

CloudBond™ 365 and User Management Pack™ 365

Standard/Standard+ Box Edition

Pro Box Edition

Enterprise Box Edition

Virtualized Edition

User Management Pack 365

Version 7.6

Table of Contents

1	Introduction	19
<hr/>		
	User Management Pack 365 Administration Tool.....	21
2	Introduction (UMP 365)	23
3	User Management Pack 365 and Skype for Business Administration	25
4	Getting Started	27
4.1	Accessing SysAdmin for the First Time	27
4.2	Installing the UMP 365 License	29
4.2.1	Installing the UMP 365 License from a File	29
4.2.2	Installing the UMP 365 License from the One Voice Operations Center License Server	29
4.3	General Access to SysAdmin	32
4.4	SysAdmin Home Page	33
4.5	Properties of a Skype for Business User	34
4.5.1	Individual User Properties	34
4.6	User Management on Premises or in Hybrid Deployments	38
4.6.1	Call Forward Settings	39
4.6.2	Editing an Individual User	40
4.6.2.1	Editing an Individual User (Telephony Settings).....	43
4.6.2.2	Editing an Individual User (Group Management)	43
4.6.2.3	Editing an Individual User (Call Forwarding)	44
4.6.2.4	Editing an Individual User (Policies).....	45
4.6.2.5	Individual User IP Phone Settings.....	46
4.6.3	Deleting an Individual User.....	46
4.6.4	Resetting a Local User Password	47
4.7	Create User (Local user)	48
4.7.1	Create User (Telephony)	48
4.8	Import User	49
4.9	Bulk Edit	50
4.10	Bulk Import	52
4.11	Bulk Import CSV	54
4.12	Lifecycle Management.....	55
4.13	Distribution List	58
4.14	Create Device	58
4.15	User Management in Cloud PBX Environments	60
4.15.1	Applying Filters	61
4.15.2	Updating the Environment	62
5	System Configuration	65
5.1	System Configuration.....	65
5.2	Self Service	66
5.3	Email Configuration.....	68
5.4	Server Management.....	68
5.5	Grouping IDs.....	69
5.6	CallPickup Groups	70

5.7	Office 365 Configuration.....	72
5.7.1	Office 365 Unified Messaging (UM) and Cloud PBX Policies	73
5.8	Music on Hold.....	76
5.9	User Authorization	77
5.10	Unassigned Number Range	78
5.11	Skype for Business Control Panel (Quick Access)	79
5.12	SBC / Gateway Administration Panel (Quick Access).....	81
5.13	Licensing Information.....	82
5.14	Monitoring CloudBond 365 in One Voice Operations Center	83
5.14.1	Configuring the CloudBond 365 and One Voice Operations Center Server Connection.....	84
6	IP Phones.....	87
6.1	Dashboard.....	87
6.2	Status	88
6.3	Alarms	88
6.4	IP Phone Management Server.....	89
7	About.....	91
8	Scheduled Tasks	93
8.1	Step 1: AcsLogCleanup	93
8.2	Step 2: AcsGroupReplication.....	93
8.3	Step 3: AcsO365Sync	93
8.4	Step 4: AcsPolicyReplication	93
8.5	Step 5: AcsUserReplication	93
8.6	Step 6: AcsMoveUsers	95
Changing Administrator Password.....		97
9	Introduction	99
10	Changing Password on Domain Controller	101
10.1	CloudBond 365 Standard/Standard+ Box Edition	101
10.2	CloudBond 365 Pro and Enterprise Box Editions.....	102
11	Changing Password on IIS Manager	103
12	Changing Password on Domain Controller Windows Services.....	105
13	Changing Password on Front End.....	113
14	Changing Password on Edge Server.....	115
15	Changing Password on BPA.....	117
16	Changing EMS Agent Password.....	119
17	Verifying Password Change.....	121
Connecting to Servers		123

18	Introduction	125
19	CloudBond 365 Desktop Access	127
20	Rear KVM Ports	129
20.1	CloudBond 365 Standard/Standard+ Editions	129
20.2	CloudBond 365 Pro-Enterprise Edition	130
21	Remote Desktop Protocol (RDP).....	131
21.1	What is RDP?	131
21.2	Access Virtual Machine Desktops using Hyper-V	132
21.2.1	Hyper-V Virtual Machine Connection	132
21.2.2	Hyper-V Manager	133
21.2.3	Login Process	134
21.3	Enable RDP on Each Server	135
22	Configuring Remote Desktop.....	137
23	Starting RDC.....	141
23.1	Setting RDC Options	142
23.2	Connecting	143
24	Ending an RDC Session	145
<hr/>		
	IP Phone Management Administrator's Tool.....	147
25	Introduction to the IP Phone Manager Admin.....	149
26	Deploying the IP Phones	151
26.1	Planning the Deployment.....	151
26.2	Preparing the Enterprise Network.....	151
26.2.1	Deployment.....	153
26.3	Logging in to the Management Server	154
26.4	The 'System User'	155
26.5	Plugging Phones into the Network.....	156
26.5.1	Devices Status	157
27	Monitoring and Maintaining the Phone Network	159
27.1	Monitoring the Network from the Dashboard	159
27.2	Checking Devices Status.....	161
27.3	Monitoring Alarms	164
27.3.1	Registration Failure Alarm	166
27.3.2	Survivable Mode Start Alarm.....	166
27.3.3	Lync Login Failure Alarm	167
27.3.4	Endpoint License Alarm.....	168
27.3.5	Endpoint Server Overloaded Alarm.....	169
27.3.6	IP Phone Speaker Firmware Download Failure	170
27.3.7	IP Phone Speaker Firmware Upgrade Failure.....	170
27.3.8	IP Phone Conference Speaker Connection Failure	171
27.3.9	IP Phone General Local Event	171
27.3.10	IP Phone Web Successive Login Failure	172
27.4	Searching for Alarms	173

27.5	Maintaining Regions	173
27.6	Maintaining Users.....	173
27.6.1	Adding a User	174
27.6.2	Adding a Phone	175
27.6.3	Editing a User	176
27.6.4	Deleting a User	176
27.7	Managing Multiple Users	177
27.8	Maintaining Multiple Devices	180
28	Troubleshooting.....	183
28.1	Displaying Log Files	183
28.2	Displaying Web Admin Log Files	183
28.3	Displaying Activity Log Files	184
29	Preparing a Configuration File.....	185
29.1	Selecting a Configuration Template.....	185
29.2	Editing a Configuration Template.....	186
29.2.1	About the Template File.....	187
29.2.2	Global Parameters.....	187
29.2.3	User-Specific Parameters.....	187
29.2.4	Restoring a Template to the Default.....	188
29.2.5	Downloading a Template	188
29.2.6	Uploading an Edited Template	188
29.2.7	Generating an Edited Template.....	188
29.2.8	Defining Template Placeholders.....	189
29.2.8.1	Default Placeholders Values	191
29.2.8.2	Region Placeholders	196
29.2.8.3	Devices Placeholders.....	197
29.3	Managing Configuration Files	201
29.4	Managing Phone Firmware Files	202
30	Provisioning Flows	205
30.1	Skype for Business Desktop Phones	205
31	Ports Required for IP Phone Management.....	207
One Voice Operations Center Management		209
32	Introduction	211
33	Status Monitoring and Navigation	213
34	CloudBond 365 Alarms.....	215
34.1.1	Commit License Failed	215
34.1.2	Component Unreachable.....	215
34.1.3	Component Restart.....	216
34.1.4	Component Performance Counter General.....	216
34.1.5	Component Performance Counter Service.....	217
34.1.6	Component Service Status	218
34.1.7	Component Event Viewer	218
34.1.8	Component Event Viewer Past Hours	219
34.1.9	Component Event Viewer Dropped	219
34.1.10	Admin License Expired	220
34.1.11	Alarm – Certificate Expired	220
34.1.12	Alarm – Disk Space	221

35 License Management.....	223
Backup and Restore.....	225
36 Introduction	227
37 Backup Architecture	229
37.1 Using Veeam Products.....	231
37.1.1 VEB.....	231
37.1.2 VBR.....	231
37.2 Using VBR Components.....	231
37.2.1 VBR Manager	231
37.2.2 Backup Repository.....	231
37.2.2.1 Backup Repository Size	232
37.3 Firewall.....	232
38 Installing VEB and VBR	233
38.1 Installing VEB on the Host Server.....	233
38.2 Installing VBR.....	238
38.2.1 Installing Patch File.....	243
39 Configuring License and Credentials.....	245
40 Backing up the Repository	247
40.1 Adding Backup Repository	247
40.2 Configure Backup Repository Permissions	258
40.3 Installing the License	259
40.4 Assigning VBR Console Credentials and VBR Roles.....	261
40.4.1 Adding a User and Role for VEB	263
40.4.1.1 For CloudBond 365 Pro Box / Enterprise Box Editions (or VBR on External Server).....	263
40.4.1.2 For CloudBond 365 Standard Box Edition	265
40.4.2 Assigning a Role for the VEB User.....	267
41 Adding CloudBond 365 Hyper-V to VBR	269
42 Configuring Backup Jobs.....	273
42.1 Configuring VEB Host Backup.....	273
42.2 Configuring VBR VMs Backup.....	279
42.3 Monitoring Backup.....	285
42.4 Using the 3-2-1 Backup Rule.....	285
42.5 Backing up the SBC	285
43 Keeping Information after Defining the Backup	287
44 Restoring a CloudBond 365 Backup	289
44.1 Booting the CloudBond 365.....	289
44.1.1 Booting CloudBond 365 from Veeam Recovery Media USB	289
44.1.2 Booting CloudBond 365 Remotely from .iso using HP iLO	290
44.2 Restoring Volume C: Using VEB	291
44.3 Performing Post-Restore – Exiting Domain Controller Safe Mode	299
44.4 Validating Network Settings.....	300

44.5	Preparing Volume D: for Restoring VMs from the VBR	301
44.6	Updating Host Virtual NIC MAC Address After Restore	305
44.7	Clearing Old Virtual Machine Data.....	306
44.8	Restoring all VMs from the VBR	307
44.9	Restoring D: and E: Drives and Files	311
44.10	Starting the Virtual Domain Controller.....	313
44.11	Restarting the CloudBond 365 Server and Testing the Restore.....	314
45	Creating the Veeam Recovery Media USB	315
46	Preparing for Veeam's Software Installation on CloudBond 365 Server....	316
47	Troubleshooting.....	317
47.1	Restoring Host Server using VEB if no or some Network Cards are Available....	317
47.2	No Boot Device Error – Setting Boot Priority.....	318
47.3	No Boot Device Error - How to Define Logical Drive and Selecting Boot Volume	319

List of Figures

Figure 4-1: Sysadmin License Required	27
Figure 4-2: Office 365 Settings.....	28
Figure 4-3: Licensing	28
Figure 4-4: Set One Voice Operations Center Configuration.....	30
Figure 4-5: SysAdmin Authentication	32
Figure 4-6: SysAdmin Home page	33
Figure 4-7: User Management List.....	38
Figure 4-8: User list with Enterprise Voice call forwarding.....	39
Figure 4-9: Setting a User for Simultaneous Ring	39
Figure 4-10: Setting a user for call forwarding.....	39
Figure 4-11: Setting a user for No Answer	40
Figure 4-12: Selecting an Existing Skype for Business User for Modification	40
Figure 4-13: Manage UnManaged User/Device.....	41
Figure 4-14: Enabling Font Download.....	42
Figure 4-15: Editing an Individual User (Telephony)	43
Figure 4-16: Editing an Individual User (Groups Management).....	44
Figure 4-17: Editing an Individual User (Call Forwarding)	44
Figure 4-18: Editing an Individual User (Policies).....	45
Figure 4-19: IP Phone User Settings.....	46
Figure 4-20: Removing a Skype for Business user	46
Figure 4-21: Resetting a Local User Password	47
Figure 4-22: Create a User (Telephony).....	48
Figure 4-23: Import User: Select Source Domain.....	49
Figure 4-24: List of Enterprise Users to Import.....	49
Figure 4-25: Import an Individual User	50
Figure 4-26: Bulk Edit	50
Figure 4-27: Bulk Edit Selected Users.....	51
Figure 4-28: Bulk Delete.....	51
Figure 4-29: Bulk Import of Selected Users.....	52
Figure 4-30: Results of bulk Import.....	53
Figure 4-31: Bulk Import CSV.....	54
Figure 4-32: Bulk Import CSV Error	55
Figure 4-33: Lifecycle Management Page.....	56
Figure 4-34: Add a New Template File	57
Figure 4-35: Deleting a Security Group from Group Replication	57
Figure 4-36: Distribution List.....	58
Figure 4-37: Creating Common Area Phone	59
Figure 4-38: Creating Analog Device	59
Figure 4-39: User Management in Cloud PBX Environments.....	60
Figure 4-40: Last Sync Status	60
Figure 4-41: Log Off	60
Figure 4-42: Filters	61
Figure 4-43: Configuring Filters.....	62
Figure 4-44: wyupdate.exe File	62
Figure 4-45: Automatic Update Utility.....	63
Figure 5-1: System Configuration Page	65
Figure 5-2: Self Service Password Reset.....	66
Figure 5-3: Self Service Password Request.....	67
Figure 5-4: Server Management (Master)	68
Figure 5-5: CloudBond 365 Grouping IDs.....	69
Figure 5-6: Adding a Grouping	69
Figure 5-7: Editing a Group Record.....	69
Figure 5-8: Deleting a Record	70
Figure 5-9: Defining CallPickup Groups	70
Figure 5-10: Defining the CallPickup Orbit	70
Figure 5-11: Defining the Call Pickup Group ID.....	71

Figure 5-12: Assigning the Call Pickup ID to a User	71
Figure 5-13: Office 365 Connector Settings	72
Figure 5-14: Assigning a user to a FE pool.....	73
Figure 5-15: Voice Routing Policies and PSTN Usages	74
Figure 5-16: Voice Routing Policies Assigned to User	74
Figure 5-17: Office365 UM	75
Figure 5-18: Office365 Exchange UMPolicy	75
Figure 5-19: Music on Hold	76
Figure 5-20: User Authorization.....	77
Figure 5-21: Edit Record	77
Figure 5-22: Add Announcement	78
Figure 5-23: Add Unassigned Number Range	78
Figure 5-24: Select a FE Server for Skype for Business Control Panel.....	79
Figure 5-25: Skype for Business Control Panel.....	80
Figure 5-26: Select an SBC/GW Server for SBC/Gateway	81
Figure 5-27: UMP 365 License	82
Figure 5-28: EMS Settings-SNMPv2.....	85
Figure 5-29: EMS Settings-SNMPv3.....	85
Figure 6-1: IP Phones Dashboard.....	87
Figure 6-2: IP Phones Status	88
Figure 6-3: IP Phones Alarms	88
Figure 6-4: IP Phones Manager	89
Figure 7-1: About Page.....	91
Figure 8-1: Scheduled Tasks.....	93
Figure 10-1: Changing Password on Domain Controller - Pro and Enterprise Box Editions	102
Figure 11-1: Changing Password on IIS Manager	103
Figure 11-2: Advanced Settings	103
Figure 11-3: Application Pool Identity.....	104
Figure 11-4: Set Credentials	104
Figure 12-1: SysAdmin.UCMA Service	105
Figure 12-2: Lync Server Deployment Wizard	106
Figure 12-3: Deploy Monitoring Reports Wizard	106
Figure 12-4: Specify Credentials	107
Figure 12-5: Specify Read-Only Group	107
Figure 12-6: Executing Commands.....	108
Figure 12-7: Task Scheduler	109
Figure 12-8: ACSGroupReplication Rule - Properties.....	109
Figure 12-9: ACSGroupReplication Properties	110
Figure 12-10: Select User, Service Account, or Group	110
Figure 12-11: ACSGroupReplication Properties (Local Computer)	111
Figure 12-12: Task Scheduler	111
Figure 13-1: SysAdmin.RemotingSrv Properties (Front End)	113
Figure 14-1: SysAdmin.RemotingSrv Properties (Edge Windows)	115
Figure 15-1: Paired Domain Controllers with No Edge Server.....	117
Figure 15-2: Paired Domain Controllers with an Edge Server	117
Figure 20-1: CloudBond 365 Standard/Standard+ Editions Rear View	129
Figure 20-2: Co-located DC and Hyper-V	129
Figure 20-3: Rear View.....	130
Figure 20-4: Hyper-V Host with Virtual Machines.....	130
Figure 21-1: Hyper-V Host Desktop	132
Figure 21-2: Hyper-V Virtual Machine Connection	132
Figure 21-3: Virtual Machines.....	133
Figure 21-4: Full screen Mode - Login Screen	134
Figure 21-5: Login Screen – Username/Password	134
Figure 22-1: Server Manager Icon on Desktop	137
Figure 22-2: Server Manager Dashboard.....	137
Figure 22-3: Server Manager - Local Server	138
Figure 22-4: Enable Remote Desktop	138
Figure 22-5: Server Manager - Windows Firewall	139

Figure 22-6: Windows Firewall Settings	139
Figure 22-7: Advanced Windows Firewall Settings	140
Figure 22-8: Inbound Rules - Remote Desktop	140
Figure 23-1: Starting RDC	141
Figure 23-2: RDC Connection Prompt	142
Figure 23-3: Setting RDC Options	142
Figure 23-4: Sharing Local C drive	143
Figure 23-5: RDC Authentication	143
Figure 23-6: CloudBond 365 Certificate	144
Figure 23-7: RDP Session Established	144
Figure 24-1: Ending RDC Session	145
Figure 26-1: Default cfg File Located on the IP Phone Management Server	152
Figure 26-2: CloudBond Management Server - IP Phone Management Server button	154
Figure 26-3: Welcome to the IP Phone Management Server	154
Figure 26-4: IP Phone Management Server User Interface - Homepage	155
Figure 26-5: Manage Users Screen Displaying Added User	155
Figure 26-6: System Settings	156
Figure 26-7: Devices Status	157
Figure 27-1: Dashboard and Users	159
Figure 27-2: Dashboard	159
Figure 27-3: Dashboard - Not Registered	160
Figure 27-4: Devices Status	161
Figure 27-5: Devices Status Filter	161
Figure 27-6: Actions Menu - Single User	162
Figure 27-7: Actions Menu - Selected Rows	163
Figure 27-8: Alarms	164
Figure 27-9: Maintain Regions	173
Figure 27-10: Manage Users	174
Figure 27-11: Add User	174
Figure 27-12: Add User Definitions	174
Figure 27-13: Add New Device to User	175
Figure 27-14: Prompt: Do you want to generate configuration files?	175
Figure 27-15: Prompt: Do you want to update the device file?	175
Figure 27-16: Manage Multiple Users	177
Figure 27-17: Manage Multiple Devices	180
Figure 28-1: System Logs	183
Figure 28-2: System Logs – Web Admin Level Log	183
Figure 28-3: System Logs – Web Admin Level txt Log File Displayed	184
Figure 28-4: System Logs – Activity Log	184
Figure 28-5: System Logs – Activity Level txt Log File Displayed	184
Figure 29-1: IP Phone Models Configuration Templates	185
Figure 29-2: IP Phone Configuration Template	186
Figure 29-3: Edit Template	187
Figure 29-4: Generate Configuration Template – 'Global files' Prompt	188
Figure 29-5: Configuration Template	189
Figure 29-6: Show Placeholders	190
Figure 29-7: Default Placeholders Values	191
Figure 29-8: System Settings	192
Figure 29-9: DHCP Option Template	193
Figure 29-10: Edit DHCP Option	193
Figure 29-11: Proxy DHCP Option Template	194
Figure 29-12: Phone Model Placeholders	195
Figure 29-13: Edit Phone Model Placeholder	195
Figure 29-14: Add New Phone Model Placeholder	196
Figure 29-15: Manage Region Placeholders	196
Figure 29-16: Edit Region Placeholder	196
Figure 29-17: Add New Region Placeholder	197
Figure 29-18: Manage Devices Placeholders	198

Figure 29-19: Change IP Phone Device Placeholder	198
Figure 29-20: Change IP Phone Device Placeholder – Selecting the Device	199
Figure 29-21: Edit IP Phone Device Placeholder	200
Figure 29-22: Manage Configuration Files	201
Figure 29-23: Phone Firmware Files	202
Figure 29-24: img Firmware File Download/Upload	202
Figure 29-25: Add IP Phone Firmware	203
Figure 29-26: Upload Configuration Firmware	203
Figure 29-27: Browse to Firmware	203
Figure 30-1: Skype for Business Desktop Phone	205
Figure 13-1: CloudBond 365 Pro Edition	213
Figure 13-2: CloudBond Device Detailed Information	213
Figure 22-1: License Pool Manager - CloudBond Devices	223
Figure 22-2: Tenant Allocations	224
Figure 37-1: Backup Architecture on Premises	229
Figure 38-1: Search Menu	234
Figure 38-2: WinZip Security Warning	234
Figure 38-3: Do you want to run this file?	235
Figure 38-4: Veeam Endpoint Backup	235
Figure 38-5: Veeam Endpoint Backup - Next	236
Figure 38-6: Veeam Endpoint Backup - Finish	236
Figure 38-7: Create Recovery Media	237
Figure 38-8: Veeam Endpoint Backup - Finish	238
Figure 38-9: Veeam Backup and Replication Setup	239
Figure 38-10: Program Features	239
Figure 38-11: System Configuration Check	240
Figure 38-12: Default Configuration	240
Figure 38-13: Data Locations	241
Figure 38-14: Ready to Install	241
Figure 38-15: Completing Veeam Backup and Replication Wizard	242
Figure 38-16: Welcome Update Installation Wizard	243
Figure 38-17: Ready to Install	243
Figure 38-18: Components Update	244
Figure 38-19: Components Update - Finish	244
Figure 40-1: VBR Backup Repository	247
Figure 40-2: New Backup Repository - Name	248
Figure 40-3: New Backup Repository - Type	248
Figure 40-4: New Backup Repository - Server	249
Figure 40-5: New Windows Server	249
Figure 40-6: New Windows Server - Credentials	250
Figure 40-7: Credentials	250
Figure 40-8: New Windows Server - Review	251
Figure 40-9: New Windows Server - Apply	251
Figure 40-10: New Windows Server - Summary	252
Figure 40-11: New Backup Repository - Server	252
Figure 40-12: New Backup Repository – Server C:\ Path	253
Figure 40-13: New Backup Repository - Repository	253
Figure 40-14: New Backup Repository - vPowerNFS	254
Figure 40-15: New Backup Repository - Review	254
Figure 40-16: New Backup Repository - Apply	255
Figure 40-17: VBR – Change Backup Location	255
Figure 40-18: Configuration Backup	256
Figure 40-19: Configuration Backup Settings	256
Figure 40-20: Removing Old Repository	257
Figure 40-21: Backup Infrastructure	258
Figure 40-22: Endpoint Backup Permissions	258
Figure 40-23: Help – License Menu	259
Figure 40-24: License Information	260
Figure 40-25: Users and Roles	261

Figure 40-26: Security	262
Figure 40-27: Local User and Groups	263
Figure 40-28: Creating a New User	264
Figure 40-29: Adding to Administrators	264
Figure 40-30: Active Directory Users and Computers	265
Figure 40-31: New Object – Name Details	265
Figure 40-32: New Object – Password Details	266
Figure 40-33: New Object – Finish	266
Figure 40-34: Users and Roles	267
Figure 40-35: Security	267
Figure 40-36: Add User	268
Figure 40-37: Security – with Added Role	268
Figure 41-1: Add Server	269
Figure 41-2: New Hyper-V Server	269
Figure 41-3: New Hyper-V Server - Type	270
Figure 41-4: New Hyper-V Server - Credentials	270
Figure 41-5: New Hyper-V Server - Apply	271
Figure 41-6: New Hyper-V Server - Results	271
Figure 41-7: New Hyper-V Server - Summary	272
Figure 41-8: Microsoft Hyper-V Server	272
Figure 42-1: Notifications Area Icons	273
Figure 42-2: Configure Backup	273
Figure 42-3: Configure Backup	274
Figure 42-4: Configure Backup - Files	274
Figure 42-5: Configure Backup - Destination	275
Figure 42-6: Configure Backup – Backup Server	275
Figure 42-7: Configure Backup – Backup Repository	276
Figure 42-8: Configure Backup – Schedule	276
Figure 42-9: Configure Backup – Summary	277
Figure 42-10: Monitoring Backup with VEB Control Panel	277
Figure 42-11: Monitoring Backup with VEB Control Panel - Status	278
Figure 42-12: Monitoring Backup with VBR Jobs	278
Figure 42-13: VBR Jobs - Backup	279
Figure 42-14: New Backup Job	279
Figure 42-15: Add Objects	280
Figure 42-16: New Backup Job – Virtual Machines	281
Figure 42-17: New Backup Job – Storage	281
Figure 42-18: New Backup Job – Guest Processing	282
Figure 42-19: New Backup Job – Schedule	283
Figure 42-20: New Backup Job – Summary	284
Figure 42-21: VBR - Monitoring	284
Figure 43-1: Backup and Replication	287
Figure 44-1: Hardware Drivers	291
Figure 44-2: Veeam Endpoint Recovery – Bare Metal Option	291
Figure 44-3: Veeam Endpoint Recovery – Backup Location	292
Figure 44-4: Network Settings	293
Figure 44-5: Veeam Endpoint Recovery – Network Storage	294
Figure 44-6: Veeam Endpoint Recovery – Backup Server	294
Figure 44-7: Veeam Endpoint Recovery – Network Storage	295
Figure 44-8: Veeam Endpoint Recovery – Shared Folder	295
Figure 44-9: Veeam Endpoint Recovery – Backup	296
Figure 44-10: Veeam Endpoint Recovery – Restore Point	296
Figure 44-11: Veeam Endpoint Recovery – Restore Mode	297
Figure 44-12: Veeam Endpoint Recovery – Disk Mapping	298
Figure 44-13: Veeam Endpoint Recovery – Summary	298
Figure 44-14: Validating Network Settings	300
Figure 44-15: Disk Management	301
Figure 44-16: Disk Management – Change Drive Letter and Paths	302

Figure 44-17: New Simple Volume Wizard - Welcome	302
Figure 44-18: New Simple Volume Wizard – Assign Drive Letter or Path	303
Figure 44-19: New Simple Volume Wizard – Format Partition.....	303
Figure 44-20: New Simple Volume Wizard – Finish.....	304
Figure 44-21: MAC Addresses After Restore.....	305
Figure 44-22: Hyper-V Manager.....	305
Figure 44-23: MAC Addresses After Update.....	305
Figure 44-24: Hyper-V Manager – Virtual Machines	306
Figure 44-25: VBR – Hyper-V.....	307
Figure 44-26: Hyper-V – Restore Type	307
Figure 44-27: Full VM Restore Wizard – Virtual Machines	308
Figure 44-28: Backup Browser.....	308
Figure 44-29: Full VM Restore Wizard – Virtual Machines	309
Figure 44-30: Full VM Restore Wizard – Restore Mode	309
Figure 44-31: Full VM Restore Wizard – Reason	310
Figure 44-32: Full VM Restore Wizard – Summary	310
Figure 44-33: VM Restore	310
Figure 44-34: File Level Restore	311
Figure 44-35: File Level Restore – Restore Point	311
Figure 44-36: File Level Restore - Summary	312
Figure 44-37: Backup Browser.....	312
Figure 44-38: Server Manager	314
Figure 45-1: Create Recovery Media	315
Figure 45-2: Create Recovery Media – Recovery Media	315
Figure 47-1: Hardware Drivers – Clear Check Box.....	317
Figure 47-2: Hardware Drivers – Setting Boot Priority	318
Figure 47-3: Defining a Logical Drive	319

List of Tables

Table 26-1: IP Phone Provisioning File Legend	152
Table 27-1: Dashboard – Status Thumbnails	160
Table 27-2: Actions Menu	162
Table 27-3: Alarms	164
Table 27-4: IP Phone Registration Failure Alarm	166
Table 27-5: IP Phone Survivable Mode Start Alarm	166
Table 27-6: IP Phone Lync Login Failure Alarm	167
Table 27-7: Managing Multiple Users - Actions	178
Table 27-8: Managing Multiple Devices - Actions	181
Table 29-1: System Settings	192
Table 29-2: DHCP Option	194
Table 31-1: Ports Required for IP Phone Management	207

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be downloaded by registered customers at <http://www.audiocodes.com/downloads>.

This document is subject to change without notice.

Date Published: October-15-2017

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
26317	Initial release of this document.
26318	Update to General Access to SysAdmin, Editing an Individual User, Bulk Edit, Bulk Import and Lifecycle Management.
26319	Updates to Sections: Getting Started; User Management ; Office 365 Unified Messaging (UM) and Cloud PBX Policies; Scheduled Tasks; CloudBond 365 Alarms Update to Part One Voice Operations Center Management. New Section: User Management in Cloud PBX Environments; Unassigned Number Range.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

Related Documentation

Document Name
CloudBond 365 Installation Manual
One Voice Operations Center User's Manual

1 Introduction

This document describes the following subjects:

- **Part I:** The administration of the AudioCodes User Management Pack 365 (UMP 365) for Skype for Business (see page 21).
- **Part II:** The procedures for changing the AudioCodes CloudBond 365 Administrator password (see page 97).
- **Part III:** The various methods of connecting to the server desktops within AudioCodes CloudBond 365 (see page 123).
- **Part IV:** The IP Phones management module (see page 147).
- **Part V:** The Management of the CloudBond 365 devices using One Voice Operations Center (see page 209).
- **Part VI:** The configuration and use of the CloudBond backup and restore functionality (see page 225).

This page is intentionally left blank.

Part I

User Management Pack 365 Administration Tool

2 Introduction (UMP 365)

This part describes the administration of the AudioCodes User Management Pack 365 (UMP 365) for Skype for Business. It also describes the Management Suite interface (SysAdmin) as well as day-to-day user administration procedures (moves, adds, changes). It is intended for System Administrators, to carry out day-to-day maintenance activities.

The User Management Pack 365 is a software application for managing Skype for Business users on premises or in Cloud PBX environment and is also part of the AudioCodes CloudBond 365 solution and applies to all CloudBond 365 editions - Standard, Standard+, Pro, Enterprise and Virtualized Edition.

This page is intentionally left blank.

3 User Management Pack 365 and Skype for Business Administration

In a typical Skype for Business installation, day-to-day administration tasks can be quite complex to carry out. Skype for Business relies on user accounts being created using Active Directory utilities, then, for user accounts and other Skype for Business settings to be modified using the Skype for Business control panel, and for further tasks to be carried out within the Skype for Business Management Shell environment.

UMP 365 maintains the availability of all these Microsoft tools, but also provides a much simpler web based administration utility. UMP 365 does not attempt to remove or re-write these Microsoft tools, and they remain available for more advanced configuration items, or more experienced users.

UMP 365 provides a simplified web based administration utility with a strong focus on telephony and Hybrid Office 365 features that allows System Administrators to carry out day to day activities, without the need for complicated access to multiple Microsoft Tools.

The UMP 365 SysAdmin utility is a series of Web pages, which can carry out various tasks within the Skype for Business environment, such as adding and changing Skype for Business users, modifying user Call forwarding settings, and monitoring the status of Skype for Business and its component services.

The UMP 365 SysAdmin utility also provides an integrated tool for managing the AudioCodes IP Phones such firmware upgrades, generate IP Phones configuration files and monitor phone status.

This page is intentionally left blank.

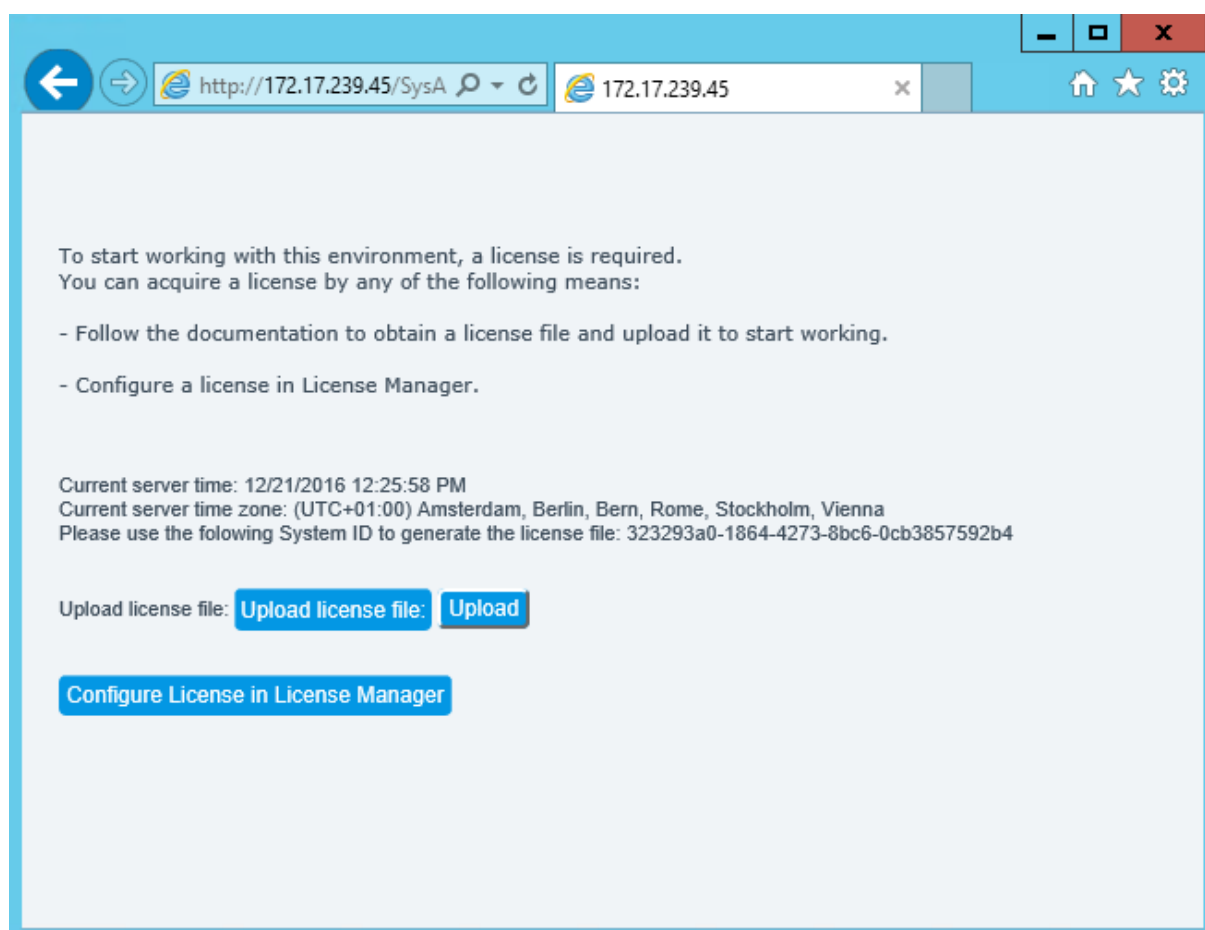
4 Getting Started

This chapter describes how to access the SysAdmin utility and how to obtain and install the license file.

4.1 Accessing SysAdmin for the First Time

On a new UMP 365 system, the first time the SysAdmin utility is accessed, you are required to upload and install a License file or obtain the license online from One Voice Operations Center license server. AudioCodes will supply a demonstration, time limited, trial license, or a full license, with each system.

Figure 4-1: Sysadmin License Required



Note: The System ID required for Licensing is displayed on this "First Time" screen, and is also available on the **System Configuration > Licensing Information** if a License has already been installed.

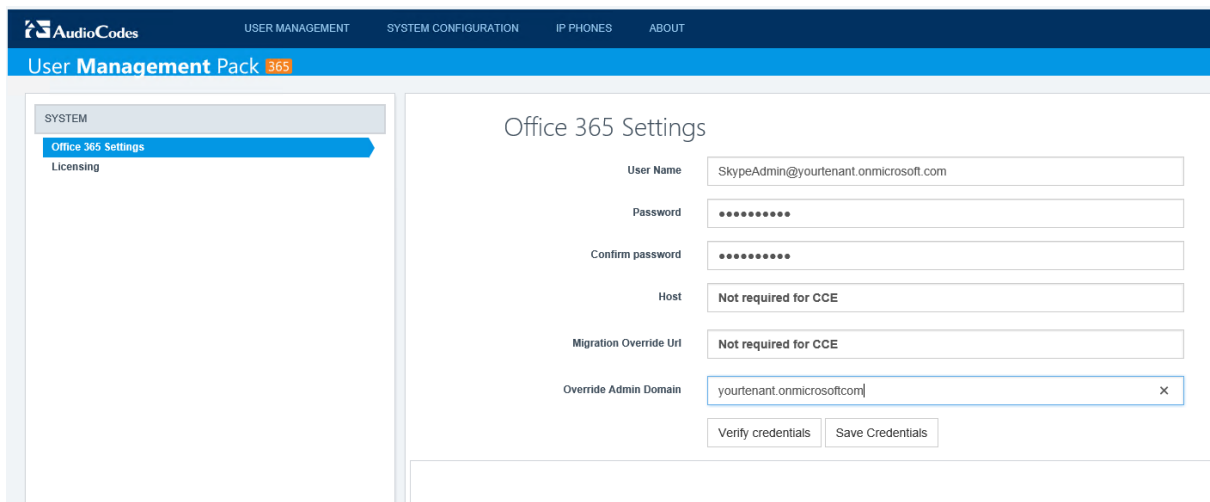


Warning: For CloudBond 365 installations, before applying a CloudBond 365 license, it is important to ensure all CloudBond 365 servers (DC, FE, and Edge) all have the correct time zone and date / time set.

If you have installed User Management Pack for Cloud PBX environments, you first need to sign in and complete the "Office 365 Settings" under "System Configuration" (see Figure 4-2) to be able to obtain the license file as the license is bound to the Office 365

tenant. Detailed information on these settings can be found in section [Office 365 Configuration](#) in this document.

Figure 4-2: Office 365 Settings



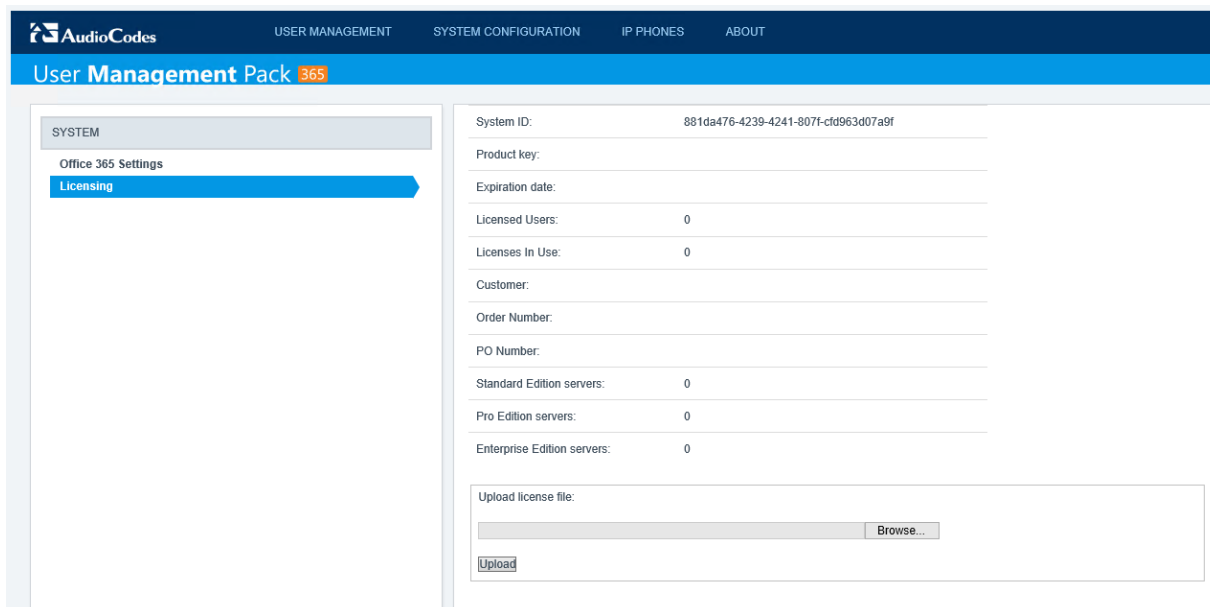
The screenshot shows the 'Office 365 Settings' page. The left sidebar has a 'SYSTEM' menu with 'Office 365 Settings' and 'Licensing' options. The main content area is titled 'Office 365 Settings' and contains the following fields:

- User Name: SkypeAdmin@yourtenant.onmicrosoft.com
- Password: (masked with dots)
- Confirm password: (masked with dots)
- Host: Not required for CCE
- Migration Override Url: Not required for CCE
- Override Admin Domain: yourtenant.onmicrosoft.com

At the bottom of the form are two buttons: 'Verify credentials' and 'Save Credentials'.

1. Open the "Licensing" page and obtain the System ID, which is required for requesting the license.

Figure 4-3: Licensing



The screenshot shows the 'Licensing' page. The left sidebar has a 'SYSTEM' menu with 'Office 365 Settings' and 'Licensing' options. The main content area displays the following information:

- System ID: 881da476-4239-4241-807f-cfd963d07a9f
- Product key:
- Expiration date:
- Licensed Users: 0
- Licenses In Use: 0
- Customer:
- Order Number:
- PO Number:
- Standard Edition servers: 0
- Pro Edition servers: 0
- Enterprise Edition servers: 0

At the bottom, there is an 'Upload license file:' section with a 'Browse...' button and an 'Upload' button.

2. Proceed to Section [Installing the UMP 365 License from a File](#) to complete the license activation.

4.2 Installing the UMP 365 License

You can obtain the UMP 365 license in the following ways:

- Installing the UMP 365 License from a File
- Installing the UMP 365 License from the One Voice Operations Center License Server

4.2.1 Installing the UMP 365 License from a File

This section describes how to obtain the UMP license from a file.

➤ **To install the UMP 365 license from a file:**

1. Install the product according to the instructions in the Installation Manual.
2. Obtain your product's Fingerprint (Serial Number) according to the instructions in "Licensing the Product" section of the Installation Manual.

Activate your product through AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>.

You need your Product Key and Fingerprint (Serial Number) for this activation process. An e-mail will subsequently be sent to you with your Product License.

3. Install the Product License according to the instructions in "**Installing the Product License**" section of the Installation Manual.

The "Product Key" is a unique key that represents the UMP 365 / CloudBond 365 initial order and is used for online license generation. The "Product Key" is used for future orders for the same system, such as a license upgrade.

4.2.2 Installing the UMP 365 License from the One Voice Operations Center License Server

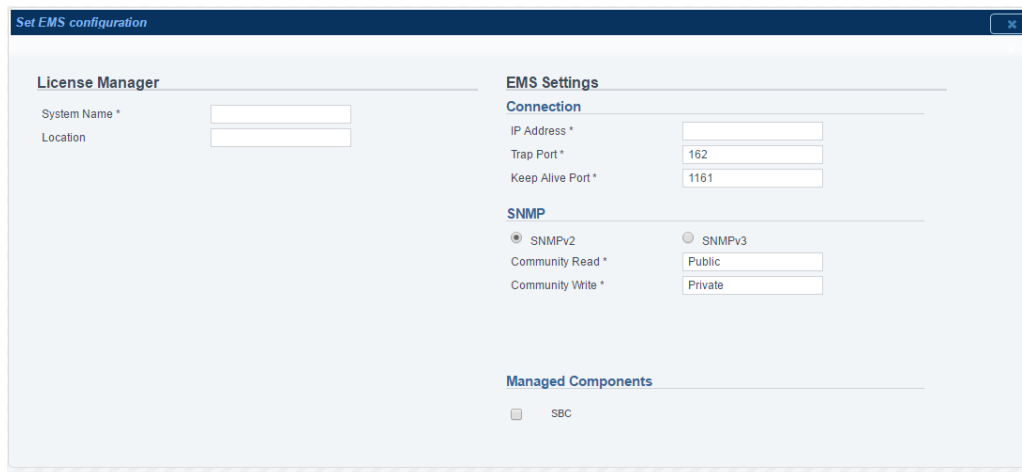
In order to obtain the license from the AudioCodes Element Management Server (One Voice Operations Center) license server, the CloudBond server must connect to the One Voice Operations Center via SNMP.

Follow the instructions below to retrieve your UMP 365 license from One Voice Operations Center:

- To install the UMP 365 license from the One Voice Operations Center license server:

1. Click the **Configure License in License Manager** button (see figure 3-1). The following screen is displayed:

Figure 4-4: Set One Voice Operations Center Configuration



2. System Info Settings:
 - System Name – The name of the system. In an environment with multiple CloudBond devices, this value must be unique.
 - Location – Optional field to describe the system location.
3. Configure the following connection settings:
 - IP Address – the IP address of the One Voice Operations Center server
 - Trap Port – Destination port to which to send traps (default value is 162)
 - Keep Alive Port – Destination port to send Keep-alive requests over SNMP (default is 1161)
4. Configure the SNMP user settings:

All the settings of the SNMP protocol must be identical to the settings of the current CloudBond system in the One Voice Operations Center (to support connecting the CloudBond devices to the One Voice Operations Center using Auto detection, you should configure the default values in parenthesis).

 - SNMP V2:
 - ◆ Community Read – Access string for SNMP get requests ('public')
 - ◆ Community Write – Access string for SNMP set requests ('private')
 - SNMP V3:
 - ◆ Security Name – Identify the SNMP user ('OVOCUser')
 - ◆ Authentication Protocol - Protocol type that used to encrypt the Security Name field ('SHA').
 - ◆ Authentication Key – Security Name encryption key. The field is valid only if Authentication Protocol selected ('123456789').
 - ◆ Private Protocol – Protocol type that is used to encrypt the SNMP message ('AES-128').
 - ◆ Private Key – SNMP message encryption key. The field is valid only if Private Protocol selected ('123456789').
5. If you would like the One Voice Operations Center to monitor the SBC in your CloudBond system, select the **SBC** button.

When you choose this option, the SBC in the CloudBond system is monitored in the One Voice Operations Center as part of the CloudBond system. SBC alarms will be displayed in the One Voice Operations Center as part of the CloudBond system.

6. Click **Apply.**

The CloudBond 365 system connects to the One Voice Operations Center server.

- 7.** Once the system is successfully detected in the One Voice Operations Center server, follow the instructions in the *One Voice Operations Center User's* manual to allocate a license from the One Voice Operations Center License Pool.
- 8.** After you have completed the license configuration in the One Voice Operations Center, the CloudBond system will retrieve the license from the One Voice Operations Center and you may login to the system.

4.3 General Access to SysAdmin

The UMP 365 SysAdmin utility is Web-based, and can be accessed via any Web browser. There is also an icon on the desktop for accessing SysAdmin.



Warning: The MS Skype for Business Control Panel (CSCP), which can be accessed from the SysAdmin Utility, is also web based, but requires MS Silverlight to be installed. For this reason, the Skype for Business Control Panel prefers to run in Internet Explorer, although it can be made to run adequately in Firefox.

The UMP 365 SysAdmin utility is installed on the CloudBond 365 Management Server. To access the SysAdmin utility, enter the following URL:

http://<CloudBond 365 ManagementServer>.<CloudBond 365 FQDN>/SysAdmin

where <CloudBond 365 ManagementServer> is the name of the CloudBond 365 Management Server, and <CloudBond 365 FQDN> is the domain specified for the CloudBond 365 Skype for Business Appliance.

For example, **http://UC-DC.cloudbond365.local/SysAdmin**.

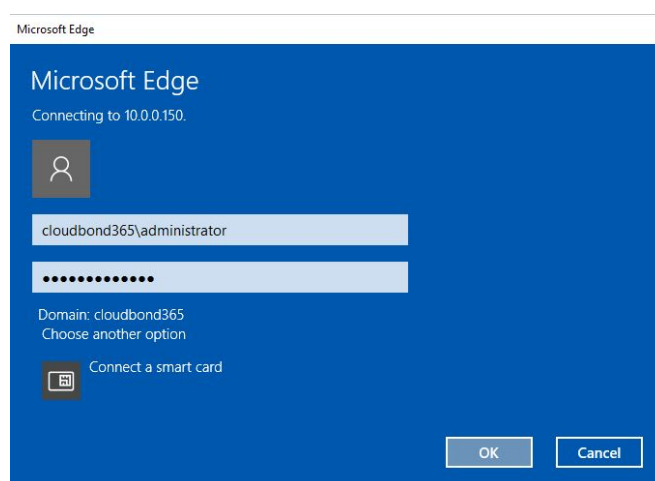
You can also use the IP address of the CloudBond 365 Management Server.

For example, **http://192.168.0.100/SysAdmin**.

When accessing the SysAdmin utility, you will be prompted to enter the user ID and password of the UMP 365 / CloudBond 365 administrator before proceeding. The user who administers the UMP 365 environment should be a member of the following UMP 365 Active Directory Domain Local security groups:

- **acs-FullAccess** allows the user to perform every aspect of management.
- **acs-ReadOnly** only allows the user to *view* management pages. Customization can be performed, but it is outside the scope of this document. Contact AudioCodes for your special access levels.

Figure 4-5: SysAdmin Authentication

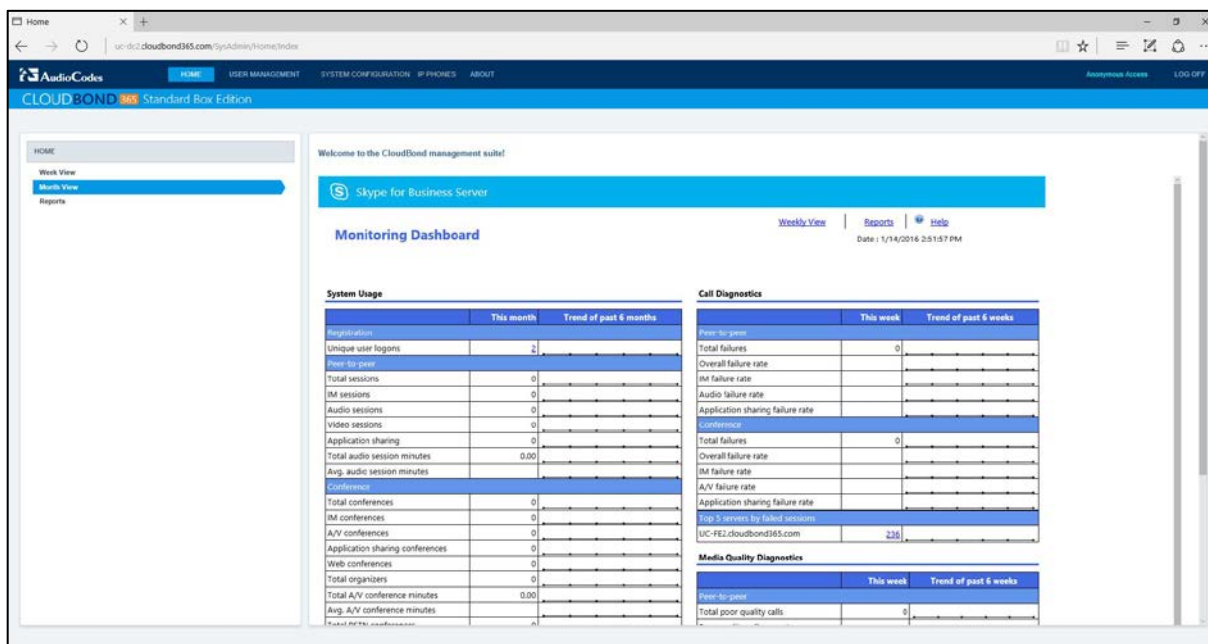


(You may be prompted a second time by the Skype for Business Monitoring and Reporting Tool for the same credentials).

4.4 SysAdmin Home Page

The SysAdmin Home page provides quick and convenient access to the Skype for Business Monitoring and Reporting tools, as well as Menu access to the remaining functions of the SysAdmin screens.

Figure 4-6: SysAdmin Home page



Use of the Skype for Business Monitoring and Reporting tool is not covered in further detail. Refer to <http://technet.microsoft.com/en-au/library/gg558662.aspx> for further information.

The SysAdmin utility provides very simple administration for Skype for Business users.

It allows:

- User Management
- Edit a user
- Remove user from Skype for Business
- Creating new local users
- Importing individual users from the Enterprise domain
- Bulk Edit of users
- Bulk Import of users
- Group Replication of users
- Distribution Lists
- Create Devices (Common Area Phones)

4.5 Properties of a Skype for Business User

Users of Skype for Business have corresponding entries within the CloudBond 365 Active Directory. These AD users have various properties, including generic AD properties, as well as Skype for Business specific properties created through the Skype for Business Schema additions. Microsoft accesses these properties through various tools, including the Active Directory Users and Computers utility, and the Skype for Business Control Panel. The UMP 365 SysAdmin utility presents these properties in a single utility. The properties which may be assigned to a Skype for Business user in the SysAdmin utility are as follows:

4.5.1 Individual User Properties

■ Account Information

Account information generally corresponds to standard Active Directory fields.

- First Name
The users first or given name
- Initials
The user's initials (optional)
- Last Name
The user's last name
- Full Name
Full name of user account, usually constructed from first name, initials, last name
- Sign-In Name
Forms the first part of the user Skype for Business sign-in account. E.g. Sign-in Name @ Domain name
- Domain Name
Forms the last part of the user Skype for Business sign-in account. E.g. Sign-in Name @ Domain name
- Registrar Pool
The Skype for Business registrar server the users signs in to. May have additional option when High Availability or Resiliency options are deployed.
- Mail
User email address for MS Exchange integration
- Preferred Language
Informative only
- Fax
Allows maintenance of the Fax number associated with the user within the UMP 365. Fax applications uses this AD field to route faxes correctly to the corresponding email address.
- Password
Sets the login password for CloudBond 365 Local users.

■ Telephony Settings

Telephony Settings control how voice calls are controlled within Skype for Business

- PC to PC
Skype for Business client to Skype for Business client direct calls are supported only. This corresponds to the lowest CAL provided by Microsoft.

- Enterprise Voice

Enterprise Voice calls allow users to make and receive calls from the PSTN, usually through a gateway or SIP trunk. This requires the highest CAL combination provided by Microsoft.
- Voice Policy

Enterprise voice requires a voice policy and a dial plan to control which calls are permitted and how they are handled.

 - ◆ Description
 - ◆ Features
 - ✓ Enable Call Forward
User is allowed to forward calls to another number or user
 - ✓ Enable Delegation
Other users may send and receive calls for this user
 - ✓ Enable Call Transfer
User may transfer calls to other users
 - ✓ Enable Team Call
User may answer calls for other members on same team
 - ✓ Enable Call Park
User may park a call and retrieve from another device
 - ✓ Enable Simultaneous Ringing of phones
Incoming calls may be set to ring on multiple devices
- Dial Plan

A dial plan controls which phone numbers can be entered and how they are translated for dialing.

 - ◆ Description
- Line URI

Enter a unique, normalized E.164 number for this user. Format – [TEL:+xxxxxxx](#)
- CloudPBX Voice Routing Policy

Used by the Office 365 Hybrid Cloud PBX feature. Can be created in the UMP 365 management suite's System Configuration pages.
- Office365 Unified Messaging (UM) Policy
- User Pin reset



Note: Voice policies and Dial Plans are configured in Skype for Business' Control Panel.

■ Group Management

- CallPickupGroup ID

Allows users to pick up calls within the specified group. Refer to System Configuration > CallPickup Groups
- GroupingID

Allows restricting which contact groups a Skype for Business user can see. Refer to System Configuration > Grouping IDs

- Response Groups and Membership
 - ◆ Response Group
A response group defined within Skype for Business
 - ◆ sipUser
Appears when user is selected as a member of that response group
 - ◆ ServerPool
The server pool the response group runs on.



Note: Response Groups are configured in the Skype for Business Control Panel.

■ Call Forwarding

These settings are normally configured independently in each end users Skype for Business Client. The options are identical to those presented in the Skype for Business client.

- Turn off call forwarding:
A traditional PBX would describe this as “Call Forward No Answer”
- Ring for this many seconds before redirecting:
Add a delay before the call is redirected
- Unanswered calls will go to:
 - ◆ Voicemail:
Direct the call to Exchange UM Voicemail
 - ◆ Tel:
Direct the call to a specified number
 - ◆ User:
Direct the call to a specified user
- Turn on call forwarding:
A traditional PBX would describe this as “Call Forward All”
 - ◆ Forward calls to:
 - ✓ Voicemail:
Direct the call to Exchange UM Voicemail
 - ✓ Tel:
Direct the call to a specified number
 - ✓ User:
Direct the call to a specified user
- Simultaneous ring:
 - ◆ Tel:
Simultaneous ring this number
 - ◆ User Delegates:
Simultaneous ring for the users Delegated group
 - ◆ User Team-Call group:
Simultaneously ring for the users Team-Call group
 - ◆ Ring for this many seconds before redirecting
Add a delay before the call is redirected

- ◆ Unanswered calls will go to:
 - ✓ Voicemail:
Direct the call to Exchange UM Voicemail
 - ✓ Tel:
Direct the call to a specified number
 - ✓ User:
Direct the call to a specified user

■ **IP Phones**

- The IP Phones tab lists all AudioCodes IP phones registered for this particular user.

■ **External Access Policy**

Select an external access policy:

- Enable Federation Access:
Enable communications with Federated (other external enterprise) users
- Enable Public Cloud Access:
Enable IM communications with Windows Live, Yahoo and AOL users. (Requires special configuration and licensing)
- Enable Public Cloud Audio/Video Access:
Enable Voice communications with Windows Live, Yahoo and AOL users. (Requires special configuration and licensing)
- Enable Outside Access:
Enable communications with External users (from this enterprise, but outside company network)

■ **Conferencing Policy**

Select a Conferencing policy.

■ **Client Policy**

Select a Client policy.

■ **Mobility Policy**

Select a Mobility policy.

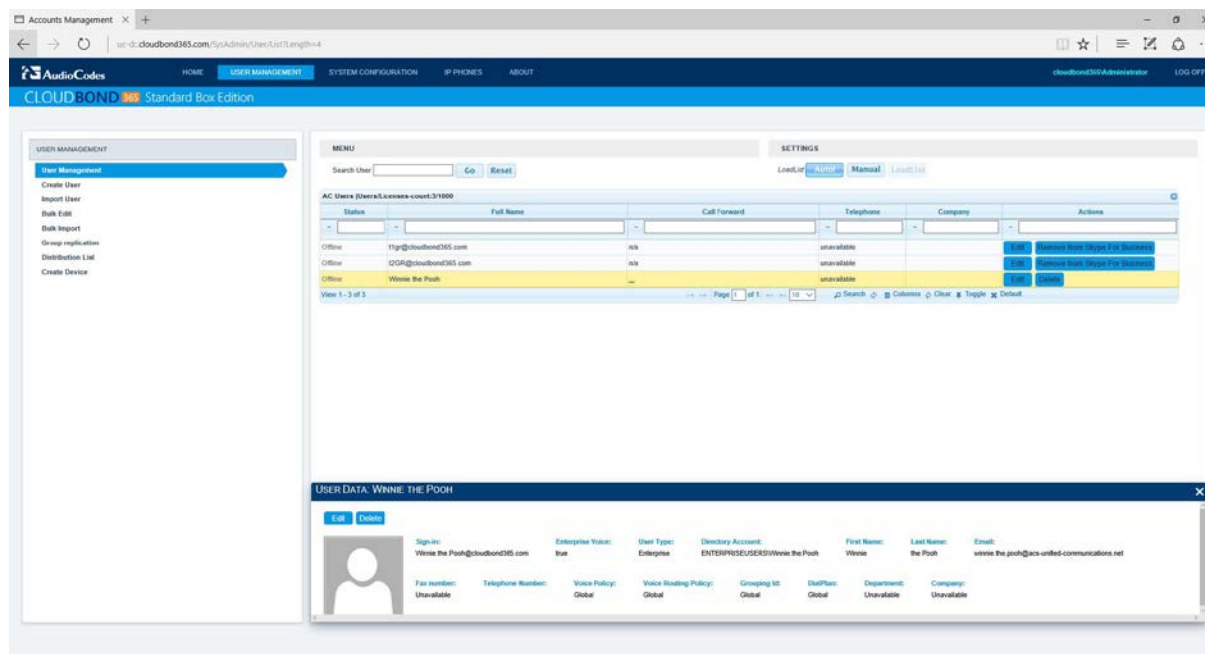


Note: External Access, Conferencing, Client and Mobility policies are defined in the Skype for Business Control Panel.

4.6 User Management on Premises or in Hybrid Deployments

The User Management page lists all users currently defined within the UMP 365. From this list, you can select a user for editing, or to remove them from Skype for Business. You can also modify the Call Forwarding settings for Enterprise Voice users.

Figure 4-7: User Management List



On this User Management List:

- Enter a user to search for, then click **Go**.
- Enter data in the search boxes to filter the displayed list.
- Click a user to highlight for [Edit or Delete](#).
- Click in the Call Forward column to change [Call Forward Settings](#) for that user

Change the page viewing options:

- Set the list refresh method to 'Auto' or 'Manual' in the Settings area.
- Change the number of entries displayed per page.
- Move forward and backward through multiple pages.
- Change the columns displayed or reset to default view.

4.6.1 Call Forward Settings

When users are enabled for Enterprise Voice, a ... link in the Call Forward column may be selected to change users Call Forward and Simultaneous ring settings.

Figure 4-8: User list with Enterprise Voice call forwarding

AC Users Users/Licenses-count:3/1000		
Status	Full Name	Call Forward
~	~	~
Offline	t1gr@cloudbond365.com	n/a
Offline	t2GR@cloudbond365.com	n/a
Offline	Winnie the Pooh	...
View 1 - 3 of 3		
		Page 1 of

The following show the various screens for entering call forwarding settings:

■ Simultaneous Ring

Figure 4-9: Setting a User for Simultaneous Ring

Winnie the Pooh's call forwarding settings

CALL FORWARDING SETTINGS

☐ Turn off call forwarding
☐ Forward calls to:
☒ Simultaneously ring:

☒ Tel:
☐ Users Delegates
☐ Users Team-Call Group

Ring for this many seconds before redirecting : 20 ▾

Unanswered call will go to:

☒ Tel:
☐ User:

Save Cancel

■ Call Forward (Call Forward All)

Figure 4-10: Setting a user for call forwarding

Winnie the Pooh's call forwarding settings

CALL FORWARDING SETTINGS

☐ Turn off call forwarding
☒ Forward calls to:
☒ Tel:
☐ User:

☐ Simultaneously ring:

Save Cancel

■ Turn off Call Forward (Call Forward No Answer)

Figure 4-11: Setting a user for No Answer

Winnie the Pooh's call forwarding settings

CALL FORWARDING SETTINGS

☒ Turn off call forwarding
 Ring for this many seconds before redirecting: 20

Unanswered call will go to:

☒ Tel:
☐ User:

☐ Turn on call forwarding
☐ Simultaneously ring:

Save Cancel

4.6.2 Editing an Individual User

When a user is selected, more details about that user are displayed at the bottom of the page, along with buttons to **Edit** or **Remove from Skype for Business**.

Figure 4-12: Selecting an Existing Skype for Business User for Modification

The screenshot shows the AudioCodes CloudBond 365 Standard Box Edition user management interface. The 'USER MANAGEMENT' sidebar is active. The main area displays a table of users with columns: Status, Full Name, Call Forward, Telephone, Company, and Actions. The user 'Winnie the Pooh' is selected. A pop-up window titled 'USER DATA: WINNIE THE POOH' displays detailed information for this user, including Sign-In, Enterprise Voice, User Type, Directory Account, First Name, Last Name, Email, Fax Number, Telephone Number, Voice Policy, Voice Routing Policy, Grouping ID, Skill Plan, Department, and Company.

If a row is selected from a user that was not managed before, the following pop-up message will appear:

Figure 4-13: Manage UnManaged User/Device

The screenshot shows a web interface for managing users. At the top, a red box highlights the header 'AC Users | Users/Licenses-count: 5 / Licenses: 5000'. Below this is a table with columns for Status, Full Name, and Call Forward. The table lists several users, including 'fe1usr1 Synthetic Transaction account', 'fe1usr2 Synthetic Transaction account', 'fe2usr1 Synthetic Transaction account', 'fe2usr2 Synthetic Transaction account', 'contoso user', 'contoso4 user', 'contoso3 user', 'contoso1 user', and 'Walter van Schaik'. A dialog box titled 'Manage unmanaged user/device' is overlaid on the right side of the table. It contains a checkbox for 'Don't show again', a message 'If you want to manage this user/device click 'yes'', and two buttons: 'Yes' and 'No'.

Status	Full Name	Call Forward
Offline	fe1usr1 Synthetic Transaction account	Off...
Offline	fe1usr2 Synthetic Transaction account	---
Offline	fe2usr1 Synthetic Transaction account	---
Offline	fe2usr2 Synthetic Transaction account	---
Offline	contoso user	---
Offline	contoso4 user	---
Offline	contoso3 user	---
Offline	contoso1 user	---
Offline	Walter van Schaik	---

View 1 - 9 of 9

Manage unmanaged user/device

☐ Don't show again

If you want to manage this user/device click 'yes'

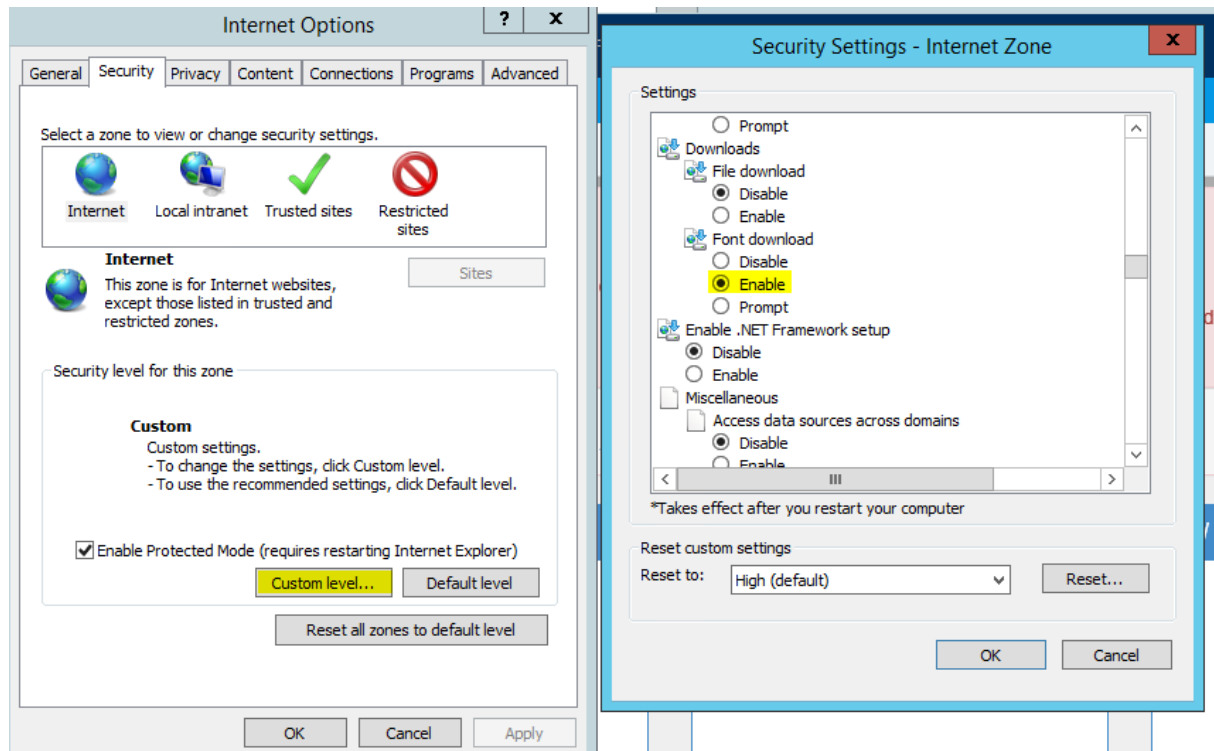
Yes No

The available users within the license disappear to the background (in the above picture highlighted in red). When clicking **Yes** to manage and saving changes within the user edit page, this user will be counted as a licensed user.



Note: If Edit is selected, the individual user details are displayed on a new page, and can be modified. The general Account Information is displayed on top of the screen. In the lower section of the page, you may select individual sub-tabs to modify Telephony (Enterprise Voice), Group Management, Call Forwarding, and Policies. You can also Reset the user's password if it was a locally created user.

Figure 4-14: Enabling Font Download



The Edit window as shown in Figure 4-12 is a floating window that might pop-up over the user-list if a full list is shown. Depending on the Internet security settings, the “X” character for closing the window might not be visible. To resolve this issue, please change the Internet security settings for the particular zone, by **enabling** the **Font download**, which is disabled by default on servers.

4.6.2.1 Editing an Individual User (Telephony Settings)

Within Telephony tab, you can choose between PC-to-PC (Skype for Business peer to peer calls), or Enterprise Voice (full PSTN access).

If Enterprise Voice is selected, then you may select a Voice Policy and Dial Plan from those already defined within Skype for Business. Details of the selected Voice Policy will be displayed.

If Enterprise Voice is selected, you must also allocate a Line URI in E.164 format. i.e., Tel:+xxxxx.

You can set/reset the user PIN using the “User PIN Set/Reset” field.

For users with Office 365 Unified Communication, you can enable/disable their Voicemail using the “Office365 Exchange UMPolicy” check box.

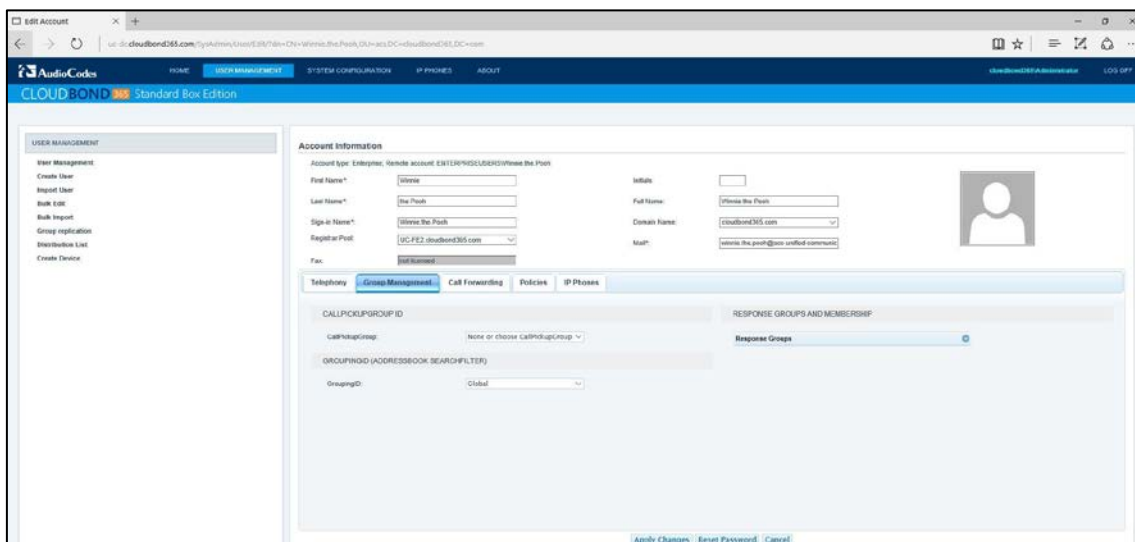
Figure 4-15: Editing an Individual User (Telephony)

The screenshot shows the 'USER MANAGEMENT' section of the CloudBond 365 Standard Box Edition interface. The 'Account Information' tab is active, displaying details for a user named 'Walter van Schaik'. The 'Telephony' tab is selected, showing options for 'PC to PC' and 'Enterprise Voice'. The 'Enterprise Voice' option is selected, and the 'Voice Policy' is set to '<Autom atic>'. The 'Office365 Exchange UMPolicy' checkbox is checked. The 'Features' section includes checkboxes for 'Enable call Forward', 'Enable Delegation', 'Enable Call Transfer', 'Enable team call', 'Enable call park', and 'Enable simultaneous ringing of phones'. The 'Dial Plan' is set to '<Autom atic>'. The 'Line URI' is set to 'tel:+31363461212'. The 'User PIN Set/Reset' field is empty, and the '(Re)Set UserPin' button is visible.

4.6.2.2 Editing an Individual User (Group Management)

The Group Management tab allows you to allocate a user to existing CallPickup Groups, GroupingIDs, and Response Groups defined within Skype for Business. For example, if you already have a Sales group defined, you can tick the appropriate selection box, and add the user to the group, without needing to use the Skype for Business control panel.

Figure 4-16: Editing an Individual User (Groups Management)



The CallPickupGroup allows you to select from groups already defined on the System Configuration → CallPickup Groups page. Callers within a pickup group can pick up a call which is ringing on another user's extension within the group.

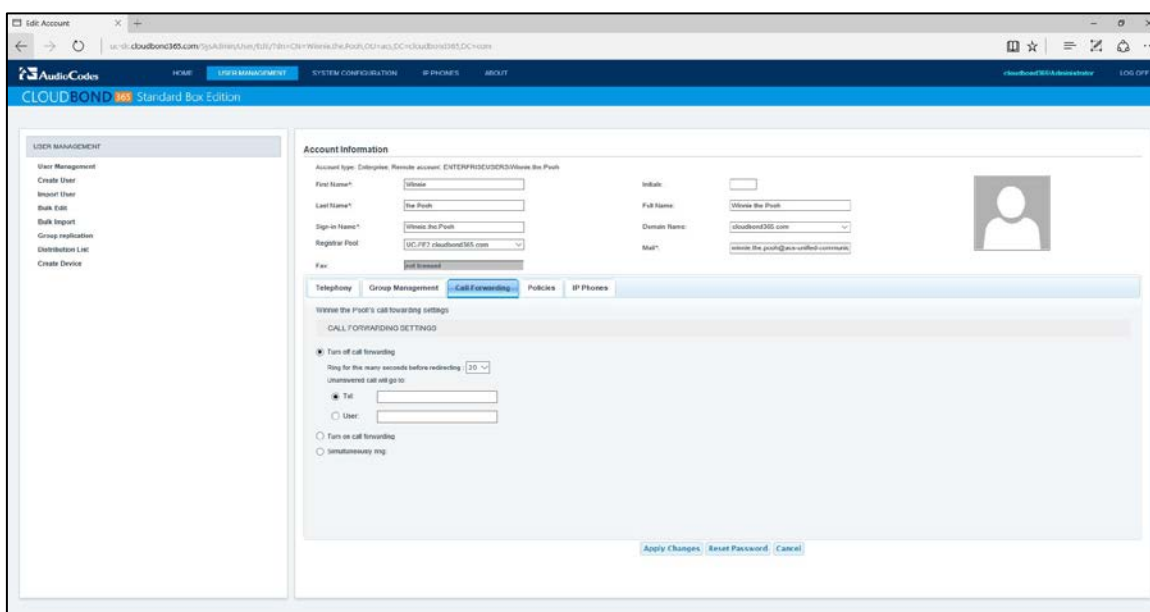
The GroupingID allows you to select from a User Group already defined on the System Configuration → Grouping IDs page. Users within a GroupID are restricted to search results within that group when locating contacts using the Skype for Business client.

4.6.2.3 Editing an Individual User (Call Forwarding)

The Call forwarding tab allows you to set or change the call forwarding options for a user. Similar functionality is available from the User Management list by clicking the ... link in the Call Forwarding column.

Typically a Skype for Business User would set their own call forwarding option from their Skype for Business Client. However, there are frequent times when a user cannot perform this task themselves, so the facility has been added to the SysAdmin web pages.

Figure 4-17: Editing an Individual User (Call Forwarding)



After completing any changes to the Users settings, click **Apply Changes** or **Cancel**.

4.6.2.4 Editing an Individual User (Policies)

The **Policies** tab allows you to determine which existing Skype for Business policies cover this user's External access and Conferencing features.

These External Access and Conferencing policies are defined in the Skype for Business Control Panel.

Figure 4-18: Editing an Individual User (Policies)

The screenshot displays the 'Account Information' section of the Skype for Business Control Panel. The 'Policies' tab is selected, showing a list of policies: External Access Policy, Conferencing Policy, Client Policy (selected), and Mobility Policy. The 'Client Policy' dropdown is set to 'Point2SixteenClientPol'. The 'Apply Changes' and 'Cancel' buttons are visible at the bottom. The 'Account Information' section includes fields for First Name, Last Name, Sign-in Name, Registrar Pool, Initials, Full Name, Domain Name, and Mail. The user's account type is 'Enterprise, Remote account, ACTIVEVOICE/DemoUser23'.

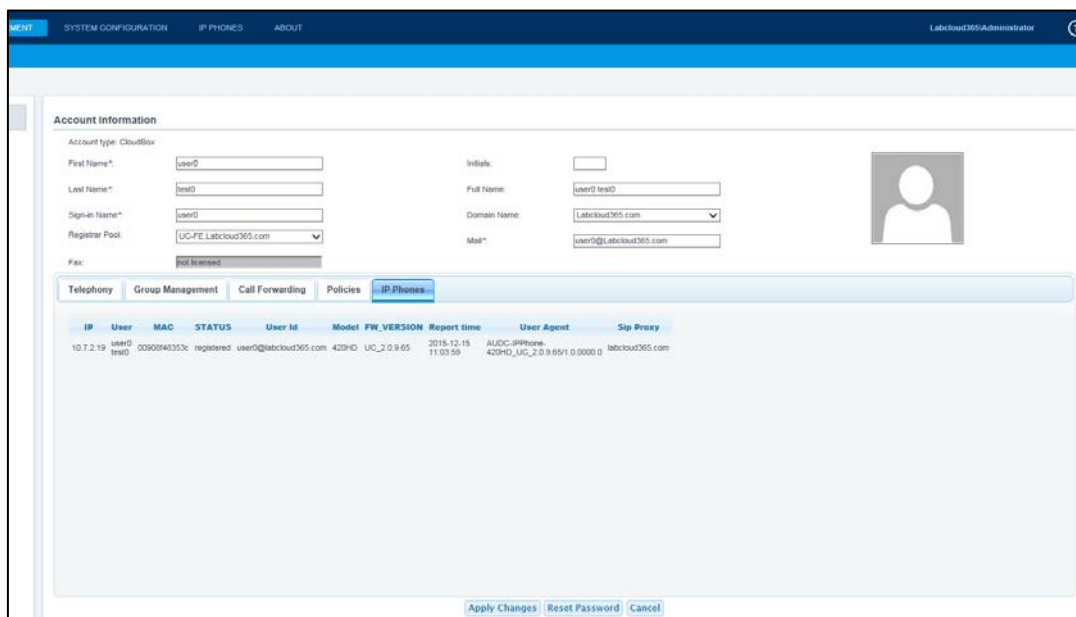
Once you have completed any changes to the Users settings, click **Apply Changes** or **Cancel**.

4.6.2.5 Individual User IP Phone Settings

The IP Phone tab allows you to see the AudioCodes IP Phone settings registered for the specific user such phone model, MAC address, firmware version, status and more.

This is very useful for remote management and troubleshooting when needed.

Figure 4-19: IP Phone User Settings



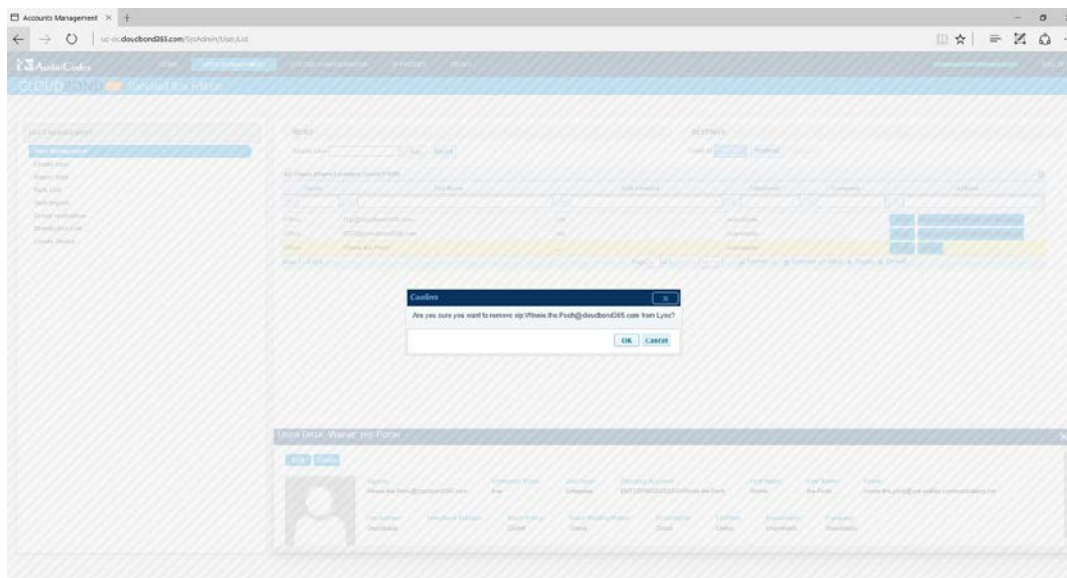
The screenshot shows the 'IP Phones' tab in the CloudBond 365 interface. The 'Account Information' section includes fields for First Name, Last Name, Sign-in Name, Registrar Pool, Initials, Full Name, Domain Name, and Title. Below this is a table of IP phone settings.

IP	User	MAC	STATUS	User Id	Model	FW_VERSION	Report time	User Agent	Sip Proxy
10.7.2.19	user0	000040353c	registered	user0@labcloud365.com	420HD	UC_2.0.9.65	2015-12-15 11:03:59	AUDC-IPPhone_420HD_UC_2.0.9.65/1.0.0000.0	labcloud365.com

At the bottom of the page are buttons for 'Apply Changes', 'Reset Password', and 'Cancel'.

4.6.3 Deleting an Individual User

Figure 4-20: Removing a Skype for Business user



The screenshot shows the 'Accounts Management' page in the CloudBond 365 interface. A confirmation dialog is displayed, asking if the user is sure they want to remove the user from the system. The dialog has 'OK' and 'Cancel' buttons.

Below the dialog, there is a section for 'User Data' with a table of user information.

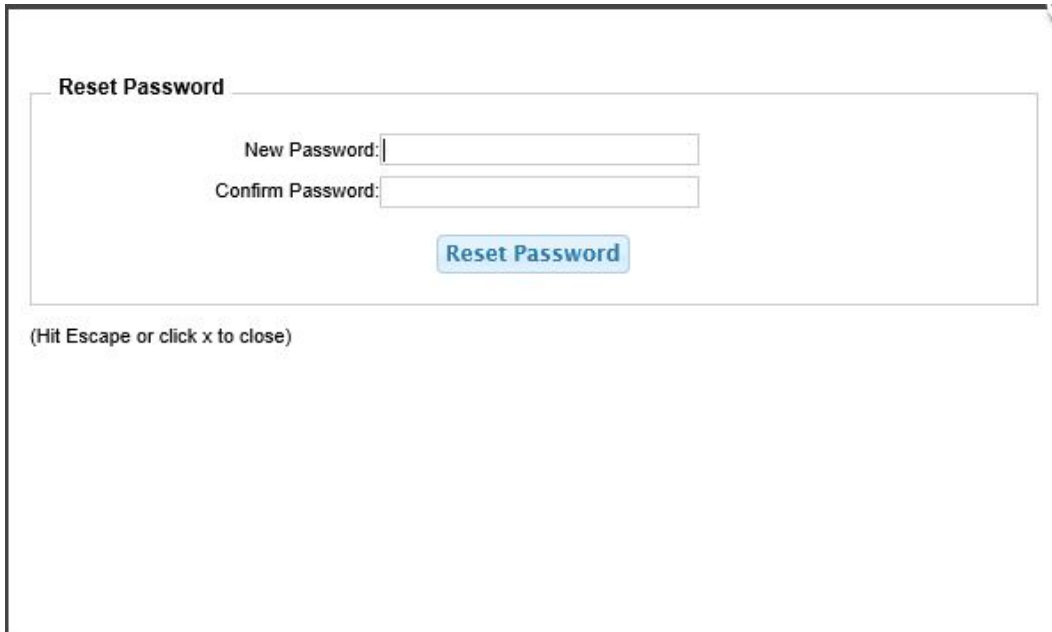
First Name	Last Name	Initials	Full Name	Domain Name	Title	Registrar Pool	MAC	Model	FW_VERSION	Report time	User Agent	Sip Proxy
user0	test0		user0 test0	labcloud365.com		UC-PE Labcloud365.com		420HD	UC_2.0.9.65	2015-12-15 11:03:59	AUDC-IPPhone_420HD_UC_2.0.9.65/1.0.0000.0	labcloud365.com

If you remove a user from Skype for Business, a popup confirmation box is displayed. Click **Yes** to confirm removal, or **No** to cancel. Removing a user from Skype for Business does not remove them from the Enterprise Active Directory.

4.6.4 Resetting a Local User Password

When editing an individual Local user, it is possible to reset their password. The **reset password** button at the bottom of the page allows entry of a new password.

Figure 4-21: Resetting a Local User Password



Note: Resetting passwords is possible for Local CloudBond 365 users only.



Note: The password selected must comply with the domain password complexity group policy. Failure to meet the complexity requirements will result in an error.

4.7 Create User (Local user)

Selecting **Create User** allows you to enter details for a user not in the Enterprise Active Directory. This allows you to create temporary accounts, accounts for visitors and contractor who do not need network privileges, or even accounts for external parties. These users are Local to the CloudBond 365 domain only.

The Create User page has several sub tabs for different attributes of the CloudBond 365 user, e.g., Telephony, Response Group, Call Pickup, Call Forwarding, User Permissions, and Policies. An account is created for these users within the CloudBond 365 Active Directory, but not within the Enterprise Active Directory.

To create an account for an Enterprise Active Directory user, use the Import user pages. Enter details for the user, and then click **Create User** at the bottom of the page.



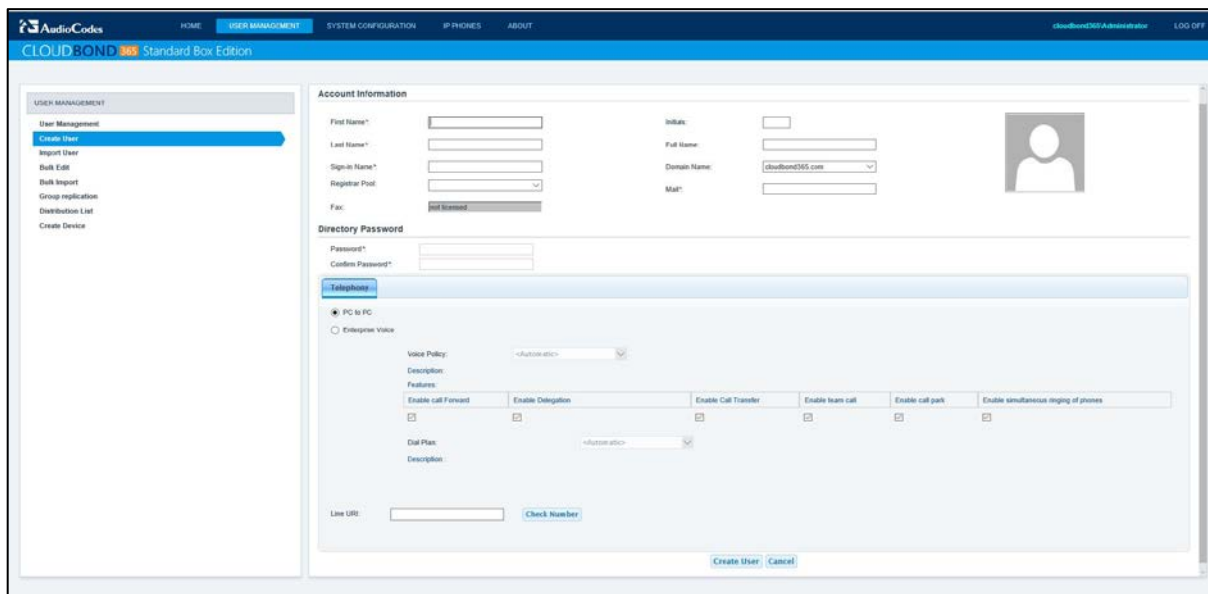
Note: Sign-in Name, Mail, and passwords are mandatory fields.



Note: Some fields (e.g., the Registrar pool, PSTN Gateway and (Sip-)domain information) are stored in a Web cache, which is refreshed every few minutes. This means that some recent changes in the Skype for Business or Active Directory backend environment are not directly visible within the administration pages, but will automatically show up after a maximum of 10 minutes. If immediate access is required, an IISRESET needs to be performed on the CloudBond 365 management server hosting the administration Web pages.

4.7.1 Create User (Telephony)

Figure 4-22: Create a User (Telephony)



See Section 4.6.2 on page 40 for more details.



Note: The password selected must comply with the domain password complexity group policy. Failure to meet the complexity requirements will result in an error.

4.8 Import User

The Import User page allows Active Directory users from the Enterprise Domain to be imported into the CloudBond 365 Domain and configured for use within Skype for Business. Use the Remote Domain and Search User fields to locate an Enterprise User, then click corresponding **Import** action link to import the user to CloudBond 365.

Figure 4-23: Import User: Select Source Domain

Figure 4-24: List of Enterprise Users to Import

User ID	First Name	Last Name	Full Name	Mail
Mickey Mouse	Mickey	Mouse	Mickey Mouse	mickey.mouse@arc-unified-communications.net
Mickey Mouse	Mickey	Mouse	Mickey Mouse	mickey.mouse@arc-unified-communications.net



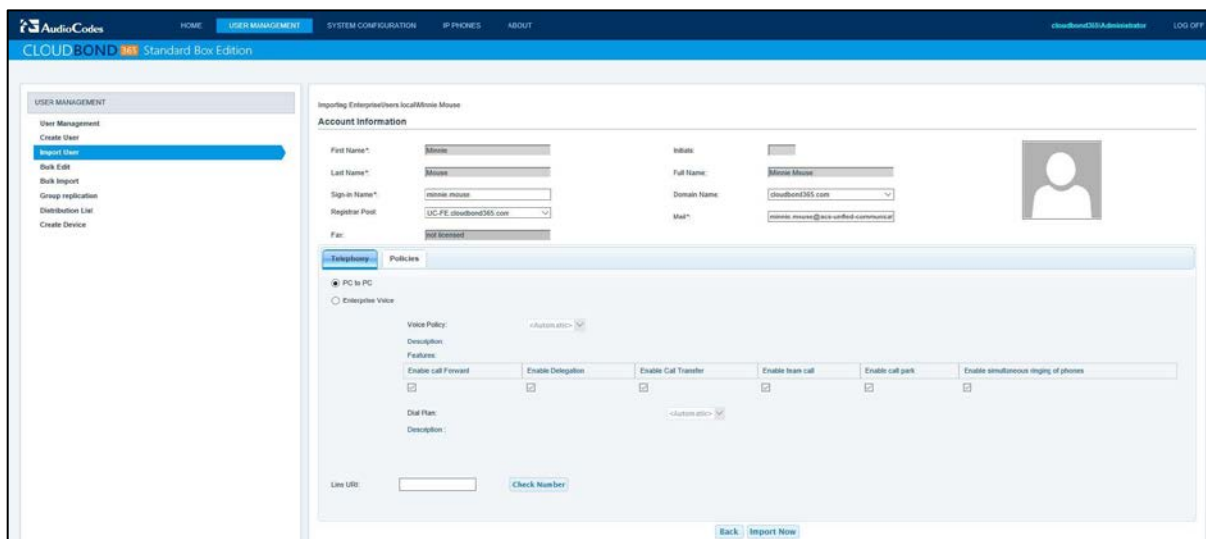
Note: The mail attribute is required for User Import. If it is not set in the user Active Directory, it can temporarily be added on the User Import page, to be able to continue the import. However, once the ACSUserReplication scheduled task runs, it overwrites the CloudBond Active Directory mail attribute again with the empty entry from the user forest. This causes the Skype for Business client's inability to contact the Exchange Web Service (EWS) for features like Calendar Integration and Conversation History. This implies that for a full-featured client experience, the mail attribute should be populated after import as well, within the user Active Director environment.



Note: Some fields (like the Registrarpool, PSTN Gateway and (Sip-)domain information for example) are stored in a web cache, which will be refreshed only every few minutes. This means that some recent changes in the Skype for Business or Active Directory backend environment are not directly visible within the administration pages, but will automatically show up after maximum 10 minutes. If immediate access is required, an IISRESET needs to be performed on the CloudBond 365 management server hosting the administration web pages.

An individual User Import page will appear with settings for this user. Modify the individual settings to meet requirements, then click **Import Now** to add the user to CloudBond 365, or **Back** to cancel the import. Individual user settings are discussed in Section 4.6.2 on page 40.

Figure 4-25: Import an Individual User



The screenshot shows the 'Import User' page in the AudioCodes CloudBond 365 Standard Box Edition. The page is divided into a left sidebar with navigation options (User Management, Create User, Import User, Bulk Edit, Bulk Import, Group replication, Distribution List, Create Device) and a main content area. The main content area has a 'Policies' tab selected, showing various settings for the user being imported. The 'Account Information' section includes fields for First Name, Last Name, Sign-in Name, Registrar Port, and a 'Full Name' field. The 'Policies' section includes checkboxes for 'PC to PC' and 'Enterprise Voice', and a 'Voice Policy' dropdown. Below these are several feature checkboxes: 'Enable call Forward', 'Enable Delegation', 'Enable Call Transfer', 'Enable team call', 'Enable call park', and 'Enable simultaneous ringing of phones'. There is also a 'Dial Plan' section with a 'Description' field. At the bottom, there is a 'Line URI' field and a 'Check Number' button. The page also includes 'Back' and 'Import Now' buttons.

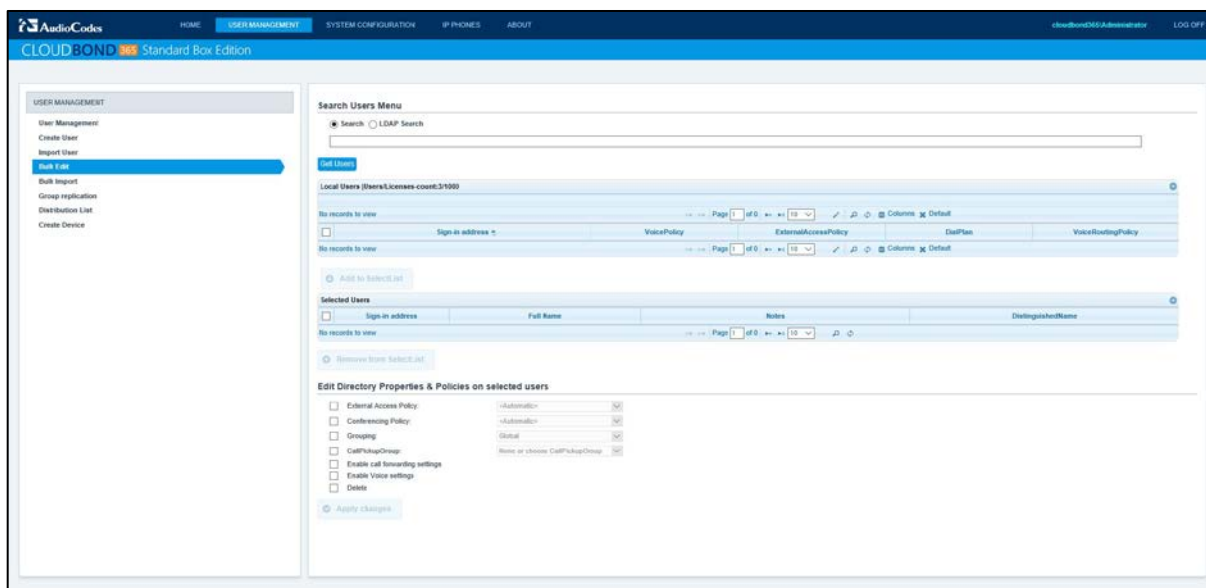


Note: Remember to change the **Domain Name** field if appropriate. This field is used for sign in on Skype for Business clients, and usually matches the customer external domain.

4.9 Bulk Edit

The Bulk Edit page allows you to make changes to multiple Skype for Business users, or even delete multiple users.

Figure 4-26: Bulk Edit

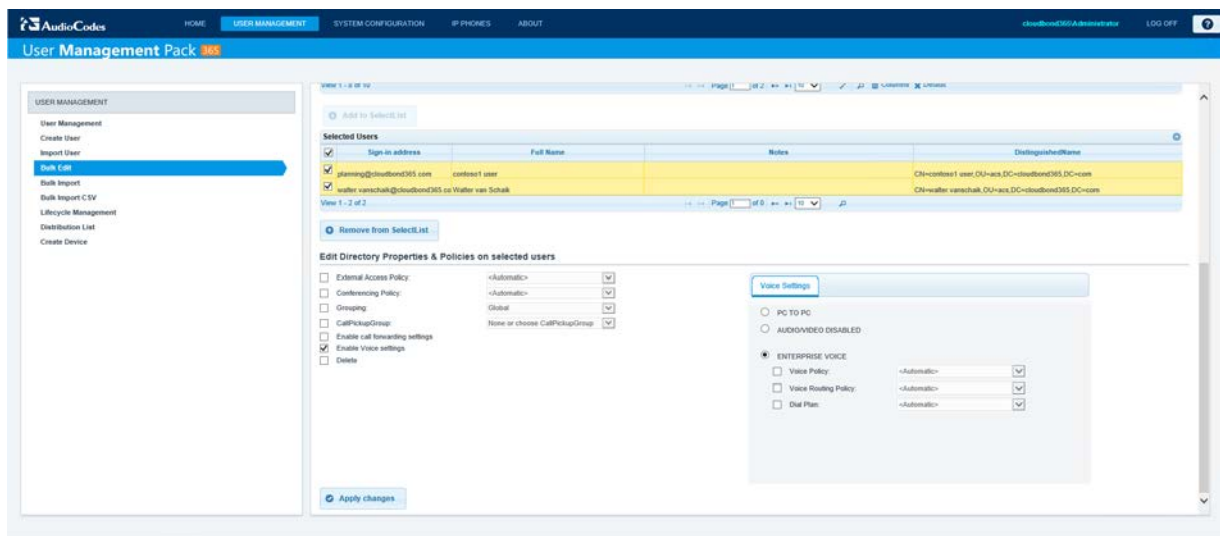


The screenshot shows the 'Bulk Edit' page in the AudioCodes CloudBond 365 Standard Box Edition. The page has a left sidebar with navigation options (User Management, Create User, Import User, Bulk Edit, Bulk Import, Group replication, Distribution List, Create Device). The main content area has a 'Search Users Menu' at the top with a search bar and a 'LDAP Search' button. Below this is a table of 'Local Users (Users/Licenses count: 3/100)'. The table has columns for 'Sign in address', 'VoicePolicy', 'ExternalAccessPolicy', 'DialPlan', and 'VoiceRoutingPolicy'. There are 'Add to Selected list' and 'Remove from Selected list' buttons. Below the table is a section for 'Edit Directory Properties & Policies on selected users'. This section includes checkboxes for 'External Access Policy', 'Conferencing Policy', 'Grouping', 'Call Pickup Group', 'Enable call forwarding settings', 'Enable Voice settings', and 'Delete'. There are also dropdown menus for 'Authentication', 'External Access Policy', 'Conferencing Policy', 'DialPlan', and 'Voice Routing Policy'. At the bottom, there is an 'Apply changes' button.

➤ **To make bulk edits:**

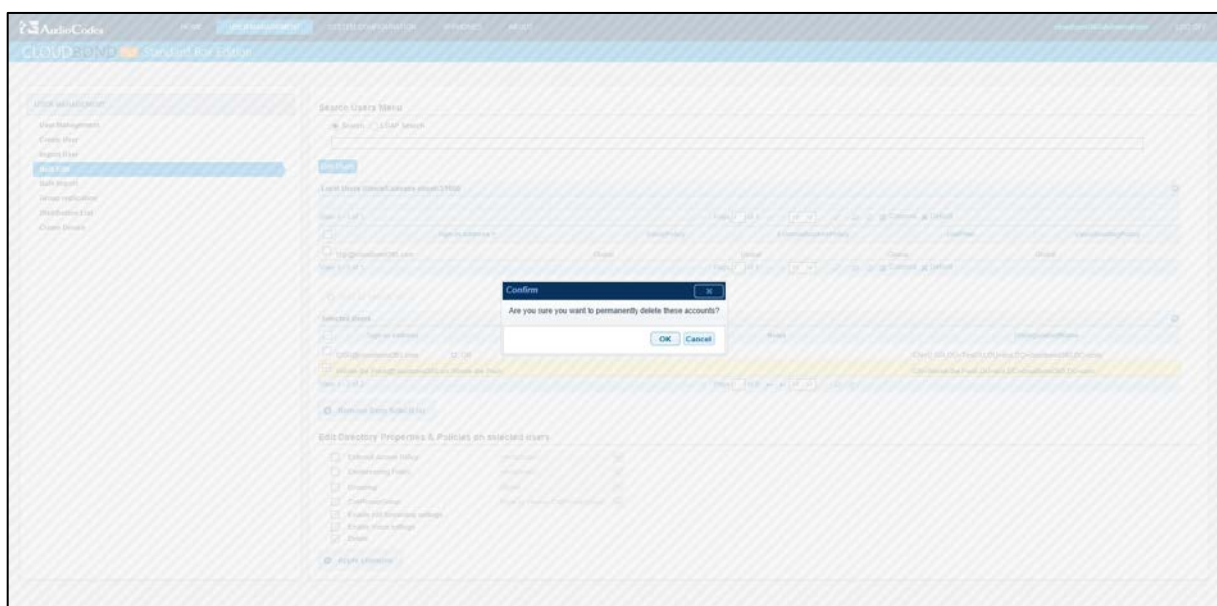
1. Enter any search criteria if required.
2. Click **Get Users**.
3. The Local UMP 365 Users list will be populated from users already in CloudBond 365.
4. Tick the desired users and click **Add to Select List**.
5. The Selected Users list will be populated. You may unselect users if desired.
6. Make any desired changes to the Directory Properties & Policies.
7. Click **Apply Changes**.

Figure 4-27: Bulk Edit Selected Users



8. If you select **Delete**, the following confirmation will be displayed

Figure 4-28: Bulk Delete



4.10 Bulk Import

Bulk import allows multiple user accounts to be imported from the Enterprise Active Directory in one action. The common Skype for Business properties for all imported users can be set.

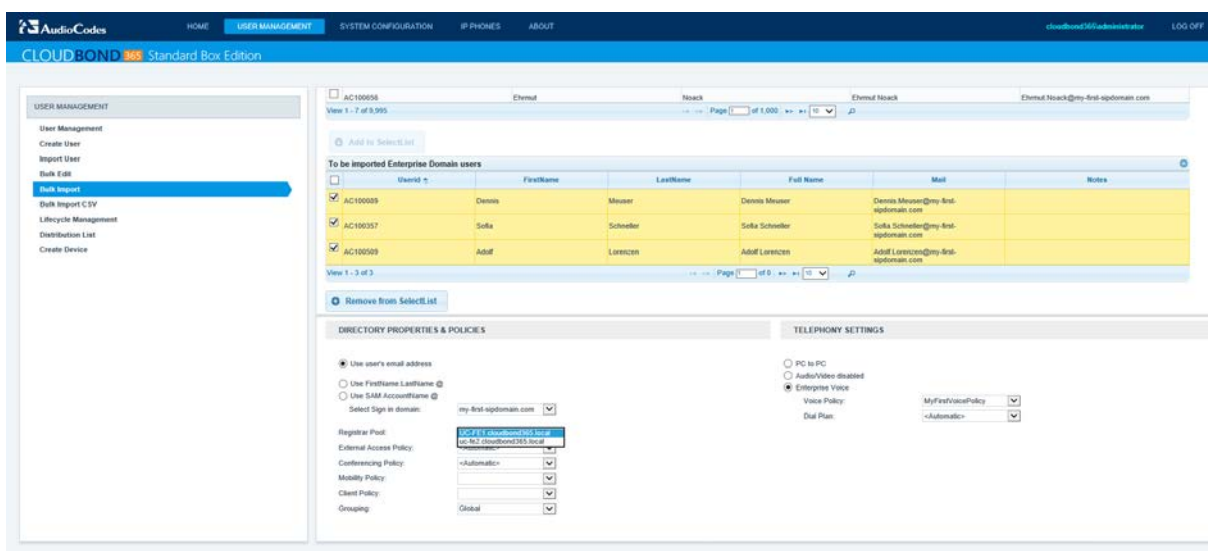


Note: It is not possible to Bulk Import users from the Enterprise Domain unless they already have an email address assigned. Email address is a mandatory field for CloudBond 365, and the bulk import utility will not allow setting of individual user values.



Note: Some fields (e.g., the Registrar pool, PSTN Gateway and (Sip-)domain information) are stored in a Web cache, which is refreshed every few minutes. This means that some recent changes in the Skype for Business or Active Directory backend environment are not directly visible within the administration pages, but will automatically show up after a maximum of 10 minutes. If immediate access is required, an IISRESET needs to be performed on the CloudBond 365 management server hosting the administration Web pages.

Figure 4-29: Bulk Import of Selected Users



The screenshot shows the CloudBond 365 administration interface. On the left is a sidebar with navigation options: User Management, Create User, Import User, Bulk Import (highlighted), Bulk Import CSV, Lifecycle Management, Distribution List, and Create Device. The main content area is titled 'CLOUDBOND 365 Standard Box Edition'. It features a 'Bulk Import' section with a table of 'To be imported Enterprise Domain users'. The table has columns: Username, First Name, Last Name, Full Name, Mail, and Notes. Three users are listed: AC100009 (Dennis Meuser), AC100037 (Sofia Schneider), and AC100009 (Adolf Lorenzen). Below the table, there are sections for 'DIRECTORY PROPERTIES & POLICIES' and 'TELEPHONY SETTINGS'. The 'DIRECTORY PROPERTIES & POLICIES' section includes options for email address, first name, last name, and domain, as well as settings for Registrar Pool, External Access Policy, Conferencing Policy, Mobility Policy, Client Policy, and Grouping. The 'TELEPHONY SETTINGS' section includes options for PC to PC, Audio/Video disabled, Enterprise Voice, Voice Policy, and Dial Plan.

➤ To perform a bulk import:

1. Select an Enterprise domain.
2. Apply search criteria if required.
3. Click **Get Users**.
4. In the Enterprise Domain Users list, tick those users to be imported, and click **Select Users**. The selected users will be moved to the **To Be Imported** list. (You can unselect users from this list).
5. Set any Directory Properties and Telephony Settings for these users. N.B. You cannot set individual setting for users here, such as Line URI. Line URI must be unique per user.

6. Click **Import** at the bottom of the page.



Note: The UserId field may or may not match the email prefix, depending upon the corporate standards employed. The Directory Properties and Policies allow you to combine the appropriate prefix with the selected domain suffix, to determine the Skype for Business SIP address / sign-in address.



Note: The 'Enterprise domain' drop-down box contains cached information to speed up loading of the Web page. This implies that it can take up to 10 minutes before a newly connected Active Directory forest (by means of a forest trust) becomes visible. If it does not appear, there might be a trust error in communicating with the remote domain. Trust errors are not logged to the screen, but can be found in the c:\acs\logs\sysadmin.log file, where the 'The specified forest does not exist or cannot be contacted' message will be logged.

The **To Be Imported** list will be updated with the results of the import.

Figure 4-30: Results of bulk Import

To Be Imported Enterprise Domain Users			
<input checked="" type="checkbox"/>	UserIdid	Full Name	Mail
<input checked="" type="checkbox"/>	Daisy Duck	Daisy Duck	daisy.duck@acs-unified-communications.net
<input checked="" type="checkbox"/>	Minnie Mouse	Minnie Mouse	minnie.mouse@acs-unified-communications.net
<input checked="" type="checkbox"/>	mickey mouse	Mickey Mouse	mickey.mouse@acs-unified-communications.net
View 1 - 3 of 3			

4.11 Bulk Import CSV

The Bulk Import CSV feature allows an administrator to import a large number of users into the local Active Directory and Skype for Business environment where the UMP is installed. This feature is especially useful when Skype for Business is installed as a legacy PBX replacement and in green field deployments, where no existing users exist within an Active Directory environment.

➤ **To use the Bulk Import from CSV feature:**

1. Select **User Management > Bulk Import CSV**.
2. Use the **choose file users.csv** button to browse for a CSV file containing the users. Once you have selected a file, the name of the file is appended in the button text.

Figure 4-31: Bulk Import CSV

The screenshot displays the AudioCodes User Management Pack 365 web interface. The top navigation bar includes links for HOME, USER MANAGEMENT (highlighted), SYSTEM CONFIGURATION, IP PHONES, and ABOUT. Below the navigation bar, the main content area is divided into two sections. On the left, a sidebar menu under 'USER MANAGEMENT' lists options: User Management, Create User, Import User, Bulk Edit, Bulk Import, Bulk Import CSV (highlighted), Lifecycle Management, Distribution List, and Create Device. The main content area on the right is titled 'Bulkimport CSV'. It contains an 'Upload CSV file:' section with a 'Choose file users.csv' button. Below this is a 'Default password' field with the text 'p@ssw0rd'. A checkbox labeled 'User must change password at next sign on' is present. The 'Registrar Pool: *' section features a dropdown menu with 'acs-s4b.ocshost.nl' selected. An 'Upload' button is located at the bottom of the form.

3. In the "Default password" box, set the default password for all users to be added and specify whether the users should change their passwords at next sign-on by selecting the checkbox.
4. Select a registrar pool in the "drop-down" box and click the **Upload** button to start the import process.

The imported CSV file should contain a header row with at least the following three attributes:

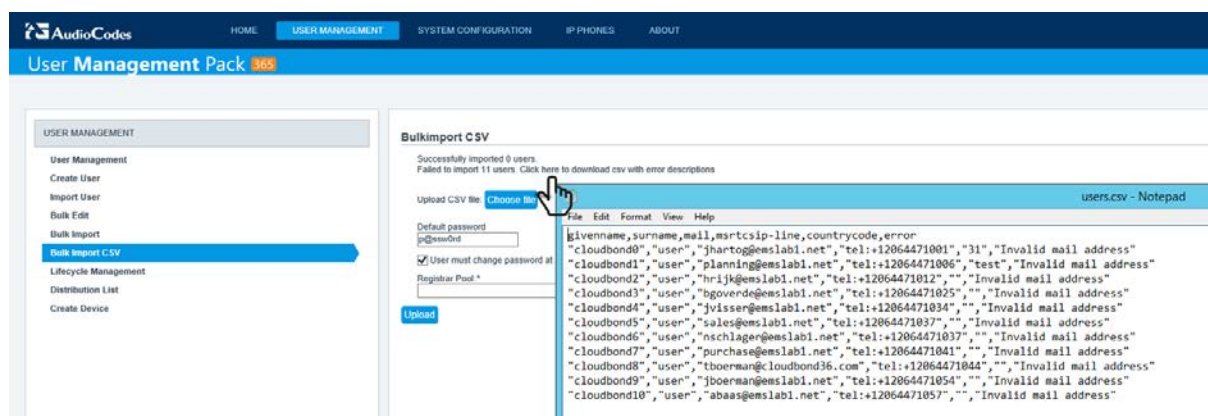
- Given name, representing the users first name
- Surname, representing the users last name
- Mail, representing the users email address that will be used to generate the SIP-address.

Additional attributes (representing Active Directory attributes) can be added to the csv file. To do this, you need to append the header row with the particular attribute that you wish to add. For example, the attribute "msrtcscip-line" can be added to the csv file and the import will also set the Skype for Business telephone number on user import.

On completion, a status message will appear at the top of the page indicating the number of successfully imported and failed users. To correct the import failures, the administrator can click the "here" link to open a csv file indicating the import errors. This csv file can be corrected and then reused for the next import session.

In the example shown below, the error indicates an incorrect email address, which in this case was caused by the fact that the email address domain name space is not one of the supported SIP domain name spaces within this Skype for Business environment.

Figure 4-32: Bulk Import CSV Error



4.12 Lifecycle Management

Lifecycle Management allows automated management of users from the Enterprise Active Directory to Skype for Business. Any users who are members of the specified Enterprise AD security groups will be automatically imported as Skype for Business users.

This will allow the Enterprise domain admin to import users into Skype for Business, simply by adding the users to the security group within the Enterprise AD.



Note: The Lifecycle management feature supports nested security groups, where users belonging to a specific group which is a group that is a member of the replicated security group, will also be automatically administered.

The groups will be assigned templates. A scheduled task will apply the policies according to these templates. The list is read top-down so if a user is a member of multiple security groups, the policies from the lowermost group will be applied and will overwrite any policies that would have been assigned by a group above.



Note: Group replication takes place as a scheduled task. An administrator can alter the frequency of replication by changing the Scheduled Task.



Warning: The Group replication scheduled task should only run on one Management server in a multi-server environment. If multiple Management servers are installed for redundancy, the scheduled tasks on the redundant servers should be disabled and only enabled if the Primary server fails to prevent Stale objects from being created in the Active Directory.



Note: Users imported through import or bulk import will not be part of group replication, even if they are added at a later stage to the user active directory forest.

➤ **To enable Lifecycle Management:**











1. Have the Enterprise Domain Administrator create one or more universal security groups, and add Enterprise domain users to those groups.
 - In the SysAdmin Lifecycle Management page, tick **Enable** Lifecycle Management
 - Click the **Add Group** link  to add a new group to the list
2. Select an Enterprise Domain and Enterprise Group from the drop down lists to add to the Select Enterprise Group list.
3. Add further security groups if required.
4. Ensure the check box of the required groups is selected.
5. Select a template to use for Importing Users.
6. Reorder the groups as required using the up and down arrow buttons .

Figure 4-33: Lifecycle Management Page

Select Enterprise Group

Group DN	Remote Domain	Replication Status	Last Replication Time	Last Synchronization Result	Actions	TemplateName
<input type="checkbox"/> CN=pc-pc-users,OU=test groups,DC=internal,DC=enterprise2016.com	internal.enterprise2016.com	New		OK	 	default
<input type="checkbox"/> CN=Q365-users,OU=test groups,DC=internal,DC=enterprise2016.com	internal.enterprise2016.com	New		OK	 	Office365
<input type="checkbox"/> CN=Ent-voice-users,OU=test groups,DC=internal,DC=enterprise2016.com	internal.enterprise2016.com	New		OK	 	Telephone from AD
<input type="checkbox"/> CN=ent-voice-unassigned-range-users,OU=test groups,DC=internal,DC=enterprise2016.com	internal.enterprise2016.com	New		OK	 	from range

View 1 - 4 of 4 Page 1 of 1 Add Group Delete Group(s)

Import Template

Telephone from AD **Edit** **Delete**

Lifecycle Management Template

TemplateName	Telephone from AD
Directory Properties & Policies	Telephone from AD
Sign in Domain	my-first-sipdomain.com
Server Pool	UC-FE1.cloudbond365.local
External Access Policy	
Conferencing Policy	MyFirstConferencingPolicy
Client Policy	
Mobility Policy	MyFirstMobilityPolicy
Grouping ID	
Telephony Settings	
Sip Acc Tmp	email
Telephony	EVOICE
Dial Plan	MyFirstDialPlan
Voice Policy	MyFirstVoicePolicy
Telephony Assignment	<input checked="" type="checkbox"/>
Telephony Assignment Type	Telephone number
Unassigned Number Range	
Use extensions	<input checked="" type="checkbox"/>
Number of digits of extension	3

➤ **To add additional templates:**

1. In the template section, click the **Edit** button; the page in which templates can be added or changed opens.
2. From the dropdown, select the template whose policies can be changed.
3. To save the changes as a new template, change the content of the 'Name' field and click **Apply changes**.
4. Click the **Back** button to return to the group replication page. Changes on the group replication page are saved instantaneously and will not require a Save action.

Figure 4-34: Add a New Template File

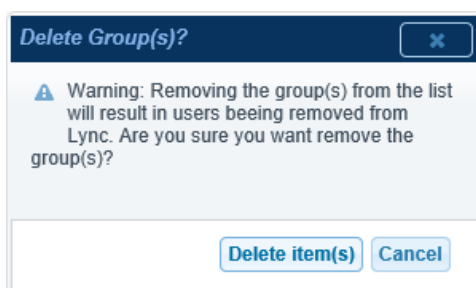
Edit Lifecycle Management Template

Template:

Name:

DIRECTORY PROPERTIES & POLICIES	TELEPHONY SETTINGS
<input checked="" type="radio"/> Use user's email address <input type="radio"/> Use FirstName.LastName @ <input type="radio"/> Use SAM AccountName @ Select Sign in domain: <input type="text" value="my-first-sipdomain.com"/>	<input type="radio"/> PC to PC <input type="radio"/> Audio/Video disabled <input checked="" type="radio"/> Enterprise Voice Voice Policy: <input type="text" value="MyFirstVoicePolicy"/> Dial Plan: <input type="text" value="MyFirstDialPlan"/>
Registrar Pool: <input type="text" value="UC-FE1.cloudbond365.local"/> External Access Policy: <input type="text" value="MyFirstExternalAccessPolicy"/> Conferencing Policy: <input type="text" value="<Automatic>"/> Mobility Policy: <input type="text" value="<Automatic>"/> Client Policy: <input type="text" value="MyFirstClientPolicy"/> Grouping: <input type="text" value="Global"/>	<input checked="" type="checkbox"/> Automatic Number Assignment Select telephony autonumbering type: <input type="text" value="Unassigned number range"/> Unassigned Number Ranges: <input type="text" value="NL"/> tel: +31365461210 - tel: +31365461249 <input type="checkbox"/> Use extension/number of digits: <input type="text" value="1"/>

5. You can remove a security group from replication by selecting it and then Clicking **Delete Group(s)**.

Figure 4-35: Deleting a Security Group from Group Replication

Warning: Removing a security group from Group Replication will also remove the corresponding users from Skype for Business.



Warning: If you remove a user from a security group in the customer forest, this user will be automatically removed from Skype for Business if the following entry is added to the <appSettings> section in the C:\acs\AcsGroupReplication\AcsGroupReplication.exe.config file:

```
<add key="DeleteEnabled" value="True" />.
```

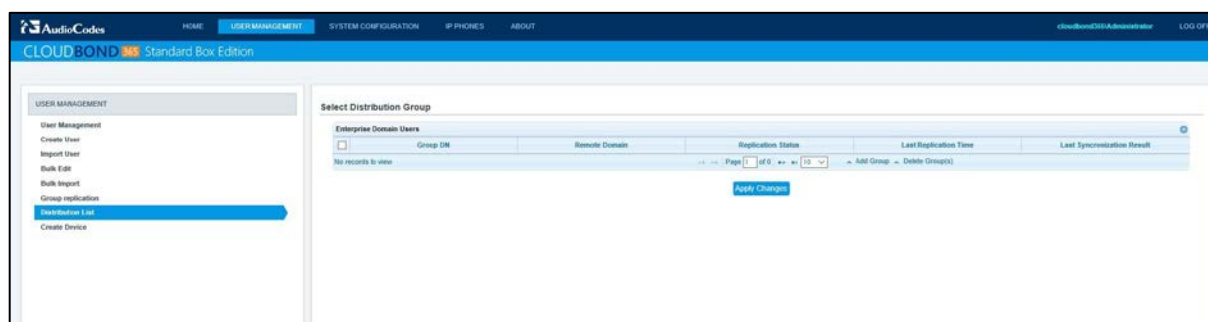
The default System Settings is to not delete the user. This implies that the Buddy List and Skype for Business Scheduled Meetings will be deleted for these users as well. Consequently if such a user was deleted by mistake and then later re-added to the security group, the Buddy List and previously scheduled meetings will also be removed.

4.13 Distribution List

The distribution list option replicates mail enabled universal distribution groups from the Enterprise AD. A mail enabled group can then be searched for in the Skype for Business client and added to the buddy list. The buddy list shows the members of the group. This way it is easy to pre-populate buddy lists.

Adding and deleting Distribution Lists is performed identically to that for Group Replication (see the previous section).

Figure 4-36: Distribution List



4.14 Create Device

The Create Device option allows the creation of Analog Devices or Common Area Phones in the Skype for Business environment, without the need to use the Skype for Business Server Management Shell, or manually create AD contact objects.

Common Area Phones are objects within Skype for Business that represents physical handsets. These devices are typically not associated with an individual user.

Analog Devices are objects within Skype for Business that represent analog devices connected to Skype for Business through a media gateway. These objects include analog handsets, fax machines etc.



Note: Some fields (like the Registrarpool, PSTN Gateway and (Sip-)domain information for example) are stored in a web cache, which will be refreshed only every few minutes. This means that some recent changes in the Skype for Business or Active Directory backend environment are not directly visible within the administration pages, but will automatically show up after maximum 10 minutes. If immediate access is required, an IISRESET needs to be performed on the CloudBond 365 management server hosting the administration Web pages.

Figure 4-37: Creating Common Area Phone

The screenshot shows the AudioCodes CloudBond 365 Standard Box Edition interface. The top navigation bar includes 'HOME', 'USER MANAGEMENT' (highlighted), 'SYSTEM CONFIGURATION', 'IP PHONES', and 'ABOUT'. The left sidebar under 'USER MANAGEMENT' lists 'User Management', 'Create User', 'Import User', 'Bulk Edit', 'Bulk Import', 'Group replication', 'Distribution List', and 'Create Device' (highlighted). The main content area is titled 'Create Analog Device or Common Area Phone'. It contains the following fields:

- Device Type*: Common Area Phone (dropdown)
- LineUri*: tel:+991234567890 (text input)
- RegistrarPool*: UC-FE2.cloudbond365.com (dropdown)
- DisplayName*: reception (text input)

A 'Create device' button is located below the fields.

Figure 4-38: Creating Analog Device

The screenshot shows the AudioCodes CloudBond 365 Standard Box Edition interface. The top navigation bar includes 'HOME', 'USER MANAGEMENT' (highlighted), 'SYSTEM CONFIGURATION', 'IP PHONES', and 'ABOUT'. The left sidebar under 'USER MANAGEMENT' lists 'User Management', 'Create User', 'Import User', 'Bulk Edit', 'Bulk Import', 'Group replication', 'Distribution List', and 'Create Device' (highlighted). The main content area is titled 'Create Analog Device or Common Area Phone'. It contains the following fields:

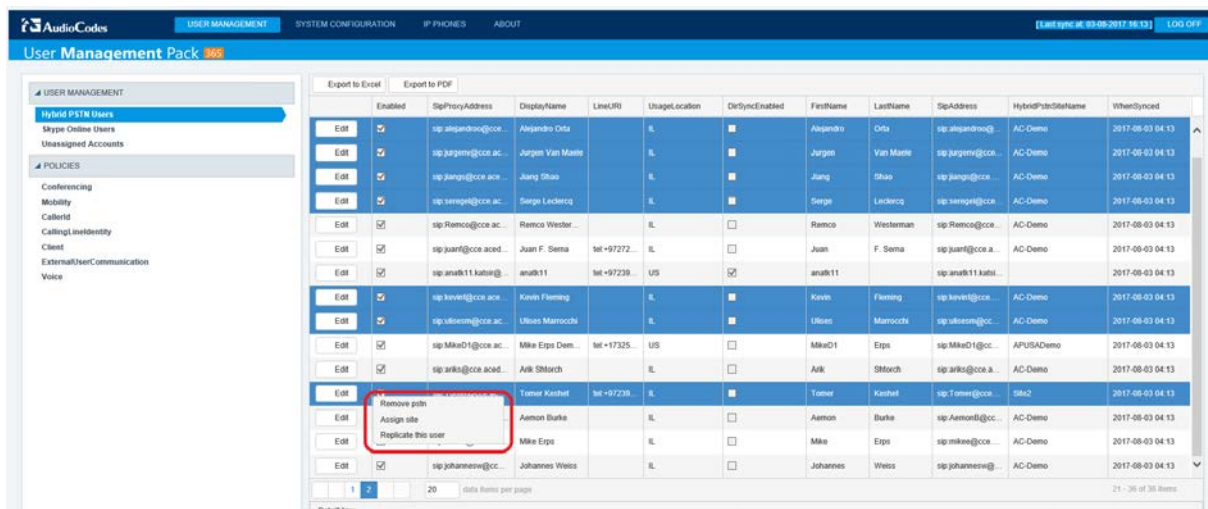
- Device Type*: Analog Device (dropdown)
- Analog Fax*: ☐
- Gateway*: 192.168.0.2 (dropdown)
- LineUri*: tel:+991234567890 (text input)
- RegistrarPool*: UC-FE2.cloudbond365.com (dropdown)
- DisplayName*: reception (text input)

A 'Create device' button is located below the fields.

4.15 User Management in Cloud PBX Environments

When deployed in Cloud PBX environments, the User Management Pack includes an enhanced a user grid (compared to the Skype for Business Server edition) by allowing multiple selection and additional context sensitive features by right-clicking into the grid.

Figure 4-39: User Management in Cloud PBX Environments

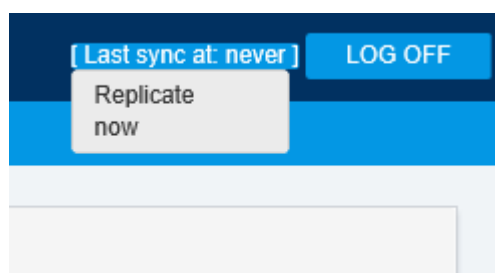


The screenshot shows the 'User Management Pack' interface. On the left is a sidebar with 'Hybrid PSTN Users' and 'POLICIES'. The main area contains a table of users. A right-click context menu is open over the user 'Amon Burke', showing options: 'Remove pin', 'Assign site', and 'Replicate this user'.

Enabled	SpProxyAddress	DisplayName	LineURI	UsageLocation	DirSyncEnabled	FirstName	LastName	SpAddress	HybridPstnStatus	WhenSynced
<input checked="" type="checkbox"/>	sp.alendro@cc...	Alejandro Orla		IL	<input checked="" type="checkbox"/>	Alejandro	Orla	sp.alendro@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.jurgem@cc...	Jurgen Van Mante		IL	<input checked="" type="checkbox"/>	Jurgen	Van Mante	sp.jurgem@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.jung@cc...	Jung Shao		IL	<input checked="" type="checkbox"/>	Jung	Shao	sp.jung@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.sergel@cc...	Serge Lickert		IL	<input checked="" type="checkbox"/>	Serge	Lickert	sp.sergel@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.Remco@cc...	Remco Wester...		IL	<input checked="" type="checkbox"/>	Remco	Westerman	sp.Remco@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.juanf@cc...	Juan F. Sema	tel +97272	IL	<input checked="" type="checkbox"/>	Juan	F. Sema	sp.juanf@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.anah11.kabi...	anah11	tel +97239	US	<input checked="" type="checkbox"/>	anah11		sp.anah11.kabi...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.kovet@cc...	Kovet Fleming		IL	<input checked="" type="checkbox"/>	Kovet	Fleming	sp.kovet@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.ubonm@cc...	Ubos Marnochi		IL	<input checked="" type="checkbox"/>	Ubos	Marnochi	sp.ubonm@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.MikeD1@cc...	Mike Epps Dem...	tel +17325	US	<input checked="" type="checkbox"/>	MikeD1	Epps	sp.MikeD1@cc...	APUSADemo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.arika@cc...	Avik Shlach		IL	<input checked="" type="checkbox"/>	Avik	Shlach	sp.arika@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.Tomer@cc...	Tomer Kishel	tel +97239	IL	<input checked="" type="checkbox"/>	Tomer	Kishel	sp.Tomer@cc...	STB2	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.AmonB@cc...	Amon Burke		IL	<input checked="" type="checkbox"/>	Amon	Burke	sp.AmonB@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.mike@cc...	Mike Epps		IL	<input checked="" type="checkbox"/>	Mike	Epps	sp.mike@cc...	AC-Demo	2017-08-03 04:13
<input checked="" type="checkbox"/>	sp.johanne@cc...	Johannes Weiss		IL	<input checked="" type="checkbox"/>	Johannes	Weiss	sp.johanne@cc...	AC-Demo	2017-08-03 04:13

Office 365 user data is cached in a backend database, which should be populated upon first sign-in by right-clicking the “Last sync status” message next to the “Log Off button” and selecting “Replicate Now”.

Figure 4-40: Last Sync Status



The status indicator changes to the status “replicating” and when finished displays the last replication time.

Figure 4-41: Log Off



The page can then be reloaded using the refresh of the browser.

4.15.1 Applying Filters

In the User Management sections, additional columns can be displayed in the Filters screen


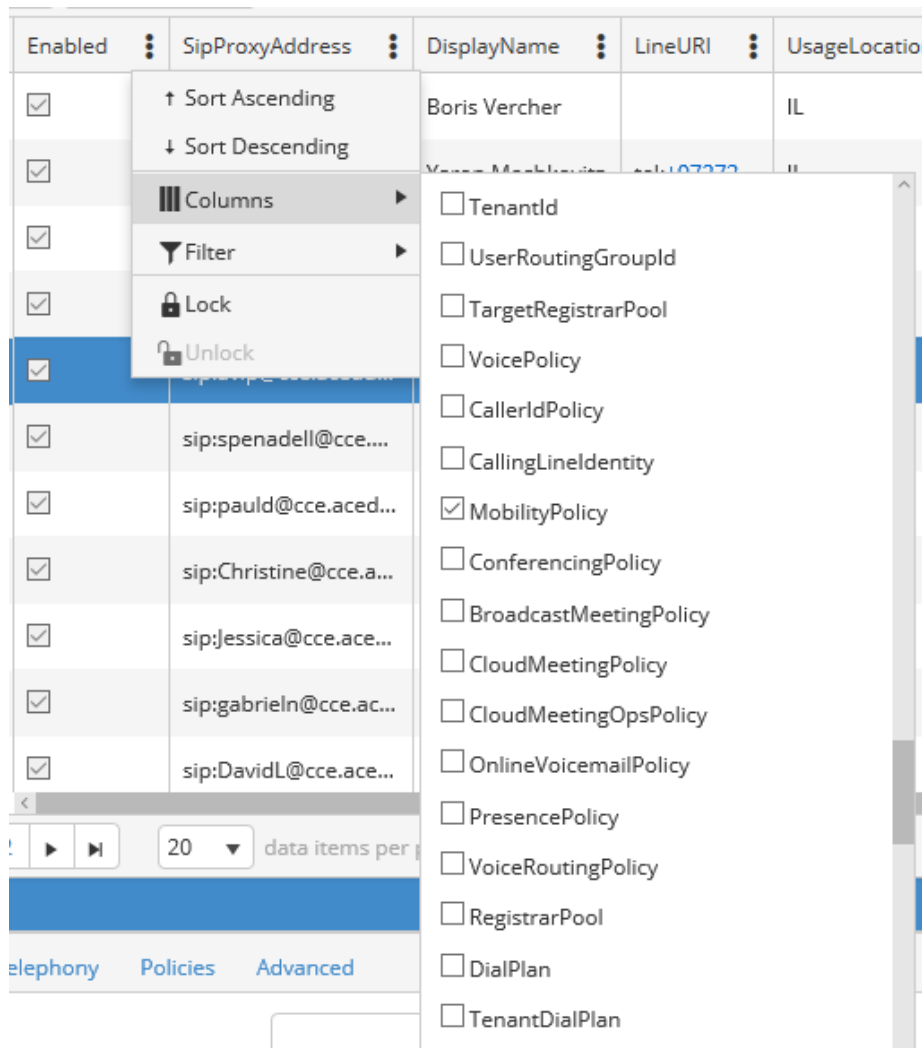
per customer requirements by selecting the  adjacent to the column headers and then selecting the check box adjacent to the column that you wish to hide or display.

Figure 4-42: Filters



Once the necessary columns are added to the view, you can filter them by selecting the filter icon and setting a value. Once a filter is applied, the background color of the three dots will change to be greyed out.

Figure 4-43: Configuring Filters

Enabled	SipProxyAddress	DisplayName	LineURI	UsageLocation
<input checked="" type="checkbox"/>	sip:borisv@cce.ace...			IL
<input checked="" type="checkbox"/>	sip:Yaron@cce.ace...		+97272...	IL
<input checked="" type="checkbox"/>	sip:Eric@cce.acedu...			
<input checked="" type="checkbox"/>	sip:victoro@cce.ace...			
<input checked="" type="checkbox"/>	sip:avip@cce.acedu...			
<input checked="" type="checkbox"/>	sip:spenadell@cce....	Spenadel Lee		
<input checked="" type="checkbox"/>	sip:pauld@cce.aced...	Paul Duarte		
<input checked="" type="checkbox"/>	sip:Christine@cce.a...	Christine Baker	tel:	

Sort Ascending
Sort Descending
Columns
Filter
Lock
Unlock

Show items with value that:
Is equal to
And
Is equal to
Filter
Clear

4.15.2 Updating the Environment

The User Management Pack in pure Cloud PBX environments (where users are homed only in Office 365 and not on premises) is a new addition to the product, which is still fully under development. As there are known issues in the product site, administrators are advised to perform an update of the Web application after first installation, by starting the C:\acs\UmpCce\wyupdate.exe application.



Note: This version is currently released to field test partners, and improvements will be made in a release in the upcoming weeks.

Figure 4-44: wyupdate.exe File

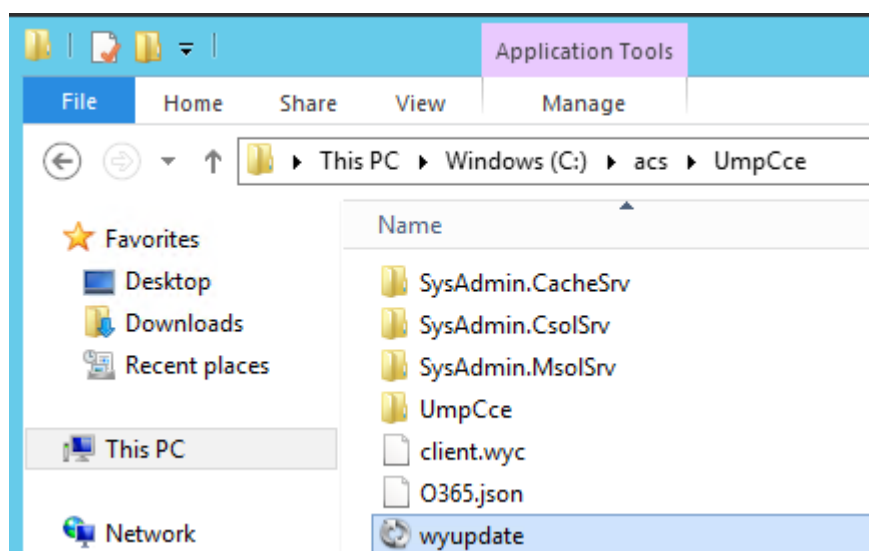
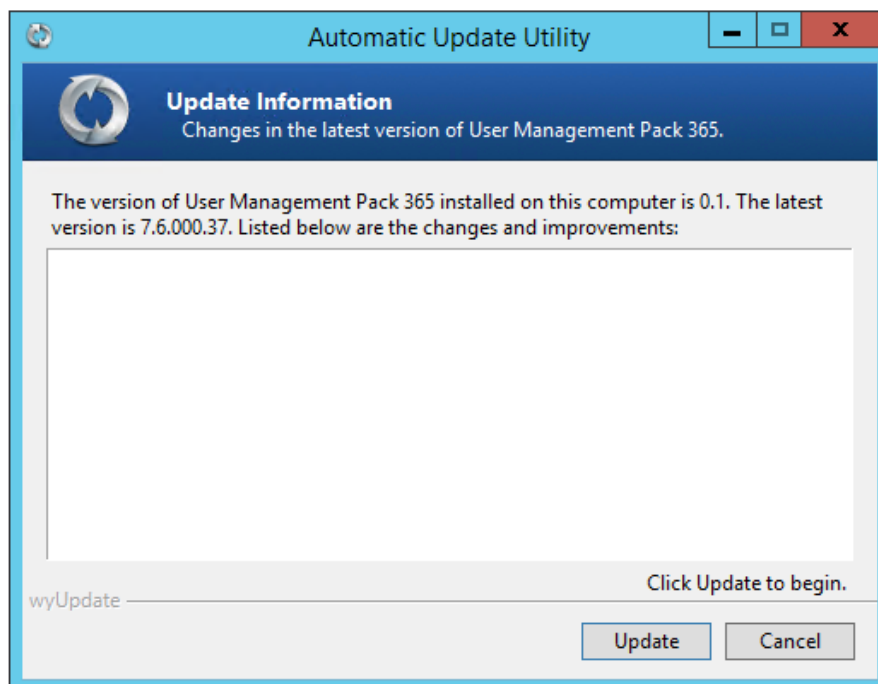


Figure 4-45: Automatic Update Utility

This page is intentionally left blank.

5 System Configuration

The UMP 365 Utility contains several System Configuration pages which provide a large amount of information about the current state of the CloudBond 365 Skype for Business Appliance. These information pages are very useful for determining the configuration of CloudBond 365, as well as diagnosing any faults.

Some of the System configuration pages also contain settings which can be updated.

5.1 System Configuration

The System Configuration page contains general information about the CloudBond 365 Skype for Business Appliance and uptime. It also allows settings for the Self Service password reset page to be configured.

Figure 5-1: System Configuration Page

The screenshot displays the 'SYSTEM CONFIGURATION' page of the CloudBond 365 Standard Box Edition. The page is divided into a left sidebar and a main content area.

Left Sidebar (SYSTEM CONFIGURATION):

- System Configuration (selected)
- Server Management
- Grouping IDs
- Call Pickup Groups
- Office 365 Configuration
- Office 365 Unified Messaging & CloudPBX Policies
- Music on Hold
- User Authentication
- Licensing Info
- EMS Settings
- Unassigned Number Range
- *Skype* Control Panel
- Select a Webserver
- skcGateway
- Select a PSTN Gateway

Main Content Area:

Active Directory

DC in use:	UC-MGR1-cloudbond365.local	
DOMAIN CONTROLLER NAME	COMPUTER TIME (GMT)	IP ADDRESS
UC-MGR1-cloudbond365.local	05/03/2017 13:42:54	10.0.0.153

Self Service

Enable Password Reset: ☒

Max number of attempts:

Reset per page:

Email Settings

Send notification email from:

Send mail for admin requests to:

Use this smtp server to route messages:

SMTP Port:

5.2 Self Service

The UMP 365 contains a Self Service password reset feature for CloudBond 365 users.



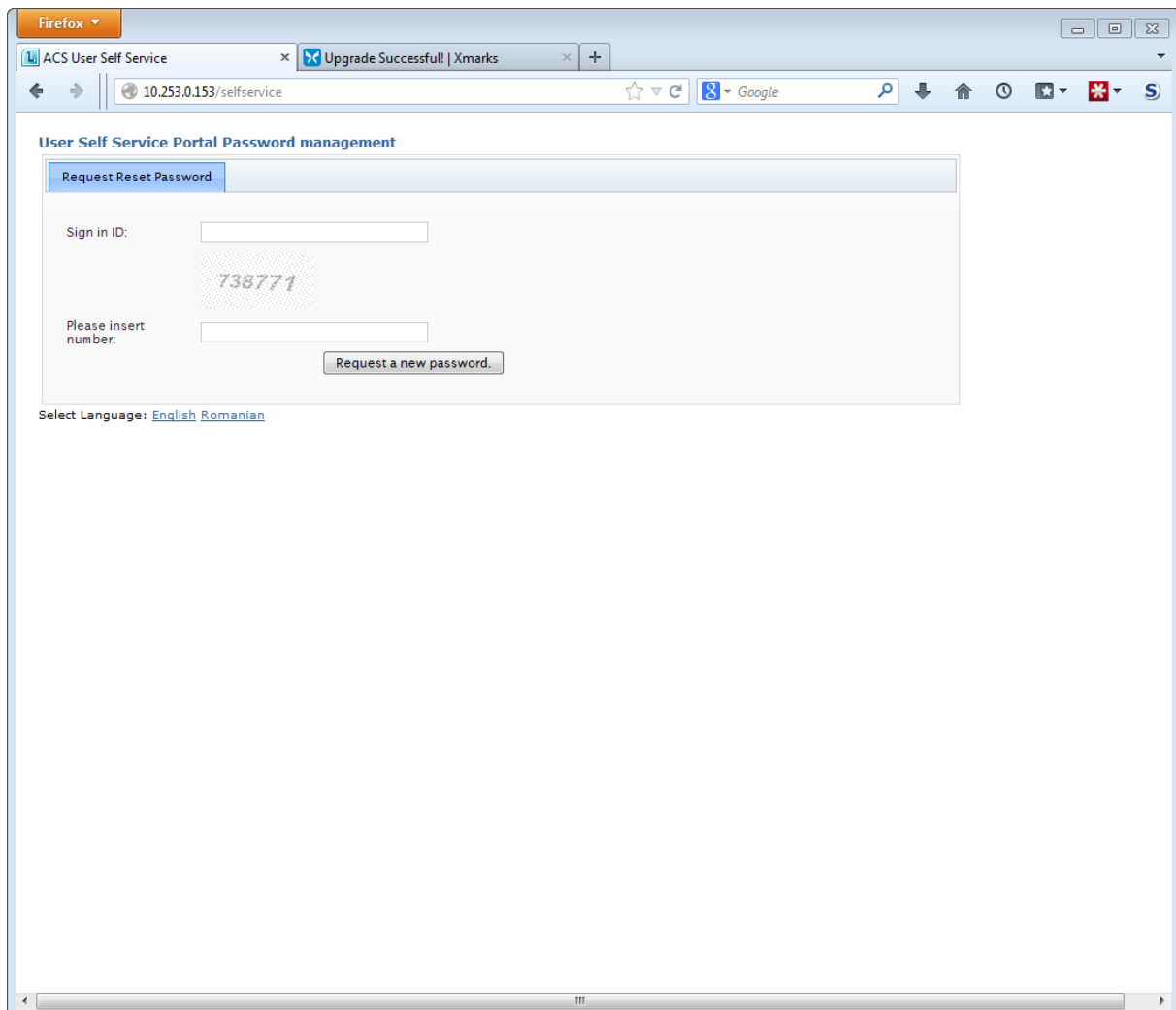
Note: This feature is intended for CloudBond 365 when deployed in Standalone mode, or for use of Local CloudBond 365 users. Users imported or replicated from the customer domain via forest trust should not use this feature.



Note: For this feature to work, it must be enabled as described on the previous page, and also have the Email configuration completed, as described in the following section.

This web page will generate an email with password reset instructions.

Figure 5-2: Self Service Password Reset



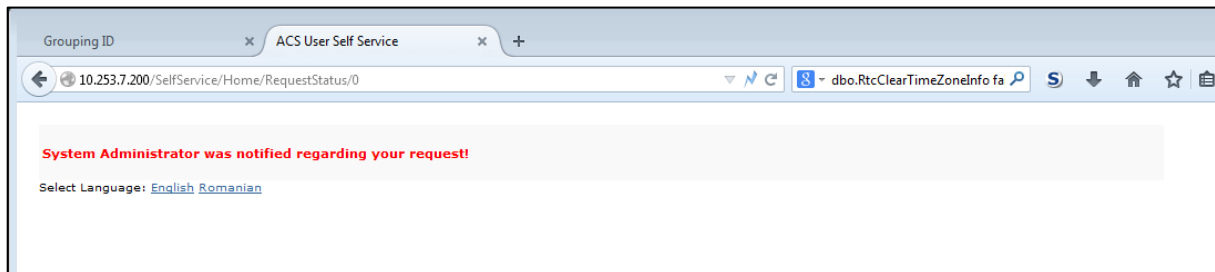
The screenshot shows a Firefox browser window with the address bar displaying `10.253.0.153/selfservice`. The page title is "User Self Service Portal Password management". Below the title, there is a section titled "Request Reset Password" with a blue header. Inside this section, there are two input fields: "Sign in ID:" and "Please insert number:". The "Please insert number:" field contains the CAPTCHA code "738771". Below the input fields is a button labeled "Request a new password...". At the bottom of the page, there is a language selection link: "Select Language: [English](#) [Romanian](#)".

The Self Service password reset page can be accessed by Skype for Business users. The Web URL is `http://<CloudBond 365 Controller>.<CloudBond 365 FQDN>/Selfservice` e.g., `http://uc-dc.ac-onebox.com/SelfService` or `http://192.168.0.100/SelfService`



Note: To make this feature more useful, make the Self Service page available to external users via a Reverse Proxy.

Figure 5-3: Self Service Password Request



5.3 Email Configuration

You can configure email server settings on the System Configuration page, to be used by the Self Service application. UMP 365 will only send email message by means of a server that is configured for relaying.



Note: If an IP address is entered in the “Use this SMTP server to route messages” instead of a Fully Qualified Domain Name, it needs to be between the “[” and “]” brackets.

5.4 Server Management

The server management pages provide a quick method to change the Network IP settings for each server within the CloudBond 365 system. The page is designed for simple IP Networks. These networks require the CloudBond 365 Controller, Front End, and Edge internal network interfaces to be on a common subnet.

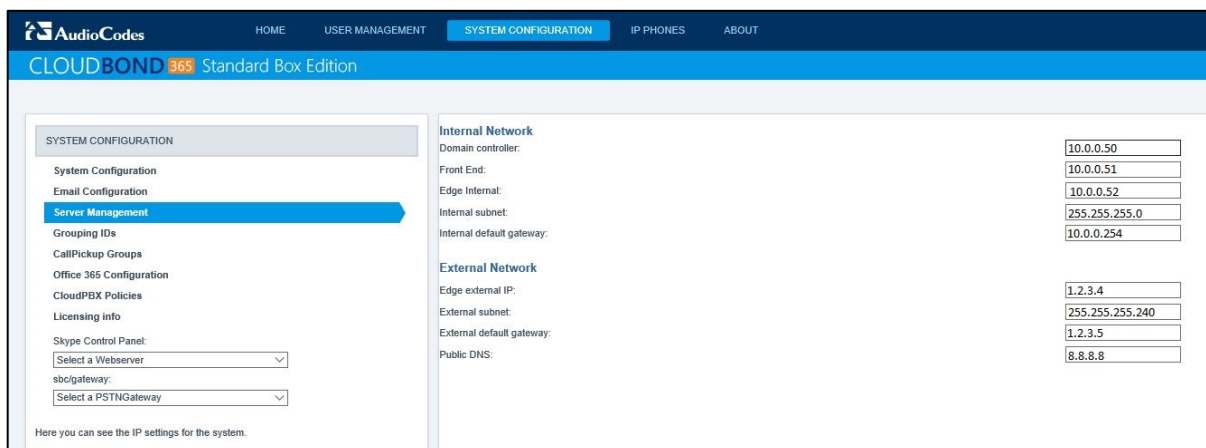


Note: Server Management pages are only available in the 'Co-Located DC and Hyper-V Host' deployment model. These pages are therefore typically only available to CloudBond 365 Standard Box Edition. For CloudBond 365 Pro and Enterprise Box Editions, see *AudioCodes CloudBond 365 Manual IP Address Configuration Guide*.

The Server Management master page allows you to quickly set the IP addresses of the CloudBond 365 servers.

Enter the required IP addresses and click **Update**. The system will validate the new IP addresses, then update each server in the correct sequence, along with the topology and DNS records.

Figure 5-4: Server Management (Master)



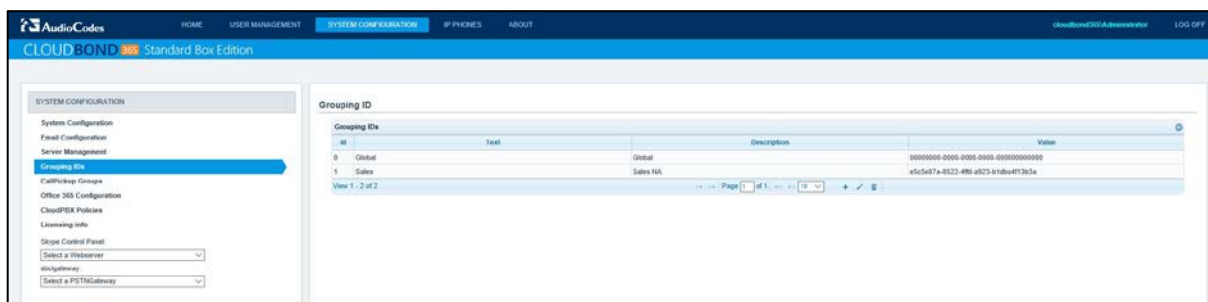

Warning: If you have already deployed the CloudBond 365 system to an enterprise network, you may need to adjust the DNS settings used in the Enterprise network to match the changes. e.g., Stub Zones used to provide Forest Trust.

5.5 Grouping IDs

Grouping IDs allow Skype for Business contacts to be separated and segregated into groups. This allows you to restrict which Skype for Business users can see which contacts within the Skype for Business environment.

Grouping IDs defined on this page are available to be applied to individual users in the User Management pages.

Figure 5-5: CloudBond 365 Grouping IDs



➤ **To add a new Grouping ID:**

1. Click the **+** icon.
2. Enter **Text** (name) and **Description**.
3. Click **Submit**.

Figure 5-6: Adding a Grouping

➤ **To Edit a Grouping ID:**

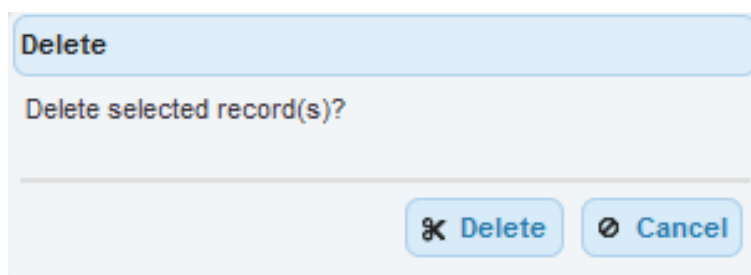
- Click the **Pencil** icon.

Figure 5-7: Editing a Group Record

➤ **To Delete a Grouping ID:**

- Click the **Trash** icon.

Figure 5-8: Deleting a Record

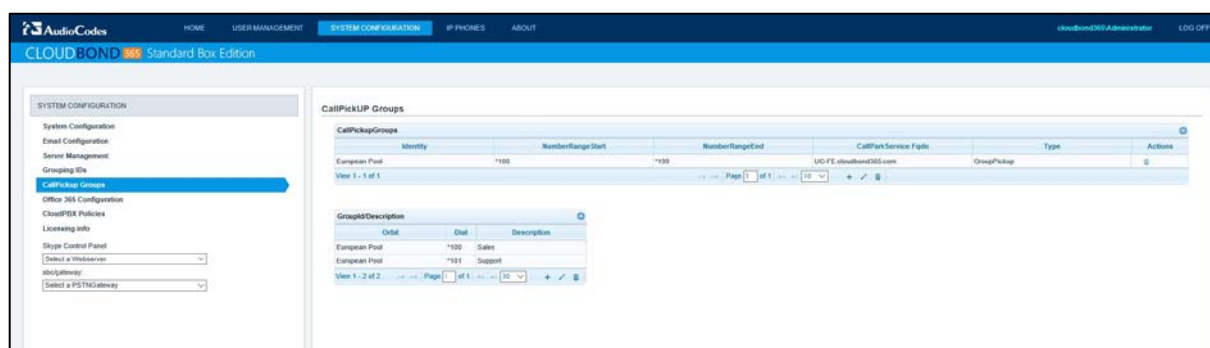


5.6 CallPickup Groups

CallPickup Groups are a feature of Skype for Business which allows members of the group to pickup calls ringing on another extension within the group.

To make configuration of CallPickup Groups easier, the feature has been added to the SysAdmin Web pages.

Figure 5-9: Defining CallPickup Groups

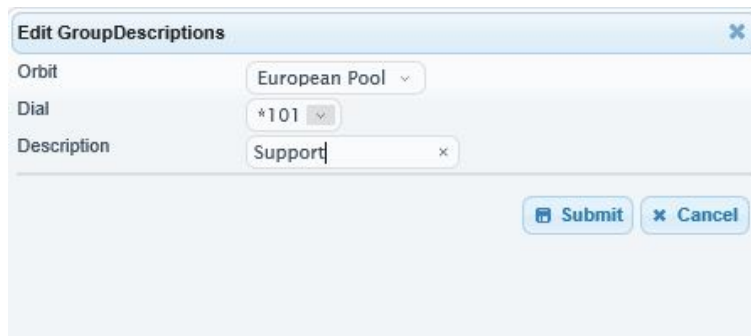


➤ **To configure a CallPickup group:**

1. Create a new call park orbit in the top section (CallPickupGroups). The orbit should contain enough extensions to support the number of simultaneous calls for the group. Click the + to create a new orbit.

Figure 5-10: Defining the CallPickup Orbit

2. Create a group id and assign it to the orbit. The Call Pickup Group ID is allocated to all users within the group. As part of the ID, you must select a pickup code from one of the orbit numbers.

Figure 5-11: Defining the Call Pickup Group ID

Edit GroupDescriptions

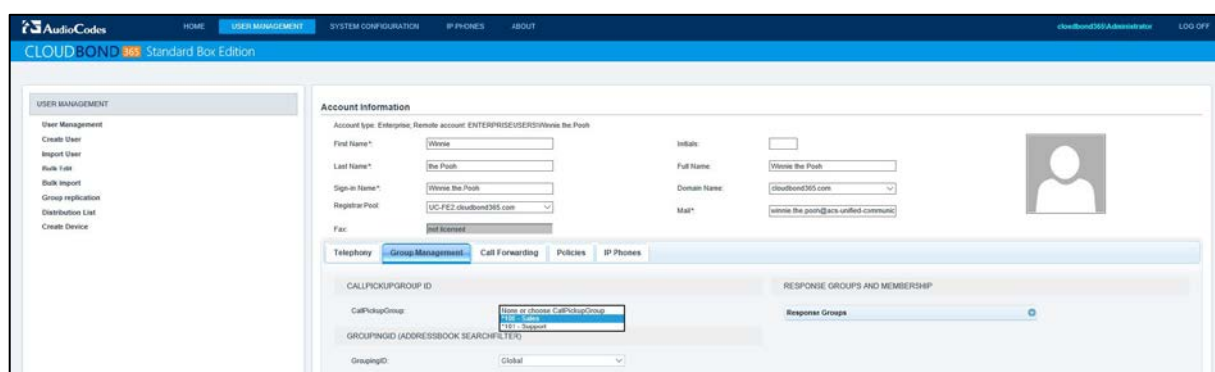
Orbit: European Pool

Dial: *101

Description: Support

Submit Cancel

3. Edit the selected Skype for Business users, and assign them to the CallPickupGroup ID under the Group Management tab.

Figure 5-12: Assigning the Call Pickup ID to a User

AudioCodes HOME USER MANAGEMENT SYSTEM CONFIGURATION IP PHONES ABOUT cloudbond365 Administrator LOG OFF

CLOUDBOND 365 Standard Box Edition

USER MANAGEMENT

- User Management
- Create User
- Import User
- Rules List
- Bulk Import
- Group replication
- Distribution List
- Create Device

Account Information

Account type: Enterprise, Remote account ENTERPRISEUSERS/Writes the Pool

First Name*: Write

Last Name*: the Pool

Sign-in Name*: Write the Pool

Registrar Pool: UC-FEZ-cloudbond365.com

Fac: not known

Initials:

Full Name: Write the Pool

Domain Name: cloudbond365.com

Mail*: write the pool@acts.unified-communications.com

Telephony **Group Management** Call Forwarding Policies IP Phones

CALLPICKUPGROUP ID

CallPickupGroup: None or choose CallPickupGroup
101 - Support
102 - Reception

GROUPINGID (ADDRESSBOOK SEARCHFILTER)

GroupingID: Global

RESPONSE GROUPS AND MEMBERSHIP

Response Groups:

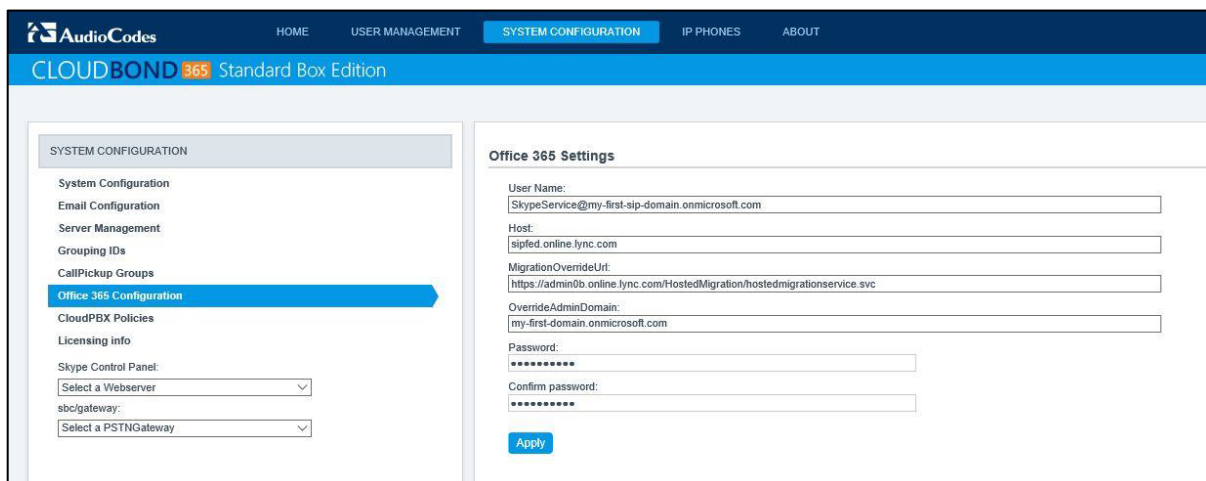
5.7 Office 365 Configuration

Refer the *AudioCodes CloudBond 365 Installation Manual* document for details on how to configure Office 365 integration with UMP 365. This document also contains information on how to obtain values required for the Office 365 Configuration screen within the UMP 365.

After completing the pre-requisite setup steps for Office 365 Integration, the process can be completed by supplying the following information on the SysAdmin page:

- **User Name:**
 - The login name of your Office 365 Administrator
- **Host:**
 - The location where your Office 365 environment is hosted
- **Migration Override URL:**
 - Refer to the document *AudioCodes CloudBond 365 Installation Guide*
- **Override Admin Domain:**
 - Your original Office 365 domain prior to applying vanity domain names
- **Password:**
 - The Office 365 Administrator password

Figure 5-13: Office 365 Connector Settings



The screenshot shows the 'Office 365 Settings' configuration page. On the left is a sidebar with a 'SYSTEM CONFIGURATION' menu where 'Office 365 Configuration' is selected. The main area contains the following fields:

- User Name:** SkypeService@my-first-sip-domain.onmicrosoft.com
- Host:** sipfed.online.lync.com
- MigrationOverrideUrl:** https://admin0b.online.lync.com/HostedMigration/hostedmigrationservice.svc
- OverrideAdminDomain:** my-first-domain.onmicrosoft.com
- Password:** (masked with asterisks)
- Confirm password:** (masked with asterisks)

An 'Apply' button is located at the bottom of the form.

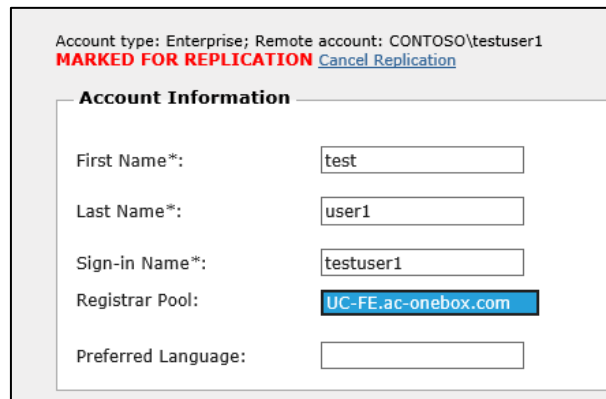
Once the Office 365 connector is fully configured and the first synchronization has been performed, it is possible to assign users to each system (CloudBond 365 or Office 365).

➤ **To change a user's assigned system:**

1. Select the user in the User Management List.
2. Click **Edit**.
3. Change the users Registrar Pool.
4. Save your changes.

Assigning a destination Frontend pool to a user:

Figure 5-14: Assigning a user to a FE pool



Account type: Enterprise; Remote account: CONTOSO\testuser1
MARKED FOR REPLICATION [Cancel Replication](#)

Account Information

First Name*:

Last Name*:

Sign-in Name*:

Registrar Pool:

Preferred Language:

5.7.1 Office 365 Unified Messaging (UM) and Cloud PBX Policies

To be able to support the Office 365 Unified Messaging (UM) and Cloud PBX feature, Voice Routing Policies need to be created to hold the PSTN Usage records that are allowed to be called by Cloud PBX users with On-Premise PSTN breakout.

The Voice Routing Policies are created in the CloudPBX VoiceRoutingPolicies Management screen. Once created, they can be assigned to the PSTN Usage Records.

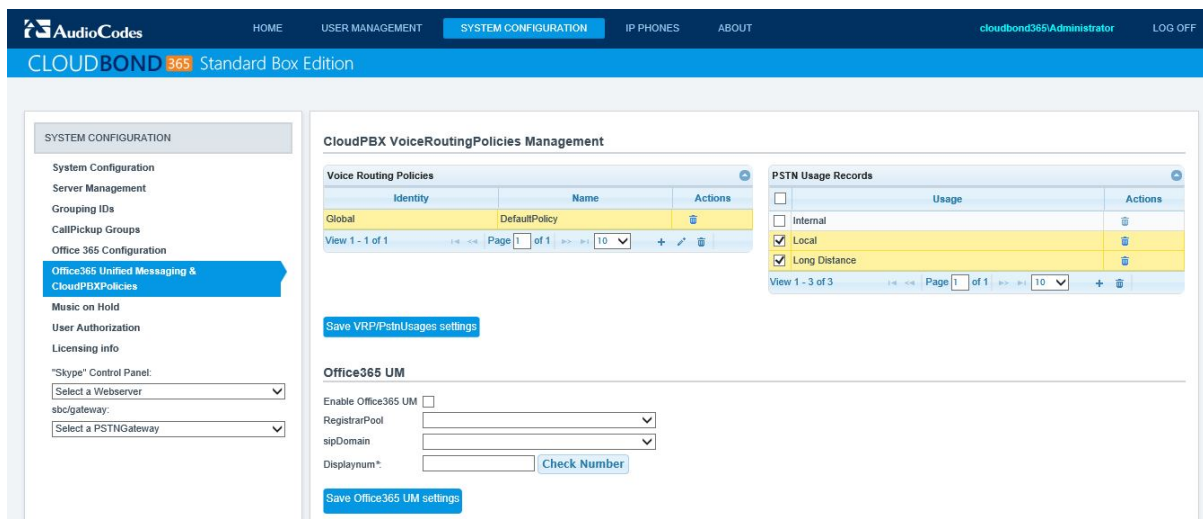


Note: UMP 365 provides native integration to Office 365 Unified Messaging (UM) by means of an intuitive interface. Once the prerequisites of Office 365 integration as outlined in the *AudioCodes CloudBond 365 Office 365 Integration Configuration Note Ver. 7.2* are configured, you can use this capability.

➤ **Do the following:**

1. Select / create a Voice Routing Policy.
2. Select the check boxes for the PSTN Usage records to bind to this policy.
3. Click **Save VRP/PstnUsages settings** to save the settings to the backend environment.

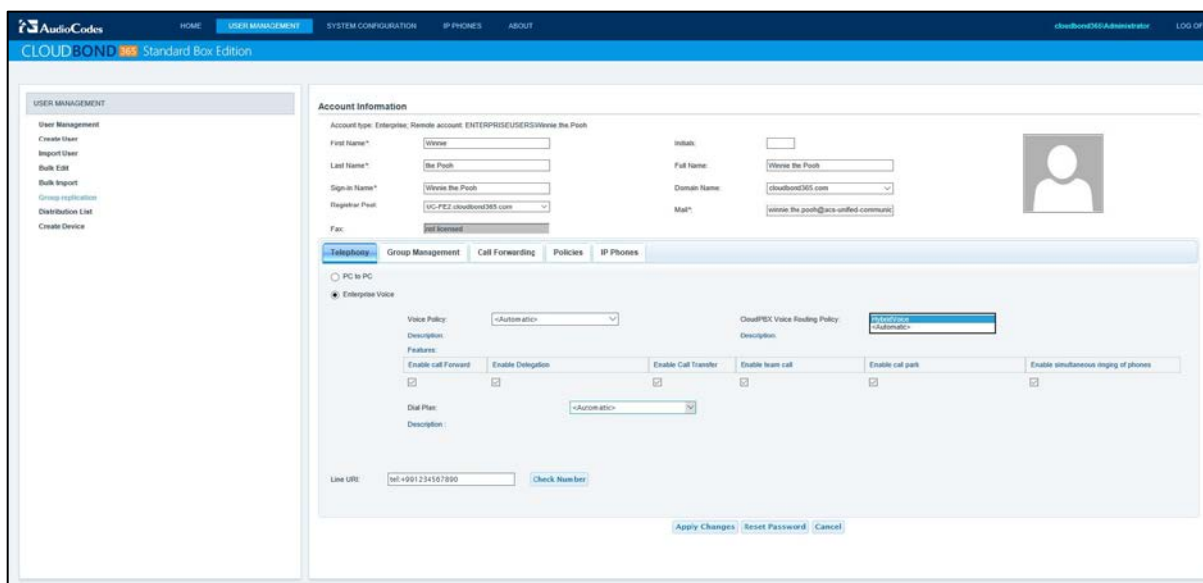
Figure 5-15: Voice Routing Policies and PSTN Usages



The screenshot shows the 'SYSTEM CONFIGURATION' page in the CloudBond 365 Standard Box Edition. The left sidebar lists various configuration options, with 'Office365 Unified Messaging & CloudPBX Policies' selected. The main content area is titled 'CloudPBX VoiceRoutingPolicies Management'. It features two tables: 'Voice Routing Policies' and 'PSTN Usage Records'. The 'Voice Routing Policies' table has columns for Identity, Name, and Actions, and shows a single policy named 'DefaultPolicy'. The 'PSTN Usage Records' table has columns for Usage and Actions, and shows three records: 'Internal', 'Local', and 'Long Distance'. Below the tables are buttons for 'Save VRP/PstnUsages settings' and 'Save Office365 UM settings'. The 'Office365 UM' section includes fields for 'Enable Office365 UM', 'RegistrarPool', 'sipDomain', and 'Displaynum*', along with a 'Check Number' button.

After the Voice Routing Policies have been created, they can be assigned to the user on the **Telephony** tab in User Edit mode (see Section 4.6.2 on page 40 for more information):

Figure 5-16: Voice Routing Policies Assigned to User



The screenshot shows the 'USER MANAGEMENT' page in the CloudBond 365 Standard Box Edition. The left sidebar lists various user management options, with 'Telephony' selected. The main content area is titled 'Account Information' and shows the details for a user named 'Vince'. The 'Telephony' tab is active, and the 'Enterprise Voice' section is expanded. It shows the 'Voice Policy' set to 'Automation' and the 'CloudPBX Voice Routing Policy' set to 'DefaultPolicy'. There are checkboxes for 'Enable call Forward', 'Enable Delegation', 'Enable Call Transfer', 'Enable team call', 'Enable call park', and 'Enable simultaneous ringing of phones'. The 'Dial Plan' is set to 'Automation'. The 'Line URI' is 'tel:+991234567890'. At the bottom are buttons for 'Apply Changes', 'Reset Password', and 'Cancel'.

➤ **To enable the Office 365 UM feature:**

1. Open the Office 365 Unified Messaging & CloudPBX Policies page under the System Configuration menu.
2. Select the 'Enable Office 365 UM' check box.
3. From the 'RegistrarPool' drop-down list, select a Registrar pool.
4. From the 'sipDomain' drop-down list, select a sipDomain.
5. In the 'Displaynum*' field, enter the telephone number to be used.
6. In the organization field, add the office365 domain to be used (use the overrideadmindomain if there are multiple domains registered within Office 365).

Figure 5-17: Office365 UM

Once enabled, users can be assigned Office 365 UM capabilities in the User Edit screen by enabling the 'Office365 Exchange UMPolicy' check box.

Figure 5-18: Office365 Exchange UMPolicy

5.8 Music on Hold

Music on Hold (MoH) files can be centrally administered using the Music on Hold page under the System Configuration menu in the sysadmin web pages:

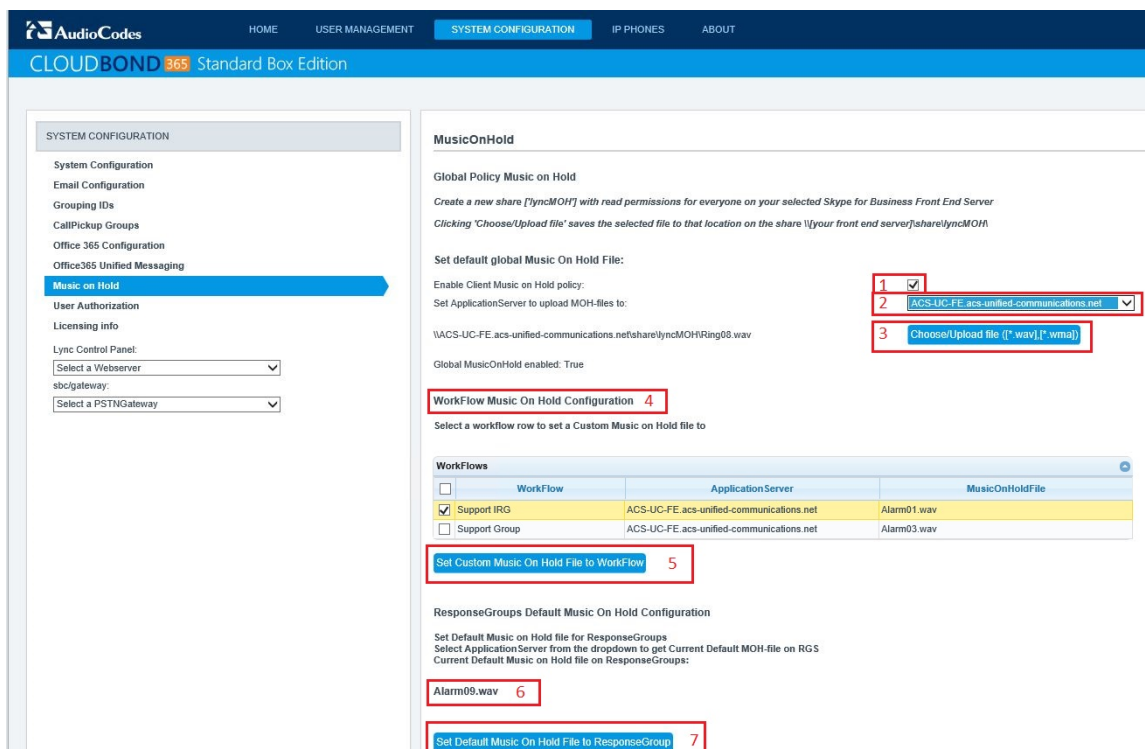
Before you start managing MoH, create a new share ['lyncMOH'] with read permissions for everyone on your selected Skype for Business Front End Server.

➤ **To configure MoH (refer to the corresponding numbers in Figure 5-13):**

1. Select the 'Enable Client Music on Hold policy' check box.
When selected, the global client policy entry EnableClientMusicOnHold is enabled, in which case, this file is played to a caller when placed on hold by a Skype client. If this option is cleared, the EnableClientMusicOnHold entry is disabled.
Note that if a MusicOnHoldAudioFile entry is present and this option is disabled, then the file will not be removed from the policy.
2. From the 'Set ApplicationServer to upload MOH-files' drop-down list, select the Front End Application server that will be used to store the MoH file.
3. Use the button to browse for and upload a MoH file to the server.
4. In the WorkFlows table, select the check box for the WorkFlow entry to set a custom MOH file.
This feature enables you to upload and assign a MOH file for the selected "Response Group" workflow.
5. Use the browse button to browse to a MoH file to upload for the selected workflow.
6. Displays the current assigned MoH file for response groups.
7. Allows changing the default MoH file for response groups.

This feature enables you to assign a default "Response Group" MOH file to play if you did not assign an MOH file to an individual Response Group" workflow in step 4.

Figure 5-19: Music on Hold



MusicOnHold

Global Policy Music on Hold

Create a new share ['lyncMOH'] with read permissions for everyone on your selected Skype for Business Front End Server
Clicking 'Choose/Upload file' saves the selected file to that location on the share \\your front end server\share\lyncMOH

Set default global Music On Hold File:

Enable Client Music on Hold policy: ☒ 1

Set ApplicationServer to upload MOH-files to: 2 ACS-UC-FE.acs-unified-communications.net

3 Choose/Upload file (*.wav;*.wma)

\\ACS-UC-FE.acs-unified-communications.net\share\lyncMOH\Ring08.wav

Global MusicOnHold enabled: True

WorkFlow Music On Hold Configuration 4

Select a workflow row to set a Custom Music on Hold file to

WorkFlows	WorkFlow	ApplicationServer	MusicOnHoldFile
<input checked="" type="checkbox"/>	Support IRG	ACS-UC-FE.acs-unified-communications.net	Alarm01.wav
<input type="checkbox"/>	Support Group	ACS-UC-FE.acs-unified-communications.net	Alarm03.wav

5 Set Custom Music On Hold File to WorkFlow

ResponseGroups Default Music On Hold Configuration

Set Default Music on Hold file for ResponseGroups
Select ApplicationServer from the dropdown to get Current Default MOH file on RGS
Current Default Music on Hold file on ResponseGroups:

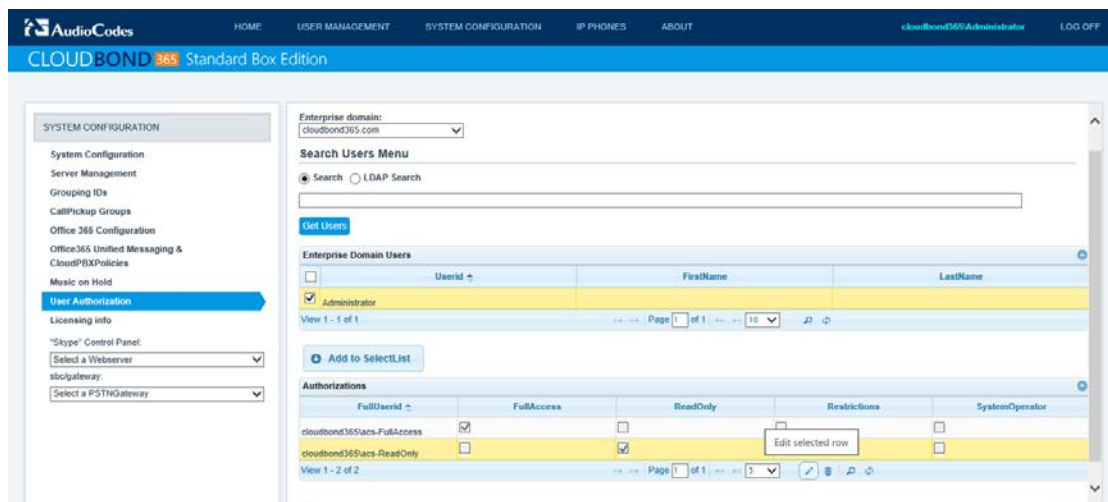
Alarm09.wav 6

7 Set Default Music On Hold File to ResponseGroup

5.9 User Authorization

Access to the Management Pack application (SysAdmin) can be given to users from the CloudBond 365 or Enterprise Forests in the User Authorization page.

Figure 5-20: User Authorization



By default, the following security groups are created:

- ACS-FullAccess – allows the administrator to perform any change using the UMP 365 Web Admin
- ACS-ReadOnly – allows the administrator view only capabilities with no ability to set any changes.


To edit a user's authorization, select the user (group) and then click the Pencil icon  in the Status bar at the bottom of the screen. A popup allows you to select the appropriate level of access:

Figure 5-21: Edit Record

When the **Restrictions** check box is selected, another selection box is displayed, where you can limit the administration based on sipDomains or RegistrarPools.

When selecting the **SystemOperator** check box, access is only given to the **System Configuration** pages by default.

5.10 Unassigned Number Range


The Unassigned Number Range allows an administrator to define ranges with numbers that belongs to the organization. If numbers in these ranges are unassigned to users, callers will hear a greeting, which can be a recorded wav file or a text to speech message, after which they will be transferred to a SIP endpoint, which can be the SIP address from a response group representing the operator.

- Unassigned Number Ranges can be used in Lifecycle Management to automatically assign telephone numbers on user creation.
- The creation of unassigned Number Ranges is a two-step process, where at first the announcement has to be created.

➤ To configure an unassigned number range:

1. Open the Add Announcement screen (**System Configuration > Unassigned Number Range**) and add a new announcement.

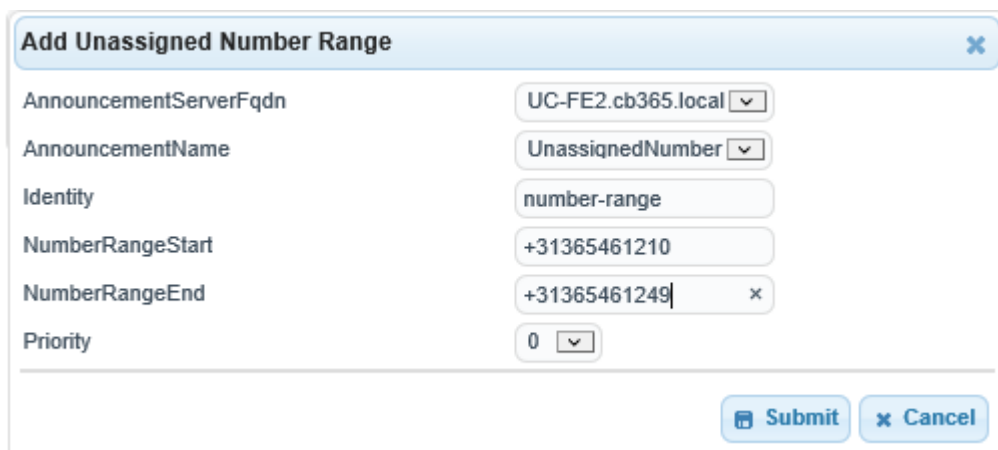
Figure 5-22: Add Announcement




Note: The TargetUri needs to start with SIP; if this is forgotten, the server will print an internal server error.

2. Assign a range with numbers to this announcement.

Figure 5-23: Add Unassigned Number Range



5.11 Skype for Business Control Panel (Quick Access)

The Skype for Business Control Panel is one of the many administration and configuration tools provided by Microsoft to manage the Skype for Business environment. The Skype for Business Control Panel is based on Silverlight, so is best run from Internet Explorer.

A quick link to the Control Panel is available within UMP 365, should you need to perform some detailed or advanced configuration.



Note: The Skype for Business Control Panel is available from each FE server in your CloudBond 365 system. Choose an FE Server from the drop down list.

Figure 5-24: Select a FE Server for Skype for Business Control Panel

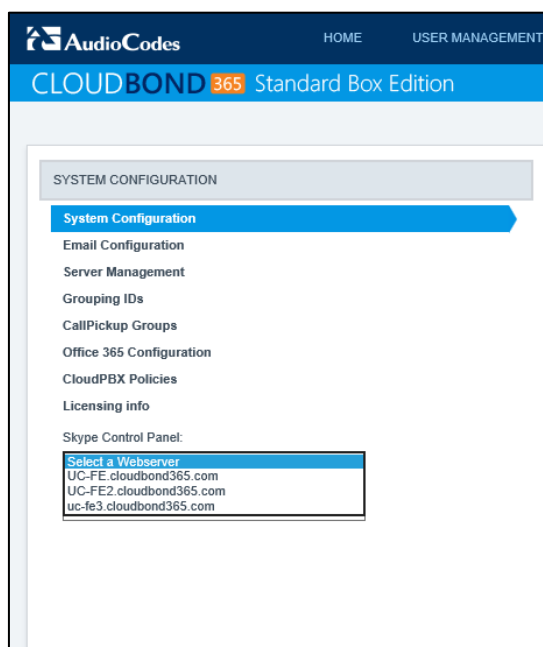
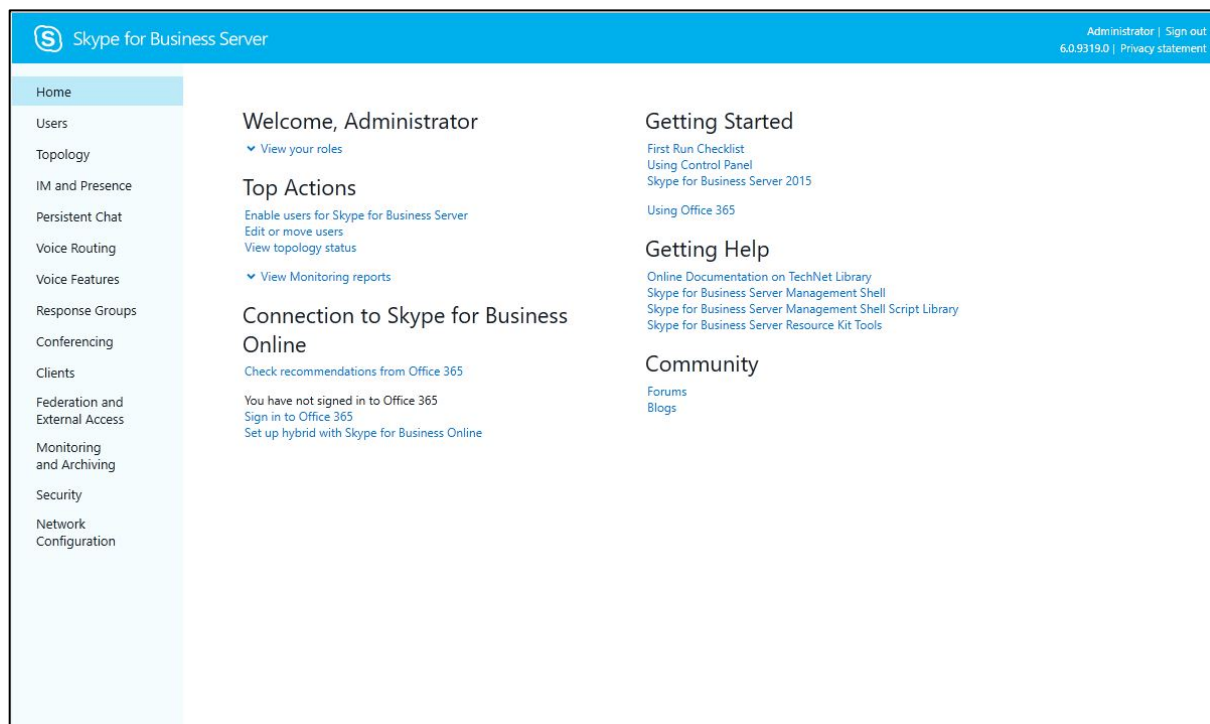
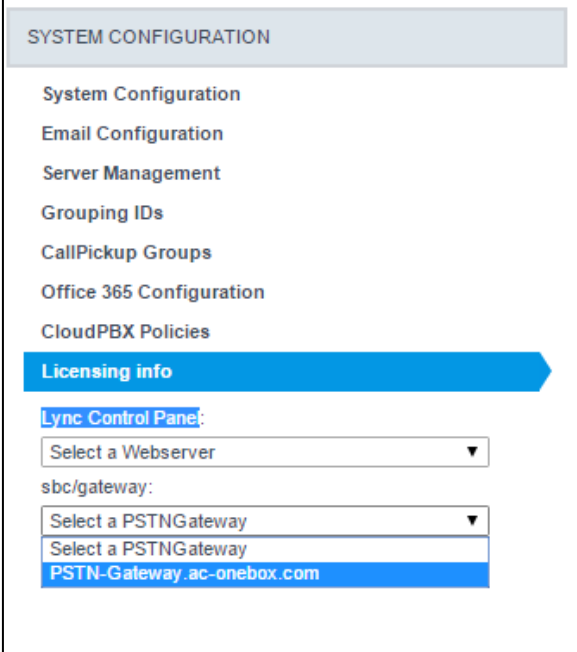


Figure 5-25: Skype for Business Control Panel


5.12 SBC / Gateway Administration Panel (Quick Access)

The SBC / Gateway Administration Panel allows you to set and manage the AudioCodes SBC/GW configuration for setting PSTN or SIP trunk connectivity. A quick link to the Administration Panel is available within UMP 365, should you need to perform some detailed or advanced configuration. Choose the SBC/GW Server from the drop-down list.

Figure 5-26: Select an SBC/GW Server for SBC/Gateway



The screenshot displays the 'SYSTEM CONFIGURATION' panel. A list of configuration categories is shown on the left, with 'Licensing info' highlighted in blue. Below this, the 'Lync Control Panel:' section contains a dropdown menu labeled 'Select a Webserver'. The 'sbc/gateway:' section features a dropdown menu labeled 'Select a PSTNGateway' with a list of options: 'Select a PSTNGateway', 'PSTN-Gateway.ac-onebox.com' (highlighted in blue), and 'PSTN-Gateway.ac-onebox.com'.

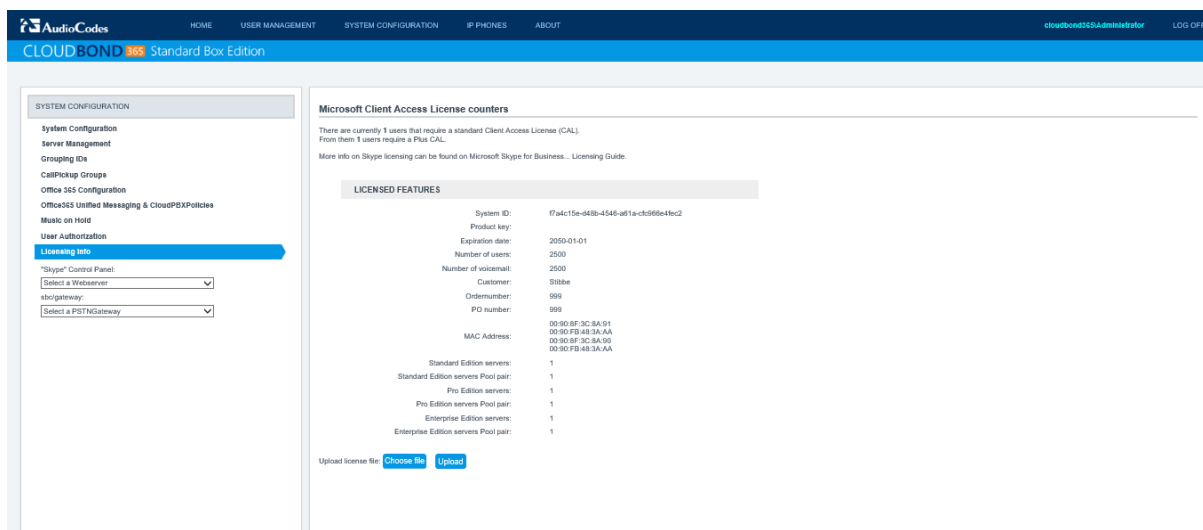
5.13 Licensing Information

The Licensing Information page displays information about your system license, including:

- Number of users
- Number of servers
- When the license will expire

This page also allows the installation of a new license, by simply browsing to the new license file, then clicking **Upload**. A system without a license file installed will not operate. UMP 365 will cease to operate once the license date expires.

Figure 5-27: UMP 365 License



The screenshot shows the CloudBond 365 Standard Box Edition web interface. The top navigation bar includes links for HOME, USER MANAGEMENT, SYSTEM CONFIGURATION, IP PHONES, and ABOUT. The user is logged in as cloudbond365Administrator. The left sidebar shows the SYSTEM CONFIGURATION menu with options like System Configuration, Server Management, Grouping IDs, Call Pickup Groups, Office365 Configuration, Office365 Unified Messaging & CloudPBX Policies, Music on Hold, User Authorization, and Licensing Info (which is highlighted). The main content area displays the Microsoft Client Access License counters, indicating 1 user requiring a standard Client Access License (CAL) and 1 user requiring a Plus CAL. Below this, the LICENSED FEATURES section lists various system details:

LICENSED FEATURES	
System ID:	074c15e-64b0-4546-a01a-ck090e4fbc2
Product key:	
Expiration date:	2050-01-01
Number of users:	2500
Number of voicemail:	2500
Customer:	Sibbe
Order number:	999
PO number:	999
MAC Address:	00:90:FB:3C:8A:91 00:90:FB:48:3A:AA 00:90:FB:3C:8A:90 00:90:FB:48:3A:AA
Standard Edition servers:	1
Standard Edition servers Pool pair:	1
Pro Edition servers:	1
Pro Edition servers Pool pair:	1
Enterprise Edition servers:	1
Enterprise Edition servers Pool pair:	1

At the bottom, there is an 'Upload license file' section with 'Choose file' and 'Upload' buttons.

5.14 Monitoring CloudBond 365 in One Voice Operations Center

The CloudBond 365 system can be monitored remotely by the One Voice Operations Center server. This monitoring includes the following features:

- Display the CloudBond system info and status:
 - The type of the CloudBond system
 - Health status of the system
 - Name of the system
 - Location of the system
 - Skype for Business version
 - Sip domains
 - Number of users
- Display the CloudBond system components

The CloudBond 365 status screen in the One Voice Operations Center contains all the components of the CloudBond environment with the following information:

 - Name
 - Component health status
 - Type
 - FQDN
 - IP Addresses
 - Serial number (if applicable)
 - OS version
 - SfB CU version (if applicable)
 - Component up time
- The following types of alarms and events are raised on the CloudBond 365 system and displayed in the One Voice Operations Center alarm browser:
 - Alarms about services that down in the components
 - Alarms about performance counter threshold exceed in the components
 - Events from components event log
 - Alarms about license problems
 - Alarms from SBC – (if monitored)



Note: To increase the efficiency of the alarm reporting, the monitoring parameters may be manually configured according to system activity.

- Obtain the license from the One Voice Operations Center License pool:

This option replaces the need for a file license. The CloudBond system retrieves its license from a license pool in the One Voice Operations Center. All the license management is done from the One Voice Operations Center.

5.14.1 Configuring the CloudBond 365 and One Voice Operations Center Server Connection

This section describes how to manage the connection settings between the CloudBond devices and the One Voice Operations Center server. If you initially obtained your CloudBond license from the One Voice Operations Center server, you already initially configured most of these settings in Section 4.2.2.

➤ To configure the CloudBond 365 One Voice Operations Center server connection:

1. Open the EMS Settings screen (**System Configuration > EMS Settings**).
2. Configure the following connection settings:
 - IP Address – the IP address of the One Voice Operations Center server
 - Trap Port – Destination port to which to send traps (default value is 162)
 - Keep Alive Port – Destination port to send Keep-alive requests over SNMP (default is 1161)
3. Configure the SNMP user settings:

All the settings of the SNMP protocol must be identical to the settings of the current CloudBond system in the One Voice Operations Center. Note that if you wish to connect the CloudBond 365 devices to the One Voice Operations Center with auto detection, then you must use the default settings shown below in parenthesis:

 - SNMPv2:
 - ◆ Community Read – Access string for SNMP get requests (default 'public')
 - ◆ Community Write – Access string for SNMP set requests (default 'private')
 - SNMPv3:
 - ◆ Security Name – Identify the SNMP user ('OVOCUser')
 - ◆ Authentication Protocol - Protocol type that used to encrypt the Security Name field ('SHA').
 - ◆ Authentication Key – Security Name encryption key. The field is valid only if Authentication Protocol selected ('123456789').
 - ◆ Private Protocol – Protocol type that is used to encrypt the SNMP message ('AES-128').
 - ◆ Private Key – SNMP message encryption key. The field is valid only if Private Protocol selected ('123456789').
4. If you would like the One Voice Operations Center to monitor the SBC in your CloudBond system, select the **SBC** button.

When you choose this option, the SBC in the CloudBond system is monitored in the One Voice Operations Center as part of the CloudBond system. SBC alarms will be displayed in the One Voice Operations Center as part of the CloudBond system.
5. Configure the System Info settings:
 - **System Name** – The name of the system. In an environment with multiple CloudBond devices, this value must be unique.
 - **Location** – Optional field to describe the system location.
6. Enter the Login URL – the URL of the CloudBond Admin login page. When you enter this URL, you can access the CloudBond Management login page from the One Voice Operations Center. The link from the One Voice Operations Center is valid only when the Admin user has HTTP/S access to the CloudBond Management Admin.

Figure 5-28: EMS Settings-SNMPv2

The screenshot displays the AudioCodes CloudBond 365 Enterprise Box Edition web interface. The top navigation bar includes links for HOME, USER MANAGEMENT, SYSTEM CONFIGURATION (active), IP PHONES, and ABOUT. The user is logged in as cloudbond3Administrator. The left sidebar shows the SYSTEM CONFIGURATION menu with options like System Configuration, Grouping IDs, Call Pickup Groups, Office 365 Configuration, Office365 Unified Messaging & CloudPEXPolicies, Music on Hold, User Authorization, and Licensing Info. The EMS Settings page is active, showing the following configuration fields:

- Connection:** IP Address * (10.21.8.30), Trap Port * (162), Keep Alive Port * (1161).
- SNMP:** SNMPv2 (selected), SNMPv3 (radio button), Community Read * (public), Community Write * (private).
- Managed Components:** SEC (checkbox).
- System Info Settings:** System Name * (SO 30NEW), Location (new_location).
- Access Settings:** Login URL (empty field).

Buttons for Apply Changes and Reset Changes are located at the bottom right.

Figure 5-29: EMS Settings-SNMPv3

The screenshot displays the AudioCodes CloudBond 365 Enterprise Box Edition web interface. The top navigation bar includes links for HOME, USER MANAGEMENT, SYSTEM CONFIGURATION (active), IP PHONES, and ABOUT. The user is logged in as cloudbond3Administrator. The left sidebar shows the SYSTEM CONFIGURATION menu with options like System Configuration, Grouping IDs, Call Pickup Groups, Office 365 Configuration, Office365 Unified Messaging & CloudPEXPolicies, Music on Hold, User Authorization, and Licensing Info. The EMS Settings page is active, showing the following configuration fields:

- Connection:** IP Address * (10.21.8.30), Trap Port * (162), Keep Alive Port * (1161).
- SNMP:** SNMPv2 (radio button), SNMPv3 (selected), Security Name * (empty field), Authentication Protocol (None), Authentication Key * (empty field), Private Protocol (None), Private Key * (empty field).
- Managed Components:** SEC (checkbox).
- System Info Settings:** System Name * (SO 30NEW), Location (new_location).
- Access Settings:** Login URL (empty field).

Buttons for Apply Changes and Reset Changes are located at the bottom right.

This page is intentionally left blank.

6 IP Phones

The UMP 365 contains several IP Phones Configuration pages which allows the system administrator to monitor and manage AudioCodes Skype for Business IP Phones. The IP Phone manager is very useful for managing IP Phones and as well as diagnosing any faults.

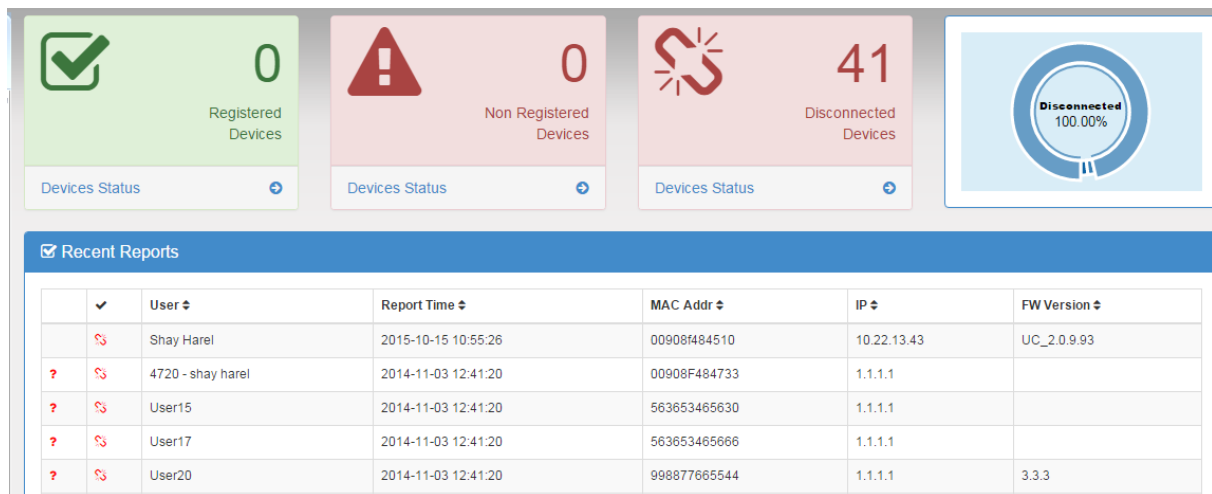
6.1 Dashboard

The Dashboard page lets you quickly identify the following:

- Which phones in the network are registered
- Which phones in the network are non-registered
- The number of registered and non-registered phones (in terms of SIP registration)
- The percentage of registered phones
- The MAC and IP address of each phone
- The time the information was reported
- The firmware version

See Introduction to the IP Phone Manager Admin on page 149 for more information.

Figure 6-1: IP Phones Dashboard

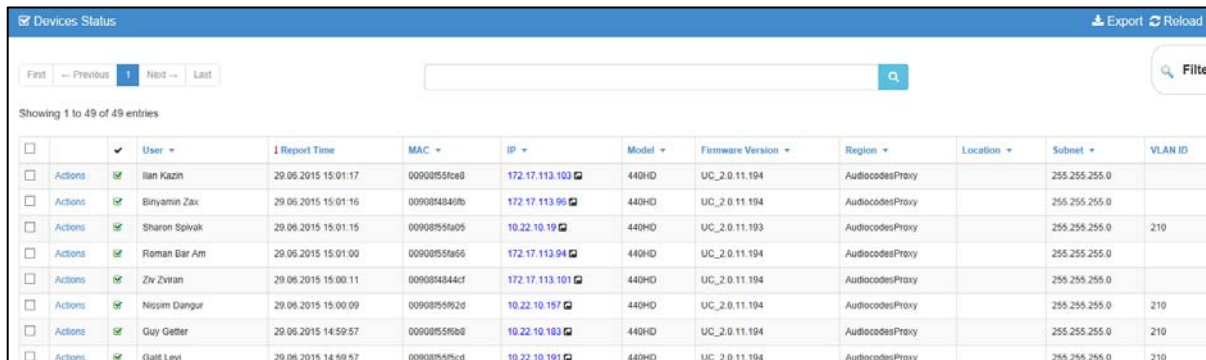


6.2 Status

The Devices Status page lets you check a phone's status.

Refer to the Introduction to the IP Phone Manager Admin on page 149 for more information.

Figure 6-2: IP Phones Status



	✓ User	Report Time	MAC	IP	Model	Firmware Version	Region	Location	Subnet	VLAN ID
Actions	Ilan Kazin	29.06.2015 15:01:17	0090855fca08	172.17.113.103	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Binyamin Zax	29.06.2015 15:01:16	0090855fca0b	172.17.113.90	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Sharon Spivak	29.06.2015 15:01:15	0090855fca05	10.22.10.19	440HD	UC_2.0.11.193	AudiocodesProxy		255.255.255.0	210
Actions	Roman Bar Am	29.06.2015 15:01:00	0090855fca06	172.17.113.94	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Ziv Zivran	29.06.2015 15:00:11	0090855fca0c	172.17.113.101	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Nissim Dangur	29.06.2015 15:00:09	0090855fca0d	10.22.10.157	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210
Actions	Guy Geter	29.06.2015 14:59:57	0090855fca0e	10.22.10.103	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210
Actions	Gali Levi	29.06.2015 14:59:57	0090855fca0f	10.22.10.191	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210

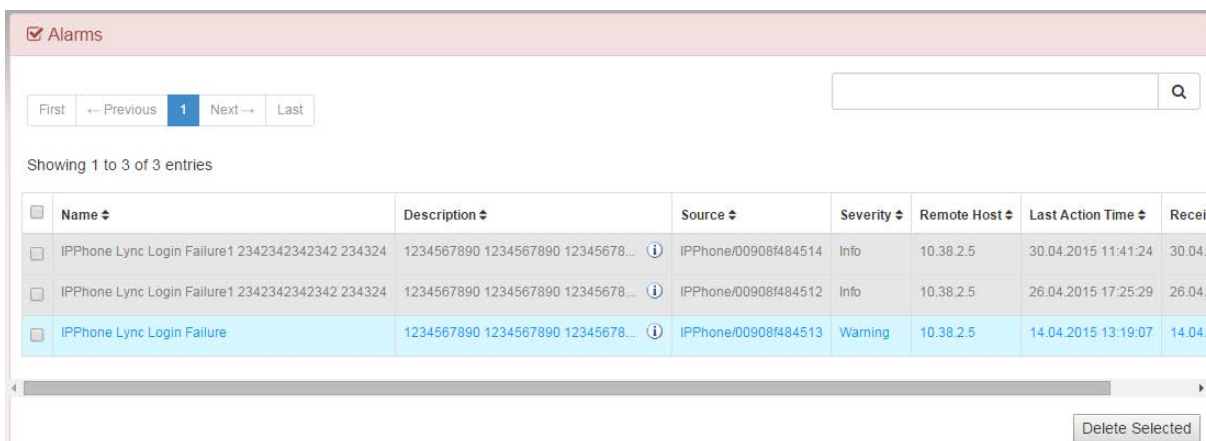
6.3 Alarms

The Alarms page displays the following information:

- Each phone alarm in the network
- A description of each alarm
- The MAC address of the phone (source)
- The alarm severity
- The IP address of the phone
- The last action time
- The date and time of receipt of the alarm

Refer to the Introduction to the IP Phone Manager Admin on page 149 for more information.

Figure 6-3: IP Phones Alarms



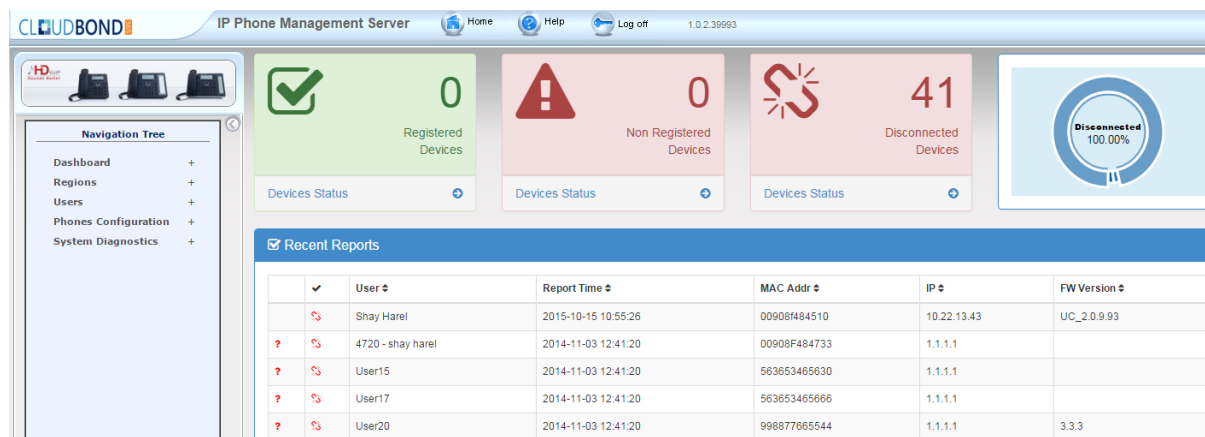
Name	Description	Source	Severity	Remote Host	Last Action Time	Received
IPPhone Lync Login Failure1 2342342342342 234324	1234567890 1234567890 12345678...	IPPhone/00908f484514	Info	10.38.2.5	30.04.2015 11:41:24	30.04.2015
IPPhone Lync Login Failure1 2342342342342 234324	1234567890 1234567890 12345678...	IPPhone/00908f484512	Info	10.38.2.5	26.04.2015 17:25:29	26.04.2015
IPPhone Lync Login Failure	1234567890 1234567890 12345678...	IPPhone/00908f484513	Warning	10.38.2.5	14.04.2015 13:19:07	14.04.2015

6.4 IP Phone Management Server

The IPP Manger opens in a new browser tab the entire IPP Manger admin with all advances features and capabilities.

Refer to the Introduction to the IP Phone Manager Admin on page 149 for more information.

Figure 6-4: IP Phones Manager

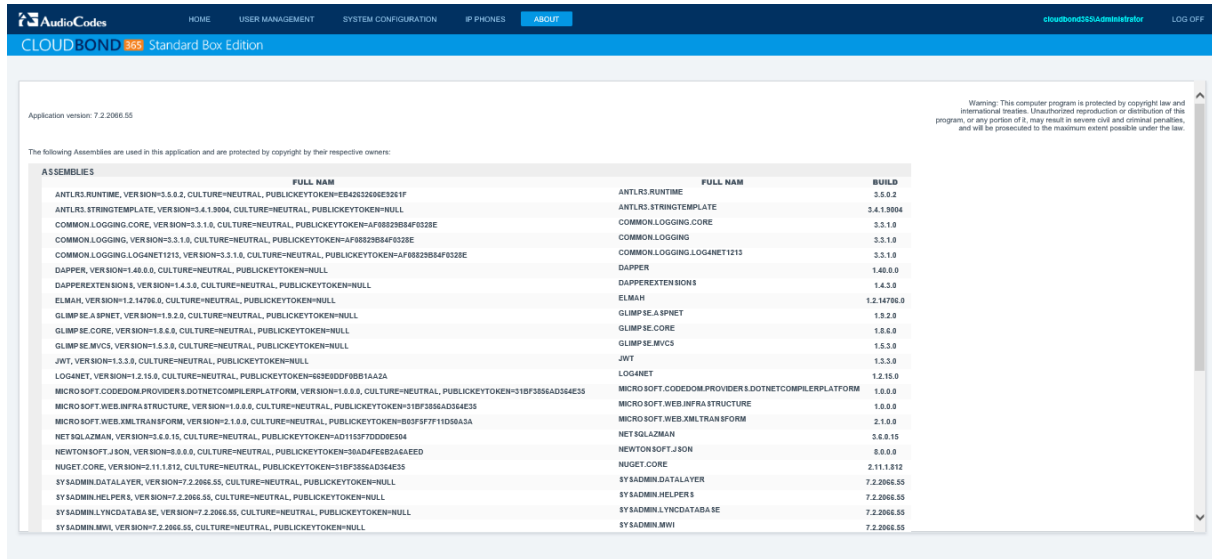


This page is intentionally left blank.

7 About

The UMP 365 About page supplies debug information about various UMP 365 / CloudBond 365 components and their build numbers.

Figure 7-1: About Page



The screenshot shows the 'About' page of the CloudBond 365 Standard Box Edition. The page header includes the AudioCodes logo and navigation links: HOME, USER MANAGEMENT, SYSTEM CONFIGURATION, IP PHONES, and ABOUT (highlighted). The user is logged in as 'cloudbond365Administrator' with a 'LOG OFF' link.

The main content area displays the application version: 7.2.2066.55. Below this, it states: 'The following Assemblies are used in this application and are protected by copyright by their respective owners:'.

A table lists the assemblies used in the application, organized into two columns. Each row includes the assembly name, its version, culture, and public key token.

ASSEMBLIES	FULL NAME	FULL NAME	BUILD
ANTLR3.RUNTIME	VER BION=3.5.0.2, CULTURE=NEUTRAL, PUBLICKEYTOKEN=ED4262260E3261F	ANTLR3.RUNTIME	3.5.0.2
ANTLR3.STRINGTEMPLATE	VER BION=3.4.1.3904, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	ANTLR3.STRINGTEMPLATE	3.4.1.3904
COMMON.LOGGING.CORE	VER BION=3.3.1.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=AF68229B84F6328E	COMMON.LOGGING.CORE	3.3.1.0
COMMON.LOGGING	VER BION=3.3.1.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=AF68229B84F6328E	COMMON.LOGGING	3.3.1.0
COMMON.LOGGING.LOG4NET1213	VER BION=3.3.1.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=AF68229B84F6328E	COMMON.LOGGING.LOG4NET1213	3.3.1.0
DAPPER	VER BION=1.48.0.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	DAPPER	1.48.0.0
DAPPER.EXTENSION1	VER BION=1.4.3.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	DAPPER.EXTENSION1	1.4.3.0
ELMAH	VER BION=1.2.14796.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	ELMAH	1.2.14796.0
GLIMPSE.ASPNET	VER BION=1.9.2.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	GLIMPSE.ASPNET	1.9.2.0
GLIMPSE.CORE	VER BION=1.8.6.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	GLIMPSE.CORE	1.8.6.0
GLIMPSE.MVC5	VER BION=1.5.3.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	GLIMPSE.MVC5	1.5.3.0
JWT	VER BION=1.5.3.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	JWT	1.5.3.0
LOG4NET	VER BION=1.2.15.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=663E9D0F8B61AA3A	LOG4NET	1.2.15.0
MICROSOFT.CODEDOM.PROVIDERS.DOTNET.COMPILEPLATFORM	VER BION=1.0.0.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=31BF3856AD364E35	MICROSOFT.CODEDOM.PROVIDERS.DOTNET.COMPILEPLATFORM	1.0.0.0
MICROSOFT.WEB-INFRASTRUCTURE	VER BION=1.0.0.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=31BF3856AD364E35	MICROSOFT.WEB-INFRASTRUCTURE	1.0.0.0
MICROSOFT.WEB.XMLTRANSFORM	VER BION=2.1.0.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=803F9F7F11D58A3A	MICROSOFT.WEB.XMLTRANSFORM	2.1.0.0
NET.SQLEZMAN	VER BION=3.6.0.15, CULTURE=NEUTRAL, PUBLICKEYTOKEN=AD1153F7DD0E594	NET.SQLEZMAN	3.6.0.15
NEWTONSOFT.JSON	VER BION=8.0.0.0, CULTURE=NEUTRAL, PUBLICKEYTOKEN=36ADAF6E826AEE0	NEWTONSOFT.JSON	8.0.0.0
NUGET.CORE	VER BION=2.11.1.812, CULTURE=NEUTRAL, PUBLICKEYTOKEN=31BF3856AD364E35	NUGET.CORE	2.11.1.812
SYSDADMIN.DATALAYER	VER BION=7.2.2066.55, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	SYSDADMIN.DATALAYER	7.2.2066.55
SYSDADMIN.HELPERS	VER BION=7.2.2066.55, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	SYSDADMIN.HELPERS	7.2.2066.55
SYSDADMINLYNC.DATABASE	VER BION=7.2.2066.55, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	SYSDADMINLYNC.DATABASE	7.2.2066.55
SYSDADMIN.MWI	VER BION=7.2.2066.55, CULTURE=NEUTRAL, PUBLICKEYTOKEN=NULL	SYSDADMIN.MWI	7.2.2066.55



Note: When placing a support call, you must supply the Application Version number of your system. e.g., CloudBond 365 v5.5.1626.585.

This page is intentionally left blank.

8 Scheduled Tasks

The User Management Pack 365 application creates six scheduled tasks that can be managed using the Windows “Task Scheduler” application. This chapter explains the purpose of these scheduled tasks.



Note: The scheduled tasks are disabled by default and should be enabled and started according to the customer needs. The configured task triggers can be used as a recommended guideline for smaller implementations only. Larger implementations usually take more time, where it is advised to only run the tasks once a day in the order described in this chapter. Each task should only be commenced after the previous task has been completed.

Figure 8-1: Scheduled Tasks

Name	Status	Triggers
AcsGroupReplication	Ready	At 12:15 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.
AcsLogCleanup	Ready	
AcsMoveUsers	Ready	At 12:45 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.
AcsO365Sync	Ready	At 10:00 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.
AcsPolicyReplication	Ready	At 12:45 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.
AcsUserReplication	Ready	At 12:30 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.

8.1 Step 1: AcsLogCleanup

AcsLogCleanup is a scheduled task that removes log files in the c:\acs\logs folder that are older than 14 days.

8.2 Step 2: AcsGroupReplication

AcsGroupReplication is part of the Lifecycle Management feature and takes care of the automatic creation and removal of user objects in the local Active Directory resource forest.

8.3 Step 3: AcsO365Sync

AcsO365Sync should only be enabled in hybrid (Split-Domain) deployments with Office365. This scheduled task reads all Office 365 Skype enabled user objects and creates corresponding identities for them in the resource forest where the UMP is installed.

8.4 Step 4: AcsPolicyReplication

AcsPolicyReplication is part of the Lifecycle management feature and takes care of the policy assignment defined in the group replication templates. If enabled, it will undo all manual changes on an account and restore the settings to what is defined in the template.

8.5 Step 5: AcsUserReplication

AcsUserReplication is part of the AD Connector and takes care of user attribute replication between all connected user forests and the resource forest where the User Management Pack 365 is installed. It replicates the following user attributes from the customer user forest(s) to the UMP resource forest:

- c (countrycode like NL for Netherlands)

- co (country in full like Netherlands)
- company
- countryCode
- department
- description
- displayName
- facsimileTelephoneNumber
- givenName (first name)
- homePhone
- initials
- ipPhone
- l (city)
- mail
- manager
- mobile
- pager
- physicalDeliveryOfficeName
- proxyAddresses (only the EUM and SMTP entries)
- sAMAccountName
- sn (Last Name)
- st (State)
- telephoneNumber
- title
- thumbnailPhoto
- userPrincipalName

If write permissions in the customer user forest(s) are given to the service account that is used to run the scheduled task named AcsUserReplication, the following attributes will be synchronized back from the UMP resource forest towards the customer user forest(s):

- msRTCSIPUserEnabled
- msRTCSIPOptionFlags
- msRTCSIPDeploymentLocator
- msRTCSIPLine
- msRTCSIPPrimaryUserAddress
- proxyAddresses (only the sip entry)



Note: The msRTCSIP attributes are only required in Office365 Hybrid deployments, where DirSync or AzureADSync are used for account synchronization from the user forest to Office 365. With the release of Microsoft's AzureADConnect in October 2015, the resource forest model is fully supported and if configured correctly, there is no longer the need to populate the msRTCSIP attributes.

8.6 Step 6: AcsMoveUsers

When a user's registrarpool is changed in the User Management Pack 365, the move to the destination pool is cached. The scheduled task 'AcsMoveUsers' takes care of the actual user move between the pools for moves both between two pools on premises or between Office365 and on premises in a hybrid deployment.

This page is intentionally left blank.

Part II

Changing Administrator Password

9 Introduction

This part describes the procedures for changing the AudioCodes CloudBond 365 Administrator password. If you decide to change this password, keep in mind that this account is also used as a service account in the background. Therefore, if you change this password, you must also change the password in the following locations:

- Domain Controller
- Internet Information Services (IIS) Manager
- Domain Controller Windows Services
- Front End Windows Services
- Edge Windows Services
- Branch Pool Appliance (BPA)

This page is intentionally left blank.

10 Changing Password on Domain Controller

The procedure below describes how to change the AudioCodes CloudBond 365 Administrator password on the Domain Controller for the following:

- CloudBond 365 Standard/Standard+ Box Edition
- CloudBond 365 Pro and Enterprise Box Editions

10.1 CloudBond 365 Standard/Standard+ Box Edition

For CloudBond 365 Standard/Standard+ Box Edition installed on the AudioCodes Mediant 800 server, the domain controller resides on the **Host server**. The password change applies to the host server and the domain controller's Administrator's account.

➤ **To change the CloudBond 365 Standard/Standard+ Box Edition Administrator password on the domain controller:**

1. Press Ctrl-Alt-Delete.
2. Select the **Change a password...**option.
3. In the appropriate fields, enter the following:
 - Old Password
 - New Password
 - Confirm Password
4. Press **Enter**.

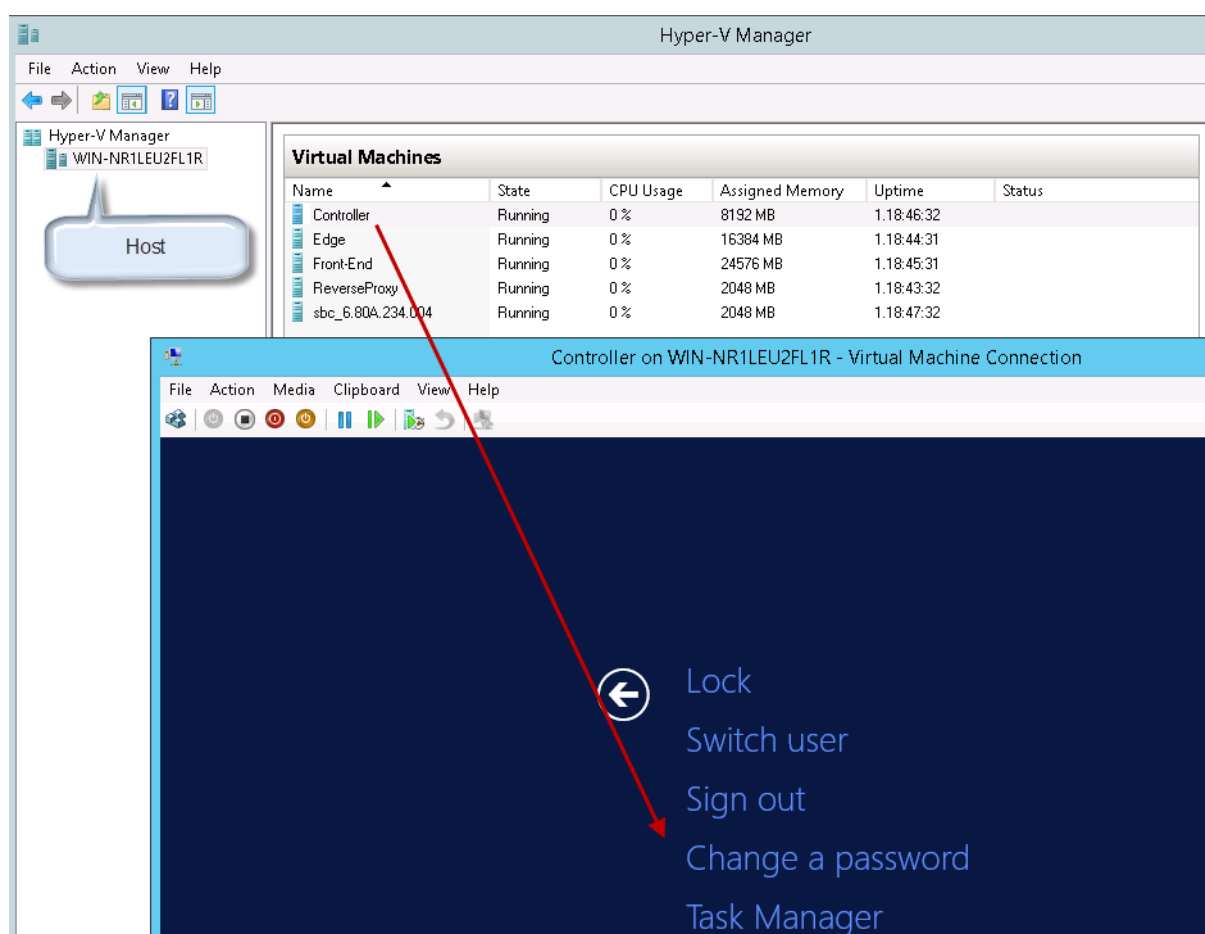
10.2 CloudBond 365 Pro and Enterprise Box Editions

For CloudBond 365 Pro and Enterprise Box Editions installed on HP servers, the domain controller is configured as a separate virtual server. The domain Administrator's password should therefore be changed on the domain controller's virtual server first.

➤ **To change the CloudBond 365 Pro and Enterprise Box Editions Administrator password on the Domain Controller:**

1. Open Hyper-V Manager.
2. Select the domain controller.

Figure 10-1: Changing Password on Domain Controller - Pro and Enterprise Box Editions



3. Press Ctrl-Alt-Delete
4. Select the **Change a password** option.
5. In the appropriate fields, enter the following:
 - Old Password
 - New Password
 - Confirm Password
6. Press **Enter**.

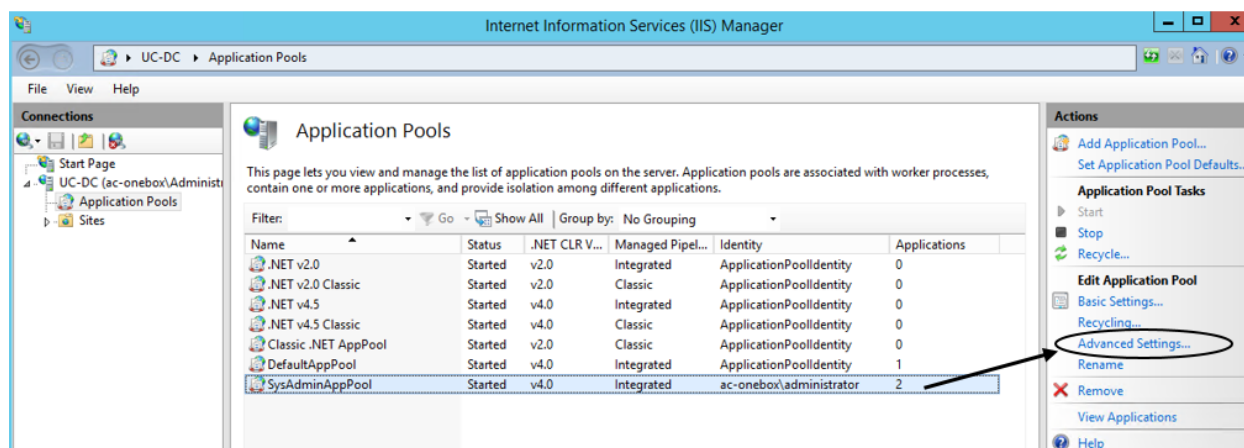
11 Changing Password on IIS Manager

The procedure below describes how to change the CloudBond 365 Administrator password on the Internet Information Services (IIS) Manager.

➤ **To change CloudBond 365 Administrator password on the IIS Manager:**

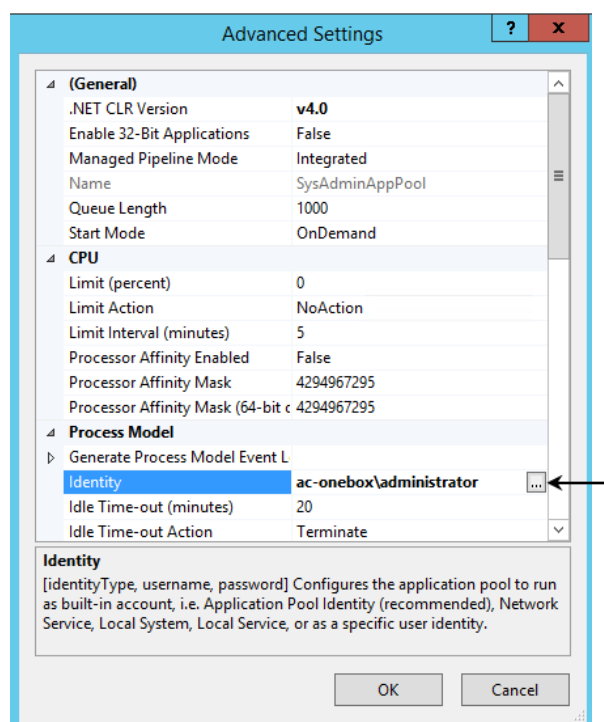
1. On the CloudBond 365 domain controller, open the IIS management console (%windir%\system32\inetmgr\inetmgr.exe)
2. Under the Server node, select **Application Pools**; the following page appears:

Figure 11-1: Changing Password on IIS Manager



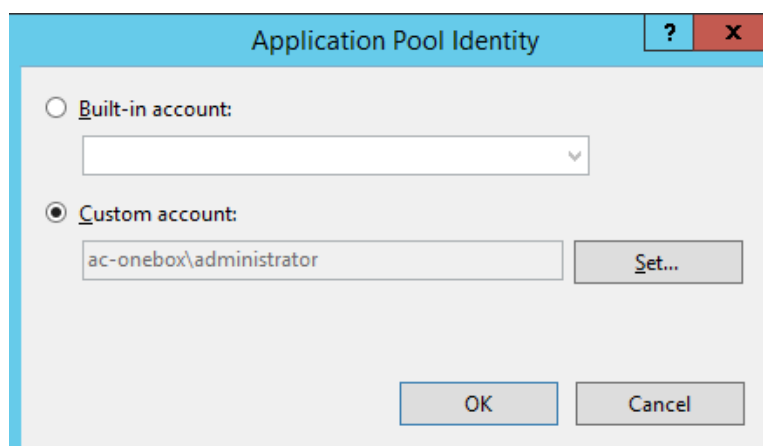
3. Select **SysAdminAppPool**.
4. In the 'Actions' pane, click **Advanced Settings**; the following page appears:

Figure 11-2: Advanced Settings



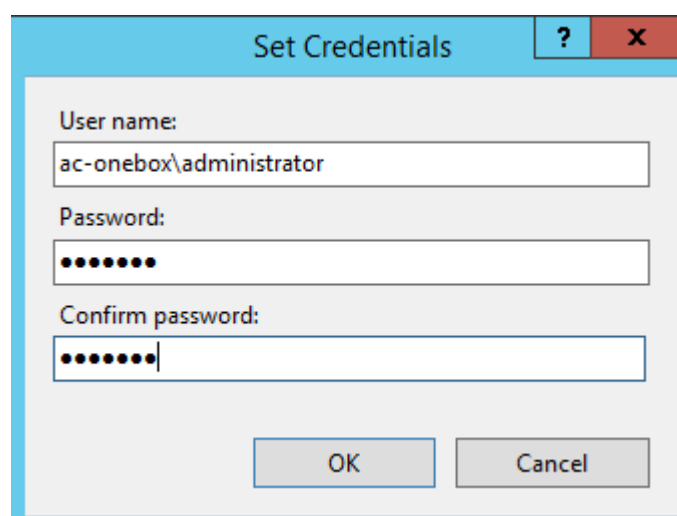
5. Click the **Browse** button (...) corresponding to the 'Identity' account; the following screen appears:

Figure 11-3: Application Pool Identity



6. Click the **Custom account** option and then click **Set....**'; the following screen appears:

Figure 11-4: Set Credentials



7. In the 'User name' field, enter the account in **<domain>\administrator** format.
8. Enter the new password in the 'Password' and 'Confirm password' fields, and then click **OK**.
9. Click **OK** on the previously opened screens (Application Pool Identity and Advanced Settings).

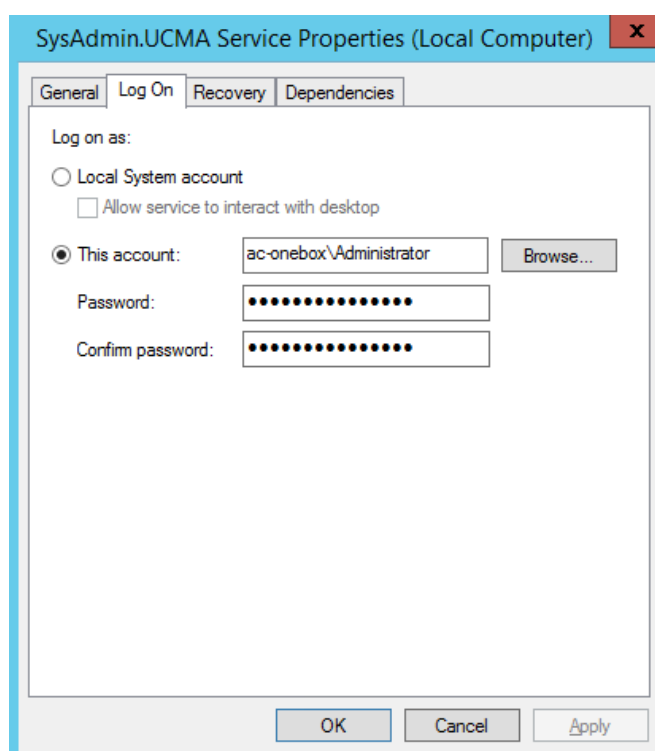
12 Changing Password on Domain Controller Windows Services

The procedure below describes how to change the AudioCodes CloudBond 365 Administrator password in Domain Controller Windows Services.

➤ **To change the CloudBond Administrator password on Domain Controller Windows Services:**

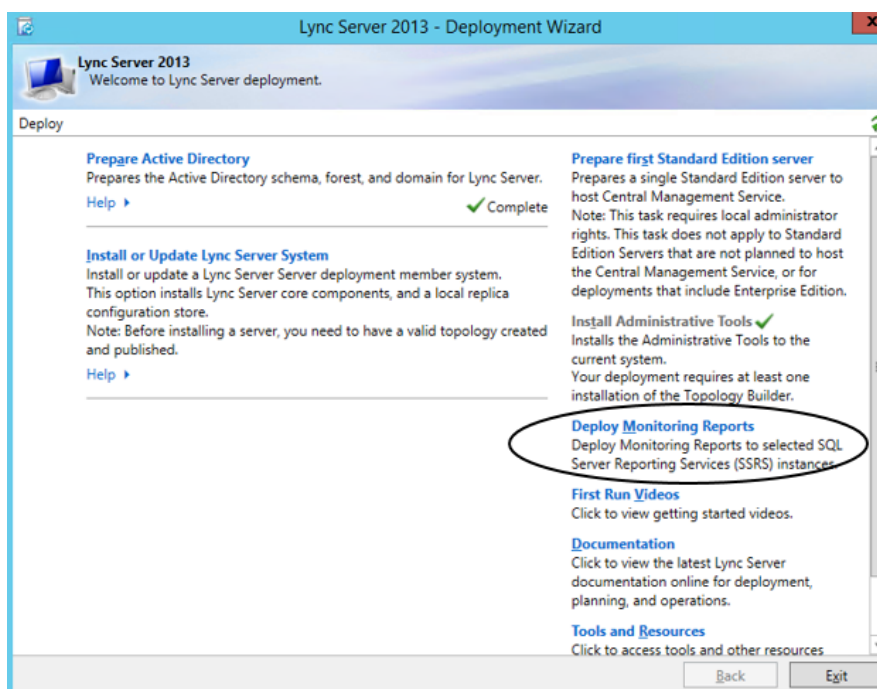
1. In the CloudBond Domain Controller, open the Services Management console.
2. Change the password in the following services:
 - SQL Server (MSSQLSERVER)
 - SQL Server Agent (MSSQLSERVER)
 - SQL Server Reporting Services (MSSQLSERVER)
 - SysAdmin.UCMA Service

Figure 12-1: SysAdmin.UCMA Service



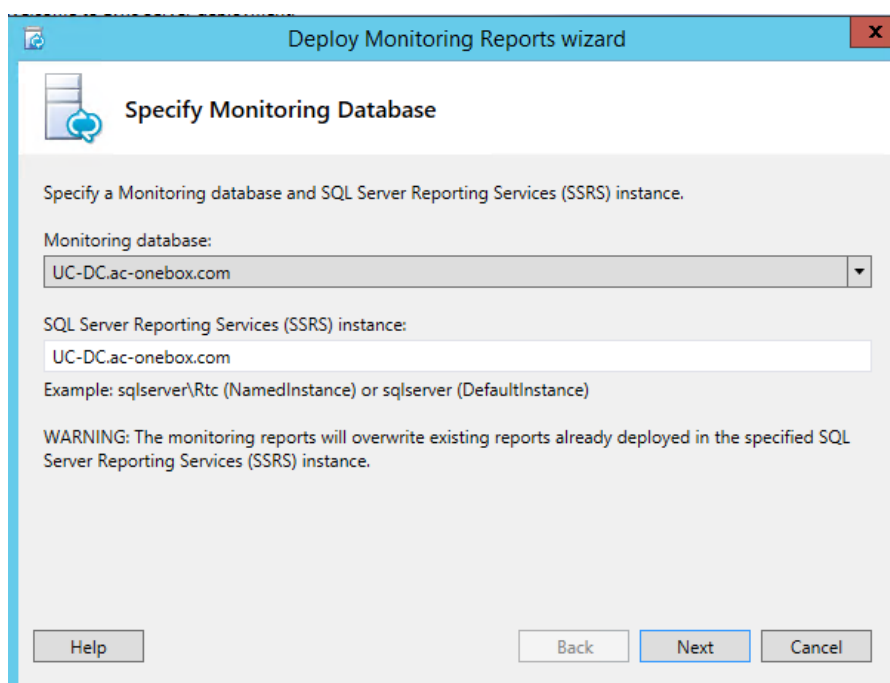
3. Run the 'Lync Server Deployment Wizard'.

Figure 12-2: Lync Server Deployment Wizard



- a. From the Welcome to Lync Server deployment page, click **Deploy Monitoring Reports**; the following screen appears:

Figure 12-3: Deploy Monitoring Reports Wizard



- b. Click **Next**; the following screen appears:

Figure 12-4: Specify Credentials

The screenshot shows a Windows wizard window titled "Deploy Monitoring Reports wizard". The current step is "Specify Credentials". The instructions state: "Specify the credentials to be used by SQL Server Reporting Services (SSRS) to access the Monitoring database." There are two input fields: "User name (domain\user name):" with the text "ac-onebox\Administrator" entered, and "Password:" with masked characters "••••••". At the bottom, there are four buttons: "Help", "Back", "Next" (which is highlighted in blue), and "Cancel".

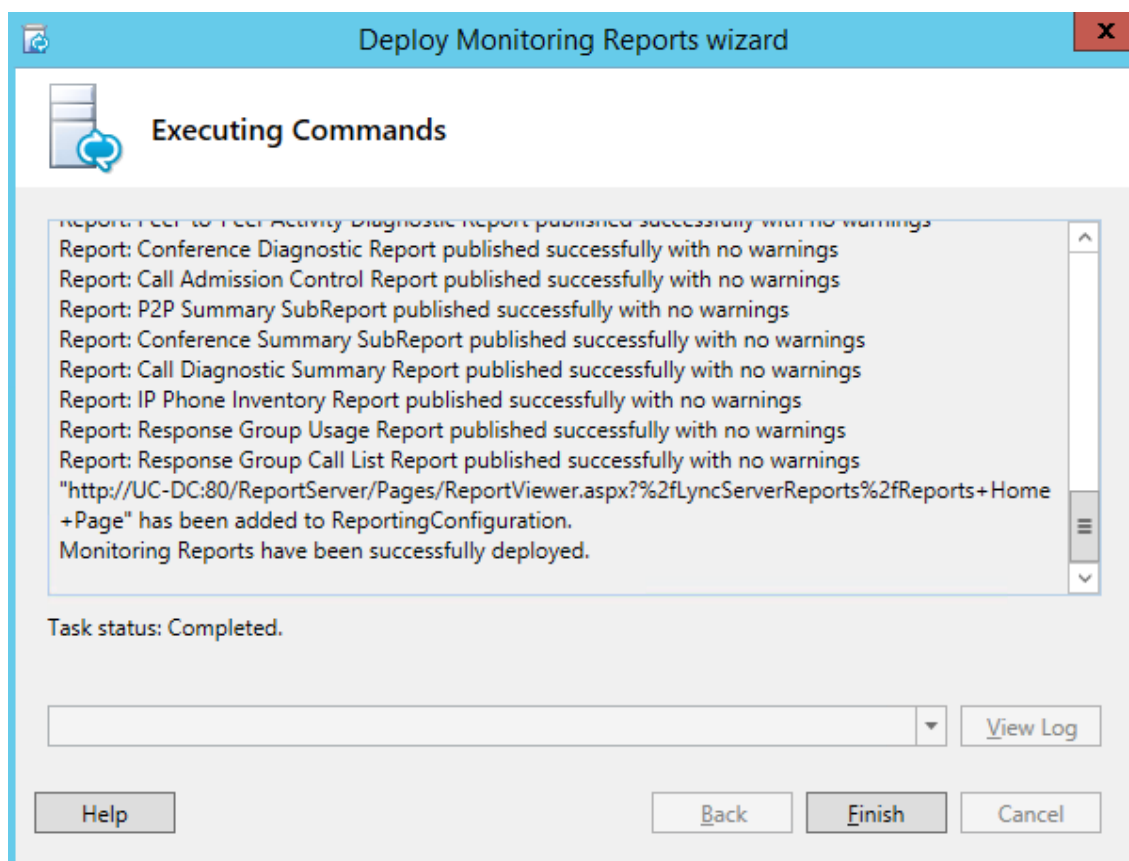
- c. In the 'User name' field, enter the account in **<domain>\administrator** format.
d. In the 'Password' field, enter your password, and then click **Next**; the following screen appears:

Figure 12-5: Specify Read-Only Group

The screenshot shows the next step in the wizard, "Specify Read-Only Group". The instructions state: "Specify a user group that has read-only access to SQL Server Reporting Services (SSRS). Members of this group can access Monitoring Reports on SSRS." There is a single input field labeled "User group:" which is currently empty. Below the field, an example is provided: "Example: contoso\accessgroup or RTCUniversalReadOnlyAdmins". At the bottom, there are four buttons: "Help", "Back", "Next" (highlighted in blue), and "Cancel".

- e. In the 'User group' field, enter a user group that has read-only access to SQL Server Reporting Services (SSRS); and then click **Next**; the following screen appears:

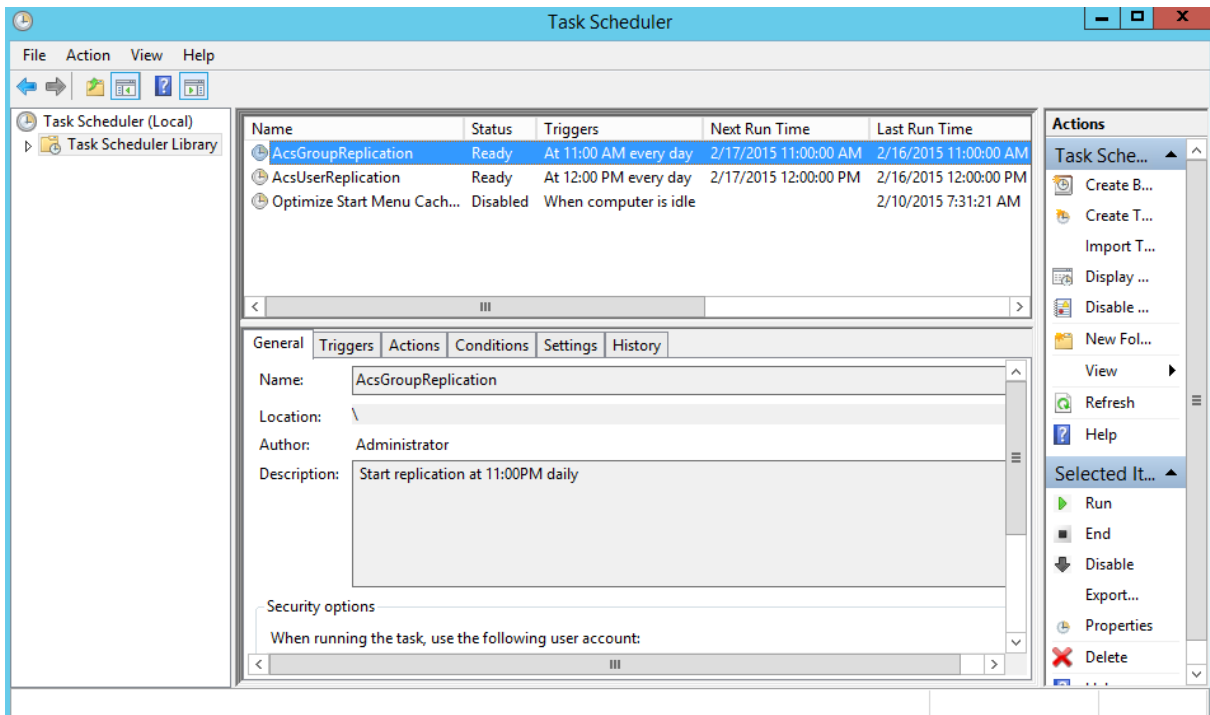
Figure 12-6: Executing Commands



- f. Click **Finish**.

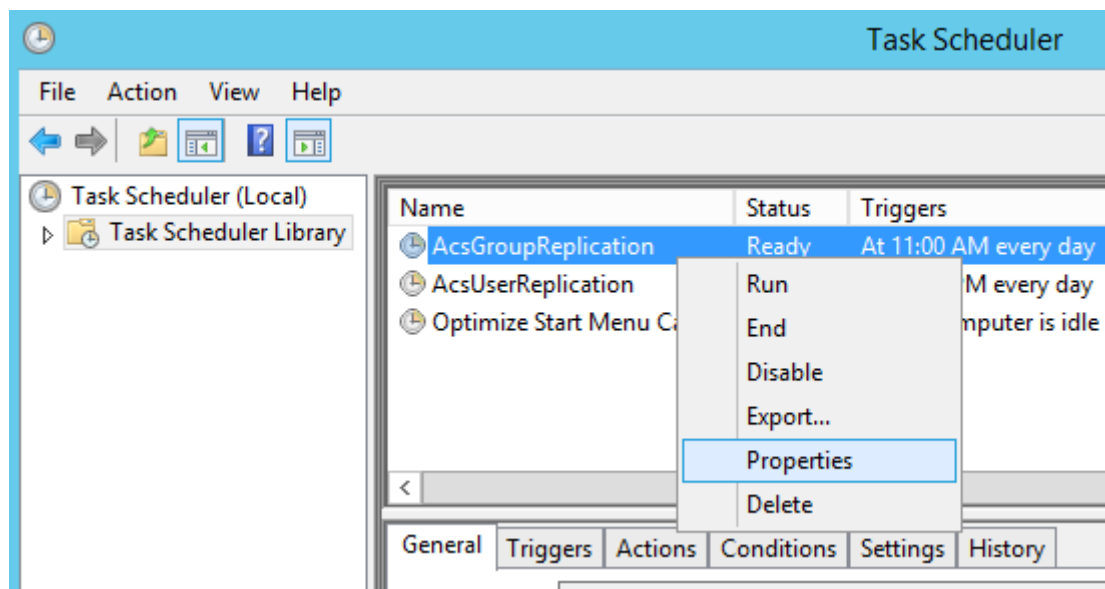
4. Open the **Task Scheduler**; the following screen appears:

Figure 12-7: Task Scheduler



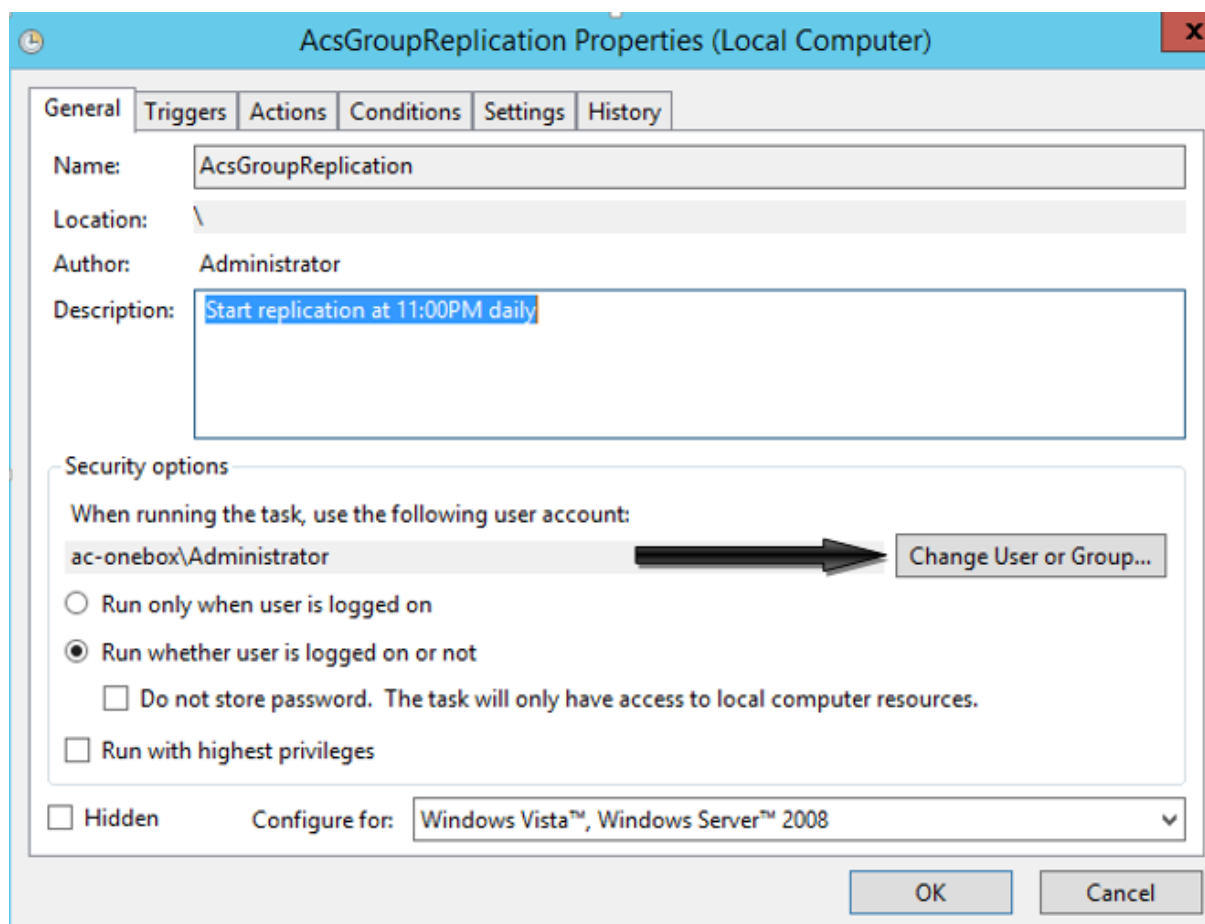
5. Right-click on the **ACSGroupReplication** rule and select **Properties**.

Figure 12-8: ACSGroupReplication Rule - Properties



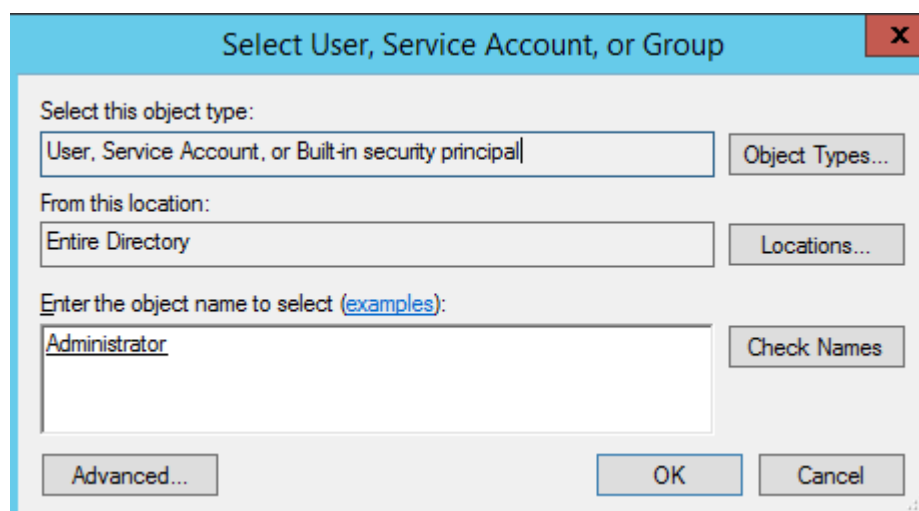
6. Click **Change User or Group**.

Figure 12-9: ACSGroupReplication Properties



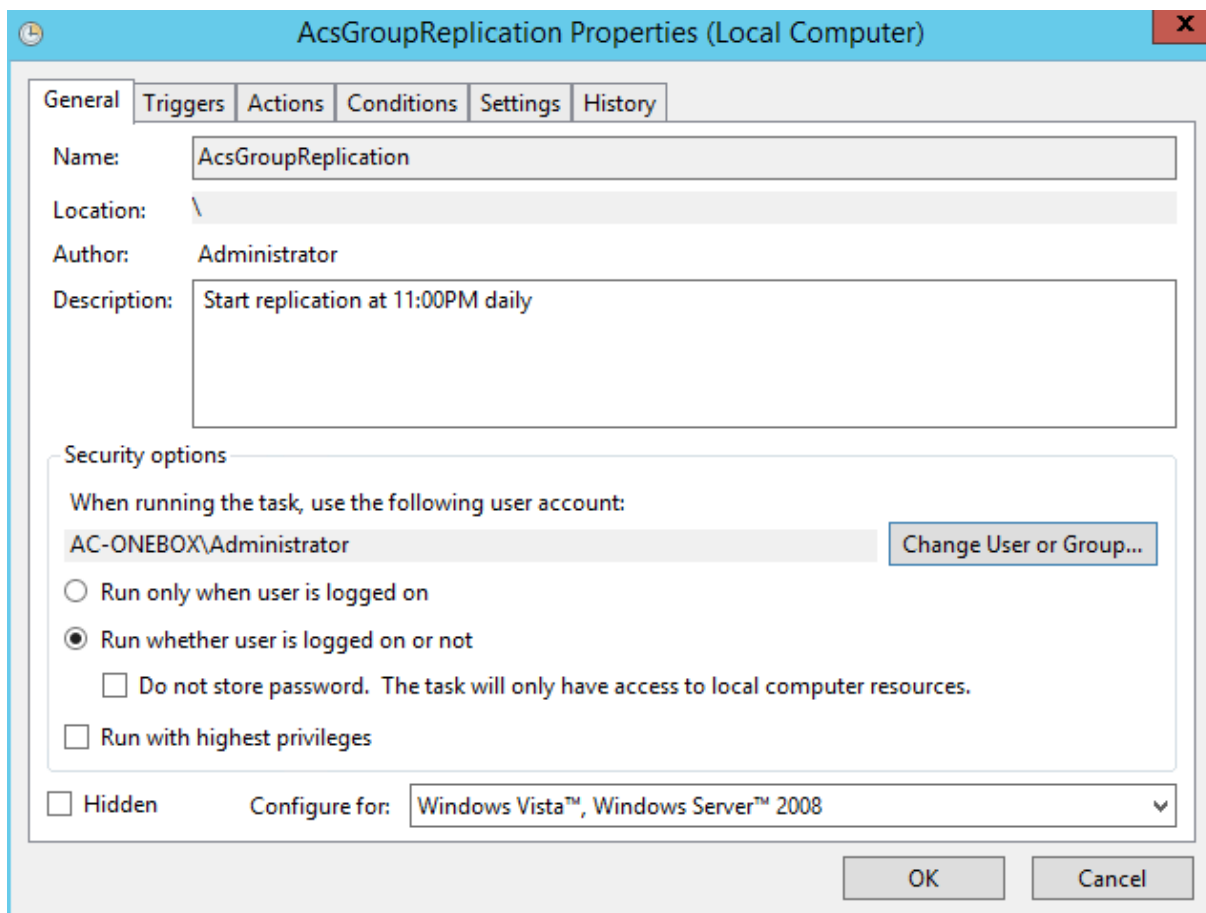
7. In the 'Enter the object name to select' field, enter "Administrator", and then click **Check Names**:

Figure 12-10: Select User, Service Account, or Group



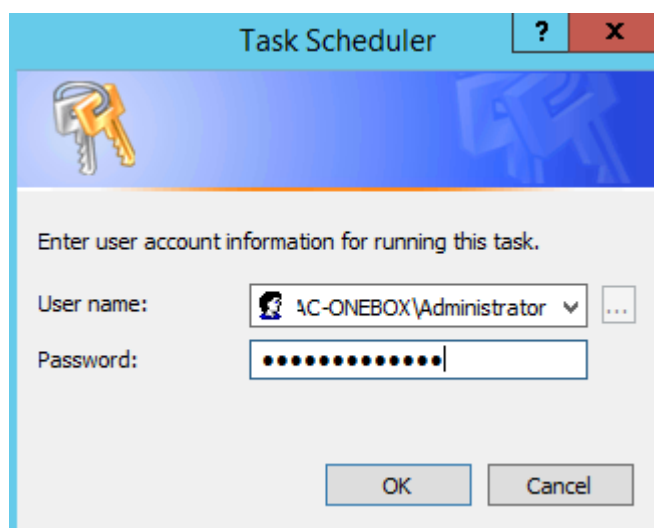
8. Click **OK**; the following screen appears:

Figure 12-11: ACSGroupReplication Properties (Local Computer)



9. Click **OK**.
10. In the 'Password' field, enter the new administrator password, and then click **OK**:

Figure 12-12: Task Scheduler



11. Repeat steps 5 - 10 for the **AcsUserReplication** rule, by first right-clicking on the **AcsUserReplication** rule and selecting **Properties** (see [Figure 12-7: Task Scheduler](#)).

This page is intentionally left blank.

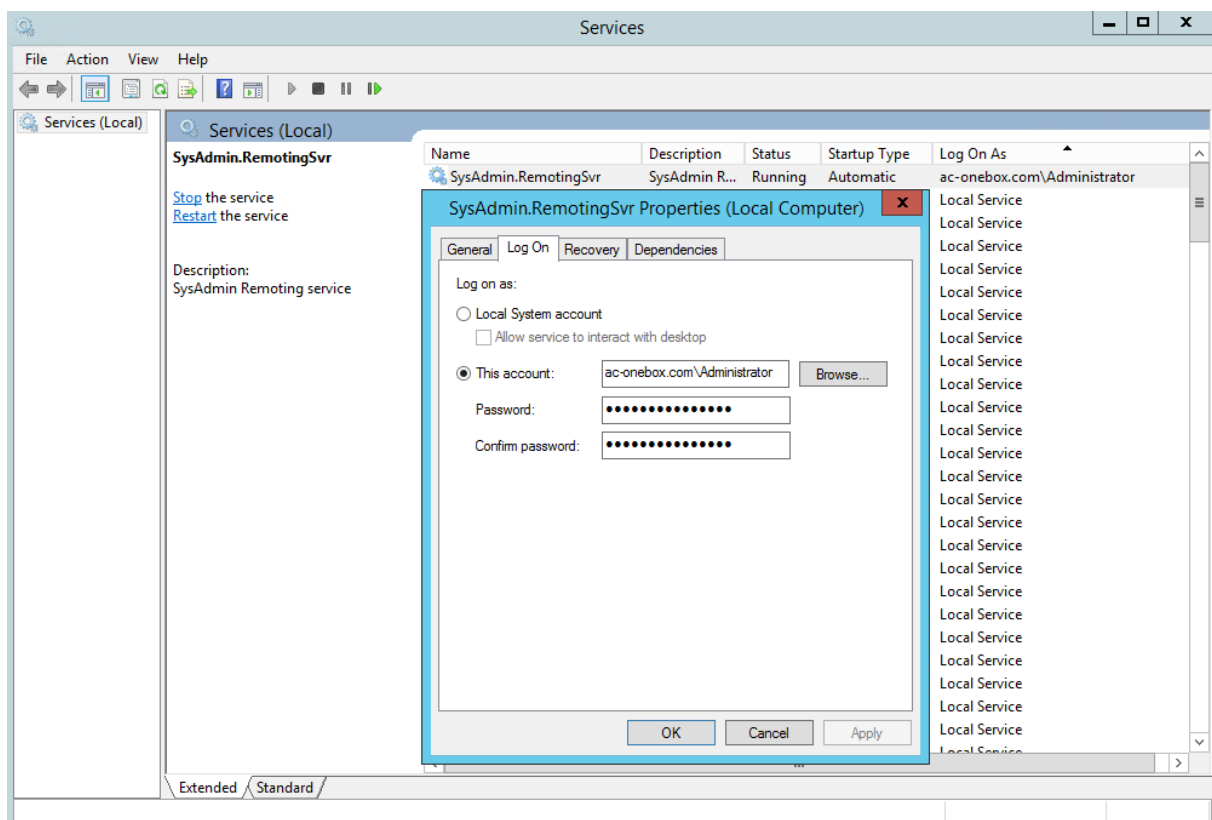
13 Changing Password on Front End

The procedure below describes how to change the AudioCodes CloudBond 365 Administrator password in the Front End Windows Services.

➤ **To change the CloudBond Administrator password in the Front End Windows Services:**

1. From the CloudBond Front End windows services, open the Services Management console.
2. Click **SysAdmin.RemotingSvr**.
3. Click the **Log On** tab.
4. Click the **This account** option.
5. In the 'Password' and 'Confirm password' fields, enter the new password.
6. Click **OK**.

Figure 13-1: SysAdmin.RemotingSrv Properties (Front End)



This page is intentionally left blank.

14 Changing Password on Edge Server

The procedure below describes how to change the AudioCodes CloudBond 365 Administrator password in Edge Windows Services.

Please note that the Edge Administrator account is a local user as the Edge server is not part of the Domain. This means that changing the default password for the Administrator in the domain, does not automatically change the password for the Administrator on the Edge machine. Both administrator accounts can have different passwords.

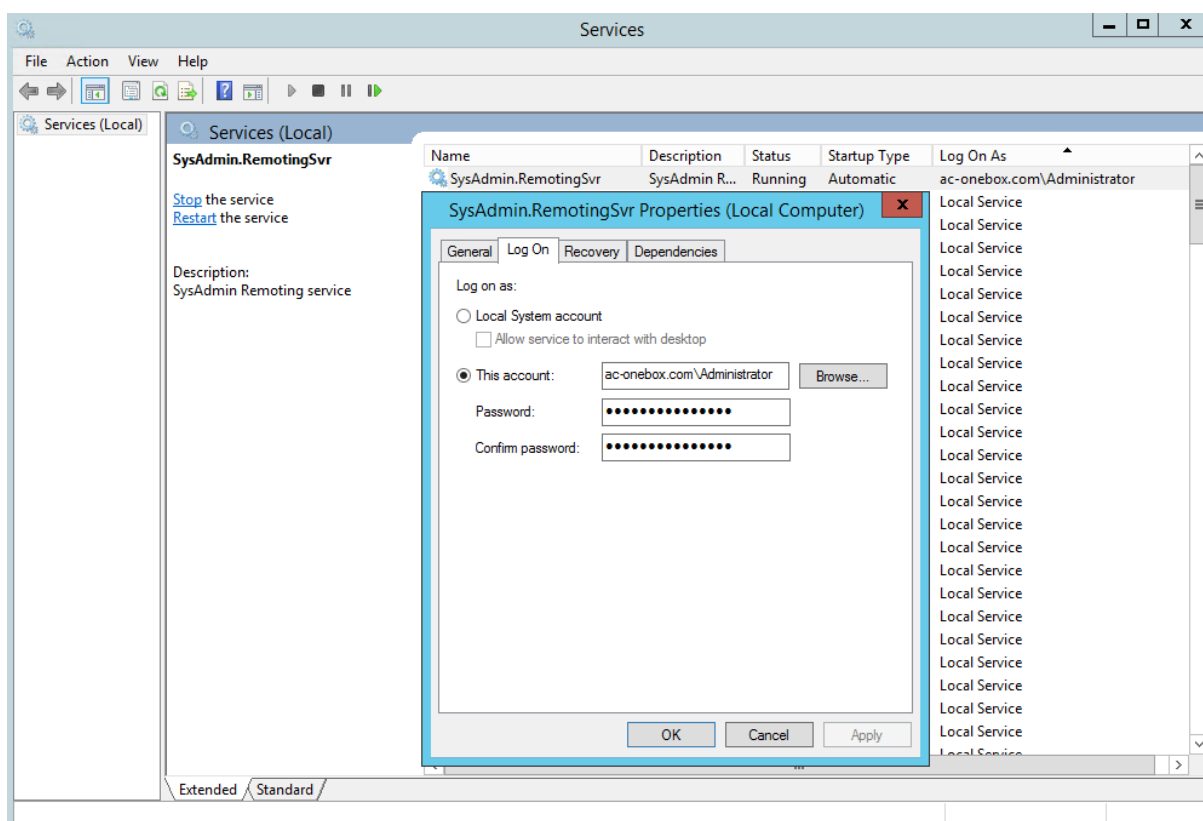
However, if you would like to adapt local administrator's password with the new domain Administrator's password you need to:

Change local administrator's password by pressing CTRL+Alt+Del and then 'Change Password' and then correlate the credentials of Edge Windows services with the new Administrator's password.

➤ **To change the CloudBond Administrator password on the Edge Windows Services:**

1. From the CloudBond Edge Services, open the Services Management Console.
2. Click **SysAdmin.RemotingSvr**.
3. Click the **Log On** tab.
4. Click the **This account** option.
5. In the 'Password' and 'Confirm password' fields, enter the new password.
6. Click **OK**.

Figure 14-1: SysAdmin.RemotingSrv Properties (Edge Windows)



This page is intentionally left blank.

15 Changing Password on BPA

In a CloudBond 365 Branch Pool Appliance (BPA) deployment, there is one primary domain controller and a secondary domain controller. To change the Administrator's password on the primary domain controller, perform the procedures in Sections 10 to 14.

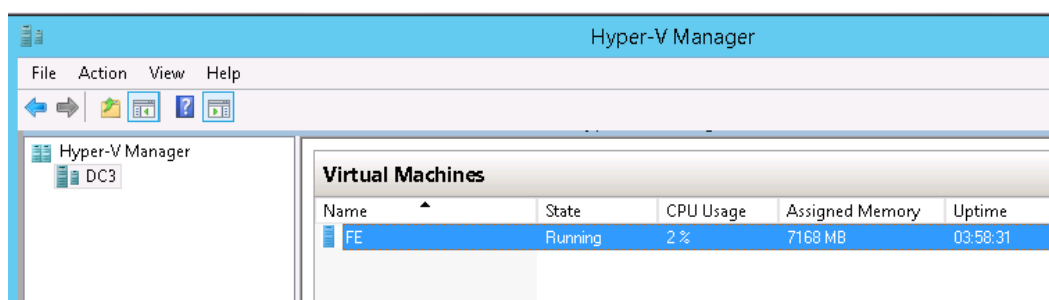
If you need to change the Administrator's password on the paired CloudBond 365 server, perform the procedures in Sections 10 to 14.



Note: Not all components on the secondary CloudBond 365 server are mandatory and therefore do not require a password change.

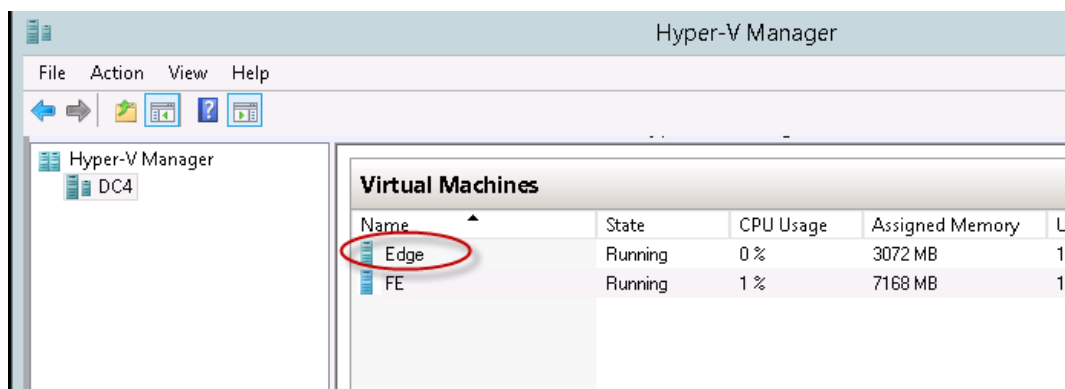
In the following screenshot, the CloudBond server (DC3) server does not have an Edge server:

Figure 15-1: Paired Domain Controllers with No Edge Server



On a paired CloudBond 365 installed on a Mediant 800 server, the Edge server is not mandatory. paired CloudBond 365 may use the Edge server of the primary CloudBond 365 server). In this case, Edge server adjustments described in Section 14 are not relevant.

Figure 15-2: Paired Domain Controllers with an Edge Server



On a paired CloudBond 365 installed on a Mediant 800 server, there is no database and therefore SQL services described in Section 12 - 2 are not relevant.

On a paired CloudBond 365 installed on a Mediant 800 server, there is no database and therefore SQL services described in Section 12 - 3 are not relevant.

This page is intentionally left blank.

16 Changing EMS Agent Password

In case your AudioCodes CloudBond 365 is managed by the One Voice Operations Center you will need to update the password that is used by the EMS Agent.

➤ **To change the EMS Agent password:**

1. Connect to the CloudBond 365 Domain Controller (DC) server
2. Open the command shell from the **Start** menu.
3. Run the command:

```
C:\Program  
Files\Audiocodes\MainAgent\Scripts\change_user_and_password.bat  
<new_username> <new_password>
```

This page is intentionally left blank.

17 Verifying Password Change

When verifying a password change:

- Ensure that you can successfully log in to CloudBond's sysadmin tool.
- Verify that you can successfully create a new user
- Ensure that you can successfully log in to CloudBond's domain controller through Remote Desktop Connection.

For BPA setup, verify that any change you perform on one server is successfully replicated on the secondary server.

This page is intentionally left blank.

Part III

Connecting to Servers

18 Introduction

This part describes various methods of connecting to the server desktops within AudioCodes CloudBond 365™.

This process is necessary to perform some Skype for Business specific tasks, such as Adding or Changing a SIP domain via Skype for Business Topology Builder.

This guide provides information such as:

- How to use the rear KVM ports on AudioCodes CloudBond 365 Standard/Standard+ Box Editions
- How to use the rear KVM ports on AudioCodes CloudBond 365 Pro and Enterprise Editions
- How to access virtual machine desktops via Hyper-V
- How to enable RDP on each server
- How to start an RDC session on your local PC
- How to connect to the AudioCodes CloudBond 365 Controller server
- How to end your RDP session

This page is intentionally left blank.

19 CloudBond 365 Desktop Access

CloudBond 365 will occasionally require access to the Desktop / Console environment of the various components servers (Host, Controller, Front-End, Edge, Reverse Proxy, SBC).

CloudBond 365 provides a Web based management suite (SysAdmin) to reduce the need for such access on a day to day basis. However, there are still times when access to desktop utilities are required. For example:

- Setting time and time zone on each server
- Initial Deployment of CloudBond 365
- Accessing Skype for Business Topology Builder
- Accessing Skype for Business Management Shell
- Accessing Skype for Business Deployment Wizard
- Debugging activities

The above activities are infrequently carried out, and are usually associated with initial installation, or with major configuration changes.

The most common, infrequent, tasks can usually be carried out on the Controller server alone.

The Deployment Wizard must be run on the FE and Edge servers independently. It cannot be run remotely.

The Co-Located Hyper-V / Domain Controller with Virtual Machines install the CloudBond 365 Controller (DC) and Hyper-V within the host machine, with the remaining CloudBond 365 Servers (FE and Edge) as Hyper-V virtual machines.

This option is suitable for CloudBond 365 Standard/Standard+ Editions (e.g., AudioCodes Mediant 800B OSN server).



Note: The SBC is a Linux based server. Hyper-V can be used to view its console, but an RDP connection cannot be established to this server.

This page is intentionally left blank.

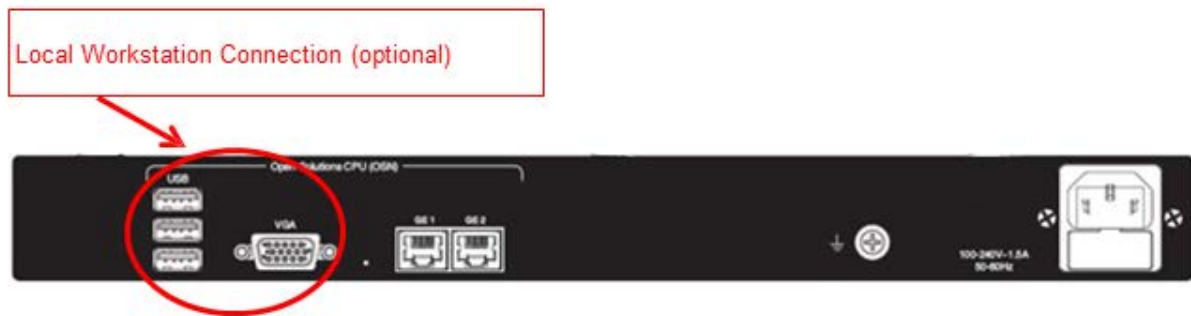
20 Rear KVM Ports

One method of accessing the CloudBond 365 server Desktops is by using the rear KVM (Keyboard, Video, Mouse) ports on the physical CloudBond 365 device. The KVM device may be a specific KVM appliance within a server rack servicing several devices, or it may be a dedicated monitor, keyboard and mouse. Each customer will have different requirements.

Depending upon where the device is located, this may or may not provide convenient access. During initial installation and deployment, it may be more convenient to enable Remote Desktop (RDP) Access, as described in the following chapter. To enable RDP, you will first need to use the rear KVM ports. After enabling RDP, the rear KVM equipment can then be disconnected.

20.1 CloudBond 365 Standard/Standard+ Editions

Figure 20-1: CloudBond 365 Standard/Standard+ Editions Rear View

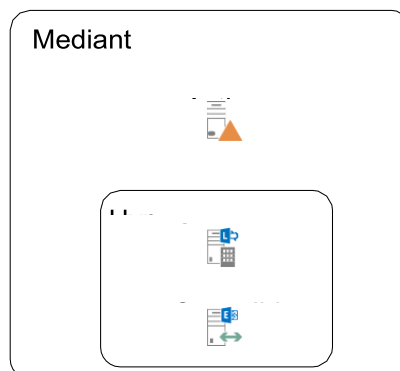


The CloudBond 365 Standard Edition device uses the **Co-located Hyper-V / Domain Controller with Virtual Machines** deployment model. This deployment model installs the CloudBond 365 Controller (DC) and Hyper-V within the host machine, with the remaining CloudBond 365 Servers (FE and Edge) as Hyper-V virtual machines.

This option is suitable for CloudBond 365 Standard Edition (e.g. AudioCodes Mediant 800B OSN server).

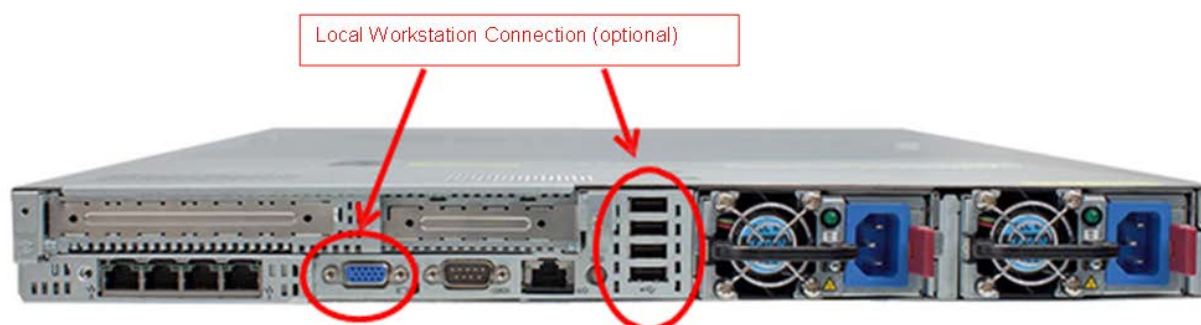
With this Deployment model, the rear KVM ports connect directly to the CloudBond 365 Controller (UC-DC). The controller runs Hyper-V, so Hyper-V manager can be used to provide access to the Front-End (FE) and Edge server desktops.

Figure 20-2: Co-located DC and Hyper-V



20.2 CloudBond 365 Pro-Enterprise Edition

Figure 20-3: Rear View

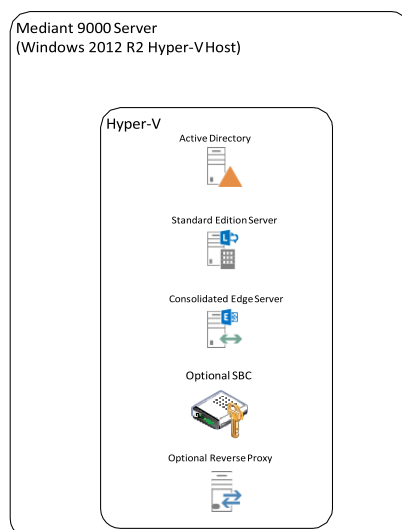


The CloudBond 365 Pro and Enterprise Edition devices will typically use the **Hyper-V Host with Virtual Machines** deployment model. This deployment model installs Hyper-V on the selected host machine, and the three CloudBond 365 Servers (Controller, FE, and Edge) as three separate virtual machines within Hyper-V.

This option is suitable for CloudBond 365 Pro, and CloudBond 365 Enterprise (e.g., AudioCodes HP Servers).

With this deployment model, the rear KVM ports provide access to the Hyper-V host only. To access the CloudBond 365 server Desktops, the Hyper-V Management Utility must be used.

Figure 20-4: Hype-V Host with Virtual Machines



21 Remote Desktop Protocol (RDP)

21.1 What is RDP?

Remote Desktop Protocol is a Microsoft desktop remote control protocol that allows you to connect with the desktop of a remote server or workstation, and operate the desktop as though you were physically present at the remote machine. A similar but independent protocol is also used to allow Desktop connection to Hyper-V guest Virtual Machines on the Host computer.

The client and server components, collectively known as Remote Desktop Services are supplied with recent versions of Windows, including Windows Vista, Windows 7, Windows 8, Windows 2003, Windows 2008, and Windows 2012.

The client for the RDP protocol is Remote Desktop Connection (mstsc.exe). This is a descendant of Microsoft Terminal Services Client, and can still be seen in the client executables name. RDC allows you to connect to another computer running the RDP Server role. RDC can connect to multiple servers simultaneously.

The server (host) component for the RDP protocol is configured through properties of the local computer or server. Typically these settings are found under Remote -> Remote Desktop, and specify whether RDP is enabled, and who can connect.

Remote Desktop Services also allow several other features beside just controlling the Desktop. Local resources, such as hard drives, sound devices, printers, the clipboard etc. can be made available to the remote host whilst the RDP session exists.

There are also some restrictions in place during an RDP session. These are typically minor, but in some circumstances may impact your work.

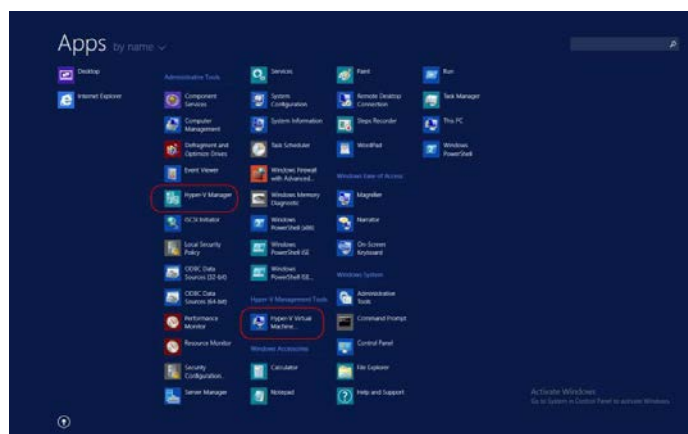
For example, RDP starts a new login session per user on the remote server. It does not let you view the physical console.

Console level access is not exactly the same as being at the physical console. (System tray icons may behave differently).

You cannot access the power button, or eject and insert CD's etc.

If the server is acting as a Hyper-V host, then the **Hyper-V Virtual Machine Connection** or **Hyper-V Manager** utilities can be used to gain RDP like access to the guest Virtual Machine consoles. No further configuration is required to access this facility.

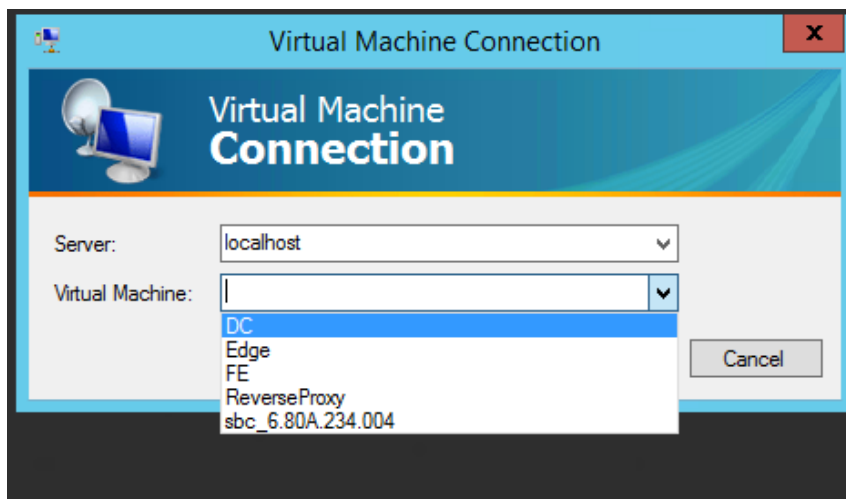
Figure 21-1: Hyper-V Host Desktop



21.2.1 Hyper-V Virtual Machine Connection

Hyper-V Virtual Machine Connection is the simplest method to use. Simply locate the utility in the start menu, Select the Host Server, then select the virtual machine. You will then be presented with the VM's login screens.

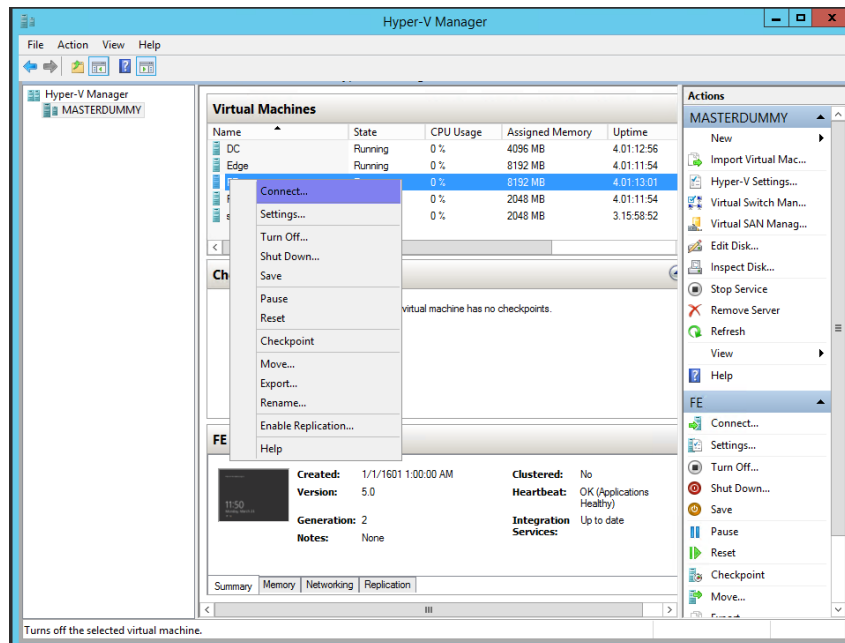
Figure 21-2: Hyper-V Virtual Machine Connection



21.2.2 Hyper-V Manager

You can also use the Hyper-V Manager utility to access a virtual machine Desktop. Locate the Hyper-V Manager in the start menu, then, in the list of virtual machines, either right click and choose Connect, or just double click the appropriate Virtual Machine.

Figure 21-3: Virtual Machines



21.2.3 Login Process

Once the connection to the VM is established, you will see the usual login screens. Tip: In full screen mode, use Ctrl-Alt-End, not Ctrl-Alt-Del.

Figure 21-4: Full screen Mode - Login Screen

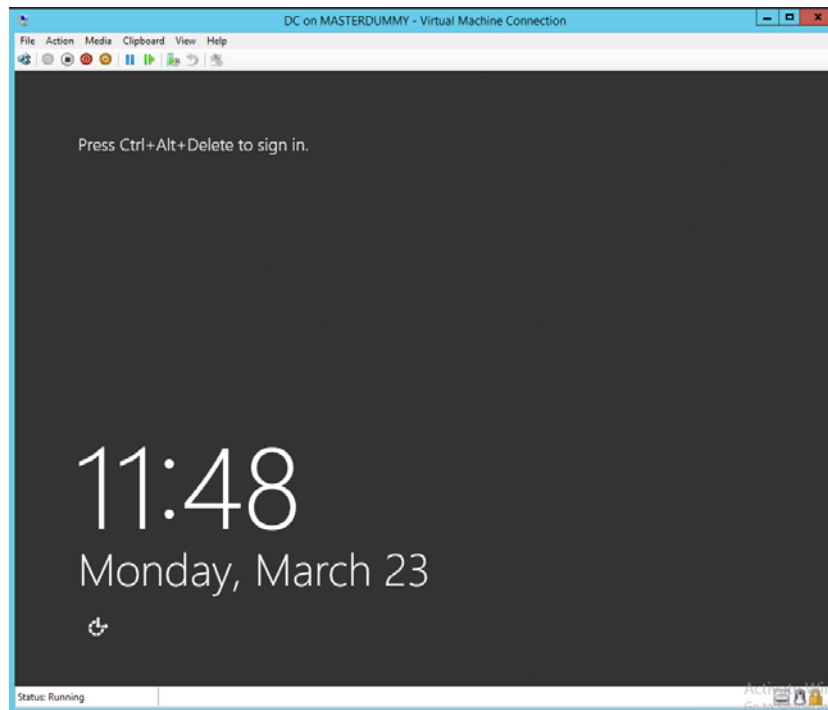
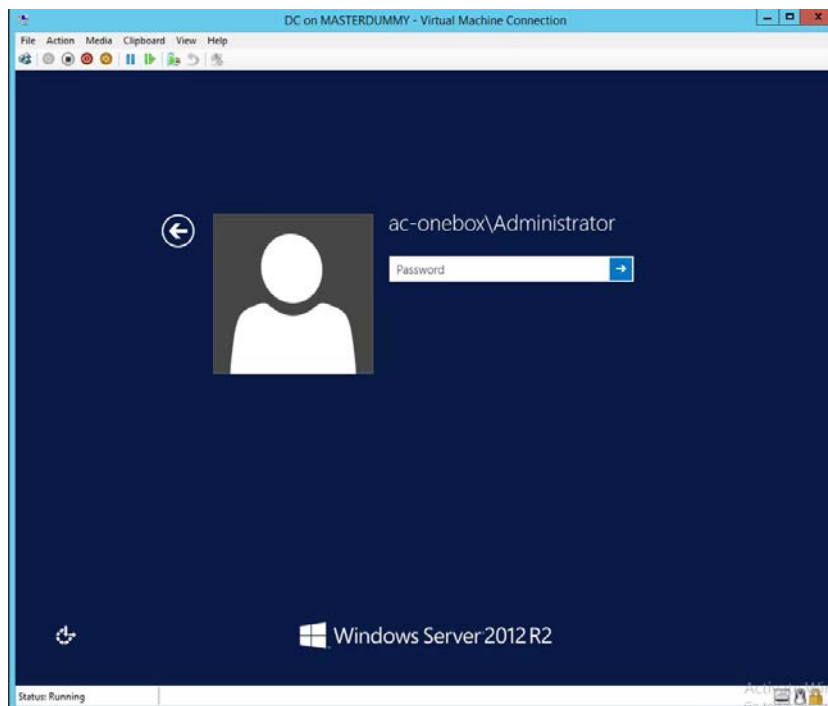


Figure 21-5: Login Screen – Username/Password



21.3 Enable RDP on Each Server

The RDP Server component is typically disabled by default on most windows versions for security reasons. If you wish to allow remote Desktop access directly to a server, you will need to enable and configure remote desktop services.

You may also need to modify the servers default firewall configuration.



Warning: Special care should be taken when enabling RDP on servers exposed to an external (untrusted) network, such as the Edge server which is connected to the DMZ.

Microsoft defaults for Windows Firewall rules typically split RDP access into two security sets based on network Profile. The first set of rules cover Domain and Private networks, the second set covers Public Networks. When enabling RDP Services, typically only the first set is enabled through the firewall. The public network access through the firewall is disabled by default.

Depending upon your network configuration, you may need to enable Public network profile access.

The Edge server is not a domain Member Server, so its internal network profile is usually classed as Public.

You should consider the following items prior to enabling RDP:

- IT policies and procedures
- Convenience of access to physical KVM ports
- Deployment model used: (**Co-Located Hyper-V / Domain Controller with Virtual Machines** or **Hyper-V Host with Virtual Machines**)
- Frequency of using Desktop access to perform tasks

You may elect to:

- Restrict desktop access to physical KVM ports only
- Allow RDP access to Hyper-V host server only
- Allow RDP access to the Controller server only (UC-DC)
- Allow RDP access to each individual server
- A combination of the above.

This page is intentionally left blank.

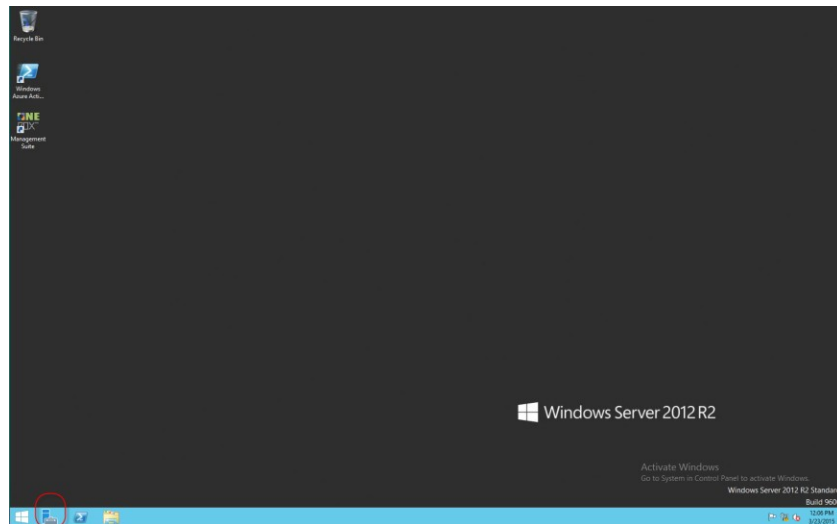
22 Configuring Remote Desktop

This chapter describes the easiest method to configure the Remote Desktop Services.

➤ **To configure Remote Desktop Services:**

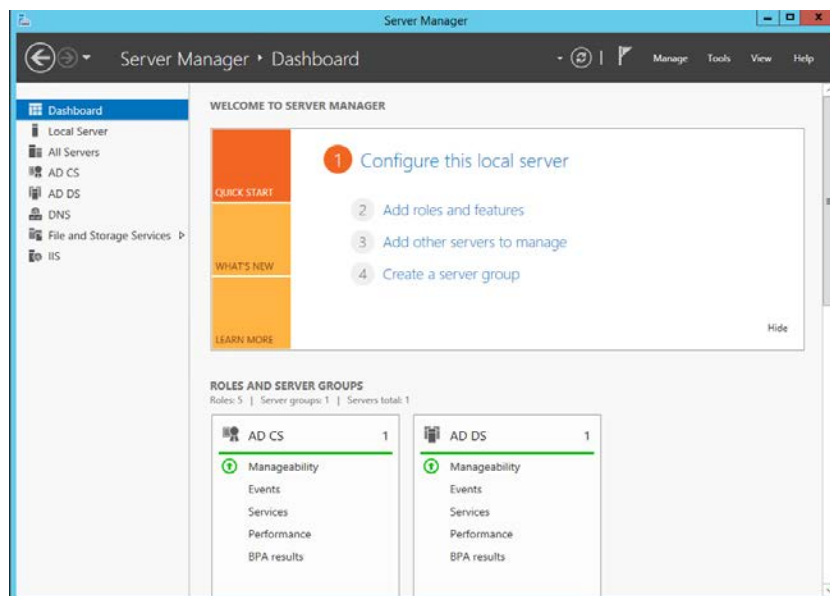
1. Locate and start Server Manager.

Figure 22-1: Server Manager Icon on Desktop



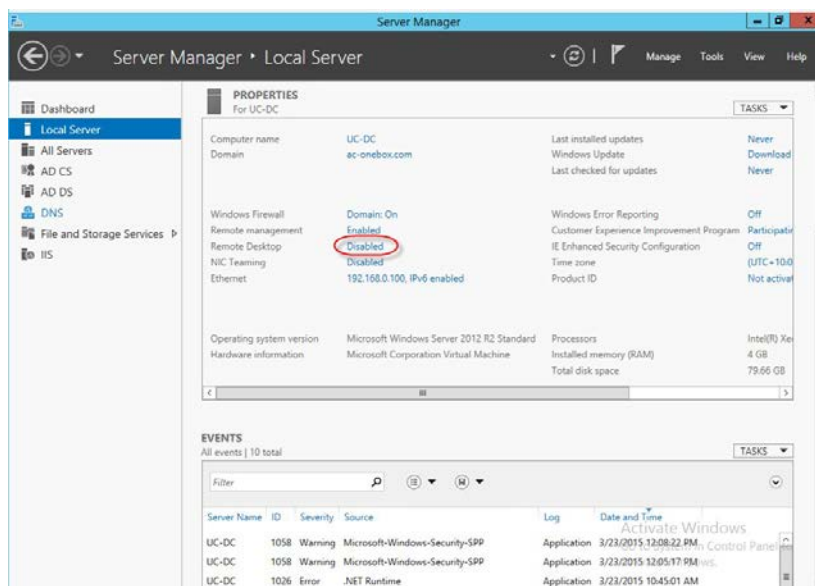
2. Select Local Server.

Figure 22-2: Server Manager Dashboard



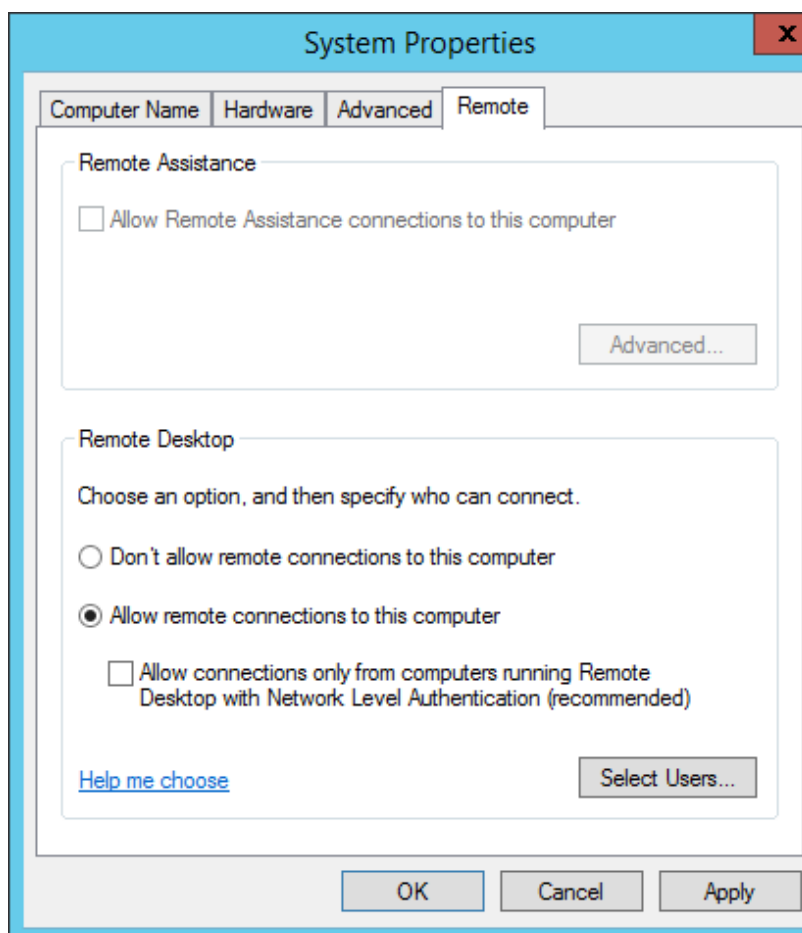
- Find the Remote Desktop entry and click on Disabled link.

Figure 22-3: Server Manager - Local Server



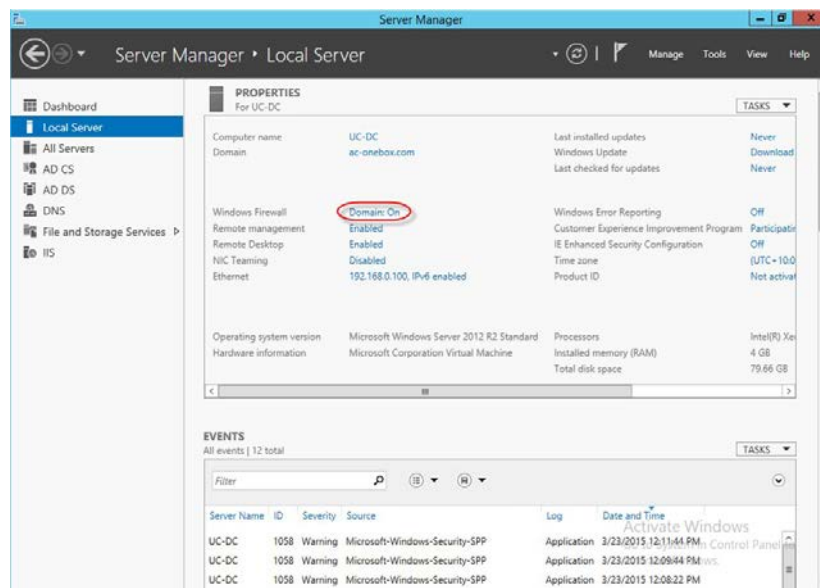
- Select Allow Remote connections to use this computer.

Figure 22-4: Enable Remote Desktop



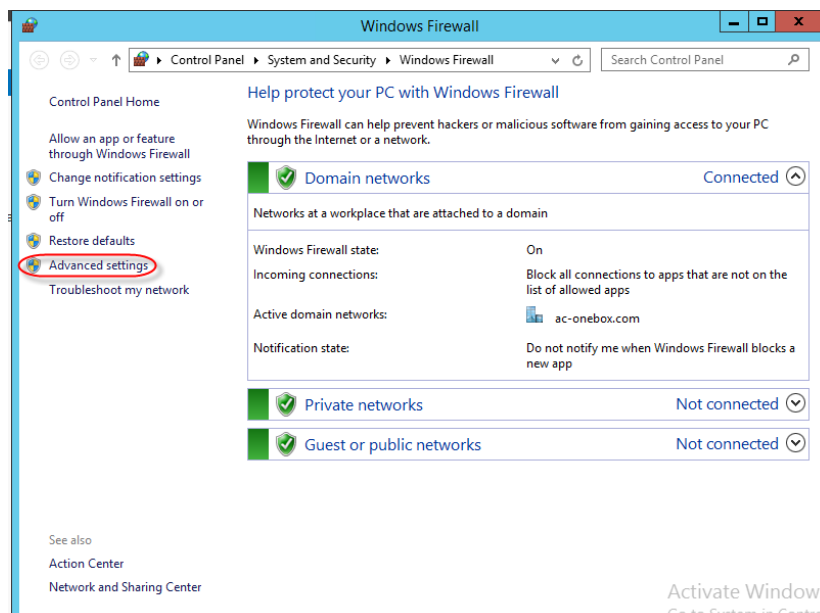
5. Click **OK**.
6. In Server Manager, find **Windows Firewall**, and then click on its link.

Figure 22-5: Server Manager - Windows Firewall



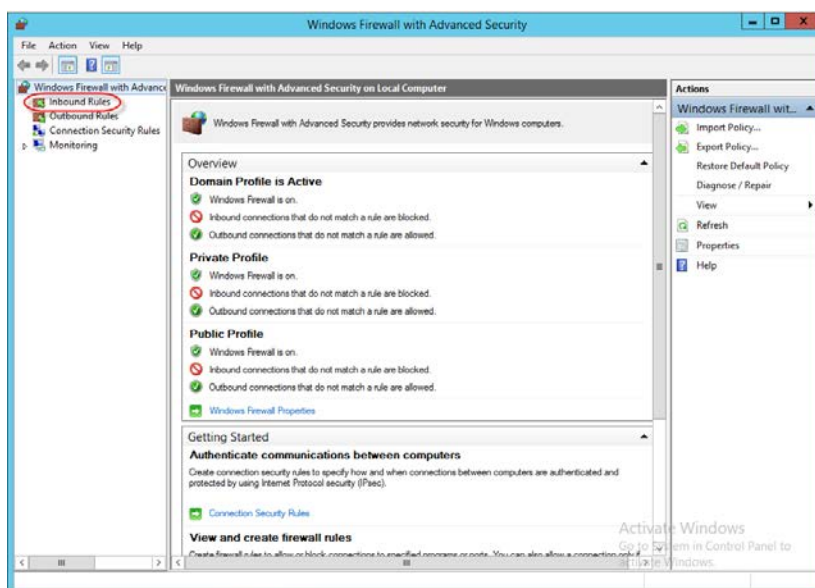
7. Click **Advance Settings**.

Figure 22-6: Windows Firewall Settings



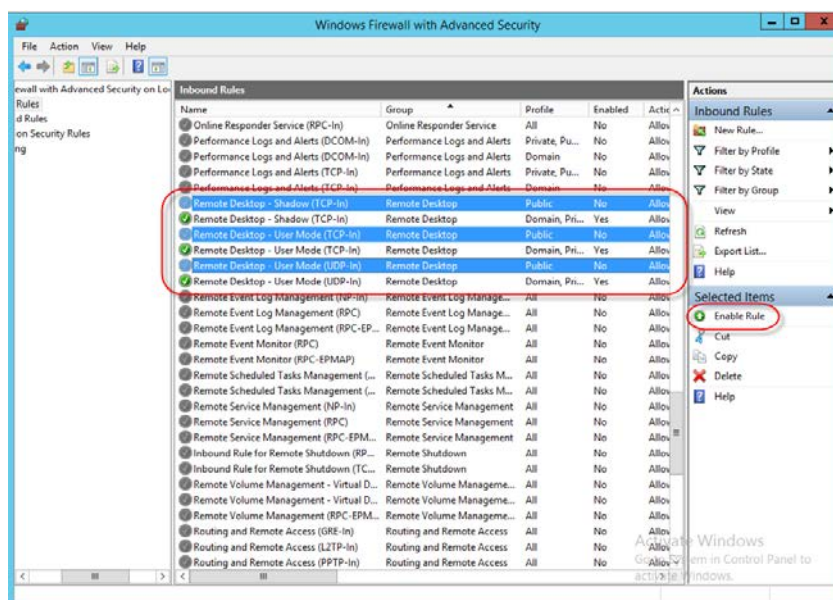
8. Click **Inbound Rules**.

Figure 22-7: Advanced Windows Firewall Settings



9. Scroll down until you locate the Remote Desktop Rules.

Figure 22-8: Inbound Rules - Remote Desktop

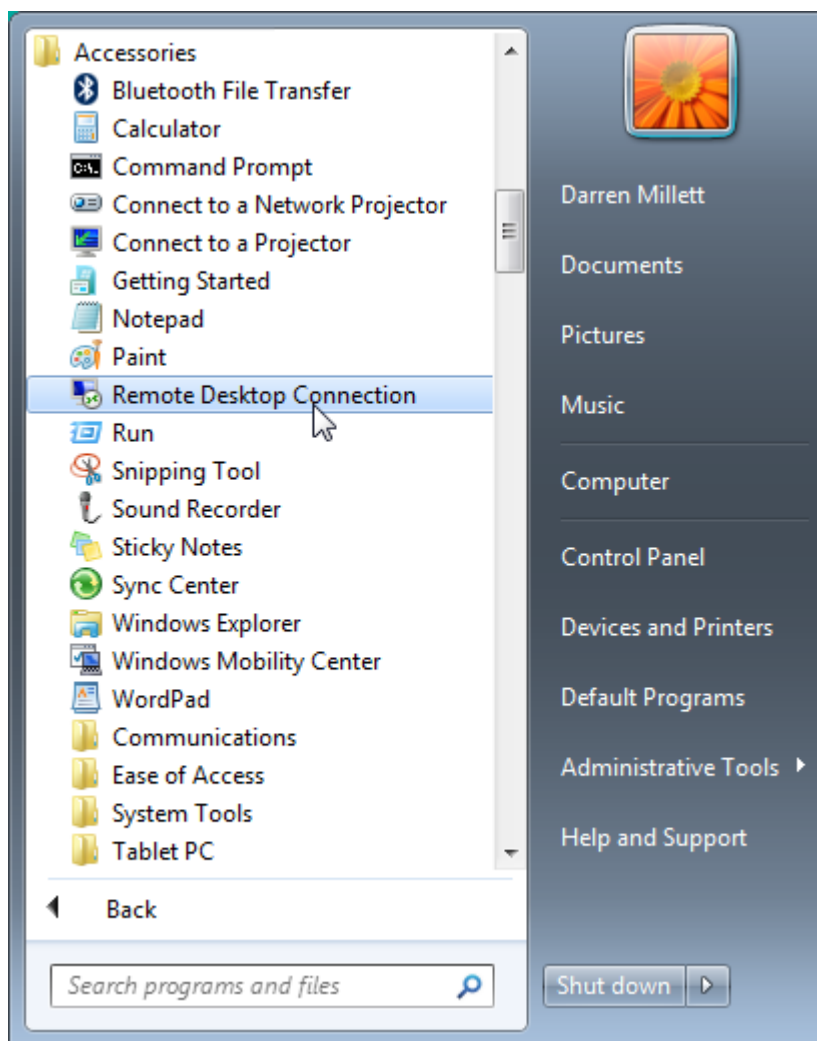


10. Note the current settings for each Profile. By default, if Remote Desktop Services are enabled, the Domain and Private profiles will be enabled, but Public profile will be disabled. Remember that the Edge server is not a Domain Member server. Its internal network connection will likely be a public profile.
11. Select the Rules you wish to change. (You can select multiple rules.)
12. Click **Enable Rule** or **Disable Rule** in the right hand panel, as required.
13. Close all windows.

23 Starting RDC

You can start RDC from the Start button. On Windows 7, it is located in **Start > Programs > Accessories > Remote Desktop Connection**. On other Windows versions it may be located in slightly different locations. You can also Search for and Run **mstsc.exe**.

Figure 23-1: Starting RDC

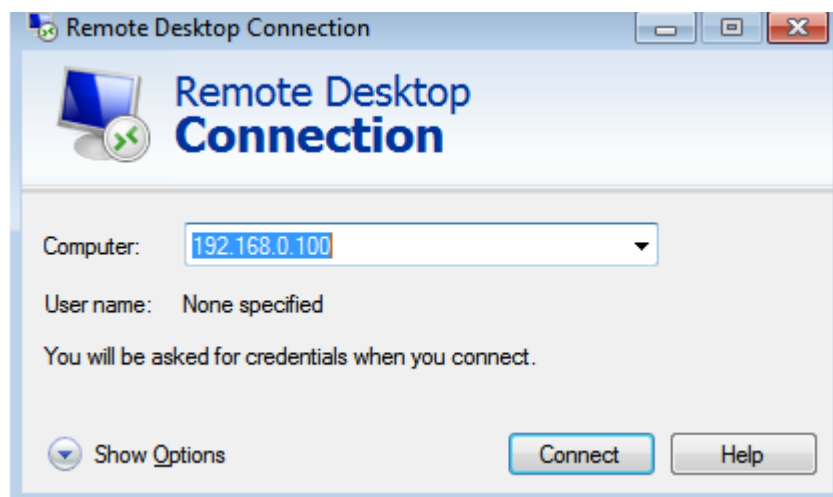


When RDC starts, you will be prompted to enter the destination computer. You can enter either an IP address, or computer DNS name. You can also select from a saved list of computers you have previously connected to.

Enter the IP Address of your UC-DC server. For a default installation, this is 192.168.0.100, if you have changed this or specified a different address during the CloudBond 365 build.

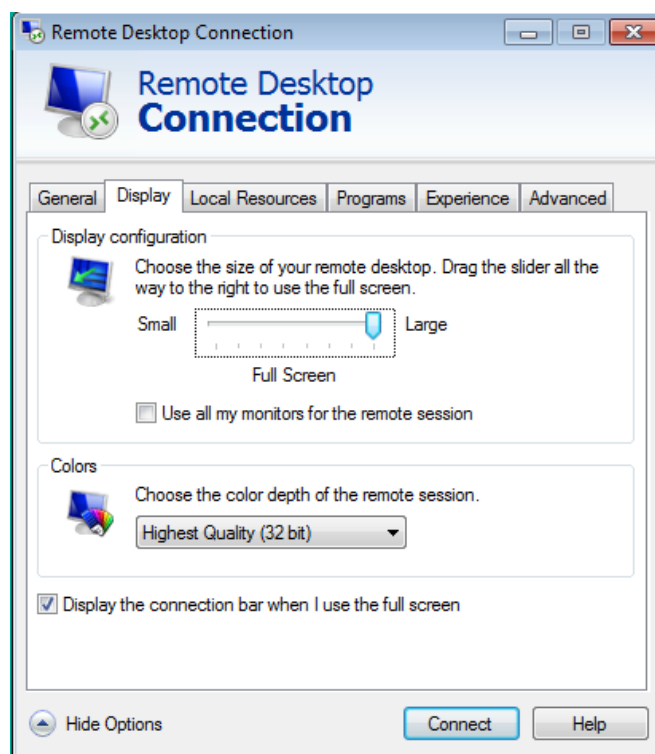
If you have not used RDP to connect to the UC-DC before, take time to set the RDC Options before pressing **Connect**.

Figure 23-2: RDC Connection Prompt



23.1 Setting RDC Options

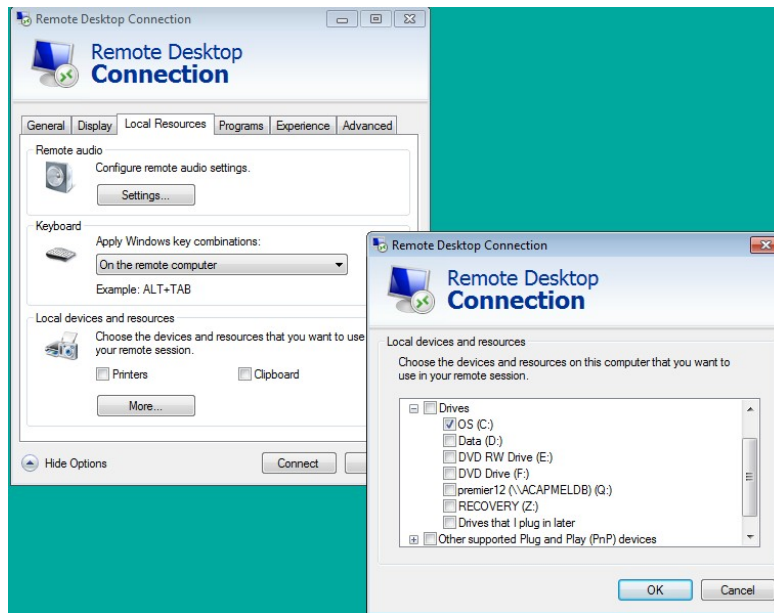
Figure 23-3: Setting RDC Options



If you click **Show Options** you will see various settings you can change to control your connection settings with the remote computer.

We recommend you set your Display Configuration to Full Screen and share your C:\ drive and clipboard as a local resource, for the best experience.

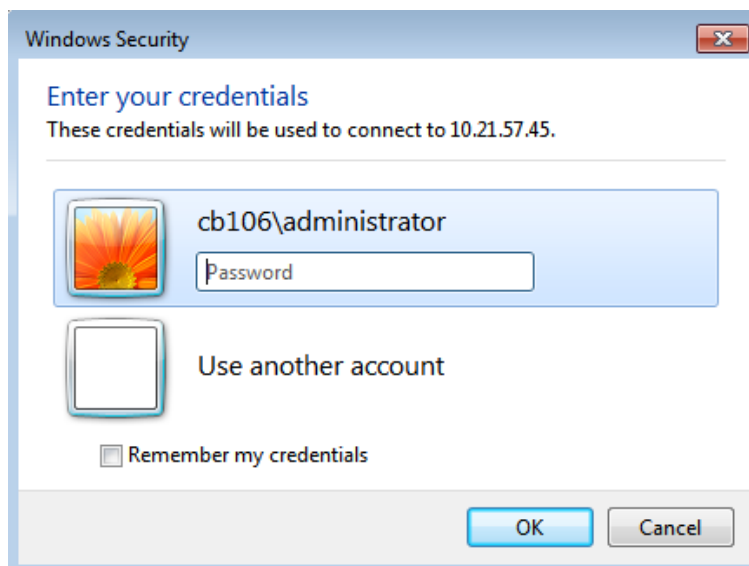
Figure 23-4: Sharing Local C drive



23.2 Connecting

After clicking the **Connect** button, you will be presented with an Authentication screen. For the CloudBond 365 Controller (UC-DC), it is simplest to log in as the CloudBond 365 Administrator. The default account is shown below.

Figure 23-5: RDC Authentication



After entering your credentials successfully, you may see the following warning. It is normal for the CloudBond 365 domain CA certificate not to be installed on end user workstations. You can optionally check the box "Don't ask me again.." to avoid displaying this warning in future.

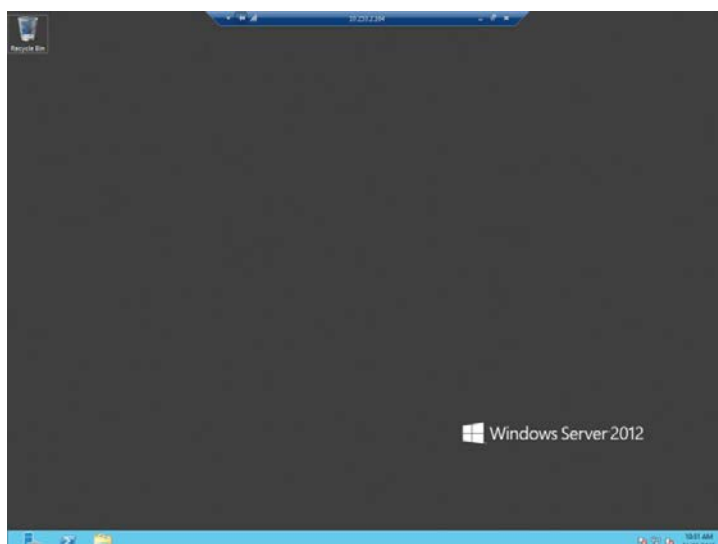
Click **Yes** to proceed.

Figure 23-6: CloudBond 365 Certificate



You will next be presented with the desktop of the selected server. From here, you can carry out most tasks as if you were physically present in front of the server, including mouse control and keyboard input.

Figure 23-7: RDP Session Established



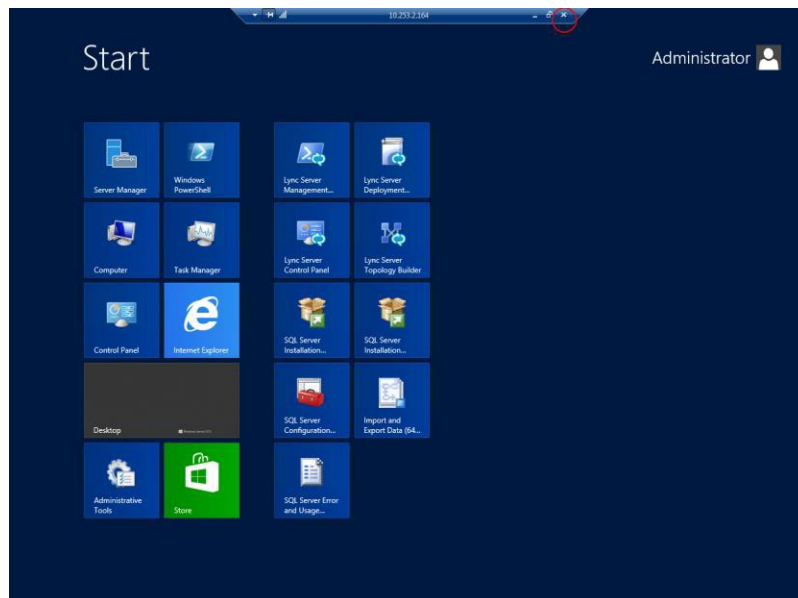
24 Ending an RDC Session

There are two ways to end an RDC session with a remote computer.

Performing a Windows Logout (not a Shutdown) is the preferred way. This ends your login session, and leaves the remote server at its login screen, ensuring any users must re-enter their credentials to login to the server.

Alternatively, you may need to leave your current login session running for a long running task etc. You can simply end the RDC session by pressing the X on the connection bar. This will leave your login session running, but lock the remote computer. Your login session can be re-established by reconnecting using RDC.

Figure 24-1: Ending RDC Session



This page is intentionally left blank.

Part IV

IP Phone Management Administrator's Tool

25 Introduction to the IP Phone Manager Admin

AudioCodes CloudBond 365 can manage AudioCodes IP Phones that are deployed in the same Microsoft Skype for Business environment, using the CloudBond 365 management suite. For managing the IP Phones, the CloudBond 365 management suite includes the IP Phones management module.

The main screen of the IP Phones management module provides basic IP Phone management and monitoring capabilities. For advanced configuration, such as loading configuration files and firmware files to multiple IP Phones, a link to the IP Phone management suite client is provided from the CloudBond 365 management interface.

This page is intentionally left blank.

26 Deploying the IP Phones

This section shows how to deploy AudioCodes IP phones in the enterprise.

26.1 Planning the Deployment

Before deploying the phones:

1. List the configurations specific to your phone network, e.g., language per region, speed dials, etc.
2. List the phone features and parameter configurations you want in each region.
3. Log in to the IP Phone Management Server (see Section 26.3).
4. Configure a 'system user' whose username is **system** and whose password is **system** (see Section 26.4).
5. Before plugging phones into the network, define parameter placeholders values for criteria such as region and phone model, to maintain an automatic provisioning scheme (see Section 29.2.80).

26.2 Preparing the Enterprise Network

This section shows how to prepare the enterprise network for IP phones.

➤ **To prepare the enterprise network:**

- Obtain the phones' latest firmware files from AudioCodes and upload them to the IP Phone Management Server - see under Section 29.4 for detailed information:
 - In the Phone Firmware Files screen, click the **Upload firmware** button.
 - Navigate to the img file and upload to the IP Phone Management Server.
- Configure your enterprise's DHCP server with DHCP Option 160 to point to the CloudBond Provisioning server's URL - if your phones are not behind a NAT. In addition to DHCP Option 160, DHCP Option 66/67 can also be used.

If your phones reside behind a NAT and an HTTP proxy is available, configure your enterprise's DHCP Server with DHCP Option 160 to point to the HTTP proxy. Phone-IP Phone Management Server communications will then be performed via the HTTP proxy rather than directly.

As DHCP clients, AudioCodes IP phones will then automatically be provisioned with the cfg and img files located on the IP Phone Provisioning server.

The figure below shows the default **dhcption160.cfg** file.

Figure 26-1: Default cfg File Located on the IP Phone Management Server

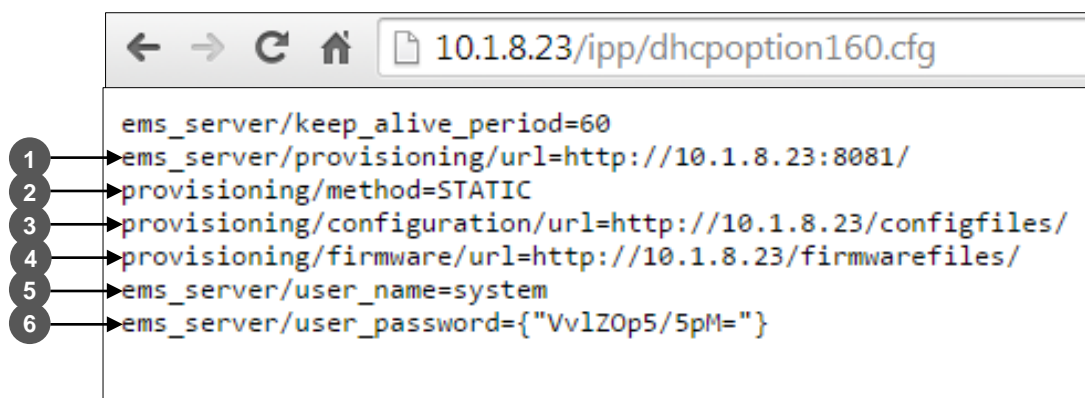


Table 26-1: IP Phone Provisioning File Legend

Legend	Description
1	Pointing to the URL of the IP Phone Management Server.
2	STATIC provisioning method, so the cfg and img files are automatically retrieved from the IP Phone Management Server rather than from the DHCP server.
3	Location of the cfg file, pulled by the phones when they're plugged into the network, on the IP Phone Management Server.
4	Location of the img file, retrieved by the phones when they're plugged into the network, on the IP Phone Management Server.
5	Name of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.
6	(Encrypted) Password of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.



Note:

- The **dhcption160.cfg** file is created when logging in for the first time to the IP Phone Management Server.
- After installation, the first, second and third lines in the file are automatically updated.

26.2.1 Deployment

This section describes how to deploy IP phones in a Skype for Business environment.



Note:

- If your phones communicate directly with the CloudBond server, make sure you have defined **http://<Server IP address>/firmwarefiles;ipp/dhcpoption160.cfg** for DHCP Option 160 in the enterprise's DHCP server. See the previous section for details.
- If your phones will communicate with an HTTP proxy rather than directly with the IP Phone Management Server, make sure you have defined **http://<Proxy SBC IP address><Proxy SBC Port>/firmwarefiles;ipp/httpproxy** for DHCP Option 160 in the enterprise's DHCP server. See the previous section for details.

➤ **To deploy IP phones:**

- Plug in the phone (see Section 26.5).

The cfg file includes default values and overwritten values according to configured placeholders. If no placeholder was configured, the cfg file will include only default values. See Section 29.2.8 for details on how to configure parameters placeholders.

26.3 Logging in to the Management Server

This section shows how to log in to the IP Phone Management Server UI. The UI is a secured web client that runs on any standard web browser supporting HTML5: Internet Explorer version 11 and later, Chrome or Firefox. Before logging in, you need to run the CloudBond Management Server.



Note: To access the IP Phone Management Server UI without running the CloudBond Management Server, point your web browser to **https://<CloudBond_IP_Address>/ipp** and then in the login screen that opens, log in.

➤ **To log in to the IP Phone Management Server via the CloudBond Management Server:**

1. Open the CloudBond Management server and click **IP Phones** in the main screen toolbar.

Figure 26-2: CloudBond Management Server - IP Phone Management Server button



The Welcome to the IP Phone Management Server screen opens:

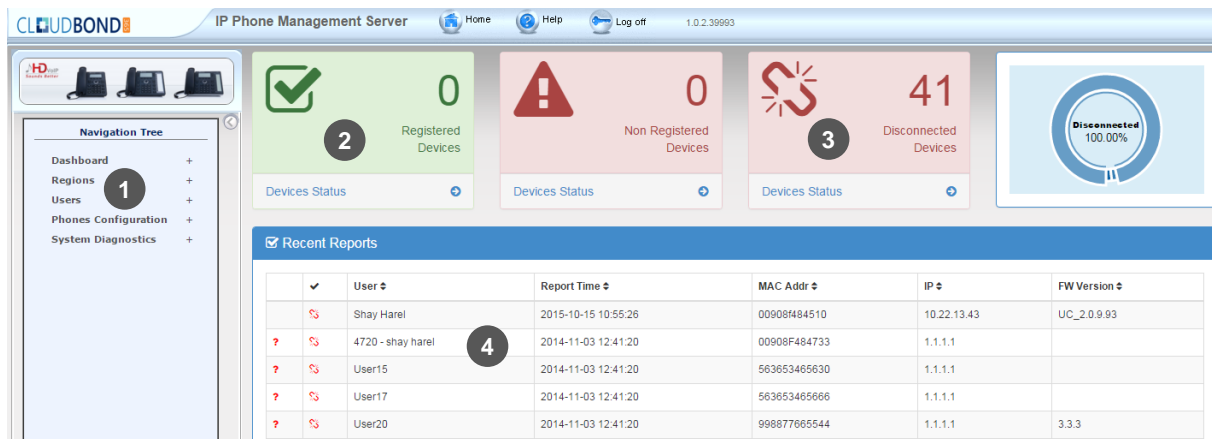
Figure 26-3: Welcome to the IP Phone Management Server




Note: The 'Username' and 'Password' used to log in to the IP Phone Management Server are the same as the windows OS.

2. Enter your Username and Password and click **Login**; the application is launched and the homepage displayed.

Figure 26-4: IP Phone Management Server User Interface - Homepage



- 1 = Navigation pane
- 2 = Network registration status
- 3 = Network health status
- 4 = List of users and their current status



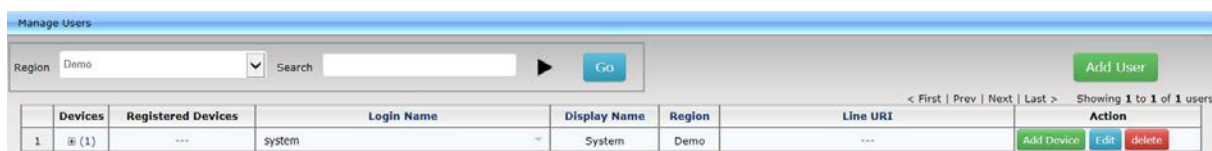
Note: After first-time login, no users and devices are displayed in the Home page.

26.4 The 'System User'

During the installation the system creates a 'system user' whose user name is **system** and whose password is **system**. This is necessary for *basic REST API authentication*, after the phones are plugged in to the network for the first time.

- Make sure in the Manage Users screen that the System user has been added.

Figure 26-5: Manage Users Screen Displaying Added User



Note: The system is now ready for monitoring and managing phones.
All you need to do is to plug in the phones.

26.5 Plugging Phones into the Network

Once you have configured the 'system user', you can plug the phones into the network.

The following describes possible user action scenarios that occur when the IP Phones are connected to CloudBond (these scenarios usually occur in the order described below):

- **Scenario 1:** Initial IP Phone connection to the CloudBond:

The phone is reported as offline and is displayed in the dashboard as follows:

?	⊗		00908f484688	10.38.2.8	UC_2.0.9.93
---	---	--	--------------	-----------	-------------

- **Scenario 2:** Phone sign-in:

The phone is reported as registered/unregistered and is displayed in the dashboard as follows:

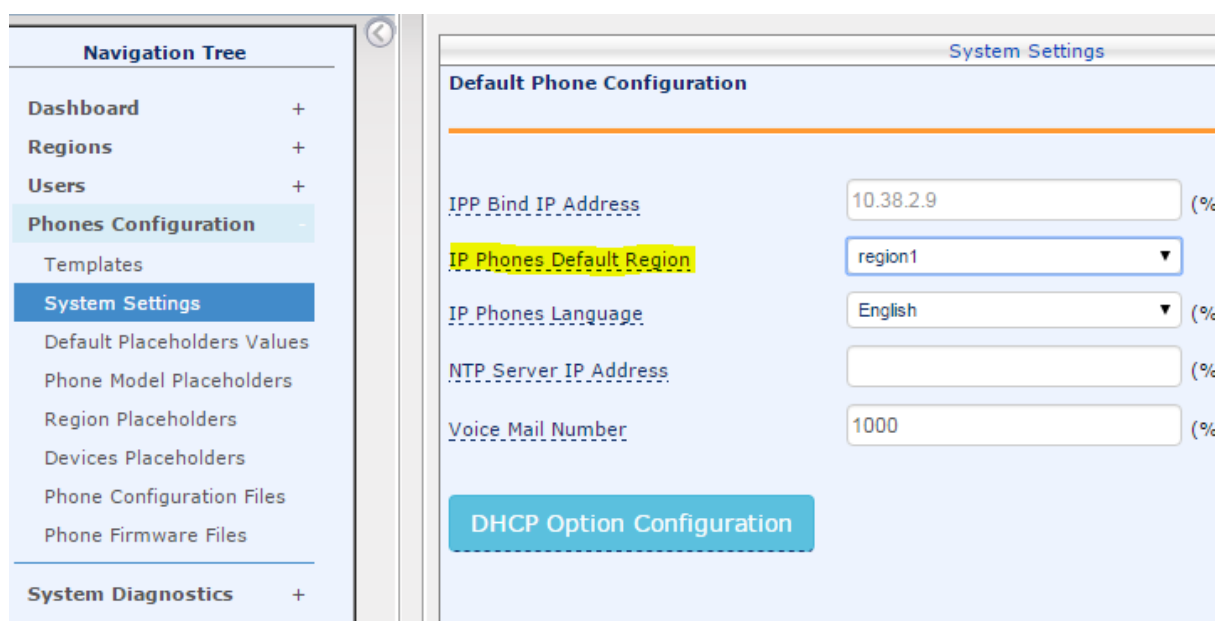
✓	Alex Agranov	16.11.2015 15:15:53	00908f48464d	10.22.11.6	UC_2.0.11.194.10.2
---	--------------	---------------------	--------------	------------	--------------------

If the sign-in was successful, a user and device are automatically created and a new <MAC>.cfg file is generated for this phone.

The user is created in the default region.

You can configure the default region in the System settings:

Figure 26-6: System Settings



Navigation Tree

- Dashboard +
- Regions +
- Users +
- Phones Configuration -
- Templates
- System Settings**
- Default Placeholders Values
- Phone Model Placeholders
- Region Placeholders
- Devices Placeholders
- Phone Configuration Files
- Phone Firmware Files
- System Diagnostics +

System Settings

Default Phone Configuration

IPP Bind IP Address: 10.38.2.9 (%)

IP Phones Default Region: region1

IP Phones Language: English (%)

NTP Server IP Address: (%)

Voice Mail Number: 1000 (%)

DHCP Option Configuration

- **Scenario 3:** Phone sign-out and sign-in with a different user:

If the user signs-out and signs-in with a different user, the endpoint along with the old <MAC>.cfg are deleted and a new endpoint with a new <MAC>.cfg are created for the sign-in user.

You can view this information in real time on the Homepage or in the Device status page.

26.5.1 Devices Status

After the phones are plugged in, they send updates to the IP Phone Management Server; however, the user names are not displayed in the interface until either sign-in is performed on the phone or until users are approved in the interface (if the user signs-in on the phone, then its automatically approved in the interface).

- In the IP Phone Management Server, open the Devices Status page (**Dashboard > Devices Status**).

Figure 26-7: Devices Status

	✓	User	Report Time	MAC	IP	Model	Firmware Version	Region	Location	Subnet
Actions	⊕		11.01.2015 13:06:35	0090083eb602	172.17.188.88	420HD	UC_2.0.9.50	RovnaRegion		255.255.255.0
Actions	⊕		07.01.2015 08:54:45	009008487914	10.13.2.78	420HD	2.2.0.7			255.255.0.0
Actions	⊕	Shay Harel	05.01.2015 13:53:00	009008484658	10.13.2.9	440HD	UC_2.0.9.65			255.255.0.0
Actions	⊕	Shay Harel2	05.01.2015 13:52:38	009008484688	10.13.2.9	440HD	UC_2.0.9.65			255.255.0.0

- 1 = Device actions: refresh, reset, download files, open web page, delete, send text message to the phone
- 2 = Device approval
- 3 = Device status: User, MAC, IP Address, SIP URI, and Location
- 4 = Search option
- 5 = Smart filters

This page is intentionally left blank.

27 Monitoring and Maintaining the Phone Network

This section shows how to monitor and maintain the phone network in the enterprise.

The following Dashboard and Users pages let you monitor and maintain the phone network:

Figure 27-1: Dashboard and Users



The sections below describe the functionality of each page.

27.1 Monitoring the Network from the Dashboard

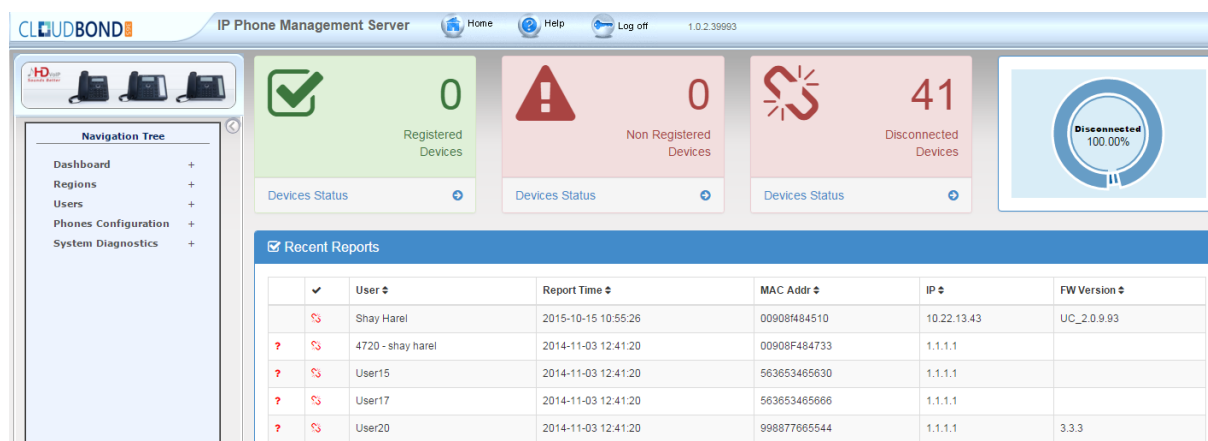
The Dashboard page lets you quickly identify the following:

- Which phones in the network are registered
- Which phones in the network are non-registered
- # of registered and non-registered phones (in terms of SIP registration)
- % of registered phones
- The MAC and IP address of each phone
- The time the information was reported
- The firmware version

➤ **To open the Dashboard page:**

- In the navigation tree, click **Dashboard > Dashboard**.

Figure 27-2: Dashboard



If a Skype for Business Desktop phone is signed out (offline, or not registered), you'll see a grey circle icon with an x inside, and the 'User' column will be blank, as shown in the figure below.

It will be counted as a Non-Registered Device.

Figure 27-3: Dashboard - Not Registered

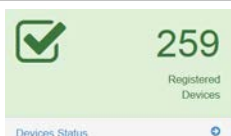





Point your mouse over the icon to view the 'offline' indication (see the figure above).

If the phone is a generic model, a red triangle enclosing an exclamation mark will be displayed, as shown in the figure above.

View the following status thumbnails on the Dashboard:

Table 27-1: Dashboard – Status Thumbnails

Status Thumbnail	Description
	The number of registered devices. Click the Devices Status link to quickly access the Devices Status page.
	The number of non-registered devices. Click the Devices Status link to quickly access the Devices Status page.
	The number of disconnected devices. Click the Devices Status link to quickly access the Devices Status page.
	The percentage of registered devices.

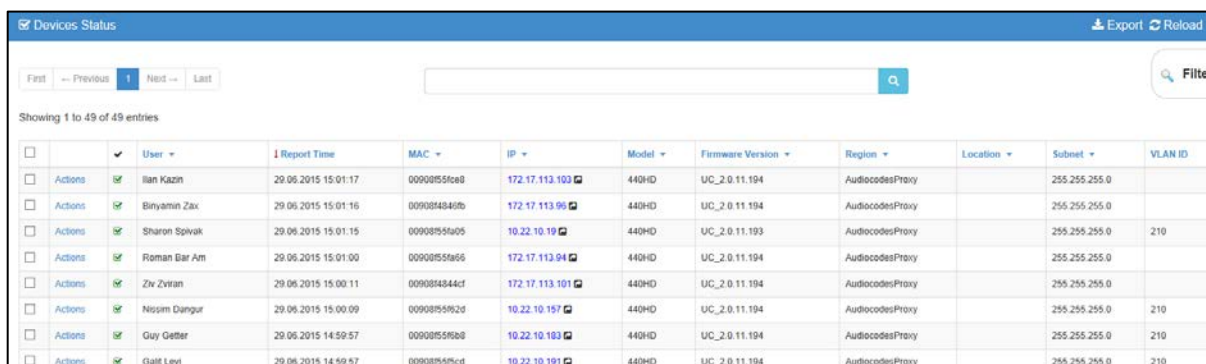
27.2 Checking Devices Status

The Devices Status page lets you check a phone's status

➤ **To check a phone's status:**

1. Open the Devices Status page (**Dashboard > Devices Statuses**).

Figure 27-4: Devices Status

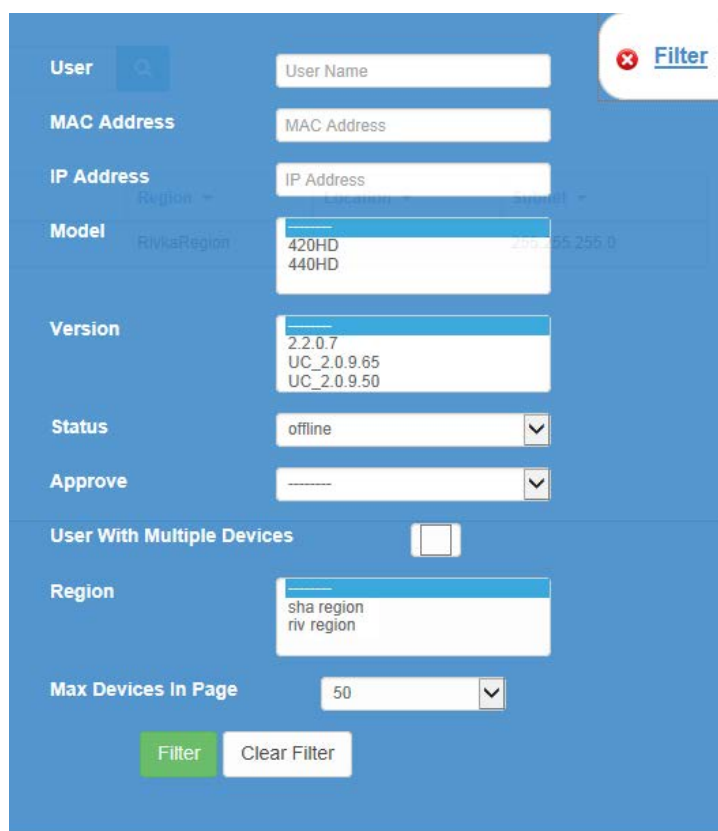


The screenshot shows the 'Devices Status' page with a table of 49 entries. The table has columns for User, Report Time, MAC, IP, Model, Firmware Version, Region, Location, Subnet, and VLAN ID. The first few rows are visible:

	User	Report Time	MAC	IP	Model	Firmware Version	Region	Location	Subnet	VLAN ID
Actions	Ilan Kazin	29.06.2015 15:01:17	0090855fca8	172.17.113.103	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Binyamin Zax	29.06.2015 15:01:16	0090854840b	172.17.113.95	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Sharon Spivak	29.06.2015 15:01:15	00908555a05	10.22.10.19	440HD	UC_2.0.11.193	AudiocodesProxy		255.255.255.0	210
Actions	Roman Bar Am	29.06.2015 15:01:00	00908555a66	172.17.113.94	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Ziv Zviran	29.06.2015 15:00:11	0090854844d	172.17.113.101	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	
Actions	Nosim Dangur	29.06.2015 15:00:09	0090855592d	10.22.10.157	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210
Actions	Guy Oetter	29.06.2015 14:59:57	00908555b08	10.22.10.183	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210
Actions	Galit Levi	29.06.2015 14:59:57	00908555fcd	10.22.10.191	440HD	UC_2.0.11.194	AudiocodesProxy		255.255.255.0	210

2. Click the **Filter**; the filter lets you quickly access specific information in the page.

Figure 27-5: Devices Status Filter



The screenshot shows the 'Filter' dialog box with the following fields and options:

- User:** Search field for User Name.
- MAC Address:** Search field for MAC Address.
- IP Address:** Search field for IP Address.
- Model:** Dropdown menu with options: 420HD, 440HD.
- Version:** Dropdown menu with options: 2.2.0.7, UC_2.0.9.65, UC_2.0.9.50.
- Status:** Dropdown menu with option: offline.
- Approve:** Dropdown menu with option: -----.
- User With Multiple Devices:** Checkbox (unchecked).
- Region:** Dropdown menu with options: sha region, riv region.
- Max Devices In Page:** Dropdown menu with option: 50.
- Buttons:** Filter (green), Clear Filter (white).

3. You can filter per user, MAC, IP address, model, and version, status (offline, registered, disconnected, approved or pending approval, or users with multiple devices).
4. The format of 'User Agent' for Skype for Business Desktop phones is **AUDC-IPPhone-430HD_UC_2.0.7.70/1.0.0000.0**.
The 'Location' is displayed if was configure correctly in the Skype for Business server.

5. You can click an individual user's **Actions** link; the following menu is displayed:

Figure 27-6: Actions Menu - Single User

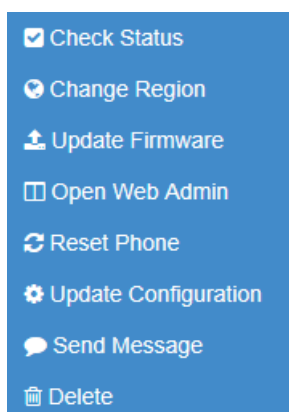
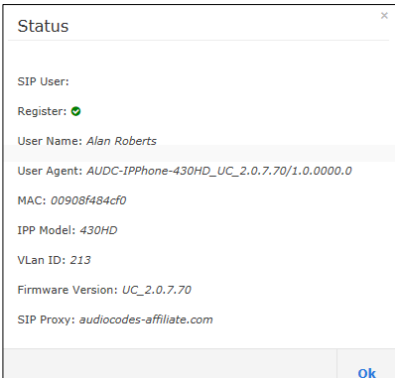
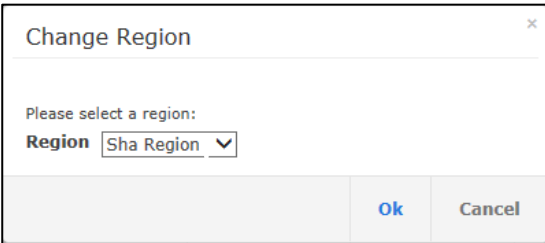
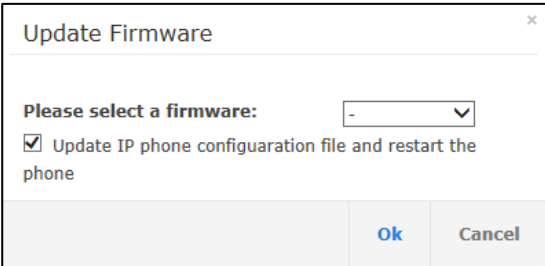


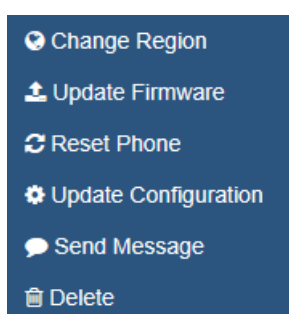
Table 27-2: Actions Menu

Action	Description
Check Status	<p>Select the 'Check Status' option; the status is displayed:</p> 
Change Region	<p>Select the 'Change Region' option:</p>  <p>From the dropdown, select the region, and then click Ok.</p>
Update Firmware	<p>You can update firmware per device, or for multiple selected devices (see step 6 below). Select the 'Update Firmware' menu option:</p>  <p>From the dropdown, select the firmware file, and then click Ok; the firmware file is updated.</p>

Action	Description
Open Web Admin	Opens the Web interface (see the <i>Administrator's Manual</i>).
Reset Phone	Sends a reset command to the selected device/s. Note that some phone models wait for the user to finish an active call, while others may perform an immediate restart.
Update configuration	Sends a command to the phone to check whether there is a new configuration file to upload and updates the phone after a configurable 'Delay Time' (Default = 2 seconds).
Send Message	Let's you send a message to the LCD/s of the selected device/s. Enter the message in the 'Text' field. You can configure for how long the message will be displayed in the LCD/s.
Delete	Deletes the devices from the Status table.

6. You can select multiple users and then click the **Selected Rows Actions** link; the following menu is displayed:

Figure 27-7: Actions Menu - Selected Rows



See the table above for descriptions. Any action you choose will apply to all selected rows. For example, select rows, click the **Selected Rows Actions** link, and then select the **Update Firmware** option; all selected devices will be updated with the firmware file that you select.

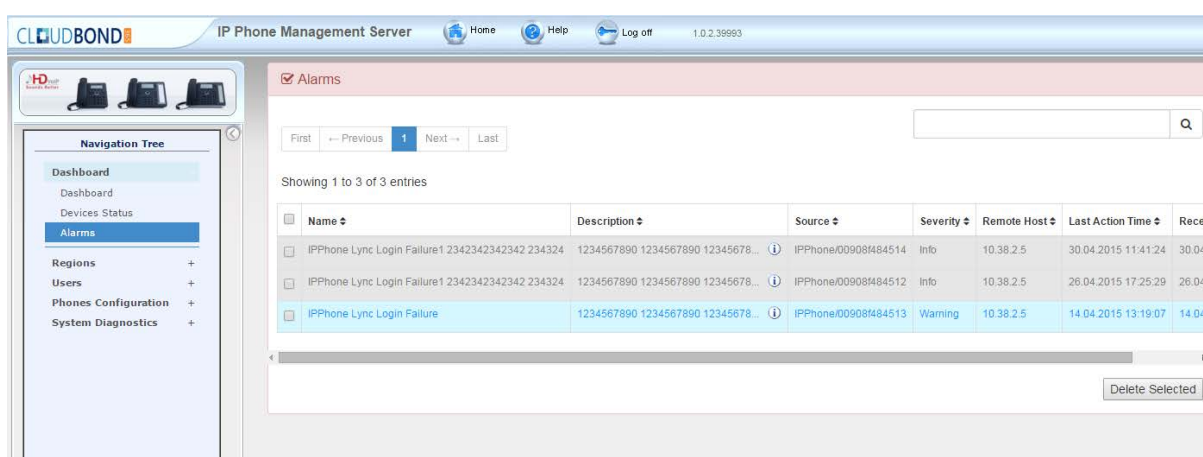
27.3 Monitoring Alarms

AudioCodes IP phones send alarms via the REST protocol.

The Alarms page (**Dashboard > Alarms**) displays the following information:

- Each phone alarm in the network
- A description of each alarm
- The MAC address of the phone (source)
- The alarm severity
- The IP address of the phone
- The last action time
- The date and time of receipt of the alarm

Figure 27-8: Alarms



Name	Description	Source	Severity	Remote Host	Last Action Time	Receive
IPPhone Lync Login Failure1 2342342342342 234324	1234567890 1234567890 12345678...	IPPhone/00908484514	Info	10.38.2.5	30.04.2015 11:41:24	30.04.2015 11:41:24
IPPhone Lync Login Failure1 2342342342342 234324	1234567890 1234567890 12345678...	IPPhone/00908484512	Info	10.38.2.5	26.04.2015 17:25:29	26.04.2015 17:25:29
IPPhone Lync Login Failure	1234567890 1234567890 12345678...	IPPhone/00908484513	Warning	10.38.2.5	14.04.2015 13:19:07	14.04.2015 13:19:07

The management server displays *active* alarms, not historical alarms.

Red indicates a severity level of "Critical"

Orange indicates a severity level of "Major"

After an alarm is cleared, it disappears from the Alarms screen.

The table below shows the alarms that users can receive.

Table 27-3: Alarms

Alarm Name	IP Phone Type	Severity
Login Failure	Skype for Business	Critical
Survivable Mode Start	Skype for Business	Major
Lync Login Failure Alarm	Skype for Business	Major
Endpoint License Alarm	Skype for Business	Critical/Major
Endpoint Server Overloaded Alarm	Skype for Business	Critical
IP Phone Speaker Firmware Download Failure	Skype for Business	Minor/Clear
IP Phone Speaker Firmware Upgrade Failure	Skype for Business	Minor/Clear

IP Phone Conference Speaker Connection Failure	Skype for Business	Minor/Clear
IP Phone General Local Event	Skype for Business	Major
IP Phone Web Successive Login Failure	Skype for Business	Major

27.3.1 Registration Failure Alarm

The table below describes the Registration Failure alarm. The alarm is issued if SIP registration, with the PBX, fails.

Table 27-4: IP Phone Registration Failure Alarm

Alarm	IPPhoneRegisterFailure
OID	1.3.6.1.4.1.5003.9.20.3.2.0.39 is the OID used in the IPP Manager to forward the IPPhoneRegisterFailure alarm.
Description	This alarm is activated when a registration failure occurs
Alarm Title	Registration Failure
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Corrective Action	The problem is typically not related to the phone; however, to the server. The user/phone may not be defined, or may be incorrectly defined, or may previously have been defined but the username (for example) may have been changed, causing the registration to fail. Make sure the username and password credentials are the same in both the server and phone, and weren't changed; server-phone credentials must be synchronized. Make sure the server is responsive.

27.3.2 Survivable Mode Start Alarm

The table below describes the Survivable Mode Start alarm.

Table 27-5: IP Phone Survivable Mode Start Alarm

Alarm	IPPhoneSurvivableModeStart
OID	1.3.6.1.4.1.5003.9.20.3.2.0.40 is the OID used in the IPP Manager to forward the IPPhoneSurvivableModeStart alarm
Description	This alarm is activated when entering survivable mode state with limited services
Alarm Title	Survivable Mode Start
Alarm Type	Other(0)
Probable Cause	other (0)
Severity	Major
Additional Info	
Corrective Action	The problem is typically not related to the phone; however, to the server or network. Make sure all servers in the enterprise network are up. If one is down, limited service will result.

27.3.3 Lync Login Failure Alarm

The table below describes the Lync Login Failure alarm.

Table 27-6: IP Phone Lync Login Failure Alarm

Alarm	IPPhoneLyncLoginFailure
OID	1.3.6.1.4.1.5003.9.20.3.2.0.41 is the OID used in the IPP Manager to forward the IPPhoneLyncLoginFailure alarm
Description	This alarm is activated when failing to connect to the Skype for Business server during sign in
Alarm Title	Lync Login Failure
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Additional Info	TlsConnectionFailure NtpServerError
Corrective Action	This alarm may typically occur if the user is not registered - or is registered incorrectly - in the Skype for Business server. Make sure in the server that the username, password and PIN code are correctly configured and valid. Try resetting them. Try redefining the user.

27.3.4 Endpoint License Alarm

Endpoint License Alarm

Description	<p>This alarm is issued for the following scenarios:</p> <ul style="list-style-type: none"> When the number of endpoints currently running on the Voice Quality server (shown as 'IP Phones Number' under 'Voice Quality' in the EMS Server Manager License screen) approaches or reaches its license capacity. When the number of endpoints currently running on the EMS server (shown as 'IP Phones Number' under 'EMS for IP Phones' in the EMS Server Manager License screen) approaches or reaches its license capacity. 		
SNMP Alarm	acEndpointLicenseAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.48		
Alarm Title	Endpoint License Alarm		
Alarm Source	Voice Quality/Management		
Alarm Type	Other		
Probable Cause	Key Expired		
Additional Info	Endpoint License capacity {0} devices.		
Corrective Action	Contact your AudioCodes partner ASAP		
Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	Currently connected devices are equivalent to 100% of Endpoints License capacity.	Currently running devices reached 100% of Endpoints License capacity.	-
Major	Currently connected devices are equivalent to reached 80% of Endpoints License capacity.	Currently running devices reached 80% of Endpoints License capacity.	-
Clear	Clearing currently active alarm	Clear - Clearing currently active alarm.	-

27.3.5 Endpoint Server Overloaded Alarm

Endpoint Server Overloaded Alarm

Description	This alarm is issued when the Voice Quality Endpoint server process is overloaded with RFC 6035 Publish messages. This causes new RFC 6035 SIP PUBLISH messages () to be dropped from the queue for this process.
SNMP Alarm	acEndpointServerOverloadAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.49
Alarm Title	Endpoint Server Overloaded Alarm
Alarm Text	Voice Quality Endpoint Server Overloaded! New Publish Messages Dropped
Alarm Source	Voice Quality
Alarm Type	Other
Probable Cause	Queue Size exceeded
Severity	Critical
Additional Info	Maximum Endpoint Server waiting queue size {0}.
Corrective Action	Reduce the endpoint traffic load on the EMS server.

27.3.6 IP Phone Speaker Firmware Download Failure

IP Phone Speaker Firmware Download Failure

Description	This alarm is raised when the phone fails to download the Jabra speaker firmware from the server (see Alarm Source).
SNMP Alarm	IPPhoneSpeakerFirmDownloadFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.54
Alarm Title	IP Phone Speaker Firmware Download Failure
Alarm Source	The server from which the download was attempted: EMS, WEB, HTTP, FTP
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

27.3.7 IP Phone Speaker Firmware Upgrade Failure

IP Phone Speaker Firmware Upgrade Failure

Description	This alarm is raised when the phone fails to load the Jabra firmware to the speaker.
SNMP Alarm	IP PhoneSpeakerFirmUpgradeFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.55
Alarm Title	IP Phone Speaker Firmware Upgrade Failure
Alarm Source	The IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

27.3.8 IP Phone Conference Speaker Connection Failure

IP Phone Conference Speaker Connection Failure

Description	This alarm is raised when there is failure for the USB connection between the phone and the Jabra speaker.
SNMP Alarm	IPPhone Conference Speaker Connection Failure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.56
Alarm Title	IP Phone Conference Speaker Connection Failure
Alarm Source	The IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Minor, Clear
Additional Info	-
Corrective Action	-

27.3.9 IP Phone General Local Event

IPPhone General Local Event

Description	This alarm provides information about the IP Phones internal operation.
SNMP Alarm	IPPhoneGeneralLocalEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.57
Alarm Title	IP Phone General Local Event
Alarm Source	The IP Phone
Alarm Type	Other(0)
Probable Cause	Other(0)
Severity	Major
Additional Info	4 digit code
Corrective Action	-

27.3.10 IP Phone Web Successive Login Failure

IP Phone Web Successive Login Failure

Description	This alarm is raised when there are five successive failed login attempts to an IP phone's Web interface.		
SNMP Alarm	IPPhoneWebSuccessiveLoginFailure		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.59		
Alarm Title	IP Phone Web Successive Login Failure		
Alarm Source	The IP Phone		
Alarm Type	SecurityServiceOrMechanismViolation(9)		
Probable Cause	UnauthorizedAccessAttempt(73)		
Additional Info	-		
Alarm Severity	Condition	Alarm Text	Corrective Action
Major	Issued on the fifth successive failed attempt to log in to the phone's Web interface	-	<ul style="list-style-type: none"> After the alarm is cleared, try to login to the Web interface using the correct username and password. If you forget the login credentials, inform the network administrator.
Clear	There are no additional WEB login failed trials during a specific time period (60 seconds) after sending the alarm.	-	-

27.4 Searching for Alarms

You can search for alarms in the Alarms page. The 'Search' field enables the functionality. You can search by the following parameters:

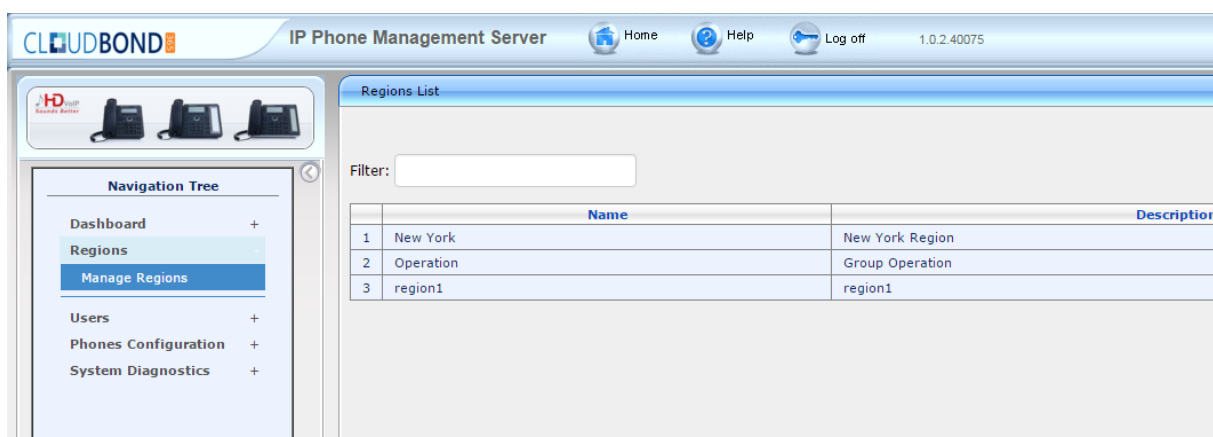
- alarm name
- a phone's MAC address
- a phone's IP address

27.5 Maintaining Regions

The Manage Regions page lets you maintain regions. You can perform the following actions:

- add a region
- edit region
- delete a region

Figure 27-9: Maintain Regions



Note: The main purpose of the Region/s is to group users in order to control the IP Phones.

27.6 Maintaining Users

The Manage Users page lets you maintain users. You can perform the following actions:

- Add a user
- Add a device to a user
- Edit user/device
- Delete a user/device
- Search for a device by region
- Search for a device by name



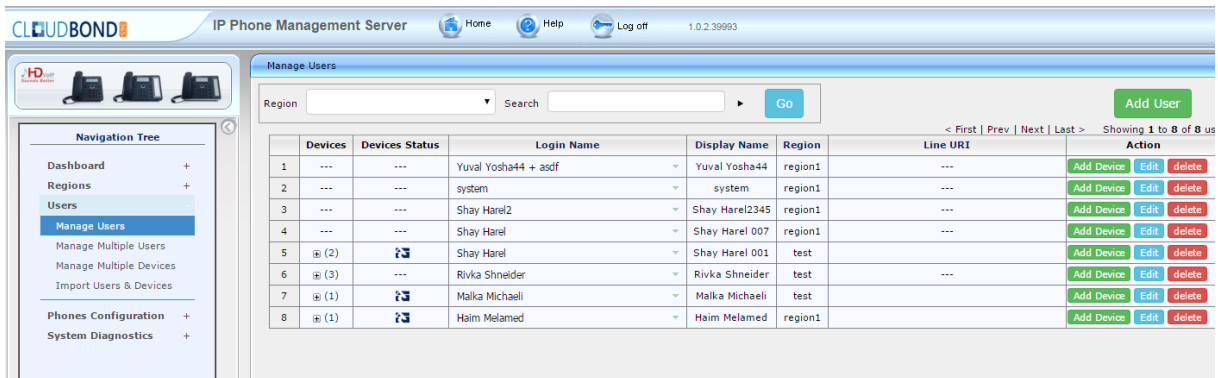
Note: In most cases adding users and devices is done automatically by the system, therefore you should not add a user or device on a regular basis

27.6.1 Adding a User

➤ To add a user to the Management Server:

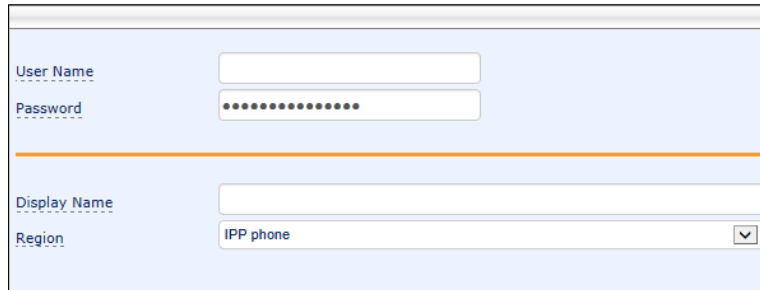
1. Access the 'Manage Users' page (**Management > Users > Users**):

Figure 27-10: Manage Users



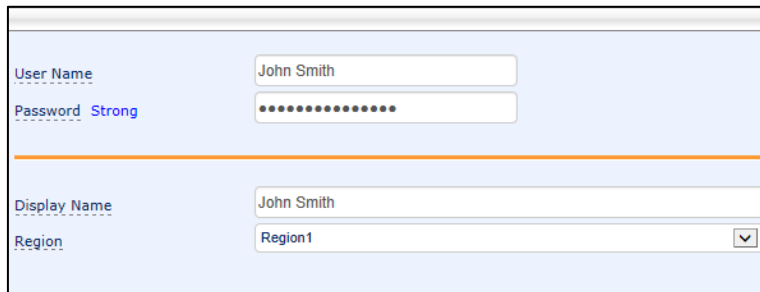
2. Click the **Add User** button (before adding phones to the IP phone management server you must add users); the following screen is displayed:

Figure 27-11: Add User



3. Define a name and password for the user.
4. Define the 'Display Name' and select a region from the 'Region' dropdown.

Figure 27-12: Add User Definitions



5. Click the **Submit** button; you're returned to the Manage Users page; locate the listed added user.

27.6.2 Adding a Phone

You can manually add a single phone to the server.

➤ **To add a phone:**

1. In the Manage Users page, click the **Add Device** button in the row of the listed added user; the following screen opens:

Figure 27-13: Add New Device to User

2. Enter the 'Display Name'. This is the name that will be displayed in the management server interface.
3. Click the **Submit** button.
4. Click **Add Device** (to associate the employee's name/line with the IP phone).
5. Enter the remaining characters of the 'MAC Address'. The prefix characters are displayed by default.
6. Click the **Submit** button; the following screen is displayed:

Figure 27-14: Prompt: Do you want to generate configuration files?

7. Click **Yes**.

Figure 27-15: Prompt: Do you want to update the device file?

8. Click **Yes**.

27.6.3 Editing a User

You can edit a user.

➤ **To edit a user:**

1. Click the **Edit** button in the row adjacent to the user; the Edit User screen opens, identical to that shown in [Figure 27-11](#).
2. Edit the same fields as when adding the device (see [Section 27.6.2](#)).

27.6.4 Deleting a User

You can delete a user.

➤ **To delete a user:**

- Click the **Delete** button in the row adjacent to the user; the user and device are removed.

27.7 Managing Multiple Users

The Manage Multiple Users page lets you easily perform a single operation on all or on many users simultaneously:

- Reset passwords
- Delete users
- Restart devices
- Generate IP phones configuration files
- Update configuration files
- Send a message to multiple phones

➤ **To manage multiple users:**

1. Access the 'Manage Multiple Users' page (**Management > Users > Manage Multiple Users**):

Figure 27-16: Manage Multiple Users


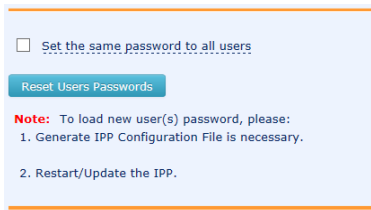
2. In the **Available Users** pane, select the users on which to perform the operation.
3. Click the right arrow (>) to add new users to the Selected Users pane. Click the left arrow (<) to remove selected users.

4. From the **Action** dropdown, select the required action.



Use the table below as reference.

Table 27-7: Managing Multiple Users - Actions

Action	Description
Set Users Region	 <p>Sets the region for users selected.</p>
Reset Users Passwords	 <p>Resets user's passwords. A random password is generated for each user. To generate a single password for all users selected, select the Set the same password to all users option.</p> <p>To load the new user passwords:</p> <ul style="list-style-type: none"> ■ Generate the phone's configuration file ■ Restart/Update the phone
Delete Users	Deletes users and applies a configurable 'Delay Time' (Default = 2 seconds) after each delete is performed.
Restart Devices	<p>Restarts devices. A reset command is sent to all selected devices. The commands are sent in batches; where each batch contains five devices with a delay of two minutes between each batch.</p> <p>From the dropdown, choose the type of restart:</p> <ul style="list-style-type: none"> ■ Graceful (default) ■ Force ■ Scheduled <p>Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart.</p>
Generate IP Phones Configuration Files	Generates new configuration files. Updates each phone with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you select the Updating IP Phones after generating files option. You can generate a private configuration file per user group, device group, or specific regions.
Update Configuration Files	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).

Action	Description
Send Message	<p>Let's you send a message to the LCDs of all user phones selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the LCD. Phones beep to alert users whenever there is an incoming message.</p> 

The page also lets you do the following:

- filter per region, before selecting the users on which to perform an action.

27.8 Maintaining Multiple Devices

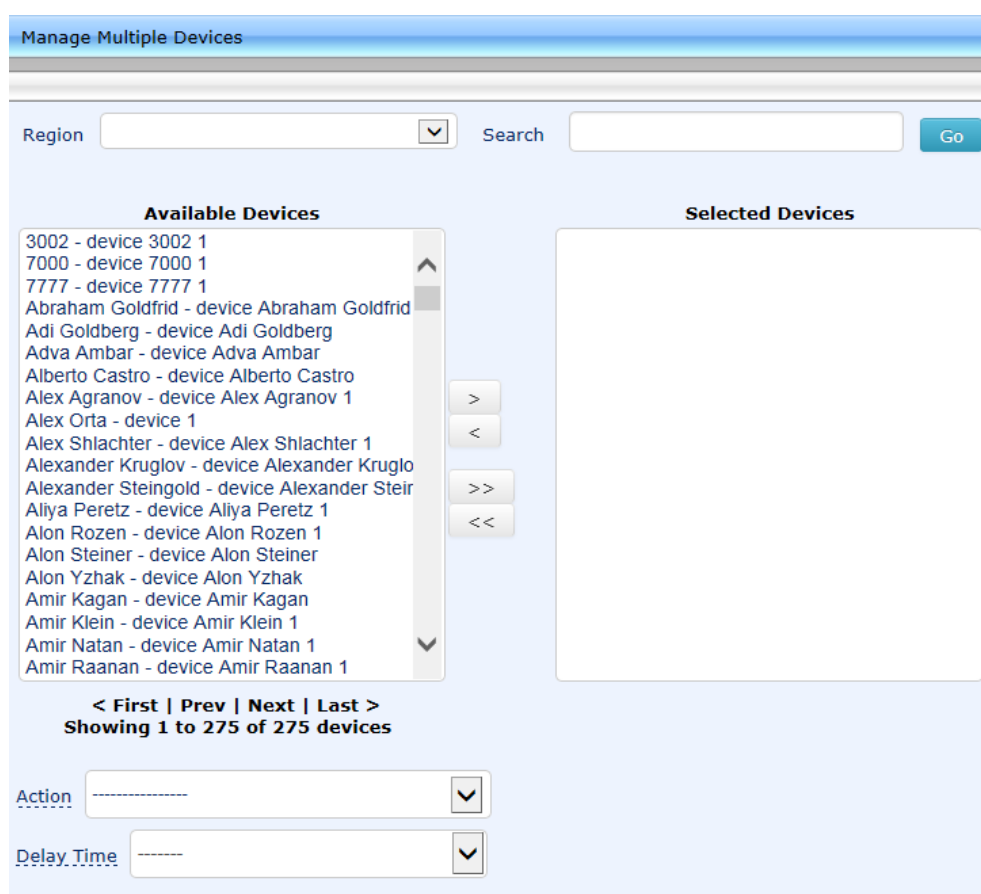
The Manage Multiple Devices page lets you perform a single operation on all or on many user devices. The page lets you do the following:

- Delete multiple devices
- Change IP phone type
- Change language
- Restart multiple devices
- Generate IP phones configuration files
- Update configuration files
- Send a message to multiple phones

➤ **To manage multiple devices:**

1. Access the 'Manage Multiple Users' page (**Management > Users > Manage Multiple Devices**):

Figure 27-17: Manage Multiple Devices

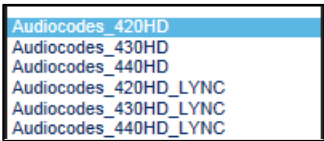
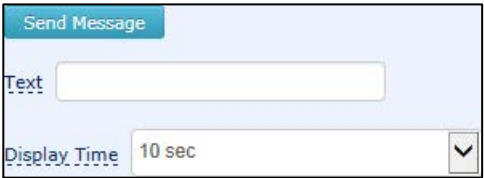


The devices are displayed in the following format:

1. You can search for devices by entering a string in the 'Search' field and then clicking **Go**.
2. You can filter the devices per region, before selecting those on which to perform an action.
3. In the Available Devices pane, select the devices on which to perform the action.
4. Click the right arrow → to add new devices to the Selected Devices pane, or use the left arrow ← to remove selected devices.

5. From the **Action** dropdown, select an action. Use the table below as reference.

Table 27-8: Managing Multiple Devices - Actions

Action	Description
Delete Devices	Deletes selected devices from the server applying a configurable 'Delay Time' (default = 2 seconds) in the process.
Change IP Phone Type	<p>You can change the phone model:</p>  <p>To view the usage of a model, click View Usage.</p> <p>To load a new phone model:</p> <ol style="list-style-type: none"> 1 Generate the phone's configuration file. 2 Restart/update the phone.
Change Language	<p>Changes the phone language. Select the language from the Language dropdown and click Change. To view the usage of a language, click View Usage.</p> <p>To load a new language:</p> <ol style="list-style-type: none"> 1 Generate the phone's configuration file. 2 Restart/update the phone.
Restart Devices	<p>Restarts online devices. Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart.</p> <p>From the dropdown, choose the type of restart:</p> <ul style="list-style-type: none"> ▪ Graceful (default) ▪ Force ▪ Scheduled
Generate IP Phone Configuration files	Generates new configuration files. Updates each phone with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you selected the Updating IP Phones after generating files option.
Update Configuration Files	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).
Send Message	<p>Let's you send a message to the LCDs of all user phones selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the LCD. Phones beep to alert users whenever there is an incoming message.</p> 

- **To update all existing configuration files according to the new template:**

- Use the **Generate IP Phones Configuration Files** option in the Manage Multiple Devices page.

This page is intentionally left blank.

28 Troubleshooting

You can display log files to help troubleshoot problems and determine the cause of the problem.

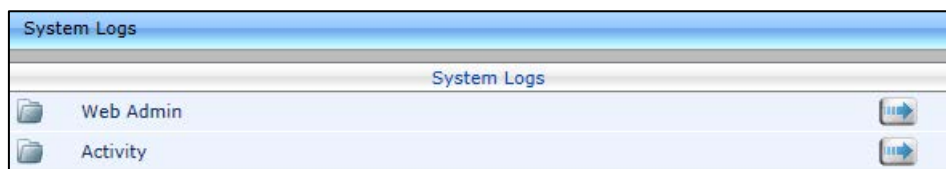
28.1 Displaying Log Files

This section describes how to display log files.

➤ **To display log files:**

1. Access the System Logs page (**System Diagnostics > System Logs**):

Figure 28-1: System Logs



2. Click the **Web Admin** arrow or the **Activity** arrow link.



Note:

- The Web Admin log displays recent actions performed in the user interface.
- The Activity log displays recent activities performed with the IPPhone Management server.

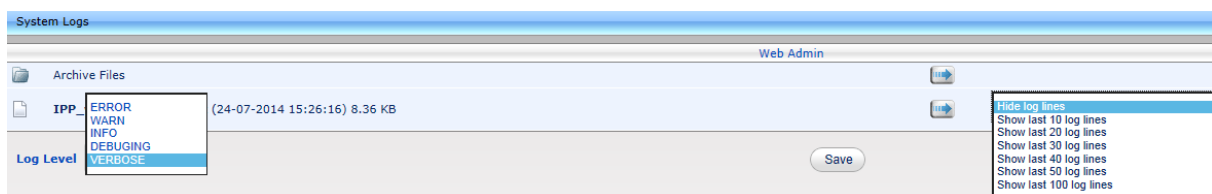
28.2 Displaying Web Admin Log Files

This section describes how to display Web Admin log files.

➤ **To display Web Admin log files:**

1. Click the **Web Admin** arrow link; the System Logs – Web Admin page opens:

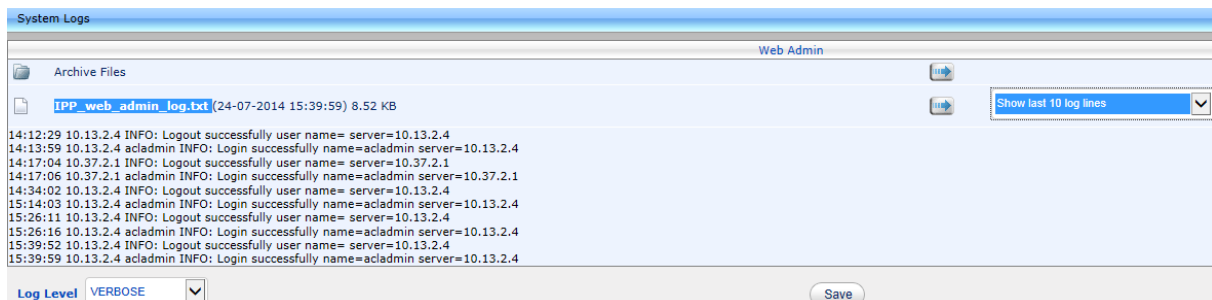
Figure 28-2: System Logs – Web Admin Level Log



2. From the 'Log Level' dropdown list, select one of the following:
 - ERROR
 - WARN
 - INFO
 - DEBUGGING
 - VERBOSE (default) – All Levels (Detailed)
3. From the 'Hide log lines' dropdown list, select one of the following:
 - Hide log lines
 - Show last 10 log lines
 - Show last 20 log lines

- Show last 30 log lines
 - Show last 40 log lines
 - Show last 50 log lines
 - Show last 100 log lines
4. View the generated IPP_web_admin_log.txt file.

Figure 28-3: System Logs – Web Admin Level txt Log File Displayed



5. Click **Save** to save the file and share it with others.

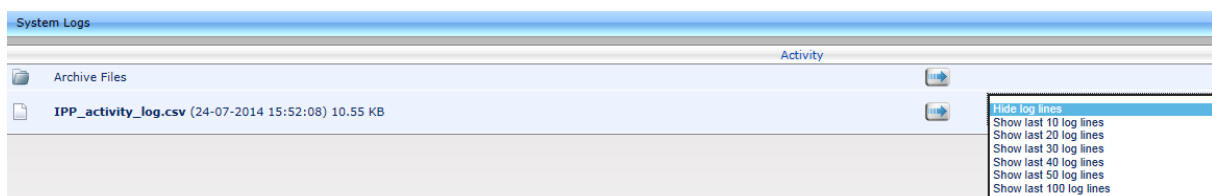
28.3 Displaying Activity Log Files

This section describes how to display activity log files.

➤ To display Activity log files:

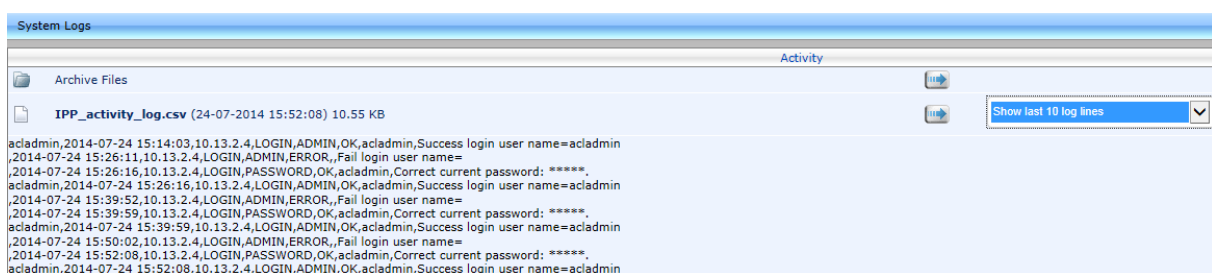
1. Click the **Activity** arrow; the System Logs – Activity page opens:

Figure 28-4: System Logs – Activity Log



2. From the 'Hide log lines' dropdown list, select one of the following:
 - Hide log lines
 - Show last 10 log lines
 - Show last 20 log lines
 - Show last 30 log lines
 - Show last 40 log lines
 - Show last 50 log lines
 - Show last 100 log lines

Figure 28-5: System Logs – Activity Level txt Log File Displayed



29 Preparing a Configuration File

You can prepare a configuration file from a template in the IP Phone Management Server UI. The template defines how a phone's configuration file is generated. The phones retrieve the cfg file from the Provisioning server.



Note: Before plugging phones into the network, define parameter placeholder's values for criteria such as region and phone model, to maintain an automatic provisioning scheme.

29.1 Selecting a Configuration Template

Configuration templates are available as follows:

- Per phone model
- Per model for Microsoft ® Skype for Business Desktop phones















Depending on the models and the server in the enterprise, select a template for the following phone models:

- AudioCodes 420HD Skype for Business Desktop phone
- AudioCodes 430HD Skype for Business Desktop phone
- AudioCodes 440HD Skype for Business Desktop phone

➤ **To select a configuration template:**

- In the navigation tree, access the IP Phones Configuration Templates page (**Phones Configuration > Templates**):

Figure 29-1: IP Phone Models Configuration Templates

	Audiocodes 405		 Edit
	Audiocodes 420HD	The 420HD SIP IP Phone is a high-definition IP phone with an affordable price.	 Edit
	Audiocodes 430HD	The 430HD SIP IP Phone is an advanced, mid-range enterprise IP Phone.	 Edit
	Audiocodes 440HD	The template file of Audiocodes 440HD is overwritten. The file location is in the system.	 Edit
	Audiocodes 420HD LYNC	The template file of Audiocodes 420HD LYNC is overwritten. The file location is in the system.	 Edit
	Audiocodes 430HD LYNC	The template file of Audiocodes 430HD LYNC is overwritten. The file location is in the system.	 Edit
	Audiocodes 440HD LYNC	The template file of Audiocodes 440HD LYNC is overwritten. The file location is in the system.	 Edit

29.2 Editing a Configuration Template

You can edit a phone model's template, however typically it's unnecessary to change it.

➤ **To edit a template:**

1. In the IP Phones Configuration Templates page, click the link of the IP phone model, or its **Edit** icon; this dialog is displayed:

Figure 29-2: IP Phone Configuration Template

IP Phone Audiocodes_430HD Configuration Template	
IP Phone Audiocodes_430HD Configuration Template	
Model:	Audiocodes_430HD
Description:	The 430HD SIP IP Phone is an advanced, mid-range enterprise IP Phone.
<div> <div>Edit:</div> <div>Edit configuration template</div> </div>	
<div> <div>Download:</div> <div>Download configuration template</div> </div>	
<div> <div>Upload:</div> <div>Upload configuration template</div> <div>1</div> </div>	
<div> <div>Generate Global Configuration Template</div> <div>Show Place Holders</div> </div>	
<div>⊕ Advanced</div>	

1 = generic templates can be modified and generated per phone model

2. Click the **Edit configuration template** button; the template opens in an integral editor:

Figure 29-3: Edit Template

The 'Edit Template' dialog box contains a text area with the following XML content:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ipphonetemplate>
  <type>audiocodes_430HD</type>
  <description>AudioCodes 430HD LYNC</description>

  <file_config>
    <type>global_file</type>
    <profile>global</profile>
    <encrypt_mode>0</encrypt_mode>
    <name>Audiocodes_430HD_global_LYNC.cfg</name>
    <destinationDir>%ITCS_destination%</destinationDir>
    <data>
<![CDATA[management/telnet/enabled=0
ems_server/keep_alive_period=60
ems_server/provisioning/url=http://%ITCS_ServerIP%:8081/
lync/BToE/CheckNetwork=0
lync/BToE/name=AudioCodes 400HD Phone
lync/moh/url=
network/lan/dhcp/domain_name/enabled=1
network/lan/dhcp/gateway/enabled=1
```

At the bottom right of the dialog are 'Save' and 'Close' buttons.

3. Edit the template and then click **Save**; the modified template is saved in its URL location on the server, for example, **<http://10.59.0.200/ipp/admin/AudioCodes.php>**. See the phone's *Administrator's Manual* for parameter descriptions. See also Section 29.2.8.

29.2.1 About the Template File

The template is an xml file. It defines how a phone's configuration file will be generated. The template shows the following sections:

- The upper section defines the *global* parameters that will be in the *global* configuration file.
- The lower section defines the *private user* parameters that will be in the *device* configuration file.

29.2.2 Global Parameters

Global parameters apply to *all* phones in the enterprise network. The **ems_server/provisioning/url** parameter, for example, is a global parameter because all phones in the enterprise network point to the same Provisioning server.

Only one file is generated for each template, so every change in the global file will automatically impact all the phones from this template.

29.2.3 User-Specific Parameters

Private user parameters apply to specific phones. They can pull global parameters using the template's 'include' function. The **network/lan/vlan/mode=%ITCS_VLANMode%** parameter, for example, is a user parameter because each user in an enterprise is defined in a user-specific VLAN.

These parameters will be stored in the MAC.cfg file for each device.

29.2.4 Restoring a Template to the Default

You can restore a template to the factory default at any time.

➤ To restore a template to the default:

- Click the **Restore to default** button (displayed only if a change was made); the phone model and its description are displayed.

29.2.5 Downloading a Template

You can download a template, for example, in order to edit it in a PC-based editor.

➤ To download a template:

- Click the **Download configuration template** button and save the *xml* file in a folder on your PC.

29.2.6 Uploading an Edited Template

You can upload a template, for example, after editing it in a PC-based editor.

➤ To upload an edited template:

- Click the **Upload configuration template** button and browse to the *xml* template file on your PC. The file will be the new template for the phone model.

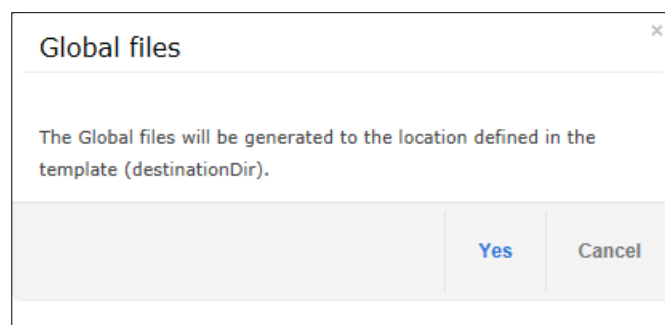
29.2.7 Generating an Edited Template

After editing a template if necessary, you must generate the edited template.

➤ To generate an edited template:

1. In the IP Phone Configuration Template page, click the **Generate Configuration Template** button; this prompt is displayed:

Figure 29-4: Generate Configuration Template – 'Global files' Prompt



2. Click **Yes**; the generated template reflecting the edit/s is available in the IP Phone Models Configuration Templates page.

29.2.8 Defining Template Placeholders

Templates include *placeholders* whose values you can define. After defining values, the placeholders are automatically resolved when you generate the template, for example, the placeholder `%ITCS_TimeZoneLocation%` is replaced with the local time zone in a globally distributed enterprise's phones. Placeholders can be defined per system, region, IP phone model, and devices.

➤ **To show placeholders:**

1. In the IP Phones Configuration Templates page (**Phones Configuration > Templates**), click the **Edit** button adjacent to the phone model; this screen opens:

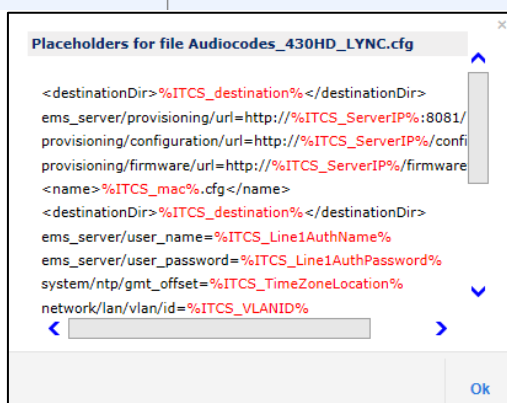
Figure 29-5: Configuration Template

IP Phone Audiocodes_420HD Configuration Template	
IP Phone Audiocodes_420HD Configuration Template	
Model:	Audiocodes_420HD
Description:	The 420HD SIP IP Phone is a high-definition IP phone with an affordable price.
<hr/>	
Edit:	<button>Edit configuration template</button>
Download:	<button>Download configuration template</button>
Upload:	<button>Upload configuration template</button>
<hr/>	
<div><button>Generate Global Configuration Template</button><button>Show Place Holders</button></div>	
<hr/>	
⊕ Advanced	

2. Click **Show Placeholders** button.

Figure 29-6: Show Placeholders

Templates Place Holders			
Templates Place Holders			
Template Model	Placeholder	IPP Parameter	
Audiocodes_420HD_LYNC	%ITCS_destination%		configuration files location on the disk
Audiocodes_420HD_LYNC	%ITCS_ServerIP%	provisioning/configuration/url	
Audiocodes_420HD_LYNC	%ITCS_mac%		The IP Phone MAC Address
Audiocodes_420HD_LYNC	%ITCS_Line1AuthName%	ems_server/user_name	The IP Phone authentication name - user M
Audiocodes_420HD_LYNC	%ITCS_Line1AuthPassword%	ems_server/user_password	The IP Phone authentication password
Audiocodes_420HD_LYNC	%ITCS_FirmwareFile%	provisioning/firmware/url	
Audiocodes_420HD_LYNC	%ITCS_TimeZoneLocation%	system/ntp/gmt_offset	Time Zone - Default is 00:00 Enables the NTP server from which the phor [0] Disable [1] Enable - obtains the time information fro
Audiocodes_420HD_LYNC	%ITCS_VLANID%	network/lan/vlan/id	VLAN ID - Only displayed when the 'VLAN The valid range is 0 to 4096. The default VL
Audiocodes_420HD_LYNC	%ITCS_VLANMode%	network/lan/vlan/mode	VLAN Discovery Mode - etermines the VLAN [Disable] Disable [Manual] Manual Configuration of LAN - Stat [CDP] Automatic Configuration of VLAN - VL [LLDP] Automatic Configuration of VLAN - VL [CDP_LLDP] Automatic Configuration of VLA
Audiocodes_420HD_LYNC	%ITCS_VLANPriority%	network/lan/vlan/priority	VLAN Priority - Only displayed when the '\ Defines the priority of traffic pertaining to th The valid range is 0 to 7 (where 7 is the higl
			Phone Display Language - Determines the l [English] English (default) [Spanish] Spanish [Russian] Russian [Portuguese] Portuguese. Displayed only if i [German] German



The figure above shows placeholders that are currently defined in the xml Configuration Template file for the 430HD Skype for Business Desktop phone model. There are four kinds of placeholders: (1) System (2) Phone Model (3) Region (4) Devices.

- To manage an available placeholder, see Section [29.2.8.1](#)
- To add/edit/delete a phone model placeholder, see Section [29.2.8.1.3](#)
- To add/edit/delete a region placeholder, see Section [29.2.8.2](#)
- To add/edit/delete a device placeholder, see Section [29.2.8.3](#)

29.2.8.1 Default Placeholders Values

You can define placeholders. Before defining values for placeholders, you can view the default placeholders values defined.

➤ **To view default placeholders values defined:**

- Access the Default Placeholders Values page (**Phones Configuration > Default Placeholders Values**):

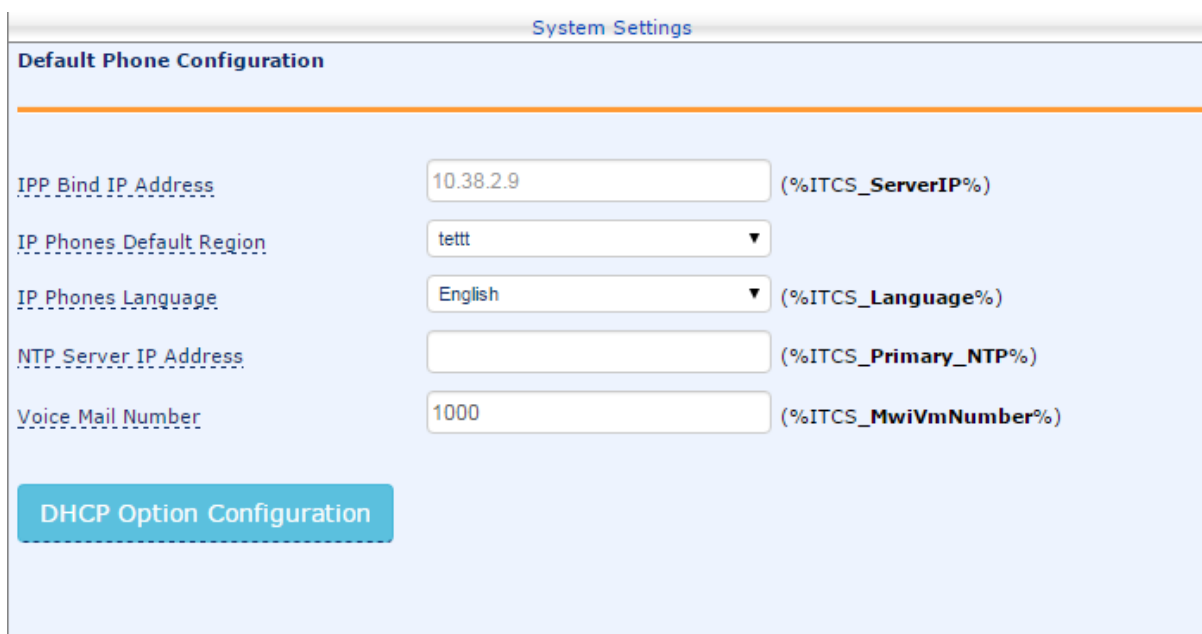
Figure 29-7: Default Placeholders Values

Placeholder	Value	Description
%ITCS_ServerIP%	10.38.2.9	
%ITCS_TimeZoneName%	FET	The IP CloudBond 365 TimeZone/Country name
%ITCS_TimeZoneLocation%	+03:00	The IP CloudBond 365 TimeZone offset format is +/-xx:xx
%ITCS_DayLightSwitch%	0	
%ITCS_MwiVmNumber%	1000	The Voice Mail number
%ITCS_Version%	1447689670	
%ITCS_Language%	English	Determines IPP display user interface language: English, Spanish
%ITCS_SRTP%	0	
%ITCS_IPPhoneUsername%	admin	The IPPhone administration user name
%ITCS_IPPhonePassword%	1234	The IPPhone administration password
%ITCS_destination%	C:/audiocodes/Onebox4IPP/ipp_files/generate/	configuration files location on the disk

➤ **To define a placeholder value:**

1. Access the System Settings page (**Phones Configuration > System Settings**).

Figure 29-8: System Settings



2. Define values for available placeholders according to your enterprise IP phone configuration requirements, and then click the **Submit** button. Use the table below as reference. Except for the 'IP Phones Language' parameter.

Table 29-1: System Settings

Parameter	Description
Server FQDN	[Recommended] Point phones to the CloudBond server using the server's name instead of its IP address. If phones are pointed to the CloudBond server's IP address, then if the server is moved due to organizational changes within the enterprise, all phones are disconnected from it. Pointing using the server's name prevents this from occurring.
Default Region	The system uses this region when creating a user after the phone sign-in and the user does not exist.
IP Phones Language	From the dropdown select the language you want displayed in the phones' LCD screens: English (default), French , German , Hebrew , Italian , Polish , Portuguese , Russian , Spanish or Ukraine .
NTP Server IP Address	Enter the IP address of the Network Time Protocol (NTP) server from which the phones can retrieve the time.
Voice Mail Number	Enter the number of the enterprise's exchange. Configuration depends on the enterprise environment, specifically, on which exchange the enterprise has setup. If the enterprise has a Skype for Business environment, ignore this parameter. Default=1000.
DHCP Option Configuration	Click this button if your phones are operating directly with a DHCP server without the mediation of an HTTP proxy which is required when the phones are behind a NAT. See Section 29.2.8.1.1.

3. View newly defined placeholder values in the IP Phone Placeholders page (**Phones Configuration > System Placeholders**).

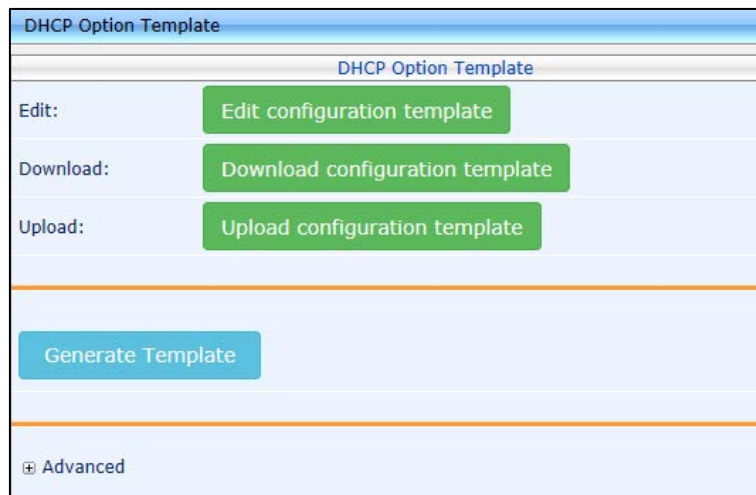
29.2.8.1.1 Configuring DHCP Option

Users can opt to edit the initial DHCP Options 160 cfg file. Choose the **DHCP Option Configuration** button if your phones are communicating directly with a DHCP server without the mediation of an HTTP proxy, which is required when the phones are located behind a NAT.

➤ **To configure DHCP Option:**

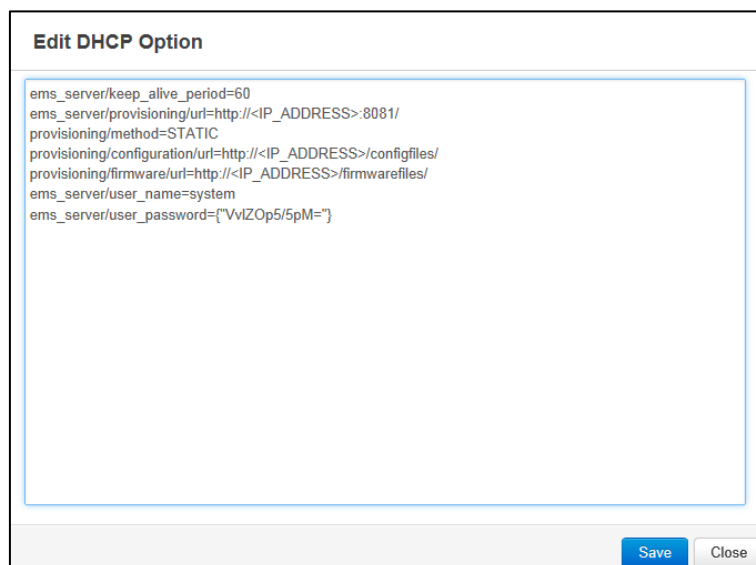
1. Access the System Settings page (**Phones Configuration > System Settings**).
2. Click the **DHCP Option Configuration** button; the DHCP Option Template dialog opens.

Figure 29-9: DHCP Option Template



3. Click the **Edit configuration template** button.

Figure 29-10: Edit DHCP Option



4. Configure the DHCP option using the table below as reference.

Table 29-2: DHCP Option

Parameter	Description
Keep alive period	You can configure how often the phones generate a Keep-alive trap towards the IP Phone Management Server. Default: Every 60 minutes. It's advisable to configure a period that does not exceed an hour. The management system may incorrectly determine that the phone is disconnected if a period of more than an hour is configured.
Provisioning URL	Defines the URL (including IP address and port) of the Provisioning server.
Provisioning Method	Defines the provisioning method, i.e., STATIC or Dynamic (DHCP). Do not change this setting. The setting must remain STATIC. If not, the phone will continuously perform restarts.
Provisioning Configuration URL	Defines the URL of the location of the configuration files (including IP address and port) in the Provisioning server.
Provisioning Firmware URL	Defines the URL of the location of the firmware files (including IP address and port) in the Provisioning server.
User Name	Defines the user name for the REST API. Default: System . Later, each phone receives its own unique user name. See Section 26.4.
User Password	Encrypted. Defines the user password for the REST API. Default: System . Later, each phone receives its own unique user password.



Note: You can always restore these settings to their defaults if necessary, however it's advisable to leave these settings unchanged.

5. Click **Save**.

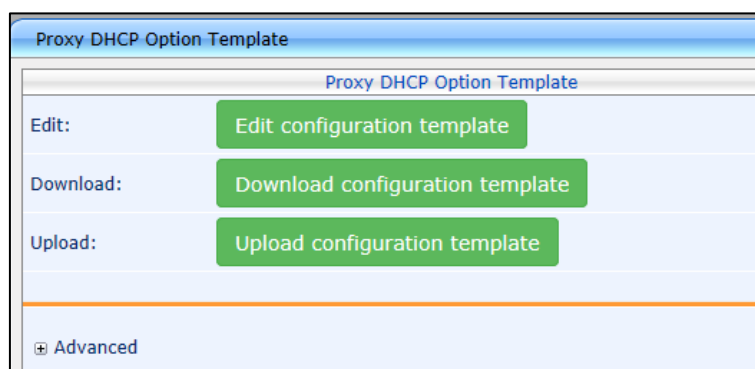
29.2.8.1.2 Configuring the HTTP Proxy

Users can opt to edit the initial DHCP Options 160 cfg file. Choose the **HTTP Proxy Configuration** button if your phones are communicating with an HTTP proxy, which is required when the phones are located behind a NAT.

➤ **To configure the HTTP proxy:**

1. Access the System Settings page (**Phones Configuration > System Settings**).
2. Click the **HTTP Proxy Configuration** button; the Proxy DHCP Option Template screen opens.

Figure 29-11: Proxy DHCP Option Template



3. Click the **Edit configuration template** button; the same Edit DHCP Option screen shown in the previous section opens. Edit as described in the previous section.
4. Click **Save**.

29.2.8.1.3 Phone Model Placeholders

You can edit the values defined for an existing phone model placeholder and/or you can add a new model placeholder.

29.2.8.1.4 Editing Phone Model Placeholders

You can edit the values for existing phone model placeholders.

- **To edit values for existing phone model placeholders:**
 - Open the Phone Model Placeholders page (Phones Configuration>Phone Model Placeholders):

Figure 29-12: Phone Model Placeholders

	Placeholder	Value	Description	
1	%ITCS_DayLightActivate%	Disable	Day Light Activate - Enable/Disable	Edit Delete
2	%ITCS_DayLightEndDay%	14	Day Light End Day	Edit Delete
3	%ITCS_DayLightEndMonth%	9	Day Light End Month	Edit Delete
4	%ITCS_DayLightStartDay%	26	Day Light Start Day	Edit Delete
5	%ITCS_DayLightStartMonth%	3	Day Light Start Month	Edit Delete
6	%ITCS_FirmwareFile%		Firmware File Name	Edit Delete
7	%ITCS_SipDigitMap%	**xxxx	Digit map for the IPP e.g. xxxx for 4 digit ...	Edit

The page shows the placeholders and their values defined for a phone model.

- **To edit a value of an existing phone model placeholder:**
 1. Click the **Edit** button; the 'Edit placeholder' screen is displayed:

Figure 29-13: Edit Phone Model Placeholder

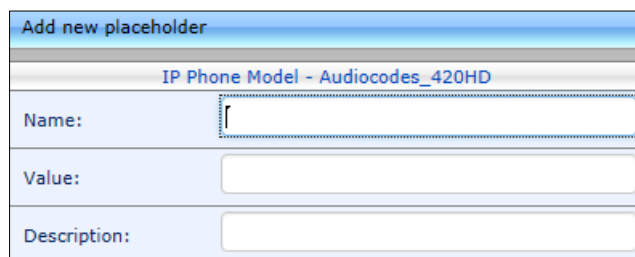
Edit placeholder	
IP Phone Model - Audiocodes_420HD	
Name:	DayLightActivate
Value:	Disable
Description:	Day Light Activate - Enable/Disable

2. In the 'Name' field, you can edit the name of the placeholder.
3. In the 'Value' field, you can edit the value of the placeholder.
4. In the 'Description' field, you can edit the placeholder description.
5. Click **Submit**; the edited placeholder is added to the table.

29.2.8.1.5 Adding a New Phone Model Placeholder

You can add a new phone model placeholder. A new placeholder can be added and assigned with a new value.

- **To add a new phone model placeholder:**
 1. Open the Phone Model Placeholders page (**Phones Configuration > Phone Model Placeholders**):
 2. From the **IP Phone Model** dropdown in the Phone Model Placeholders page, select the model, e.g., IP Phone Model – Audiocodes_420HD.
 3. Click the **Add new placeholder** button.

Figure 29-14: Add New Phone Model Placeholder


4. In the 'Name' field, enter the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. In the 'Description' field, enter a short description for the new placeholder.
7. Click **Submit**; the new placeholder is added to the table.

29.2.8.2 Region Placeholders

You can edit values for existing region placeholders and/or you can add new region placeholders.

29.2.8.2.1 Editing Region Placeholders

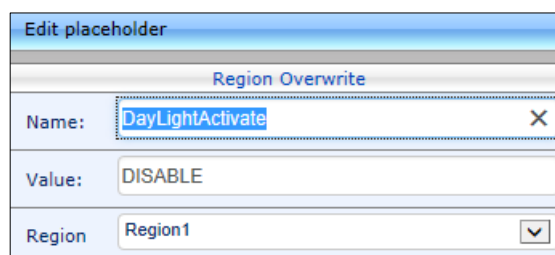
You can edit the values for existing region placeholders.

- **To edit values for existing region placeholders:**
 - Access the Manage Region Placeholders page (**Phones Configuration > Region Placeholders**):

Figure 29-15: Manage Region Placeholders


	Placeholder	Value	Region	Edit	Delete
1	%ITCS_DayLightActivate%	DISABLE	Region1	Edit	Delete
2	%ITCS_KeepAlivePeriod%	5	Region1	Edit	Delete
3	%ITCS_SpeedDialName1%	123K	Region1	Edit	Delete
4	%ITCS_SpeedDialName2%	Marina	Region1	Edit	Delete
5	%ITCS_SpeedDialNumber1%	4006	Region1	Edit	Delete
6	%ITCS_SpeedDialNumber2%	5555	Region1	Edit	Delete
7	%ITCS_test2%	test3	Region1	Edit	Delete

- **To edit a value of an existing region placeholder:**
 1. Click the **Edit** button; the 'Edit placeholder' screen is displayed:

Figure 29-16: Edit Region Placeholder


2. In the 'Name' field, you can edit the name of the placeholder.
3. In the 'Value' field, you can edit the value of the placeholder.
4. From the 'Region' dropdown, you can select another region.
5. Click **Submit**; the edited placeholder is added to the table.

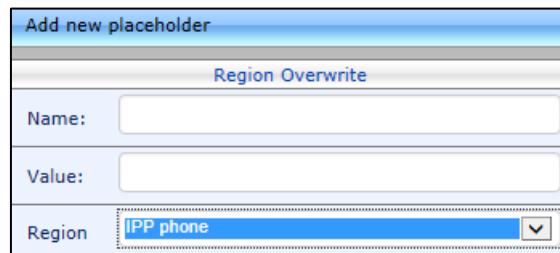
29.2.8.2 Adding a New Region Placeholder

You can add a new region placeholder.

➤ **To add a new region placeholder:**

1. Access the Manage Region Placeholders page (**Phones Configuration > Region Placeholders**):
2. From the **Region** dropdown, select a region, and then click the **Add new placeholder** button.

Figure 29-17: Add New Region Placeholder



Add new placeholder	
Region Overwrite	
Name:	<input type="text"/>
Value:	<input type="text"/>
Region	IPP phone ▼

3. In the 'Name' field, enter the name of the new placeholder.
4. In the 'Value' field, enter the value of the new placeholder.
5. From the 'Region' dropdown, select a new region.
6. Click **Submit**; the new placeholder is added to the table.

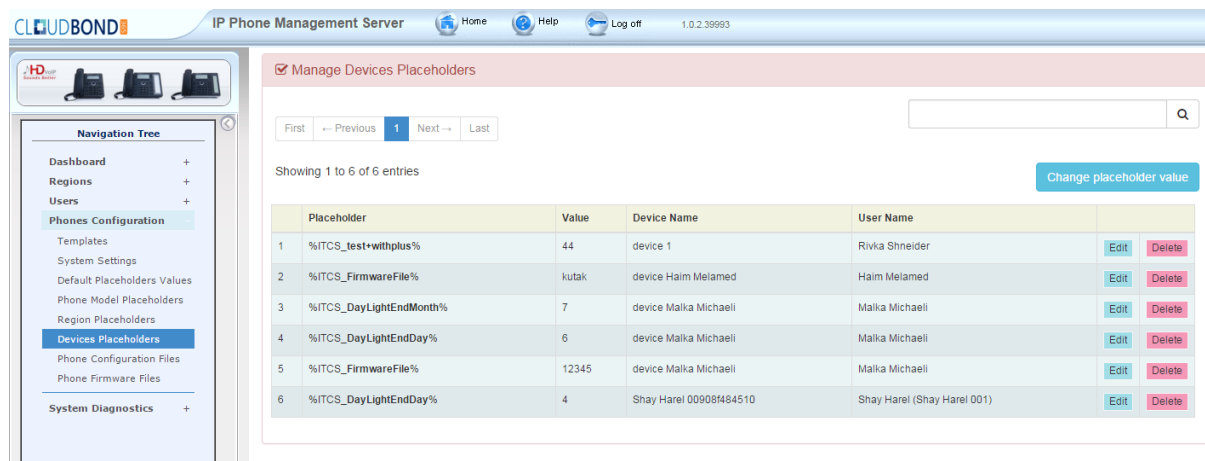
29.2.8.3 Devices Placeholders

You can change placeholder's values for specific phones, for example, you can change placeholder's values for the CEO's phone. You can also edit a phone's placeholder's values.

29.2.8.3.1 Changing a Device Placeholder Value

- To change a device placeholder value:
- 1. Access the Manage Devices Placeholders page (**Phones Configuration > Devices Placeholders**):

Figure 29-18: Manage Devices Placeholders



Placeholder	Value	Device Name	User Name		
1 %TCS_test+withplus%	44	device 1	Rivka Shneider	Edit	Delete
2 %TCS_FirmwareFile%	kutak	device Haim Melamed	Haim Melamed	Edit	Delete
3 %TCS_DayLightEndMonth%	7	device Malka Michaeli	Malka Michaeli	Edit	Delete
4 %TCS_DayLightEndDay%	6	device Malka Michaeli	Malka Michaeli	Edit	Delete
5 %TCS_FirmwareFile%	12345	device Malka Michaeli	Malka Michaeli	Edit	Delete
6 %TCS_DayLightEndDay%	4	Shay Harel 00908484510	Shay Harel (Shay Harel 001)	Edit	Delete



Tip: Use the 'Filter' field to quickly find a specific device if there are many devices listed. You can search for a device by its name or by its extension.

- 2. Click the **Change placeholder value** button; the Change IP Phone Device Placeholder screen opens.

Figure 29-19: Change IP Phone Device Placeholder



Change IP Phone Device Placeholder

Device 

(IP Phone Model)

Key

(Default Value)

Overwrite Value

- 3. From the **Device** dropdown, select the device.

Figure 29-20: Change IP Phone Device Placeholder – Selecting the Device

Change IP Phone Device Placeholder

Change IP Phone Device Placeholder

Please select a device

First ← 1 → Last

Enter device name

Showing 1 to 7 of 7 entries

Name	Display Name
Rivka Shneider	device 1
Rivka Shneider	device 2
Haim Melamed	device Haim Melamed
Malka Michaeli	device Malka Michaeli
Rivka Shneider	Rivka - device 3
Shay Harel (Shay Harel 001)	Shay Harel 00908f484510
Shay Harel (Shay Harel 001)	Shay Harel 00908f484510(1)

Note: Click on the table row to select device

Figure 29-21: Edit IP Phone Device Placeholder

Showing 1 to 7 of 7 entries

Name	Display Name
Rivka Shneider	device 1
Rivka Shneider	device 2
Haim Melamed	device Haim Melamed
Malka Michaeli	device Malka Michaeli
Rivka Shneider	Rivka - device 3
Shay Harel (Shay Harel 001)	Shay Harel 00908f484510
Shay Harel (Shay Harel 001)	Shay Harel 00908f484510(1)

Note: Click on the table row to select device

Device  device 2 - Rivka Shneider

(IP Phone Model **Audiocodes_420HD_LYNC**)

Key

(Default Value ****xxxx**)

Overwrite Value

- From the **Key** dropdown, choose the phone configuration key.
- Enter the device's overwrite value in the 'Overwrite Value' field, and then click the **Submit** button.

29.2.8.3.2 Editing a Device Placeholder Value

You can edit a device placeholder value.

➤ **To edit a device placeholder value:**

- Access the Manage Devices Placeholders page (**Phones Configuration > Devices Placeholders**).
- Click the **Edit** button; the 'Edit placeholder' screen is displayed, as shown above.
- In the 'Overwrite Value' field, you enter a new value.
- Click **Submit**; the edited device placeholder is added to the table.



Note: The new overwrite value is not automatically generated in the device IP phone configuration file. To generate the new device in the IP phone configuration template file, click the **Generate Configuration Template** button in the Templates page (**Phones Configuration > Templates**).

29.3 Managing Configuration Files

You can manage IP phones configuration files. All cfg files are created and located on the CloudBond server. You can view and manage storage and upload and delete files from storage. To avoid network congestion, a delay feature enables an interval between each installation.

➤ To manage IP phone configuration files:

- Access the Manage Configuration Files page (**Phones Configuration > Phone Configuration Files**).

Figure 29-22: Manage Configuration Files

	Name	Size	Date	
<input type="checkbox"/>	009080556x30.cfg	9.4 KB	August 10, 2014, 4:46 pm	Download
<input type="checkbox"/>	009080564x30.cfg	6.25 KB	August 10, 2014, 3:33 pm	Download
<input type="checkbox"/>	AudioCodes_420HD_global_GENERIC.cfg	3.01 KB	August 10, 2014, 3:22 pm	Download
<input type="checkbox"/>	AudioCodes_430HD_global_LYNC.cfg	2 KB	August 10, 2014, 3:33 pm	Download
<input type="checkbox"/> Select All				
<input type="button" value="Delete Selected Files"/>				

In this page you can do the following:

- Filter by filename the cfg configuration files listed.
- Browse to a location on your PC and upload a cfg configuration file.
- Select and delete any or all of the cfg configuration files listed.
- Open any of the cfg configuration files listed in an editor.
- Save any of the cfg configuration files listed.
- Download any of the cfg configuration files listed.
- View all configuration files currently located on the server (global configuration files, company directory configuration files, and IP phone configuration files).

29.4 Managing Phone Firmware Files

You can manage the phones' img firmware files.

➤ **To manage the img firmware files:**

- Access the Phone Firmware Files page (**Phones Configuration > Phone Firmware Files**).

Figure 29-23: Phone Firmware Files

Phone firmware files					
					Add new IP Phone firmware
	Name	Description	Version	File Name	
1	420HD_test	test	420HD2.2.0.7	420HD_test.img	Edit Delete
2	Alan_FW	test	440HDUC_2.0.9.65	Alan_FW.img	Edit Delete
3	409HD	409HD - default firmware			Edit Delete
4	430HD	440HD - default firmware			Edit Delete
5	440HD	440HD - default firmware	440HDUC_2.0.9.65	440HD.img	Edit Delete
6	test	test desc	430HD2.0.2.63_ems	test.img	Edit Delete
7	420_test2	420	420HDUC_2.0.9.50	420_test2.img	Edit Delete

In this page you can do the following:

- View all img firmware files currently located on the server
- Add a new IP phone firmware file. Note that if default names are used (e.g., 420HDimg), all devices of this type will automatically use it.
- Filter the img firmware files listed by filename. img.
- Determine from the phone's name if it does not have firmware loaded – it will be **red**-coded. If so, you must upload the phone's img firmware file that you obtained from AudioCodes, to the CloudBond Provisioning server:
 - Click the name of the phone; this screen opens:

Figure 29-24: img Firmware File Download/Upload

IP Phone 420HD_test Firmware


IP Phone 420HD_test Firmware

Name: 420HD_test
 Description: test
 Version: 420HD2.2.0.7
 File Name: 420HD_test.img

Download: [Download configuration firmware](#)
 Upload: [Upload configuration firmware](#)

- Click the **Upload firmware** button, and then navigate to the img file you received from AudioCodes and save it on the CloudBond Provisioning server. You can perform this part of the installation procedure before or after configuring your enterprise's DHCP server with DHCP Option 160 (see also Section 26.2).
- Download a phone's img firmware file to the PC. Click the phone's Name; the screen shown in Figure 29-23 opens. Click the **Download firmware** button.
 - Edit a phone's img firmware file. Click the name or click the **Edit** button in the row.
 - Delete any img firmware file listed. Click the **Delete** button in the row.

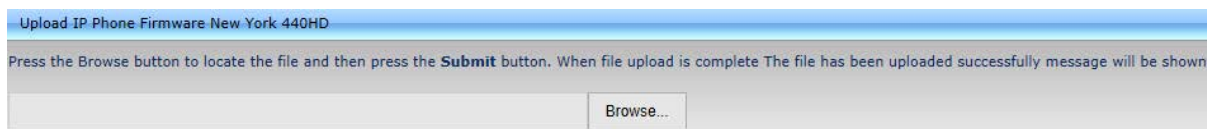
- Manage img firmware files by grouping them.
- a. Click the **Add new IP Phone firmware** button.

Figure 29-25: Add IP Phone Firmware

- b. Define an intuitive 'Name' and 'Description' to facilitate easy identification. You can leave the 'Version' field empty, and then click the **Submit** button; this screen is displayed:

Figure 29-26: Upload Configuration Firmware

- c. Click **Upload firmware**; this screen is displayed:

Figure 29-27: Browse to Firmware

- d. Click **Browse**, navigate to the img file, and then click the **Submit** button; the 'Version' field is populated and the img file is uploaded to the phone.

This page is intentionally left blank.

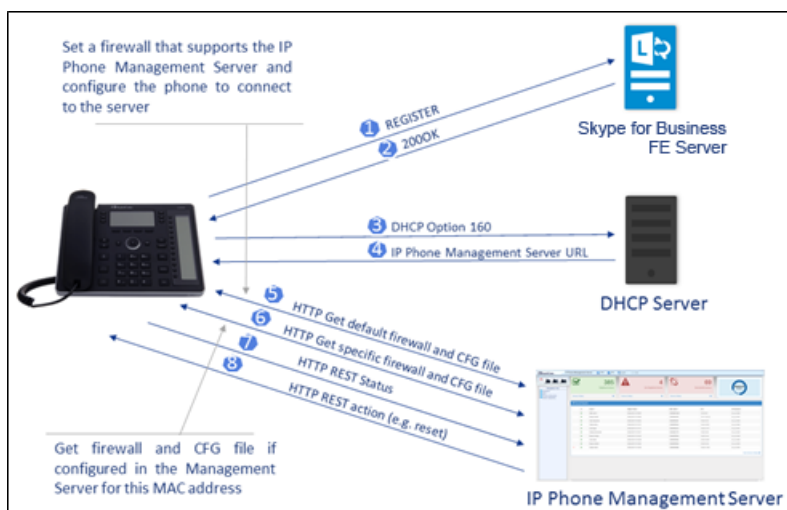
30 Provisioning Flows

This chapter illustrates the provisioning flows between phones and IP Phone Management server.

30.1 Skype for Business Desktop Phones

The figure below shows the provisioning flow between the Skype for Business Desktop phone and the IP Phone Management server.

Figure 30-1: Skype for Business Desktop Phone



This page is intentionally left blank.

31 Ports Required for IP Phone Management

The table below shows the firewall ports configuration required for IP phone management to set up, configure, and maintain AudioCodes IP phones in an enterprise network, from a single centralized point.

Table 31-1: Ports Required for IP Phone Management

Connection	Port Type	Port Number	Purpose	Port Side / Flow Direction
CloudBond ↔ IP Phone Management Server	TCP (HTTP)	80	HTTP connection between the CloudBond server and the IP Phone Manager Web browser that is used for Web management, for downloading firmware and for REST requests sent from the IP Phone Manager to the phones.	CloudBond 365 server side / Bi-Directional
	TCP (HTTPS)	443	HTTPS connection between the CloudBond 365 server and the IP Phone Manager Web browser that is used for Web management and for downloading firmware.	CloudBond 365 server side / Bi-Directional

This page is intentionally left blank.

Part V

One Voice Operations Center Management

32 Introduction

The CloudBond 365 product series can be managed remotely using AudioCodes One Voice Operations Center. The One Voice Operations Center supports the management of the following product configurations:

- CloudBond 365 Standard Edition (Mediant 800B platform)
- CloudBond 365 Standard Plus Edition (Mediant 800B platform)
- CloudBond 365 Pro Edition (Mediant Server platform)
- CloudBond 365 Enterprise Edition (Mediant Server platform)
- CloudBond 365 Virtualized Edition

This page is intentionally left blank.

33 Status Monitoring and Navigation

The One Voice Operations Center Network Topology screen displays summary information for the CloudBond 365 device. For detailed information, click the Show button.

Figure 13-1: CloudBond 365 Pro Edition

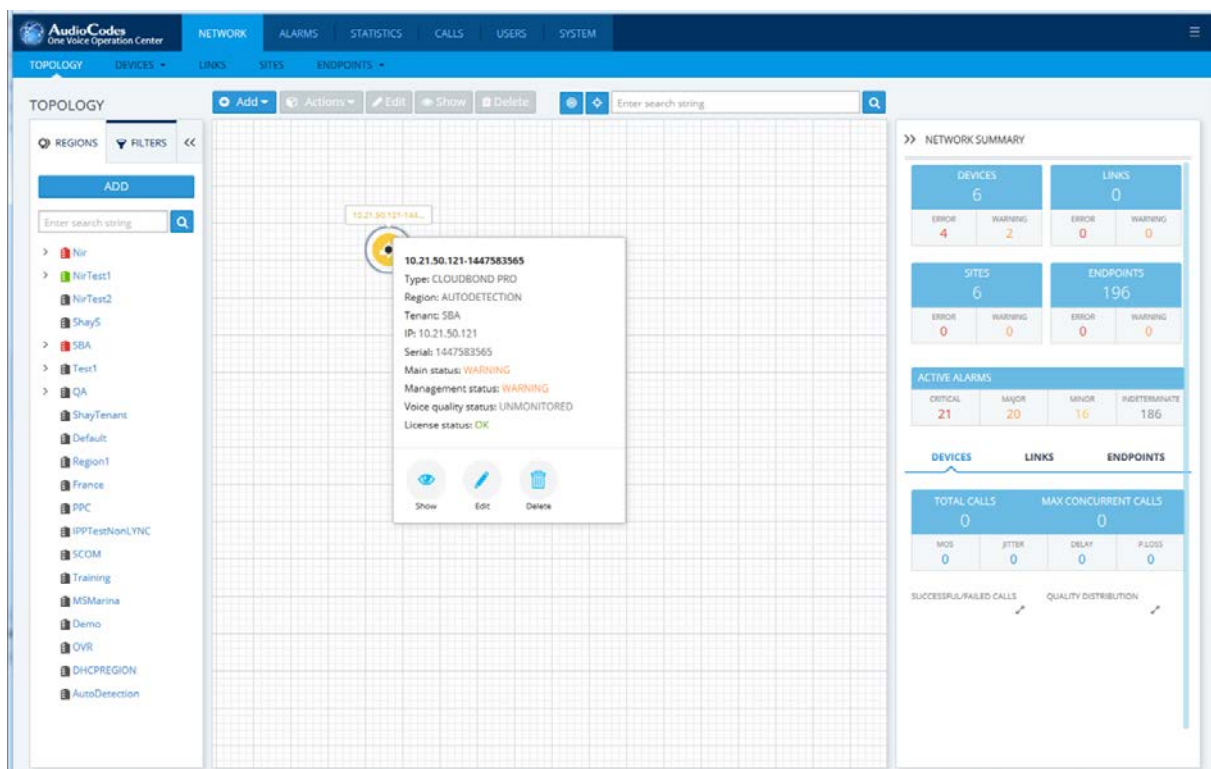
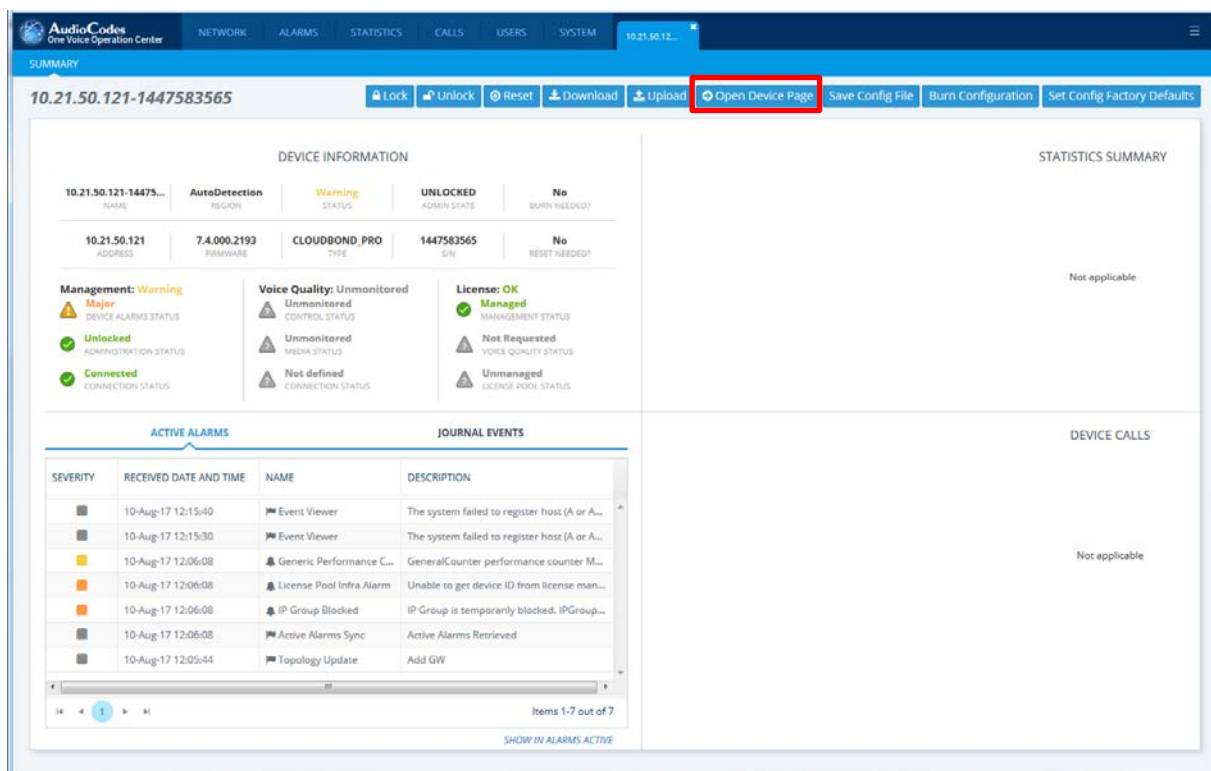


Figure 13-2: CloudBond Device Detailed Information



The above screen shows all active alarms, journal events and summary statutes.
For more information, refer to the *One Voice Operations Center User's Manual*.
You can click the Open Device Page link to open the CloudBond devices Web interface.



Note: Single Sign-on is not supported for the CloudBond 365 product. Consequently when you click the above link, the CloudBond 365 Login screen is displayed and you must then enter your login credentials.

34 CloudBond 365 Alarms

This chapter describes the CloudBond 365 alarms that are raised on the CloudBond 365 platform and sent to the One Voice Operations Center server. These alarms are displayed in the Alarm Browser pane in the Status screen (see Chapter 33). Double-click the alarm whose details you wish to display.

34.1.1 Commit License Failed

Commit License Failed

Description	This alarm is raised when the EMS Main Agent is unable to store the license in the Active Directory.		
SNMP Alarm	acCbManLicenseCommitAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.1		
Alarm Source	N/A		
Alarm Title	Commit License Failed		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Major	Unable to store the license in the Active Directory	Unable to commit the license in Active Directory.	Verify that EMS Agent can access the local Active Directory. Verify that the local Active Directory contains the contact 'CbLicense'.
Cleared	The license has been successfully stored in the Active Directory.	-	

34.1.2 Component Unreachable

Component Unreachable

Description	This alarm is raised when the EMS Main Agent is unable to connect to one of the client agents in the CloudBond environment.		
SNMP Alarm	acCbManEnvUnreachableAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.2		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Unreachable		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action

Major	Client agent is unavailable	Unable to connect to the client agent on <CloudBond component name>.	
Cleared	Client agent is available again.	-	

34.1.3 Component Restart

Component Restart

Description	This alarm is raised when a CloudBond component has restarted.		
SNMP Alarm	acCbManEnvRestartEvent		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.3		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Restart		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	The restart reason		
Alarm Severity	Condition	<text>	Corrective Action
Major	Indeterminate	CloudBond component <component name> restarted	-
Cleared	-	-	

34.1.4 Component Performance Counter General

Component Performance Counter General

Description	This alarm is raised when the generic performance counter has reached a pre-defined threshold for memory, CPU and disk space.		
SNMP Alarm	acCbCompPcGenAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.11		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter General		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-

Major	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-
Warning	Pre-defined severity per counter type.	<Performance counter> high level <x>.	-
Cleared	When counter returns below the threshold level.	-	-

34.1.5 Component Performance Counter Service

Component Performance Counter Service

Description	This alarm is raised when the service-related performance counter has reached a pre-defined threshold. This alarm is related to activity of Skype for Business/Lync services.		
SNMP Alarm	acCbCompPcServAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.12		
Alarm Source	<n>\<g>\<p> (where n is the component name, g is the performance group and p is performance counter name)		
Alarm Title	Component Performance Counter Service		
Alarm Type	QualityOfServiceAlarm		
Probable Cause	-		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Major	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Warning	Pre-defined severity per each counter type	<Performance counter> high level <x>	-
Cleared	When counter returns below the threshold level.	-	-

34.1.6 Component Service Status

Component Service Status

Description	This alarm is raised when a component service is down.		
SNMP Alarm	acCbCompSrvAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.13		
Alarm Source	<n>\<sn> (where n is the component name and sn is the service name)		
Alarm Title	Component Service Status		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Major	Service is down	SERVICE_STOPPED (indicates which service is down)	-
Warning	Service is down	SERVICE_STOPPED. (indicates which service is down)	-
Cleared	Service is running	SERVICE_RUNNING	-
Note: the severity is determined according to the service's importance to system functionality.			

34.1.7 Component Event Viewer

Component Event Viewer

Description	This alarm is raised when report is generated in the Event Viewer for a component error.		
SNMP Alarm	acCbCompEventViewer		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.14		
Alarm Source	<n>\<e> (where n is the component name and e is Type of event (System/Security..))		
Alarm Title	Component Event Viewer		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	Contains the original severity of the event. This event is displayed in the EMS as type "Info".		
Alarm Severity	Condition	<text>	Corrective Action
Indeterminate	-	The text of the event	-

34.1.8 Component Event Viewer Past Hours

Component Event Viewer Past Hours

Description	This alarm is raised when an error is generated in the Event Viewer in the past 24 hours.		
SNMP Alarm	acCbCompEventLogAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.15		
Alarm Source	<n> (where n is the component name)		
Alarm Title	Component Event Viewer Past Hours		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Event Log has a Critical alarm.	The event log has errors	-
Major	Event Log has a Major alarm.	The event log has errors	-
Warning	Event Log has a Warning alarm.	The event log has errors	-
Cleared	No errors have occurred in the past hours.	-	-

34.1.9 Component Event Viewer Dropped

Component Event Viewer Dropped

Description	This alarm is raised when events from the Event Viewer are dropped and not sent to the EMS after the sending rate threshold has been exceeded.		
SNMP Alarm	acCbCompEventViewerDropped		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.16		
Alarm Source	N/A		
Alarm Title	Component Event Viewer Dropped		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Indeterminate		

34.1.10 Admin License Expired

Admin License Expired

Description	This alarm is raised by the CloudBond administrator when the CloudBond user license is invalid.		
SNMP Alarm	acCbAdminLicInvalidAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.21		
Alarm Source	N/a		
Alarm Title	Admin License Expired		
Alarm Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	Condition	<text>	Corrective Action
Major	License is invalid/expired	<ul style="list-style-type: none"> License expired on <Data of the license> Invalid license or missing license in Active Directory 	-
Cleared	License is valid	-	-

34.1.11 Alarm – Certificate Expired

Description	This alarm is raised when the certificate in the CloudBond component is about to expire.		
SNMP Alarm	acCceAdminCertificateExpiredAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.32		
Alarm Source	<n> (where n is the component name)		
Alarm Text	Certificate will expires in <days left> days		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Major	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Warning	Pre-defined severity per threshold	Certificate will expires in <days left> days	Verify which certificate will expire soon and renew it.
Cleared	When certificate is renewed.	-	-

34.1.12 Alarm – Disk Space

Description	This alarm is raised when the CloudBond component's disk space is above the pre-defined threshold.		
SNMP Alarm	acCceDiskSpaceAlarm		
SNMP OID	1.3.6.1.4.1.5003.9.80.3.2.0.36		
Alarm Source	<e> (drive letter 'c:')		
Alarm Text	Disk space usage is over {0}%		
Alarm Type	Other		
Probable Cause	Other		
Alarm Severity	Condition	<text>	Corrective Action
Critical	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Major	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Warning	Pre-defined severity for percentage of used disk space.	Disk space usage is over {0}%	Free temporary files and other unnecessary file from the disk.
Cleared	Used disk space is below threshold.	-	-

This page is intentionally left blank.

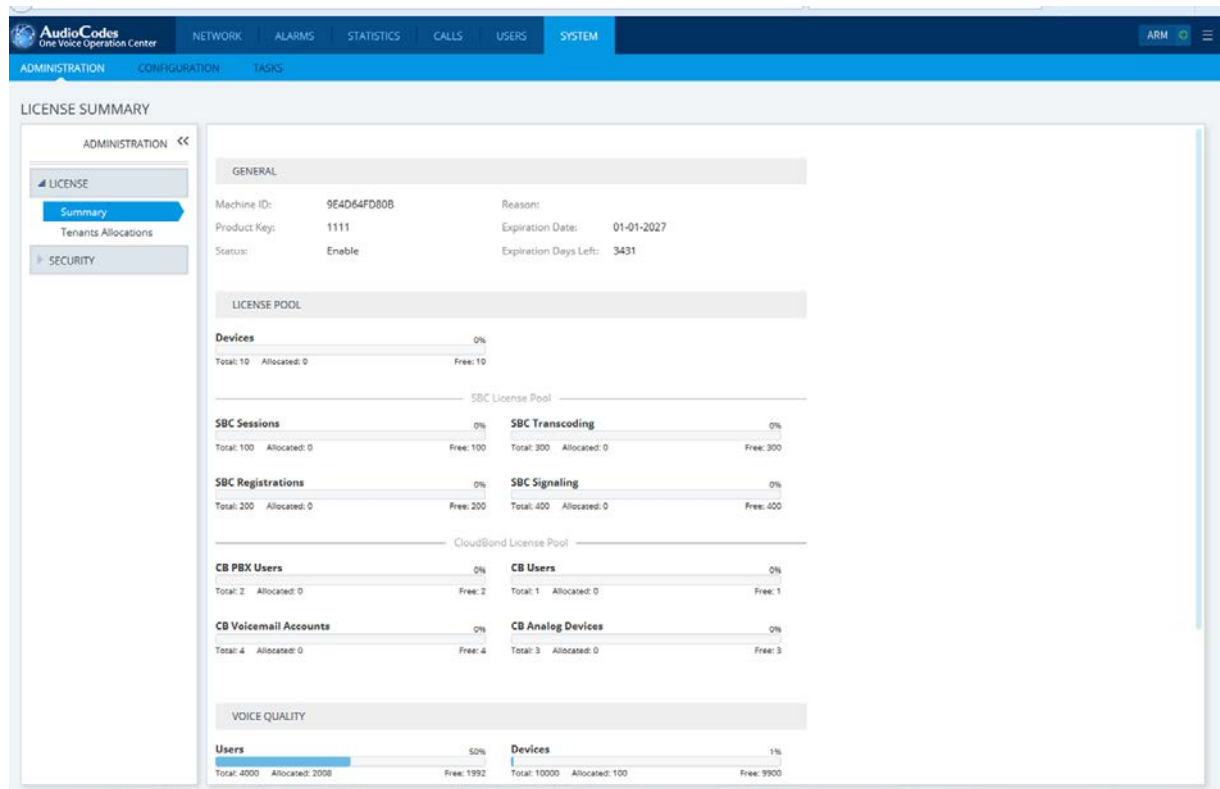
35 License Management

The "License Pool Manager" enables operators to centrally manage and distribute session licenses for multiple CloudBond 365 devices using a flexible license pool. The operator can allocate and de-allocate the licenses for the devices in the pool according to their capacity requirements.

➤ **To access the License Pool Manager:**

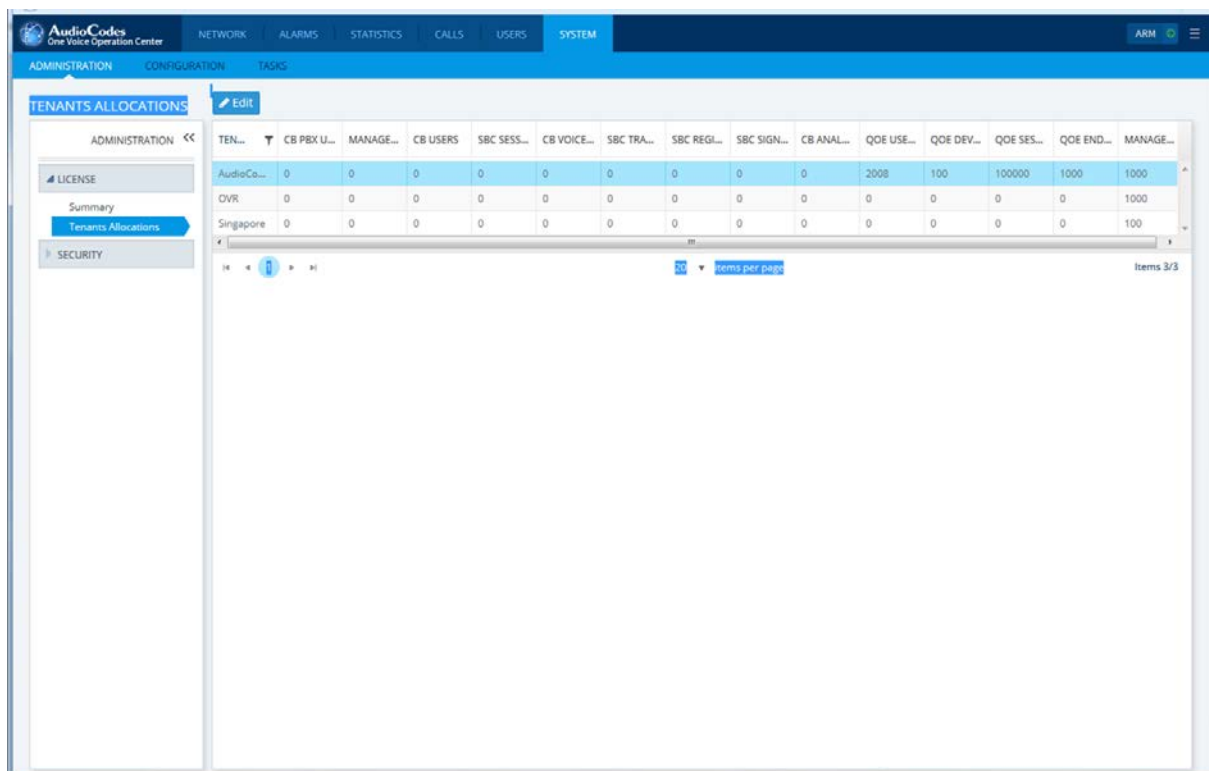
1. In the One Voice Operations Center Main Menu, open the License Summary page (**System** tab > **License** > **Summary**). The License Pool Manager Summary screen is displayed:

Figure 22-1: License Pool Manager - CloudBond Devices



The following license parameters can be managed for CloudBond 365 devices:

- The number of CB user sessions
 - The number of CB PBX users (for future use)
 - The number of CB analog devices (for future use)
 - The number of CB voicemail accounts (for future use)
2. Select the **Tenant Allocations** tab.

Figure 22-2: Tenant Allocations


The screenshot shows the AudioCodes One Voice Operation Center interface. The top navigation bar includes tabs for NETWORK, ALARMS, STATISTICS, CALLS, USERS, and SYSTEM. The left sidebar has a menu with ADMINISTRATION, CONFIGURATION, and TASKS. Under ADMINISTRATION, there are sub-menus for LICENSE, Summary, Tenants Allocations (highlighted), and SECURITY. The main content area displays the 'TENANTS ALLOCATIONS' table with an 'Edit' button. The table has columns for TEN..., CB PBX U..., MANAGE..., CB USERS, SBC SESS..., CB VOICE..., SBC TRA..., SBC REGL..., SBC SIGN..., CB ANAL..., QOE USE..., QOE DEV..., QOE SES..., QOE END..., and MANAGE... The table contains three rows: AudioCo..., OVR, and Singapore. The bottom of the table shows a pagination bar with 'Items per page' and 'Items 3/3'.

TEN...	CB PBX U...	MANAGE...	CB USERS	SBC SESS...	CB VOICE...	SBC TRA...	SBC REGL...	SBC SIGN...	CB ANAL...	QOE USE...	QOE DEV...	QOE SES...	QOE END...	MANAGE...
AudioCo...	0	0	0	0	0	0	0	0	0	2008	100	100000	1000	1000
OVR	0	0	0	0	0	0	0	0	0	0	0	0	0	1000
Singapore	0	0	0	0	0	0	0	0	0	0	0	0	0	100

- Assign the relevant licenses to the tenants. For more information, refer to the *One Voice Operation Center User's Manual*.

Part VI

Backup and Restore

36 Introduction

This part describes how to configure and use the CloudBond backup and restore functionality.

The functionality uses two third-party components:

- **Veeam Endpoint Backup (VEB):** A designated tool installed on the host server to back up the host itself, without its virtual machines (i.e., Front End and Edge servers).
- **Veeam Backup and Replication (VBR):** A designated tool installed on the CloudBond host server or on an external server, to back up the CloudBond virtual machines (VM) only.

CloudBond products are divided to two main topologies, and two different hardware types:

- Main Topologies:
 - Standalone configuration
 - Pool-paired branch - Branch Pool Appliance (BPA)
- Hardware:
 - Mediant 800
 - HP Server (host)

Some procedures require a different setup, depending on hardware and topology. If a different setup is required, the correct hardware and topology is noted.



Note: Backup and restore are critical functions. It is important to follow all steps described in the procedures in this document. Do not skip any steps when performing Backup or Restore.

This page is intentionally left blank.

37 Backup Architecture

This section describes the different backup architecture options and components which are used for CloudBond 365. Veeam components consist of the following:

- VEB
- VBR Manager
- Backup Repository

One of the important issues regarding backup and restore procedures is the location of CloudBond 365 – whether it is at the Service Provider or at the customer premises. The backup and restore infrastructure must be on the same local network as the CloudBond 365.

This document does not distinguish between the different locations of the CloudBond 365. The setup is similar for both locations. You must design your architecture with the limitation that the backup and restore infrastructure must be on the same LAN as the CloudBond 365 (except for the cloud repository that is always on the cloud).

Figure 37-1: Backup Architecture on Premises

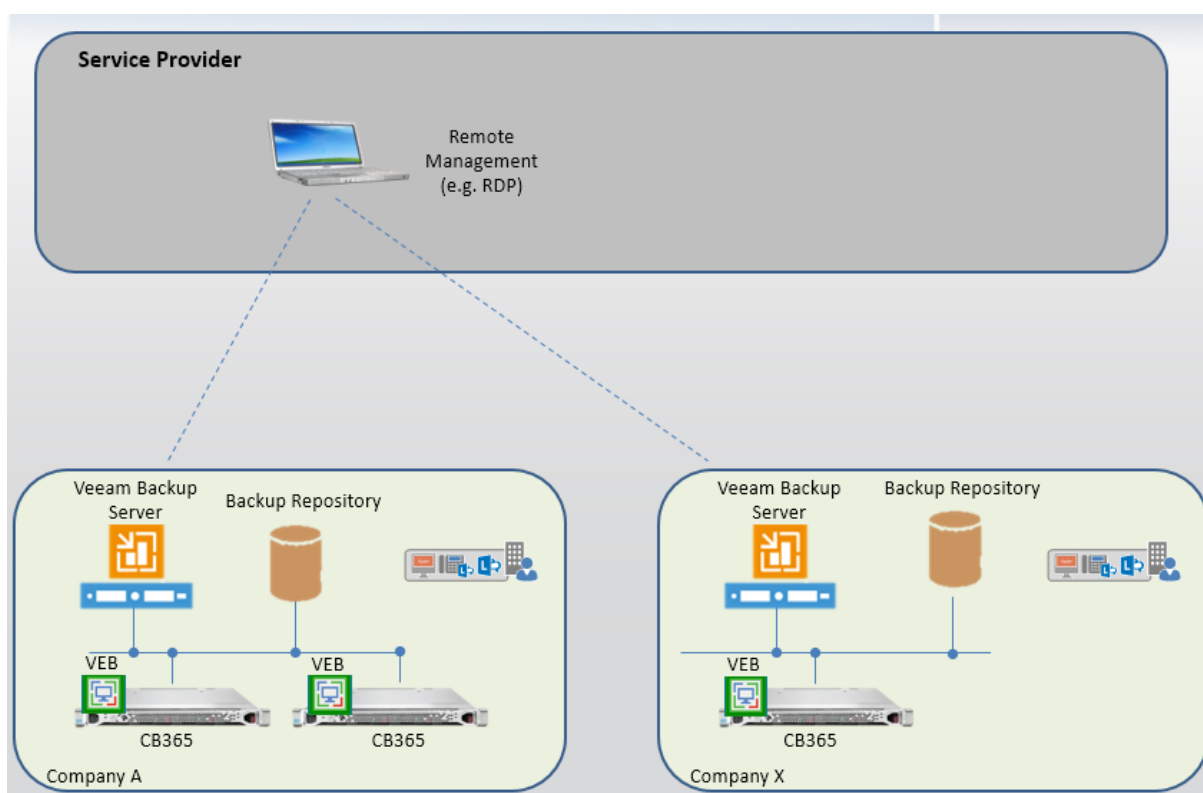
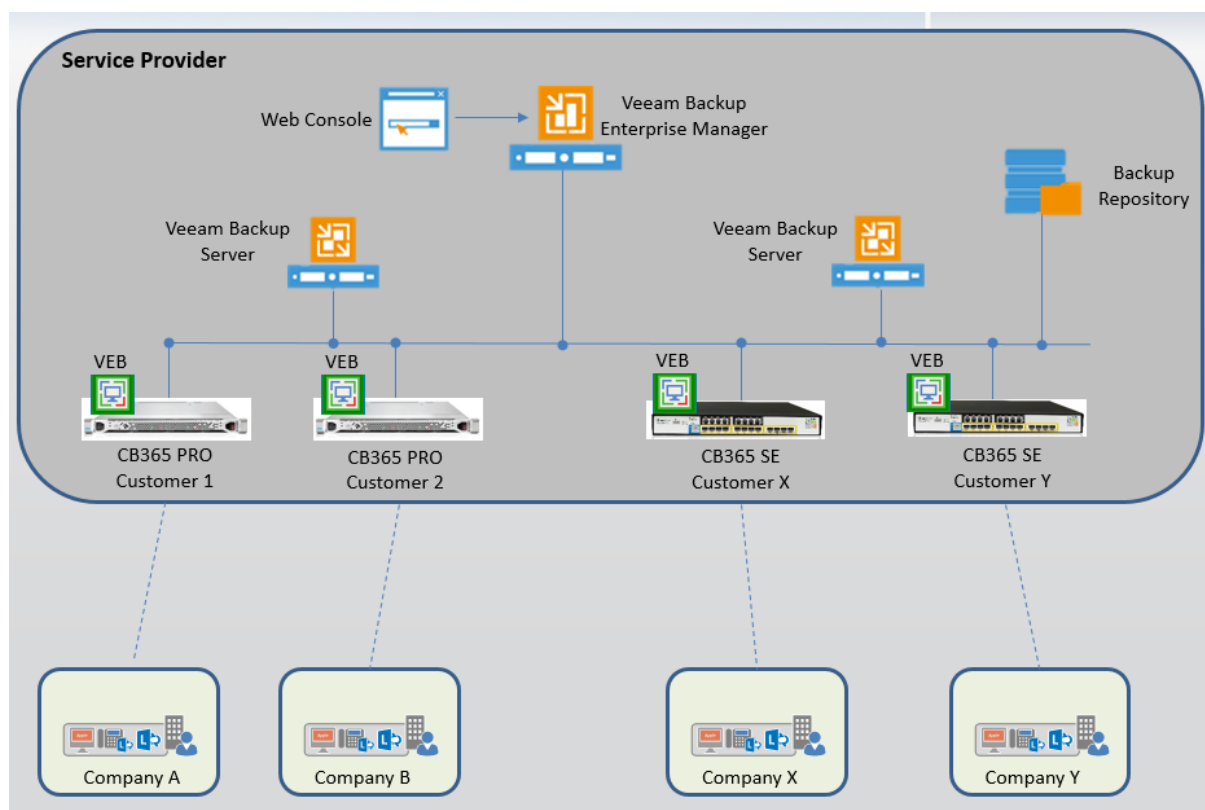


Figure 37-2: Backup Architecture on Service Provider



37.1 Using Veeam Products

37.1.1 VEB

VEB software is installed on every CloudBond 365. This software only backs up the Host server. For standalone configurations, the system volume and extra volume/files are also backed up. For BPA topology, there is usually no database for the paired CloudBond 365 server and therefore the system volume and extra volume/files are not backed up.

37.1.2 VBR

VBR is a distributed system. CloudBond uses only part of the available components. The Veeam Backup Server is the VBR management component and can be run on the CloudBond Host or it can be run on external server. If the Backup Repository is external and it is a Windows server, it is recommended to run the VBR Manager so that it can back up several CloudBond systems on the same branch.

37.2 Using VBR Components

37.2.1 VBR Manager

The VBR manager can be run on the CloudBond 365 host or on an external server. The external server can run the backup repository and the VBR Manager. To run the VBR Manager on an external server, refer to the server requirements in the *Veeam Backup & Replication User Guide* under **Planning and Preparation > Requirements > System Requirements > Veeam Backup Server**.

37.2.2 Backup Repository

The Backup Repository can be external. There are several types of Backup Repositories which are supported and can be used:

- Microsoft Windows server with local or directly attached storage
- Linux server with local, directly attached storage or mounted NFS
- Common Internet File System (CIFS)

For more information, refer to the *Veeam Backup & Replication User Guide* under **Overview > Solution Architecture > Components > Backup Repository**.



Note: The repository can be a local disk connected to CloudBond 365. However, this document does not describe this topology in details.

37.2.2.1 Backup Repository Size

The following lists backup repository size requirements per CloudBond 365 type:

- **Standard Box Edition:** 150 GB
- **Standard Plus Box Edition:** 200 GB
- **Pro Box Edition:** 300 GB
- **Enterprise Box Edition:** 300 GB



Note: It is not intended for the Backup tool to back up the CloudBond 365 SBC. To back up the CloudBond 365 SBC, it is recommended to manually backup the SBC Settings INI files and VM. The VM can also be found on the CloudBond 365 USB. For more information, refer to the Saving Configuration sub-section of the *AudioCodes SBC User's Manual*.

37.3 Firewall

There are several ports used between the CloudBond 365 server and the Veeam components that must be open if the Firewall is used on the network. Refer to the list of ports requirements in the *Veeam Endpoint Backup User Guide* under **System Requirements > Used Ports**.

38 Installing VEB and VBR

This section describes how to install and configure VEB and VBR. Version 7.0 backup setup files can be downloaded from: https://s3.eu-central-1.amazonaws.com/downloads-audiocodes/CB365Backup/CB365_Backup_7.0.0.zip

When selecting this hyperlink, the following files appear in the WinZip window:

- Endpoint Backup 1.1.2.119.zip
- Backup & Replication 8.0.0.817.iso
- Veeam Backup & Replication_8.0.0.2084_Update3.zip (patch file)

38.1 Installing VEB on the Host Server



Note: This document is applicable to VEB version **1.1.2.119**.

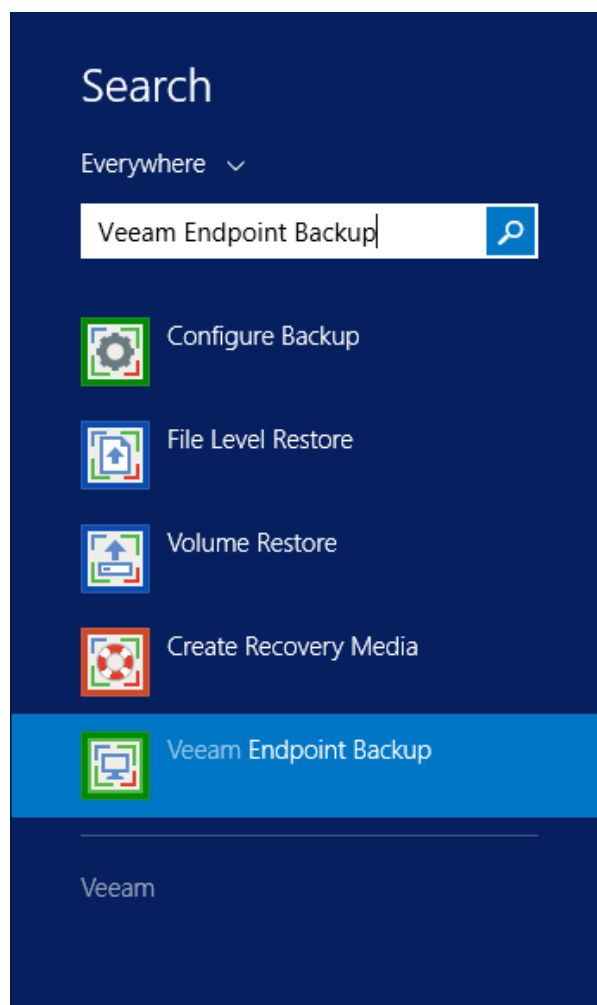
The VEB should be installed on the host server. If you already have the current version 1.1.2.119 installed, skip this procedure.

If you have an older version, install the new one and follow the upgrade instructions. This requires two re-boots.

To confirm that VEB has been installed, search for Veeam Endpoint backup on the **Start** window.

To confirm which version is installed on your system, open **Veeam Endpoint Backup** and navigate to the **Update** menu.

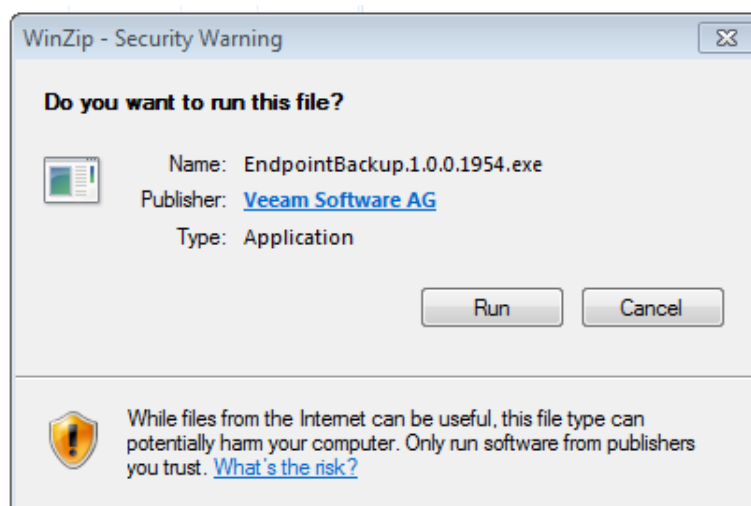
Figure 38-1: Search Menu



➤ **To install VEB on the host server:**

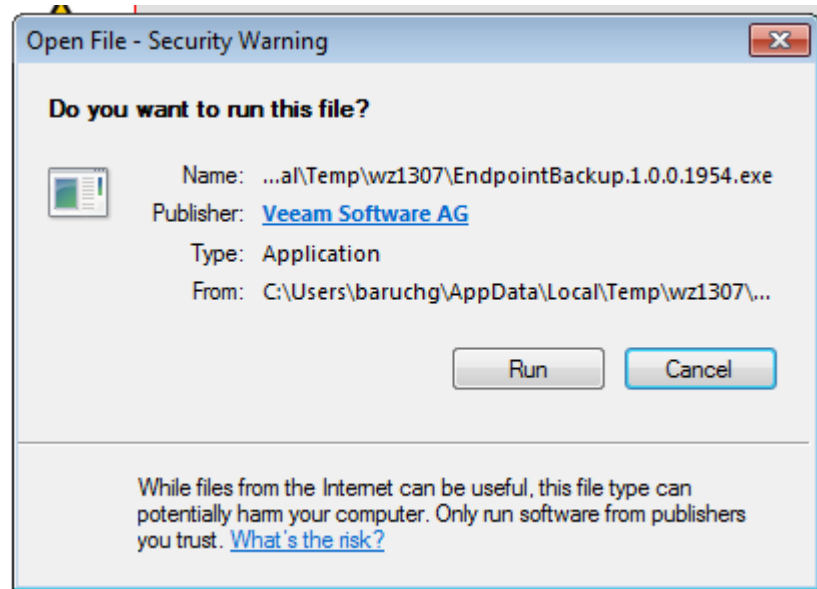
1. Unzip *EndpointBackup.1.1.2.119.zip* file
2. Run the *EndpointBackup.1.1.2.119.exe* file.

Figure 38-2: WinZip Security Warning



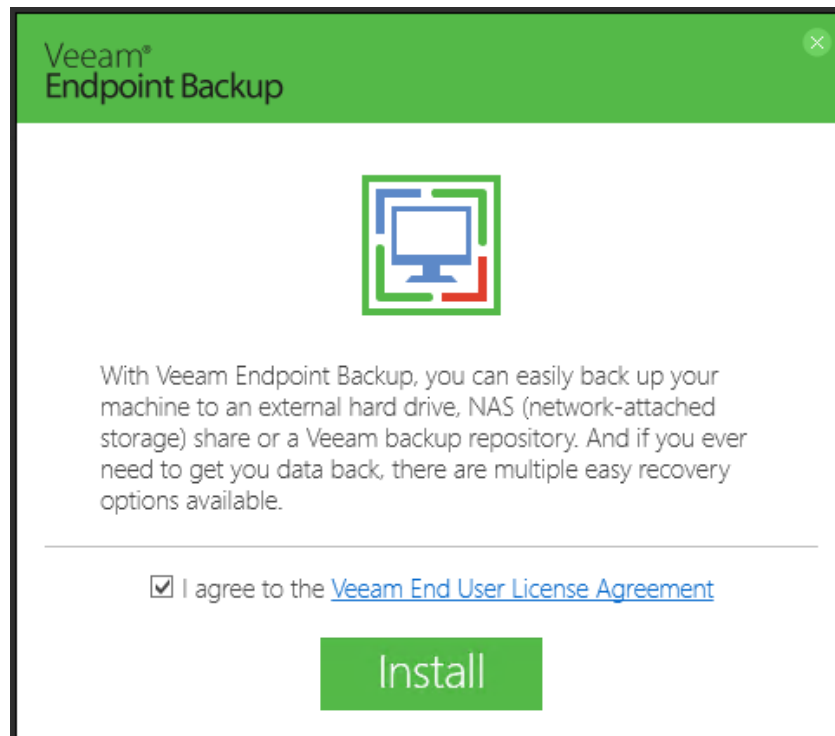
3. Click **Run**.

Figure 38-3: Do you want to run this file?



4. When the following screen appears, select the 'I agree...' checkbox.

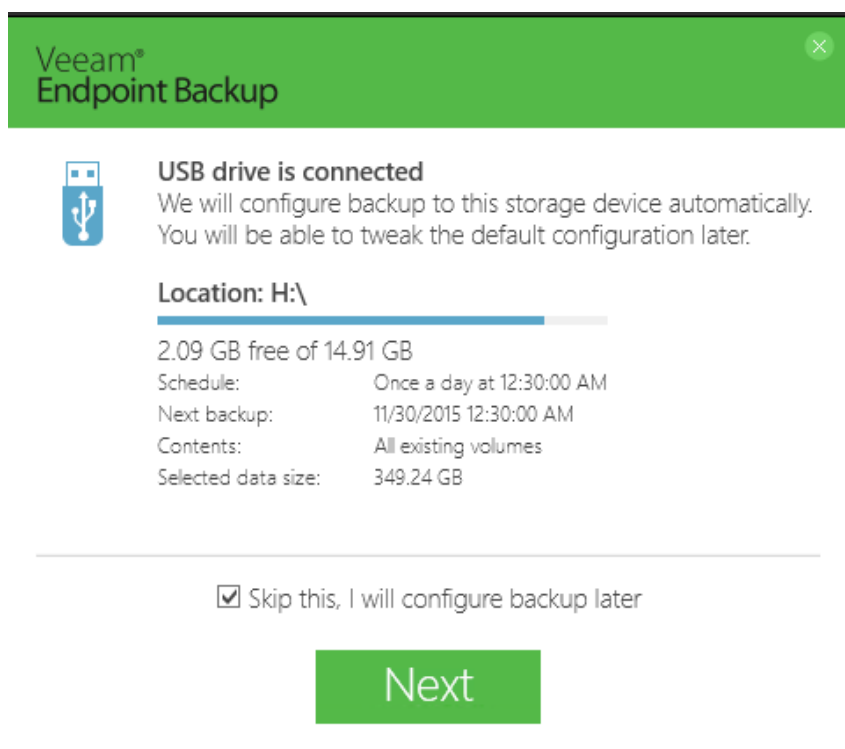
Figure 38-4: Veeam Endpoint Backup



5. Click **Install**.
6. Select the 'Skip this, I will...' checkbox.

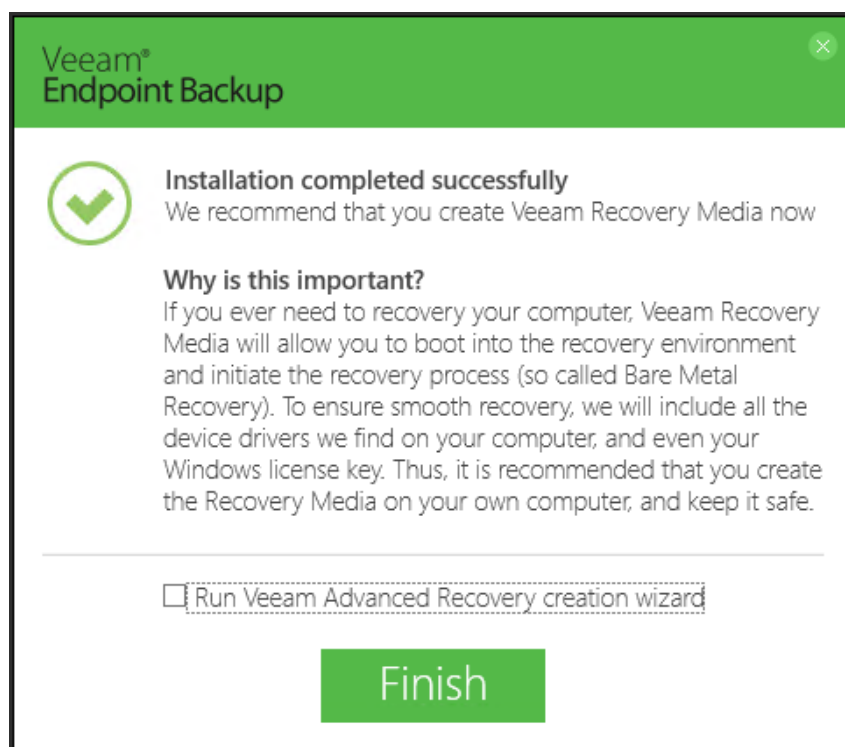
7. Click **Next**.

Figure 38-5: Veeam Endpoint Backup - Next



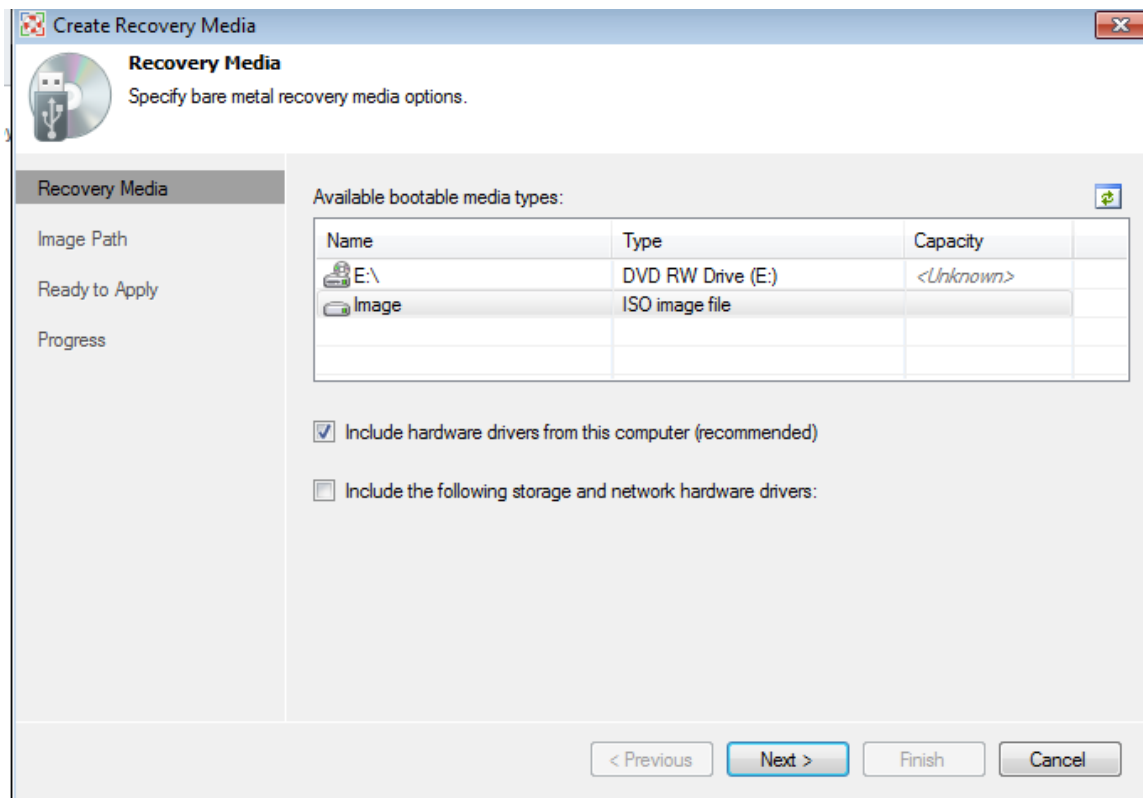
8. Clear the 'Run Veeam Advanced Recovery creation wizard' check box.
9. Click **Finish**.

Figure 38-6: Veeam Endpoint Backup - Finish



10. Click **Cancel**.

Figure 38-7: Create Recovery Media



38.2 Installing VBR

The VBR can be installed on every CloudBond 365 Host or on the recommended external server (the same server that can be used as the backup repository).

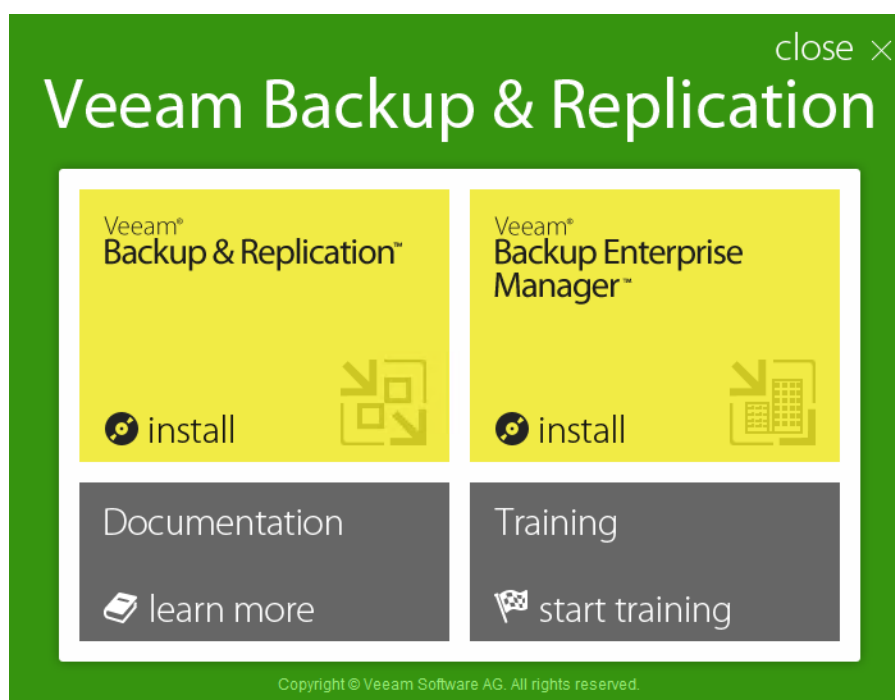
Before you begin the installation process, check the following prerequisites:

- The computer on which you plan to install Veeam Backup & Replication must meet the system requirements. Refer to the server requirements in the *Veeam Backup & Replication User Guide* under **Planning and Preparation > Requirements > System Requirements > Veeam Backup Server**.
- Communication between components requires a number of ports to be open. Refer to the **Requirements > Used Ports** section in the *Veeam Endpoint Backup User Guide*.



Note: The VBR installation requires a server restart.

Figure 38-8: Veeam Endpoint Backup - Finish

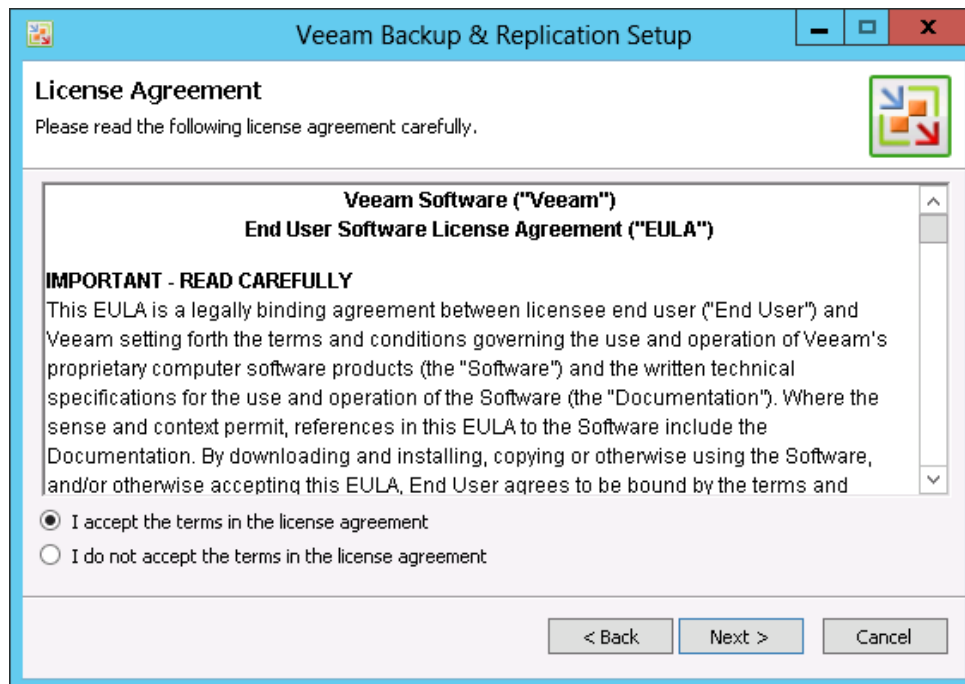


➤ **To install the VBR:**

1. Select **Install** in the 'Veeam Backup & Replication' window.
2. On the **Welcome** step of the wizard, click **Next** to start the installation.

3. Read the license agreement and then accept it, by clicking the **I accept the terms in the license agreement** option, and then click **Next**.

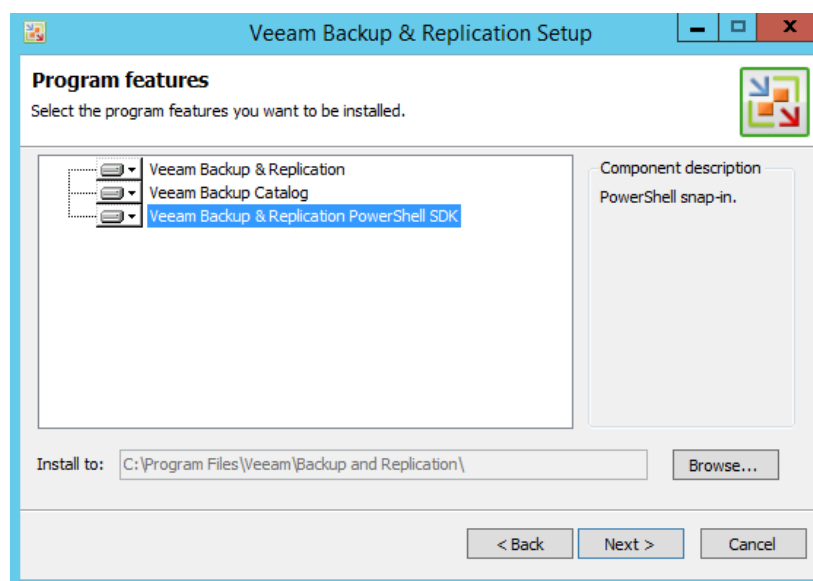
Figure 38-9: Veeam Backup and Replication Setup



Note: You must have a valid trial license or full paid license for Veeam Backup & Replication.

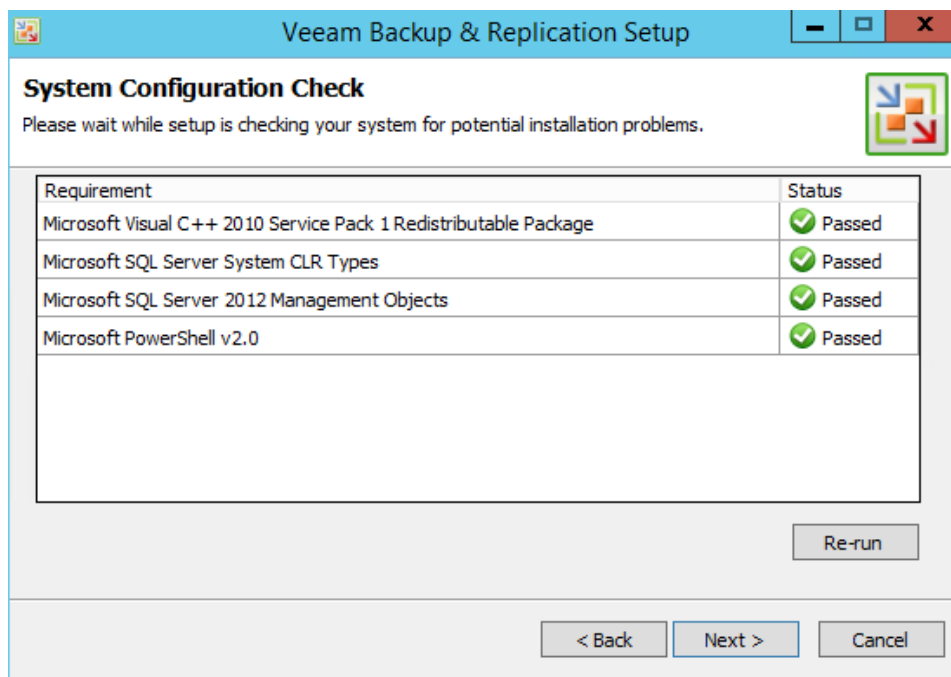
4. Select the three features to be installed and then click **Next**.

Figure 38-10: Program Features



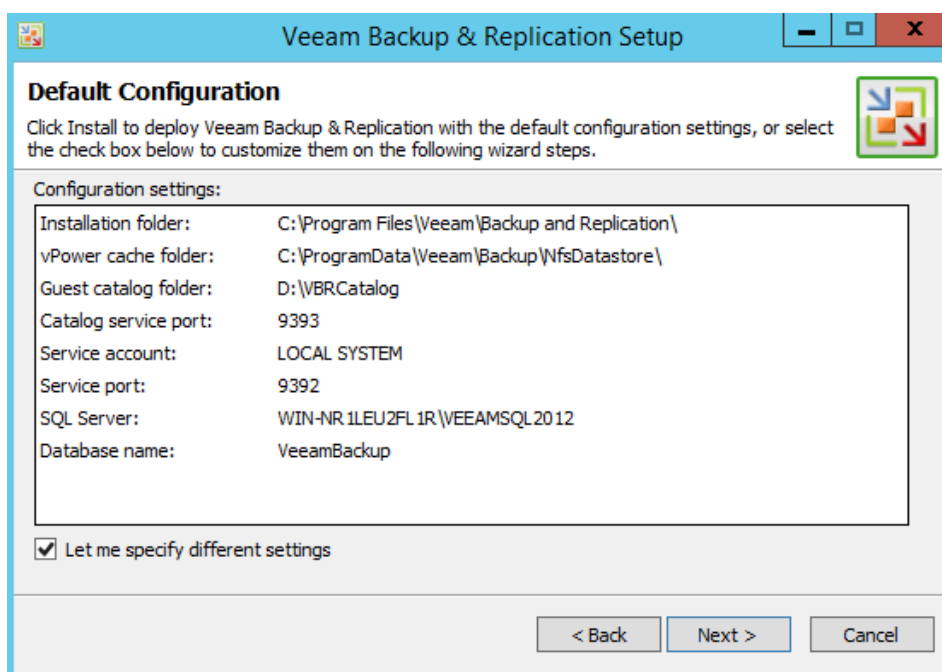
5. The setup checks your system for potential installation problems. Click **Next**; the missing components are installed.

Figure 38-11: System Configuration Check



6. Select the 'Let me specify different settings' checkbox, and then click **Next**.

Figure 38-12: Default Configuration



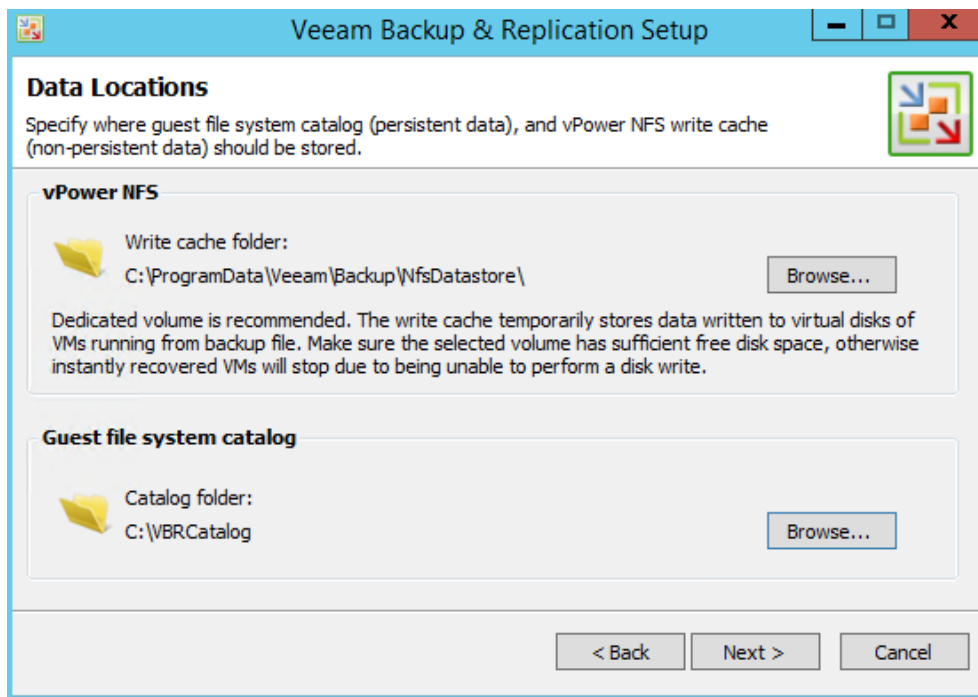
- For the 'Catalog folder', click **Browse** to select "C:\VBRCatalog".



Note: You first need to create this folder.

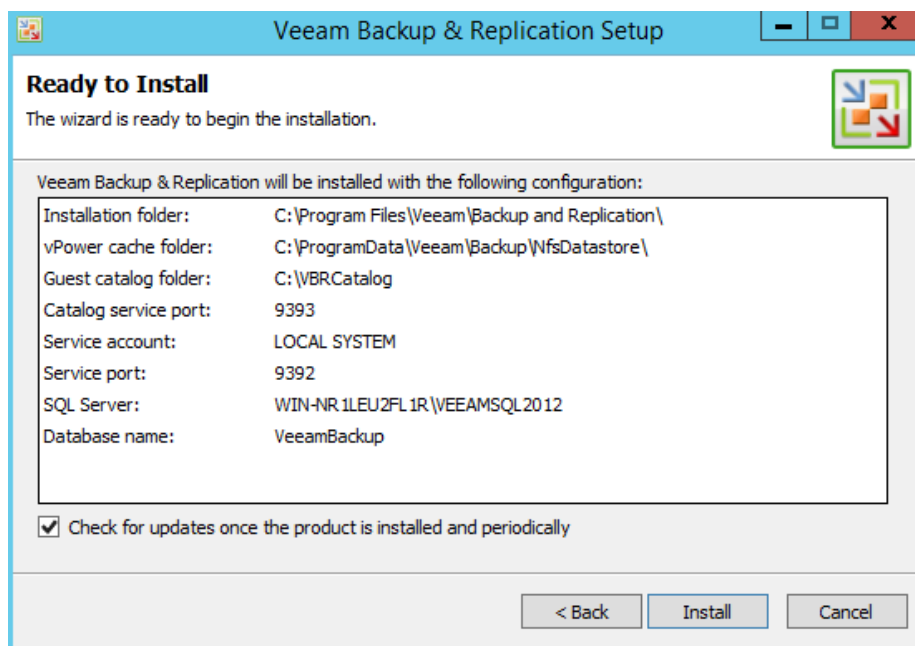
- Click **Next**.

Figure 38-13: Data Locations



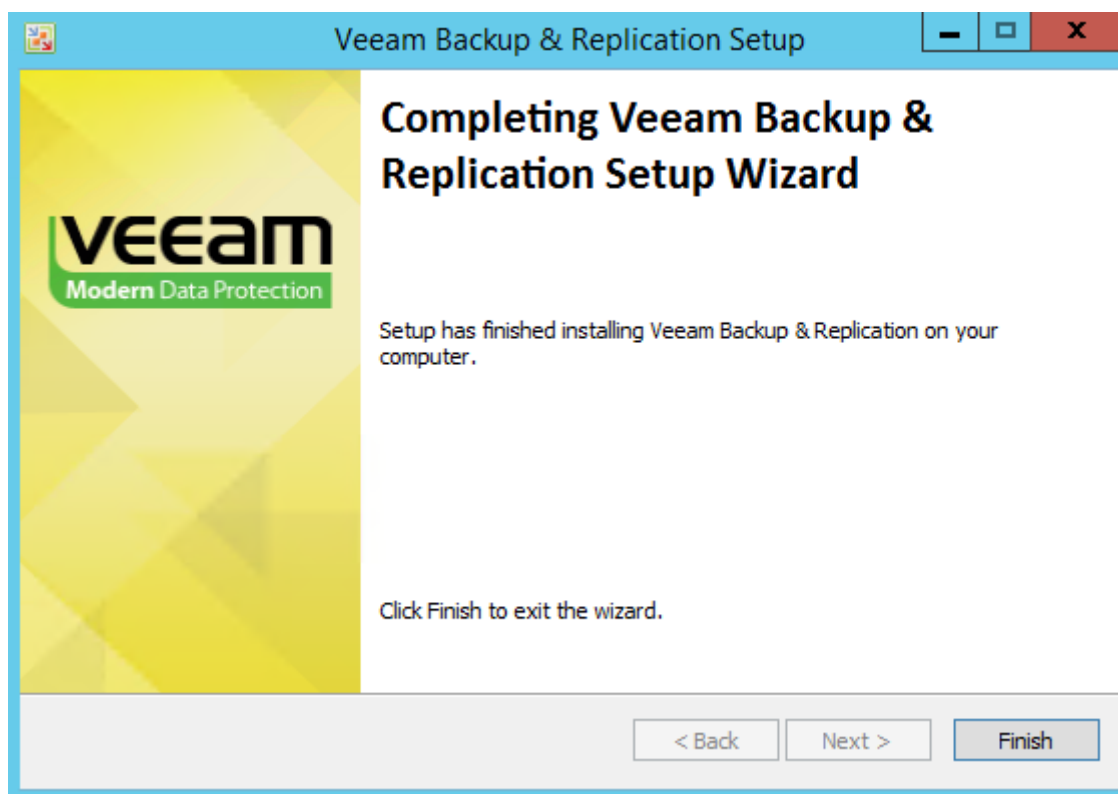
- Click **Install**.

Figure 38-14: Ready to Install



10. Click **Finish**, and then close the above screen.

Figure 38-15: Completing Veeam Backup and Replication Wizard



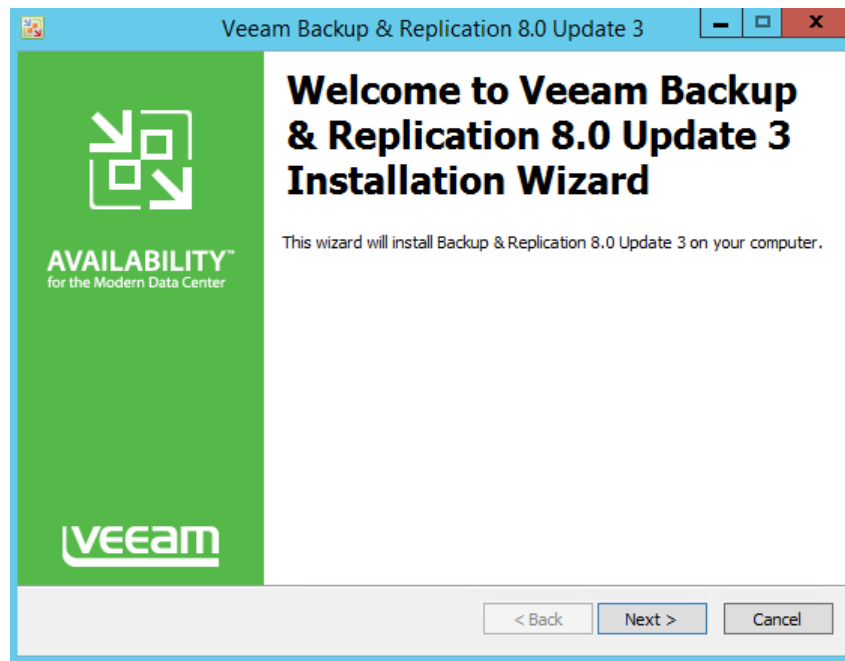
38.2.1 Installing Patch File

The following procedure describes how to install the patch file update *VBR Update3: VeeamBackup&Replication_8.0.0_Update3*.

➤ **To install the patch file:**

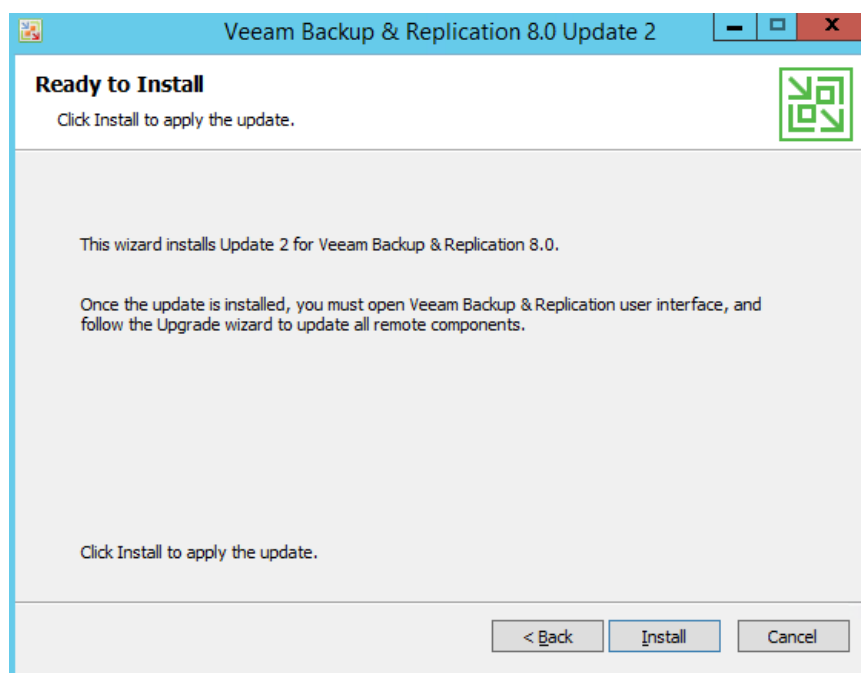
1. Run the patch file with an Administrator login.
2. Click **Next**.

Figure 38-16: Welcome Update Installation Wizard



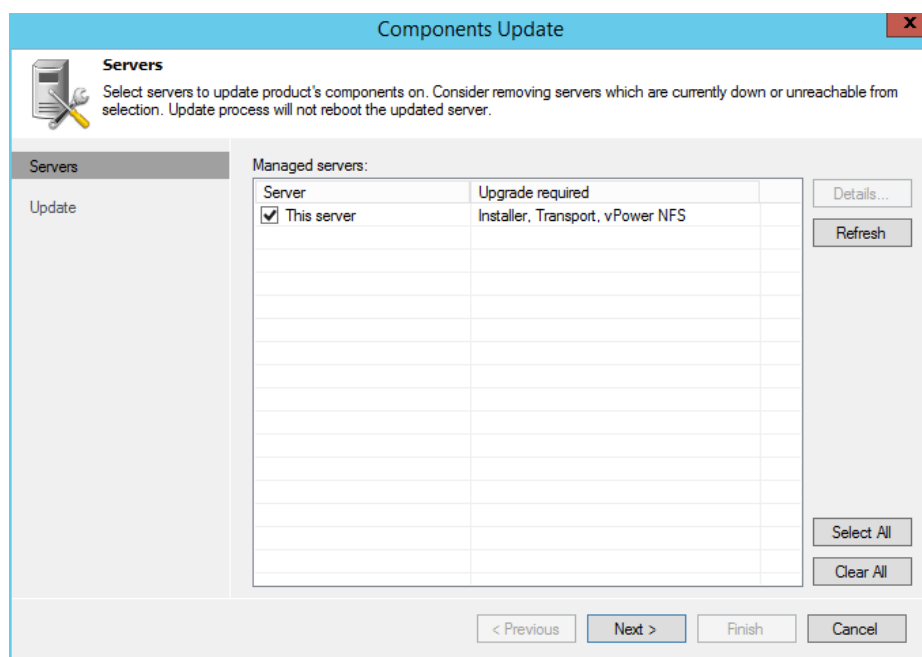
3. Click **Install**; the following screen appears.

Figure 38-17: Ready to Install



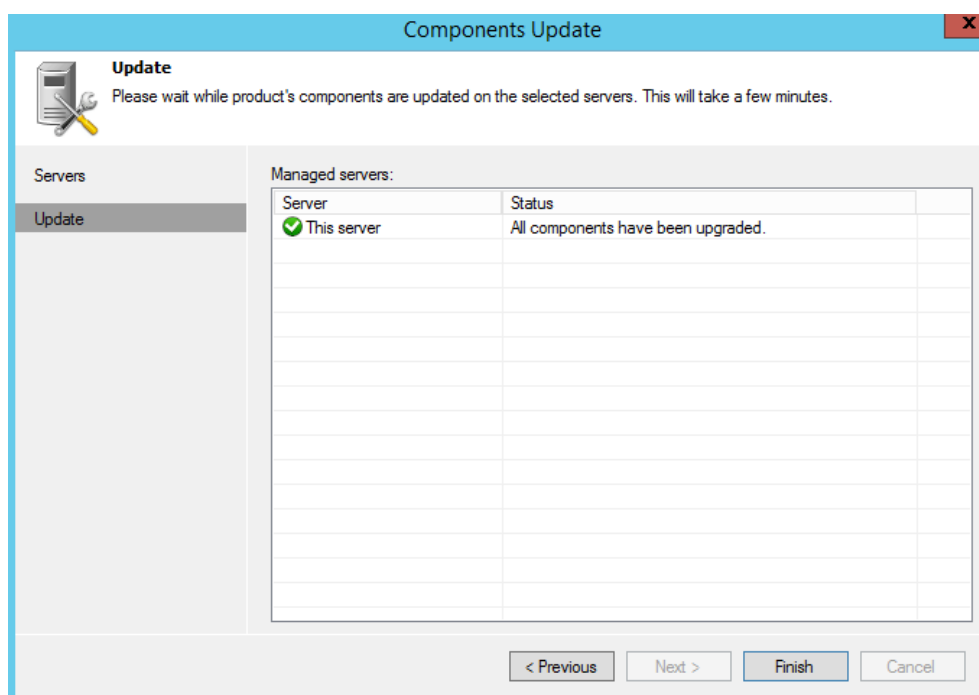
4. Click **Finish** when the installation has finished.
5. Open the VBR Console from the desktop by double-clicking the Veeam Backup icon.
6. Click **Next**.

Figure 38-18: Components Update



7. When the components have been updated, click **Finish**.

Figure 38-19: Components Update - Finish



39 Configuring License and Credentials

The following procedure describes how to configure the license and credentials.

This page is intentionally left blank.

40 Backing up the Repository

The following procedures describe how to setup the backup repository.

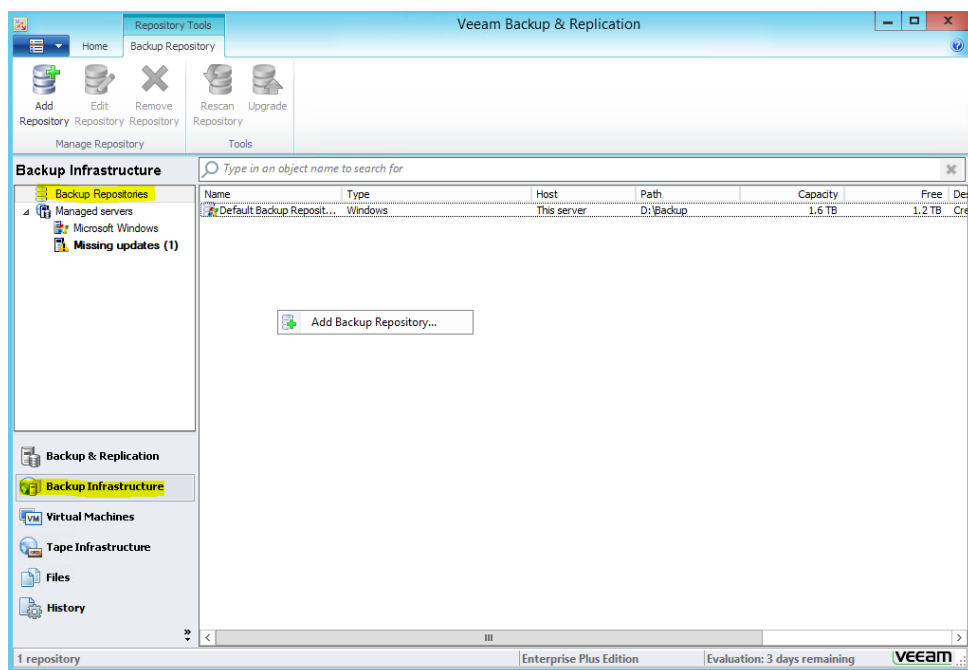
40.1 Adding Backup Repository

The following procedure describes how to add a backup repository in VBR.

➤ **To add a backup repository:**

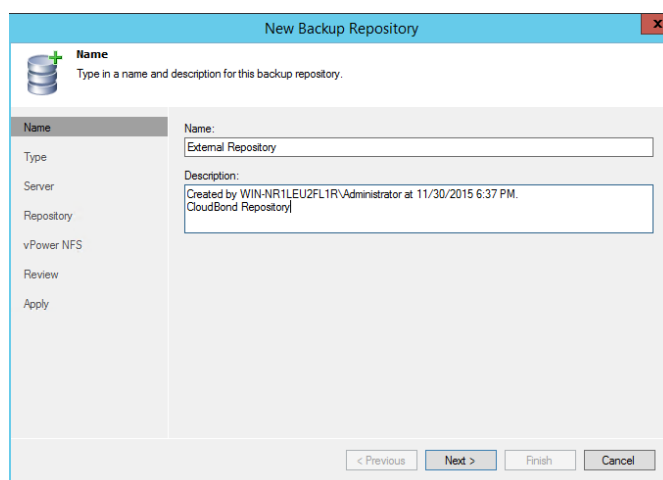
1. Open the VBR main console screen.
2. From the menu options on the left-side of the screen, select **Backup Infrastructure** and navigate to **Repository Tools > Backup Repository**.
3. Right-click on the repository and then, select **Add Backup Repository**.

Figure 40-1: VBR Backup Repository



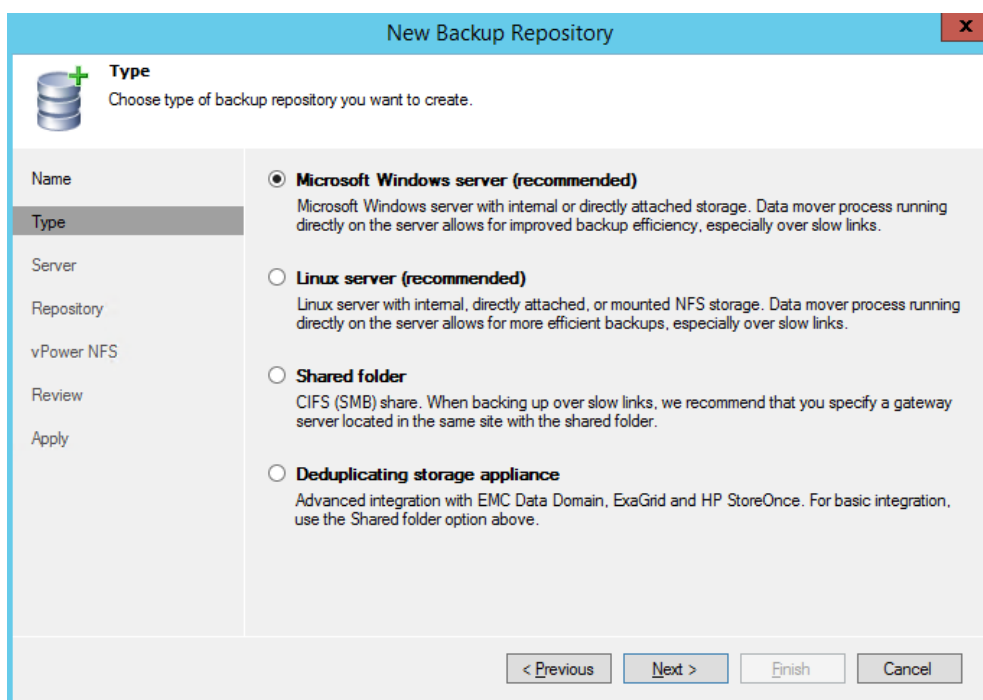
4. On the New Backup Repository screen, enter the **Name** and **Description** of the repository, and then click **Next**.

Figure 40-2: New Backup Repository - Name



5. Select the backup repository type that you want to create, and then click **Next**.

Figure 40-3: New Backup Repository - Type



- On the New Backup Repository - Server screen, click **Add New**.

Figure 40-4: New Backup Repository - Server

New Backup Repository

Server
Choose server backing your repository. You can select server from the list of managed servers added to the console.

Name
Type
Server
Repository
vPower NFS
Review
Apply

Repository server:
This server Add New...

Path	Capacity	Free

Populate

< Previous Next > Finish Cancel

- In the 'DNS name or IP address' field, enter the IP address/DNS Name, and then click **Next**.

Figure 40-5: New Windows Server

New Windows Server

Name
Specify DNS name or IP address of Microsoft Windows server.

Name
Credentials
Review
Apply
Summary

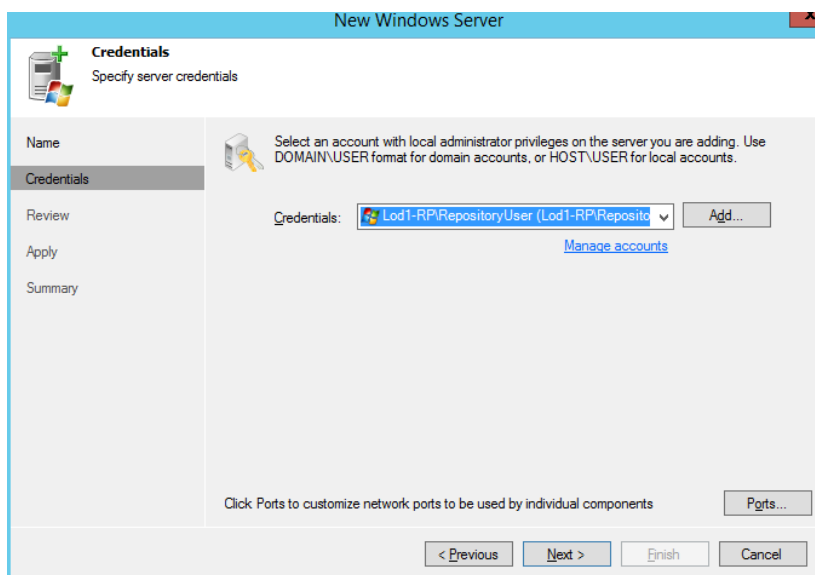
DNS name or IP address:
192.168.11.104

Description:
Created by WIN-NR1LEU2FL1R\Administrator at 11/30/2015 6:40:43 PM.]

< Previous Next > Finish Cancel

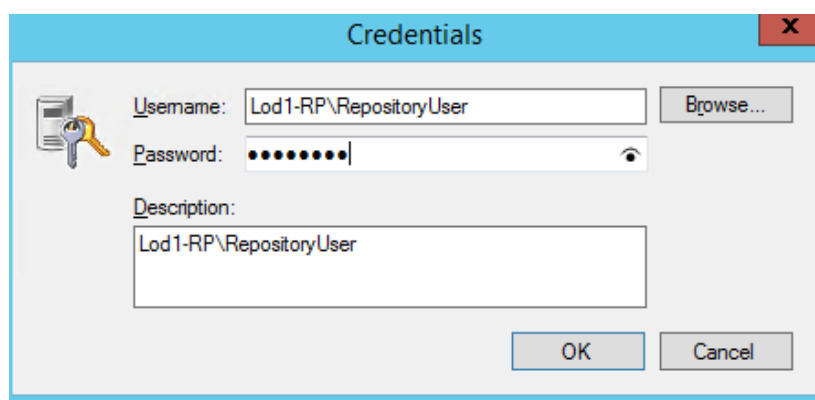
- Select the Repository Credentials (which must be a local Administrator on the Repository) and then click **Next**.
- If you do not have the credentials and you wish to add the credentials, click **Add**.

Figure 40-6: New Windows Server - Credentials



10. Enter the **Username** and **Password**, and then click **OK**.

Figure 40-7: Credentials



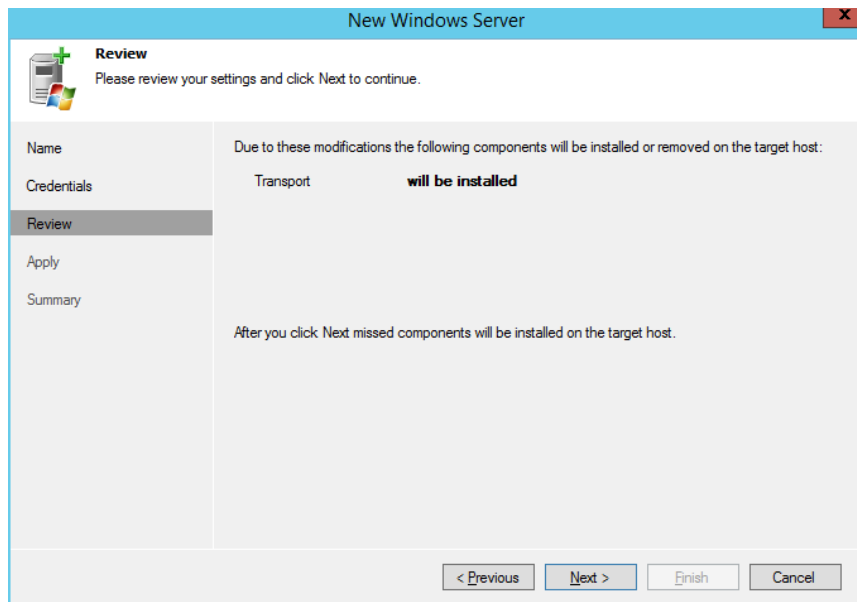
11. The Repository server is analyzed to see if you need to install the agent. You are informed which agents are going to be installed on the Repository.



Note: The required ports must be open between the VBR server and the Repository server.

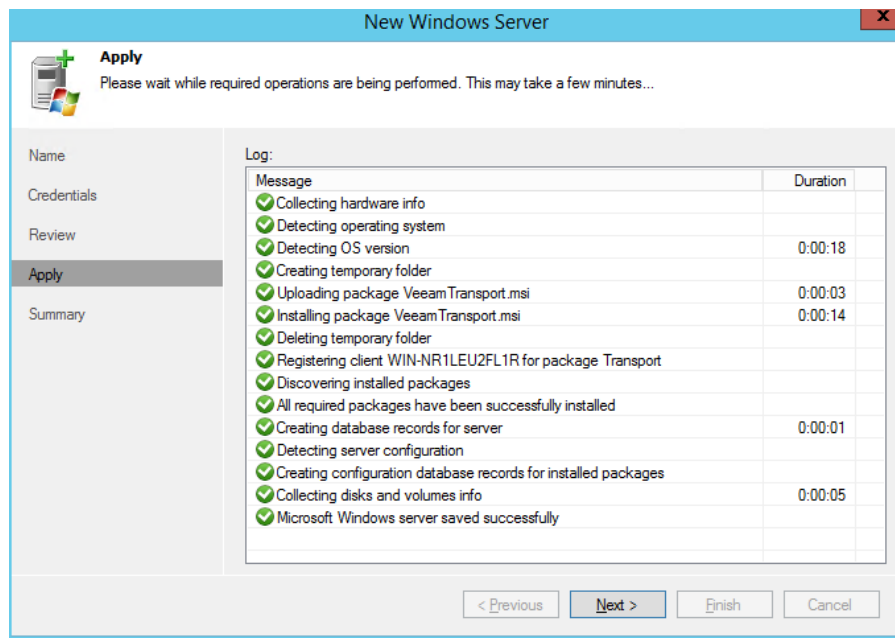
12. Click **Next**.

Figure 40-8: New Windows Server - Review



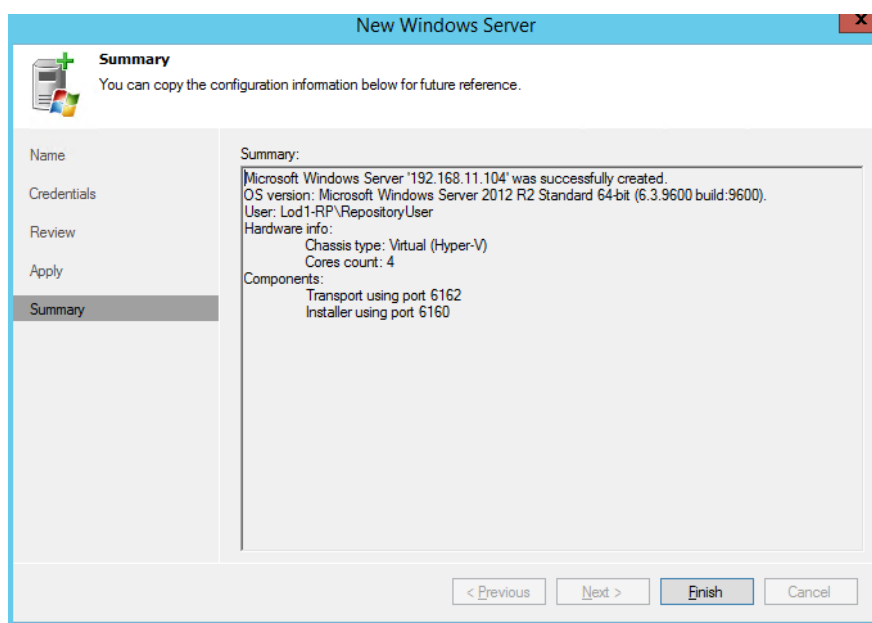
13. Please wait while the required operations are being performed. When the installation has completed, click **Next**

Figure 40-9: New Windows Server - Apply



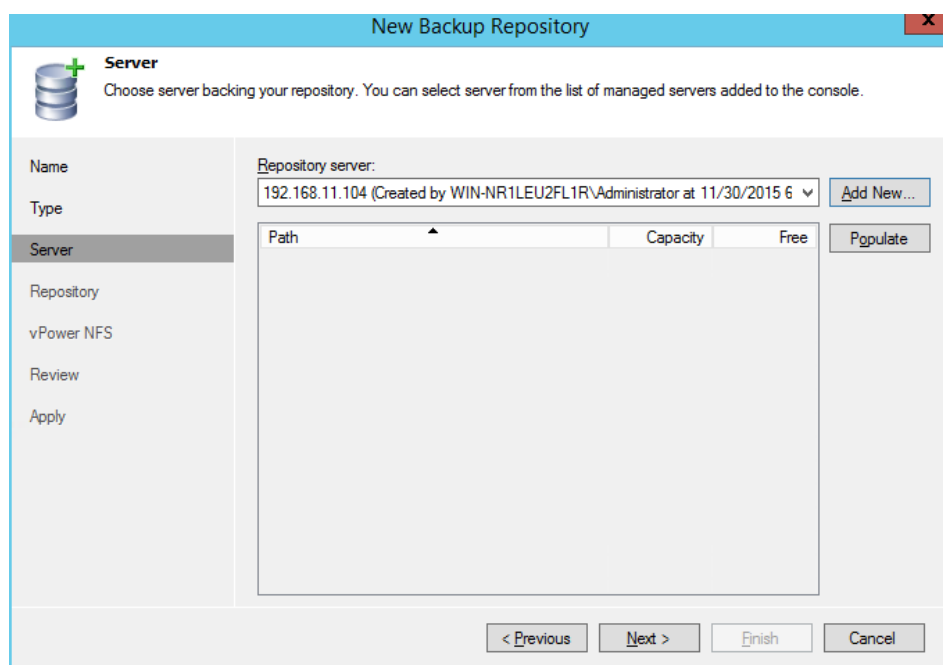
14. Click **Finish**.

Figure 40-10: New Windows Server - Summary



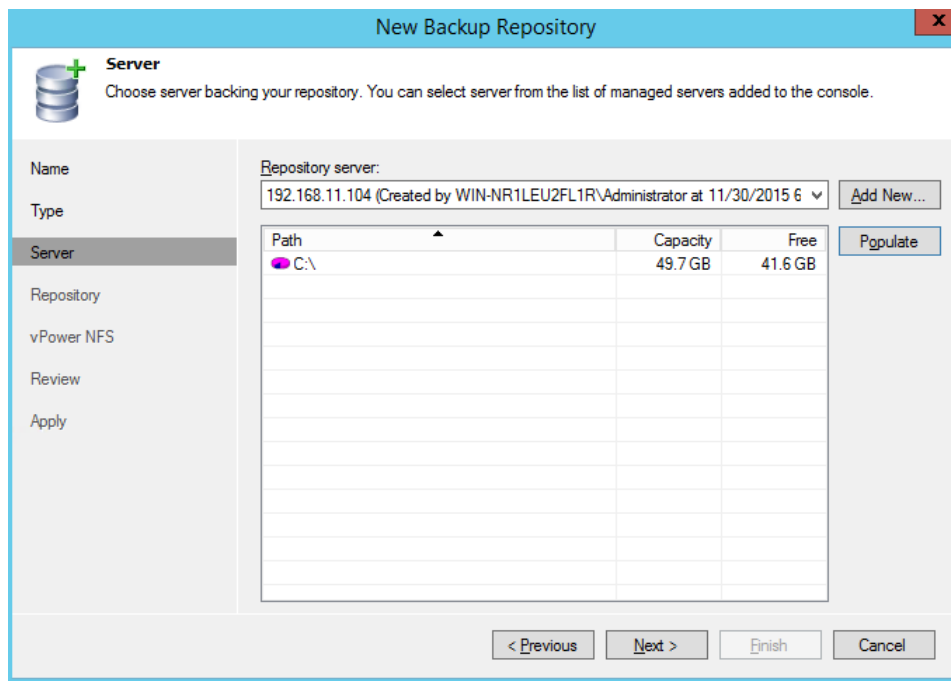
15. Click **Populate** to select the volume for the repository, and then click **Next**.

Figure 40-11: New Backup Repository - Server



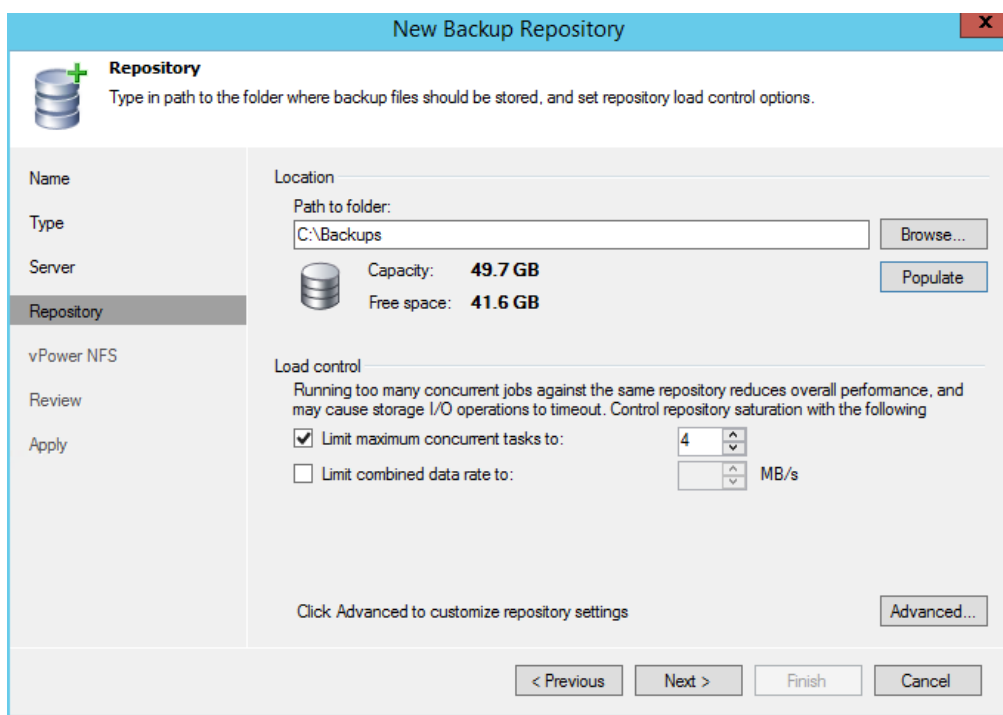
16. In the 'Path to folder' field, select the path to be used as the root for the repository.

Figure 40-12: New Backup Repository – Server C:\ Path



17. Click **Populate** to see available free space.
18. You can limit the number of concurrent tasks to the Repository, depending on the hardware resources, or limit the data rate, if needed. If you are running the repository on the CloudBond 365, you need to limit concurrent tasks to 1.
19. Click **Next**.

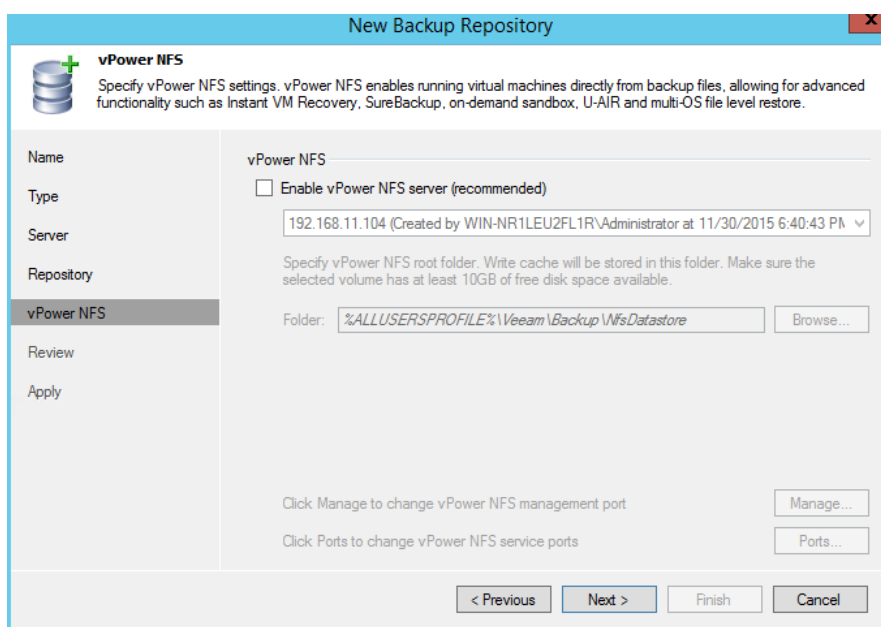
Figure 40-13: New Backup Repository - Repository



20. Clear the 'Enable vPower NFS server' check box to disable vPower NFS.

21. Click **Next**.

Figure 40-14: New Backup Repository - vPowerNFS



New Backup Repository

vPower NFS

Specify vPower NFS settings. vPower NFS enables running virtual machines directly from backup files, allowing for advanced functionality such as Instant VM Recovery, SureBackup, on-demand sandbox, U-AIR and multi-OS file level restore.

Name: vPower NFS

Type: ☐ Enable vPower NFS server (recommended)

Server: 192.168.11.104 (Created by WIN-NR1LEU2FL1R\Administrator at 11/30/2015 6:40:43 PM)

Repository: Specify vPower NFS root folder. Write cache will be stored in this folder. Make sure the selected volume has at least 10GB of free disk space available.

Folder: %ALLUSERSPROFILE%\Veeam\Backup\NfsDatastore Browse...

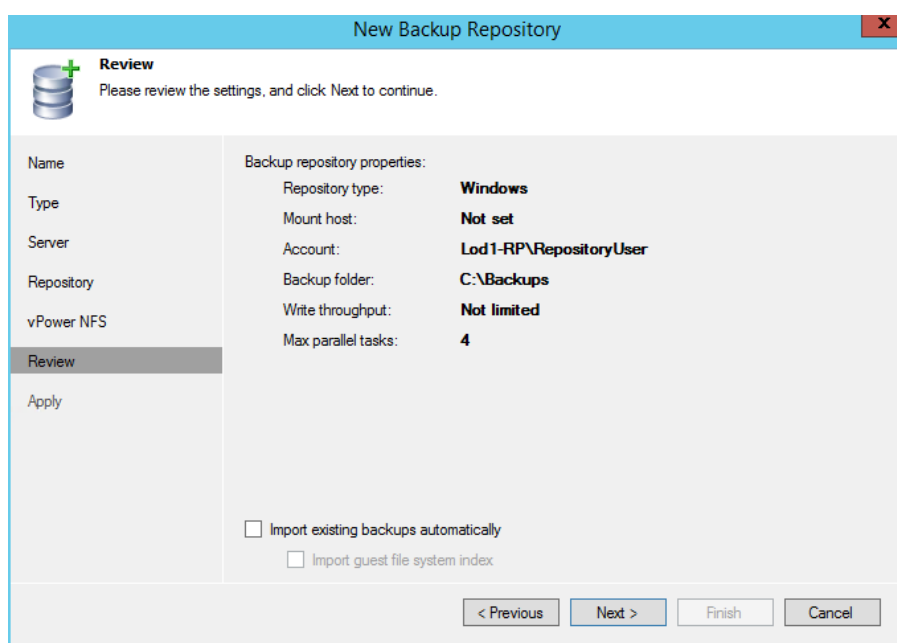
Click Manage to change vPower NFS management port Manage...

Click Ports to change vPower NFS service ports Ports...

< Previous Next > Finish Cancel

22. Click **Next**.

Figure 40-15: New Backup Repository - Review



New Backup Repository

Review

Please review the settings, and click Next to continue.

Name: Backup repository properties:

Type: Repository type: **Windows**

Server: Mount host: **Not set**

Repository: Account: **Lod1-RP\RepositoryUser**

vPower NFS: Backup folder: **C:\Backups**

Write throughput: **Not limited**

Max parallel tasks: **4**

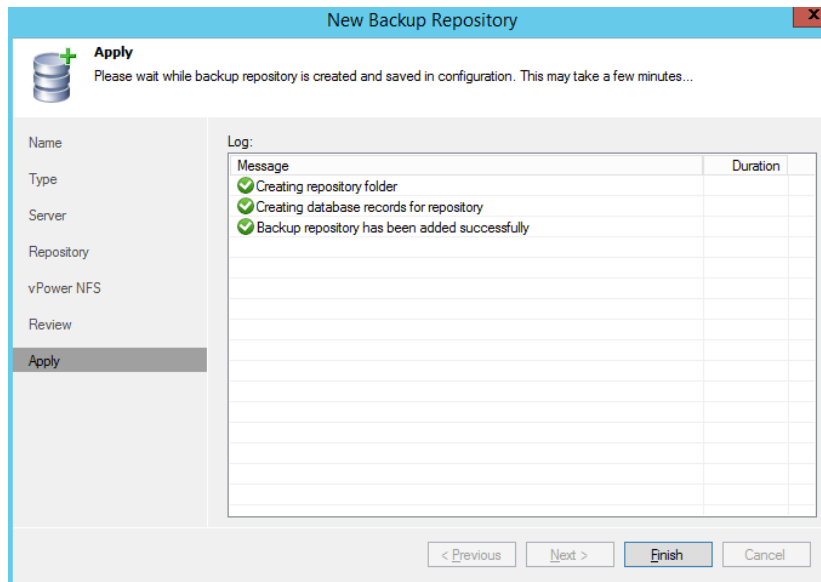
☐ Import existing backups automatically

☐ Import guest file system index

< Previous Next > Finish Cancel

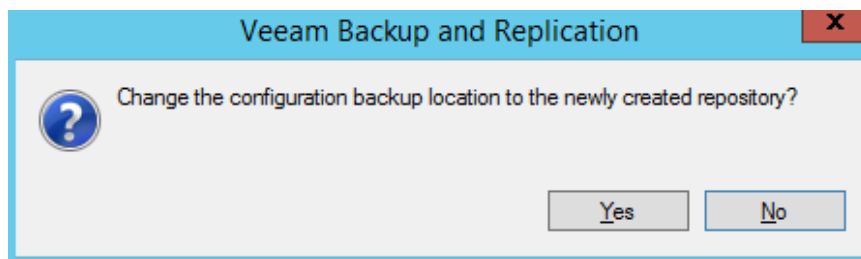
23. Click **Finish**.

Figure 40-16: New Backup Repository - Apply



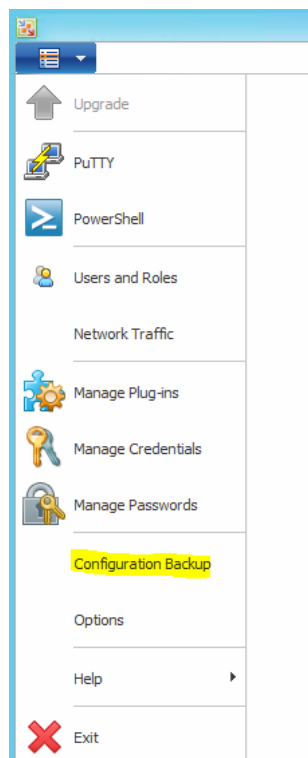
24. Set the new Repository as the default for configuration backup, and then click **Yes**.

Figure 40-17: VBR – Change Backup Location



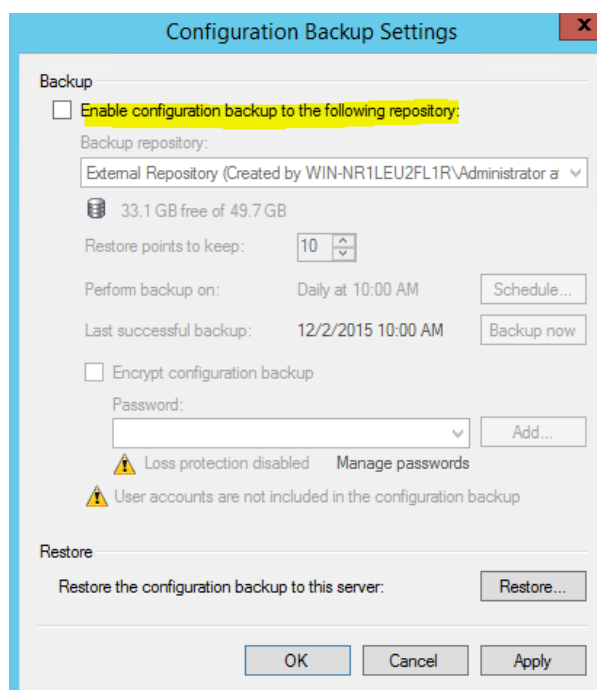
25. If the VBR is installed on the CloudBond 365, disable the configuration backup by doing the following:
 - a. From the VBR main console screen, click the Menu icon (in the top-left corner of the screen).
 - b. Select the **Configuration Backup** menu.

Figure 40-18: Configuration Backup



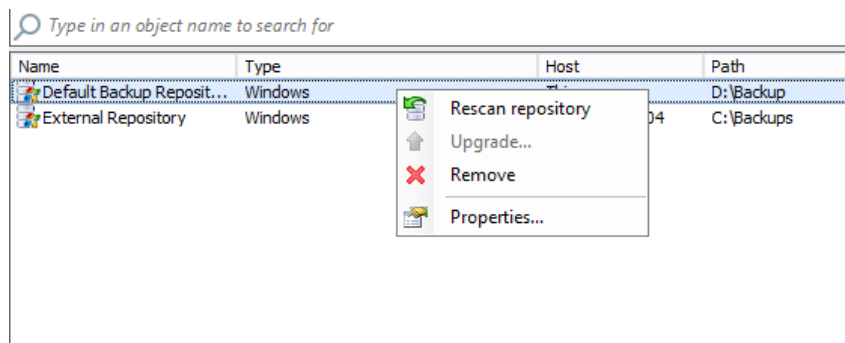
- c. Clear the 'Enable configuration backup to the following repository' check-box.

Figure 40-19: Configuration Backup Settings



26. Delete the old local repository by right-clicking it as shown in the screen below.
27. Select **Remove**.

Figure 40-20: Removing Old Repository



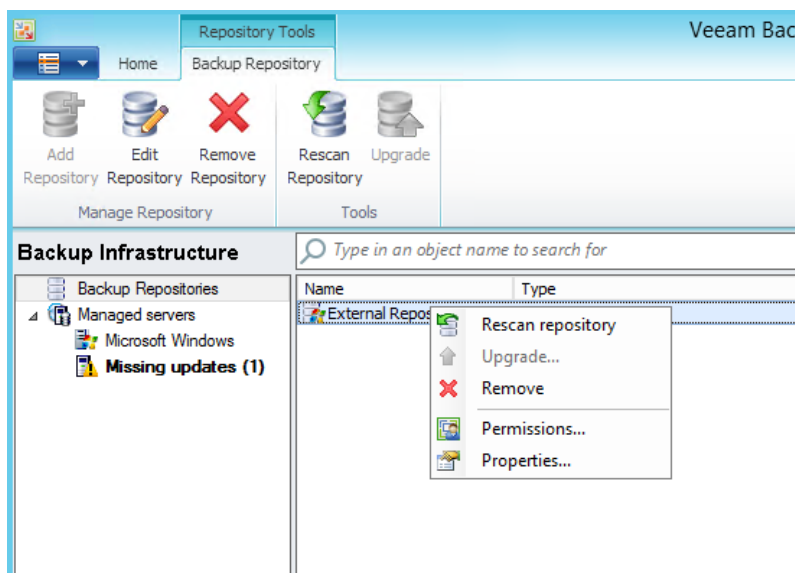
40.2 Configure Backup Repository Permissions

The following procedure describes how to configure Backup Repository permissions.

➤ **To configure Backup Repository permissions.**

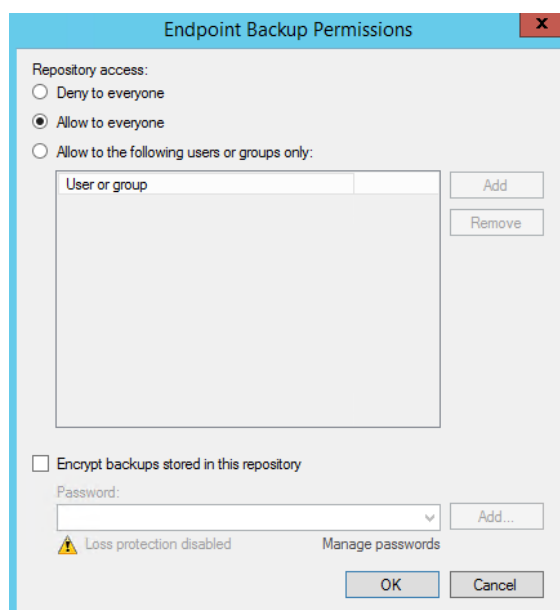
1. Open the VBR main console screen.
2. Press **Ctrl** and right-click on the External Repository that was previously added.
3. Select **Permissions**.

Figure 40-21: Backup Infrastructure



4. By default, the Repository is blocked for everyone. However, you can change the permissions to allow access to everyone as shown in the example below. Alternatively, you can define which users or groups can have access. For more information, refer to the *Veeam Endpoint Backup User Guide*.

Figure 40-22: Endpoint Backup Permissions



5. Select the 'Encrypt backup stored in this repository' check-box to define that all the data on the repository should be encrypted. If you want to do this, you need to define a password for the encryption. For more information, refer to the *Veeam Endpoint Backup User Guide Version*.
6. Click **OK**.

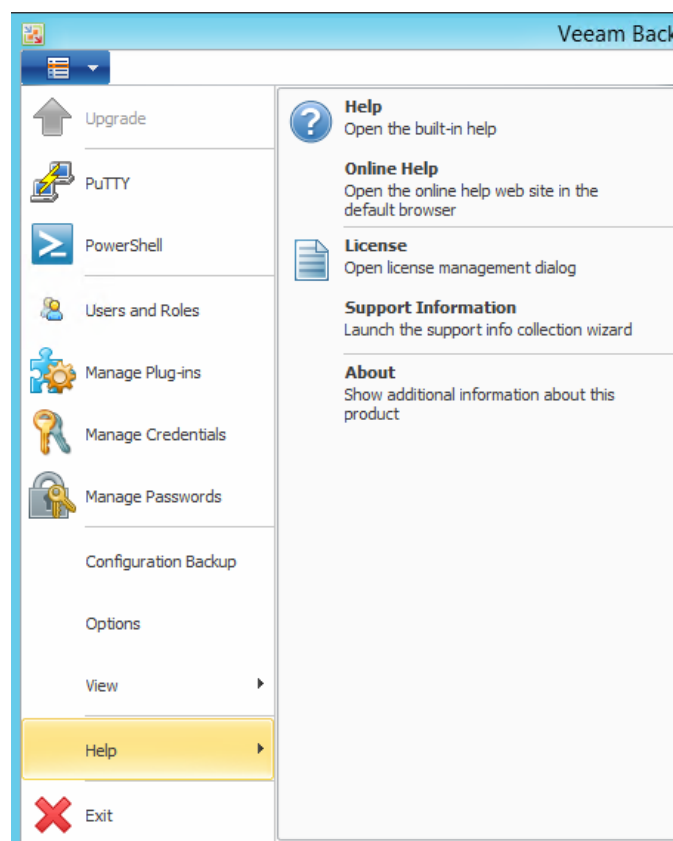
40.3 Installing the License

If the license was not supplied during the Installation step, you must install a license.

➤ **To install the license:**

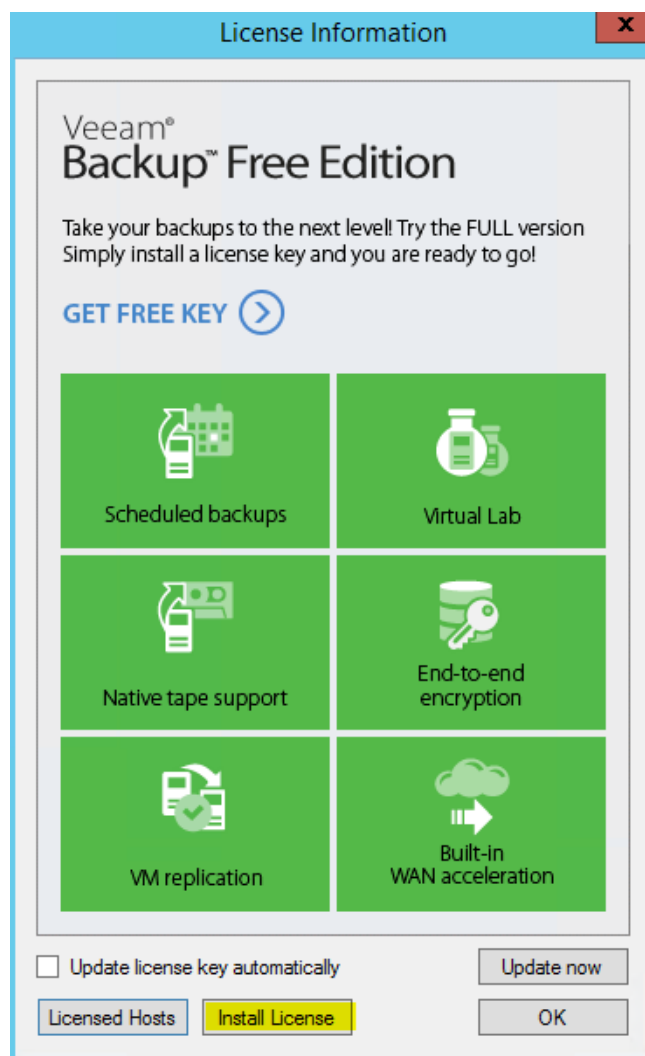
1. Open the VBR Console from the desktop by double-clicking the Veeam Backup menu icon.
2. Open the **Help** menu and navigate to the **License** sub-menu.

Figure 40-23: Help – License Menu



3. From the **License** sub-menu, click **License**.
4. Click **Install License** and select the license file.

Figure 40-24: License Information



40.4 Assigning VBR Console Credentials and VBR Roles

The account used to start the VBR console must have the Local Administrator permissions on the Veeam backup server.

You can assign one of the following roles to users or groups of users:

- Veeam Backup & Replication
- Veeam Restore Operator
- Veeam Backup Viewer
- Veeam Backup Operator
- Veeam Backup Administrator

A role assigned to the user defines the user activity scope and what operations in Veeam Backup & Replication the user can perform. Role security settings affect the following operations:

- Starting and stopping jobs
- Performing restore operations

By default, during installation the Veeam Backup Administrator role is assigned to users in the Local Administrators group. If you change the default settings, make sure that you assign the Veeam Backup Administrator role to the necessary user account. Changing the role is done through the Users and Roles menu option accessible from the main menu.

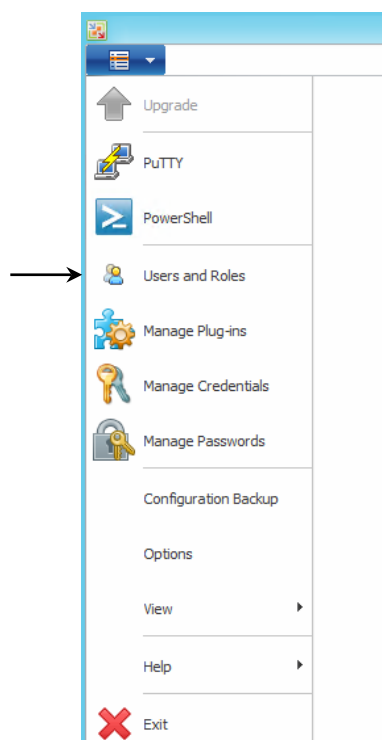
By default, the Local Administrators group is defined as the Veeam Backup Administrator.

You can confirm this by following this procedure.

➤ **To confirm the Veeam Backup Administrator:**

1. From the VBR main console screen, click the **Menu** icon (in the top-left corner of the screen); the following menu options appear:

Figure 40-25: Users and Roles



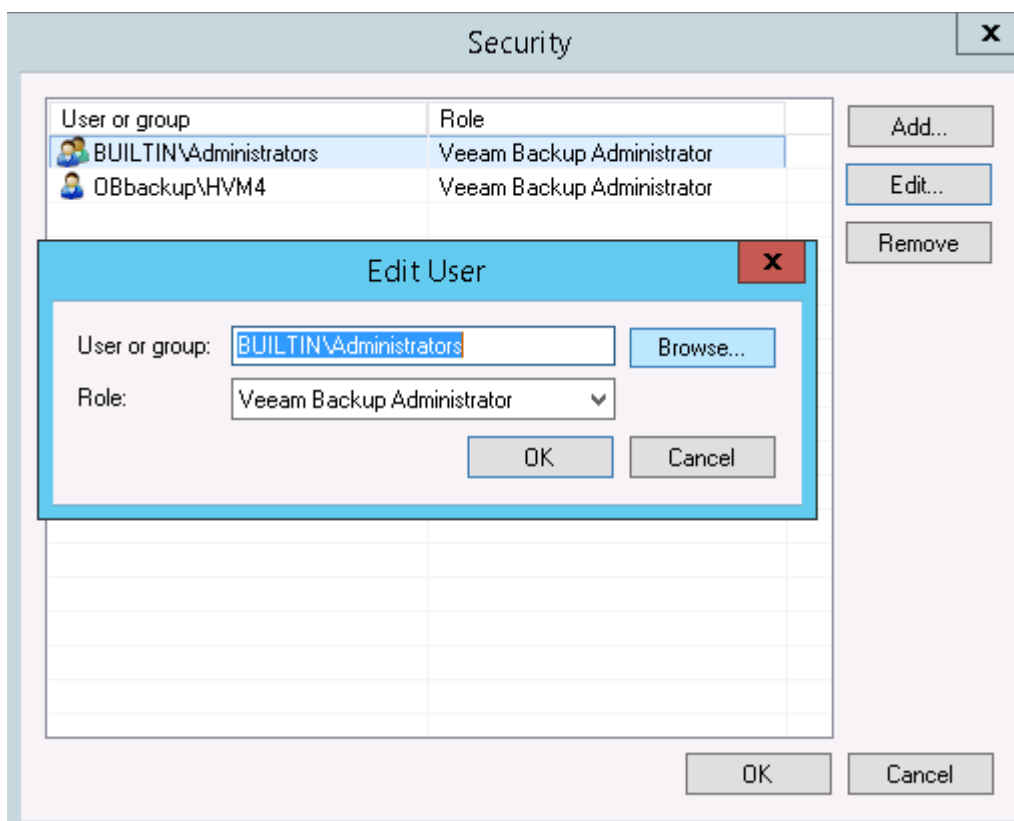
2. Select **Users and Roles**; the following screen appears.



Note: On the Mediant 800, where the host is the Domain Controller (DC), this is the CloudBond 365 domain Administrator group and not the local server Administrator group.

3. Select the User or Group, and then click **Edit**.
4. Confirm that the role is correct.

Figure 40-26: Security



40.4.1 Adding a User and Role for VEB

You need to add a user for the VEB and assign a role to it.



Notes:

- Every CloudBond 365 must have a different user (with a different user name) for the VEB because the name of the user is part of the directory path on the backup file system. Add a user that has local Administrator credentials e.g., CloudBondVEB1.
- If you have several CloudBond 365 devices that use the same backup repository, even if they are standalone, you must allocate different user names for the VEB.

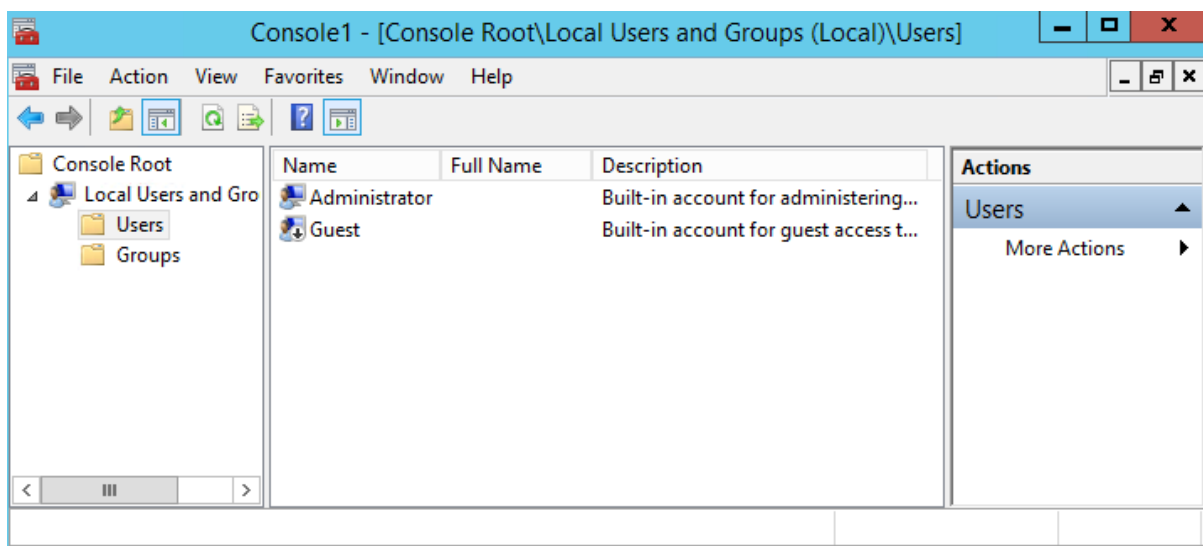
40.4.1.1 For CloudBond 365 Pro Box / Enterprise Box Editions (or VBR on External Server)

The following procedure describes how to add a new user for CloudBond 365 Pro Box / Enterprise Box Editions.

➤ **To add a new user for CloudBond 365 Pro Box / Enterprise Box Editions:**

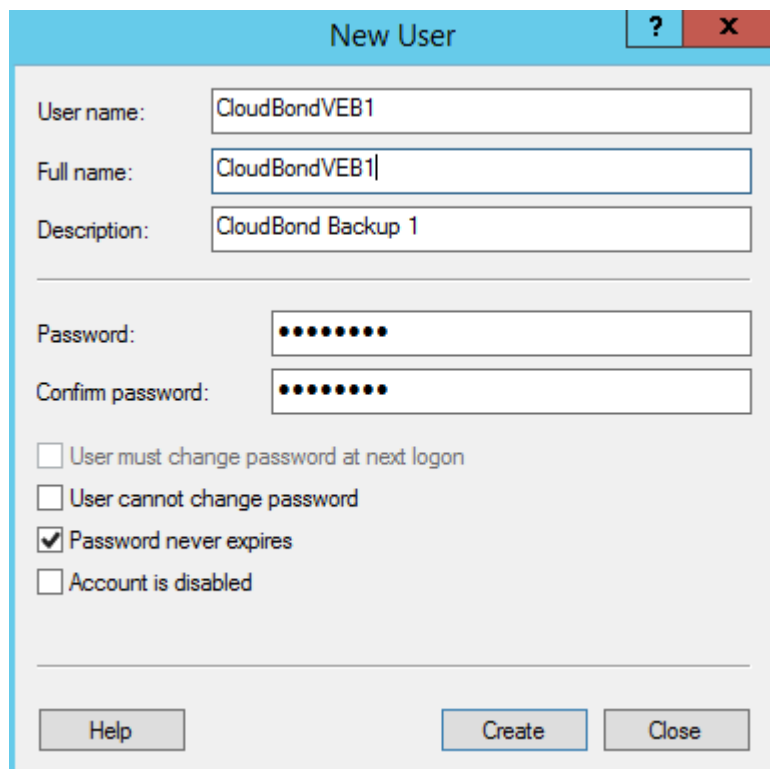
1. Create the user as a local Administrator that belongs to the Local Server Administrators group.
2. Open the Local User and Groups using Microsoft Management Console (MMC).

Figure 40-27: Local User and Groups



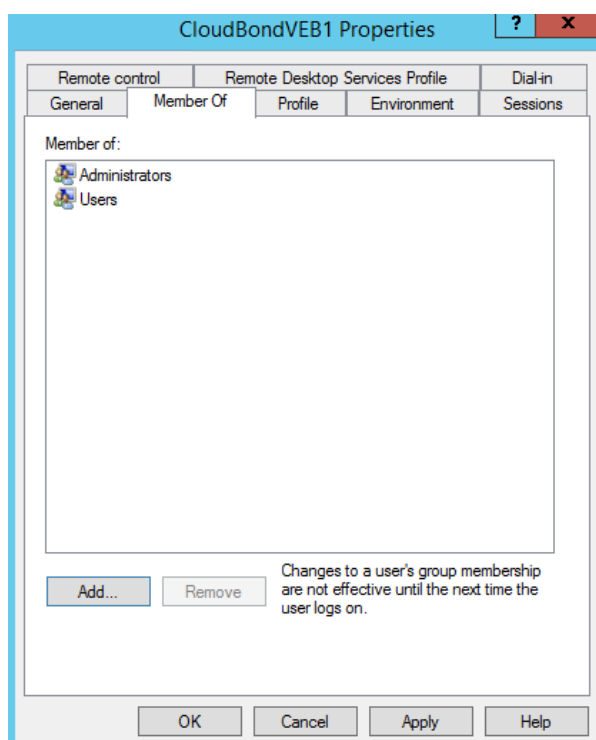
3. Enter the new user details on the New User screen.
4. Click **Create**.

Figure 40-28: Creating a New User



5. On the CloudBondVEB1 Properties screen, click the **Member of** tab.
6. Add the new user to the Local Administrators Group, and then click **Add**.
7. Click **OK**.

Figure 40-29: Adding to Administrators



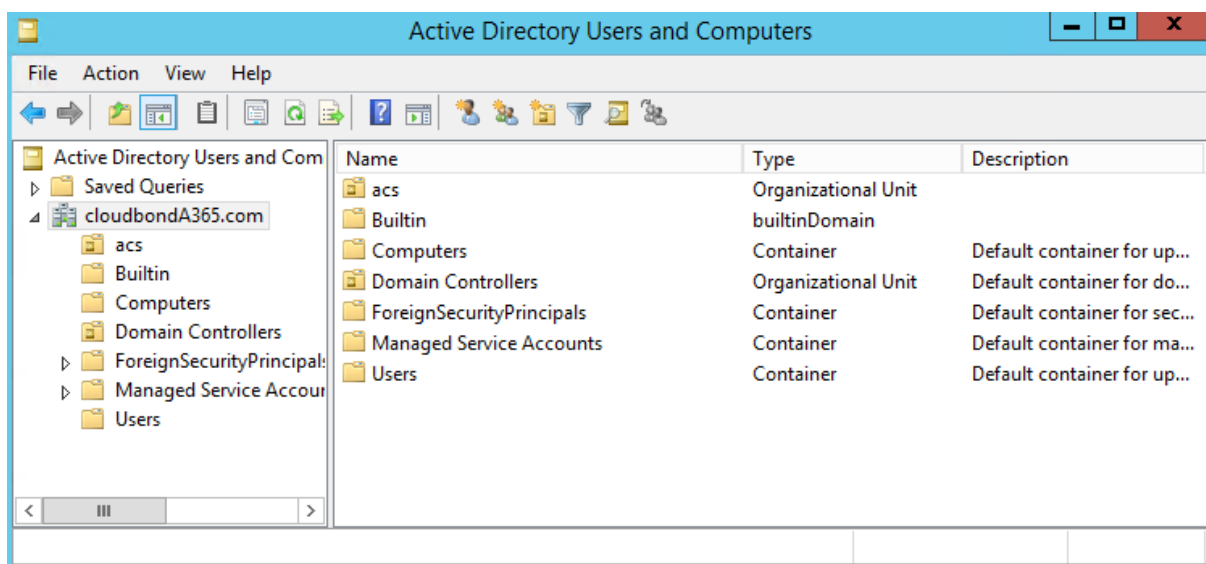
40.4.1.2 For CloudBond 365 Standard Box Edition

The following procedure describes how to add a new user for CloudBond 365 Standard Box Edition.

➤ **To add a new user for CloudBond 365 Standard Box Edition:**

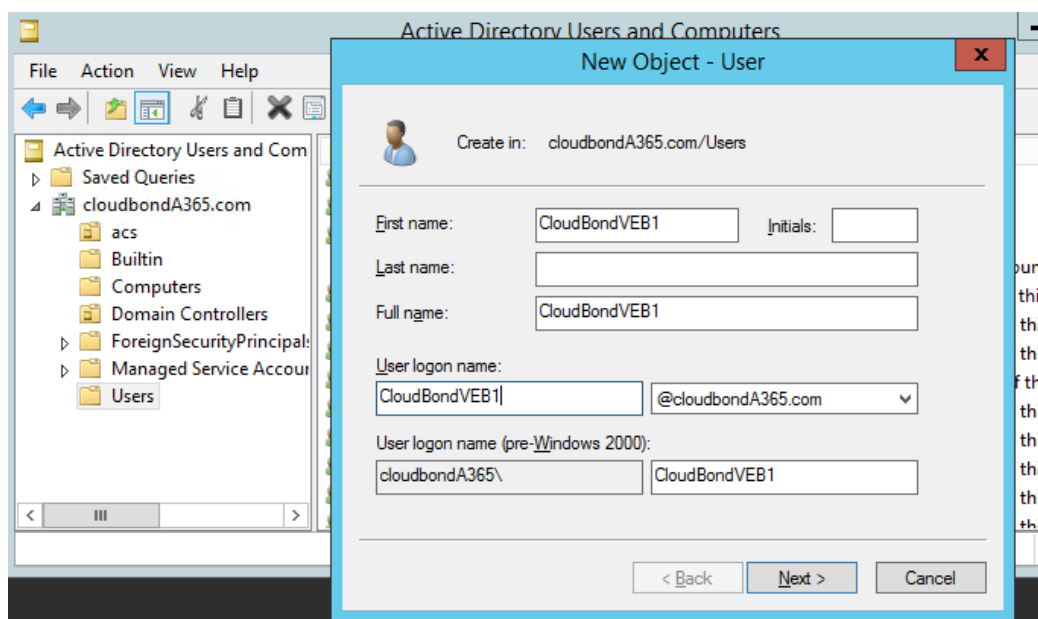
1. Create the new user on the CloudBond 365 domain which belongs to the CloudBond 365 domain Administrators group.
2. Open the **Active Directory User and Computers** tool.

Figure 40-30: Active Directory Users and Computers



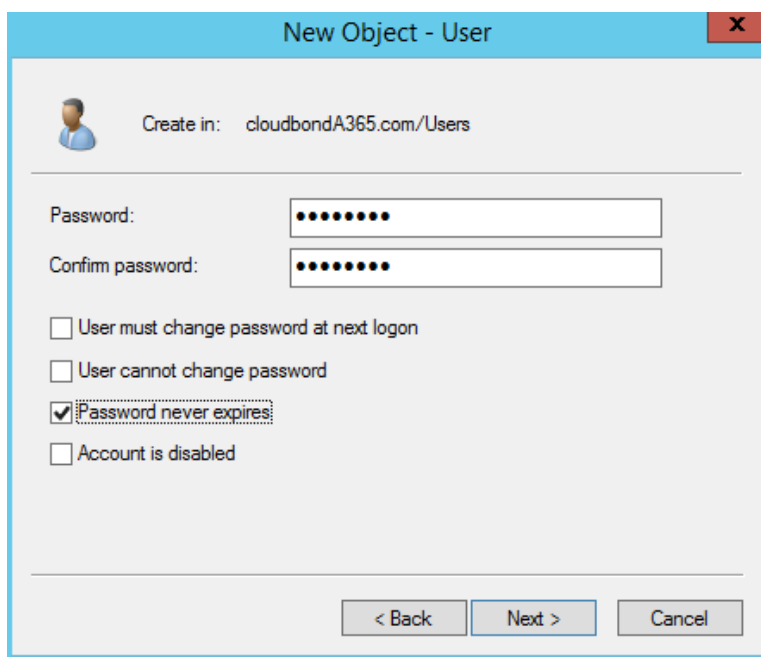
3. Select the **Users** folder and create a new user.
4. On the New Object – User screen, enter the name details, and then click **Next**.

Figure 40-31: New Object – Name Details



5. Enter the password credentials, and then click **Next**.

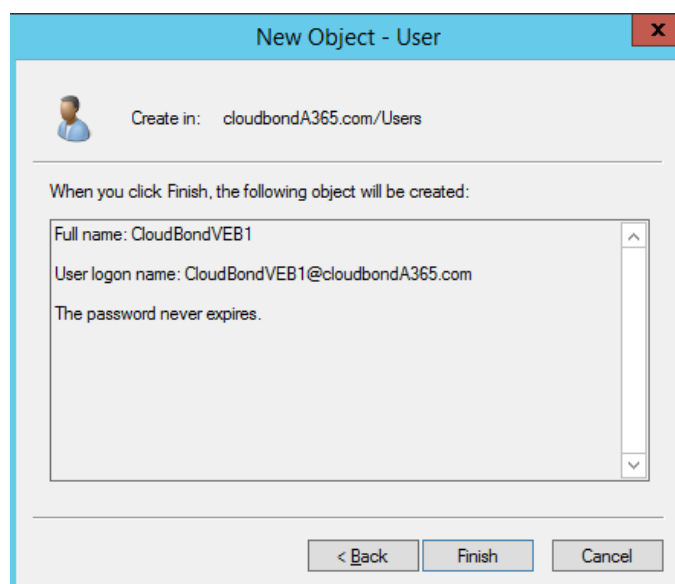
Figure 40-32: New Object – Password Details



The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It shows a user icon and the text "Create in: cloudbondA365.com/Users". Below this, there are two password input fields: "Password:" and "Confirm password:", both containing masked characters (dots). Below the password fields are four checkboxes: "User must change password at next login", "User cannot change password", "Password never expires" (which is checked), and "Account is disabled". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

6. Click **Next**.

Figure 40-33: New Object – Finish



The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It shows a user icon and the text "Create in: cloudbondA365.com/Users". Below this, there is a text area that says "When you click Finish, the following object will be created:". Inside this text area, the following information is displayed: "Full name: CloudBondVEB1", "User logon name: CloudBondVEB1@cloudbondA365.com", and "The password never expires." At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

7. Click **Finish**.

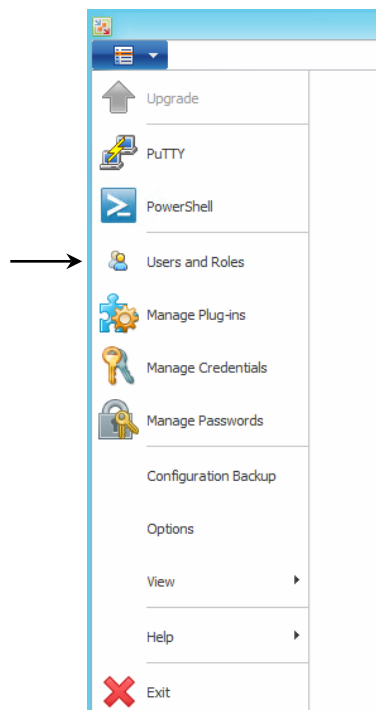
40.4.2 Assigning a Role for the VEB User

The following procedure below describes how to assign a role for the VEB user.

➤ **To assign a role for the VEB user:**

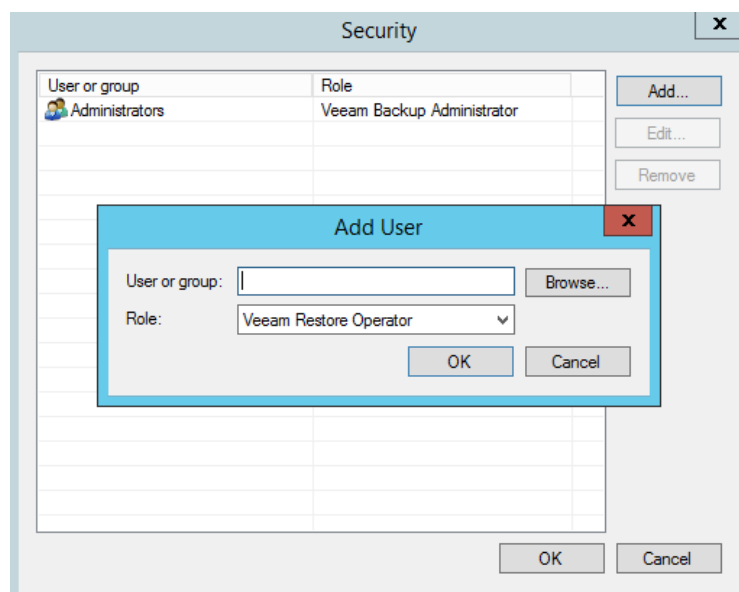
1. From the VBR main console screen, click the **Menu** icon (in the top-left corner of the screen); the following menu options appear:

Figure 40-34: Users and Roles



2. Select **Users and Roles**; the following screen appears.

Figure 40-35: Security



3. Click **Add**.
4. In the 'user or group' field, enter the user that was created before for the VEB or use

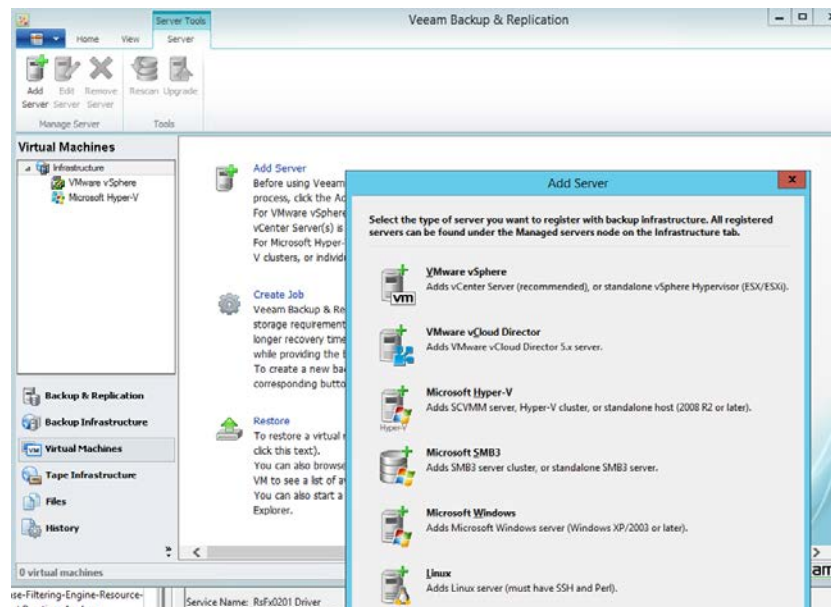
41 Adding CloudBond 365 Hyper-V to VBR

The following procedure describes how to add CloudBond 365 Hyper-V to VBR.

➤ **To add CloudBond 365 Hyper-V to VBR:**

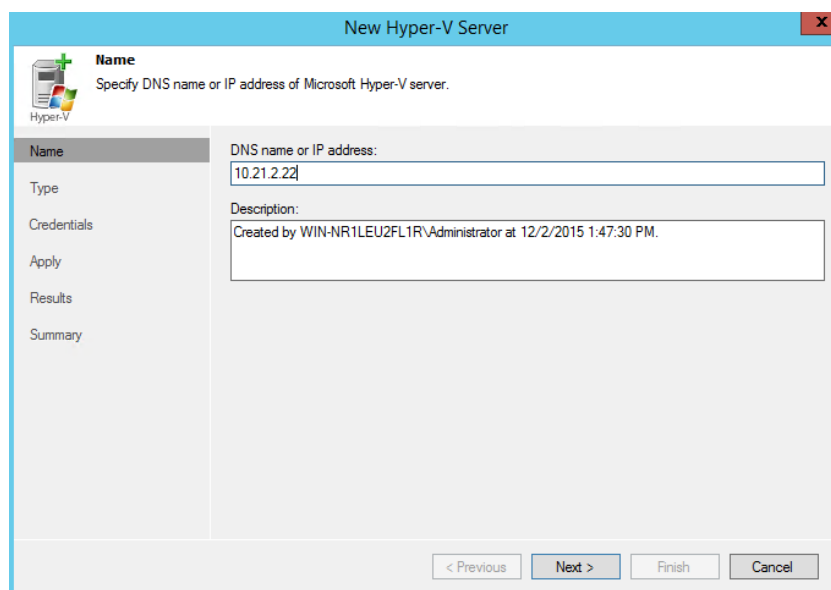
1. From the VBR main console screen, select **Virtual Machines**.
2. Select **Add Server**.
3. Select **Microsoft Hyper-V**.

Figure 41-1: Add Server



4. In the 'DNS name or IP address' field, enter the CloudBond 365 Host IP address.
5. In the 'Description' field add a description of the new Hyper-V server.

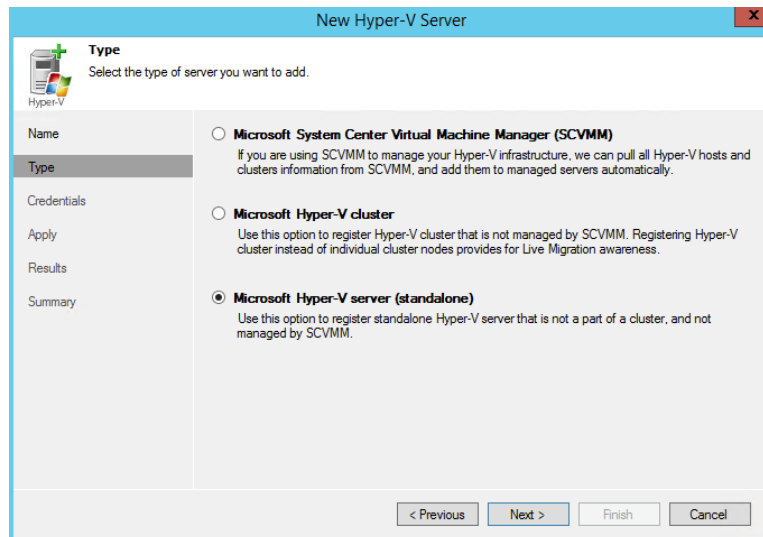
Figure 41-2: New Hyper-V Server



6. Click **Next**.

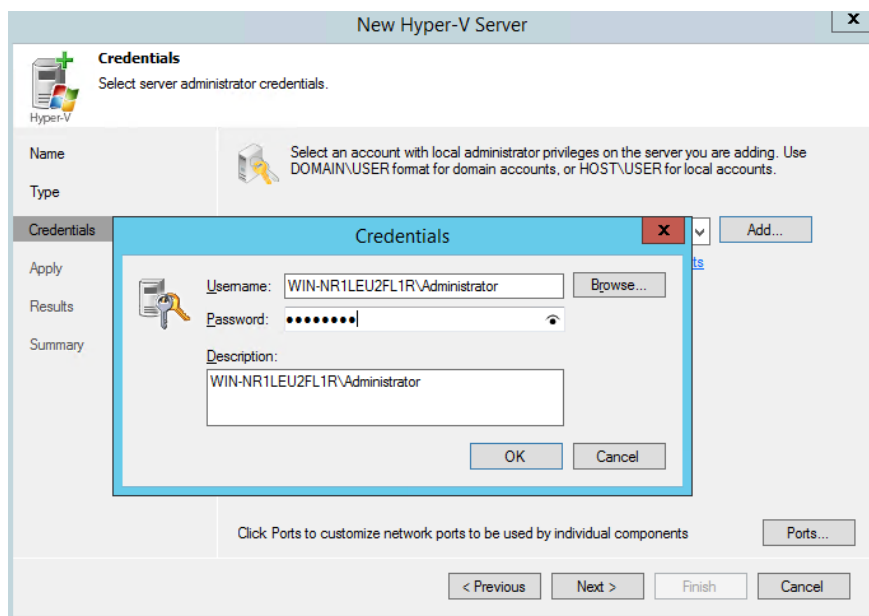
7. Click the **Microsoft Hyper-V Server (standalone)** option, and then click **Next**.

Figure 41-3: New Hyper-V Server - Type



8. You must have local Administrator credentials on the server.
9. From the 'Credentials' drop-down list, select an existing or add credentials to access the Hyper-V host.

Figure 41-4: New Hyper-V Server - Credentials



Notes:

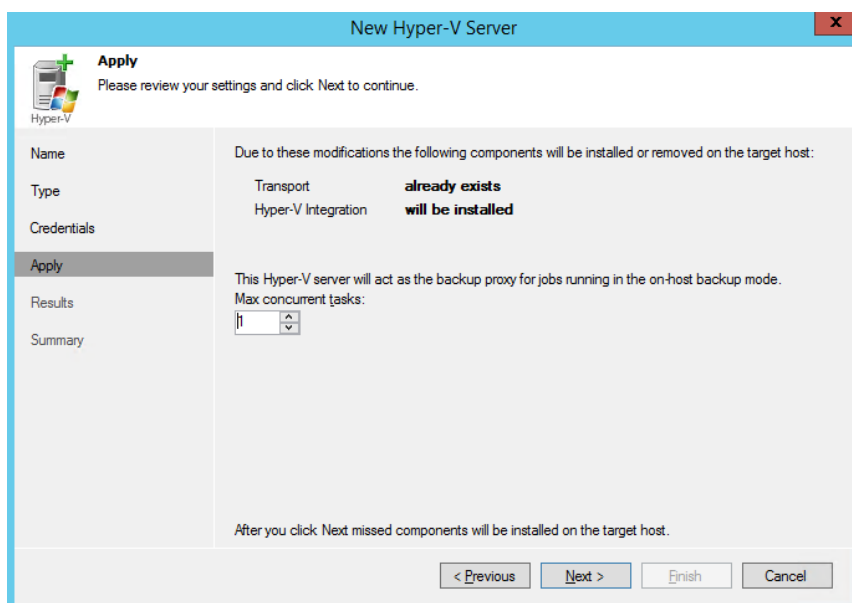
- If CloudBond 365 is backed up, the host can be a Domain Controller. If so, use a User which belongs to the Domain Administrators (e.g., CloudBond 365/Administrator).
- If the HyperV host is not a Domain Controller, use the following format for the user name: <computer Name>\<user>



10. On the Credentials screen, click **OK**, and then click **Next**. The VBR examines the Target server, which can take several minutes.

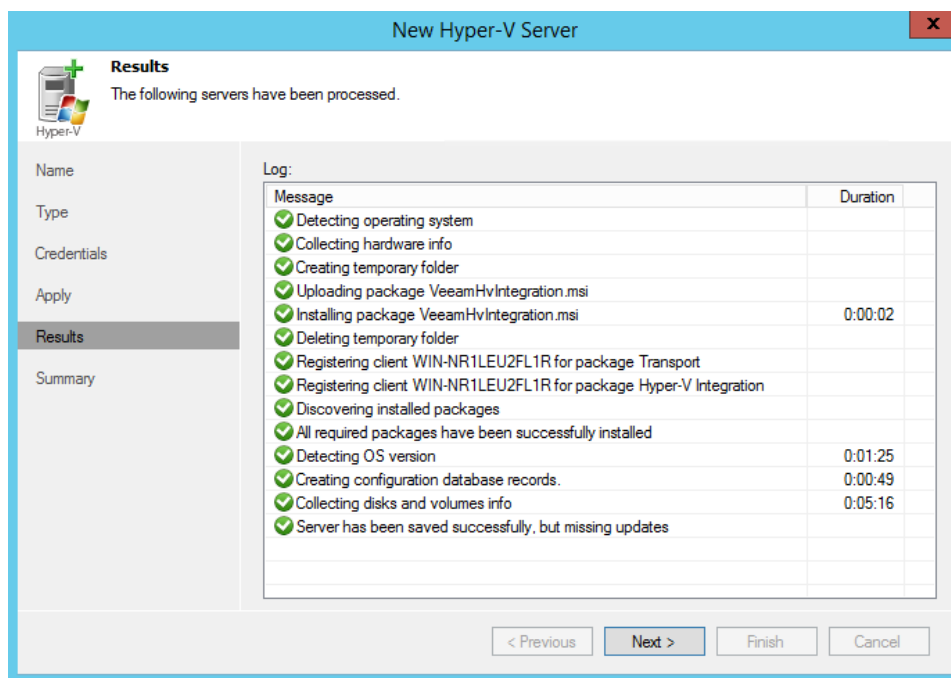
11. In the 'Max concurrent tasks' field, select **1**, and then click **Next**.

Figure 41-5: New Hyper-V Server - Apply



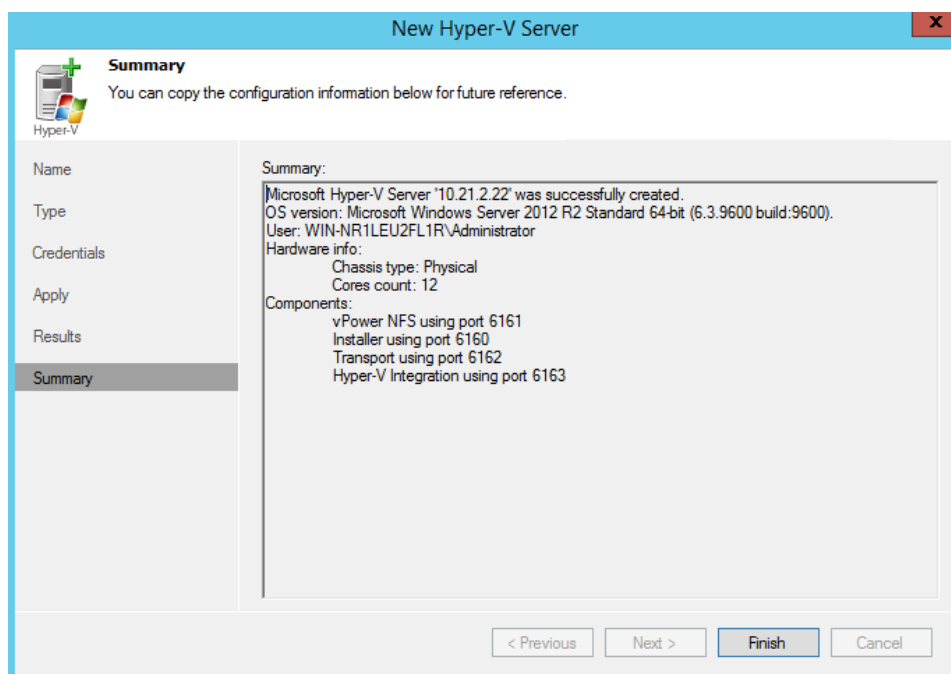
12. The missing components are installed on the CloudBond 365. This takes several minutes.
13. On the Results screen, click **Next**.

Figure 41-6: New Hyper-V Server - Results



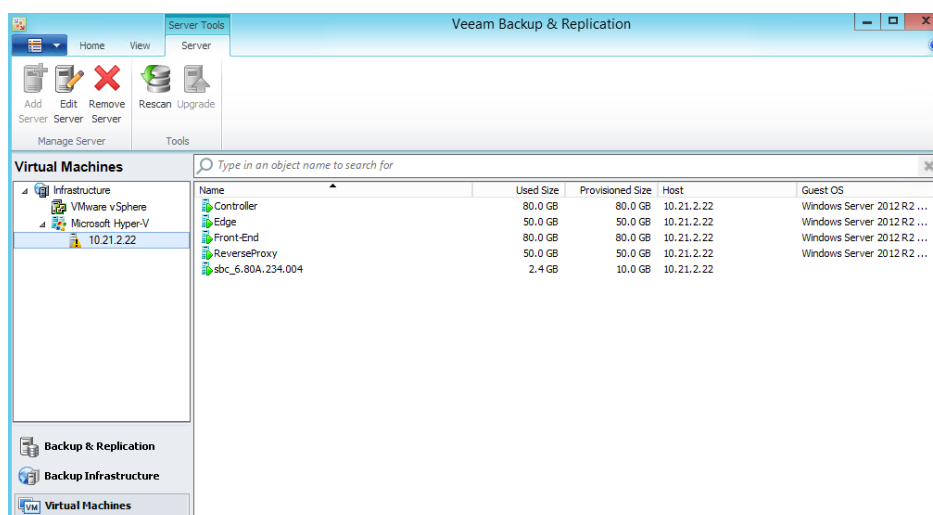
14. On the Summary screen, click **Finish**.

Figure 41-7: New Hyper-V Server - Summary



15. The VBR informs you which Windows updates are missing and need to be installed.
16. The Microsoft Hyper-V server with its Virtual Machines appears on the screen.

Figure 41-8: Microsoft Hyper-V Server



42 Configuring Backup Jobs

The following procedures describe how to configure backup jobs.

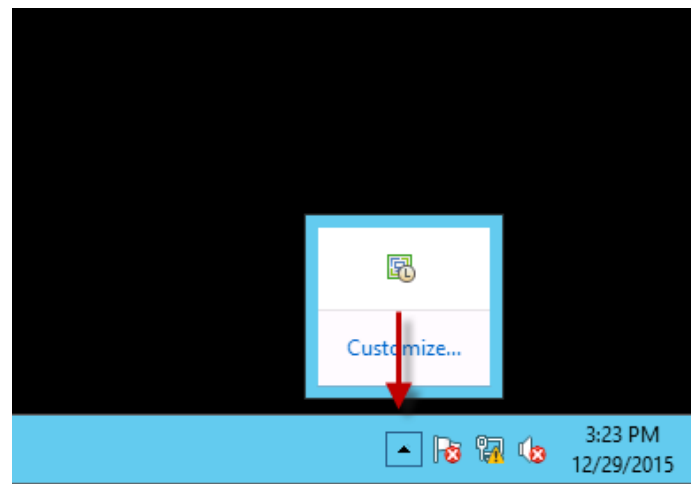
42.1 Configuring VEB Host Backup

The following procedure describes how to configure the backup for the host server.

➤ **To configure the backup for the host server:**

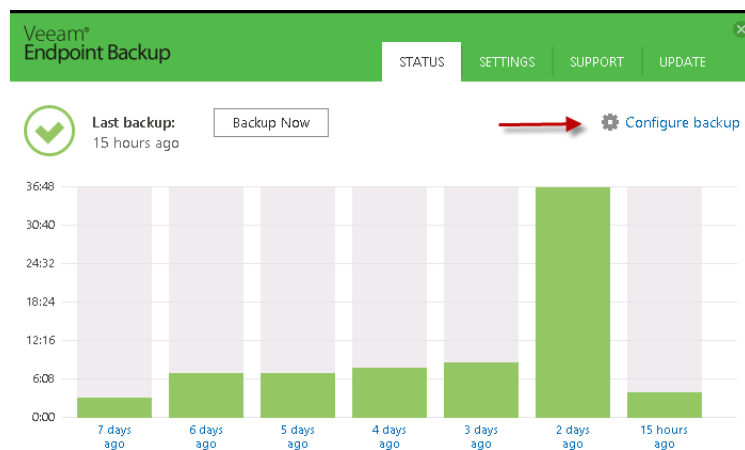
1. From the Notifications Area icons, double-click on VEB.

Figure 42-1: Notifications Area Icons



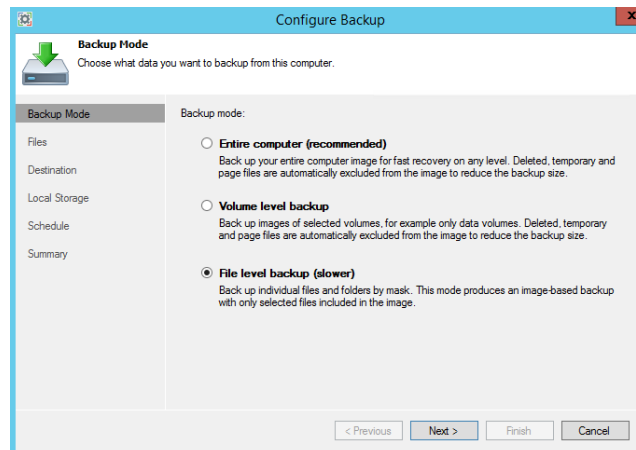
2. Run **Configure Backup**.

Figure 42-2: Configure Backup



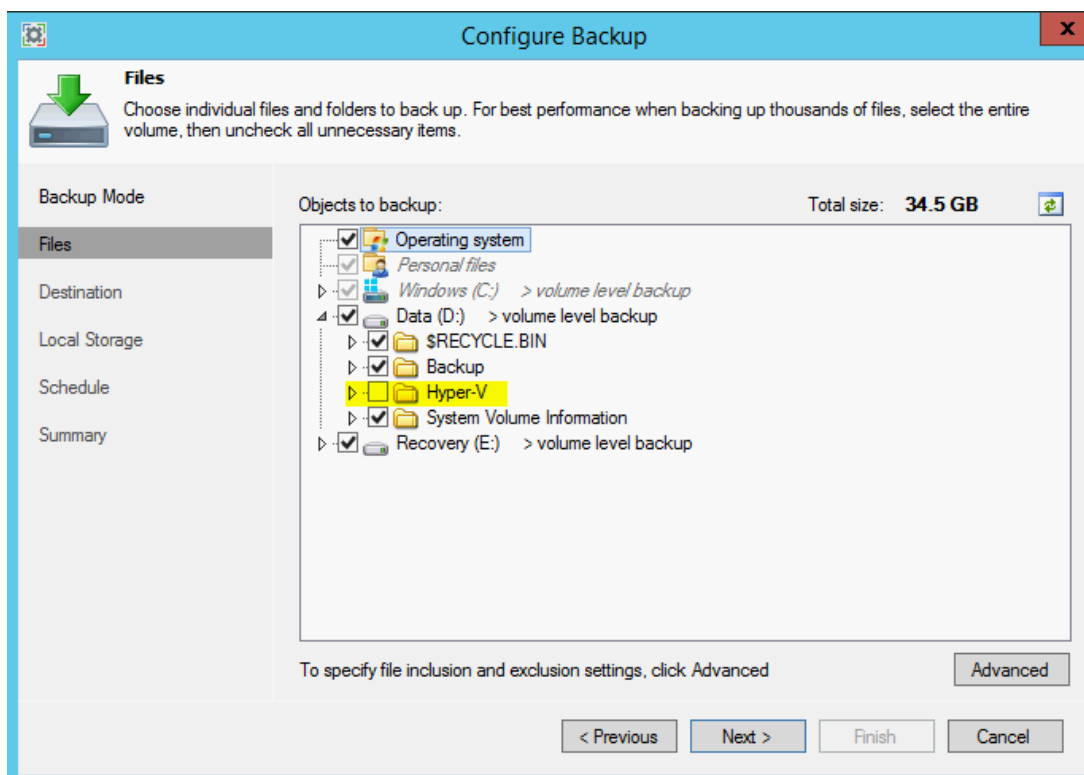
3. Click the **File level backup (slower) mode** option, and then click **Next**.

Figure 42-3: Configure Backup



4. Select the 'Operating system' check box (automatically checks Volume C and personal files),
5. Select 'Volume D'.
6. Clear the Hyper-V folder check box under Volume D.
7. Click **Next**.

Figure 42-4: Configure Backup - Files



Note: Volume E: is used only when installing the CloudBond 365. All its information exists on the CloudBond 365 USB. If you want to back it up, select the Volume E check box as well.

8. Select the **Veeam Backup & Replication repository** option as the Destination, and then click **Next**.

Figure 42-5: Configure Backup - Destination

Configure Backup

Destination
Choose where you want to backup your data to. We highly recommend that you do not store your backups on the same computer that you are protecting.

Backup Mode
Files
Destination
Backup Server
Backup Repository
Schedule
Summary

☐ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

☐ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

☒ **Veeam Backup & Replication repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication 8.0 Update 2 or later server.

< Previous Next > Finish Cancel

9. On the Backup Server screen, enter the VBR IP address that runs on the CloudBond 365 host or on the external one (if you selected to run it on an external server).
10. Enter the VEB credentials that you defined in Section 40.4.1, and then click **Next**.

Figure 42-6: Configure Backup – Backup Server

Configure Backup

Backup Server
Specify a Veeam Backup & Replication server to query for backup repositories available to you.

Backup Mode
Files
Destination
Backup Server
Backup Repository
Schedule
Summary

Veeam backup server name or IP address:
10.21.2.22

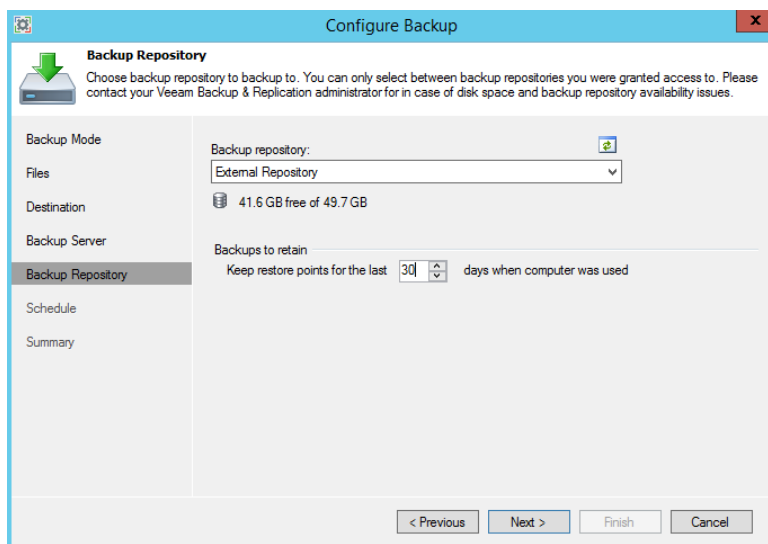
☒ **Specify your personal credentials:**

Username: CloudBondVEB1
Password:
Port: 10001

< Previous Next > Finish Cancel

11. Select the Backup Repository from the drop-down list.
12. In the 'backups to retain' field, select how many backups should be retained, and then click **Next**

Figure 42-7: Configure Backup – Backup Repository



Configure Backup

Backup Repository
Choose backup repository to backup to. You can only select between backup repositories you were granted access to. Please contact your Veeam Backup & Replication administrator for in case of disk space and backup repository availability issues.

Backup repository: External Repository

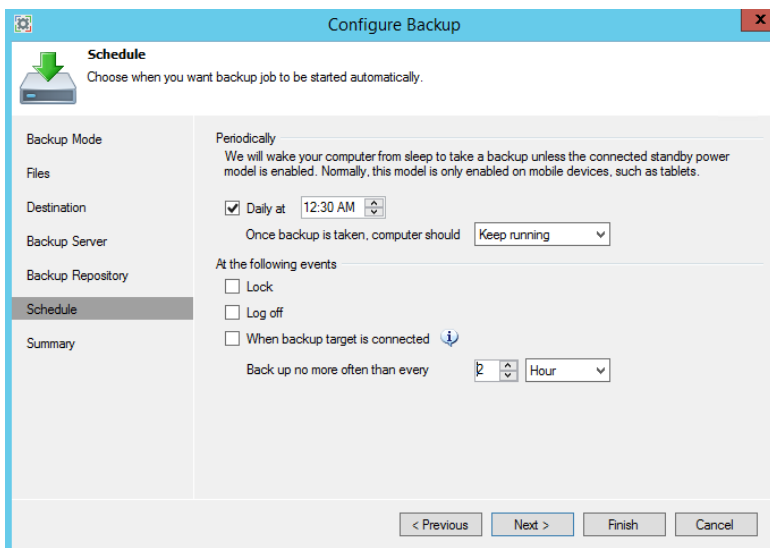
41.6 GB free of 49.7 GB

Backups to retain: 30 days when computer was used

< Previous Next > Finish Cancel

13. Set the time to perform the backup. (The preferred time is at night when the system is less loaded.)
14. Click **Next**.

Figure 42-8: Configure Backup – Schedule



Configure Backup

Schedule
Choose when you want backup job to be started automatically.

Periodically
We will wake your computer from sleep to take a backup unless the connected standby power model is enabled. Normally, this model is only enabled on mobile devices, such as tablets.

☒ Daily at 12:30 AM

Once backup is taken, computer should: Keep running

At the following events

☐ Lock

☐ Log off

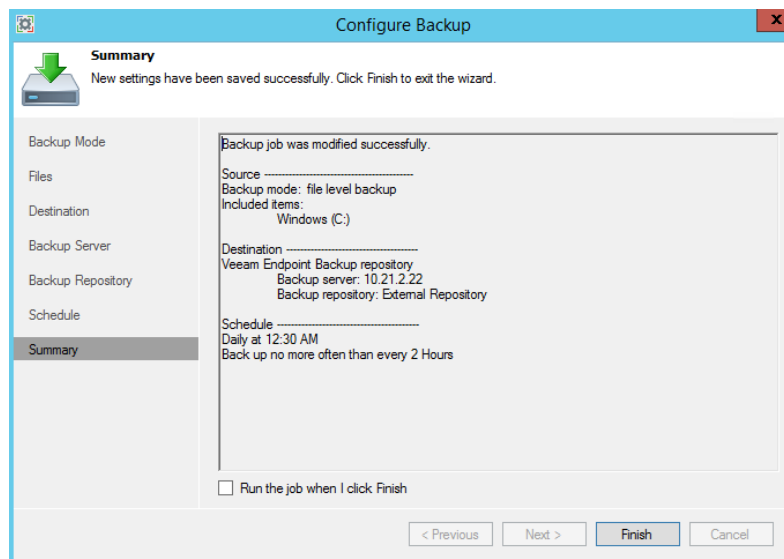
☐ When backup target is connected

Back up no more often than every 2 Hour

< Previous Next > Finish Cancel

15. You can check the 'Run the job when I click Finish' check box, to perform a full backup now. This is recommended so you can check that the backup is correctly set.
16. Click **Finish**.

Figure 42-9: Configure Backup – Summary



17. If you selected to perform a backup now, you can monitor the backup from:
 - **VEB Control Panel:** Navigate to **Start > Control Panel**.

Figure 42-10: Monitoring Backup with VEB Control Panel

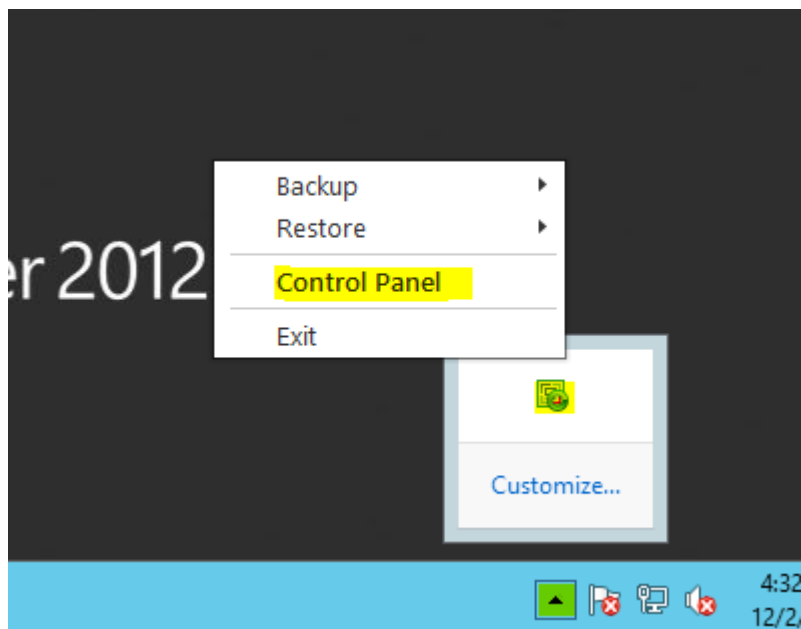
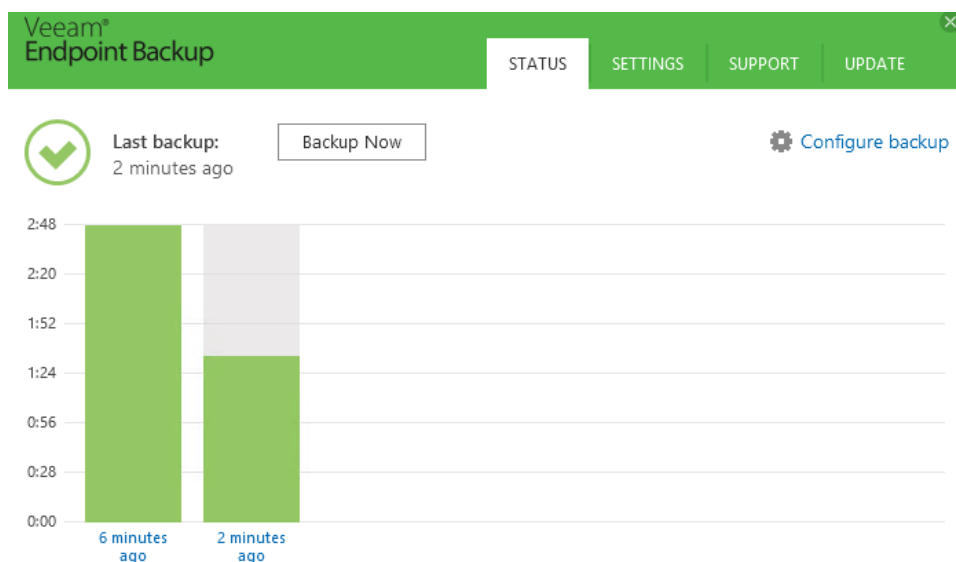
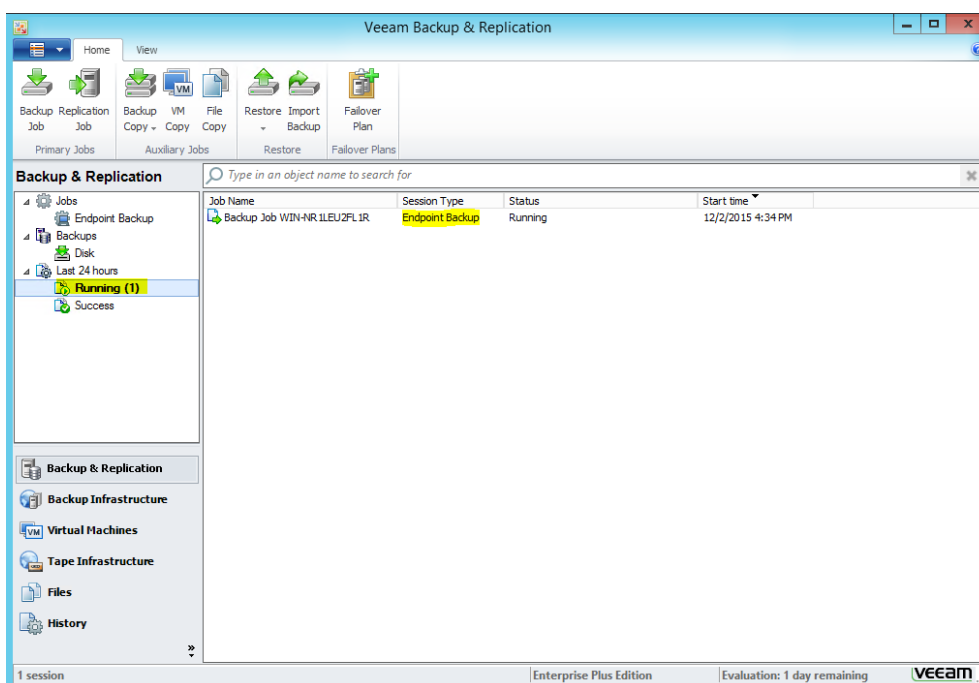


Figure 42-11: Monitoring Backup with VEB Control Panel - Status



- **VBR Jobs:** Click **Running** to view display.

Figure 42-12: Monitoring Backup with VBR Jobs



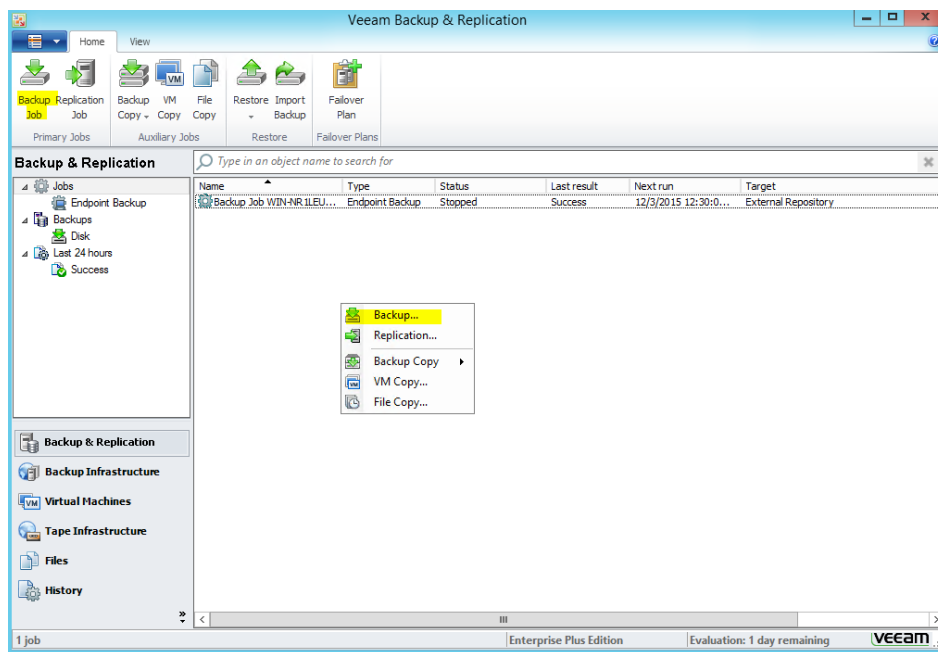
42.2 Configuring VBR VMs Backup

The following procedure describes how to configure the VBR backup for the VMs.

➤ **To set the backup for the Virtual Machines on the CloudBond 365 server:**

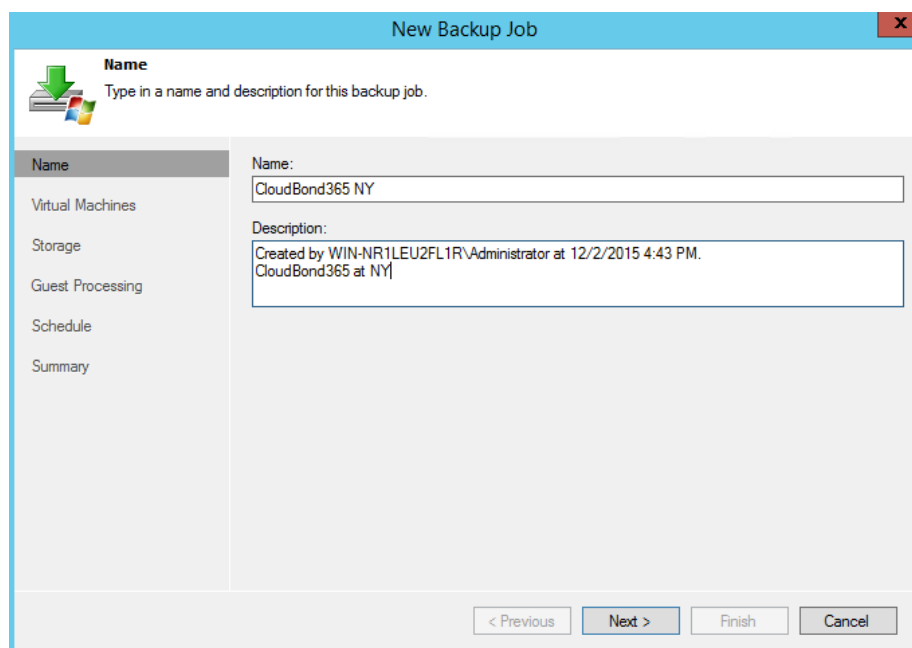
1. Run Veeam Backup and Replication (VBR).
2. Create a backup job from the **Home** menu or by right-clicking the **Jobs** window.

Figure 42-13: VBR Jobs - Backup



3. Enter the name and description and then click **Next**.

Figure 42-14: New Backup Job



4. Select **Add** to add VMs to the job.

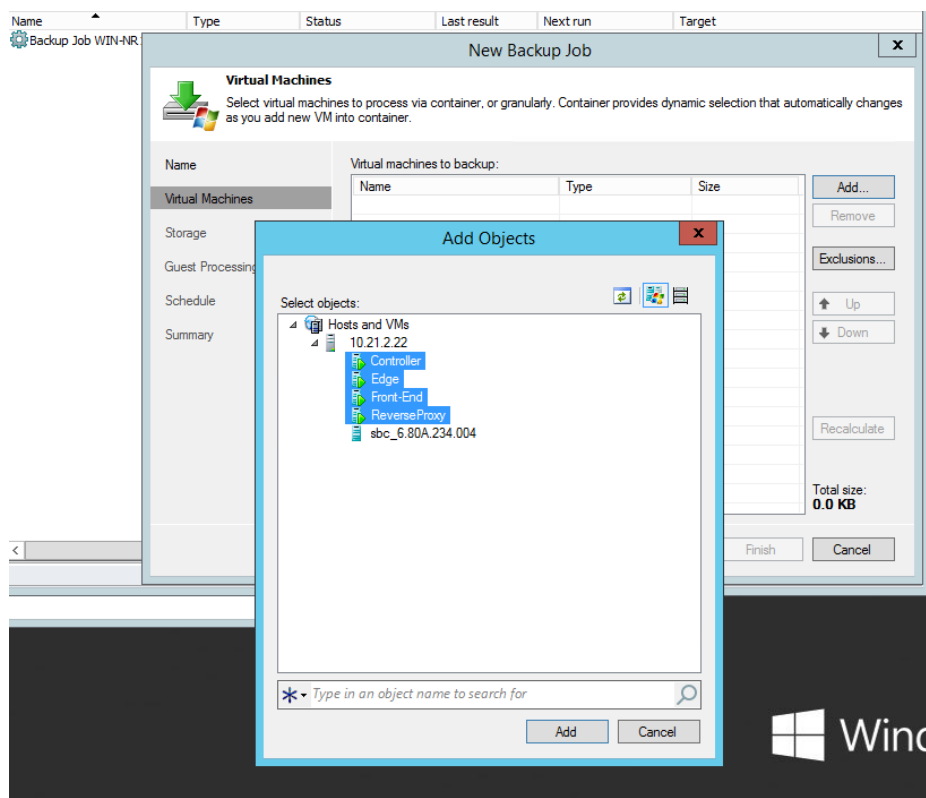
5. Select all the VMs **except the SBC**. The VMs list is according to the CloudBond 365 model and setup that was selected. The number of VMs that are allowed to be backed up is calculated according to your license.



Note: To back up the SBC, it is recommended to manually back up the SBC Settings INI file. For more information, refer to the Saving Configuration sub-section of the *AudioCodes SBC User's Manual*.

6. Click **Add**.

Figure 42-15: Add Objects



7. Click **Next**.

Figure 42-16: New Backup Job – Virtual Machines

Virtual Machines
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.

Name	Type	Size
Controller	VM	80.0 GB
Edge	VM	50.0 GB
Front-End	VM	80.0 GB
ReverseProxy	VM	50.0 GB

Total size: **260.0 GB**

< Previous Next > Finish Cancel

8. Confirm that the correct repository has been selected and that the number of restore points to keep is correct.
9. Click **Next**.

Figure 42-17: New Backup Job – Storage

Storage
Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy:
Off-host backup (automatic proxy selection) Choose...

Backup repository:
External Repository (Created by WIN-NR1LEU2FL1R\Administrator at 11/30/201) Map backup

Retention policy
Restore points to keep on disk: 14 ⓘ

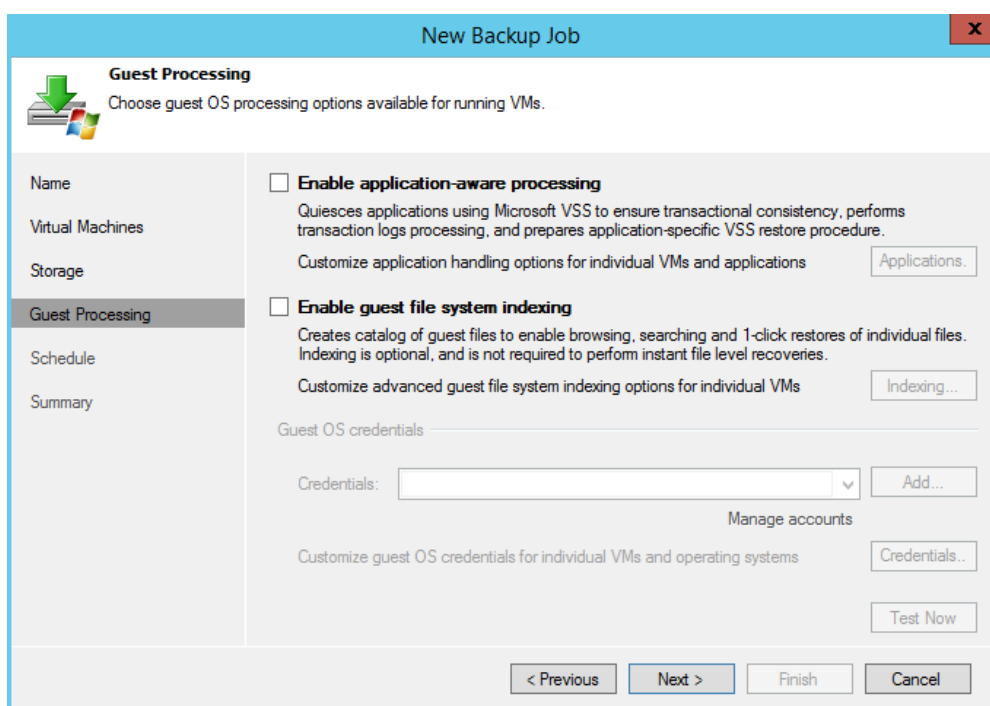
☐ Configure secondary destinations for this job
Use the backups produced by this job to satisfy backup requirement by archiving backups to tape, or efficiently creating remote backups and replicas over WAN.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. Advanced

< Previous Next > Finish Cancel

10. Click **Next**.

Figure 42-18: New Backup Job – Guest Processing



New Backup Job

Guest Processing
Choose guest OS processing options available for running VMs.

Name
Virtual Machines
Storage
Guest Processing
Schedule
Summary

☐ **Enable application-aware processing**
Quiesces applications using Microsoft VSS to ensure transactional consistency, performs transaction logs processing, and prepares application-specific VSS restore procedure.
Customize application handling options for individual VMs and applications [Applications...](#)

☐ **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual VMs [Indexing...](#)

Guest OS credentials

Credentials: [Add...](#)

Manage accounts

Customize guest OS credentials for individual VMs and operating systems [Credentials..](#)

[Test Now](#)

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

11. Select the 'Backup window' check box to terminate the job if it exceeds the allowed backup window.



Note: If the job does not complete within the allocated backup window, it is terminated to prevent a snapshot commit during production hours.

12. Define the schedule for the job and click **Create**.



Note: It is recommended to schedule this backup job at least 60 minutes later than the VEB backup scheduled time.

Figure 42-19: New Backup Job – Schedule

New Backup Job

Schedule
Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

☒ **Run the job automatically**

☒ **Daily at this time:** 2:00 AM Everyday Days...

☐ **Monthly at this time:** 10:00 PM Fourth Saturday Months...

☐ **Periodically every:** 1 Hours Schedule...

☐ **After this job:**

Automatic retry

☒ **Retry failed VMs processing:** 3 times

Wait before each retry attempt for: 10 minutes

Backup window

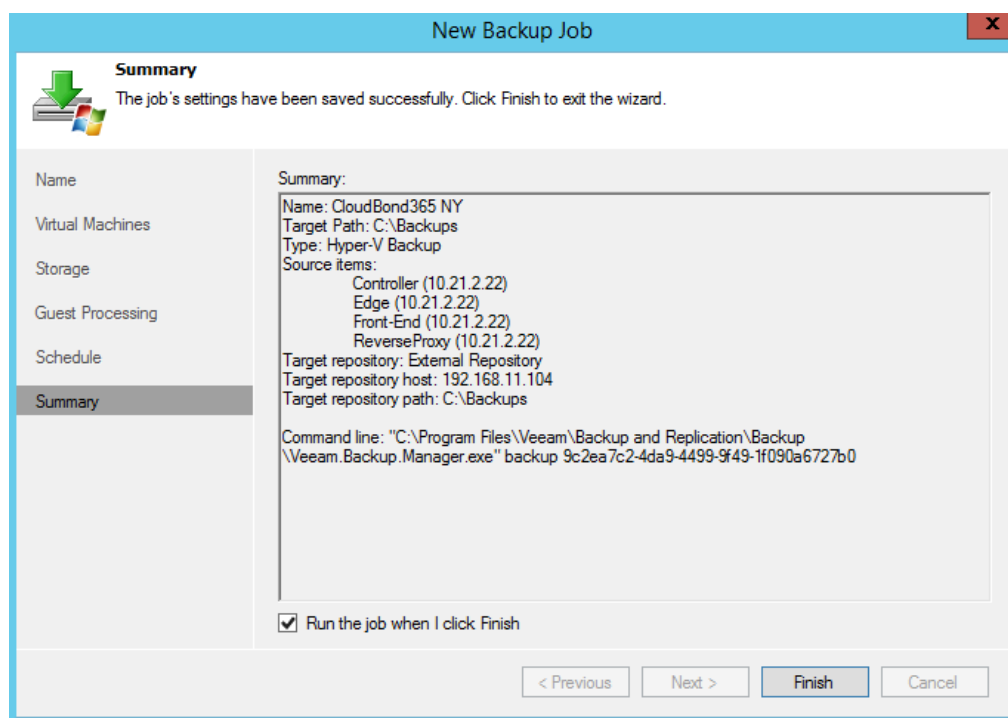
☐ **Terminate job if it exceeds allowed backup window** Window...

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

< Previous Create Finish Cancel

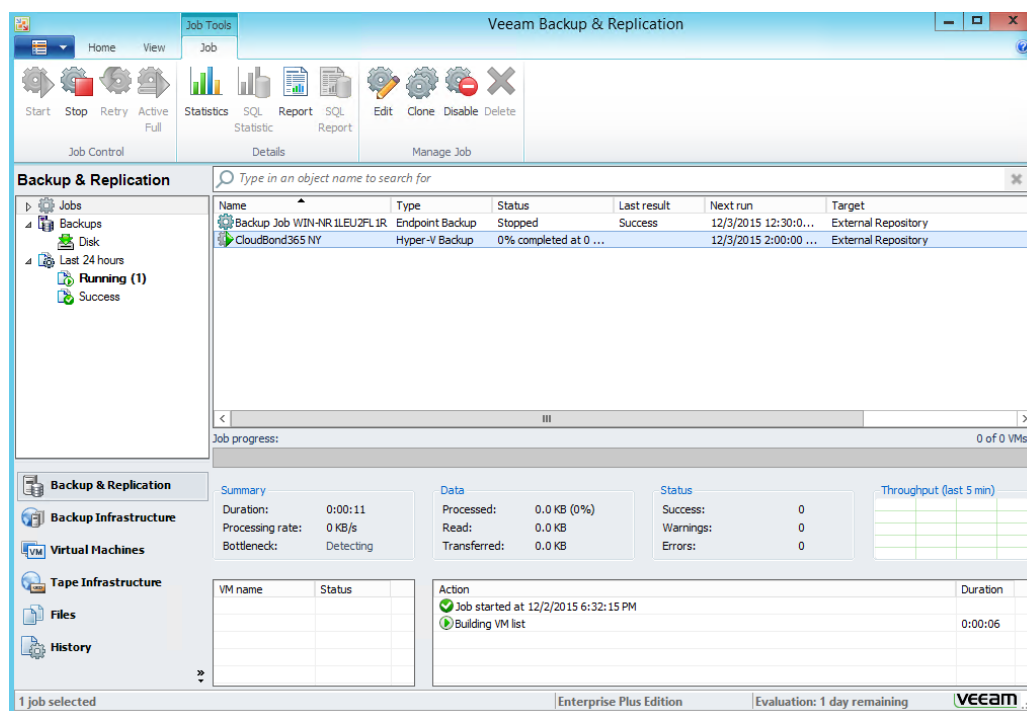
13. Click **Finish**.
14. It is recommended to select the 'Run the job when I click Finish' check box, so that you can run the job immediately to test the backup.

Figure 42-20: New Backup Job – Summary



15. You can monitor the job using the VBR.

Figure 42-21: VBR - Monitoring



42.3 Monitoring Backup

You can monitor the backup process using either:

- Email
- SNMP

The setup is done using the VBR: Refer to *Veeam Backup & Replication User Guide*. You can receive notification on the status of backup jobs and on system parameters.

42.4 Using the 3-2-1 Backup Rule

In making back up files, use the 3-2-1 rule:

- Have at least **three copies of your data**.
- Store the copies on **two different media**.
- Keep **one backup copy offsite**.

The above procedure provides the ability to create one local backup. Creating another two copies and one offsite is not described in this document. The VBR tool can be used for creating extra jobs to copy the backup to another place and to store the backup offsite using the Veeam cloud. For more information, contact AudioCodes.

42.5 Backing up the SBC

The SBC (software and hardware SBC) can be backed up by saving its *ini* files. For more information on how to save the *ini* files, refer to the *SBC User Manual*.

For Pro Box and Enterprise Box editions, where software SBC is used, you must restore the SBC VM first and then configure it with the *ini* files. We recommend you export the SBC VM after setting it to the C: drive, so that the VEB will back it up.

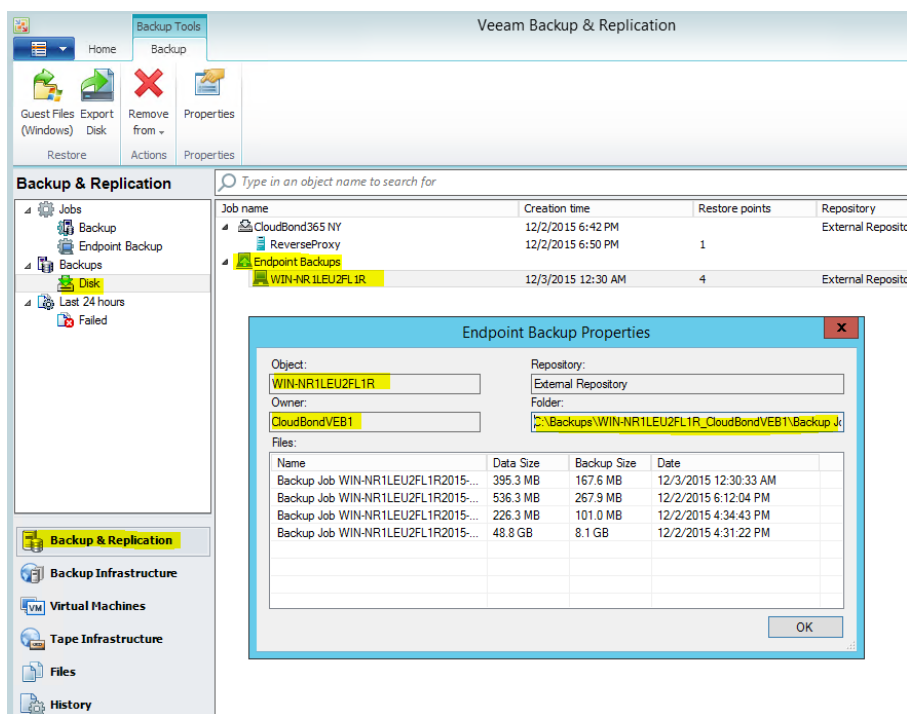
This page is intentionally left blank.

43 Keeping Information after Defining the Backup

A restore can be done years after you defined the backup. It is recommended to enter the following information per CloudBond 365, so it will be available if needed for recovery.

- **Location of the recovered USB:** It is recommended to update the USB using your server as explained in Chapter 45 to keep your system drivers.
- **Architecture used:** Note what architecture is used for VBR on the CloudBond 365 or on an external server. Either the repository is external or on the CloudBond (attached USB Disk)
- **Password used:** Note the password used if you encrypt the backup.
- **CloudBond 365 topology:** (with Domain Controller or without).
- **D: and E: drive/files:** If you backed up D: and E: drives, you will need to restore them.
- **IP address:** Note the IP address of the Repository server.
- **Network Settings:** Note the network settings, IP address and which virtual network is associated with a physical network card.
- **Username and Password of the Repository server:**
- **Username and Password of the VEB:** (for every CloudBond 365 it is a different user)
- **The full network path of the VEB backup:** This can be seen after you perform one backup from the VBR console. The full local path is displayed in the 'Folder' field.

Figure 43-1: Backup and Replication



- Network setup for all Network interfaces – Host and VM
- Hyper-V Virtual Network switch configuration.

This page is intentionally left blank.

44 Restoring a CloudBond 365 Backup

The Restore procedure is for a full system restore and not one for a virtual machine, even though that the Backup system supports it. When restoring to different hardware, a new license is required. The basic system functionality works without the new license. If you change your hardware, you need a new license for CloudBond 365 SysAdmin, because the license is based on the device's hardware IDs.



Note: Please contact AudioCodes to obtain this license.

Before you begin the restore process, check that the date and time on the CloudBond 365 server BIOS are correct.



Note: The Restore procedure is divided into several Restore tasks. It is recommended that when restoring, the same Restore date for all tasks is used.

44.1 Booting the CloudBond 365

The following procedures describe two different ways of how to boot the CloudBond 365:

- From Veeam Recovery Media USB
- Remotely from .iso using HP iLO

44.1.1 Booting CloudBond 365 from Veeam Recovery Media USB

The following procedure below describes how to boot the CloudBond 365 from a Veeam Recovery Media USB.

➤ **To boot the CloudBond 365 from a Veeam Recovery Media USB:**

1. Plug the Veeam Recovery Media USB into the CloudBond 365.



Notes:

- The Veeam Recovery Media USB comes with the CloudBond 365. If you don't have the Veeam Recovery Media USB, see Chapter 45 for instructions on how to create it.
- If the Veeam software was updated on your server, it is recommended to update the USB. See Chapter 45 for more information.
- The Veeam Recovery Media USB is a different USB than the CloudBond 365 Recovery USB. The CloudBond Recovery USB is used for a clean system re-install using the CloudBond 365 Installation wizard.

2. Start the server and boot from the USB:
 - **On CloudBond Standard and Standard+ Editions:** From the BIOS, select **Save and Exit Menu** and select to boot from USB.
 - **On CloudBond 365 Pro Box and Enterprise Box Editions:** While booting, click F11. Select Option 3 to boot once from the USB

44.1.2 Booting CloudBond 365 Remotely from .iso using HP iLO

The recovery can be performed remotely using HP Integrity Integrated Lights-Out (iLO) management for CloudBond 365 Pro Ent (HP server). You need to boot the CloudBond 365 from an *iso* file, instead of a USB.

The *.iso* file can be downloaded from <https://s3.eu-central-1.amazonaws.com/downloads-audiocodes/CB365Backup/VeeamRecoveryMedia.iso>.

Another option is to put the USB with the *.iso* file and set the iLO to boot from the *.iso* on the USB. This *.iso* file can be prepared the same way as preparing the USB in Chapter 45, but you need to select *.iso* boot type.

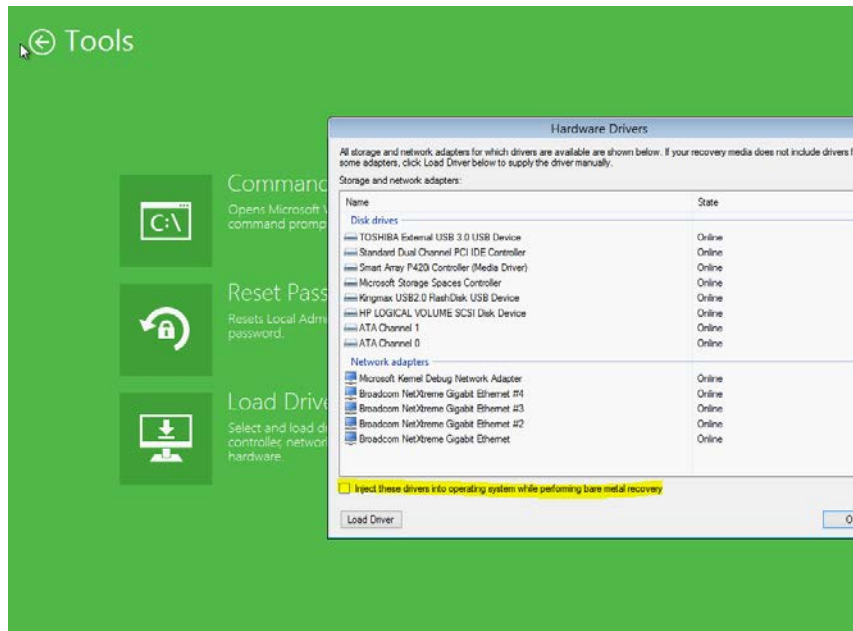
44.2 Restoring Volume C: Using VEB

The procedure below describes how to restore Volume C using the VEB.

➤ **To restore Volume C: using VEB:**

1. Boot the system using either a USB or .iso file.
2. From the main menu, select **Tools**, and then select the **Load Driver** menu option.

Figure 44-1: Hardware Drivers



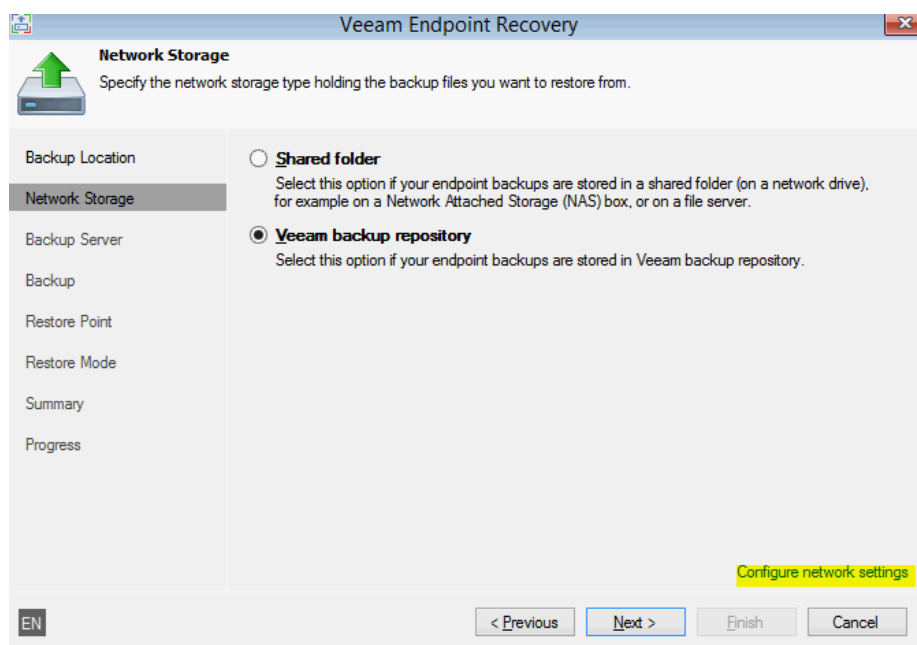
3. Clear the 'Inject these drivers...' check box, and click **OK**.
4. Return to the main screen
5. On the Veeam Endpoint Recovery screen, select the **Bare Metal Recovery** option.

Figure 44-2: Veeam Endpoint Recovery – Bare Metal Option



6. Click the **Network storage** option.

Figure 44-3: Veeam Endpoint Recovery – Backup Location



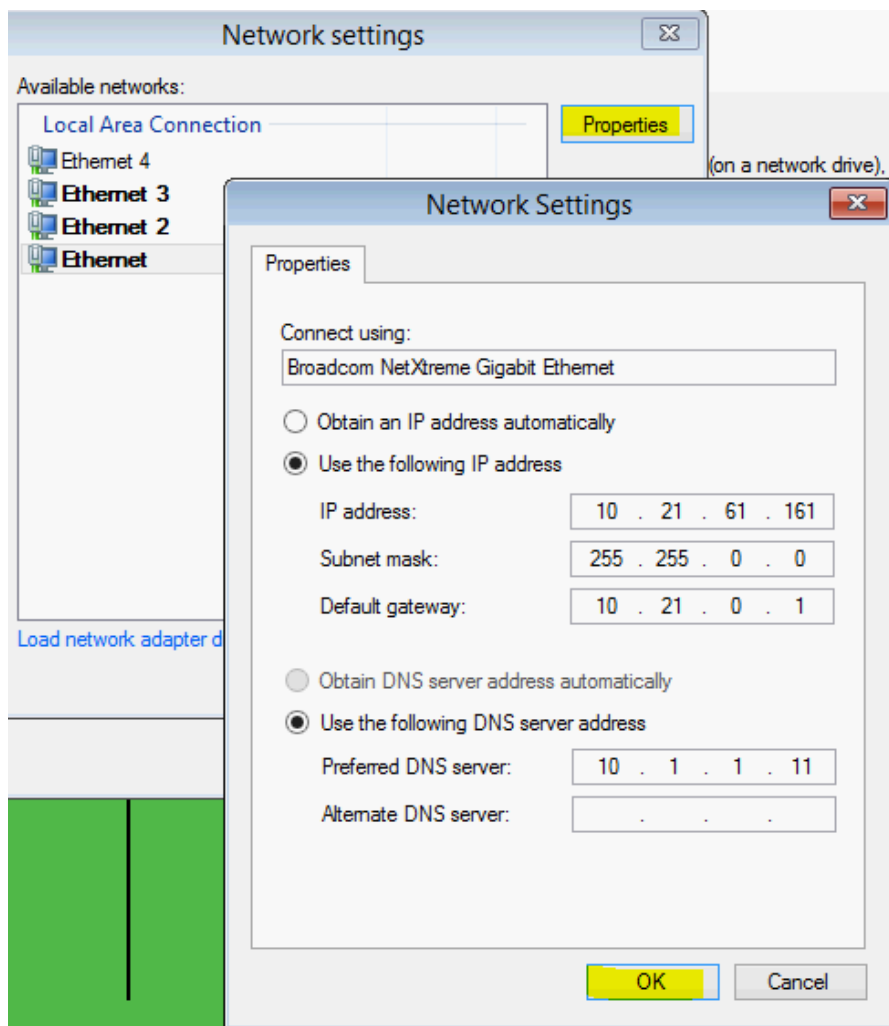
Notes:

- It is possible to perform a restore by using the **Local Storage** (USB Disk) option. To do so, copy the appropriate directory from the backup repository to the USB Disk. Connect it to the CloudBond 365, and then select **Local Storage** on the Backup Location screen.
- If the backup topology is connecting the local USB disk to the CloudBond 365, select the Local storage option (Shared folder option) and browse to the relevant directory to select the *vbm* file. In this case, the steps below are not relevant.



7. Set the IP address for the recovery session by selecting **Configure Network Settings**.

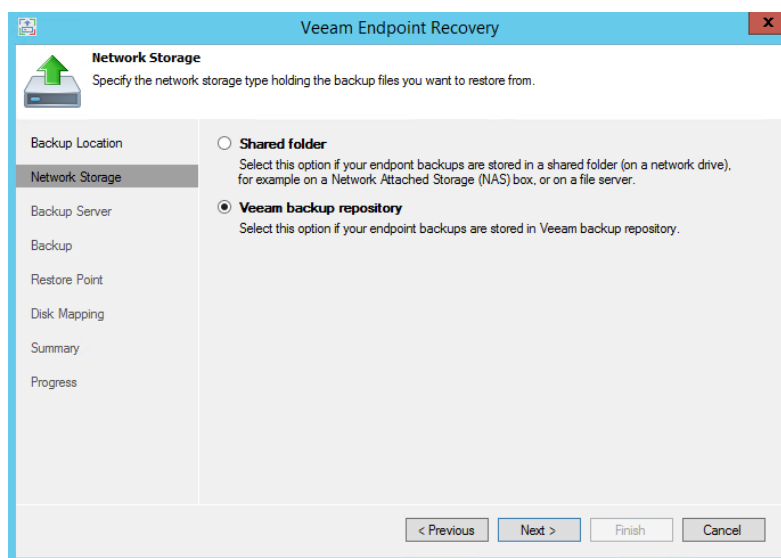
Figure 44-4: Network Settings



8. Select the correct network adapter with the valid IP address, and then click **OK**.
9. Click **Next**.
10. On the Network Storage screen:
 - If the VBR is running on a CloudBond 365 host, click the **Shared folder** because the VBR cannot be accessed.
 - If the VBR is running on an external server, click the **Veeam backup repository** option.
11. Click **Next**.

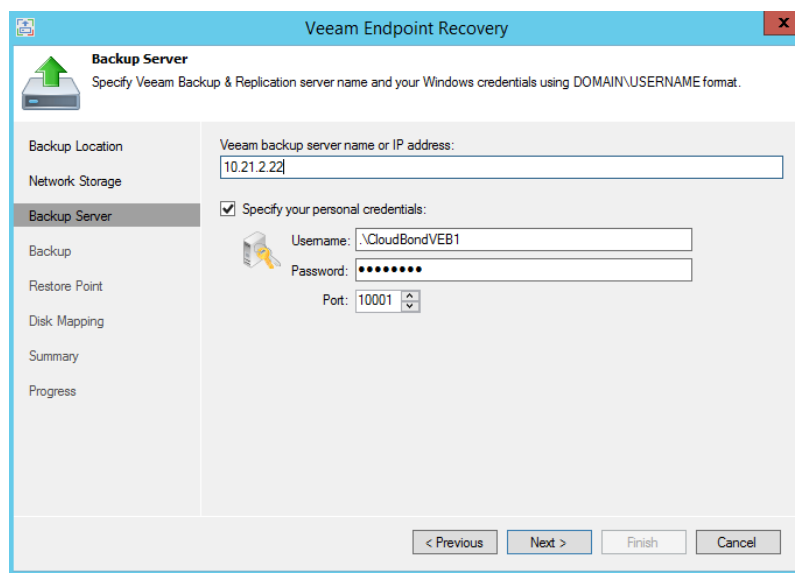
12. The **Veeam backup repository** option is selected.

Figure 44-5: Veeam Endpoint Recovery – Network Storage

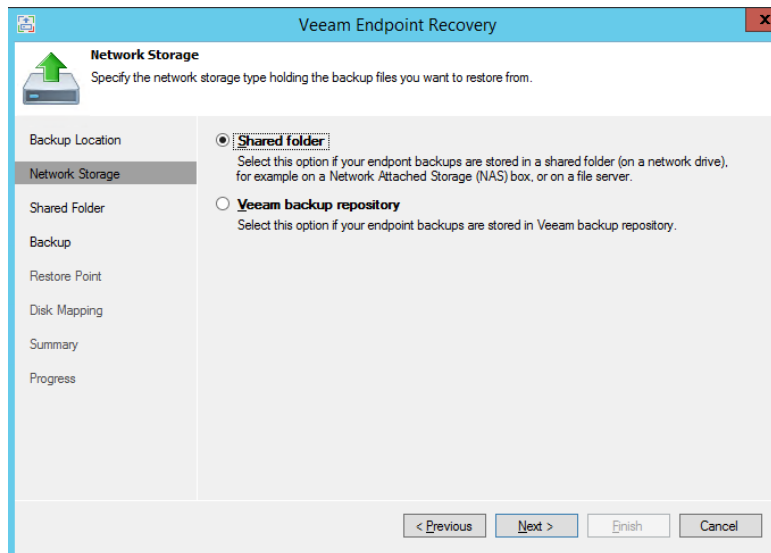


13. Provide the VEB credentials that you defined when you configured the backup, and then click **Next**.

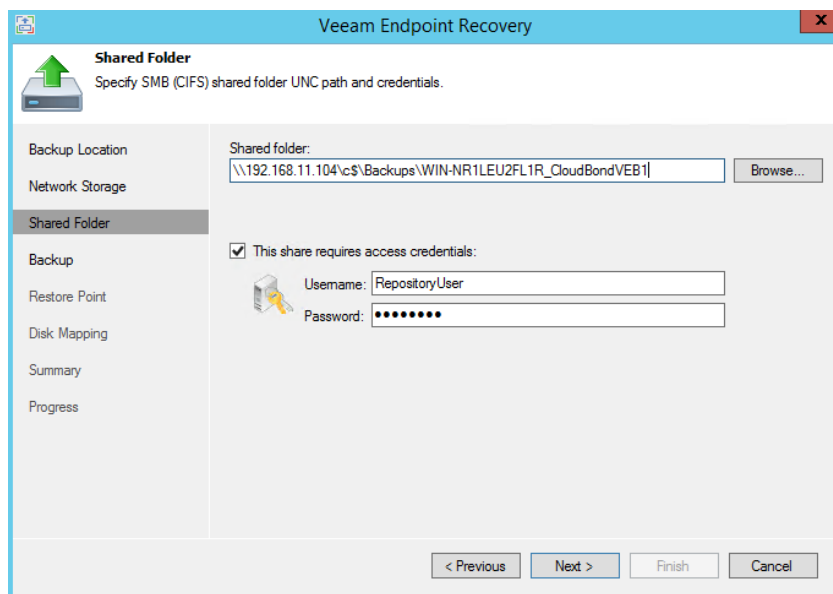
Figure 44-6: Veeam Endpoint Recovery – Backup Server



14. The **Shared Folder** option is selected; click **Next**.

Figure 44-7: Veeam Endpoint Recovery – Network Storage

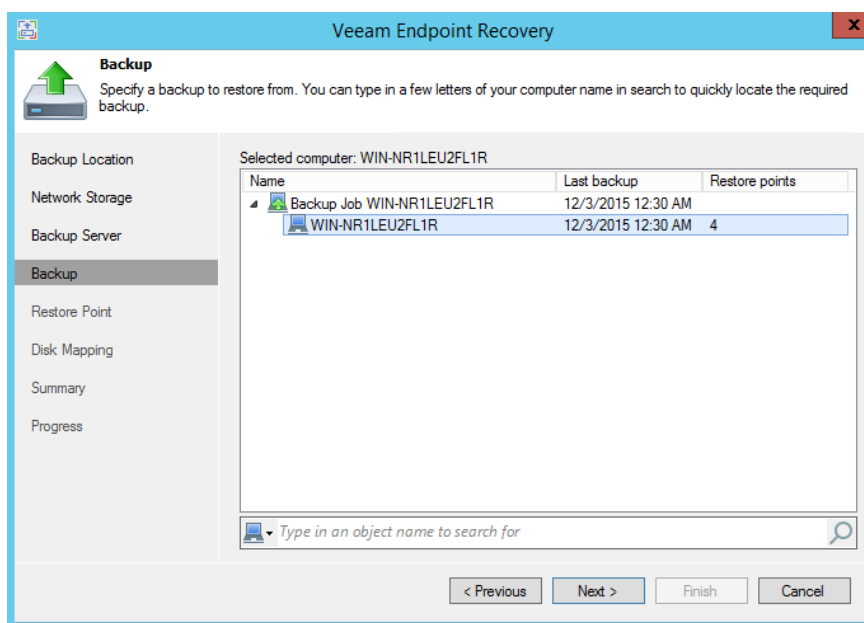
15. You need to provide the full shared folder path to the VEB backup that is on the repository server. The name of the directory of the VEB backup is a combination of the *server name* and the *VEB user name*. Browse to the backup repository using another server to see what the full path name is.
16. Enter the credentials of the backup repository, and then click **Next**.

Figure 44-8: Veeam Endpoint Recovery – Shared Folder

17. You should only see one computer name because only the VEB backup is done through the specific VEB user. One VEB user is defined per CloudBond 365 for the VEB backup.

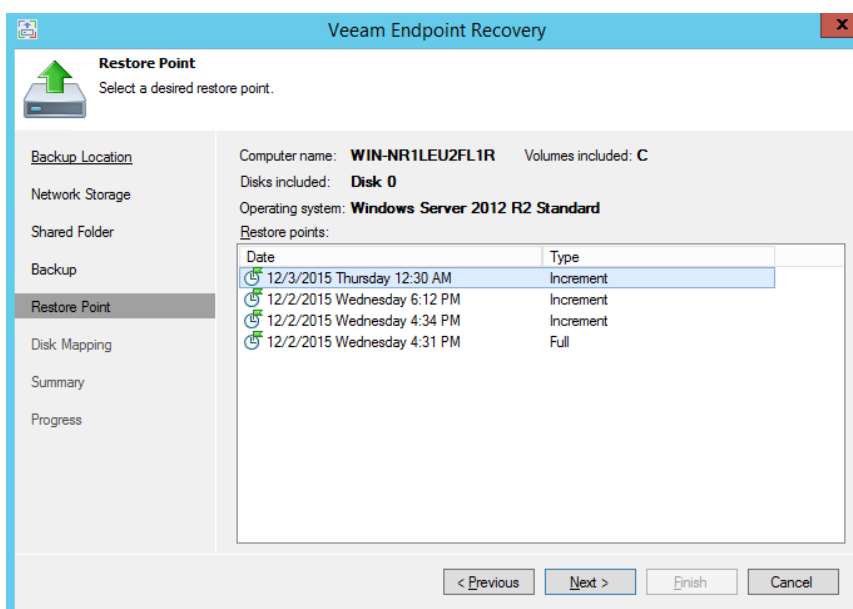
18. Select the computer to recover from, and then click **Next**.

Figure 44-9: Veeam Endpoint Recovery – Backup



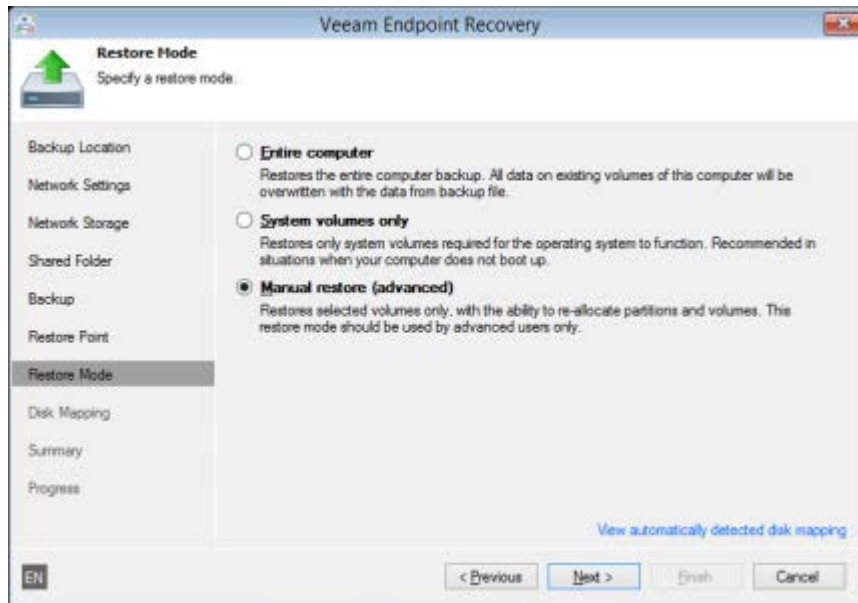
19. From the Restore Point screen, select the appropriate restore point, and then click **Next**.

Figure 44-10: Veeam Endpoint Recovery – Restore Point



20. Select the **Manual restore (advanced)** option, to choose what computer volumes you want to restore and manually allocate disk space on the restored volumes, and then click **Next**. (To view the current disk allocations settings on your computer, click **View automatically detected disk mapping** on the bottom of the screen. Delete unwanted volumes on that screen.)

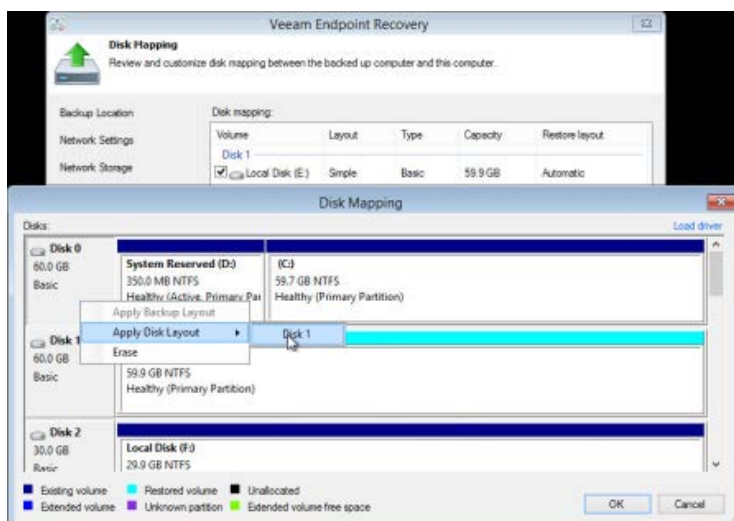
Figure 44-11: Veeam Endpoint Recovery – Restore Mode



21. can map volumes that you want to restore from the backup to disks on the target computer. To map volumes:
 - a. Select the check box of the volume that you want to restore from the backup.
 - b. By default, VEB restores all volumes to their initial location. To map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**. In the **Disk Mapping** window, specify which volumes must be restored:
 - c. Right-click the target disk on the left side of the screen and select the necessary disk layout.
 - ◆ **Apply Backup Layout:** Select this option if you want to apply to the disk, the settings that were used on your computer when you performed the backup.
 - ◆ **Apply Disk Layout:** Select this option if you want to apply to the current disk settings of another disk.
 - ◆ **Erase** - Select this option if you want to discard the current disk settings.

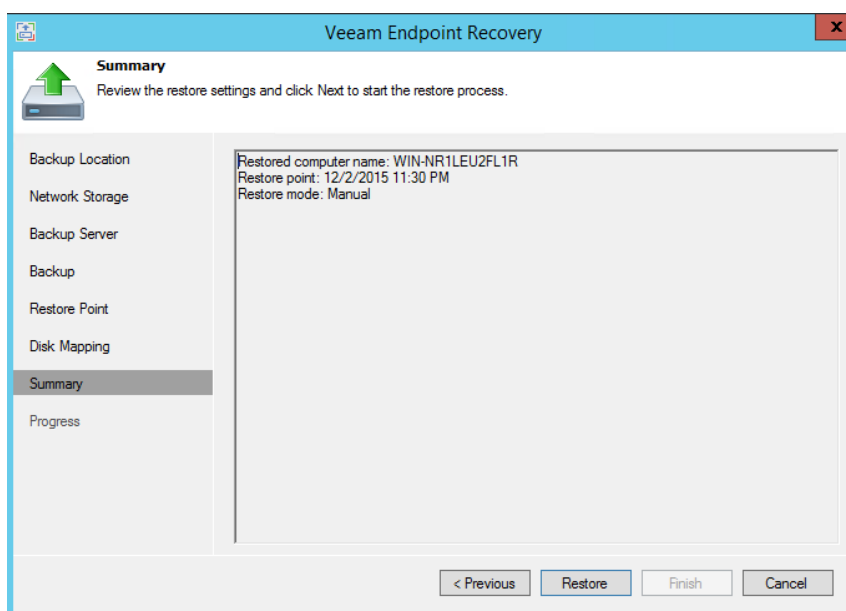
22. Click **OK**, and then **Next**.

Figure 44-12: Veeam Endpoint Recovery – Disk Mapping



23. Click **Restore** to start the recovery.
24. When the Restore process ends, restart the server.

Figure 44-13: Veeam Endpoint Recovery – Summary



44.3 Performing Post-Restore – Exiting Domain Controller Safe Mode

If the host is a Domain Controller, log in with Safe boot mode. If the host is not a Domain Controller, skip this procedure.

After performing a full Virtual Machine restore, the Domain Controller computer boots up in what appears to be Safe mode. When the Domain Controller boots for the first time, it is actually in Active Directory Services Restore mode as you are booting from a backup file. However it should automatically re-boot.

➤ **To exit the Domain Controller in Safe mode:**

1. Log in with the Directory Services Restore mode account (typically `.administrator`).
2. Open a command prompt and run the following:

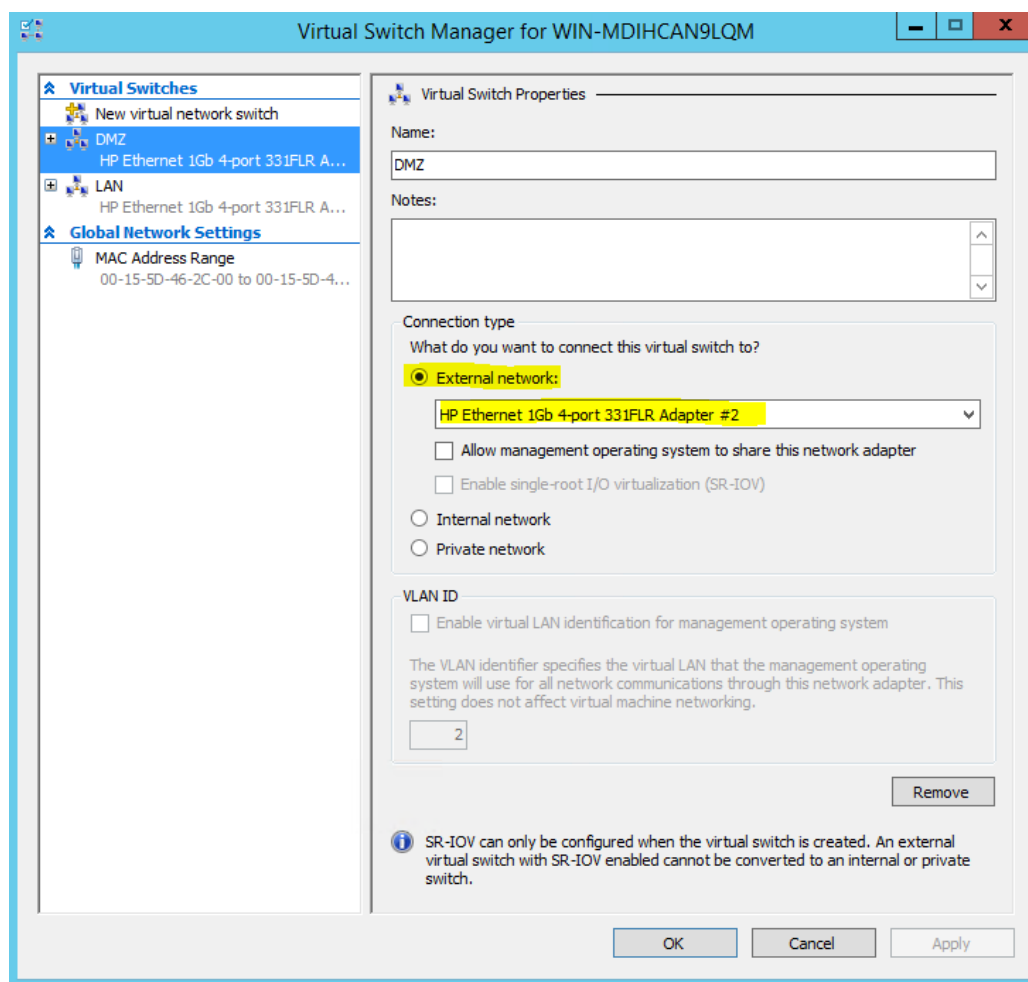
```
bcdedit /set safeboot dsrepair
bcdedit /deletevalue safeboot
shutdown -t 01 -r
```
3. CloudBond 365 should then re-boot in Normal mode.
4. Log in to the Domain Controller as the Domain Administrator
5. For more information, refer to the Microsoft Knowledge Base article in [http://technet.microsoft.com/en-us/library/cc816897\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816897(WS.10).aspx).

44.4 Validating Network Settings

You need to confirm that **all** network cards are valid and have the correct IP addresses. (You can only check the host network and not the VM in this step). Compare it to the information you saved when you defined the backup (See Chapter 43 on page 287).

Validate that the Hyper-V virtual network switch is set correctly. Every virtual network is connected to a real physical card. Compare it to the information you saved when you defined the backup.

Figure 44-14: Validating Network Settings



1. If the Network cards are not functioning correctly, refer to the Troubleshooting (Chapter 47).

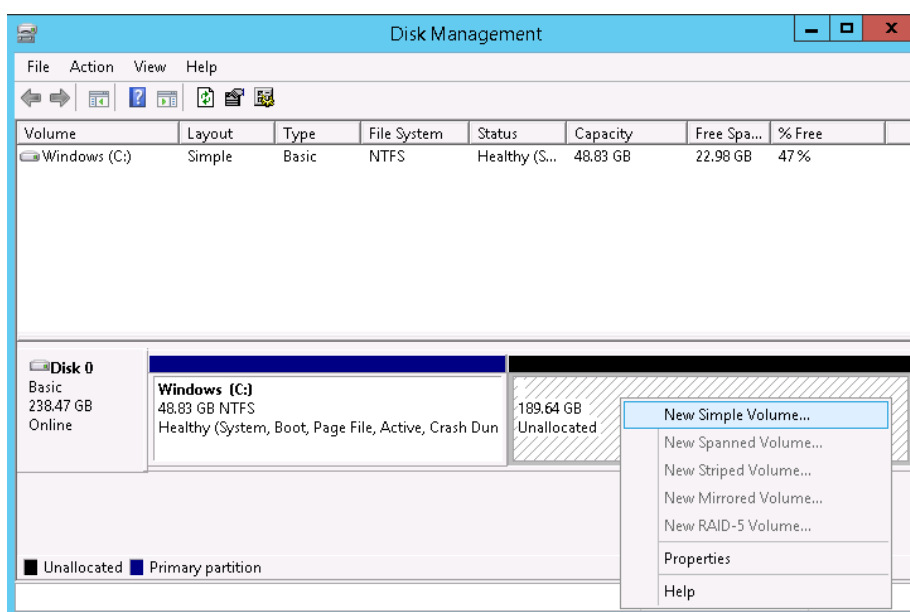
44.5 Preparing Volume D: for Restoring VMs from the VBR

The following procedure describes how to prepare Volume D: for restoring the VMs from the VBR, as described in Section 44.8 on page 307.

➤ **To prepare Volume D: for restoring the VMs from the VBR:**

1. Login to the host in Normal mode.
2. Open the Disk Management screen and create Volume D: , if it does not exist. Volume D: should use all the free disk size. and it depends on the CloudBond 365 type.

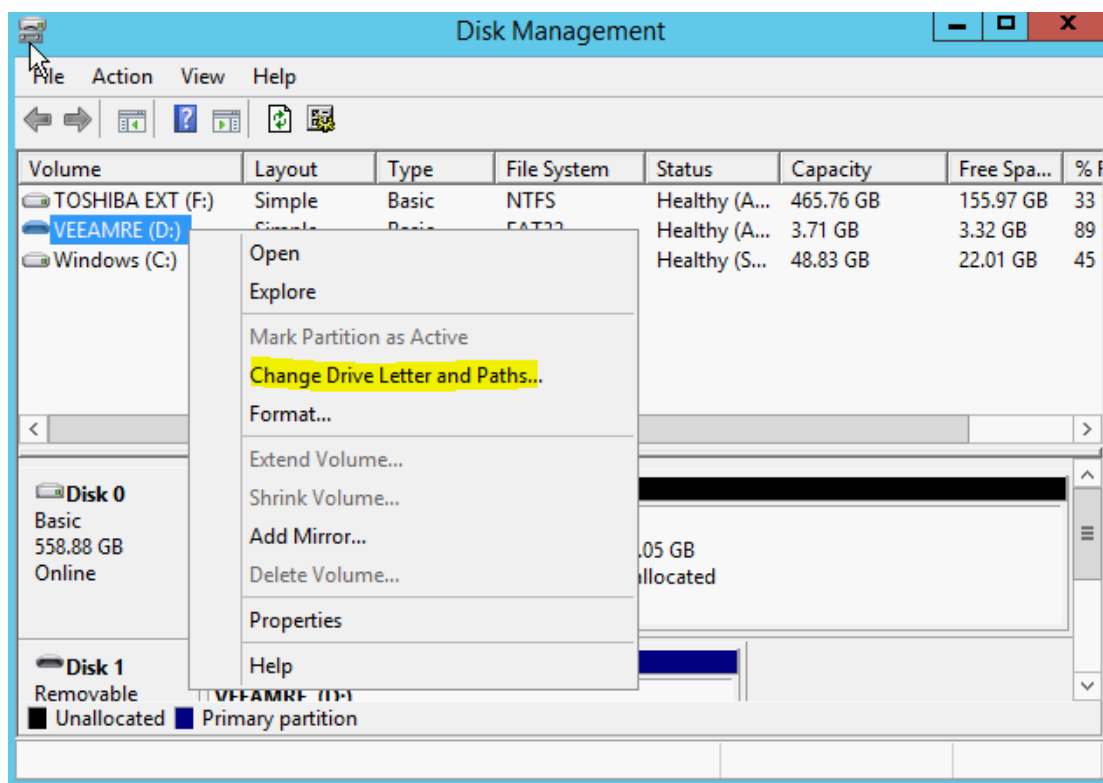
Figure 44-15: Disk Management



Notes:

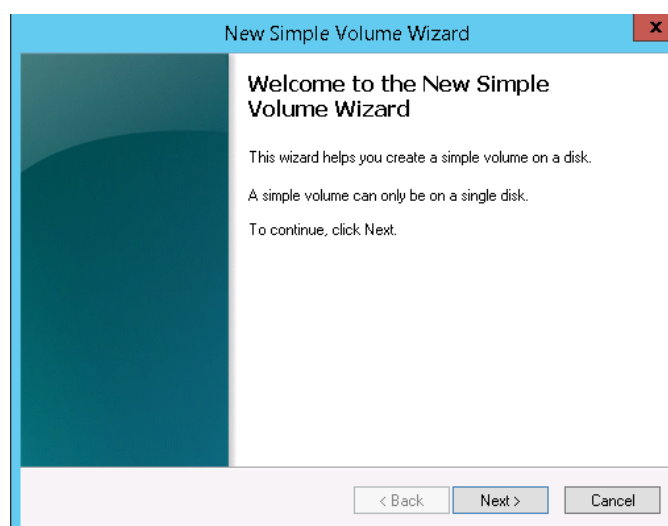
- If the D: drive is already assigned to USB storage, change the drive letter to something else before you continue.
- If you wish to also restore Volume E:, make sure you have 32 GB of available disk space.

Figure 44-16: Disk Management – Change Drive Letter and Paths

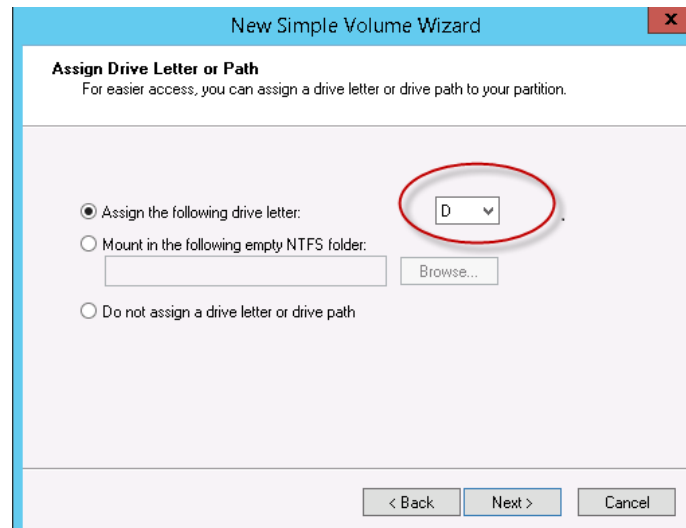


3. Right-click on the disk.
4. Select **New Simple Volume**; the Welcome New Simple Volume Wizard .
5. Click **Next**.

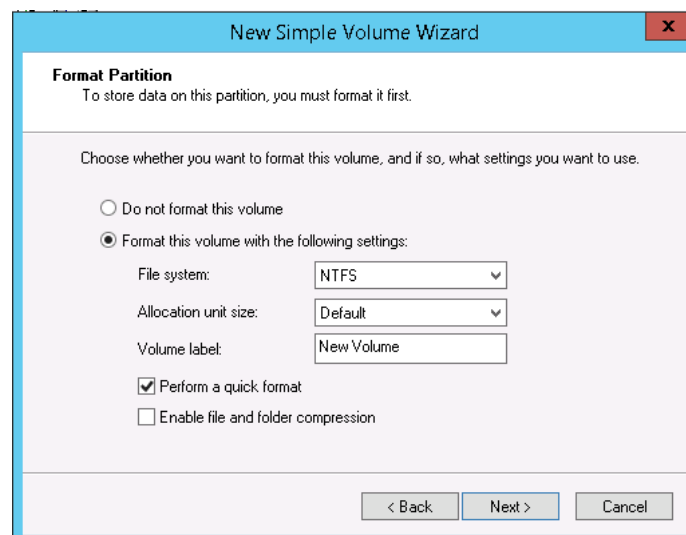
Figure 44-17: New Simple Volume Wizard - Welcome



6. Click the **Assign the following drive letter** option.
7. From the drop-down list, select the drive letter, and then click **Next**.

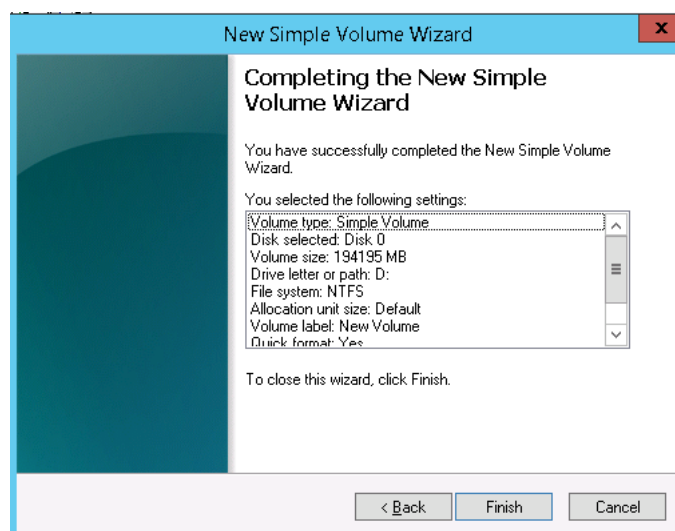
Figure 44-18: New Simple Volume Wizard – Assign Drive Letter or Path

8. Click the **Format this volume with the following settings** option.
9. Enter the appropriate values as shown in the screen below, and then click **Next**.

Figure 44-19: New Simple Volume Wizard – Format Partition

10. Click **Finish**.

Figure 44-20: New Simple Volume Wizard – Finish



44.6 Updating Host Virtual NIC MAC Address After Restore

When CloudBond 365 is working correctly, its vEthernet (VLAN) NIC interface receives one of the physical MAC addresses of the server and uses it. After a Restore, the vEthernet NIC interface receives a unique MAC address, which needs to be updated. After a Restore, the MAC addresses appear as follows:

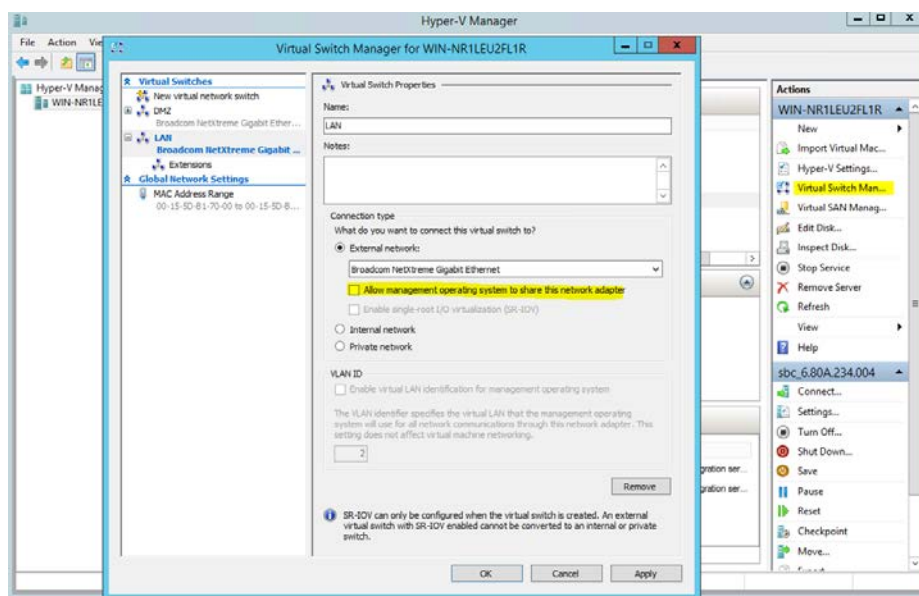
Figure 44-21: MAC Addresses After Restore

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
vEthernet (LAN)	Hyper-V Virtual Ethernet Adapter #2	19	Up	00-90-FB-50-9B-D9	10 Gbps
Ethernet 3	Intel(R) 82574L Gigabit Network Co...#2	14	Disconnected	00-90-8F-5F-03-C2	0 bps
Ethernet 2	Intel(R) 82579LM Gigabit Network Conn...	13	Up	00-90-FB-4F-AA-2B	100 Mbps
Ethernet	Intel(R) 82574L Gigabit Network Conn...	12	Disconnected	00-90-8F-5F-03-C3	0 bps

➤ To update the Host Virtual NIC MAC Address After Restore

1. Open the **Hyper-V Manager**.
2. Navigate to the **Virtual Switch Manager**.
3. Under **Connection type**, clear the 'Allow management operating system to share this network adapter' check box, and then click **Apply**.

Figure 44-22: Hyper-V Manager



4. Click **OK**.
5. After the update, the MAC address should look like **00-90-FB-50-9B-D9**.

Figure 44-23: MAC Addresses After Update

```
PS C:\Users\Administrator> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
vEthernet (LAN)	Hyper-V Virtual Ethernet Adapter #2	22	Up	00-90-FB-50-9B-D9	10 Gbps
Ethernet 3	Intel(R) 82574L Gigabit Network Co...#2	14	Disconnected	00-90-8F-5F-03-B4	0 bps
Ethernet	Intel(R) 82579LM Gigabit Network Conn...	12	Up	00-90-FB-50-9B-D9	100 Mbps
Ethernet 2	Intel(R) 82574L Gigabit Network Conn...	13	Disconnected	00-90-8F-5F-03-B5	0 bps

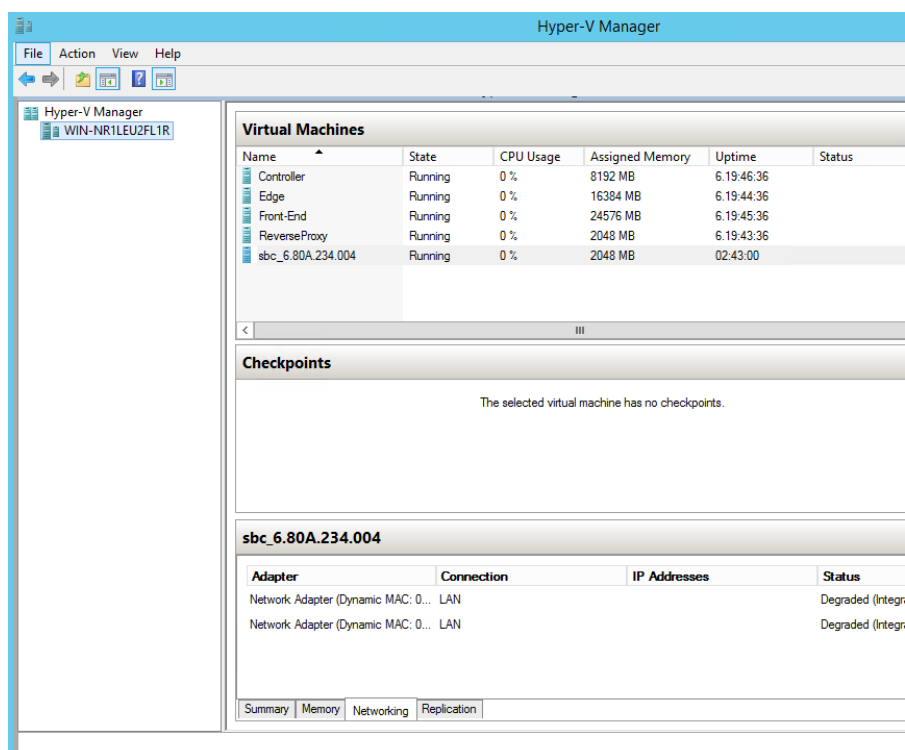
44.7 Clearing Old Virtual Machine Data

The procedure below describes how to clear old Virtual Machine (VM) data.

➤ **To clear old Virtual Machine data:**

1. Open the Hyper-V Manager.
2. From the Hyper-V main page, delete all the VMs including checkpoints.

Figure 44-24: Hyper-V Manager – Virtual Machines



3. You need a clean Hyper-V Manager without any VMs before restoring the VMs.

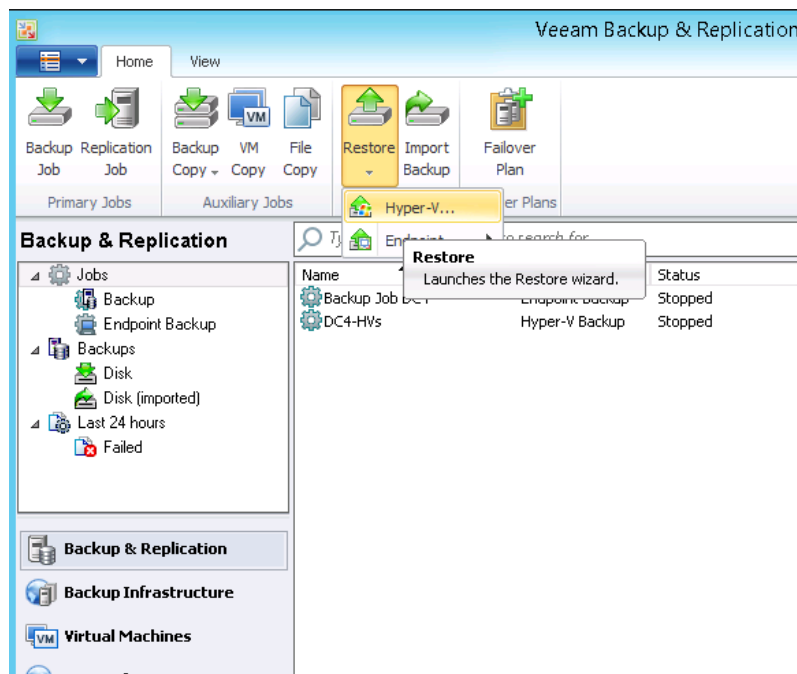
44.8 Restoring all VMs from the VBR

The procedure below describes how to restore all VMs from the VBR.

➤ **To restore all VMs from the VBR:**

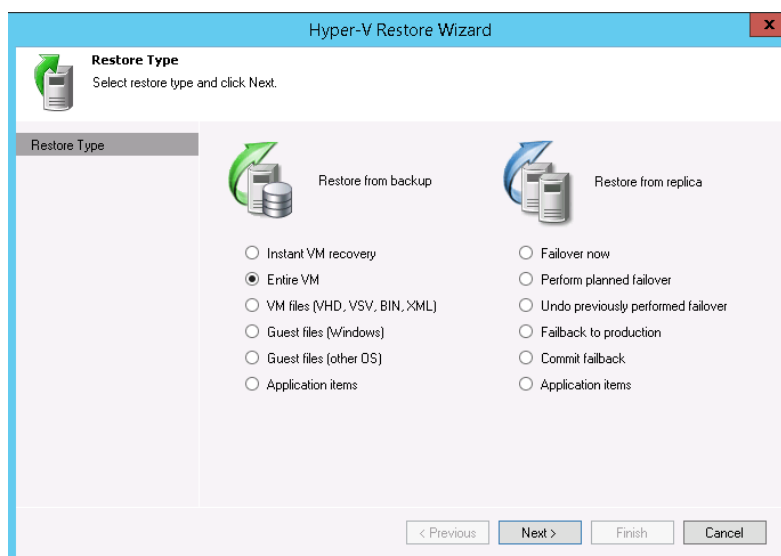
1. Open the VBR console.
2. Launch the Restore wizard (**Home** tab > **Restore** menu > **Hyper-V - Restore**).

Figure 44-25: VBR – Hyper-V



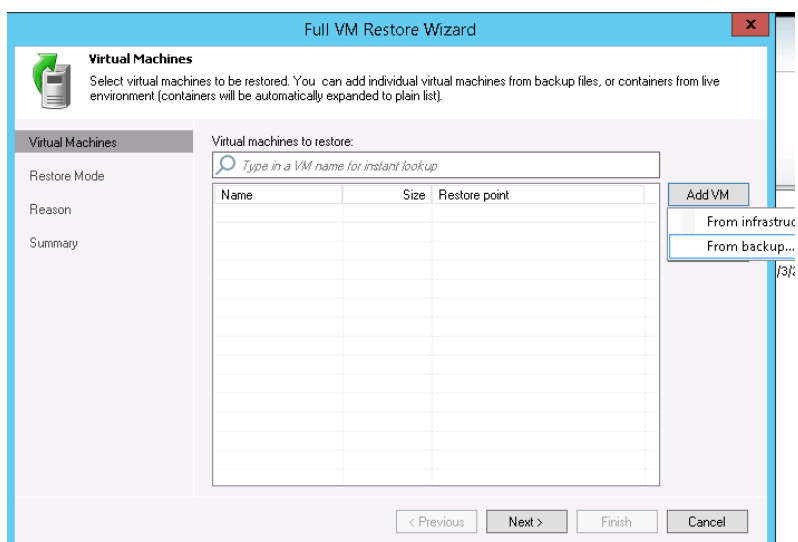
3. Select **Restore from backup** and then click the **Entire VM** option.
4. Click **Next**.

Figure 44-26: Hyper-V – Restore Type



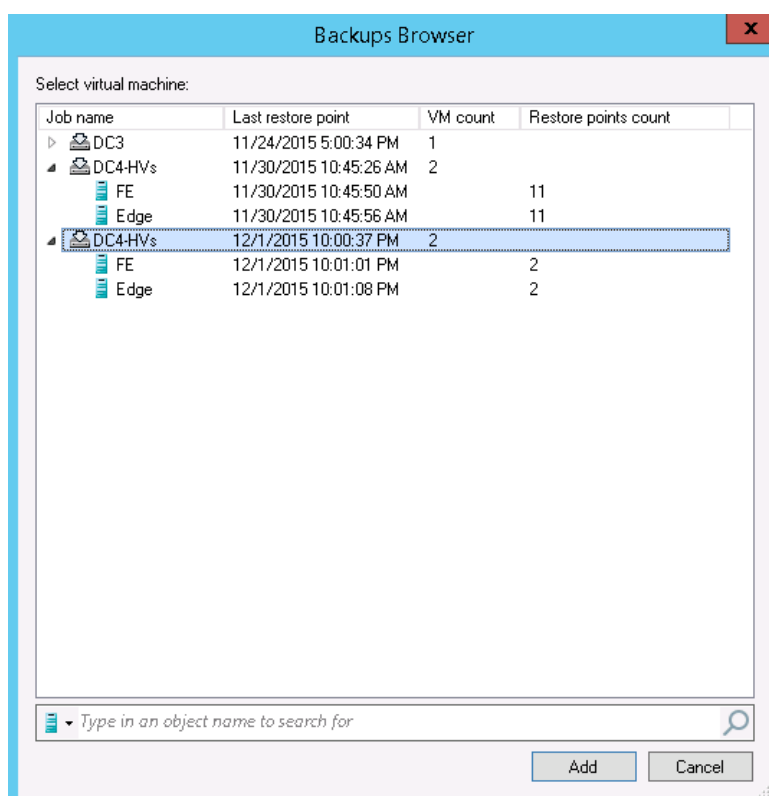
5. Click **Add VM**, and then select the **From backup** option.
6. Click **Next**.

Figure 44-27: Full VM Restore Wizard – Virtual Machines




7. Select the server you wish to restore (e.g., DC4-HVs), and then click **Add**.

Figure 44-28: Backup Browser



- 8.** Click **Next**.

Figure 44-29: Full VM Restore Wizard – Virtual Machines



Virtual Machines

Select virtual machines to be restored. You can add individual virtual machines from backup files, or containers from live environment (containers will be automatically expanded to plain list).

Virtual Machines

Restore Mode

Reason

Summary

Virtual machines to restore:

Type in a VM name for instant lookup


Name	Size	Restore point
Edge	40.0 GB	12/1/2015 Tuesday 10:01 PM
FE	80.0 GB	12/1/2015 Tuesday 10:01 PM

Add VM
Point...
Remove

< PreviousNext >FinishCancel

9. Click the **Restore to the original location** option, and then click **Next**.

Figure 44-30: Full VM Restore Wizard – Restore Mode



Restore Mode

Specify the desired restore mode.

Virtual Machines

Restore Mode

Reason

Summary

☒ **Restore to the original location**

Quickly initiate restore of selected VMs to the original location, and with the original name and settings. This option minimizes the chance of user input error.

☐ **Restore to a new location, or with different settings**

Customize restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the default settings.

☐ **Quick rollback (restore changed blocks only)**

Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous

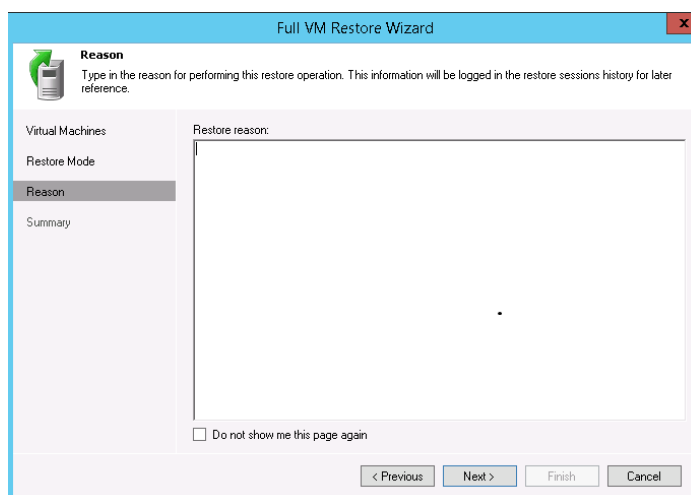
Next >

Finish

Cancel

10. Add the **Restore reason**, and then click **Next**.

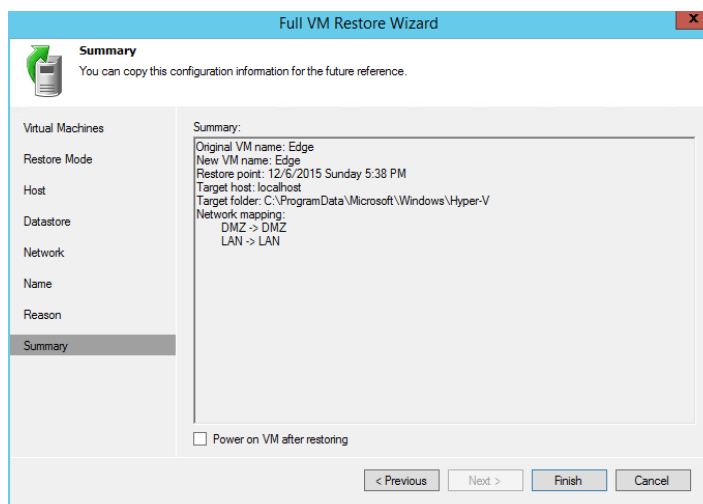
Figure 44-31: Full VM Restore Wizard – Reason



The screenshot shows the 'Reason' step of the Full VM Restore Wizard. The title bar reads 'Full VM Restore Wizard'. On the left, a sidebar contains 'Virtual Machines', 'Restore Mode', 'Reason' (selected), and 'Summary'. The main area has a heading 'Reason' with a subtext: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this is a large text input field. At the bottom, there is a checkbox labeled 'Do not show me this page again' and four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

11. Make sure the 'Power on VM after restoring' check box is cleared.
12. Click **Finish**, and then wait for the Restore process to end.

Figure 44-32: Full VM Restore Wizard – Summary



The screenshot shows the 'Summary' step of the Full VM Restore Wizard. The title bar reads 'Full VM Restore Wizard'. The sidebar on the left has 'Summary' selected. The main area has a heading 'Summary' with a subtext: 'You can copy this configuration information for the future reference.' Below this is a large text area containing the following summary information:

Summary:

Original VM name: Edge

New VM name: Edge

Restore point: 12/6/2015 Sunday 5:38 PM

Target host: localhost

Target folder: C:\ProgramData\Microsoft\Windows\Hyper-V

Network mapping:

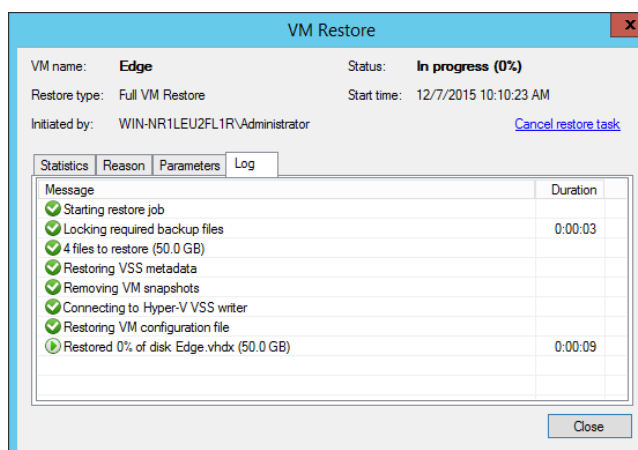
DMZ -> DMZ

LAN -> LAN

At the bottom, there is a checkbox labeled 'Power on VM after restoring' which is currently unchecked. Four buttons are at the bottom: '< Previous', 'Next >', 'Finish', and 'Cancel'.

13. Click **Close**.

Figure 44-33: VM Restore



The screenshot shows the 'VM Restore' progress window. The title bar reads 'VM Restore'. It displays the following information:

VM name: Edge

Status: In progress (0%)

Restore type: Full VM Restore

Start time: 12/7/2015 10:10:23 AM

Initiated by: WIN-NR1LEU2FL1R\Administrator

There is a link 'Cancel restore task' on the right.

Below this is a tabbed interface with 'Statistics', 'Reason', 'Parameters', and 'Log'. The 'Statistics' tab is active, showing a table with two columns: 'Message' and 'Duration'.

Message	Duration
Starting restore job	
Locking required backup files	0:00:03
4 files to restore (50.0 GB)	
Restoring VSS metadata	
Removing VM snapshots	
Connecting to Hyper-V VSS writer	
Restoring VM configuration file	
Restored 0% of disk Edge.vhdx (50.0 GB)	0:00:09

 At the bottom right is a 'Close' button.

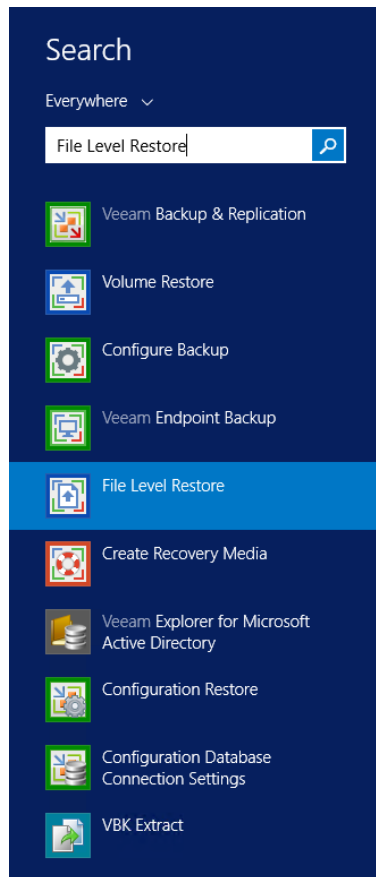
44.9 Restoring D: and E: Drives and Files

If the D: and E: drives were backed up, you need to restore them.

➤ **To restore D: and E: Drives and files:**

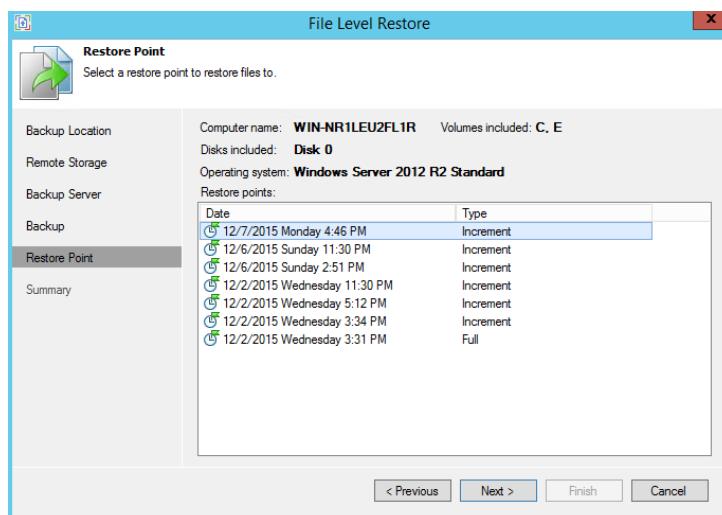
1. From the Veeam main screen, run the **File Level Restore** menu option.

Figure 44-34: File Level Restore



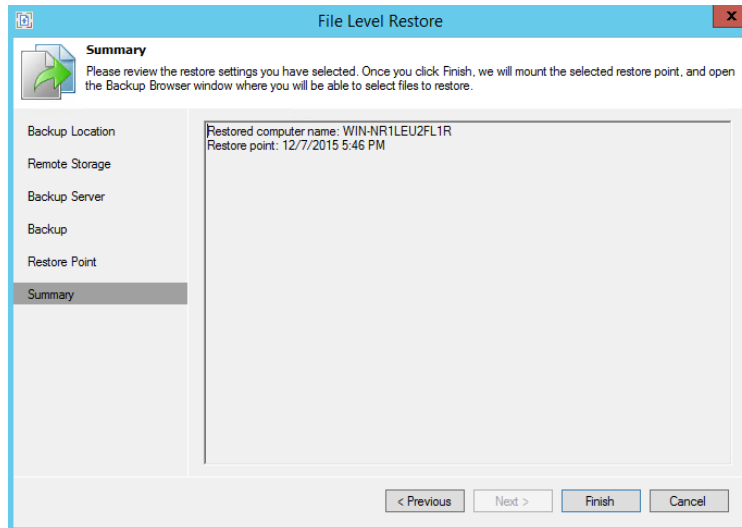
2. Select the restore point, and then click **Next**.

Figure 44-35: File Level Restore – Restore Point



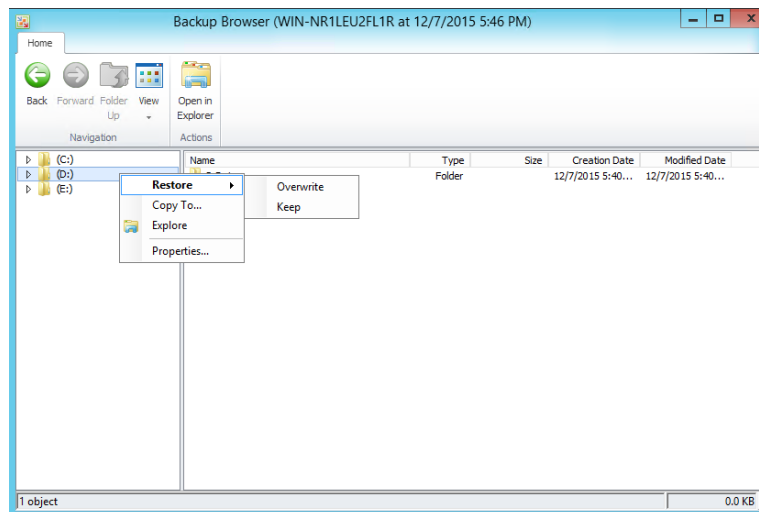
3. Click **Finish**.

Figure 44-36: File Level Restore - Summary



4. On the Backup Browser, select the drive you wish to restore.
5. Right-click on the appropriate drive.
6. Select **Restore** > **Overwrite**.

Figure 44-37: Backup Browser



44.10 Starting the Virtual Domain Controller

If the Domain Controller is a Virtual Machine, it automatically starts in **Safe** mode. If it does not, skip this procedure.

When the Domain Controller boots for the first time, it is actually in Active Directory Services Restore mode as you are booting from a backup file. However it should automatically re-boot.

➤ **To Start the Virtual Domain Controller:**

1. Login with the Directory services restore mode account (typically .\administrator)
2. Open the command prompt and run the following:

```
bcdedit /set safeboot dsrepair  
bcdedit /deletevalue safeboot
```
3. Re-boot the virtual Domain Controller. It should re-boot in Normal mode.
4. Login to the Domain Controller with the domain administrator.
5. For more information, refer to the Microsoft Knowledge Base Article below for further details [http://technet.microsoft.com/en-us/library/cc816897\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816897(WS.10).aspx).

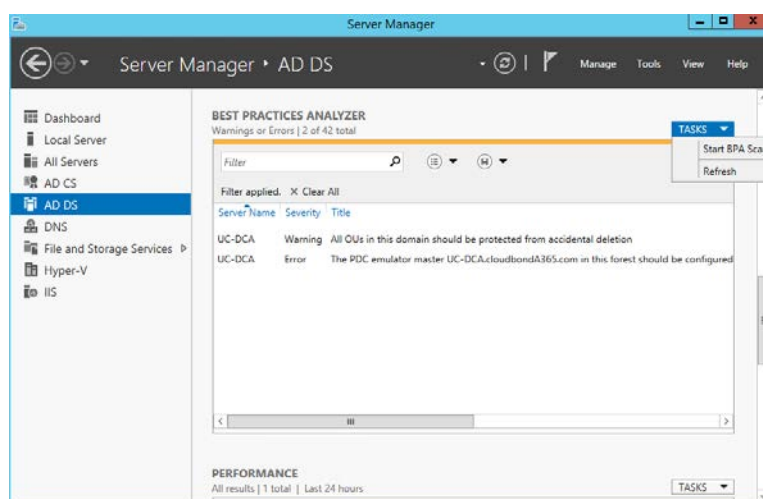
44.11 Restarting the CloudBond 365 Server and Testing the Restore

The procedure below describes the tests the need to perform to validate the restoreLog and perform the following tests to confirm successful restore. These tests must be done to check that the restore process successfully completed.

➤ **To confirm that the restore process was successful:**

1. Restart the CloudBond 365 server.
2. If the Virtual Machine belongs to the domain, log in to every Virtual Machine as the Domain Administrator. If not, log in as the local Administrator. If a Trust error message appears, reset the computer account using the Active directory.
3. Check that all services are running.
4. Confirm that the date and time are correct and if necessary update them.
5. Check that the Windows License has been activated. If not activate it according to the instructions on the sticker.
6. Log in to SysAdmin and confirm that SysAdmin is working.
7. From the Server Manager, select the **AD DS** menu option.
8. From the 'TASKS' drop-down list, run the Best Practices Analyzer by selecting **Start BPA Scan**. Confirm that there are no errors which are as a result of the recovery.

Figure 44-38: Server Manager



9. From the command line, run the **dcldiag** command on the Domain Controller. All tests should pass (ignore if the MSDFS test fails).
10. One day after the Restore process has completed, confirm that the backup process still works automatically.
11. For BPA / Pool Pairing, run **repadmin /showreps** from the command line and then confirm that the DC was replicated.
12. If the system was installed in Resource Forest mode, confirm that the trust with the company forest is valid.
13. Confirm that the VBR Job has been enabled. If not, re-scan the repository (right click on the repository – and select Re-scan) when finishing enabling the job.
14. Run the backup job and confirm that you are able to backup.
15. One day after the restore, confirm that the backup is still working automatically for the VEB.
16. Validate that all VMs don't have Checkpoints – in case they have need to delete it.

45 Creating the Veeam Recovery Media USB

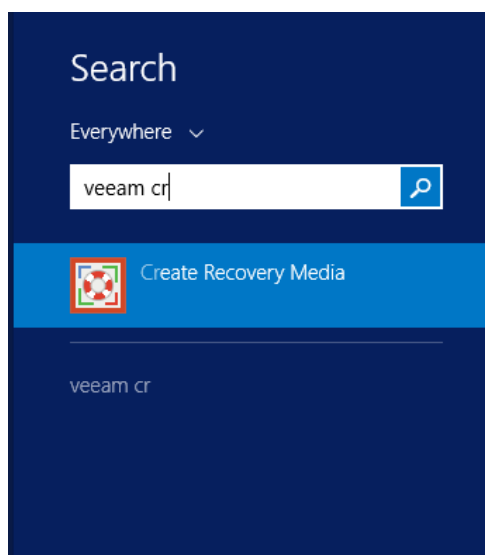
It is recommended to update the Restore Recovery USB that you get with the system, according to the following procedure. It keeps several settings which are relevant for your server (Drivers/IP). The USB minimum required size 4 GB.

This chapter describes how to create a Veeam Recovery Media USB.

➤ **To create a Veeam Recovery Media USB:**

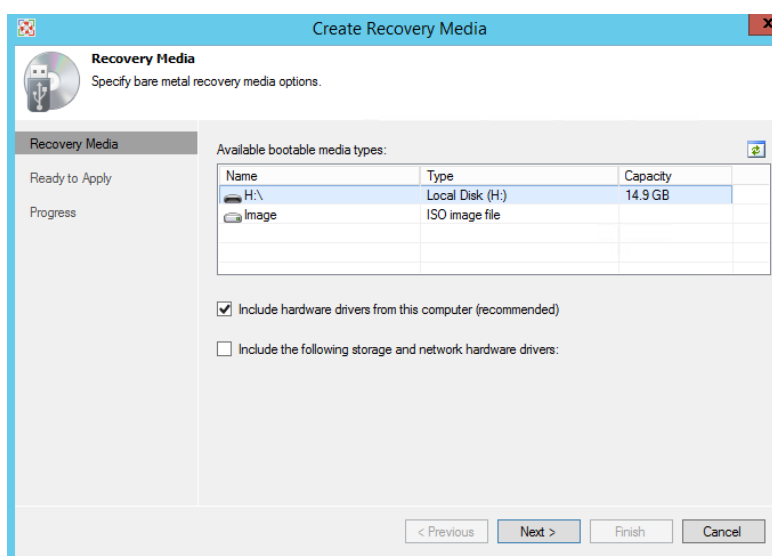
1. Insert the USB in to the CloudBond 365 device.
2. From the Start menu, run the Veeam Create Recovery Media.

Figure 45-1: Create Recovery Media



3. On the Recovery Media screen, select the USB drive.

Figure 45-2: Create Recovery Media – Recovery Media



4. Click **Next** until the Progress step is displayed.
5. When the process has completed, click **Finish**.
6. Remove the USB from the device.

46 Preparing for Veeam's Software Installation on CloudBond 365 Server

The following must be done before installing Veeam's software on the CloudBond 365 server.



Note: Installing backup may require a server restart.

Before installing Veeam's Software on CloudBond 365 Server, do the following:

1. Decide which backup architecture is required according to the available options.
2. Confirm that all servers are working (up and running).
3. To install Veeam software, you must use the Remote Desktop Connection to the CloudBond 365 and to the Backup server (VBR).
4. Download the software on the VBR server.
5. CloudBond 365 may require Windows updates to support the backup.

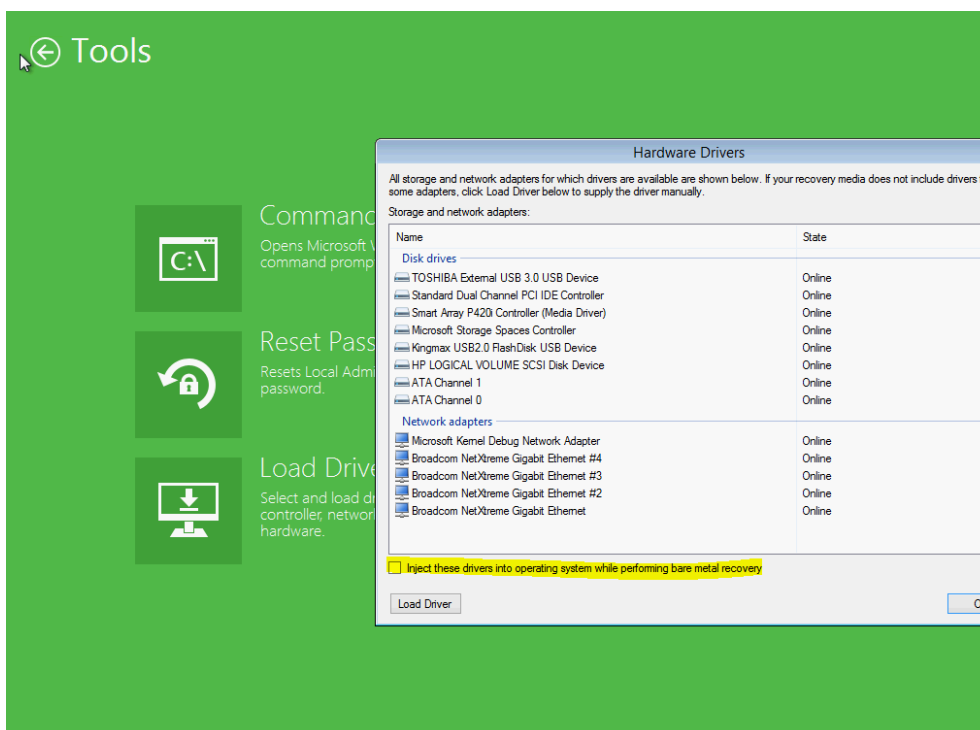
47 Troubleshooting

The following provides information to assist you in troubleshooting issues.

47.1 Restoring Host Server using VEB if no or some Network Cards are Available

Make sure that when you are restoring the Host server using VEB, you first clear the 'Inject these drivers...' checkbox. If you didn't do this, perform the restore procedure again correctly.

Figure 47-1: Hardware Drivers – Clear Check Box



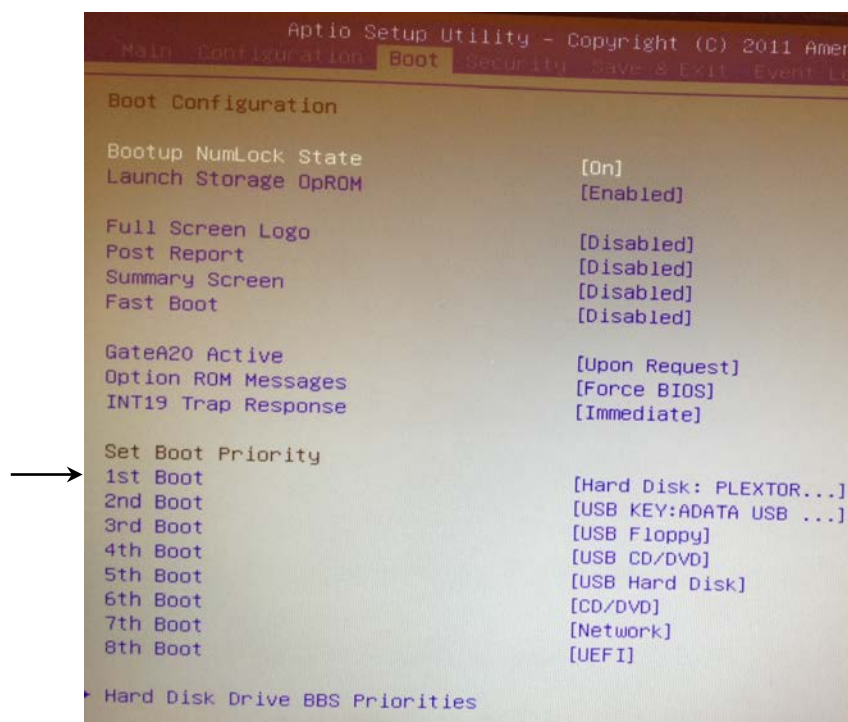
➤ **To restore the Host Server using VEB if no or some network cards are available:**

1. Open the device manager and enable the 'Shown hidden device' option from the **View** menu.
2. Delete all the network cards which are marked with an error flag.
3. From **Action** menu select the **Scan** option.
4. Ensure that all networks are available now.
5. Restart the server.
6. Define the HyperV virtual switch again, using the same names as was done previously (e.g., LAN and DMZ).

47.2 No Boot Device Error – Setting Boot Priority

If a USB (Key or Disk) is connected to the server, confirm that the boot order in the BIOS is correct and that the hard disk is set as the first priority, as shown in the figure below.

Figure 47-2: Hardware Drivers – Setting Boot Priority



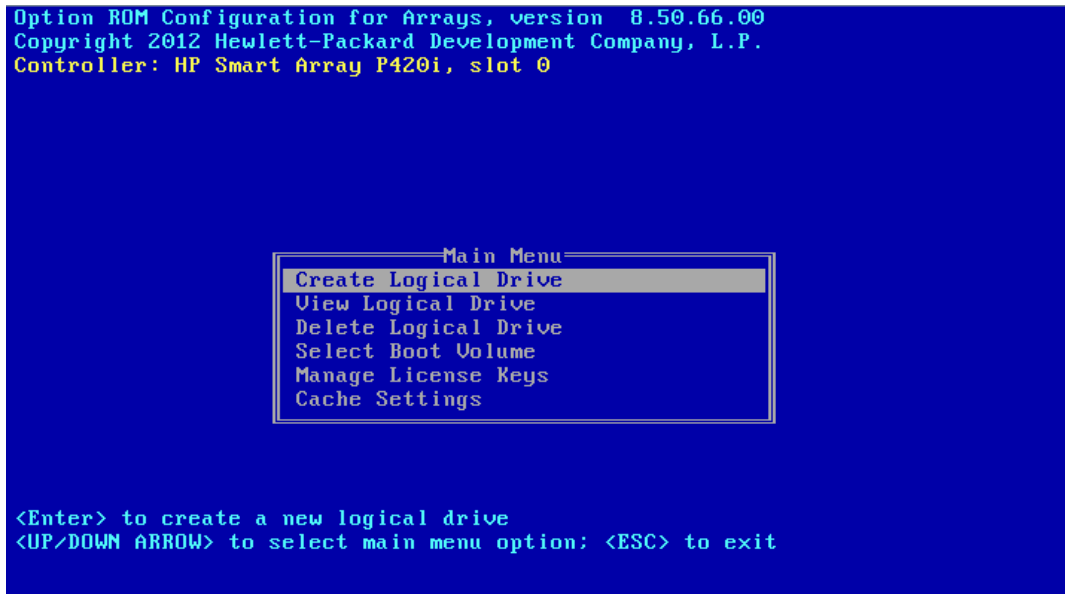
47.3 No Boot Device Error - How to Define Logical Drive and Selecting Boot Volume

This section is relevant only for CloudBond 365 Pro Box and Enterprise Box editions.

➤ To define the logical drive and select the boot volume:

1. Re-boot the CloudBond 365 server, and then press **F8**; the following screen appears:

Figure 47-3: Defining a Logical Drive



From this menu you can:

- View a logical drive. For the Pro Box edition, the name of the drive should be **RAID 1**. For the Enterprise Box edition it should be **RAID 5**.
- Delete the current logical Drive
- Create a logical drive
- Select the boot volume

If the RAID setup is incorrect, delete the current one and define the correct one. If you see a Boot Error message, select the boot volume as the logical drive that attaches to the server.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/contact

Website: www.audiocodes.com

©2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-26319

