

Grandstream Networks, Inc.

UCM6510 IP PBX

User Manual



COPYRIGHT

©2017 Grandstream Networks, Inc. <http://www.grandstream.com>. All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this user manual is available for download here:

<http://www.grandstream.com/support>

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.

CAUTION

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

WARNING

Please do not use a different power adaptor with your devices as it may cause damage to the products and void the manufacturer warranty.



GNU GPL INFORMATION

UCM6510 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:

<http://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download>



Table of Content

DOCUMENT PURPOSE.....	23
CHANGE LOG	24
Firmware Version 1.0.14.24.....	24
Firmware Version 1.0.14.23.....	24
Firmware Version 1.0.14.21.....	24
Firmware Version 1.0.13.14.....	25
Firmware Version 1.0.12.19.....	25
Firmware Version 1.0.11.27.....	26
Firmware Version 1.0.10.44.....	27
Firmware Version 1.0.10.39.....	27
Firmware Version 1.0.2.7.....	28
Firmware Version 1.0.2.5.....	28
Firmware Version 1.0.1.12.....	29
Firmware Version 1.0.0.25.....	30
WELCOME	31
PRODUCT OVERVIEW.....	32
Feature Highlights	32
Technical Specifications	32
INSTALLATION	35
Equipment Packaging.....	35
Connect your UCM6510	35
Safety Compliances.....	37
Warranty	37
GETTING STARTED	38
Use The LCD Menu	38
Use The LED Indicators	40
Use The Web GUI	41
<i>Access Web GUI</i>	<i>41</i>
<i>Setup Wizard</i>	<i>42</i>
<i>Web GUI Configurations.....</i>	<i>43</i>
<i>Web GUI Languages</i>	<i>44</i>
<i>Save And Apply Changes.....</i>	<i>44</i>



Make Your First Call	45
SYSTEM SETTINGS	46
User Management	46
<i>User Information</i>	46
<i>Custom Privilege</i>	48
<i>Concurrent Multi-User Login</i>	50
<i>Operation Log</i>	50
Change Password	52
<i>Change Binding Email</i>	53
Network Settings	54
<i>Basic Settings</i>	54
<i>DHCP Client List</i>	59
<i>802.1X</i>	60
<i>Static Routes</i>	62
<i>Port Forwarding</i>	64
<i>OpenVPN</i>	66
<i>DDNS Settings</i>	67
Security Settings	69
<i>Static Defense</i>	70
<i>Dynamic Defense</i>	72
<i>Fail2ban</i>	73
<i>SSH Access</i>	75
LDAP Server	76
<i>LDAP Server Configurations</i>	77
<i>LDAP Phonebook</i>	78
<i>LDAP Client Configurations</i>	81
HTTP Server	83
Email	84
<i>Email Settings</i>	84
<i>Email Templates</i>	86
<i>Email Send Log</i>	87
Time Settings	89
<i>Auto Time Updating</i>	89
<i>Set Time Manually</i>	90
<i>Office Time</i>	91
<i>Holiday</i>	92
NTP Server	94
Recordings Storage	95
Login Settings	96
Google Service Settings Support	98



PROVISIONING	100
Overview.....	100
Configuration Architecture for End Point Device	100
Auto Provisioning Settings.....	101
Discovery	104
Global Configuration.....	106
<i>Global Policy</i>	106
<i>Global Templates</i>	114
Model Configuration	116
<i>Model Templates</i>	116
<i>Model Update</i>	118
Device Configuration	119
<i>Create New Device</i>	119
<i>Manage Devices</i>	120
Sample Application	126
EXTENSIONS.....	131
Create New User	131
<i>Create New SIP Extension</i>	131
<i>Create New IAX Extension</i>	139
<i>Create New FXS Extension</i>	143
Batch Add Extensions.....	149
<i>Batch Add SIP Extensions</i>	149
<i>Batch Add IAX Extensions</i>	152
Search and Edit Extension	154
Export Extensions.....	155
Import Extensions.....	156
E-mail Notification.....	163
Multiple Registrations per Extension	165
SMS Message Support.....	166
EXTENSION GROUPS.....	167
Configure Extension Groups	167
Use Extension Groups.....	168
ANALOG TRUNKS	169
Analog Trunks Configuration	169
PSTN Detection.....	172
DAHDI and Analog Hardware Configuration	175
DIGITAL TRUNKS	178



Digital Hardware Configuration	178
Digital Trunk Configuration	188
Direct Outward Dialing (DOD) via Digital Trunks	189
Digital Trunk Troubleshooting	189
DATA TRUNK.....	191
VOIP TRUNKS	193
VoIP Trunk Configuration.....	193
Direct Outward Dialing (DOD) via VoIP Trunks	203
SLA STATION	205
Create/Edit SLA Station	205
Sample Configuration	206
CALL ROUTES	208
Outbound Routes	208
<i>Configuring Outbound Routes</i>	208
<i>Outbound Blacklist</i>	211
<i>PIN Groups</i>	211
Inbound Routes	214
<i>Inbound Rule Configurations</i>	214
<i>Inbound Route: Prepend Example</i>	218
<i>Inbound Route: Multiple Mode</i>	219
<i>Fax Intelligent Route</i>	220
<i>Fax with Two Media</i>	220
<i>Blacklist Configurations</i>	220
CONFERENCE BRIDGE.....	222
<i>Conference Bridge Configurations</i>	222
<i>Join a Conference Call</i>	224
<i>Invite Other Parties to Join Conference</i>	224
<i>During The Conference</i>	225
<i>Record Conference</i>	227
CONFERENCE SCHEDULE	228
Conference Schedule Configuration	228
IVR	232
Configure IVR	232
Black/White List in IVR	235



Create Custom Prompt.....	237
LANGUAGE SETTINGS FOR VOICE PROMPT	238
Download and Install Voice Prompt Package.....	238
Customize Specific Prompt	240
VOICEMAIL.....	241
Configure Voicemail.....	241
Access Voicemail.....	243
Extension Voicemail Count.....	244
Voicemail Email Settings	245
Configure Voicemail Group.....	246
RING GROUP.....	247
Configure Ring Group.....	247
Remote Extension in Ring Group.....	249
PAGING AND INTERCOM GROUP	252
Configure Paging/Intercom Group.....	252
CALL QUEUE	254
Configure Call Queue	254
Call Center Settings & enhancements	258
Queue Statistics	260
Switchboard.....	261
PICKUP GROUPS.....	263
Configure Pickup Groups	263
Configure Pickup Feature Code	263
PIN GROUPS	265
MUSIC ON HOLD.....	267
FAX SERVER.....	270
Configure Fax/T.38	270
Receiving FAX	271
<i>Sample Configuration to Receive Fax from PSTN Line</i>	<i>271</i>
<i>Sample Configuration for Fax-To-Email</i>	<i>274</i>
Fax Sending	275
BUSY CAMP-ON.....	277



PRESENCE	278
FOLLOW ME	280
SPEED DIAL	283
DISA	284
CALLBACK	286
BLF AND EVENT LIST	288
BLF	288
Event List.....	288
DIAL BY NAME	291
Dial By Name Configuration	291
ACTIVE CALLS AND MONITOR	294
Active Calls Status.....	294
Hang Up Active Calls.....	296
Call Monitor	296
CALL FEATURES	298
Feature Codes.....	298
Call Recording	303
Call Park	303
<i>Park a Call</i>	303
<i>Retrieve Parked Call</i>	304
Enable Spy	304
PBX INTERNAL OPTIONS	305
PBX Settings/General.....	305
PBX Settings/Custom Prompt	307
<i>Record New Custom Prompt</i>	307
<i>Upload Custom Prompt</i>	308
<i>Download All Custom Prompt</i>	308
PBX Settings/Jitter Buffer	309
PBX Settings/RTP Settings	309
PBX Settings/Payload	310
IAX SETTINGS	311



IAX Settings/General	311
IAX Settings/Registration.....	311
IAX Settings/Security.....	312
SIP SETTINGS	313
SIP Settings/General	313
SIP Settings/Misc	313
SIP Settings/Session Timer	314
SIP Settings/TCP and TLS	315
SIP Settings/NAT	316
SIP Settings/TOS.....	316
Transparent Call-Info header.....	318
CTI SERVER	319
ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS).....	320
CRM INTEGRATION	321
SugarCRM.....	321
Salesforce CRM	322
PMS INTEGRATION.....	325
HMobile PMS Connector	325
Mitel PMS	326
Basic Settings	327
PMS Features.....	327
<i>Room Status</i>	327
<i>Wake Up Service</i>	329
<i>Mini Bar</i>	330
WAKEUP SERVICE	333
WakeUp Service using admin login.....	333
WakeUp service from User portal.....	334
WakeUp service using feature code.....	334
ANNOUNCEMENTS CENTER.....	335
Announcements Center Setting	335
Group Setting	336
STATUS AND REPORTING	339
PBX Status	339



<i>Trunks</i>	339
<i>Extensions</i>	341
<i>Interfaces Status</i>	342
System Status	344
<i>General</i>	344
<i>Network</i>	345
<i>Storage Usage</i>	345
<i>Resource Usage</i>	346
System Events	347
<i>Alert Events List</i>	347
<i>Alert Log</i>	349
<i>Alert Contact</i>	351
CDR	351
<i>CDR Improvement</i>	355
<i>Downloaded CDR File</i>	356
<i>Statistics</i>	357
<i>Recording Files</i>	359
<i>API Configuration Files</i>	359

USER PORTAL361

Basic Information	363
Personal Data	363
Value-added Features	363

MAINTENANCE364

Upgrading	364
<i>Upgrading via Network</i>	364
<i>Upgrading via Local Upload</i>	365
<i>No Local Firmware Servers</i>	367
Backup	367
<i>Backup/Restore</i>	367
<i>Data Sync</i>	369
<i>Restore Configuration from Backup File</i>	371
System Cleanup/Reset	372
<i>Reset and Reboot</i>	372
<i>Cleaner</i>	372
<i>USB/SD Card Files Cleanup</i>	374
Syslog	375
Network Troubleshooting	375
<i>Ethernet Capture</i>	375
<i>IP Ping</i>	376



<i>Traceroute</i>	377
Signaling Troubleshooting	377
<i>PRI/SS7/MFC/R2 Signaling Trace</i>	377
<i>Analog Record Trace</i>	378
<i>E&M Immediate Record Trace</i>	379
<i>Service Check</i>	380
<i>Network Status</i>	380
EXPERIENCING THE UCM6510 SERIES IP PBX	382



Table of Tables

Table 1: Technical Specifications	32
Table 2: UCM6510 Equipment Packaging	35
Table 3: LCD Menu Options	39
Table 4: UCM6510 LED Indicators	40
Table 5: User Management – Create New User	47
Table 6: Operation Log Column Header	51
Table 7: Change Binding Email option	54
Table 8: UCM6510 Network Settings→Basic Settings.....	54
Table 9: UCM6510 Network Settings→802.1X	62
Table 10: UCM6510 Network Settings→Static Routes	62
Table 11: UCM6510 Network Settings→Port Forwarding	64
Table 12: UCM6510 Settings→Network Settings→OpenVPN.....	66
Table 13: UCM6510 Security Settings→Static Defense→Current Service	70
Table 14: Typical Firewall Settings	70
Table 15: Firewall Rule Settings.....	71
Table 16: UCM6510 Firewall Dynamic Defense	72
Table 17: Fail2Ban Settings	75
Table 18: HTTP Server Settings.....	84
Table 19: Email Settings.....	84
Table 20: Email Log.....	88
Table 21: Auto Time Updating	89
Table 22: Create New Office Time	92
Table 23: Create New Holiday.....	93
Table 24: Auto Provision Settings	103
Table 25: Global Policy Parameters – Localization.....	107
Table 26: Global Policy Parameters – Phone Settings	108
Table 27: Global Policy Parameters – Contact List.....	109
Table 28: Global Policy Parameters – Maintenance	110
Table 29: Global Policy Parameters – Network Settings	112
Table 30: Global Policy Parameters – Customization	113
Table 31: Create New Template	114
Table 32: Create New Model Template	116
Table 33: SIP Extension Configuration Parameters – Basic Settings.....	132
Table 34: SIP Extension Configuration Parameters – Media	133
Table 35: SIP Extension Configuration Parameters – Features	135
Table 36: SIP Extension Configuration Parameters – Specific Time	139
Table 37: IAX Extension Configuration Parameters – Basic Settings.....	139
Table 38: IAX Extension Configuration Parameters – Media.....	140



Table 39: IAX Extension Configuration Parameters – Features	141
Table 40: IAX Extension Configuration Parameters – Specific Time	143
Table 41: FXS Extension Configuration Parameters – Basic Settings	144
Table 42: FXS Extension Configuration Parameters – Media.....	145
Table 43: FXS Extension Configuration Parameters – Features	146
Table 44: FXS Extension Configuration Parameters – Specific Time	148
Table 45: Batch Add SIP Extension Parameters.....	149
Table 46: Batch Add IAX Extension Parameters.....	152
Table 47: SIP Extensions Imported File Example	157
Table 48: IAX extensions Imported File Example	159
Table 49: FXS extensions Imported File Example	161
Table 50: Analog Trunk Configuration Parameters	169
Table 51: PSTN Detection for Analog Trunk	174
Table 52: Analog Hardware Configuration Parameters.....	176
Table 53: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE	179
Table 54: Digital Hardware Configuration Parameters: E1 - SS7	181
Table 55: Digital Hardware Configuration Parameters: E1 - MFC/R2	182
Table 56: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE.....	184
Table 57: Digital Hardware Configuration Parameters: T1/J1 - SS7.....	186
Table 58: Digital Hardware Configuration Parameters: T1-E&M Immediate/E&M Wink.....	187
Table 59: Digital Trunk Configuration Parameters	188
Table 60: Data Trunk Configuration Parameters.....	192
Table 61: Create New SIP Trunk.....	193
Table 62: SIP Register Trunk Configuration Parameters	194
Table 63: SIP Peer Trunk Configuration Parameters	198
Table 64: Create New IAX Trunk.....	201
Table 65: IAX Register Trunk Configuration Parameters	201
Table 66: IAX Peer Trunk Configuration Parameters	202
Table 67: SLA Station Configuration Parameters	205
Table 68: Outbound Route Configuration Parameters.....	208
Table 69: Outbound Routes/PIN Group	211
Table 70: Inbound Rule Configuration Parameters.....	214
Table 71: Conference Bridge Configuration Parameters	222
Table 72: Conference Settings	223
Table 73: Conference Caller IVR Menu	226
Table 74: Conference Schedule Parameters	228
Table 75: IVR Configuration Parameters	233
Table 76: Voicemail Settings	242
Table 77: Voicemail IVR Menu	243
Table 78: Voicemail Email Settings	245
Table 79: Voicemail Group Settings	246



Table 80: Ring Group Parameters	247
Table 81: Paging/Intercom Group Configuration Parameters	252
Table 82: Call Queue Configuration Parameters	254
Table 83: Call Center Parameters	259
Table 84: Switchboard Parameters	261
Table 85: PIN Group	265
Table 86: FAX/T.38 Settings	270
Table 87: SIP Presence Status	279
Table 88: Follow Me Settings	281
Table 89: Follow Me Options	282
Table 90: DISA Settings	284
Table 91: Callback Configuration Parameters	286
Table 92: Event List Settings	289
Table 93: UCM6510 Feature Codes	298
Table 94: PBX Settings /General	305
Table 95: Internal Options/Jitter Buffer	309
Table 96: Internal Options/RTP Settings	309
Table 97: Internal Options/Payload	310
Table 98: IAX Settings/General	311
Table 99: IAX Settings/Registration	311
Table 100: IAX Settings/Static Defense	312
Table 101: SIP Settings/General	313
Table 102: SIP Settings/Misc	313
Table 103: SIP Settings/Session Timer	314
Table 104: SIP Settings/TCP and TLS	315
Table 105: SIP Settings/NAT	316
Table 106: SIP Settings/ToS	316
Table 107: SugarCRM Settings	321
Table 108: Salesforce Settings	323
Table 109: PMS Supported Features	326
Table 110: PMS Basic Settings	327
Table 111: PMS Wake up Service	329
Table 112: Create New Mini Bar	330
Table 113: Create New Maid	331
Table 114: Wakeup Service	334
Table 115: Announcements Center Setting	335
Table 116: Group Setting	336
Table 117: Trunk Status	340
Table 118: Extension Status	341
Table 119: Interface Status Indicators	342
Table 120: System Status→General	344



Table 121: System Status→Network.....	345
Table 122: CDR Filter Criteria	351
Table 123: CDR Statistics Filter Criteria.....	358
Table 124: CDR API Configuration Files	359
Table 125: Network Upgrade Configuration	365
Table 126: Data Sync Configuration	370
Table 127: Cleaner Configuration	373
Table 128: USB/SD Card Files Cleanup	374
Table 129: Ethernet Capture	376



Table of Figures

Figure 1: UCM6510 Front View.....	35
Figure 2: UCM6510 Back View	35
Figure 3: UCM6510 T1/E1/J1 Crossover Cable Pin-out	36
Figure 4: UCM6510 Web GUI Login Page.....	41
Figure 5: Default Random Password	42
Figure 6: UCM6510 Setup Wizard	43
Figure 7: UCM6510 Web GUI Language	44
Figure 8: UCM6510 Web GUI: Apply Changes.....	44
Figure 9: User Management Page Display	46
Figure 10: Create New User	47
Figure 11: User Management – New Users	48
Figure 12: General User.....	49
Figure 13: Create New Custom Privilege.....	50
Figure 14: Multiple User Operation Error Prompt	50
Figure 15: Operation Logs	51
Figure 16: Operation Logs Filter	52
Figure 17: Change Password.....	53
Figure 18: Change Binding Email	53
Figure 19: UCM6510 Network Interface Method: Route.....	58
Figure 20: UCM6510 Network Interface Method: Switch.....	58
Figure 21: UCM6510 Network Interface Method: Dual	59
Figure 22: DHCP Client List	59
Figure 23: Add MAC Address Bind	60
Figure 24: Batch Add MAC Address Bind	60
Figure 25: UCM6510 Using 802.1X as Client.....	61
Figure 26: UCM6510 Using 802.1X EAP-MD5.....	61
Figure 27: UCM6510 Static Route Sample	63
Figure 28: UCM6510 Static Route Configuration.....	64
Figure 29: Create New Port Forwarding	65
Figure 30: UCM6510 Port Forwarding Configuration	65
Figure 31: GXP2160 Web Access Using UCM6510 Port Forwarding	66
Figure 32: OpenVPN feature on the UCM6510	67
Figure 33: Register Domain Name on noip.com.....	68
Figure 34: UCM6510 DDNS Setting	68
Figure 35: Using Domain Name to Connect to UCM6510	69
Figure 36: Create New Firewall Rule	71
Figure 37: Configure Dynamic Defense	73
Figure 38: Fail2ban Settings	74



Figure 39: SSH Access	76
Figure 40: LDAP Server Configurations.....	77
Figure 41: Default LDAP Phonebook DN.....	77
Figure 42: Default LDAP Phonebook Attributes.....	78
Figure 43: Add LDAP Phonebook	78
Figure 44: Edit LDAP Phonebook	79
Figure 45: Import Phonebook.....	79
Figure 46: Phonebook CSV File Format.....	80
Figure 47: LDAP Phonebook After Import.....	80
Figure 48: Export Selected LDAP Phonebook.....	81
Figure 49: LDAP Client Configurations	82
Figure 50: GXP2170 LDAP Phonebook Configuration	83
Figure 51: UCM6510 Email Settings.....	85
Figure 52: UCM6510 Email Settings: Send Test Email.....	86
Figure 53: Email Templates.....	86
Figure 54: Conference Schedule Template.....	87
Figure 55: Email Send log.....	88
Figure 56: Email Logs	89
Figure 57: Set Time Manually	90
Figure 58: Create New Office Time.....	91
Figure 59: System Settings→Time Settings→Office Time.....	92
Figure 60: Create New Holiday	93
Figure 61: System Settings→Time Settings→Holiday.....	94
Figure 62: PBX Settings→Recordings Storage	95
Figure 63: Recordings Storage Prompt Information	95
Figure 64: Recording Storage Category	96
Figure 65: Login Timeout Settings	97
Figure 66: Google Service Settings: OAuth2.0 Authentication	98
Figure 67: Google Service: New Project.....	98
Figure 68: Google Service: Create new credential	99
Figure 69: Google Service: OAuth2.0 login	99
Figure 70: Zero Config Configuration Architecture for End Point Device	101
Figure 71: UCM6510 Zero Config.....	102
Figure 72: Auto Provision Settings.....	103
Figure 73: Auto Discover.....	105
Figure 74: Discovered Devices	105
Figure 75: Managing Discovered Devices	106
Figure 76: Global Policy Categories	107
Figure 77: Edit Global Template.....	115
Figure 78: Edit Model Template	117
Figure 79: Template Management	118



Figure 80: Upload Model Template Manually.....	119
Figure 81: Create New Device	120
Figure 82: Manage Devices	120
Figure 83: Edit Device.....	121
Figure 84: Edit Customize Device Settings.....	122
Figure 85: Add P Value in Customize Device Settings	123
Figure 86: Modify Selected Devices—Same Model	124
Figure 87: Modify Selected Devices—Different Models.....	125
Figure 88: Device List in Zero Config.....	126
Figure 89: Zero Config Sample – Global Policy.....	127
Figure 90: Zero Config Sample – Device Preview 1	128
Figure 91: Zero Config Sample – Device Preview 2.....	129
Figure 92: Zero Config Sample – Device Preview 3.....	130
Figure 93: Create New Device	131
Figure 94: Manage Extensions	154
Figure 95: Export Extensions	155
Figure 96: Export Extensions	156
Figure 97: Import File	157
Figure 98: Import Error.....	163
Figure 99: E-mail Notification Prompt Information	163
Figure 100: E-mail Notification: Account Registration Information and QR Code	164
Figure 101: E-mail Notification LDAP Client Information and QR Code	164
Figure 102: Multiple Registrations per Extension	165
Figure 103: Extension - Concurrent Registration.....	165
Figure 104: SMS Message Support.....	166
Figure 105: Edit Extension Group.....	167
Figure 106: Select Extension Group in Outbound Route.....	168
Figure 107: UCM6510 FXO Tone Settings	172
Figure 108: UCM6510 PSTN Detection.....	172
Figure 109: UCM6510 PSTN Detection: Auto Detect	173
Figure 110: UCM6510 PSTN Detection: Semi-Auto Detect.....	173
Figure 111: FXS Ports Signaling Preference	175
Figure 112: FXO Ports ACIM Settings	175
Figure 113: Dahdi Settings.....	177
Figure 114: Digital Hardware Configuration	178
Figure 115: Troubleshooting Digital Trunks.....	190
Figure 116: Data Trunk Web Page.....	191
Figure 117: Data Trunk Configuration	191
Figure 118: DOD extension selection	204
Figure 119: Edit DOD	204
Figure 120: SLA Station	205



Figure 121: Enable SLA Mode for Analog Trunk.....	206
Figure 122: Analog Trunk with SLA Mode Enabled	206
Figure 123: SLA Example - SLA Station	207
Figure 124: SLA Example - MPK Configuration.....	207
Figure 125: Create New PIN Group	212
Figure 126: PIN members	212
Figure 127: Outbound PIN	213
Figure 128: CDR Record.....	213
Figure 129: Country Codes	214
Figure 130: Inbound Route feature: Prepend	218
Figure 131: Inbound Route - Multiple Mode.....	219
Figure 132: Blacklist Configuration Parameters.....	221
Figure 133: Blacklist csv File.....	221
Figure 134: Conference	224
Figure 135: Conference Invitation From Web GUI.....	225
Figure 136: Conference Recording	227
Figure 137: Conference Schedule	231
Figure 138: Create New IVR.....	232
Figure 139: Key Pressing Events.....	235
Figure 140: Black/White List	236
Figure 141: Click on Prompt to Create IVR Prompt.....	237
Figure 142: Language Settings for Voice Prompt	239
Figure 143: Voice Prompt Package List.....	239
Figure 144: New Voice Prompt Language Added.....	240
Figure 145: Upload Single Voice Prompt for Entire Language Pack	240
Figure 146: Voicemail Settings.....	241
Figure 147: Voicemail Count.....	244
Figure 148: Voicemail Email Settings	245
Figure 149: Voicemail Group.....	246
Figure 150: Ring Group.....	247
Figure 151: Ring Group Configuration	249
Figure 152: Sync LDAP Server option	250
Figure 153: Manually Sync LDAP Server	251
Figure 154: Ring Group Remote Extension	251
Figure 155: Paging/Intercom Group.....	252
Figure 156: Page/Intercom Group Settings	253
Figure 157: Call Queue	254
Figure 158: Static Agents limitation.....	257
Figure 159: Agent Login Settings.....	258
Figure 160: Call Queue Statistics	260
Figure 161: Call Queue Switchboard	261



Figure 162: Edit Pickup Group	263
Figure 163: Edit Pickup Feature Code	264
Figure 164: Create New PIN Group	265
Figure 165: PIN members	266
Figure 166: Outbound PIN	266
Figure 167: CDR Record.....	266
Figure 168: Music On Hold Default Class	267
Figure 169: Play Custom Prompt.....	268
Figure 170: Information Prompt	268
Figure 171: Record Custom Prompt	269
Figure 172: Fax Settings	270
Figure 173: Configure Analog Trunk without Fax Detection	272
Figure 174: Configure Extension For Fax Machine	273
Figure 175: Configure Extension for Fax Machine: Analog Settings	273
Figure 176: Configure Inbound Rule for Fax.....	274
Figure 177: Create Fax Extension	274
Figure 178: Inbound Route to Fax Extension	275
Figure 179: Fax Sending in Web GUI	276
Figure 180: SIP Presence Configuration	278
Figure 181: SIP Presence Feature Code	279
Figure 182: Edit Follow Me	280
Figure 183: Speed Dial Destinations	283
Figure 184: Create New DISA.....	284
Figure 185: Create New Event List	289
Figure 186: Create Dial By Name Group	291
Figure 187: Configure Extension First Name and Last Name	292
Figure 188: Dial By Name Group In IVR Key Pressing Events	293
Figure 189: Dial By Name Group In Inbound Rule	293
Figure 190: Status→PBX Status→Active Calls - Ringing.....	294
Figure 191: Status→PBX Status→Active Calls – Call Established	294
Figure 192: call connection less than half hour.....	295
Figure 193: call connection between half an hour and one hour	295
Figure 194: call connection more than one hour.....	296
Figure 195: Configure to Monitor an Active Call	296
Figure 196: Enable/Disable Feature codes.....	302
Figure 197: Download Recording File from CDR Page	303
Figure 198: Record New IVR Prompt	307
Figure 199: Upload IVR Prompt.....	308
Figure 200: Download All Custom Prompt.....	308
Figure 201: Transparent Call-Info	318
Figure 202: CTI Server Listening port.....	319



Figure 203: SugarCRM Basic Settings	321
Figure 204: CRM User Settings	322
Figure 205: Salesforce Basic Settings	323
Figure 206: Salesforce User Settings	324
Figure 207: UCM & PMS interaction	325
Figure 208: UCM & PMS interaction	326
Figure 209: Create New Room	328
Figure 210: Room Status	328
Figure 211: Add batch rooms	329
Figure 212: Create New Wake Up Service	329
Figure 213: Wakeup Call executed	330
Figure 214: Create New Mini Bar	330
Figure 215: Create New Maid	331
Figure 216: Create New Consumer Goods.....	331
Figure 217: Mini Bar	332
Figure 218: Create New Wakeup Service	333
Figure 219: Wakeup Service Feature Code.....	334
Figure 220: Announcements Center	335
Figure 221: Announcements Center Group Configuration.....	337
Figure 222: Announcements Center Code Configuration	337
Figure 223: Announcements Center example.....	338
Figure 224: Status→PBX Status	339
Figure 225: Trunk Status	340
Figure 226: Extension Status	341
Figure 227: System Status→Storage Usage	346
Figure 228: System Status→Resource Usage	346
Figure 229: System Events→Alert Events Lists: Disk Usage	347
Figure 230: System Events→Alert Events Lists: External Disk Usage.....	348
Figure 231: System Events→Alert Events Lists: Memory Usage	348
Figure 232: System Events→Alert Events Lists: System Crash.....	349
Figure 233: System Events→Alert Log	349
Figure 234: System Events→Alert Log	350
Figure 235: Filter for Alert Log	350
Figure 236: CDR Filter	351
Figure 237: Call Report	353
Figure 238: Call Report Entry with Audio Recording File.....	355
Figure 239: Automatic Download Settings	355
Figure 240: CDR Report	356
Figure 241: Detailed CDR Information.....	356
Figure 242: Downloaded CDR File Sample	356
Figure 243: Downloaded CDR File Sample - Source Channel and Dest Channel 1	357



Figure 244: Downloaded CDR File Sample - Source Channel and Dest Channel 2.....	357
Figure 245: CDR Statistics.....	358
Figure 246: CDR→Recording Files.....	359
Figure 247: Edit User Information by Super Admin	361
Figure 248: User Portal Login	362
Figure 249: User Portal Layout	362
Figure 250: Network Upgrade.....	364
Figure 251: Local Upgrade.....	365
Figure 252: Upgrading Firmware Files.....	366
Figure 253: Reboot UCM6510	366
Figure 254: Create New Backup.....	368
Figure 255: Backup / Restore	368
Figure 256: Local Backup	369
Figure 257: Data Sync	370
Figure 258: Restore UCM6510 from Backup File.....	371
Figure 259: Reset and Reboot.....	372
Figure 260: Cleaner	373
Figure 261: USB/SD Card Files Cleanup.....	374
Figure 262: Ethernet Capture.....	376
Figure 263: PING	377
Figure 264: Traceroute.....	377
Figure 265: Troubleshooting Analog Trunks	378
Figure 266: A Key Dial-up FXO.....	379
Figure 267: E&M Immediate Record Trace.....	380
Figure 268: Service Check.....	380
Figure 269: Network Status.....	381



DOCUMENT PURPOSE

This document describes UCM6510 IP PBX specifications, features and will help you to configure your system via Web GUI menu to fully manipulate the supported features. The intended audiences of this document are device administrators. To learn more about UCM6510 IP PBX features, please visit <http://www.grandstream.com/support> to download available how-to guides.

This guide covers following topics:

- [Product overview](#)
- [Installation](#)
- [Getting started](#)
- [System settings](#)
- [Provisioning](#)
- [Extensions](#)
- [Analog trunks](#)
- [Digital trunks](#)
- [Data trunk](#)
- [VoIP trunks](#)
- [SLA station](#)
- [Call routes](#)
- [Conference bridge](#)
- [Conference schedule](#)
- [IVR](#)
- [Language settings for voice prompt](#)
- [Voicemail](#)
- [Ring group](#)
- [Paging and intercom group](#)
- [Call queue](#)
- [Pickup groups](#)
- [PIN Groups](#)
- [Music on hold](#)
- [Fax Server](#)
- [Busy camp-on](#)
- [Presence](#)
- [Follow me](#)
- [Speed Dial](#)
- [DISA](#)
- [Callback](#)
- [BLF and event list](#)
- [Dial by name](#)
- [Active calls and monitor](#)
- [Call features](#)
- [Call recording](#)
- [CTI Server](#)
- [Asterisk manager interface \(AMI\)](#)
- [CRM integration](#)
- [PMS integration](#)
- [Wakeup service](#)
- [Announcements center](#)
- [Status and reporting](#)
- [CDR \(Call Details Record\)](#)
- [User Portal](#)
- [Upgrading and maintenance](#)
- [Backup/restore](#)
- [Troubleshooting](#)



CHANGE LOG

This section documents significant changes from previous versions of the UCM6510 user manual. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.14.24

- Added protection to prevent HTTP rogue login.

Firmware Version 1.0.14.23

- Restored ability to view voicemail count in the Extension/Trunk overview. [Extension Voicemail Count]
- Restored the ability to set custom numbers for call forwarding settings. [Call Forward Unconditional] [Call Forward No Answer] [Call Forward Busy]
- Restored previous format for entering multiple dial plans (one pattern per line) for inbound/outbound rules. [Pattern] [Pattern]
- Restored Zero Config's sorting by column and introduced a search bar. [Managing discovered devices]

Firmware Version 1.0.14.21

- Implementing a new Web GUI consistent operating style which can display and update the system's status in real time.
- Added support for SIP Presence. [PRESENCE]
- Added support for CallCenter feature/ Virtual Call Queue. [Call Center Settings & enhancements]
- Added support for Call Queue position announcement. [Call Center Settings & enhancements]
- Added support for Call Queue Statistics. [Queue Statistics]
- Added support for Call Queue Auto-Fill. [Queue Auto fill enhancement]
- Added switchboard for call queue monitoring. [Switchboard]
- Added ability to restore blind transfer call to transferrer. [Allow callback when blind transfer fails]
- Added support for external disk cleaner. [USB/SD cleaner]
- Added option to enable DOD when call is being diverted/forwarded. [Use callee DOD on FWD or Ring Simultaneously]
- Change follow me settings to extension level settings. [Follow Me]
- Added support for call forward whitelist. [FWD Whitelist]
- Added Fail2Ban defense from web login attack. [Login Attack Defense]
- Added limitation for maximum number of call queue static agents. [Static Agents limitation]
- Added support for wakeup service module in Custom privilege. [Custom Privilege]
- Added IPv6 support for T.38.
- Added DAHDI settings. [DAHDI Settings]



- Added ability to pass through SIP Call-Info header to support GXP phone JPEG_Over_HTTP with encryption and authentication to open door for GDS3710. [Transparent Call-Info header]

Firmware Version 1.0.13.14

- Added extension whitelist/blacklist for IVR dialing. [IVR]
- Added ability to include DOD in PPI Header for SIP trunk. [Use DOD in PPI]
- Added ability to customize PAI Header. [PAI Header]
- Added blacklist for outbound calls. [Outbound Blacklist]
- Added support to upload/download MOH package from Web GUI. [MUSIC ON HOLD]
- Added support to download custom prompts from Web GUI. [Download All Custom Prompt]
- Added option to configure prompt timeout in Dial By Name. [DIAL BY NAME]
- Added description field in ZeroConfig settings to configure Softkey/Line/MPK for GXP series phones. [PROVISIONING]
- Improved seamless transfer privilege control. [Seamless transfer privilege control]
- Added RTP Keep-alive support. [RTP Keep-alive]
- Added Email Send Log. [Email Send Log]
- Added support for Mitel simulation/protocol interfaces for PMS module. [PMS INTEGRATION]
- Added support for up to 10 failover trunks. [Use Failover Trunk]

Firmware Version 1.0.12.19

- Added support for binding a mobile phone number to extension. [Mobile Phone Number]
- Added support OPUS codec.
- Added support call-barging privilege settings based on extensions. [Monitor privilege control]
- Added support for Seamless Transfer. [Enable Seamless Transfer]
- Added support for Custom Call-Info for Auto Answer. [Custom Call-info for Auto Answer]
- Added support for DND Whitelist. [Do Not Disturb]
- Added Field Description on Softkey, Line keys and MPK from Zero Config.
- Added support to select interval for numbers on Batch add extension. [Extension Interval]
- Added support for Batch Add CallerID Number. [CallerID Number]
- Added support for Search Extensions Using CallerID Name.
- Added support to Enable/Disable Inbound and Outbound Route [Disable This Route / Disable This Route]
- Added support for Outbound Route Time Condition. [Time Condition]
- Added support for IPv6. [IPv6 Address]
- Added support for MTU configurable. [MTU]
- Added support of CRM. [CRM]
- Added support for Custom Privilege in User Management. [Custom Privilege]
- Added Hotline support for FXS Extension. [Hotline]



- Added support for Separate Wakeup Service. [WAKEUP SERVICE]
- Added ability to provision phones from different network subnets using zero config. [Subnet Whitelist]
- One-key-dial is replaced by Speed Dial to support more than one digit. [SPEED DIAL]
- Added append extension number in the end of DOD. [Direct Outward Dialing (DOD) via VoIP Trunks]
- Support Japan CID NTT Detect.
- Added support for Ethernet Capture Auto Sync to SFTP Server. [Enable SFTP Data Sync]
- Added support for Ethernet Capture saved to External Storage Device. [PBX Settings/Payload]
- Added support for Disable Extension Range on the Setup Wizard. [Setup Wizard]
- Added more support for Port Forwarding. [Port Forwarding]
- Added support for USB/SD Card Files Cleanup. [USB/SD Card Files Cleanup]
- Added support for A Key Dial-up FXO. [PBX Settings/RTP Settings]
- Added support for ACIM Detect Option for FXO. [DAHDI and Analog Hardware Configuration]
- Added support for some special character on the file name of FW. [Upgrading via Local Upload]
- Added more search criteria of CDR. [CDR]
- Added support of "Allow outgoing calls if registration failure" for register trunks. [Allow outgoing calls if registration failure]
- Added support for music on hold playback from webGUI. [MUSIC ON HOLD]
- Added support to enable delete recording files for user privilege. [Consumer]
- Added support disk Inode usage in "Storage Usage" page. [Storage Usage]
- Added support for Ring Group/Call Queue/IVR Display Option for Caller ID. [Replace Caller ID | Replace Caller ID | Replace Display Name]
- Added support to Detect talking users in conference. [CONFERENCE BRIDGE]
- Added support of Mini Bar for PMS. [Mini Bar]

Firmware Version 1.0.11.27

- Added ability to sort extension status on Web GUI.
- Added one click enable / disable feature code. [Feature Codes]
- Added Uruguay time zone support. [Auto Time Updating]
- Added distinctive ring tone support. [Configure Call Queue] [Configure IVR] [Create New SIP Extension]
- Added special character support for SFTP client account. [Data Sync]
- Added destination directory support for data sync. [Data Sync]
- Added ring group music on hold. [Configure Ring Group]
- Added CDR multi-email / time condition support. [CDR]
- Added blacklist anonymous call block. [Blacklist Configurations]
- Added ability to sort selected extension in Eventlist. [Event List]
- Added banned user list for Web GUI login attempts. [Login Settings]
- Added Email template support. [Email Templates]
- Added outbound route country restriction.
- Added external disk usage alert option. [Alert Events List]
- Added range IP input support for dynamic defense white list. [Dynamic Defense]



- Added blacklist support for Fail2ban. [Fail2ban]
- Added ability to reboot device from zero config page. [Discovery]
- Added GXP1628B template for zero config. [Model Update]
- Added PIN group support. [PIN GROUPS]
- Added PMS support. [PMS INTEGRATION]
- Added call queue custom prompt support. [Configure Call Queue]
- Added call queue retry time support. [Configure Call Queue]
- Added support for DHCP Client List. [DHCP Client List]

Firmware Version 1.0.10.44

- Added Zero Config DP750 support. [Model Templates]
- Added Configure framing with “esf” or “d4” in T1/J1. [Table 56: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE]

Firmware Version 1.0.10.39

- Added multiple modes support for inbound route. [Inbound Route: Multiple Mode]
- Added option “Enable Inbound Multiple Mode”, “Inbound Default Mode” and “Inbound Mode 1” for switching inbound route mode via feature code. [Feature Codes]
- Added prepending prefix for inbound route. [Inbound Route: Prepend Example]
- Added multiple registration per extension. [Multiple Registrations per Extension]
- Added SIP Message support. [SMS Message Support]
- Added 100rel option for 100rel support. [Table 106: SIP Settings/ToS]
- Added video preview support. [Table 97: Internal Options/Payload]
- Added User Portal Page Fax sending support.
- Added Fax intelligent routing. [Fax Intelligent Route]
- Added Re-Invite with two media (audio, image) support for fax sending. [Fax with Two Media]
- Added option “Max Concurrent Sending Fax” in Fax settings. [Configure Fax/T.38]
- Added option “Fax Queue Length” in Fax settings. [Configure Fax/T.38]
- Added Google Service Setting Support. [Google Service Settings Support]
- Added Conference Schedule. [CONFERENCE SCHEDULE]
- Added Setup Wizard. [Setup Wizard]
- Added ability to customize specific prompt. [Customize Specific Prompt]
- Added option “ALL” when making backup file. [Backup/Restore]
- Added “Enable Destination” and “Default Destination” in Follow Me settings. [FOLLOW ME]
- Added “Call Duration Limit” option in Web GUI→PBX→Internal Options→General. [PBX Settings/General]
- Added “Enable Auto E-mail Notification” option in Web GUI→PBX→Internal Options→General. [PBX Settings/General]
- Added options “ICE Support” and “STUN Server” in Web GUI→PBX→Internal Options→RTP Settings. [PBX Settings/RTP Settings]



- Added payload type setting for VP8 in Web GUI→PBX→Internal Options→Payload. [PBX Settings/Payload]
- Added options “External Host” and “Use IP address in SDP” in Web GUI→PBX→SIP Settings→NAT. [SIP Settings/NAT]
- Improved CDR. [CDR Improvement]
- Added Network Status page under web GUI System Status→Network Status. [Network Status]

Firmware Version 1.0.2.7

- Added PRI T310 configuration. [Table 53: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE]
- Added Announcement Center. [ANNOUNCEMENTS CENTER]

Firmware Version 1.0.2.5

- Added option to enable/disable SSH access via LCD or Web GUI. [SSH Access]
- Added ability to select voicemail storage (Email + WAV is supported). [Table 78: Voicemail Email Settings]
- Added support to allow remote peer extensions in ring group. [Remote Extension in Ring Group]
- Added ability to strip and prepend digits in inbound routes. [Table 70: Inbound Rule Configuration Parameters]
- Added ability to search extensions on Extension page.
- Added user portal for users to log in with extension number, access user information, extension configuration and CDR. [USER PORTAL]
- Added support to send Fax via Web GUI. [Fax Sending]
- Added “Enable LDAP” option to skip the extension from UCM default LDAP phonebook. [Table 33: SIP Extension Configuration Parameters]
- Added video RE-INVITE support.
- Added DDNS Support. [DDNS Settings]
- Added support for Call Barging using feature codes. [Enable Spy]
- Added ability to search the CDR by called number. [Table 122: CDR Filter Criteria]
- Added ability to select the file types for automatic backup. [Backup/Restore]
- Added automatic backup support on SD Card or USB storage. [Backup/Restore]
- Added support to skip trunk authentication by time condition.
- Added option to send P-Asserted-Identity header in SIP Register Trunk. [Table 62: SIP Register Trunk Configuration Parameters]
- Added ability to specify trunks in CDR filters. [CDR]
- Added ability to use Pattern in Caller Number to filter CDR. [CDR]
- Added support to send UNREGISTER when VoIP trunk is disabled. [Table 62: SIP Register Trunk Configuration Parameters]
- Added LDAP client support. [LDAP Client Configurations]



- Added option to specify the chronological order to voice mails. [Table 76: Voicemail Settings]
- Added option to configure whether to skip pressing 1/2 to accept or reject calls from Follow Me [Table 88: Follow Me Settings]
- Added option to specify port range in Port Forwarding configuration. [Table 11: UCM6510 Network Settings→Port Forwarding]
- Added ability to go back to IVR menu from Dial By Name by pressing the star key. [Dial By Name Configuration]
- Added support to upgrade SIP end device via SD card in Zero Config. [Table 28: Global Policy Parameters – Maintenance]
- Added ability to filter alert logs. [Alert Log]
- Added ability to delete alert logs. [Alert Log]
- Added NAT option for peer trunk. [Table 68: Outbound Route Configuration Parameters]
- Improved Automatic Download CDR result format. [CDR]
- Fixed Digital Trunk SS7 signaling mode inbound / outbound call problem.
- Fixed Asterisk is crashed while using external MCB and CEI.

Firmware Version 1.0.1.12

- Added Active Calls feature to monitor call status and barge in active calls.
- Added support to disable the trunk for VoIP trunk and analog trunk. [Table 61: Create New SIP Trunk] [Table 50: Analog Trunk Configuration Parameters]
- Added RBS support on T1.
- Added Frame Relay support on Data Trunk. [DATA TRUNK]
- Added 'Assign CIC to D-channel' option on SS7 settings page. [Table 54: Digital Hardware Configuration Parameters: E1 - SS7]
- Added 'First CIC' option in SS7 configuration. [Table 54: Digital Hardware Configuration Parameters: E1 - SS7]
- Added 'D-Chan' selection for PRI and SS7 in editing digital ports. [Table 53: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE] [Table 54: Digital Hardware Configuration Parameters: E1 - SS7]
- Added support for Ring simultaneously feature for extensions. [Table 33: SIP Extension Configuration Parameters]
- Added support for Music On Hold selection per extension. [Table 33: SIP Extension Configuration Parameters]
- Added support to disable this extension per extension. [Table 33: SIP Extension Configuration Parameters]
- Added ability to set personal password for making outbound calls per extension. [Table 33: SIP Extension Configuration Parameters]
- Added 'TEL URI' configuration for SIP extension/VoIP trunk. [Table 33: SIP Extension Configuration Parameters] [Table 61: Create New SIP Trunk]



- Added E&M Immediate and E&M Wink signaling for T1. [Table 58: Digital Hardware Configuration Parameters: T1-E&M Immediate/E&M Wink]
- Renamed the 'network backup' settings items to 'data sync'. [Data Sync]
- Added "Download Search Result" in CDR. [CDR]
- Added office time and holiday setting support. [Office Time] [Holiday]
- Added time condition for call forward. [EXTENSIONS]
- Added support to monitor FXO trunk using SLA. [SLA STATION]
- Added One-Key Dial function.
- Added Follow Me support. [FOLLOW ME]
- Supported external number as the key pressing event of an IVR.
- Improved APIs for Zero Config templates and settings. [PROVISIONING]
- Supported GXP16XX, Surveillance and GS_wave models in Zero Config. [PROVISIONING]
- Added advanced settings for devices discovered in Zero Config. [Device Configuration]
- Added ability to delete multiple recording files at one time. [Recording Files]
- Added call queue destination if no answer/timeout. [Table 82: Call Queue Configuration Parameters]
- Added call queue Music on Hold customization. [Table 82: Call Queue Configuration Parameters]
- Added restricted AMI access. [AMI]
- Added ability to choose the type(s) of files to be cleaned in cleaner.
- Added DTMF configuration per SIP trunk. [Table 61: Create New SIP Trunk]
- Added ability to upload and play ring group announcement. [Table 80: Ring Group Parameters]
- Added ability to upload and play paging call announcement. [PAGING AND INTERCOM GROUP]
- Added Alert-info configuration for distinctive ringing on inbound route. [Table 70: Inbound Rule Configuration Parameters]
- Added ability to prepend digits/trunk name to inbound calls' caller ID. [Table 70: Inbound Rule Configuration Parameters]
- Modified Static Routes Interface display when network method is changed. [Static Routes]

Firmware Version 1.0.0.25

- This is the initial version.



WELCOME

Thank you for purchasing Grandstream UCM6510 IP PBX appliance. The UCM6510 is an innovative IP PBX appliance for E1/T1/J1 networks that brings enterprise-grade unified communications and security protection to enterprises, small-to-medium businesses (SMBs), retail environments and residential settings in an easy-to-manage fashion. Powered by an advanced hardware platform and revolutionary software functionalities, the UCM6510 offers a breakthrough turnkey solution for converged voice, video, data, fax, security surveillance, and mobility applications out of the box without any extra license fees or recurring costs.

 **Caution:**

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

 **Warning:**

Please do not use a different power adapter with the UCM6510 as it may cause damage to the products and void the manufacturer warranty.

This document is subject to change without notice. The latest electronic version of this user manual is available for download here:

<http://www.grandstream.com/support>

Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.



PRODUCT OVERVIEW

Feature Highlights

- 1 GHz quad-core Cortex A9 application processor, large memory (1GB DDR3 RAM, 32GB Flash), and dedicated high performance multi-core DSP array for advanced voice processing
- 1 Integrated 1 T1/E1/J1 interface, 2 PSTN trunk FXO ports, 2 analog telephone/Fax FXS ports with lifeline capability in case of power outage, and up to 50 SIP trunk accounts
- Hardware DSP based 128ms-tail-length carrier-grade line echo cancellation (LEC), hardware based caller ID/call progress tone and smart automated impedance matching for various countries
- Gigabit network port(s) with integrated PoE, USB, SD card; integrated NAT router with advanced QoS support
- Strong defense against malicious attacks (Fail2ban, Whitelist, Blacklist, alerts, etc.)
- Data communication via T1/E1/J1 and data-voice combined communication via T1/E1/J1 with SS7 or PRI
- Supports up to 2000 SIP endpoint registrations, up to 200 concurrent calls (up to 100 SRTP encrypted concurrent calls), and up to 64 conference attendees
- Flexible dial plan, call routing, site peering, call recording (manual and automatic per SIP call and SIP trunk), central control panel for endpoints, integrated NTP server, and integrated LDAP contact directory
- Automated detection and provisioning of IP phones, video phones, ATAs, gateways, SIP cameras, and other endpoints for easy deployment
- Strongest-possible security protection using SRTP, TLS, and HTTPS with hardware encryption accelerator
- Redundant power supply, advanced support for Hot Standby Clustering and High Availability to minimize system down time (pending)
- Automatic export of previous day's data; periodically cleans up user data

Technical Specifications

Table 1: Technical Specifications

Interfaces	
Analog Telephone FXS Ports	2x RJ11 ports (both with lifeline capability in case of power outage)
PSTN Line FXO Ports	2x RJ11 ports (both with lifeline capability in case of power outage)
T1/E1/J1 Interface	1x RJ45 port
Network Interfaces	Dual Gigabit ports (switched or routed) with PoE; A 3 rd Gigabit port for Hot-Standby Clustering
NAT Router	Yes (user configurable)
Peripheral Ports	USB, SD



LED Indicators	Power 1/2, PoE, USB, SD, T1/E1/J1, FXS 1/2, FXO 1/2, LAN, WAN, Cluster Heartbeat
LCD Display	128x32 dot matrix graphic LCD with DOWN and OK buttons
Reset Switch	Yes, long press for factory reset and short press for reboot
Voice/Video Capabilities	
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection and auto-switch to G.711
Voice and Fax Codecs	G.711 A-law/U-law, G.722, G.723.1 5.3K/6.3K, G.726, G.729A/B, iLBC, GSM, AAL2-G.726-32, ADPCM; T.38
Video Codecs	H.264, H.263, H.263+
QoS	Layer 3 QoS, Layer 2 QoS
Signaling and Control	
DTMF Methods	In Audio, RFC2833, and SIP INFO
Digital Signaling	PRI, SS7, MFC/R2, E&M
Provisioning Protocol and Plug-and-Play	TFTP/HTTP/HTTPS, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66/multicast SIP SUBSCRIBE/mDNS), Eventlist between local and remote trunks
Network Protocols	TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, SIP (RFC3261), STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay
Disconnect Methods	Call Progress Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect, Busy Tone
Security	
Media	SRTP, TLS, HTTPS, SSH
Advanced Defense	Fail2ban, alert events, Whitelist, Blacklist, strong password based access control
Physical	
Universal Power Supply	Input: 100-240VAC, 50-60Hz; Output: DC+12VDC, 1.5A
Physical	Unit Weight: 2.165 Kg; Package weight: 3.012 Kg
Dimensions	440mm (L) x 185mm (W) x 44mm (H)
Environmental	Operating: 32 – 113°F / 0 – 45°C, Humidity 10-90% (non-condensing) Storage: 14 – 140°F / -10 – 60°C, Humidity 10-90% (non-condensing)
Mounting	Rack mount and Desktop



Additional Features

Multi-language Support	English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech for Web GUI; Customizable IVR/voice prompts for English, Chinese, British English, German, Spanish, Greek, French, Italian, Dutch, Polish, Portuguese, Russian, Swedish, Turkish, Hebrew and Arabic
Caller ID	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 – BT, NTT Japan
Polarity Reversal/ Wink	Yes, with enable/disable option upon call establishment and termination
Call Center	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/busy level, in-queue announcement
Customizable Auto Attendant	Up to 5 layers of IVR (Interactive Voice Response)
Maximum Call Capacity	Up to 2000 registered SIP endpoints, up to 200 concurrent calls
Conference Bridges	Up to 8 bridges, up to 64 simultaneous conference attendees
Call Features	Call park, call forward, call transfer, DND, DISA, ring group, pickup group, blacklist, paging/intercom and etc
Compliance	<ul style="list-style-type: none"> • FCC: Part 15 (CFR 47) Class B, Part 68 • CE: EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, TBR21, RoHS • A-TICK: AS/NZS CISPR 22 Class B, AS/NZS CISPR 24, AS/NZS 60950, AS/ACIF S002 • ITU-T K.21 (Basic Level); UL 60950 (power adapter) • T1: TIA-968-B Section 5.2.4 • E1: TBR12/TBR13, E1: AS/ACIF



INSTALLATION

Before deploying and configuring the UCM6510 series, the device needs to be properly powered up and connected to network. This section describes detailed information on installation, connection and warranty policy of the UCM6510 series.

Equipment Packaging

Table 2: UCM6510 Equipment Packaging

Main Case	Yes (1)
Power Adapter	Yes (2)
Ethernet Cable	Yes (1)
Wall Mount	Yes (2)
Screws	Yes (6)
Quick Installation Guide	Yes (1)

Connect your UCM6510

The following screenshots illustrate the front and back panels of the UCM6510:

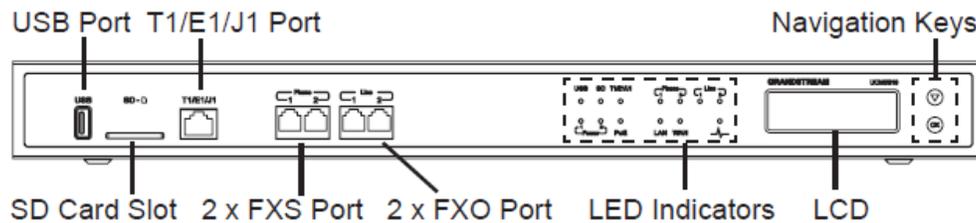


Figure 1: UCM6510 Front View

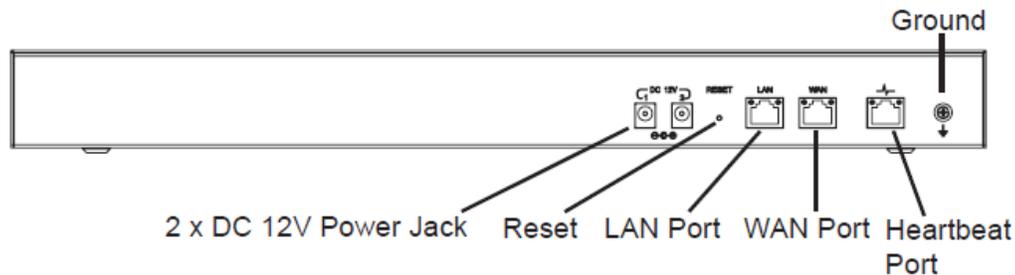


Figure 2: UCM6510 Back View

Follow the steps below to connect the UCM6510 for initial setup:



1. Connect one end of an RJ-45 Ethernet cable (cable type: straight through) into the WAN port of the UCM6510; connect the other end into the uplink port of an Ethernet switch/hub.
2. Connect the 12V DC power adapter into the DC 12V power jack 1 on the back of the UCM6510. Insert the main plug of the power adapter into a surge-protected power outlet. (Connect the second power adapter into the DC 12V power jack 2 for failover purpose in case the first one is down).
3. Wait for the UCM6510 to boot up. The LCD in the front will show its hardware information when the bootup process is done.
4. Once the UCM6510 is successfully connected to the network, the LED indicator for the WAN port in the front will be in solid green and the LCD shows up the IP address.

Depending on how the UCM6510 is used, users can follow the steps below for optional setup:

1. PSTN Line Connection: connect PSTN lines from the wall jack to the UCM6510 LINE ports (FXO ports).
2. Analog Line Connection: connect analog lines (phone and fax) to the PHONE ports (FXS ports).
3. T1/E1/J1 Line Connection: connect one end of the T1/E1/J1 cable provided from the service provider into the T1/E1/J1 port of the UCM6510; connect the other end into the T1/E1/J1 wall jack. T1/E1/J1 crossover cable should be used and it's not provided in the UCM6510 package. Please see T1/E1/J1 crossover cable pin-out in the figure below:

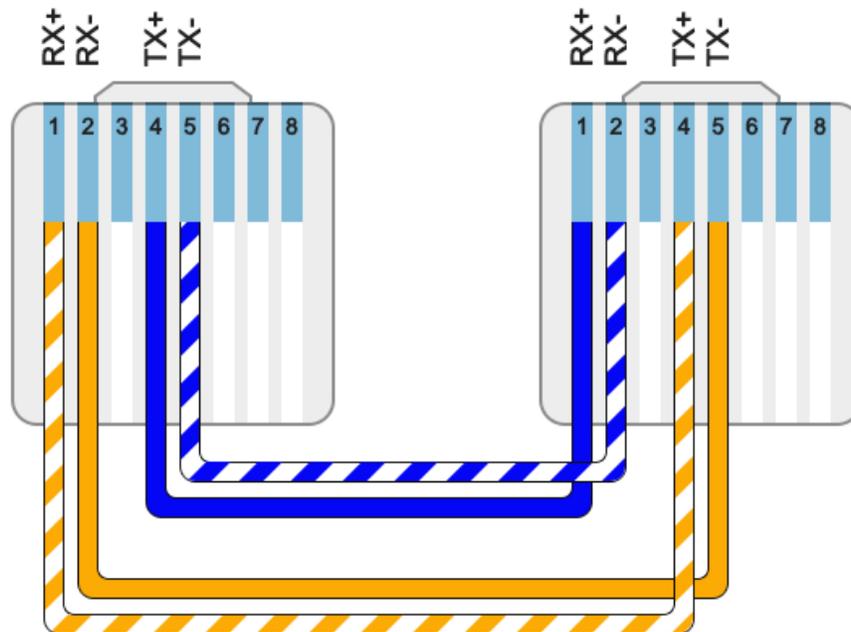


Figure 3: UCM6510 T1/E1/J1 Crossover Cable Pin-out

Safety Compliances

The UCM6510 series IP PBX complies with FCC/CE and various safety standards. The UCM6510 power adapter is compliant with the UL standard. Use the universal power adapter provided with the UCM6510 package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If the UCM6510 series IP PBX was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream Networks, contact our Technical Support Team for a RMA (Return Materials Authorization) number before the product is returned. Grandstream Networks reserves the right to remedy warranty policy without prior notification.

 **Warning:**

Use the power adapter provided with the UCM6510 series IP PBX. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.



GETTING STARTED

The UCM6510 provides LCD interface, LED indication and Web GUI configuration interface.

- The LCD displays hardware, software and network information. Users could also navigate in the LCD menu for device information and basic network configuration.
- The LED indication at the front of the device provides interface connection and activity status.
- The Web GUI gives users access to all the configurations and options for UCM6510 setup.

This section provides step-by-step instructions on how to use the LCD menu, LED indicators and Web GUI of the UCM6510. Once the basic settings are done, users could start making calls from UCM6510 extension registered on a SIP phone as described at the end of this section.

Use The LCD Menu

- **Default LCD Display**

By default, when the device is powered up, the LCD will show device model (e.g., UCM6510), hardware version (e.g., V1.4A) and IP address. Press “Down” button and the system time will be displayed (e.g., 2014-10-21 14:20).

- **Menu Access**

Press “OK” button to start browsing menu options. Please see menu options in [Table 3: LCD Menu Options].

- **Menu Navigation**

Press the “Down” arrow key to browser different menu options. Press the “OK” button to select an entry.

- **Exit**

If “Back” option is available in the menu, select it to go back to the previous menu. For “Device Info” “Network Info” and “Web Info” which do not have “Back” option, simply press the “OK” button to go back to the previous menu. Additionally, the LCD will display default idle screen after staying in menu option for 15 seconds.

- **LCD Backlight**

The LCD backlight will be on upon key pressing. The backlight will go off after the LCD stays in idle for 30 seconds.



The following table shows the LCD menu options.

Table 3: LCD Menu Options

View Events	<ul style="list-style-type: none"> • Critical Events • Other Events
Device Info	<ul style="list-style-type: none"> • Hardware: Hardware version number • Software: Software version number • P/N: Part number • WAN MAC: WAN side MAC address • LAN MAC: LAN side MAC address • Uptime: System up time since the last reboot
Network Info	<ul style="list-style-type: none"> • WAN Mode: DHCP, Static IP, or PPPoE • WAN IP: IP address • WAN Subnet Mask • LAN IP: IP address • LAN Subnet Mask
Network Menu	<ul style="list-style-type: none"> • WAN Mode: Select WAN mode as DHCP, Static IP or PPPoE • Static Routes Reset: Click to reset the static route setting
Factory Menu	<ul style="list-style-type: none"> • Reboot • Factory Reset • LCD Test Patterns Press “OK” to start. Then press “Down” button to test different LCD patterns. When done, press “OK” button to exit. • Fan Mode Select “Auto” or “On”. • LED Test Patterns Select “All On” “All Off” or “Blinking” and check LED status for USB, SD, T1/E1/J1, Phone 1/Phone 2, Line 1/Line 2 ports. After the LED test, select “Back” in the menu and the device will show the LED actual status again. • RTC Test Patterns Select “2022-02-22 22:22” or “2011-01-11 11:11” to start the RTC (Real-Time Clock) test pattern. Check the system time from LCD idle screen by pressing “DOWN” button, or from Web GUI→System Status→General page. After the test, reboot the device manually and the device will display the correct time.



	<ul style="list-style-type: none"> • Hardware Testing Select "Test SVIP" to perform SVIP test on the device. This is mainly for factory testing purpose which verifies the hardware connection inside the device. The diagnostic result displays on the LCD after the test is done.
Web Info	<ul style="list-style-type: none"> • Protocol: Web access protocol. HTTP or HTTPS. By default, it's HTTPS • Port: Web access port number. By default, it's 8089
SSH Switch	<ul style="list-style-type: none"> • Enable SSH: Enable SSH access. • Disable SSH: Disable SSH access. <p>By default the SSH access is disabled.</p>

Use The LED Indicators

The UCM6510 has LED indicators in the front to display connection status. The following table shows the status definitions.

Table 4: UCM6510 LED Indicators

LED Indicator	LED Status
Power 1/Power 2 PoE LAN WAN USB SD Phone 1 /Phone 2 (FXS) Line 1/Line 2 FXO	<ul style="list-style-type: none">  Solid: Connected  Fast Blinking: Data Transferring  Slow Blinking: Trying to connect  OFF: Not Connected
T1/E1/J1	<ul style="list-style-type: none">  Solid: Connected and working  Fast Blinking (0.5s on/0.5s off): No cable is connected; or connected but the link is not working at all.  Slow Blinking (1s on/1s off): Connected but the link is only working one-way



Use The Web GUI

Access Web GUI

The UCM6510 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE (version 8+), Mozilla Firefox, Google Chrome and etc.

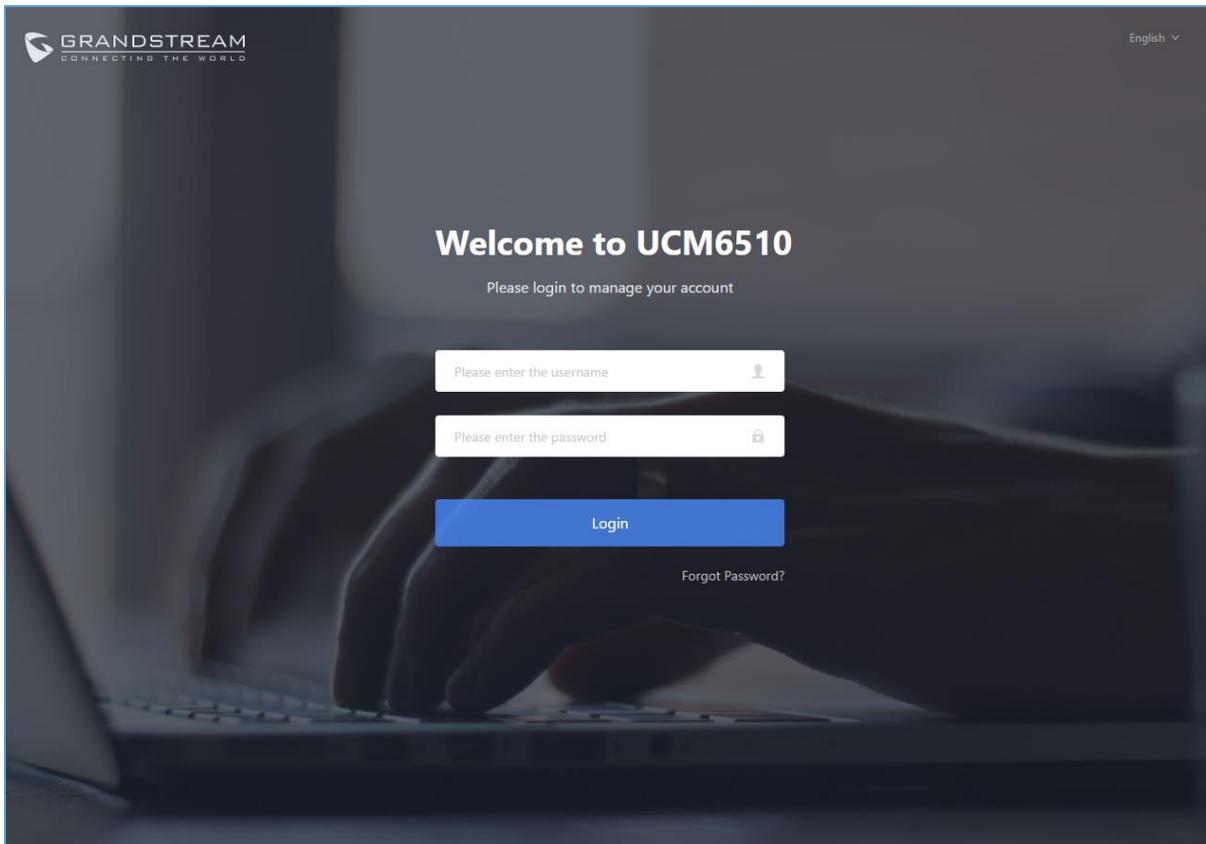


Figure 4: UCM6510 Web GUI Login Page

To access the Web GUI:

1. Connect the computer to the same network as the UCM6510.
2. Ensure the device is properly powered up and shows its IP address on the LCD.
3. Open a web browser on the computer and enter the IP address in the address bar. The web login page will display as shown above.
4. Enter default administrator username “admin” and password.

Note: Units manufactured starting January 2017 have a unique random password printed on the sticker located on the back of the unit. It is highly recommended to change the default password after login for the first time. Older units have default password “admin”. See bellow pictures for the location of the default random password:



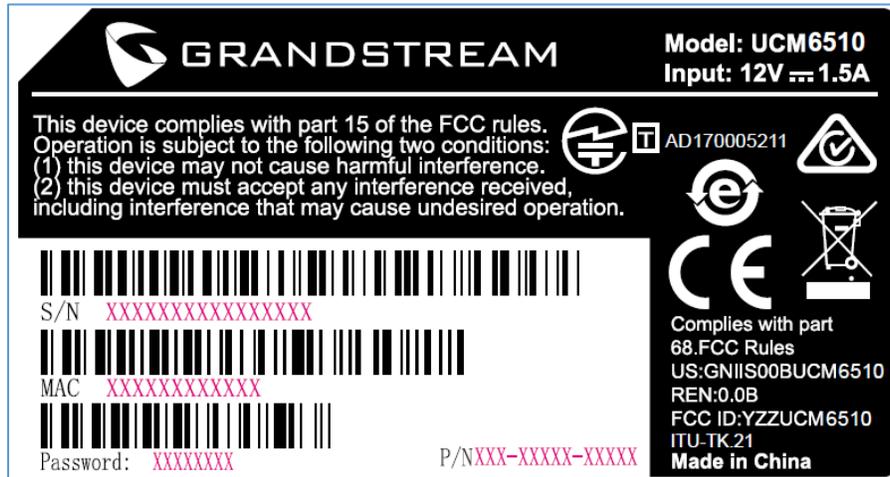


Figure 5: Default Random Password

 **Note:**

By default, the UCM6510 has “Redirect From Port 80” enabled. Therefore, if users type in the UCM6510 IP address in the web browser, the web page will be automatically redirected to the page using HTTPS and port 8089.

For example, if the LCD shows 192.168.40.167, please enter 192.168.40.167 in your web browser and the web page will be redirected to:

<https://192.168.40.167:8089>

The option “Redirect From Port 80” can be configured under the UCM6510 Web GUI→**Settings**→**HTTP Server**.

Setup Wizard

When the user logs in the UCM6510 Web GUI for the first time, a setup wizard will guide the user to set up basic configuration. Configurations in setup wizard includes: **Time zone, Change password, Network settings, Extensions, Trunk and routes.**

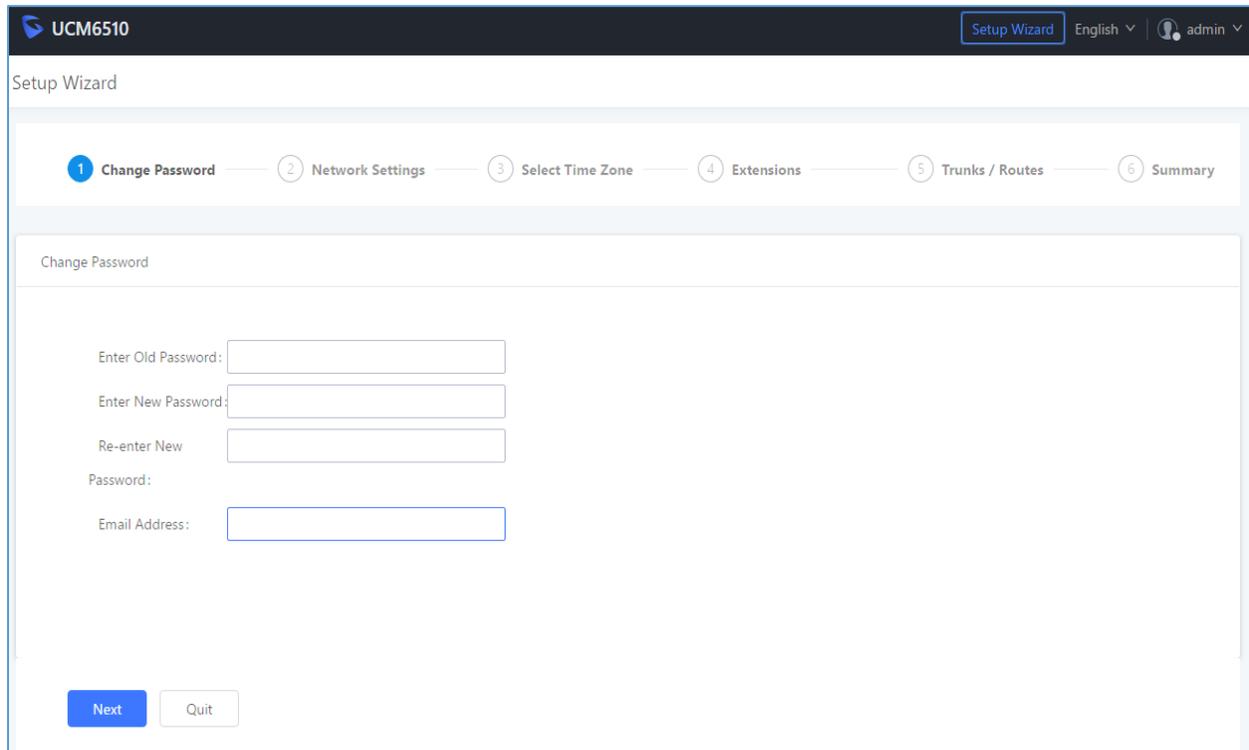


Figure 6: UCM6510 Setup Wizard

Users can disable the Extension Range during configuration on the Extensions.

During the wizard, the user can quit the setup wizard at any time to start over with manual configuration. At the last step of the wizard, the user will be provided with summary for review, before the configuration is loaded. Once the setup is completed, the system is ready to go.

Web GUI Configurations

There are four main sections on the Web GUI for users to view the PBX status, configure and manage the PBX.

- **Status:** Displays PBX status, System Status, System Events and CDR.
- **PBX:** To configure extensions, trunks, call routes, zero config for auto provisioning, call features, internal options, IAX settings, SIP settings, as well as ports configuration for digital trunks.
- **Settings:** To configure network settings, firewall settings, change password, LDAP Server, HTTP Server, Email Settings, Time Settings and NTP server.
- **Maintenance:** To perform firmware upgrade, backup configurations, cleaner setup, reset/reboot, syslog setup and troubleshooting.



Web GUI Languages

Currently the UCM6510 Web GUI supports the following languages:

English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, Russian, Italian, Polish, German.

Users can select the displayed language in Web GUI login page, or at the upper right after logging in.

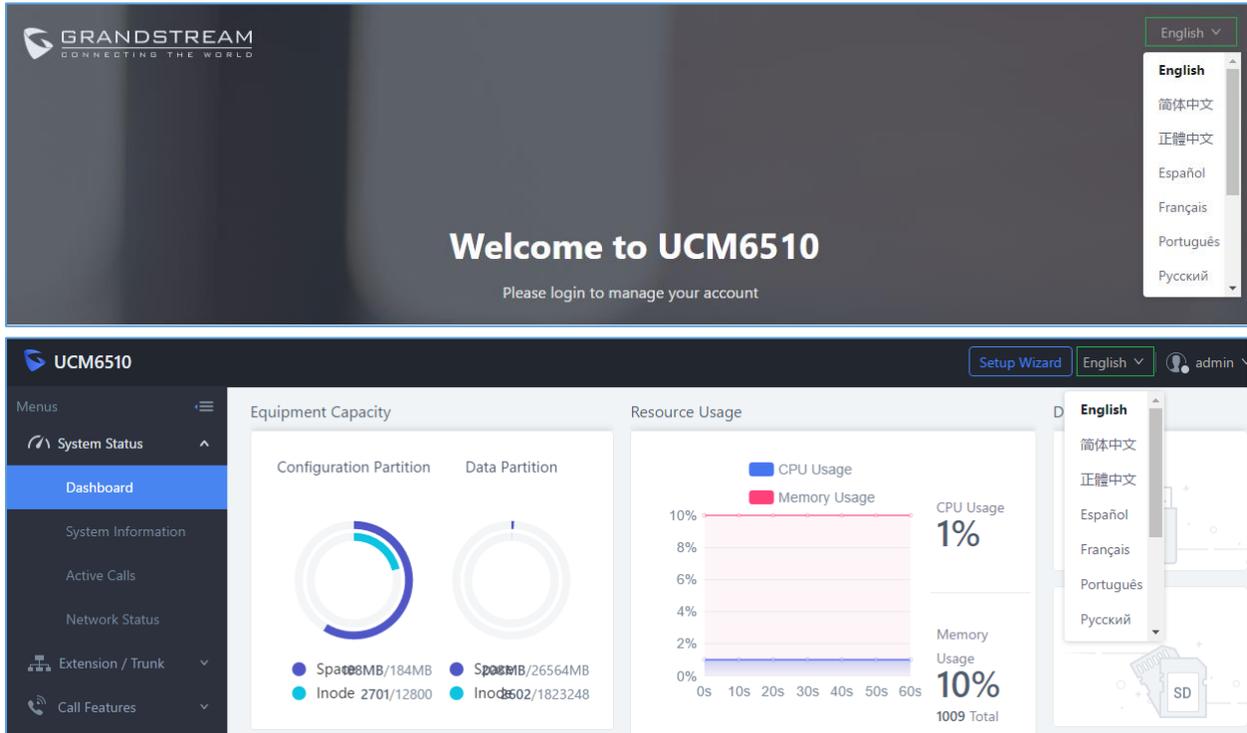


Figure 7: UCM6510 Web GUI Language

Save And Apply Changes

Click on “Save” button after configuring the Web GUI options in one page. After saving all the changes, make sure click on “Apply Changes” button on the upper right of the web page to submit all the changes. If the change requires reboot to take effect, a prompted message will pop up for you to reboot the device.

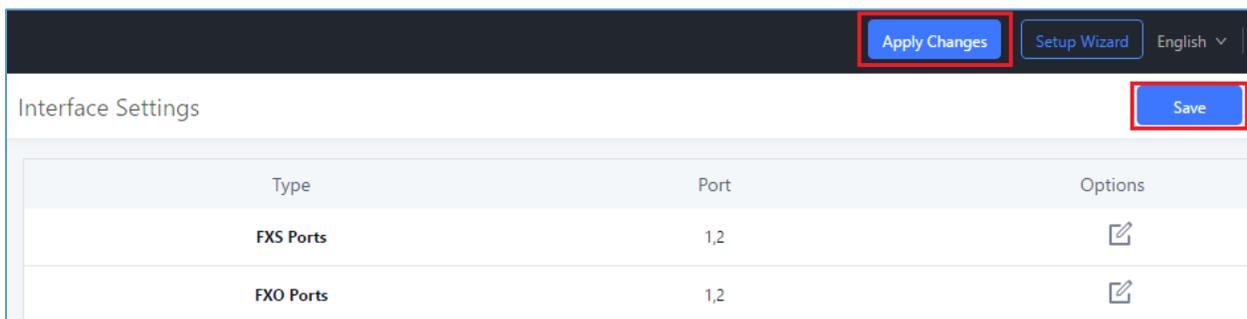


Figure 8: UCM6510 Web GUI: Apply Changes



Make Your First Call

Power up the UCM6510 and your SIP end point phone. Connect both devices to the network. Then follow the steps below to make your first call.

1. Log in the UCM6510 Web GUI, go to **Extension/Trunk→Extensions**.
2. Click on “Create New SIP Extension” to create a new extension. You will need User ID, Password and Voicemail Password information to register and use the extension later.
3. Register the extension on your phone with the SIP User ID, SIP server and SIP Password information. The SIP server address is the UCM6510 IP address.
4. When your phone is registered with the extension, dial *97 to access the voicemail box. Enter the Voicemail Password once you hear “Password” voice prompt.
5. Once successfully logged in to the voicemail, you will be prompted with the Voice Mail Main menu.
6. You are successfully connected to the PBX system now.



SYSTEM SETTINGS

This section explains configurations for system-wide parameters on the UCM6510. Those parameters include Network Settings, Firewall, Change Password, LDAP server, HTTP server, Email settings, Time Settings and NTP Server settings.

User Management

User management is on Web GUI→**System Maintenance**→**User Management** page. User could create multiple accounts for different administrators to log in the UCM6510 Web GUI. Additionally, the system will automatically create user accounts along with creating new extensions for extension users to login to the Web GUI using their extension number and password. All existing user accounts for Web GUI login will be displayed on User Management page as shown in the following figure.

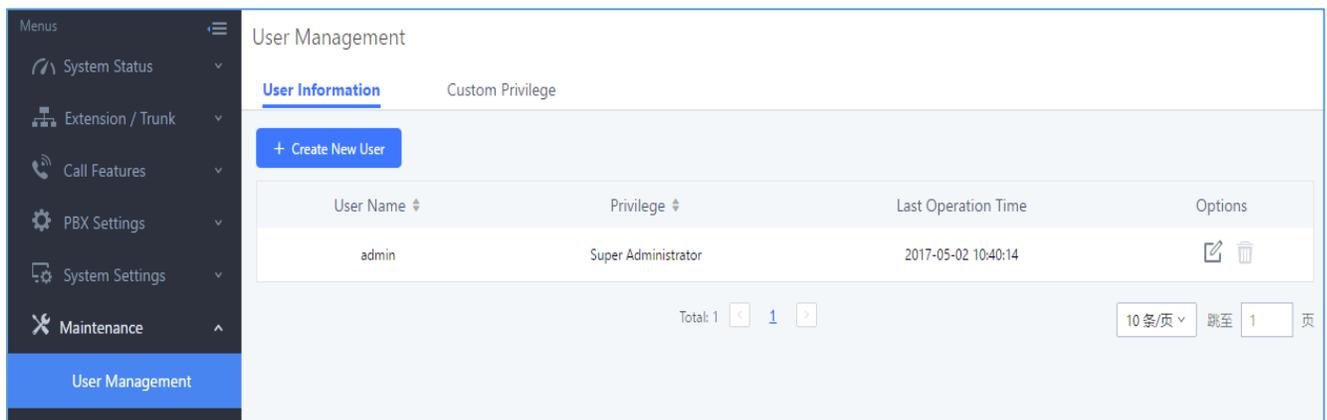


Figure 9: User Management Page Display

User Information

When logged in as Super Admin, click on [+ Create New User](#) to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.



Create New User Information

* User Name: <input style="width: 90%;" type="text" value="John"/>	* User Password: <input style="width: 90%;" type="text" value="admin123"/>
Privilege: <input style="border-bottom: 1px solid #ccc;" type="text" value="Administrator"/>	Department: <input style="width: 90%;" type="text" value="IT"/>
Fax: <input style="width: 90%;" type="text"/>	Email Address: <input style="width: 90%;" type="text" value="john@domain.local"/>
First Name: <input style="width: 90%;" type="text" value="John"/>	Last Name: <input style="width: 90%;" type="text" value="DOE"/>
Home Number: <input style="width: 90%;" type="text"/>	Mobile Phone Numb... <input style="width: 90%;" type="text" value="123456789"/>

Figure 10: Create New User

Table 5: User Management – Create New User

User Name	Configures a username to identify the user which will be required in Web GUI login. Letters, digits and underscore are allowed in the user name.
User Password	Configures a password for this user which will be required in Web GUI login. Letters, digits and underscore are allowed.
Privilege	This is the role of the Web GUI user. Currently only “Admin” is supported when Super Admin creates a new user.
Department	Enters the necessary information to keep a record for this user.
Fax	
Email Address	
First Name	
Last Name	
Home Number	
Phone Number	

Once created, the Super Admin can edit the users by clicking on  or delete the user by clicking on .



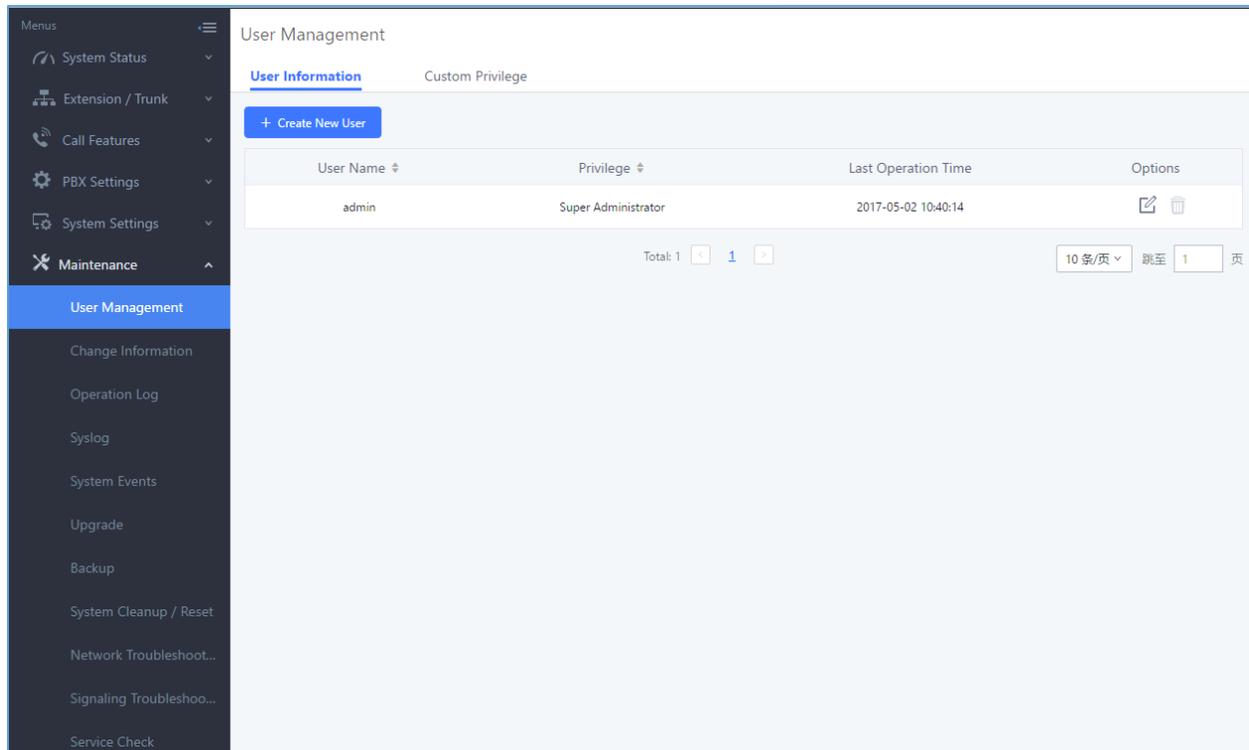


Figure 11: User Management – New Users

Custom Privilege

Four privilege levels are supported:

- **Super Administrator**

- This is the highest privilege. Super Admin can access all pages on UCM6510 Web GUI, change configuration for all options and execute all the operations.
- Super Admin can create, edit and delete one or more users with “Admin” privilege
- Super Admin can edit and delete one or more users with “Consumer” privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account “admin” is configured with “Super Admin” privilege and it’s the only user with “Super Admin” privilege. The User Name and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on Web GUI→**Maintenance**→**Change Information** page.
- Super Admin could view operations done by all the users in Web GUI→**Maintenance**→**Operation Log**.



- **Administrator**

- Users with “Admin” privilege can only be created by “Super Admin” user.
- “Admin” privilege users are not allowed to access the following pages:
 - Maintenance→Upgrade**
 - Maintenance→Backup**
 - Maintenance→Cleaner**
 - Maintenance→Reset/Reboot**
 - Maintenance→User Management→Operation Log**
- “Admin” privilege users cannot create new users for login.

- **Consumer**

- A user account for Web GUI login is created automatically by the system when a new extension is created.
- The user could log in the Web GUI with the extension number and password to access user information, extension configuration and CDR of that extension.
- The SuperAdmin user can click on  the “General_User” in order to enable/disable the custom privilege of deleting their own recording files in user level login.

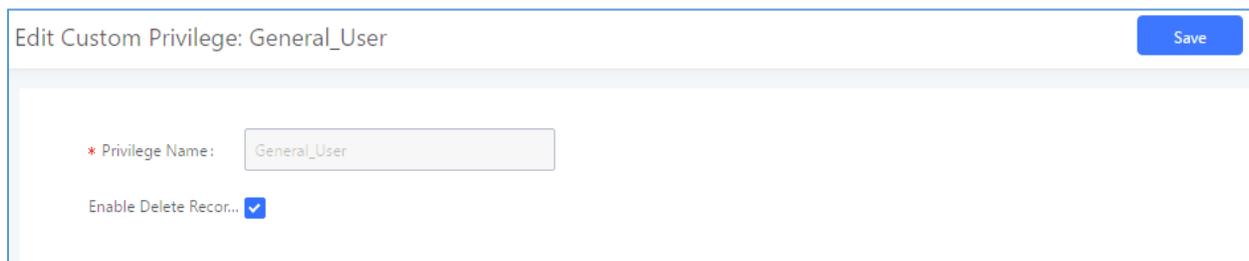


Figure 12: General User

- **Custom Privilege**

The Super Admin user can create users with different privileges. 6 modules are available for privilege customization.

- System Status
- Conference
- System Events
- CDR Records
- CDR API
- Wakeup Service

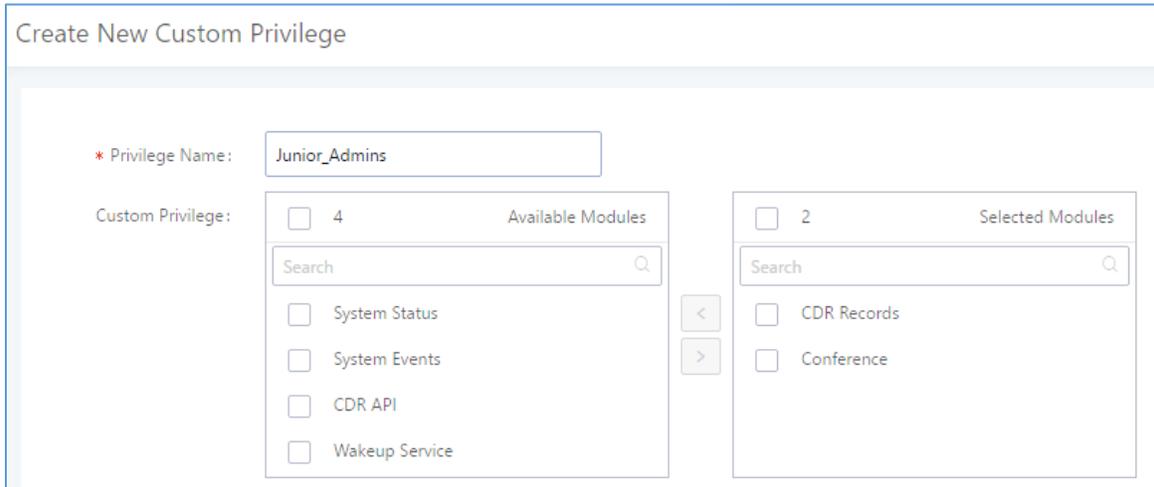


Figure 13: Create New Custom Privilege

Log in UCM6510 as super admin and go to **Maintenance**→**User Management**→**Custom Privilege**, create privilege with customized available modules.

To assign custom privilege to a sub-admin, navigate to UCM webUI→**Maintenance**→**User Management**→**User Information**→**Create New User/Edit Users**, select the custom privilege from “Privilege” option.

Concurrent Multi-User Login

When there are multiple Web GUI users created, concurrent multi-user login is supported on the UCM6510. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on “Apply Changes”), a prompt will pop up as shown in the following figure.

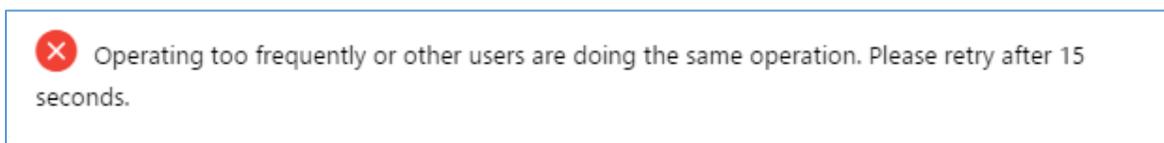


Figure 14: Multiple User Operation Error Prompt

Operation Log

Super Admin has the authority to view operation logs on UCM6510 Web GUI→**Maintenance**→**User Management**→**Operation Log** page. Operation logs list operations done by all the Web GUI users, for example, Web GUI login, creating trunk, creating outbound rule and etc. There are 6 columns to record the operation details “Date”, “User Name”, “IP Address”, “Results”, “Page Operation” and “Specific Operation”.



Operation Log Filter

Delete Search Result (s)
Delete All Logs

Date	User Name	IP Address	Results	Page Operation	Specific Operation
2017-05-02 10:56:40	admin	192.168.6.245	Operation successful	Apply Changes	
2017-05-02 10:56:38	admin	192.168.6.245	Operation successful	Extensions: Create New SIP Extension	User Password: *****; Extension: 1002; Permission: internal. ⓘ
2017-05-02 10:56:38	admin	192.168.6.245	Operation successful	addFollowme	ⓘ
2017-05-02 10:56:34	admin	192.168.6.245	Operation successful	Extensions: Create New SIP Extension	User Password: *****; Extension: 1001; Permission: internal. ⓘ
2017-05-02 10:56:34	admin	192.168.6.245	Operation successful	addFollowme	ⓘ
2017-05-02 10:54:50	admin	192.168.6.245	Operation successful	Login: Login	User Name: admin.
2017-05-02 10:54:44	1000	192.168.6.245	Operation successful	Extensions: Logout	User Name: 1000.
2017-05-02 10:52:37	1000	192.168.6.245	Operation successful	Login: Login	User Name: 1000.
2017-05-02 10:51:57	admin	192.168.6.245	Operation successful	Extensions: Logout	User Name: admin.
2017-05-02 10:51:46	admin	192.168.6.245	Operation successful	Apply Changes	

Figure 15: Operation Logs

The operation log can be sorted and filtered for easy access. Click on the header of each column to sort. For example, clicking on “Date” will sort the logs according to operation date and time. Clicking on “Date” again will reverse the order.

Table 6: Operation Log Column Header

Date	The date and time when the operation is executed.
User Name	The username of the user who performed the operation.
IP Address	The IP address from which the operation is made.
Results	The result of the operation.
Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
Specific Operation	Click on ⓘ to view the options and values configured by this operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on Filter.



Start Time:	<input type="text" value="2017-05-01 15:57"/>	End Time:	<input type="text" value="2017-05-03 15:58"/>
IPv4/IPv6 Address:	<input type="text"/>	User Name:	<input type="text" value="All Users"/>

Date	User Name	IP Address	Results	Page Operation	Specific Operation
2017-05-02 10:56:40	admin	192.168.6.245	Operation successfu 	Apply Changes	
2017-05-02 10:56:38	admin	192.168.6.245	Operation successfu 	Extensions: Create New SIP Extensio n	User Password: *****; Extension: 1002; Permission: internal.
2017-05-02 10:56:38	admin	192.168.6.245	Operation successfu 	addFollowme	
2017-05-02 10:56:34	admin	192.168.6.245	Operation successfu 	Extensions: Create New SIP Extensio n	User Password: *****; Extension: 1001; Permission: internal.
2017-05-02 10:56:34	admin	192.168.6.245	Operation successfu 	addFollowme	

Figure 16: Operation Logs Filter

The above figure shows an example that operations made by user “support” on device with IP 192.168.40.173 from 2014-11-01 00:00 to 2014-11-06 15:38 are filtered out and displayed.

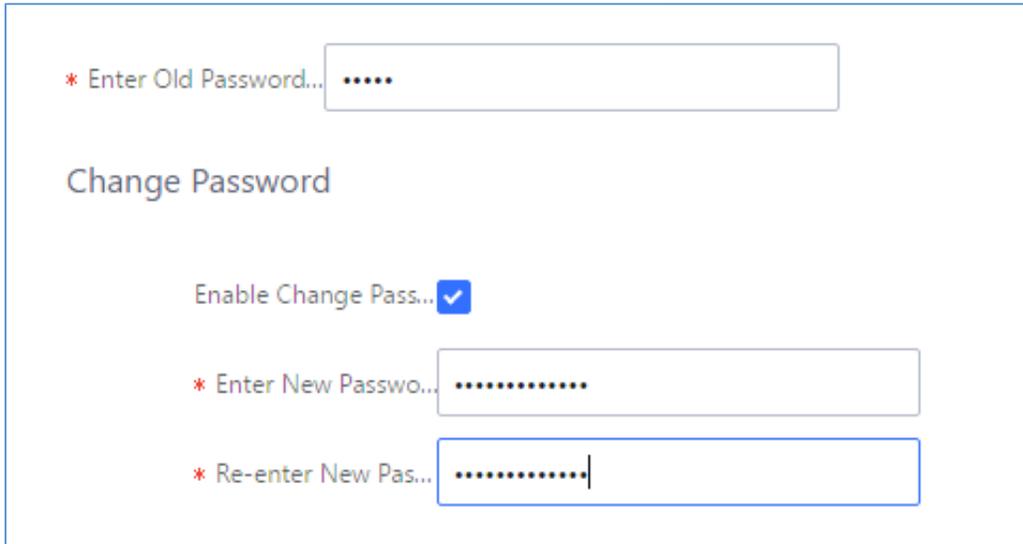
To delete operation logs, users can perform filtering first and then click on to delete the filtered result of operation logs. Or users can click on to delete all operation logs at once.

Change Password

After logging in the Web GUI for the first time, it is highly recommended for users to change the default password “admin” to a more complicated password for security purpose. Follow the steps below to change the Web GUI access password.

1. Go to Web GUI→**Maintenance**→**Change Information** page.
2. Enter the old password first.
3. Enter the new password and retype the new password to confirm. The new password has to be at least 4 characters. The maximum length of the password is 16 characters.
4. Configure the Email Address that is used when login credential is lost.
5. Click on “Save” and the user will be automatically logged out.
6. Once the web page comes back to the login page again, enter the username “admin” and the new password to login.





* Enter Old Password... [password field]

Change Password

Enable Change Pass...

* Enter New Passwo... [password field]

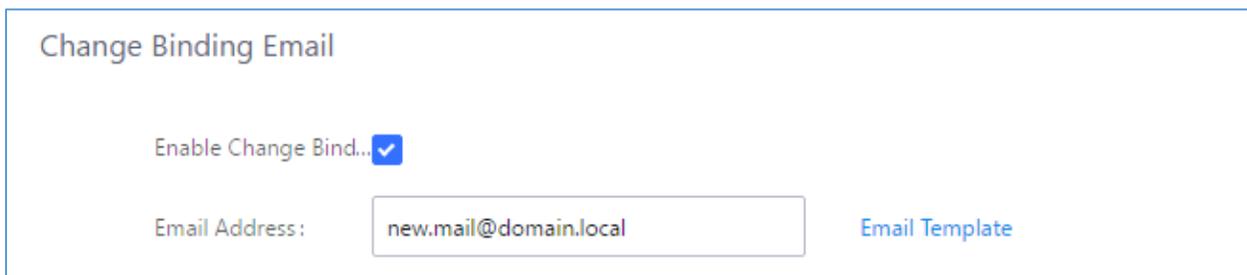
* Re-enter New Pas... [password field]

Figure 17: Change Password

Enter Old Password	Enter the Old Password for UCM6510
Enter New Password	Enter the New Password for UCM6510
Retype New Password	Retype the New Password for UCM6510
Email Address	Configure the Email address for UCM6510. In case login credential is lost, Email address is used to retrieve login credential

Change Binding Email

UCM6510 allows user to configure binding email in case login password is lost. UCM6510 login credential will be sent to the designated email address. The feature can be found under Web GUI→Maintenance→Change Information→Change Binding Email.



Change Binding Email

Enable Change Bind...

Email Address: [new.mail@domain.local] [Email Template](#)

Figure 18: Change Binding Email



Table 7: Change Binding Email option

Enter the password of the account	Enter the current login user credential for UCM6510
Email Address	Email Address is used to retrieve password when password is lost

Network Settings

After successfully connecting the UCM6510 to the network for the first time, users could log in the Web GUI and go to **System Settings**→**Network Settings** to configure the network parameters for the device. Select each tab in Web GUI→**System Settings**→**Network Settings** page to configure LAN/WAN settings, 802.1X and Port Forwarding.



Note:

To connect the UCM6510 to network, T1/E1/J1 data trunk can also be used, instead of using the WAN/LAN port. Please see section **[DATA TRUNK]** to use UCM6510 data trunk to connect the device to Internet.

Basic Settings

Please refer to the following tables for basic network configuration parameters on the UCM6510.

Table 8: UCM6510 Network Settings→**Basic Settings**

Method	<p>Select “Route”, “Switch” or “Dual” mode on the network interface of UCM6510. The default setting is “Route”.</p> <ul style="list-style-type: none"> • Route WAN port interface will be used for uplink connection. LAN port interface will be used to serve as router. • Switch WAN port interface will be used for uplink connection. LAN port interface will be used as bridge for PC connection. • Dual Both ports can be used for uplink connection. Users will need assign LAN 1 or LAN 2 as the default interface in option “Default Interface” and configure “Gateway IP” for this interface if static IP is used for the interface.
MTU	Specify the Maximum Transmission Unit. (By default, it's 1500)



IPv4 Address

Preferred DNS Server	Enter the preferred DNS server address. If Preferred DNS is configured, the UCM6510 will use it as Primary DNS server.
-----------------------------	--

WAN (when “Method” is set to “Route”)

IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for WAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for WAN port. The default value is 0.

LAN (when Method is set to “Route”)

IP Address	Enter the IP address assigned to LAN port. The default setting is 192.168.2.1.
Subnet Mask	Enter the subnet mask. The default setting is 255.255.255.0.
DHCP Server Enable	Enable or disable DHCP server capability. The default setting is “Yes”.
DNS Server 1	Enter DNS server address 1. The default setting is 8.8.8.8.
DNS Server 2	Enter DNS server address 2. The default setting is 208.67.222.222.
Allow IP Address From	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.

LAN (when Method is set to “Switch”)

IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.



User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.

LAN 1 / LAN 2 (when Method is set to "Dual")

Default Interface	If "Dual" is selected as "Method", users will need assign the default interface to be LAN 1 (mapped to UCM6510 WAN port) or LAN 2 (mapped to UCM6510 LAN port) and then configure network settings for LAN1 and LAN 2. Default interface is LAN2.
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings when the port is assigned as default interface. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. Default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.

IPv6 Address

WAN (when "Method" is set to "Route")

IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.

LAN (when Method is set to "Route")

DHCP Server	Select Disable, Auto or DHCPv6. Disable: the DHCPv6 server is disabled. Auto: Stateless address auto configuration using NDP protocol. DHCPv6: Stateful address auto configuration using DHCPv6 protocol.
DHCP Prefix	Enter DHCP prefix. (Default is 2001:db8:2:2::)



DHCP prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings. Default is (2001:4860:4860::8888)
DNS Server 2	Enter the DNS server 2 address for static settings. Default is (2001:4860:4860::8844)
Allow IP Address From	Configure starting IP address assigned by the DHCP prefix and DHCP prefixlen.
Allow IP Address To	Configure the ending IP address assigned by the DHCP Prefix and DHCP prefixlen.
Default IP Lease Time	Configure the lease time (in seconds) of the IP address.

LAN (when Method is set to "Switch")

IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.

LAN 1 / LAN 2 (when Method is set to "Dual")

Default Interface	Users will need assign the default interface to be LAN 1 (mapped to UCM6510 WAN port) or LAN 2 (mapped to UCM6510 LAN port) and then configure network settings for LAN 1/LAN 2. The default interface is LAN 2.
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.

- **Method: Route**

WAN port interface is used for uplink connection; LAN port interface is used as a router. Please see a sample diagram below.



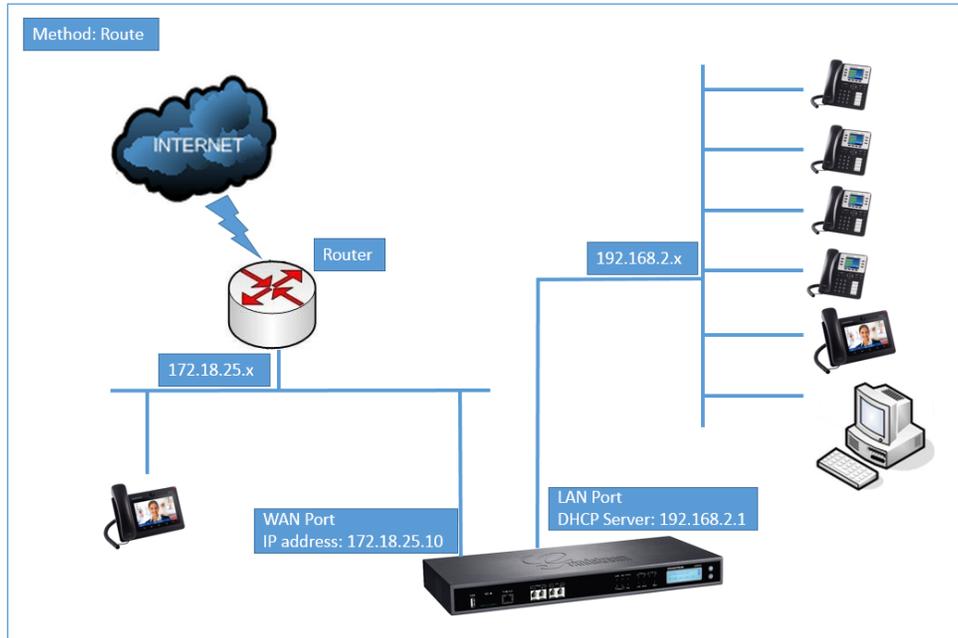


Figure 19: UCM6510 Network Interface Method: Route

- **Method: Switch**

WAN port interface is used for uplink connection; LAN port interface is used as bridge for PC connection.

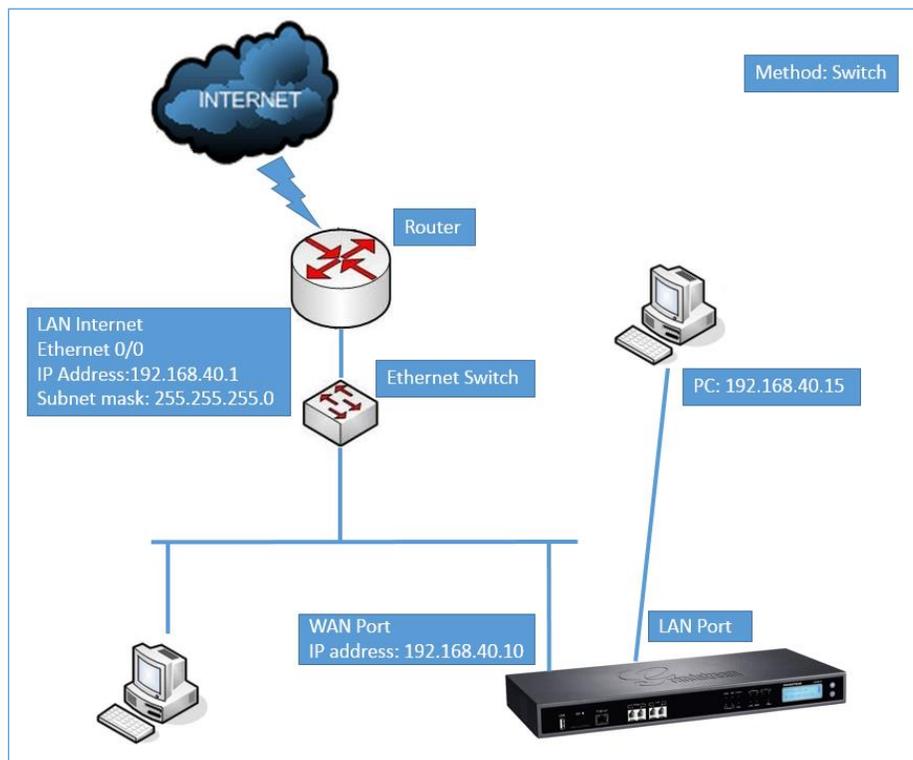


Figure 20: UCM6510 Network Interface Method: Switch



- **Method: Dual**

Both WAN port and LAN port are used for uplink connection. WAN port will be mapped to LAN 1 interface; LAN port will be mapped to LAN 2 interface. Users will need assign LAN 1 or LAN 2 as the default interface in option “Default Interface” and configure “Gateway IP” if static IP is used for this interface.

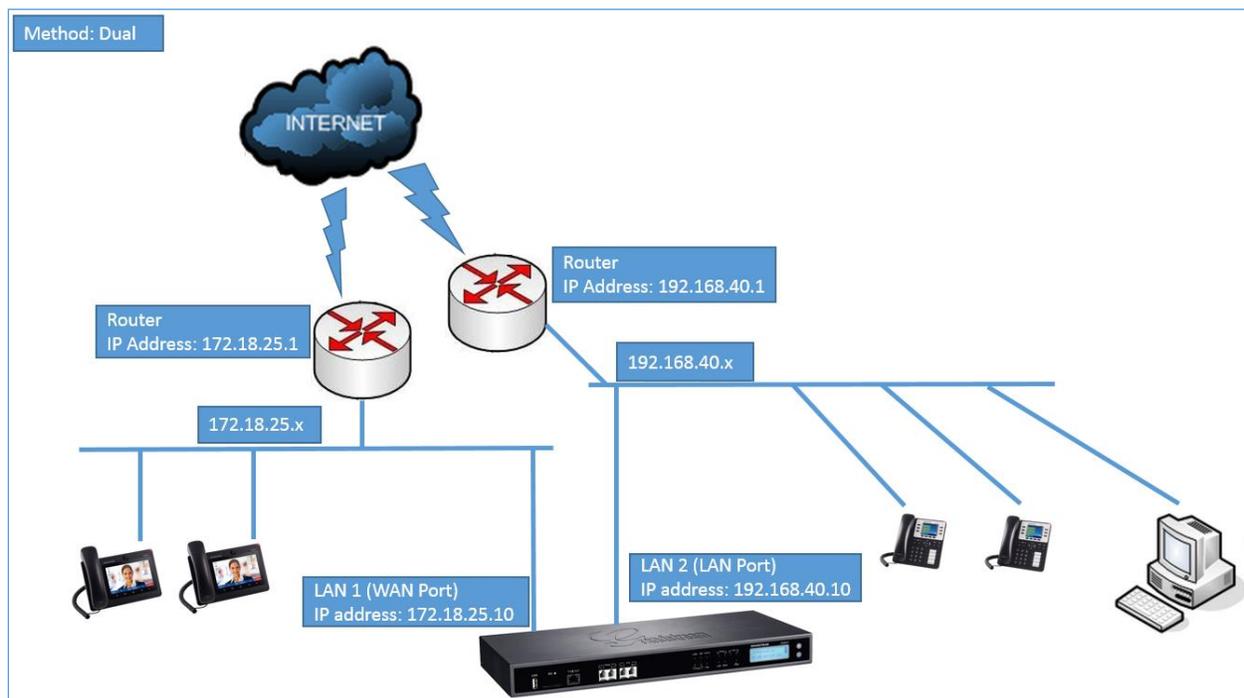


Figure 21: UCM6510 Network Interface Method: Dual

DHCP Client List

This feature can bind MAC to IP address on the LAN port.

When devices receive IP addresses from UCM6510 LAN port, they will be listed on the webUI under “Settings > Network Settings > DHCP Client List” as shown below.

Network Settings				
Basic Settings	DHCP Client List	802.1X Settings	Static Routes	Port Forwarding
<input type="button" value="+ Add Mac Address Bind"/> <input type="button" value="Batch add MAC addresses to bind"/> <input type="button" value="Batch Release MAC Address Bind"/>				
<input type="checkbox"/>	MAC Address ↕	IP Address ↕	Bind Status ↕	Options
<input type="checkbox"/>	dc4a3e78dd25	192.168.2.100	Unbind	

Figure 22: DHCP Client List



User can bind manually a MAC to an IP address by clicking on **+ Add Mac Address Bind**, the following figure will pop up.

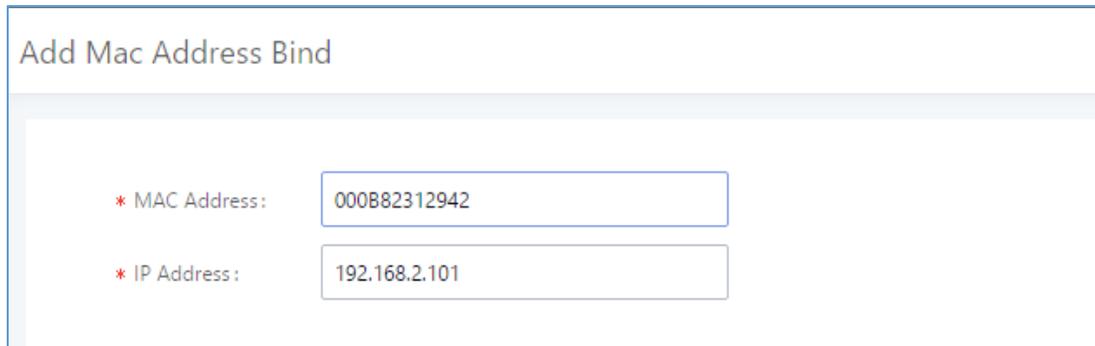


Figure 23: Add MAC Address Bind

User needs to set the device MAC address and the IP that will be bound to it (the IP address needs to be within the UCM6510 DHCP range).

In order to bind a batch of listed MAC addresses, user needs to check first the MAC addresses to bind and click on **Batch add MAC addresses to bind**. A confirmation popup will be shown, click **OK** to bind the addresses.

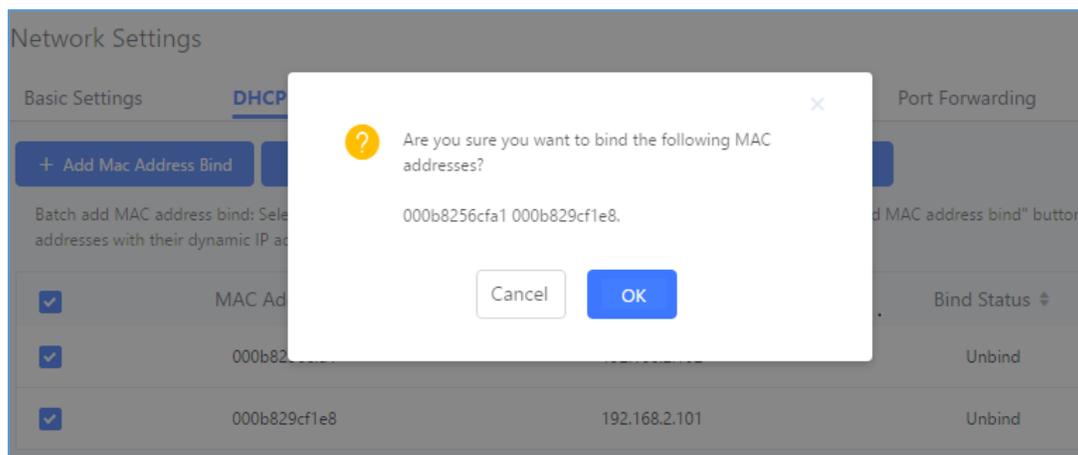


Figure 24: Batch Add MAC Address Bind

After Clicking “OK” to confirm the binding, the “Bind Status” will change from “Unbind” to “Binding”.

802.1X

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to device before the device is allowed to access Internet or other LAN resources. The UCM6510 supports 802.1X as a supplicant/client to be authenticated.



The following diagram and figure show UCM6510 uses 802.1X mode “EAP-MD5” on WAN port as client in the network to access Internet.

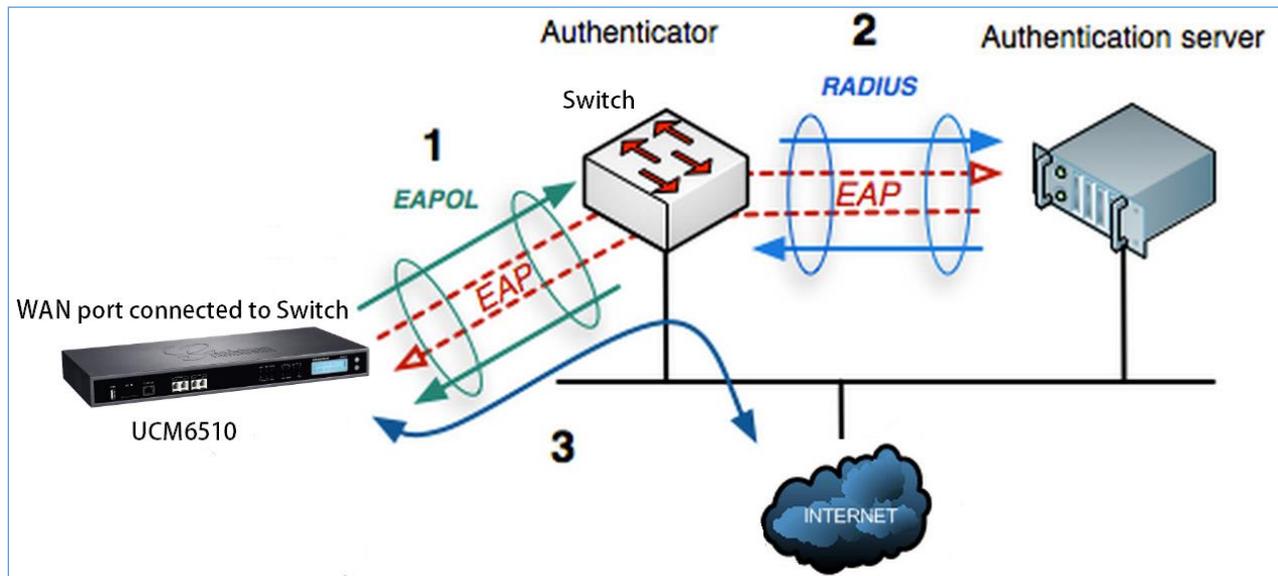


Figure 25: UCM6510 Using 802.1X as Client

Network Settings

Basic Settings
DHCP Client List
802.1X Settings
Static Routes
Port Forwarding

WAN

802.1X Mode:

* Identity:

* MD5 Password:

Figure 26: UCM6510 Using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on UCM6510. Identity and MD5 password are required for authentication, which should be provided by the network administrator obtained from the RADIUS server. If “EAP-TLS” or “EAP-PEAPv0/MSCHAPv2” is used as the 802.1X mode, users will also need upload 802.1X CA Certificate and 802.1X Client Certificate, which should be also generated from the RADIUS server.



Table 9: UCM6510 Network Settings→802.1X

802.1X Mode	Select 802.1X mode. The default setting is “Disable”. The supported 802.1X mode are: <ul style="list-style-type: none"> • EAP-MD5 • EAP-TLS • EAP-PEAPv0/MSCHAPv2
Identity	Enter 802.1X mode Identity information.
MD5 Password	Enter 802.1X mode MD5 password information.
802.1X CA Certificate	Select 802.1X certificate from local PC and then upload.
802.1X Client Certificate	Select 802.1X client certificate from local PC and then upload.

Static Routes

A static route is a pre-determined path that the network traffic travels to reach a specific host or network. On the UCM6510, the static route function allows the device to use manually configured routes, rather than dynamically assigned routes or default gateway configured in the UCM6510 Web GUI→**Network Settings**→**Basic Settings** to forward traffic. It can be used to define a route when no other routes are available or necessary, or used in complementary with existing routing on the UCM6510 as a failover backup, and etc.

- Click on  to create a new static route. The configuration parameters are listed in the table below.
- Once added, users can select  to edit the static route.
- Select  to delete the static route.
- Static routes configuration can be reset from LCD menu→Network Menu.

Table 10: UCM6510 Network Settings→Static Routes

Destination	Configure the destination IP address or the destination IP subnet for the UCM6510 to reach using the static route. <u>Example:</u> IP address – 192.168.66.4 IP subnet – 192.168.66.0
Netmask	Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255. <u>Example:</u> 255.255.255.0



Gateway	Configure the gateway address so that the UCM6510 can reach the destination via this gateway. Gateway address is optional. <u>Example:</u> 192.168.40.5
Interface	Specify the network interface “LAN”, “WAN” or “Data trunk 1” (“Data Trunk 1” option will show only when the data trunk is enabled) on the UCM6510 to reach the destination using the static route.

The following diagram shows a sample application of static route usage on UCM6510.

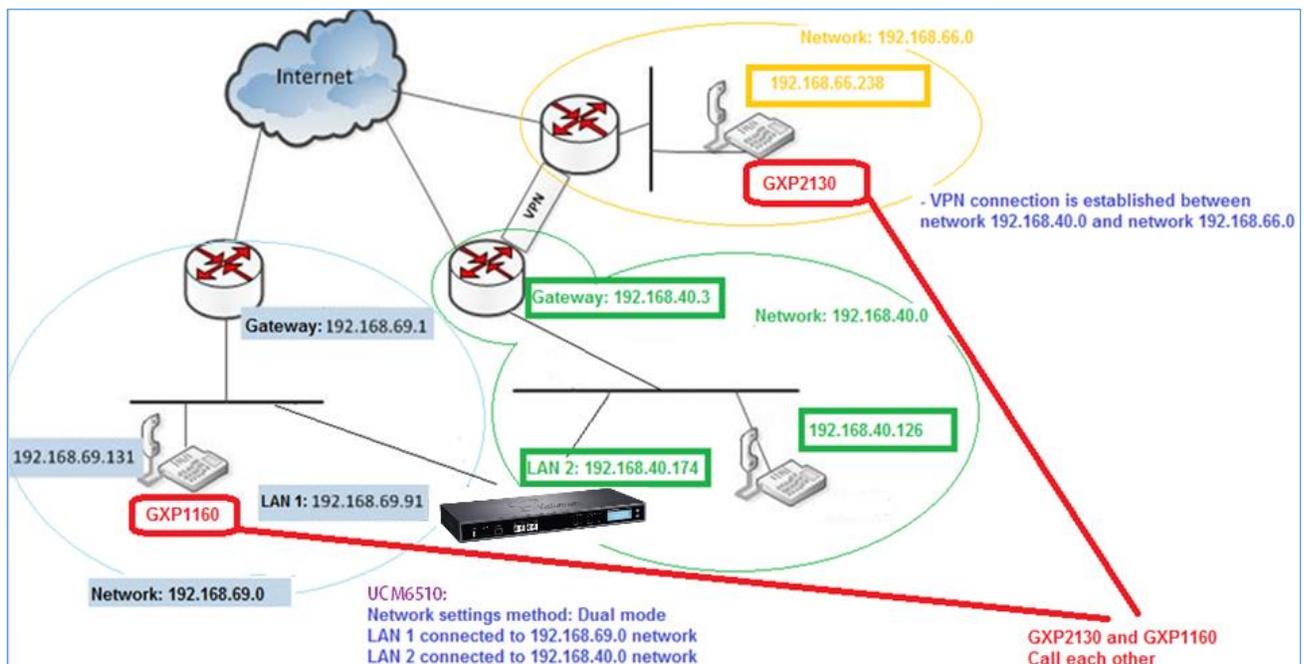


Figure 27: UCM6510 Static Route Sample

The network topology of the above diagram is as below:

- Network 192.168.69.0 has IP phones registered to UCM6510 LAN 1 address
- Network 192.168.40.0 has IP phones registered to UCM6510 LAN 2 address
- Network 192.168.66.0 has IP phones registered to UCM6510 via VPN
- Network 192.168.40.0 has VPN connection established with network 192.168.66.0

In this network, by default the IP phones in network 192.168.69.0 are unable to call IP phones in network 192.168.66.0 when registered on different interfaces on the UCM6510. Therefore, we need configure a static route on the UCM6510 so that the phones in isolated networks can make calls between each other.

Create New IPV4 Static Route

* Destination:	192.168.66.0
Subnet Mask:	255.255.255.0
Gateway:	192.168.40.3
* Protocol Type:	WAN ▼

Figure 28: UCM6510 Static Route Configuration

Port Forwarding

The UCM6510 network interface supports router functions which provides users the ability to do port forwarding. If the UCM6510 is set to “Route” under Web GUI→**System Settings**→**Network Settings**→**Basic Settings: Method**, port forwarding is available for configuration.

The port forwarding configuration is under Web GUI→**System Settings**→**Network Settings**→**Port Forwarding** page. Please see related settings in the table below.

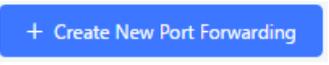
Table 11: UCM6510 Network Settings→Port Forwarding

WAN Port	Specify the WAN port number or a range of WAN ports. Unlimited number of ports can be configured. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
LAN IP	Specify the LAN IP address.
LAN Port	Specify the LAN port number or a range of LAN ports. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
Protocol Type	Select protocol type “UDP Only”, “TCP Only” or “TCP/UDP” for the forwarding in the selected port. The default setting is “UDP Only”.



The following figures demonstrate a port forwarding example to provide phone's Web GUI access to public side:

- The UCM6510 network mode is set to “Route”
- The UCM6510 WAN port is connected to uplink switch, with a public IP address configured, e.g. 1.1.1.1.
- The UCM6510 LAN port provides DHCP pool that connects to multiple phone devices in the LAN network 192.168.2.x. The UCM6510 is used as a router, with gateway address 192.168.2.1
- There is a GXP2160 connected under the LAN interface network of the UCM6510. It obtains IP address 192.168.2.100 from UCM6510 DHCP pool
- On the UCM6510 Web GUI→**System Settings**→**Network Settings**→**Port Forwarding**, configure a port forwarding entry as the figure shows below.

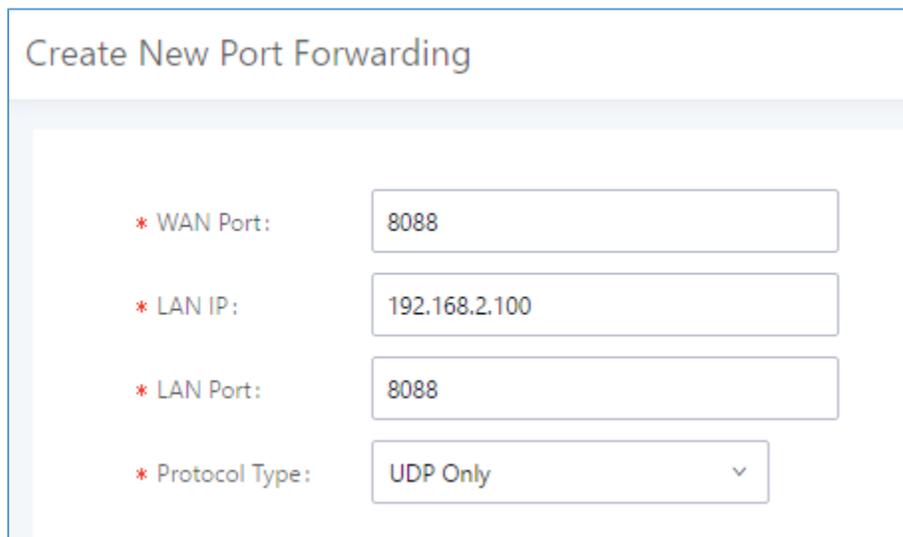
- Click on 

WAN Port: This is the port opened up on the WAN side for access purpose.

LAN IP: This is the GXP2160 IP address, under the LAN interface network of the UCM6510.

LAN Port: This is the port opened up on the GXP2160 side for access purpose.

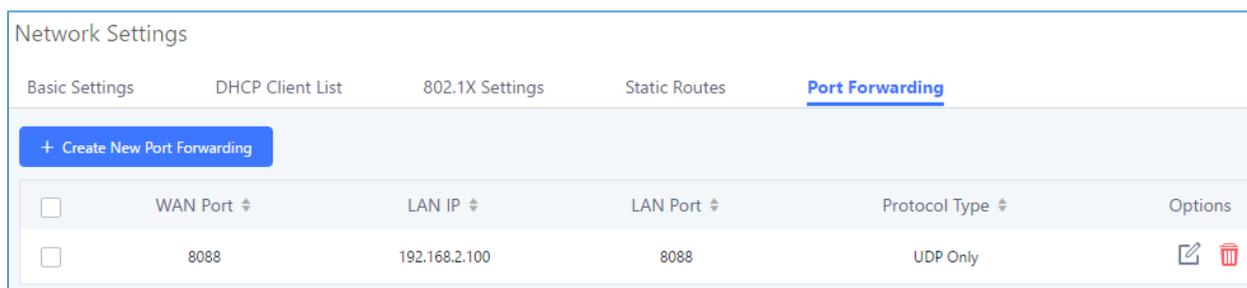
Protocol Type: We select TCP here for Web GUI access using HTTP.



The screenshot shows a form titled "Create New Port Forwarding" with the following fields:

- * WAN Port: 8088
- * LAN IP: 192.168.2.100
- * LAN Port: 8088
- * Protocol Type: UDP Only (dropdown menu)

Figure 29: Create New Port Forwarding



The screenshot shows the "Network Settings" page with the "Port Forwarding" tab selected. Below the "Create New Port Forwarding" button is a table with the following configuration:

<input type="checkbox"/>	WAN Port ⇅	LAN IP ⇅	LAN Port ⇅	Protocol Type ⇅	Options
<input type="checkbox"/>	8088	192.168.2.100	8088	UDP Only	 

Figure 30: UCM6510 Port Forwarding Configuration

This will allow users to access the GXP2160 Web GUI from public side, by typing in address “1.1.1.1:8088”.

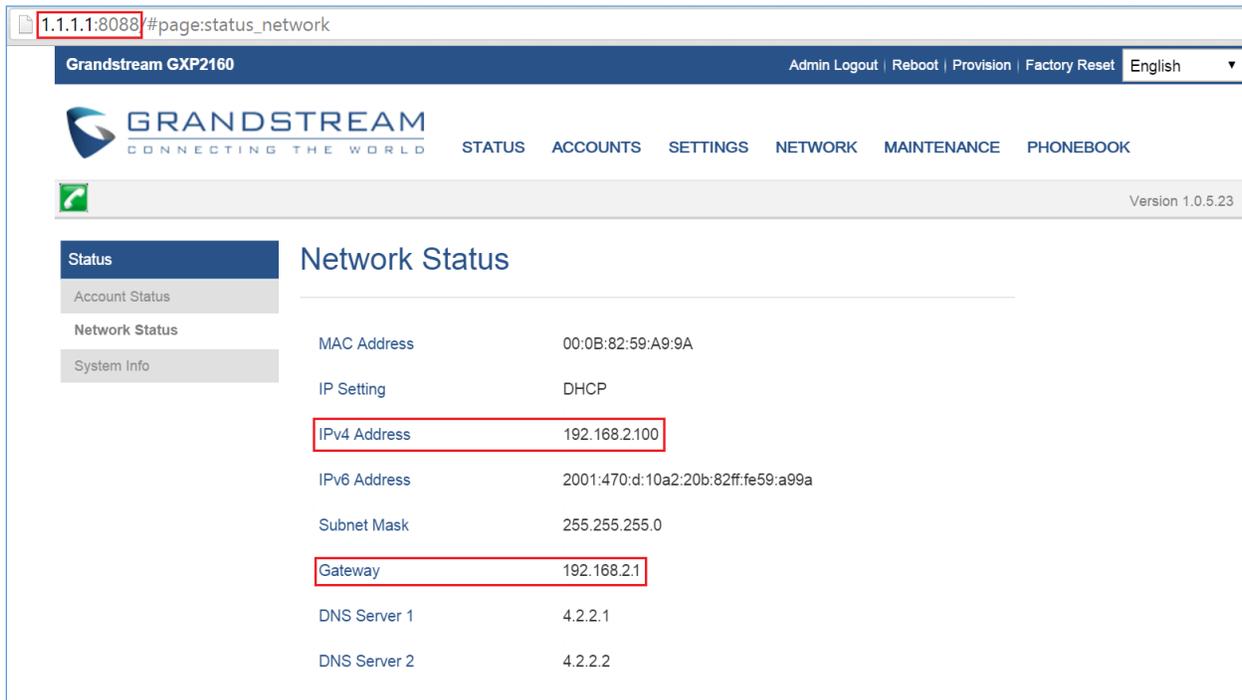


Figure 31: GXP2160 Web Access Using UCM6510 Port Forwarding

OpenVPN

Open VPN settings allow the users to configure UCM6510 to use VPN features.

Table 12: UCM6510 Settings→Network Settings→OpenVPN

Enable	Enable / Disable the open VPN feature.
Server Address	Configure the hostname/IP and port of the server. For example: 192.168.1.2:22
Server Protocol	Specify the protocol user, user should use the same settings as used on the server
Device Mode	Use the same setting as used on the server. Dev TUN: Create a routed IP tunnel. Dev TAP: Create an Ethernet tunnel.
User Compression	Compress tunnel packets using the LZO algorithm on the VPN link. Don't enable this unless it is also enabled in the server config file.
CA Cert	Upload as SSL/TLS root certificate. This file will be renamed as 'ca.crt' automatically.
Client Cert	Upload a client certificate. This file will be renamed as 'cliend.crt' automatically.
Client Key	Upload a client private key. This file will be renamed as 'client.key' automatically.



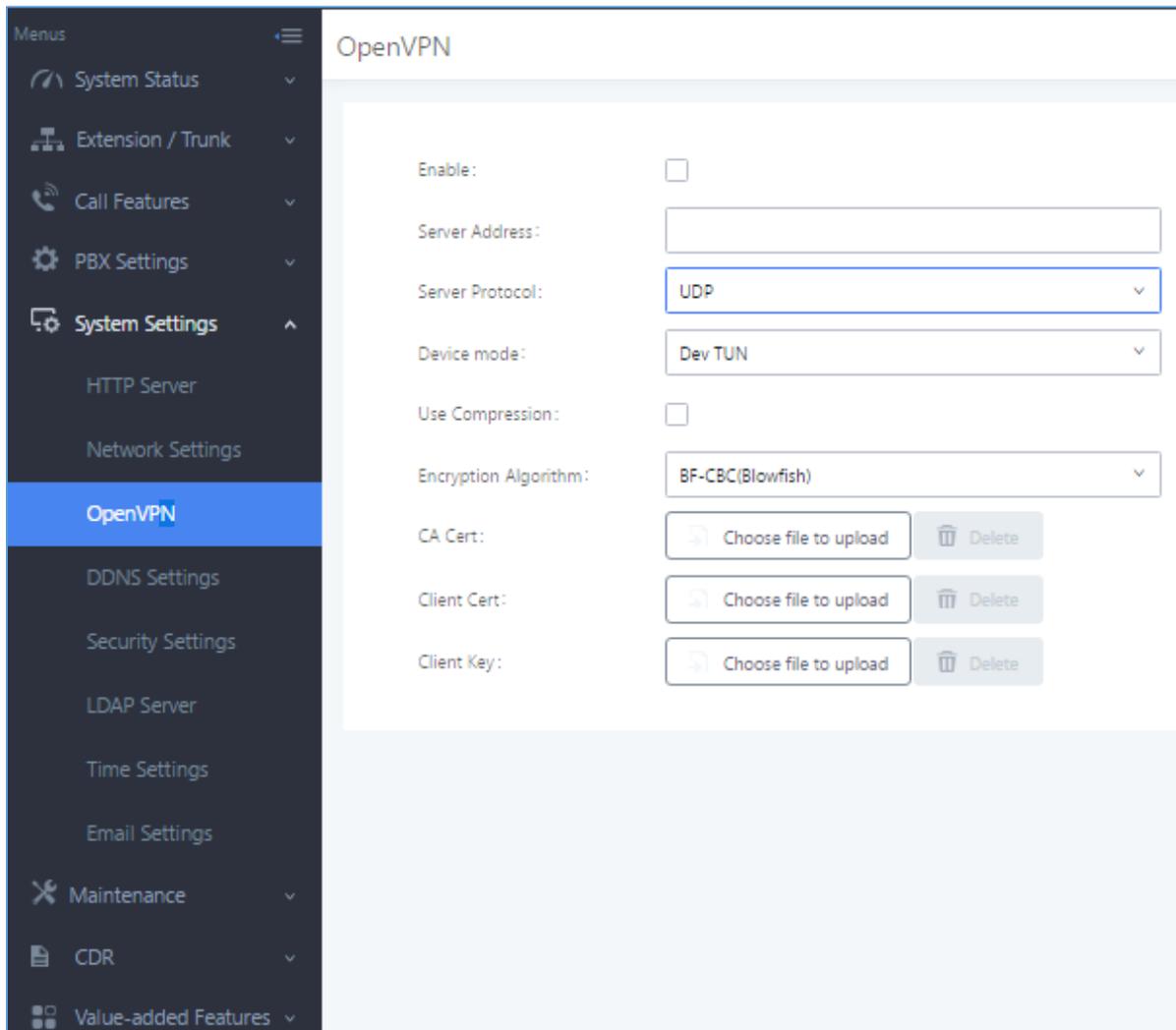


Figure 32: OpenVPN feature on the UCM6510

DDNS Settings

DDNS setting allows user to access UCM6510 via domain name instead of IP address.

The UCM6510 supports DDNS service from the following DDNS provider:

- dydns.org
- noip.com
- freedns.afraid.org
- zoneedit.com
- oray.net



Below is an example of using noip.com for DDNS.

1. Register domain in DDNS service provider. Please note the UCM6510 needs to have public IP access.

Hostname Information	
Hostname:	haograndstream.ddns.net 👉
Host Type:	<input checked="" type="radio"/> DNS Host (A) <input type="radio"/> DNS Host (Round Robin) <input type="radio"/> DNS Alias (CNAME) 👉 <input type="radio"/> Port 80 Redirect <input type="radio"/> Web Redirect
IP Address:	<input type="text" value="1.2.3.4"/> Last Update: 2015-01-07 17:29:20 PST 👉
Assign to Group:	<input type="text" value="- No Group -"/> 👉 Configure Groups
Enable Wildcard:	Wildcards are a Plus / Enhanced feature. Upgrade Now! 👉
Advanced Records:	TXT, SPF, and SRV records and the use of some special clients are Plus / Enhanced features. Upgrade now to use them. 👉

Figure 33: Register Domain Name on noip.com

2. On Web GUI→**System Settings**→**Network Settings**→**DDNS Settings**, enable DDNS service and configure username, password and host name.

Menus	DDNS Settings
System Status	DDNS Server: <input type="text" value="no-ip.com"/>
Extension / Trunk	Enable DDNS: <input checked="" type="checkbox"/>
Call Features	* Username: <input type="text" value="user_no_IP"/>
PBX Settings	* Password: <input type="text" value="....."/>
System Settings	* Host Name: <input type="text" value="MyGSPBX.ddns.net"/>
HTTP Server	
Network Settings	
OpenVPN	
DDNS Settings	

Figure 34: UCM6510 DDNS Setting



- Now you can use domain name instead of IP address to connect to the UCM6510 Web GUI.

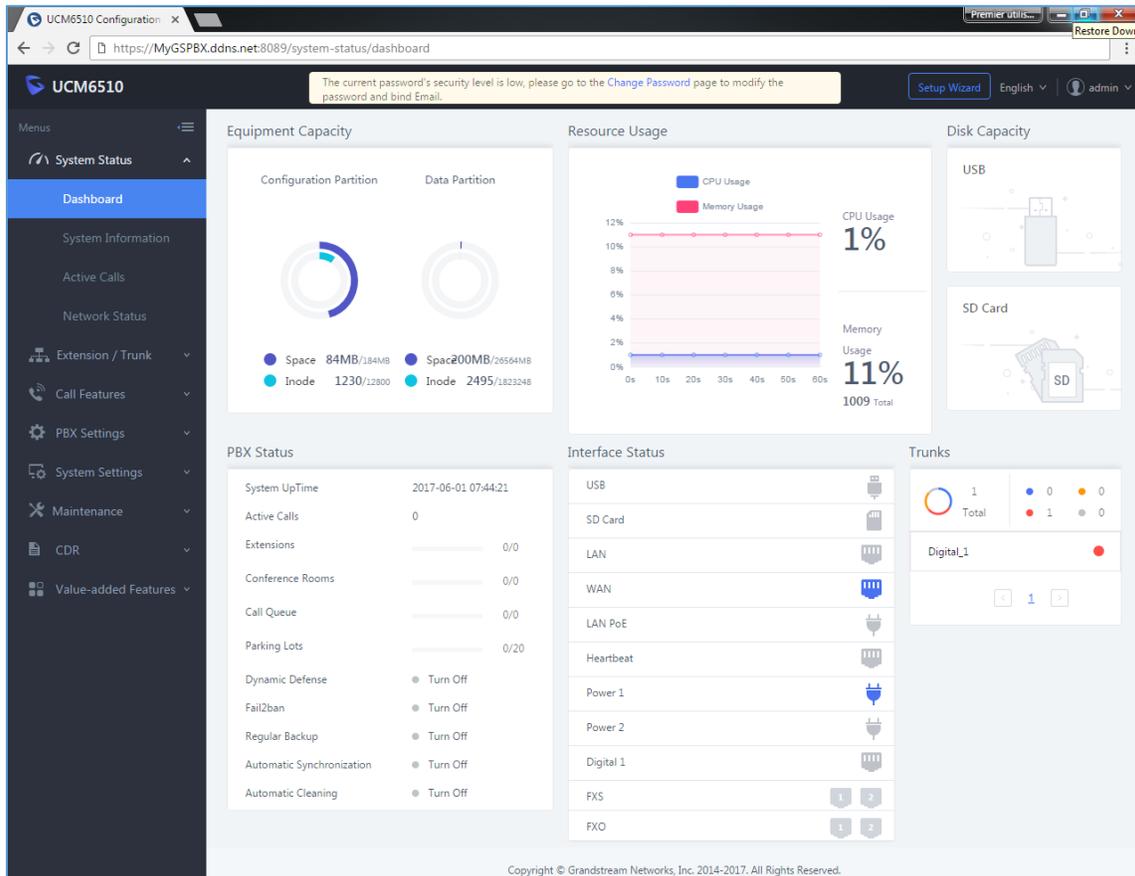


Figure 35: Using Domain Name to Connect to UCM6510

Security Settings

The UCM6510 provides users firewall configurations to prevent certain malicious attack to the UCM6510 system. Users could configure to allow, restrict or reject specific traffic through the device for security and bandwidth purpose. The UCM6510 also provides Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE.

To configure firewall settings in UCM6510, go to Web GUI→**System Settings**→**Security Settings** page.



Static Defense

Under Web GUI→**System Settings**→**Security Settings**→**Static Defense** page, users will see the following information:

- Current service information with port, process and type.
- Typical firewall settings.
- Custom firewall settings.

The following table shows a sample current service status running on the UCM6510.

Table 13: UCM6510 Security Settings→Static Defense→Current Service

Port	Process	Type
7777	Asterisk	TCP/IPv4
389	Slapd	TCP/IPv4
22	Dropbear	TCP/IPv4
80	Lighthttpd	TCP/IPv4
8089	Lighthttpd	TCP/IPv4
69	Opentftpd	UDP/IPv4
9090	Asterisk	UDP/IPv4
6060	zero_config	UDP/IPv4
5060	Asterisk	UDP/IPv4
4569	Asterisk	UDP/IPv4
5353	zero_config	UDP/IPv4
37435	Syslogd	UDP/IPv4

For typical firewall settings, users could configure the following options on the UCM6510.

Table 14: Typical Firewall Settings

Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping request. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN interface.
Ping-of-Death Defense Enable	Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN interface.

Under “Custom Firewall Settings”, users could create new rules to accept, reject or drop certain traffic going through the UCM6510. To create new rule, click on “Create New Rule” button and a new window will pop up for users to specify rule options.



The following figure shows a firewall rule example that will deny SSH access for the UCM6510 from WAN side.

Create New Firewall Rule

* Rule Name:

* Action:

* Type:

* Interface:

* Service:

Figure 36: Create New Firewall Rule

Table 15: Firewall Rule Settings

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. <ul style="list-style-type: none"> • ACCEPT • REJECT • DROP
Type	Select the traffic type. <ul style="list-style-type: none"> • IN If selected, users will need specify the network interface “LAN”, “WAN” or “Both” for the incoming traffic. • OUT
Service	Select the service type. <ul style="list-style-type: none"> • FTP • SSH • Telnet • TFTP • HTTP • LDAP • Custom If selected, users will need specify Source (IP and port), Destination (IP and port) and Protocol (TCP, UDP or Both) for the service. Please note if the source or the destination field is left blank, it will be used as “Anywhere”.



The new rule will be listed at the bottom of the page with sequence number, rule name, action, protocol, type, source, destination and operation. Users can click on  to edit the rule, or click on  to delete the rule. Save the change and reboot the device for the configuration to take effect.

Dynamic Defense

Dynamic defense can blacklist hosts dynamically when the UCM6510 is set to “Route” under Web GUI→**System Settings**→**Network Settings**→**Basic Settings: Method**. If enabled, the traffic via TCP connection coming into the UCM6510 can be monitored, which helps prevent massive connection attempts or brute force attacks to the device. The blacklist can be created and updated by the UCM6510 firewall, which will then be displayed in the web page. Please refer to the following table for dynamic defense options on the UCM6510.

Table 16: UCM6510 Firewall Dynamic Defense

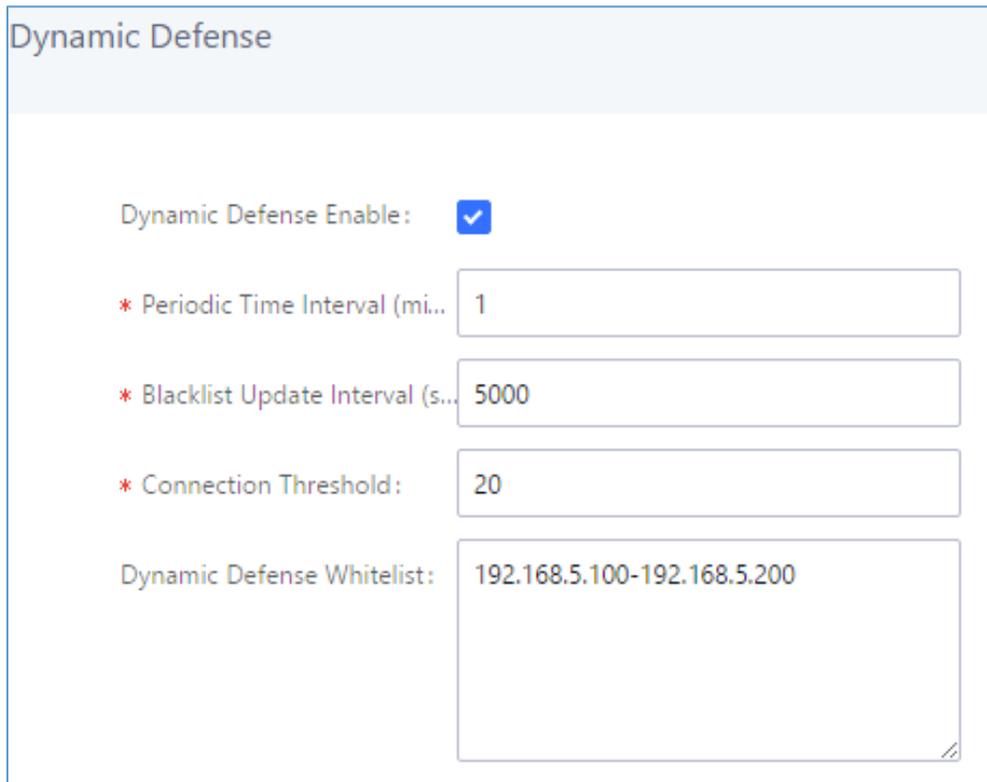
Dynamic Defense Enable	Enable dynamic defense. The default setting is disabled.
Periodical Time Interval	Configure the dynamic defense periodic time interval (in minutes). If the number of TCP connections from a host exceeds the “Connection Threshold” within this period, this host will be added into Blacklist. The valid value is between 1 and 59 when dynamic defense is turned on. The default setting is 59.
Blacklist Update Interval	Configure the blacklist update time interval (in seconds). The default setting is 120. This defines how long the IP will be blocked once added into the UCM6510 blacklist. For example, if it’s set to 300 seconds, the blocked IP address will only be able to establish TCP connection with the UCM6510 again after 300 seconds.
Connection Threshold	Configure the connection threshold. Once the number of connections from the same host reaches the threshold during “Periodical Time Interval”, it will be added into the blacklist. The default setting is 100.
Dynamic Defense Whitelist	Allowed IPs and ports range, multiple IP addresses and port range. For example: 192.168.5.100- 192.168.5.200 1500:2000

The following figure shows a configuration example like this:

- If a host at IP address 192.168.5.7 initiates more than 20 TCP connections to the UCM6510 within 1 minute, it will be added into UCM6510 blacklist.
- This host 192.168.5.7 will be blocked by the UCM6510 for 500 seconds.



- Since IP range 192.168.5.100-192.168.5.200 is in whitelist, if a host initiates more than 20 TCP connections to the UCM6510 within 1 minute, it will not be added into UCM6510 blacklist. It can still establish TCP connection with the UCM6510.



Dynamic Defense

Dynamic Defense Enable:

* Periodic Time Interval (mi... 1

* Blacklist Update Interval (s... 5000

* Connection Threshold: 20

Dynamic Defense Whitelist: 192.168.5.100-192.168.5.200

Figure 37: Configure Dynamic Defense

Fail2ban

Fail2Ban feature on the UCM6510 provides intrusion detection and prevention for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. Once the entry is detected within “Max Retry Duration”, the UCM6510 will take action to forbid the host for certain period as defined in “Banned Duration”. This feature helps prevent SIP brute force attacks to the PBX system.



Security Settings

Static Defense Dynamic Defense **Fail2ban** SSH Access

Global Settings

Enable Fail2Ban:

* Banned Duration:

* Max Retry Duration:

* MaxRetry:

Fail2ban Whitelist:

Local Settings

Asterisk Service:

Listening port number: UDP Port

* MaxRetry:

Login Attack Defense:

Listening port number: TCP Port

* MaxRetry:

Figure 38: Fail2ban Settings



Table 17: Fail2Ban Settings

Global Settings	
Enable Fail2Ban	Enable Fail2Ban. The default setting is disabled. Please make sure both “Enable Fail2Ban” and “Asterisk Service” are turned on in order to use Fail2Ban for SIP authentication on the UCM6510.
Banned Duration	Configure the duration (in seconds) for the detected host to be banned. The default setting is 600. If set to 0, the host will be always banned.
Max Retry Duration	Within this duration (in seconds), if a host exceeds the max times of retry as defined in “MaxRetry”, the host will be banned. The default setting is 600.
MaxRetry	Configure the number of authentication failures during “Max Retry Duration” before the host is banned. The default setting is 5.
Fail2Ban Whitelist	Configure IP address, CIDR mask or DNS host in the whitelist. Fail2Ban will not ban the host with matching address in this list. Up to 5 addresses can be added into the list.
Local Settings	
Asterisk Service	Enable Asterisk service for Fail2Ban. The default setting is disabled. Please make sure both “Enable Fail2Ban” and “Asterisk Service” are turned on in order to use Fail2Ban for SIP authentication on the UCM6510.
Protocol	Configure the listening port number for the service. Currently only 5060 (for UDP) is supported.
MaxRetry	Configure the number of authentication failures during “Max Retry Duration” before the host is banned. The default setting is 10. Please make sure this option is properly configured as it will override the “MaxRetry” value under “Global Settings”.
Login Attack Defense	Enables defense against excessive login attacks to the UCM’s web GUI. The default setting is disabled.
Listening Port Number	This is the Web GUI listening port number which is configured under System Settings → HTTP Server → Port . The default is 8089.
MaxRetry	When the number of failed login attempts from an IP address exceeds the MaxRetry number, that IP address will be banned from accessing the UCM Web UI.
Blacklist	
Blacklist	Users will be able to view the IPs that have been blocked by UCM.

SSH Access

SSH switch now is available via Web GUI and LCD. User can enable or disable SSH access directly from Web GUI or LCD screen. For web SSH access, please log in UCM6510 web interface and go to **System Settings**→**Security Settings**→**SSH Access**. By default, SSH access is disabled for security concerns. It is highly recommended to only enable SSH access for debugging purpose.



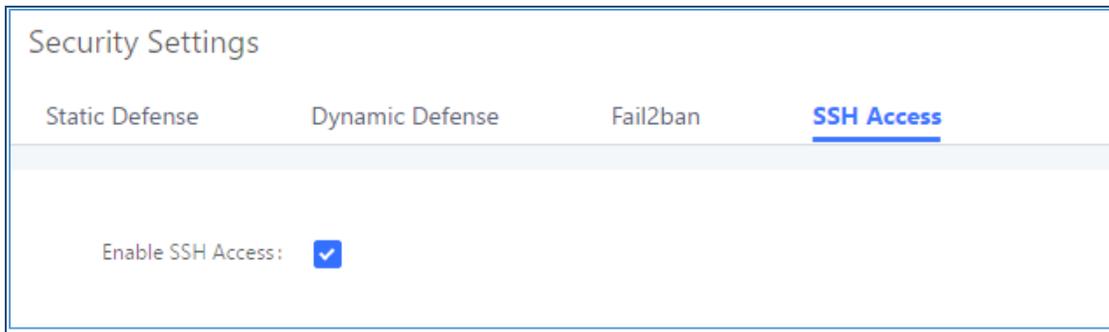


Figure 39: SSH Access

LDAP Server

The UCM6510 has an embedded LDAP server for users to manage corporate phonebook in a centralized manner.

- By default, the LDAP server has generated the first phonebook with **PBX DN** "ou=pbx,dc=pbx,dc=com" based on the UCM6510 user extensions already.
- Users could add new phonebook with a different **Phonebook DN** for other external contacts. For example, "ou=people,dc=pbx,dc=com".
- All the phonebooks in the UCM6510 LDAP server have the same **Base DN** "dc=pbx,dc=com".
- "cn" "ou" and "dc" are parts of LDAP data Interchange Format according to RFC 2849, which is how the LDAP tree is filtered.
 cn= Common Name
 ou= Organization Unit
 dc= Domain Component
- Here is an example of how the search for "ou=pbx,dc=pbx,dc=com" is performed in LDAP server query. From the dc=com Domain Component, find the dc=pbx Domain Component first. In the dc=pbx Domain Component, find the Organizational Unit called pbx (ou=pbx) and then find the object that has a Common Name of admin.

If users have the Grandstream phone provisioned by the UCM6510, the LDAP directory has been set up on the phone and can be used right away for users to access all phonebooks generated in the UCM6510.

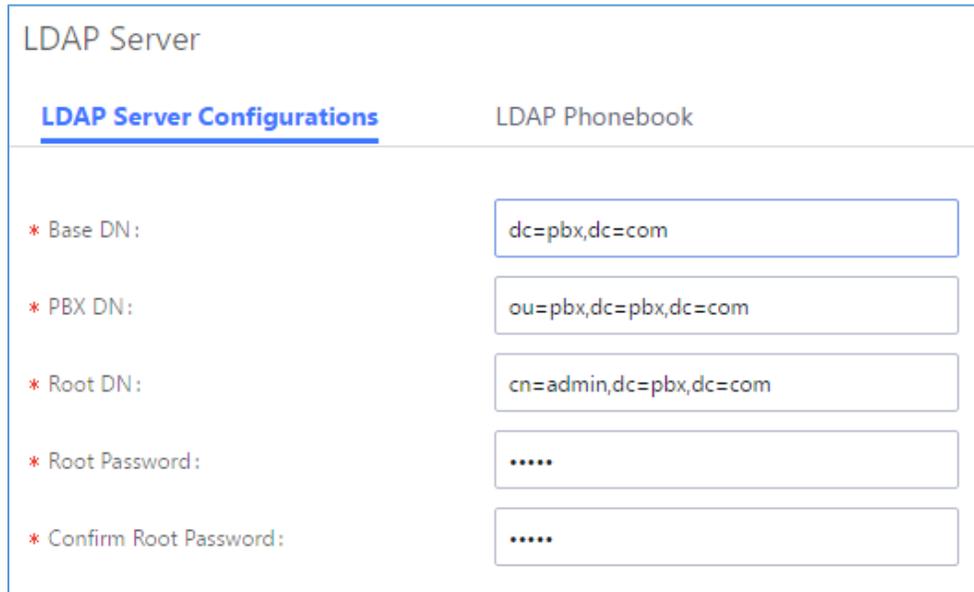
Additionally, users could manually configure the LDAP client settings to manipulate the built-in LDAP server on the UCM6510. If the UCM6510 has multiple LDAP phonebooks created, in the LDAP client configuration, users could use "dc=pbx,dc=com" as Base DN to have access to all phonebooks on the UCM6510 LDAP server, or use a specific phonebook DN, for example "ou=people,dc=pbx,dc=com", to access to phonebook with Phonebook DN "ou=people,dc=pbx,dc=com " only.



To access LDAP Server settings, go to **Web GUI→System Settings→LDAP Server**.

LDAP Server Configurations

The following figure shows the default LDAP server configurations on the UCM6510.



The screenshot shows the 'LDAP Server' configuration page with two tabs: 'LDAP Server Configurations' (active) and 'LDAP Phonebook'. The configuration fields are as follows:

Field	Value
* Base DN:	dc=pbx,dc=com
* PBX DN:	ou=pbx,dc=pbx,dc=com
* Root DN:	cn=admin,dc=pbx,dc=com
* Root Password:
* Confirm Root Password:

Figure 40: LDAP Server Configurations

The UCM6510 LDAP server supports anonymous access (read-only) by default. Therefore, the LDAP client doesn't have to configure username and password to access the phonebook directory. The "Root DN" and "Root Password" here are for LDAP management and configuration where users will need provide for authentication purpose before modifying the LDAP information.

The default phonebook list in this LDAP server can be viewed and edited by clicking on  for the first phonebook under LDAP Phonebook.

<input type="checkbox"/>	Phonebook DN ⇅	Options
<input type="checkbox"/>	ou=pbx,dc=pbx,dc=com	 

Figure 41: Default LDAP Phonebook DN



Edit Phonebook: pbx

+ Add Contact

AccountNumber ↕	CallerID Name ↕	Options
1000	John DOE	 
1001		 
1002		 
1003		 
1004		 
1005		 

Figure 42: Default LDAP Phonebook Attributes

LDAP Phonebook

Users could use the default phonebook, edit the default phonebook as well as add new phonebook on the LDAP server. The first phonebook with default phonebook dn “ou=pbx,dc=pbx,dc=com” displayed on the LDAP server page is for extensions in this PBX. Users cannot add or delete contacts directly. The contacts information will need to be modified via Web GUI→**Extension/Trunk**→**Extensions** first. The default LDAP phonebook will then be updated automatically.

- **Add new phonebook**

A new sibling phonebook of the default PBX phonebook can be added by clicking on “Add” under “LDAP Phonebook” section.

Add Phonebook
×

* Phonebook Prefix:

Phonebook DN:

Figure 43: Add LDAP Phonebook



Configure the “Phonebook Prefix” first. The “Phonebook DN” will be automatically filled in. For example, if configuring “Phonebook Prefix” as “people”, the “Phonebook DN” will be filled with “ou=people,dc=pbx,dc=com”.

Once added, users can select  to edit the phonebook attributes and contact list (see figure below), or select  to delete the phonebook.

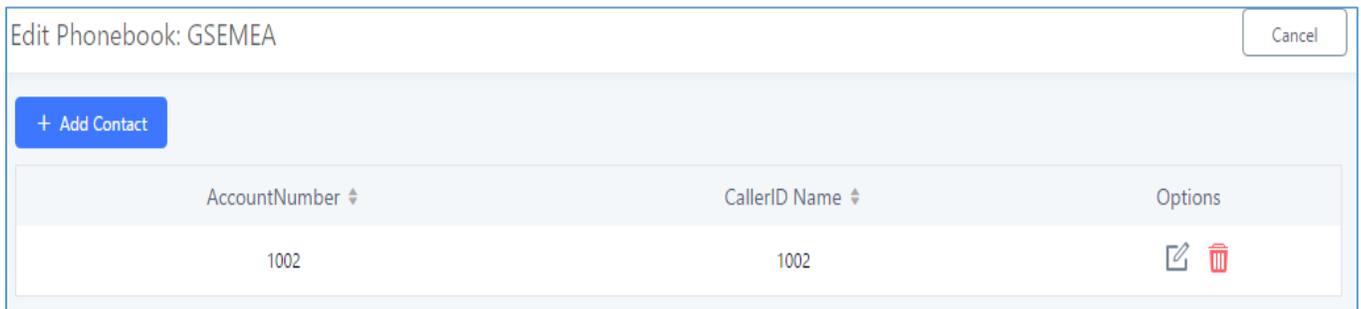


Figure 44: Edit LDAP Phonebook

- **Import phonebook from your computer to LDAP server**

Click on “Import Phonebook” and a dialog will prompt as shown in the figure below.

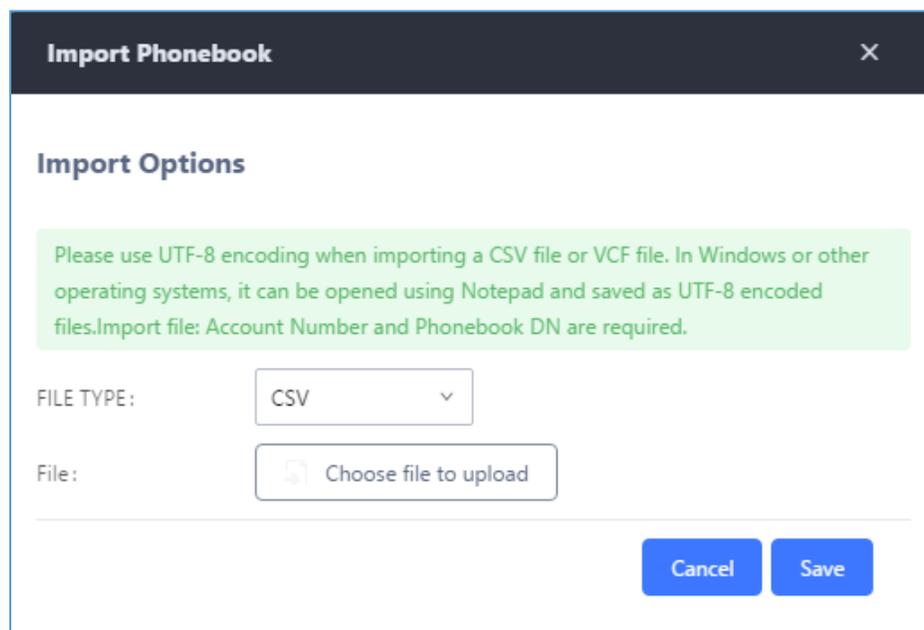


Figure 45: Import Phonebook

The file to be imported must be a CSV file with UTF-8 encoding. Users can open the CSV file with Notepad and save it with UTF-8 encoding.

Here is how a sample CSV file. Please note “Account Number” and “Phonebook DN” fields are required. Users could export a phonebook file from the UCM6510 LDAP phonebook section first and use it as a sample to start with.

	A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	1004	1004		Accounting	1004000000			phonebook
6	Steve	Chang	1005	1005		Support	1005000000			others

Figure 46: Phonebook CSV File Format

The Phonebook DN field is the same “Phonebook Prefix” entry as when the user clicks on “Add” to create a new phonebook. Therefore, if the user enters “phonebook” in “Phonebook DN” field in the CSV file, the actual phonebook DN “ou=phonebook,dc=pbx,dc=com” will be automatically created by the UCM6510 once the CSV file is imported.

In the CSV file, users can specify different phonebook DN fields for different contacts. If the phonebook DN already exists on the UCM6510 LDAP Phonebook, the contacts in the CSV file will be added into the existing phonebook. If the phonebook DN doesn’t exist on the UCM6510 LDAP Phonebook, a new phonebook with this phonebook DN will be created.

The sample phonebook CSV file in above picture will result in the following LDAP phonebook in the UCM6510.

LDAP Server

LDAP Server Configurations [LDAP Phonebook](#)

+ Add
Phonebook Download Configurations
Import Phonebook
Export Selected Phonebook

Note: The first phonebook is for extensions in this PBX. The contacts cannot be added or deleted directly. To add or delete the contacts, please modify the accounts in “Extensions” page first. To modify the read-only attributes, please edit the corresponding items in “Extension” page, and the phone book will be automatically updated when the change is saved and applied. Users can add other phonebooks for external accounts. For those phonebooks, users can edit LDAP attributes and add or delete contacts directly.

	Phonebook DN	Options
<input type="checkbox"/>	ou=GSEMEA,dc=pbx,dc=com	
<input type="checkbox"/>	ou=others,dc=pbx,dc=com	
<input type="checkbox"/>	ou=pbx,dc=pbx,dc=com	

Figure 47: LDAP Phonebook After Import

As the default LDAP phonebook with DN “ou=pbx,dc=pbx,dc=com” cannot be edited or deleted in LDAP phonebook section, users cannot import contacts with Phonebook DN field “pbx” if existed in the CSV file.



- **Export phonebook to your computer from UCM6510 LDAP server**

Select the checkbox for the LDAP phonebook and then click on “Export Selected Phonebook” to export the selected phonebook. The exported phonebook can be used as a record or a sample CSV file for the users to add more contacts in it and import to the UCM6510 again.

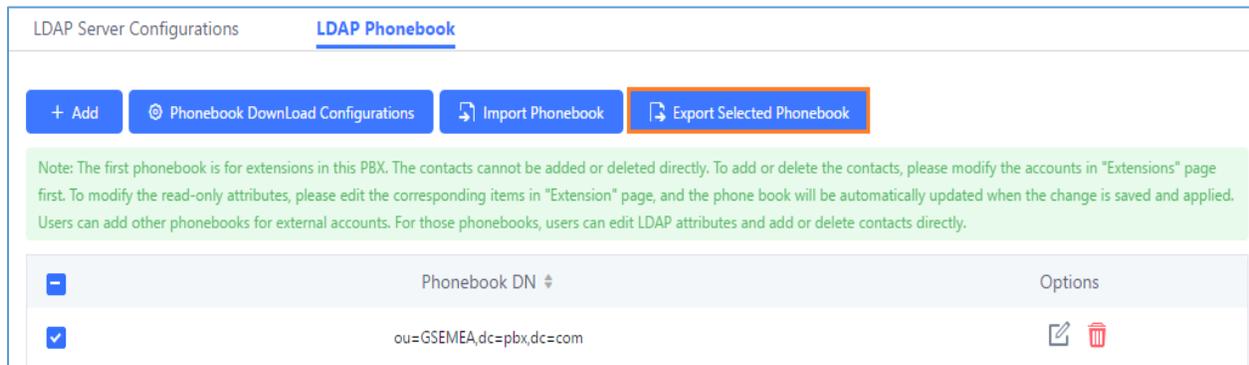


Figure 48: Export Selected LDAP Phonebook

LDAP Client Configurations

The configuration on LDAP client is similar when you use other LDAP servers. Here we provide an example on how to configure the LDAP client on the SIP end points to use the default PBX phonebook.

Assuming the server base dn is “dc=pbx,dc=com”, configure the LDAP clients as follows (case insensitive):

Base DN: dc=pbx,dc=com

Login DN: Please leave this field empty

Password: Please leave this field empty

Anonymous: Please enable this option

Filter: ((CallerIDName=%)(AccountNumber=%))

Port: 389

The following figure gives a sample configuration for UCM6510 acting as a LDAP client.

Phonebook DownLoad Configurations

<p>* LDAP Server: <input style="width: 80%;" type="text" value="LdapClient"/></p> <p>* Base DN: <input style="width: 80%;" type="text" value="dc=pbx,dc=com"/></p> <p>Password: <input style="width: 80%;" type="text" value="cn=admin,dc=pbx,d"/></p> <p>* Port: <input style="width: 80%;" type="text" value="389"/></p>	<p>* Server Address: <input style="width: 80%;" type="text" value="192.168.1.1"/></p> <p>User Name: <input style="width: 80%;" type="text" value="cn=admin,dc=pbx,d"/></p> <p>* Filter: <input style="width: 80%;" type="text" value="(objectClass=*)"/></p>
--	--

Figure 49: LDAP Client Configurations

To configure Grandstream IP phones as the LDAP client, please refer to the following example:

Server Address: The IP address or domain name of the UCM6510

Base DN: dc=pbx,dc=com

User Name: Please leave this field empty

Password: Please leave this field empty

LDAP Name Attribute: CallerIDName Email Department FirstName LastName

LDAP Number Attribute: AccountNumber MobileNumber HomeNumber Fax

LDAP Number Filter: (AccountNumber=%)

LDAP Name Filter: (CallerIDName=%)

LDAP Display Name: AccountNumber CallerIDName

LDAP Version: If existed, please select LDAP Version 3

Port: 389

The following figure shows the configuration information on a Grandstream GXP2170 to successfully use the LDAP server as configured in **[Figure 40: LDAP Server Configurations]**.



LDAP

LDAP protocol	<input type="text" value="LDAP"/>
Server Address	<input type="text" value="192.168.40.134"/>
Port	<input type="text" value="389"/>
Base	<input type="text" value="dc=pbx,dc=com"/>
User Name	<input type="text"/>
Password	<input type="password"/>
LDAP Number Filter	<input type="text" value="(AccountNumber=%)"/>
LDAP Name Filter	<input type="text" value="(CallerIDName=%)"/>
LDAP Version	<input type="radio"/> Version 2 <input checked="" type="radio"/> Version 3
LDAP Name Attributes	<input type="text" value="CallerIDName"/>
LDAP Number Attributes	<input type="text" value="AccountNumber"/>
LDAP Display Name	<input type="text" value="AccountNumber CallerIDName"/>
Max. Hits	<input type="text" value="50"/>
Search Timeout	<input type="text" value="30"/>
Sort Results	<input checked="" type="radio"/> No <input type="radio"/> Yes
LDAP Lookup	<input checked="" type="checkbox"/> Incoming Calls <input checked="" type="checkbox"/> Outgoing Calls
Lookup Display Name	<input type="text"/>

Figure 50: GXP2170 LDAP Phonebook Configuration

HTTP Server

The UCM6510 embedded web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow the users to configure the PBX through a web browser such as Microsoft IE, Mozilla Firefox and Google Chrome. By default, the PBX can be accessed directly by typing IP address in the PC's web browser (e.g., 192.168.40.50). It will then be automatically redirected to HTTPS using Port 8089 (e.g., <https://192.168.40.50:8089>). Users could also change the access protocol and port as preferred under Web GUI→**System Settings**→**HTTP Server**.



Table 18: HTTP Server Settings

Redirect From Port 80	Enable or disable redirect from port 80. On the PBX, the default access protocol is HTTPS and the default port number is 8089. When this option is enabled, the access using HTTP with Port 80 will be redirected to HTTPS with Port 8089. The default setting is “Enable”.
Protocol Type	Select HTTP or HTTPS as the protocol to access the HTTP server. The default setting is “HTTPS”. This also defines whether to use HTTP or HTTPS to download the config file in zero config as the UCM6510 is served as HTTP/HTTPS server that has the device config files for zero config.
Port	Specify port number to access the HTTP server. The default port is 8089.

Once the change is saved, the web page will be redirected to the login page using the new URL. Enter the username and password to login again.

Email

Email Settings

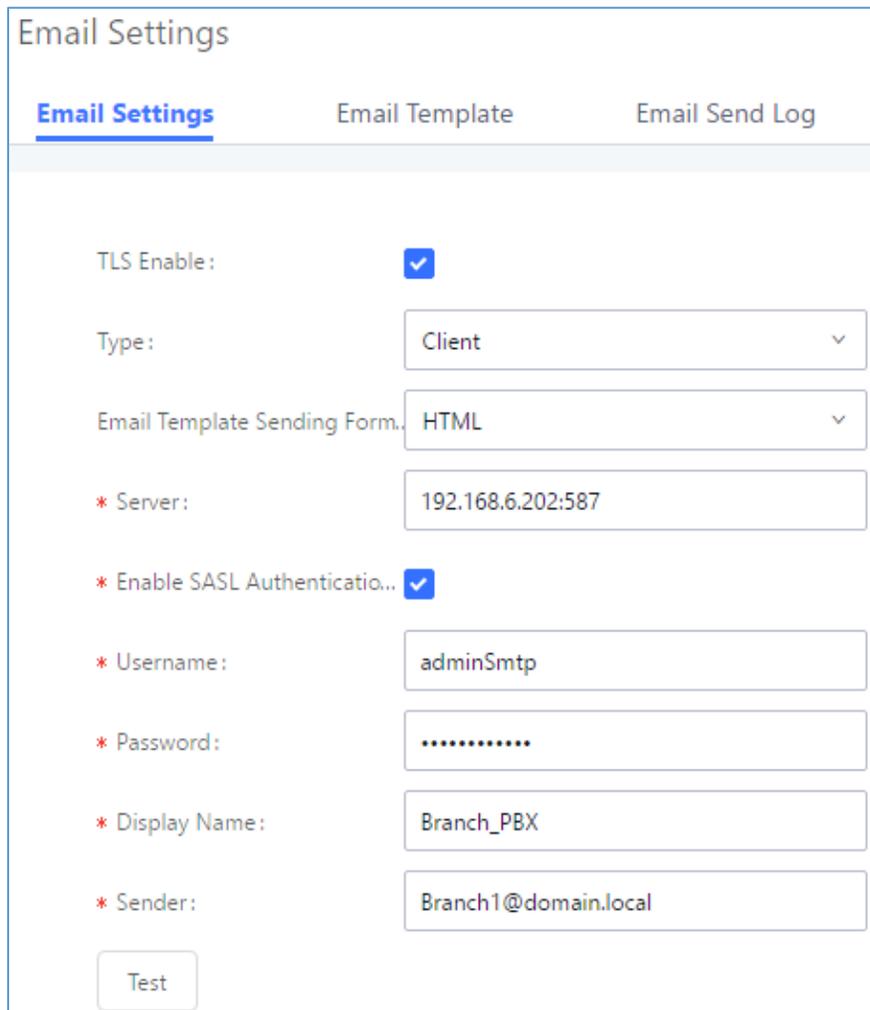
The Email application on the UCM6510 can be used to send out alert event Emails, Fax (Fax-To-Email), Voicemail (Voicemail-To-Email) and etc. The configuration parameters can be accessed via Web GUI→**System Settings**→**Email Settings**.

Table 19: Email Settings

TLS Enable	Enable or disable TLS during transferring/submitted your Email to another SMTP server. The default setting is “Yes”.
Type	<ul style="list-style-type: none"> • MTA: Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it or no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. • Client: Submit Emails to the SMTP server. A SMTP server is required and users need login with correct credentials.
Domain	Specify the domain name to be used in the Email when using type “MTA”.
Server	Specify the SMTP server when using type “Client”. For example, if using Gmail as the SMTP server, you can configure it as <i>smtp.gmail.com:465</i> .
Username	Username is required when using type “Client”. Normally it’s the Email address.
Password	Password to log in for the above Username (Email address) is required when using type “Client”.
Display Name	Specify the display name in the FROM header in the Email.
Sender	Specify the sender’s Email address. For example: <i>pbx@example.mycompany.com</i> .



The following figure shows a sample Email settings on the UCM6510, assuming the Email is using *smtp.gmail.com* as the SMTP server and the port number is 465.



The screenshot shows the 'Email Settings' configuration page. It has three tabs: 'Email Settings' (selected), 'Email Template', and 'Email Send Log'. The configuration includes the following fields:

- TLS Enable:**
- Type:** Client (dropdown menu)
- Email Template Sending Form..:** HTML (dropdown menu)
- * Server:** 192.168.6.202:587
- * Enable SASL Authenticatio...:**
- * Username:** adminSmtP
- * Password:** (masked)
- * Display Name:** Branch_PBX
- * Sender:** Branch1@domain.local

A 'Test' button is located at the bottom left of the configuration area.

Figure 51: UCM6510 Email Settings

Once the configuration is finished, click on “Save” first. Then click on “Test” button to make sure the Email setting is working.

The following figure shows the new dialog prompted to test the Email setting. Fill in a valid Email address to send a test Email to verify the Email settings on the UCM6510.

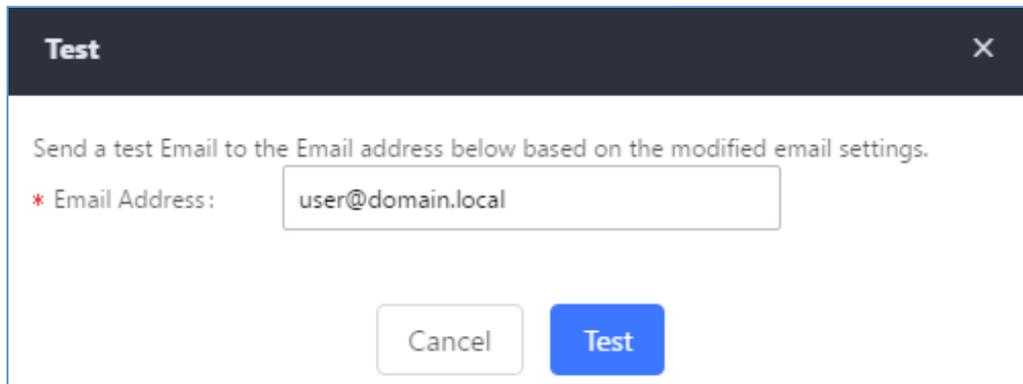


Figure 52: UCM6510 Email Settings: Send Test Email

Email Templates

The Email templates on the UCM6510 can be used for email notification the configuration parameters can be accessed via Web GUI→**System Settings**→**Email Settings**→**Email Templates**.

Email Settings				
Email Settings	<u>Email Template</u>	Email Send Log		
Type	Name	Time		Options
Extension	account_template.html	2017-05-02 10:20:22 UTC-04:00		
CDR	cdr_template.html	2017-05-02 10:20:22 UTC-04:00		
User Password	password_template.html	2017-05-02 10:20:22 UTC-04:00		
Alert Events	alert_template.html	2017-05-02 10:20:22 UTC-04:00		
Conference Schedule	conference_template.html	2017-05-02 10:20:22 UTC-04:00		
Voicemail	voicemail_template.html	2017-05-02 10:20:22 UTC-04:00		
Fax	fax_template.html	2017-05-02 10:20:22 UTC-04:00		

Figure 53: Email Templates

To configure the email template, simply click the  button under Options column, and edit the template as desired.



Edit Email Template: Conference Schedule
Save

* Subject:

* Message in Text Format:

```
{HELLO}
{CNFR_MSG}

Conference Schedule Details

This is the information of the schedule conference which you will attendee.

Topic:
{CNFR_TOPIC}
```

Message in HTML Format:

B I U ABB X² X₂ A A^{ab} A^{ab} | 段落 宋体 16px

```
{HELLO}
    {CNFR_MSG}

Conference Schedule Details

This is the information of the schedule conference which you will attendee.

Topic:
{CNFR_TOPIC}

Description:
{CNFR_DESCRIPTION}

Schedule Time:
```

Template Variables:
 {CNF_ACTION} : The action of this scheduled conference
 {CNF_THEME} : The theme of this conference email
 {CNF_STARTTIME} : The start time of this conference
 {CNF_ENDTIME} : The end time of this conference
 {CNF_ZONE} : Time Zone

Figure 54: Conference Schedule Template

Email Send Log

Under UCM Web GUI→**System Settings**→**Email Settings**→**Email Send Log**, users could search, filter and check whether the Email is sent out successfully or not. This page will also display the corresponding error message if the Email is not sent out successfully.



Email Settings

Email Settings Email Template Email Send Log

Email Send Log Filter

Show All Logs Delete All Logs

250 Mail sent successfully.

501 Address format parsing error. In MTA mode, If the recipient's email address contains unsupported characters, a 501 message will be returned. Please check if the format of the recipient's email address is correct. In Client mode, some servers also return 501 when the sender and mail accounts do not match. Please correct "Sender" for your "Mail Account".

535 There was a problem with account/password verification in client mode. Please check that "account and password" are configured correctly.

550 Possible Causes: (1)The recipient's email address does not exist or is in a disabled state. Please check the recipient's email address for errors.
 (2)The number of destination addresses sent by the sender exceeds the maximum daily limit and is temporarily blacklisted. Please decrease the sending frequency or try again the next day.
 (3)The sending IP does not pass the SPF permission detection of the sending domain. Messages sent in MTA mode may still return the error code even if they are sent successfully.

552 The message sent is too large, or the message attachment type is disabled.

553 Sender and mail account inconsistencies. Please configure the "Sender" for your "Mail Account".

554 The message is identified as spam. Please decrease the sending frequency or retry the next day.

none Means no return code. If the "sending result" is deferred, there may be a problem with the mail server configuration, Please check to see if the "server" configuration is correct. If the result is bounced, there may be a problem with the domain name of the recipient's email address. Please check the message's "recipient" to make sure it is correct. If in MTA mode, please make sure that "Domain" is configured to be in the same domain as the recipient.

In MTA mode, you cannot receive SPF authentication. Therefore, even if mail is sent successfully, the return code of 550 will still be returned. Many mail servers will place non-SPF-certified mail into the trash or quarantine mailbox. If the recipient has not received sent mail, please check to see if the sent mail was placed in the recipient's trash or quarantine mailbox.

In Client mode, a 250 return code means that the Email has been sent successfully from the UCM to your proxy mail server. The Email still fails to be sent due to invalid destination address or other reasons. Please login in your configuration mail account and check whether there is System bounce notification to confirm the cause of the failure.

Figure 55: Email Send log

Table 20: Email Log

Field	Description
Start Time	Enter the start time for filter
End Time	Enter the end time for filter
Receivers	Enter the email recipient, while searching for multiple recipients, please separate then with comma and no spaces.
Send Result	Enter the status of the send result to filter with
Return Code	Enter the email code to filter with
Email Send Module	Select the email module to filter with from the drop-down list, which contains: All Modules Extension Voicemail Conference Schedule User Password Alert Events CDR Fax Test



Email logs will be shown on bottom of “Email Send Log” page, as shown on the following figure.

Email Generated Time	Email Send Module	Receivers	Last Send Time	Last Send Address	Send Result	Return Code	Options
2017-05-03 03:43:16	Test	mbaomar@grandstream.com	05-03 03:43:18	mbaomar@grandstream.com	sent	250	
2017-05-03 03:43:10	Test	mbaomar@grandstream.com	05-03 03:43:13	mbaomar@grandstream.com	sent	250	

Figure 56: Email Logs

Time Settings

Auto Time Updating

The current system time on the UCM6510 is displayed on status web page. It can be found under Web GUI→**System Status**→**Dashboard**.

To configure the UCM6510 to update time automatically, go to Web GUI→**System Settings**→**Time Settings**→**Auto Time Updating**.



Note:

The configurations under Web GUI→**System Settings**→**Time Settings**→**Time Auto Updating** page require reboot to take effect. Please consider configuring auto time updating related changes when setting up the UCM6510 for the first time to avoid service interrupt after installation and deployment in production.

Table 21: Auto Time Updating

Remote NTP Server	Specify the URL or IP address of the NTP server for the UCM6510 to synchronize the date and time. The default NTP server is ntp.ipvideotalk.com.
Enable DHCP Option 2	If set to “Yes”, the UCM6510 can get provisioned for Time Zone from DHCP Option 2 in the local server automatically. The default setting is “Yes”.
Enable DHCP Option 42	If set to “Yes”, the UCM6510 is allowed to get provisioned for NTP Server from DHCP Option 42 in the local server automatically. This will override the manually configured NTP Server. The default setting is “Yes”.
Time Zone	Select the proper time zone option so the UCM6510 can display correct time accordingly. If “Self-Defined Tome Zone” is selected, please specify the time zone parameters in “Self-Defined Time Zone” field as described in below option.



Self-Defined Time Zone

If “Self-Defined Time Zone” is selected in “Time Zone” option, users will need define their own time zone following the format below.

The syntax is: std offset dst [offset], start [/time], end [/time]

Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0

MTZ+6MDT+5

This indicates a time zone with 6 hours offset and 1 hour ahead for DST, which is U.S central time. If it is positive (+), the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian); If it is negative (-), the local time zone is east.

M4.1.0,M11.1.0

The 1st number indicates Month: 1, 2, 3..., 12 (for Jan, Feb...Dec.).

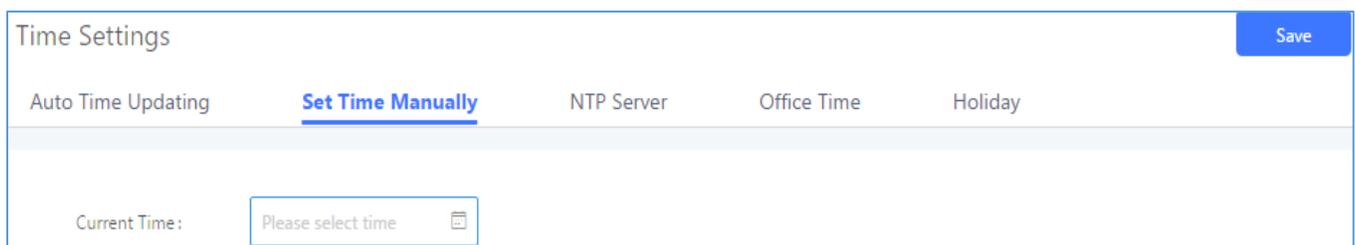
The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday...). Normally 1, 2, 3, 4 are used. If 5 is used, it means the last iteration of the weekday.

The 3rd number indicates weekday: 0, 1, 2...6 (for Sun, Mon, Tues... Sat).

Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.

Set Time Manually

To manually set the time on the UCM6510, go to Web GUI→**System Settings**→**Time Settings**→**Set Time Manually**. The format is YYYY-MM-DD HH:MI:SS.



Time Settings Save

Auto Time Updating Set Time Manually NTP Server Office Time Holiday

Current Time: 

Figure 57: Set Time Manually



Note:

Manually setup time will take effect immediately after saving and applying change in the Web GUI. If users would like to reboot the UCM6510 and keep the manually setup time setting, please make sure “Remote NTP Server”, “Enable DHCP Option 2” and “Enable DHCP Option 42” options under Web GUI→**System Settings**→**Time Settings**→**Time Auto Updating** page are unchecked or set to empty. Otherwise, time auto updating settings in this page will take effect after reboot.

Office Time

On the UCM6510, the system administrator can define “office time”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure office time, go to Web GUI→**System Settings**→**Time Settings**→**Office Time**. Click on “Create New Office Time” to create an office time.

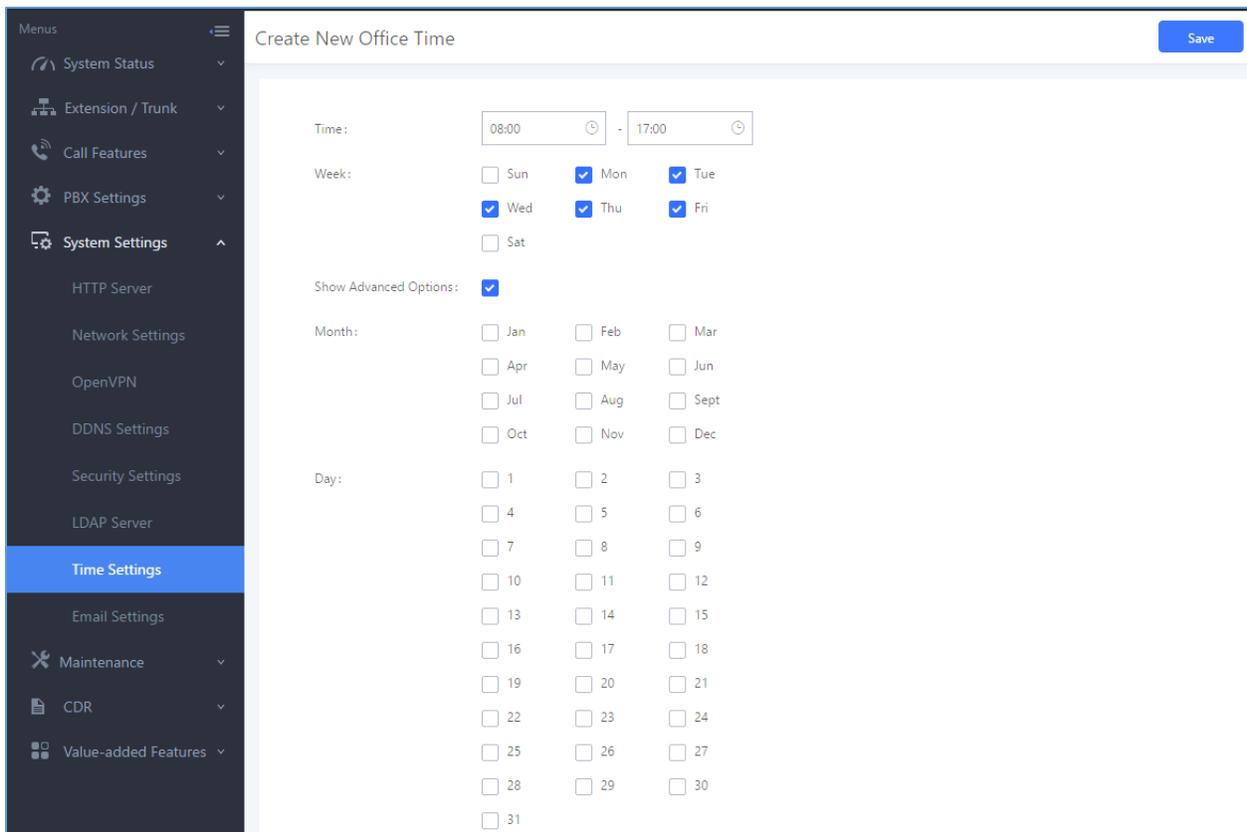


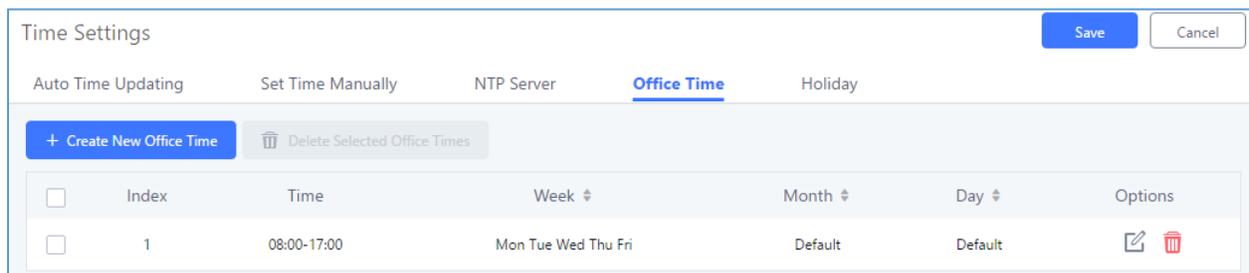
Figure 58: Create New Office Time



Table 22: Create New Office Time

Start Time	Configure the start time for office hour.
End Time	Configure the end time for office hour
Week	Select the work days in one week.
Show Advanced Options	Check this option to show advanced options. Once selected, please specify “Month” and “Day” below.
Month	Select the months for office time.
Day	Select the work days in one month.

Select “Start Time”, “End Time” and the day for the “Week” for the office time. The system administrator can also define month and day of the month as advanced options. Once done, click on “Save” and then “Apply Change” for the office time to take effect. The office time will be listed in the web page as the figure shows below.


Figure 59: System Settings→Time Settings→Office Time

- Click on  to edit the office time.
- Click on  to delete the office time.
- Click on “Delete Selected Office Times” to delete multiple selected office times at once.

Holiday

On the UCM6510, the system administrator can define “holiday”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure holiday, go to Web GUI→**System Settings**→**Time Settings**→**Holiday**. Click on “Create New Holiday” to create holiday time.

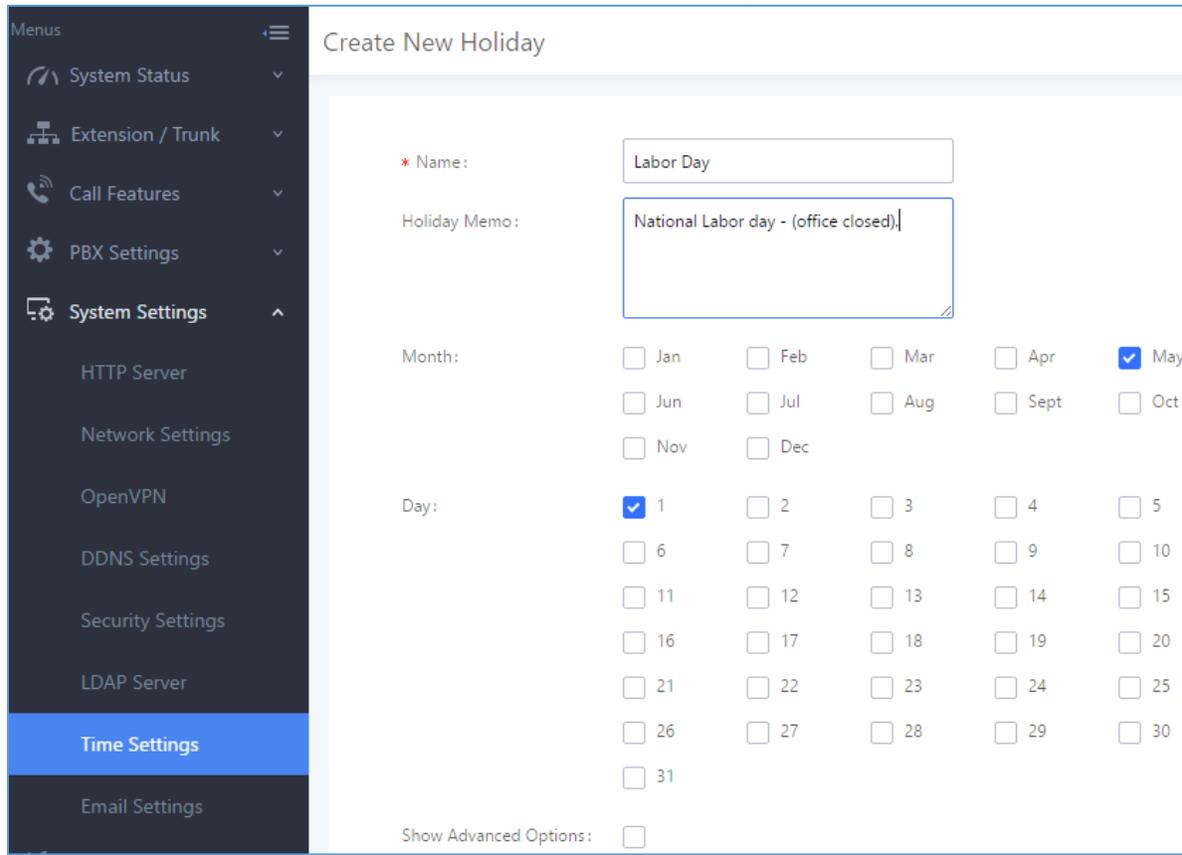


Figure 60: Create New Holiday

Table 23: Create New Holiday

Name	Specify the holiday name to identify this holiday.
Holiday Memo	Create a note for the holiday.
Month	Select the month for the holiday.
Day	Select the day for the holiday.
Show Advanced Options	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
Week	Select the days as holiday in one week.

Enter holiday “Name” and “Holiday Memo” for the new holiday. Then select “Month” and “Day”. The system administrator can also define days in one week as advanced options. Once done, click on “Save” and then “Apply Change” for the holiday to take effect. The holiday will be listed in the web page as the figure shows below.



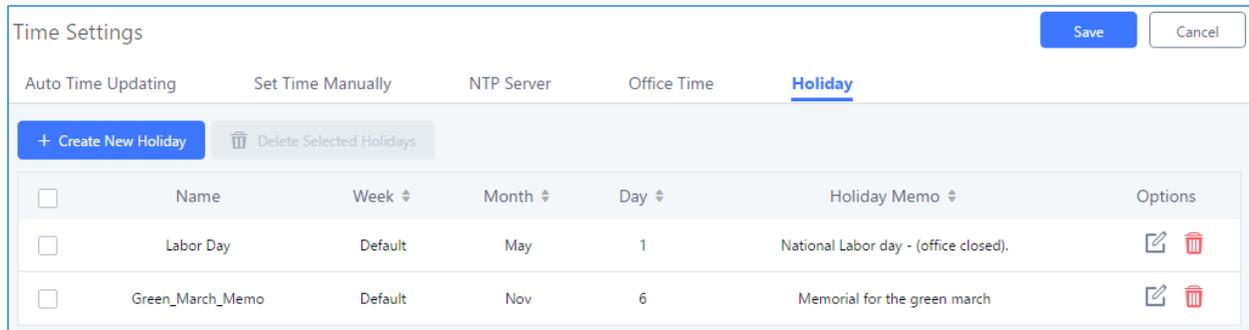


Figure 61: System Settings→Time Settings→Holiday

- Click on  to edit the holiday.
- Click on  to delete the holiday.
- Click on “Delete Selected Holidays” to delete multiple selected holidays at once.

 **Note:**

For more details on how to use office time and holiday, please refer to the link below:

http://www.grandstream.com/sites/default/files/Resources/How_to_use_office_time_and_holiday_UCM6xx.pdf

NTP Server

The UCM6510 can be used as a NTP server for the NTP clients to synchronize their time with. To configure the UCM6510 as the NTP server, set “Enable NTP server” to “Yes” under Web GUI→**System Settings→Time Settings→NTP Server**. On the client side, point the NTP server address to the UCM6510 IP address or host name to use the UCM6510 as the NTP server.



Recordings Storage

The UCM6510 supports call recordings automatically or manually and the recording files can be saved in external storage plugged in the UCM6510 or on the UCM6510 locally. To manage the recording storage, users can go to UCM6510 Web GUI→**PBX Settings**→**Recordings Storage** page and select whether to store the recording files in USB Disk, SD card or locally on the UCM6510.

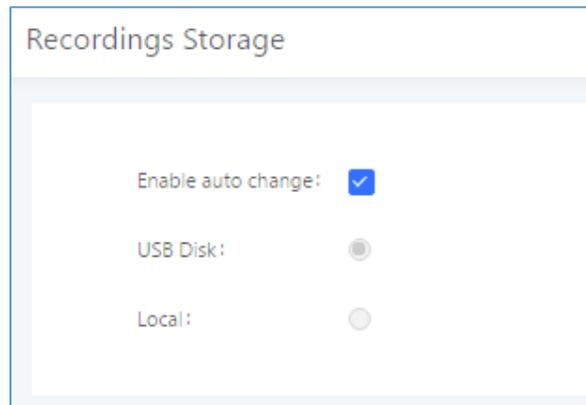


Figure 62: PBX Settings→Recordings Storage

- If **“Enable Auto Change”** is selected, the recording files will be automatically saved in the available USB Disk or SD card plugged into the UCM6510. If both USB Disk and SD card are plugged in, the recording files will be always saved in the USB Disk.
- If **“Local”** is selected, the recordings will be stored in UCM6510 internal storage.
- If **“USB Disk”** or **“SD Card”** is selected, the recordings will be stored in the corresponding plugged in external storage device. Please note the options “USB Disk” and “SD Card” will be displayed only if they are plugged into the UCM6510.

Once “USB Disk” or “SD Card” is selected, click on “OK”. The user will be prompted to confirm to copy the local files to the external storage device.

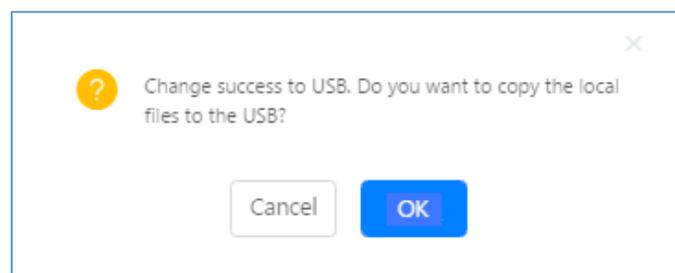


Figure 63: Recordings Storage Prompt Information



Click on “OK” to continue. The users will be prompted a new dialog to select the categories for the files to be copied over.

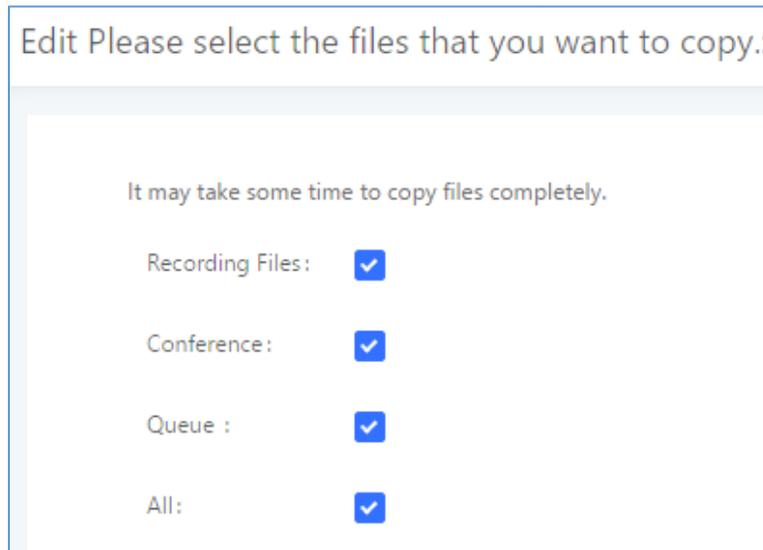


Figure 64: Recording Storage Category

On the UCM6510, recording files are generated and exist in 3 categories: normal call recording files, conference recording files, and call queue recording files. Therefore, users have the following options when select the categories to copy the files to the external device:

- **Recording Files:** Copy the normal recording files to the external device.
- **Conference:** Copy the conference recording files to the external device.
- **Queue:** Copy the call queue recording files to the external device.
- **All:** Copy all recording files to the external device.

Login Settings

After the user logs in the UCM6510 Web GUI, the user will be automatically logged out after certain timeout, or he/she can be banned for a specific period if the login timeout is exceeded. Those values can be specified under UCM6510 Web GUI→**Maintenance**→**Change Information**→**Login Settings** page.

The “**User Login Timeout**” value is in minute and the default setting is 10 minutes. If the user doesn’t make any operation on Web GUI within the timeout, the user will be logged out automatically. After that, the Web GUI will be redirected to the login page and the user will need to enter username and password to log in. If set to 0, there is no timeout for the Web GUI login session and the user will not be automatically logged out.



“**Maximum number of login attempts**” can prevent the UCM6510 from brutal force decryption, if this number is exceeded user IP address will be banned from accessing the UCM for a period of time based on user configuration, the default value is 5.

“**User ban period**” specify the period of time in minutes an IP will be banned from accessing the UCM if the User max number of try login is exceeded, the default value is 5.

“**Login Banned User List**” show the list of IPs’ banned from the UCM.

“**Login White List**” User can add a list of IPs’ to avoid the above restriction, thus, they can exceed the User max number of try login

Change Information Save

Change Password / Email [Login Settings](#)

* User Login Timeout:

* Maximum number of login attempts:

* User ban period:

Login Banned User List

No Data

Login Whitelist

[+ Add](#)

The IP addresses in the Login Whitelist will not be restricted. This option doesn't support network segment format.

No Data

Figure 65: Login Timeout Settings



Google Service Settings Support

UCM6510 now supports Google OAuth 2.0 authentication. This feature is used for supporting UCM6510 conference scheduling system. Once OAuth 2.0 is enabled, UCM6510 conference system can access Google calendar to schedule or update conference.

Google Service Settings can be found under Web GUI → **Call Features** → **Conference** → **Google Service Settings**.

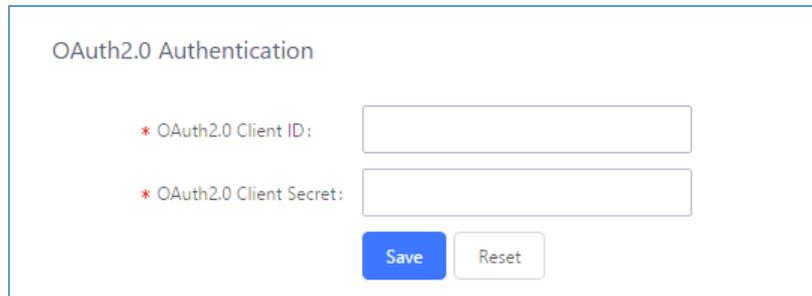


Figure 66: Google Service Settings: OAuth2.0 Authentication

If you already have OAuth2.0 project set up on **Google Developers** web page, please use your existing login credential for “OAuth2.0 Client ID” and “OAuth2.0 Client Secret” in the above figure for the UCM6510 to access Google Service.

If you do not have OAuth2.0 project set up yet, please following the steps below to create new project and obtain credentials:

1. Go to Google Developers page <https://console.developers.google.com/start> Create a New Project in Google Developers page.

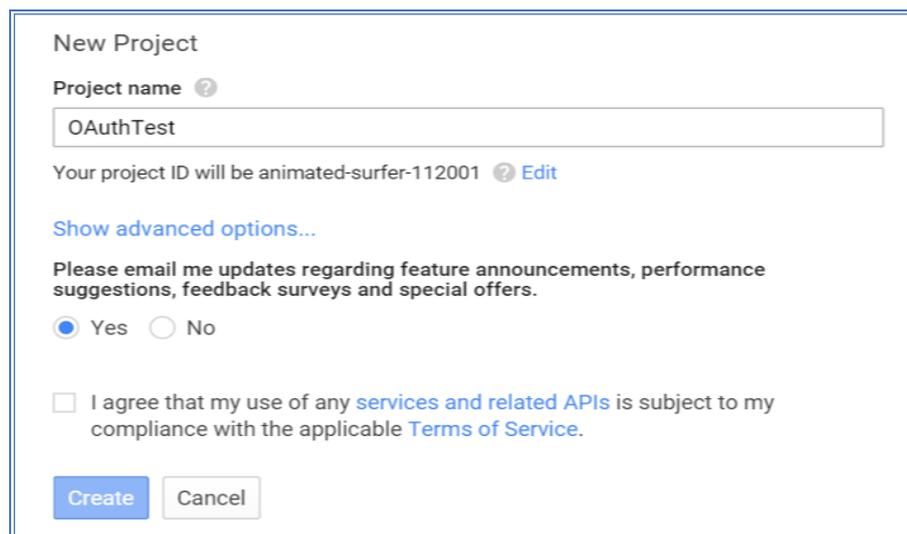


Figure 67: Google Service: New Project



2. Enable Calendar API from API Library.
3. Click “Credentials” on the left drop down menu to create new OAuth2.0 login credentials.

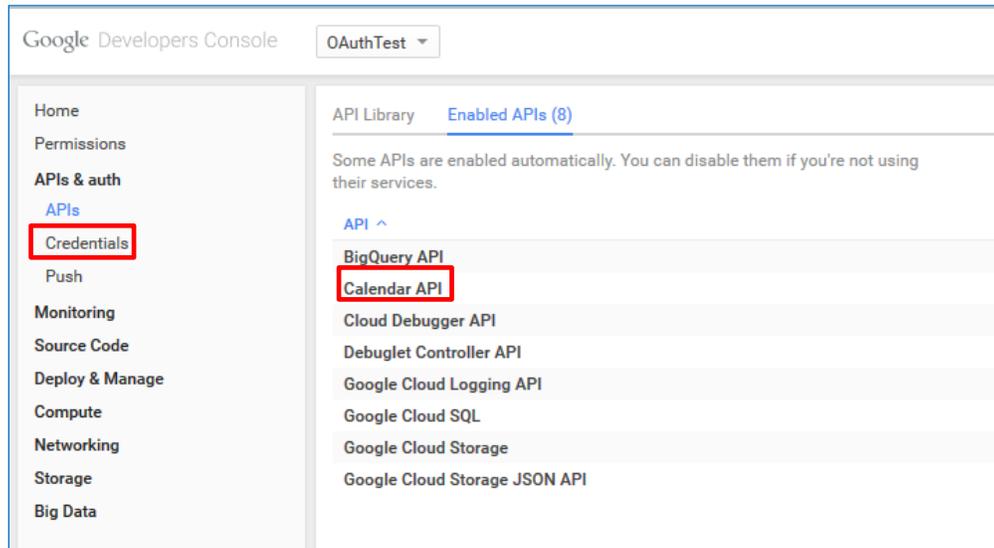


Figure 68: Google Service: Create new credential

4. Use the newly created login credential to fill in “OAuth2.0 Client ID” and “OAuth2.0 Client Secret”.
5. Click “Get Authentication Code” to obtain authentication code from Google Service.

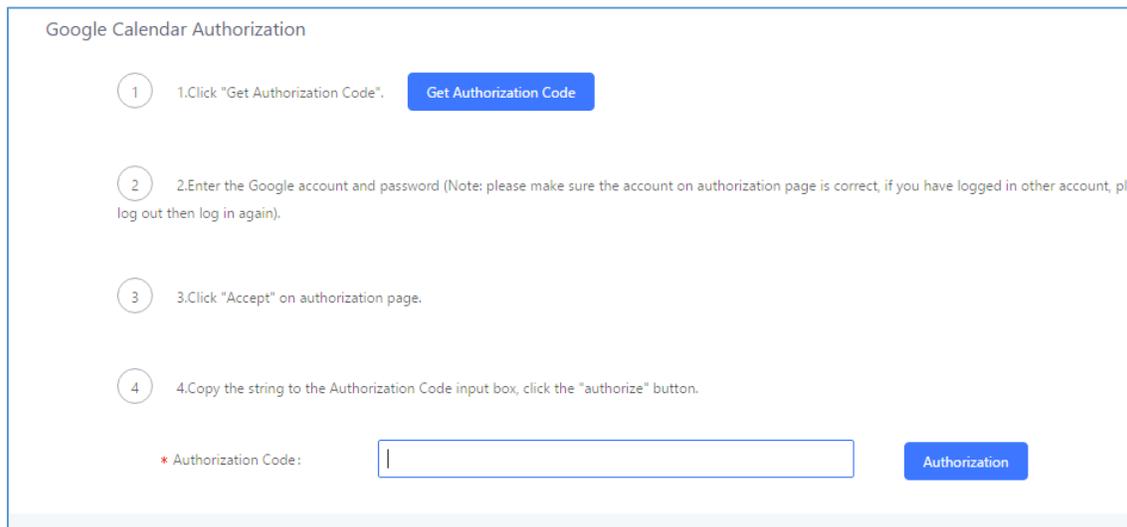


Figure 69: Google Service: OAuth2.0 login

6. Now UCM6510 is connected with Google Service.



PROVISIONING

Overview

Grandstream SIP Devices can be configured via Web interface as well as via configuration file through TFTP/HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file and XML format configuration file. The UCM6510 provides a Plug and Play mechanism to auto-provision the Grandstream SIP devices in a zero configuration manner by generating XML config file and having the phone to download it within LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

To provision a phone, three steps are involved, i.e., discovery, configuration and provisioning. This section explains how Zero Config works on the UCM6510. The settings for this feature can be accessed via Web GUI→**Value-added Features**→**Zero Config**.

Configuration Architecture for End Point Device

The end point device configuration in Zero Config is divided into the following three layers with priority from the lowest to the highest:

- **Global**

This is the lowest layer. Users can configure the most basic options that could apply to all Grandstream SIP devices during provisioning via Zero Config.

- **Model**

In this layer, users can define model-specific options for the configuration template.

- **Device**

This is the highest layer. Users can configure device-specific options for the configuration for individual device here.

Each layer also has its own structure in different levels. Please see figure below. The details for each layer are explained in sections **[Global Configuration]**, **[Model Configuration]** and **[Device Configuration]**.



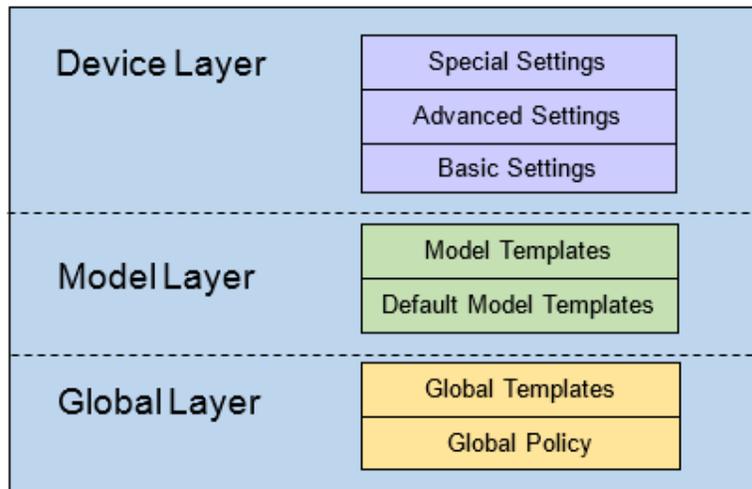


Figure 70: Zero Config Configuration Architecture for End Point Device

The configuration in model layer and device layer have all the options in global layers already, i.e., the options in global layer is a subset of the options in model layer and device layer. If an option is set in all three layers with different values, the highest layer value will override the value in lower layer. For example, if the user selects English for Language setting in Global Policy and Spanish for Language setting in Default Model Template, the language setting on the device to be provisioned will use Spanish as model layer has higher priority than global layer. To sum up, **configurations in higher layer will always override the configurations for the same options/fields in the lower layer when presented at the same time.**

After understanding the Zero Config configuration architecture, users could configure the available options for end point devices to be provisioned by the UCM6510 by going through the three layers. This configuration architecture allows users to set up and manage the Grandstream end point devices in the same LAN area in a centralized way.

Auto Provisioning Settings

By default, the Zero Config feature is enabled on the UCM6510 for auto provisioning. Two methods of auto provisioning are used.



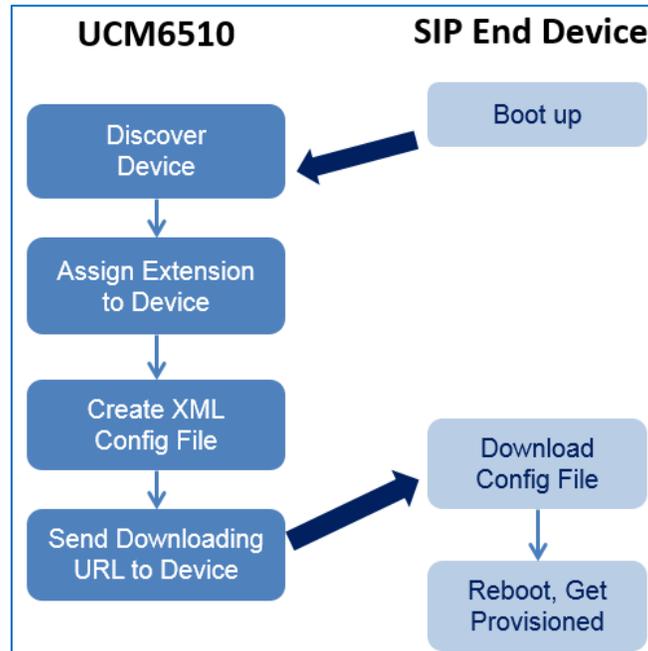


Figure 71: UCM6510 Zero Config

- **SIP SUBSCRIBE**

When the phone boots up, it sends out SUBSCRIBE to a multicast IP address in the LAN. The UCM6510 discovers it and then sends a NOTIFY with the XML config file URL in the message body. The phone will then use the path to download the config file generated in the UCM6510 and take the new configuration.

- **DHCP OPTION 66**

This method should be used only when the UCM6510 is set to “Route” mode under Web GUI→**System Settings**→**Network Settings**→**Basic Settings**: Method. When the phone restarts (by default DHCP Option 66 is turned on), it will send out a DHCP DISCOVER request. The UCM6510 receives it and returns DHCP OFFER with the config server path URL in the Option 66, for example, <https://192.168.2.1:8089/zccgi/>. The phone will then use the path to download the config file generated in the UCM6510.

To start the auto provisioning process, under Web GUI→**Value-added Features**→**Zero Config**→**Zero Config Settings**, fill in the auto provision information.



Zero Config

[Zero Config](#) [Global Policy](#) [Global Templates](#) [Model Templates](#) [Model Update](#) [Zero Config Settings](#)

Basic Settings

Enable Zero Config:

Enable Automatic Configura...

Extension Assignment

Auto provision automatically provides an extension to the device.
 There are two methods of auto provision: SIP SUBSCRIBE and DHCP Option 66.

For example, when the device boots up, it will send SIP SUBSCRIBE multicast in the LAN. The PBX will find it, create an account and return a URL of the config file for the device to download.

Auto Assign Extension:

Zero Config Extension Segm...5000 - 6299 [Zero Config Extension Segment](#)

Enable Pick Extension:

Pick Extension Segment: 4000 - 4999 [Pick Extension Segment](#)

Pick Extension Period (hour)...

Network Settings

Subnet Whitelist: +

[Save](#)

Figure 72: Auto Provision Settings

Table 24: Auto Provision Settings

Enable Zero Config	Enable or disable the Zero Config feature on the PBX. The default setting is enabled.
Enable Automatic Configuration Assignment	<p>By default, this is disabled. If disabled, when SIP device boots up, the UCM6510 will only send the configuration path to the device when you have any manual configuration on the device. This manual configuration includes:</p> <ul style="list-style-type: none"> Any configuration under BASIC and CUSTOM page of the device in Zero Config page If any global or model template (except for the default template) is selected for the assigned device in Zero Config page. <p>Note: When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the UCM6510 which will include the XML config file URL for the SIP device to download.</p>

Auto Assign Extension	If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in “Zero Config Extension Segment” to the device. The default setting is disabled.
Zero Config Extension Segment	Click on the link “Zero Config Extension Segment” to specify the extension range to be assigned if “Automatically Assign Extension” is enabled. The default range is 5000-6299. Zero Config Extension Segment range can be defined in Web GUI→ PBX Settings → General Settings page→Extension Preference section: “Auto Provision Extensions”.
Enable Pick Extension	If enabled, the extension list will be sent out to the device after receiving the device’s request. This feature is for the GXP series phones that support selecting extension to be provisioned via phone’s LCD. The default setting is disabled.
Pick Extension Segment	Click on the link “Pick Extension Segment” to specify the extension list to be sent to the device. The default range is 4000 to 4999. Pick Extension Segment range can be defined in Web GUI→ PBX Settings → General Settings → General page→Extension Preference section: “Pick Extensions”.
Pick Extension Period (hour)	Specify the number of minutes to allow the phones being provisioned to pick extensions.
Subnet Whitelist	<p>This feature allows the UCM to provision devices in different subnets other than UCM network.</p> <p>Enter subnets IP addresses to allow devices within these subnets to be provisioned. The syntax is <IP>/<CIDR>.</p> <p><u>Examples:</u></p> <p>10.0.0.1/8</p> <p>192.168.6.0/24</p> <p>Note: Only private IP ranges (10.0.0.0 172.16.0.0 192.168.0.0) are supported.</p>

Please make sure an extension is manually assigned to the phone or “Automatically Assign Extension” is enabled during provisioning. After the configuration on the UCM6510 Web GUI, click on “Save” and “Apply Changes”. Once the phone boots up and picks up the config file from the UCM6510, it will take the configuration right away.

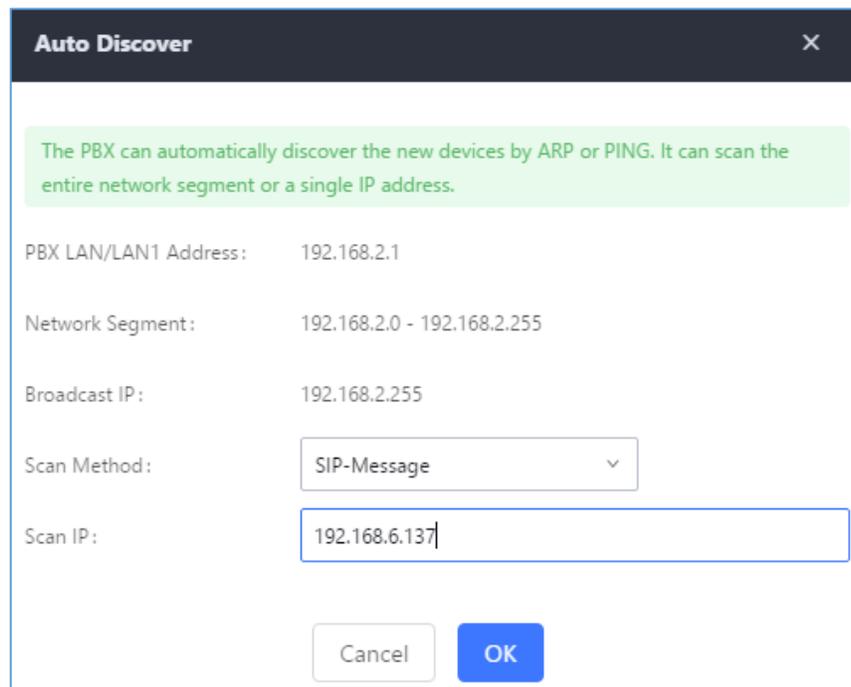
Discovery

Grandstream endpoints are automatically discovered after bootup. Users could also manually discover device by specifying the IP address or scanning the entire LAN network. Three methods are supported to scan the devices.



- PING
- ARP
- SIP Message (NOTIFY)

Click on “Auto Discover” under Web GUI→**Value-added Features**→**Zero Config**→**Zero Config**, fill in the “Scan Method” and “Scan IP”. The IP address segment will be automatically filled in based on the network mask detected on the UCM6510. If users need scan the entire network segment, enter 255 (for example, 192.168.5.255) instead of a specific IP address. Then click on “Save” to start discovering the devices within the same network. To successfully discover the devices, “Zero Config” needs to be enabled on the UCM6510 Web GUI→**Value-added Features**→**Zero Config**→**Auto Provisioning Settings**.



Auto Discover [X]

The PBX can automatically discover the new devices by ARP or PING. It can scan the entire network segment or a single IP address.

PBX LAN/LAN1 Address: 192.168.2.1

Network Segment: 192.168.2.0 - 192.168.2.255

Broadcast IP: 192.168.2.255

Scan Method: SIP-Message

Scan IP: 192.168.6.137

Cancel OK

Figure 73: Auto Discover

The following figure shows a list of discovered phones. The MAC address, IP Address, Extension (if assigned), Version, Vendor, Model, Connection Status, Create Config, Options Edit /Delete /Update /Reboot /Access Device WebGUI) are displayed in the list.

<input type="checkbox"/>	MAC Address ↕	IP Address ↕	Extension	Version ↕	Vendor ↕	Model ↕	Create Config ↕	Options
<input type="checkbox"/>	0008825C6926	192.168.2.104	--	1.0.9.17	GRANDSTREAM	GXP2160	--	    
<input type="checkbox"/>	000882836616	192.168.6.175	--	1.0.9.14	GRANDSTREAM	GXP2160	--	    
<input type="checkbox"/>	000882866015	192.168.2.101	--	1.0.9.11	GRANDSTREAM	GXP2170	--	    
<input type="checkbox"/>	000882A206D8	192.168.6.241	--	1.0.8.50	GRANDSTREAM	GXP2160	--	    
<input type="checkbox"/>	00088275C8B8	192.168.6.137	--	1.0.8.50	GRANDSTREAM	GXP2130	--	    

Figure 74: Discovered Devices

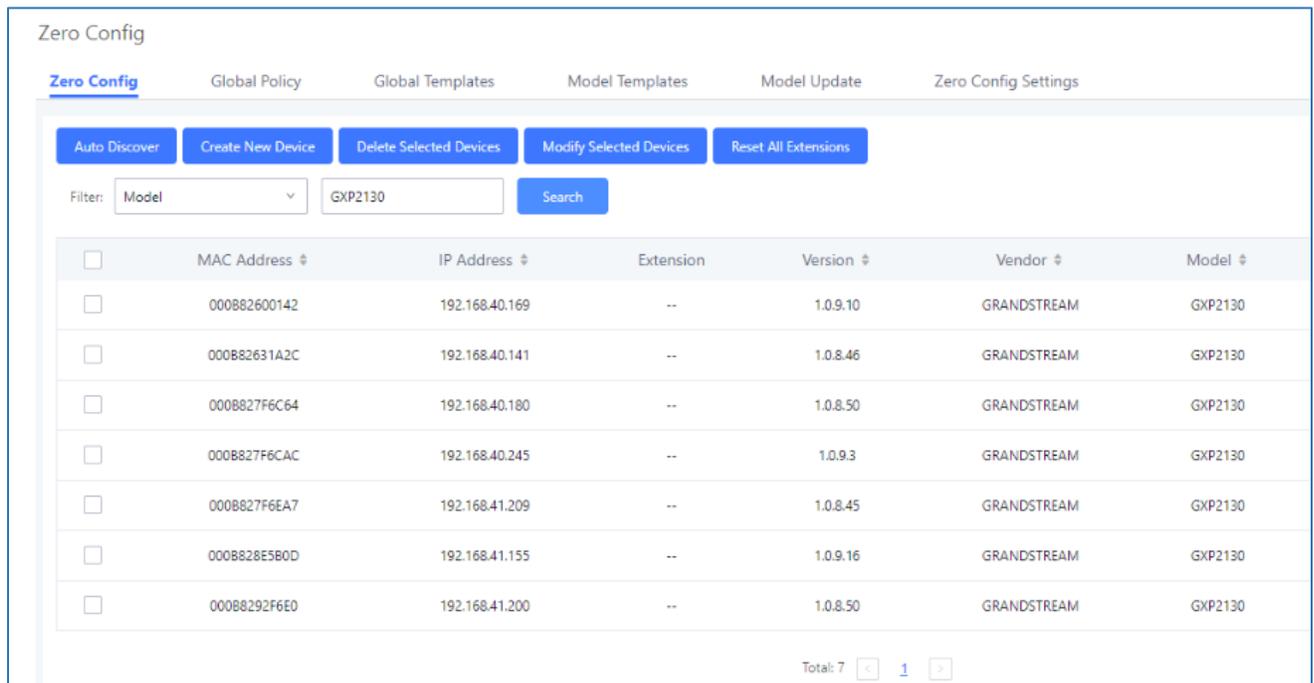


Managing discovered devices:

- **Sorting:** Press ▲ or ▼ to sort per MAC Address, IP Address, Version, Vendor, Model or Create Config columns from lower to higher or higher to lower respectively.

Filter:

- **Filter:** Select a filter to display corresponding results.
 - **All:** Display all discovered devices.
 - **Scan Results:** Display only manually discovered devices. [Discovery]
 - **IP Address:** Enter device IP and press **Search** button.
 - **MAC Address:** Enter device MAC and press **Search** button.
 - **Model:** Enter a model name and press **Search** button. Example: GXP2130.



The screenshot shows the 'Zero Config' web interface. At the top, there are navigation tabs: 'Zero Config' (selected), 'Global Policy', 'Global Templates', 'Model Templates', 'Model Update', and 'Zero Config Settings'. Below the tabs are several action buttons: 'Auto Discover', 'Create New Device', 'Delete Selected Devices', 'Modify Selected Devices', and 'Reset All Extensions'. A search section includes a 'Filter:' dropdown menu set to 'Model', a text input field containing 'GXP2130', and a 'Search' button. Below this is a table with the following columns: 'MAC Address', 'IP Address', 'Extension', 'Version', 'Vendor', and 'Model'. The table contains 7 rows of data, all with 'GRANDSTREAM' as the vendor and 'GXP2130' as the model. At the bottom right of the table, it says 'Total: 7' with pagination controls.

	MAC Address †	IP Address †	Extension	Version †	Vendor †	Model †
<input type="checkbox"/>	000882600142	192.168.40.169	--	1.0.9.10	GRANDSTREAM	GXP2130
<input type="checkbox"/>	000882631A2C	192.168.40.141	--	1.0.8.46	GRANDSTREAM	GXP2130
<input type="checkbox"/>	0008827F6C64	192.168.40.180	--	1.0.8.50	GRANDSTREAM	GXP2130
<input type="checkbox"/>	0008827F6CAC	192.168.40.245	--	1.0.9.3	GRANDSTREAM	GXP2130
<input type="checkbox"/>	0008827F6EA7	192.168.41.209	--	1.0.8.45	GRANDSTREAM	GXP2130
<input type="checkbox"/>	0008828E580D	192.168.41.155	--	1.0.9.16	GRANDSTREAM	GXP2130
<input type="checkbox"/>	00088292F6E0	192.168.41.200	--	1.0.8.50	GRANDSTREAM	GXP2130

Figure 75: Managing Discovered Devices

Global Configuration

Global Policy

Global configuration will apply to all the connected Grandstream SIP end point devices in the same LAN with the UCM6510 no matter what the Grandstream device model it is. It is divided into two levels:

- Web GUI→**Value-added Features**→**Zero Config**→**Global Policy**
- Web GUI→**Value-added Features**→**Zero Config**→**Global Templates**.
- **Global Templates** configuration has higher priority to **Global Policy** configuration.



Global Policy can be accessed in Web GUI→**Value-added Features**→**Zero Config**→**Global Policy** page. On the top of the configuration table, users can select category in the “Options” dropdown list to quickly navigate to the category. The categories are:

- **Localization:** configure display language, data and time.
- **Phone Settings:** configure dial plan, call features, NAT, call progress tones and etc.
- **Contact List:** configure LDAP and XML phonebook download.
- **Maintenance:** configure upgrading, web access, Telnet/SSH access and syslog.
- **Network Settings:** configure IP address, QoS and STUN settings.
- **Customization:** customize LCD screen wallpaper for the supported models.

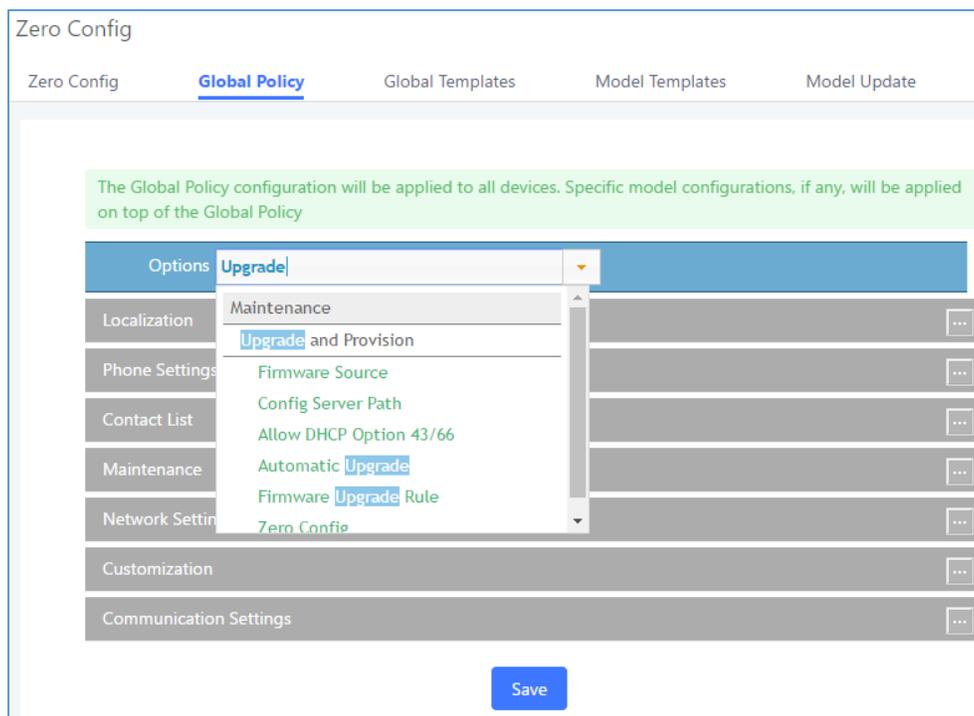


Figure 76: Global Policy Categories

Select the checkbox on the left of the parameter you would like to configure to activate the dropdown list for this parameter.

The following tables list the Global Policy configuration parameters for the SIP end device.

Table 25: Global Policy Parameters – Localization

Language settings	
Language	Select the LCD display language on the SIP end device.
Date and Time	
Date Format	Configure the date display format on the SIP end device’s LCD.



Time Format	Configure the time display in 12-hour or 24-hour format on the SIP end device's LCD.
NTP Server	Configure the URL or IP address of the NTP server. The SIP end device may obtain the date and time from the server.
Time Zone	Configure the time zone used on the SIP end device.

Table 26: Global Policy Parameters – Phone Settings

Default Call Settings	
Dial Plan	Configure the default dial plan rule. For syntax and examples, please refer to user manual of the SIP devices to be provisioned for more details.
Enable Call Features	When enabled, “Do Not Disturb”, “Call Forward” and other call features can be used via the local feature code on the phone. Otherwise, the ITSP feature code will be used.
Use # as Dial Key	If set to “Yes”, pressing the number key “#” will immediately dial out the input digits.
Auto Answer by Call-info	If set to “Yes”, the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info header sent from the server/proxy. The default setting is enabled.
NAT Traversal	Configure if NAT traversal mechanism is activated.
User Random Port	If set to “Yes”, this parameter will force random generation of both the local SIP and RTP ports.
General Settings	
Call Progress Tones	Configure call progress tones including ring tone, dial tone, second dial tone, message waiting tone, ring back tone, call waiting tone, busy tone and reorder tone using the following syntax: f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; <ul style="list-style-type: none"> • Frequencies are in Hz and cadence on and off are in 10ms). • “on” is the period (in ms) of ringing while “off” is the period of silence. Up to three cadences are supported. • Please refer to user manual of the SIP devices to be provisioned for more details
HEADSET Key Mode	Select “Default Mode” or “Toggle Headset/Speaker” for the Headset key. Please refer to user manual of the SIP devices to be provisioned for more details.



Table 27: Global Policy Parameters – Contact List

LDAP Phonebook	
Source	Select “Manual” or “PBX” as the LDAP configuration source. <ul style="list-style-type: none"> If “Manual” is selected, the LDAP configuration below will be applied to the SIP end device. If “PBX” is selected, the LDAP configuration built-in from UCM6510 Web GUI→System Settings→LDAP Server will be applied.
Address	Configure the IP address or DNS name of the LDAP server.
Port	Configure the LDAP server port. The default value is 389.
Base DN	This is the location in the directory where the search is requested to begin. Example: <ul style="list-style-type: none"> dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com
User Name	Configure the bind “Username” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Password	Configure the bind “Password” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Number Filter	Configure the filter used for number lookups. Please refer to user manual for more details.
Name Filter	Configure the filter used for name lookups. Please refer to user manual for more details.
Version	Select the protocol version for the phone to send the bind requests. The default value is 3.
Name Attribute	Specify the “name” attributes of each record which are returned in the LDAP search result. Example: <ul style="list-style-type: none"> gn cn sn description
Number Attribute	Specify the “number” attributes of each record which are returned in the LDAP search result. Example: <ul style="list-style-type: none"> telephoneNumber telephoneNumber Mobile
Display Name	Configure the entry information to be shown on phone’s LCD. Up to 3 fields can be displayed. Example: <ul style="list-style-type: none"> %cn %sn %telephoneNumber
Max Hits	Specify the maximum number of results to be returned by the LDAP server. Valid range is 1 to 3000. The default value is 50.



Search Timeout	Specify the interval (in seconds) for the server to process the request and client waits for server to return. Valid range is 0 to 180. Default value is 30.
Sort Results	Specify whether the searching result is sorted or not. Default setting is No.
Incoming Calls	Configure to enable LDAP number searching when receiving calls. The default setting is No.
Outgoing Calls	Configure to enable LDAP number searching when making calls. The default setting is No.
Lookup Display Name	Configures the display name when LDAP looks up the name for incoming call or outgoing call. It must be a subset of the LDAP Name Attributes.
XML Phonebook	
Phonebook XML Server	<p>Select the source of the phonebook XML server.</p> <ul style="list-style-type: none"> • Disable Disable phonebook XML downloading. • Manual Once selected, users need specify downloading protocol HTTP, HTTPS or TFTP and the server path to download the phonebook XML file. The server path could be IP address or URL, with up to 256 characters. • Local UCM Server Once selected, click on the Server Path field to upload the phonebook XML file. Please note: after uploading the phonebook XML file to the server, the original file name will be used as the directory name and the file will be renamed as phonebook.xml under that directory.
Phonebook Download Interval	Configure the phonebook download interval (in Minute). If set to 0, automatic download will be disabled. Valid range is 5 to 720.
Remove manually-edited entries on download	If set to “Yes”, when XML phonebook is downloaded, the entries added manually will be automatically removed.

Table 28: Global Policy Parameters – Maintenance

Upgrade and Provision	
Firmware Source	<p>Firmware source via ZeroConfig provisioning could a URL for external server address, local UCM directory or USB media if plugged in to the UCM6510. Select a source to get the firmware file:</p> <ul style="list-style-type: none"> • URL If select to use URL to upgrade, complete the configuration for the following four parameters: “Upgrade Via”, “Server Path”, “File Prefix” and “File Postfix”.



	<ul style="list-style-type: none"> Local UCM Server Firmware can be uploaded to the UCM6510 internal storage for firmware upgrade. If selected, click on “Manage Storage” icon next to “Directory” option, upload firmware file and select directory for the end device to retrieve the firmware file. Local USB Media If selected, the USB storage device needs to be plugged into the UCM6510 and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory. Local SD Card Media If selected, an SD card needs to be plugged into the UCM6510 and the firmware file must be put under a folder named “ZC_firmware” in the USB storage root directory.
Upgrade via	When URL is selected as firmware source, configure upgrade via TFTP, HTTP or HTTPS.
Server Path	When URL is selected as firmware source, configure the firmware upgrading server path.
File Prefix	When URL is selected as firmware source, configure the firmware file prefix. If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone, if URL is selected as firmware source.
File Postfix	When URL is selected as firmware source, configure the firmware file postfix. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Allow DHCP Option 43/66	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
Automatic Upgrade	<p>If enabled, the end point device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week or by minute.</p> <ul style="list-style-type: none"> By week Once selected, specify the day of the week to check HTTP/TFTP server for firmware upgrades or configuration files changes. By day Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes. By minute Once selected, specify the interval X that the SIP end device will request for new firmware every X minutes.
Firmware Upgrade Rule	Specify how firmware upgrading and provisioning request to be sent.



Web Access	
Admin Password	Configure the administrator password for admin level login.
End-User Password	Configure the end-user password for the end user level login.
Web Access Mode	Select HTTP or HTTPS as the web access protocol.
Web Server Port	Configure the port for web access. The valid range is 1 to 65535.
Security	
Disable Telnet/SSH	Enable Telnet/SSH access for the SIP end device. If the SIP end device supports Telnet access, this option controls the Telnet access of the device; if the SIP end device supports SSH access, this option controls the SSH access of the device.
Syslog	
Syslog Server	Configure the URL/IP address for the syslog server.
Syslog Level	Select the level of logging for syslog.
Send SIP Log	Configure whether the SIP log will be included in the syslog message.

Table 29: Global Policy Parameters – Network Settings

Basic Settings	
IP Address	<p>Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected.</p> <ul style="list-style-type: none"> DHCP Once selected, users can specify the Host Name (option 12) of the SIP end device as DHCP client, and Vendor Class ID (option 60) used by the client and server to exchange vendor class ID information. PPPoE Once selected, users need specify the Account ID, Password and Service Name for PPPoE.
Advanced Setting	
Layer 3 QoS	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0-63.
Layer 2 QoS Tag	Assign the VLAN Tag of the Layer 2 QoS packets. Valid range is 0 -4095.
Layer 2 QoS Priority Value	Assign the priority value of the Layer 2 QoS packets. Valid range is 0-7.
STUN Server	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Keep Alive Interval	Specify how often the phone will send a blank UDP packet to the SIP server in order to keep the “ping hole” on the NAT router to open. Valid range is 10-160.



Table 30: Global Policy Parameters – Customization

Wallpaper	
Screen Resolution 1024 x 600	<p>Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> • Source Configure the location where wallpapers are stored. • File If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 800 x 400	<p>Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> • Source Configure the location where wallpapers are stored. • File If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 480 x 272	<p>Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> • Source Configure the location where wallpapers are stored. • File If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 320 x 240	<p>Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper.</p> <ul style="list-style-type: none"> • Source Configure the location where wallpapers are stored. • File If “URL” is selected as source, specify the URL of the wallpaper file. If “Local UCM Server” is selected as source, click to upload wallpaper file to the UCM6510.



Global Templates

Global Templates can be accessed in Web GUI→**Value-added Features**→**Zero Config**→**Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates. Later on, when the user configures the device in Edit Device dialog→Advanced Settings, the user can select to use one of the global template for the device. Please refer to section [Manage Devices] for more details on using the global templates.

When creating global template, users can select the categories and the parameters under each category to be used in the template. The global policy and the selected global template will both take effect when generating the config file. However, the selected global template has higher priority to the global policy when it comes to the same setting option/field. If the same option/field has different value configured in the global policy and the selected global template, the value for this option/field in the selected global template will override the value in global policy.

- Click on “Create New Template” to add a global template. Users will see the following configurations.

Table 31: Create New Template

Template Name	Create a name to identify this global template.
Description	Provide a description for the global template. This is optional.
Active	Check this option to enable the global template.

- Click on  to edit the global template.

The window for editing global template is shown in the following figure. In the “Options” field, after entering the option name key word, the options containing the key word will be listed. Users could then select the options to be modified and click on “Add Option” to add it into the global template.



Edit Global Templates: Branch
Save

* Template Name:

Description:

Active:

Options
Phone Settings
▼
Add Option

Phone Settings
▼

Default Call Settings

Dial Plan:

Enable Call Features:

Use # as Dial Key:

Auto Answer by Call-Info:

Figure 77: Edit Global Template

The added options will show in the list. Users can then enter or select value for each option to be used in the global template. On the left side of each added option, users can click on  to remove this option from the template. On the right side of each option, users can click on  to reset the option value to the default value.

- Click on “Save” to save this global template.
- The created global templates will show in the Web GUI→**Value-added Features**→**Zero Config**→**Global Templates** page. Users can click on  to delete the global template or click on “Delete Selected Templates” to delete multiple selected templates at once.
- Click on “Toggle Selected Template(s)” to toggle the status between enabled/disabled for the selected templates.



Model Configuration

Model Templates

Model layer configuration allows users to apply model-specific configurations to different devices. Users could create/edit/delete a model template by accessing Web GUI, page **Value-added Features**→**Zero Config**→**Model Templates**. If multiple model templates are created and enabled, when the user configures the device in Edit Device dialog→Advanced Settings, the user can select to use one of the model template for the device. Please refer to section **[Manage Devices]** for more details on using the model template.

For each created model template, users can assign it as default model template. If assigned as default model template, the values in this model template will be applied to all the devices of this model. There is always only one default model template that can be assigned at one time on the UCM6510.

The selected model template and the default model template will both take effect when generating the config file for the device. However, the model template has higher priority to default model template when it comes to the same setting option/field. If the same option/field has different value configured in the default model template and the selected model template, the value for this option/field in the selected model template will override the value in default model template.

- Click on “Create New Template” to add a model template.

Table 32: Create New Model Template

Model	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
Template Name	Create a name for the model template.
Description	Enter a description for the model template. This is optional.
Default Model Template	Select to assign this model template as the default model template. The value of the option in default model template will be overridden if other selected model template has a different value for the same option.
Active	Check this option to enable the model template.

- Click on  to edit the model template.

The editing window for model template is shown in the following figure. In the “Options” field, enter the option name key word, the option that contains the key word will be listed. User could then select the option and click on “Add Option” to add it into the model template.



Once added, the option will be shown in the list below. On the left side of each option, users can click on  to remove this option from the model template. On the right side of each option, users can click on  to reset the option to the default value.

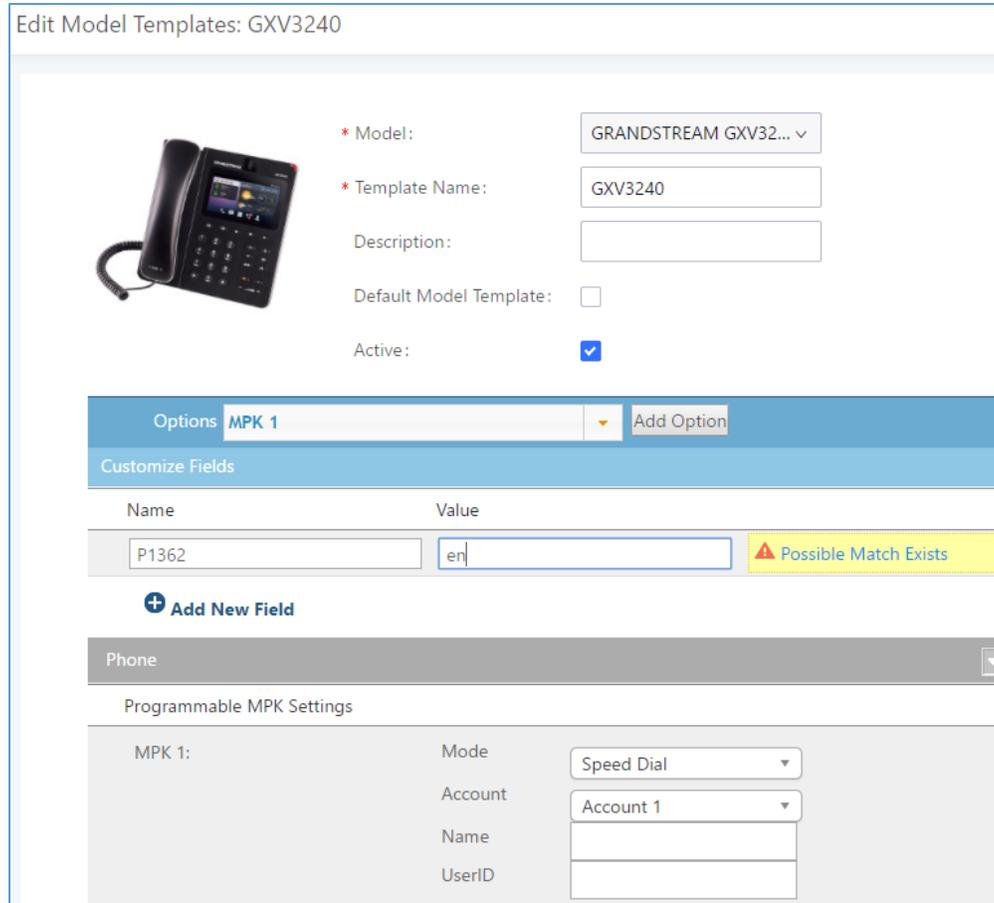


Figure 78: Edit Model Template

User could also click on “Add New Field” to add a P value number and the value to the configuration. The following figure shows setting P value “P1362” to “en”, which means the display language on the LCD is set to English. For P value information of different models, please refer to configuration template here <http://www.grandstream.com/sites/default/files/Resources/config-template.zip>.

- Click on Save when done. The model template will be displayed on Web GUI→**Value-added Features**→**Zero Config**→**Model Templates** page.
- Click on  to delete the model template or click on “Delete Selected Templates” to delete multiple selected templates at once.
- Click on “Toggle Selected Template(s)” to toggle the status between enabled/disabled for the selected model templates.



Model Update

UCM6510 zero config feature supports provisioning all models of Grandstream SIP end devices. Templates for most of the Grandstream models are built in with the UCM6510 already. Templates for GXP16XX, GSWave and Surveillance products requires user to download on UCM6510 Web GUI→**Value-added Features**→**Zero Config**→**Model Update** first as those products are more often used as needed. After downloading the model template, it will show in the dropdown list for “Model” selection when editing the model template.

- Click on  to download the template.
- Click on  to upgrade the model template. Users will see this icon available if the device model has template updated in the UCM6510.

Model Template Package List					
<input type="checkbox"/>	Vendor	Model	Version	Size	Options
<input type="checkbox"/>	Grandstream	DP750	1.0	26K	
<input type="checkbox"/>	Grandstream	GAC2500	1.0	24K	
<input type="checkbox"/>	Grandstream	GDS3710	1.1	97K	
<input type="checkbox"/>	Grandstream	GSWave	1.0	7.9K	
<input type="checkbox"/>	Grandstream	GVC3200	1.0	18K	
<input type="checkbox"/>	Grandstream	GVC3202	1.0	13K	
<input type="checkbox"/>	Grandstream	GXP1100	1.0	729K	
<input type="checkbox"/>	Grandstream	GXP1105	1.0	297K	
<input type="checkbox"/>	Grandstream	GXP1600C	1.0	21K	
<input type="checkbox"/>	Grandstream	GXP1615	1.0	22K	

Figure 79: Template Management

In case the UCM6510 is placed in the private network and Internet access is restricted, users will not be able to get packages by downloading and installing from the remote server. Model template package can be manually uploaded from local device through Web GUI. Please contact Grandstream customer support if the model package is needed for manual uploading.



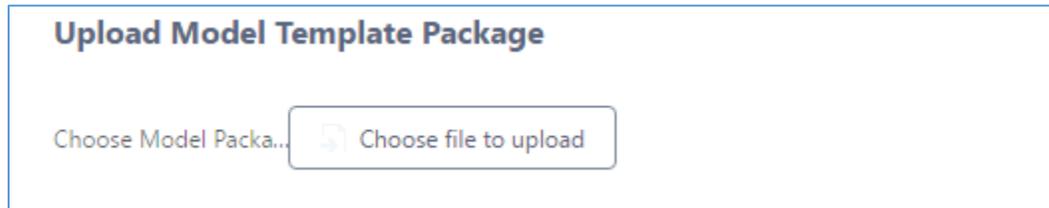


Figure 80: Upload Model Template Manually

Device Configuration

On Web GUI, page **Value-added Features**→**Zero Config**→**Zero Config**, users could create new device, delete existing device(s), make special configuration for a single device, or send NOTIFY to existing device(s).

Create New Device

Besides configuring the device after the device is discovered, users could also directly create a new device and configure basic settings before the device is discovered by the UCM6510. Once the device is plugged in, it can then be discovered and provisioned. This gives the system administrator adequate time to set up each device beforehand.

Click on “Create New Device” and the following dialog will show. Follow the steps below to create the configurations for the new device.

1. Firstly, select a model for the device to be created and enter its MAC address, IP address and firmware version (optional) in the corresponding field.
2. Basic settings will show a list of settings based on the model selected in step 1. Users could assign extensions to accounts, assign functions to Line Keys and Multiple-Purposed Keys if supported on the selected model.
3. Click on “Create New Device” to save the configuration for this device.



Create New Device



Model: GRANDSTREAM GXP2130 ▼

MAC

Address:

IP

Address:

Version:

Basic
Advanced

Accounts

<input type="checkbox"/>	Hot Desking:	No ▼
<input checked="" type="checkbox"/>	Account 1:	1001 ▼
<input type="checkbox"/>	Account 2:	1001 ▼
<input type="checkbox"/>	Account 3:	1001 ▼

Figure 81: Create New Device

Manage Devices

The device manually created or discovered from Auto Discover will be listed in the Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page. Users can see the devices with their MAC address, IP address, vendor, model and etc.

<input type="checkbox"/>	000B825C6927	192.168.6.162	1.0.9.9	Grandstream	GXP2160	1	
<input type="checkbox"/>	000B826B1958	192.168.6.115	1.0.3.167	Grandstream	GXV3240	1	
<input type="checkbox"/>	000B826B1FF7	192.168.6.158	1.0.3.171	Grandstream	GXV3240	1	

Figure 82: Manage Devices

1. Click on to access the Web GUI of the phone.
2. Click on to edit the device configuration.



A new dialog will be displayed for the users to configure “Basic” settings and “Advanced” settings. “Basic” settings have the same configurations as displayed when manually creating a new device, i.e., account, line key and MPK settings; “Advanced” settings allow users to configure more details in a five-level structure.

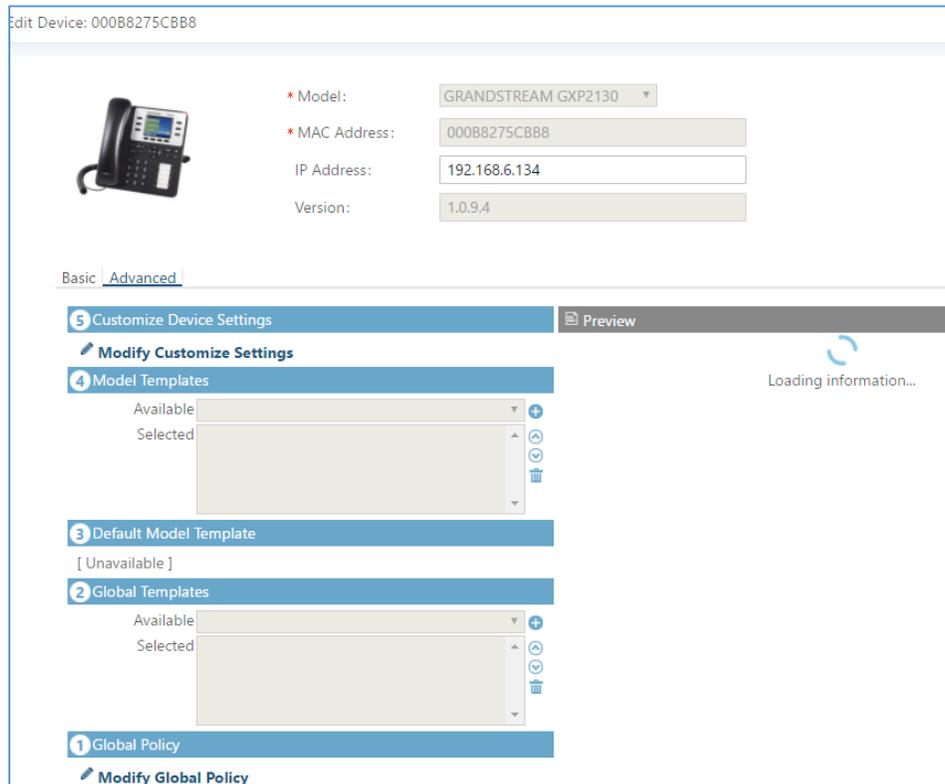


Figure 83: Edit Device

A preview of the “Advanced” settings is shown in the above figure. There are five levels configurations as described in (1) (2) (3) (4) (5) below, with priority from the lowest to the highest. The configurations in all levels will take effect for the device. If there are same options existing in different level configurations with different value configured, the higher level configuration will override the lower level configuration.

(1) Global Policy

This is the lowest level configuration. The global policy configured in Web GUI→**Value-added Features**→**Zero Config**→**Global Policy** will be applied here. Clicking on “Modify Global Policy” to redirect to page **Value-added Features**→**Zero Config**→**Global Policy**.

(2) Global Templates

Select a global template to be used for the device and click on  to add. Multiple global templates can be selected and users can arrange the priority by adjusting orders via  and . All the selected global templates will take effect. If the same option exists on multiple selected global templates, the value in the template with higher priority will override the one in the template with lower priority. Click on  to remove the global template from the selected list.



(3) Default Model Template

Default Model Template will be applied to the devices of this model. Default model template can be configured in model template under Web GUI→**Value-added Features**→**Zero Config**→**Model Templates** page. Please see default model template option in *[Table 32: Create New Model Template]*.

(4) Model Templates

Select a model template to be used for the device and click on  to add. Multiple global templates can be selected and users can arrange the priority by adjusting orders via  and . All the selected model templates will take effect. If the same option exists on multiple selected model templates, the value in the template with higher priority will override the one in the template with lower priority. Click on  to remove the model template from the selected list.

(5) Customize Device Settings

This is the highest level configuration in the “Advanced” settings of the device. Click on “Modify Customize Device Settings” and following dialog will show.

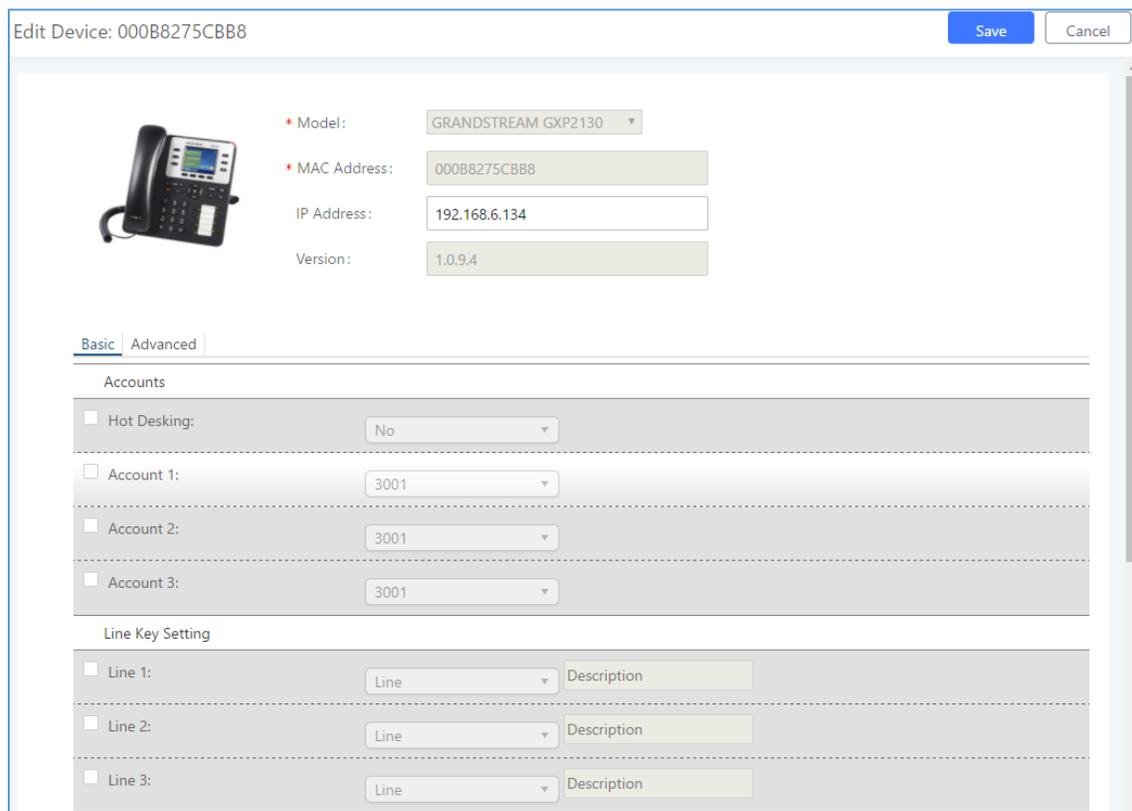


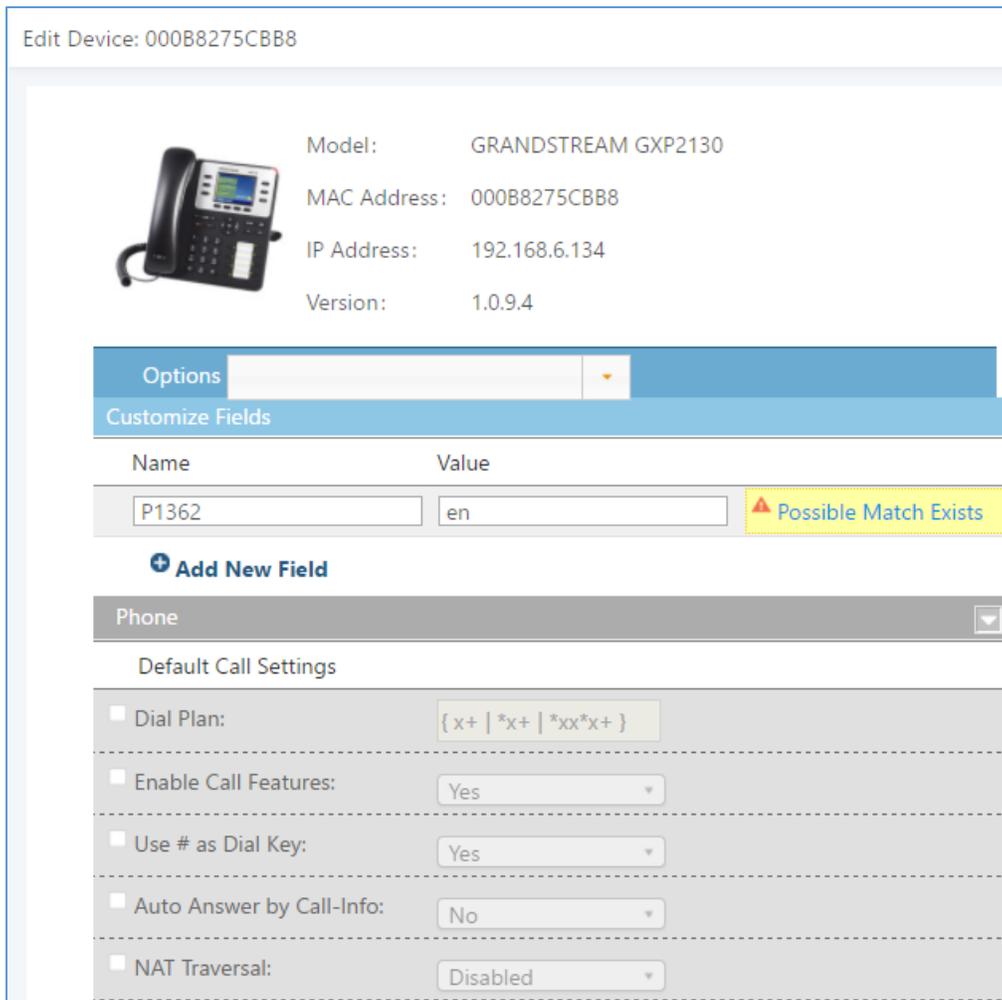
Figure 84: Edit Customize Device Settings

Scroll down in the dialog to view and edit the device-specific options. If the users would like to add more options which are not in the pre-defined list, click on “Add New Field” to add a P value number and the value to the configuration. The following figure shows setting P value “P1362” to “en”, which means the display language on the LCD is set to English.

The warning information next to the P value field indicates that the option matching the P value number exists in the configuration already.

For P value information of different models, please refer to configuration template here:

http://www.grandstream.com/sites/default/files/Resources/config-template_0.zip.



Edit Device: 000B8275CBB8


 Model: GRANDSTREAM GXP2130
 MAC Address: 000B8275CBB8
 IP Address: 192.168.6.134
 Version: 1.0.9.4

Options

Customize Fields

Name	Value
<input type="text" value="P1362"/>	<input type="text" value="en"/> ▲ Possible Match Exists

[+ Add New Field](#)

Phone

Default Call Settings

- Dial Plan:
- Enable Call Features:
- Use # as Dial Key:
- Auto Answer by Call-Info:
- NAT Traversal:

Figure 85: Add P Value in Customize Device Settings

- Select multiple devices that need to be modified and then click on Modify Selected Devices to batch modify devices.



If selected devices are of the same model, the configuration dialog is like the following figure. Configurations in five levels are all available for users to modify.

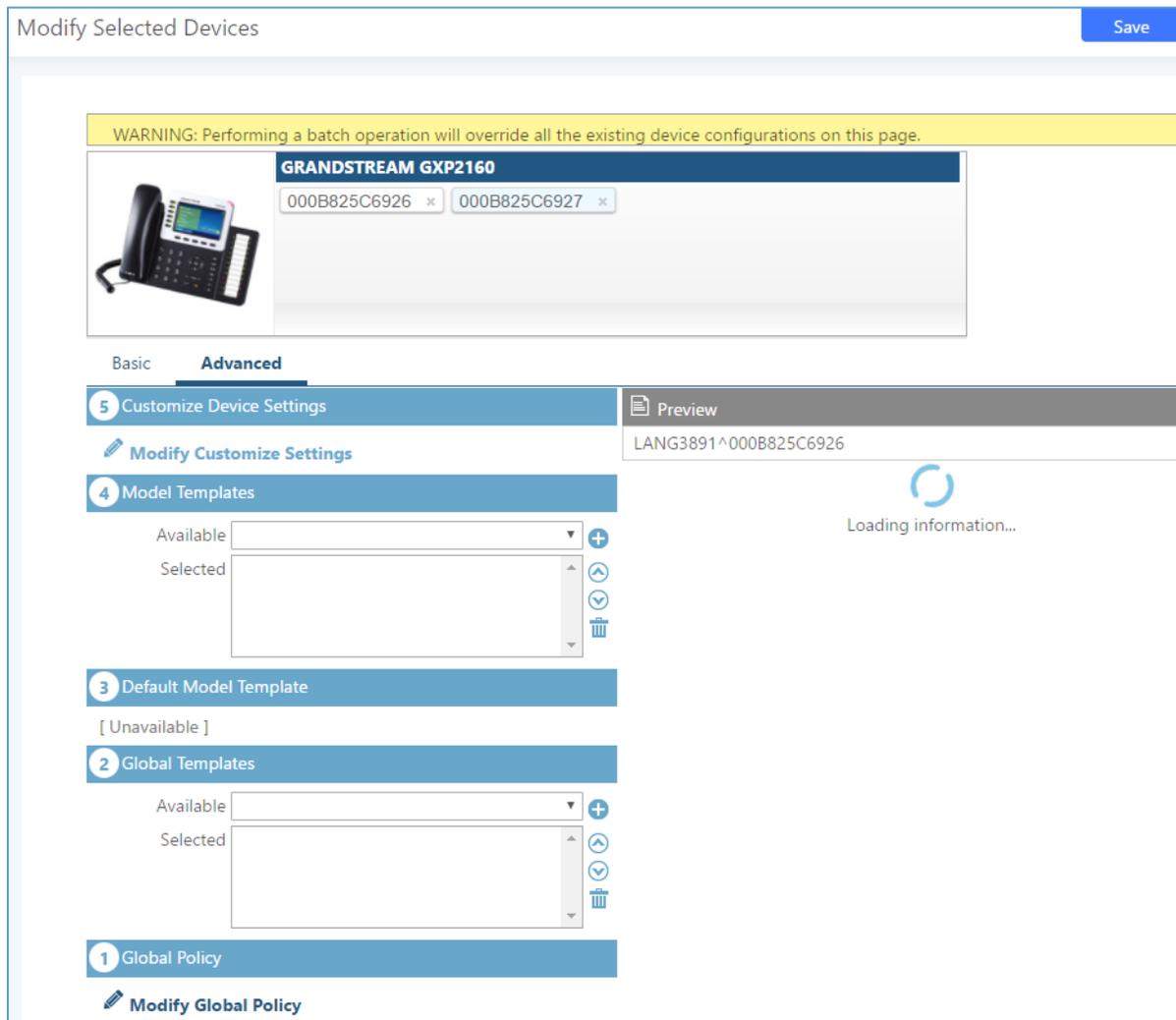


Figure 86: Modify Selected Devices–Same Model

If selected devices are of different models, the configuration dialog is like the following figure. Click on  to view more devices of other models. Users are only allowed to make modifications in Global Templates and Global Policy level.



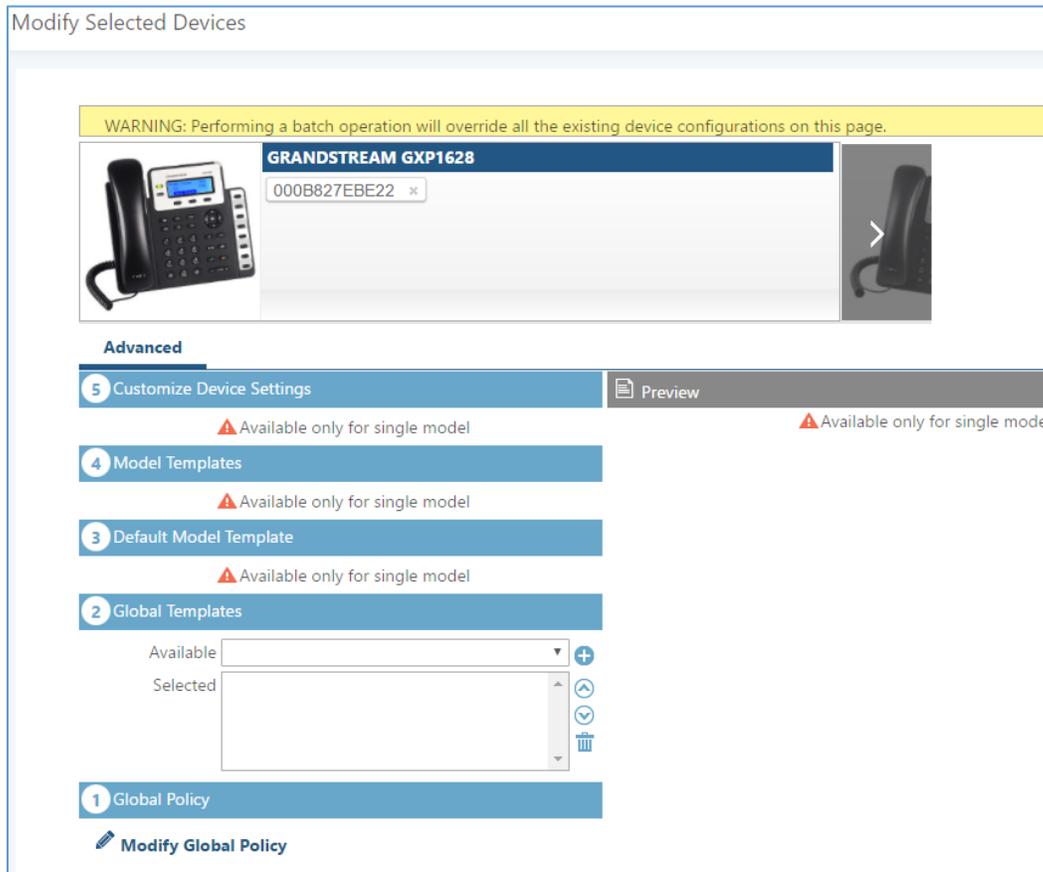


Figure 87: Modify Selected Devices—Different Models

 **Warning:**

Perform batch operation will override all the configurations made when editing a single device. For example, if the user configures a GXP2140 to use template “TempA” in Global Templates level by editing a single device and then selects several devices including that GXP2140 to batch modify devices selecting “TempB” in Global Templates level, the user will see the global templates changed to “TempB” when viewing the configurations for the GXP2140.

After the above configurations, save the changes and go back to Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page. Users could then click on  to send NOTIFY to the SIP end point device and trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.



Zero Config

[Zero Config](#) [Global Policy](#) [Global Templates](#) [Model Templates](#) [Model Update](#) [Zero Config Settings](#)

Filter:

<input type="checkbox"/>	MAC Address ↕	IP Address ↕	Extension	Version ↕	Vendor ↕	Model ↕	Create Config ↕	Options
<input type="checkbox"/>	0008823F8CB0	192.168.6.176	--	1.0.14.100	GRANDSTREAM	HT503	--	
<input type="checkbox"/>	000882415D27	192.168.6.72	--	1.0.7.80	GRANDSTREAM	GKV3140	--	
<input type="checkbox"/>	0008825C5806	192.168.6.218	--	1.0.8.50	GRANDSTREAM	GXP2140	--	
<input type="checkbox"/>	0008825C6926	192.168.2.104	--	1.0.9.17	GRANDSTREAM	GXP2160	--	
<input type="checkbox"/>	000882681052	192.168.6.146	--	1.0.3.177	GRANDSTREAM	GKV3240	--	
<input type="checkbox"/>	000882681FF7	192.168.6.144	--	1.0.3.144	GRANDSTREAM	GKV3240	--	
<input type="checkbox"/>	0008826824CD	192.168.6.45	--	1.0.3.177	GRANDSTREAM	GKV3275	--	
<input type="checkbox"/>	000882718249	192.168.6.119	--	1.0.4.60	GRANDSTREAM	GXP1625	--	
<input type="checkbox"/>	000882718419	192.168.6.195	--	1.0.4.56	GRANDSTREAM	GXP1610	--	
<input type="checkbox"/>	00088275C888	192.168.6.137	--	1.0.8.50	GRANDSTREAM	GXP2130	--	
<input type="checkbox"/>	000882784681	192.168.6.224	--	0.6.9.61	GRANDSTREAM	GXP1628	--	

Figure 88: Device List in Zero Config

In this web page, users can also click on “Reset All Extensions” to reset the extensions of all the devices.

Sample Application

Assuming in a small business office where there are 8 GXP2140 phones used by customer support and 1 GXV3275 phone used by customer support supervisor. 3 of the 8 customer support members speak Spanish and the rest speak English. We could deploy the following configurations to provisioning the office phones for the customer support team.

1. Go to Web GUI→**Value-added Features**→**Zero Config**→**Auto Provision Settings**, select “Enable Zero Config”.
2. Go to Web GUI→**Value-added Features**→**Zero Config**→**Global Policy**, configure Date Format, Time Format and Firmware Source as follows.



Localization	
Language Settings	
<input type="checkbox"/> Language:	English
Date and Time	
<input checked="" type="checkbox"/> Date Format:	mm-dd-yyyy
<input checked="" type="checkbox"/> Time Format:	24-hour Clock
<input type="checkbox"/> Enable NTP:	Disabled
<input type="checkbox"/> NTP Server:	
<input type="checkbox"/> NTP Update Interval:	1440
<input type="checkbox"/> Time Zone:	GMT-12:00 (Internatio..
<input type="checkbox"/> Enable Daylight Saving Time:	Disabled
Phone Settings	
Contact List	
Maintenance	
Upgrade and Provision	
<input checked="" type="checkbox"/> Firmware Source:	Source: URL Upgrade via: TFTP Server Path: fm.grandstream.com/gs File Prefix: File Postfix:
<input type="checkbox"/> Config Server Path:	192.168.2.1:8089/zccgi/

Figure 89: Zero Config Sample – Global Policy

3. Go to Web GUI→**Value-added Features**→**Zero Config**→**Model Templates**, create a new model template “English Support Template” for GXP2140. Add option “Language” and set it to “English”. Then select the option “Default Model Template” to make it the default model template.
4. Go to Web GUI→**Value-added Features**→**Zero Config**→**Model Templates**, create another model template “Spanish Support Template” for GXP2140. Add option “Language” and set it to “Español”.



5. After 9 devices are powered up and connected to the LAN network, use “Auto Discover” function or “Create New Device” function to add the devices to the device list on Web GUI→**Value-added Features**→**Zero Config**→**Zero Config**.
6. On Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on  to edit the device settings.
7. For each of the 5 phones used by English speaking customer support, in “Basic” settings select an available extension for account 1 and click on “Save”. Then click on “Advanced” settings tab to bring up the following dialog. Users will see the English support template is applied since this is the default model template. A preview of the device settings will be listed on the right side.

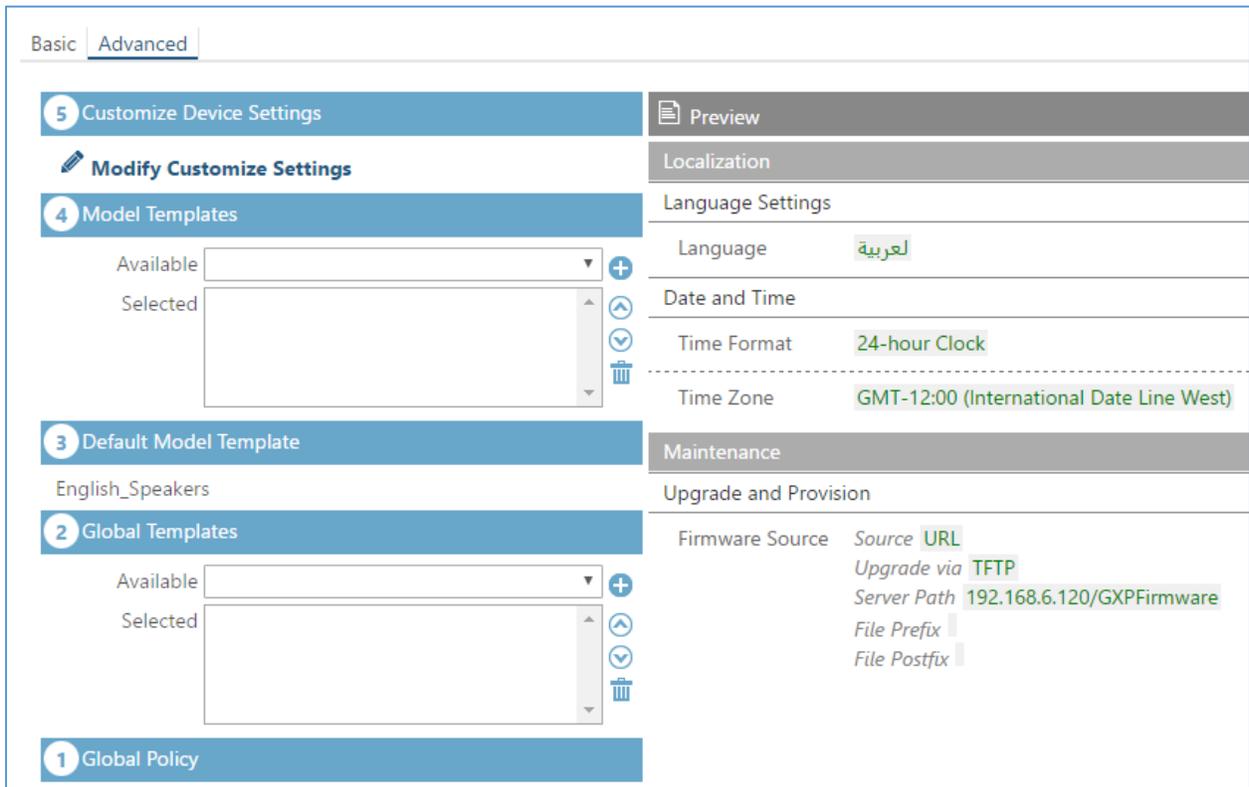
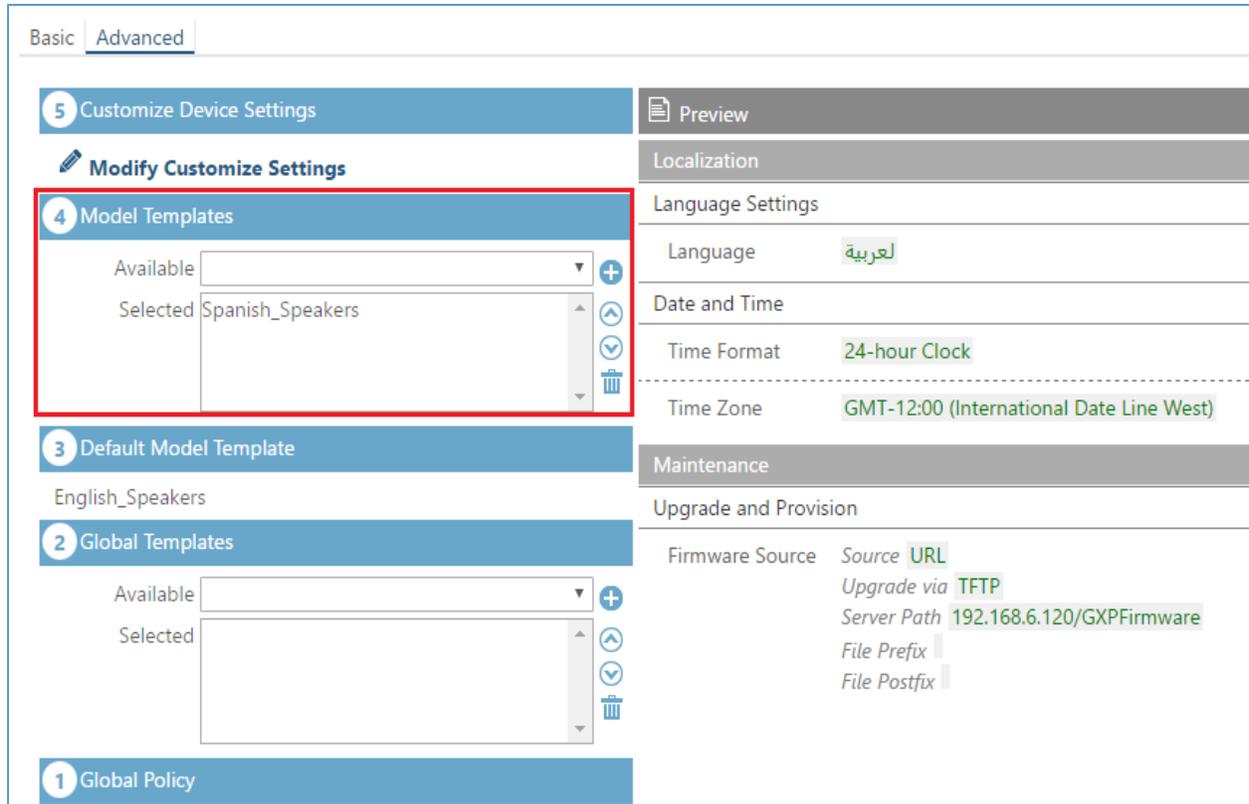


Figure 90: Zero Config Sample – Device Preview 1

8. For the 3 phones used by Spanish support, in “Basic” settings select an available extension for account 1 and click on “Save”. Then click on “Advanced” settings tab to bring up the following dialog.





The screenshot displays the 'Advanced' settings page for a device. On the left, a sidebar contains five sections: '5 Customize Device Settings' (with a 'Modify Customize Settings' icon), '4 Model Templates' (highlighted with a red box, showing 'Available' and 'Selected' dropdowns with 'Spanish_Speakers' chosen), '3 Default Model Template' (showing 'English_Speakers'), '2 Global Templates' (with empty dropdowns), and '1 Global Policy'. On the right, a 'Preview' pane shows configuration details: 'Localization' (Language: العربية), 'Date and Time' (Time Format: 24-hour Clock, Time Zone: GMT-12:00 (International Date Line West)), 'Maintenance', and 'Upgrade and Provision' (Firmware Source: Source URL, Upgrade via: TFTP, Server Path: 192.168.6.120/GXPFirmware, File Prefix, File Postfix).

Figure 91: Zero Config Sample – Device Preview 2

Select “Spanish Support Template” in “Model Template”. The preview of the device settings is displayed on the right side and we can see the language is set to “Español” since Model Template has the higher priority for the option “Language”, which overrides the value configured in default model template.

9. For the GXV3275 used by the customer support supervisor, select an available extension for account 1 on “Basic” settings and click on “Save”. Users can see the preview of the device configuration in “Advanced” settings. There is no model template configured for GXV3275.



Basic <u>Advanced</u>	
5 Customize Device Settings	Preview
Modify Customize Settings	Localization
4 Model Templates	Language Settings
Available <input type="text"/>	Language العربية
Selected <input type="text"/>	Date and Time
	Time Format 24-hour Clock
	Time Zone GMT-12:00 (International Date Line West)
3 Default Model Template	Maintenance
English_Speakers	Upgrade and Provision
2 Global Templates	Firmware Source Source URL
Available <input type="text"/>	Upgrade via TFTP
Selected <input type="text"/>	Server Path 192.168.6.120/GXP Firmware
	File Prefix <input type="text"/>
	File Postfix <input type="text"/>
1 Global Policy	Syslog
Modify Global Policy	Syslog Server 192.168.6.120
	Syslog Level DEBUG
	Send SIP Log Yes

Figure 92: Zero Config Sample – Device Preview 3

10. Click on “Apply Changes” to apply saved changes.
11. On the Web GUI→**Value-added Features**→**Zero Config**→**Zero Config** page, click on  to send NOTIFY to trigger the device to download config file from UCM6510.

Now all the 9 phones in the network will be provisioned with a unique extension registered on the UCM6510. 3 of the phones will be provisioned to display Spanish on LCD and the other 5 will be provisioned to display English on LCD. The GXV3275 used by the supervisor will be provisioned to use the default language on LCD display since it's not specified in the global policy.



EXTENSIONS

Create New User

Create New SIP Extension

To manually create new SIP user, go to Web GUI→**Extension/Trunk**→**Extensions**. Click on "Add" and a new dialog window will show for users to fill in the extension information.

Create New Extension
Save

Basic Settings
Media
Features
Specific Time
Follow Me

* Select Extension Type:

Select Add Method:

General

<p>* Extension: <input type="text" value="1003"/></p> <p>* Permission: <input type="text" value="Internal"/></p> <p>AuthID: <input type="text"/></p> <p>* Voicemail Password: <input type="text" value="081347"/></p> <p>Enable Keep-alive: <input type="checkbox"/></p> <p>Disable This Extension: <input type="checkbox"/></p>	<p>CallerID Number: <input type="text"/></p> <p>* SIP/IAX Password: <input type="text" value="X7a0c4s"/></p> <p>Enable Voicemail: <input checked="" type="checkbox"/></p> <p>Skip Voicemail Password V... <input type="checkbox"/></p> <p>* Keep-alive Frequency: <input type="text" value="60"/></p>
--	---

User Settings

<p>First Name: <input type="text"/></p> <p>Email Address: <input type="text"/></p> <p>* Language: <input type="text" value="Default"/></p> <p>Mobile Phone Number: <input type="text"/></p>	<p>Last Name: <input type="text"/></p> <p>* User Password: <input type="text" value="L9J6iz"/></p> <p>* Concurrent Registration... <input type="text" value="1"/></p>
---	---

Figure 93: Create New Device

SIP extension options are divided into four categories:

- Basic Settings
- Media
- Features
- Specific Time
- Follow Me



Click on the tab to view or edit options belonging to that category.
 The configuration parameters are as follows.

Table 33: SIP Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”. Note: Users need to have the same level as or higher level than an outbound rule’s privilege in order to make outbound calls using this rule.
SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purpose.
Support Hot-Desking Mode	If enabled, SIP Password will accept only alphabet characters and digits; AuthID will be changed to the same as Extension.
Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
Enable Voicemail	Enable voicemail for the user. The default setting is “Yes”.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Enable Keep-alive	If enabled, empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is “Yes”.
Keep-alive Frequency	Configure the Keep-alive interval (in seconds) to check if the host is up. The default setting is 60 seconds.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default, this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. Note: The disabled extension still exists on the PBX but can’t be used on the end device.



User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is “Default” which is the selected voice prompt language under Web GUI→ PBX Settings → Voice Prompt → Language Settings . The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting “Check Prompt List” under Web GUI→ PBX Settings → Voice Prompt → Language Settings .
Concurrent Registrations	The maximum endpoints which can be registered into this extension. For security concerns, the default value is 1.
Mobile Phone Number	Configure the phone number for the extension, user can type the related star code for phone number followed by the extension number to call directly this number. <u>Example:</u> user can type *881000 to call the mobile number associated with extension 1000.

Table 34: SIP Extension Configuration Parameters – Media

SIP Settings	
NAT	Use NAT when the UCM6510 is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it’s related to NAT configuration or Firewall’s support of SIP and RTP ports. The default setting is enabled.
Can Direct Media	By default, the UCM6510 will route the media steams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the UCM6510 to negotiate endpoint-to-endpoint media routing. The default setting is “No”.



DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is “RFC2833”. If “Info” is selected, SIP INFO message will be used. If “Inband” is selected, 64-kbit PCMU and PCMA are required. When “Auto” is selected, RFC2833 will be used if offered, otherwise “Inband” will be used.
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. “User=Phone” parameter will be attached to the Request-Line and “TO” header in the SIP request to indicate the E.164 number. If set to “Enable”, “Tel” will be used instead of “SIP” in the SIP request.
Alert-Info	Configure the Alert-Info, when UCM6510 receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.
Enable T.38 UDPTL	Enable or disable T.38 UDPTL support.
SRTP	Enable SRTP for the call. The default setting is disabled.
Fax Mode	Select Fax mode. The default setting is “None”. <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.
Strategy	This option controls how the extension can be used on devices within different types of network. <ul style="list-style-type: none"> • Allow All Device in any network can register this extension. • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address Only the device on the specific IP address can register this extension. The default setting is “Allow All”.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263 and H.263p.



Table 35: SIP Extension Configuration Parameters – Features

Call Transfer	
Presence Status	<p>Select which presence status to set for the extension and configure call forward conditions for each status. Six possible options are possible: “Available”, “Away”, “Chat”, “Custom”, “DND” and “Unavailable”. More details at [PRESENCE]</p>
Call Forward Unconditional	<p>Enable and configure the Call Forward Unconditional target number. Available options for target number are:</p> <ul style="list-style-type: none"> • “None”: Call forward deactivated. • “Extension”: Select an extension from dropdown list as CFU target. • “Custom Number”: Enter a customer number as target. For example: *97. • “Voicemail”: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • “Ring Group”: Select a ring group from dropdown list as CFU target. • “Queues”: Select a queue from dropdown list as CFU target. • “Voicemail Group”: Select a voicemail group from dropdown list as CFU target. <p>The default setting is “None”.</p>
CFU Time Condition	<p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	<p>Configure the Call Forward No Answer target number. Available options for target number are:</p> <ul style="list-style-type: none"> • “None”: Call forward deactivated. • “Extension”: Select an extension from dropdown list as CFN target. • “Custom Number”: Enter a customer number as target. For example: *97. • “Voicemail”: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • “Ring Group”: Select a ring group from dropdown list as CFN target.



	<ul style="list-style-type: none"> • “Queues”: Select a queue from dropdown list as CFN target. • “Voicemail Group”: Select a voicemail group from dropdown list as CFN target. <p>The default setting is “None”.</p>
CFN Time Condition	<p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	<p>Configure the Call Forward Busy target number. Available options for target number are:</p> <ul style="list-style-type: none"> • “None”: Call forward deactivated. • “Extension”: Select an extension from dropdown list as CFB target. • “Custom Number”: Enter a customer number as target. For example: *97. • “Voicemail”: Select an extension from dropdown list. Incoming calls will be forwarded to voicemail of selected extension. • “Ring Group”: Select a ring group from dropdown list as CFB target. • “Queues”: Select a queue from dropdown list as CFB target. • “Voicemail Group”: Select a voicemail group from dropdown list as CFB target. <p>The default setting is “None”.</p>
CFB Time Condition	<p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Do Not Disturb	<p>If enabled the extension will ignore all incoming calls</p>



DND Time Condition	<p>Select time condition for Do Not Disturb. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. <p>Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.</p>
DND Whitelist	<p>If DND is enabled, all calls to this extension will be rejected except the numbers listed on this list.</p> <p>Note: The maximum number on the Whitelist is 10.</p>
FWD Whitelist	<p>If call forward is enabled, all calls to this extension will be forwarded except the calls coming from the specified numbers on this list.</p> <p>Note: The Maximum number on the whitelist is 10.</p>
CC Settings	
Enable CC	<p>If enabled, UCM6510 will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default, It is disabled.</p>
CC Mode	<p>Two modes for Call Completion are supported:</p> <ul style="list-style-type: none"> • Normal: This extension is used as ordinary extension. • For Trunk: This extension is registered from a PBX. <p>The default setting is “Normal”.</p>
CC Max Agents	<p>Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. Min. value is 1.</p>
CC Max Monitors	<p>Configure the maximum number of monitor structures which may be created for this device. This number tells how many callers may request CC services for a specific device at one time.</p> <p>The minimum value is 1.</p>
Ring Simultaneously	
Ring Simultaneously	<p>Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.</p>



External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Use callee DOD on FWD or Ring Simultaneously	Use the DOD number when calls are being diverted/forwarded to external destinations or when ring simultaneous is configured.
Monitor privilege control	
Allowed to call-barging	Add members from "Available Extensions" to "Selected Extensions" so that the selected extensions can spy on the used extension using feature code.
Seamless transfer privilege control	
Allowed to seamless transfer	Any extensions on the UCM can perform seamless transfer. When using Pickup Incall feature, only extensions available on the "Selected Extensions" list can perform seamless transfer to the edited extension.
Other Settings	
Ring Timeout	<p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→General Settings: General Preference. The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→ CDR → Recording Files .
Skip Trunk Auth	<ul style="list-style-type: none"> • If set to 'Yes', users can skip entering the password when making outbound calls. • If set to 'By Time', users can skip entering the password when making outbound calls during the selected time condition. • If set to 'No', users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Support Hot-Desking Mode	If enabled, SIP Password will accept only alphabet characters and digits. Auth ID will be changed to the same as Extension.



Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX list.
Enable WebRTC Support	Enable registration and call from Web RTC.
Music On Hold	Specify which Music On Hold class to suggest to the bridged channel when putting them on hold.
Enable Seamless Transfer	Enable the seamless transfer for this extension.
Permission	Set the permission for this extension when using the seamless transfer
Call Duration Limit	The maximum duration of call-blocking.
Custom Call-info for Auto Answer	If enabled, when a call is sent to this extension from UCM, the SIP INVITE message will contain a Call-info header indicating auto answer.

Table 36: SIP Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.

Create New IAX Extension

The UCM6510 supports Inter-Asterisk eXchange (IAX) protocol. IAX is used for transporting VoIP telephony sessions between servers and terminal devices. IAX is similar to SIP but also has its own characteristic. For more information, please refer to RFC5465.

To manually create new IAX user, go to Web GUI→**Extension/Trunk**→**Extensions**. Click on "Add" and a new dialog window will show for users which need to make sure first to select the extension type to be IAX Extension before proceeding to fill in the extension information. The configuration parameters are as follows.

Table 37: IAX Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". Note: Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls using this rule.



SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purpose.
Enable Voicemail	Enable voicemail for the user. The default setting is “Yes”.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. Note: The disabled extension still exists on the PBX but can’t be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is “Default” which is the selected voice prompt language under Web GUI→ PBX Settings → Voice Prompt → Language Settings . The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting “Check Prompt List” under Web GUI→ PBX Settings → Voice Prompt → Language Settings .

Table 38: IAX Extension Configuration Parameters – Media

SIP Settings	
Max Number of Calls	Configure the maximum number of calls allowed for each remote IP address.
Require Call Token	Configure to enable/disable requiring call token. If set to “Auto”, it might lock out users who depend on backward compatibility when peer



	authentication credentials are shared between physical endpoints. The default setting is “Yes”.
SRTP	Enable SRTP for the call. The default setting is disabled.
Fax Mode	<p>Select Fax Mode. The default setting is “None”.</p> <ul style="list-style-type: none"> • None: Disable Fax. This is the default setting. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.
Strategy	<p>This option controls how the extension can be used on devices within different types of network.</p> <ul style="list-style-type: none"> • Allow All Device in any network can register this extension. • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address Only the device on the specific IP address can register this extension. <p>The default setting is “Allow All”.</p>
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G,726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263 and H.263p.

Table 39: IAX Extension Configuration Parameters – Features

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	<p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period.



	<ul style="list-style-type: none"> • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	<p>Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	<p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.



Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Other Settings	
Ring Timeout	<p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→General Settings: General Preference. The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→ CDR → Recording Files .
Skip Trunk Auth	<ul style="list-style-type: none"> • If set to “Yes”, users can skip entering the password when making outbound calls. • If set to “By Time”, users can skip entering the password when making outbound calls during the selected time condition. • If set to “No”, users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If “Skip Trunk Auth” is set to “By Time”, select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, the extension will be added to LDAP Phonebook PBX lists.
Music On Hold	Configure the Music On Hold class to suggest to the bridged channel when putting them on hold.
Call Duration Limit	The maximum duration of call-blocking.

Table 40: IAX Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.

Create New FXS Extension

The UCM6510 supports Foreign eXchange Subscriber (FXS) interface. FXS is used when user needs to connect analog phone lines or FAX machines to the UCM6510.



To manually create new FXS user, go to Web GUI→**Extension/Trunk**→**Extensions**. Click on "Add" and a new dialog window will show for users which need to make sure first to select the extension type to be FXS Extension before proceeding to fill in the extension information. The configuration parameters are as follows.

Table 41: FXS Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
Analog Station	Select the FXS port to be assigned for this extension.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. Note: The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”. Note: Users need to have the same level as or higher level than an outbound rule’s privilege in order to make outbound calls using this rule.
Enable Voicemail	Enable voicemail for the user. The default setting is “Yes”.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. Note: The disabled extension still exists on the PBX but can’t be used on the end device.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.



User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is “Default” which is the selected voice prompt language under Web GUI→ PBX Settings → Voice Prompt → Language Settings . The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting “Check Prompt List” under Web GUI→ PBX Settings → Voice Prompt → Language Settings .

Table 42: FXS Extension Configuration Parameters – Media

Analog Settings	
Call Waiting	Configure to enable/disable call waiting feature. The default setting is “No”.
User ‘#’ as SEND	If configured, the # key can be used as SNED key after dialing the number on the analog phone. The default setting is “Yes”.
RX Gain	Configure the RX gain for the receiving channel of analog FXS port. The valid range is -30Db to +6Db. The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of analog FXS port. The valid range is -30Db to +6Db. The default setting is 0.
MIN RX Flash	Configure the minimum period of time (in milliseconds) that the hook-flash must remain unpressed for the PBX to consider the event as a valid flash event. The valid range is 30ms to 1000ms. The default setting is 200ms.
MAX RX Flash	Configure the maximum period of time (in milliseconds) that the hook-flash must remain unpressed for the PBX to consider the event as a valid flash event. The minimum period of time is 256ms and it can’t be modified. The default setting is 1250ms.
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as hang up on a polarity reversal. The default setting is “Yes”.
Echo Cancellation	Specify “ON”, “OFF” or a value (the power of 2) from 32 to 1024 as the number of taps of cancellation. Note: When configuring the number of taps, the number 256 is not translated into 256ms of echo cancellation. Instead, 256 taps mean $256/8 = 32$ ms. The default setting is “ON”, which is 128 taps.



3-Way Calling	Configure to enable/disable 3-way calling feature on the user. The default setting is enabled.
Send CallerID After	Configure the number of rings before sending CID. Default setting is 1.
Fax Mode	<p>For FXS extension, there are three options available in Fax Mode. The default setting is “None”.</p> <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38. • Fax Gateway: If selected, the UCM6510 can support conversation and processing of Fax data from T.30 to T.38 or T.38 to T.30. This feature is only available for FXS or FXO port.

Table 43: FXS Extension Configuration Parameters – Features

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	<p>Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Note:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.



	<p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	<p>Select time condition for Call Forward Busy. The available time conditions are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.</p> <p>Notes:</p> <ul style="list-style-type: none"> • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page System Settings→Time Settings→Office Time/Holiday page.
CC Settings	
Enable CC	If enabled, UCM6510 will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason.
Ring Simultaneously	
Ring Simultaneously	<p>Enable this option to have an external number ring simultaneously along with the extension.</p> <p>If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.</p>
External Number	Set the external number to be rang simultaneously. ‘-’ is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Hotline	
Enable Hotline	If enabled, hotline dialing plan will be activated, a pre-configured number will be used according to selected Hotline Type.



Hotline Number	Configure the Hotline Number
Hotline Type	Configure the Hotline Type: <ul style="list-style-type: none"> • Immediate Hotline: When the phone is off-hook, UCM6510 will immediately dial the preset number • Delay Hotline: When the phone is off-hook, if there is no dialing within 5 seconds, UCM6510 will dial the preset number.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under Web GUI→ PBX Settings → General Settings : General Preference. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→ CDR → Recording Files .
Skip Trunk Auth	<ul style="list-style-type: none"> • If set to “Yes”, users can skip entering the password when making outbound calls. • If set to “By Time”, users can skip entering the password when making outbound calls during the selected time condition. • If set to “No”, users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If “Skip Trunk Auth” is set to “By Time”, select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.
Enable LDAP	If enabled, this extension will be added to LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
Music On Hold	Select which Music On Hold class to suggest to extension when putting the active call on hold.
Call Duration Limit	Configure the maximum duration of call-blocking.

Table 44: FXS Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.



Batch Add Extensions

Batch Add SIP Extensions

In order to add multiple SIP extensions, BATCH add can be used to create standardized SIP extension accounts. However, unique extension user name can't be set using BATCH add.

Under Web GUI→**Extension/Trunk**→**Extensions**, click on "Add" and select extension type as SIP extension, and "add method" as Batch.

Table 45: Batch Add SIP Extension Parameters

General	
Start Extension	Configure the starting extension number of the batch of extensions to be added.
Create Number	Specify the number of extensions to be added. The default setting is 5.
Extension Interval	Specify the interval between extensions as preferred when creating a batch of extension.
Permission	<p>Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".</p> <p>Note: Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls using this rule. If the outbound rule privilege is disabled, this option will not take effect.</p>
Enable Voicemail	<p>Enable Voicemail for the user. The default setting is "Yes".</p>
SIP/IAX Password	<p>Configure the SIP/IAX password for the users. Two options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"> User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. Enter a password to be used on all the extensions in the batch.
Voicemail Password	<p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"> User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. Enter a password to be used on all the extensions in the batch.
CallerID Number	<p>Configure CallerID Number when adding Batch Extensions.</p> <ul style="list-style-type: none"> Use Extension as Number Users can choose to use the extension number as CallerID



	<ul style="list-style-type: none"> Use as Number Users can choose to set a specific number instead of using the extension number as CallerID.
Ring Timeout	<p>Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under Web GUI→Internal Options: General Preference. The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
Auto Record	<p>Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files will be saved in external storage if plugged in and can be accessed under Web GUI→CDR→Recording Files.</p>
Skip Voicemail Password Verification	<p>When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.</p>
Music On Hold	<p>Select which Music On Hold class to suggest to extensions when putting them on hold.</p>
Enable LDAP	<p>If enabled, the batch added extensions will be added to LDAP Phonebook PBX list; if disabled, the batch added extensions will be skipped when creating LDAP Phonebook.</p>
Enable WebRTC Support	<p>If enabled, extensions will be able to login to user portal and use Web RTC features.</p>
Call Duration Limit	<p>Configure the maximum duration of call-blocking.</p>
SIP Settings	
NAT	<p>Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it's related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.</p>
Can Direct Media	<p>By default, the PBX will route the media streams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing. The default setting is "No".</p>



DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is “RFC2833”. If “Info” is selected, SIP INFO message will be used. If “Inband” is selected, 64-kbit codec PCMU and PCMA are required. When “Auto” is selected, RFC2833 will be used if offered, otherwise “Inband” will be used.
Enable Keep-alive	If enabled, empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is “Yes”.
Keep-alive Frequency	Configure the number of seconds for the host to be up for Keep-alive. The default setting is 60 seconds.
TEL URI	If the end device/phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. Then a “User=Phone” parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to “Enable”, “Tel:” will be used instead of “SIP:” in the SIP request. The default setting is disabled.
Concurrent Registrations	The maximum endpoints which can be registered into this extension. For security concerns, the default value is 1.
Other Settings	
SRTP	Enable SRTP for the call. The default setting is “No”.
Fax Mode	<p>Select Fax mode for this user. The default setting is “None”.</p> <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38. <p>Note: If enabled, Fax Pass-through cannot be used.</p>
Strategy	<p>This option controls how the extension can be used on devices within different types of network.</p> <ul style="list-style-type: none"> • Allow All Device in any network can register this extension. • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address Only the device on the specific IP address can register this extension. <p>The default setting is “Allow All”.</p>
Enable T.38 UDPTL	Enable or disable T.38 UDPTL Support.
Skip Trunk Auth	If enabled, users will not need enter the “PIN Set” required by the outbound rule to make outbound calls. The default setting is “No”.



Codec Preference

Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.722, G.729, G.723, ILBC, ADPCM, LPC10, H.264, H.263 and H.263p. In the selected codec list, users can click on UP or DOWN arrow to adjust the order for the codec priority.

Batch Add IAX Extensions

Under Web GUI→**Extension/Trunk**→**Extensions**, click on "Add" and select extension type as IAX extension, and "add method" as Batch.

Table 46: Batch Add IAX Extension Parameters

General	
Start Extension	Configure the starting extension number of the batch of extensions to be added.
Create Number	Specify the number of extensions to be added. The default setting is 5.
Permission	<p>Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".</p> <p>Note:</p> <p>Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls from this rule.</p>
Enable Voicemail	Enable Voicemail for the user. The default setting is "Yes".
SIP/IAX Password	<p>Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions.</p> <ul style="list-style-type: none"> User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Voicemail Password	<p>Configure Voicemail password (digits only) for the users.</p> <ul style="list-style-type: none"> User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. Use Extension as Password. Enter a password to be used on all the extensions in the batch.
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the



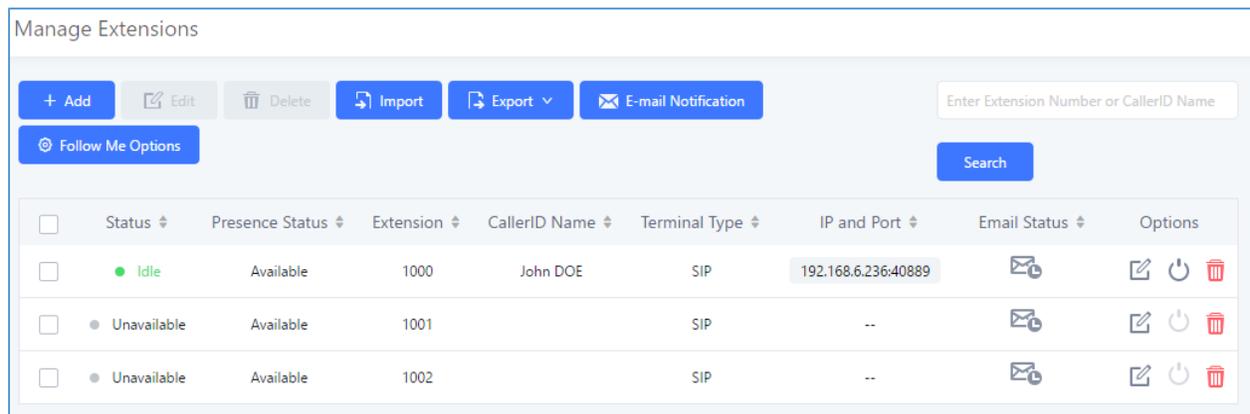
	<p>UCM6510, which can be configured in the global ring timeout setting under Web GUI→PBX Settings→General Settings: General Preference. The valid range is between 5 seconds and 600 seconds.</p> <p>Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.</p>
Auto Record	<p>Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.</p>
Skip Voicemail Password Verification	<p>When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.</p>
Music On Hold	<p>Select which Music On Hold class to suggest to extensions when putting them on hold.</p>
Call Duration Limit	<p>Configure the maximum duration of call-blocking.</p>
Enable LDAP	<p>If enabled, the batch added extensions will be added to LDAP Phonebook PBX list; if disabled, the batch added extensions will be skipped when creating LDAP Phonebook.</p>
IAX Settings	
Max Number of Calls	<p>Configure the maximum number of calls allowed for each remote IP address.</p>
Require Call Token	<p>Configure to enable/disable requiring call token. If set to “Auto”, it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints. The default setting is “Yes”.</p>
Other Settings	
SRTP	<p>Enable SRTP for the call. The default setting is “No”.</p>
Fax Mode	<p>Select Fax Mode for this user. The default setting is “None”.</p> <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.
Strategy	<p>This option controls how the extension can be used on devices within different types of network.</p> <ul style="list-style-type: none"> • Allow All Device in any network can register this extension.



	<ul style="list-style-type: none"> • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address. Only the device on the specific IP address can register this extension. The default setting is “Allow All”.
Skip Trunk Auth	If enable “All”, users do not need to enter password when making an outbound call. If enable “Follow Me”, the call can dial out via follow me without password.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.722, G.729, G.723, ILBC, ADPCM, LPC10, H.264, H.263 and H.263p.

Search and Edit Extension

All the UCM6510 extensions are listed under Web GUI→**Extension/Trunk**→**Extensions**, with status, Extension, CallerID Name, Technology (SIP, IAX and FXS), IP and Port. Each extension has a checkbox for users to “Modify Selected Extensions” or “Delete Selected Extensions”. Also, options “Edit” , “Reboot”  and “Delete”  are available per extension. User can search an extension by specifying the extension number to find an extension quickly.



The screenshot shows the 'Manage Extensions' interface. At the top, there are buttons for '+ Add', 'Edit', 'Delete', 'Import', 'Export', and 'E-mail Notification'. A search bar is labeled 'Enter Extension Number or CallerID Name'. Below the buttons is a 'Follow Me Options' button. The main part of the interface is a table with the following columns: Status, Presence Status, Extension, CallerID Name, Terminal Type, IP and Port, Email Status, and Options. The table contains three rows of data:

Status	Presence Status	Extension	CallerID Name	Terminal Type	IP and Port	Email Status	Options
Idle	Available	1000	John DOE	SIP	192.168.6.236:40889		
Unavailable	Available	1001		SIP	--		
Unavailable	Available	1002		SIP	--		

Figure 94: Manage Extensions

- **Status**

Users can see the following icon for each extension to indicate the SIP status.

- **Green:** Free
- **Blue:** Ringing
- **Yellow:** In Use
- **Grey:** Unavailable



- **Edit single extension**

Click on  to start editing the extension parameters.

- **Reboot the user**

Click on  to send NOTIFY reboot event to the device which has an UCM6510 extension already registered. To successfully reboot the user, “Zero Config” needs to be enabled on the UCM6510 Web GUI→**Value-added Features**→**Zero Config**→**Auto Provisioning Settings**.

- **Delete single extension**

Click on  to delete the extension. Or select the checkbox of the extension and then click on “Delete Selected Extensions”.

- **Modify selected extensions**

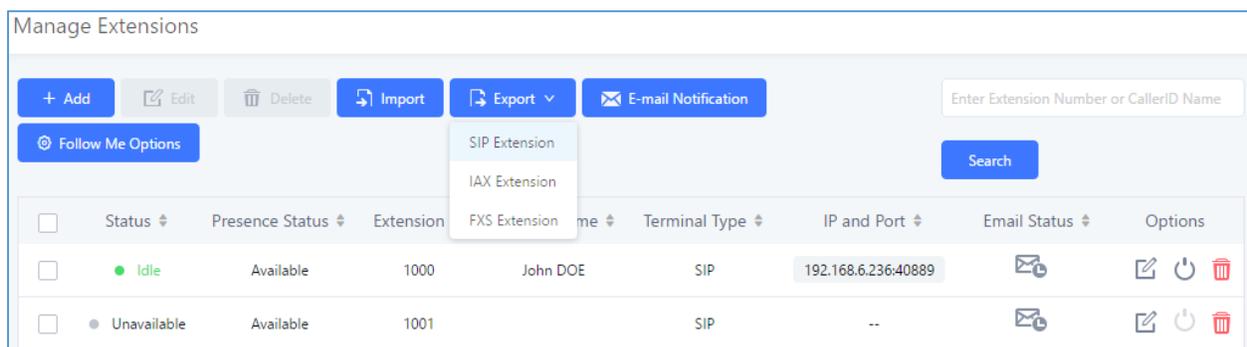
Select the checkbox for the extension(s). Then click on “Modify Selected Extensions” to edit the extensions in a batch.

- **Delete selected extensions**

Select the checkbox for the extension(s). Then click on “Delete Selected Extensions” to delete the extension(s).

Export Extensions

The extensions configured on the UCM6510 can be exported to csv format file with selected technology “SIP”, “IAX” or “FXS”. Click on “Import Extensions” scroll down to select “Export Extensions” button and select technology in the prompt.



The screenshot shows the 'Manage Extensions' interface. At the top, there are buttons for '+ Add', 'Edit', 'Delete', 'Import', 'Export', and 'E-mail Notification'. The 'Export' button is active, and a dropdown menu is open, showing options for 'SIP Extension', 'IAX Extension', and 'FXS Extension'. Below the buttons is a search bar with the placeholder text 'Enter Extension Number or CallerID Name' and a 'Search' button. The main area contains a table with columns: Status, Presence Status, Extension, Name, Terminal Type, IP and Port, Email Status, and Options. Two rows are visible in the table:

Status	Presence Status	Extension	Name	Terminal Type	IP and Port	Email Status	Options
Idle	Available	1000	John DOE	SIP	192.168.6.236:40889		
Unavailable	Available	1001		SIP	--		

Figure 95: Export Extensions

The exported csv file can also serve as a template for users to fill in desired extension information to be imported to the UCM6510.



Import Extensions

The capability to import extensions to the UCM6510 provides users flexibility to batch add extensions with similar or different configurations quickly.

1. Export extension csv file from the UCM6510 by clicking on “Export Extensions” button.
2. Fill up the extension information you would like in the exported csv template.
3. Click on “Import Extensions” button. The following dialog will be prompted.

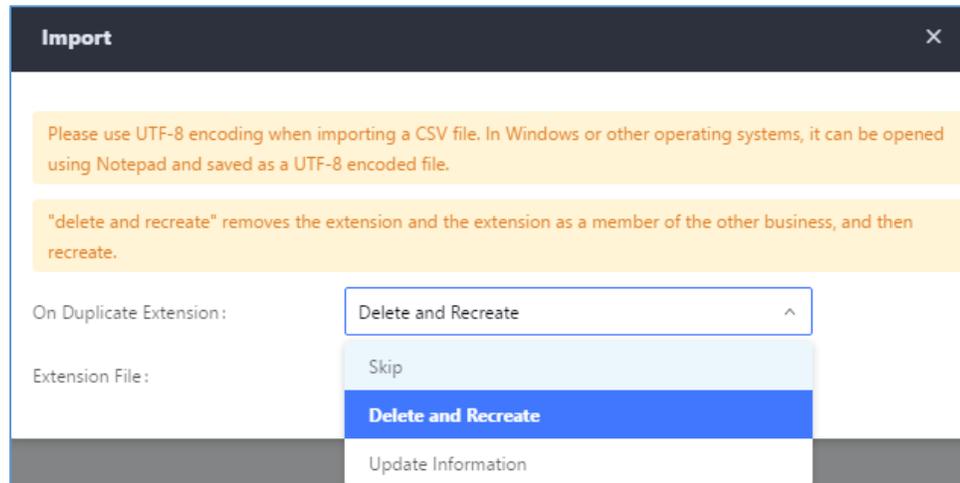


Figure 96: Export Extensions

4. Select the option in “On Duplicate Extension” to define how the duplicate extension(s) in the imported csv file should be treated by the PBX.
 - Skip: Duplicate extensions in the csv file will be skipped. The PBX will keep the current extension information as previously configured without change.
 - Delete and Recreate: The current extension previously configured will be deleted and the duplicate extension in the csv file will be loaded to the PBX.
 - Update Information: The current extension previously configured in the PBX will be kept. However, if the duplicate extension in the csv file has different configuration for any options, it will override the configuration for those options in the extension.
5. Click on “choose file to upload” to select csv file from local directory in the PC for uploading.
6. Click on “Save” to import the csv file.
7. Click on “Apply Changes” to apply the imported file on the UCM6510.

Note: The imported file should look like the following:



A	B	C	D	E	F	G	H	I	J	K	L	M	N
Extension	Technology	Enable Voicemail	CallerID	SIP/IAX Password	Voicema	Skip Voicemail Password Verification	Ring Timeout	Auto Record	SRTP	Fax Mode	Strategy	Local Subnet 1	Local Sub
1000	SIP	yes	1000	admin123	61783	no		no	no	None	Allow All		
1001	SIP	yes	1001	admin123	955921	no		no	no	None	Allow All		
1002	SIP	yes	1002	admin123	269824	no		no	no	None	Allow All		
1003	SIP	yes	1003	admin123	363196	no		no	no	None	Allow All		
1004	SIP	yes	1004	admin123	12860	no		no	no	None	Allow All		

Figure 97: Import File

Table 47: SIP Extensions Imported File Example

Field	Supported values
Extension	Digits
Technology	SIP/SIP(WebRTC)
Enable Voicemail	yes/no
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Fax Mode	None/Fax Detection
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask
Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
NAT	yes/no
DTMF Mode	RFC2833/info/inband/auto



Insecure	Port
Enable Keep-alive	Yes/no
Keep-alive Frequency	Value from 1-3600
AuthID	Alphanumeric value without special characters
TEL URI	Disabled/user=phone/enabled
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Support Hot-Desking Mode	Yes/no
Dial Trunk Password	Digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Enable T.38 UDPTL	Yes/no
Max Contacts	Values from 1-10
Enable WebRTC	Yes/no



Alert-Info	None/Ring 1/Ring2/Ring3/Ring 4/Ring 5/Ring 6/Ring 7/ Ring 8/Ring 9/Ring 10/bellcore-dr1/bellcore-dr2/ bellcore- dr3/ bellcore-dr4/ bellcore-dr5/custom
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Custom Auto answer	Yes/no
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.
Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits
Call-Barging Monitor	Extensions allowed to call barging
Seamless Transfer Members	Extensions allowed to seamless transfer

Table 48: IAX extensions Imported File Example

Field	Supported values
Extension	Digits
Technology	IAX
Enable Voicemail	yes/no
CallerID Number	Digits
SIP/IAX Password	Alphanumeric characters
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
SRTP	yes/no
Fax Mode	None/Fax Detection
Strategy	Allow All/Local Subnet Only/A Specific IP Address
Local Subnet 1	IP address/Mask
Local Subnet 2	IP address/Mask
Local Subnet 3	IP address/Mask
Local Subnet 4	IP address/Mask
Local Subnet 5	IP address/Mask
Local Subnet 6	IP address/Mask
Local Subnet 7	IP address/Mask



Local Subnet 8	IP address/Mask
Local Subnet 9	IP address/Mask
Local Subnet 10	IP address/Mask
Specific IP Address	IP address
Skip Trunk Auth	yes/no/bytime
Codec Preference	PCMU,PCMA,GSM,G.726,G.722,G.729,H.264,ILBC,AAL2-G.726-32,ADPCM,G.723,H.263,H.263p,vp8,opus
Permission	Internal/Local/National/International
NAT	yes/no
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Require Call Token	Yes/no/auto
Max Number of Calls	Values from 1-512
Dial Trunk Password	Digits
Disable This Extension	Yes/no
CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Limit Max time (s)	empty
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.



Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits
Call-Barging Monitor	Extensions allowed to call barging
Seamless Transfer Members	Extensions allowed to seamless transfer

Table 49: FXS extensions Imported File Example

Field	Supported values
Extension	Digits
Technology	FXS
Analog Station	FXS1/FXS2
Enable Voicemail	yes/no
CallerID Number	Digits
Voicemail Password	Digits
Skip Voicemail Password Verification	yes/no
Ring Timeout	Empty/ 3 to 600 (in second)
Auto Record	yes/no
Fax Mode	None/Fax Detection
Skip Trunk Auth	Yes/no/bytime
Permission	Internal/Local/National/International
Call Forward Busy	Digits
Call Forward No Answer	Digits
Call Forward Unconditional	Digits
Call Waiting	Yes/no
Use # as SEND	Yes/no
RX Gain	Values from -30→6
TX Gain	Values from -30→6
MIN RX Flash	Values from: 30 – 1000
MAX RX Flash	Values from: 40 – 2000
Enable Polarity Reversal	Yes/no
Echo Cancellation	On/Off/32/64/128/256/512/1024
3-Way Calling	Yes/no
Send CallerID After	1/2
Dial Trunk Password	digits
Disable This Extension	Yes/no



CFU Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFN Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
CFB Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Music On Hold	Default/ringbacktone_default
CC Agent Policy	If CC is disabled use: never If CC is set to normal use: generic If CC is set to trunk use: native
CC Monitor Policy	Generic/never
CCBS Available Timer	3600/4800
CCNR Available Timer	3600/7200
CC Offer Timer	60/120
CC Max Agents	Value from 1-999
CC Max Monitors	Value from 1-999
Ring simultaneously	Yes/no
External Number	Digits
Time Condition for Ring Simultaneously	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Time Condition for Skip Trunk Auth	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Enable LDAP	Yes/no
Enable Hotline	Yes/no
Hotline Type	Immediate hotline/delay hotline
Hotline Number	digits
Limit Max time (s)	empty
Do Not Disturb	Yes/no
DND Time Condition	All time/Office time/out of office time/holiday/out of holiday/out of office time or holiday/specific time
Do Not Disturb Whitelist	Empty/digits
User Password	Alphanumeric characters.
First Name	Alphanumeric without special characters.
Last Name	Alphanumeric without special characters.
Email Address	Email address
Language	Default/en/zh
Phone Number	Digits



Call-Barging Monitor	Extensions allowed to call barging
Seamless Transfer Members	Extensions allowed to seamless transfer

The CSV file should contain all the above fields, if one of them is missing or empty, the UCM6510 will display the following error message for missing fields.

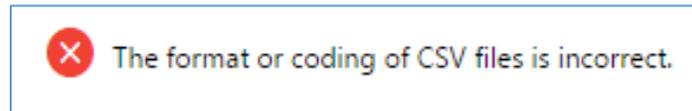


Figure 98: Import Error

E-mail Notification

Once the extensions are created with Email address, the PBX administrator can click on button “E-mail Notification” to send the account registration and configuration information to the user. Please make sure Email setting under Web GUI→**System Settings**→**Email Settings** is properly configured and tested on the UCM6510 before using “E-mail Notification”.

When click on “E-mail Notification” button, the following message will be prompted in the web page. Click on OK to confirm sending the account information to all users’ Email addresses.

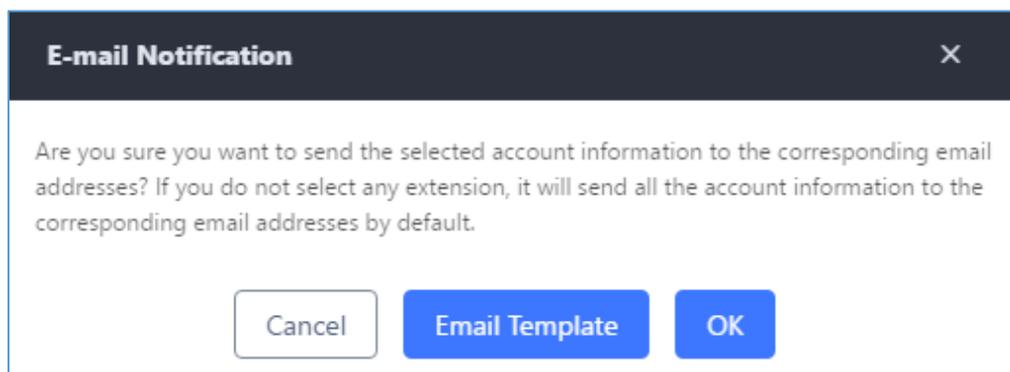


Figure 99: E-mail Notification Prompt Information

The user will receive Email including account registration information and LDAP configuration. A QR code is also generated for Mobile applications to scan it and get automatically provisioned. QR code provisioning is supported on Grandstream Softphone GS Wave Android™ application.

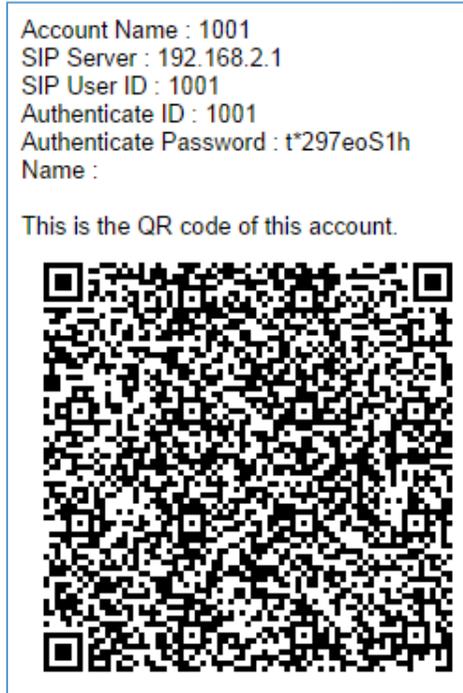


Figure 100: E-mail Notification: Account Registration Information and QR Code



Figure 101: E-mail Notification LDAP Client Information and QR Code

Multiple Registrations per Extension

UCM6510 supports multiple registrations per extension so that users can use the same extension on devices in different locations.

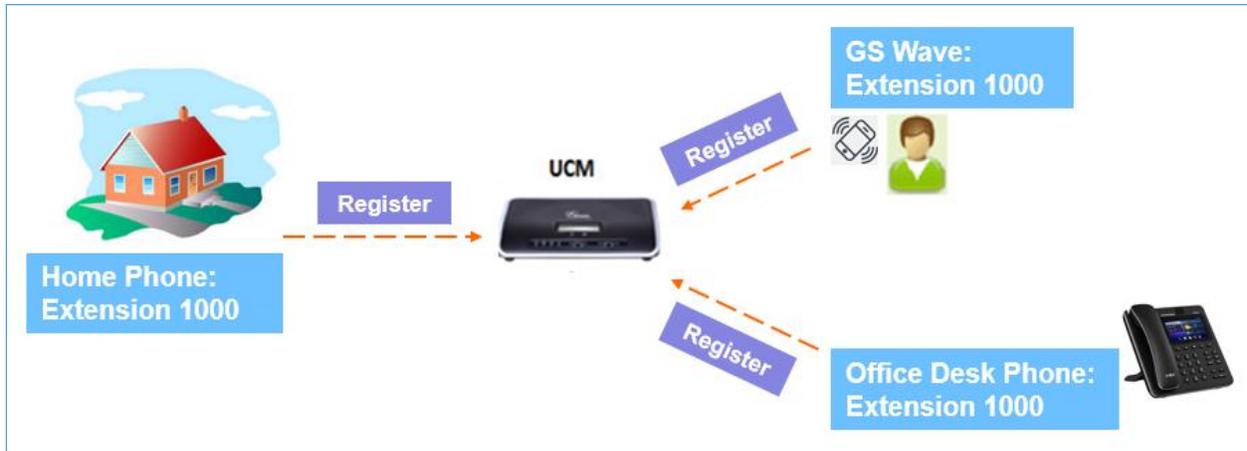


Figure 102: Multiple Registrations per Extension

This feature can be enabled by configuring option “Concurrent Registrations” under Web GUI → **Extension/Trunk** → **Edit Extension**. The default value is set to 1 for security purpose. Maximum is 10.

Edit Extension: 1000 Save

Basic Settings Media Features Specific Time Follow Me

General

* Extension: <input type="text" value="1000"/>	CallerID Number: <input type="text"/>
* Permission: <input type="text" value="Internal"/>	* SIP/IAX Password: <input type="text" value="DGc7BjoG"/>
AuthID: <input type="text"/>	Enable Voicemail: <input checked="" type="checkbox"/>
* Voicemail Password: <input type="text" value="791020"/>	Skip Voicemail Password V... <input type="checkbox"/>
Enable Keep-alive: <input type="checkbox"/>	* Keep-alive Frequency: <input type="text" value="60"/>
Disable This Extension: <input type="checkbox"/>	

User Settings

First Name: <input type="text" value="John"/>	Last Name: <input type="text" value="DOE"/>
Email Address: <input type="text" value="mbaomar@grandstream.com"/>	* User Password: <input type="text" value="*****"/>
* Language: <input type="text" value="Default"/>	* Concurrent Registration... <input style="border: 2px solid green;" type="text" value="3"/>
Mobile Phone Number: <input type="text"/>	

Figure 103: Extension - Concurrent Registration



SMS Message Support

The UCM6510 provides built-in SIP SMS message support. For SIP end devices such as Grandstream GXP or GXV phones that supports SIP message, after an UCM6510 account is registered on the end device, the user can send and receive SMS message. Please refer to the end device documentation on how to send and receive SMS message.

SMS Message support is a new feature added since firmware 1.0.10.x.



Figure 104: SMS Message Support

EXTENSION GROUPS

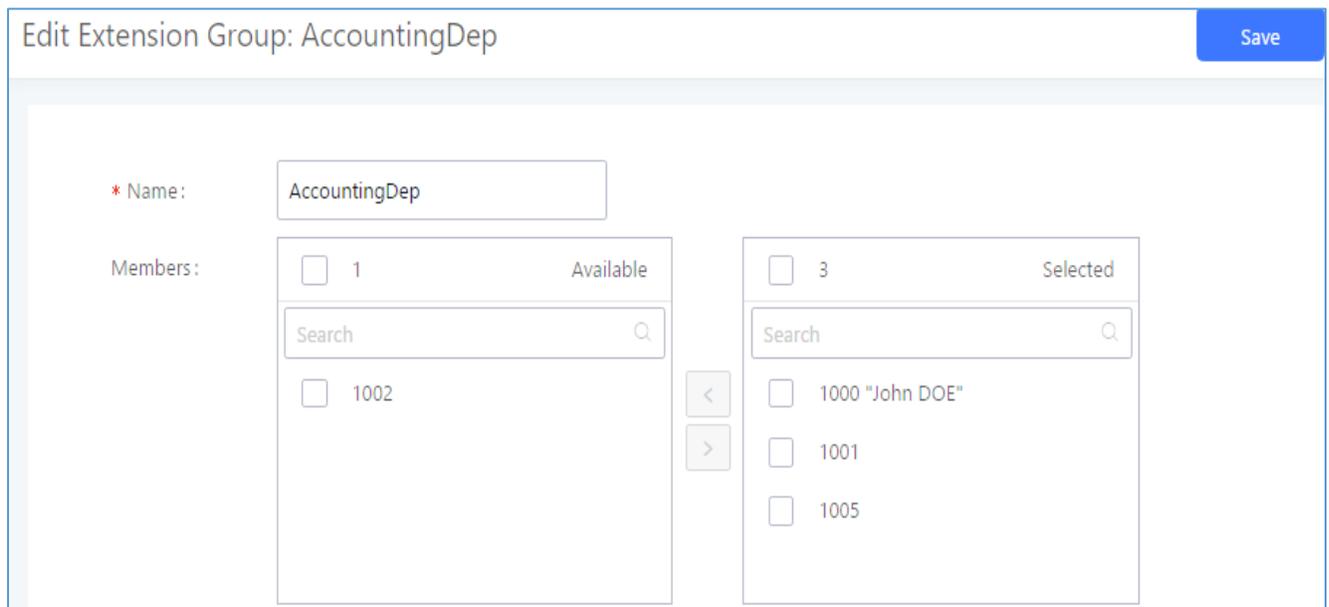
The UCM6510 extension group feature allows users to assign extensions to different groups to better manage the configurations on the PBX. For example, when configuring "Enable Filter on Source Caller ID", users could select a group instead of each person's extension to assign. This feature simplifies the configuration process and helps manage and categorize the extensions for business environment.

Configure Extension Groups

Extension group can be configured via Web GUI→**Call Features**→**Extension Groups**.

- Click on "Create New Extension Group" to create a new extension group.
- Click on  to edit the extension group.
- Click on  to delete the extension group.

Select extensions from the list on the left side to the right side.



The screenshot shows the 'Edit Extension Group' interface for a group named 'AccountingDep'. It features a 'Name' field with the value 'AccountingDep' and a 'Save' button. Below, there are two columns for managing members: 'Available' and 'Selected'. The 'Available' column contains a search bar and one member '1002'. The 'Selected' column contains a search bar and three members: '1000 "John DOE"', '1001', and '1005'. Navigation arrows are located between the two columns.

Figure 105: Edit Extension Group



Use Extension Groups

Here is an example where the extension group can be used. Go to Web GUI→**Extension/Trunk**→**Outbound Routes** and select "Enable Filter on Source Caller ID". Both single extensions and extension groups will show up for users to select.

Edit Outbound Rule: National
Save

<p>* Calling Rule Name: <input style="width: 80%;" type="text" value="National"/></p> <p>Disable This Route: <input type="checkbox"/></p> <p>Password: <input style="width: 80%;" type="text"/></p>	<p>* Pattern: <input style="width: 80%;" type="text" value="_xxxxxxxx"/></p> <p>PIN Groups: <input style="border: none; border-bottom: 1px solid #ccc; background-color: #f9f9f9; padding: 2px 5px; font-size: 0.9em; font-family: sans-serif; margin-bottom: 2px;" type="text" value="None"/> v</p> <p>Privilege Level: <input style="border: none; border-bottom: 1px solid #ccc; background-color: #f9f9f9; padding: 2px 5px; font-size: 0.9em; font-family: sans-serif; margin-bottom: 2px;" type="text" value="Disable"/> v</p>
---	--

Enable Filter on Source Caller ID

Enable Filter on Source.

Available Extensions/E...

* Custom Dynamic Ro...

Figure 106: Select Extension Group in Outbound Route



ANALOG TRUNKS

To set up analog trunk on the UCM6510:

- Go to Web GUI→**Extension/Trunk**→**Analog Trunks** to add and edit analog trunks.
- Go to Web GUI→**PBX Settings**→**Interface Settings** to configure analog hardware settings.

Analog Trunks Configuration

Go to Web GUI→**Extension/Trunk**→**Analog Trunks** to add and edit analog trunks.

- Click on “Create New Analog Trunk” to add a new analog trunk.
- Click on  to edit the analog trunk.
- Click on  to delete the analog trunk.

The analog trunk options are listed in the table below.

Table 50: Analog Trunk Configuration Parameters

Channels	Select the channel for the analog trunk.
Trunk Name	Specify a unique label to identify the trunk when listed in outbound routes, inbound routes and etc.
SLA Mode	Enable this option to satisfy two primary use cases, which include emulating a simple key system and creating shared extensions on a PBX. Enable SLA Mode will disable polarity reversal.
Barge Allowed	The barge option specifies whether or not other stations are allowed to join a call in progress on this trunk. If enabled, the other stations can press the line button to join the call. The default setting is Yes.
Hold Access	The hold option specifies hold permissions for this trunk. If set to “Open”, any station can place this trunk on hold and any other station is allowed to retrieve the call. If set to “Private”, only the station that places the call on hold can retrieve the call. The default setting is Yes.
Advanced Options	
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as “hang up” on a polarity reversal. The default setting is “No”.



Polarity on Answer Delay	When FXO port answers the call, FXS may send a Polarity Reversal. If this interval is shorter than the value of “Polarity on Answer Delay”, the Polarity Reversal will be ignored. Otherwise, the FXO will on-hook to disconnect the call. The default setting is 600ms.
Current Disconnect Threshold (ms)	This is the periodic time (in ms) that the UCM6510 will use to check on a voltage drop in the line. The default setting is 200. Valid range is 50 to 3000.
Ring Timeout	Configure the ring timeout (in ms). Trunk (FXO) devices must have a timeout to determine if there was a hang up before the line is answered. This value can be used to configure how long it takes before the UCM6510 considers a non-ringing line with hang up activity. Default setting is 8000.
RX Gain	Configure the RX gain for the receiving channel of analog FXO port. The valid range is from -13.5 (Db) to + 12.0 (Db). The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of analog FXO port. The valid range is from -13.5 (Db) to + 12.0 (Db). The default setting is 0.
Use CallerID	Configure to enable CallerID detection. The default setting is “Yes”.
Fax Detection	Enable to detect Fax signal from the trunk during the call and send the received Fax to the default Email address in Fax setting page under Web GUI→ Call Features → Fax/T.38 . The default setting is “No”. Note: If enabled, Fax Pass-through cannot be used.
Caller ID Scheme	Select the Caller ID scheme for this trunk. If you are not sure which scheme to choose, please select “Auto Detect”. The default setting is “Bellcore/Telcordia”.
FXO Dial Delay(ms)	Configure the time interval between off-hook and first dialed digit for outbound calls.
Auto Record	Enable automatic recording for the calls using this trunk. The default setting is disabled. The recording files are saved in external storage device if plugged in and can be accessed under Web GUI→ CDR → Recording Files .
Disable This Trunk	If selected, the trunk will be disabled.
DAHDI Out Line Selection	This is to implement analog trunk outbound line selection strategy. Three options are available: <ul style="list-style-type: none"> • Ascend: When the call goes out from this analog trunk, it will always try to use the first idle FXO port. The port order that the call will use to go out would be port 1→port 2→port 10→port 16. Every time it will start with port 1 (if it’s idle). • Poll: When the call goes out from this analog trunk, it will use the port that is not used last time. And it will always use the port in the order of port 1→2→10→16→1→2→10→16→1→2→10→16..., following the last port being used.



	<ul style="list-style-type: none"> • Descend: When the call goes out from this analog trunk, it will always try to use the last idle FXO port. The port order that the call will use to go out would be port 16→port 10→port 2→port 1. Every time it will start with port 16 (if it's idle). The default setting is "Ascend" mode.
Tone Settings	
Busy Detection	Busy Detection is used to detect far end hang up or for detecting busy signal. The default setting is "Yes".
Busy Tone Count	If "Busy Detection" is enabled, users can specify the number of busy tones to be played before hanging up. The default setting is 2. Better results might be achieved if set to 4, 6 or even 8. Please note that the higher the number is, the more time is needed to hang up the channel. However, this might lower the probability to get random hang up.
Congestion Detection	Congestion detection is used to detect far end congestion signal. The default setting is "Yes".
Congestion Count	If "Congestion Detection" is enabled, users can specify the number of congestion tones to wait for. The default setting is 2.
Tone Country	Select the country for tone settings. If "Custom" is selected, users could manually configure the values for Busy Tone and Congestion Tone. The default setting is "United States of America (USA)".
Busy Tone	<p><u>Syntax:</u> <code>f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]];</code> Frequencies are in Hz and cadence on and off are in ms. Frequencies Range: [0, 4000] Busy Level Range: (-300, 0) Cadence Range: [0, 16383]. Select Tone Country "Custom" to manually configure Busy Tone value. <u>Default value:</u> <code>f1=480@-50,f2=620@-50,c=500/500</code></p>
Congestion Tone	<p><u>Syntax:</u> <code>f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]];</code> Frequencies are in Hz and cadence on and off are in ms. Frequencies Range: [0, 4000] Busy Level Range: (-300, 0) Cadence Range: [0, 16383]. Select Tone Country "Custom" to manually configure Busy Tone value. <u>Default value:</u> <code>f1=480@-50,f2=620@-50,c=250/250</code></p>



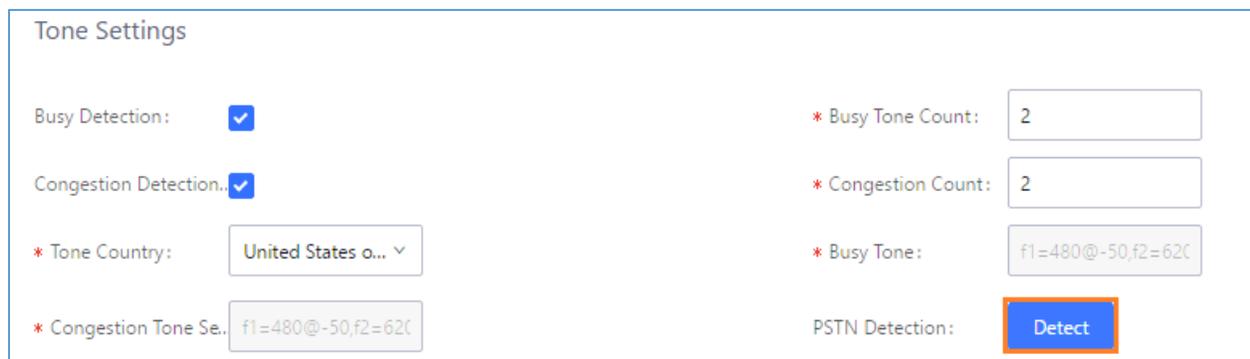
PSTN Detection

Click on “Detect” to detect the busy tone, Polarity Reversal and Current Disconnect by PSTN. Before the detecting, please make sure there are more than one channel configured and working properly. If the detection has busy tone, the “Tone Country” option will be set as “Custom”.

PSTN Detection

The UCM6510 provides PSTN detection function to help users detect the busy tone, Polarity Reversal and Current Disconnect by making a call from the PSTN line to another destination. The detecting call will be answered and up for about 1 minute. Once done, the detecting result will show and can be used for the UCM6510 settings.

1. Go to UCM6510 Web GUI→**Extension/Trunk**→**Analog Trunks** page.
2. Click to edit the analog trunk created for the FXO port.
3. In the dialog window to edit the analog trunk, go to “Tone Settings” section and click on “Detect” for “PSTN Detection”.



Tone Settings

Busy Detection:

Congestion Detection:

* Tone Country:

* Congestion Tone Se.:

* Busy Tone Count:

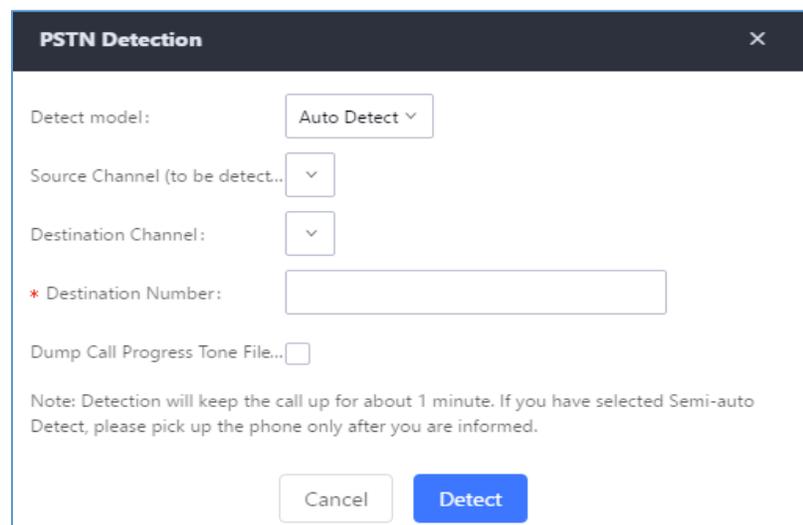
* Congestion Count:

* Busy Tone:

PSTN Detection:

Figure 107: UCM6510 FXO Tone Settings

4. Click on “Detect” to start PSTN detection.



PSTN Detection [X]

Detect model:

Source Channel (to be detect..):

Destination Channel:

* Destination Number:

Dump Call Progress Tone File...

Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please pick up the phone only after you are informed.

Figure 108: UCM6510 PSTN Detection



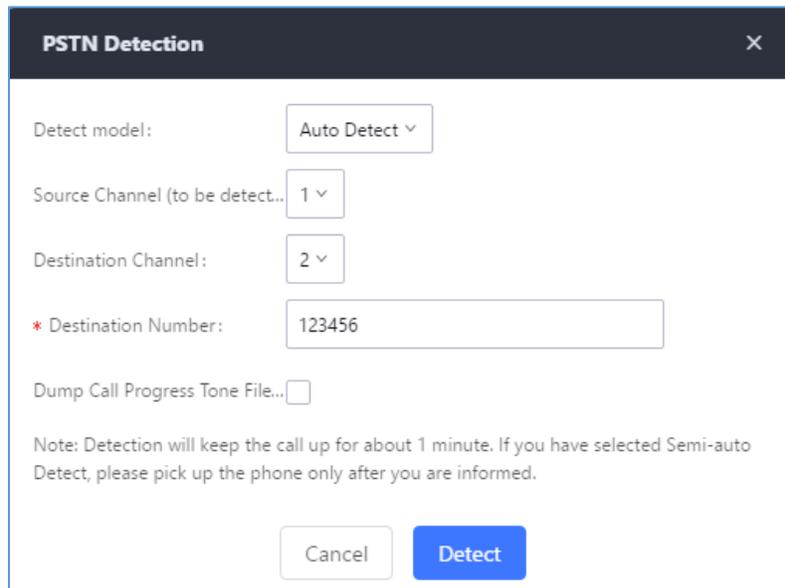
- If there are two FXO ports connected to PSTN lines, use the following settings for auto-detection.

Detect Model: Auto Detect.

Source Channel: The source channel to be detected.

Destination Channel: The channel to help detecting. For example, the second FXO port.

Destination Number: The number to be dialed for detecting. This number must be the actual PSTN number for the FXO port used as the destination channel.



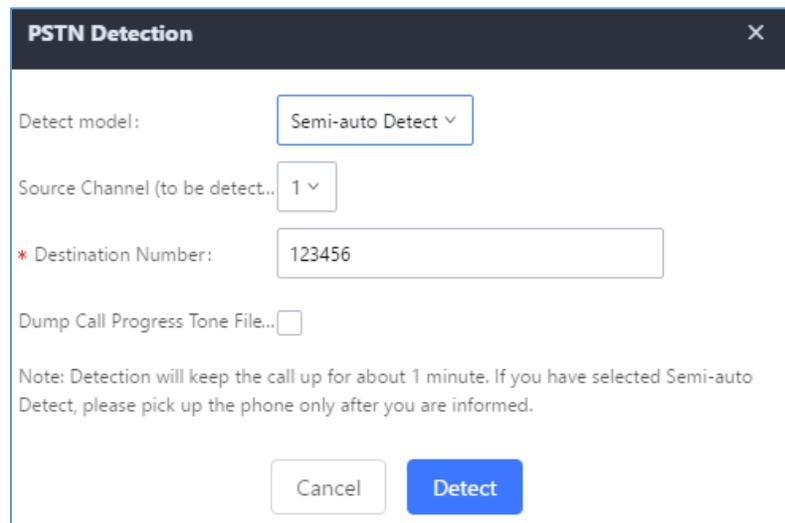
The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The settings are as follows:

- Detect model: Auto Detect (dropdown menu)
- Source Channel (to be detect...): 1 (dropdown menu)
- Destination Channel: 2 (dropdown menu)
- * Destination Number: 123456 (text input field)
- Dump Call Progress Tone File...:

Below the input fields is a note: "Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please pick up the phone only after you are informed." At the bottom are two buttons: "Cancel" and "Detect".

Figure 109: UCM6510 PSTN Detection: Auto Detect

- If there is only one FXO port connected to PSTN line, use the following settings for auto-detection.



The screenshot shows a dialog box titled "PSTN Detection" with a close button (X) in the top right corner. The settings are as follows:

- Detect model: Semi-auto Detect (dropdown menu)
- Source Channel (to be detect...): 1 (dropdown menu)
- * Destination Number: 123456 (text input field)
- Dump Call Progress Tone File...:

Below the input fields is a note: "Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please pick up the phone only after you are informed." At the bottom are two buttons: "Cancel" and "Detect".

Figure 110: UCM6510 PSTN Detection: Semi-Auto Detect



Detect Model: Semi-auto Detect.

Source Channel: The source channel to be detected.

Destination Number: The number to be dialed for detecting. This number could be a cell phone number or other PSTN number that can be reached from the source channel PSTN number.

5. Click “Detect” to start detecting. The source channel will initiate a call to the destination number. For “Auto Detect”, the call will be automatically answered. For “Semi-auto Detect”, the UCM6510 Web GUI will display prompt to notify the user to answer or hang up the call to finish the detecting process.
6. Once done, the detected result will show. Users could save the detecting result as the current UCM6510 settings.

Table 51: PSTN Detection for Analog Trunk

Detect Model	<p>Select “Auto Detect” or “Semi-auto Detect” for PSTN detection.</p> <ul style="list-style-type: none"> • Auto Detect Please make sure two or more channels are connected to the UCM6510 and in idle status before starting the detection. During the detection, one channel will be used as caller (Source Channel) and another channel will be used as callee (Destination Channel). The UCM6510 will control the call to be established and hang up between caller and callee to finish the detection. • Semi-auto Detect Semi-auto detection requires answering or hanging up the call manually. Please make sure one channel is connected to the UCM6510 and in idle status before starting the detection. During the detection, source channel will be used as caller and send the call to the configured Destination Number. Users will then need follow the prompts in Web GUI to help finish the detection. <p>The default setting is “Auto Detect”.</p>
Source Channel	Select the channel to be detected.
Destination Channel	Select the channel to help detect when “Auto Detect” is used.
Destination Number	Configure the number to be called to help the detection.



Note:

- The PSTN detection process will keep the call up for about 1 minute.
- If “Semi-auto Detect” is used, please pick up the call only after informed from the Web GUI prompt.
- Once the detection is successful, the detected parameters “Busy Tone”, “Polarity Reversal” and “Current Disconnect by PSTN” will be filled into the corresponding fields in the analog trunk configuration.



DAHDI and Analog Hardware Configuration

Analog Hardware

The analog hardware (FXS port and FXO port) on the UCM6510 can be configured under Web GUI→**PBX Settings**→**Interface Settings**. Click on  to edit signaling preference for FXS port or configure ACIM settings for FXO port.

Select “Loop Start” or “Kewl Start” for each FXS port. And then click on “Update” to save the change.

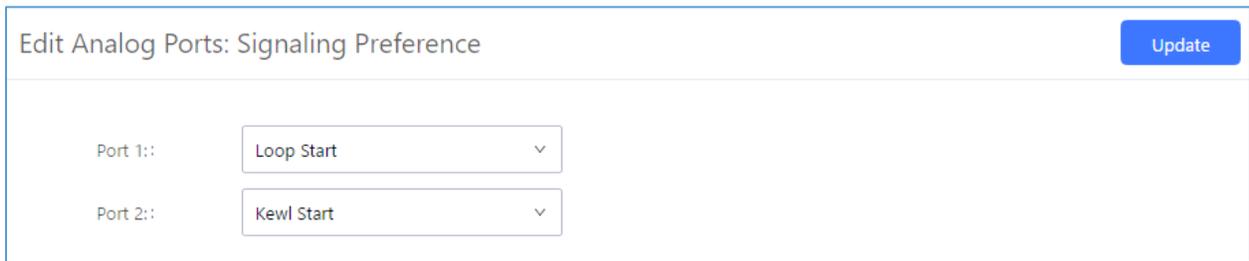


Figure 111: FXS Ports Signaling Preference

For FXO port, users could manually enter the ACIM settings by selecting the value from dropdown list for each port. Or users could click on "Detect" and choose the detection algorithm, two algorithms exist (ERL, Pr) for the UCM6510 to automatically detect the ACIM value. The detecting value will be automatically filled into the settings.

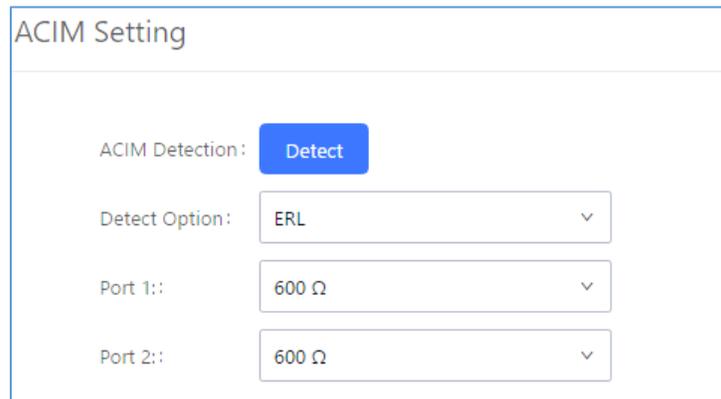


Figure 112: FXO Ports ACIM Settings

 **Note:**

ACIM setting is very important for the FXO/PSTN line to work properly on the UCM6510. If the users experience echo, caller ID or disconnecting issue, please make sure to run the ACIM detection to find out the correct value for impedance setting.

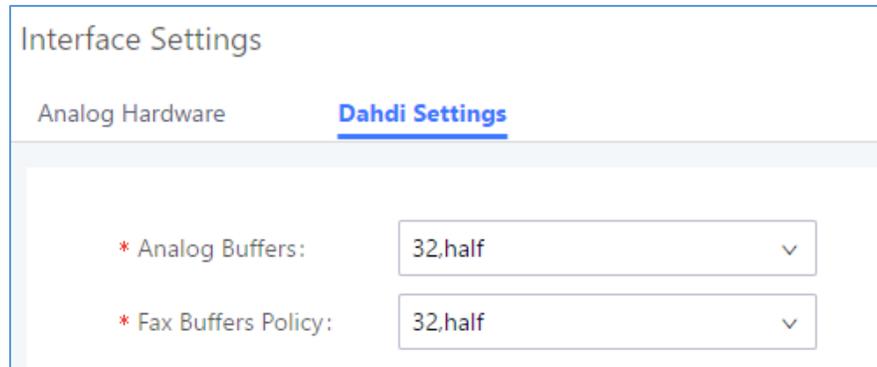
Table 52: Analog Hardware Configuration Parameters

Tone Region	Select country to set the default tones for dial tone, busy tone, ring tone and etc to be sent from the FXS port. The default setting is “United States of America (USA)”.
Advanced Settings	
FXO Opermode	Select country to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country’s analog line characteristics. The default setting is “USA”.
FXS Opermode	Select country to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country’s analog line characteristics. The default setting is “United States of America (USA)”.
FXS TISS Override	Configure to enable or disable override Two-Wire Impedance Synthesis (TISS). The default setting is No. If enabled, users can select the impedance value for Two-Wire Impedance Synthesis (TISS) override. The default setting is 600Ω.
PCMA Override	Select the codec to be used for analog lines. North American users should choose PCMU. All other countries, unless already known, should be assumed to be PCMA. The default setting is PCMU. Note: This option requires system reboot to take effect.
Boost Ringer	Configure whether normal ringing voltage (40V) or maximum ringing voltage (89V) for analog phones attached to the FXS port is required. The default setting is “Normal”.
Fast Ringer	Configure to increase the ringing speed to 25HZ. This option can be used with “Low Power” option. The default setting is “Normal”.
Low Power	Configure the peak voltage up to 50V during “Fast Ringer” operation. This option is used with “Fast Ringer”. The default setting is “Normal”.
Ring Detect	If set to “Full Wave”, false ring detection will be prevented for lines where Caller ID is sent before the first ring and proceeded by a polarity reversal, as in UK. The default setting is “Standard”.
FXS MWI Mode	Configure the type of Message Waiting Indicator on FXS lines. The default setting is “FSK”. <ul style="list-style-type: none"> • FSK: Frequency Shift Key Indicator • NEON: Light Neon Bulb Indicator.



DAHDI Settings

When users encounter issues such as audio delay in outbound calls using the analog trunk, they can adjust DAHDI settings on the UCM to attempt to lessen or resolve the issues.



Interface Settings

Analog Hardware **DAHDI Settings**

* Analog Buffers: 32,half

* Fax Buffers Policy: 32,half

Figure 113: Dahdi Settings

For the value of the option such as “32, half”:

The number in the option indicates the number of read/write buffers for TDM (DAHDI).

The “Half”, “Immediate” or “Full” option indicates the strategy when reading/writing data from buffer.

- “Half”: Data will be read/written from buffer when half of the buffer is occupied with data.
- “Immediate”: Read/write from buffer whenever there is data occupying the buffer.
- “Full”: Data will be read/written from buffer when buffer is fully occupied with data.



DIGITAL TRUNKS

The UCM6510 supports E1/T1/J1 which are physical connection technology used in digital network. T1 is the North American standard, J1 is used in Japan, whereas E1 is the European standard.

UCM6510 supports four signaling protocols: PRI, MFC/R2, SS7, E&M Immediate and E&M Wink. PRI provides a varying number of channels depending on the standards in the country of implementation (E1, T1 or J1); MFC/R2 is a signaling protocol heavily used over E1 trunks; SS7 uses out-of-band signaling, which travels on a separate, dedicated channel rather than within the same channel as the telephone call, providing more efficiency and higher security level when the telephone calls are set up. E&M Immediate and E&M Wink are only valid when using T1 port.

To set up digital trunk on the UCM6510:

1. Go to Web GUI→**PBX Settings**→**Interface Settings**→**Digital Hardware** to configure port type and channels.
2. Go to Web GUI→**Extension/Trunk**→**Digital Trunks** to add and edit digit trunk.
3. Go to Web GUI→**Extension/Trunk**→**Outbound Routes** and **Inbound Routes** to configure outbound and inbound rule for the digital trunk.

Digital Hardware Configuration

Go to Web GUI→ **PBX Settings**→**Interface Settings**→**Digital Hardware** page and configure the following:

Interface Settings			
<u>Digital Hardware</u>		Analog Hardware	
Type	Port	Options	
<input type="checkbox"/> E1	1	 	
Group Name	Channel	Options	
DefaultGroup1	1-8	 	
Test	9-15,17-31	 	

Figure 114: Digital Hardware Configuration



- **Step 1:** Click on  to edit digital ports. Please see configuration parameters in the tables below.
- **Step 2:** Click on  to edit group. This assigns channels to be used for the digital port. For E1, 30 B channels can be assigned to the default group; for T1/J1, 23 B channels can be assigned to the default group.
- **Step 3:** If fewer than 30 B channels for E1 or 23 B channels for T1/J1 are assigned in default group, users can click on  to add more groups. This is not necessary in most cases and only default group is needed.

 **Note:**

Currently, the group configuration in digit trunks settings is to manage outbound routes only. It doesn't control inbound routes. Therefore, if the users have configured multiple groups for the digital trunk, please make sure the inbound routes for those groups have the same inbound rule configured. Otherwise, inbound call using the digital trunk might not work properly.

The UCM6510 currently supports E1, T1 and J1 digital hardware type. When different signaling is selected for E1, T1 or J1, the settings in basic options and advanced options will be different. The following tables list all the settings to configure digital ports when selecting each signaling.

Table 53: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
LBO	<p>The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0Db unless the distance is long.</p>
RX Gain	<p>Configure the RX gain for the receiving channel of digital port. The valid range is from -24Db to +12Db.</p>
TX Gain	<p>Configure the TX Gain for the transmitting channel of digital port. The valid range is -24Db to +12Db.</p>
Codec	<p>Select alaw or ulaw. If set to default, alaw will be used for E1.</p>



Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Advanced Settings	
Switch Type	Select switch type. <ul style="list-style-type: none"> • EuroISDN: EuroISDN (common in Europe) • NI2: National ISDN type 2 (common in the US) • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
Coding	Select “HDB3” or “AMI”.
CRC	Select whether to use CRC4 or not.
PRI Dial Plan	This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is “unknown”. In some very unusual circumstances, you may need set to “Dynamic” or “Redundant”. <p>Note: When one type is selected, you might not be able to dial another class of numbers. For example, if “National” is configured, you won’t be able to dial local or international numbers.</p>
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
D-Chan	Indicates the D channel for control.
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. <ul style="list-style-type: none"> • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.
Reset Interval	The interval that restarts idle channels.



PRI Exclusive	This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.
Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.
Overlap Dial	Configure this option to send overlap digits. If enabled, SETUP message can include some digits of callee number, and rest of the digits can be sent using INFORMATION message. If disabled, callee number will be sent via SETUP message when all the digits are ready.
NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom".

Table 54: Digital Hardware Configuration Parameters: E1 - SS7

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	<p>Originating point code is used to identify the node originating the message, always provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	<p>Destination point code is the address to send the message to, always be provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	<p>When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353].</p> <p>When Span Type is T1/J1, ITU & CHINA Range: [0, 4072], ANSI Range: [0, 16360].</p>
Assign CIC To D-channel	If set to yes, D-channel will be assigned a CIC. Else, D-channel will not be assigned. By default, it is set to No.



Network Indicator	Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, alaw will be used for E1.
Advanced Settings	
Coding	Select "HDB3" or "AMI".
CRC	Select whether to use CRC4 or not.
Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
D-Chan	Indicates the D channel for control
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Table 55: Digital Hardware Configuration Parameters: E1 - MFC/R2

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.



Variant	MFC/R2 multinational adaption. UCM6510 supports MFC/R2 standards by ITU and MFC/R2 standards in different countries or regions including Argentina, Brazil, China, Czech Republic, Colombia, Ecuador, Indonesia, Mexico, the Philippines and Venezuela.
Get ANI First	If enabled, the callee side will request the caller to send caller number first and then called number. Note: Options "Get ANI First" and "Skip Category" cannot be enabled at the same time.
Category	Select the category of the caller. UCM6510 supports four categories: National Subscriber, National Priority Subscriber, International Subscriber and International Priority Subscriber.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Advanced Settings	
Coding	Select "HDB3" or "AMI".
CRC	Select whether to use CRC4 or not.
MF Back Timeout (ms)	MFC/R2 value in milliseconds for MF timeout. Values smaller than 500ms are not recommended. -1 represents default value.
Metering Pulse Timeout (ms)	MFC/R2 value in milliseconds for the metering pulse timeout. Metering pulse is sent by some telcos for some R2 variants during a call presumably for billing purposes to indicate costs. Should not last more than 500ms, -1 represents default value, and for Argentina the default value is 400ms, for others is 0ms.
Allow Collect Calls	Brazil has a special calling party category for collect calls (llamadas por cobrar) instead of using the operator (as in Mexico). The R2 spec in Brazil says a special GB tone should be used to reject collect calls. By default, this is disabled, which means collect calls will be blocked.
Double Answer	Some PBXs require a double-answer process to block collect calls. If users have problem blocking collect calls using Group B signals, please try enabling this option.



Accept On Offer	By default, it's enabled. In most of cases, this option should be enabled.
Skip Category	If enabled, the callee side will request the caller to send caller category before sending caller number. Note: "Get ANI First" and "Skip Category" cannot be enabled at the same time.
Charge Calls	Whether or not report to the other end "accept call with charge". This setting has no effect with most telecoms. The default setting is enabled (recommended).
Custom Options	Click on "Custom Options" button (on the right top of the configuration dialog) and then user can customize desired tone and timer options accordingly.

Table 56: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.
Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Framing	Select "esf" or "d4". Default setting is esf.



Advanced Settings	
Switch Type	Select switch type. <ul style="list-style-type: none"> • EuroISDN: EuroISDN (common in Europe) • NI2: National ISDN type 2 (common in the US) • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
Coding	Select "B8ZS" or "AMI".
PRI Dial Plan	This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is "unknown". In some very unusual circumstances, you may need set to "Dynamic" or "Redundant". <p>Note:</p> When one type is selected, you might not be able to dial another class of numbers. For example, if "National" is configured, you won't be able to dial local or international numbers.
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
D-Chan	Indicates the D channel for control.
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. <ul style="list-style-type: none"> • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.
Reset Interval	The interval that restarts idle channels.
PRI Exclusive	This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.



Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.
Overlap Dial	Configure this option to send overlap digits. If enabled, SETUP message can include some digits of callee number, and rest of the digits can be sent using INFORMATION message. If disabled, callee number will be sent via SETUP message when all the digits are ready.
NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom", "accunet".

Table 57: Digital Hardware Configuration Parameters: T1/J1 - SS7

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	<p>Originating point code is used to identify the node originating the message, always provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	<p>Destination point code is the address to send the message to, always be provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	<p>When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353].</p> <p>When Span Type is T1/J1, ITU & CHINA Range: [0,4072], ANSI Range: [0, 16360].</p>
Assign CIC to D-Channel	If set to yes, D-channel will be assigned with a CIC. Else, D-channel will not be assigned with a CIC. By default, it is set to No.
Network Indicator	Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.



LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.
Framing	Select "esf" or "d4". Default setting is esf.
Advanced Settings	
Coding	Select "B8ZS" or "AMI".
Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
D-Chan	Indicates the D channel for control.
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Table 58: Digital Hardware Configuration Parameters: T1-E&M Immediate/E&M Wink

Basic Setting	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.



TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. The default codec is ulaw for T1.
Framing	Select "esf" or "d4". Default setting is esf.
Advanced Settings	
Coding	Select B8ZS or AMI. The default setting is B8ZS for T1.
OutgoingDialDelay	The option is only valid for E&M Wink signaling. The dial delay interval after received WINK event in an outgoing call. The default value is 200ms.
rxwink	Configure receive wink timing. The default setting is 300ms.

Digital Trunk Configuration

After configuring digital hardware, go to Web GUI→**Extension/Trunk**→**Digital Trunks**.

- Click on "Create New Digital Trunk" to add a new digital trunk.
- Click on  to configure detailed parameters for the digital trunk.
- Click on  to configure Direct Outward Dialing (DOD) for the digital Trunk.
- Click on  to delete the digital trunk.

The digital trunk parameters are listed in the table below.

Table 59: Digital Trunk Configuration Parameters

Trunk Name	Configure trunk name to identify the digital trunk.
Channel Group	Configure the digital channel group used by the trunk.
Hide CallerID	Configure to hide outgoing caller ID. The default setting is "No".
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Caller ID	<p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist:</p> <ul style="list-style-type: none"> • The CallerID configured for the extension will be looked up first. • If "Keep Trunk CID" is enabled, the CallerID configured for the trunk will be used.



	<ul style="list-style-type: none"> If the above two are missing, the "Global Outbound CID" defined in Web GUI→PBX Settings→General Settings will be used.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files are saved in external storage device if plugged in and can be accessed under Web GUI→ CDR → Recording Files .
Fax Detection	<p>Enable to detect Fax signal from the trunk during the call and send the received Fax to the default Email address in Fax setting page under Web GUI→Call Features→Fax/T.38.</p> <p>Note: If enabled, Fax Pass-through cannot be used.</p>

Direct Outward Dialing (DOD) via Digital Trunks

Please refer to section [\[Direct Outward Dialing \(DOD\) via VoIP Trunks\]](#).

Digital Trunk Troubleshooting

After configuring the digital trunk on the UCM6510 as described above, if it doesn't work as expected, users can go to capture signaling trace on the UCM6510 Web GUI for troubleshooting purpose.

Depending on the signaling selected for the digital trunk, users can go to the following pages to capture trace:

PRI Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**PRI Signaling Trace**

SS7 Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**SS7 Signaling Trace**

MFC/R2 Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**MFC/R2 Signaling Trace**

E&M Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**E&M Immediate Record Trace**

Here is the step to capture trace:

1. Click on "Start" to start capturing trace. The output result shows "Capturing..."
2. Once the test is done, click on "Stop" to stop the trace.
3. Click on "Download" to download the trace.



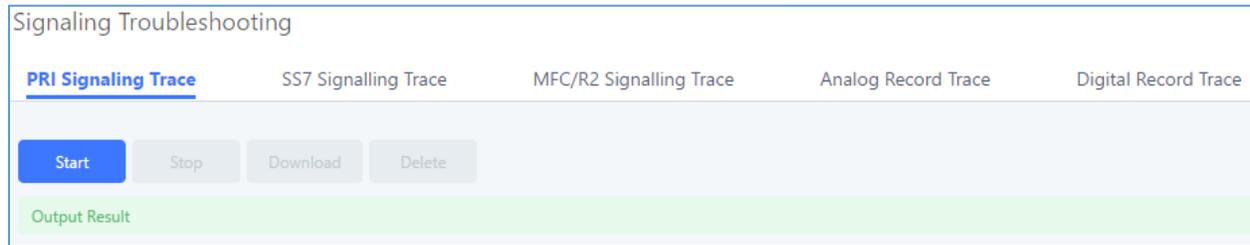


Figure 115: Troubleshooting Digital Trunks

For E&M Immediate Signaling, user could configure “Record Direction” and “Record File Mode”.

After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved.

<http://www.grandstream.com/support>



DATA TRUNK

The UCM6510 E1/T1/J1 interface also supports data trunk function that allows users to access Internet. Users can select HDLC, HDLC-ETH, Cisco and PPP protocol for the data trunk.

To use data trunk,

1. Go to Web GUI→**PBX Settings**→**Interface Settings**→**Digital Hardware** page and click  to create a new group. Designate a channel for data trunk usage in the group setting.
2. Go to Web GUI→**Extension/Trunk**→**Data Trunks** page, click on  to edit the data trunk.
3. Save the configuration and click on “Apply Changes” for the change to take effect.
4. Once connected, the data trunk will periodically ping and check the status, with status indicator shown for the data trunk on the web page. The status indicator shows  if connected successfully.
5. If the user happens to lose connection or experience unstable connection, click on  to reconnect to help resolve the problem.

Configure digital channels for data communication. If the line happens to have synchronization problems, please try reconnecting.				
Status	Enabled	Port	Encapsulation	Options
●	Turn Off	1	HDLC	 

Figure 116: Data Trunk Web Page

Data Trunk

Data Enable:

* Channel Group:

Encapsulation:

* Local IP:

* Subnet Mask:

* Remote IP:

* DNS Server 1:

DNS Server 2:

Default Interface:

Figure 117: Data Trunk Configuration



Table 60: Data Trunk Configuration Parameters

Data Enable	Select the checkbox to enable/disable data trunk. Users can also click on the ON/OFF switch in data trunk web page to enable/disable this.
Channel Group	Select the digital channel group from the dropdown list to be used for data trunk. Users will need create a new group under Web GUI→ PBX Settings → Interface Settings → Digital Hardware page for this purpose.
Encapsulation	Select the protocol used for the data trunk. The UCM6510 supports HDLC, HDLC-ETH, PPP, Cisco and Frame Relay.
Local IP	Configure the local IP address for the data port. This IP address shouldn't conflict with the WAN or LAN side IP of the UCM6510.
Subnet Mask	Configure the subnet mask for the data port.
Remote IP	Configure the remote IP address for the data port. This IP will be the gateway IP address if "Default Interface" is enabled for the data trunk.
DNS Server 1	Configure DNS server 1.
DNS Server 2	Configure DNS server 2.
Default Interface	If enabled, this data port will be used as the default interface for Internet connection. The "Remote IP" will be the gateway IP address. This has higher priority than the "Default Interface" assignment (LAN 1 or LAN 2) under Web GUI→ Settings if "Dual" is selected as the network method.



VOIP TRUNKS

VoIP Trunk Configuration

VoIP trunks can be configured in UCM6510 under Web GUI→**Extension/Trunk**→**VoIP Trunks**. Once created, the VoIP trunks will be listed with Provider Name, Type, Hostname/IP, Username and Options to edit/detect the trunk.

- Click on "Create New SIP Trunk" or "Create New IAX Trunk" to add a new VoIP trunk.
- Click on  to configure detailed parameters for the VoIP trunk.
- Click on  to configure Direct Outward Dialing (DOD) for the SIP Trunk.
- Click on  to start LDAP Sync.
- Click on  to delete the VoIP trunk.

For VoIP trunk example, please refer to the following document:

http://www.grandstream.com/sites/default/files/Resources/how_to_interconnect_multiple_ucm6510_using_peer_trunk.pdf

The VoIP trunk options are listed in the table below.

Table 61: Create New SIP Trunk

Type	Select the VoIP trunk type. <ul style="list-style-type: none"> • Peer SIP Trunk • Register SIP Trunk
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this setting when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall.



Disable This Trunk	<p>If checked, the trunk will be disabled.</p> <p>Note: If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.</p>
TEL URI	<p>If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.</p>
Caller ID	<p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist:</p> <ul style="list-style-type: none"> • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI→PBX→Internal Options→General will be used.
Need Registration	<p>Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.</p>
Username	<p>Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.</p>
Password	<p>Enter the password to register to the trunk from the provider when "Register SIP Trunk" is selected.</p>
Auth ID	<p>Enter the Authentication ID for "Register SIP Trunk" type.</p>
Auto Record	<p>Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.</p>

Table 62: SIP Register Trunk Configuration Parameters

Basic Settings	
Provider Name	<p>Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.</p>
Host Name	<p>Configure the IP address or URL for the VoIP provider's server of the trunk.</p>
Transport	<p>Configure the SIP transport protocol to be used in this trunk. The default setting is "All - UDP Primary".</p> <ul style="list-style-type: none"> • UDP Only • TCP Only



	<ul style="list-style-type: none"> • TLS Only • All - UDP Primary: UDP is the primary transport protocol when all the other SIP transport methods are available too. • All - TCP Primary: TCP is the primary transport protocol when all the other SIP transport methods are available too. • All – TLS Primary: TLS is the primary transport protocol when all the other SIP transport methods are available too.
Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override “Keep Trunk CID” option. Please make sure that the peer PBX at the other side supports to match user entry using “username” field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension’s CID when the extension has CID configured. The default setting is “No”.
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it’s related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	<p>If selected, the trunk will be disabled.</p> <p>Note: If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.</p>
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.
Allow outgoing calls if registration failure	<p>If enabled outgoing calls even if the registration to this trunk fail will still be able to go through.</p> <p>Note that if we uncheck “Need Registration” option, this option will be ignored.</p>
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
From Domain	<p>Configure the actual domain name where the extension comes from. This can be used to override the “From” Header.</p> <p>For example, "trunk.UCM6510.provider.com" is the From Domain in From Header: sip:1234567@trunk.UCM6510.provider.com.</p>



From User	<p>Configure the actual user name of the extension. This can be used to override the "From" Header. There are cases where there is a single ID for registration (single trunk) with multiple DIDs.</p> <p>For example, "1234567" is the From User in From Header: sip:1234567@trunk.UCM6510.provider.com.</p>
Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for "Register SIP Trunk" type.
Auth Trunk	If enabled, the UCM will send 401 response to the incoming call to authenticate the trunk.
Auto Record	<p>Enable automatic recording for the calls using this trunk (for SIP trunk only).</p> <p>The default setting is disabled. The recording files can be accessed under Web GUI→CDR→Recording Files.</p>
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
Send PPI Header	<p>If enabled, the SIP INVITE message sent to the trunk will contain PPI (P-Preferred-Identity) header. The default setting is "No".</p> <p>Note: "Send PPI Header" and "Send PAI Header" cannot be enabled at the same time. Only one of the two headers are allowed to be contained in the SIP INVITE message.</p>
Use DOD in PPI	<p>If enabled, the SIP INVITE message sent to the trunk will contain PAI (P-Asserted-Identity) header.</p> <p>The PPI header will include the configured DOD for this extension.</p> <p>Note: "Send PPI Header" needs to be enabled in order to use this feature.</p>
Send PAI Header	<p>If enabled, the SIP INVITE message sent to the trunk will contain PAI (P-Asserted-Identity) header including configured PAI Header. The default setting is "No".</p> <p>Note: "Send PPI Header" and "Send PAI Header" cannot be enabled at the same time. Only one of the two headers are allowed to be contained in the SIP INVITE message.</p>



PAI Header	<p>If “Send PAI Header” is enabled and “PAI Header” is configured as “123456” for instance, the PAI header in the SIP message sent from the UCM will contain “123456”. If “Send PAI Header” is enabled and “PAI Header” is configured as “empty”, the PAI header in the SIP message sent from the UCM will contain the original CID.</p> <p>Note: “Send PAI Header” needs to be enabled in order to use this feature</p>
Outbound Proxy Support	Select to enable outbound proxy in this trunk. The default setting is "No".
Outbound Proxy	When outbound proxy support is enabled, enter the IP address or URL of the outbound proxy.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	<p>Configure the default DTMF mode when sending DTMF on this trunk.</p> <ul style="list-style-type: none"> • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under Web GUI→PBX Settings→SIP Settings→ToS. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64-bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband will be used.
Enable Heartbeat Detection	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
Fax Mode	<p>Select Fax mode. The default setting is “None”.</p> <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".



CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. This number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

Table 63: SIP Peer Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "All - UDP Primary". <ul style="list-style-type: none"> • UDP Only • TCP Only • TLS Only • All - UDP Primary: UDP is the primary transport protocol when all the other SIP transport methods are available too. • All - TCP Primary: TCP is the primary transport protocol when all the other SIP transport methods are available too. • All – TLS Primary: TLS is the primary transport protocol when all the other SIP transport methods are available too.
Keep Original CID	Keep the CID from the inbound call when dialing out, this setting will override "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it's related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.



TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Caller ID	<p>Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.</p> <p>When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist:</p> <ul style="list-style-type: none"> • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI→PBX Settings→General Settings will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under Web GUI→ CDR → Recording Files .
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	<p>Configure the default DTMF mode when sending DTMF on this trunk.</p> <ul style="list-style-type: none"> • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under Web GUI→PBX Settings→SIP Settings→ToS. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64 bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband will be used.



Enable Heartbeat Detection	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
Fax Mode	Select Fax mode. The default setting is "None". <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
Sync LDAP Enable	If enabled, the local UCM6510 will automatically provide and update the local LDAP contacts to the remote UCM6510 SIP peer trunk. In order to ensure successful synchronization, the remote UCM6510 peer also needs to enable this option on the SIP peer trunk. The default setting is "No".
Sync LDAP Password	This is the password used for LDAP contact file encryption and decryption during the LDAP sync process. The password must be the same on both UCM6510 peers to ensure successful synchronization.
Sync LDAP Port	Configure TCP port used LDAP sync feature between two peer UCM6510.
LDAP Outbound Rule	Specify an outbound rule for LDAP sync feature. UCM6510 will automatically modify the remote contacts by adding prefix parsed from this rule.
LDAP Dialed Prefix	Specify the prefix for LDAP sync feature. The UCM6510 will automatically modify the remote contacts by adding this prefix.
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. Min. value is 1.



Table 64: Create New IAX Trunk

Type	Select the VoIP trunk type. <ul style="list-style-type: none"> Peer IAX Trunk Register IAX Trunk
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Username	Enter the username to register to the trunk from the provider when "Register IAX Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register IAX Trunk" type is selected.
Disable This Trunk	If selected, the trunk will be disabled.

Table 65: IAX Register Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: <ul style="list-style-type: none"> The CallerID configured for the extension will be looked up first. If no CallerID configured for the extension, the CallerID configured for the trunk will be used. If the above two are missing, the "Global Outbound CID" defined in Web GUI→PBX→Internal Options→General will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Username	Enter the username to register to the trunk from the provider.
Password	Enter the password to register to the trunk from the provider.



Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
Enable Heartbeat Detection	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limited.
Fax Mode	Select Fax mode. The default setting is "None". <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.

Table 66: IAX Peer Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: <ul style="list-style-type: none"> • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI→PBX Settings→General Settings will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.



Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
Enable Heartbeat Detection	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limited.
Fax Mode	Select Fax mode. The default setting is "None". <ul style="list-style-type: none"> • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under Web GUI→Call Features→Fax/T.38.

Direct Outward Dialing (DOD) via VoIP Trunks

The UCM6510 provides Direct Outward Dialing (DOD) which is a service of a local phone company (or local exchange carrier) that allows subscribers within a company's PBX system to connect to outside lines directly.

Example of how DOD is used:

Company ABC has a SIP trunk. This SIP trunk has 4 DID's associated to it. The main number of the office is routed to an auto attendant. The other three numbers are direct lines to specific users of the company. At the moment when a user makes an outbound call their caller ID shows up as the main office number. This poses a problem as the CEO would like their calls to come from their direct line. This can be accomplished by configuring DOD for the CEO's extension.

Steps on how to configure DOD on the UCM:

1. To setup DOD go to UCM6510 Web GUI→**Extension/Trunk**→**VoIP Trunks** page.
2. Click  to access the DOD options for the selected SIP Trunk.
3. Click "Create a new DOD" to begin your DOD setup.



4. For "DOD Number" enter one of the numbers (DIDs) from your SIP trunk provider. In the example above Company ABC received 4 DIDs from their provider. ABC will enter the number for the CEO's direct line.
5. If extension number need to be appended to the DID number click on "Add Extension".
6. Select an extension from the "Available Extensions" list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO's extension. After making the selection, click on the  button to move the extension(s) to the "Selected Extensions" list.

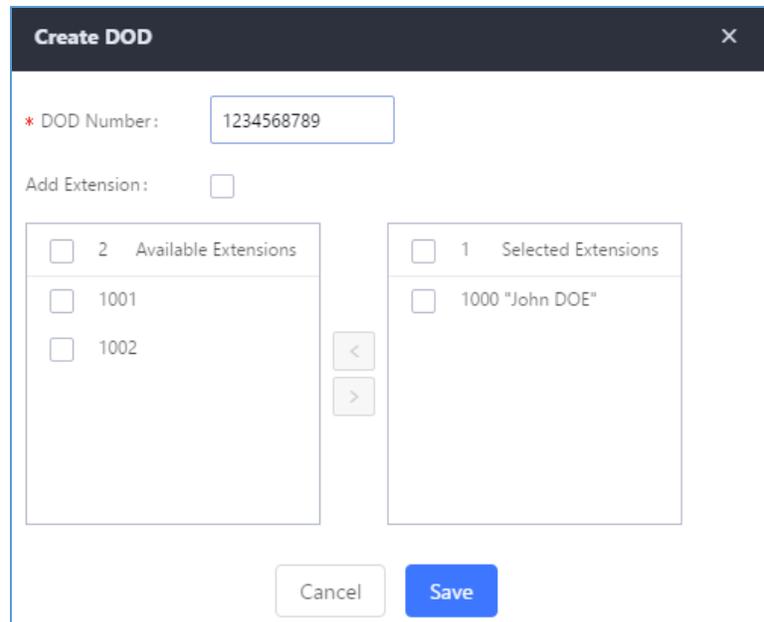
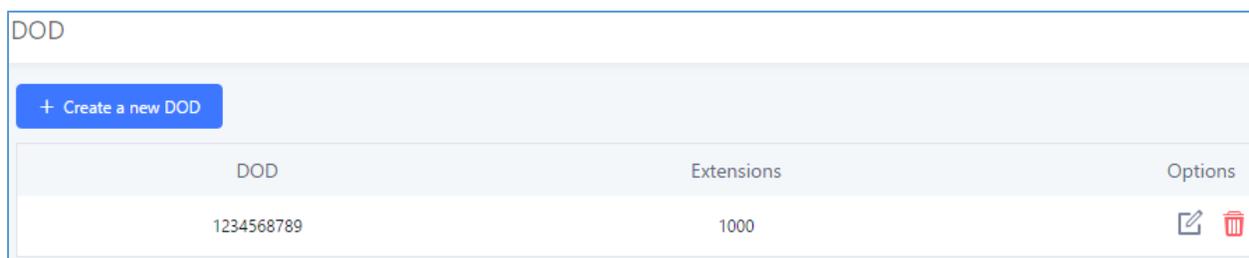


Figure 118: DOD extension selection

7. Click "Save" at the bottom.

Once completed, the user will return to the **Edit DOD** page that shows all the extensions that are associated to a particular DOD.



DOD	Extensions	Options
1234568789	1000	 

Figure 119: Edit DOD

SLA STATION

UCM6510 supports SLA that allows mapping the key with LED on a multi-line phone to different external lines. When there is an incoming call and the phone starts to ring, the LED on the key will flash in red and the call can be picked up by pressing this key. This allows users to know if the line is occupied or not. The SLA function on the UCM6510 is similar to BLF but SLA is used to monitor external line i.e., analog trunk on the UCM6510. Users could configure the phone with BLF mode on the MPK to monitor the analog trunk status or press the line key pick up call from the analog trunk on the UCM6510.

Create/Edit SLA Station

SLA Station can be configured on Web GUI → **Extension/Trunk** → **SLA Station**.

SLA Station				
<div style="display: flex; justify-content: space-between;"> + Add Delete </div>				
<input type="checkbox"/>	Station Name ↕	Station ↕	Associated SLA Trunks ↕	Options
<input type="checkbox"/>	FX01	1000	Telco1	 

Figure 120: SLA Station

- Click on “Create New SLA Station” to add a SLA Station.
- Click on  to edit the SLA Station. The following table shows the SLA Station parameters.
- Click on  to delete the SLA Station.

Table 67: SLA Station Configuration Parameters

	Configure a name to identify the SLA Station.
Station	Specify a SIP extension as a station that will be using SLA.
Available SLA Trunks	Existing Analog Trunks with SLA Mode enabled will be listed here.
Selected SLA Trunks	Select a trunk for this SLA from the Available SLA Trunks list. Click on     to arrange the order. If there are multiple trunks selected, when there are calls on those trunks at the same time, pressing the LINE key on the phone will pick up the call on the first trunk here.
SLA Station Options	
Ring Timeout	Configure the time (in seconds) to ring the station before the call is considered unanswered. No timeout is set by default. If set to 0, there will be no timeout.



Ring Delay	Configure the time (in seconds) for delay before ringing the station when a call first coming in on the shared line. No delay is set by default. If set to 0, there will be no delay.
Hold Access	This option defines the competence of the hold action for one particular trunk. If set to “open”, any station could hold a call on that trunk or resume one held session; if set to “private”, only the station that places the trunk call on hold could resume the session. The default setting is “open”.

Sample Configuration

1. On the UCM6510, go to Web GUI→**Extension/Trunk**→**Analog Trunks** page. Create analog trunk or edit the existing analog trunk. Make sure “SLA Mode” is enabled for the analog trunk. Once enabled, this analog trunk will be only available for the SLA stations created under Web GUI→**Extension/Trunk**→**SLA Station** page.

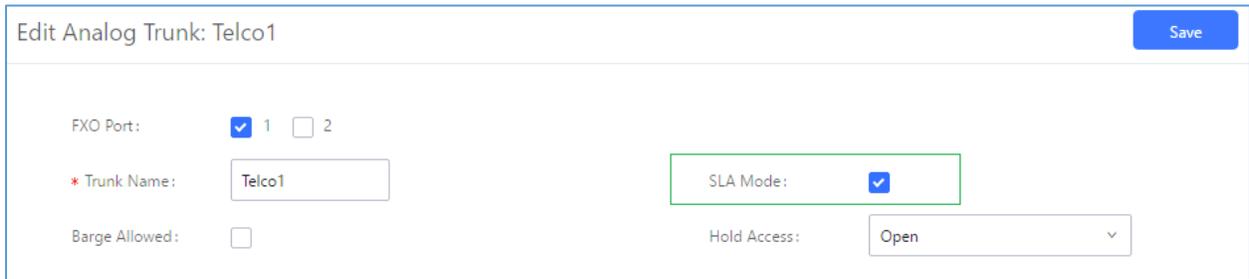
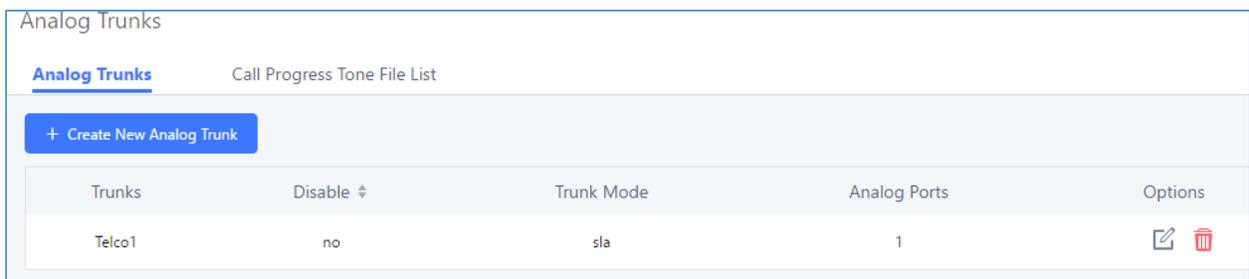


Figure 121: Enable SLA Mode for Analog Trunk

Click on “Save”. The analog trunk will be listed with trunk mode “SLA”.



Analog Trunks				
Analog Trunks		Call Progress Tone File List		
+ Create New Analog Trunk				
Trunks	Disable	Trunk Mode	Analog Ports	Options
Telco1	no	sla	1	 

Figure 122: Analog Trunk with SLA Mode Enabled

2. On the UCM6510, go to Web GUI→**Extension/Trunk**→**SLA Station** page, click on “Create New SLA Station”. Please refer to section [\[Create/Edit SLA Station\]](#) for the configuration parameters. Users can create one or more SLA stations to monitor the analog trunk. The following figure shows two stations, 1002 and 1005, are configured to be associated with SLA trunk “fxo1”.



<input type="checkbox"/>	Station Name ↕	Station ↕	Associated SLA Trunks ↕	Options
<input type="checkbox"/>	SLA1	1005	Telco1	 

Figure 123: SLA Example - SLA Station

- On the SIP phone 1, configure to register UCM6510 extension 1002. Configure the MPK as BLF mode and the value must be set to “extension_trunkname”, which is 1002_fxo1 in this case.
- On the SIP phone 2, configure to register UCM6510 extension 1005. Configure the MPK as BLF mode and value must be set to “extension_trunkname”, which is 1005_fxo1 in this case.

	Mode	Account	Description	Value
MPK 1	Busy Lamp Field (BLF) ▼	Account 2 ▼	1005_fxo1	1005_fxo1

Figure 124: SLA Example - MPK Configuration

Now the SLA station is ready to use. The following functions can be achieved by this configuration.

- **Making an outbound call from the station/extension, using LINE key**
 When the extension is in idle state, pressing the line key for this extension on the phone to off hook. Then dial the station’s extension number, for example, dial 1002 on phone 1 (or dial 1005 on phone 2), to hear the dial tone. Then the users could dial external number for the outbound call.
- **Making an outbound call from the station/extension, using BLF key**
 When the extension is in idle state, pressing the MPK and users could dial external numbers directly.
- **Answering call using LINE key**
 When the station is ringing, pressing the LINE key to answer the incoming call.
- **Barging-in active call using BLF key**
 When there is an active call between an SLA station and an external number using the SLA trunk, other SLA stations monitoring the same trunk could join the call by pressing the BLF key if “Barge Allowed” is enabled for the analog trunk.
- **Hold/UnHold using BLF key**
 If the external line is previously put on hold by an SLA station, another station that monitors the same SLA trunk could UnHold the call by pressing the BLF key if “Hold Access” is set to “open” on the analog trunk and the SLA station.



CALL ROUTES

Outbound Routes

Configuring Outbound Routes

In the UCM6510, an outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g., "Local" 7-digit dials through a FXO while "Long distance" 10-digit dials through a low-cost SIP trunk). Users can also set up a failover trunk to be used when the primary trunk fails.

Go to Web GUI→**Extension/Trunk**→**Outbound Routes** to add and edit outbound rules.

- Click on "Create New Outbound Rule" to add a new outbound route.
- Click on  to edit the outbound route.
- Click on  to delete the outbound route.
- On the UCM6510, the outbound route priority is based on "Best matching pattern". For example, the UCM6510 has outbound route A with pattern 1xxx and outbound route B with pattern 10xx configured. When dialing 1000 for outbound call, outbound route B will always be used first. This is because pattern 10xx is a better match than pattern 1xxx. Only when there are multiple outbound routes with the same pattern configured, users can click on     to move the outbound route up/down to arrange the priority among those outbound routes.

Table 68: Outbound Route Configuration Parameters

Calling Rule Name	Configure the name of the calling rule (e.g., local, long_distance, and etc). Letters, digits, _ and - are allowed.
Pattern	<ul style="list-style-type: none"> • All patterns are prefixed with the "_". • Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9. <p>Notes:</p> <ul style="list-style-type: none"> ▪ Multiple patterns can be used. Each pattern should be entered in new line.



	<ul style="list-style-type: none"> Users can add comments to a dial plan by typing “/*” and “*/” before and after each comment respectively. <u>Example:</u> _X. _NNXXNXXXXX /* 10-digit long distance */ _818X. /* Any number with leading 818 */
Disable This Route	After creating the outbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in UCM. Users can enable it again when it’s needed.
Password	Configure the password for users to use this rule when making outbound calls.
Call Duration Limit	Once call duration limit is enabled, it will set the maximum duration of call-blocking.
Maximum Call Duration	User can customize the maximum call duration (in seconds) that is allowed for the outbound call. By default, this value is set to 0 means there is no limit for the call duration.
Warning Time	This option will give caller warning when call duration is approaching to its limit. If the warning time is set to ‘y’, the warning tone will be played to caller when y seconds is left to end the call by UCM.
Warning Repeat Interval	Once this option is set to ‘z’, it will repeatedly be warning caller every z seconds after the first warning.
PIN Groups	If selected, the Password, Privilege Level and Enable Filter on Source Caller ID will not take effect.
Password	Configure the password for users to use this rule when making outbound calls.
Privilege Level	<p>Select privilege level for the outbound rule.</p> <ul style="list-style-type: none"> Internal: The lowest level required. All users can use this rule. Local: Users with Local, National, or International level are allowed to use this rule. National: Users with National or International level are allowed to use this rule. International: The highest level required. Only users with international level can use this rule. <p>The default setting is "Disable".</p> <p>Please be aware of the potential security risks when using "Internal" level, which means all users can use this outbound rule to dial out from the trunk.</p>



Enable Filter on Source Caller ID	<p>When enabled, users could specify extensions allowed to use this outbound route. "Privilege Level" is automatically disabled if using "Enable Filter on Source Caller ID".</p> <p>The following two methods can be used at the same time to define the extensions as the source caller ID.</p> <ol style="list-style-type: none"> 1. Select available extensions/extension groups from the left to the right. This allows users to specify arbitrary single extensions available in the PBX. 2. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one. <ul style="list-style-type: none"> • All patterns are prefixed with the "_". • Special characters: <ul style="list-style-type: none"> X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. .": Wildcard. Match one or more characters. "!: Wildcard. Match zero or more characters immediately. <p>Example: [12345-9] - Any digit from 1 to 9.</p> <p><u>Note</u>: Multiple patterns can be used. Patterns should be separated by comma ",". Example: _X. , _NNXXNXXXXX , _818X.</p>
Send This Call Through Trunk	
Use Trunk	Select the trunk for this outbound rule.
Strip	<p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p><u>Example</u>:</p> <p>The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.</p>
Prepend	<p>Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.</p>
Use Failover Trunk	
Failover Trunk	<p>Failover trunks can be used to make sure that a call goes through an alternate route, when the primary trunk is busy or down. If "Use Failover Trunk" is enabled and "Failover trunk" is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through. UCM6510 support up to 10 failover trunks.</p> <p><u>Example</u>:</p> <p>The user's primary trunk is a VoIP trunk and the user would like to use the PSTN when the VoIP trunk is not available. The PSTN trunk can be</p>



	configured as the failover trunk of the VoIP trunk.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. <u>Example:</u> The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Time Condition	
Time Condition	Users could customize holiday time, office time or a specified time to allow the outbound route to be used.

Outbound Blacklist

The UCM6510 allows users to configure blacklist for outbound routes. If the dialing number matches the blacklist numbers or patterns, the outbound call will not be allowed. The outbound blacklist can be configured under UCM Web GUI → **Extension/Trunk** → **Outbound Routes**: Outbound Blacklist.

Users can configure number, pattern or select country code to add in the blacklist. Please note that the blacklist settings apply to all outbound routes.

PIN Groups

The UCM6510 supports pin group. Once this feature is configured, users can apply pin group to specific outbound routes. When placing a call on pin protected outbound routes, caller will be asked to input the group pin number, this feature can be found on the webGUI → **Extension/Trunk** → **Outbound Routes** → **PIN Groups**.

Table 69: Outbound Routes/PIN Group

Name	Specify the name of the group
Record In CDR	Specify whether to enable/disable record in CDR
PIN Number	Specify the code that will asked once dialing via a trunk
PIN Name	Specify the name of the PIN

Once user click on [PIN Groups](#) the following figure shows to configure the new PIN.



Create New PIN Group
Save

* Name:

Record in CDR:

Members

* PIN Number:

* PIN Name:

✓ Save
✗ Cancel

PIN Number: 2020 PIN Name: John
✎ ✖

Figure 125: Create New PIN Group

The following screenshot shows an example of created PIN Groups and members:

PIN Groups

+ Add
Choose file to upload

	Name	Record in CDR	Options
-	GSEMEA	yes	✎ ✖

	PIN Number	PIN Name
	2020	John
	2025	Emily
	3009	Jane

Figure 126: PIN members

Note:

If PIN group is enabled on outbound route level, password, privilege level and enable filter on source caller ID will be disabled.



Edit Outbound Rule: National Save

* Calling Rule Name:

Disable This Route:

Password:

* Pattern:

PIN Groups:

Privilege Level:

Figure 127: Outbound PIN

If pin group CDR is enabled, the call with PIN group information will be displayed as part of CDR under Account Code field.

CDR

Delete All
 Download All Records
 Download Search Result (s)
 Automatic Download Settings

Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code
+	1002	7946541 [Trunk: BranchOffice]	DIAL	2017-05-05 04:59:51	0:00:08	Emily/GSEMEA
+	1002	7654654 [Trunk: BranchOffice]	DIAL	2017-05-05 04:59:12	0:00:06	Jane/GSEMEA
+	1002	7564654 [Trunk: BranchOffice]	DIAL	2017-05-05 04:58:38	0:00:06	John/GSEMEA

Figure 128: CDR Record



Outbound blacklist
Cancel

The blacklist (based on CalleID) is used for all outbound routes.

Country Codes:

- North America
- South America
- Europe
- Asia and the Middle East
- Africa
- Australia

North America

- United States 1201 1202 1203 1205 10+
- Canada 1204 1226 1236 1249 10+
- Anguilla 1264
- Antigua and Barbuda 1268
- Bahamas 1242
- Barbados 1246
- Bermuda 1441

Blacklist Manage

* Add Blacklist Rule: +

Blacklist list:

Continent	Country	Blacklist Rule	Options
Custom	Custom	412354	
Custom	Custom	698xxx	

Figure 129: Country Codes

Inbound Routes

Inbound routes can be configured via Web GUI→**Extension/Trunk**→**Inbound Routes**.

- Click on "Create New Inbound Rule" button to add a new inbound route.
- Click on "Blacklist" button to configure blacklist for all inbound routes.
- Click on to edit the inbound route.
- Click on to delete the inbound route.

Inbound Rule Configurations

Table 70: Inbound Rule Configuration Parameters

Trunks

Select the trunk to configure the inbound rule.



Pattern	<ul style="list-style-type: none"> All patterns are prefixed with the "_". Special characters: <ul style="list-style-type: none"> X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9. The pattern can be composed of two parts, <i>Pattern</i> and <i>CallerID Pattern</i>. The first part is used to specify the dialed number while the second part is used to specify the caller ID and it is optional, if set it means only the extension with the specific caller ID can call in or call out. For example, pattern '_2XXX/1234' means the only extension with the caller ID '1234' can use this rule. <p><u>Notes:</u></p> <ul style="list-style-type: none"> Multiple patterns can be used. Each pattern should be entered in new line. Users can add comments to a dial plan by typing <i>"/*</i> and <i>*/</i> before and after each comment respectively. Example: <table border="1" data-bbox="618 1024 1417 1205"> <thead> <tr> <th>Pattern</th> <th>CallerID Pattern</th> </tr> </thead> <tbody> <tr> <td>_X.</td> <td>1000</td> </tr> <tr> <td>_NNXXNXXXXX /* 10-digit long distance */</td> <td>1001</td> </tr> <tr> <td>_818X. /* Any number with leading 818 */</td> <td></td> </tr> </tbody> </table>	Pattern	CallerID Pattern	_X.	1000	_NNXXNXXXXX /* 10-digit long distance */	1001	_818X. /* Any number with leading 818 */	
Pattern	CallerID Pattern								
_X.	1000								
_NNXXNXXXXX /* 10-digit long distance */	1001								
_818X. /* Any number with leading 818 */									
Disable This Route	After creating the inbound route, users can choose to enable and disable it. If the route is disabled, it will not take effect anymore. However, the route settings will remain in UCM. Users can enable it again when it's needed.								
Prepend Trunk Name	If enabled, the trunk name will be added to the caller id name as the displayed caller id name.								
Prepend User Defined Name	Prepend a user defined name to display name.								
Alert-Info	Configure the Alert-Info, when UCM6510 receives an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.								
Inbound Multiple Mode	Multiple mode allows user to switch between destinations of the inbound rule by feature codes. Configure related feature codes in the "Feature Codes" page. If this option is enabled, user can use feature code to switch between different destinations.								
Dial Trunk	This option shows up only when "By DID" is selected. If enabled, the external users dialing in to the trunk via this inbound route can dial outbound call using the UCM6510's trunk.								



Privilege Level	<p>Disable: Only the selected Extensions or Extension Groups are allowed to use this rule, when enabled Filter on Source Caller ID.</p> <p>Internal: The lowest level required. All users are allowed to use this rule, check this level might be risky for security purpose.</p> <p>Local: User with Local level, National or International level are allowed to use this rule.</p> <p>National: Users with National or International Level are allowed to use this rule.</p> <p>International: The highest level required. Only users with international level are allowed to use this rule.</p>
DID Destination	<p>This option shows up only when "By DID" is selected. This controls the destination that can be reached by the external caller via the inbound route. The DID destination are:</p> <ul style="list-style-type: none"> • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Groups • IVR • Voicemail Groups • Fax Extension • Dial By Name • All
Default Destination	<p>Select the default destination for the inbound call.</p> <ul style="list-style-type: none"> • Extension • Voicemail • Conference Room • Call Queue • Ring Group • Paging/Intercom • Voicemail Group • Fax • DISA • IVR • External Number • By DID <p>When "By DID" is used, the UCM6510 will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, voicemail groups and Fax extension as configured in "DID destination". If the dialed number</p>



	<p>matches the DID pattern, the call will be allowed to go through.</p> <ul style="list-style-type: none"> • Dial By Name • Callback
Strip	Specify the number of digits to strip from the beginning of the DID. This is used when "By DID" is selected in "Default Destination".
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Dial Trunk	Configure to allow the inbound call to dial out from the PBX's trunk or not. The default setting is disabled. Please be aware of potential security risk if "Dial Trunk" is enabled. The inbound call might be able to dial out international calls from the PBX's trunk if allowed by the privilege level.
DID Destination	<p>Select the DID destination if "By DID" is selected in "Default Destination". Only the selected category can be reached by DID using this inbound route.</p> <ul style="list-style-type: none"> • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Group • IVR • Voicemail Groups • Fax Extension • Dial By Name • All
Time Condition	
Start Time	Select the start time "hour:minute" for the trunk to use the inbound rule.
End Time	Select the end time "hour:minute" for the trunk to use the inbound rule.
Date	Select "By Week" or "By Day" and specify the date for the trunk to use the inbound rule.
Week	Select the day in the week to use the inbound rule.
Destination	<p>Select the destination for the inbound call under the defined time condition.</p> <ul style="list-style-type: none"> • Extension • Voicemail • Conference Room • Call Queue • Ring Group • Paging/Intercom • Voicemail Group • Fax • DISA



- IVR
- By DID

When "By DID" is used, the UCM6510 will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, voicemail groups and Fax extension as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through. Configure the number of digits to be stripped in "Strip" option.
- Dial By Name
- External Number
- Callback

Inbound Route: Prepend Example

UCM6510 now allows user to prepend digits to an inbound DID pattern, with strip taking precedence over prepend. With the ability to prepend digits in inbound route DID pattern, user no longer needs to create multiple routes for the same trunk in order to route calls to different extensions.

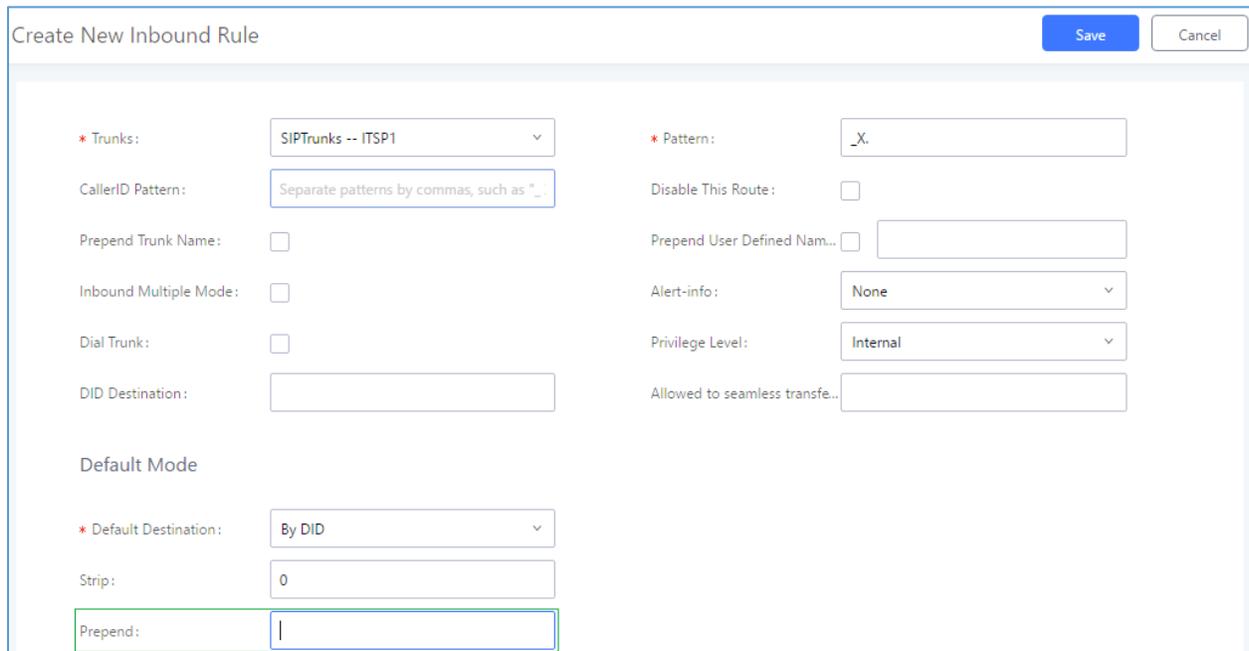


Figure 130: Inbound Route feature: Prepend

The following example demonstrates the process:

1. If Trunk provides a DID pattern of 18005251163.
2. If **Strip** is set to 8, UCM6510 will strip the first 8 digits.



3. If **Prepend** is set to 2, UCM6510 will then prepend a 2 to the stripped number, now the number become 2163.
4. UCM6510 will now forward the incoming call to extension 2163.

Inbound Route: Multiple Mode

In UCM6510, user can configure inbound route to enable multiple mode to switch between different destinations. The inbound multiple mode can be enabled under Inbound Route settings.

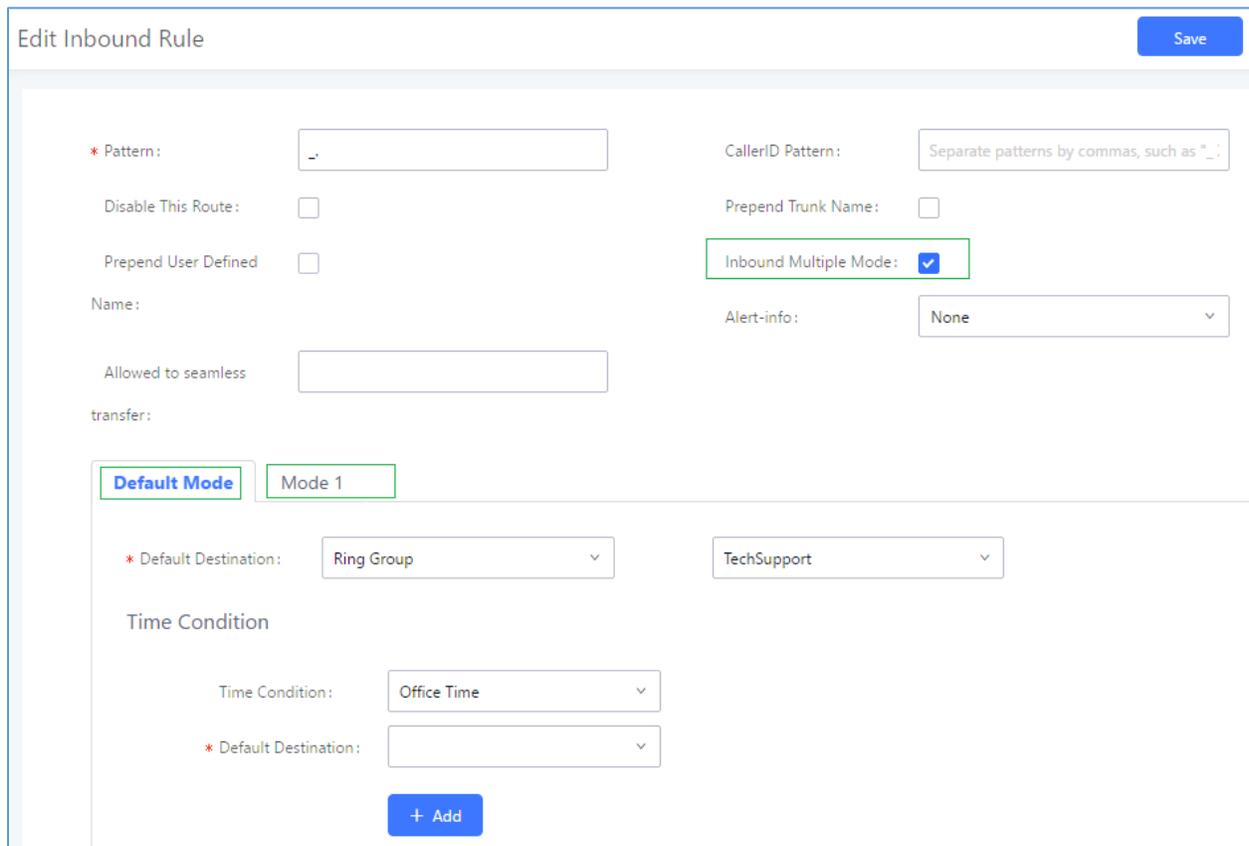


Figure 131: Inbound Route - Multiple Mode

When Multiple Mode is enabled for the inbound route, the user can configure a “Default Destination” and a “Mode 1” destination for this route. By default, the call coming into this inbound route will be routed to the default destination.

SIP end devices that have registered on the UCM6510 can dial feature code *62 to switch to inbound route “Mode 1” and dial feature code *61 to switch back to “Default Destination”. Switching between different mode can be easily done without Web GUI login.



For example, the customer service hotline destination has to be set to a different IVR after 7PM. The user can dial *62 to switch to "Mode 1" with that IVR set as the destination before off work.

Fax Intelligent Route

The UCM6510 can automatically detect Fax and phone signal coming from the FXO port, and then forward Fax or phone signal to the right destination. For example, when a regular phone call is coming, the UCM65100 will be able to detect the phone signal and forward it through the correct inbound route to the destination; if Fax signal is coming, the UCM6510 will be able to forward it to the FXS extension where the Fax machine is connected.

Fax with Two Media

UCM6510 with Asterisk 13 system now supports fax re-invite with multiple codec negotiation. If a fax re-invite contains both T.38 and PCMA/PCMU codec, UCM6510 will choose T.38 codec over PCMA/PCMU. Where in the old Asterisk 1.8 system, multiple codec in the re-invite is prohibited and will be dropped by UCM6510.

Blacklist Configurations

In the UCM6510, Blacklist is supported for all inbound routes. Users could enable the Blacklist feature and manage the Blacklist by clicking on "Blacklist".

- Select the checkbox for "Blacklist Enable" to turn on Blacklist feature for all inbound routes. Blacklist is disabled by default.
- Enter a number in "Add Blacklist Number" field and then click  to add to the list. Anonymous can also be added as a Blacklist Number.
- To remove a number from the Blacklist, select the number in "Blacklist list" and click on .



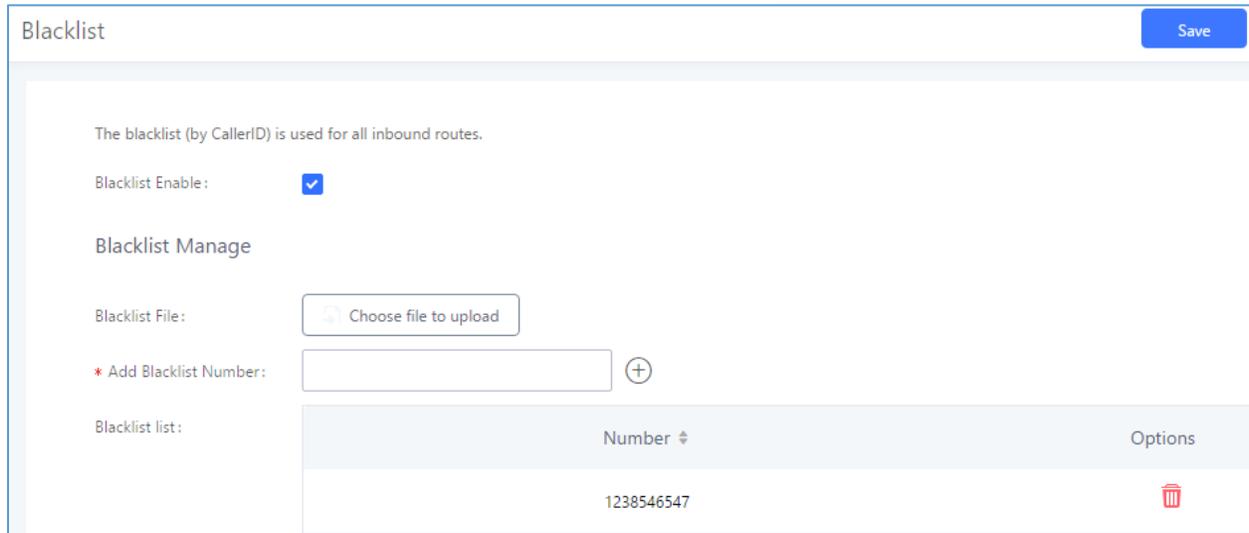


Figure 132: Blacklist Configuration Parameters

- To add blacklist number in batch, click on “Choose file to upload” to upload blacklist file in csv format. The supported csv format is as below.

	A	B	C	D	E
1	13238680006	12135958547	12136268547	6262357999	
2					
3					
4					
5					

Figure 133: Blacklist csv File

⚠ Note:

Users could also add a number to the Blacklist or remove a number from the Blacklist by dialing the feature code for "Blacklist Add" (default: *40) and "Blacklist Remove" (default: *41) from an extension. The feature code can be configured under Web GUI→**Call Features**→**Feature Codes**.



CONFERENCE BRIDGE

The UCM6510 supports Conference Bridge allowing 64 participants with up to 8 bridges at the same time. The conference bridge configurations can be accessed under Web GUI→**Call Features**→**Conference**. In this page, users could create, edit, view, invite, manage the participants and delete conference bridges. The conference bridge status and conference call recordings (if recording is enabled) will be displayed in this web page as well.

Conference Bridge Configurations

- Click on "Create New Conference Room" to add a new conference bridge.
- Click on  to edit the conference bridge.
- Click on  to delete the conference bridge.

Table 71: Conference Bridge Configuration Parameters

Extension	Configure the conference number for the users to dial into the conference.
Password	<p>When configured, the users who would like to join the conference call must enter this password before accessing the conference bridge.</p> <p>Note:</p> <ul style="list-style-type: none"> • If "Public Mode" is enabled, the password is not required to join the conference bridge thus this field is invalid. • The password has to be at least 4 characters.
Admin Password	<p>Configure the password to join the conference bridge as administrator. Conference administrator can manage the conference call via IVR (if "Enable Caller Menu" is enabled) as well as invite other parties to join the conference by dialing "0" (permission required from the invited party) or "1" (permission not required from the invited party) during the conference call.</p> <p>Note:</p> <ul style="list-style-type: none"> • If "Public Mode" is enabled, the password is not required to join the conference bridge thus this field is invalid. • The password has to be at least 4 characters.
Enable Caller Menu	If enabled, conference participant could press the * key to access the conference bridge menu. The default setting is "No".
Record Conference	If enabled, the calls in this conference bridge will be recorded automatically in a .wav format file. All the recording files will be displayed and can be downloaded in the conference web page. The default setting is "No".



Quiet Mode	<p>If enabled, if there are users joining or leaving the conference, voice prompt or notification tone won't be played. The default setting is "No".</p> <p>Note: "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.</p>
Wait For Admin	<p>If enabled, the participants will not hear each other until the conference administrator joins the conference. The default setting is "No".</p> <p>Note: If "Quiet Mode" is enabled, the voice prompt for "Wait For Admin" will not be announced.</p>
Enable User Invite	<p>If enabled, users could press 0 to invite other users (with the users' permission) or press 1 to invite other users (without the user's permission) to join the conference. The default setting is "No".</p> <p>Note: Conference administrator can always invite other users without enabling this option.</p>
Announce Callers	<p>If enabled, the caller will be announced to all conference participants when there the caller joins the conference. The default setting is "No".</p> <p>Note: "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.</p>
Public Mode	<p>If enabled, no authentication will be required when joining the conference call. The default setting is "Yes".</p>
Play Hold Music	<p>If enabled, the UCM6510 will play Hold music to the first participant in the conference until another user joins in. The default setting is "No".</p>
Music On Hold	<p>Select the music on hold class to be played in conference call. This option shows up if "Play Hold Music For First Caller" is enabled. Music On Hold class can be set up under Web GUI→PBX Settings→Music On Hold.</p>
Skip Authentication When Inviting User via Trunk from Web GUI	<p>If enabled, the invitation from Web GUI for a conference bridge with password will skip the authentication for the invited users. The default setting is "No".</p>

Conference Settings contains the following options:

Table 72: Conference Settings

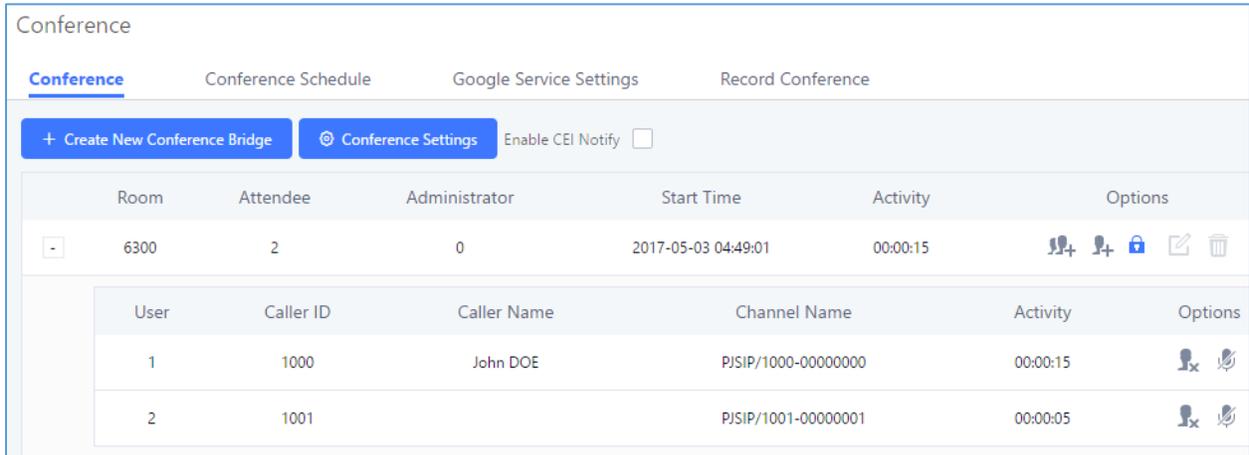
Enable Talk detection	<p>If enabled, the AMI will send the corresponding event when a user starts or ends talking.</p>
DSP Talking Threshold	<p>The time in milliseconds of sound above what the dsp has established as base line silence for a user before a user is considered to be talking. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 128.</p>



DSP Silence Threshold

The time in milliseconds of sound falling within the what the dsp has established as base line silence before a user is considered to be silent. This value affects several operations and should not be changed unless the impact on call quality is fully understood, the default value is 2500.

Users can check the talking Caller IDs in conference control page (UCM WebUI→**Call Features**→**Conference**). The image will move up and down when the user is talking.



Conference						
Conference						
+ Create New Conference Bridge @ Conference Settings <input type="checkbox"/> Enable CEI Notify						
Room	Attendee	Administrator	Start Time	Activity	Options	
6300	2	0	2017-05-03 04:49:01	00:00:15		
User	Caller ID	Caller Name	Channel Name	Activity	Options	
1	1000	John DOE	PJSIP/1000-00000000	00:00:15		
2	1001		PJSIP/1001-00000001	00:00:05		

Figure 134: Conference

Join a Conference Call

Users could dial the conference bridge extension to join the conference. If password is required, enter the password to join the conference as a normal user, or enter the admin password to join the conference as administrator.

Invite Other Parties to Join Conference

When using the UCM6510 conference bridge, there are two ways to invite other parties to join the conference.

- **Invite from Web GUI**

For each conference bridge in UCM6510 Web GUI→**Call Features**→**Conference**, there is an icon  for option "Invite a participant". Click on it and enter the number of the party you would like to invite. Then click on "Add". A call will be sent to this number to join it into the conference.

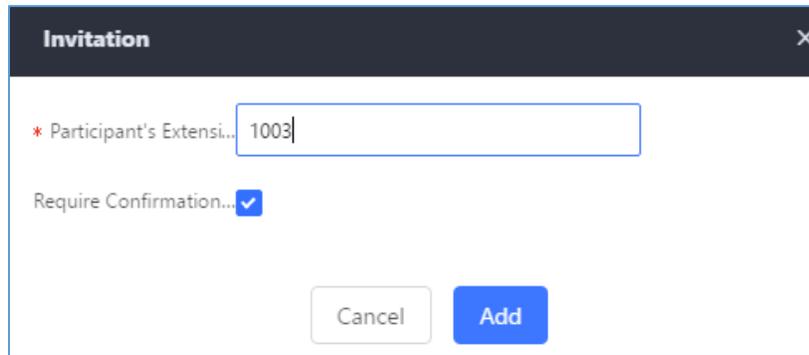


Figure 135: Conference Invitation From Web GUI

- **Invite by dialing 0 or 1 during conference call**

A conference participant can invite other parties to the conference by dialing from the phone during the conference call. Please make sure option "Enable User Invite" is turned on for the conference bridge first. Enter 0 or 1 during the conference call. Follow the voice prompt to input the number of the party you would like to invite. A call will be sent to this number to join it into the conference.

0: If 0 is entered to invite other party, once the invited party picks up the invitation call, a permission will be asked to "accept" or "reject" the invitation before joining the conference.

1: If 1 is entered to invite other party, no permission will be required from the invited party.

 **Note:**

Conference administrator can always invite other parties from the phone during the call by entering 0 or 1. To join a conference bridge as administrator, enter the admin password when joining the conference. A conference bridge can have multiple administrators.

During The Conference

During the conference call, users can manage the conference from Web GUI or IVR.

- **Manage the conference call from Web GUI.**

Log in UCM6510 Web GUI during the conference call, the participants in each conference bridge will be listed.

1. Click on  to kick a participant from the conference.
2. Click on  to mute the participant.
3. Click on  to lock this conference bridge so that other users cannot join it anymore.
4. Click on  to invite other users into the conference bridge.



- **Manage the conference call from IVR.**

If "Enable Caller Menu" is enabled, conference participant can input * to enter the IVR menu for the conference. Please see options listed in the table below.

Table 73: Conference Caller IVR Menu

Conference Administrator IVR Menu	
1	Mute/unmute yourself.
2	Lock/unlock the conference bridge.
3	Kick the last joined user from the conference.
4	Decrease the volume of the conference call.
6	Increase the volume of the conference call.
7	Decrease your volume.
9	Increase your volume.
8	More options: <ul style="list-style-type: none"> • 1: List all users currently in the conference call. • 2: Kick all non-Administrator participants from the conference call. • 3: Mute/Unmute all non-Administrator participants from the conference call. • 4: Enable/disable conference call recording. • 8: Exit the caller menu and return to the conference.
Conference User IVR Menu	
1	Mute/unmute yourself.
4	Decrease the volume of the conference call.
6	Increase the volume of the conference call.
7	Decrease your volume.
9	Increase your volume.
8	Exit the caller menu and return to the conference.



Note:

When there is participant in the conference, the conference bridge configuration cannot be modified.



Record Conference

The UCM6510 allows users to record the conference call and retrieve the recording from Web GUI→**Call Features**→**Conference**.

To record the conference call, when the conference bridge is in idle, enable "Record Conference" from the conference bridge configuration dialog. Save the setting and apply the change. When the conference call starts, the call will be automatically recorded in .wav format.

The recording files will be listed as below once available. Users could click on  to download the recording or click on  to delete the recording.

Conference					
Conference		Conference Schedule	Google Service Settings	<u>Record Conference</u>	
<input type="button" value="Delete Selected Recording Files"/> <input type="button" value="Delete All Recording Files"/> <input type="button" value="Batch Download Recording Files"/> <input type="button" value="Download All Recording Files"/>					
<input type="checkbox"/>	Name ↕	Room	Date	Size	Options
<input type="checkbox"/>	confbridge-6300-1493801742.wav	6300	2017-05-03 04:56:17 UTC-04:00	541.92 KB	 

Figure 136: Conference Recording

CONFERENCE SCHEDULE

Conference Schedule Configuration

Conference Schedule can be found under UCM6510 Web GUI→**Call Features**→**Conference Schedule**. Users can create, edit, view and delete a Conference Schedule.

- Click on “Create New Conference Schedule” to add a new Conference Schedule.
- Click on the scheduled conference to edit or delete the event.

After the user configures UCM6510 with Google Service Settings **[Google Service Settings Support]** and enables Google Calendar for Conference Schedule, the conference schedule on the UCM6510 can be synchronized with Google Calendar for authorized Google account.

Table 74: Conference Schedule Parameters

Schedule Options	
Conference Topic	Configure the name of the scheduled conference. Letters, digits, _ and - are allowed.
Conference Room	Select a conference room for this scheduled conference.
Kick Time(m)	Set kick time before conference starts. When kick time is reached, a warning prompt will be played for all attendees in the conference room. After 5 minutes, this conference room will be cleared and locked for the scheduled conference to begin. Note: Kick Time cannot be less than 6 minutes in order to clear the conference room.
Description	The description of scheduled conference.
Repeat	Repeat interval of scheduled conference. By default, set to single event.
Schedule Time	Configure the beginning date and duration of scheduled conference. Note: Please pay attention to avoid time conflict on schedules in the same conference room.
Enable Google Calendar	Select this option to sync scheduled conference with Google Calendar. Note: Google Service Setting OAuth2.0 must be configured on the UCM6510. Please refer to section [Google Service Settings Support] .



Conference Administrator	Select the administrator of scheduled conference from selected extensions. Note: “Public Mode” must be disabled from Conference Room Options tab.
Local Extension	Select available extensions from the list to attend scheduled conference.
Remote Extension	Select available extensions from the remote peer PBX. Note: “LDAP Sync” must be enabled on the UCM6510 in order to view remote extensions here.
Special Extension	Add extensions that are not in the list (both local and remote list). If the user wishes to add the special extension, please match the pattern on the outbound route.
Remote Conference	Invite a remote conference.
Conference Room Options	
Password	Configure conference room password. Please note that if “Public Mode” is enabled, this option is automatically disabled.
Admin Password	Configure the password to join as conference administrator. Please note that if “Public Mode” is enabled, this option is automatically disabled.
Enable Caller Menu	If this option is enabled, conference participants will be able to access conference bridge menu by pressing the * key.
Record Conference	If this option is enabled, conference call will be recorded in .wav format. The recorded file can be found from Conference page.
Quiet Mode	If this option is enabled, the notification tone or voice prompt for joining or leaving the conference won’t be played. Note: Option “Quiet Mode” and option “Announce Caller” cannot be enabled at the same time.
Wait For Admin	If this option is enabled, the participants in the conference won’t be able to hear each other until conference administrator joins the conference. Note: If “Quiet Mode” is enabled, voice prompt for this option won’t be played.
Enable User Invite	If this option is enabled, the user can: <ul style="list-style-type: none"> • Press ‘0’ to invite others to join the conference with invited party’s permission • Press ‘1’ to invite without invited party’s permission • Press ‘2’ to create a multi-conference bridge to another conference room • Press ‘3’ to drop all current multi-conference bridges Note: Conference Administrator is always allowed to access this menu.



Announce Callers	<p>If this option is enabled, when a participant joins the conference room, participant's name will be announced to all members in the conference room.</p> <p>Note: Option "Quiet Mode" and option "Announce Caller" cannot be enabled at the same time.</p>
Public Mode	<p>If this option is enabled, no authentication is required for entering the conference room.</p> <p>Note: Please be aware of the potential security risks when turning on this option.</p>
Play Hold Music	<p>If this option is enabled, UCM6510 will play Hold Music while there is only one participant in the conference room or the conference is not yet started.</p>
Skip Authentication When Inviting Users via Trunk from Web GUI	<p>If this option is enabled, the invitation from Web GUI via a trunk with password won't require authentication.</p> <p>Note: Please be aware of the potential security risks when turning on this option.</p>

- **Cleaner Options**

Cleaner Options	
Enable Conference Schedules Cleaner	If this option is enabled, conference schedules will be automatically cleaned as configured.
Conference Schedules Clean Time	Enter the clean time (in hours). The valid range is from 0 to 23.
Clean Interval	Enter the clean interval (in days). The valid range is from 1 to 30.

- **Show/hide Conference Schedule Table**

Enable this option will allow Web GUI to display scheduled conference in Conference Schedule Table. Please see figure below.



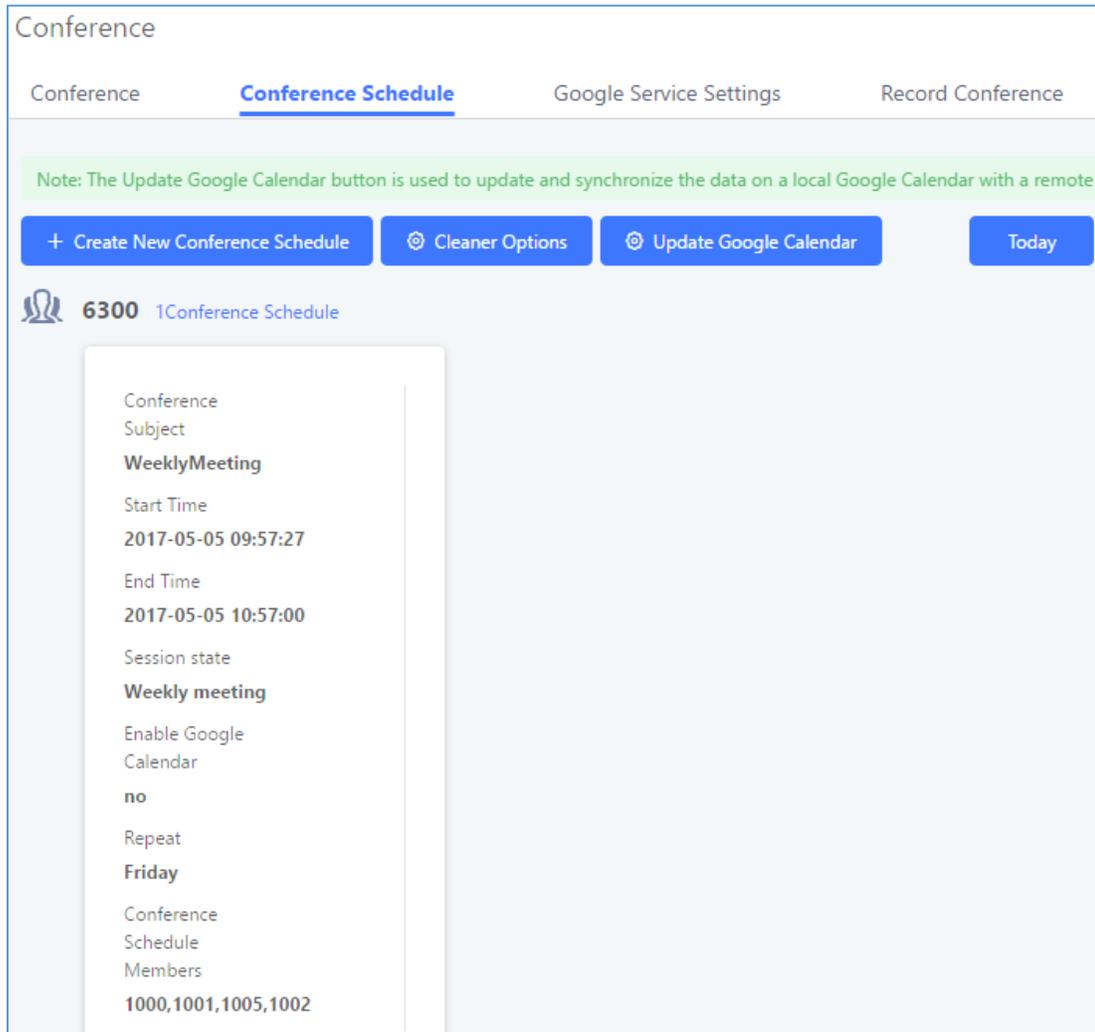


Figure 137: Conference Schedule

Once the conference room is scheduled, at the kick time, all users will be removed from conference room and no extension is allowed to join the conference room anymore. At the scheduled conference time, UCM6510 will send INVITE to the extensions that have been selected for conference.

⚠ Note:

- Please make sure that outbound route is properly configured for remote extensions to join the conference.
 - Once Kick Time is reached, Conference Schedule is locked and cannot be modified.
-



IVR

Configure IVR

IVR configurations can be accessed under the UCM6510 Web GUI → **Call Features** → **IVR**. Users could create, edit, view and delete an IVR.

- Click on "Create New IVR" to add a new IVR.
- Click on  to edit the IVR configuration.
- Click on  to delete the IVR.

Create New IVR

* Name:

* Extension:

Dial Trunk:

* Permission:

Dial Other Extensions: Extension Conference Call Queue
 Ring Group Paging/Intercom Groups
 Voicemail Groups Fax Extension
 Dial By Name
 All

* IVR Black/Whitelist:

Internal Black/Whitelist:

Available	Selected
1	3
1005 "Marcel LAST"	1001
	1002
	1000 "John DOE"

External Blacklist/Whitelist:

Replace Display Name:

Alert-info:

* Prompt: Prompt

* Digit Timeout:

* Response Timeout:

* Response Timeout Promp...: Prompt

* Invalid Prompt: Prompt

* Response Timeout Repeat...:

* Invalid Repeat Loops:

Language:

Figure 138: Create New IVR



Table 75: IVR Configuration Parameters

Basic Settings	
Name	Configure the name of the IVR. Letters, digits, _ and - are allowed.
Extension	Enter the extension number for users to access the IVR.
Dial Trunk	If enabled, all callers to the IVR can use trunk. The permission must be configured for the users to use the trunk first. Default setting is No.
Permission	Assign permission level for outbound calls if "Dial Trunk" is enabled. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the IVR, the UCM6510 will compared the IVR's permission level with the outbound route's privilege level. If the IVR's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Dial Other Extensions	This controls the destination that can be reached by the external caller via the inbound route. The available destinations are: <ul style="list-style-type: none"> • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Groups • Voicemail Groups • Fax Extension • Dial By Name • All
IVR Black/White List	If enabled only numbers inside of the White List or outside of the Black List can be called from IVR.
Internal Black/White List	Contain numbers, either of Black List or White List.
External Black/White List	This feature can be used only when Dial Trunk is enabled, it contains external numbers allowed or denied to call from the IVR, the allowed format is the following: Number1, number2, number3,
Replace Caller ID	If enabled, the UCM will replace the caller display name with the IVR name the caller know whether the call is incoming from a direct extension or an IVR.
Alert-Info	When present in an INVITE request, the alert-Info header field specifies and alternative ring tone to the UAS.
Welcome Prompt	Select an audio file to play as the welcome prompt for the IVR. Click on "Prompt" to add additional audio file under Web GUI→ PBX Settings → Voice Prompt → Custom Prompt .



Digit Timeout	Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, the UCM6510 will consider the entries complete. The default timeout is 3 seconds.
Response Timeout	After playing the prompts in the IVR, the UCM6510 will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout prompt will be played. The default setting is 10 seconds.
Response Timeout Prompt	Select the prompt message to be played when timeout occurs.
Invalid Prompt	Select the prompt message to be played when an invalid extension is pressed.
Response Timeout Repeat Loops	Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3.
Invalid Repeat Loops	Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3.
Language	Select the voice prompt language to be used for this IVR. The default setting is "Default" which is the selected voice prompt language under Web GUI→ PBX Settings → Voice Prompt → Language Settings . The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under Web GUI→ PBX Settings → Voice Prompt → Language Settings .

Key Pressing Events

Key Press Event: Press 0 Press 1 Press 2 Press 3 Press 4 Press 5 Press 6 Press 7 Press 8 Press 9 Press * Timeout Invalid	Select the event for each key pressing for 0-9, *, Timeout and Invalid. The event options are: <ul style="list-style-type: none"> • Extension • Voicemail • Conference Rooms • Voicemail Group • IVR • Ring Group • Queues • Page Group • Fax • Custom Prompt • Hangup • DISA • Dial By Name
--	---



- External Number
- Callback

Edit IVR: OfficeOpen

Basic Settings Key Pressing Events

Press 0:	Extension ▾	2000 ▾
Press 1:	IVR ▾	Sales ▾
Press 2:	IVR ▾	Support ▾
Press 3:	Select an Op... ▾	
Press 4:	Select an Op... ▾	
Press 5:	Select an Op... ▾	
Press 6:	Select an Op... ▾	
Press 7:	Select an Op... ▾	
Press 8:	Select an Op... ▾	
Press 9:	Select an Op... ▾	
Press *:	Select an Op... ▾	
Timeout:	Custom Pro... ▾	goodbye ▾
Invalid:	Custom Pro... ▾	goodbye ▾

Figure 139: Key Pressing Events

Black/White List in IVR

In some scenarios, the IPPBX administrator needs to restrict the extensions that can be reached from IVR. For example, the company CEO and directors prefer only receiving calls transferred by the secretary, some special extensions are used on IP surveillance end points which shouldn't be reached from external calls via IVR for privacy reason. UCM has now added blacklist and whitelist in IVR settings for users to manage this.

To use this feature, log in UCM Web GUI and navigate to **Call Features**→**IVR**→Create/Edit IVR: IVR Black/White List.

- If the user selects “Blacklist Enable” and adds extension in the list, the extensions in the list will not be allowed to be reached via IVR.



- If the user selects “Whitelist Enable” and adds extension in the list, only the extensions in the list can be allowed to be reached via IVR.

Create New IVR

* Name:

* Extension:

Dial Trunk:

* Permission:

Dial Other Extensions: Extension Conference Call Queue
 Ring Group Paging/Intercom Groups
 Voicemail Groups Fax Extension
 Dial By Name
 All

* IVR Black/Whitelist:

Internal Black/Whitelist:		Selected
<input type="checkbox"/> 1	Available	<input type="checkbox"/> 3
<input type="text" value="Search"/>		<input type="text" value="Search"/>
<input type="checkbox"/> 1005 "Marcel LAST"	< >	<input type="checkbox"/> 1001 <input type="checkbox"/> 1002 <input type="checkbox"/> 1000 "John DOE"

External Blacklist/Whitelist:

Replace Display Name:

Alert-info:

* Prompt: Prompt

* Digit Timeout:

* Response Timeout:

* Response Timeout Promp...: Prompt

* Invalid Prompt: Prompt

* Response Timeout Repeat...:

* Invalid Repeat Loops:

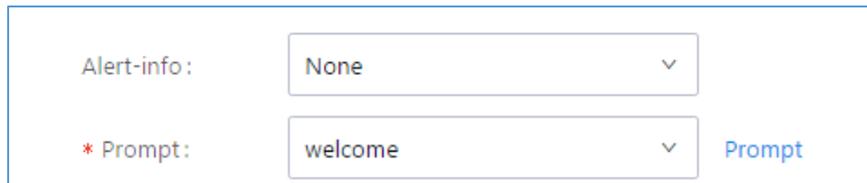
Language:

Figure 140: Black/White List



Create Custom Prompt

To record new IVR prompt or upload IVR prompt to be used in IVR, click on "Prompt" next to the "Welcome Prompt" option and the users will be redirected to IVR Prompt page. Or users could go to Web GUI→**PBX Settings**→**Voice Prompt**→**Custom Prompt** page directly.



Alert-info:	None	▼
* Prompt:	welcome	▼

Prompt

Figure 141: Click on Prompt to Create IVR Prompt

Once the IVR prompt file is successfully added to the UCM6510, it will be added into the prompt list options for users to select in different IVR scenarios.

LANGUAGE SETTINGS FOR VOICE PROMPT

The UCM6510 supports multiple languages in Web GUI as well as system voice prompt. The following languages are currently supported in system voice prompt:

English (United States)
Arabic
Chinese
Dutch
English (United Kingdom)
French
German
Greek
Hebrew
Italian
Polish
Portuguese
Russian
Spanish
Swedish
Turkish

English (United States) and Chinese voice prompts are built in with the UCM6510 already. The other languages provided by Grandstream can be downloaded and installed from the UCM6510 Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the UCM6510.

Language settings for voice prompt can be accessed under Web GUI→**PBX Settings**→**Voice Prompt**→**Language Settings**.

Download and Install Voice Prompt Package

To download and install voice prompt package in different languages from UCM6510 Web GUI, click on "Check Prompt List" button.



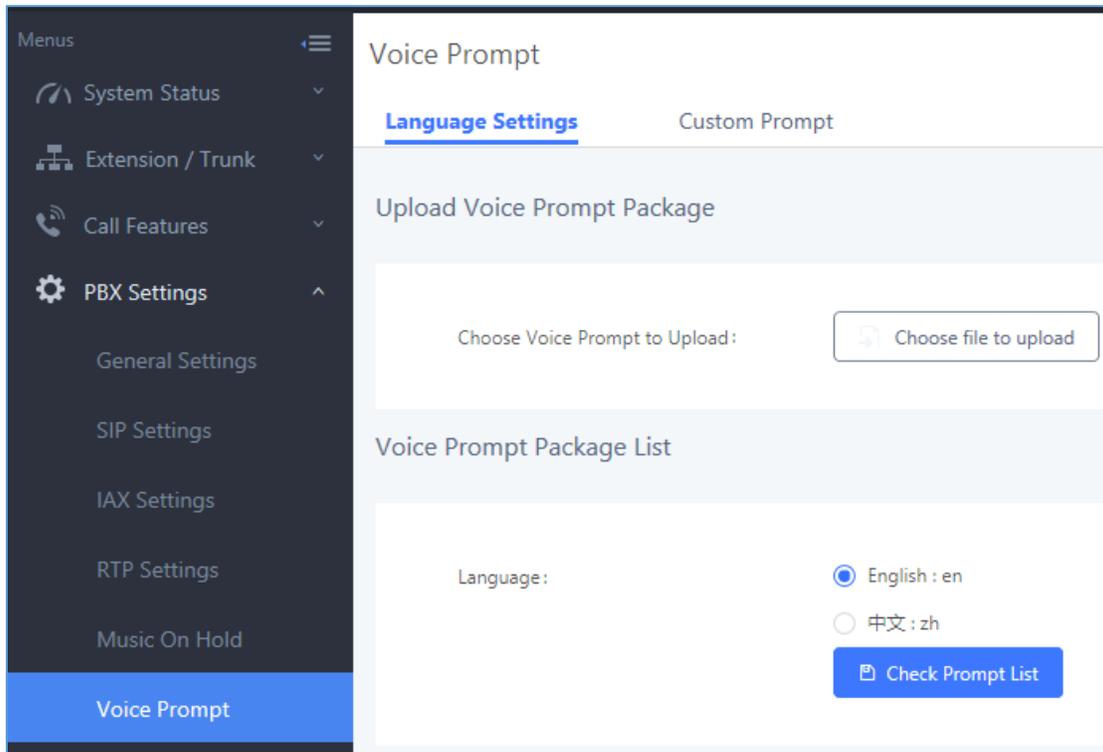


Figure 142: Language Settings for Voice Prompt

A new dialog window of voice prompt package list will be displayed. Users can see the version number (latest version available V.S. current installed version), package size and options to upgrade or download the language.

Voice Prompt Package List	Version (Remote / Local)	Size	Options
Deutsch	1.4/-	3.8M	
English	1.5/1.5	5.5M	
Español	1.6/-	4.0M	
Español(Español)	1.4/-	3.6M	
Ελληνικά	1.4/-	3.9M	
Français	1.4/-	3.7M	
Italiano	1.4/-	3.6M	

Cancel

Figure 143: Voice Prompt Package List



Click on  to download the language to the UCM6510. The installation will be automatically started once the downloading is finished.

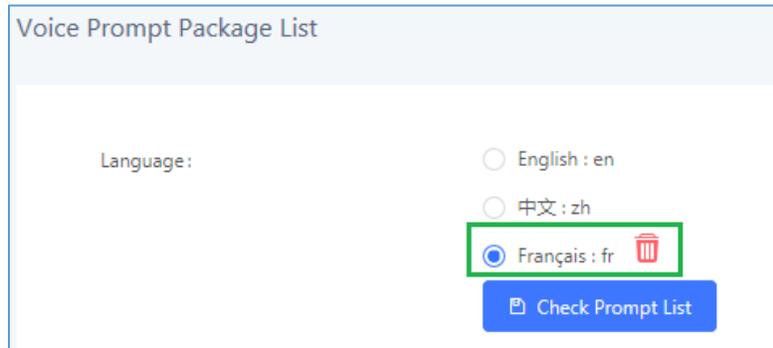


Figure 144: New Voice Prompt Language Added

A new language option will be displayed after successfully installed. Users then could select it to apply in the UCM6510 system voice prompt or delete it from the UCM6510.

Customize Specific Prompt

On the UCM6510, if the user needs to replace some specific customized prompt, the user can upload a single specific customized prompt from Web GUI→**PBX Settings**→**Voice Prompt**→**Language Settings** instead of the entire language pack.

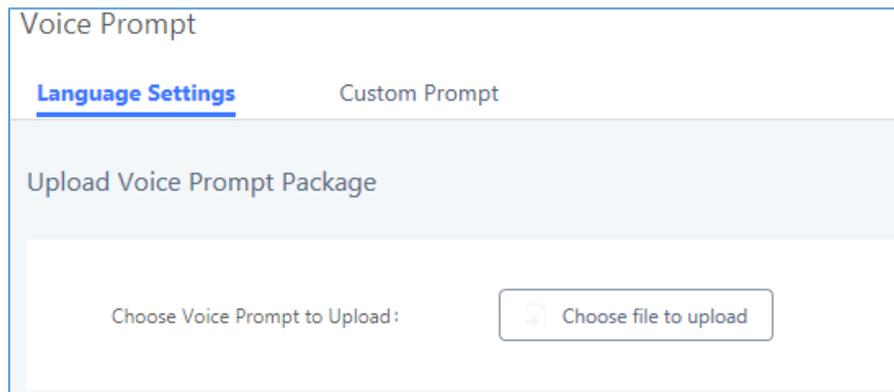


Figure 145: Upload Single Voice Prompt for Entire Language Pack

VOICEMAIL

Configure Voicemail

If the voicemail is enabled for UCM6510 extensions, the configurations of the voicemail can be globally set up and managed under Web GUI→**Call Features**→**Voicemail**.

General Voicemail Settings

Voicemail
Voicemail Groups

Voicemail Email Settings

* Max Greeting (s):

Dial "0" for Operator:

Operator Extension: ▾

* Max Messages Per

Folder:

Max Message Time: ▾

Min Effective Message ▾

Time:

Announce Message

Caller-ID:

Announce Message

Duration:

Play Envelope:

Play from Last:

Allow User Review:

Figure 146: Voicemail Settings



Table 76: Voicemail Settings

Max Greeting	Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds.
Dial '0' For Operator	If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator's extension.
Operator Extension	Select the operator extension, which will be dialed when users press 0 to exit voicemail application. The operator extension can also be used in IVR option.
Max Messages Per Folder	Configure the maximum number of messages per folder in users' voicemail. The valid range 10 to 1000. The default setting is 50.
Max Message Time	<p>Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the max message time. The default setting is 15 minutes. The available options are:</p> <ul style="list-style-type: none"> • 1 minute • 2 minutes • 5 minutes • 15 minutes • 30 minutes • Unlimited
Min Effective Message Time	<p>Configure the minimum effective duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Effective Message Time. The default setting is 3 seconds. The available options are:</p> <ul style="list-style-type: none"> • No minimum • 1 second • 2 seconds • 3 seconds • 4 seconds • 5 seconds <p>Note: Silence and noise duration are not counted in message time.</p>
Announce Message Caller-ID	If enabled, the caller ID of the user who has left the message will be announced at the beginning of the voicemail message. The default setting is "No".
Announce Message Duration	If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is "No".
Play Envelope	If enabled, a brief introduction (received time, received from, and etc) of each message will be played when accessed from the voicemail application. The default setting is "Yes".



Play from Last	If enabled, UCM6510 will play from the voice message left most recently; if disabled, UCM6510 will play from the earliest left voice message
Allow User Review	If enabled, users can review the message following the IVR before sending the message out. The default setting is "No".

Access Voicemail

If the voicemail is enabled for UCM6510 extensions, the users can dial the voicemail access feature code (by default *98 or *97) to access the extension's voicemail. The users will be prompted to enter the voicemail password and then can enter digits from the phone keypad to navigate in the IVR menu for different options.

Table 77: Voicemail IVR Menu

Main Menu	Sub Menu 1	Sub Menu 2
1 – New messages	3 - Advanced options	1 - Send a reply
		2 - Call the person who sent this message
		3 - Hear the message envelop
		4 - Leave a message
		* - Return to the main menu
	5 - Repeat the current message	
	7 - Delete this message	
	8 - Forward the message to another user	
	9 - Save	
	* - Help	
	# - Exit	
2 – Change folders	0 - New messages	
	1 - Old messages	
	2 - Work messages	
	3 - Family messages	
	4 - Friend messages	
	# - Cancel	
3 – Advanced options	1 - Send a reply	
	2 - Call the person who sent this message	
	3 - Hear the message envelop	

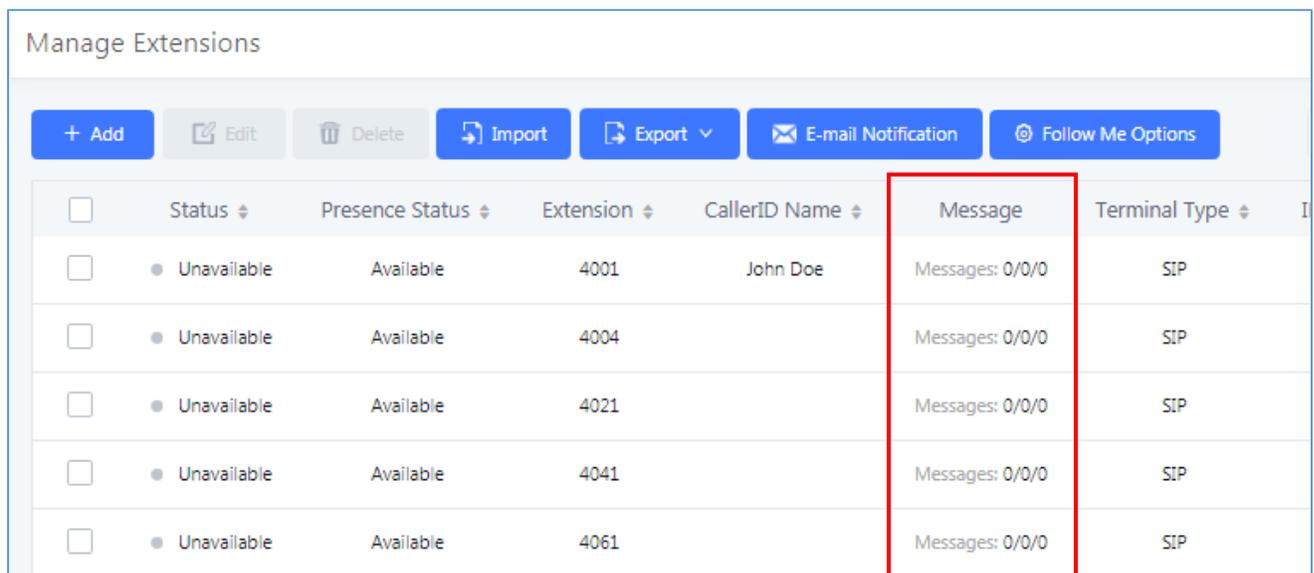


	4 - Leave a message	
	* - Return to the main menu	
0 – Mailbox options	1 - Record your unavailable message	1 - Accept this recording 2 - Listen to it 3 - Re-record your message
	2 - Record your busy message	1 - Accept this recording 2 - Listen to it 3 - Re-record your message
	3 - Record your name	1 - Accept this recording 2 - Listen to it 3 - Re-record your message
	4 - Record temporary greeting	1 - Accept this recording 2 - Listen to it 3 - Re-record your message
	5 - Change your password	
	* - Return to the main menu	

Extension Voicemail Count

The UCM6510 provides an easy way to check the number of voicemail messages for each extension directly from UCM web GUI → Extension/Trunk → Extensions overview page.

Voicemail count (“Message” column) is displayed in the format ***Urgent / Total / Read***.



Manage Extensions							
<input type="button" value="+ Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="E-mail Notification"/> <input type="button" value="Follow Me Options"/>							
<input type="checkbox"/>	Status	Presence Status	Extension	CallerID Name	Message	Terminal Type	
<input type="checkbox"/>	● Unavailable	Available	4001	John Doe	Messages: 0/0/0	SIP	
<input type="checkbox"/>	● Unavailable	Available	4004		Messages: 0/0/0	SIP	
<input type="checkbox"/>	● Unavailable	Available	4021		Messages: 0/0/0	SIP	
<input type="checkbox"/>	● Unavailable	Available	4041		Messages: 0/0/0	SIP	
<input type="checkbox"/>	● Unavailable	Available	4061		Messages: 0/0/0	SIP	

Figure 147: Voicemail Count



Voicemail Email Settings

The UCM6510 can be configured to send the voicemail as attachment to Email. Click on "Voicemail Email Settings" button to configure the Email attributes and content.

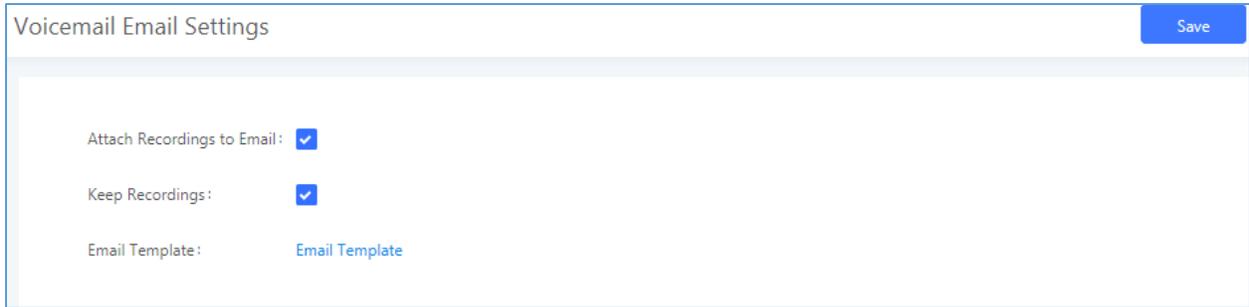


Figure 148: Voicemail Email Settings

Click on "Email Template" button to view the default template as an example.

Table 78: Voicemail Email Settings

Attach Recordings to E-Mail	If enabled, voicemails will be sent to user's Email address. The default setting is "Yes".
Keep Recordings	If enabled, voicemail will be stored in the UCM6510 after email is sent. The default setting is "Yes".
Template For Voicemail Emails	<p>Fill in the "Subject:" and "Message:" content, to be used in the Email when sending to the user.</p> <p>The template variables are:</p> <ul style="list-style-type: none"> • \t: TAB • \${VM_NAME}: Recipient's first name and last name • \${VM_DUR}: The duration of the voicemail message • \${VM_MAILBOX}: The recipient's extension • \${VM_CALLERID}: The caller ID of the person who has left the message • \${VM_MSGNUM}: The number of messages in the mailbox • \${VM_DATE}: The date and time when the message is left



Configure Voicemail Group

The UCM6510 supports voicemail group and all the extensions added in the group will receive the voicemail to the group extension. The voicemail group can be configured under Web GUI→**Call Features**→**Voicemail Group**. Click on "Create New Voicemail Group" to configure the group.

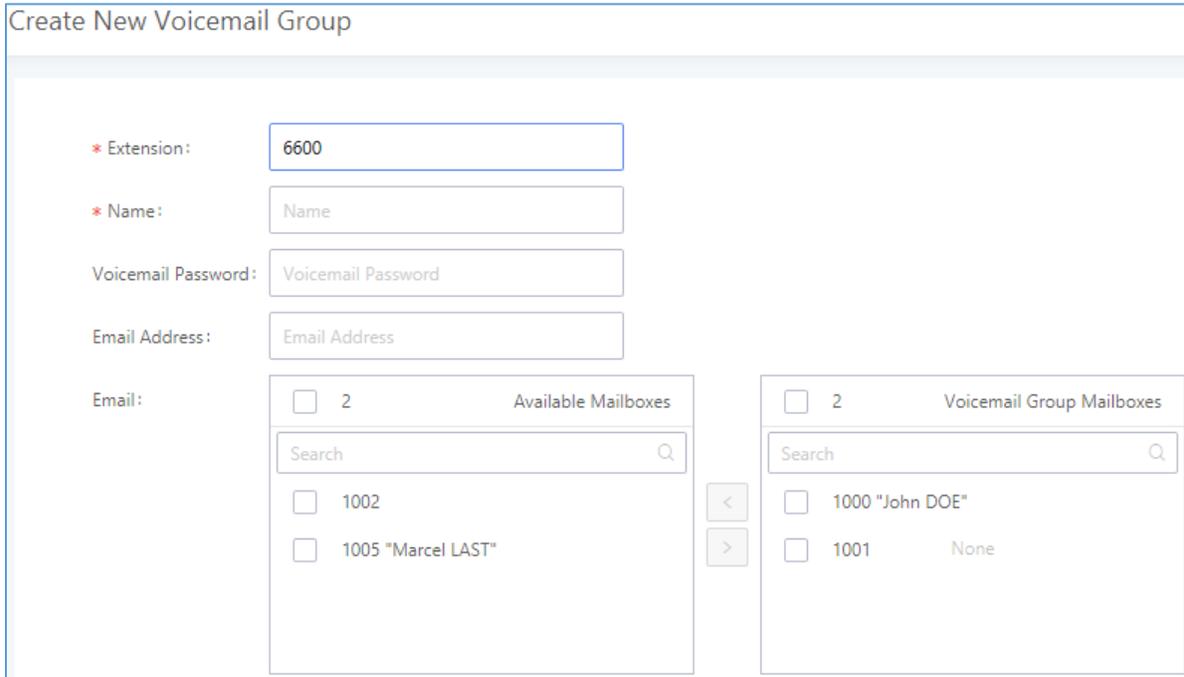


Figure 149: Voicemail Group

Table 79: Voicemail Group Settings

Voicemail Group Extension	Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members.
Name	Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed.
Voicemail Password	The Voicemail password for the user to check Voicemail messages.
Email Address	The Email address of current user.
Voicemail Group Mailboxes	Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list.

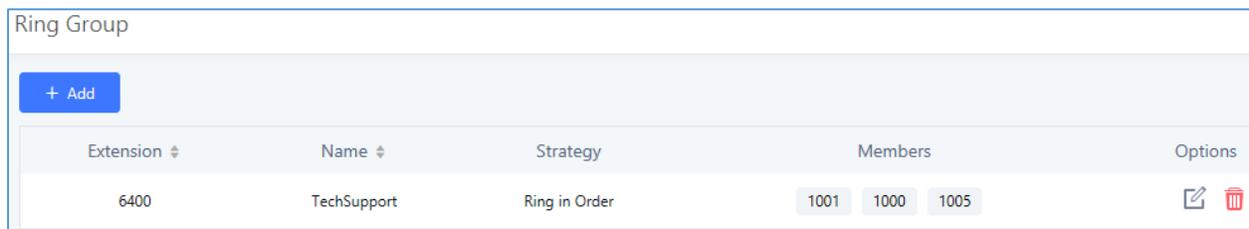


RING GROUP

The UCM6510 supports ring group feature with different ring strategies applied to the ring group members. This section describes the ring group configuration on the UCM6510.

Configure Ring Group

Ring group settings can be accessed via Web GUI → **Call Features** → **Ring Group**.



Extension	Name	Strategy	Members	Options
6400	TechSupport	Ring in Order	1001 1000 1005	

Figure 150: Ring Group

- Click on "Create New Ring Group" to add ring group.
- Click on to edit the ring group. The following table shows the ring group configuration parameters.
- Click on to delete the ring group.

Table 80: Ring Group Parameters

Ring Group Name	Configure ring group name to identify the ring group. Letters, digits, _ and - are allowed.
Extension	Configure the ring group extension.
Ring Group Members	Select available users from the left side to the ring group member list on the right side. Click on to arrange the order.
Selected LDAP Numbers	Select available remote users from the left side to the ring group member list on the right side. Click on to arrange the order. Note: LDAP Sync must be enabled first.
Ring Strategy	Select the ring strategy. The default setting is "Ring in order". <ul style="list-style-type: none"> • Ring simultaneously Ring all the members at the same time when there is incoming call to the ring group extension. If any of the member answers the call, it will stop ringing.



	<ul style="list-style-type: none"> • Ring in order Ring the members with the order configured in ring group list. If the first member doesn't answer the call, it will stop ringing the first member and start ringing the second member.
Music On Hold	Select the "Music On Hold" Class of this Ring Group, "Music On Hold" can be managed from the "Music On Hold" panel on the left.
Custom Prompt	This option allows user to customize prompt for a ring group to announce to caller. The file can be uploaded from Web GUI→Internal Options→Custom Prompt, or click the 'Prompt' to add additional record.
Ring Timeout on Each Member	Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 30 seconds. Note: The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.
Auto Record	Once this option is enabled, the calls using this extension or trunk will be automatically recorded.
Replace Caller ID	If enabled, the UCM will replace the caller display name with the Ring Group name the caller know whether the call is incoming from a direct extension or a Ring Group.
Enable Destination	If enabled, users could select extension, voicemail, ring group, IVR, call queue, voicemail group as the destination if the call to the ring group has no answer. Secret and Email address are required if voicemail is selected as the destination.
Secret	Configure the password to access the ring group extension's voicemail. Note: The password has to be at least 4 characters.
Email Address	Configure the Email address of the ring group extension's voicemail. If "Attach Recordings to E-mail" is enabled from Web GUI→PBX→Voicemail→Voicemail Email Settings, the voicemail can be sent to the ring group's Email address as attachment.



Edit Ring Group: 6400
Save

* Ring Group Name:

* Extension:

Members:

1 Available Extensions

Search

1002

3 Selected Extensions

Search

1001

1000 "John DOE"bne

1005 "Marcel LAST"

<
>

LDAP Phonebook:

1 Available LDAP

Search

1002(ou=GSEMEA,dc=pbx,dc=com)

None

0 Selected LDAP

Search

None

<
>

Ring Group Options

Ring Strategy:

Music On Hold:

Custom Prompt: [Prompt](#)

* Ring Timeout on E...:

Auto Record:

Figure 151: Ring Group Configuration

Remote Extension in Ring Group

Remote extensions from the peer trunk of a remote UCM6510 can be included in the ring group with local extension. An example of Ring Group with peer extensions is presented in the following:

1. Creating SIP Peer Trunk between both UCM6510_A and UCM6510_B. **SIP Trunk** can be found under Web GUI→**PBX**→**Extension/Trunk**→**VoIP Trunks**. Also, please configure their Inbound/Outbound routes accordingly.
2. Click edit button in the menu , and check if **Sync LDAP Enable** is selected, this option will allow UCM6510_A update remote LDAP server automatically from peer UCM6510_B. In addition, **Sync**



LDAP Password must match for UCM6510_A and UCM6510_B in order to sync LDAP contact automatically. Port number can be anything between 0~65535, and use the outbound rule created in step 1 for the **LDAP Outbound Rule** option.

Edit SIP Trunk: BranchOffice

Basic Settings Advanced Settings

Codec Preference:

<input type="checkbox"/> 9 Available Codecs	<input type="checkbox"/> 6 Selected Codecs
<input type="checkbox"/> G.722	<input type="checkbox"/> PCMU
<input type="checkbox"/> AAL2-G.726-3...	<input type="checkbox"/> PCMA
<input type="checkbox"/> ADPCM	<input type="checkbox"/> GSM
<input type="checkbox"/> G.723	<input type="checkbox"/> G.726
<input type="checkbox"/> H.263	<input type="checkbox"/> G.729

Send PPI Header:

Send PAI Header:

DID Mode: Request-line

DTMF Mode: Default

Enable Heartbeat Detection:

* The Maximum Number of Call Lines: 1

Fax Mode: None

SRTP: Disabled

Sync LDAP Enable:

* Sync LDAP Password: admin123

* Sync LDAP Port: 36789

LDAP Outbound Rule: Self-defined

* LDAP Dialed Prefix: 1

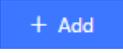
Figure 152: Sync LDAP Server option

- In case if LDAP server doesn't sync automatically, user can manually sync LDAP server. Under **VoIP Trunks** page, click sync button shown in the following figure to manually sync LDAP contacts from peer UCM6510.



Provider Name	Terminal Type	Type	Hostname/IP	Username	Options
BranchOffice	SIP	peer	192.168.6.203		   

Figure 153: Manually Sync LDAP Server

- Under **Ring Groups** setting page, click . **Ring Groups** can be found under Web GUI→**Call Features**→**Ring Groups**.
- If LDAP server is synced correctly, **Available LDAP Numbers** box will display available remote extensions that can be included in the current ring group. Please also make sure the extensions in the peer UCM6510 can be included into that UCM6510's LDAP contact.

Create New Ring Group Save

* Ring Group Name:

* Extension:

Members:

Available Extensions

106

1000

1001

1002

1003

Selected Extensions

0

None

LDAP Phonebook: Available LDAP

15

5000(ou=ucm6510,dc=pbx,dc=com)

5001(ou=ucm6510,dc=pbx,dc=com)

5002(ou=ucm6510,dc=pbx,dc=com)

5003(ou=ucm6510,dc=pbx,dc=com)

Selected LDAP

0

None

Ring Group Options

Ring Strategy:

Music On Hold:

Custom Prompt: [Prompt](#)

* Ring Timeout on

Figure 154: Ring Group Remote Extension



PAGING AND INTERCOM GROUP

Paging and Intercom Group can be used to make an announcement over the speaker on a group of phones. Targeted phones will not ring but answer immediately using speaker. The UCM6510 paging and intercom can be used via feature code to a single extension or a paging/intercom group. This section describes the configuration of paging/intercom group under Web GUI→**Call Features**→**Paging/Intercom**.

Configure Paging/Intercom Group

- Click on "Create New Paging/Intercom Group" to add paging/intercom group.

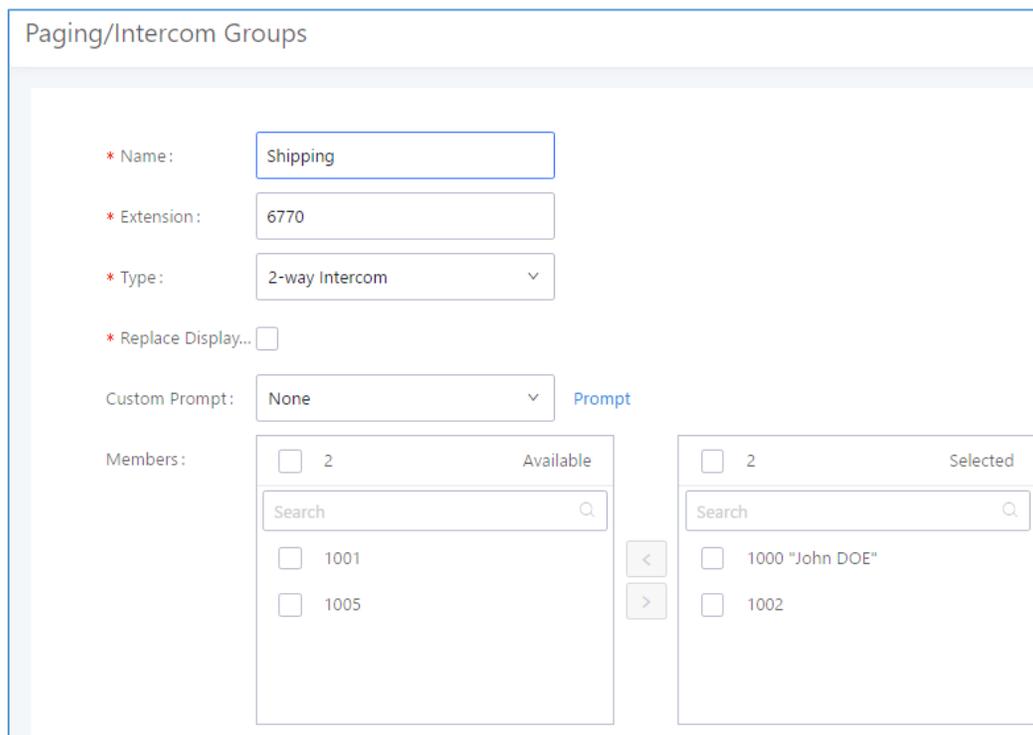


Figure 155: Paging/Intercom Group

Table 81: Paging/Intercom Group Configuration Parameters

Name	Configure paging/intercom group name.
Extension	Configure the paging/intercom group extension.
Type	Select "2-way Intercom" or "1-way Page".
Custom Prompt	This option is setting a custom prompt used as announcement placed to the person receiving a paging/internal call. The file can be uploaded from the Web GUI → Internal Options → Custom Prompt , or click the 'Prompt' to add additional recorded.
Page/Intercom Group Members	Select available users from the left side to the paging/intercom group member list on the right.



- Click on  to edit the paging/intercom group.
- Click on  to delete the paging/intercom group.
- Click on "Paging/Intercom Group Settings" to edit Alert-Info Header. This header will be included in the SIP INVITE message sent to the callee in paging/intercom call.

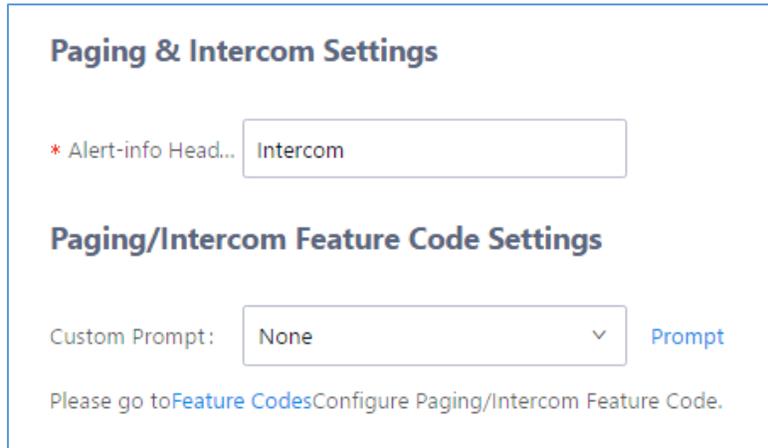


Figure 156: Page/Intercom Group Settings

- The UCM6510 has pre-configured paging/intercom feature code. By default, the Paging Prefix is *81 and the Intercom Prefix is *80. To edit page/intercom feature code, click on "Feature Codes" in the "Paging/Intercom Group Settings" dialog. Or users could go to Web GUI→**Call Features**→**Feature Codes** directly.

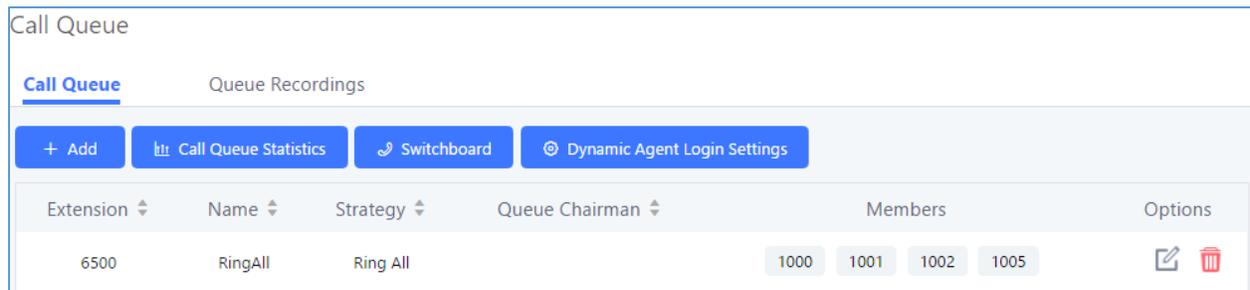
CALL QUEUE

The UCM6510 supports call queue by using static agents or dynamic agents. Call Queue system can accept more calls than the available agents. Incoming calls will be hold until next representative is available in the system. This section describes the configuration of call queue under Web GUI→**Call Features**→**Call Queue**.

Configure Call Queue

Call queue settings can be accessed via Web GUI→**Call Features**→**Call Queue**.

- Click on  to add call queue.
- Click on  to edit the call queue. The call queue configuration parameters are listed in bellow table.
- Click on  to delete the call queue.



Extension	Name	Strategy	Queue Chairman	Members	Options
6500	RingAll	Ring All		1000 1001 1002 1005	 

Figure 157: Call Queue

Table 82: Call Queue Configuration Parameters

Basic Settings	
Extension	Configure the call queue extension number.
Name	Configure the call queue name to identify the call queue.
Strategy	Select the strategy for the call queue. <ul style="list-style-type: none"> • Ring All Ring all available Agents simultaneously until one answers. • Linear Ring agents in the specified order. • Least Recent Ring the agent who has been called the least recently.

	<ul style="list-style-type: none"> • Fewest Calls Ring the agent with the fewest completed calls. • Random Ring a random agent. • Round Robin Ring the agents in Round Robin scheduling with memory. <p>The default setting is "Ring All".</p>
Music On Hold	<p>Select the Music On Hold class for the call queue.</p> <p>Note: Music On Hold classes can be managed from Web GUI→PBX Settings→Music On Hold.</p>
Max Queue Length	<p>Configure the maximum number of calls to be queued at once. This number does not include calls that have been connected with agents. It only includes calls not connected yet. The default setting is 0, which means unlimited. When the maximum value is reached, the caller will be treated with busy tone followed by the next calling rule after attempting to enter the queue.</p>
Wrapup Time	<p>Configure the number of seconds before a new call can ring the queue after the last call on the agent is completed. If set to 0, there will be no delay between calls to the queue. The default setting is 10 seconds.</p>
Retry Time	<p>Configure the number of seconds to wait before ringing the next agent.</p>
Ring Time	<p>Configure the number of seconds an agent will ring before the call goes to the next agent. The default setting is 30 seconds.</p>
Auto Record	<p>If enabled, the calls on the call queue will be automatically recorded. The recording files can be accessed in Queue Recordings under Web GUI→Call Features→Call Queue.</p>
Max Wait Time	<p>Configure the timeout after which users will be disconnected from the call queue. The default setting is "0" which means unlimited.</p> <p>Note: It is recommended to configure "Wait Time" longer than the "Wrapup Time".</p>
Destination	<p>Once Max Wait Time has been configured, select to which destination send the calls that have timed out. The default is to "Hang up" the call.</p>
Destination Prompt Cycle	<p>Configure the voice prompt cycle (in seconds) of the call queue. Once all agents are busy and the voice prompt will be played and you can press the appropriate key to transfer to failover destination.</p>
Custom Prompt	<p>When playing a custom prompt, press 1 to transfer to failover destination.</p>
Destination	<p>Select failover destination to send callers after pressing 1 upon hearing the custom prompt.</p>



Advanced Settings	
<ul style="list-style-type: none"> - Virtual Queue - Position - Announcement - Queue Chairman 	Refer to Call Center Settings & enhancements section for detailed information about these features.
Enable Agent Login	Enables dynamic agent login/logout features.
Leave When Empty	<p>Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict".</p> <ul style="list-style-type: none"> • Yes Callers will be disconnected from the queue if all agents are paused or invalid. • No Never disconnect the callers from the queue when the queue is empty. • Strict Callers will be disconnected from the queue if all agents are paused, invalid or unavailable.
Dial in Empty Queue	<p>Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No".</p> <ul style="list-style-type: none"> • Yes Callers can always dial into a call queue. • No Callers cannot dial into a queue if all agents are paused or invalid. • Strict Callers cannot dial into a queue if the agents are paused, invalid or unavailable.
Report Hold Time	If enabled, the UCM6510 will report (to the agent) the duration of time of the call before the caller is connected to the agent. The default setting is "No".
Replace Display Name	If enabled, the UCM will replace the caller display name with the Call Queue name so that the caller knows the call is incoming from a Call Queue.
Enable Feature Codes	Enable feature codes option for call queue. For example, *83 is used for "Agent Pause"
Dynamic Login Password	If enabled, the configured PIN number is required for dynamic agent to log in. The default setting is disabled.
Alert-Info	Configure the call destination for the call to be routed to if no agent in this call queue answers the call.



Agents	
Agents	Go to “Agents” Tab and Select the available users to be the static agents in the call queue. Choose from the available users on the left to the static agents list on the right. Click on <input type="checkbox"/> <input type="checkbox"/> to choose. And use UP and Down arrow to select the order of the agent within the call queue.

Static Agents limitation:

To guarantee a high level of audio quality with the call queue feature, UCMs will limit the number of static agents allowed to be assigned depending on the UCM model used. If the user attempts to configure the number of static agents to be more than the maximum allowed number, a warning message will appear.

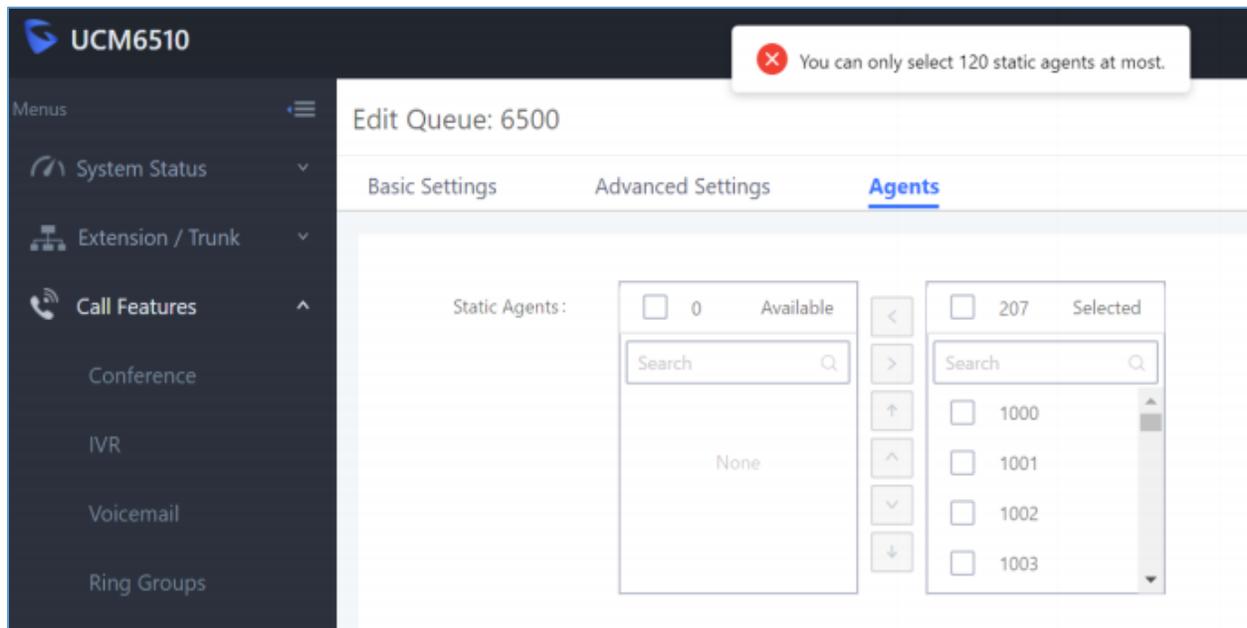


Figure 158: Static Agents limitation

The following table lists the maximum number of static agents for each UCM model:

UCM Model	Max Static Agents in Call Queue
UCM6102 and UCM6202	18
UCM6104 and UCM6204	27
UCM6108 and UCM6116	36
UCM6208	60
UCM6510	120



- Click on "Dynamic Agent Login Settings" to configure Agent Login Extension Postfix and Agent Logout Extension Postfix. Once configured, users could log in the call queue as dynamic agent.

Dynamic Agent Login Settings

Agent Login Extension P...

Agent Logout Extension ...

Example: If Queue Extension is 6500,
 Agent Login Extension Postfix is *,
 Agent Logout Extension Postfix is **,
 Dial **6500*** to log in, dial **6500**** to log out.

Note: Remove postfix will lead the agent that has
 not log out yet cannot logout.

Figure 159: Agent Login Settings

For example, if the call queue extension is 6510, Agent Login Extension Postfix is * and Agent Logout Extension Postfix is **, users could dial 6510* to login to the call queue as dynamic agent and dial 6510** to logout from the call queue. Dynamic agent doesn't need to be listed as static agent and can log in/logout at any time.

- Call queue feature code "Agent Pause" and "Agent Unpause" can be configured under Web GUI→**Call Features**→**Feature Codes**. The default feature code is *83 for "Agent Pause" and *84 for "Agent Unpause".
- Queue recordings are shown on the Call Queue page under "Queue Recordings" Tab. Click on  to download the recording file in .wav format; click on  to delete the recording file. To delete multiple recording files by one click, select several recording files to be deleted and click on "Delete Selected Recording Files" or click on "Delete All Recording Files" to delete all recording files.

Call Center Settings & enhancements

UCM supports light weight call center features including virtual call queue and position announcement, allowing the callers to know their position on the call queue and giving them the option to either stay on the line waiting for their turn or activate a callback which will be initiated by the UCM once an agent is free.



In order to configure call center features, press  on an existing call queue and go under the advanced settings tab. Following parameters are available:

Table 83: Call Center Parameters

Enable Virtual Queue	Enable virtual queue to activate call center features.
Virtual Queue Period	Configure the time in (s) after which the virtual queue will take effect and the menu will be presented to the caller to choose an option. Default is 20s.
Virtual Queue Mode	<p>Offered to caller after timeout: After the virtual queue period passes, the caller will enter the virtual call queue and be presented with a menu to choose an option, the choices are summarized below:</p> <ul style="list-style-type: none"> • Press * to set current number as callback number. • Press 0 to set a callback number different than current caller number. • Press # to keep waiting on the call queue. <p>Triggered on user request: on this mode, the callers can activate the virtual queue by pressing 2, then they will be presented with the menu to choose an option as bellow:</p> <ul style="list-style-type: none"> • Press * to set current number as callback number. • Press 0 to set a callback number different than current caller number. • Press # to keep waiting on the call queue.
Virtual Queue Outbound Prefix	System will add this prefix to dialed numbers when calling back users.
Enable Position Announcement	Enable the announcement of the caller's position periodically.
Position Announcement Interval	Configure the period of time in (s) during which the UCM will announce the caller's position in the call queue.
CTI Chairman	Select the extension to act as chairman of the queue (monitoring).

Queue Auto fill enhancement:

In previous UCM firmware, the call queue has a serial type behavior in that the queue will make all waiting callers wait in the queue even if there is more than one available member ready to take calls until the head caller is connected with the member they were trying to get to. The next waiting caller in line then becomes the head caller, and they are then connected with the next available member and all available members and waiting callers waits while this happens.

Starting from 1.0.14.x, the waiting callers are connecting with available members in a parallel fashion until there are no more available members or no more waiting callers.

For example, in a call queue with linear method, if there are two available agents, when two callers call in the queue at the same time, UCM will assign the two callers to each of the two available agents at the same time, rather than assigning the second caller to second available agent after the first agent answers the call from the first caller.



Queue Statistics

Along with call center features, users can also gather detailed call queue statistics allowing them to make better changes/decision to manage better the call distribution and handling based on time, agent and queue.

To access call queue statistics, go to Web GUI→**Call Features**→**Call Queue** and click on “Call Queue Statistics”, the following page will be displayed:

Call Queue Statistics
Save

* Start Time:

* Queues:

* End Time:

* Agents:

Statistics Report

Report Information

Total Information

Call Distribution By Queue

Call Distribution By Agent

Call Distribution By Hour

Call Distribution By Day

Call Distribution By Day of Week

Call Distribution By Week

Call Distribution By Month

Virtual Queue Total Information

Virtual Queue Distribution By Queue

Virtual Queue Distribution By Agent

Virtual Queue Distribution By Hour

Virtual Queue Distribution By Day

Virtual Queue Distribution By Day of Week

Virtual Queue Distribution By Week

Virtual Queue Distribution By Month

Report Information

Queues	Agents			Start Time	End Time	Select Time Period
6500	1004	1002	1003	2017-05-09	2017-05-09	1 days

Total Information

Received	Answered	Unanswered	Abandoned	Transferred	% Answ	% Unansw	% Abandon	% Trans	Login	Logoff	Avg Talk	Av
17	3	0	14	0	17.65 %	0.00 %	82.35 %	0.00 %	0	0	00:00:30	0

Figure 160: Call Queue Statistics

Select the time interval along with the queue(s) and agent(s) to get detailed statistics, then press on which information to be displayed (call distribution by agent, virtual queue distribution by hour etc).



Switchboard

Switchboard is a Web GUI tool for call queue monitoring and management, admin can access to it from the menu **Call Features**→**Call Queue** then press « Switchboard ».

Following page will be displayed:

Switchboard
Cancel

[6500 \(RingAll\)](#)

Waiting

Status	Caller	Callee	Position	Talk Time	Options
	1009	6500	1	2017-05-09 05:58:46	

Proceeding

Status	Caller	Callee	Talk Time	Options
	1000	1002	2017-05-09 05:59:16	

Agents

Extension Status	Extension	Answered	Abandoned	Talk Time	Agent Status
In Use	1002	0	3	00:00:00	Static
Ringing	1003	0	4	00:00:00	Static
Unavailable	1004	0	0	00:00:00	Static

Figure 161: Call Queue Switchboard

The table below gives a brief description for the main menus:

Table 84: Switchboard Parameters

Waiting	This menu shows the current waiting calls along with the caller id and the option to hang-up call by pressing on the button.
Proceeding	Shows the current established calls along with the caller id and the callee (agent) as well as the option to hang-up, transfer, add conference or barge-in the call using the options button .
Agents	Displays the list of agents in the queue and the extension status (idle, ringing, in use or unavailable) along with some basic call statistics and agent's mode (static or dynamic).



There are three different privilege levels for Call Queue management from the switchboard: Super Admin, Queue Chairman, and Queue Agent.

- **Super Admin** - Default admin of the UCM. Call queue privileges include being able to view and edit all queue agents, monitor and execute actions for incoming and ongoing calls for each extension in Switchboard, and generate Call Queue reports to track performance.
- **Queue Chairman** - User appointed by Super Admin to monitor and manage an assigned queue extension via Switchboard. The Queue Chairman can log into the UCM user portal with his extension number and assigned user password. To access the Switchboard, click on “*Value-added Features*” in the side menu and click on “*Call Queue*”. In the image below, User 1012 is the Queue Chairman appointed to manage Queue Extension 6500 and can see all the agents of the queue in the Switchboard.
- **Queue Agent** - User appointed by Super Admin to be a member of a queue extension. A queue agent can log into the UCM user portal with his extension number and assigned user password. To access the Switchboard, click on “*Value-added Features*” in the side menu and click on “*Call Queue*”. However, a queue agent can view and manage only his own calls and statistics, but not other agents’ in the queue extension. In the image below, User 1007 is a queue agent and can see only his own information in the Switchboard.



PICKUP GROUPS

The UCM6510 supports pickup group feature which allows users to pick up incoming calls for other extensions if they are in the same pickup group, by dialing "Pickup Extension" feature code (by default *8).

Configure Pickup Groups

Pickup groups can be configured via Web GUI → **Call Features** → **Pickup Groups**.

- Click on  to create a new pickup group.
- Click on  to edit the pickup group.
- Click on  to delete the pickup group.

Select extensions from the list on the left side to the right side.

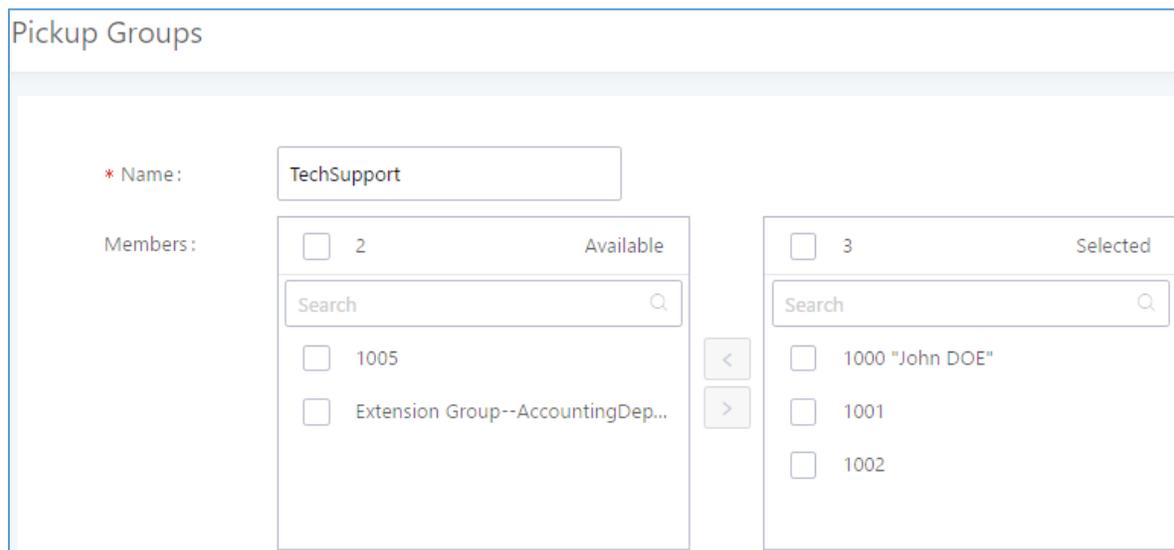


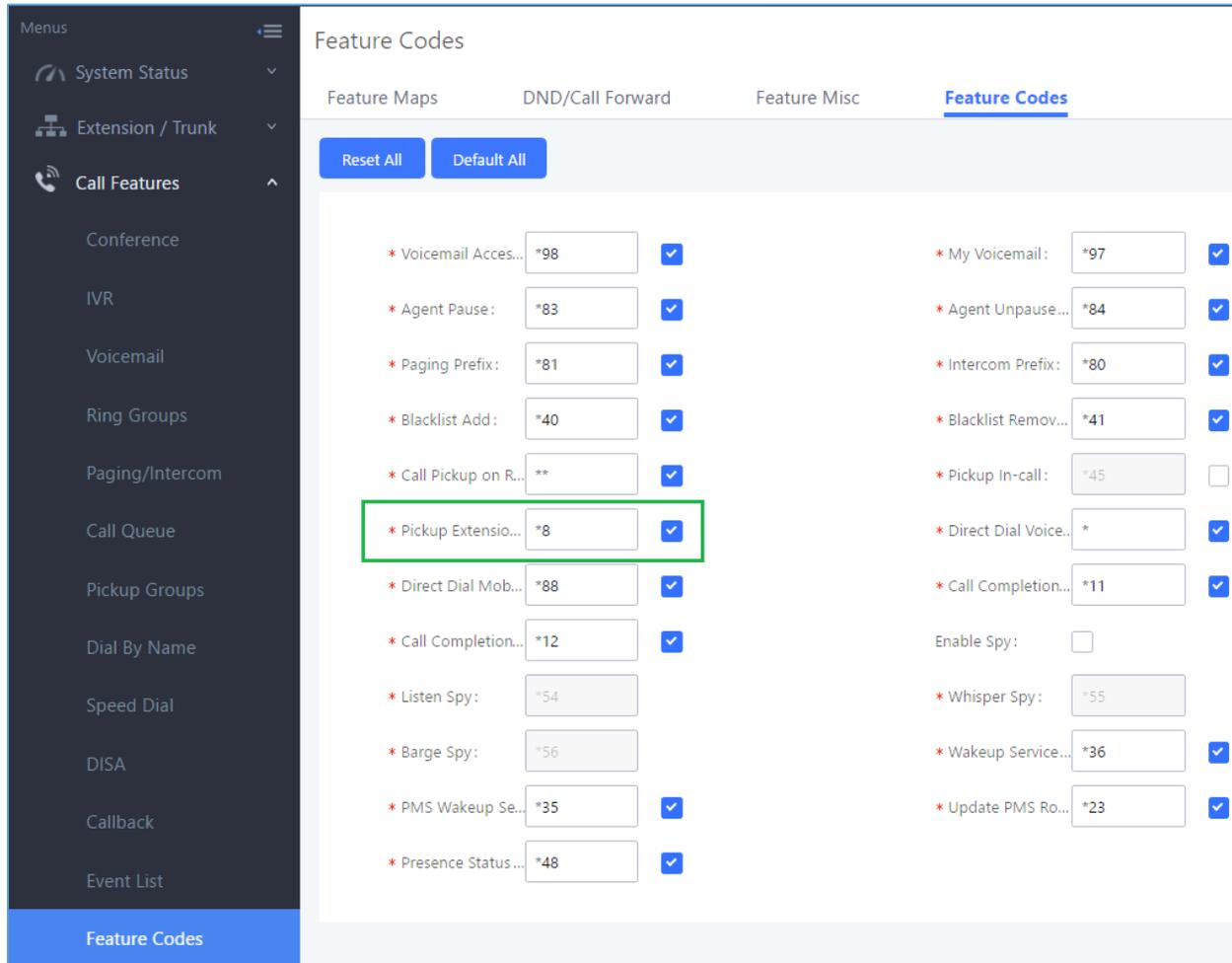
Figure 162: Edit Pickup Group

Configure Pickup Feature Code

When picking up the call for the pickup group member, the user only needs to dial the pickup feature code. It's not necessary to add the extension number after the pickup feature code. The pickup feature code is configurable under Web GUI → **Call Features** → **Feature Codes**.



The default pickup feature code is *8 as shown on the following screenshot.



The screenshot shows the 'Feature Codes' configuration page in the Grandstream interface. The left sidebar contains a 'Menus' section with 'Call Features' expanded. The main content area has tabs for 'Feature Maps', 'DND/Call Forward', 'Feature Misc', and 'Feature Codes' (which is selected). Below the tabs are 'Reset All' and 'Default All' buttons. A table of feature codes is displayed, with the 'Pickup Extension' row highlighted by a green box.

Feature Name	Code	Enabled
* Voicemail Acces...	*98	<input checked="" type="checkbox"/>
* Agent Pause:	*83	<input checked="" type="checkbox"/>
* Paging Prefix:	*81	<input checked="" type="checkbox"/>
* Blacklist Add:	*40	<input checked="" type="checkbox"/>
* Call Pickup on R...	**	<input checked="" type="checkbox"/>
* Pickup Extensio...	*8	<input checked="" type="checkbox"/>
* Direct Dial Mob...	*88	<input checked="" type="checkbox"/>
* Call Completion...	*12	<input checked="" type="checkbox"/>
* Listen Spy:	*54	<input type="checkbox"/>
* Barge Spy:	*56	<input type="checkbox"/>
* PMS Wakeup Se...	*35	<input checked="" type="checkbox"/>
* Presence Status ...	*48	<input checked="" type="checkbox"/>
* My Voicemail:	*97	<input checked="" type="checkbox"/>
* Agent Unpause...	*84	<input checked="" type="checkbox"/>
* Intercom Prefix:	*80	<input checked="" type="checkbox"/>
* Blacklist Remov...	*41	<input checked="" type="checkbox"/>
* Pickup In-call:	*45	<input type="checkbox"/>
* Direct Dial Voice...	*	<input checked="" type="checkbox"/>
* Call Completion...	*11	<input checked="" type="checkbox"/>
Enable Spy:		<input type="checkbox"/>
* Whisper Spy:	*55	<input type="checkbox"/>
* Wakeup Service...	*36	<input checked="" type="checkbox"/>
* Update PMS Ro...	*23	<input checked="" type="checkbox"/>

Figure 163: Edit Pickup Feature Code

PIN GROUPS

The UCM6510 supports pin group. Once this feature is configured, users can apply pin group to specific outbound routes. When placing a call on pin protected outbound routes, caller will be asked to input the group pin number, this feature can be found on the webGUI→**Extension/Trunk**→**Outbound Routes**→**PIN Groups**.

Table 85: PIN Group

Name	Specify the name of the group
Record In CDR	Specify whether to enable/disable record in CDR
PIN Number	Specify the code that will asked once dialing via a trunk
PIN Name	Specify the name of the PIN

Once user click on PIN Groups the following figure pop's up for configuring the new Pin.

Create New PIN Group
Save

* Name:

Record in CDR:

Members

* PIN Number:

* PIN Name:

✓ Save
✗ Cancel

PIN Number: 2020 PIN Name: John

✎
🗑️

Figure 164: Create New PIN Group

The following screenshot shows an example of created PIN Groups and members:



PIN Groups

[+ Add](#) [Choose file to upload](#)

Name	Record in CDR	Options
GSEMEA	yes	

PIN Number	PIN Name
2020	John
2025	Emily
3009	Jane

Figure 165: PIN members

Please note, if pin group is enabled on outbound route level, password, privilege level and enable filter on source caller ID will be disabled.

Edit Outbound Rule: National [Save](#)

* Calling Rule Name:	<input type="text" value="National"/>	* Pattern:	<input type="text" value="_xxxxxxxx"/>
Disable This Route:	<input type="checkbox"/>	PIN Groups:	<input type="text" value="GSEMEA"/>
Password:	<input type="text"/>	Privilege Level:	<input type="text" value="Disable"/>

Figure 166: Outbound PIN

If PIN group CDR is enabled, the call with pin group information will be displayed as part of CDR under Account Code field.

CDR

[Delete All](#) [Download All Records](#) [Download Search Result \(s\)](#) [Automatic Download Settings](#)

Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code
	1002	7946541 [Trunk: BranchOffice]	DIAL	2017-05-05 04:59:51	0:00:08	Emily/GSEMEA
	1002	7654654 [Trunk: BranchOffice]	DIAL	2017-05-05 04:59:12	0:00:06	Jane/GSEMEA
	1002	7564654 [Trunk: BranchOffice]	DIAL	2017-05-05 04:58:38	0:00:06	John/GSEMEA

Figure 167: CDR Record



MUSIC ON HOLD

Music On Hold settings can be accessed via Web GUI→**PBX Settings**→**Music On Hold**. In this page, users could configure music on hold class and upload music files. The "default" Music On Hold class already has 5 audio files defined for users to use.

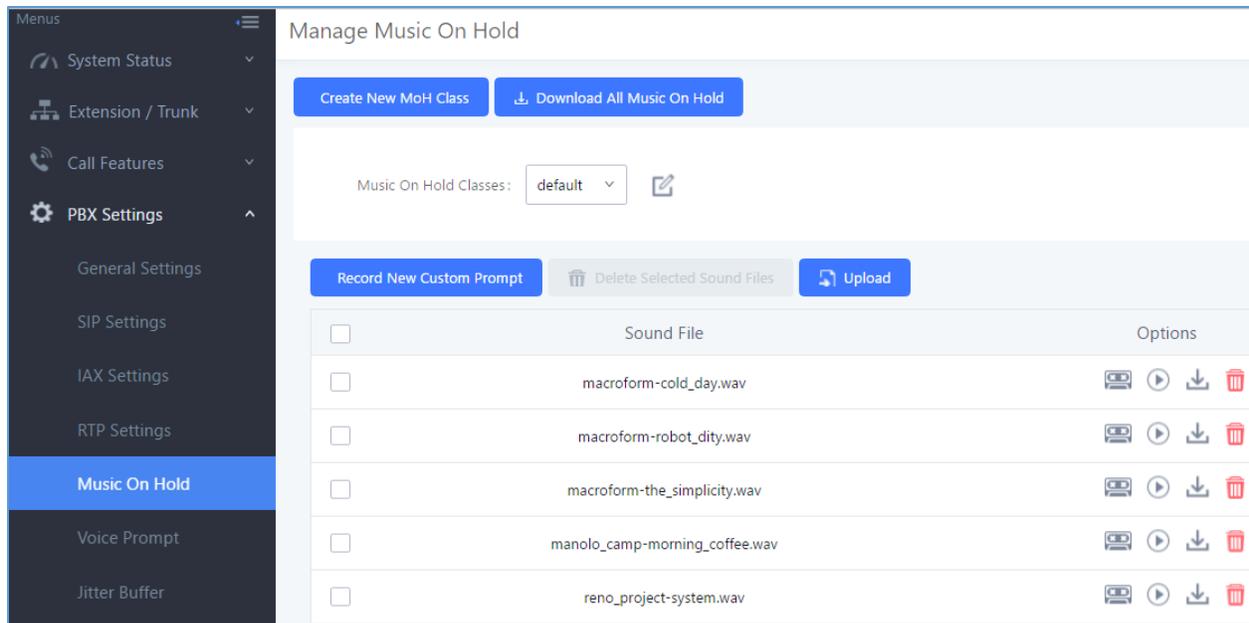
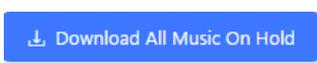


Figure 168: Music On Hold Default Class

- Click on "Create New MOH Class" to add a new Music On Hold class.
- Click on  to configure the MOH class sort method to be "Alpha" or "Random" for the sound files.
- Click on  next to the selected Music On Hold class to delete this Music On Hold class.
- Click on  to start uploading. Users can upload:
 - Single files with 8KHz Mono Music file, or
 - Music on hold files in a compressed package with .tar, .tar.gz and .tgz as the suffix. The file name can only be letters, digits or special characters - _
 - the size for the uploaded file should be less than 30M, the compressed file will be applied to the entire MoH.
- Users could also download all the music on hold files from UCM. In the Music On Hold page, click on  and the file will be downloaded to your local PC.



- Click on  next to the sound file to delete it from the selected Music On Hold Class.
- Select the sound files and click on  to delete all selected music on hold files.

The UCM6510 allows Users to select the Music on Hold file from WebGUI to play it. The UCM6510 will initiate a call to the selected extension and play this Music on Hold file once the call is answered.

Steps to play the music on hold file:

1. Click on the  button for the Music on Hold file.
2. In the prompted window, select the extension to playback and click .

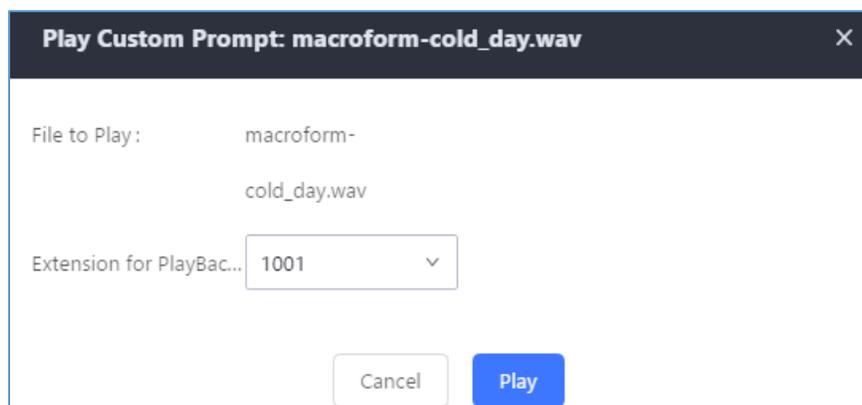


Figure 169: Play Custom Prompt

3. The selected extension will ring.
4. Answer the call to listen to the music playback.

Users could also record their own Music on hold to override an existing custom prompt, this can be done by following those steps:

1. Click on .
2. A prompt of confirmation will pop up, as shown below.

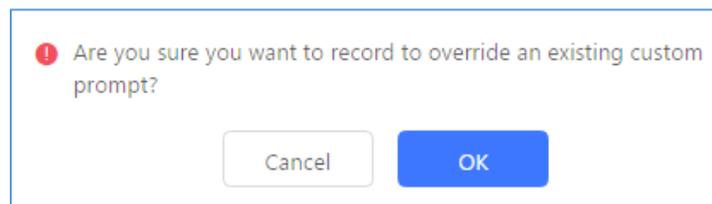


Figure 170: Information Prompt

3. Click .



4. In the prompted window, select the extension to playback and click .

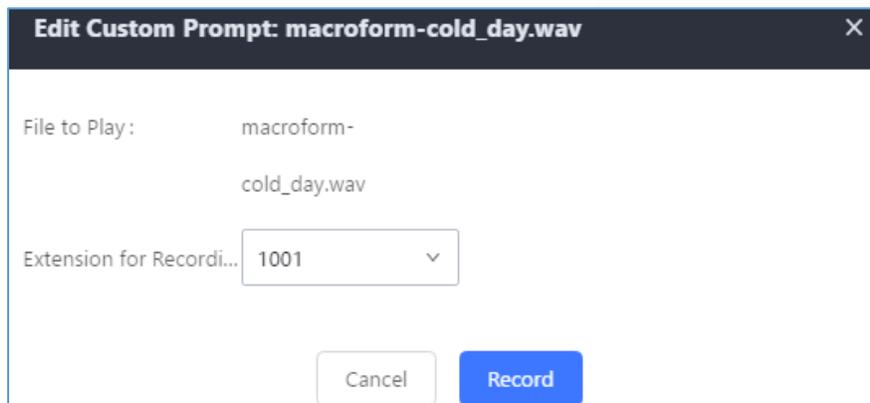


Figure 171: Record Custom Prompt

5. Answer the call and start to record your new music on hold.
6. Hangup the call and refresh Music On Hold page then you can listen to the new recorded file.

 **Note:**

In case the users have deleted the system MOH files, there are two ways to recover.

1. Users could download the MOH file from this link:

<http://downloads.asterisk.org/pub/telephony/sounds/releases/asterisk-moh-opsound-wav-2.03.tar.gz>

After downloading, unzip the pack and upload the music files to the UCM6510.

2. Factory reset could also recover the MOH file on the UCM.
-



FAX SERVER

The UCM6510 supports T.30/T.38 Fax and Fax Pass-through. It can also convert the received Fax to PDF format and send it to the configured Email address. Fax/T.38 settings can be accessed via Web GUI→**Call Features**→**Fax/T.38**.

Configure Fax/T.38

- Click on "Create New Fax Extension". In the popped-up window, fill the extension, name and Email address to send the received Fax to.
- Click on "Fax Settings" to configure the Fax parameters.
- Click on  to edit the Fax extension.
- Click on  to delete the Fax extension.

Fax Settings

* Enable Error Correction Mode:

* Maximum Transfer Rate:

* Minimum Transfer Rate:

* Max Concurrent Sending Fax:

* Fax Queue Length:

Fax Header Information:

Default Email Address: [Email](#)

[Template](#)

Figure 172: Fax Settings

Table 86: FAX/T.38 Settings

Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is "Yes".
-------------------------------------	--



Maximum Transfer Rate	Configure the maximum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14400. The default setting is 14400.
Minimum Transfer Rate	Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14000. The default setting is 2400.
Max Concurrent Sending Fax	Configure the concurrent fax that can be sent by UCM6510. <ul style="list-style-type: none"> • Only mode supports single user fax sending • More mode supports multiple concurrent fax sending By default, this option is set to “only”.
Fax Queue Length	Configure the maximum length of Fax Queue.
Fax Header Information	Adds fax header into the fax file.
Default Email Address	Configure the Email address to send the received Fax to if user's Email address cannot be found. Note: The extension's Email address or the Fax's default Email address needs to be configured in order to receive Fax from Email. If neither of them is configured, Fax will not be received from Email.
Template Variables	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users. The template variables are: <ul style="list-style-type: none"> • \${CALLERIDNUM} : Caller ID Number • \${CALLERIDNAME} : Caller ID Name • \${RECEIVEEXTEN} : The extension to receive the Fax • \${FAXPAGES} : Number of pages in the Fax • \${VM_DATE} : The date and time when the Fax is received

Receiving FAX

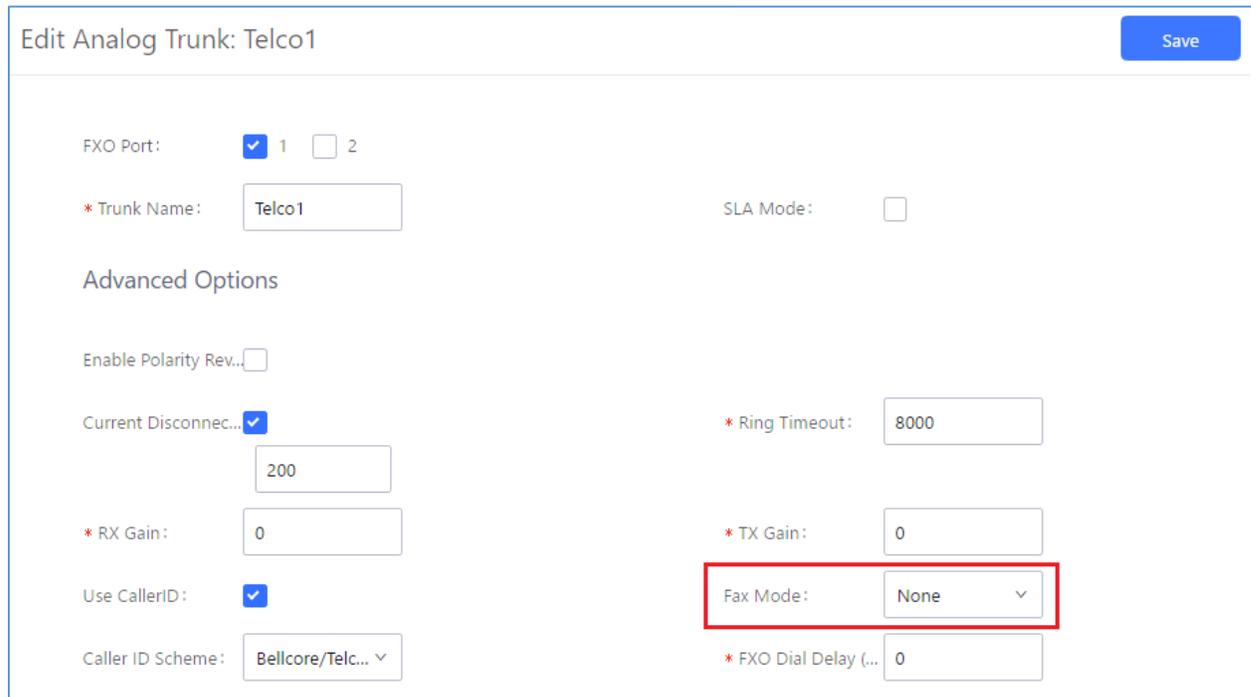
Sample Configuration to Receive Fax from PSTN Line

The following instructions describe how to use the UCM6510 to receive Fax from PSTN line on the Fax machine connected to the UCM6510 FXS port.

1. Connect Fax machine to the UCM6510 FXS port.
2. Connect PSTN line to the UCM6510 FXO port.
3. Go to Web GUI→**Extension/Trunk** page.
4. Create or edit the analog trunk for Fax as below.



Fax Detection: Make sure "Fax Detection" option is set to "No".



Edit Analog Trunk: Telco1 Save

FXO Port: 1 2

* Trunk Name: SLA Mode:

Advanced Options

Enable Polarity Rev...

Current Disconnec...

* Ring Timeout:

* RX Gain:

* TX Gain:

Use CallerID:

Fax Mode:

Caller ID Scheme:

* FXO Dial Delay (...

Figure 173: Configure Analog Trunk without Fax Detection

5. Go to UCM6510 Web GUI → **Extension/Trunk** → **Extensions** page.
6. Create or edit the extension for FXS port.
 - **Analog Station:** Select FXS port to be assigned to the extension. By default, it's set to "None".
 - Once selected, analog related settings for this extension will show up in "**Analog Settings**" section.



Create New Extension Save

Basic Settings Media Features Specific Time Follow Me

* Select Extension Type: FXS Extension

Select Add Method: Single

General

* Extension: 500 Analog Station: FXS 1

CallerID Number: * Permission: Internal

Enable Voicemail: * Voicemail Password: 5682659

Skip Voicemail Passwo... Disable This Extension ...

Figure 174: Configure Extension For Fax Machine

Create New Extension Save

Basic Settings **Media** Features Specific Time Follow Me

Analog Settings

Call Waiting: Use "#" as SEND:

* RX Gain: 0 * TX Gain: 0

* MIN RX Flash: 200 * MAX RX Flash: 1250

Enable Polarity Reversal: * Echo Cancellation: ON

3-way Calling: * Send CallerID After: 1

* Fax Mode: Fax Gateway

None

Fax Detection

Fax Gateway

Figure 175: Configure Extension for Fax Machine: Analog Settings

7. Go to Web GUI→**Extension/Trunk**→**Inbound Routes** page.
8. Create an inbound route to use the Fax analog trunk. Select the created extension for Fax machine in step 4 as the default destination.



Create New Inbound Rule
Save

* Trunks:

CallerID Pattern:

Prepend Trunk Name:

Inbound Multiple Mode...

Dial Trunk:

DID Destination:

* Pattern:

Disable This Route:

Prepend User Defined N...

Alert-info:

Privilege Level:

Allowed to seamless tran...

Default Mode

* Default Destination:

Figure 176: Configure Inbound Rule for Fax

Now the Fax configuration is done. When there is an incoming Fax calling to the PSTN number for the FXO port, it will send the Fax to the Fax machine.

Sample Configuration for Fax-To-Email

The following instructions describe a sample configuration on how to use Fax-to-Email feature on the UCM6510.

1. Connect PSTN line to the UCM6510 FXO port.
2. Go to UCM6510 Web GUI→**Internal Options**→**Fax/T.38** page. Create a new Fax extension.

Create New Fax Extension

* Extension:

* Name:

* Email Address:

Figure 177: Create Fax Extension



3. Go to UCM6510 Web GUI→**Extension/Trunk**→**Analog Trunks** page. Create a new analog trunk with "FAX Detection" set to "No".
4. Go to UCM6510 Web GUI→**Extension/Trunk**→**Inbound Routes** page. Create a new inbound route and set the default destination to the Fax extension.

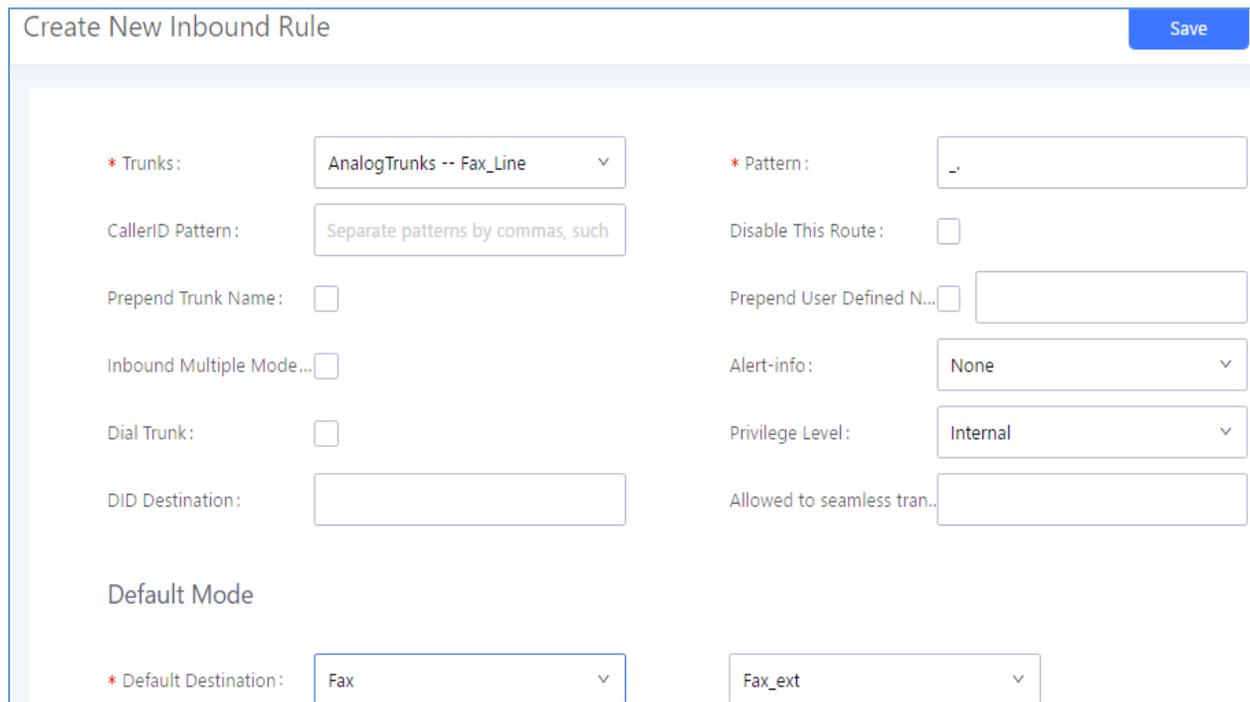


Figure 178: Inbound Route to Fax Extension

5. Once successfully configured, the incoming Fax from external Fax machine to the PSTN line number will be converted to PDF file and sent to the Email address **fax@domain.local** as attachment.

Fax Sending

The UCM6510 supports sending Fax via Web GUI access. This feature can be found on Web GUI→**Value-added Features**→**Fax Sending** page. In order to send fax, pre-setup for analog trunk and outbound route is required.

After making sure analog trunk or VoIP Trunk is setup properly and UCM6510 can reach out to PSTN numbers via the trunk, on Fax Sending page, enter the fax number and upload the file to be faxed. Then click on "Send" to start. The progress of sending fax will be displayed in Web GUI. Users can also view the sending history is in the same web page.



Fax Sending

* External Fax Number:

Fax File:

File Send Progress

Figure 179: Fax Sending in Web GUI



BUSY CAMP-ON

The UCM6510 supports busy camp-on/call completion feature that allows the PBX to camp on a called party and inform the caller as soon as the called party becomes available given the previous attempted call has failed.

The configuration and instructions on how to use busy camp-on/call completion feature can be found in the following guide:

http://www.grandstream.com/sites/default/files/Resources/ucm6xxx_busy_camp_on_guide.pdf



PRESENCE

UCM does support SIP presence feature which allows users to advertise their current availability status and willingness to receive calls, this way other users can use their phones in order to monitor the presence status of each user and decide whether to call them or not based on their advertised availability.

This feature is different than BLF which is mainly used to monitor the dialog status for each extension (Ringing, Idle or Busy). Instead the SIP presence module gives more options for users to choose which state they want to put themselves in.

In order to configure the presence status of an extension from the web GUI, users can access the menu of configuration using one of the two following methods:

- From admin account, go under the menu **Extension/Trunk→Extensions** and choose the desired extension to edit then navigate to the “Features” tab.

OR

- From the User Portal, go under the menu Basic **Information→Extensions** and navigate to the Features tab to have the following options.

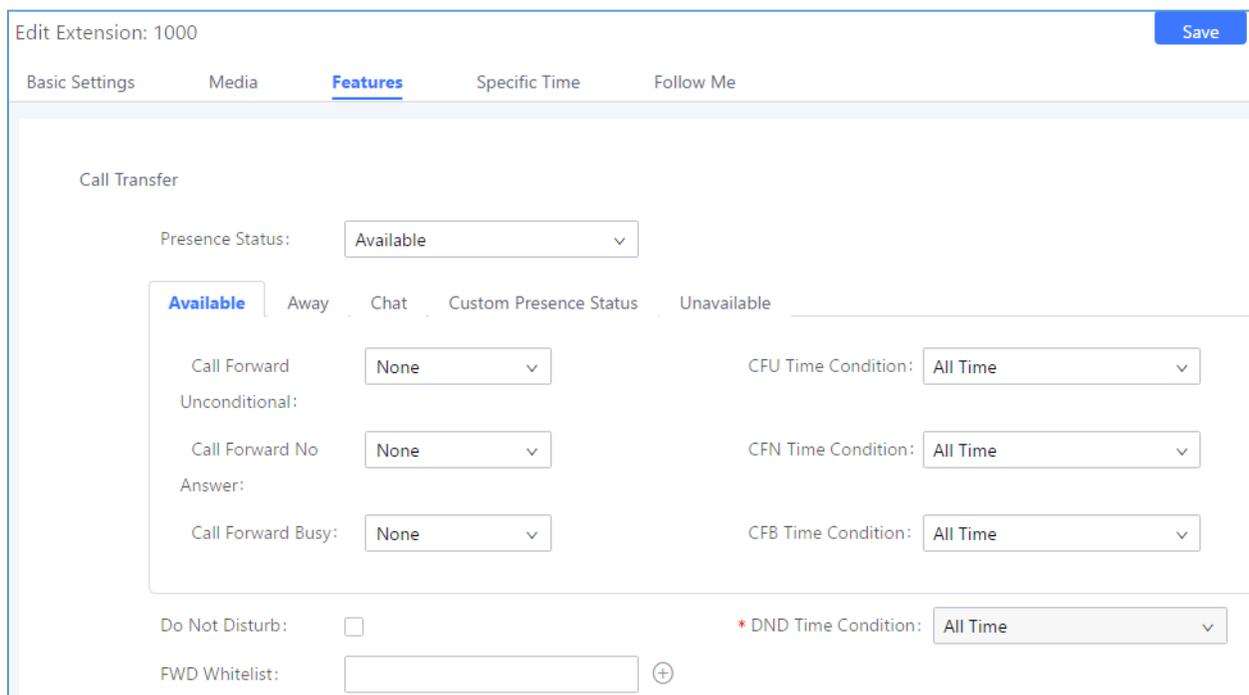


Figure 180 shows the 'Edit Extension: 1000' configuration page with the 'Features' tab selected. The 'Presence Status' is set to 'Available'. Below this, there are tabs for 'Available', 'Away', 'Chat', 'Custom Presence Status', and 'Unavailable'. Under the 'Available' tab, there are three call forwarding options: 'Call Forward Unconditional', 'Call Forward No Answer', and 'Call Forward Busy', each with a 'None' dropdown and a 'Time Condition' dropdown set to 'All Time'. There is also a 'Do Not Disturb' checkbox (unchecked) and a 'DND Time Condition' dropdown set to 'All Time'. At the bottom, there is a 'FWD Whitelist' input field with a plus sign icon.

Figure 180: SIP Presence Configuration

Select which status to set from the presence status selection drop list, six options are available and below is a brief description of these states:

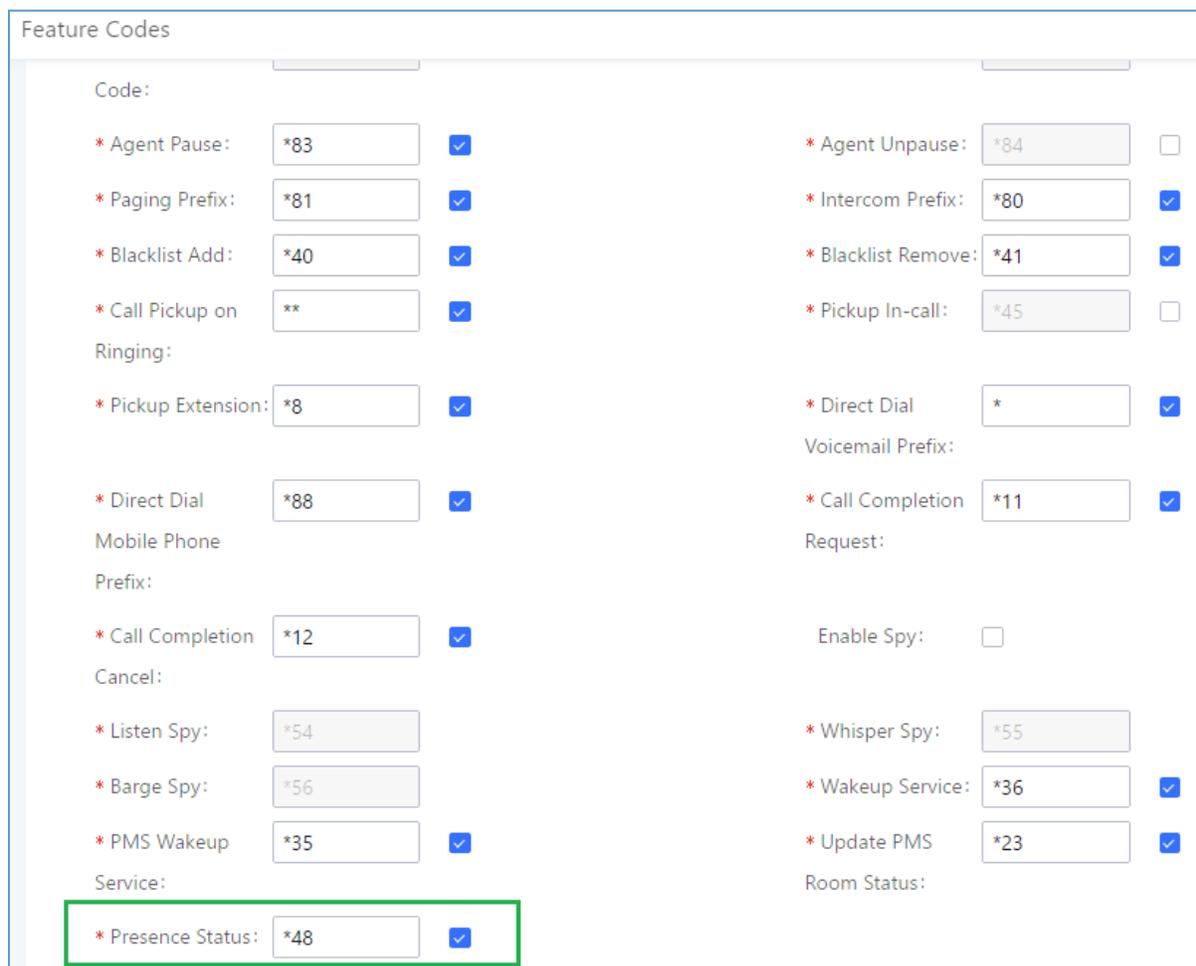


Table 87: SIP Presence Status

Available	The contact is online and can participate in conversations/phone calls.
Away	The contact is currently away (ex: for lunch break).
Chat	The contact has limited conversation flexibility and can only be reached via chat.
Do Not Disturb	The Contact is on DND (Do Not Disturb) mode.
Custom Presence Status	Please enter the presence status for this mode on the Web GUI.
Unavailable	The contact is unreachable for the moment, please try to contact later.

Another option to set the presence status and which is more practical is using the feature code from the user's phone, one the user dials the feature code (default is *48), a prompt will be played to select which status they want to put themselves in by pressing the corresponding key.

The feature code can be enabled/customized from the Web GUI → **Call Features** → **Feature Codes**.



Feature Codes

Code:

* Agent Pause:	<input type="text" value="*83"/>	<input checked="" type="checkbox"/>	* Agent Unpause:	<input type="text" value="*84"/>	<input type="checkbox"/>
* Paging Prefix:	<input type="text" value="*81"/>	<input checked="" type="checkbox"/>	* Intercom Prefix:	<input type="text" value="*80"/>	<input checked="" type="checkbox"/>
* Blacklist Add:	<input type="text" value="*40"/>	<input checked="" type="checkbox"/>	* Blacklist Remove:	<input type="text" value="*41"/>	<input checked="" type="checkbox"/>
* Call Pickup on Ringing:	<input type="text" value="**"/>	<input checked="" type="checkbox"/>	* Pickup In-call:	<input type="text" value="*45"/>	<input type="checkbox"/>
* Pickup Extension:	<input type="text" value="*8"/>	<input checked="" type="checkbox"/>	* Direct Dial	<input type="text" value="*"/>	<input checked="" type="checkbox"/>
* Direct Dial	<input type="text" value="*88"/>	<input checked="" type="checkbox"/>	Voicemail Prefix:		
Mobile Phone Prefix:			* Call Completion	<input type="text" value="*11"/>	<input checked="" type="checkbox"/>
* Call Completion	<input type="text" value="*12"/>	<input checked="" type="checkbox"/>	Request:		
Cancel:			Enable Spy:	<input type="checkbox"/>	
* Listen Spy:	<input type="text" value="*54"/>		* Whisper Spy:	<input type="text" value="*55"/>	
* Barge Spy:	<input type="text" value="*56"/>		* Wakeup Service:	<input type="text" value="*36"/>	<input checked="" type="checkbox"/>
* PMS Wakeup	<input type="text" value="*35"/>	<input checked="" type="checkbox"/>	* Update PMS	<input type="text" value="*23"/>	<input checked="" type="checkbox"/>
Service:			Room Status:		
* Presence Status:	<input type="text" value="*48"/>	<input checked="" type="checkbox"/>			

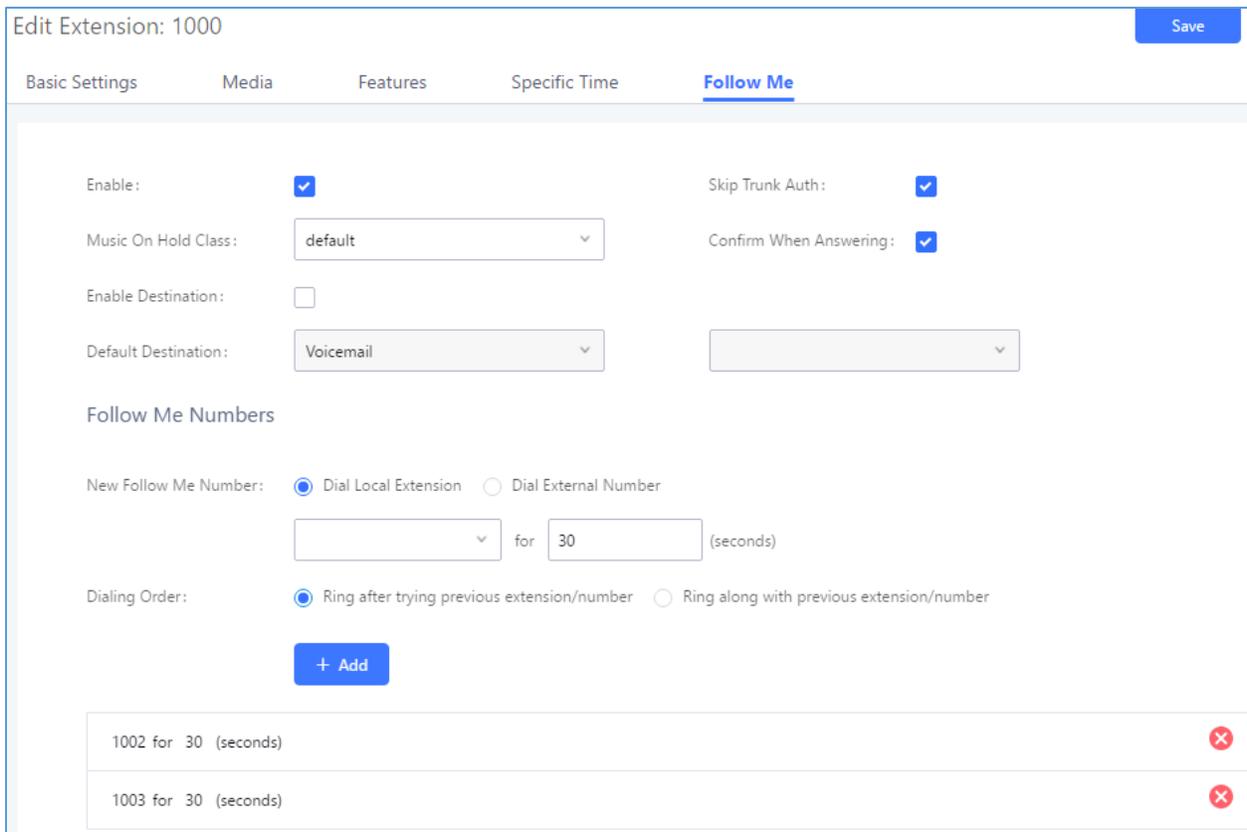
Figure 181: SIP Presence Feature Code


FOLLOW ME

UCM supports Follow Me feature which allows users to direct calls to other phone numbers and have them ring all at once or one after the other. Calls can be directed to users' home phone, office phone, mobile and etc. The calls will get to the user no matter where they are. Follow Me option can be found under extension settings page Web GUI→**Extension/Trunk**→**Extensions**.

To configure follow me:

1. Choose the extension and click on .
2. Go to the Follow me tab to add destination numbers and enable the feature.



Edit Extension: 1000 Save

Basic Settings Media Features Specific Time **Follow Me**

Enable: Skip Trunk Auth:

Music On Hold Class: default Confirm When Answering:

Enable Destination:

Default Destination: Voicemail

Follow Me Numbers

New Follow Me Number: Dial Local Extension Dial External Number

for 30 (seconds)

Dialing Order: Ring after trying previous extension/number Ring along with previous extension/number

1002 for 30 (seconds)	<input type="button" value="X"/>
1003 for 30 (seconds)	<input type="button" value="X"/>

Figure 182: Edit Follow Me

3. Click on “Add Follow Me Number” to add local extensions or external numbers to be called after ringing the extension selected in the first step.
4. Once created, it will be displayed on the follow me web page list. Click on  to edit the Follow Me configuration. Click on  to delete the Follow Me.



The following table shows the Follow Me configuration parameters.

Table 88: Follow Me Settings

Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If external number is added in the Follow Me, please make sure this option is enabled or the “Skip Trunk Auth” option of the extension is enabled, otherwise the external Follow Me number cannot be reached.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	By default, it is enabled and user will be asked to press 1 to accept the call or to press 2 to reject the call after answering a Follow Me call. If it is disabled, the Follow Me call will be established once after the user answers it.
Enable Destination	If enabled, the call will be routed to the default destination if no one in the Follow Me answers the call.
Default Destination	Configure the destination if no one in the Follow Me answers the call, available options are: <ul style="list-style-type: none"> • Extension • Voicemail • Queues • Ring Group • Voicemail Group • IVR • External Number
Follow Me Numbers	The added numbers are listed here. Click on   to arrange the order. Click on  to delete the number. Click on  to add new numbers.
New Follow Me Number	Add a new Follow Me number which could be a ‘Local Extension’ or ‘External Number’. The selected dial plan should have permissions to dial the defined external number.
Dialing Order	Select the order in which the Follow Me destinations will be dialed to reach the user: ring all at once or ring one after the other.

Click on “Follow Me Options” under Web GUI→**Extension/Trunk**→**Extension** page to enable or disable the options listed in the following table.



Table 89: Follow Me Options

Playback Incoming Status Message	If enabled, the PBX will playback the incoming status message before starting the Follow Me steps.
Record the Caller's Name	If enabled, the PBX will record the caller's name from the phone so it can be announced to the callee in each step.
Playback Unreachable Status Message	If enabled, the PBX will playback the unreachable status message to the caller if the callee cannot be reached.

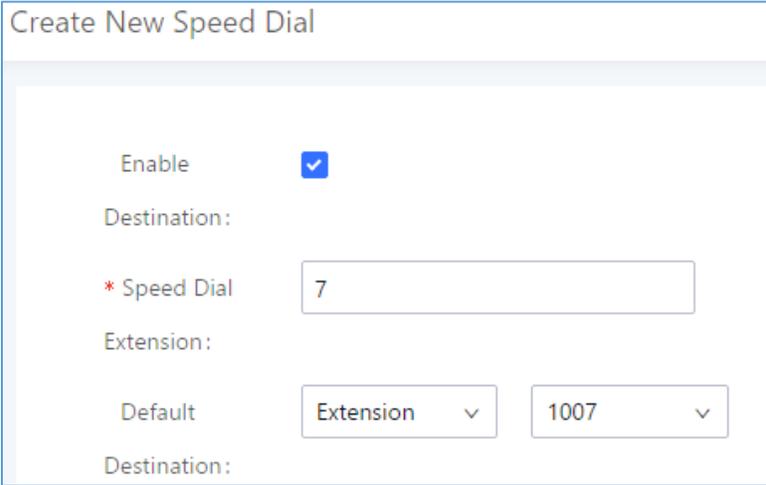


SPEED DIAL

The UCM6510 supports Speed Dial feature that allows users to call a certain destination by pressing one or two digits on the keypad allowing 99 extensions to be configured. This creates a system-wide speed dial access for all the extensions on the UCM6510.

To enable Speed Dial, on the UCM6510 Web GUI, go to page Web GUI→**Call Features**→**Speed Dial**.

User should first click on . Then decide a one digit or two digits used for Speed Dial and select a dial destination from “Default Destination”. The supported destinations include extension, voicemail, conference room, voicemail group, IVR, ring group, call queue, page group, fax, DISA, Dial by Name and external number.



Create New Speed Dial

Enable

Destination:

* Speed Dial

Extension:

Default

Destination:

Figure 183: Speed Dial Destinations



DISA

In many situations, the user will find the need to access his own IPPBX resources but he is not physically close to any one of his extensions. However, he does have access to his own cell phone. In this case, we can use what is commonly known as DISA (Direct Inward System Access). Under this scenario, the user will be able to call from the outside first, whether it's using his cell phone, pay phone, regular PSTN and etc, and then call into a SIP trunk or PSTN trunk connected to UCM6510 as it is an internal extension.

The UCM6510 supports DISA to be used in IVR or inbound route. Before using it, create new DISA under Web GUI→**Call Features**→**DISA**.

- Click on "Create New DISA" to add a new DISA.
- Click on  to edit the DISA configuration.
- Click on  to delete the DISA.

Create New DISA

* Name:

* Password:

Permission: Internal ▼

* Response Timeout...:

* Digit Timeout:

Allow Hang-up:

Replace Display Nam...:

Figure 184: Create New DISA

Table 90: DISA Settings

Name	Configure DISA name to identify the DISA.
Password	Configure the password (digit only) required for the user to enter before using DISA to dial out. Note: The password has to be at least 4 digits.



Permission	Configure the permission level for DISA. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the DISA, the UCM6510 will compare the DISA's permission level with the outbound route's privilege level. If the DISA's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Response Timeout	Configure the maximum amount of time the UCM6510 will wait before hanging up if the user dials an incomplete or invalid number. The default setting is 10 seconds.
Digit Timeout	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
Allow Hangup	If enabled, during an active call, users can enter the UCM6510 Hangup feature code (*0 by default) to disconnect the call or hang up directly. A new dial tone will be heard shortly for the user to make a new call. The default setting is "No".
Replace Display Name	If enabled, the UCM will replace the caller display name with the DISA name.

Once successfully created, users can configure the inbound route destination as "DISA" or IVR key event as "DISA". When dialing into DISA, users will be prompted with password first. After entering the correct password, a second dial tone will be heard for the users to dial out.



CALLBACK

Callback is mainly designed for users who often use their mobile phones to make long distance or international calls which may have high service charges. The callback feature provides an economic solution for reduce the cost from this.

The callback feature works as follows:

1. Configure a new callback on the UCM6510.
2. On the UCM6510, configure destination of the inbound route for analog trunk to callback.
3. Save and apply the settings.
4. The user calls the PSTN number of the UCM6510 using the mobile phone, which goes to callback destination as specified in the inbound route.
5. Once the user hears the ringback tone from the mobile phone, hang up the call on the mobile phone.
6. The UCM6510 will call back the user.
7. The user answers the call.
8. The call will be sent to DISA or IVR which directs the user to dial the destination number.
9. The user will be connected to the destination number.

In this way, the calls are placed and connected through trunks on the UCM6510 instead of to the mobile phone directly. Therefore, the user will not be charged on mobile phone services for long distance or international calls.

To configure callback on the UCM6510, go to Web GUI→**Call Features**→**Callback** page and click on

 **+ Create New Callback**

. Configuration parameters are listed in the following table.

Table 91: Callback Configuration Parameters

Name	Configure a name to identify the Callback.
CallerID Pattern	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the CallerID match this pattern so that the caller can get callback after hanging up the call. Note: If leaving as blank, all numbers are allowed to use this callback.



Outbound Prepend	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.
Delay Before Callback	Configure the number of seconds to be delayed before calling back the user.
Destination	Configure the destination which the callback will direct the caller to. Two destinations are available: <ul style="list-style-type: none">• IVR• DISA The caller can then enter the desired number to dial out via UCM6510.



BLF AND EVENT LIST

BLF

The UCM6510 supports BLF monitoring for extensions, ring group, call queue, conference room and parking lot. For example, on the user's phone, configure the parking lot number 701 as the BLF monitored number. When there is a parked call on 701, the LED for this BLF key will light up in red, meaning a call is parked against this parking lot. Pressing this BLF key can pick up the call from this parking lot.

 **Note:**

- On the Grandstream GXP phones, the MPK supports "Call Park" mode, which is normally used to park the call by configuring the MPK number as call park feature code (e.g., 700). Users could also use "Call Park" mode to monitor and pick up the call on this parking lot by configuring the MPK number as parking lot number (e.g., 701).

Event List

Besides BLF, users can also configure the phones to monitor event list. By using event list, local extensions on the same UCM6510 or remote extensions on the VOIP trunk can be monitored. The event list settings are under Web GUI→**Call Features**→**Event List**.

- Click on "Create New Event List" to add a new event list.
- Sort selected extensions manually in the Eventlist.
- Click on  to edit the event list configuration.
- Click on  to delete the event list.



Create New Event List

* URI:

Event Type:

Local Extensions:

Available Extensions/Extension Groups
 1000 "John DOE"
 1001
 1002
 1003
 1004

Selected Extensions/Extension Groups

Not Found

Remote Extensions:

1 Available Extensions
 GSEMEA--1002 "1002"

0 Selected Extensions

Not Found

Special Extensions:

Figure 185: Create New Event List

Table 92: Event List Settings

URI	Configure the name of this event list (for example, office_event_list). Please note the URI name cannot be the same as the extension name on the UCM6510. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions listed on the local UCM6510 to be monitored in the event list.
Remote Extensions	If LDAP sync is enabled between the UCM6510 and the peer UCM6510, the remote extensions will be listed under "Available Extensions". If not, manually enter the remote extensions under "Special Extensions" field.
Special Extensions	Manually enter the remote extensions in the peer/register trunk to be monitored in the event list. Valid format: 5000,5001,9000



Remote extension monitoring works on the UCM6510 via event list BLF, among Peer SIP trunks or Register SIP trunks (register to each other). Therefore, please properly configure SIP trunks on the UCM6510 first before using remote BLF feature. Please note the SIP end points need support event list BLF in order to monitor remote extensions.

When an event list is created on the UCM6510 and remote extensions are added to the list, the UCM6510 will send out SIP SUBSCRIBE to the remote UCM6510 to obtain the remote extension status. When the SIP end points register and subscribe to the local UCM6510 event list, it can obtain the remote extension status from this event list.

Once successfully configured, the event list page will show the status of total extension and subscribers for each event list. Users can also select the event URI to check the monitored extension's status and the subscribers' details.

 **Note:**

- To configure LDAP sync, please go to UCM6510 Web GUI→**Extension/Trunk**→**VoIP Trunk**. You will see "Sync LDAP Enable" option. Once enabled, please configure password information for the remote peer UCM6510 to connect to the local UCM6510. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM6510 and remote UCM6510 need enable LDAP sync option with the same password for successful connection and synchronization.
 - Currently LDAP sync feature only works between two UCM6510s.
 - (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM6510 PBX. However, it might not work the other way around depending on whether the non-UCM6510 PBX supports event list BLF or remote monitoring feature.
-

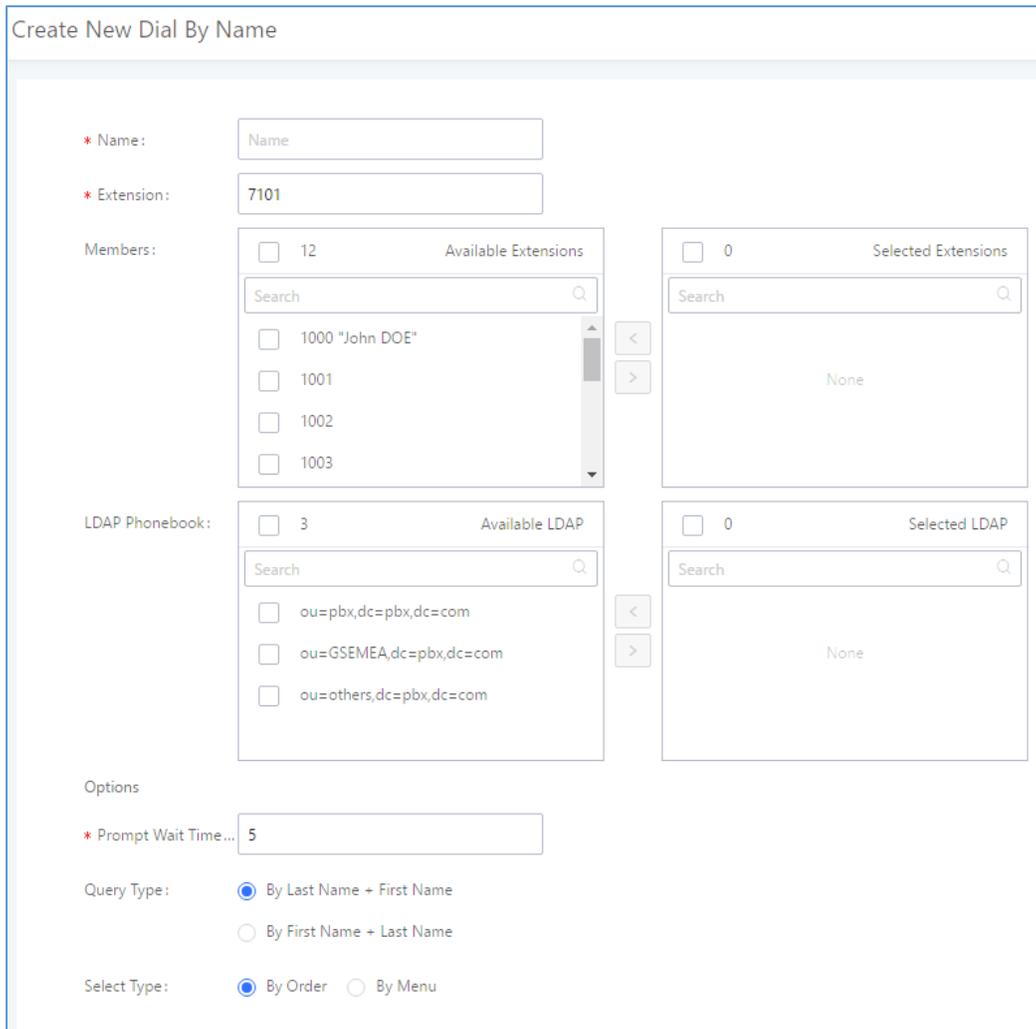


DIAL BY NAME

Dial By Name is a feature on the PBX that allows caller to search a person by first or last name via his/her phone's keypad. The administrator can define the Dial By Name directory including the desired extensions in the directory and the searching type by "first name" or "last name". After dialing in, the PBX IVR/Auto Attendant will guide the caller to spell the digits to find the person in the Dial By Name directory. This feature allows customers/clients to use the guided automatic system to get in touch with the enterprise employees without having to know the extension number, which brings convenience and improves business image for the enterprise.

Dial By Name Configuration

The administrators can create the dial by name group under Web GUI→**Call Features**→**Dial By Name**.



The screenshot shows the 'Create New Dial By Name' configuration page. It includes the following fields and options:

- Name:** A text input field containing the word 'Name'.
- Extension:** A text input field containing the number '7101'.
- Members:** A section with a count of '12' under 'Available Extensions'. It contains a search bar and a list of extensions: '1000 "John DOE"', '1001', '1002', and '1003'. To the right is a 'Selected Extensions' box with a count of '0' and the text 'None'.
- LDAP Phonebook:** A section with a count of '3' under 'Available LDAP'. It contains a search bar and a list of LDAP entries: 'ou=pbx,dc=pbx,dc=com', 'ou=GSEMEA,dc=pbx,dc=com', and 'ou=others,dc=pbx,dc=com'. To the right is a 'Selected LDAP' box with a count of '0' and the text 'None'.
- Options:**
 - Prompt Wait Time...**: A text input field containing the number '5'.
 - Query Type:** Two radio button options: 'By Last Name + First Name' (which is selected) and 'By First Name + Last Name'.
 - Select Type:** Two radio button options: 'By Order' (which is selected) and 'By Menu'.

Figure 186: Create Dial By Name Group



User Settings

First Name: <input style="width: 80%;" type="text" value="John"/>	Last Name: <input style="width: 80%;" type="text" value="DOE"/>
Email Address: <input style="width: 80%;" type="text"/>	* User Password: <input style="width: 80%;" type="password" value="*****"/>
* Language: <input style="border-bottom: 1px solid #ccc; border-top: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc;" type="text" value="Default"/> v	* Concurrent Registration... <input style="width: 80%;" type="text" value="1"/>
Mobile Phone Number: <input style="width: 80%;" type="text"/>	

Figure 187: Configure Extension First Name and Last Name

1. Name

Enter a Name to identify the Dial By Name group.

2. Extension

Configure the direct dial extension for the Dial By Name group.

3. Available Extensions/Selected Extensions

Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have a valid first name and last name configured under Web GUI→**Extension/Trunk**→**Extensions** in order to be searchable in Dial By Name directory through IVR. By specifying the extensions here, the administrators can make sure unscreened calls will not reach the company employee if he/she doesn't want to receive them directly.

4. Prompt Wait Time

Configure “Prompt Wait Time” for Dial By Name feature. During Dial By Name call, the caller will need to input the first letters of First/Last name before this wait time is reached. Otherwise, timeout will occur and the call might hang up. The timeout range is between 3 and 60 seconds.

5. Query Type

Specify the query type. This defines how the caller will need to enter to search the directory.

By First Name: enter the first 3 digits of the first name to search the directory.

By Last Name: enter the first 3 digits of the last name to search the directory.

By Full Name: enter the first 3 digits of the first name or last name to search the directory.

6. Select Type

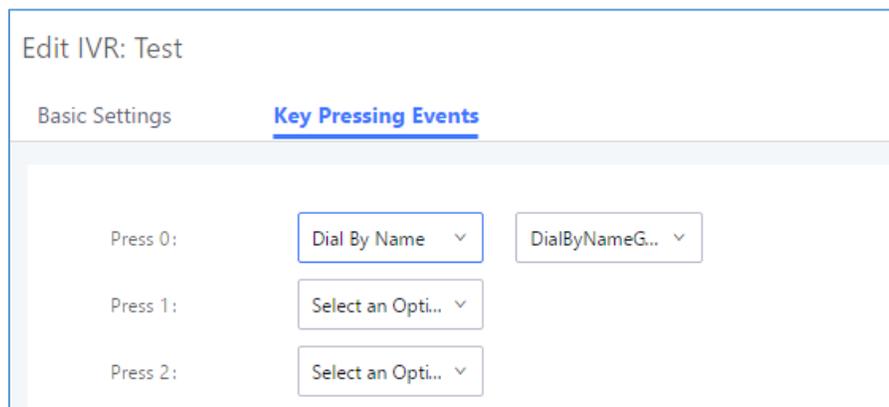
Specify the select type on the searching result. The IVR will confirm the name/number for the party the caller would like to reach before dialing out.



By Order: After the caller enters the digits, the IVR will announce the first matching party's name and number. The caller can confirm and dial out if it's the destination party, or press * to listen to the next matching result if it's not the desired party to call.

By Menu: After the caller enters the digits, the IVR will announce 8 matching results. The caller can press number 1 to 8 to select and call, or press 9 for results in next page.

The Dial By Name group can be used as the destination for inbound route and key pressing event for IVR. The group name defined here will show up in the destination list when configuring IVR and inbound route. If Dial By Name is set as a key pressing event for IVR, user could use "*" to exit from Dial By Name, then re-enter IVR and start a new event. The following example shows how to use this option.



Edit IVR: Test

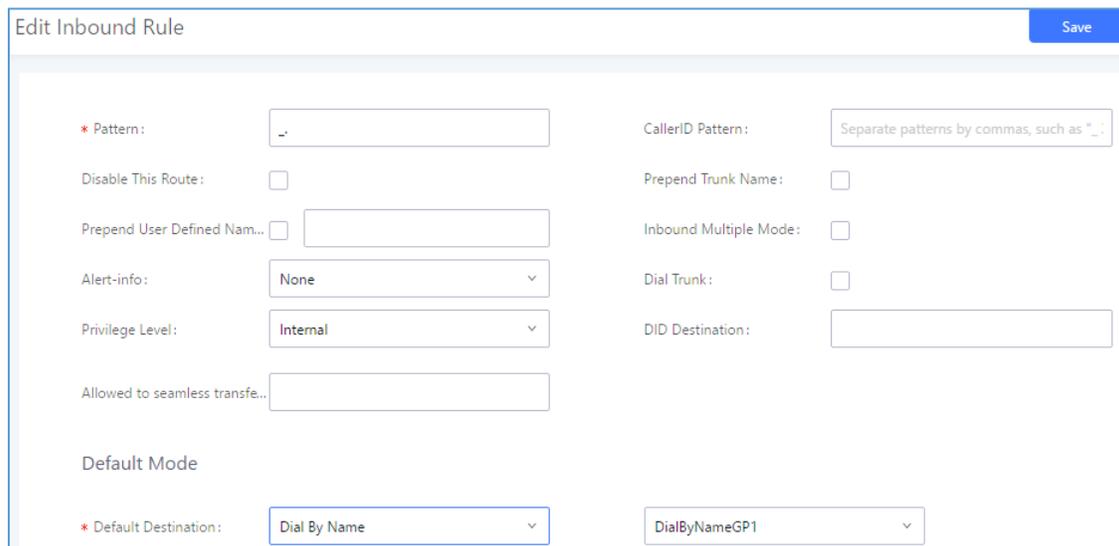
Basic Settings **Key Pressing Events**

Press 0: Dial By Name ▼ DialByNameG... ▼

Press 1: Select an Opti... ▼

Press 2: Select an Opti... ▼

Figure 188: Dial By Name Group In IVR Key Pressing Events



Edit Inbound Rule Save

* Pattern: - CallerID Pattern: Separate patterns by commas, such as " ":

Disable This Route:

Prepend Trunk Name:

Prepend User Defined Nam... Inbound Multiple Mode:

Alert-info: None ▼ Dial Trunk:

Privilege Level: Internal ▼ DID Destination:

Allowed to seamless transfe...

Default Mode

* Default Destination: Dial By Name ▼ DialByNameGP1 ▼

Figure 189: Dial By Name Group In Inbound Rule

ACTIVE CALLS AND MONITOR

The active calls on the UCM6510 are displayed in Web GUI→**System Status**→**Active Calls** page. Users can monitor call status, hang up active call(s) as well as barge in active call(s) in real time manner.

Active Calls Status

To view the status of active calls, navigate to Web GUI→**System Status**→**Active Calls**. The following figure shows extension 1002 is calling 1004. 1004 is ringing.

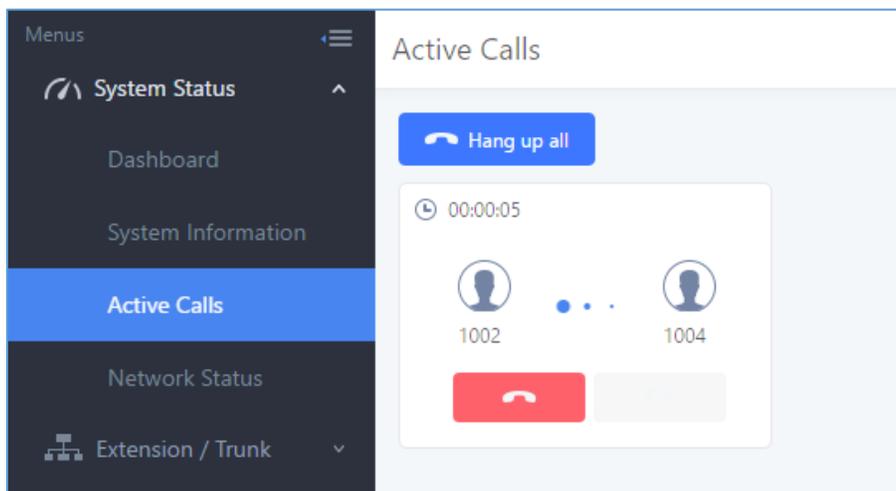


Figure 190: Status→PBX Status→Active Calls - Ringing

The following figure shows the call between 1002 and 1003 is established.

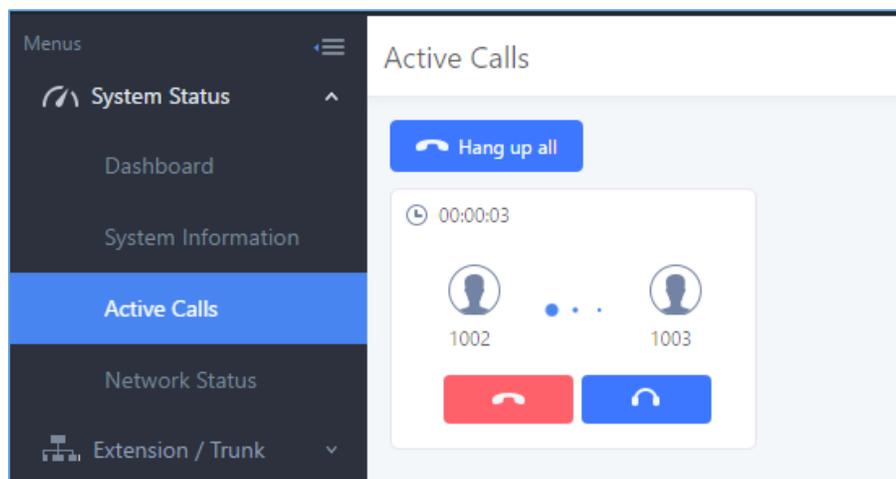


Figure 191: Status→PBX Status→Active Calls – Call Established



The green color of the active call means the connection of call time is less than half an hour. It means this call is normal.

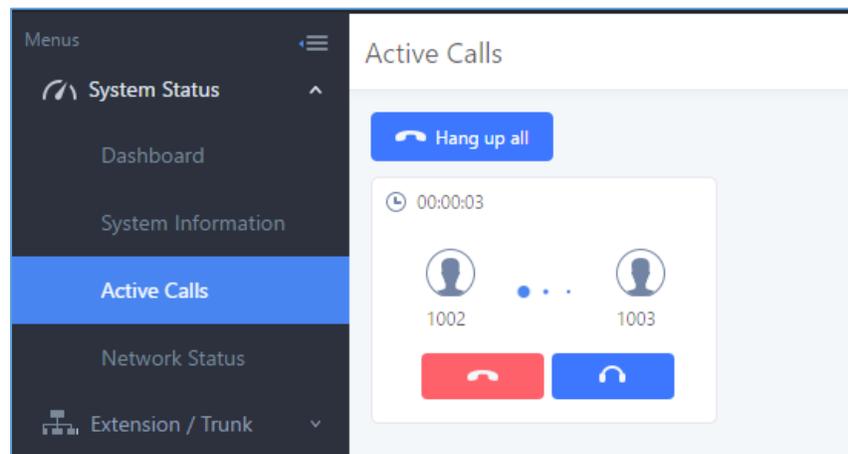


Figure 192: call connection less than half hour

The yellow color of the active call means the connection of call time is greater than half an hour but less than one hour. It means this call is a bit long.

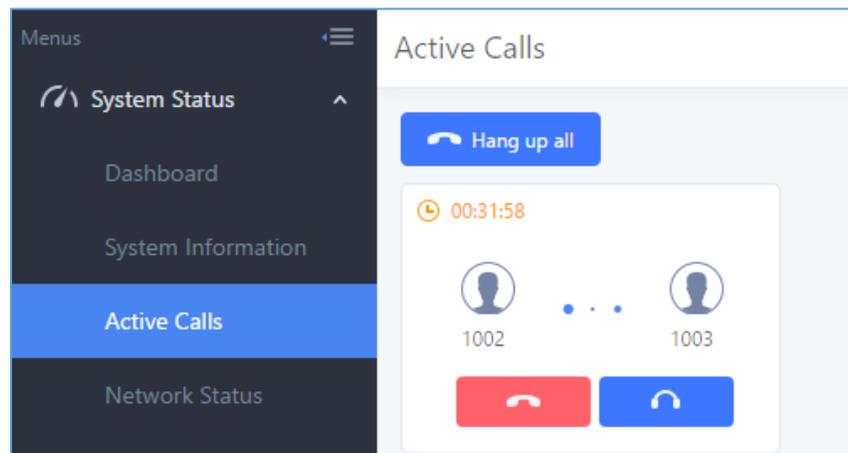


Figure 193: call connection between half an hour and one hour

The red color of the active call means the connection of call time is more than one hour. It means this call could be abnormal.



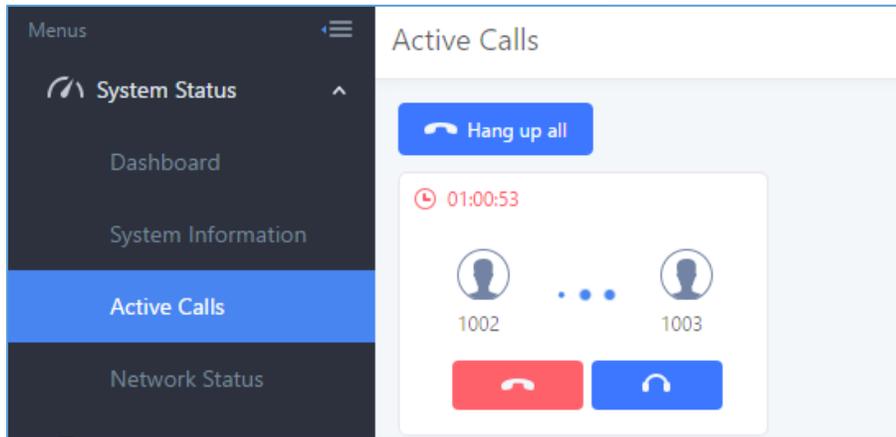


Figure 194: call connection more than one hour

Hang Up Active Calls

To hang up an active call, click on  icon in the active call dialog. Users can also click on  to hang up all active calls shown on the Active Calls page.

Call Monitor

During an active call, click on icon  and the Monitor dialog will pop up.

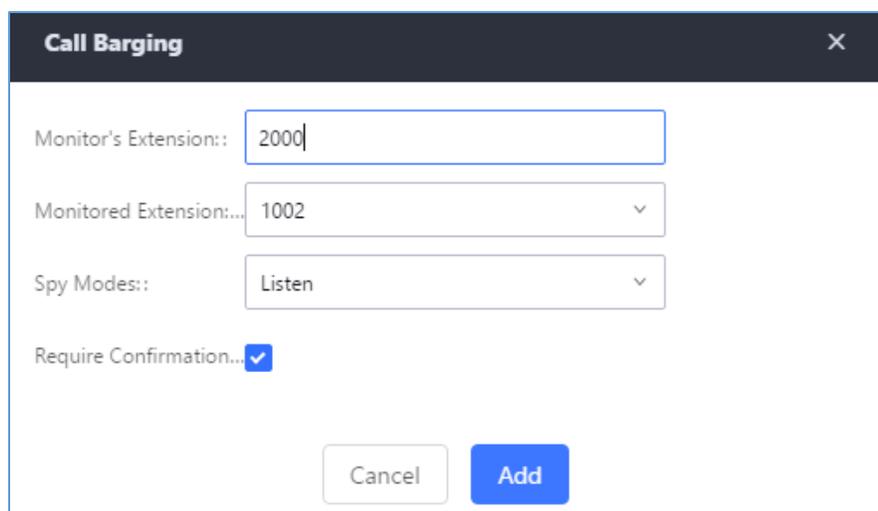


Figure 195: Configure to Monitor an Active Call

In the “Monitor” dialog, configure the following to monitor an active call:



1. Enter an available extension for “Monitor’s Extension” which will be used to monitor the active call.
2. “Monitored Extension” must be one of the parties in the active call to be monitored.
3. Select spy mode. There are three options in “Spy Mode”.
 - **Listen**

In “Listen” mode, the extension monitoring the call can hear both parties in the active call but the audio of the user on this extension will not be heard by either party in the monitored active call.
 - **Whisper**

In “Whisper” mode, the extension monitoring the call can hear both parties in the active call. The user on this extension can only talk to the selected monitored extension and he/she will not be heard by the other party in the active call. This can be usually used to supervise calls.
 - **Barge**

In “Barge” mode, the extension monitoring the call can talk to both parties in the active call. The call will be established similar to three-way conference.
4. Enable or disable “Require Confirmation” option. If enabled, the confirmation of the invited monitor’s extension is required before the active call can be monitored. This option can be used to avoid adding participant who has auto-answer configured or call forwarded to voicemail.
5. Click on “Add”. An INVITE will be sent to the monitor’s extension. The monitor can answer the call and start monitoring. If “Require Confirmation” is enabled, the user will be asked to confirm to monitor the call.

Another way to monitor active calls is to dial the corresponding feature codes from an extension. Please refer to [\[Table 93: UCM6510 Feature Codes\]](#) and [\[Enable Spy\]](#) section for instructions.



CALL FEATURES

The UCM6510 supports call recording, transfer, call forward, call park and other call features via feature code. Feature Codes settings can be found at Web GUI→**Call Features**→**Feature Codes**. This section lists all the feature codes in the UCM6510 and describes how to use the call features.

Feature Codes

Table 93: UCM6510 Feature Codes

Feature Maps	
Blind Transfer	<ul style="list-style-type: none"> • Default code: #1. • Enter the code during active call. After hearing "Transfer", you will hear dial tone. Enter the number to transfer to. Then the user will be disconnected and transfer is completed. • Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Attended Transfer	<ul style="list-style-type: none"> • Default code: *2. • Enter the code during active call. After hearing "Transfer", you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. • Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Seamless Transfer	<p>Seamless Transfer allows user to perform blind transfer using UCM feature code without having music on hold presented during the transfer process, it minimizes the interruption during transfer, making the process smooth and simple.</p> <p>During an active call use the feature code (*44 which is the default) followed by the number you want to transfer to in order to perform the seamless transfer.</p>



Disconnect	<ul style="list-style-type: none"> • Default code: *0. • Enter the code during active call. It will disconnect the call. • Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Call Park	<ul style="list-style-type: none"> • Default code: #72. • Enter the code during active call to park the call. • Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
Audio Mix Record	<ul style="list-style-type: none"> • Default code: *3. • Enter the code followed by # or SEND to start recording the audio call and the UCM6510 will mix the streams natively on the fly as the call is in progress. • Options: Disable Allow Caller: Enable the feature code on caller side only. Allow Callee: Enable the feature code on callee side only. Allow Both: Enable the feature code on both caller and callee.
DND/Call Forward	
Do Not Disturb (DND) Activate	<ul style="list-style-type: none"> • Default code: *77.
Do Not Disturb (DND) Deactivate	<ul style="list-style-type: none"> • Default code: *78.
Call Forward Busy Activate	<ul style="list-style-type: none"> • Default Code: *90. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward Busy Deactivate	<ul style="list-style-type: none"> • Default Code: *91.
Call Forward No Answer Activate	<ul style="list-style-type: none"> • Default Code: *92. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward No Answer Deactivate	<ul style="list-style-type: none"> • Default Code: *93.
Call Forward Unconditional Activate	<ul style="list-style-type: none"> • Default Code: *72. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.



Call Forward Unconditional Deactivate	<ul style="list-style-type: none"> • Default Code: *73.
Feature Misc	
Feature Code Digits Timeout	<ul style="list-style-type: none"> • Default Setting: 1000. • Configure the maximum interval (in milliseconds) between the digits input to activate the feature code.
Call Park	<ul style="list-style-type: none"> • Default Extension: 700. • During an active call, initiate blind transfer and then enter this code to park the call.
Parked Lots	<ul style="list-style-type: none"> • Default Extension: 701-720. • These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.
Use Parklot as extension	If checked, the Parklot number will be used as extension, you can transfer to the Parklot number for parking your call. If the parking lots overlap existing extensions, there will be conflict.
Parking Timeout (s)	<ul style="list-style-type: none"> • Default setting: 300. • This is the timeout allowed for a call to be parked. After the timeout, if the call is not picked up, the extension who parks the call will be called back.
Music On Hold Classes	Select the Music on Hold Class.
Feature Codes	
Voicemail Access Code	<ul style="list-style-type: none"> • Default Code: *98. • Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box.
My Voicemail	<ul style="list-style-type: none"> • Default Code: *97. • Press *97 to access the voicemail box.
Agent Pause	<ul style="list-style-type: none"> • Default Code: *83. • Pause the agent in all call queues.
Agent Unpause	<ul style="list-style-type: none"> • Default Code: *84. • Unpause the agent in all call queues.
Paging Prefix	<ul style="list-style-type: none"> • Default Code: *81. • To page an extension, enter the code followed by the extension number.
Intercom Prefix	<ul style="list-style-type: none"> • Default Code: *80. • To intercom an extension, enter the code followed by the extension number.
Blacklist Add	<ul style="list-style-type: none"> • Default Code: *40. • To add a number to blacklist for inbound route, dial *40 and follow the voice prompt to enter the number.



Blacklist Remove	<ul style="list-style-type: none"> • Default Code: *41. • To remove a number from current blacklist for inbound route, dial *41 and follow the voice prompt to remove the number.
Call Pickup on Ringing	<ul style="list-style-type: none"> • Default Code: **. • To pick up a call for any extension xxxx, enter the code followed by the extension number xxxx.
Pickup Incall	If “Pickup Incall” feature is enabled (by default *45), only the extensions added in “Allowed to seamless transfer” in the extension’s Seamless Transfer Privilege Control List” can pick up the call.
Pickup Extension	<ul style="list-style-type: none"> • Default Code: *8. • This code is for the pickup group which can be assigned for each extension on the extension configuration page. • If there is an incoming call to an extension, the other extensions within the same pickup group can dial *8 directly to pick up the call.
Direct Dial Voicemail Prefix	<ul style="list-style-type: none"> • Default Code: * • This code is for the user to directly dial or transfer to an extension’s voicemail. • For example, directly dial *5000 will have to call go into the extension 5000’s voicemail. If the user would like to transfer the call to the extension 5000’s voicemail, enter *5000 as the transfer target number.
Direct Dial Mobile Phone Prefix	If you have the permission to call mobile phone number, use this prefix plus the extension number can dial the mobile phone number of this extension directly.
Call Completion Request	<p>Default Code: *11</p> <p>This code is for the user who wants to use Call Completion to complete a call.</p>
Call Completion Cancel	<p>Default Code: *12</p> <p>This code is for the user who wants to cancel Call Completion request.</p>
Enable Spy	Check this box to enable spy feature codes.
Listen Spy	This is the feature code to listen in on a call to monitor performance. Monitor’s line will be muted, and neither party will hear from the monitor’s extension. The default setting is *54.
Whisper Spy	This is the feature code to speak to one side of the call (for example, whisper to employees to help them handle a call). Only one side will be able to hear from the monitor’s extension. The default setting is *55.



Barge Spy	This is the feature code to join in on the call to assist both parties. The default setting is *56 .
Wakeup Service	Dial this code to access UCM wakeup service, you can add, update, activate or deactivate wakeup service.
PMS Wakeup Service	Dial this code to access UCM PMS wakeup service, you can add, update, activate or deactivate PMS wakeup service.
Update PMS Room Status	Use this code with maid code to update PMS room status. Choose the status to set after hearing the prompt, for example: for maid 001 dial *23001 and then 1 after hearing the prompt.
Presence Status	Dial this code to set the presence status of the extension. Possible options are 1:"unavailable",2:"available",3:"away",4:"chat",5:"dnd",6:"userdef"
Enable Inbound Multiple Mode	If enabled, user can switch between different inbound route modes with feature code. By default, this option is disabled.
Inbound Default Mode	This feature code is used to switch inbound route mode to default mode. The default setting is *61 .
Inbound Mode 1	This feature code is used to switch inbound route mode to mode 1. The default setting is *62 .

The UCM6510 also allows user to enable / disable specific feature code by one click. As shown below:

Feature Codes

Feature Maps
DND/Call Forward
Feature Misc
Feature Codes

Reset All
Default All

<p>* Voicemail Access C... <input type="text" value="*98"/> <input checked="" type="checkbox"/></p> <p>* Agent Pause: <input type="text" value="*83"/> <input checked="" type="checkbox"/></p> <p>* Paging Prefix: <input type="text" value="*81"/> <input type="checkbox"/></p> <p>* Blacklist Add: <input type="text" value="*40"/> <input checked="" type="checkbox"/></p> <p>* Call Pickup on Rin... <input type="text" value="**"/> <input type="checkbox"/></p> <p>* Pickup Extension: <input type="text" value="*8"/> <input checked="" type="checkbox"/></p> <p>* Direct Dial Mobile ... <input type="text" value="*88"/> <input checked="" type="checkbox"/></p>	<p>* My Voicemail: <input type="text" value="*97"/> <input checked="" type="checkbox"/></p> <p>* Agent Unpause: <input type="text" value="*84"/> <input checked="" type="checkbox"/></p> <p>* Intercom Prefix: <input type="text" value="*80"/> <input checked="" type="checkbox"/></p> <p>* Blacklist Remove: <input type="text" value="*41"/> <input checked="" type="checkbox"/></p> <p>* Pickup In-call: <input type="text" value="*45"/> <input type="checkbox"/></p> <p>* Direct Dial Voicem... <input type="text" value="*"/> <input checked="" type="checkbox"/></p> <p>* Call Completion Re... <input type="text" value="*11"/> <input checked="" type="checkbox"/></p>
---	--

Figure 196: Enable/Disable Feature codes



Call Recording

The UCM6510 allows users to record audio during the call. If "Auto Record" is turned on for extension or trunk, the call will be automatically recorded when there is established call with the extension or trunk. Otherwise, please follow the instructions below to manually record the call.

1. Make sure the feature code for "Audio Mix Record" is configured and enabled.
2. After establishing the call, enter the "Audio Mix Record" feature code (by default *3) followed by # or SEND to start recording.
3. To stop the recording, enter the "Audio Mix Record" feature code (by default *3) followed by # or SEND again. Or the recording will be stopped once the call hangs up.
4. The recording file can be retrieved under Web GUI→**CDR**. Click on  to show and play the recording or click on  to download the recording file.

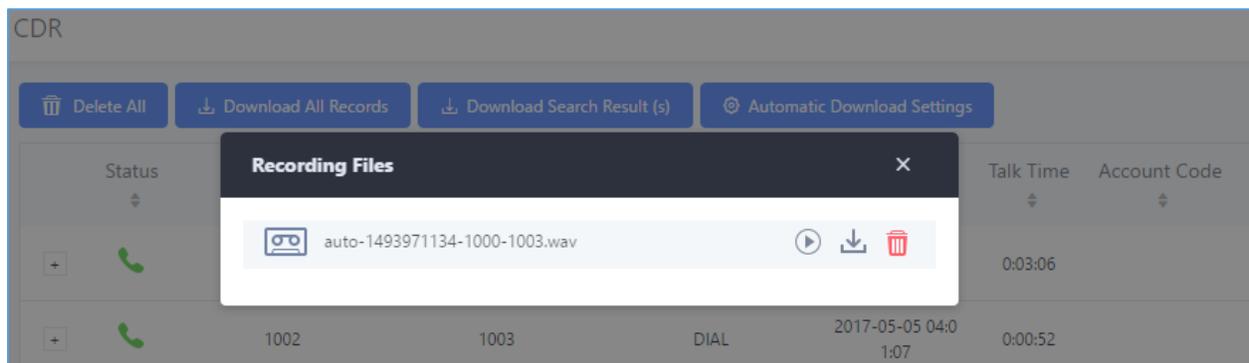


Figure 197: Download Recording File from CDR Page

The above recorded call's recording files are also listed under the UCM6510 Web GUI→**CDR**→**Recording Files**.

Call Park

The UCM6510 provides call park and call pickup features via feature code.

Park a Call

There are two feature codes that can be used to park the call.

- **Feature Maps→Call Park (Default code #72)**

During an active call, press #72 and the call will be parked. Parking lot number (default range 701 to 720) will be announced after parking the call.



- **Feature Misc→Call Park (Default code 700)**

During an active call, initiate blind transfer (default code #1) and then dial 700 to park the call. Parking lot number (default range 701 to 720) will be announced after parking the call.

Retrieve Parked Call

To retrieve the parked call, simply dial the parking lot number and the call will be established. If a parked call is not retrieved after the timeout, the original extension who parks the call will be called back.

Enable Spy

If “Enable Spy” option is enabled, feature codes for Listen Spy, Whisper Spy and Barge Spy are available for users to dial from any extension to perform the corresponding actions.

Assume a call is on-going between extension A and extension B, user could dial the feature code from extension C to listen on their call (*54 by default), whisper to one side (*55 by default), or barge into the call (*56 by default). Then the user will be asked to enter the number to call, which should be either side of the active call, extension A or B in this example.

 **Warning:**

“Enable Spy” allows any user to listen to any call by dialing feature codes. This may result in the leakage of user privacy. Please be aware of the associated potential security risk when enabling this feature.



PBX INTERNAL OPTIONS

This section describes internal options that haven't been mentioned in previous sections yet. The settings in this section can be applied globally to the UCM6510, including general configurations, jitter buffer, RTP settings, hardware config and STUN monitor. The options can be accessed via Web GUI→**PBX Settings**→**General Settings**.

PBX Settings/General

Table 94: PBX Settings /General

General Preferences	
Global Outbound CID	Configure the global CallerID used for all outbound calls when no other CallerID is defined with higher priority. If no CallerID is defined for extension or trunk, the global outbound CID will be used as CallerID.
Global Outbound CID Name	Configure the global CallerID Name used for all outbound calls. If configured, all outbound calls will have the CallerID Name set to this name. If not, the extension's CallerID Name will be used.
Ring Timeout	Configure the number of seconds to ring an extension before the call goes to the user's voicemail box. The default setting is 60. Note: This is the global value used for each extension if "Ring Timeout" field is left empty on the extension configuration page.
Call Duration Limit	Configure the maximum duration of call-blocking.
Record Prompt	If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the UCM6510 will play voice prompt "The call will be recorded". The default setting is "No".
Extension Preferences	
Enforce Strong Passwords	If enabled, strong password will be enforced for the password created on the UCM6510. The default setting is enabled. Strong Password Rules: 1. Password for voicemail, voicemail group, outbound route, DISA, call queue and conference requires non-repetitive and non-sequential digits, with a minimum length of 4 digits. Repetitive digits pattern (such as 0000, 1111, 1234, 2345, and etc), or common digits' pattern (such as 111222, 321321 and etc) are not allowed to be configured as password.



	<p>2. Password for extension registration, Web GUI admin login, LDAP and LDAP sync requires alphanumeric characters containing at least two categories of the following, with a minimum length of 4 characters.</p> <ul style="list-style-type: none"> • Numeric digits • Lowercase alphabet characters • Uppercase alphabet characters • Special characters
Enable Random Password	<p>If enabled, random password will be generated when the extension is created. The default setting is "Yes". It is recommended to enable it for security purpose.</p>
Enable Auto E-mail Notification	<p>If enabled, UCM6510 will send Email notification to user automatically after editing extension settings or adding a new extension.</p>
Disable Extension Range	<p>If set to "Yes", users could disable the extension range pre-configured/configured on the UCM6510. The default setting is "No". The default extension range assignment is shown in "Extension Ranges" below.</p> <p>Note: It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.</p>
Extension Ranges	<p>The default extension range assignment is:</p> <ul style="list-style-type: none"> • <u>User Extensions</u>: 1000-6299 User Extensions is referring to the extensions created under Web GUI→Extension/Trunk→Extensions page. • <u>Pick Extensions</u>: 4000-4999 This refers to the extensions that can be manually picked from end device when being provisioned by the UCM6510. There are two related options in zero config page→Auto Provision Settings, "Pick Extension Segment" and "Enable Pick Extension". If "Enable Pick Extension" under zero config settings is selected, the extension list defined in "Pick Extension Segment" will be sent out to the device after receiving the device's request. This "Pick Extension Segment" should be a subset of the "Pick Extensions" range here. This feature is for the GXP series phones that support selecting extension to be provisioned via phone's LCD. • <u>Auto Provision Extensions</u>: 5000-6299 This sets the range for "Zero Config Extension Segment" which is the extensions can be assigned on the UCM6510 to provision the end device.



- Conference Extensions: 6300-6399
- Ring Group Extensions: 6400-6499
- Queue Extensions: 6500-6599
- Voicemail Group Extensions: 6600-6699
- IVR Extensions: 7000-7100
- Dial By Name Extensions: 7101-7199
- Fax Extensions: 7200-8200

PBX Settings/Custom Prompt

Record New Custom Prompt

In the UCM6510 Web GUI → **PBX Settings** → **Voice Prompt** → **Custom Prompt** page, click on "Record New IVR Prompt" and follow the steps below to record new IVR prompt.

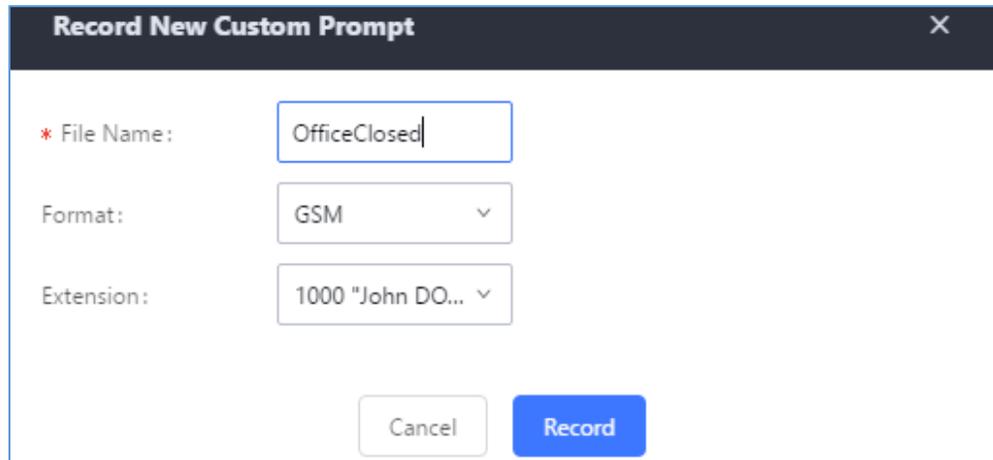


Figure 198: Record New IVR Prompt

1. Specify the IVR file name.
2. Select the format (GSM or WAV) for the IVR prompt file to be recorded.
3. Select the extension to receive the call from the UCM6510 to record the IVR prompt.
4. Click the "Record" button. A request will be sent to the UCM6510. The UCM6510 will then call the extension for recording the IVR prompt from the phone.
5. Pick up the call from the extension and start the recording following the voice prompt.
6. The recorded file will be listed in the IVR Prompt web page. Users could select to re-record, play or delete the recording.



Upload Custom Prompt

If the user has a pre-recorded IVR prompt file, click on "Upload IVR Prompt" in Web GUI→**PBX Settings**→**Voice Prompt**→**Custom Prompt** page to upload the file to the UCM6510. The following are required for the IVR prompt file to be successfully uploaded and used by the UCM6510:

- PCM encoded.
- 16 bits.
- 8000Hz mono.
- In .mp3 or .wav format; or raw/ulaw/alaw/gsm file with .ulaw or .alaw suffix.
- File size under 5M.

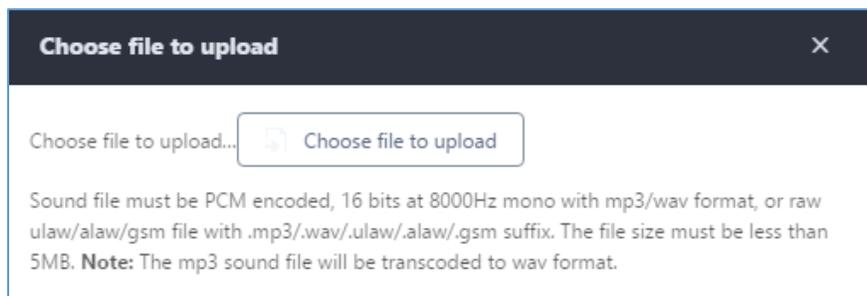


Figure 199: Upload IVR Prompt

Click on “choose file to upload” to select audio file from local PC and to start uploading. Once uploaded, the file will appear in the IVR Prompt web page.

Download All Custom Prompt

On the UCM6510, the users can download all custom prompts from UCM Web GUI to local PC. To download all custom prompt, log in UCM Web GUI and navigate to **PBX Settings**→**Voice Prompt**→**Custom Prompt** and click on . The following window will pop up in order to set a name for the downloaded file.

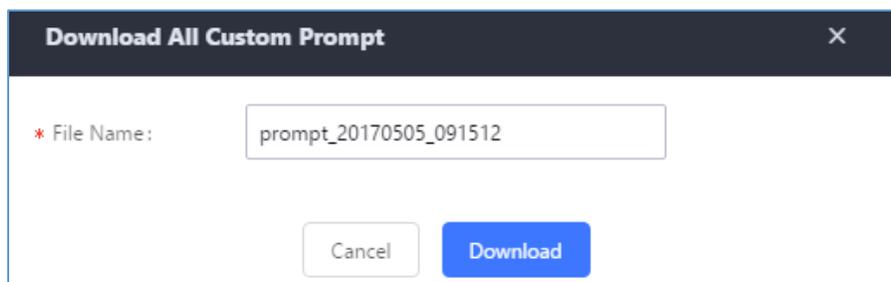


Figure 200: Download All Custom Prompt

Note: The downloaded file will have a .tar extension.



PBX Settings/Jitter Buffer

Table 95: Internal Options/Jitter Buffer

SIP Jitter Buffer	
Enable Jitter Buffer	Select to enable jitter buffer on the sending side of the SIP channel. The default setting is "No".
Jitter Buffer Size	Configure the time (in ms) to buffer. This is the jitter buffer size used in "Fixed" jitter buffer, or used as the initial time for "adaptive" jitter buffer. The default setting is 100.
Max Jitter Buffer	Configure the maximum time (in ms) to buffer for "Adaptive" jitter buffer implementation, or used as the jitter buffer size for "Fixed" jitter buffer implementation. The default setting is 200.
Implementation	<p>Configure the jitter buffer implementation on the sending side of a SIP channel. The default setting is "Fixed".</p> <ul style="list-style-type: none"> • Fixed The size is always equal to the value of "Max Jitter Buffer". • Adaptive The size is adjusted automatically and the maximum value equals to the value of "Max Jitter Buffer".

PBX Settings/RTP Settings

Table 96: Internal Options/RTP Settings

RTP Start	Configure the RTP port starting number. The default setting is 10000.
RTP End	Configure the RTP port ending address. The default setting is 20000.
Strict RTP	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is "Disable".
RTP Checksums	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".
ICE Support	Configure whether to support ICE, ICE is the integrated use of STUN and TURN structure to provide reliable VoIP or video calls and media transmission, via a SIP request/ response model or multiple candidate endpoints exchanging IP addresses and ports, such as private addresses and TURN server address. It is enabled by default.



STUN Server

Configure STUN server address, STUN protocol is a Client / Server – is also a Request / Response protocol, where it is used to check the connectivity between the two terminals, such as maintaining NAT binding entries keep alive agreement.

The default STUN Server is `stun.ipvideotalk.com`

Valid format:

`[(hostname | IP-address) [:' port]`

The default port number is 3478 if not specified.

PBX Settings/Payload

The UCM6510 payload type for audio codecs and video codes can be configured here.

Table 97: Internal Options/Payload

AAL2-G.726	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112.
DTMF	Configured payload type for DTMF. The default setting is 101.
G.721 Compatible	Configure to enable/disable G.721 compatible. The default setting is Yes.
G.726	Configure the payload type for G.726 if "G.721 Compatible" is disabled. The default setting is 111.
iLBC	Configure the payload type for iLBC. The default setting is 97.
H.264	Configure the payload type for H.264. The default setting is 99.
H.263P	Configure the payload type for H.263+. The default setting is 100 103.
VP8	Configure the payload type for VP8. The default setting is 108.



IAX SETTINGS

The UCM6510 IAX global settings can be accessed via Web GUI→**PBX**→**IAX Settings**.

IAX Settings/General

Table 98: IAX Settings/General

Bind Port	Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569.
Bind Address	Configure the address that the IAX2 will be forced to bind to. The default setting is 0.0.0.0, which means all addresses.
IAX1 Compatibility	Select to configure IAX1 compatibility. The default setting is "No".
No Checksums	If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this feature. The default setting is "No".
Delay Reject	If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is "No".
ADSI	Select to enable ADSI phone compatibility. The default setting is "No".
Music On Hold Interpret	Specify which Music On Hold class this channel would like to listen to when being put on hold. This music class is only effective if this channel has no music class configured and the bridged channel putting the call on hold has no "Music On Hold Suggest" setting.
Music On Hold Suggest	Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold.
Bandwidth	Configure the bandwidth for IAX settings. The default setting is "Low".

IAX Settings/Registration

Table 99: IAX Settings/Registration

IAX Registration Options	
Min Reg Expire	Configure the minimum period (in seconds) of registration. The default setting is 60.
Max Reg Expire	Configure the maximum period (in seconds) of registration. The default setting is 3600.
IAX Thread Count	Configure the number of IAX helper threads. The default setting is 10.
IAX Max Thread Count	Configure the maximum number of IAX threads allowed. The default setting is 100.



Auto Kill	If set to "yes", the connection will be terminated if ACK for the NEW message is not received within 2000ms. Users could also specify number (in milliseconds) in addition to "yes" and "no". The default setting is "yes".
Authentication Debugging	If enabled, authentication traffic in debugging will not show. The default setting is "No".
Codec Priority	Configure codec negotiation priority. The default setting is "Reqonly". <ul style="list-style-type: none"> • Caller Consider the callers preferred order ahead of the host's. • Host Consider the host's preferred order ahead of the caller's. • Disabled Disable the consideration of codec preference all together. • Reqonly This is almost the same as "Disabled", except when the requested format is not available. The call will only be accepted if the requested format is available.
Type of Service	Configure ToS bit for preferred IP routing.
IAX Trunk Options	
Trunk Frequency	Configure the frequency of trunk frames (in milliseconds). The default setting is 20.
Trunk Time Stamps	If enabled, time stamps will be attached to trunk frames. The default setting is "No".

IAX Settings/Security

Table 100: IAX Settings/Static Defense

Call Token Optional	Enter a single IP address or a range of IP addresses for which call token validation is not required. For example: 11.11.11.11 11.11.11.11/22.22.22.22.
Max Call Numbers	Configure the maximum number of calls allowed for a single IP address.
Max Unvalidated Call Numbers	Configure the maximum number of Unvalidated calls for all IP addresses.
Call Number Limits	Configure to limit the number of calls for a give IP address of IP range.
IP or IP Range	Enter the IP address or a range of IP addresses to be considered for call number limits. For example: 11.11.11.11 11.11.11.11/22.22.22.22.



SIP SETTINGS

The UCM6510 SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

SIP Settings/General

Table 101: SIP Settings/General

Realm For Digest Authentication	Configure the host name or domain name for the UCM6510. Realms MUST be globally unique according to RFC3261. The default setting is grandstream.
Bind UDP Port	Configure the UDP port used for SIP. The default setting is 5060.
Bind IP Address	Configure the IP address to bind to. The default setting is 0.0.0.0, which means binding to all addresses.
Allow Guest Calls	<p>If enabled, the UCM6510 allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is "No".</p> <p>Warning: Please be aware of the potential security risk when enabling "Allow Guest Calls" as this will allow any user with the UCM6510 address to dial into the UCM6510.</p>
Allow Transfer	If set to "No", all transfers initiated by the endpoint in the UCM6510 will be disabled (unless enabled in peers or users). The default setting is "Yes".
MWI From	When sending MWI NOTIFY requests, this value will be used in the "From:" header as the "name" field. If no "From User" is configured, the "user" field of the URI in the "From:" header will be filled with this value.
Enable Diversion Header	If disabled, the UCM will not forward the diversion header.

SIP Settings/Misc

Table 102: SIP Settings/Misc

Outbound SIP Registrations	
Register Timeout	Configure the register retry timeout (in seconds). The default setting is 20.
Register Attempts	Configure the number of registration attempts before the UCM6510 gives up. The default setting is 0, which means the UCM6510 will keep trying until the server side accepts the registration request.
Video	
Max Bit Rate (kb/s)	Configure the maximum bit rate (in kb/s) for video calls. The default setting is 384.



Support SIP Video	Select to enable video support in SIP calls. The default setting is "Yes".
Reject Non-Matching INVITE	If enabled, when rejecting an incoming INVITE or REGISTER request, the UCM6510 will always reject with "401 Unauthorized" instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. The default setting is "No".
SDP Attribute Passthrough	
Enable Attribute Passthrough	If enable, and if the service doesn't know the attribute of FEC/FECC/BFCP, then the attribute will be passthrough.
Early Media	
Enable Use Final SDP	If enabled, call negotiation will use final response SDP.
Blind Transfer	
Allow callback when blind transfer fails.	If enabled, the UCM will callback to the transferrer when blind transfer fails (reason of failure includes: busy and no answer). Note: This feature takes effect only on internal calls.
Blind transfer timeout	Configure the timeout in (s) for the transferrer waiting for the destination to answer. Default is 60s.

SIP Settings/Session Timer

Table 103: SIP Settings/Session Timer

Session Timers	Select the session timer mode. The default setting is "Accept". The options are: <ul style="list-style-type: none"> • Originate Always request and run session timer. • Accept Run session timer only when requested by another UA. • Refuse Do not run session timer.
Session Expire	Configure the maximum session refresh interval (in seconds). The default setting is 1800.
Min SE	Configure the minimum session refresh interval (in seconds). The default setting is 90.
Session Refresher	Select the session refresher to be UAC or UAS. The default setting is UAC.



SIP Settings/TCP and TLS



Note:

The configuration in this section requires system reboot to take effect.

Table 104: SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the UCM6510. The default setting is "No".
TCP Bind Address	Configure the IP address for TCP server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5060 will be used.
TLS Enable	Configure to allow incoming TLS connections with the UCM6510. The default setting is "No".
TLS Bind Address	Configure the IP address for TLS server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5061 will be used. Note: The IP address must match the common name (hostname) in the certificate. Please do not bind a TLS socket to multiple IP addresses. For details on how to construct a certificate for SIP, please refer to the following document: http://tools.ietf.org/html/draft-ietf-sip-domain-certs
TLS Client Protocol	Select the TLS protocol for outbound client connections. The default setting is TLSv1.
TLS Do Not Verify	If enabled, the TLS server's certificate won't be verified when acting as a client. The default setting is "Yes".
TLS Self-Signed CA	This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server's public key. This file will be renamed as "TLS.ca" automatically. Note: The size of the uploaded ca file must be under 2MB.
TLS Cert	This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as "TLS.pem" automatically. Note: The size of the uploaded certificate file must be under 2MB.



TLS CA Cert	<p>This file must be named with the CA subject name hash value. It contains CA's (Certificate Authority) public key, which is used to verify the accessed servers.</p> <p>Note: The size of the uploaded CA certificate file must be under 2MB.</p>
TLS CA List	Display a list of files under the CA Cert directory.

SIP Settings/NAT

Table 105: SIP Settings/NAT

External Host	Configure a static IP address and port (optional) used in outbound SIP messages if the UCM6510 is behind NAT. If it is a host name, it will only be looked up once.
Use IP address in SDP	If enabled, the SDP connection will use the IP address resolved from the external host.
External TCP Port	Configure the externally mapped TCP port when the UCM6510 is behind a static NAT or PAT.
External TLS Port	Configures the externally mapped TLS port when UCM6510 is behind a static NAT or PAT.
Local Network Address	<p>Specify a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly.</p> <p>A sample configuration could be as follows: 192.168.0.0/16</p>

SIP Settings/TOS

Table 106: SIP Settings/ToS

ToS For SIP	Configure the Type of Service for SIP packets. The default setting is None.
ToS For RTP Audio	Configure the Type of Service for RTP audio packets. The default setting is None.
ToS For RTP Video	Configure the Type of Service for RTP video packets. The default setting is None.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120.
Max Registration/Subscription Time	Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the UCM6510. The default setting is 3600.



Min Registration/Subscription Time	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM6510. The default setting is 60.
Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".
DTMF Mode	Select DTMF mode to send DTMF. The default setting is RFC2833. If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, 64-kbit codec PCMU and PCMA are required. When "Auto" is selected, "RFC2833" will be used if offered, otherwise "Inband" will be used. The default setting is "RFC2833".
RTP Timeout	During an active call, if there is no RTP activity within the timeout (in seconds), the call will be terminated. The default setting is no timeout. Note: This setting doesn't apply to calls on hold.
RTP Hold Timeout	When the call is on hold, if there is no RTP activity within the timeout (in seconds), the call will be terminated. This value of RTP Hold Timeout should be larger than RTP Timeout. The default setting is no timeout.
RTP Keep-alive	This feature can be used to avoid abnormal call drop when the remote provider requires RTP traffic during proceeding. For example, when the call goes into voicemail and there is no RTP traffic sent out from UCM, configuring this option can avoid voicemail drop. When configured, RTP keep-alive packet will be sent to remote party at the configured interval. If set to 0, RTP keep-alive is disabled.
100rel	Configure the 100rel setting on UCM6510. The default setting is "Yes".
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted. The default setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
Generate In-Band Ringing	Configure whether the UCM6510 should generate inband ringing or not. The default setting is "Never". <ul style="list-style-type: none"> • Yes: The UCM6510 will send 180 Ringing followed by 183 Session Progress and in-band audio. • No: The UCM6510 will send 180 Ringing if 183 Session Progress has not been sent yet. If audio path is established already with 183 then send in-band ringing. • Never: Whenever ringing occurs, the UCM6510 will send 180 Ringing as long as 200OK has not been set yet. Inband ringing will not be generated even the end point device is not working properly.
Server User Agent	Configure the user agent string for the UCM6510.
Send Compact SIP Headers	If enabled, compact SIP headers will be sent. The default setting is "No".



Transparent Call-Info header

UCM supports transparent call info header in order to integrate GDS door system with GXP21XX Color phones, the UCM will forward the call-info header to the phone in order to request the live view from GDS door system and give the option to open the door via softkey.

```
Session Initiation Protocol (INVITE)
+ Request-Line: INVITE sip:3001@192.168.6.36:5064 SIP/2.0
- Message Header
+ Via: SIP/2.0/UDP 192.168.6.187:5060;rport;branch=z9hG4bKPj3217e67b-e74f-4f9f-b06f-afd3dcbbe29b
+ From: "3002" <sip:3002@192.168.6.187>;tag=202dca4f-2b9d-4880-924c-d48cea7d0596
+ To: <sip:3001@192.168.6.36>
+ Contact: <sip:68aae6ea-f1d4-4e62-9987-446e718a2448@192.168.6.187:5060>
  Call-ID: 7f66bb20-0b9f-4828-a355-698853b8d9fb
+ CSeq: 17559 INVITE
  Allow: OPTIONS, INFO, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REGISTER, REFER
  Supported: 100rel, timer, replaces, norefersub
  Session-Expires: 1800
  Min-SE: 90
  Call-Info: <https://192.168.6.186:443/capture/8001> ;purpose=GDS-view
  Max-Forwards: 70
  User-Agent: Grandstream UCM6202V1.5A 1.0.13.15
  Content-Type: application/sdp
  Content-Length: 547
+ Message Body
```

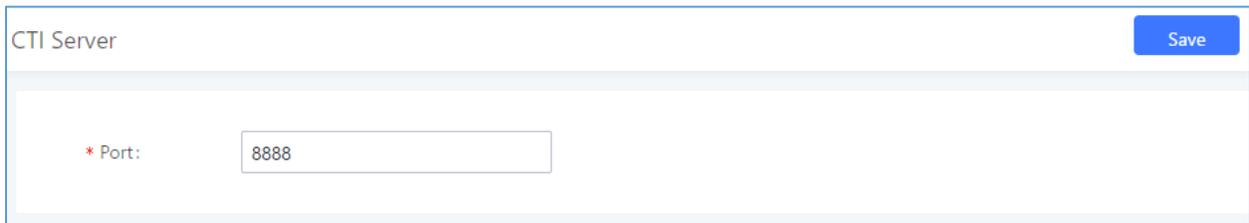
Figure 201: Transparent Call-Info

CTI SERVER

UCM does support CTI server capabilities which are designed to be a part of the CTI solution suite provided by Grandstream, including GXP21XX and GXP17XX enterprise IP phones along with GS Affinity app.

Mainly the UCM will by default listening on port TCP 8888 for the connections from GS affinity application in order to interact, modify and serve data requests by the application which includes setting call features for the connected extension as call forward and DND.

Users can change the listening port under the menu page, Web GUI→**Value-added Features**→**CTI Server** as shown on below screenshot:



CTI Server Save

* Port:

Figure 202: CTI Server Listening port

More information about GS affinity and CTI Support on Grandstream products series please refer to the following link: http://www.grandstream.com/sites/default/files/Resources/GS_Affinity_Guide.pdf

ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)

Starting from firmware 1.0.1.10, the UCM6510 supports Asterisk Manager Interface (AMI) with restricted access. AMI allows a client program to connect to an Asterisk instance commands or read events over a TCP/IP stream. It's particularly useful when the system admin tries to track the state of a telephony client inside Asterisk.

User could configure AMI parameters on UCM6510 Web GUI→**Value-added Features**→**AMI**. For details on how to use AMI on UCM6510, please refer to the following AMI guide:

http://www.grandstream.com/sites/default/files/Resources/UCM_series_AMI_guide.pdf

 **Warning:**

Please do not enable AMI on the UCM6510 if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM6510 system. Please be cautious when enabling AMI access on the UCM6510 and restrict the permission granted to the AMI user. By using AMI on UCM6510 you agree you understand and acknowledge the risks associated with this.



CRM INTEGRATION

Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers.

The UCM6510 support two CRM API, SugarCRM and Salesforce CRM, which allows users to look for contact information in the Contacts, Leads and / or Accounts tables, shows the contact record in CRM page, and saves the call information in the contact's history.

SugarCRM

Configuration page of the SugarCRM can be accessed via admin login, on the UCM webGUI→**Value-added Features**→**CRM**.

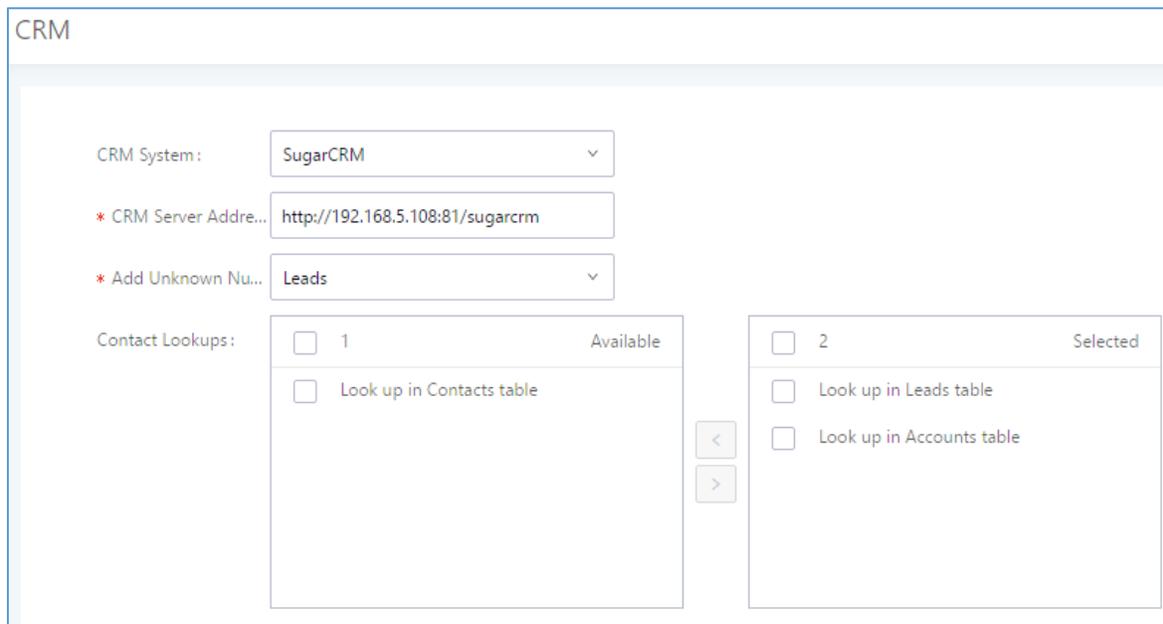


Figure 203: SugarCRM Basic Settings

1. Select “SugarCRM” from the CRM System Dropdown in order to use SugarCRM.

Table 107: SugarCRM Settings

CRM System	Select a CRM system from the Drop down, two CRM systems are available: Salesforce and SugarCRM.
CRM Server Address	Enter the IP address of the CRM server.
Add Unknown Number	Add the new number to this module if it can't be found in the selected module.



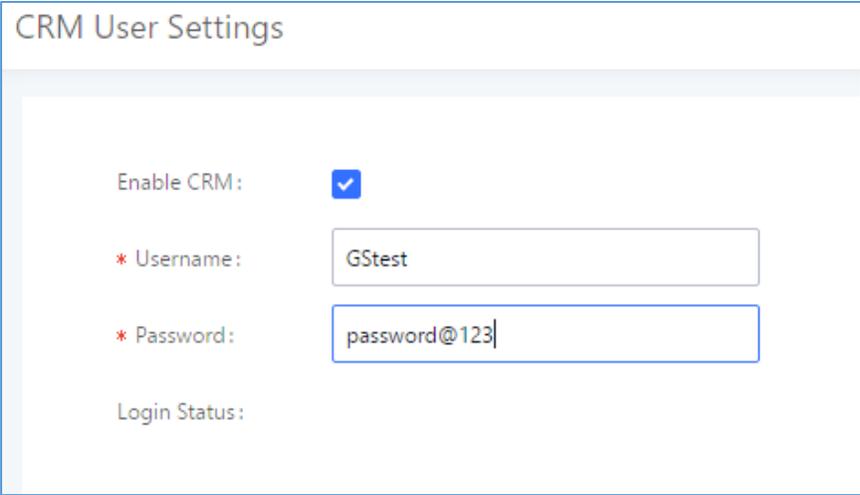
Contact Lookups

Select from the “**Available**” list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Once settings on admin access are configured:

2. Click on  and .
3. Logout from admin access.
4. Login to the UCM as user and navigate under “User Portal→Value-added Feature→CRM User Settings”.

Click on “**Enable CRM**” and enter the username/password associated with the CRM account then click on  and . The status will change from “Logged Out” to “Logged In”. User can start then using SugarCRM features.



The screenshot shows the 'CRM User Settings' interface. It includes a title bar 'CRM User Settings' and a form with the following fields:

- Enable CRM:** A checkbox that is checked with a blue checkmark.
- * Username:** A text input field containing the value 'GSstest'.
- * Password:** A text input field containing the value 'password@123'.
- Login Status:** A label with no associated input field.

Figure 204: CRM User Settings

Salesforce CRM

Configuration page of the Salesforce CRM can be accessed via admin login, on the UCM Web GUI→**Value-added Features→CRM**”.



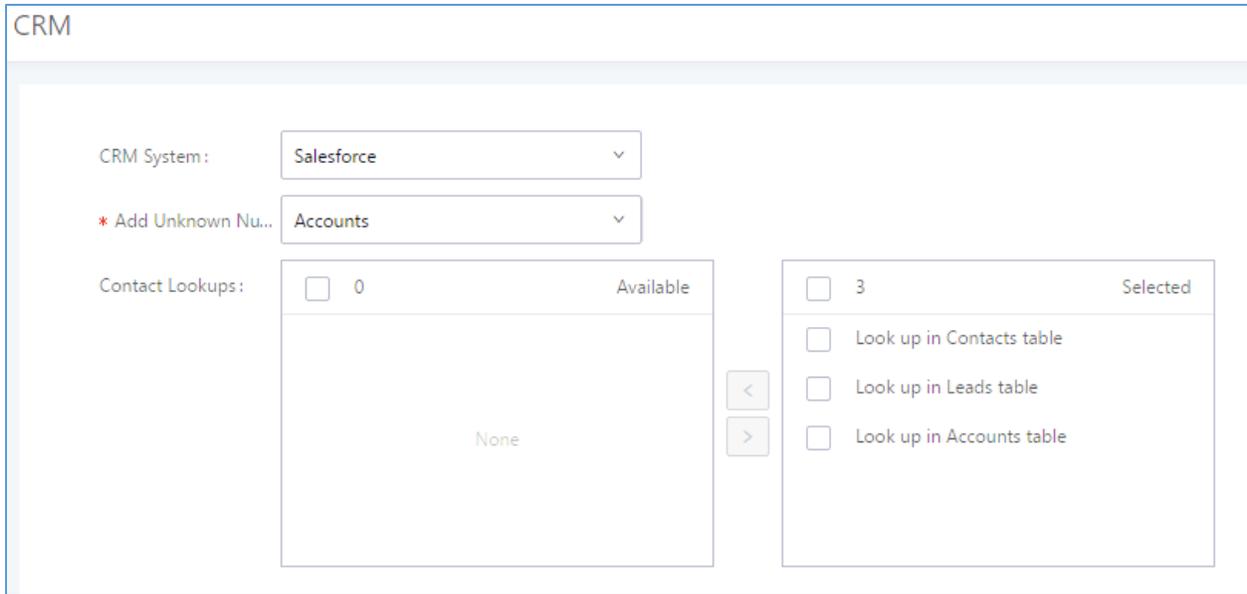


Figure 205: Salesforce Basic Settings

1. Select “Salesforce” from the CRM System Dropdown in order to use Salesforce CRM.

Table 108: Salesforce Settings

CRM System	Select a CRM system from the Drop down, two CRM systems are available: Salesforce and SugarCRM.
Add Unknown Number	Add the new number to this module if it can't be found in the selected module.
Contact Lookups	Select from the “ Available ” list of lookups and press   to select where the UCM can perform the lookups on the CRM tables, Leads, Accounts, and Contacts.

Once settings on admin access are configured:

2. Click on  and .
3. Logout from admin access.
4. Login to the UCM as user and navigate under “User Portal→Value-added Feature→CRM User Settings”.

Click on “**Enable CRM**” and enter the **username**, **password** and **Security Token** associated with the CRM account then click on  and . The status will change from “Logged Out” to “Logged In”. User can start then using Salesforce CRM features.



CRM User Settings

Enable CRM:

* Username:

* Password:

* Security Token:

Login Status:

Figure 206: Salesforce User Settings



PMS INTEGRATION

UCM6510 supports Hotel Property Management System PMS, including check-in/check-out services, wakeup calls, room status, Do Not Disturb which provide an ease of management for hotel applications. This feature can be found on Web GUI→**Value-added Features**→**PMS**.

Note: The PMS integration on UCM is currently supported only with one of the two following solutions.

HMobile PMS Connector

In this mode, the system can be divided into three parts:

- PMS (Property Management System)
- PMSI (Property Management System Interface)
- PBX

Grandstream UCM6XXX series have integrated HMobile Connect PMSI which supports a large variety of PMS software providing following hospitality features: Check-in, Check-out, set Room Status, Wake-up call and more.

The following figure illustrates the communication flow between the PBX (Grandstream UCM6xxx Series) and PMS software, which is done through a middleware system (HMobile Connect) acting as interface between both parties.

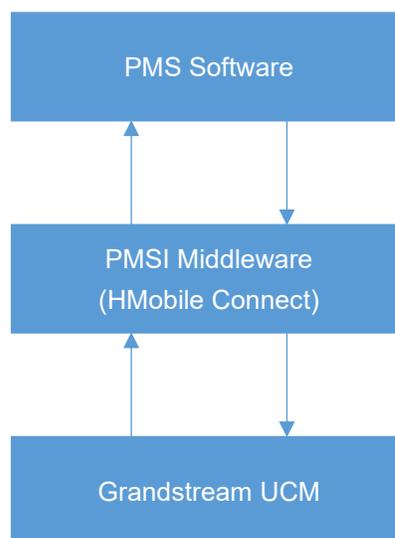


Figure 207: UCM & PMS interaction



Mitel PMS

In this mode, the system can be divided into two parts:

- PMS (Property Management System)
- PBX

Grandstream UCM6XXX series have integrated Mitel PMS providing following hospitality features: Check-in, Check-out, set Room Status, Wake-up call and more.

The following figure illustrates the communication flow between the PBX (Grandstream UCM6xxx Series) and PMS software (Mitel). The communication between both parties is direct with no middleware.

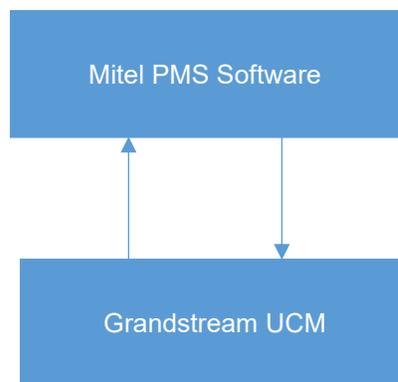


Figure 208: UCM & PMS interaction

The PMS module built-in the UCM supports the following features based on each solution:

Table 109: PMS Supported Features

Feature	Mitel	HMobile
Check-In	✓	✓
Check-out	✓	✓
Wake-up Call	✓	✓
Name Change	✓	X
Update	X	✓
Set Credit	✓	X
Set Station Restriction	✓	X
Room Status	X	✓
Room Move	X	✓
Do Not Disturb	X	✓
Mini Bar	X	✓
MSG	X	✓



In order to use all PMS features Please activate the feature code associated under “**Call Features→Feature Codes**”

- Enable PMS
- Update PMS Room Status
- PMS Wake Up Service Activate
- PMS Wake Up Service Deactivate

Basic Settings

On the UCM WebGUI→**Value-added Features→PMS→Basic Settings**” set the connection information for the HMobile platform.

Table 110: PMS Basic Settings

Field	Description
PMS Module	Users can select the desired PMS module from the drop-down list. Hmobile. Mitel.
Wake Up Prompt	Prompt used when answering the wakeup calls it can be customized from “PBX>Internal Options>Custom Prompt
PMS URL	Enter the PMS system URL
UCM Port	Enter the Port used by the PMS system
Username	Enter the Username to connect to the PMS system
Password	Enter the password to connect to the PMS system

PMS Features

Room Status

User can create Rooms by clicking on , the following Figure will be displayed then.



Create New Room

* Address:

* Room Number:

* Extension:

Guest Account:

Guest Category Cod...

Guest Credit Money...

Maid Code:

Arrival Date:

Departure Date:

Figure 209: Create New Room

Click “Save” to create the new room, the fields above can be configured from the HMobile platform, once set the following screen will be shown:

PMS

Basic Settings
Room Status
Wakeup Service
Mini Bar

	Address	Room Number	Extension	Room Status	User Name	Guest Account	Guest Category Code	Guest Credit Money	Maid Code	Options
<input type="checkbox"/>	1000	1000	1000	Check-out	John DOE					<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	1001	1001	1001	Check-out						<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 210: Room Status

User can create a batch of rooms as well by clicking on , the following window will pop up:



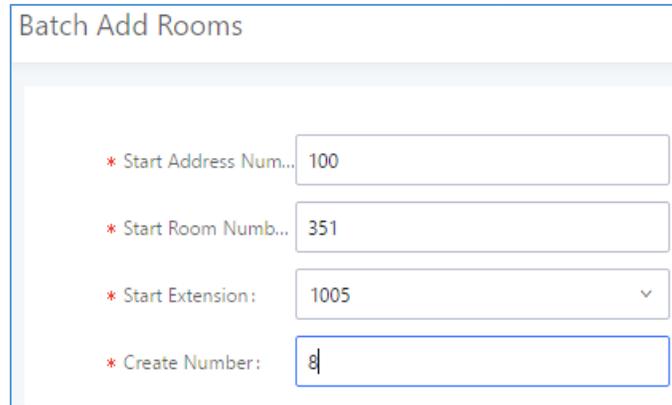


Figure 211: Add batch rooms

Wake Up Service

In order to create a New Wake up service, user can click on [+ Create New Wakeup Service](#), the following window will pop up:

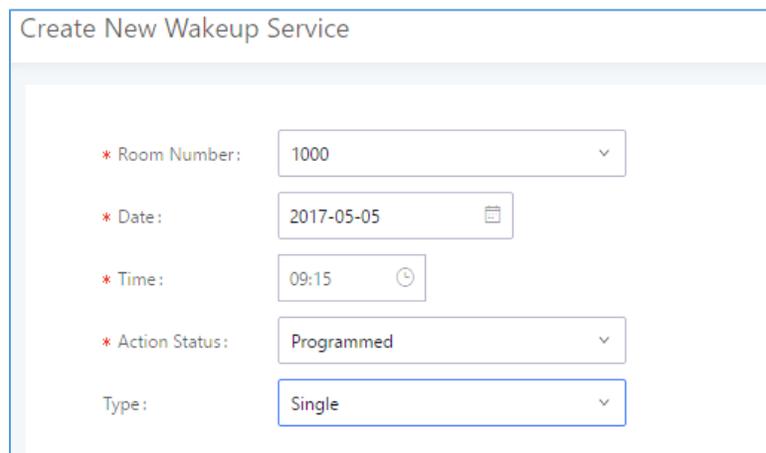


Figure 212: Create New Wake Up Service

Table 111: PMS Wake up Service

Field	Description
Room Number	Select the room number where to call
Time	Set the time of the wakeup call
Action Status	Show the status of the call: <ul style="list-style-type: none"> <u>Programmed</u>: the call is scheduled for the time set <u>Cancelled</u>: the call is canceled <u>Executed</u>: the wakeup call is made
Type	<ul style="list-style-type: none"> <u>Single</u>: The call will be made once on the specific time. <u>Daily</u>: The call will be repeated every day on the specific time



Once the call is made on the time specified, the following figure show the status of the wakeup call.

<input type="checkbox"/>	Name ▾	Extension ▾	Status	Action Status ▾	Answer Status ▾	Date	Time	Options
<input type="checkbox"/>	John	1000	Enabled	Executed	Answered	2017-05-04	05:18	 

Figure 213: Wakeup Call executed

This call has been executed but has been rejected, that why we can see the “**Busy**” status.

Mini Bar

In order to create a new mini bar, click on  under UCM webGUI→**Value-added Features**→**PMS**→**Mini Bar**, the following window will pop up:

Create New Mini Bar

* Code:

* Name:

* Prompt: Prompt

Skip Maid and Passw...

Enable Continuous M...

Figure 214: Create New Mini Bar

Table 112: Create New Mini Bar

Code	Enter a non-existing extension number to be dialed when using the mini bar feature.
Name	Enter a name for the mini bar.
Prompt	Select the Prompt to play once connected to the mini bar.
Skip Maid and Password Authentication	If enabled, the default maid code will be 0000, no authentication is required. (Enter 0000 followed by # to access the consumer goods)
Enable Continuous Multi Goods Billing	If enabled, please separate the goods' codes by*.



In order to create a new maid, click on [+ Create New Maid](#) under UCM webGUI→**Value-added Features**→**PMS**→**Mini Bar**, the following window will popup.



Figure 215: Create New Maid

Table 113: Create New Maid

Maid Code	Enter the Code to use when the maid wants to use the Mini Bar.
Secret	Enter the password associated with the maid.

In order to create a new consumer goods, click on [+ Create New Consumer Goods](#) under UCM webGUI→**Value-added Features**→**PMS**→**Mini Bar**, the following window will popup.

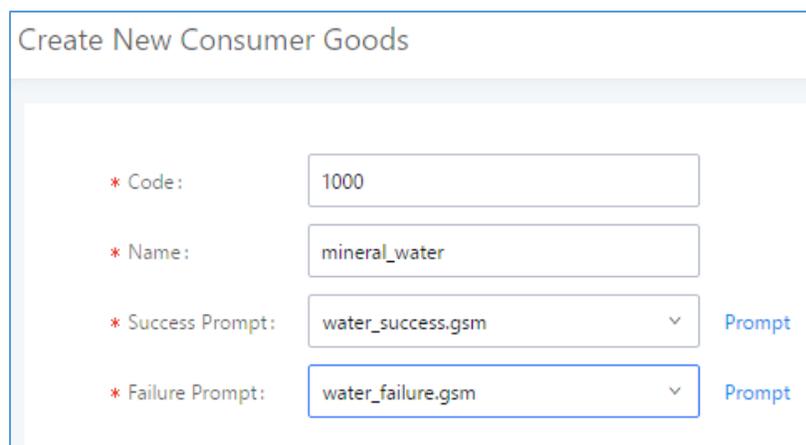


Figure 216: Create New Consumer Goods

Code	Enter the Goods Code.
Name	Enter the Name of the Goods
Success Prompt	Select the success prompt when typing the code of the goods by the maid.
Failure Prompt	Select the failure prompt.



The Minibar page displays as:

PMS

Basic Settings Room Status Wakeup Service **Mini Bar**

+ Create New Mini Bar

Code	Name	Options
4000	MiniBar	 

+ Create New Maid

Maid Code	Secret	Options
1100	123456	 

Total: 1 < 1 > 10 条/页 跳至 1 页

+ Create New Consumer Goods

Code	Name	Options
7000	mineral_water	 

Total: 1 < 1 > 10 条/页 跳至 1 页

Figure 217: Mini Bar



WAKEUP SERVICE

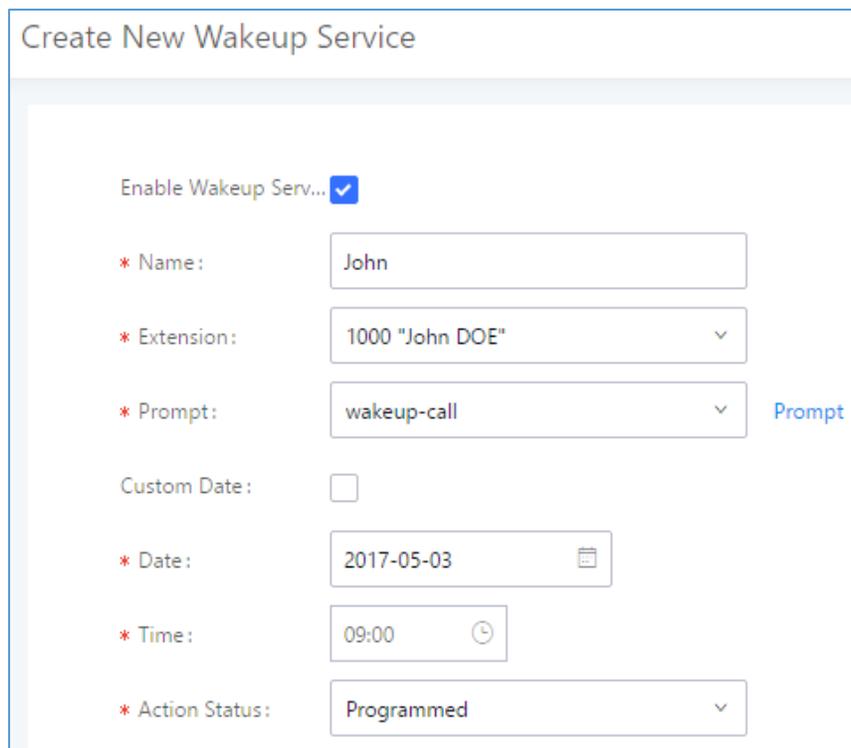
The WakeUp service can be used to schedule a reminder or wake up calls to any valid destination. This service is available on the UCM6510 as a separated module.

There are three ways to set up Wakeup Service:

- Using admin login
- Using user portal
- Using feature code

WakeUp Service using admin login

1. Login to the UCM as admin.
2. WakeUp service can be found under Web GUI→**Value-added Features**→**Wakeup Service**, click on  to create a new wakeup service. The following window will popup.



Create New Wakeup Service

Enable Wakeup Serv...

* Name:

* Extension:

* Prompt: Prompt

Custom Date:

* Date:

* Time:

* Action Status:

Figure 218: Create New Wakeup Service

3. Click  and  to apply the changes.



Table 114: Wakeup Service

Enable Wakeup Service	Enable Wakeup service.
Name	Enter a name to identify the wakeup service.
Extension	Select the extension to call.
Prompt	Select the prompt to play for that extension.
Custom Date	If disabled, users can select a specific date and time. If enabled users can select multiple days of the week to perform the wakeup.
Date	Select the date or dates when to performs the wakeup call.
Time	Select the time when to play the wakeup call.

WakeUp service from User portal

1. Login to the user portal on the UCM6510.
2. WakeUp service can be found under “Value-added Features→Wakeup Service”, click on  to create a new wakeup service.
3. Configures the Name, Prompt, Date and Time for the user to make the wakeup to.
4. Click  and  to apply the changes.

WakeUp service using feature code

- Login to the UCM as admin.
- Enable “Wakeup Service” from the WebGUI under “PBX→Internal Options→Feature Codes”.



The screenshot shows a configuration page for Feature Codes. It contains several rows of settings, each with a label, a text input field, and a checkbox. The 'Wakeup Service' row is highlighted with an orange border. The settings are as follows:

* Listen Spy:	<input type="text" value="*54"/>	
* Barge Spy:	<input type="text" value="*56"/>	
* PMS Wakeup Servi...	<input type="text" value="*35"/>	<input checked="" type="checkbox"/>
* Presence Status:	<input type="text" value="*48"/>	<input checked="" type="checkbox"/>
* Whisper Spy:	<input type="text" value="*55"/>	
* Wakeup Service:	<input type="text" value="*36"/>	<input checked="" type="checkbox"/>
* Update PMS Room...	<input type="text" value="*23"/>	<input checked="" type="checkbox"/>

Figure 219: Wakeup Service Feature Code

- Click  and  to apply the changes.
- Dial “*36” which is the feature code by default to access to the UCM wakeup service in order to add, update, activate or deactivate UCM wakeup service.



ANNOUNCEMENTS CENTER

UCM6510 supports Announcements Center features start from firmware 1.0.2.7. Announcements Center allows user to previously record and store voice message into UCM6510 with a specified code, and user can also create groups with specified extensions. When code and group number is dialed together, the specified voice message is sent to all group members and only extensions in the group will hear the voice message.

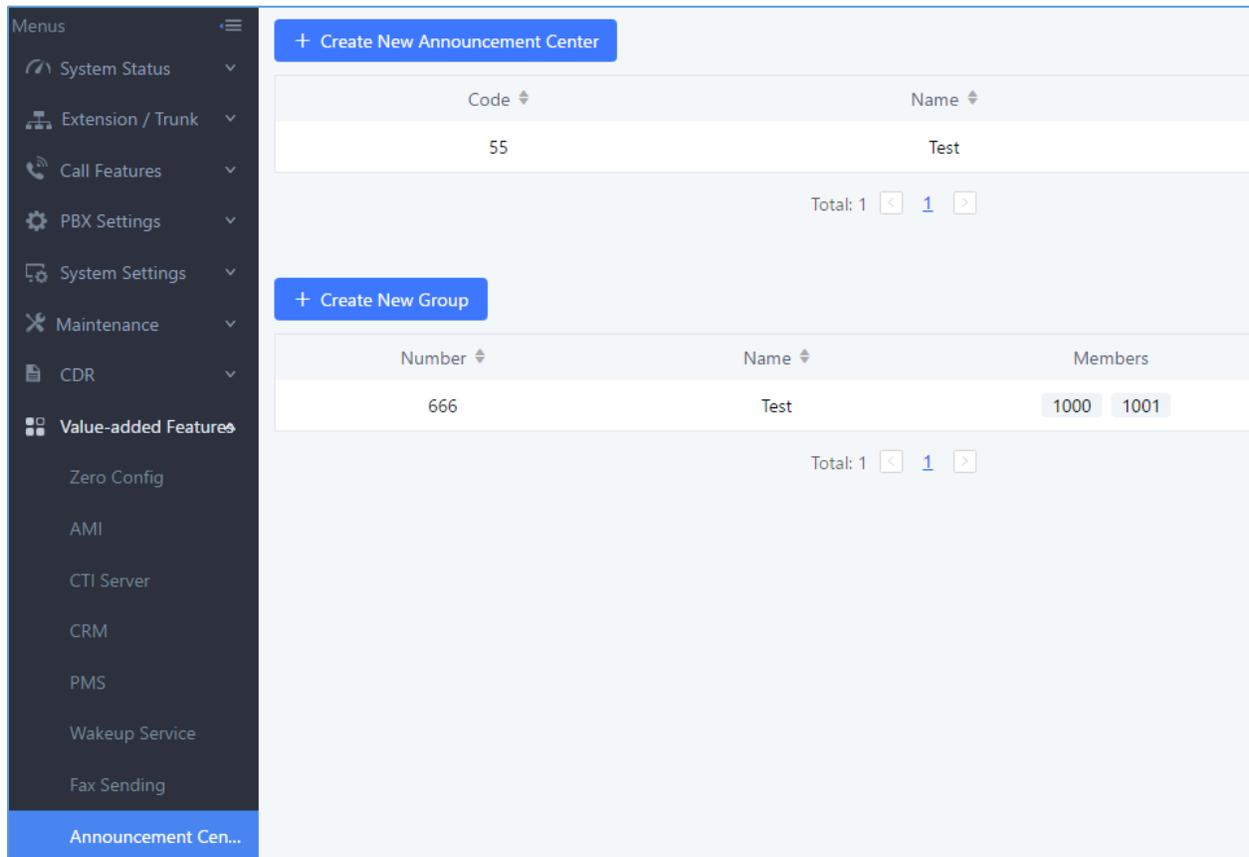


Figure 220: Announcements Center

Announcements Center Setting

Table 115: Announcements Center Setting

Name	Configure a name for the newly created Announcements Center, the name can be anything.
Code	Enter a code number for the customer prompt. This code is used in combination with group number. For example, if the code is 55, and group number is 666. User dial 55666 will send prompt 55 to all members in group 666.



	Note: The final number must not conflict with any number, like extensions or conference number.
Custom Prompt	This option is for setting a custom prompt as an announcement to notify group members. The file can be uploaded from page 'Custom Prompt'. Click 'Prompt' to add additional record.
Ring Timeout	Configure the ring timeout for the group members. The default value is 30 seconds.

Group Setting

Table 116: Group Setting

Name	Configure a name for the newly created group, the name can be anything.
Number	Configure the group number. The group number is used in combination with code. For example, if group number is 666, and code is 55. User dials 55666 will send prompt 55 to all members in group 666. Note: The group number must not conflict with any other numbers, such as extension or conference number.

Announcements Center feature can be found under Web GUI → **Value-added Features** → **Announcements Center**. The following example demonstrates the usage of this feature.

1. Click  to create new group.
2. Give a name for the newly created group, and the Number is used later with code to send voice message.
3. Select the extensions that want to be included in the group.



Create New Group

* Name:

* Number:

Members:

Available	Selected
<input type="checkbox"/> 1 <input type="checkbox"/> 1005 "Fax Extension"	<input type="checkbox"/> 3 <input type="checkbox"/> 1000 "John DOE" <input type="checkbox"/> 1001 <input type="checkbox"/> 1002

Figure 221: Announcements Center Group Configuration

In this example, Group Test has number 666, and extension 1000, 1001 and 1002 is in the current group.

1. Click [+ Create New Announcement Center](#) to create a new Announcement Center.
2. Give a name for the newly created Announcements Center, and the Code is used to specify the message that will be sent to the group.
3. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click Prompt and follow the instruction.

Create New Announcement Center

* Name:

* Code:

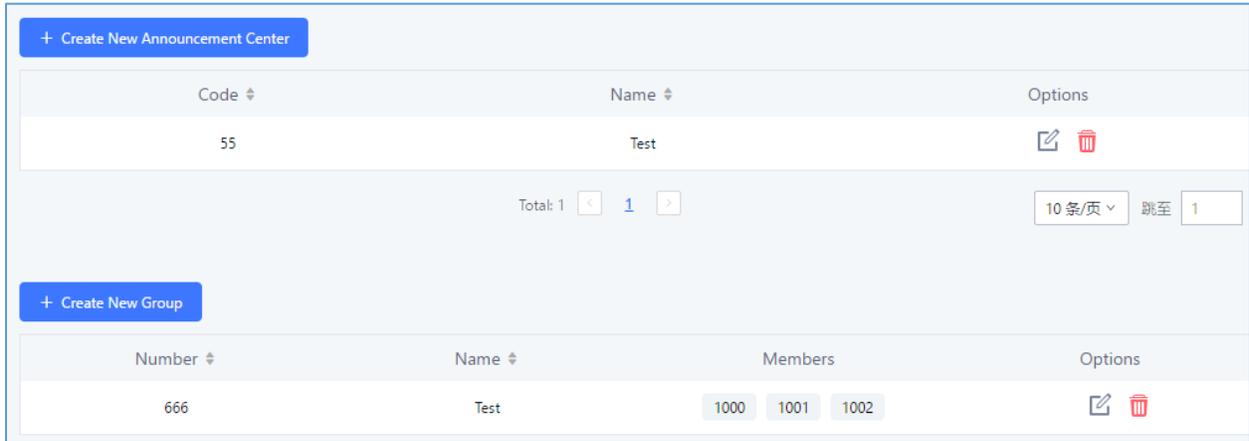
* Custom Prompt: Prompt

* Ring Timeout:

Figure 222: Announcements Center Code Configuration

Code and Group number are used together to direct specified message to the target group. All extensions in the group will received the message. For example, in this example, we can send code 55 to group 666.

To use, we can simply pick up any extension registered at UCM6510, dial number 55666 which is the code with the group number. Extension 1000, 1001 and 1002 will receive this voice message.



The screenshot displays two sections of the Grandstream management interface. The top section, titled '+ Create New Announcement Center', contains a table with the following data:

Code	Name	Options
55	Test	 

Below the table, there is a pagination control showing 'Total: 1' and a dropdown menu set to '10 条/页'. A '跳至' (Jump to) field is set to '1'.

The bottom section, titled '+ Create New Group', contains a table with the following data:

Number	Name	Members	Options
666	Test	1000 1001 1002	 

Figure 223: Announcements Center example



STATUS AND REPORTING

PBX Status

The UCM6510 monitors the status for Trunks, Extensions, Queues, Conference Rooms, Interfaces, Digital Channels and Parking lot. It presents administrators the real-time status in different sections under Web GUI → **System Status** → **Dashboard**.

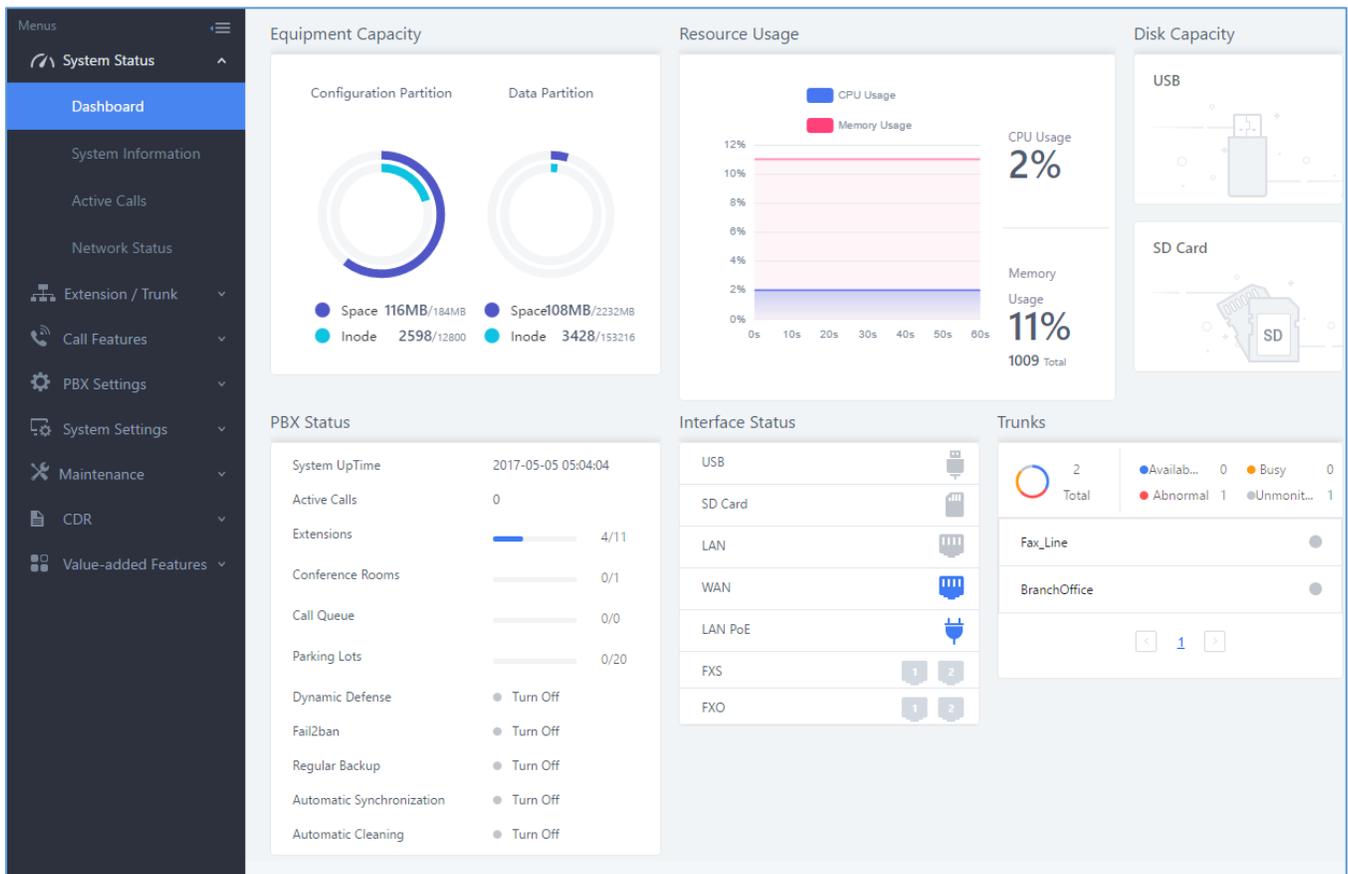


Figure 224: Status → PBX Status

Trunks

Users could see all the configured trunk status in this section.



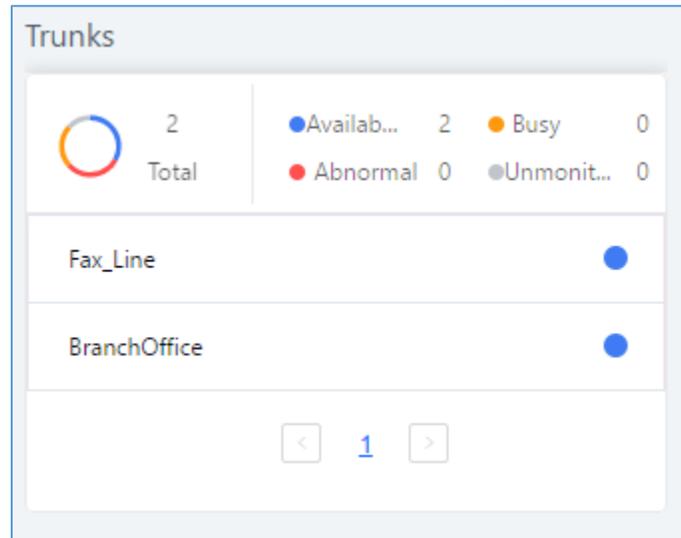


Figure 225: Trunk Status

Table 117: Trunk Status

Status	Display trunk status. <ul style="list-style-type: none"> Analog trunk/Digital trunk status: <ul style="list-style-type: none"> Available Busy Unavailable Unknown Error Error Configured: Incorrect signaling configuration between the two devices. For example, both of the devices are configured as CPE or NET. SIP Peer trunk status: <ul style="list-style-type: none"> Unreachable: The hostname cannot be reached. Unmonitored: QUALIFY feature is not turned on to be monitored. Reachable: The hostname can be reached. SIP Register trunk status: <ul style="list-style-type: none"> Registered Unrecognized Trunk
Trunks	Display trunk name
Type	Display trunk Type: <ul style="list-style-type: none"> Analog E1/T1/J1 SIP IAX
Username	Display username for this trunk.
Port/Hostname/IP	Display Port for analog trunk, or Hostname/IP for VoIP (SIP/IAX) trunk.

Extensions

Extensions Status can be seen from the same configuration page, users can go under Web GUI→**Extension/Trunk**→**Extensions** and following page will be displayed listing the extensions and their status information.

Follow Me Options		Search						
<input type="checkbox"/>	Status	Presence Status	Extension	CallerID Name	Terminal Type	IP and Port	Email Status	Options
<input type="checkbox"/>	In Use	Available	1000	John DOE	SIP	192.168.6.238:46365		
<input type="checkbox"/>	Unavailable	Available	1001		SIP	--		
<input type="checkbox"/>	In Use	Available	1002		SIP	192.168.6.238:46365		
<input type="checkbox"/>	Ringing	Available	1003		SIP	192.168.6.102:5060		
<input type="checkbox"/>	Idle	Available	1004		SIP	192.168.6.102:5062		

Figure 226: Extension Status

Table 118: Extension Status

Status	Display extension number (including feature code). The color indicator has the following definitions. <ul style="list-style-type: none"> ● Green: Free ● Blue: Ringing ● Yellow: In Use ● Grey: Unavailable
Presence Status	Display the presence status of the extension.
Extension	Display the extension number.
CallerID Name	First name and last name of the extension.
IP and Port	Display the IP and port number of the registered device.
Email	Display Email Notification status for the extension. When notification is waiting for be sent, shows and once sent it will display
Terminal Type	Displays extension type. <ul style="list-style-type: none"> ● SIP User ● IAX User ● Analog User ● Ring Groups ● Voicemail Groups



Interfaces Status

This section displays interface connection status on the UCM6510 for USB, SD Card, LAN, WAN, LAN PoE, Heartbeat, Power 1, Power 2, Digital, FXS and FXO ports.

Table 119: Interface Status Indicators

FXO	
	Disconnected
	Connected but not configured
	Connected and idle
	Connected and in use
FXS	
	Connected but not configured
	Connected and idle
	Connected and in use
SD Card	
	SD Card plugged in
	SD Card unplugged
USB	
	USB plugged in
	USB unplugged
LAN PoE	
	PoE is used



	PoE is not used
Power 1/2	
	Power supply is working
	Power supply is abnormal
	No power supply
LAN/WAN/Heart Beat	
	Connected
	Not connected
Digital Port T1/E1/J1	
	Connected and working
	RED alarm: there is physical wiring problem, loss of connectivity, or a framing/line-coding mismatch with the remote switch.
	<p>YELLOW alarm: connected but the link is working only one-way. This means that the remote switch is not able to maintain sync with you, or is not receiving your transmission.</p> <p>The following example scenarios could trigger YELLOW alarm:</p> <ol style="list-style-type: none"> 1. The T1 port is connected with J1 connection. 2. Incorrect cable is used. 3. When using E1, one end is using CRC4 while the other end is not.

	<p>BLUE alarm: the port goes into BLUE alarm when it receives all unframed 1s on all timeslots from the remote switch. This is a special signal to indicate that the remote switch is having problem with its upstream connection.</p>
	<p>Cannot start up</p>

System Status

The UCM6510 system status can be accessed via Web GUI→**System Status**, which displays the following system information.

General

Under Web GUI→**System Status**→**System Information**→**General**, users could check the hardware and software information for the UCM6510. Please see details in the following table.

Table 120: System Status→General

System Status →System Information→General	
Model	Product model.
Part Number	Product part number.
System Time	Current system time. The current system time is also available on the upper right of each web page.
Up Time	System up time since the last reboot.
Idle Time	System idle time since the last reboot.
Boot	Boot version.
Core	Core version.
Base	Base version.
Program	Program version. This is the main software release version.
Recovery	Recovery version.

Network

Under Web GUI→**System Status**→**System Information**→**Network**, users could check the network information for the UCM6510. Please see details in the following table.

Table 121: System Status→Network

System Status→System Information→Network	
MAC Address	Global unique ID of device, in HEX format. The MAC address can be found on the label coming with original box and on the label located on the bottom of the device.
IP Address	IP address.
Gateway	Default gateway address.
Subnet Mask	Subnet mask address.
DNS Server	DNS Server address.

Storage Usage

Users could access the storage usage information from Web GUI→**System Status**→**Dashboard**→**Storage Usage**. It shows the available and used space for Space Usage and Inode Usage.

Space Usage includes:

- Configuration partition
- This partition contains PBX system configuration files and service configuration files.
- Data partition
- Voicemail, recording files, IVR file, Music on Hold files and etc.
- USB disk
- USB disk will display if connected.
- SD Card
- SD Card will display if connected.

Inode Usage includes:

- Configuration partition
- Data partition

Note: Inode is the pointer used for file reference in the system. The system usually has limited resources of pointers.



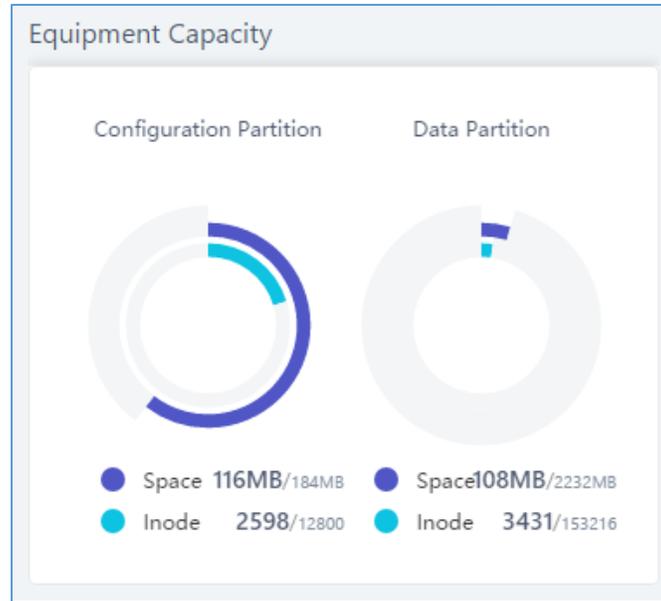


Figure 227: System Status→Storage Usage

Resource Usage

When configuring and managing the UCM6510, users could access resource usage information to estimate the current usage and allocate the resources accordingly. Under Web GUI→**System Status**→**Dashboard**→**Resource Usage**, the current CPU usage and Memory usage are shown in the pie chart.

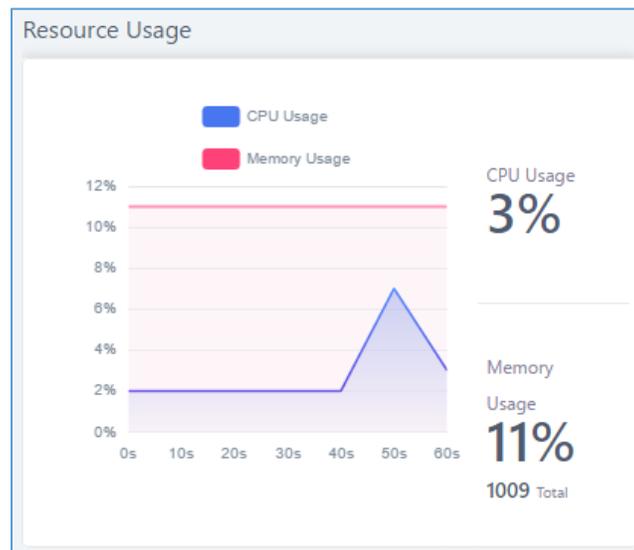


Figure 228: System Status→Resource Usage

System Events

The UCM6510 can monitor important system events, log the alerts and send Email notifications to the system administrator.

Alert Events List

The system alert events list can be found under Web GUI→**Maintenance**→**System Events**. The following event are currently supported on the UCM6510 which will have alert and/or Email generated if occurred:

Disk Usage

External Disk Usage

Modify Admin Password

Memory Usage

System Reboot

System Update

System Crash

Register SIP Failed

Register SIP Trunk Failed

Restore Config

User Login Success

User Login Failed

SIP Internal Call Failure

SIP Outgoing Call through Trunk Failure

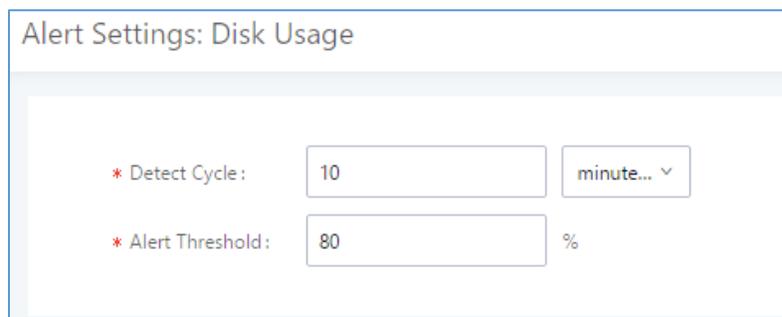
Fail2ban Blocking

SIP Lost Registration

SIP Peer Trunk Status

Click on  to configure the parameters for each event.

1. Disk Usage



The screenshot shows the 'Alert Settings: Disk Usage' configuration page. It contains two main settings:

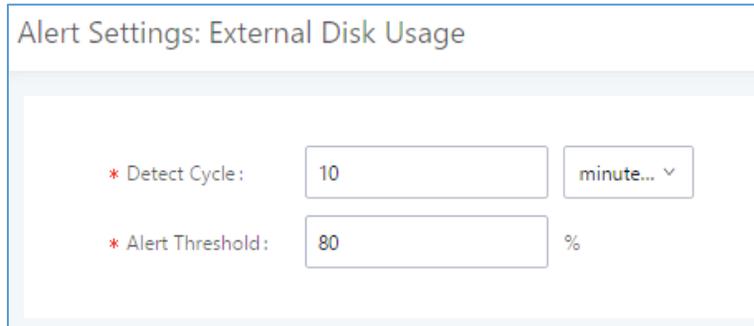
- * Detect Cycle:** A text input field containing the value '10' and a dropdown menu set to 'minute...'. The dropdown menu is currently open, showing 'minute...' as the selected option.
- * Alert Threshold:** A text input field containing the value '80' followed by a '%' symbol.

Figure 229: System Events→Alert Events Lists: Disk Usage



- **Detect Cycle:** The UCM6510 will perform the internal disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM6510 system will send the alert.

2. External Disk Usage



Alert Settings: External Disk Usage

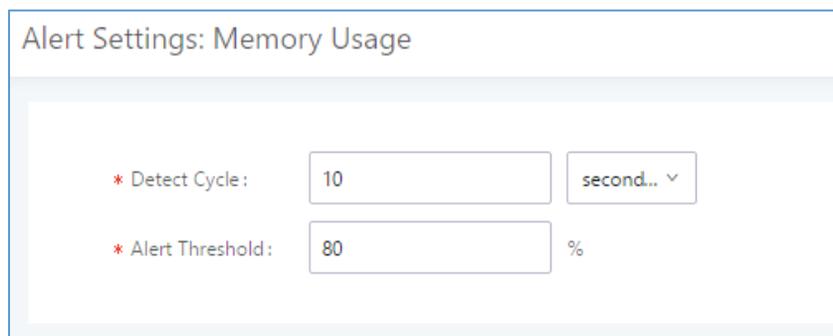
* Detect Cycle:

* Alert Threshold: %

Figure 230: System Events→Alert Events Lists: External Disk Usage

- **Detect Cycle:** The UCM6510 will perform the External disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM6510 system will send the alert.

3. Memory Usage



Alert Settings: Memory Usage

* Detect Cycle:

* Alert Threshold: %

Figure 231: System Events→Alert Events Lists: Memory Usage

- **Detect Cycle:** The UCM6510 will perform the memory usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the UCM6510 system will send the alert.



4. System Crash

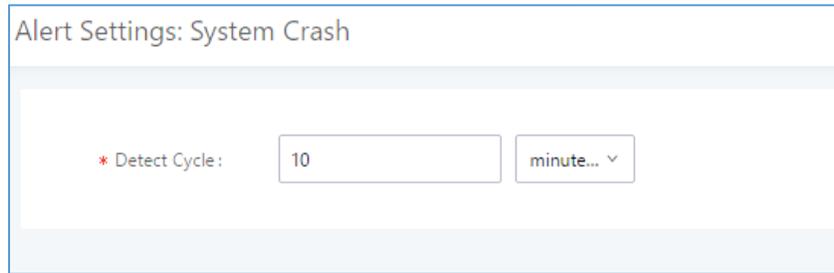


Figure 232: System Events→Alert Events Lists: System Crash

- Detect Cycle:** The UCM6510 will detect the event at each cycle based on the specified time. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

Click on the switch   to turn on/off the alert and Email notification for the event.

Users could also select the checkbox for each event and then click on button "Alert On", "Alert Off", "Email Notification On", "Email Notification Off" to control the alert and Email notification configuration.

Alert Log

Under Web GUI→**Status**→**System Events**→**Alert Log**, system messages are listed when the alert is triggered for the configured system events. The following picture shows disk usage alert log. We can tell the detect cycle for the disk usage is 10 minutes and the disk usage is restored to normal after the administrator cleans up the disk storage below the threshold.

2013-10-09 21:32:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 21:42:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 21:52:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 22:02:00	Disk Usage	Restore to normal	Disk usage has been restored to normal

Figure 233: System Events→Alert Log

The following screenshot shows system crash alert logs.



System Events

[Alert Log](#) Alert Events List Alert Contact

Alert Log Filter

Delete Search Result (s) Delete All

Time	Event Name	Type	Content
2017-05-04 04:33:20	User login success	Generate Alert	Logged in system successfully! The username is: adminIP:192.168.6.246
2017-05-04 04:33:15	User login failed	Generate Alert	Logged in system failed! The username is: adminIP:192.168.6.246

Figure 234: System Events→Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on Filter. Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.
2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

User could filter out alert logs of “Generate Alert” or “Restore to Normal” by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of “Restore to Normal”.

[Alert Log](#) Alert Events List Alert Contact

Alert Log Filter Reset

Event Name:

Type:

Start Time:

End Time:

Delete Search Result (s) Delete All

Time	Event Name	Type	Content
2017-05-04 04:33:15	User login failed	Generate Alert	Logged in system failed! The username is: adminIP:192.168.6.246

Figure 235: Filter for Alert Log



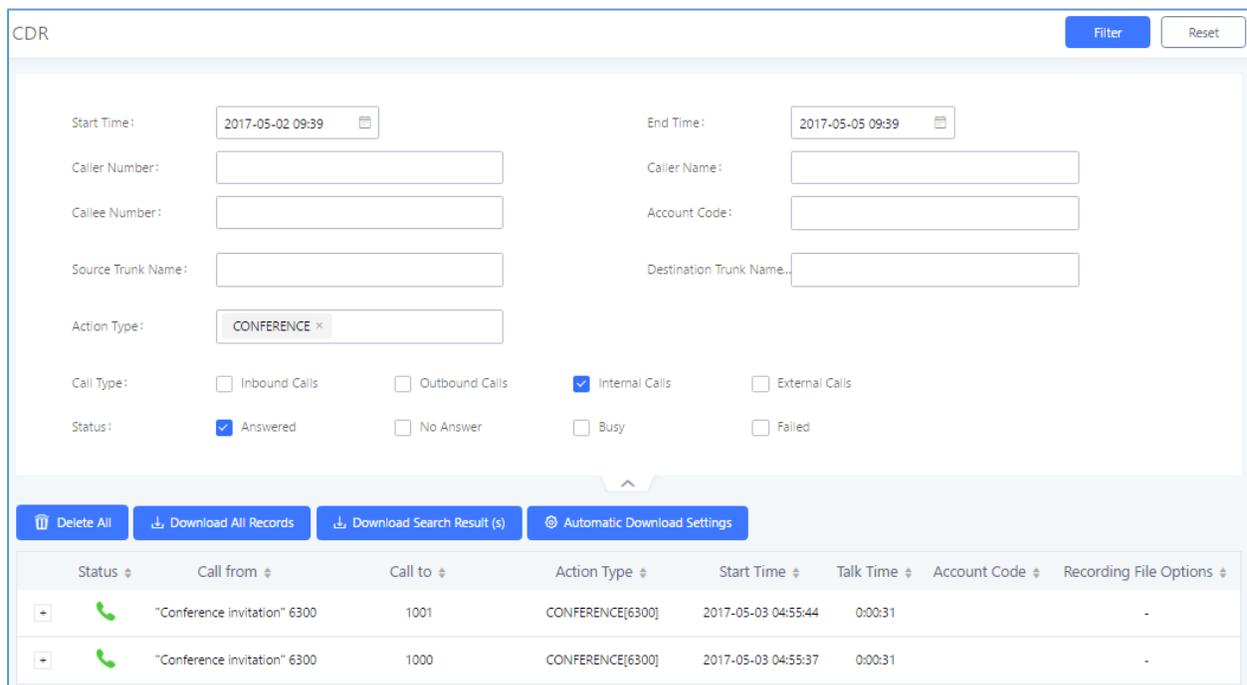
Alert Contact

Users could add administrator's Email address under Web GUI→**Maintenance**→**System Events**→**Alert Contact** to send the alert notification to. Up to 10 Email addresses can be added.

CDR

CDR (Call Detail Record) is a data record generated by the PBX that contains attributes specific to a single instance of phone call handled by the PBX. It has several data fields to provide detailed description for the call, such as phone number of the calling party, phone number of the receiving party, start time, call duration, and etc.

On the UCM6510, the CDR can be accessed under Web GUI→**CDR**→**CDR**. Users could filter the call report by specifying the date range and criteria, depending on how the users would like to include the logs to the report. Click on "Search" button to display the generated report.



Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options
	"Conference invitation" 6300	1001	CONFERENCE[6300]	2017-05-03 04:55:44	0:00:31		-
	"Conference invitation" 6300	1000	CONFERENCE[6300]	2017-05-03 04:55:37	0:00:31		-

Figure 236: CDR Filter

Table 122: CDR Filter Criteria

Call Type	Groups the following:
	<ul style="list-style-type: none"> Inbound calls: Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension. Outbound calls: Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension.



	<ul style="list-style-type: none"> • Internal calls: Internal calls are calls from one internal extension to another extension, which are not sent over a trunk. • External calls: External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension.
Status	Filter with the call status, the available statuses are the following: <ul style="list-style-type: none"> • Answered • No Answer • Busy • Failed
Source Trunk Name	Select source trunk(s) and the CDR of calls going through inbound the trunk(s) will be filtered out.
Destination Trunk Name	Select destination trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.
Action Type	Filter calls using the Action Type, the following actions are available: <ul style="list-style-type: none"> • Dial • Announcements • Callback • Call Forward • Conference • Disa • Fax • Follow Me • IVR • Page • Parked Call • Queue • Ring Group • Transfer • VFax • VM • VMG • Wakeup
Account Code	Select the account Code to filter with. If pin group CDR is enabled, the call with pin group information will be displayed as part of the CDR under Account Code Field.
Start Time	Specify the start time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
End Time	Specify the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
Caller Number	Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out.



	<p>User could specify a particular caller number or enter a pattern. '.' matches zero or more characters, only appears in the end. 'X' matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end.</p> <p><u>For example:</u></p> <p>3XXX: It will filter out CDR that having caller number with leading digit 3 and of 4 digits' length.</p> <p>3.: It will filter out CDR that having caller number with leading digit 3 and of any length.</p>
Caller Name	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
Callee Number	Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out.

The call report will display as the following figure shows.

Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options
	"John DOE" 1000	1001	DIAL	2017-05-04 04:41:49	0:00:05		-

Figure 237: Call Report

The CDR report has the following data fields:

- Start Time**
 Format: 2016-09-03 00:06:16
- Call Type**
 Example:
 IVR
 DIAL
 WAKEUP
- Call From**
 Example format:
 "John Doe" 2000
- Call To**
 Example format:
 2002



- **Call Time**
Format: 0:00:02
- **Talk Time**
Format: 0:00:00
- **Account Code**
Example format:
Grandstream/Test
- **Status**
Answered, Busy, No answer or Failed.

Users could perform the following operations on the call report.

- **Sort by “Start Time”**
Click on the header of the column to sort the report by "Start Time". Clicking on "Start Time" again will reverse the order.
- **Download Searched Results**
Click on “Download Search Result(s)” to export the records filtered out to a .csv file.
- **Download All Records**
Click on “Download All Records” to export all the records to a .csv file.
- **Delete All**
On the bottom of the page, click on "Delete All" button to remove all the call report information.
- **Play/Download/Delete Recording File (per entry)**
If the entry has audio recording file for the call, the three icons on the most right column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

Click on  to play the recording file; click on  to download the recording file in .wav format;

click on  to delete the recording file (the call record entry will not be deleted).



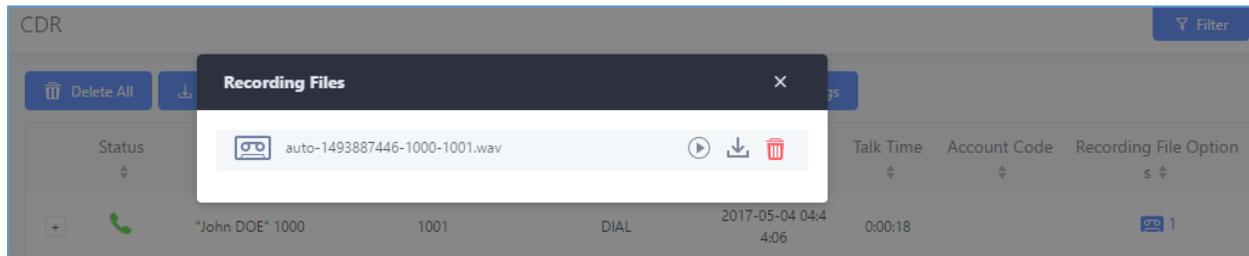


Figure 238: Call Report Entry with Audio Recording File

- **Automatic Download CDR Records**

User could configure the UCM6510 to automatically download the CDR records and send the records to an Email address. Click on “Automatic Download Settings”, and configure the parameters in the dialog below.

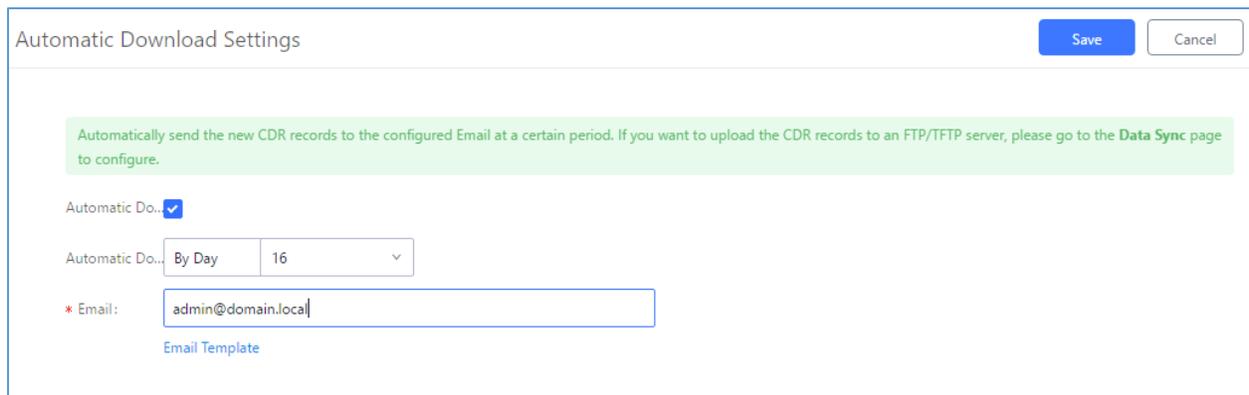


Figure 239: Automatic Download Settings

To receive CDR record automatically from Email, check “Enable” and select a time period “By Day” “By Week” or “By Month”, select Hour of the day as well for the automatic download period. Make sure you have entered an Email or multiple email addresses where to receive the CDR records.

CDR Improvement

Starting from UCM6510 firmware 1.0.10.x, transferred call will no longer be displayed as a separate call entry in CDR. It will display within call record in the same entry. CDR new features can be found under Web GUI→CDR→CDR. The user can click on the option icon for a specific call log entry to view details about this entry, such as premier caller and transferred call information.



Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options
	1002	1001	DIAL	2017-05-04 04:47:58	0:00:29		-

Figure 240: CDR Report

Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options																								
	1002	1001	DIAL	2017-05-04 04:47:58	0:00:29		-																								
<table border="1"> <thead> <tr> <th>Status</th> <th>Call from</th> <th>Call to</th> <th>Action Type</th> <th>Start Time</th> <th>Talk Time</th> <th>Account Code</th> <th>Recording File Options</th> </tr> </thead> <tbody> <tr> <td></td> <td>1002</td> <td>1001</td> <td>DIAL</td> <td>2017-05-04 04:47:58</td> <td>0:00:14</td> <td></td> <td>-</td> </tr> <tr> <td></td> <td>1002</td> <td>1002</td> <td>TRANSFER</td> <td>2017-05-04 04:48:13</td> <td>0:00:15</td> <td></td> <td>-</td> </tr> </tbody> </table>								Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options		1002	1001	DIAL	2017-05-04 04:47:58	0:00:14		-		1002	1002	TRANSFER	2017-05-04 04:48:13	0:00:15		-
Status	Call from	Call to	Action Type	Start Time	Talk Time	Account Code	Recording File Options																								
	1002	1001	DIAL	2017-05-04 04:47:58	0:00:14		-																								
	1002	1002	TRANSFER	2017-05-04 04:48:13	0:00:15		-																								

Figure 241: Detailed CDR Information

Downloaded CDR File

The downloaded CDR (.csv file) has different format from the Web GUI CDR. Here are some descriptions.

- **Caller number, Callee number**

"Caller number": the caller ID.

"Callee number": the callee ID.

If the "Source Channel" contains "DAHDI", this means the call is from FXO/PSTN line.

caller number	callee number	context	calerid	source channel	dest channel	lastapp
	2009	from-internal	"Wake Up Call" <WakeUp>	Local/2009@from-internal-00000001;2	PJSIP/2009-00000013	Dial
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	Dial
2009	1100	from-internal	"John Doe" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial
1100	2014	from-did-direct	"1100" <1100>	DAHDI/1-1	PJSIP/2014-00000017	Dial

Figure 242: Downloaded CDR File Sample

- **Context**

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.

ext-did-XXXXX: inbound calls. It starts with "ext-did", and "XXXXX" content varies case by case, which also relate to the order when the trunk is created.

ext-local: internal calls between local extensions.



- **Source Channel, Dest Channel**

Sample 1:

caller number	callee number	context	calerid	source channel	dest channel	disposition
2007	31100	from-internal	"" <2007>	PJSIP/2007-00000014	DAHDI/1-1	ANSWERED

Figure 243: Downloaded CDR File Sample - Source Channel and Dest Channel 1

DAHDI means it is an analog call, FXO or FXS.

For UCM6510, DAHDI/(1-2) are FXO ports, and DAHDI(3-4) are FXS ports.

Sample 2:

caller number	callee number	context	calerid	source channel	dest channel	lastapp
2009	1100	from-internal	"Mhammed Elmrabet" <2009>	PJSIP/2009-00000015	PJSIP/trunk_1-00000016	Dial

Figure 244: Downloaded CDR File Sample - Source Channel and Dest Channel 2

"SIP" means it's a SIP call. There are three possible format:

- (a) **PJSIP/NUM-XXXXXX**, where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.
- (c) **PJSIP/trunk_X/NUM**, where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.
- (c) **PJSIP/trunk_X-XXXXXX**, where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

There are some other possible values, but these values are almost the application name which are used by the dialplan.

IAX2/NUM-XXXXXXX: it means this is an IAX call.

Local/@from-internal-XXXXX: it is used internally to do some special feature procedure. We can simply ignore it.

Hangup: the call is hung up from the dialplan. This indicates there are some errors or it has run into abnormal cases.

Playback: play some prompts to you, such as 183 response or run into an IVR.

ReadExten: collect numbers from user. It may occur when you input PIN codes or run into DISA

Statistics

CDR Statistics is an additional feature on the UCM6510 which provides users a visual overview of the call report across the time frame. Users can filter with different criteria to generate the statistics chart.



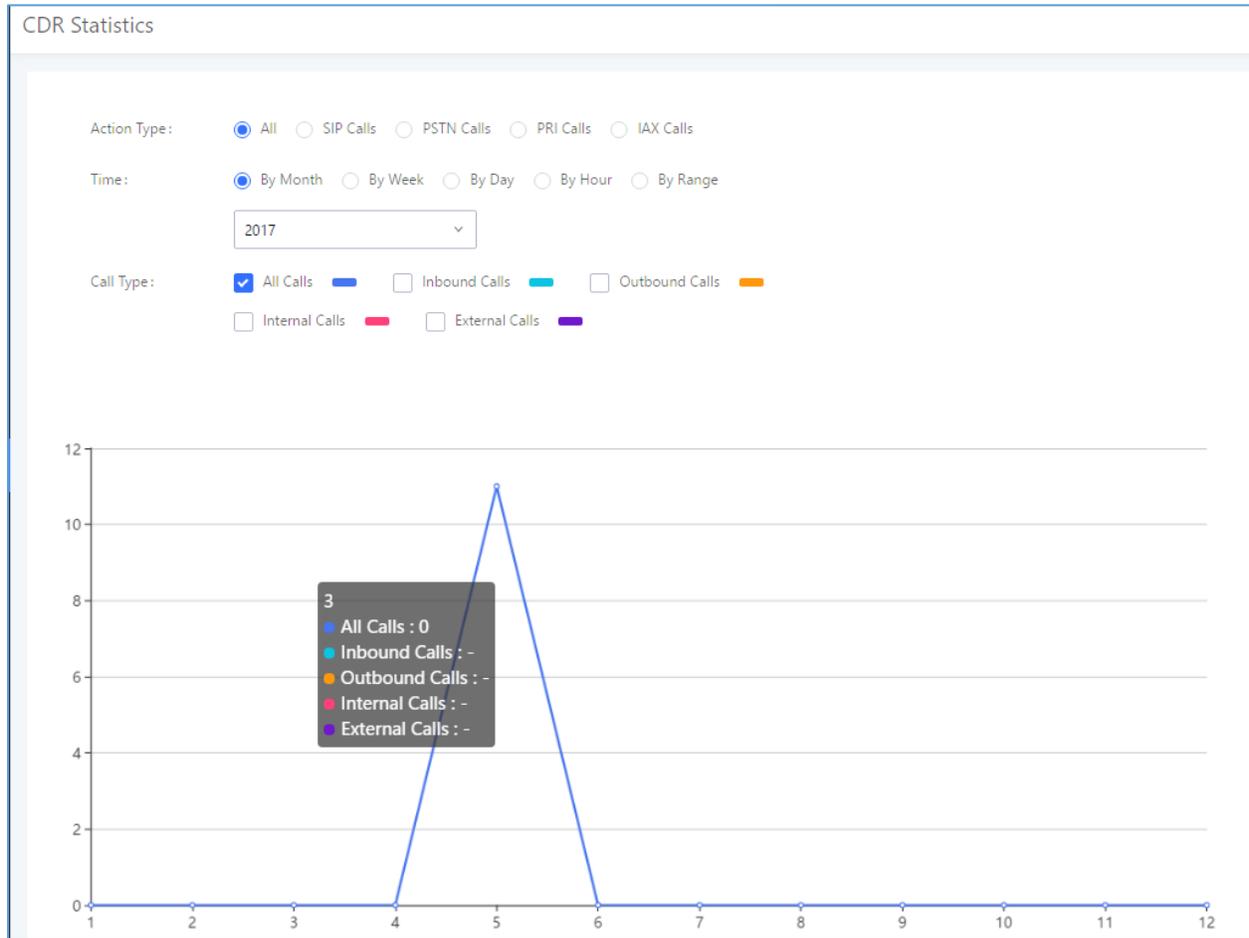


Figure 245: CDR Statistics

Table 123: CDR Statistics Filter Criteria

Trunk Type	Select one of the following trunk type. <ul style="list-style-type: none"> • All • SIP Calls • PSTN Calls
Call Type	Select one or more in the following checkboxes. <ul style="list-style-type: none"> • Inbound calls • Outbound calls • Internal calls • External calls • All calls
Time Range	<ul style="list-style-type: none"> • By month (of the selected year). • By week (of the selected year). • By day (of the specified month for the year). • By hour (of the specified date). • By range. For example, 2013-01 To 2013-03.



Recording Files

This page lists all the recording files recorded by "Auto Record" per extension/ring group/call queue/trunk, or via feature code "Audio Mix Record". If external storage device is plugged in, for example, SD card or USB drive, the files are stored on the external storage. Otherwise, internal storage will be used on the UCM6510.

<input type="checkbox"/> Delete Selected Recording Files <input type="button" value="Delete All Recording Files"/> <input type="button" value="Batch Download Recording Files"/> <input type="button" value="Download All Recording Files"/>						
<input type="checkbox"/>	Name ↕	Caller	Callee	Call Time	Size	Options
<input type="checkbox"/>	auto-1493887446-1000-1001.wav	1000	1001	2017-05-04 04:44:25 UTC-04:00	282.54 KB	<input type="button" value="Download"/> <input type="button" value="Delete"/>

Figure 246: CDR→Recording Files

- Click on "Delete Selected Recording Files" to delete the recording files.
- Click on "Delete All Recording Files" to delete all recording files.
- Click on  to download the recording file in .wav format.
- Click on  to delete the recording file.
- To sort the recording file, click on the title "Caller", "Callee" or "Call Time" for the corresponding column. Click on the title again can switch the sorting mode between ascending order or descending order.

API Configuration Files

The UCM6510 supports third party billing interface API for external billing software to access CDR and call recordings on the PBX. The API uses HTTPS to request the CDR data and call recording data matching given parameters as configured on the third-party application.

Before accessing the API, the administrators need enable API and configure the access/authentication information on the UCM6510 first. The API configuration parameters are listed in the table below.

Table 124: CDR API Configuration Files

Enable	Enable/Disable CDR API. The default setting is disabled.
TLS Bind Address	Configure the IP address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional and the default port number is 8443. The IP address must match the common name (host name) in the certificate so that the TLS socket won't bind to multiple IP addresses. The default setting is 0.0.0.0:8443.



TLS Private Key	Upload TLS private key. The size of the key file must be under 2MB. This file will be renamed as 'private.pem' automatically.
TLS Cert	Upload TLS cert. The size of the certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection. This file will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.
Username	Configure the Username for API Authentication.
Password	Configure the Password for API Authentication.
Permitted IPs	Specify a list of IP addresses permitted by API. This creates an IP-specific access control list. Multiple entries are allowed. For example, "192.168.5.20/255.255.255.255" denies access from all IP addresses except 192.168.5.20 The default setting is blank, meaning all IPs will be denied. Users must set permitted IP address before connecting to the API.

For more details on CDR API (Access to Call Detail Records) and REC API (Access to Call Recording Files), please refer the document in the link here:

http://www.grandstream.com/sites/default/files/Resources/ucm6xxx_cdr_rec_api_guide.pdf

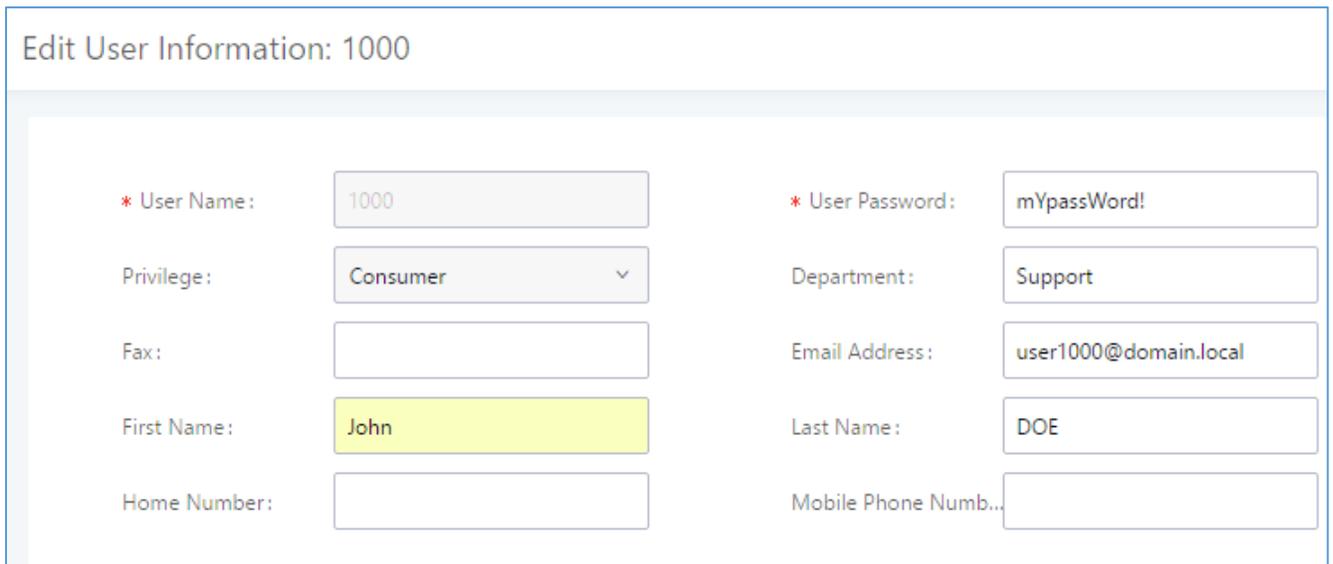


USER PORTAL

Users could log into their web GUI portal using the extension number and user password. When an extension is created in the UCM6510, the corresponding user account for the extension is automatically created. The user portal allows access to a variety of features which include user information, extension configuration and CDR as well as settings and managing value-added features like webRTC, Fax Sending, Call Queue, Wakeup Service and CRM.

Users also can access their personal data files (call recordings, Fax files, Voicemail Prompts ...).

The login credentials are configured by Super Admin. The following figure shows the dialog of editing the account information by Super Admin. The User Name must be the extension number and it's not configurable, and the password is set on "User Password" field and it should not be confused with the SIP extension password.



Edit User Information: 1000

* User Name:	<input type="text" value="1000"/>	* User Password:	<input type="text" value="mYpassWord!"/>
Privilege:	<input type="text" value="Consumer"/>	Department:	<input type="text" value="Support"/>
Fax:	<input type="text"/>	Email Address:	<input type="text" value="user1000@domain.local"/>
First Name:	<input type="text" value="John"/>	Last Name:	<input type="text" value="DOE"/>
Home Number:	<input type="text"/>	Mobile Phone Numb...:	<input type="text"/>

Figure 247: Edit User Information by Super Admin

The following screenshot shows an example of login page using extension number 1000 as the username.



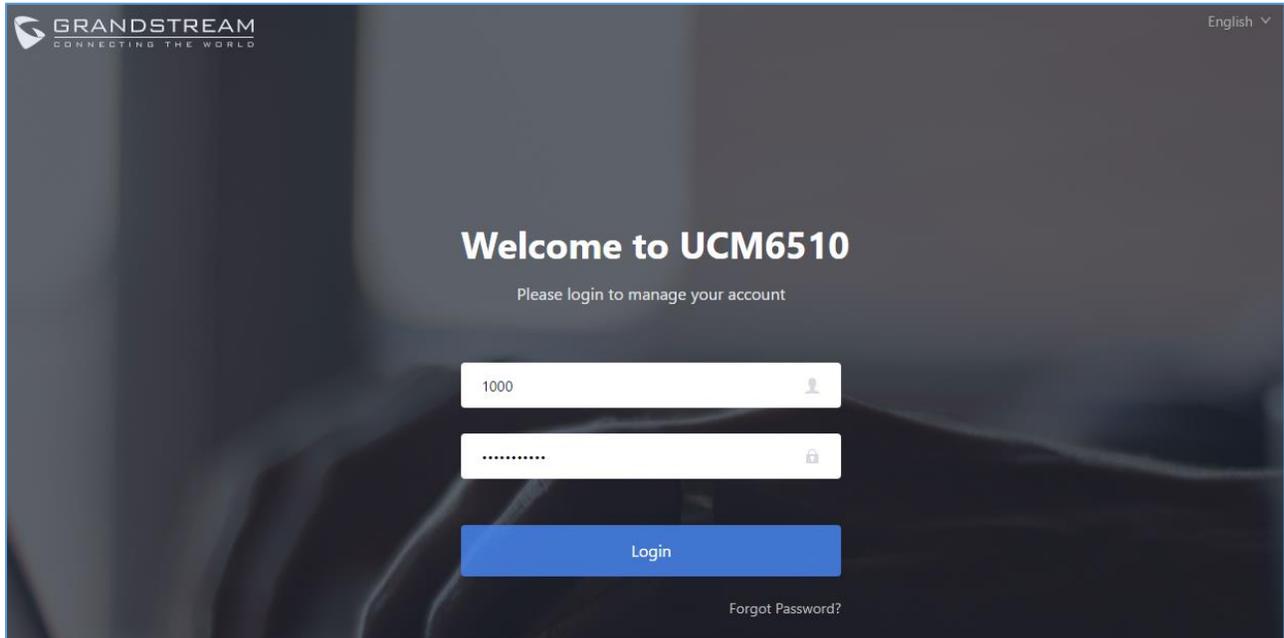


Figure 248: User Portal Login

After login, the Web GUI display is shown as below.

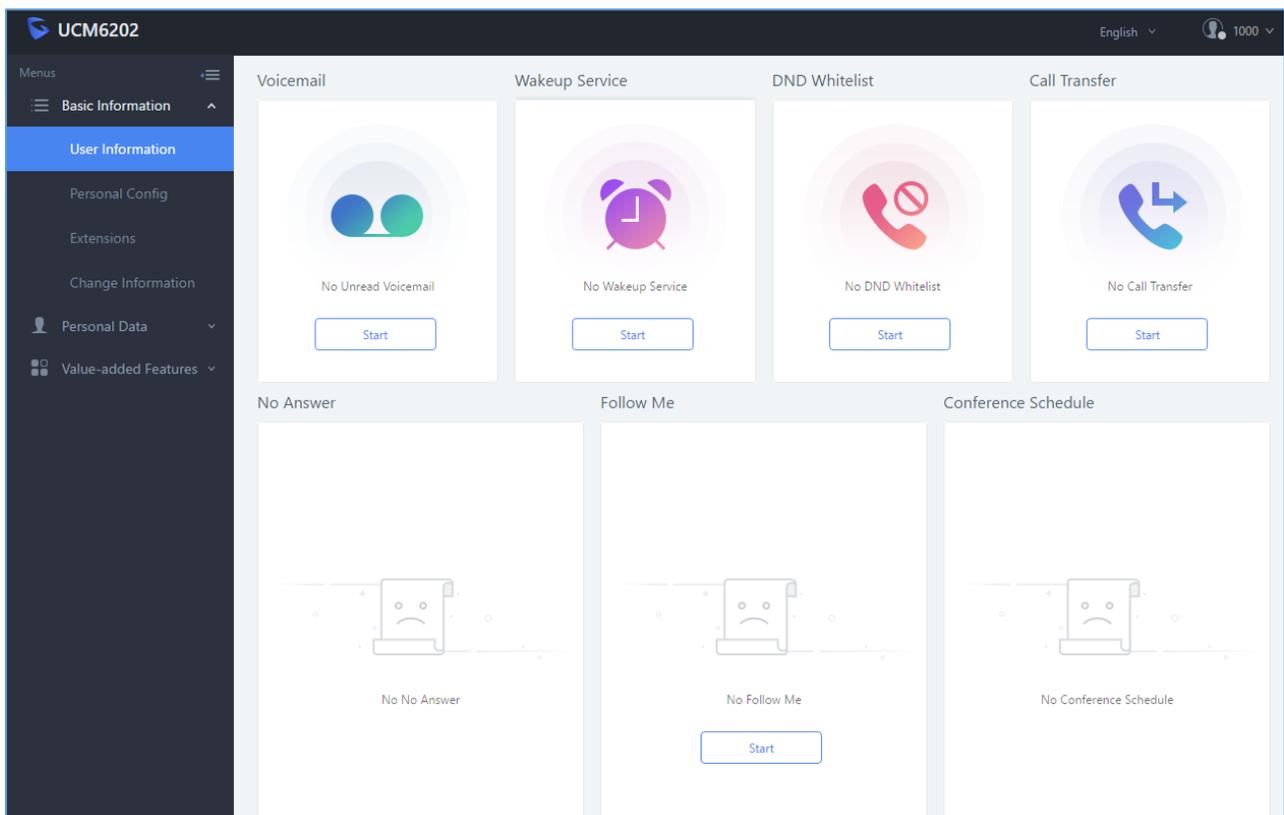


Figure 249: User Portal Layout



After successful login, the user has the following three configuration tabs:

Basic Information

Under this menu, the user can configure and change his/her personal information including (first name, last name, password, email address, department...). And they can also set and activate their extension features (presence status, call forward, DND) to be reflected on the UCM.

Also, the user can see from this menu the Call Details Records and search for specific ones along with the possibility to download the records on CSV format for later usage.

Personal Data

Under this section, the user can access and manage their personal data files which includes (voicemail files, call recordings, and fax files) along with the possibility to set Follow me feature to without requesting the Super admin to set the feature from admin account.

Value-added Features

On this section, the user has access to manage and use all rich value-added features which includes.

- WebRTC connection and making calls from the browser.
- Sending Fax files using PDF or TIF/TIFF format.
- If user is a member of call queue, they can check the queue's activity from the "Call Queue" section.
- Create and enable WakeUp service.
- Enable and configure CRM connection to either SugarCRM or Salesforce.

For the configuration parameter information in each page, please refer [\[Table 5: User Management – Create New User\]](#) for options in **User Portal**→**Basic Information**→**User Information** page; please refer to [\[EXTENSIONS\]](#) for options in **User Portal**→**Basic Information**→**Extension** page; please refer to [\[CDR\]](#) for **User Portal**→**Basic Information**→**CDR** page.



MAINTENANCE

Upgrading

The UCM6510 can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your UCM6510 via network or local upload.

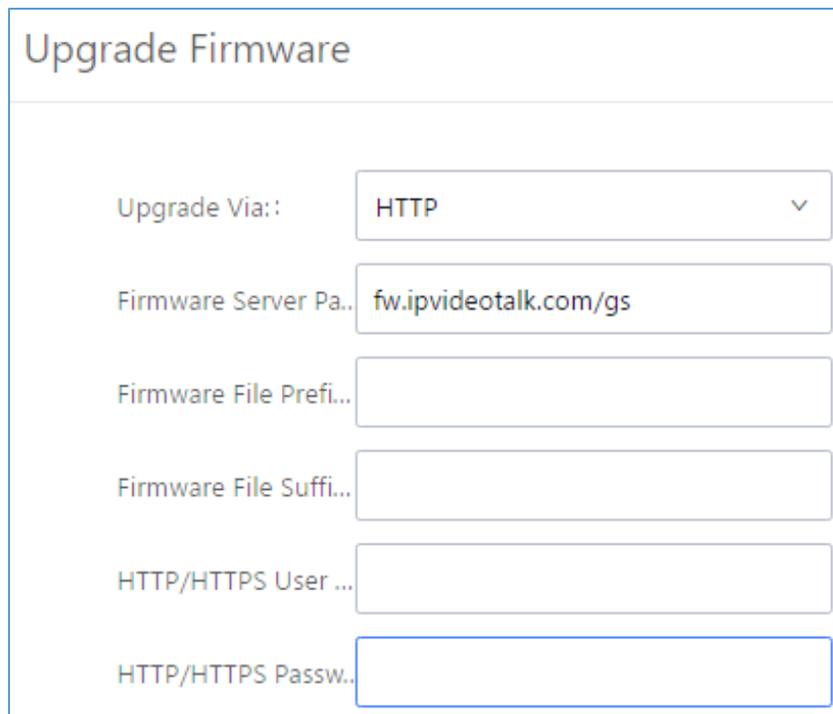
Upgrading via Network

The UCM6510 can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

The upgrading configuration can be accessed via Web GUI→**Maintenance**→**Upgrade**.



Upgrade Firmware

Upgrade Via: HTTP

Firmware Server Pa.. fw.ipvideotalk.com/gs

Firmware File Prefi..

Firmware File Suffi..

HTTP/HTTPS User ...

HTTP/HTTPS Passw..

Figure 250: Network Upgrade



Table 125: Network Upgrade Configuration

Upgrade Via	Allow users to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
Firmware Server Path	Define the server path for the firmware server.
Firmware File Prefix	If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the UCM6510.
Firmware File Suffix	If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the UCM6510.
HTTP/HTTPS User Name	The user name for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.

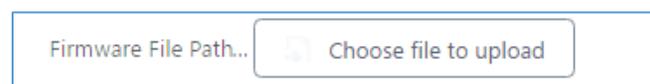
Please follow the steps below to upgrade the firmware remotely.

1. Enter the firmware server path under Web GUI→**Maintenance**→**Upgrade**.
2. Click on "Save". Then reboot the device to start the upgrading process.
3. Please be patient during the upgrading process. Once done, a reboot message will be displayed in the LCD.
4. Manually reboot the UCM6510 when it's appropriate to avoid immediate service interruption. After it boots up, log in the Web GUI to check the firmware version.

Upgrading via Local Upload

If there is no HTTP/TFTP server, users could also upload the firmware to the UCM6510 directly via Web GUI. Please follow the steps below to upload firmware locally.

1. Download the latest UCM6510 firmware file from the following link and save it in your PC.
2. <http://www.grandstream.com/support/firmware>
3. Log in the Web GUI as administrator in the PC.
4. Go to Web GUI→**Maintenance**→**Upgrade**, upload the firmware file by clicking on "Choose file to upload" and select the firmware file from your PC. The default firmware file name is ucm6510fw.bin


Figure 251: Local Upgrade

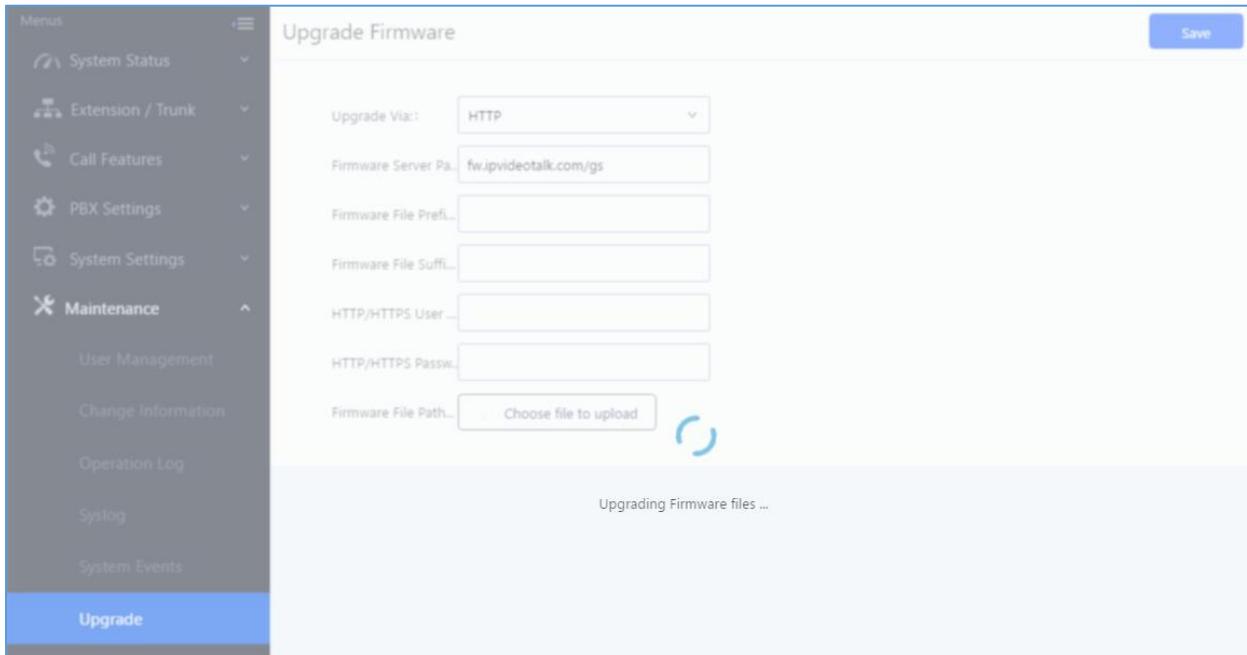



Figure 252: Upgrading Firmware Files

1. Wait until the upgrading process is successful and a window will be popped up in the Web GUI.

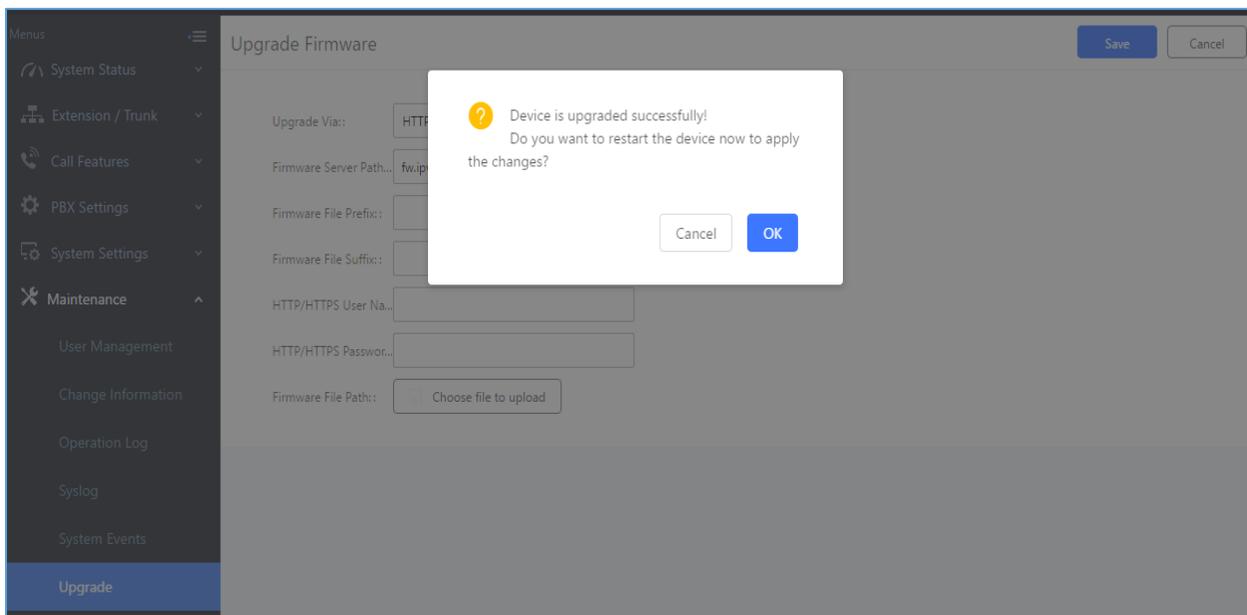


Figure 253: Reboot UCM6510

2. Click on "OK" to reboot the UCM6510 and check the firmware version after it boots up.



**Notes:**

- Please do not interrupt or power cycle the UCM6510 during upgrading process.
 - The firmware file name allows the use of the following special characters: “_@#*~&”.
-

No Local Firmware Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have TFTP/HTTP/HTTPS server. Some free windows version TFTP servers are available for download from http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
<http://tftpd32.jounin.net>

Please check our website at <http://www.grandstream.com/support/firmware> for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the UCM6510 to the same LAN segment;
3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the UCM6510 web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the UCM6510.

End users can also choose to download a free HTTP server from <http://httpd.apache.org/> or use Microsoft IIS web server.

Backup

The UCM6510 configuration can be backed up locally or via network. The backup file will be used to restore the configuration on UCM6510 when necessary.

Backup/Restore

Users could backup the UCM6510 configurations for restore purpose under Web GUI→**Maintenance**→**Backup**→**Backup/Restore**. Click on  to create a new backup. Then the following dialog will show.



Create New Backup

[Backup](#)

Choose Backup Fil... Config File CDR Records

Recording Files Fax Files

Voice Mail

Voice Prompt Files

ZeroConfig Storage

All

* Choose Storage ...

* File Name:

Warning: backing up data files could take a while and may require larger disk space. Please use an SD card, USB disk or other external storage devices.

Figure 254: Create New Backup

1. Choose the files to be included in the backup.
2. Choose where to store the backup file: USB Disk, SD Card or Local.
3. Name the backup file.
4. Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download , restore , or delete  it from the UCM6510 internal storage or the external device.

Click on [Upload Backup File](#) to upload backup file from the local device to UCM6510. The uploaded backup file will also be displayed in the web page and can be used to restore the UCM6510.

Backup Configuration

[+ Create New Backup](#)
[Upload Backup File](#)
[Regular Backup File](#)

List of Previous Configuration Backups

 Delete Selected Backup File (s)

	Name	Date	Size	Options
<input type="checkbox"/>	backup_2017504_083408.tar	2017-05-04 03:36:21 UTC-04:00	4.1 MB	  

Figure 255: Backup / Restore



The **Regular Backup File** option allows UCM6510 to perform automatically backup on the user specified time. Regular backup file can only be stored in USB / SD card / SFTP server. User is allowed to set backup time from 0-23 and how frequent the backup will be performed.

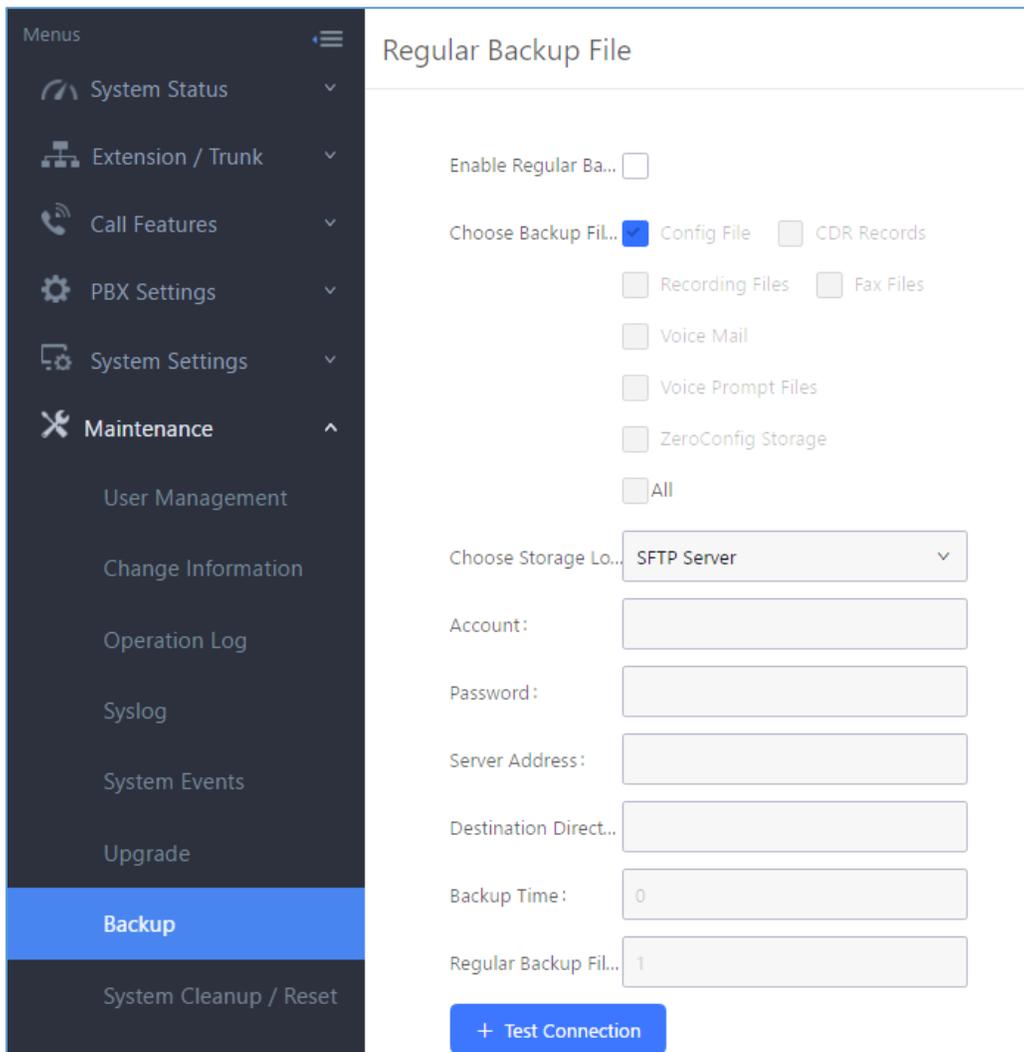


Figure 256: Local Backup

Data Sync

Besides local backup, users could backup the voice records/voice mails/CDR/FAX in a daily basis to a remote server via SFTP protocol automatically under Web GUI → **Maintenance** → **Backup** → **Data Sync**.

The client account supports special characters such as @ or “.”. This change allows user to use email address as SFTP accounts. It allows users as well to specify the destination directory on SFTP server for backup file. If the directory doesn't exist on the destination, UCM6510 will create the directory automatically.



Backup/Restore
Data Sync

Sync your voice records/voicemails/CDR/Fax every day via SFTP protocol automatically

Data Sync Configuration

Enable Data Sync:

Choose Data Sync Files: CDR Records Recording Files
 Voice Mail Fax

* Account:

Password:

* Server Address:

Destination Directory:

* Sync Time:

+ Test Connection
+ Synchronize All Data

Data Sync Log

Clean

Figure 257: Data Sync

Table 126: Data Sync Configuration

Enable Data Sync	Enable the auto backup function. The default setting is "No".
Account	Enter the Account name on the SFTP backup server.
Password	Enter the Password associate with the Account on the SFTP backup server.
Server Address	Enter the SFTP server address.
Destination Directory	Specify the directory in SFTP server to keep the backup file. Format: 'xxx/xxx/xxx', If this directory does not exist, UCM will create this directory automatically.
Sync Time	Enter 0-23 to specify the backup hour of the day.



Before saving the configuration, users could click on "Test Connection". The UCM6510 will then try connecting the server to make sure the server is up and accessible for the UCM6510.

Save the changes and all the backup logs will be listed on the web page.

Restore Configuration from Backup File

To restore the configuration on the UCM6510 from a backup file, users could go to Web GUI→**Maintenance**→**Backup**→**Backup/Restore**.

- A list of previous configuration backups is displayed on the web page. Users could click on  of the desired backup file and it will be restored to the UCM6510.
- If users have other backup files on PC to restore on the UCM6510, click on "Upload Backup File" first and select it from local PC to upload on the UCM6510. Once the uploading is done, this backup file will be displayed in the list of previous configuration backups for restore purpose. Click on  to restore from the backup file.
- User could also restore using the backup file saved in SD card or USB device plugged into the UCM6510.

Backup Configuration

+ Create New Backup
 Upload Backup File
Regular Backup File

List of Previous Configuration Backups

 Delete Selected Backup File (s)

<input type="checkbox"/>	Name ↕	Date ↕	Size ↕	Options
<input type="checkbox"/>	backup_2017504_083408.tar	2017-05-04 03:36:21 UTC-04:00	4.1 MB	  

Figure 258: Restore UCM6510 from Backup File

 **Note:**

- The uploaded backup file must be a tar file with no special characters like *,!,#,@,&,\$,%^,(,),/, \,space in the file name.
- The uploaded back file size must be under 10MB.



System Cleanup/Reset

Reset and Reboot

Users could perform reset and reboot under Web GUI→**Maintenance**→**Reset and Reboot**. To factory reset the device, select the mode type first. There are two different types for reset.

- **User Data**
All the data including voicemail, recordings, IVR Prompt, Music on Hold, CDR and backup files will be cleared.
- **All**
All the configurations and data will be reset to factory default.

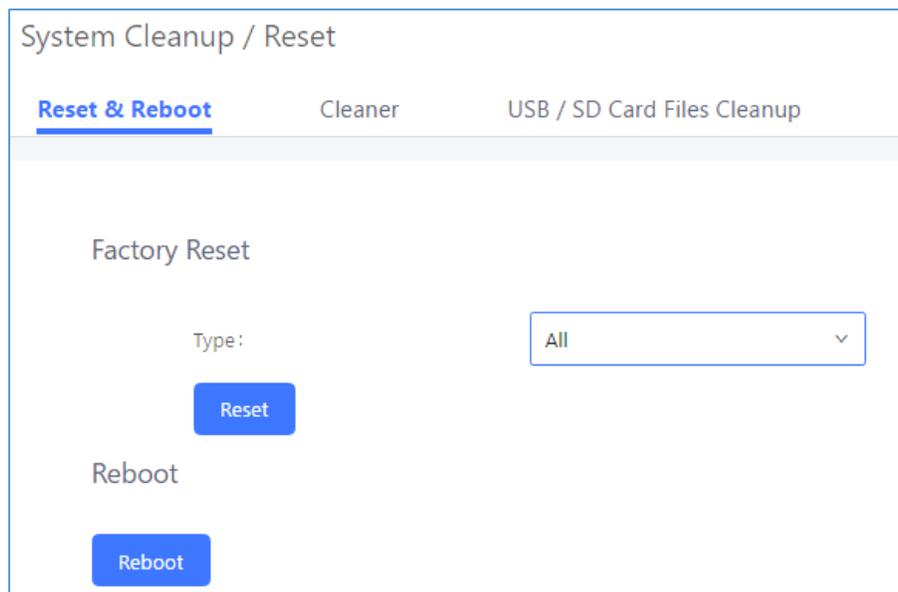


Figure 259: Reset and Reboot

Cleaner

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails/FAX automatically under Web GUI→**Maintenance**→**Cleaner**.



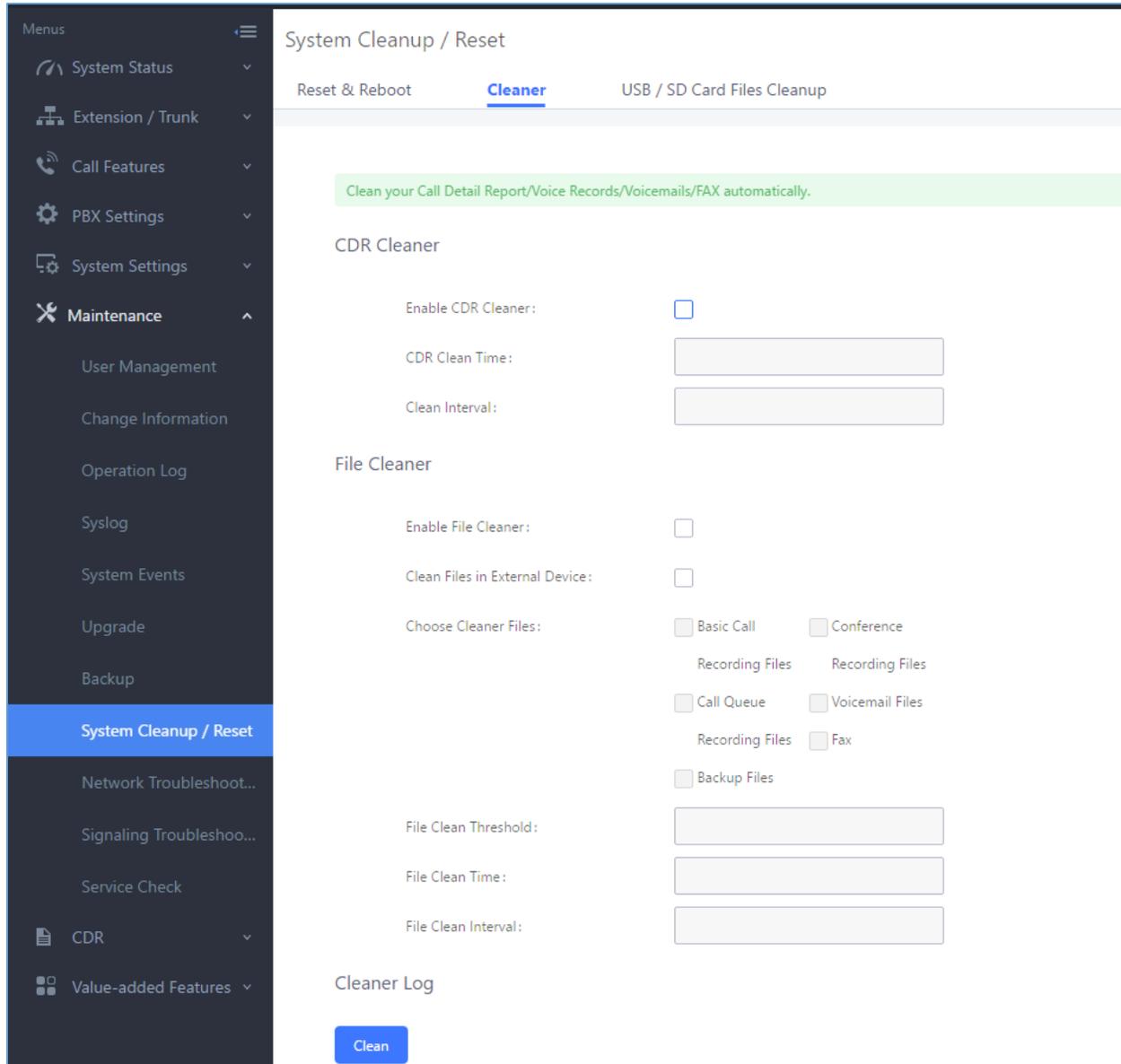


Figure 260: Cleaner

Table 127: Cleaner Configuration

Enable CDR Cleaner	Enable the CDR Cleaner function.
Clean Files in External Device	If enabled the files in external device (USB/SD card) will be atomically cleaned up as configured.
CDR Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Clean Interval	Enter 1-30 to specify the day of the month to clean up CDR.
Enable File Cleaner	Enter the Voice Records Cleaner function.
Choose Cleaner File	Select the files for system automatic clean. <ul style="list-style-type: none"> Basic Call Recording Files.

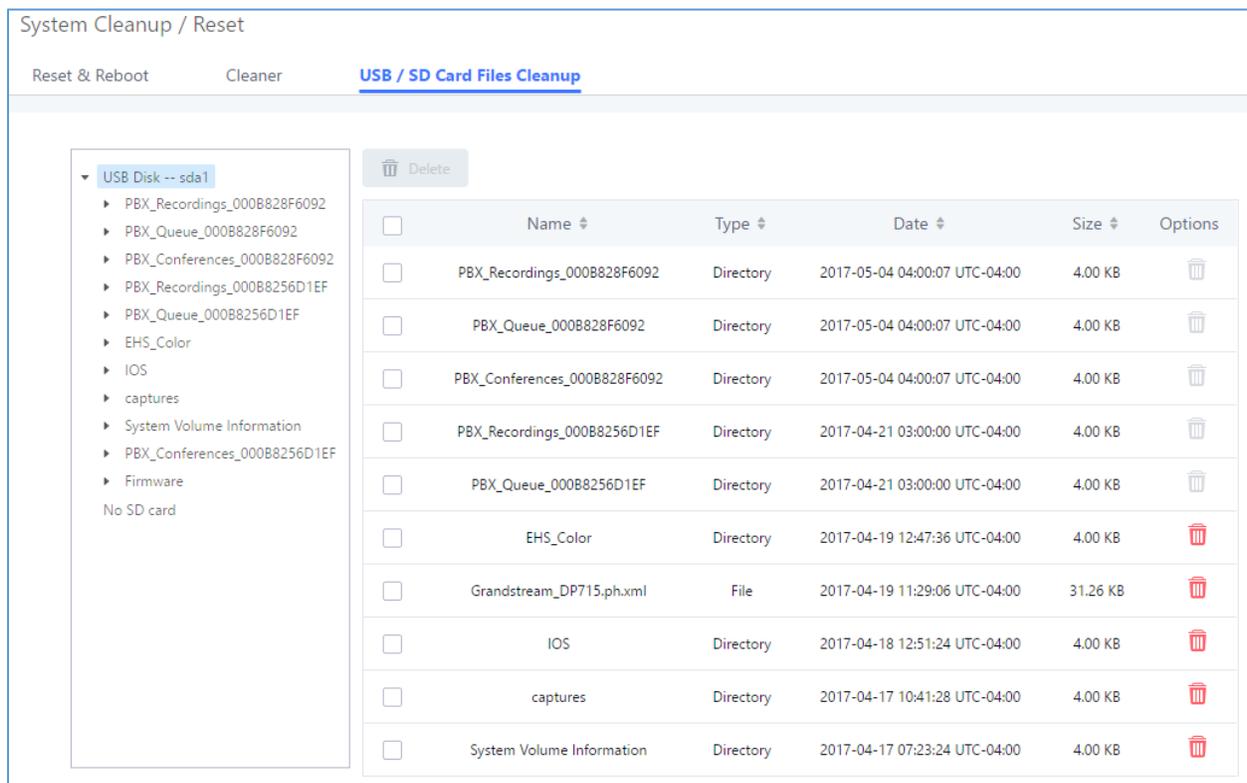


	<ul style="list-style-type: none"> • Conference Recording Files. • Call Queue Recording Files. • Voicemail Files. • Fax • Backup Files.
File Clean Threshold	Specify the threshold of local storage usage from 0 to 99 (in percentage).
File Clean Time	Enter 0-23 to specify the hour of the day to clean up the files.
File Clean Interval	Enter 1-30 to specify the day of the month to clean up the files.

All the cleaner logs will be listed on the bottom of the page.

USB/SD Card Files Cleanup

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails/FAX automatically under Web GUI→Maintenance→Cleaner→USB / SD Card Files Cleanup.



System Cleanup / Reset

Reset & Reboot Cleaner **USB / SD Card Files Cleanup**

Delete

USB Disk -- sda1

- ▶ PBX_Recordings_000B828F6092
- ▶ PBX_Queue_000B828F6092
- ▶ PBX_Conferences_000B828F6092
- ▶ PBX_Recordings_000B8256D1EF
- ▶ PBX_Queue_000B8256D1EF
- ▶ EHS_Color
- ▶ IOS
- ▶ captures
- ▶ System Volume Information
- ▶ PBX_Conferences_000B8256D1EF
- ▶ Firmware
- No SD card

<input type="checkbox"/>	Name	Type	Date	Size	Options
<input type="checkbox"/>	PBX_Recordings_000B828F6092	Directory	2017-05-04 04:00:07 UTC-04:00	4.00 KB	
<input type="checkbox"/>	PBX_Queue_000B828F6092	Directory	2017-05-04 04:00:07 UTC-04:00	4.00 KB	
<input type="checkbox"/>	PBX_Conferences_000B828F6092	Directory	2017-05-04 04:00:07 UTC-04:00	4.00 KB	
<input type="checkbox"/>	PBX_Recordings_000B8256D1EF	Directory	2017-04-21 03:00:00 UTC-04:00	4.00 KB	
<input type="checkbox"/>	PBX_Queue_000B8256D1EF	Directory	2017-04-21 03:00:00 UTC-04:00	4.00 KB	
<input type="checkbox"/>	EHS_Color	Directory	2017-04-19 12:47:36 UTC-04:00	4.00 KB	
<input type="checkbox"/>	Grandstream_DP715.ph.xml	File	2017-04-19 11:29:06 UTC-04:00	31.26 KB	
<input type="checkbox"/>	IOS	Directory	2017-04-18 12:51:24 UTC-04:00	4.00 KB	
<input type="checkbox"/>	captures	Directory	2017-04-17 10:41:28 UTC-04:00	4.00 KB	
<input type="checkbox"/>	System Volume Information	Directory	2017-04-17 07:23:24 UTC-04:00	4.00 KB	

Figure 261: USB/SD Card Files Cleanup

Table 128: USB/SD Card Files Cleanup

Current Path	Displays the current path.
Directory	Select the directory user want to clean.
Delete Selected File	Select multiple entries to delete from USB or SD card.



Syslog

On the UCM6510, users could dump the syslog information to a remote server under Web GUI→**Maintenance**→**Syslog**. Enter the syslog server hostname or IP address and select the module/level for the syslog information.

The default syslog level for all modules is "error", which is recommended in your UCM6510 settings because it can be helpful to locate the issues when errors happen.

Some typical modules for UCM6510 functions are as follows and users can turn on "notice" and "verb" levels besides "error" level.

pbx: This module is related to general PBX functions.

chan_sip: This module is related to SIP calls.

chan_dahdi: This module is related to analog calls (FXO/FXS).

app_meetme: This module is related to Conference Bridge.



Note:

Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog print might cause traffic and affect system performance.

Network Troubleshooting

On the UCM6510, users could capture traces, ping remote host and traceroute remote host for troubleshooting purpose under Web GUI→**Maintenance**→**Network Troubleshooting**.

Ethernet Capture

The captured trace can be downloaded for analysis. Instructions or result will be displayed in the Web GUI output result.



Network Troubleshooting

Ethernet Capture IP Ping Traceroute

Interface Type: Enable SFTP Data Sy...

Storage to External D... Capture Filter:

USB Disk

Output Result

Figure 262: Ethernet Capture

Table 129: Ethernet Capture

Interface Type	Select the network interface to monitor.
Enable SFTP Data Sync	Check this box to save the capture files in the SFTP server. Please make sure the configuration of data synchronization works before.
Storage to External Device	Check this box to activate storage of the capture either on the USB or SD Card.
Capture Filter	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto...).
Start	Click to start the trace.
Stop	Click to stop the trace.
Download	Click to download the trace if trace is stored locally.

The output result is in .pcap format. Therefore, users could specify the capture filter as used in general network traffic capture tool (host, src, dst, net, protocol, port, port range) before starting capturing the trace.

IP Ping

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



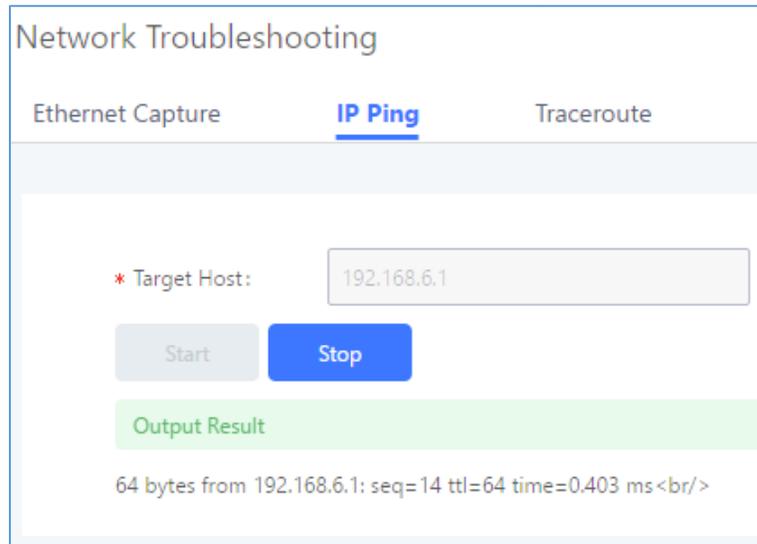


Figure 263: PING

Traceroute

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.

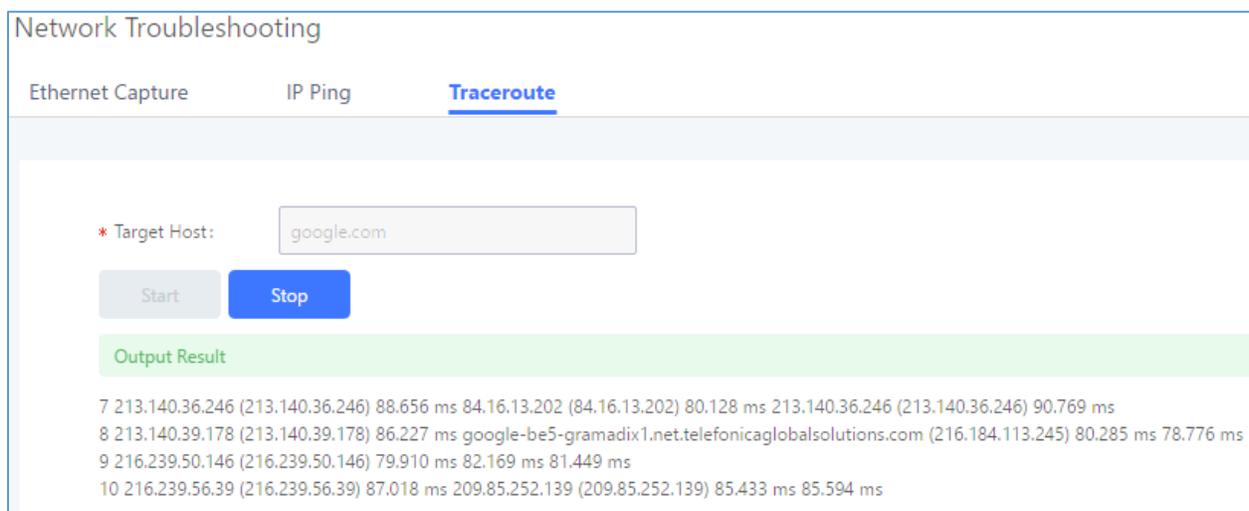


Figure 264: Traceroute

Signaling Troubleshooting

PRI/SS7/MFC/R2 Signaling Trace

Please see section [\[Digital Trunk Troubleshooting\]](#).



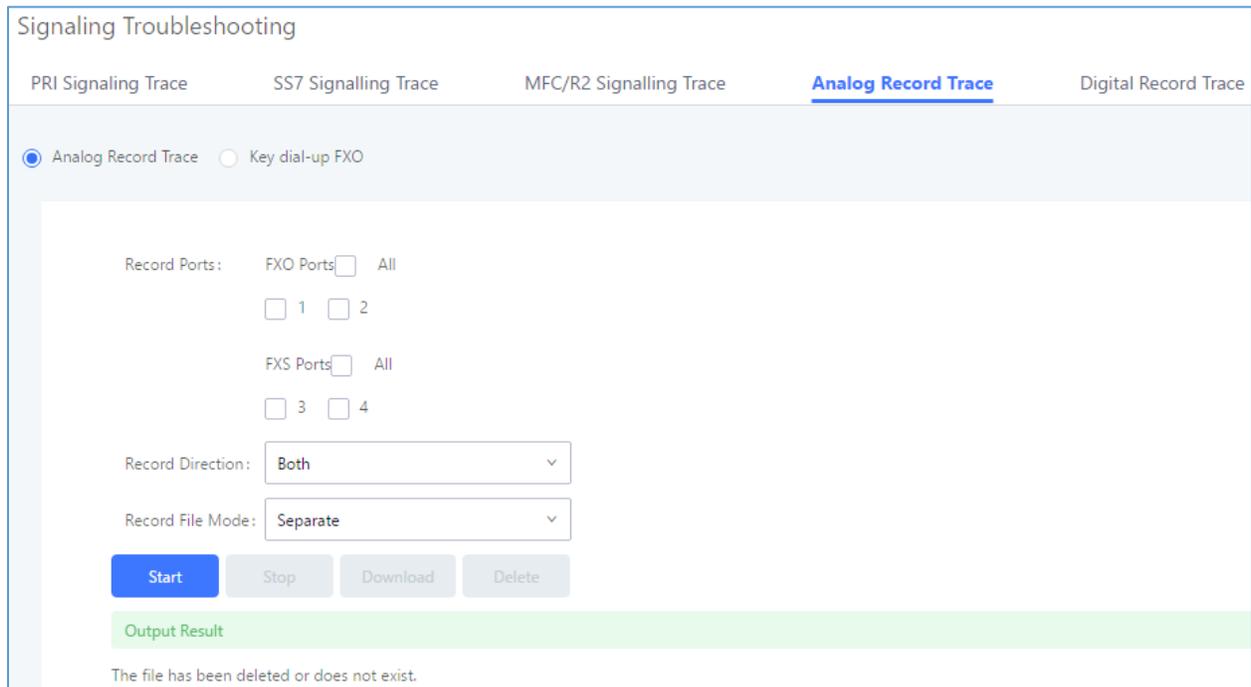
Analog Record Trace

- **Analog Record Trance**

Analog record trace can be used to troubleshoot analog trunk issue, for example, the UCM6510 user has caller ID issue for incoming call from Analog trunk. Users can access analog record trance under Web GUI→**Maintenance**→**Signal Troubleshooting**→**Analog Record Trace**.

Here is the step to capture trace:

1. Select FXO or FXS for "Record Ports". If the issue happens on FXO 1, select FXO port 1 to record the trace.
2. Select "Record Direction".
3. Select "Record File Mode" to separate the record per direction or mix.
4. Click on "Start".
5. Make a call via the analog port that has the issue.
6. Once done, click on "Stop".
7. Click on "Download" to download the analog record trace.



The screenshot shows the 'Signaling Troubleshooting' web interface. At the top, there are tabs for 'PRI Signaling Trace', 'SS7 Signalling Trace', 'MFC/R2 Signalling Trace', 'Analog Record Trace' (which is selected and underlined), and 'Digital Record Trace'. Below the tabs, there are two radio buttons: 'Analog Record Trace' (selected) and 'Key dial-up FXO'. The main configuration area includes:

- 'Record Ports': 'FXO Ports' with checkboxes for 'All', '1', and '2'.
- 'FXS Ports' with checkboxes for 'All', '3', and '4'.
- 'Record Direction': A dropdown menu set to 'Both'.
- 'Record File Mode': A dropdown menu set to 'Separate'.
- Four buttons: 'Start' (highlighted in blue), 'Stop', 'Download', and 'Delete'.
- An 'Output Result' section with a green background, containing the text: 'The file has been deleted or does not exist.'

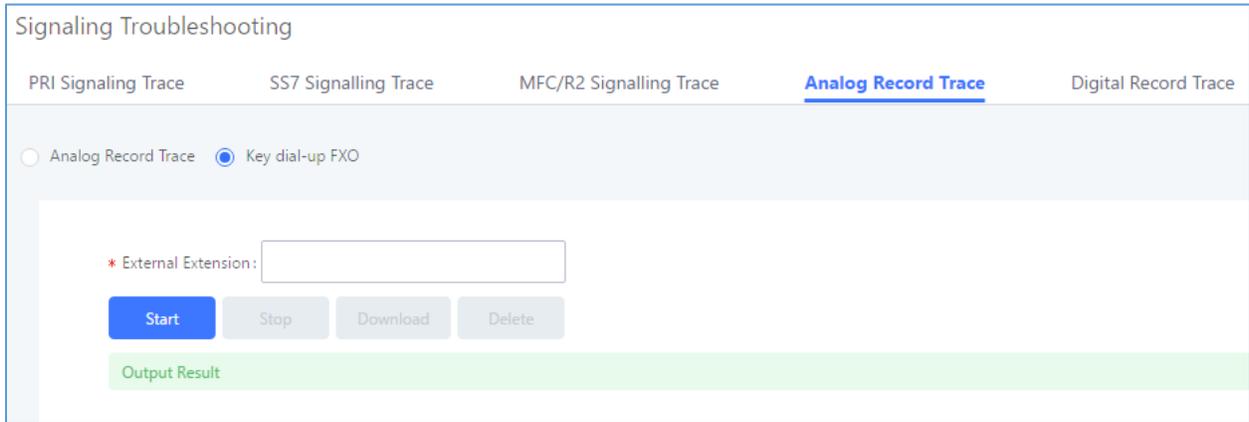
Figure 265: Troubleshooting Analog Trunks

- **A key Dial-up FXO**

Users can directly set a PSTN number on the “**External Extension**” text box to troubleshoot issues related to the analog trunk easily, the following steps shows how to use this feature:



1. Configure analog trunk on UCM, including outbound route.
2. Enter a reachable external number in “**External Extension**”.
3. Press “**Start**” button. The call will be initiated to the external number.
4. Answer and finish the call before pressing “Stop” button.
5. The trace will be available for analysis to download after output result shows “Done! Click on Download to download the captured packets”.



The screenshot shows the 'Signaling Troubleshooting' interface. At the top, there are five tabs: 'PRI Signaling Trace', 'SS7 Signalling Trace', 'MFC/R2 Signalling Trace', 'Analog Record Trace' (which is selected and underlined), and 'Digital Record Trace'. Below the tabs, there are two radio buttons: 'Analog Record Trace' (unselected) and 'Key dial-up FXO' (selected). Underneath, there is a text input field labeled '* External Extension:' with a red asterisk indicating a required field. Below the input field are four buttons: 'Start' (highlighted in blue), 'Stop', 'Download', and 'Delete'. At the bottom of the interface, there is a green bar labeled 'Output Result'.

Figure 266: A Key Dial-up FXO

Note: When using a Key Dial-up FXO feature the outbound trunk for the analog trunk need to have internal permission. As well as it should be the trunk with the highest outbound route priority.

After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved.

<http://www.grandstream.com/support>

E&M Immediate Record Trace

Before capturing the trace for E&M, user could configure “Record Direction” and “Record File Mode”. “Record File Mode” can be separate (one record per direction) or mix. Then click on “Start” to start to capture.



Signaling Troubleshooting

[PRI Signaling Trace](#)
 [SS7 Signalling Trace](#)
 [MFC/R2 Signalling Trace](#)
 [Analog Record Trace](#)
 [Digital Record Trace](#)

the recording: Record Direction:

channels:

Record File Mode:

Output Result

The file has been deleted or does not exist.

Figure 267: E&M Immediate Record Trace

Service Check

Enable Service Check to periodically check UCM6510. Check Cycle is configurable in seconds and the default setting is 60 sec. Check Times is the maximum number of failed checks before restart the UCM6510. The default setting is 3. If there is no response from UCM6510 after 3 attempts (default) to check, current status will be stored and UCM6510 will be restarted.

Service Check

Enable Server Check:

* Check Cycle:

* Check times:

Figure 268: Service Check

Network Status

UCM6510 supports Network Status to display active internet connections (Severs and Established). User can use Network Status to troubleshoot connection issue between UCM6510 and other services. This information can be found under Web GUI→**System Status**→**Network Status**, the users can view active Internet connections. This information can be used to troubleshoot connection issue between UCM6510 and other services.



Network Status

Active Internet Connections (Servers And Established)

Proto	Recv-Q	Send-Q	Local-Address	Foreign-Address	State
tcp	0	0	0.0.0.0:7681	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:7777	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:389	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:2000	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8888	0.0.0.0:*	LISTEN

Active Unix Domain Sockets (Servers And Established)

Proto	RefCnt	Flags	Type	State	I-Node
unix	2	[ACC]	STREAM	LISTENING	8487
unix	2	[ACC]	STREAM	LISTENING	8491
unix	2	[ACC]	STREAM	LISTENING	8494
unix	2	[ACC]	STREAM	LISTENING	8498
unix	2	[ACC]	STREAM	LISTENING	8501

Figure 269: Network Status



EXPERIENCING THE UCM6510 SERIES IP PBX

Please visit our website: <http://www.grandstream.com> to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our [product related documentation](#), [FAQs](#) and [User and Developer Forum](#) for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all of your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

Thank you again for purchasing Grandstream UCM6510 IP PBX appliance, it will be sure to bring convenience and color to both your business and personal life.

*** Asterisk is a Registered Trademark of Digium, Inc.**

