log.gz
feedback/20100224163806-sallyuser/SipSubscriber.txt.gz
feedback/20100224163806-sallyuser/Softphonemanager.log.gz

Files attached to the problem report may be viewed and downloaded using the "View
log files" functionality provided by Server Manager.

Click the following link to access Server Manager:
https://uca_server.xyzcompany.com/server-manager/

-----
This notification is an automatically generated e-mail message.
Do not reply to this message.
```

**Figure 28: Problem Report Notification E-mail Example**

## Additional Client Log Files and Troubleshooting Tools

Table 36 [UC Advanced Client Log Files and Troubleshooting Tools](#) provides information about the UC Advanced client log files and troubleshooting tools.



The default installation directory for UC Advanced client varies for 32-bit vs. 64-bit operating systems:

- **32-bit:** C:\Program Files\Mitel\Unified Communicator Advanced 6.0
- **64-bit:** C:\Program Files (x86)\Mitel\Unified Communicator Advanced 6.0

Specific to Lync PlugIn client:

- **32-bit:** C:\Program Files\Mitel\LyncPlugIn
- **64-bit:** C:\Program Files (x86)\Mitel\LyncPlugIn

**Table 36: UC Advanced Client Log Files and Troubleshooting Tools**

Location	Log File/Tool	Description
<client installation directory>	 UCA.exe.config	Includes IP settings/ports for the UC Server, Collaboration server and telephony server of client. NHtraceswitch settings for logging.
<client installation directory>		Executable used to launch UC Advanced client application.
For Windows XP C:\Documents and Settings\<username>\Application Data\Mitel\UC For Windows Vista/Windows 7 C:\users\<username>\AppData\Roaming\Mitel\UC	uca.log <sup>1</sup>	Main log file for the Desktop Client.
	uc.mdb	Client database which contains call log, contacts, groups, and messenger IDs.
	user.config	user.config contains all persistent settings of the application, including configuration settings and UI layout settings. Deleting this file resets the Desktop Client to default settings.
	SipSubscriber.txt	Includes low level logging for the SIP component of UCA client.
	uca.dmp	A Microsoft mini-dump file, created if the client shuts down unexpectedly.
	SoftphoneManager.log	Provides logs for the Softphone process, which handles the softphone component of UC Advanced.

<sup>1</sup>. Includes all logs with this file name.

## Desktop Client Troubleshooting Table

Table 37 [Client Troubleshooting Issues](#) provides troubleshooting information for the Desktop Client.

**Table 37: Client Troubleshooting Issues**

Problem or Error	Probable Cause	Corrective Action
Users are experiencing difficulty with dialing rules.	To control how UC Advanced dials numbers, users should configure Windows dialing rules and use the International Dialing Format.	Instruct the user to refer to the <b>Phone Number Formats</b> topic in the Desktop Client help for additional information.
No phone devices are available.	UC Advanced cannot set a MiTAI monitor, or there is a firewall blocking or other network issue.	<p>Check the following:</p> <ul style="list-style-type: none"> <li>On MCD PBXs check system options to ensure "MiTAI TAPI computer" is set to <b>Yes</b>.</li> <li>Ensure MCD COS for the UC Advanced sets has "HCI" enabled.</li> <li>Ping the MCD PBX.</li> <li>Ping the desk phone.</li> <li>Does the desk phone have the same issue? (independent of UC Advanced)</li> <li>Is the problem local or remote? <ul style="list-style-type: none"> <li>Are VLAN's configured properly?</li> <li>Check VPN.</li> </ul> </li> <li>Is telephony service started? <ul style="list-style-type: none"> <li>Check telephony server logs for errors.</li> <li>Stop and restart telephony server service.</li> </ul> </li> <li>Use MiTAI test tool to verify if it is a MiTAI issue.</li> </ul> <p>If it fails check MCD programming.</p>
User joins a collaboration session as a participant rather than the leader when launched from UCA client. If they join the Web conference from the MCA interface, they are correctly joined as the leader.	MCA has LDAP enabled and LDAP sync is set. Users login name and username of the work e-mail address are set different then account on UCA.	Add the user work e-mail as the first e-mail address under contact information for that account.
Page 1 of 4		

**Table 37: Client Troubleshooting Issues (continued)**

Problem or Error	Probable Cause	Corrective Action
No presence, or client keeps changing from online to offline.	UC Advanced client or UC Server is not communicating with the presence server.	<p>Check the following:</p> <ul style="list-style-type: none"> <li>• Has the presence server service started?</li> <li>• Does the UC Server have a DNS entry?</li> <li>• Is the UC Server communicating with the Presence server on the correct port?</li> <li>• Is the telephony server working properly?</li> <li>• Is the UC Advanced client communicating with the Presence server?</li> <li>• Check uca.log and verify the ports.</li> <li>• UC Advanced client firewall blocking necessary ports.</li> <li>• Check Presence server log and see if it is updating.</li> <li>• Check telephony server logs to see if it keeps losing connectivity.</li> </ul>
Windows Live Messenger presence not displayed, but other forms of presence are available.	The Messenger installation has been corrupted.	Reinstall Windows Live Messenger.
The External Dial feature was removed from the user's account, but the click to call functionality is still enabled on the user's computer.	The External Dial feature was not completely removed from the account.	<p><b>To remove the External Dial feature (and disable click to call on the user's computer):</b></p> <ol style="list-style-type: none"> <li>1. Disable the External Dial feature in the user's account.</li> <li>2. Reinstall the client on the user's computer.</li> </ol>
"Failed to initialize VBox" message appears, interface locks up.	UC Advanced is conflicting with VBox. VBox is an anti-piracy / copy protection application that is included in a number of applications, including ACT!.	If you are using ACT!, ensure that it is fully licensed rather than using a trial version. If this error is occurring regardless of the status of your ACT! license, contact your software provider.
UC Advanced Desktop Client Interface fails to display completely or stops responding.	UC Advanced is running on a computer that has an out-of-date video driver.	Update the computer's video driver with a current version.
Page 2 of 4		

Table 37: Client Troubleshooting Issues (continued)

Problem or Error	Probable Cause	Corrective Action
Calls are not routing to the device specified for the Dynamic Status.	The user has enabled forwarding using the Phone Settings - <b>Forward my calls to</b> option, which overrides the normal routing specified in the Dynamic Status.	The options the user selects on the Phone Settings tab for the Dynamic Status (Add/Edit dialog box - More Options) override the routing specified in the <b>Send my calls to</b> field. Instruct users to specify call routing using the <b>Send my calls to</b> field and leave the fields in the Phone Settings tab blank.
	The proper COS options are not enabled for the device in the user's Personal Ring Group.	Verify that the proper COS options are enabled for devices in the user's Personal Ring Group.
The user cannot access voice mail messages from the Desktop Client's Visual Voice Mail view.	The user was accessing his or her voice mailbox using the Telephony User Interface (TUI) when he or she logged in to the Desktop Client and the Visual Voice Mail view failed to load.	Instruct the user to disconnect from his or her voice mailbox, exit the Desktop Client, and log back in to the Desktop Client.
The user's list of default Dynamic Statuses is deleted.	This problem occurs when an account created earlier (manually or via PBX or LDAP synchronization) is deleted and then recreated using any of the possible approaches.	Instruct the user to <a href="#">"Repair the Desktop Client"</a> on page 217 to re-establish the default list of Dynamic Statuses.
A remote UC Advanced user on the Mitel 5000 PBX sent or received an instant message, which caused the Desktop Client to go offline.	SIP Fixup is enabled in the firewall.	Disable SIP Fixup completely, or disable it for SIP messages sent to UC Server.
The user has selected an EHDU device for call routing from his or her Ring Group, but calls are not routing to the external number.	The external number is not logged into the EHDU.	Manually log the external number in or select "Permanent Login" from the Class of Service options.
The user is unable to upgrade the Desktop Client to a newer software version and also cannot uninstall the current version.	<ul style="list-style-type: none"> <li>There is a possible Microsoft Windows Installer issue on the user's PC.</li> <li>Windows Installer Service caches the location of the installer and uses that location when it upgrades to invoke the uninstall portion of the previous install. In this instance the previous installer is no longer available</li> </ul>	Use Add/Remove Programs from the control panel to uninstall the Desktop Client, and then install the client version. For additional information, refer to: <ul style="list-style-type: none"> <li>Mitel KB article <a href="#">4759</a></li> <li><a href="#">Microsoft KB article 2438651</a></li> </ul>
When the user tries the "Call me and play messages" function from the Visual Voice Mail view, nothing happens.	There is a possible configuration issue with the NuPoint UM application.	For all voice mail function to operate properly, UC Advanced requires certain parameters be configured for NuPoint UM. See <a href="#">"NuPoint UM Configuration"</a> on page 101 for details.
Page 3 of 4		

**Table 37: Client Troubleshooting Issues (continued)**

Problem or Error	Probable Cause	Corrective Action
You cannot establish a call using your SIP softphone on your Desktop Client in Teleworker mode even though your SIP softphone is registered.	Utilizing an unsupported router: D-Link DIR-615.	You should try a different router.
Desktop client unable to connect after uploading the new client software. Gets prompted to upgrade but will not connect.	Microsoft Video Network connection gets created when a USB camera is installed, and a new driver is applied which impacts our product to connect to the UCA server (UCA client picks an invalid IP connection).	Reboot the PC and Windows will remove this invalid video connection.
iPad SIP Softphone says it is connected after a steal from either Desktop or Android client	Timing related issue related to the GAP register feature on MBG.	The issue can be avoided by turning off the "Gap register" option on MBG.
Some of the Google contacts are not imported on the Desktop Client. Occurs after contacts are moved from the main corporate directory to a personal group.	Google send these contacts with no name when UCA imports it. Also see defect report against Google. <a href="http://code.google.com/a/google.com/p/apps-api-issues/issues/detail?id=3171">http://code.google.com/a/google.com/p/apps-api-issues/issues/detail?id=3171</a>	The workaround is to go to that group and re-enter or edit the name then it will import properly.
Page 4 of 4		

## Desktop Client Error and Warning Messages

This section provides common error and warning messages for the following situations:

- [Initialization Messages](#) below
- ["Configuration Change Messages"](#) on page 249
- ["Teleworker Setup Message"](#) on page 250
- ["File Sending Message"](#) on page 250
- ["ACD Messages"](#) on page 250
- ["PIM Integration Messages"](#) on page 251

## Initialization Messages

Table 38 [Initialization Messages](#) lists client initialization messages and their possible causes.

**Table 38: Initialization Messages**

Message	Possible Cause	Options
UC Advanced failed to connect to server <FQDN>. UC Advanced will start up in Offline mode. Do you wish to continue?	<ul style="list-style-type: none"> <li>The UC Server is not running.</li> <li>There is no route to the UC Server.</li> <li>UC Advanced cannot set a MiTAI monitor on the extension number.</li> <li>There may be a firewall/network/DNS issue or a PBX configuration problem.</li> <li>A remote user is trying to connect without configuring teleworker settings. Remote MCD users must configure teleworker settings after acknowledging this error.</li> </ul>	<ul style="list-style-type: none"> <li>Show Details</li> <li>OK</li> <li>Cancel</li> </ul>
There are no devices available (desk phone:<ext> or softphone <ext> on switch xxx.xxx.xxx.xxx). Would you like to work offline?	<ul style="list-style-type: none"> <li>The UC Server has not finished configuring the system.</li> <li>The telephony server is a MiTAI proxy from the UC Server to the MCD PBX. If the telephony server loses connectivity to the PBX then UC Advanced loses it's MiTAI monitor of the UC Advanced extension.</li> <li>A user does not have either a deskphone or softphone extension programmed in the UC Server.</li> </ul>	<ul style="list-style-type: none"> <li>OK</li> <li>Cancel</li> </ul>
UC Advanced failed to connect to the UC Server through the Teleworker Gateway. UC Advanced will startup in Offline mode. Do you wish to continue?	<ul style="list-style-type: none"> <li>The user ID was not found on the UC Server.</li> <li>There was a port issue between UC Advanced client or the UC Server and the teleworker gateway.</li> </ul>	<ul style="list-style-type: none"> <li>Show Details</li> <li>OK</li> <li>Cancel</li> </ul>
Irreconcilable discrepancy between the UC Advanced client's set of lines and the PBX's set of lines. Restart UC Advanced.	<ul style="list-style-type: none"> <li>Line changes have been made on the switch.</li> <li>UC Advanced and the PBX switch are out of synch. Restart the UC Server.</li> </ul>	OK
Your device appears to be out of service. Please contact your system administrator for assistance. Would you like to go to offline mode now? Click OK to continue to use UC Advanced in offline mode. Click Cancel to quit UC Advanced.	The desk phone is not plugged in.	<ul style="list-style-type: none"> <li>OK</li> <li>Cancel</li> </ul>



**Table 38: Initialization Messages (continued)**

Message	Possible Cause	Options
This is a Demo version of UC Advanced and will startup in Offline mode. For a fully licensed copy of UC Advanced, please contact your System Administrator. Do you wish to continue?	<ul style="list-style-type: none"> <li>If the UC Server is licensed (a license key has been applied) but the user trying to log in does not appear in the UC Server then they will receive this message and be able to login offline.</li> <li>The user logging in may be listed as an account on the UC Server, but doesn't have a UC Advanced base license assigned to it, will get this error and be able to log in using offline mode.</li> </ul>	<ul style="list-style-type: none"> <li>OK</li> <li>Cancel</li> </ul>
Your account is not licensed for desk phone or softphone. Please contact your system administrator. Would you like to work offline?	The user's account does not have both deskphone and softphone licensing.	<ul style="list-style-type: none"> <li>OK</li> <li>Cancel</li> </ul>
Page 2 of 2		

## Configuration Change Messages

Table 39 [Configuration Change Messages](#) provides configuration change warning messages and their possible causes.

**Table 39: Configuration Change Messages**

Message	Possible Cause	Options
Changes to the user interface language will not take effect until you restart UC Advanced.	This message is displayed when the language settings have been changed.	OK
There are changes made to the configuration of UC Advanced that have not been applied yet. Please choose what you would like to do with them.	This message is displayed when configuration changes have been made then the user cancels out of the configuration screen without saving or applying the changes.	<ul style="list-style-type: none"> <li>Apply</li> <li>Review</li> <li>Discard</li> </ul>

## Teleworker Setup Message

Table 40 [Teleworker Setup Message](#) provides a teleworker setup message.

**Table 40: Teleworker Setup Message**

Message	Possible Cause	Options
Directory number is not valid. Please type in the correct value and try again.	An invalid directory number was entered (non numeric) Resolution: Re-enter the directory number.	OK
Configuration file for SSL component is invalid.	The user was attempting to retrieve a certificate from the Desktop Client Configuration\Teleworker Settings dialog box when he or she received this message. This certificate error occasionally occurs after an upgrade from UC Advanced 2.0 or YA 5.0.  Instruct the user to restart the UC Advanced Desktop Client and try retrieving the certificate again.	OK

## File Sending Message

Table 41 [File Sending Message](#) provides a file sending message.

**Table 41: File Sending Message**

Message	Possible Cause	Options
The file or files you attempted to send exceed the maximum file transfer size of 10 megabytes.	While in the People view or chat window attempting to send a file over 10 megabytes to another UC user.	OK

## ACD Messages

Table 42 [ACD Messages](#) provides ACD errors and their possible causes.

**Table 42: ACD Messages**

Message	Possible Cause	Options
Either the agent does not exist, is already logged in elsewhere, or the phone you are monitoring is not configured for ACD. Press OK to return to UC Advanced.	<ul style="list-style-type: none"> <li>An incorrect Agent ID has been entered.</li> <li>Agent selected is already logged in elsewhere.</li> <li>Phone not configured for ACD.</li> </ul>	OK
The Agent ID is invalid. The Agent ID cannot be blank.	The agent Id has not been entered.	OK

## PIM Integration Messages

Table 43 [PIM Integration Messages](#) provides PIM integration messages and their possible causes.

**Table 43: PIM Integration Messages**

Message	Possible Cause	Options
Microsoft Outlook is running under another profile. Please restart this application under the default profile.	User selected some profile other than the default mail profile (set in the Windows Control Panel "Mail") when the PIM was started.	OK
UC Advanced is experiencing issues using Microsoft Outlook. Please make sure this application is working properly and try again.	The PIM is malfunctioning in an unspecified way.	OK
Please install and set up any of these supported applications before using this feature: <ul style="list-style-type: none"> <li>• Windows Address Book</li> <li>• Act</li> <li>• Microsoft Outlook</li> <li>• Lotus Notes</li> </ul>	User attempted to select PIM folders for importing or indexing contacts when no PIM was installed and configured.	OK
Microsoft Outlook is not responding. Please make sure this application is working properly and try again.	The PIM is not responding. Restart the PIM and then restart the Desktop Client.	OK
Microsoft Outlook appears to be unavailable. Please make sure this application is working properly and restart UC Advanced when convenient.	The PIM is not available. UC Advanced must be restarted when the PIM is working again.	OK

## Audio Problems

Table 44 [UC Advanced Audio Problems](#) provides client troubleshooting information audio problems.

**Table 44: UC Advanced Audio Problems**

Problem or Error	Probable Cause	Corrective Action
<p>When using a headset:</p> <ul style="list-style-type: none"> <li>MUTE button on the volume control of the headset turns on by itself, and will not turn off.</li> <li>Disconnecting and reconnecting the headset to the PC causes the system to freeze and require a power down and restart.</li> <li>Windows loses the connection to the USB headset. Windows no longer detects the headset.</li> <li>Loss of audio during a phone call, while the call window stays up.</li> <li>Answering or making a softphone call using, and experiencing no audio.</li> <li>Loud hissing, static or popping heard through the headset speakers.</li> <li>Windows loses the USB connection to the headset.</li> <li>UC Advanced no longer detects the USB headset. (Tools - Configuration - Handle Calls Using).</li> <li>UC Advanced automatically changes the audio devices for softphone calls to the PC sound card or another audio device.</li> </ul>	<p>The headset is defective or misconfigured on the PC.</p>	<p>Make sure that the USB headset connected to the UC Advanced client PC is functioning correctly.</p> <ul style="list-style-type: none"> <li>Ensure that Microsoft Windows is detecting the USB connected headset. (Windows - Hardware Devices).</li> <li>Verify with the headset manufacturer that the correct drivers and firmware have been installed for the Microsoft Operating System installed on the UC Advanced client PC.</li> <li>Check the headset manufacturer's Web site for white papers and support articles for related symptoms with the headsets. (i.e. Intermittent loss of audio, disconnects and reconnects causing system failure, etc.).</li> <li>Check the PC manufacturer's Web site for articles relating to USB device connectivity problems. (Root USB Controller vs. front USB ports, USB power distribution, etc.).</li> </ul> <p>Contact the USB headset vendor to ensure that the headsets are configured and operating as intended.</p> <p>Also see Supported Headsets and Handsets Table 21 on <a href="#">page 83</a>.</p>
<p>When using the softphone the call "breaks up" while using other programs.</p>	<p>Some Windows tasks run at elevated priorities, briefly preventing other applications from performing their own tasks.</p> <p>Windows Desktop tasks can run at the highest of priorities. A common problem is the animation used when minimizing and maximizing windows.</p> <p>This animation takes about 200 ms (1/5th of a second) and produces a noticeable break in a conversation.</p>	<p><b>To disable the animation in XP:</b></p> <ol style="list-style-type: none"> <li>In the Windows Control Panel, select <b>Performance and Maintenance</b>.</li> <li>Select <b>System Properties</b>.</li> <li>On the Advanced tab, click the Performance "Settings" button.</li> <li>Clear the "Animate windows when minimizing and maximizing" option in the Visual Effects tab.</li> </ol>

**Table 44: UC Advanced Audio Problems (continued)**

Problem or Error	Probable Cause	Corrective Action
One-way audio or no audio.	Firewall blocking or call path cannot route.	Check the gateway IP address. Is default gateway aware of all networks? <ul style="list-style-type: none"> <li>• In DMZ - NIC of external firewall.</li> <li>• Ensure firewall isn't blocking any necessary ports.</li> <li>• Is it a fully routable path?</li> </ul>
Active SIP softphone call on data network (cellular data network) is disconnected when switching to a WiFi connection.	3G/4G data and WiFi connections cannot operate simultaneously.	This is normal and unavoidable behavior.
Page 2 of 2		

## Video Problems

Table 45 [UC Advanced Video Problems](#) provides client troubleshooting information video problems.

**Table 45: UC Advanced Video Problems**

Problem or Error	Probable Cause	Corrective Action
When a UCA server A connected to 3300 MCD is peered with UCA server B connected to 5000 PBX, then users on UCA server A cannot escalate the SIP softphone audio call with another user on UCA server B, to video even though the call window shows the video button.	5000 PBX does not support SIP Video	

## Device Error

Table 46 [Device Errors](#) provides troubleshooting information for a device error.

**Table 46: Device Errors**

Error	Probable Cause	Corrective Action
The “P-Asserted-Identity <MCD IP Address>” error message appears on the 5610 SIP phone display when a call from the PBX rings in.	The “P-Asserted-Identity <MCD IP Address>” header is included in the SIP INVITE message to the 5610 phone.	None. Although this error message appears on the display, the user can still answer and complete the call attempt.

## MiVoice for Lync Troubleshooting

Table 47 [MiVoice for Lync Troubleshooting Issues](#) provides troubleshooting items for MiVoice for Lync (Lync PlugIn).

**Table 47: MiVoice for Lync Troubleshooting Issues**

Problem or Error	Probable Cause	Corrective Action
User can log in but is unable to use any of the MiVoice features, such as setting DND, Call Forward, calling operations, etc...	User account is not licensed properly.	From UC server, Accounts Tab go to Licensed Features and add Desk Phone and Softphone licenses to user's profile. MiVoice for Lync must have at least the Desktop Client SDK feature (see <a href="#">Table 1</a> ). Also need to restart the Lync client after making a change to licenses (MiVoice will automatically connect once the Lync client restarts).
Added custom attributes are not visible on MiVoice for Lync (Lync PlugIn).	Only the default telephone fields (like Home, Mobile, IP Phone and Work phone) which are visible to Lync Contact card by default will be visible to MiVoice for Lync.	This is normal behavior. Any field which is added via custom attribute in Active Directory or UC Server will not be visible to MiVoice for Lync.

## Web Portal Troubleshooting

Table 48 [Web Portal Troubleshooting Issue](#) provides troubleshooting items for the Web Portal.

**Table 48: Web Portal Troubleshooting Issue**

Problem or Error	Probable Cause	Corrective Action
Attempts to log in to the UC Advanced Web portal using the Safari Web browser fails in a crashed browser on iOS4 with an iPhone 3G.  When browsing with Safari to an untrusted site, you get the Cancel, Details, Continue options. Click <b>Continue</b> .	Safari is set to AutoFill and capture logins.	Turn off the Autofill setting in the Safari browser, and then try logging in again.  See " <a href="#">Web Portal Requirements</a> " on <a href="#">page 84</a> for a list of supported browsers.

# Android Device Troubleshooting

Table 49 [Android Troubleshooting Issues](#) provides troubleshooting items for Android devices.

**Table 49: Android Troubleshooting Issues**

Problem or Error	Probable Cause	Corrective Action
Incoming call to Android device may take up to 30 seconds before it starts ringing. Occurs after device is idle and has gone to sleep.	Advanced settings "Best Wi-Fi Performance" is unchecked (disabled).	Set or enable the advanced settings "Best Wi-Fi Performance".



# BlackBerry Device Troubleshooting

Table 50 [BlackBerry Device Troubleshooting Issue](#) provides troubleshooting items for BlackBerry devices.

**Table 50: BlackBerry Device Troubleshooting Issue**

Problem or Error	Probable Cause	Corrective Action
The user's BlackBerry device is displaying an HTTP 302 error when attempting to connect to the UC Server.	The Remote Proxy Services server (v2.0.4.0) is not properly formatting URLs passed from the BlackBerry device to the UC Server.	<p>Execute the following commands on the Remote Proxy Services server (not the UC Server) to resolve this issue:</p> <ol style="list-style-type: none"> <li>1. Open a secure shell session (for example, using PuTTY) to the Remote Proxy Services server, logging in as root.</li> <li>2. Type the following command on a single line and then press <b>Enter</b> at the end of the command:  <pre>db proxyapps setprop uca ForceTrailingSlash no</pre> <p>This command modifies the Remote Proxy Server configuration.</p> </li> <li>3. Type the following command on a single line and then press <b>Enter</b> at the end of the command:  <pre>signal-event proxyrules-update</pre> <p>This command applies the configuration changes.</p> </li> </ol>
The user's mobile client does not show real-time notifications.	The firewall or MBG server is not forwarding traffic on TCP port 36008 to the UC server.	Refer to section " <a href="#">Configure UC Advanced Mobile for Smart Devices</a> " on page 107.

## UCA Mobile for BlackBerry Secure Connections

The Use Secure Connection option is presented in the Setup Wizard after users download and install the UC Advanced Mobile for BlackBerry client application. It is also available from the Account Options screen.

To configure a secure connection to the UC Server from a BlackBerry mobile device, users are required to know the key store password on their device to accept the UC Server SSL certificate.

*To configure a secure connection to the UC Server:*

1. From the BlackBerry mobile device, enable the Use Secure Connection option from one of the following in the UC Advanced Mobile for BlackBerry client:
  - Setup wizard
  - Account Options screen

A dialog box appears prompting you to confirm that you want to configure a secure connection.

2. Select **Yes**.
3. Select **Test Connection**. The client application attempts to connect to the server using a secure connection. A dialog box informs you that the server's certificate is not trusted.
4. Select **Trust Certificate**. If you have never created a password for the key store on your device, you are prompted to enter one. If you have created a password for the key store, skip to [step 6](#).
5. Enter a key store password in the two boxes, and then select **OK**.
6. When prompted, enter your key store password to allow the client application access to your Handheld Key Store.



**Note:** Use a password that you will not forget. Entering an incorrect password 10 times will delete all personal data from the device and restore it to a default state.

7. When prompted, select **OK** to allow the client application access to your Trusted Key Store.



**Note:** A dialog box may appear indicating that the certificate could not be added to the Trusted Key Store. Select **OK** to dismiss the dialog box.

The Connection Successful message appears.

8. Press the BlackBerry End/Power key to return to the device's home page screen.

At this point, the UC Server's SSL certificate is in the device's key store. However, you must complete the following procedure to configure the certificate as trusted.

*To configure the UC Server's SSL certificate as trusted:*

1. Navigate to the BlackBerry device Options screen and select **Security Options**.
2. Select **Certificates** from the Security Options menu.
3. From the Certificates screen, scroll down the page to locate the UC Server certificate, as indicated by the UC Server Fully Qualified Domain Name (FQDN). The UC Server certificate will have a red X next to the FQDN indicating that the certificate is not trusted.
4. Highlight the UC Server certificate and press the BlackBerry Menu key.
5. Select **Trust**.
6. If you are prompted for your key store password again, enter it and select **OK**.
7. Return to the UC Advanced Mobile for BlackBerry application.
8. Exit the application and save the changes.
9. Open the application and go to the UC Mobile home screen.
10. Press the BlackBerry menu button, and then select **Update Status**.



**Note:** Entering an incorrect password 10 times will delete all personal data from the device and restore it to a default state.

## Access Point Name Settings

In order for the chat functionality to work properly on the UCA Mobile for BlackBerry application, you must ensure that the Access Point Name (APN) is set appropriately for your BlackBerry operating system.

For more information and instructions for setting these properly, refer to <http://btsc.webapps.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB05327>.

## Transport Layer Security Settings

In order for the chat functionality to work properly on the UCA Mobile for BlackBerry application, you must ensure that the Transport Layer Security (TLS) settings are correct for your BlackBerry operating system. Perform ONE of the following procedures:

1. Set the **Allow Untrusted HTTPS Connections** and **Allow Untrusted TLS Connections** to **True**.
  - For BlackBerry® Enterprise Server 4.1 or later, in BlackBerry Manager, select the BlackBerry® Mobile Data System Connection Service that is being used by the BlackBerry Client, and click **Edit Properties**.
  - For BlackBerry Enterprise Server 4.0 or earlier, in BlackBerry Manager, select the BlackBerry MDS that is being used by the BlackBerry Client, and click **Edit Properties**.
2. In the **Properties** column, click **TLS/HTTPS** and change the **Allow untrusted HTTPS** and **Allow untrusted TLS** connections settings to **True**.
3. Click **Apply**, and then click **OK**.
4. Restart the BlackBerry MDS or BlackBerry MDS Connection Service.



**Note:** Restarting certain BlackBerry Enterprise Server services delays email message delivery to BlackBerry devices.

**OR**

1. On the BlackBerry device, set the TLS Default option from **Proxy** to **Handheld**.

### **For BlackBerry® Device Software 4.0 to 4.7.x**

- a. On the Home screen of the device, click **Options > Security > TLS**.
- b. Click **TLS default** and select **Handheld**.
- c. Click **Prompt For Server Trust** and select **No**.
- d. Click **Prompt If Client Cert Not Found** and select **No**.
- e. Display the menu and select **Save**.

**For BlackBerry Device Software 5.0**

- a. From the Home screen of the device, click **Options > Security Options > Advanced Security Options**.
- b. Choose **TLS** and then set the TLS Default to **Handheld**.
- c. Set **Prompt For Server Trust** to **No**.
- d. Set **Prompt If Client Cert Not Found** to **No**.
- e. Display the menu and select **Save**.

**For BlackBerry Device Software 6.0**

- a. From the Home screen of the device, click **Options > Security > Advanced Security Settings**.
- b. Choose **TLS**.
- c. In the Proxy TLS section, set **Enabled turned off** (this means that handheld settings are used).
- d. Display the menu and select **Save**.

## UCA for VMware Horizon View Troubleshooting

Table 51 [UCA for VMware Horizon View Problems](#) describes troubleshooting procedures for issues that can arise when installing, configuring, and running UCA for VMware Horizon View.

**Table 51: UCA for VMware Horizon View Problems**

Issue	Probable Cause	Corrective Action
No audio or poor audio after connecting a USB headset.	The headset is selected for USB redirection.	Ensure that the headset is not enabled for USB redirection.
No audio or poor audio after connecting any type of headset.	RDP protocol is enabled for the virtual desktop.	Ensure PCoIP protocol is enabled.
Poor audio after connecting any type of headset.	Thin Client operating in Wireless mode.	Ensure Thin Client is operating in LAN Mode.
Unable to select Headset in the UCA Desktop Configuration/Softphone settings	The Thin / Thick Client physical endpoint does not have Headset set as the default Sound device.	Select Headset as the default Sound device on the physical endpoint device.

## MCA Collaboration Troubleshooting

Table 52 [MCA Collaboration Problems](#) provides MCA errors and their possible causes. After the user accesses the MCA Web pages, he or she can access troubleshooting information from the MCA online help.

**Table 52: MCA Collaboration Problems**

Problem or Error	Possible Cause	Corrective Action
Users cannot create or view conferences.	The MCA URL is not configured correctly on the UC Server Administrator interface.	<p>Determine the correct hostname of the MCA server and configure the URL on the Collaboration Server Details page in the UC Server Administration interface.</p> <p>To test the URL:</p> <ol style="list-style-type: none"> <li>1. From the UC Server Administrator interface, click the <b>Collaboration</b> tab.</li> <li>2. Copy the URL configured for the collaboration server.</li> <li>3. Paste the URL in a Web browser. The browser should show a page with links to the MCA User Portal and Server Manager.</li> </ol> <p>In most cases, the MCA URL should be of the form <code>http://&lt;awc-server-hostname&gt;</code>. The URL may also be <code>https</code>.</p>
	The MCA hostname is not resolvable from the UC Server or the address is unreachable.	<p>Verify that the nameserver specified in Server Manager for the UC Server contains an entry for the specified MCA server. You may need to specify that DNS resolution should be performed using "Corporate DNS servers" in the <b>Manage domains</b> page in Server Manager. See the MSL documentation for more information.</p>
	You have configured the wrong type of collaboration server for the enterprise in the UC Server Administrator interface.	<p>To configure MCA as the collaboration server:</p> <ol style="list-style-type: none"> <li>1. From the UC Server Administrator interface, click the <b>Enterprise</b> tab.</li> <li>2. Review the setting for the <b>Collaboration server type</b> field. If it is not configured as Mitel Audio and Web Conferencing, delete the enterprise and then re-create it using MCA as the collaboration server.</li> </ol>
Page 1 of 2		

**Table 52: MCA Collaboration Problems (continued)**

Problem or Error	Possible Cause	Corrective Action
The user says that the Collaboration menu is not available from the Desktop Client.	The user is not licensed for the Collaboration feature.	<p>To enable the Collaboration feature for the user:</p> <ol style="list-style-type: none"> <li>1. From the UC Server Administrator interface, click the <b>Accounts</b> tab.</li> <li>2. Locate the user and click the link to open the Account Details page for the user.</li> <li>3. Under <b>Licensed Features</b>, enable the Collaboration feature for the user.</li> <li>4. Instruct the user to restart the Desktop Client. The Collaboration menu is available.</li> </ol>
	When the account was created, the <b>Default Account Settings</b> on the Enterprise tab did not specify a collaboration server.	<p>To determine the Default Account Settings collaboration server setting:</p> <ol style="list-style-type: none"> <li>1. From the UC Server Administrator interface, click the <b>Enterprise</b> tab.</li> <li>2. Under <b>Default Account Settings</b>, if the collaboration server is set to <b>[None]</b>, then none of the accounts created in the enterprise will have collaboration server specified.</li> </ol> <p>To specify a collaboration server for an account:</p> <ol style="list-style-type: none"> <li>3. From the UC Server Administrator interface, click the <b>Accounts</b> tab.</li> <li>4. Locate the user and click the link to open the Account Details page for the user.</li> <li>5. Under <b>Account Settings</b>, select the appropriate server for the Collaboration server field.</li> <li>6. Instruct the user to restart the Desktop Client. The Collaboration menu is available.</li> </ol>
The user cannot join a Web conference or Audio and Web conference as the host or leader when initiating a conference from the Desktop Client.	The user did not enter his or her e-mail address when joining the conference.	<p>When the user starts a Web or Audio and Web conference from the Desktop Client, a Web browser opens to the MCA Join page.</p> <p>To join the conference as a participant, the user can type his or her name in the box (for example, Sally) and clicks <b>Join</b>.</p> <p>To join the conference as the host, the user must type his or her e-mail address in the box (for example, Sally_User@mitel.com) and clicks <b>Join</b>.</p>



GLOBAL HEADQUARTERS	U.S.	EMEA	CALA	ASIA PACIFIC
Tel: +1(613) 592-2122 Fax: +1(613) 592-4784	Tel: +1(480) 961-9000 Fax: +1(480) 961-1370	Tel: +44(0)1291-430000 Fax: +44(0)1291-430400	Tel: +1(613) 592-2122 Fax: +1(613) 592-7825	Tel: +61(0) 2 9023 9500 Fax: +61(0) 2 9023 9501

FOR MORE INFORMATION ON OUR WORLDWIDE OFFICE LOCATIONS, VISIT OUR WEBSITE AT [MITEL.COM/OFFICES](http://MITEL.COM/OFFICES)

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel to be accurate as of the date of its publication, is subject to change without notice. Mitel assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.

© Copyright 2012, Mitel Networks Corporation. All Rights Reserved.

[mitel.com](http://mitel.com)

