Videoconferencing Systems

Media Xchange Manager™
Version 4.0

Administrator’s Guide

DOC01094 Rev. 4.0 08.03
Limited Warranty

VCON Ltd. warrants that SOFTWARE will perform according to accompanying user documentation for a period of 90 (ninety) days from the date of receipt; replacement SOFTWARE will be warranted for 90 (ninety) days from the date of receipt. This Limited Warranty shall not apply to any product that in the opinion of VCON Ltd. has not been installed or upgraded according to accompanying documentation from VCON Ltd. or been subject to misuse, misapplication, negligence or accident while in the hands of the purchaser.

GRANT OF LICENCE VCON Ltd. grants the Purchaser a non-exclusive and non-transferable license to use the SOFTWARE product and to make one copy solely for backup or archival purposes, which may include user documentation provided via online or other electronic form. Additional copies may not be made nor may anyone else be allowed to copy or otherwise reproduce any part of the licensed software without prior written consent of VCON Ltd.
About this Administrator’s Guide

This Administrator Guide explains how to work with the VCON Media Xchange Manager (MXM) system. The following chapter summary briefly describes this guide’s contents:

Chapter 1  Welcome to Media Xchange Manager™
Introduction to the MXM and to this Administrator’s Guide

Chapter 2  Getting Started
Instructions for installing the MXM.

Chapter 3  A Quick Tour of the MXM Administrator
Brief description of the main MXM applications’ screens.

Chapter 4  Managing the MXM
Procedures for configuring administrators and MXMs, monitoring status within the video network, and setting up hunting and administrative groups.
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Setting MXM System Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 5</td>
<td>Descriptions of the various properties that comprise the MXM’s system configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Defining End Point Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 6</td>
<td>Procedures for defining registered end points which run VCON or third-party videoconferencing applications.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Registering Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 7</td>
<td>Procedures for registering, setting up a gateway’s MXM configuration and setting up available gateway services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Registering an MCU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 8</td>
<td>Procedures for registering, setting up an MCU’s MXM configuration, defining MCU service properties, and setting up MCU service permission groups.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Neighboring Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 9</td>
<td>Procedures for setting up an MXM-managed network that includes more than one zone of videoconferencing users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Registering with LDAP Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 10</td>
<td>Procedures and required information for setting up the MXM’s configuration in online directory servers such as ILS and NDS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Initiating Videoconferences From the MXM Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 11</td>
<td>Instructions for setting up and starting videoconferences from the Administrator application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12</th>
<th>Setting Up Multipoint Videoconferences Managed by a VCB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 12</td>
<td>Instructions for setting up VCON Conference Bridge for initiating ad-hoc multipoint videoconferences.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13</th>
<th>Customizing the MXM Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 13</td>
<td>Procedures for customizing the Administrator application according to your personal preferences.</td>
</tr>
</tbody>
</table>
Chapter 14  Remote Upgrade of Videoconferencing Devices Software
Instructions for upgrading the videoconferencing software of registered end points through the Remote Software Upgrade utility.

Chapter 15  Least Cost Routing of Gateway Calls
Description and instructions for determining the most cost-efficient gateway services for IP-to-ISDN calls originating from the MXM’s zone.

Chapter 16  Managing SIP Networks
Instructions for registering SIP User Agents, setting up SIP Proxy Server, and initiating calls involving SIP User Agents.

Chapter 17  Configuring ALG Proxy Servers
Instructions for configuring the ALG Proxy Server (from VCON’s SecureConnect family), which provide connectivity for videoconferencing networks in organizations that have also installed NATs and firewalls.

Appendix A  vPoint™ End Point Properties
Definitions of configuration properties for vPoint end points.

Appendix B  MeetingPoint® End Point Properties
Definitions of configuration properties for MeetingPoint 4.5 (and higher) end points.

Appendix C  Falcon™ End Point Properties
Definitions of configuration properties for Falcon end points.

Appendix D  QoS Priority Values
List of available QoS priority level settings for IP Precedence and DiffServ.

Appendix E  Using Accord® MGC™ with the MXM
Instructions for setting up the Accord MGC’s configuration for management within the MXM’s network.
Appendix F  Upgrading Falcon Software
Procedures for updating your VCON Falcon devices to the latest software version.

Appendix G  Setting Up the IPNexus Configuration
Instructions for setting up the IPNexus configuration in the MXM.

VCON Technical Support
This Administrator’s Guide was designed to help you set up and work with your MXM easily so that you can enjoy its many features.

If a situation occurs that is not covered by the supplied documentation, please request help from our Technical Support channels. VCON’s organization will make its strongest efforts to help you resume your videoconferencing as soon as possible.

1. Contact your local VCON distributor, and request assistance from its technical support department.

2. Send an e-mail message fully describing the condition plus your system’s configuration to techsup@vcon.co.il.
# Table of Contents

- Limited Warranty ........................................................................................................... ii
- About this Administrator’s Guide ................................................................................... iii
- VCON Technical Support ............................................................................................... vi

## 1 Welcome to Media Xchange Manager™ .............................................................. 1
  1.1 About the MXM Server ....................................................................................... 1
  1.2 About the MXM Administrator ........................................................................... 2
  1.3 About the VCON Conference Bridge (VCB) ..................................................... 3
  1.4 About IPNexus ..................................................................................................... 4
  1.5 About SecureConnect .......................................................................................... 5
  1.6 Glossary of MXM Terms ..................................................................................... 6

## 2 Getting Started ...................................................................................................... 9
  2.1 Minimum System Requirements ........................................................................... 9
      MXM Server ............................................................................................................. 9
      MXM Administrator Application ............................................................................ 10
      VCON Conference Bridge .................................................................................... 10
      Encryption Client .................................................................................................. 11
      IPNexus Server ..................................................................................................... 12
      IPNexus Client ...................................................................................................... 12
  2.2 Installing the MXM Server ................................................................................... 13
  2.3 Installing the MXM Administrator ...................................................................... 15
  2.4 Installing the VCON Conference Bridge ............................................................ 16
  2.5 Installing the IPNexus Server .............................................................................. 17
  2.6 Installing the IPNexus Client .............................................................................. 18
  2.7 Replacing the MXM License Key ......................................................................... 19
  2.8 Running the MXM ............................................................................................... 20
  2.9 Basic MXM Operations ....................................................................................... 22

## 3 A Quick Tour of the MXM Administrator ............................................................ 25
  3.1 The Main View .................................................................................................... 25
      Connected MXMs ................................................................................................ 26
      Registered Nodes .................................................................................................. 27
      Neighboring MXMs and Gatekeeper Zones ....................................................... 28
      Software Upgrade Indication ............................................................................. 28
      Filtering the Main View ...................................................................................... 29
  3.2 The Node Status View ....................................................................................... 30
  3.3 The Login Status View ....................................................................................... 30
  3.4 The Event Log ..................................................................................................... 31
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>LDAP Servers</td>
<td>31</td>
</tr>
<tr>
<td>4</td>
<td>Managing the MXM</td>
<td>33</td>
</tr>
<tr>
<td>4.1</td>
<td>Setting Up Administrators</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Adding an Administrator</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Changing Administrator Properties</td>
<td>35</td>
</tr>
<tr>
<td>4.2</td>
<td>Editing Nodes</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Adding Nodes</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Deleting a Login Request</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Setting a Node’s Properties</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Finding Nodes and Objects in the Administrator</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Editing Multiple Nodes</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Changing Directory Numbers</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Deleting a Node</td>
<td>44</td>
</tr>
<tr>
<td>4.3</td>
<td>Status Monitoring</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Monitoring Nodes in the Main View</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Viewing the Login Status</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Viewing the Node Status</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Event Log Monitoring</td>
<td>49</td>
</tr>
<tr>
<td>4.4</td>
<td>Setting Up Templates</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Editing a Template</td>
<td>55</td>
</tr>
<tr>
<td>4.5</td>
<td>Adding Hunting Groups</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>General Properties</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Call Forwarding Properties</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Hunting Group Properties</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Hunting Group LDAP Properties</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Additional ID Properties</td>
<td>63</td>
</tr>
<tr>
<td>4.6</td>
<td>Adding an Administrative Group</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Changing Group Member Properties</td>
<td>65</td>
</tr>
<tr>
<td>4.7</td>
<td>Adding a Short Dial Number</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>General Properties</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Call Forwarding Properties</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>LDAP Properties</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Additional ID Properties</td>
<td>67</td>
</tr>
<tr>
<td>5</td>
<td>Setting MXM System Properties</td>
<td>69</td>
</tr>
<tr>
<td>5.1</td>
<td>MXM Properties</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>Connection</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>System Info</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Dial Plan</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>LDAP Settings</td>
<td>77</td>
</tr>
</tbody>
</table>
# Table of Contents

## 5.2 Call Control Properties ................................................................. 78
- Bandwidth Control ............................................................................. 79
- Call Settings ..................................................................................... 80
- Ad-hoc Resources ............................................................................. 81

## 5.3 ISDN Call Routing Properties .................................................... 82
- System Location ................................................................................ 82
- Dialing Prefixes ............................................................................... 83

## 5.4 Security Properties ....................................................................... 85
- Security Mode .................................................................................... 85
- License .............................................................................................. 87
- Non-Registered Devices ................................................................... 89

## 5.5 H.323 & SIP Properties ................................................................. 90
- Zone Settings ..................................................................................... 90
- Advanced Settings ............................................................................ 92

## 5.6 Reporting Properties ................................................................. 93
- Billing .............................................................................................. 93
- Event Log ......................................................................................... 94

## 6 Defining End Point Nodes ............................................................... 95
### 6.1 Setting Up an End Point ............................................................. 95
- Login Attempt by Duplicate Users ..................................................... 96

### 6.2 Setting End Point MXM Properties .......................................... 97
- General ............................................................................................ 97
- Status .............................................................................................. 99
- Call Forwarding ............................................................................... 100
- Bandwidth Control Properties ......................................................... 101
- Pickup Permissions .......................................................................... 103
- MCU Service .................................................................................. 104
- Gateway Services ........................................................................... 105
- ISDN Call Routing .......................................................................... 106
- Product Info .................................................................................... 108
- LDAP .............................................................................................. 109
- Additional IDs ................................................................................ 111

## 7 Registering Gateways ................................................................. 113
### 7.1 Logging in a New Gateway ....................................................... 113
### 7.2 Setting Gateway Properties ..................................................... 116
- General ............................................................................................ 116
- Product Info .................................................................................... 117
- ISDN Dialing .................................................................................. 118
- Call Routing ................................................................................... 120
# Table of Contents

7.3 Setting Gateway Service Properties ................................................. 123  
   General ................................................................................................. 123  
   Bandwidth Control ............................................................................... 124  

7.4 Gateway Service Hunting Groups ............................................. 125

8 **Registering an MCU** .............................................................. 127  

8.1 Logging in a New MCU ................................................................. 127  
8.2 Setting MCU Properties ................................................................. 129  
   General ................................................................................................. 129  
   Bandwidth Control ............................................................................... 130  
   Product Info ........................................................................................ 131  
8.3 MCU Services .................................................................................. 133  
   General ................................................................................................. 134  
   Bandwidth Control ............................................................................... 135  
   Ad-Hoc Conference ............................................................................. 136  
   LDAP .................................................................................................... 137  
   Additional ID ........................................................................................ 137  
8.4 MCU Service Permission Groups ............................................... 138  
   General ................................................................................................. 139  
   Permission Group ............................................................................... 140  
8.5 Dedicated MCU Services .............................................................. 141  
8.6 Ad-hoc Permission Groups ............................................................. 142  
   General ................................................................................................. 143  
   Permission Group ............................................................................... 144  

9 **Neighboring Zones** ................................................................. 147  

9.1 The MXM’s Relationship with Neighboring Zones ..................... 147  
9.2 Logging in New Zones ................................................................. 148  
   Adding Zones Automatically ............................................................. 148  
   Adding Zones Manually .................................................................. 149  
9.3 Setting Zone Properties ................................................................. 150  
   General ................................................................................................. 150  
   Zone Settings ..................................................................................... 151  
   Bandwidth Control ............................................................................... 153  
   MCU Services ..................................................................................... 154  
   Gateway Services ............................................................................... 156  
   ISDN Call Routing ............................................................................... 158  
   Product Info ........................................................................................ 159  
   Additional IDs ..................................................................................... 160  
   Redundancy ....................................................................................... 161  
   Advanced ............................................................................................ 162
9.4 Permanent Non-Registered Devices .......................................................... 164
   Adding a Permanent Non-Registered Device ........................................ 164
9.5 Inter-Zone Videoconferencing Management ........................................... 165
   Setting Up Inter-Zone Dialing ............................................................... 165
   Directory Gatekeepers ........................................................................... 169
   Restricting Bandwidth Allotment ......................................................... 173
   Restricting H.450 Exchange Functions .................................................. 175
   Sharing Gateway and MCU Services with Other Zones ....................... 177

10 Registering with LDAP Directories ......................................................... 181
10.1 Registering the MXM with an ILS ......................................................... 183
    Setting Up the ILS Configuration in the MXM Administrator .............. 185
10.2 Registering the MXM with Microsoft Exchange Server ...................... 187
    Setting Up the Exchange Server Configuration in the MXM Administrator ............................................................... 190
10.3 Registering the MXM with Windows 2000 Active Directory .............. 192
    Adding an Administrator with Full Configuration Rights .................... 192
    Adding the MXM Attributes ............................................................... 193
    Adding the MXMNode Class ............................................................... 195
    Granting Full Control for the MXMNode Class to an Active Directory User ........................................................................................................... 199
    Setting the Properties of the MXM Attributes ................................... 200
    Creating an Organizational Unit for Your MXM ................................. 201
    Setting Up the LDAP Configuration in the MXM Administrator .......... 202
10.4 Registering the MXM with Novell Directory Services (NDS) .............. 203
    Creating MXM Attributes .................................................................... 204
    Creating the MXMNode Class ............................................................... 207
    Creating an MXM Container ................................................................ 210
    Setting Up the LDAP Group Object Configuration ............................... 211
    Adding a Trustee for the MXMNode Container .................................... 213
    Setting Up the LDAP Configuration in the MXM Administrator .......... 214
10.5 Registering the MXM with ILS on Windows 2000 ............................ 215
    Setting Up the LDAP Configuration in the MXM Administrator .......... 215
10.6 Registering the MXM with Netscape Directory Server ..................... 216
    Setting Up the LDAP Configuration in the MXM Administrator .......... 218

11 Initiating Videoconferences From the MXM Administrator ............... 219
11.1 Administrator-Initiated LAN Dialing .................................................. 219
    Setting Point-to-Point Videoconference Properties .............................. 220
11.2 Administrator-Initiated ISDN Dialing .................................................. 222
    Setting ISDN Videoconference Properties ........................................... 221
11.3 Administrator-Initiated Hang Up ....................................................... 222
# Table of Contents

12 Setting Up Multipoint Videoconferences Managed by a VCB .... 223
   12.1 Overview of the VCON Conference Bridge ................................. 223
   12.2 Logging in a New VCB............................................................... 225
   12.3 Setting VCB Properties .......................................................... 227
       General .................................................................................. 228
       License ................................................................................ 229
       Firewall ............................................................................... 230
       Product Info ...................................................................... 231
   12.4 Setting VCB Services Properties ............................................. 232
       General ................................................................................ 233
       Ad-Hoc Conference ................................................................ 234
       Session ................................................................................ 235
       Multicast ............................................................................ 237
       Advanced ........................................................................... 238
       QoS .................................................................................... 239
       LDAP .................................................................................. 240
       Additional ID ...................................................................... 240
   12.5 Expanding to an Ad-hoc Videoconference ................................. 241

13 Customizing the MXM Administrator ........................................... 243
   13.1 Defining the Main View Options ............................................. 243
       Tree Styles .......................................................................... 243
       Item Attributes .................................................................. 245
   13.2 Setting Up the Workspace .................................................... 247
       Defining Workspace Options ............................................. 247
       Managing Workspaces ...................................................... 249
   13.3 Customizing the Toolbar ....................................................... 254
       Defining the Toolbar Display ............................................. 254
       Adding and Removing Toolbar Buttons .............................. 256
       Creating a Custom Toolbar ................................................ 257
   13.4 Customizing the Status Views ............................................... 258
       Setting Table On-Screen Display Properties ....................... 258
       Style Formats for Table Elements or Types of Information ... 261
       Showing and Hiding Columns ............................................ 265

14 Remote Upgrade of Videoconferencing Devices Software .......... 267
   14.1 Defining a Software Upgrade ................................................ 268
   14.2 Setting Software Upgrade Properties .................................... 269
       Selecting a Software Version ............................................. 270
       Setting a Target Location for the Upgrade .......................... 271
       Setting Up User Login ......................................................... 274
       Setting the Upgrade Schedule ............................................ 275
### Table of Contents

- Confirm Upgrade Definition ................................................................. 277
- 14.3 Selecting Nodes to Upgrade ............................................................ 278
  - Node Software Upgrade Properties .................................................. 278
- 14.4 Monitoring Software Upgrade Status ............................................. 284

#### 15 Least Cost Routing of Gateway Calls ........................................... 285
- 15.1 Setting ISDN Call Routing Properties .............................................. 286
- 15.2 Setting Gateway Call Routing Properties ....................................... 288
- 15.3 Setting Preference of Using Least Cost Routing or Bandwidth Rules . 288
- 15.4 Testing for the Optimal Gateway Service ....................................... 290

#### 16 Managing SIP Networks ............................................................... 293
- 16.1 SIP User Agents ........................................................................... 293
- 16.2 SIP Servers .................................................................................. 294
  - SIP Proxy ......................................................................................... 294
  - SIP Redirect Server ....................................................................... 295
  - SIP Registrar .................................................................................. 295
- 16.3 Logging in New SIP User Agents .................................................... 296
- 16.4 Setting the MXM SIP Advanced Settings ....................................... 297
- 16.5 Registering a Windows XP Messenger SIP User Agent to the MXM . 298
- 16.6 Dialing Unlisted Users in Windows XP Messenger ....................... 300

#### 17 Configuring ALG Proxy Servers ..................................................... 301
- 17.1 Setting ALG Proxy Properties in the MXM Administrator ............. 302
  - General ............................................................................................ 303
  - Server Settings ............................................................................... 304
  - License ............................................................................................. 305
  - Encryption Settings ........................................................................ 306
  - Proxy Timeouts .............................................................................. 307
  - Firewall/Network Settings ............................................................... 308
  - QoS ................................................................................................. 309

#### A vPoint™ End Point Properties ....................................................... 311
- A.1 Conversation Properties ................................................................. 311
  - Video ............................................................................................... 311
  - Data ................................................................................................. 313
- A.2 Calls Properties ............................................................................. 314
  - Incoming Calls ................................................................................ 314
  - Outgoing Calls ............................................................................... 315
  - Ringing ............................................................................................. 316
  - 3rd Party Viewer .............................................................................. 317
  - Interactive Multicast ...................................................................... 319
Table of Contents

A.3 User Data Properties ................................................................. 322
A.4 Communication Properties ................................................... 323
  LAN ........................................................................................ 323
  Firewall ............................................................................... 325
  Login .................................................................................. 326
A.5 Hardware Properties ............................................................... 327
  Audio .................................................................................. 327
  Camera ............................................................................... 330
A.6 Advanced Properties .............................................................. 331
  System Info ......................................................................... 331
  QoS .................................................................................. 332
  Intras ............................................................................... 333
  Advanced Video ................................................................. 334
  Advanced Audio ................................................................. 335

B  MeetingPoint® End Point Properties ........................................ 337
  B.1 Conversation Properties ..................................................... 337
    Video ................................................................................ 337
    Data ............................................................................... 340
  B.2 Calls Properties ................................................................. 342
    Incoming Calls .................................................................. 342
    Ringing ........................................................................... 343
    3rd Party Viewer ......................................................... 344
    Interactive Multicast .................................................... 346
  B.3 User Data Properties ............................................................ 348
  B.4 Communication Properties .................................................. 349
    LAN ............................................................................... 349
    Firewall ........................................................................... 351
    Login ............................................................................... 352
    Connection ....................................................................... 353
  B.5 Telephony Properties ............................................................ 354
    Phone Numbers .............................................................. 354
    Switch Type ..................................................................... 355
    SPID Numbers ................................................................ 356
    MSN ............................................................................... 357
    Subaddressing ............................................................... 358
    Dialing ........................................................................... 359
  B.6 Hardware Properties ............................................................. 360
    Audio ............................................................................... 360
    Camera ........................................................................... 367
## Table of Contents

B.7 Advanced Properties .............................................................. 368  
System Info ................................................................................. 368  
QoS .............................................................................................. 369  
Intras .......................................................................................... 371  
Advanced Video ......................................................................... 372  
Advanced Audio ......................................................................... 373  

C Falcon™ End Point Properties ......................................................... 375  
C.1 Network Configuration .......................................................... 376  
LAN Connection and Registration .............................................. 376  
Firewall ....................................................................................... 377  
H.323 Management .................................................................... 378  
QoS .............................................................................................. 380  
Phone Numbers .......................................................................... 381  
Switch Type ................................................................................ 382  
SPID Numbers ........................................................................... 383  
C.2 Video Properties ..................................................................... 384  
C.3 Audio Properties ..................................................................... 385  
C.4 Options ................................................................................ 387  
General Options ......................................................................... 387  
Version ...................................................................................... 388  
Security ...................................................................................... 389  

D QoS Priority Values ...................................................................... 391  
D.1 IP Precedence Values ........................................................... 391  
D.2 DiffServ Values ...................................................................... 392  

E Using Accord® MGC™ with the MXM .......................................... 393  
E.1 MGC Configuration ............................................................... 393  
Network Services Configuration .................................................. 393  
H.323 Card Configuration ............................................................. 398  
E.2 Adding an Accord Meeting Room .......................................... 399  
E.3 Setting Meeting Room Properties .......................................... 400  
General ....................................................................................... 400  
Ad-hoc Conference .................................................................. 401  
Hunting Group ........................................................................ 402  
LDAP .......................................................................................... 403  
Additional ID ........................................................................... 403  
E.4 Adding an Accord Gateway ................................................... 404
E.5 Setting Accord Gateway Properties .............................................. 405
  General ......................................................................................... 405
  Dialing ........................................................................................... 406
  Resources ....................................................................................... 408
  Call Routing .................................................................................... 409
E.6 Adding Accord Gateway Services .............................................. 409

F Upgrading Falcon Software ........................................................... 411
  F.1 Running the Upgrade Program ..................................................... 412
  F.2 Applying the New Upgrade ......................................................... 414
  F.3 Post-Upgrade Procedures ........................................................... 415
  F.4 Installer Mode ............................................................................ 415
  F.5 Software Key Upgrade ............................................................... 416

G Setting Up the IPNexus Configuration ........................................... 417
  G.1 Creating an IPNexus User Type ................................................... 418
  G.2 Installing Internet Information Services (IIS) ............................ 419
  G.3 Creating an IPNexus Folder for FTP/Web Access ........................ 420
  G.4 Creating a Virtual FTP Directory ................................................ 421
  G.5 Creating a Virtual Web Directory ............................................... 422
  G.6 Setting FTP Properties in the MXM .......................................... 422
  G.7 Setting Options Properties in the MXM ..................................... 424
  G.8 Setting Up WebSharing ............................................................. 425

Index .............................................................................................. 427
1 WELCOME TO MEDIA XCHANGE MANAGER™

Congratulations on your entry into the revolutionary world of VCON’s Media Xchange Manager™ (MXM). The MXM centralizes the management of Video over IP communication within an enterprise-wide network.

1.1 About the MXM Server

The MXM provides centralized videoconferencing management services for corporate networks running on IP. It transfers many administration and configuration tasks from the individual computers, called end points, to the network, where they belong.

The MXM provides the following services:

- H.323 Revision 2-compliant Gatekeeper functions, including login and security:
  - Auto-discovery and registration of nodes, such as videoconferencing end points, gateways, MCUs and their respective services.
  - Address translation of IP addresses, H.323 aliases, E.164 numbers, e-mail addresses and URLs.
- Call Forwarding, Pickup, Transfer, Ad-hoc Conferencing and Hunting Groups
- Search capabilities for nodes in zones managed by other MXMs and gatekeepers
- Simplified gateway and MCU dialing for registered end points
- Control of the usage of gateway and MCU services by registered users
- Bandwidth management for allocating available bandwidth to registered nodes
- Compatibility with external online directory services (LDAP)
- IP-Nexus messaging and chat
- Network usage reports (Call Details Records and Asset Management Reports) - optional
- Integrated Videoconferencing Bridge (VCB) - optional.
1.2 About the MXM Administrator

The Administrator application provides an interface for performing the management and monitoring of the MXM network. It may be installed on the same computer as the MXM Server as well as on additional computers, therefore providing remote management capability.

The Administrator application enables:

- Remote configuration and management of VCON vPoint, MeetingPoint, Falcon, and VCB nodes
- Registration, configuration and management of H.323 end points, such as VCON’s and other vendors’ H.323 Rev. 1 & 2-compliant videoconferencing systems
- Registration, configuration and management of SIP User Agents, such as SIP phones and Windows XP Messenger applications.
- Registration, configuration and management of Gateways, MCUs and their respective services
- Configuration of videoconferencing policies between the local MXM and zones of nodes managed by other MXMs and gatekeepers
- Monitoring of connection states, login status, and events logging
- Creation of hunting groups (groups of end points that may be called through one common number)
- Creation of administrative groups that reflect the organization’s corporate structure and enables efficient configuration of these groups’ stations
- Setting limits on the permitted bandwidth usage
- Initiation and hangup of point-to-point calls between two end points
- Utility for upgrading the videoconferencing software of registered end points
- Testing for Least Cost Routing of gateway calls.
1.3 About the VCON Conference Bridge (VCB)

The VCON Conference Bridge (VCB) is an economical means of initiating and managing videoconferences that have more than two participants. The VCB serves both as a dial-in multipoint conferencing bridge and an ad-hoc conferencing bridge, in which additional users are “invited and joined” by conference participants.

VCB features include:

- Up to 64 concurrent participants (8x8, 4x16, 2x32, 1x64, or mixture), depending on the audio codec used by the sessions.
  - Up to 64 participants (8x8, 4x16, 2x32, or mixture) in all sessions using G.711 audio
  - Up to 32 participants (4x8, 2x16, 1x32, or mixture) in all sessions using G.722 audio or mixed G.711/G.722
- G.722 audio support with transcoding (G.711)
- Dynamic resource allocation pool – Unallocated ports may be used as overflow for configured sessions.
- Simultaneous streaming of active multicast conferences
- Support for sessions including H.323 end points/devices and SIP User Agents (through the MXM's embedded SIP proxy server).
- Administrator configuration of voice-switching delay value (through MXM).
- Multi-point sessions can be joined (cascaded) onto other sessions, contingent on similar data rates, display types, and audio/video algorithms.
  - VCB to VCB
  - VCB to other
- Generation of MCU statistics reports
  - Intra requests per second (from end point to VCB)
  - Packet loss (from end point to VCB and from VCB to end point
  - Effective data rate (video transmission and reception)
- vPoint endpoints up to size of the MXM included.
1.4 About IPNexus

IPNexus is a secure instant messaging and data collaboration application that helps users communicate and work more efficiently across geographic, departmental and organizational boundaries.

IPNexus provides the following:

- Secure enterprise-wide instant messaging
- Switching to videoconferencing or voice session
- IPQuickNotes - sending instant notes that open up on the recipient’s screen
- IPQuickPoll - quick surveys and responses to common questions among multiple users
- IPSnapShot - capturing an application or screen section and sending it to other participants
- IPAppShare - sharing an application or screen section with other participants
- File transfer between participants
- Sending e-mail to participants in a messaging session
- Up to 1000 (scalable) concurrent logged-in users.
1.5 About SecureConnect

The SecureConnect system enables communication between NATs or firewall-protected networks and external networks. It allows your organization to safely carry on videoconferencing through your firewalls and also provides encryption to the sessions. The SecureConnect system comprises the following components:

- **The ALG (Application Level Gateway) Proxy Server** translates H.323 messages between the private LAN or NAT and the public WAN. It also routes management channels across network boundaries. The VCON ALG Proxy translates private IP addresses to public ones and conversely, from public to private addresses. It also relays every packet towards the correct destination according to its mapping configuration. Network interface cards (NIC) connect the private LAN and public networks.

  Throughout this guide, the name, “ALG Proxy,” refers to the ALG Proxy Server.

- **The Advanced Encryption Server** authenticates the various clients and assigns public encryption keys to them. The AES encrypts videoconferences and other data transmissions across public or private networks.

- **The Encryption Client** is an application which may be installed on PC-based devices such as end points, MCUs and other servers within your organization. The Encryption Client operates as a virtual network card, and encrypts all data transmissions from devices in which this client application is installed. The Encryption Client applies the encryption to signaling and media streams immediately as they leave the Client’s host.
1.6 Glossary of MXM Terms

This section lists special MXM terms that are commonly used in this guide.

Ad-hoc conference
A videoconference that expands from a point-to-point session to a multipoint session while it remains open. Additional end points are "invited" by one of the parties.

Administrator
User whose responsibilities may include monitoring and managing the MXM network. Three levels of Administrator provide various rights for managing, controlling, monitoring, and viewing information.

End point
An H.323 terminal, Gateway, or MCU. An end point can call and be called. It generates and/or terminates information streams.

Firewall
A means of providing a network security from intruders. Firewalls may employ a single router or a combination of routers and servers that perform firewall processing of incoming and outgoing traffic.

Gatekeeper
Application that controls registration (login) into a computer or network, translates addresses, and manages bandwidth within a network.

Gateway
A network device that enables communication between two different types of networks, such as IP and ISDN telephony.

Hunting group
A group of users within an organization that may be reached through one common number.

LDAP
Lightweight Directory Access Protocol - used to access online directory servers, for registering and searching for other online users.

Login
The process of gaining entry, or registering, into a computer or a network.

MCU
Multipoint Control Unit - a device used to connect three or more end points in a single video meeting.

MXM Node
A node that is registered in the local MXM.
| **NAT** | Network Address Translation - An IETF standard that allows an organization to present itself to the Internet with one address. |
| **Neighbor Node** | A node that is registered in a neighboring zone. |
| **Neighboring Zone** | A zone that is known and listed in the local MXM. |
| **Node** | A device on a LAN. For example, end points, gateways and MCUs are nodes. |
| **Service** | A configuration for the allocation of available bandwidth during videoconferences through gateways or MCUs. |
| **Template** | A complete set of default properties for new nodes. |
| **Zone** | A collection of nodes that MXMs and gatekeepers register and manage. |
2  **GETTING STARTED**

2.1  **Minimum System Requirements**

The components of the MXM may be installed and operated on any computer that meets the following minimum requirements:

**MXM Server**

For optimum performance, install the MXM Server on a workstation or server that contains only the Windows 2000 operating system with Service Pack 3 or higher. We recommend that no other applications except MXM Administrator, VCON Conference Bridge (VCB), or IP-Nexus are installed on it at any time. The presence of other applications (even if they are not open) may cause unpredictable operating results.

1. No other application may use the computer’s default H.323 TCP/IP ports.
2. MXM installation program installs MDAC 2.7, which upgrades the ODBC driver, and MSDE 2000.

**Basic Version**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 2000 Server with Service Pack 3 or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>1 GHz</td>
</tr>
<tr>
<td>Recommended Memory</td>
<td>at least 512 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>200 MB</td>
</tr>
</tbody>
</table>

**With 2 VCB Session Support**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 2000 Server with Service Pack 3 or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>1.4 GHz</td>
</tr>
<tr>
<td>Recommended Memory</td>
<td>at least 512 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>300 MB</td>
</tr>
</tbody>
</table>
2.1 Minimum System Requirements

With IP-Nexus

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 2000 Server with Service Pack 3 or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>1.4 GHz</td>
</tr>
<tr>
<td>Recommended Memory</td>
<td>at least 512 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>300 MB</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Installed on same network</td>
</tr>
</tbody>
</table>

MXM Administrator Application

The MXM Administrator application may be installed on any workstation(s) on the network that meet the following specifications:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 98/XP/2000/NT 4.0 with Service Pack 5 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>166 MHz</td>
</tr>
<tr>
<td>Minimum Memory</td>
<td>64 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>10 MB</td>
</tr>
</tbody>
</table>

VCON Conference Bridge

The VCON Conference Bridge (VCB) may be installed on any workstation(s) on the network that meet the specifications detailed in this section.

1. MXM Server may be installed on the same computer as a VCB supporting up to 2 sessions.
2. VCON MediaConnect 9000 may be installed on the same computer as a VCB supporting 1 session.
3. VCBs managing 2 or more sessions must run on a dedicated computer with no other applications (except MXM Administrator) running.
4. The VCB must be registered to the MXM (version 2.01 or later).
## 8 Port Support

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 2000 Server with Service Pack 3 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>1.4 GHz</td>
</tr>
<tr>
<td>Minimum Memory</td>
<td>512 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>300 MB</td>
</tr>
</tbody>
</table>

## 16, 32, or 64 Port Support

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 2000 Server with Service Pack 3 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Minimum Memory</td>
<td>512 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>300 MB</td>
</tr>
</tbody>
</table>

## Encryption Client

The Encryption Client may be installed on any workstation(s) on the network that meet the following specifications:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows 98/XP/2000/NT 4.0 with Service Pack 4 or higher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU Speed</td>
<td>200 MHz</td>
</tr>
<tr>
<td>Minimum Memory</td>
<td>64 MB</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>7 MB</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Internet Explorer 5 (for Windows 98FE)</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 4.01 with Service Pack 1 (for Windows 98SE, 98ME, NT4, 2000, XP.</td>
</tr>
</tbody>
</table>
2.1 Minimum System Requirements

**IPNexus Server**

If the IPNexus Server will be installed on a computer other than that hosting the MXM, the computer must meet the following minimum requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 2000 Server with Service Pack 3 or higher.</td>
</tr>
<tr>
<td>Minimum CPU Speed</td>
<td>500 MHz</td>
</tr>
<tr>
<td>Minimum Memory</td>
<td>256 MB</td>
</tr>
<tr>
<td>Network</td>
<td>Connection to IP network</td>
</tr>
<tr>
<td>Remote Access (optional)</td>
<td>Internet access</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Read/write access</td>
</tr>
</tbody>
</table>

**IPNexus Client**

The IPNexus Client may be installed on any computer that meets the following specifications.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 95 or higher.</td>
</tr>
<tr>
<td>Computer type</td>
<td>Pentium Class</td>
</tr>
<tr>
<td>System Display</td>
<td>16-bit color or higher</td>
</tr>
<tr>
<td>Minimum Free Disk Space</td>
<td>10 MB</td>
</tr>
<tr>
<td>Network</td>
<td>Connection to IP network</td>
</tr>
<tr>
<td>Remote Access (optional)</td>
<td>Internet access</td>
</tr>
</tbody>
</table>
2.2 Installing the MXM Server

The MXM server must be installed on a Windows 2000 Server dedicated to the management of your organization’s videoconferencing network.

To install the MXM Server

1. Insert the MXM Setup CD-ROM in your computer’s CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.
   Otherwise, click Start in the Windows taskbar and then click Run.
   Browse to the CD-ROM drive and double-click the Setup.exe file. The Installation program appears.
4. Follow the instructions in the Setup Wizard, clicking Next to continue.
   The installation program installs the Server components.

If upgrading from a previous MXM version, the Installation program detects it. Click OK to continue. The Installation program saves the previous version’s database settings, except for Call Details Records (CDRs) and the Event Log.

5. The Wizard asks where to install and use Microsoft SQL database. To install it on the same computer as the MXM (default setting), click Next.
   To install it on a different computer, click Choose Location and then enter the appropriate computer name or IP address.
   The installation program builds a system database, which requires a few minutes.
2.2 Installing the MXM Server

6. At another stage, the Enter Serial Number dialog box appears. Type the serial number that’s on the supplied key code agreement and click **OK**.

   If you received a version for evaluation, click **Cancel**. To continue installing the evaluation version (limited no. of users for a short period), click **Yes** to confirm.

   Whether this is a first-time installation or an upgrade, your initial key code is valid for 30 days. For instructions on making it permanent or increasing the permitted number of registered end points, see “Replacing the MXM License Key” on page 19.

7. When the Wizard informs that the installation is complete, click **Finish**.

8. To install the MXM Administrator application on the same computer, keep the Installation program open (see the next section).

   To exit the Installation program, click **Exit**.
2.3 Installing the MXM Administrator

The Administrator application may be installed on the same computer as the above applications and/or other workstations from which you may perform remote administration.

The new version of the MXM Administrator may be installed over a previous version of the application. You do not need to uninstall the previous version.

➤ To install the MXM Administrator

1. Insert the MXM Setup CD-ROM in your computer’s CD-ROM drive.
2. If Autorun is enabled, the Setup wizard will appear automatically.
   Otherwise, click Start in the Windows taskbar and then click Run. Browse to the CD-ROM drive and double-click the Setup.exe file. The Setup wizard appears.
3. Select MXM Administrator.
4. Follow the instructions in the wizard, clicking Next to continue.
5. The wizard provides a checkbox for installing the Falcon Upgrade Utility, which provides you with the ability to upgrade the software version of VCON Falcons connected to your organization’s network. If your organization has VCON Falcons, we recommend that you select to install this application.
   Click Next to continue.
6. If you selected to install the Falcon Upgrade Utility, the wizard proceeds to its installation process. Follow the instructions in the wizard, clicking Next to continue to the next page.
7. When the Wizard informs that the installation is complete, click Finish.
8. To exit the Installation program, click Exit.
2.4 Installing the VCON Conference Bridge

The VCON Conference Bridge (VCB) may be installed on the same computer as the MXM Server or a VCON MediaConnect 9000.

➤ To install the VCB

1. Insert the MXM Setup CD-ROM in your computer’s CD-ROM drive.
   
   If Autorun is enabled, the Setup wizard will appear automatically. Otherwise, click Start in the Windows taskbar and then click Run. Browse to the CD-ROM drive and double-click the Setup.exe file.

2. In the Setup window, select VCB.

3. Follow the instructions in the Setup wizard, clicking Next to continue.

4. At one stage, the wizard provides a choice between installing the VCB on the same computer as VCON’s MediaConnect 9000 or installing it on a computer that does not run a videoconferencing application.
   
   — To install it on MediaConnect 9000’s computer, select Yes. The computer must have two IP addresses to support this configuration. In the wizard, enter the IP address for the VCB (the other address is reserved for the MediaConnect 9000).
   
   — Otherwise, select No. Click Next.

5. At another stage, the wizard requires the address of the MXM Server with which the VCB registers and provides services. Enter the MXM Server’s IP address or DNS name. Click Next.

6. After completing the Setup wizard, restart the computer.

If the address of the associated MXM changed, if MXM is uninstalled and reinstalled, or if VCB will work on a different MXM:

In the Start Menu, point to Programs, VCON, VCB, and click Update MXM Address.
2.5 Installing the IPNexus Server

The IPNexus Server may be installed on the same server as the MXM, on its own Windows 2000 Server, in the DMZ, or on the public Internet.

1. The IPNexus is available only for organizations who purchased a license for the IPNexus Server option. If you want to add this option to your MXM, please contact your local VCON distributor.

2. For moderate to heavy data collaboration use, install the IPNexus Server on a dedicated FTP server.

➤ To install the IPNexus Server

1. Insert the MXM Setup CD-ROM in your computer’s CD-ROM drive.
   If Autorun is enabled, the Setup wizard will appear automatically. Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the **Setup.exe** file.

2. In the Setup window, select **IPNexus Server**.

3. Follow the instructions in the Setup wizard, clicking **Next** to continue.

4. At one stage, the wizard requests the address of the connected MXM.
   — If you’re installing the IPNexus Server on the same computer as the local MXM, keep the default setting, **localhost**.
   — Otherwise, type the IP address of another MXM on your network. Click **OK**.

5. After completing the Setup wizard, click **Finish**.
2.6 Installing the IPNexus Client

The IPNexus Client may be installed on any computer running Windows 95 or higher. For more specifications, see page 12.

The IPNexus is available only for organizations who purchased a license for the IPNexus Server option. If you want to add this option to your MXM, please contact your local VCON distributor.

➢ To install the IPNexus Client

1. Insert the MXM Setup CD-ROM in your computer’s CD-ROM drive.
   If Autorun is enabled, the Setup wizard will appear automatically. Otherwise, click Start in the Windows taskbar and then click Run. Browse to the CD-ROM drive and double-click the Setup.exe file.

2. In the Setup window, select IPNexus Client.

3. Follow the instructions in the Setup wizard, clicking Next to continue.

4. After completing the Setup wizard, click Finish.
2.7 Replacing the MXM License Key

The following circumstances require replacement of your MXM license key:

- Replacing a temporary demo version with a permanent, purchased version. Your initial key code is valid for 30 days.
- Changing the number of permitted registered end points.
- Adding optional features to your MXM.

This process requires that an initial MXM is already set up. For instructions on setting up an MXM, see Chapters 4 and 5.

To replace your MXM’s license key

1. In the Administrator window, right-click the MXM node at the top, point to Property (opening another menu), and click License.

2. In the Properties dialog box’s License tab, click Export Key to create a license file for the MXM on the host computer.

3. Send the license file to your local VCON distributor. You will then receive a new key code from the distributor.

4. Save the new license code file to a location on your network.
2.8 Running the MXM

5. After receiving a new license file from your VCON distributor, run the MXM Administrator application. Enter the MXM Properties License tab again.

6. Click New Key. The Open dialog box appears.

7. Browse to the location where you saved the license code file. Click Open.

8. When prompted to apply the license code, click OK.

9. To implement the license change and close the dialog box, click OK again.

2.8 Running the MXM

The MXM server opens automatically during the host computer’s startup, and runs unseen as an NT service.

➤ To run the MXM Administrator

☑ In the Windows desktop, click Start, point to Programs and click MXM Administrator.

Starting the MXM Administrator

When you open the MXM Administrator application for the first time, you must open a new MXM object in the Main View.
2.8 Running the MXM

➤ To open a new MXM

1. In the **MXM** menu, click **Log in to New MXM**.

2. Enter the IP network address of the computer that it’s installed on. Then, enter the default User name and default password during the startup. Afterwards, you may change these values to meet your own operating needs (see “Adding an Administrator” on page 33).

   **Default user**  su
   **Default password**  1234

3. Click **Login**. The new MXM is displayed in the Main View of the Administrator application. You can expand the MXM to see an initial system tree (see Chapter 3, “A Quick Tour of the MXM Administrator,” for more details).

4. To save the administrator application configuration, open the **File** menu and click **Save As**. Save the configuration as a **.vca** file.
2.9 Basic MXM Operations

This section will list the various tasks required to set up the MXM for a typical video network. At the end of each description, the location of detailed explanations are provided.

1. Set up administrators.

   Enter the administrators and their various privileges into the system. The available privilege levels are Super User, Monitor System and View System Properties. See “Setting Up Administrators” on page 33.

2. Set up the MXM’s configuration.

   Define the various properties of the system’s configuration, such as connection details, open or closed mode for registering end points, and so on. See Chapter 5, “Setting MXM System Properties.”

3. Define default settings for end points and other nodes in templates.

   A template includes the characteristic properties for a type of node or service. Any new created item in the system will initially have the default properties defined in the template. See “Setting Up Templates” on page 54.

4. Set up end point configurations.

   End points may be registered with the default properties defined in a template or be set following their login requests. See Chapter 6, “Defining End Point Nodes.”

5. Create and set up hunting groups.

   A hunting group includes a series of nodes that may be grouped together within an organization for a variety of reasons, but may be reached through one common address. See “Adding Hunting Groups” on page 57.

6. Create and set up administrative groups.

   Administrative Groups of nodes in the Main View can help maintain a visual structure for nodes and the teams and departments to which they belong. This also makes it easier to control end point properties that need to be common within a team or department, such as limiting the available bandwidth for the group. See “Adding an Administrative Group” on page 64.
7. Set up the MXM’s configuration in an Lightweight Directory Access Protocol (LDAP) online directory server.

By listing MXM registered users in an LDAP server, they will be able to locate and call all other users listed in the same directory. The MXM supports several LDAP server applications. See Chapter 10, “Registering with LDAP Directories.”

8. Prepare the MXM to provide gateway dialing services to ISDN connections for the registered end points.

If gateways register with the MXM, you must set their MXM configurations and their services’ configurations in the Administrator application. Then, you may define least-cost-gateway-dialing rules in order to reduce your organization’s call costs. See Chapter 7, “Registering Gateways” and Chapter 15, “Least Cost Routing of Gateway Calls.”

9. Set up the MXM configurations for Multipoint Control Units (MCU) that register with the MXM.

MCUs are used for connecting registered end points with a number of other end points in a multipoint videoconference. MCU services are available after the particular MCU is granted login permission to the MXM. See Chapter 8, “Registering an MCU.”

10. To enable the expansion of point-to-point IP videoconferences into ad-hoc multipoint videoconferences, set up MCU services for use in ad-hoc sessions.

If your organization has at least one VCON Conference Bridge (VCB) installed, set up the VCB services configurations. You can also control the use of ad-hoc session resources by creating ad-hoc service permission groups and associating end points to them. See Chapter 8, “Registering an MCU” and Chapter 12, “Setting Up Multipoint Videoconferences Managed by a VCB.”

11. If your organization has more than one network of videoconferencing users, set up the MXM configurations for additional zones managed by other MXMs or gatekeepers on your MXM Administrator application.

The configuration of additional zones enables end points registered in the local MXM to engage in videoconferences with end points in these other zones. You can set bandwidth allocation, enable inter-zone Call Details Records (CDR) generation, and other inter-zone videoconferencing management policies. See Chapter 9, “Neighboring Zones.”
12. Set up a videoconferencing software upgrade process that includes all or most of the end points registered to the MXM (available for VCON vPoint, VCB and the MXM Administrator application).

The software upgrade process enables you to place a new software version on a server location and then either schedule an upgrade time or run the upgrade program immediately for all the relevant end points. In this way, you can make sure that all end points (of specific models) in the organization are using the same and/or latest software. See Chapter 14, “Remote Upgrade of Videoconferencing Devices Software.”

13. If your organization employs NAT (Network Address Translation) networks and/or firewalls, but wants to permit videoconferencing within and outside its network, install and set up VCON’s SecureConnect system.

The ALG Proxies in your organization may be configured through the MXM Administrator. See Chapter 17, “Configuring ALG Proxy Servers.”
3 **A Quick Tour of the MXM Administrator**

Your work with the MXM takes place inside the Administrator application, which provides several elements and tools for performing the system management tasks.

In addition, the Administrator application provides various views and tables:

- **Main View**
  Displays a connected MXM and its registered nodes, hunting groups, and templates. From this window, you can view status, monitor activity, and configure properties of these registered users.

- **Node Status**
  Displays connection information about specific nodes that you want to monitor.

- **Login Status**
  Displays nodes that tried to register but were denied login - you can monitor registration and login procedures for nodes.

- **Event Log**
  Displays information about system events and operating conditions.

- **LDAP Servers**
  Displays information about the various online directories in which this MXM lists its registered nodes.

3.1 **The Main View**

Information about MXMs and their managed objects appears in the Main View. These include:

- Connected MXMs
- Administrators and their privileges
- Registered nodes and services, including user numbers and addresses, connection and call status
- Neighboring MXMs and Gatekeeper zones
- Software version indication for VCON vPoint end points and VCON Conference Bridge nodes.

In addition to displaying an MXM’s entire local and neighboring zones, viewing filters are available for showing smaller subsets of the registered nodes.
3.1 The Main View

The Administrator Application Main View

Connected MXMs

An Administrator may log in multiple MXMs. Each logged-in MXM is represented in the Main View by an entry that has an expandable system tree. When this tree is expanded, you can view nodes (such as VCON users, gateways, MCUs, and other administrators) that have logged in to that particular MXM. In addition, associated hunting groups, templates, and neighboring zones are shown in the system tree.

The system tree also shows units that tried to register but were not accepted automatically. In these cases, you have to grant login permission and set up the units’ MXM properties.

For each MXM, the Administrator application stores property information such as name/address, login settings, and various network settings (connection, timeouts, bandwidth management, etc.). For more information, see Chapter 5, “Setting MXM System Properties”.
Registered Nodes

The MXM supports the registration of VCON and other H.323 end points, administrators, gatekeepers, gateways, MCUs, gateway services and MCU services. In this Administrator’s Guide, registered nodes are also referred to as MXM nodes.

These nodes are visible when the system tree is expanded. For each of these items, the Administrator application stores property information such as name/address, bandwidth limits, online directory (LDAP) registration, and more.

*Falcon and MediaConnect 9000 with ISDN support*

These are represented in the Main View by icons ( for Falcon, for MediaConnect 9000) that display the status of the ISDN connections. Green indicates that the ISDN line is connected. Red indicates that the line is not connected.
3.1 The Main View

Displaying Call Status in the Main View

Neighboring MXMs and Gatekeeper Zones

If the local MXM is set to Open Mode for listing other MXMs and gatekeepers from the connected network, the MXM lists them in the Main View after it detects them. You can then set up the configurations for handling calls between each zone and the local MXM.

Nodes from a known neighboring zone may also be listed under their associated zone objects. In this way, neighboring nodes will be available for tasks such as call initiation and bandwidth management.

For more information about setting up and working with zones, see Chapter 9, “Neighboring Zones.”

Software Upgrade Indication

The MXM Administrator application provides the ability to update software for registered vPoint end points, Video Conference Bridge (VCB) end points, or the MXM Administrator itself.

After an upgrade operation has been set up, an icon next to the relevant nodes indicates if they require upgrade to the latest available version. After successful installation of the latest version, the icon disappears.
Filtering the Main View

You can control the amount of information that appears in the Main View by selecting filters according to the details that are important to you. You can set filtering according to the following criteria:

- Entire System
- Systems Not Logged In
- Systems Logged In
- Systems In Call
- Systems with an outdated (software) version

➤ To filter the main view

☐ In the Main View toolbar, open the Filter list and choose one of the options.
3.2 The Node Status View

The Node Status View makes it easier to see the connection information only about specific nodes instead of viewing the entire system tree. You can monitor the following:

- End points
- Administrator nodes
- Gateways and services
- MCUs and services
- Neighboring zones
- Gatekeeper
- LDAP proxy
- SIP proxy.

Right-click the Node Name of the entry to open a shortcut menu that contains commands that relate to the selected item.

<table>
<thead>
<tr>
<th>Node Description</th>
<th>Node Number</th>
<th>Status</th>
<th>Connection State</th>
<th>Direction</th>
<th>Bandwidth (kbps)</th>
<th>Audio Codec</th>
<th>Video Codec</th>
<th>T.120</th>
<th>MLP</th>
<th>HMLP</th>
<th>LSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>FalconDemo</td>
<td>1011</td>
<td>In Call</td>
<td>Outgoing</td>
<td>720</td>
<td>640</td>
<td>ON</td>
<td>ON</td>
<td>OFF</td>
<td>OFF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #1</td>
<td>50202705</td>
<td>Synchronized with 001512...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>OFF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #2</td>
<td>50202705</td>
<td>Synchronized with 001512...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>OFF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #3</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #4</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #5</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #6</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DavidScher</td>
<td>1002</td>
<td>Talking to 2205</td>
<td>20000</td>
<td>722.64k</td>
<td>H.264</td>
<td>OFF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC6000 - Teco...</td>
<td>2205</td>
<td>Talking to 1002</td>
<td>20000</td>
<td>722.64k</td>
<td>H.264</td>
<td>OFF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC6000DEMO</td>
<td>2802</td>
<td>Not Logged In</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Node Status Table

3.3 The Login Status View

The Login Status View lists nodes that tried to register, but were not given login and registration permission. This table makes it easier to monitor registration and login procedures for specific nodes instead of viewing the entire system tree.

<table>
<thead>
<tr>
<th>Login Category</th>
<th>Network Address</th>
<th>Alias</th>
<th>Login Name</th>
<th>Login Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>212.23.219.215</td>
<td>demo</td>
<td>demo</td>
<td>Login Permission Requested</td>
</tr>
<tr>
<td>Falcon IP</td>
<td>10.0.10.126</td>
<td>FalconTSCH</td>
<td>FalconTSCH</td>
<td>Login Permission Requested</td>
</tr>
</tbody>
</table>
3.4 The Event Log

The Event Log displays information about system events and operating conditions. You can refer to it for troubleshooting and isolating a problem.

The following illustration shows all the types of information (according to column) that the Event Log provides. If you want to display only a few important details, you can define filters that reduce the amount of displayed records according to various criteria.

3.5 LDAP Servers

The LDAP Servers View provides information about the MXM’s connection and registration in an LDAP (Lightweight Directory Access Protocol) online directory. The administrator may list the MXM and its registered nodes in any one of these online directories.
4 MANAGING THE MXM

This chapter provides instructions for organizing your MXM Administrator system so that you can manage your organization’s videoconferencing network. The tasks include:

- Setting Up Administrators
- Editing Nodes
- Status Monitoring
- Setting Up Templates
- Adding Hunting Groups
- Adding an Administrative Group
- Adding a Short Dial Number

4.1 Setting Up Administrators

Adding an Administrator

At any time, you can register additional administrators to the MXM. Each administrator must have an administration level (privileges) and a password.

In addition, you can change the privileges and other properties of the registered administrators at any time.

➤ To add an Administrator

1. Click the New Administrator button. The New Administrator Properties dialog box appears.

2. Type the Administrator’s Name. Click Next.
4.1 Setting Up Administrators

3. Enter the following privileges and security information:

**Administration Level**

- **Monitor System** - The Administrator may only observe the Main View and the Node Status View, and initiate videoconferences between known end points.

- **View System Properties** - The Administrator may only observe the Main View, the Node Status View, view other nodes’ properties, and initiate videoconferences between known end points.

- **Super User** - The Super User may change node and system configurations, in addition to the activities allowed for the other options.

**Change Password**

In the **New** box, type a new password for the new Administrator. In the **Confirm** box, type the new password again.
4. Click **Finish** to complete the setup. A new administrator appears in the Main View under the **Administrator** icon.

### Changing Administrator Properties

If necessary, you may change the properties of existing administrators.

➤ **To change an administrator node’s properties**

1. In the Main View, expand the Administrator group to view a list of Administrators.

2. Double-click an Administrator to open the Properties dialog box.

3. Change the appropriate properties. For a description of them, see “Adding an Administrator” on page 33.

4. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.
4.2 Editing Nodes

Adding Nodes

After a node connects to the MXM, it is added to the MXM’s database. The MXM may automatically accept the registration attempt, require manual registration by the administrator, or reject the attempt.

Granting Login Permission

To receive login requests, the MXM may be in Open Mode for certain types of nodes, and/or in Closed Mode for all other nodes.

**Open Mode**

- **VCON end points** allows automatic login to all VCON end points that register with the MXM (Escort, Cruiser 150/384, ViGO, MediaConnect 6000/8000, Falcon, VCON Conference Bridge).

- **Non-VCON end points** allows automatic login to any non-VCON H.323 videoconferencing end point that registers.

- **MCUs** allows automatic login to any MCU that registers.

- **Neighboring Gatekeepers (Zones)** allows the MXM to list any neighboring zones management device (MXM or gatekeeper) that contacts it (see Chapter 9, “Neighboring Zones.”).

- **SIP User Agents** allows automatic login to any SIP end point that registers.

**Closed Mode**

The administrator can manually grant login permission to nodes or reject them by ignoring their requests.

For nodes registering in Closed Mode (or nodes that cannot be registered automatically, such as gateways), a Login Request entry appears on the system tree in the Main View.

<table>
<thead>
<tr>
<th>Video Conferencing Item</th>
<th>Number/Address</th>
<th>Connection State</th>
</tr>
</thead>
<tbody>
<tr>
<td>telefon - su logged in</td>
<td>10.0.3.252</td>
<td>No Calls</td>
</tr>
<tr>
<td>Login Requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Matthew Duncan</td>
<td>10.0.1.123</td>
<td></td>
</tr>
</tbody>
</table>

*Login Request Indication*
4.2 Editing Nodes

➤ **To grant login permission**

1. Expand the Login Request item.

2. Right-click the item name and then click **Grant Login Permission**. A message appears, asking if you want to register the node now.

3. Click **OK** if you want to manually set the node’s properties, such as directory number or call forwarding. The Add Wizard appears (for definitions of the node properties, see “Setting End Point MXM Properties” on page 97). The original property values are the default values defined in the node type template (see “Setting Up Templates” on page 54).

   If you click **Cancel**, the node will not log in, but remains under the Login Requests object until you delete it (and the node stops trying to log in). See the next section, “Deleting a Login Request”.

4. Change properties according to your specifications, or keep the default settings. When you finish each page of the wizard, click **Next**.

5. When you finish the last page, click **Finish**.

   The node is registered. It appears as an entry in an appropriately labelled location of the system tree.

   If the registering node is a VCON Personal system (MeetingPoint 4.5 or higher) or vPoint system, the login process does not continue automatically after you click **Finish**. Instruct the node to log in again (user must click **Connect**) in order to complete the registration.
4.2 Editing Nodes

Deleting a Login Request

You may choose to reject any login requests that require you to grant permission manually.

➤ To delete a login request

☐ Right-click the Login Request item and then click Delete Login Request. Click Yes to confirm.

If the node continues trying to register, ask the user to try logging in to another gatekeeper or to operate stand-alone.

Setting a Node’s Properties

The MXM and all of its registered nodes have definable properties, or characteristics, which define their functionality and operation. Setting up and maintaining these properties is the key to efficient videoconferencing network management. At any time, an Administrator with Super User privileges can change properties of a registered node.

In addition, the videoconferencing configurations of vPoint, MeetingPoint 4.5 (and higher), and Falcon end points may also be edited. For vPoint end point configuration, see Appendix A, “vPoint™ End Point Properties.” For MeetingPoint end point configuration, see Appendix B, “MeetingPoint® End Point Properties.” For Falcon configuration, see Appendix C, “Falcon™ End Point Properties.”

➤ To set a node’s properties

1. In the Main View, browse the system tree until you find the node that you want to edit. If necessary, click a category’s plus sign to expand the tree and display additional items.

2. Right-click the node, point to Property, and then click the specific property type. The node’s Properties dialog box opens to the property type that you clicked.

   -or-

   Double-click the node. The node’s Properties dialog box opens to the General tab.
3. Change any appropriate properties.
   
   If you want to continue to another property group, click that group’s tab. In dialog boxes with many tabs, you may have to click the right or left arrow on the tab row to access all of them.

4. Click **OK** to implement all the changes and close the dialog box.

**Finding Nodes and Objects in the Administrator**

The Find and Find Next utilities help you search for specific items in the MXM Administrator. This feature is very useful if your enterprise’s network is large and not all nodes are visible in the Administrator application window.

**Find in Main View**

In the Main View, you can search for any words, phrases or numbers in all of the columns.

➤ **To find nodes and objects in the Main View**

   1. To search the whole system tree, click at the top of the Main View.

   2. Click the Find button. The Find dialog box appears.

   ![Find Dialog Box](image)

   **Find Dialog Box**

   3. In the **Find What** box, type a name and/or number.

   4. If necessary, define additional search parameters:

      **Match whole word only**

      Select this option to match only complete words or phrases. For example, if you enter **Gate**, the search ignores the word, “Gateway”.

      If you want to find characters that may be part of a longer word or part of a phrase, deselect this option.
4.2 Editing Nodes

**Match exact phrase**
Select this option to match only complete phrases. For example, if you enter *Gateway Hunting Group*, the search ignores any items including only the word, “Gateway”.

**Match case**
Select this option to match items whose capitalization is identical to the item in the **Find What** box. For example, if you enter *GW*, the search ignores any items that include “gw” or “Gw”.

To find all matching items, regardless of capitalization, deselect this option.

**Find backwards**
Select this option to search up the tree from the selected location. To select down the tree, deselect this option.

5. Click **Find Next**. The first matching item in the Main View is selected. To search for more matching items, click **Find Next** again.

*Finding an Item in the Main View*
Find in Other Views

In the MXM Administrator application’s other Views, you can search for the names of entries. The search covers the first column of the table.

➢ To find entries in other Views

1. Open the View in which you want to work.

2. Click the Find button. The Find dialog box appears.

3. In the Find What box, type the name of the entry.

4. If necessary, define additional search parameters:

   **Match case**
   Select this option to match items whose capitalization is identical to the item in the Find What box. For example, if you enter GW, the search ignores any items that include “gw” or “Gw”.

   To find all matching items, regardless of capitalization, deselect this option.

   **Direction**
   Select the direction from the selected entry to search in the View, Up or Down.

5. Click Find Next. The first matching entry in the View is selected. To search for more matching entries, click Find Next again.
4.2 Editing Nodes

Editing Multiple Nodes

You can select more than one node at the same time and define certain properties with identical values. If the selection of nodes contains more than one node type, only the common properties among them may be changed. Other properties will be unavailable.

➤ **To edit multiple nodes**

1. Select the nodes that you want to change, using the standard Windows object selection techniques:
   - To select consecutive nodes, click the first node, press <Shift> and click the last node in the series that you want.
   - To select non-consecutive nodes, click the first node, hold down <Ctrl> and click all the other nodes that you want.

2. Right-click one of the selected nodes, and then click **Properties**.
   The Properties dialog box appears. Only common properties among the selected nodes are available for change.

3. Change the appropriate properties. Remember that this change affects all the selected nodes.

4. Click **OK** to complete the change.

![Sample Properties Dialog Box - Multiple Nodes](image)
4.2 Editing Nodes

Changing Directory Numbers

All end points, services, hunting groups, and other registered items are assigned an internal directory number (also called E.164 number). Any registered node can call another registered item simply by dialing the destination’s directory number. This number is usually only a few digits, and can be adopted from the node’s IP address, telephone extension number, or randomly.

The administrator may change the directory numbers of one or a range of several registered nodes.

➤ To change the directory number of a single node

1. Double-click the node. The General tab of the node’s Properties dialog box appears.

2. In the Directory Number box, type the new number. Press OK.

➤ To change a range of directory numbers

1. In the Administrator window, find the nodes whose numbers you want to change. If necessary, click a category’s plus sign to expand the tree and display additional items.

Select the relevant nodes.

2. In the toolbar, click the Change Numbers button. The Change Number Range dialog box appears. The title bar shows the number of nodes in the selected range.

Changing Node Numbering

3. In the Start Numbering At box, type the new number for the start of the range.
4.3 Status Monitoring

4. Select **Ascending** for the numbering range to go up from the number that you typed (for example, 60, 61, 62, 63, ...). This new assignment affects the numbers for all other selected nodes.

Select **Descending** for the numbering range to go down from the number that you typed (for example, 63, 62, 61, 60, ...).

5. Click **Update** to implement the number change. On the Administrator tree, the new numbers for the selected nodes appear. From this point, a registered node must dial the new number to complete a call to the respective node.

Deleting a Node

If a node is not relevant to the network anymore, you can delete it from the MXM.

➤ **To delete a node**

☐ Click the node and then click the **Delete** button.

Click **Yes** to confirm.

4.3 Status Monitoring

The Administrator application provides a number of views for monitoring the operations of the MXM and its registered nodes:

- Main View
- Login Status View
- Node Status View
- Event Log.

Monitoring Nodes in the Main View

The Main View’s Connection State column (right side of table) provides status information about the current activity of registered nodes. This column may display nodes’ login status, or if nodes are currently in a videoconference and the amount of bandwidth being used.

<table>
<thead>
<tr>
<th>Icon</th>
<th>System Type</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Escort Systems</td>
<td>703</td>
<td>Logged In</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>VCON vPoint 5.1 Version Systems</td>
<td>704</td>
<td>In call: 2360 Kbps</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>VIGI Systems</td>
<td>706</td>
<td>In call: 2360 Kbps</td>
</tr>
</tbody>
</table>

**Indication of Nodes in a Videoconference**
4.3 Status Monitoring

Viewing the Login Status

Use the Login Status View to monitor registration and login procedures for nodes. The table lists nodes that tried to register, but were not given login and registration permission. This table makes it easier to see the login information only about specific nodes instead of viewing the entire system tree.

To open the Login Status table

- Click the Login Status View button.

<table>
<thead>
<tr>
<th>Login Category</th>
<th>Network Address</th>
<th>Alias</th>
<th>Login Name</th>
<th>Login Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>212.29.213.213</td>
<td>demo</td>
<td>demo</td>
<td>Login Permission Requested</td>
</tr>
<tr>
<td>Falcon P</td>
<td>10.0.10.125</td>
<td>FalconTECH</td>
<td>FalconTECH</td>
<td>Login Permission Requested</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Login Permission Granted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Login Permission Requested</td>
</tr>
</tbody>
</table>

Login Status View

The Login Status table provides the following information:

- **Login Category**: The type of node that tried to register.
- **Network Address**: Address of this node.
- **Alias**: Name of this node.
- **Login Name**: The node’s user name, as entered during the login procedure. If the node cannot provide a user name to the MXM, this space remains blank.
- **Login Status**: Describes what happened when the node last tried to log in to the MXM.

In the Login Status table, you can grant login permission by clicking the node’s Login Status column and then selecting Login Permission Granted (see the preceding figure). The node login process continues (see “Adding Nodes” on page 36).
4.3 Status Monitoring

Viewing the Node Status

The Node Status View makes it easier to see the connection information only about specific nodes instead of viewing the entire system tree. You can monitor the following:

- End points
- Gatekeeper
- Administrator nodes
- Gateways
- MCUs
- Neighboring Zones
- LDAP Proxy

To monitor nodes in the Node Status View

1. Click the **Node Status View** button. The Node Status View appears.
2. In the main Administrator window, select any number of nodes.
3. Drag the nodes into the Node Status View window. The information about the selected nodes appears in the table.

### Node Status Table

<table>
<thead>
<tr>
<th>Node Description</th>
<th>Node Number</th>
<th>Status</th>
<th>Connection Status</th>
<th>Direction</th>
<th>Bandwidth (kbps)</th>
<th>Audio Codec</th>
<th>Video Codec</th>
<th>T.400</th>
<th>MLP</th>
<th>H.323</th>
<th>LSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fxs1000</td>
<td>1011</td>
<td>In Call</td>
<td>Outgoing</td>
<td>525</td>
<td>G.722 16k</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #1 6500'250'</td>
<td>Synchronized with 001512</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #2 6500'250'</td>
<td>Synchronized with 001512</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #3</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #4</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #5</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line #6</td>
<td>Idle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ericsson 1002</td>
<td>Talking to 2006</td>
<td>2730</td>
<td>G.722 64k</td>
<td>M 301</td>
<td>Off</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEC5000 2001</td>
<td>Talking to 1002</td>
<td>2730</td>
<td>G.722 64k</td>
<td>M 301</td>
<td>Off</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEC5000D160</td>
<td>2002</td>
<td>Not Logged In</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.3 Status Monitoring

MXMs Displayed in Node Status Table

4. To go back to the Main Administrator View, click the Administrator tab at the bottom of the window.

Multiple Node Status Tables

You can make more than one Node Status Table to view different groups of nodes.

➤ To create a new Node Status table

1. At the bottom of the Node Status View, click the Add New Tab button.

2. Double-click the tab name.

3. Press the <Delete> key as many times as required until the default name is deleted.

4. Type a new tab name and press <Enter>.

➤ To delete a Node Status table

1. Click the tab of the table.

2. At the bottom of the Node Status View, click the Remove Tab button. The tab is deleted.
### Node Status Table Information

The Node Status View provides the following information:

| **MXM Name** | Name of the MXM in which the node is registered. Applicable if more than one MXM is connected. |
| **MXM Address** | IP address of the MXM in which the node is registered. Applicable if more than one MXM is connected. |
| **Node Name** | Name for the node - it may be the node’s alias or any other arbitrary name. |
| **Node Number** | MXM directory number of the node. |
| **Status** | Connection status as indicated by icon. |
| **Direction** | Applicable to ISDN calls. Indicates if the node initiated (Outgoing) or received the call (Incoming). |
| **Connection State** | Describes the current connection or activity status of the node. For example, this column may indicate that a node is currently in a videoconference. |
| **Bandwidth** | Amount of bandwidth that is consumed by the node during the current call. If the node (such as an MCU) is engaged in more than one session, both total and per-session bandwidths appear. |
| **Audio Codec** | If the node is in a call, this column indicates the audio transmission standard being used. |
| **Video Codec** | If the node is in a call, this column indicates the video transmission standard being used. |
| **T.120** | Data sharing specification that lets users share documents and applicants during an H.323 videoconference. |
| **MLP** | Multilayer Protocol. T.120 must use the MLP or HMLP channel for transmitting data. MLP data and audio can only be placed in the first 64 kbps channel of a connection. |
Event Log Monitoring

The Event Log displays information about system events and operating conditions. You can view all network events during a time period, events involving a specific node, specific types of events, events of a certain severity level, and more. Refer to it if you need to troubleshoot and to isolate a problem.

➢ To view the Event Log for the MXM

1. Click the Event Log button.

2. To see events that occurred before those in the table, click the Prior Events button.

To see events that occurred after those in the table, click the Next Events button.

To update the table and display new events, click the Refresh button.

➢ To view the Event Log for a specific node

1. Right-click the node and then click View Events.

2. The Event Log opens for the specific node only.
4.3 Status Monitoring

Changing Record-Keeping Periods

From the Event Log View, you can change the periods of time that the MXM keeps records of specific types of events.

➤ To change the record-keeping period

1. In the Event Log View, click the Event Log Settings button. The MXM’s Event Log properties tab appears.

2. Change the appropriate record-keeping periods (see “Event Log” on page 94).

Event Log Information

The Event Log provides the following information:

- **Handled**: Indication if the event no longer needs administrator attention.
- **Name**: Name of the node associated with the event.
- **Severity**: Classification of the type of event that occurred. This can determine the level of attention that’s required from the administrator.
- **Date/Time**: Date and time that the event occurred.
- **Application Type**: Type of node or group in which the event occurred.
- **Network Address**: IP address of the node or group shown in the Application Type column.
- **Error Code**: Indication of the type of error or event.
- **Details**: Description of the event.
Filtering the Event Log

You can control the level of information that appears in the Event Log by defining filters according to the details that are important to you. You can set filtering according to all or any combination of the following criteria:

- Severity level
- Application (node type)
- Handled/unhandled events
- Number of displayed records
- Date and time
- IP Address range
- Error code
- Event description.
4.3 Status Monitoring

➤ To set Event Log view filters

1. In the Event Log, click the Filter button. The Filter Records dialog box appears.

2. Define the particular filters according to the specific criteria that you require for reducing the possible accounts that you want to check (for definitions of the categories, see “Filtering Criteria” on page 53).

3. Click OK.

➤ To save a filter for future use

1. In the Event Log, click Create New.

2. In the Create New Filter dialog box, type a name for the new filter scheme.

3. Click OK.

Saving a Filter Scheme

The scheme name now appears in the Scheme list.

To delete a scheme, select it from the Scheme list and click Delete.
Filtering Criteria

This section provides explanations for the various Event Log filtering categories (for definitions of the categories, see “Event Log Information” on page 50):

- **Severity**: Set the log to display only certain types of events which affect the network’s functioning.

- **Application Type**: Set the log to display only events that occur in specific types of nodes.

- **Show Handled Events**: Show events that are defined as handled (or fixed) or unhandled or both. This category helps you indicate if events no longer need administrator attention.

- **Query Size**: Set the log to display a maximum number of records on the screen. If the log contains more than this number of records, you can click **Prior Events** and/or **Next Events** to display them.

- **Time**: Set the log to display only records within a specific time range. Select one of the following options:

  - Any time
  - Up to 60 days before the current day
  - A time range according to the following criteria:

    - **After**, **Before**, **Between**, **On or after**, **On or before** a specific date and time.

If you select **Between**, you have to set an earliest and latest time limit.

Setting a Time Range Filter
**4.4 Setting Up Templates**

**Time (cont.)**

To specify the time limit, click the large down arrow to open a calendar in which you can browse and choose an exact date and year.

In addition, you can select one-by-one the date, month, year, hour, minute, and/or AM/PM. Then, click the small up or down arrows until the value that you want appears.

**Application Network Address**

Filters the event log to display events only from nodes whose IP addresses meet the criterion defined here.

In the adjacent box, type the address range that fits the phrase selected from the list.

For example, clicking **Begins with** and then typing **100.100.100.** will display records for accounts whose IP address is in the range greater than 100.100.100.0.

**Error Code**

Indicates the type of error or event that occurred.

**Description**

Set the log to display only records whose Details contains, does not contain, ends or begins with (and other criteria) a specific text string.

---

**4.4 Setting Up Templates**

When you manually grant permission to a new node to register, or if you add a new service, you have to confirm or change the item’s properties before the item is added to the MXM’s tree and database. The original default properties were set at VCON’s production facility.

An administrator with Super User privileges may change various default properties by setting up a template. A template includes the characteristic properties for a type of node or service. Any newly created item in the system will initially have the default properties defined in the template.

Any changes to a template only affect new nodes that you create afterwards - they do not affect existing nodes.
4.4 Setting Up Templates

**Editing a Template**

Templates are provided for the following items. For explanations about a template’s properties, see the referred section.

- Accord Gateway — See pages 405 to 409.
- Accord Meeting Room — See pages 400 to 403.
- Ad-hoc Permission Group — See pages 142 to 145.
- ALG Proxy Server — See pages 302 to 310.
- Desktop systems — See pages 97 to 111 and App. B.
- Falcon — See pages 97 to 111 and App. C.
- Gateway — See pages 116 to 122.
- Gateway Service — See pages 123 to 124.
- Gateway Service Hunting Group — See page 125 to 126.
- H.323 (non-VCON) End Point — See pages 97 to 111.
- Hunting Group — See pages 57 to 63.
- MCU — See pages 129 to 132.
- MCU Permission Group — See pages 138 to 140.
- MCU Service — See pages 133 to 137.
- MediaConnect 6000 — See pages 97 to 111.
- Permanent Non-registered Device — See pages 97 to 111.
- Short Dial — See pages 66 to 67.
- SIP User Agent — See pages 97 to 111.
- VCB Service — See pages 232 to 240.
- VCON Conference Bridge — See pages 227 to 231.
- vPoint systems — See pages 97 to 111 and App. A
- Zones (neighboring) — See pages 150 to 163.
4.4 Setting Up Templates

To edit a template

1. In the Main view, expand the Templates group to display all available templates.

2. Right-click a template, and then click Properties.

   The Properties dialog box appears.

3. Change the appropriate properties (see the list on the previous page for the locations of the relevant properties explanations). If applicable, click on other tabs in the dialog box to change more properties.

4. Click OK to complete the change. If you want to discard the change, click Cancel.
4.5 Adding Hunting Groups

A hunting group includes a series of nodes that may be grouped together within an organization for a variety of reasons, but may be reached through one common number. When the common number is dialed, the MXM searches for a free node.

For example, if the first node is busy, the system tries to contact the next node, and so on. If all nodes are engaged, the MXM rejects the call.

The most important characteristic of a hunting group is the order in which calls are routed to members of the group. When you create a hunting group, you can determine the “hunting” order and method (see “Hunting Group Properties” on page 60).

Gateway Service hunting groups operate under a similar principle. You can set the order in which gateway services are requested when the hunting group’s access number is dialed (see “Gateway Service Hunting Groups” on page 125).

➢ To create a hunting group


2. Change properties according to your hunting group requirements. To move to the next properties page, click Next. For explanations about the various properties, see pages 58 to 63.

3. Click Finish. In the Main View, the new hunting group appears under the Hunting Group object.
General Properties

The **General** page appears when you open the Hunting Group wizard. It contains identity information about the hunting group.

**Hunting Group - General Properties**

Set the following **General** Properties:

- **Directory Number**: The number to be dialed in order to call this hunting group.
- **Description**: Description or name for the group. This name appears in the Main View under the Hunting Groups object.
Call Forwarding Properties

In the Hunting Group Properties **Call Forwarding** page, set an alternate destination for the MXM to route calls.

**Hunting Group - Call Forwarding Properties**

*No Response*

**When this group is not responding, dial this number**

Set an alternate destination for a call if none of the group members answers after a specified time. From the list, select the alternate destination.
4.5 Adding Hunting Groups

Hunting Group Properties

In the Hunting Group Properties page, you can set the default hunting method, place specific nodes in the hunting group, and set the preferred order of hunting.

Hunting Group Properties

Set hunting group properties as follows:

**Calling Rule**

- **Default “hunting” method**
- **Least Recently Called** - Calls are routed first to the node which has not received a call in the longest time.
- **Circular** - Calls are routed first to the node in the hunting group list that follows the last node that was called.
- **Fixed Order** - The search starts at the first node in the hunting group list, then the second node, third node, and so on, until a free node is found.
- **Simultaneous** - Simultaneous calls go to every member of the hunting group. Upon the first acceptance of a call, all the other calls disconnect.
4.5 Adding Hunting Groups

<table>
<thead>
<tr>
<th>Description/Number</th>
<th>Select the nodes that will belong to this hunting group.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>— To place all nodes in the hunting group, click <strong>Select All</strong>.</td>
</tr>
<tr>
<td></td>
<td>— To clear all the selections, click <strong>Clear All</strong>.</td>
</tr>
</tbody>
</table>

**Setting the Hunting Order**

In the New Hunting Group Properties dialog box, selected nodes are automatically placed in the top part of the list. You can then move them to different places in the hunting order. Their locations in the list, together with the Calling Rules setting, determines the hunting order.

➤ **To set the hunting order of the selected nodes**

1. Click the name *(not the checkbox)* of a selected node. To move the node up and down the list to its designated place, click **Move Up** or **Move Down** as many times as necessary.
   
   Repeat this step for as many nodes as necessary.

2. Click **OK** to implement the settings and close the dialog box.
4.5 Adding Hunting Groups

Hunting Group LDAP Properties

In the LDAP page, you can define the hunting group’s registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server.

List node in the following LDAP servers

Select LDAP servers that can contain the subdirectory in which the hunting group should be listed. Hunting groups may be registered in all LDAP servers in which the MXM is registered.

If the hunting group has been previously registered in an LDAP server, its entry name or number (node entry) appears in the list.

— To be listed in all LDAP servers (depending on MXM registration in them), click Select All.
— To clear all the selections, click Clear All.

Open the LDAP Servers View to see all LDAP server details.

Hunting Group - LDAP Properties
4.5 Adding Hunting Groups

Additional ID Properties

In addition to its directory (E.164) number, a hunting group may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 ID. In the Additional ID page, you may enter these, if applicable. For example, the Description entered in the General page will appear as an Additional ID as an H.323 ID.

For more information about adding Additional IDs, see “Additional IDs” on page 111.
4.6 Adding an Administrative Group

You can create Administrative Groups of nodes that reflect the needs of the enterprise’s organization. Administrative groups in the Main View can help maintain a visual structure for nodes and the teams and departments to which they belong. This also makes it easier to set common end point properties within a team or department, such as limiting the available bandwidth for the group.

For example, you can create groups for Management, Sales, Finance, R&D, or others and place end points accordingly.

➤ To create an administrative group

1. Click the **New Administrative Group** button. The New Group wizard appears.

   ![New Administrative Group Properties](image)

   **New Administrative Group Properties**

2. In the **Description** box, type a name for the group and click **Finish**. This name will appear on the system tree.

3. To create more groups, repeat steps 1 and 2.

4. To see the created groups in the Main View, expand the Groups object.
You can also add administrative subgroups as branches under other created groups. To do this, select an existing administrative group before clicking the Add Administrative Group button.

➢ To place nodes into an administrative group

1. In the Main View, select one or more nodes.
2. Drag the nodes to the administrative group.

<table>
<thead>
<tr>
<th>Video Conferencing Item</th>
<th>Number/Address</th>
<th>Connection State</th>
</tr>
</thead>
<tbody>
<tr>
<td>techxm - su logged in</td>
<td>10.0.10.96</td>
<td>No Calls</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R&amp;D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charlie Brown</td>
<td>701</td>
<td>Logged In</td>
</tr>
<tr>
<td>Sharon Green</td>
<td>704</td>
<td>Logged In</td>
</tr>
<tr>
<td>Matthew Duncan</td>
<td>702</td>
<td>Logged In</td>
</tr>
<tr>
<td>David Schar</td>
<td>700</td>
<td>Logged In</td>
</tr>
</tbody>
</table>

Sample Administrative Group

Changing Group Member Properties

Administrative groups make it easier to control end point properties that need to be common within a team or department, such as limiting the available bandwidth for the members of a group.

➢ To change common properties for all group members

1. Right-click the group name, point to Member Property, and click the specific property type.

   A Properties dialog box for all group members opens to the property type that you clicked. Common properties among the group members are available for change.

2. Change the appropriate properties. Remember that this change affects all the group members.

3. Click OK to complete the change. If you want to discard the change, click Cancel.
4.7 Adding a Short Dial Number

A Short Dial Number is a number, that when dialed, is routed to another specific registered user. It ideally is used as an easy-to-remember number intended to reach a department or a location instead of a specific person. It can also be used to include ISDN entries in the network and online directories (LDAP).

For example, you can set up a Short Dial Number, “444”, that reaches a sales representative whose personal directory number is “4792”. All calls dialed to “444” would automatically be forwarded to “4792”.

➤ To add a Short Dial number

1. In the Main View’s toolbar, click the New Short Dial button. The New Short Dial Wizard appears.

2. Change properties according to your short dial requirements. To move to the next properties page, click Next. For explanations about the various properties, see the following subsections.

3. Click Finish. In the Main View, the new Short Dial entry appears under the Short Dial Numbers object.

General Properties

The General page appears when you open the New Short Dial wizard. It contains identity information about the entry.

![Short Dial - General Properties](image)
4.7 Adding a Short Dial Number

Set the following **General** Properties:

- **Directory Number**
  The number to be dialed in order to call the user that this entry represents.

- **Description**
  Description or name for the entry. This name appears in the Main View under the Short Dial Numbers object.

**Call Forwarding Properties**

In the **Call Forwarding** tab, select the user who will receive any videoconference calls dialed to the Short Dial number.

**LDAP Properties**

The **LDAP** tab provides information about the Short Dial number’s registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes’ LDAP Properties, see “LDAP” on page 109.

**Additional ID Properties**

In addition to its directory (E.164) number, a Short Dial number may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see “Additional IDs” on page 111.
5 Setting MXM System Properties

MXM servers have system properties that define their operation. In the MXM Properties dialog box, the properties are divided into various categories:

- **MXM**
  - Connection, System Information, Dial Plan, LDAP Settings
  - See page 70.

- **Call Control**
  - System Bandwidth Control, Call Settings, Ad-hoc Resources
  - See page 78.

- **ISDN Call Routing**
  - System Location, Dialing Prefixes
  - See page 82.

- **Security**
  - Security Mode, License, Non-registered Devices
  - See page 85.

- **H.323 & SIP**
  - Zone Settings, Advanced Settings
  - See page 90.

- **Reporting**
  - Billing, Event Log
  - See page 93.

➤ To define MXM Server system properties

1. In the Administrator window, right-click the MXM node at the top, point to **Property** (opening another menu), and click the specific property type.

   -or-

   Click the MXM node and then click the **Display Properties** button.

2. In the Properties dialog box, change properties according to the system’s specifications. To set different types of system properties, click the appropriate category icon on the left side of the dialog box, and then click the tab at the top of the dialog box. For explanations about the various properties, see the above list for their locations.

3. To implement the change and proceed to another set of MXM properties, click **Apply** and then the appropriate category icon and tab.

4. To implement all the changes and close the dialog box, click **OK**.
5.1 MXM Properties

In the MXM system Properties dialog box, click the MXM icon to access the following property pages:

- Connection
- System Info
- Dial Plan
- LDAP Settings

Connection

The Connection tab contains information about the MXM Administrator application’s connection to the MXM.

![MXM Connection Properties](image-url)
Set the connection properties as follows:

**Automatically Connect at Administrator Startup**
Select this option if you want to connect to this MXM automatically whenever you start the Administrator application.

**MXM Address**
IP address or DNS name of the MXM.

**Port**
TCP/IP port number. Automatically provided by the system.

**Connection State**
Informs you if the MXM Administrator application is connected and available for management, trying to connect, or not trying to connect to the MXM.

**Login**
Provides information about the current login state:

- **User**
The administrator name.

- **Level**
Level of administration privileges permitted to the User.

- **Status**
Current state of the login attempt.

Clicking **Advanced** displays the following properties:

**Network Connection**

**Check if MXM is online**
Select if you want the Administrator application to periodically check that the MXM is still connected, when there is no traffic over the connection.

Next to that property, select the number of seconds between checks if there is no activity over the connection.

**Message Acknowledge Timeout**
Select the number of seconds that the Administrator application waits to receive an update response from the MXM. After this interval, a message states that the MXM did not respond.
System Info

The System Info tab provides information about the installation of the current MXM version. Provide this information if you contact VCON’s Technical Support.

**System Name**
The identifying name for the MXM. This name does not affect the operation of the system.

**Build Number**
The number and date of the MXM software version.

**MXM Running Since**
Date and time when the MXM started operating.
Dial Plan

In the **Dial Plan** tab, define how the MXM assigns directory numbers (E.164-type) to registered end points and other nodes. Entering directory numbers are a convenient way for registered users to dial other nodes.

This tab also includes the names of the supplemental exchange functions and the default Telephony User Interface (TUI) numbers that the end point may dial to activate each of them. You may change the number for any of the functions.

For more information about how end points use exchange functions, see the MXM’s Online Help’s *Telephony Exchange Functions* topics.
Set directory numbering as following:

**Node numbering (E.164) starts at**

This number is the starting point for assigning directory numbers to registering nodes. You can provide for two, three, four, etc. digits for numbering nodes.

For example, if this number is “700”, new nodes will receive the first 3-digit number available between 700 and 999. To increase the numbering capacity (according to the license key code’s specification), you can specify a larger 3-digit range or add a fourth digit.

**End Points’ E.164 Numbering Request**

- **If not used, accept requested number**
  - Select to grant any E.164 number requests, if available, by registering end points.
  - If deselected, the MXM assigns directory numbers only according to the Node numbering definition above, and rejects all user E.164 numbering requests.

- **If already used**
  - **Assign new number**
    - Select to accept the login request, but to assign a directory number according to the Node numbering definition above.
  - **Reject login request**
    - Select to reject the login request if the specified E.164 number is already assigned to another node.

The Exchange Functions table lists the available functions and their corresponding TUI numbers.

**To change the TUI number of an exchange function**

- Click in the **Number** column of the entry that you want to change.
  - Delete the previous number and type a new number.
  - To replace other numbers, repeat this step as many times as necessary.

vPoint provides access to call pickup, forwarding and transfer functions from its manual dialer and shortcut panel.

MeetingPoint 4.5 and 4.6 provides similar access from its Conference Panel.
The available functions are:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gateway Service</strong></td>
<td>For starting an ISDN videoconference over a gateway. The end point must enter this number, followed by the ISDN channel numbers, and then click Dial.</td>
<td>9</td>
</tr>
<tr>
<td><strong>Pickup</strong></td>
<td>For picking up a call that’s intended for any destination for which the end point has pickup permission. The end point enters this number and then clicks Dial.</td>
<td>*17</td>
</tr>
<tr>
<td><strong>Specific Pickup</strong></td>
<td>For picking up a call that's intended for a specific destination (for which the end point has pickup permission). The end point enters this number, followed by the directory number of the destination end point, and then clicks Dial.</td>
<td>*19</td>
</tr>
<tr>
<td><strong>TUI Busy Forward</strong></td>
<td>If the end point is busy in a videoconference, the MXM forwards all incoming calls for it to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks Dial.</td>
<td>*71</td>
</tr>
<tr>
<td><strong>TUI No Answer Forward</strong></td>
<td>If the end point does not answer, the MXM forwards a call to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks Dial.</td>
<td>*70</td>
</tr>
<tr>
<td><strong>TUI Unconditional Forward</strong></td>
<td>The MXM forwards ALL calls intended for the end point to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks Dial.</td>
<td>*72</td>
</tr>
</tbody>
</table>
### 5.1 MXM Properties

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ad-hoc Conference</strong></td>
<td>For inviting additional users to an open point-to-point videoconference. The end point enters this number, followed by the directory number of the target end point, and then clicks <strong>Dial</strong>.</td>
<td><em>77</em></td>
</tr>
<tr>
<td><strong>Transfer</strong></td>
<td>For transferring an open videoconference to another end point (and disconnecting from the transferring end point). The transferring end point enters this number, followed by the directory number of the target end point, and then clicks <strong>Dial</strong>.</td>
<td><em>45</em></td>
</tr>
</tbody>
</table>
5.1 MXM Properties

LDAP Settings

In the **LDAP Settings** tab, enable the MXM to periodically update its registered users in connected LDAP (Lightweight Directory Access Protocol) online directories. For more information about LDAP, see Chapter 10, “Registering with LDAP Directories.”

**LDAP Settings Properties**

Set LDAP Settings as follows:

- **Enable Update of LDAP Servers**
  - Select to enable the MXM to update its registered users information in the LDAP directories.

- **Prefix E.164 numbers with local zone number**
  - If neighboring zones are included in your online directories, select this option to append zone numbers to the directory numbers of all listed nodes.

**Proxy Pending Messages**

If no communication was received from the LDAP directory after a certain interval, the MXM asks the LDAP Proxy server if its directory list (for the MXM registered users) requires updating.

- **Trigger Time**
  - Enter the interval between update request messages sent by the MXM to the LDAP Proxy server.
5.2 Call Control Properties

Time to Live
Enter the interval for discarding an update request message that is not received by the LDAP Proxy server.

LDAP Servers View
For information about the available LDAP servers, click this link. The LDAP Servers table appears, displaying location and access information about the available servers.

If you update the MXM’s LDAP settings, you must also update the same configuration settings in the LDAP server (see Chapter 10, “Registering with LDAP Directories”).

5.2 Call Control Properties

In the MXM system Properties dialog box, click the Call Control icon to access the following property pages:

- Bandwidth Control
- Call Settings
- Ad-hoc Resources
Bandwidth Control

In the Bandwidth Control tab, define how the MXM manages the available bandwidth within its zone.

Local MXM’s Bandwidth Control Properties

Set bandwidth control properties as follows:

- **Network Bandwidth**
  - Total amount of bandwidth available to the LAN.

- **Limit total bandwidth of MXM calls**
  - Select to define the percentage of total network bandwidth to be allocated for calls managed by the MXM.

- **Limit maximum number of calls to**
  - Select to define the maximum number of videoconferences managed by this MXM, that can carry on at the same time. The amount of open videoconferences cannot exceed the bandwidth limit defined above.
5.2 Call Control Properties

Call Settings

The **Call Settings** tab includes properties defining call connection throughout the videoconferencing network.

### Call Settings Properties

Set Call Settings properties as follows:

**Ad-hoc Conference**

**Revert to point-to-point call when 2 parties remain**

Select to return to a point-to-point call when only two parties remain in an ad-hoc videoconference.

**Wait __ seconds before reverting to point-to-point**

After a third party disconnects, the videoconference will revert to a point-to-point session after this interval.

**Maximum Call Redirections**

**___ redirections**

Select the maximum number of times that a call can be forwarded sequentially to other nodes before the call is cancelled.

**Unlimited**

Select to allow calls to be forwarded to as many destinations as necessary until they are answered.
Ad-hoc Resources

The Ad-hoc Resources table contains a list of MCU and VCB services registered with the MXM, together with the MCU or VCB with which they are associated. Select the services that the MXM may use to initiate an ad-hoc videoconference.

Available Ad-hoc Resources
5.3 ISDN Call Routing Properties

In the MXM system Properties dialog box, click the ISDN Call Routing icon to access the following property pages:

- System Location
- Dialing Prefixes

System Location

In the System Location tab, enter the country and area code in which the local MXM is located. This information is used when the MXM computes ISDN and gateway call rates.

Local MXM Location
Dialing Prefixes

In the **Dialing Prefixes** tab, enter the prefixes which are required for dialing international and long-distance videoconferencing calls. If the call requires routing through a gateway, the MXM uses this information when it determines the optimum gateway and service (see “Testing for the Optimal Gateway Service” on page 290).

For example, international calls may require that you add a prefix such as 00 or 1 before dialing a country code. This number is provided by the local telephone company or other ISDN provider.

Long distance calls within a country also may require a prefix such as 0 or 1 before the remainder of the ISDN number.

![Gateway Dialing Prefixes for Local MXM Network](image)

**To add prefixes**

1. Click the New Prefix button.
2. Type the prefix and press <Enter>.
3. To add more prefixes, repeat steps 1 and 2 as many times as required.
4. Click **Apply** to implement the settings while remaining in the dialog box.
   -or-
   Click **OK** to implement the settings and close the dialog box.
5.3 ISDN Call Routing Properties

➤ To delete prefixes

1. Select the prefix that you want to delete.

2. Click the Delete button.

3. Click Apply to implement the settings while remaining in the dialog box.
   -or-
   Click OK to implement the settings and close the dialog box.
5.4 Security Properties

In the MXM system Properties dialog box, click the Security icon to access the following property pages:

- Security Mode
- License
- Non-Registered Devices

Security Mode

In the Security Mode tab, set the properties for restricting login to specific users. You can set up the MXM in any or all of the available Open Modes, or in Closed Mode to all nodes.
5.4 Security Properties

Set the security mode as follows:

*System Security Mode*

**Open Mode**
- Select to allow automatic login privileges to various types of nodes, which are listed below this option. A deselected type must be manually granted or refused login permission by the administrator.

**VCON end points**
- Select to automatically accept VCON systems that register (Escort, Cruiser 150/384, ViGO, MediaConnect 6000/8000, Falcon, VCON Conference Bridge).

**Non-VCON end points**
- Select to automatically log in any non-VCON H.323 videoconferencing node that registers.

**MCUs**
- Select to automatically log in any MCU that registers.

**Neighboring Gatekeepers (Zones)**
- Select to automatically list other MXMs and Gatekeepers that the local MXM calls or that contact it. In addition, this selection enables registered MXM nodes to receive calls from other zones. These zones appear automatically in the Main View.

**SIP User Agents**
- Select to automatically log in any SIP user agent that registers.

**Closed Mode**
- Select to restrict login privileges. All nodes that attempt to register must be granted login permission manually or rejected by the administrator.

**Login Status View**
- Click this link to display the Login Status Table. The far right column of the table shows the login status for specified nodes. For more details about the Login Status Table, see “Viewing the Login Status” on page 45.

**Allow versions that are not registered via the software upgrade to log in**
- Select this option to grant registration and login to nodes that are using a videoconferencing application version not defined in a Software Upgrade task (see “Selecting a Software Version” on page 270).

If this option is deselected, the MXM refuses to grant login to these nodes until their software matches a Software Upgrade task.
5.4 Security Properties

License

The **License** tab shows the number of registered users that the MXM is licensed to service. If you need to increase these numbers, contact your local VCON distributor.

![License Properties](image)

**License Properties**

- **Serial Number**: The license number of your MXM system.
- **Capacity**
  - **Number of Users**: Actual and maximum numbers, respectively, of non-vPoint Software-only end points that this MXM is permitted to register, according to its current license.
  - **Number of Logged On Users**: Actual and maximum numbers, respectively, of non-vPoint software-only end points that are logged in at the current time.
  - **Number of Concurrent Calls**: Actual and maximum numbers, respectively, of registered nodes that can be engaged in calls at one time.
  - **Number of vPoint Seats**: Actual and maximum numbers, respectively, of vPoint software-only end points that this MXM is permitted to register, according to its current license.
5.4 Security Properties

Expiration Date  Depending on your license, this will be either Never or the date that your MXM license expires. If your license is temporary, see “Replacing the MXM License Key” on page 19 for information about updating your license.

VCON Conference Bridge

Max. Number of VCB Conferences  The number of simultaneous ad-hoc videoconferences managed by the VCB allowed.

Expiration Date  Depending on your license, this will be either Never or the date that this license expires.

IP-Nexus Server

Option Installed  Indicates if your MXM includes the IP-Nexus Server option, which provides instant messaging, application sharing, file transfer, and other services to users who register with the IP-Nexus Server.

Expiration Date  Depending on your license, this will be either Never or the date that this license expires.

Max. Number of Concurrent Users  The maximum number of users that can be logged in at one time.

License Key

Export Key  Your initial key code is valid for 30 days. To purchase a license for more ports, click Export Key to create a license file for the MXM on its host computer. Send the file to your local VCON distributor. You will then receive the appropriate key without time restrictions.

Show Key  Click to view the key code for the current MXM Server installation.

New Key  After receiving a new license file from your VCON distributor, click this button, browse to select the file and click Open.
When prompted to apply the license code, click OK.
To implement the license change and close the dialog box, click OK again.
Non-Registered Devices

In the Non-Registered Devices tab, define how the MXM allows registered end points to engage in videoconferences with nodes that are unable to register with the MXM.

**Non-Registered End Point Settings**

Set the properties as follows:

- **Maximum Number of Concurrent Calls with Non-registered Devices**: Maximum number of simultaneous calls involving non-registered end points that the MXM may handle.

- **Total Network Bandwidth Allowed for Calls with Non-registered Devices**: Select the limit on the amount of bandwidth (in Kbps) that may be allocated to these videoconferences. The value must be a multiple of 100 (such as 200, 5000, 999000).
5.5 H.323 & SIP Properties

In the MXM system Properties dialog box, click the H.323 & SIP icon to access the following property pages:

- Zone Settings
- Advanced Settings

Zone Settings

In the **Zone Settings** tab, define the method of search that the MXM uses when a registered end point dials a party in a different zone (*neighbor node*).

**MXM Gatekeeper Zone Settings**

**Search Policy**

**If a dialed address is not found**, the MXM will continue (or not) to search for that address according to one of the following policies:

- **Don’t search in other zones**  The MXM will reject the call without searching in other zones.
### Search other zones

If the dialed address is unknown to the local MXM, the MXM will send out Location Requests (LRQs) to other MXMs and gatekeepers, according to the policy defined here.

<table>
<thead>
<tr>
<th><strong>First Try/Then Try</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First Try</strong></td>
<td>In the <strong>First Try</strong> list, select the search method that the local MXM employs first.</td>
</tr>
<tr>
<td><strong>Then Try</strong></td>
<td>In the first and second <strong>Then Try</strong> lists, select alternative search methods in case the first method fails to find the dialed node.</td>
</tr>
</tbody>
</table>

| **Send Multicast Location Requests** | The MXM sends out identical LRQs to all detected zones. The call is connected to the first zone that sends a positive response (party found) to the MXM. |
| **Defined Neighbor Zones**         | The MXM only sends LRQs to zones that are listed in the MXM Administrator, or “known” to the MXM. The call is connected to the first zone that sends a positive response (party found) to the MXM. |

| **Directory Gatekeepers** | The MXM sends LRQs only to directory gatekeepers known to it. |
| **Don't Try Anymore**      | At this stage, the MXM stops sending LRQs. |

| **Search for disconnected nodes in other zones** | If a call is dialed to an MXM node that is currently not logged in, the MXM continues to search for that node in other known zones. |

| **Location Request Reply Timeout** | Select the maximum interval for the MXM to receive a reply from the dialed destination's gatekeeper. If this interval passes before the MXM receives this reply, the call is disconnected. |
5.5 H.323 & SIP Properties

Advanced Settings

In the **Advanced Settings** tab, set the intervals at which the MXM activates various timeouts.

![MXM Gatekeeper Advanced Settings](image)

**Set Capabilities Timeout**
Select the maximum interval for registered end points to receive the H.323 capabilities of the dialed destination. If this interval passes before the end point receives this information, the MXM disconnects the call.

**Close Channel Timeout**
Select the maximum time for H.323 logical channels to close when a videoconference ends.

**Collect OLCs Regular Timeout**
The maximum period that the MXM collects information transmitted by H.323 devices (except gateways) in order to synchronize a SIP-H.323 conversation.

**Collect OLCs Slow Timeout**
The maximum period that the MXM collects information transmitted by H.323 gateways in order to synchronize a SIP-H.323 conversation.

**Check if device is online**
Select the interval for checking if all registered nodes are connected to the MXM. At this time, the MXM polls the devices. If it does not receive a response from a node, the node is logged off.
5.6 Reporting Properties

In the MXM system Properties dialog box, click the Reporting icon to access the following property pages:

- Billing
- Event Log

**Billing**

In the **Billing** tab, select **Enable Billing** to list all videoconferences and audio calls within the local zone in a Call Details Record (CDR).

For more information about CDRs and call accounting, see **Working with the MXM>Reporting Option>Call Accounting** in the MXM’s online help.
5.6 Reporting Properties

Event Log

In the Event Log tab, define the length of time that the MXM keeps records of specific types of events.

![Event Log Properties](image)

*Event Log Properties*

Set record-keeping periods as follows:

- **Delete Informatory Records After**
  - Amount of time until informative records are deleted from the log.

- **Delete Warning Records After**
  - Amount of time until warning records are deleted from the log.

- **Delete Severe Records After**
  - Amount of time until severe error records are deleted from the log.

- **Delete Alarm Records After**
  - Amount of time until alarm records are deleted from the log.

- **Event Log View**
  - To view the event log, click this link.
6 \textit{DEFINING END POINT NODES}

End point nodes can represent several different types of users who log in to the MXM and require its services. This chapter provides explanations for defining the MXM management configuration for registered VCON vPoint, MeetingPoint, Group System end points, or non-VCON videoconferencing applications.

The videoconferencing system configurations of registered VCON vPoint end points (ViGO, software only), MeetingPoint 4.5/4.6 end points (ViGO, Escort, Cruiser, MediaConnect 8000/9000) and Falcon may be viewed and changed from the MXM. For more information see Appendixes A, B, and C, respectively.

6.1 \textit{Setting Up an End Point}

In order to register, an end point contacts the MXM (see "Granting Login Permission" on page 36). If login permission is granted automatically (Open Mode), the end point retains the default MXM properties. These default properties may be viewed or changed in the following templates:

- vPoint template (for ViGO 5.0 and higher, and Software-only systems)
- Desktop template (for ViGO, Escort and Cruiser systems running MeetingPoint 4.5 or 4.6)
- Falcon template
- MC6000 template (for MediaConnect 6000 systems)
- H.323 end point template (for other H.323 end points).

When you grant login permission manually, you can register the node with the default MXM properties or set the properties during the login process.

\begin{itemize}
  \item To set up an end point’s properties
  \begin{enumerate}
    \item After login permission is granted:
      \begin{description}
        \item[Open Mode] In the Administrator window, registered VCON end points appear under the \textit{VCON Systems} group. Non-VCON end points appear under the \textit{H.323 End Points} group. Double-click the new end point to set up its properties.
        \item[Closed Mode] The New End Point Wizard appears.
      \end{description}
  \end{enumerate}
\end{itemize}
6.1 Setting Up an End Point

2. Change properties according to your system specifications. To set different types of end point properties, click the appropriate tab at the top of the dialog box (in the New end point Wizard, click Next to advance to the next properties page). For explanations about the various properties, see “Setting End Point MXM Properties” on page 97.

3. To implement all the changes and close the dialog box, click OK (in the last page of the New end point Wizard, click Finish).

Login Attempt by Duplicate Users

The same User Name may not be logged in to the MXM from more than one end point at the same time.

In case of a duplicate login attempt from a MeetingPoint 4.5 (or higher) end point, the user is given the choice of:

- Continuing to log in using the same name, causing the other end point to be disconnected from the server.
- Logging in using a different User Name.

Duplicate User Login Message  Message onDisconnected End Point

For other VCON and non-VCON end points, duplicate login attempts are rejected without explanation from the MXM.
6.2 Setting End Point MXM Properties

The administrator can set MXM properties for all videoconferencing end points. MXM end point properties define how the end points operate as parts of the MXM videoconferencing network.

1. If an end point logs in during Closed Mode, the administrator can set these properties during the initial registration process or keep the default values.

2. The properties described in this section are applicable also to SIP User Agents (see Chapter 16, “Managing SIP Networks” on page 293).

General

The General tab contains identity information of the selected end point.

**vPoint End Point - General Properties**

The General Properties tab contains the following properties:

- **Directory Number**: Internal directory number (E.164 number) assigned to the end point. Any other end point registered with this MXM can call this end point by dialing this number.

- **Description**: Identity or description for the end point. This name will appear in the Main View after the login process is finished.
### 6.2 Setting End Point MXM Properties

<table>
<thead>
<tr>
<th>Alias</th>
<th>The end point’s alias name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of address used by the end point for registering with the MXM.</td>
</tr>
<tr>
<td>Additional IDs page</td>
<td>Click this link to view any additional IDs that have been configured for this end point.</td>
</tr>
<tr>
<td>Network Address</td>
<td>IP address of the end point.</td>
</tr>
</tbody>
</table>
| Build Number | *For MeetingPoint 4.5 and higher version only*  
Version information for the end point’s videoconferencing application. |
| Change Login Properties | *For MeetingPoint 4.5 and higher version only*  
For changing the end point’s MXM login password. This change takes effect the next time the end point logs in. |

1. In the **New** box, type a new password for the end point.
2. In the **Confirm** box, type the new password again.
Status

The **Status** tab displays the most recent dates that the selected node logged in and out of the MXM.

![vPoint End Point - Status Properties](image)

---

**Note:** Adapted from the VCON MXM Administrator's Guide.
6.2 Setting End Point MXM Properties

Call Forwarding

In the **Call Forwarding** tab, set alternate destinations for the MXM to route calls. Call forwarding for a specific node may be performed:

- At all times (unconditionally)
- If the node is busy in another videoconference
- If the call is not answered by the node.

![vPoint End Point - Call Forwarding Properties](image)

Set alternate destination numbers for the following conditions:

**Unconditional Forward**

When this extension is called, dial this number

Select this option to set an alternate destination for every call to this end point. In the list, choose the alternate destination. The forwarding occurs unconditionally and immediately.

If this option is selected, the **Busy** and **No Answer** options are not available.
6.2 Setting End Point MXM Properties

**Busy**

**When this extension is busy, dial this number**
Select this option to set an alternate destination for a call if this end point is engaged in another call at the same time. In the list, choose the alternate destination. The forwarding occurs immediately.

**No Answer**

**When this extension is not answering, dial this number**
Select this option to set an alternate destination for a call if this node does not answer after a specified time. In the list, select the alternate destination.

**Time extension can ring without being answered**
Type the number of seconds before the system forwards unanswered calls.

A “*” entry indicates that the particular forwarding setting is not active.

**Bandwidth Control Properties**

In the **Bandwidth Control** tab, you can define the permitted amount of bandwidth that the end point can use when communicating with others.

![Bandwidth Control Properties](image)

*H.323 End Point - Bandwidth Control*
Set bandwidth properties as follows:

**Allow calls with Non-registered Devices**
- Select to enable this end point to engage in videoconferences with parties that are not listed or cannot register with the local MXM.

**Limit Number of Concurrent Calls to**
- Select the number of calls that can go to or from the end point at the same time. This feature is available only to end points that support concurrent videoconferences.

**Bandwidth Limits**

**Limit Maximum to**
- Select this option to define the highest amount of bandwidth that the end point may use. In the list, choose the bandwidth.

**Limit Minimum to**
- Choose the lowest amount of bandwidth that the end point may use.

**Default IP Call Bandwidth**
- This feature is applicable in vPoint and Falcon end points only.
  - Set the default bandwidth for calls initiated by this end point. Unless the bandwidth is changed before dialing, the outgoing call will use this bandwidth.

**Multicast Bandwidth**
- This feature is applicable in vPoint 5.1 or higher, Desktop and MediaConnect 9000 end points only.

**Limit Session to**
- Select this option to define a bandwidth limit for the end point’s participation in an Interactive Multicast videoconference. The end point is not permitted to take part in a multicast session that exceeds this limit.
  - In the list, choose the bandwidth limit.

**Default Multicast Bandwidth**
- The default bandwidth for Interactive Multicast sessions. The actual bandwidth will depend on the amount of available bandwidth during the session.

**Maximum Bandwidth when Offline**
- Maximum bandwidth required for the end point to initiate videoconferences.
Pickup Permissions

In the **Pickup Permissions** tab, you can authorize other end points to answer a video meeting call to the selected end point. Only end points that are registered with the same MXM may receive pickup permission for each other.

For example, suppose Rachel is a video meeting call’s destination. If David has pickup permission for Rachel’s calls, he can answer this video meeting call.

In the list, select any number of end points that may pick up a call to this specific end point.

- To grant pickup permission to all end points in the list, click **Select All**.
- To clear all the selections, click **Clear All**.

![vPoint End Point - Pickup Permissions](image.png)
6.2 Setting End Point MXM Properties

MCU Service

In the MCU Services tab, define bandwidth allocation policy for any multipoint conferences that this end point engages in.

![Image](image.png)

**vPoint End Point - MCU Services Properties**

**MCU Service Permission Group**

Select the name of the MCU Service Permission group from which this end point can receive services. The available options are all MCU Service Permission groups that are listed in the Main View.

**Ad-hoc Permission Group**

Select the name of the Ad-hoc Permission Group from which this end point can choose a service for initiating an ad-hoc conference.

**Dedicated Service**

An ad-hoc service resource that may be used only if a specific end point is one of the parties of the resulting ad-hoc conference (either one of the original two end points of the conference or the invited end point).

If you want to dedicate a specific MCU or VCB service for this end point, select the service from the list.

To be a dedicated service, the service must be set up as an ad-hoc resource. See “Ad-Hoc Conference” on page 136.
6.2 Setting End Point MXM Properties

Gateway Services

In the **Gateway Services** tab, you can define bandwidth allocation policy for any MCU conferences or calls through a gateway that this end point engages in.

![Gateway Services Tab](image)

**vPoint End Point - Gateway Services Properties**

Set the Services properties as follows:

**Gateway Service Group**

Select the name of the gateway service hunting group from which this end point can receive services. If the end point dials the defined gateway access number (default is “9”), it may use any of the included services within that particular Service group.

The available options are all gateway service hunting groups that are listed in the Main View.

Some calls through the gateway may specify a required bandwidth. The following options define how the MXM allocates bandwidth in this situation:

- **Exact same bandwidth**
  Provide a choice only among services that provide the exact bandwidth required.

- **Equal or higher bandwidth**
  Provide a choice only among services that provide the exact bandwidth required or more.

- **Equal or lower bandwidth**
  Provide a choice only among services that provide the exact bandwidth required or less.
### 6.2 Setting End Point MXM Properties

| Equal or higher bandwidth - if not found, lower bandwidth | Provide a choice among services that provide the exact bandwidth required or more. If none exist, then offer services allocating lower than required bandwidth. |
| Equal or lower bandwidth - if not found, higher bandwidth | Provide a choice among services that provide the exact bandwidth required or less. If none exist, then offer services allocating higher than required bandwidth. |
| Limit bandwidth to ___ Kbps more (or less) than requested | Select the appropriate option to enable only a specific amount of deviation (higher or lower) from the requested bandwidth. From the appropriate list, choose the amount of deviation (in Kbps) allowed. For example, if you want to allow no more than an additional 128 Kbps, then choose **128** from the appropriate list. |

## ISDN Call Routing

In the **ISDN Call Routing** tab, define how the MXM decides how to route calls through gateways. The MXM can prioritize between several sets of gateway routing rules:

- Least Cost Routing Rules (see “Testing for the Optimal Gateway Service” on page 290)
- Bandwidth Rules (nodes’ Properties **Services** tab - see “Gateway Services” on page 105)

Set ISDN Call Routing properties as follows:

| Use least cost routing rules when this end point makes a call | Select to allow the MXM to apply least cost routing to the end points’ gateway calls. |
6.2 Setting End Point MXM Properties

*Bandwidth/Cost Preference*

Select one of the following:

- **Bandwidth rules precede least cost routing rules**
  When initiating a gateway call, the MXM chooses a gateway service based on the rules defined in the initiating end point’s Service properties.

- **Least cost routing rules precede bandwidth rules**
  When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.

---

*H.323 End Point - ISDN Call Routing Properties*
Product Info

The **Product Info** tab shows identification information about the end point’s videoconferencing system's manufacturer and model.

![vPoint End Point - Product Information Properties](image)

The tab provides the following information:

- **Vendor ID**  
  Identity of the end point manufacturer

- **Product ID**  
  Identity of the conferencing tool used by the end point.

- **Version ID**  
  Version number of the videoconferencing tool, for identification purposes.
6.2 Setting End Point MXM Properties

LDAP

The LDAP tab provides information about the end point’s registration, if applicable, in LDAP (Lightweight Directory Access Protocol) servers based on the X.500 standard for directory services. LDAP servers (also known as online directories) are lists of contacts whose videoconferencing systems are online and registered with that directory.

End points may be registered in more than one LDAP server, on condition that the MXM is registered and configured in them.

![Chart showing LDAP properties]

**vPoint End Point - LDAP Properties**

Set the end point’s LDAP configuration as follows:

- **Display Online Directory from this Server**
  - The online directory that is available for this end point.
  - The end point can dial any other videoconferencing user listed in this online directory.
6.2 Setting End Point MXM Properties

List node in the following LDAP servers

Select LDAP servers that can contain the subdirectory in which the end point should be listed. End points may be registered in all LDAP servers in which the MXM is registered.

If the end point has been previously registered in an LDAP server, its entry name or number (node entry) appears in the list.

- To be listed in all LDAP servers (depending on MXM registration in them), click Select All.
- To clear all the selections, click Clear All.

LDAP Servers View

Click this link to see location and access information about the available LDAP servers.

For more information about registering in LDAP servers, see Chapter 10, “Registering with LDAP Directories”.
**Additional IDs**

In addition to its directory (E.164) number, a node may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** tab, you may enter these, if applicable.

For example, this feature supports the Multiple Subscriber Network (MSN) service, which assigns multiple phone numbers to one ISDN line. MSN is supported by some ISDN switches.

![vPoint End Point - Additional IDs Properties](image)

**To add additional IDs for a node**

1. Click **Add** to display a table row.
2. In the **Alias** column, type the node’s additional E.164 number, H.323 alias, URL, or e-mail address.
3. In the **Type** column, click and select the address type.

To delete an entry, click in its row and then click **Delete**.
7 REGISTERING GATEWAYS

The MXM supports the use of H.323 gateways for connecting calls from registered end points to remote parties over ISDN networks. A gateway works as mediator between the two systems, translating between IP and ISDN protocols.

Each type of gateway has its own access number and dialing syntax. The dialing syntax usually includes the gateway's access number and the ISDN number of the remote party. For greater dialing flexibility, the syntax may also include delimiters.

Gateway services are also added to the MXM while gateways are granted login permission to the MXM. A gateway service defines the amount of available bandwidth and the type of information transmitted (such as voice only, video\voice, video\voice\data). One Gateway Service access number is created for each service type. At any time, you can add or edit available service entries from the Main View.

You can also organize sets of services within Gateway Service Hunting Groups. By associating end points with Gateway Service Hunting Groups, you can allocate available bandwidth to your organization’s end points according to a certain resources allocation policy or geographic considerations. When an end point dials the Gateway access number, the MXM searches in the end point’s Gateway services hunting group for an available service.

The registration and configuration procedures differ for Accord Gateways. For more details, see “Adding an Accord Gateway” on page 404.

7.1 Logging in a New Gateway

A gateway cannot register automatically to the MXM. To accept the initial login attempt, the administrator must manually grant permission and then define its MXM properties.

➢ To register a gateway to the MXM

1. In the Gateway’s configuration application, enter the IP address of the MXM and complete the appropriate commands to register.

   In the MXM Administrator application, a Login Request notification appears on the Administrator tree.

2. Expand the Login Request item.
7.1 Logging in a New Gateway

Login Request Notification for Gateway

3. Right-click the Gateway name and then click **Grant Login Permission**.

   A message appears, asking if you want to register the gateway now.

Gateway Registration Request

4. Click **OK** if you want to manually set the gateway’s properties. The New Gateway Wizard appears. The original property values are the default values defined in the H.323 gateway template (see “Setting Up Templates” on page 54).

   If you click **Cancel**, the gateway does not log in, but remains under the Login Requests object until you delete it (and the gateway stops trying to log in). See “Deleting a Login Request” on page 38.

5. Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see “Setting Gateway Properties” on page 116.

6. When you finish the last page, click **Finish**.

   The Add New Services dialog box displays a list of all gateway services configured in the new gateway.
7. Select the services that will be available in the MXM’s zone, and then click Add.

The New Gateway Services wizard appears.

8. Define the gateway service properties according to your system and gateway specifications, or keep the default settings. When you finish each page of the wizard, click Next. For explanations about the various properties, see “Setting Gateway Service Properties” on page 123.

The wizard is repeated for each service that you selected in the previous step.

9. When you finish the last page, click Finish.
7.2 Setting Gateway Properties

In step 5 of “Logging in a New Gateway” on page 114, the New Gateway Wizard provided the chance to change various gateway properties. This section describes these properties.

General

The General page contains identity information of the new gateway.

New Gateway - General Properties

The following information appears:

- **Description**: Identity of the gateway. This name will appear in the Main View after the login process is finished.

- **H.323 Address**
  - **Alias**: The gateway’s alias name.
  - **Type**: The type of address used by the gateway for registering with the MXM.

- **Network Address**: IP address of the gateway.

Changing the gateway’s IP address must be done through its configuration utility. The address cannot be changed from the MXM.
Product Info

The Product Info page provides information about the gateway's manufacturer and model. In addition, you can enable or disable the exchange functionalities supported for videoconference calls through the gateway.

New Gateway - Product Information Properties

- **Vendor ID**: Identity of the manufacturer.
- **Product ID**: Manufacturer's identity of the gateway product.
- **Version ID**: Manufacturer's version identification of the gateway product.
- **Location**: Physical location of the gateway.
- **MXM Transfer Model**: If selected, videoconferences through this gateway may be transferred to another end point.
- **H.450.3 (Call Diversion services)**: If selected, calls through this gateway may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.
- **Forward Facility messages**: If selected, calls through this gateway may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.
7.2 Setting Gateway Properties

If the selected gateway supports both H.450.3 and Forward Facility, we recommend enabling H.450.3.

Empty Capability Set
If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place. This option helps increase the speed of call transfer and ad-hoc videoconferences.

Information Request Messages (IRQ)
An IRQ is a request for status information from gatekeeper to terminal. If selected, the MXM can send IRQ messages checking if the gateway is online.

Add New Services to this Group
If a new gateway service is added to this gateway’s configuration, it will automatically be included in the hunting group selected here. To avoid adding services to hunting groups automatically, select No Group.

ISDN Dialing
Dialing conventions vary among gateways, according to the vendor. Refer to your gateway’s documentation for the specific delimiters or other characters that are required in order to access the gateway’s services.

New Gateway - ISDN Dialing Properties

New Gateway - ISDN Dialing Properties
In the **Dialing** page, define the following information:

**ISDN Dialing**

- **Delimiter between Service Number and First Number**
  Type the character, if applicable, that the MXM adds before the first ISDN number.

- **Delimiter between Phone Numbers**
  Type the character, if applicable, that the MXM adds between each ISDN number to be dialed.

- **Dialing sequence is terminated with**
  Type the character, if applicable, that the MXM must enter at the end of the dialing string.

All of the above values must be identical to the dialing configuration of the Gateway.

- **Send the Service Alias when dialing to this gateway**
  Video gateways support multiple services. If the gateway dialing syntax requires the inclusion of a service number, select this option.

- **Treat H.323 messages sent from this gateway as if they were sent from its service**
  Select this option if the new gateway does not define services. The MXM will handle messages sent through the gateway as H.323 64K Voice messages.
Call Routing

In the **Call Routing** page, enter the physical location of the gateway and define the cost rates for using the gateway’s services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see “Testing for the Optimal Gateway Service” on page 290).

To add a gateway location

1. If the location does not appear in the **Select Location** list, click the **Add New Location** button. The New Gateway Location Wizard appears.

2. Enter a **Name** of the location and a **Description** (optional). Select a **Country** and enter the location’s local **Area Code**.
7.2 Setting Gateway Properties

To go to the next page, click **Next**.

3. In the Add Default Dialing Rules dialog box, define the costs for calls through this gateway that originate in the MXM’s zone.

Select if MXM nodes may use this gateway for **Local**, **Long Distance**, and **International** calls, respectively.

Enter the rate (cost per minute) for each call type.

To go to the next page, click **OK**.
7.2 Setting Gateway Properties

4. In the Dialing Rules page, a table lists the information that you provided in the previous step.

![New Gateway Location - Dialing Rules Properties](image)

**New Gateway Location - Dialing Rules**

To add another rule, click the Add New Rule button and choose the appropriate call type (Local, Long Distance, and International).

To delete a rule, select that entry and click the Remove Rule button.

5. Click **Finish**. The gateway location now appears in the gateway’s Call Routing Properties.
7.3 Setting Gateway Service Properties

Gateway services are added to the MXM during the gateway registration process. A gateway service defines the amount of available bandwidth and the type of information transmitted (such as voice only, video\voice, video\voice\data - set in the gateway device’s configuration). One Gateway Service access number is created for each service type. At any time, you can add or edit available service entries from the Main View.

General

The General page contains identity information of the new gateway service.

> New Gateway Service - General Properties

Define the following information:

- **Directory Number**: Directory number of this service. This number will appear in the Main View after the login process finishes.
- **Description**: Identity of the service.
- **Alias**: The service’s alias.
- **Type**: The type of alias or address.
- **Network Address**: IP address of the gateway.
7.3 Setting Gateway Service Properties

Bandwidth Control

In the **Bandwidth Control** page, enter the exact bandwidth defined in the gateway’s configuration.

![New Gateway Service - Bandwidth Control Properties](image)
7.4 Gateway Service Hunting Groups

A Gateway Service hunting group contains multiple gateway services that are available to particular end points when they start LAN to ISDN videoconferences. One Gateway Service Hunting Group can contain different bandwidths and different Gateway devices.

Every registered end point may be associated with a gateway services hunting group (see “Gateway Services” on page 105). When an end point dials the gateway access number, the MXM searches for the services available to its associated group.

For example, if an end point specifies 384 Kbps bandwidth, the MXM checks in the associated hunting group if a gateway service providing 384 Kbps is permitted for the end point. If not, the MXM searches for the closest available service (in accordance to the end point’s Service properties).

This ability can help you allocate available ISDN resources to various end points according to a certain resources allocation policy or geographic considerations.

➤ To set up a hunting group of gateway services

1. Click the New Gateway Service Hunting Group button.

   The New Gateway Service Hunting Group wizard opens to the General Properties dialog box.
2. In the **General** page, type a name for this hunting group in the Description box. This description appears in the MXM Administrator under the Gateway Service Hunting Group object.

Click **Next**. The Hunting Group Properties dialog box appears.

![Gateway Services Hunting Group - Hunting Group Properties](image)

3. Select any number of services from the list to be in the hunting group. The selected services will be the only ones available to associated end points.
   - To place all services in the hunting group, click **Select All**.
   - To clear all the selections, click **Clear All**.

4. Click **Finish** to implement the settings and close the dialog box.
8  **REGISTERING AN MCU**

The VCON MXM supports the use of Multipoint Control Units (MCU) for connecting registered end points with a number of other end points in a multipoint videoconference.

*For Accord MGC users*

The operation of Accord MGC in conjunction with the MXM requires a special configuration. For more information, see Appendix E, “Using Accord® MGCTM with the MXM”.

### 8.1 Logging in a New MCU

If the MXM is in Open Mode for MCUs, any MCU that attempts to register is automatically logged in.

If the system is in Closed Mode for MCUs, an MCU must be granted login permission by an administrator with Super User privileges. During this process, the administrator must define or confirm the MCU’s MXM properties.

➢ **To register an MCU to the MXM**

1. In the MCU’s configuration application, enter the IP address of the MXM and complete the appropriate commands to register.

   If the MXM is in Closed Mode for MCUs, a Login Request notification will appear on the Administrator tree after several seconds.

2. Expand the Login Request item.
8.1 Logging in a New MCU

3. Right-click the MCU name and then click **Grant Login Permission**.

   A message appears, asking if you want to register the MCU now.

   ![MCU Registration Request](image)

   **MCU Registration Request**

4. Click **OK** if you want to manually set the MCU’s properties, such as exchange function capabilities (Product Info). The New MCU Wizard appears. The original property values are the default values defined in the H.323 MCU template (see “Setting Up Templates” on page 54).

   If you click **Cancel**, the MCU does not log in, but remains under the Login Requests object until you delete it (and the MCU stops trying to log in). See “Deleting a Login Request” on page 38.

5. Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see “Setting MCU Properties” on page 129.

6. When you finish the last page, click **Finish**.
8.2 Setting MCU Properties

In step 5 of “Logging in a New MCU” on page 128, the Add Wizard provided the chance to change various MCU properties. This section describes these properties.

General

The General page contains identity information of the new MCU.

![New MCU - General Properties](image)

*New MCU - General Properties*

In the General Properties tab, the following properties appear:

- **Description**: Identity of the MCU. This name will appear in the Main View after the login process is finished.
- **Alias**: The MCU’s alias name.
- **Type**: The type of address used by the MCU for registering with the MXM.
- **Network Address**: IP address of the MCU.

Changing the MCU’s IP address must be done through its configuration utility. The address cannot be changed from the MXM.
8.2 Setting MCU Properties

Bandwidth Control

In the Bandwidth Control tab, select Allow calls with Non-registered Devices to allow non-registered devices to participate in any multipoint videoconferences managed by this MCU.

![New MCU - Bandwidth Control Properties](image)

_New MCU - Bandwidth Control Properties_
Product Info

The **Product Info** page provides information about the MCU's manufacturer and model. In addition, you can enable or disable the exchange functionalities supported for multipoint videoconferences through the MCU.

![New MCU - General Properties](image)

**New MCU - H.323 Properties**

- **Vendor ID**: Identity of the manufacturer.
- **Product ID**: Manufacturer's identity of the MCU product.
- **Version ID**: Manufacturer's version identification of the MCU product.
- **Location**: Physical location of the MCU.
- **MXM Transfer Model**: If selected, videoconferences through this MCU may be transferred to another end point.
- **H.450.3 (Call Diversion services)**: If selected, calls through this MCU may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.
8.2 Setting MCU Properties

**Forward Facility messages**
If selected, calls through this MCU may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.

If the selected MCU supports both H.450.3 and Forward Facility, we recommend enabling H.450.3.

**Empty Capability Set**
If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place. This option helps increase the speed of Call Transfer and Ad-hoc Videoconferences.

**Information Request Messages (IRQ)**
An IRQ is a request for status information from gatekeeper to terminal. If selected, the MXM can send IRQ messages checking if the MCU is online.

**Add New Services to this Group**
If a new MCU service is added to this MCU’s configuration, it will automatically be included in the permission group selected here. To avoid adding services to permission groups automatically, select No Group.
8.3 MCU Services

MCU Services define the MCU resources used during a multipoint videoconference.

A registered MCU’s services are automatically listed in the MXM Administrator after the particular MCU is granted login permission to the MXM. One directory number is created for each service type. At any time, you can edit service entries from the Main View.

For Accord MGC users
In the Accord MGC, MCU services are provided through Meeting Rooms. For information about defining Meeting Room properties, see “Setting Meeting Room Properties” on page 400.

➢ To view or edit MCU Services

1. Double-click an MCU Service node. The specific service’s Properties dialog box appears.

2. Define the MCU Service properties according to your system and MCU specifications, or keep the default settings.

3. To implement the changes and proceed to another tab in the dialog box, click the appropriate tab.

4. To implement all the changes and close the dialog box, click OK.

The following subsections describe the MCU Service properties.
8.3 MCU Services

General

The General tab contains identity information of the new MCU Service.

![MCU Service - General Properties](image)

In the General tab, the following properties appear:

- **Directory Number**: Number to be dialed for using this service.
- **Description**: Name of the service. This name will appear in the Main View after the login process is finished.
- **Alias**: The MCU’s alias as it is defined by its operating system.
- **Type**: The type of address used by the MCU for registering with the MXM.
- **Additional IDs page**: Click this link to view any additional IDs that have been configured for this MCU.
- **Network Address**: IP address of the MCU.

Changing the MCU’s IP address must be done through its configuration utility. The address cannot be changed from the MXM.
**Bandwidth Control**

In the **Bandwidth Control** tab, select **Allow calls with Non-registered Devices** to allow non-registered devices to participate in any multipoint videoconferences using this MCU service.

*MCU Service - Bandwidth Control Properties*
Ad-Hoc Conference

A point-to-point conference becomes an ad-hoc conference when additional end points are "invited" by one of the parties and they join the session. In the Ad-hoc Conference tab, you can make the selected MCU Service available for use in ad-hoc conferences. This availability may be in addition to basic multipoint videoconferencing or exclusive for ad-hoc conferences.

**MCU Service - Ad-hoc Conference Properties**

**Use this service as an ad-hoc conference resource**

Select to make this service available for use when expanding to an ad-hoc videoconference.

If this service will be a Dedicated Service for a specific end point (see “MCU Service” on page 104), this option must be selected. The specific end point must either be one of the original two end points of the conference or the invited end point.

**Use this service exclusively for ad-hoc conferences**

Select to make this service available only for use in ad-hoc videoconferences, and unavailable for point-to-point sessions.
8.3 MCU Services

LDAP

The LDAP tab provides information about the MCU service’s registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes’ LDAP Properties, see “LDAP” on page 109.

Additional ID

In addition to its directory (E.164) number, an MCU service may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the Additional ID page, you may enter these, if applicable. For more information about adding Additional IDs, see “Additional IDs” on page 111.
8.4 MCU Service Permission Groups

An MCU Service Permission group is a set of MCU services that may be used by specific nodes. Its purpose is to control the use of MCU resources among an organization’s end points.

An MCU Service Permission group may consist of one service, multiple services, or all available services. It may also include combinations of services from more than one registered MCU. In addition, you can define the automatic addition of new MCU services to a specific permission group (see “Product Info” on page 131).

By default, every registered end point is assigned to the default permission group. This may be changed when manually adding a new end point, or by editing the end point’s properties (see “Gateway Services” on page 105). An end point is only permitted to use those services listed in its assigned permission group. If it attempts to dial a service not listed in its group, the MXM rejects the call.

MCU Service Permission Groups in the Administrator Window

To create an MCU Service Permission Group

1. Click the New MCU Permission Group button. The New MCU Permission Group dialog box appears.

2. Change properties according to your permission group requirements. To move to the next properties page, click Next. For explanations about the various properties, see pages 139 to 140.

3. Click Finish. In the Main View, the new group appears under the MCU Service Permission Group object.
8.4 MCU Service Permission Groups

General

In the **Description** box, type a name for the MCU Service Permission Group. This name will appear on the system tree and in nodes properties **MCU Services** tabs.

![New MCU Permission Group - General Properties](image)

*New MCU Permission Group - General Properties*
Permission Group

The **Permission Group** Properties page includes all registered services from all registered MCUs.

Select any number of services from the list to be in the permission group. The group may also include combinations of services from more than one registered MCU.

- To place all services in the permission group, click **Select All**.
- To clear all the selections, click **Clear All**.

![New MCU Permission Group Properties](image)

*New MCU Permission Group Properties*
8.5 **Dedicated MCU Services**

A dedicated MCU service is set up only for expansion to an ad-hoc conference that includes a specific end point. That is, the service is “dedicated” to that end point. That specific end point must be either one of the original two end points of a point-to-point conference or the invited end point.

➤ **To dedicate a service to a specific end point**

1. Right-click the MCU Service, point to Property, and then click Ad-Hoc Conference. The Ad-Hoc Conference tab appears.

2. Select **Use this service as an ad-hoc conference resource** and then click OK (in addition, you may also set the service to be exclusive for ad-hoc conferences only).

3. Right-click the end point, point to Property, MXM, and then click MCU Services. The MCU Services tab appears.

4. In the Dedicated MCU Service list, select the service.
8.6 Ad-hoc Permission Groups

8.6 Ad-hoc Permission Groups

An Ad-hoc Permission group is a set of MCU and VCB services that are defined for use in ad-hoc conferences. Its purpose is to control the use of resources for expanding to ad-hoc conferences.

An Ad-hoc Permission group may consist of one service or multiple services. It may also include combinations of services from more than one registered VCB and/or MCU. The order in which services are requested is important and controllable by Super User-level administrators.

During expansion to an ad-hoc conference, the MXM only uses those services listed in its assigned permission group. After an end point invites another end point, the MXM first tries to use the first service defined in the permission group. If the first service is not available, it tries to use the second defined service, and so on. If all enabled services are unavailable, the MXM does not complete the "invitation" to the additional end point.

By default, every registered end point is assigned to the default Ad-hoc Permission Group. This may be changed when manually adding a new end point, or by editing the end point’s properties.

➤ To add an Ad-hoc Permission Group

1. In the toolbar, click the New Ad-hoc Permission Group button. The New Ad-hoc Permission Group dialog box appears.

2. Change properties according to your permission group requirements. To move to the next properties page, click Next. For explanations about the various properties, see pages 139 to 140.

3. Click Finish. In the Main View, the new group appears under the Ad-hoc Permission Group object.
8.6 Ad-hoc Permission Groups

General

In the **Description** box, type a name for the Ad-hoc Permission Group. This name will appear on the system tree and in node Properties dialog boxes' MCU Services tab.

![New Ad-hoc Permission Group - General Properties](image)

*New Ad-hoc Permission Group - General Properties*
8.6 Ad-hoc Permission Groups

Permission Group

The Permission Group Properties page includes all registered services that are defined for use as an ad-hoc resource (see “Ad-Hoc Conference” on page 136).

Select any number of MCU or VCB services from the list to be in the Ad-hoc Permission Group. The group may also include combinations of services from more than one registered VCB and/or MCU.

— To place all services in the permission group, click Select All.
— To clear all the selections, click Clear All.
Setting the Usage Order

The services' locations in the list determines the order in which the MXM tries to use them. After an end point invites another end point, the MXM first tries to use the first service defined in the permission group. If the first service is not available, it tries to use the second defined service, and so on. If all enabled services are unavailable, the MXM does not complete the "invitation" to the additional end point.

In the Permission Group page, you can move the services to different places in the usage order.

➢ To set the usage order of the selected services

☐ Click the name (not the checkbox) of a selected service. To move the service up and down the list to its designated place, click Move Up or Move Down as many times as necessary.

Repeat this step for as many services as necessary.
9 Neighboring Zones

9.1 The MXM's Relationship with Neighboring Zones

In addition to its own registered nodes, the MXM provides an organization with the ability to carry on videoconferences with nodes outside its administrative area. These nodes may be managed by other MXMs or third-party Gatekeepers, or unregistered with any management device.

The collections of nodes that MXMs and Gatekeepers register and manage are called zones. Multiple zones may be listed in the Administrator’s system tree, where you may manage the communication between them and the local MXM.

Neighboring zones may be added automatically if calls are made between it and the local MXM’s zone, or added manually by you. Additional zones must be configured, according to the inter-zone management policy that you implement. After zones are added to the tree, you may manually add entries for end points, MCUs and Gateways that are registered in those zones.

After zones are set up in the Administrator Main View, you can perform the following inter-zone management tasks (see “Inter-Zone Videoconferencing Management” on page 165):

- Start a point-to-point videoconference between two end points
- Setting up a dialing plan, which defines how to dial users in other zones
- Restrict the bandwidth allotment for inter-zone videoconferences
- Generate Call Details Records (CDR) records for inter-zone videoconference calls
- Share gateway services and MCU services with neighboring zones
- Restrict the use of exchange features such as Call Transfer and Call Forwarding.
9.2 Logging in New Zones

Inter-zone functions are available between the local MXM and zones known to it. Neighboring MXMs or Gatekeepers may be listed in the MXM automatically or manually.

Registered MXMs and Gatekeepers appear on the system tree under the Zones object. You can manually add any neighbor node (end point, MCU, or gateway) from a specific zone under that same zone in the Administrator. You can then initiate calls involving these nodes and manage their MXM configuration (see “Setting End Point MXM Properties” on page 97) in the same way as nodes registered with the local MXM (MXM node).

Listing of Neighboring MXMs and Gatekeepers

Adding Zones Automatically

The MXM System Properties include an option for adding zones in Open Mode. If this option is selected, the MXM will automatically add other MXMs’ and Gatekeepers’ zones only after one of the following occurs:

- The local MXM tries to dial using the Multicast search method.
- An incoming call from another zone arrives.

Discovered zones are listed in the Administrator (see the illustration above).

➢ To add zones automatically

1. Right-click the MXM node, point to Property and then Security, and click Security Mode. The Security Mode tab opens.

2. Select the Open Mode and Neighboring Gatekeepers (Zones) options.

The other MXMs and/or gatekeepers must also be in Open Mode.

3. Click the H.323 & SIP icon on the left side of the dialog box. By default, the Zone Settings tab is open.
4. We recommend the Multicast search technique for searches of zones and neighboring nodes. Select **First Multicast Location Requests, then in Defined Zones** (default selection) or **Send Multicast Location Requests** (see “Zone Settings” on page 90).

5. Click **OK**.

![Setting Open Mode for Neighboring MXMs and Gatekeepers](image)

**Adding Zones Manually**

If the MXM is in Closed Mode for zones, neighboring MXMs and Gatekeepers may only be added to the Administrator manually. In this process, you must define or confirm each node’s properties.

➤ **To add a zone manually**

1. Click the New Zone button. The New Zone Wizard appears. The original property values are the default values defined in the Zone template (see “Setting Up Templates” on page 54)

2. Change properties according to your network specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see “Setting Zone Properties” on page 150.

3. When you finish the last page, click **Finish**.
9.3 Setting Zone Properties

The main objective of defining zone properties is the definition of policies and the allocation of bandwidth for inter-zone videoconferences. This section describes these properties.

To define zone properties

1. Double-click a neighboring zone. The zone’s Properties dialog box appears.

2. Define the zone properties according to your network’s videoconferencing needs and specifications, or keep the default settings.

3. To implement the changes and proceed to another tab in the dialog box, click Apply and then the appropriate tab.

4. To implement all the changes and close the dialog box, click OK.

The following sections describe the zone properties.

General

The General tab contains identity information of the new MXM or Gatekeeper.

[Image: Zone - General Properties]
In the **General** Properties tab, the following properties appear:

- **Zone Prefix**: Directory number (E.164 number) assigned to the MXM or Gatekeeper. The zone prefix functions as an “area code,” which may be used by the MXM to dial nodes in the selected zone (to enable zone prefix dialing, see the next section, “Zone Settings”).

- **Description**: Identifying name of the zone. This name will appear in the Main View.

- **Network Address**: IP address of the zone’s MXM or Gatekeeper.

### Zone Settings

In the **Zone Settings** tab, define the local MXM’s intercommunication relationship with the neighboring zone. This relationship includes permission to make and receive calls, generation of CDR reports, and the use of prefixes when dialing.

![Zone - Zone Settings Properties](image-url)
9.3 Setting Zone Properties

In the **Zone Settings** Properties tab, the following properties appear:

**Making Calls to this Zone**

- **Allow Making Calls to this Zone**
  - If selected, all local MXM nodes may start videoconferences with neighbor nodes registered in this zone.

- **Generate CDR records for calls made to this Zone**
  - If selected, all calls to neighbor nodes in this zone will be listed in a Call Details Record (CDR). For more details about CDRs, see *Getting Started* > *Monitoring System Status* > *Call Accounting* in the MXM’s online help.

- **Always use Zone prefix when searching for end points**
  - Select this option to enable dialing to gatekeepers that require their prefix in the dialing syntax (non-VCON gatekeepers). To dial nodes managed by these gatekeepers, users must receive the appropriate prefixes from the system administrator or from the remote party.

**Receiving Calls from this Zone**

- **Allow receiving calls from this zone**
  - If selected, local MXM nodes may receive videoconference calls from neighboring nodes registered in this zone.

- **Generate CDR records for calls received from this Zone**
  - If selected, all calls from neighbor nodes in this zone will be listed in a Call Details Record (CDR). For more details about CDRs, see *Working with the MXM* > *Reporting Option* > *Call Accounting* in the MXM’s online help.

- **Location**
  - Enter a general physical location of the zone’s MXM or Gatekeeper and its end points
9.3 Setting Zone Properties

Bandwidth Control

In the **Bandwidth Control** tab, you can define the available amount of bandwidth for all concurrent videoconferencing calls between the local zone and the neighboring zone.

![Zone - Bandwidth Control Properties](image)

**Zone - Bandwidth Control Properties**

Set bandwidth control properties as follows:

- **Limit Number of Concurrent Calls to**
  Select the maximum number of calls between the two zones at the same time. The default setting is **5**.

- **Limit Maximum to**
  Select this option to define the total available bandwidth that the local MXM allocates to all calls to the neighboring zone. In the list, select the bandwidth.
9.3 Setting Zone Properties

MCU Services

In the MCU Services tab, define how the local MXM allocates MCU resources for incoming videoconferencing calls from the neighboring zone.

![MCU Services Properties](image)

**MCU Service Permission Group**

If you want to limit the usage of MCU services during incoming videoconferences from the neighboring zone, select an MCU Service Permission Group. The available options are all MCU Service Permission Groups that are listed in the current Administrator Main View. For more information about MCU Service Permission Groups, see “MCU Service Permission Groups” on page 138.

To disable the selection of MCU services, select No Group. As a result, nodes in the neighboring zone will not be able to participate in MCU-managed videoconferences that include nodes from the local MXM’s zone.

**Ad-hoc Service Permission Group**

Select the name of the Ad-hoc Service Permission Group from which the neighboring zone's end points can choose a service for initiating an ad-hoc conference to the local zone. For more information about Ad-hoc Service Permission Groups, see “Ad-hoc Permission Groups” on page 142.
Dedicated Service

A dedicated service is an ad-hoc service resource that may be used only if any of the neighboring zone's end points are in the resulting ad-hoc conference (either one of the original two end points of the conference or the invited end point).

If you want to dedicate a specific MCU or VCB service for this neighboring zone's end points, select the service from the list.

To be a dedicated service, the service must be set up as an ad-hoc resource. See “Ad-Hoc Conference” on page 136.
9.3 Setting Zone Properties

Gateway Services

In the Gateway Services tab, define how the local MXM allocates gateway resources for incoming videoconferencing calls from the neighboring zone.

![Gateway Services Property Settings](image)

**Gateway Service Group**

Select the Gateway Service hunting group that defines the services that will be available for incoming videoconferences from the neighboring zone. If a neighbor node dials the defined gateway access number (default is “9”), it may use any of the included services within that particular Service group.

The available options are all Gateway Service hunting groups that are listed in the current Administrator Main View (see “Gateway Service Hunting Groups” on page 125).

Some calls from the neighboring zone through a gateway may specify a required bandwidth. The following options define how the MXM allocates bandwidth in this situation:

- **Exact same bandwidth**
  - Provide a choice only among services that provide the exact bandwidth required.

- **Equal or higher bandwidth**
  - Provide a choice only among services that provide the exact bandwidth required or more.
<table>
<thead>
<tr>
<th>Setting Zone Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal or lower bandwidth</td>
<td>Provide a choice only among services that provide the exact bandwidth required or less.</td>
</tr>
<tr>
<td>Equal or higher bandwidth - if not found, lower bandwidth</td>
<td>Provide a choice among services that provide the exact bandwidth required or more. If none exist, then offer services allocating lower than required bandwidth.</td>
</tr>
<tr>
<td>Equal or lower bandwidth - if not found, higher bandwidth</td>
<td>Provide a choice among services that provide the exact bandwidth required or less. If none exist, then offer services allocating higher than required bandwidth.</td>
</tr>
</tbody>
</table>
| Limit bandwidth to ___ Kbps more (or less) than requested | Select the appropriate option to enable only a specific amount of deviation (higher or lower) from the requested bandwidth. From the appropriate list, choose the amount of deviation (in Kbps) allowed.  
For example, if you want to allow no more than an additional 128 Kbps, then choose 128 from the appropriate list. |
ISDN Call Routing

In the ISDN Call Routing tab, define how the MXM decides how to route gateway calls to this zone. The MXM can prioritize between several sets of gateway routing rules:

- Least Cost Routing Rules (see “Testing for the Optimal Gateway Service” on page 290)
- Bandwidth Rules (nodes’ Properties Gateway Services tab - see “Gateway Services” on page 105)

Set ISDN Call Routing properties as follows:

**Use least cost routing rules when this endpoint makes a call**

Select to allow the MXM to apply least cost routing to gateway calls to this zone.
9.3 Setting Zone Properties

Bandwidth/Cost Preference

Select one of the following:

**Bandwidth rules precede least cost routing rules**

- **Bandwidth rules**: When initiating a gateway call, the MXM chooses a gateway service based on the rules defined in the initiating end point’s Service properties.

- **Least cost routing rules precede bandwidth rules**: When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.

Product Info

In the **Product Info** tab, select the exchange functionalities that are supported by the neighboring zone's MXM or gatekeeper.

![Zone - Product Info Properties](image-url)
### 9.3 Setting Zone Properties

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXM Transfer Model</td>
<td>If selected, videoconferences between neighbor nodes and MXM nodes may be transferred to another endpoint.</td>
</tr>
<tr>
<td>H.450.3 (Call Diversion services)</td>
<td>If selected, calls between the neighboring zone and the local MXM's zone may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.</td>
</tr>
<tr>
<td>Forward Facility messages</td>
<td>If selected, calls between the neighboring zone and the local MXM's zone may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.</td>
</tr>
<tr>
<td>Empty Capability Set</td>
<td>If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place between the neighboring zone and the local MXM's zone. This selection also enables the joining of neighbor nodes in ad-hoc videoconferences.</td>
</tr>
</tbody>
</table>

### Additional IDs

In addition to its zone prefix, a neighboring zone may have additional prefixes to which its nodes may be dialed, such as additional E.164 addresses and/or H.323 IDs (node name).

For more information about adding Additional IDs, see “Additional IDs” on page 111.
Redundancy

In addition to its main gatekeeper (as defined in this configuration), a zone may also have redundant gatekeepers. When a call is made from the local zone to this zone, the local MXM tries to route the call through the main and redundant gatekeepers. The first gatekeeper that responds connects the call to the destination.

➤ To add a redundant gatekeeper

1. In the **Redundancy** tab, click **Add**. An entry line appears in the Gatekeeper Network Addresses table.
2. Type the IP address of the gatekeeper.
3. To add another gatekeeper, repeat steps 1 and 2.

➤ To delete a redundant gatekeeper

1. In the **Redundancy** tab, select the gatekeeper entry.
2. Click **Delete**.
Advanced

In the Advanced tab, define the local MXM’s intercommunication relationship with the neighboring zone. This relationship includes permission to make and receive calls, generation of CDR reports, and the use of prefixes when dialing.

Set Advanced Properties as follows

Zone Hierarchy

Neighbor

The selected zone is a neighboring zone. Nodes registered in the local MXM zone may carry on videoconferences with nodes registered in the selected zone.

Parent Directory Gatekeeper

The selected zone contains records of gatekeepers and nodes within its domain, which is usually a LAN or WAN covering a local region. Within the network, Location Requests (LRQ) arrive here from other MXMs and gatekeepers. The directory gatekeeper switches the request and the call to the zone in which the destination node resides.

For more information about directory gatekeepers, see “Directory Gatekeepers” on page 169.
9.3 Setting Zone Properties

Child Gatekeeper

The selected zone covers an area inside a parent gatekeeper's domain which is identified by a specific dialing prefix.

Zone Type

MXM Zone

Select this option if an MXM provides management and gatekeeper services to this neighboring zone. If the zone is managed by a non-VCON gatekeeper, deselect this option.

SecureConnect Settings

Located Behind an ALG Proxy

Select this option if an ALG Proxy is installed between the local MXM and this neighboring zone. The MXM will automatically address calls to the neighboring zone through the ALG Proxy.
9.4 Permanent Non-Registered Devices

There may be situations where nodes will not register with any gatekeeper, but should still be available for videoconferencing with registered end points. In such a case, you can make the node known to the MXM by listing it as a *permanent non-registered device*.

**Adding a Permanent Non-Registered Device**

A non-registered node may be “discovered” if it is in a videoconference with an MXM node. In such a case, the non-registered node appears on the system tree under the Non-registered Devices object during the duration of this call. The administrator may then permanently add the node to the tree (depending on the system Non-registered Device Properties - see page 89).

![Non-registered Device Appearing in Main View](image)

**To add a non-registered node to the system tree**

1. Right-click the node and then click **Make Permanent**. The New Permanent Non-registered Device Wizard appears.

2. Set the properties according to your system specifications. When you complete a page, click **Next** to advance to the next properties page). For explanations about the various properties, see “Setting End Point MXM Properties” on page 97.

3. Click **Finish** to exit the wizard.
9.5 Inter-Zone Videoconferencing Management

You can perform the following inter-zone management tasks:

- Setting up a dialing plan, which defines how the MXM starts point-to-point videoconferences between MXM nodes and neighbor nodes, or with a non-registered node.
- Restrict the bandwidth allotment for inter-zone videoconferences
- Restrict the use of exchange features such as Call Transfer and Call Forward.
- Sharing gateway resources with other zones.

Setting Up Inter-Zone Dialing

If your organization contains more than one MXM or other gatekeepers, you likely want to provide the ability of end points to videoconference with nodes in the other zones, as well as to zones outside the organization. This section explains how to set up the relevant configurations to permit inter-zone videoconferencing.

To permit dialing between nodes in different zones, the MXMs and the relevant zones must have a specific configuration. Perform the following tasks:

1. Within your own organization, we recommend that you assign different directory numbering ranges in all MXMs. If identical directory numbers exist in different zones, zone prefixes must be added to numbers when dialing, and must be added to the node configurations (for more details, see “Dial Plan” on page 73).
2. If your organization is using an online directory (such as ILS or NDS), enable the zone prefix to be appended to each entry’s configuration. If a node is moved to a different zone, the MXM also updates the prefix in the online directory (for more details, see “LDAP Settings” on page 77).

Enable the zone prefix to be appended to each entry’s configuration in online directories.

3. All of the respective zones must be known to each other. If the MXM is set to Open Mode registration, any neighboring zones managed by MXMs and H.323 gatekeepers may be listed automatically in the Main View. If the MXM is set to Closed Mode registration, you have to add the neighboring MXMs and gatekeepers to the Main View manually (to set the MXM to Open or Closed Mode, see “Security Mode” on page 85).

Set Open Mode for Neighboring Gatekeepers (Zones)

Open Mode for Adding Neighboring MXMs and Gatekeepers

Make sure that the zone prefixes (directory numbers) are listed identically in all known MXMs and gatekeepers.
4. Inter-zone search for addresses must be enabled in the MXMs. You can set the MXMs to search using a combination of the Multicast Location Requests, Defined Neighbor Zones, and Directory Gatekeeper methods. See the figure on the next page (for more details, see the MXM’s “Zone Settings” on page 90).

Select the method of searching for addresses in other zones

Selecting Address Search Method

5. The ability to receive and send calls must be enabled in the Zone Settings of each relevant zone’s properties (for more details, see the zone’s “Zone Settings” on page 151).

Allow calling to and receiving calls from the selected zone

Allow Videoconferences Between this Zone and the Local Zone
6. To enable dialing to gatekeepers that require their prefix in the dialing syntax (non-VCON gatekeepers), select the **Always use Zone prefix when searching for end points** option in the Zone Settings of the zone. To dial nodes managed by these gatekeepers, users must receive the appropriate prefixes from the system administrator or from the remote party (for more details, see the zone’s “Zone Settings” on page 151).

Select to allow local MXM nodes to call nodes managed by a non-VCON gatekeeper

*Allow Videoconferences Between a Zone Managed by a non-VCON Gatekeeper and the Local Zone*
Directory Gatekeepers

Directory gatekeepers are used for connecting neighbor gatekeepers and end points over WANs. They simplify the process of searching for dialed addresses in different zones over large areas.

The MXM can operate within a network that includes a hierarchy of directory gatekeepers (DGK). A typical hierarchy maintained by telephony and Internet service providers may include a global gatekeeper, country gatekeepers, regional and local gatekeepers. By concentrating address searches through such a hierarchy, an organization can significantly simplify the search and connection process.

A typical DGK hierarchy is based on parent-children-type relationships among the gatekeepers, including MXMs. The following is a sample hierarchy:

<table>
<thead>
<tr>
<th>Tier</th>
<th>Parent/Child Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global gatekeeper</td>
<td>Children - Country gatekeepers</td>
</tr>
<tr>
<td>Country gatekeeper</td>
<td>Parent - Global gatekeeper</td>
</tr>
<tr>
<td></td>
<td>Children - Local gatekeepers</td>
</tr>
<tr>
<td>Regional or Local gatekeeper</td>
<td>Parent - Country gatekeeper</td>
</tr>
<tr>
<td></td>
<td>Children - End points</td>
</tr>
<tr>
<td>End point</td>
<td>Registered with Local MXM/gatekeeper</td>
</tr>
</tbody>
</table>

MXMs are usually located within the Regional/Local tier. Depending on the size and range of the network, there may be multiple layers of regional and/or local directory gatekeepers.

If the Search policy among your network is set to Directory Gatekeepers, the MXM routes calls to its parent directory gatekeeper, which searches its database to see if the prefix of the dialed number is known to it. If not, the parent gatekeeper routes the call to its parent gatekeeper, and so on, if necessary, until it reaches the global gatekeeper. The global gatekeeper then routes the call to a child gatekeeper matching the prefix. From this point, each gatekeeper continues switching the call to the appropriate child entity (according to area codes and local exchange codes).
9.5 Inter-Zone Videoconferencing Management

Global Tier
00

Country Tier
Japan
81

Regional Tier
Tokyo
45

Local Tier
All Nippon University
477

End Point Tier
81-45 477-9511

Country Tier
USA
1

Regional Tier
Los Angeles
213

Local Tier
LA Tech University
742

End Point Tier
1-213-742-0658

Sample Call Through Directory Gatekeeper Hierarchy
Illustration Legend

1. End point managed by LA Tech University MXM in Los Angeles dials end point in Japan.

2. LA Tech University MXM does not have the global code (00) listed in its registered nodes. It forwards call to its parent, the Los Angeles regional directory gatekeeper.

3. Los Angeles gatekeeper does not have the global code (00) listed in its database. It forwards call to its parent, the USA country gatekeeper.

4. USA gatekeeper forwards call to its parent, the global gatekeeper (00).

5. The global gatekeeper routes the call to Japan country gatekeeper (81).

6. Japan gatekeeper locates the 45 exchange and routes the call to Tokyo regional gatekeeper.

7. Tokyo gatekeeper locates the 477 exchange's zone controlled by the All Nippon University MXM.

8. All Nippon University MXM completes the call to the 9511 end point.
9.5 Inter-Zone Videoconferencing Management

Setting Up an MXM-Directory Gatekeeper Configuration

To set up your MXM to work with a Directory Gatekeeper, perform the following tasks:

1. To configure the local MXM to send location requests (LRQs) to directory gatekeepers, set the Search policy in the MXM System Zone Settings (for more details, see “Zone Settings” on page 90).

2. Define any directory gatekeeper listed in the MXM Administrator Main View as a Parent or Child directory gatekeeper in its Zone Settings (for more details, see “Zone Settings” on page 151).

3. Create additional IDs, such as aliases, for the directory gatekeeper (see “Additional IDs” on page 111).
Restricting Bandwidth Allotment

For each neighboring zone, you can restrict the amount of bandwidth that is available for all concurrent videoconferences between that zone and the local MXM. For individual nodes, you can also define a maximum bandwidth allotment.

➤ To set bandwidth allotment for inter-zone calls

1. Double-click the neighboring zone and click the Bandwidth Control tab.
   -or-
   Right-click the neighboring zone, point to Property and then click Bandwidth Control.

2. In the Bandwidth Control page, select Limit Maximum to to define the total bandwidth that the local MXM allocates for all calls to the neighboring zone. In the list, select the bandwidth in Kbps.

3. Select Limit Number of Concurrent Calls to restrict the number of simultaneous calls allowed between the local MXM and the neighboring zone. From the list, choose the number of calls.

4. To implement the changes and close the dialog box, click OK.

For example, if you allocated 384 Kbps for all calls and there are four concurrent calls, a possible distribution of the available bandwidth for all calls would be 128, 128, 64 and 64 Kbps.

<table>
<thead>
<tr>
<th>Number of simultaneous calls allowed between the local MXM and the neighboring zone</th>
<th>Total bandwidth allocated for all calls to the neighboring zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit number of concurrent calls to 5 Calls.</td>
<td>Limit maximum to 384 Kbps.</td>
</tr>
</tbody>
</table>

Setting Bandwidth Allotment for Inter-zone Calls
To set bandwidth allotment for calls between the local MXM and a neighbor node

1. Double-click the neighbor node and click the **Bandwidth Control** tab.

   -or-

   Right-click the neighbor node, point to **Property** and then click **Bandwidth Control**.

2. In the Bandwidth Control page, select **Limit Maximum to** to define the total bandwidth that the local MXM allocates for all concurrent calls to the neighbor node. In the list, select the bandwidth in kbps.

3. Select **Limit Number of Concurrent Calls** to restrict the number of simultaneous calls allowed between the local MXM and the neighbor node. From the list, choose the number of calls.

4. To implement the changes and close the dialog box, click **OK**.
Restricting H.450 Exchange Functions

You can allow or forbid H.450 Exchange functions, such as Call Forwarding and Call Transfer, between the local MXM and the neighboring zone or node.

➤ To allow H.450 Exchange functions to the neighboring zone

1. Double-click the neighboring zone and then click the Product Info tab.
   -or-
   Right-click the neighboring zone, point to Property and then click Product Info.

2. In the Product Info page, select MXM Transfer Model to allow Call Transfer to all nodes in the neighboring zone.

3. Select H.450.3 (Call Diversion services) to allow Call Forwarding to all nodes in the neighboring zone.

4. To implement the changes and close the dialog box, click OK.
To allow H.450 Exchange functions to a neighbor node

1. Double-click the neighbor node and then click the Product Info tab.
   -or-
   Right-click the neighbor node, point to Property and then click Product Info.

2. In the Product Info page, select MXM Transfer Model to allow Call Transfer to the neighbor node only.

3. Select H.450.3 (Call Diversion services) to allow Call Forwarding to the neighbor node only.

4. To implement the changes and close the dialog box, click OK.
Sharing Gateway and MCU Services with Other Zones

Gateway and MCU services from local and neighbor MXMs may be made available to nodes registered with the involved MXMs.

**Direct Gateway Service Dialing**

This method may be used for providing neighbor nodes with gateway services that are registered in the local MXM.

➤ **To set up direct gateway service dialing**

1. Right-click the neighbor zone, point to **Properties**, and then click **Gateway Services**. The **Gateway Services** tab appears.

2. Select a Gateway Service Hunting Group and bandwidth allocation policy (see page 156). To limit the gateway services available to neighbor nodes, you can even create a specific Gateway Service Hunting Group (see “Gateway Service Hunting Groups” on page 125).

3. Click **OK**.

*Dialing a Gateway Service*

To obtain a gateway service, the neighbor node must dial:

**[Zone Prefix]**[Gateway Access Number]**[ISDN number of remote party]**

For example, **4009334444**, where

400 is the prefix, 9 is the access number, and 334444 is the ISDN number.
9.5 Inter-Zone Videoconferencing Management

Direct MCU Service Dialing

This method may be used for providing neighbor nodes with MCU services that are registered in the local MXM. It is easy to set up but requires users to obtain the local MXM’s zone prefix and enter it while dialing.

➤ To set up direct MCU service dialing

1. Right-click the neighbor zone, point to Properties, and then click MCU Services. The MCU Services tab appears.

2. Select an MCU Service Permission Group. To limit the MCU services available to neighbor nodes, you can even create a specific Permission Group (see “MCU Service Permission Groups” on page 138).

3. Click OK.

Dialing an MCU Service

To obtain an MCU service, the neighbor node must dial:

[Zone Prefix][MCU's directory number]

For example, 4004444, where

400 is the prefix and 4444 is the MCU’s directory number.
9.5 Inter-Zone Videoconferencing Management

Adding Neighbor Gateways and MCUs to other MXMs

This method may be used for providing MXM nodes with gateway and MCU services that are registered in a neighboring zone. Listing gateways, MCUs, and their services under their neighboring zone in the Main View offers the following advantages:

- Users do not need to obtain and add zone prefixes when they dial.
- The listed services may be placed in Gateway Service Hunting Groups or MCU Service Permission Groups in the local MXM.

The available operations for setting up this situation are:

- Drag-and-drop
- Copy and paste
- Manually adding a gateway or MCU

To copy a gateway or MCU to a neighboring MXM

1. Log in to the MXM to which you want to make services available (see page 21).
2. Drag the gateway or MCU entry from your local MXM to the local MXM entry under the neighboring MXM’s Zones object.

-or-

Copy the gateway or MCU entry from your local MXM and paste it on the neighboring MXM’s Zones object.

Gateway and its Services Copied to another MXM

Dragging gateways and MCUs to your MXM’s corresponding zone in the neighboring MXM makes all their services available to nodes in the neighboring zone. If you do not want all the services available in the neighboring zone, create a Gateway Service Hunting Group, MCU Service Permission Group or delete the unwanted services.
To manually add a neighbor gateway or MCU to the local MXM

1. Right-click the neighboring zone, point to **Add Node to Zone**, and then click **Add Gateway** or **Add MCU**.

2. In the new node’s wizard, edit the node’s properties according to its configuration and your network specifications (for details, see “Setting Gateway Properties” on page 116 or “Setting MCU Properties” on page 129). Click **OK** to finish.

3. After adding the gateway or MCU, right-click it and then click **Add Service**. The New Service wizard appears.

4. Edit the service’s properties according to its configuration and your network specifications (for details, see “Setting Gateway Service Properties” on page 123 or “MCU Services” on page 133). Click **OK** to finish.

5. To add additional services, repeat step 4 as many times as necessary.

The neighbor gateway or MCU and its services are now listed in the local MXM.

The gateway may be dialed by MXM nodes simply by entering the gateway access number and the remote party’s ISDN number. The gateway’s services are now available for inclusion in Gateway Service Hunting Groups (see “Gateway Service Hunting Groups” on page 125).

**Neighbor Gateway and Service**

The MCU may be dialed by MXM nodes simply by dialing the MCU’s directory number. The MCU's services are now available for inclusion in MCU Service Permission Groups (see “MCU Service Permission Groups” on page 138).
10 Registering with LDAP Directories

10.1 Overview of LDAP

Online directories, such as Microsoft ILS Servers and Novell NDS, are lists of persons or network resources which include descriptive and contact information about all entries. They may be used to look up someone’s contact information or to retrieve a list of e-mail addresses. They are accessible through an Internet connection. The MXM supports access to online directories.

Using the Lightweight Directory Access Protocol (LDAP), MXM end points may locate any other person or node on a public X.500-based network (X.500 is a standard for directory services in a network). In such a network, directory information is consolidated in central servers located throughout the network. These servers coordinate their directory information so that each maintains an updated, current mail client directory.

An LDAP directory is usually organized in a "tree" hierarchy with levels of objects (similar to the System tree in the Main Administrator window). Each object in the hierarchy must have a unique name. An LDAP directory tree may consist of the following levels:

- The "root" directory (the starting place or the source of the tree)
- Countries
- Organizations (such as a company or government ministry)
- Organizational units (such as divisions and departments)
- Individuals (such as persons, files, and shared resources such as printers).
For example, a sample hierarchy may look like this:

![Sample LDAP Directory Hierarchy](image)

**Sample LDAP Directory Hierarchy**

An LDAP directory can be distributed among many servers. All of the LDAP servers may contain identical versions of the total directory which are synchronized periodically. An LDAP server that receives a request from a user may pass it to other servers as necessary, but ensures a single coordinated response for the user.

The MXM supports the following directory servers:

- Microsoft Internet Location Server (ILS)
- Microsoft Exchange Server
- Microsoft Window 2000 Active Directory
- Novell Directory Services (NDS)

You may register an MXM’s end points and various other nodes in more than one LDAP server directory. There are several reasons why an organization would make such an arrangement. For example, a company may create a list of all employees and another list in which senior managers are removed. The company can provide the first list to its managers, and preserve its managers’ online information by providing non-management employees with the latter list.

This chapter provides the configuration settings required for the MXM to register with the respective LDAP directories. For information and instructions for installing and working with these applications, see the specific application’s user guides.
10.2 Registering the MXM with an ILS

By supporting both Microsoft NetMeeting and Internet Location Server (ILS), the MXM can register with ILS servers, therefore providing its registered nodes with ILS services.

This section provides the required configuration information and values for registering the MXM and its users in the ILS.

To set up the MXM’s configuration in the ILS

1. Run the Microsoft Internet Information Server (IIS) application and open the Microsoft Management Console (MMC).
2. In the Console menu, click Add\Remove Snap-in. In the Add\Remove Snap-in dialog box, click Microsoft Information Server and then click Add. Click OK to confirm.
3. In the MMC, right-click LDAP and click Properties. The LDAP Service Properties appears. The following illustrations show suggested settings.

You may enter your own choices as the Anonymous Login User Name and Password (optional).

![Recommended LDAP Service Settings](image)
10.2 Registering the MXM with an ILS

Recommended LDAP ILS Server Settings

Recommended LDAP Advanced Settings
10.2 Registering the MXM with an ILS

4. To complete the configuration, you must perform the ILS Installation Verification.

In your web browser, enter the location http://IP address of local host/ils. Click the Installation Verification link.

Follow the onscreen instructions to complete the verification process.

Setting Up the ILS Configuration in the MXM Administrator

Finally, you have to set up the ILS configuration for the MXM in the MXM Administrator.

➤ To set up the ILS configuration in the MXM

1. In the Main view, expand the Templates group. Right-click Desktop (or other node type to be registered in the LDAP Server), point to Property, then MXM, and then click LDAP. In the Create an Entry in Server list, choose ILS and then click Apply.

   ![Template’s LDAP Properties](image)

   Template’s LDAP Properties

2. Click Show LDAP Servers. The LDAP Servers View appears.
3. Make sure that the following information appears in the table:

   - **Host address** - Exact host name or IP address of the LDAP server.
   - **Port** - **389**
   - **Refresh Connection Interval** - number of seconds. This value must be greater than **0** ("0" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
   - **Default Directory** - Folder as created in the ILS Server, reflecting the assigned organization ("o") and object class. For example, **o=Microsoft, objectClass=RTPerson**.
   - **Domain, User, Password** - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.
10.3 Registering the MXM with Microsoft Exchange Server

For systems using the Microsoft Exchange Server 5.5 for their messaging and collaboration, the MXM is compatible. The Exchange Server sets up directories in the form of a tree-like hierarchy (see the illustration on page 182). For example, your company may be the top of the tree, the next level may be an organization unit such as the MXM, Sales or Administration, and the next level may be individual Recipients, such as individual end points.

This section provides the required configuration information and values for registering the MXM and its users in a Microsoft Exchange Server.

To be listed, a Recipient must already have an open account in the Microsoft Exchange Server.

➤ To add MXM users to the Exchange Server

1. Run the Microsoft Exchange Administrator application and connect to a server.

2. In the Administrator tree, click the Organizational Unit (such as MXM) under which the users will be listed.

3. In the File menu, point to New Other and click Recipients Container. The Recipient’s Properties dialog box appears.

4. In the General tab, enter a Display Name for the Recipient and the Directory Name under which the Recipient will appear on the tree.

   In the Permissions tab, the name of the MXM appears as the source of the Recipient’s various conferencing privileges.

5. In the Administrator tree, expand the MXM’s Configuration object. Click Protocol to display available protocol entries.

6. Double-click LDAP (Directory) Site Defaults. The following illustrations show suggested settings.
Set your firewall to permit anonymous access to and from the directory.
10.3 Registering the MXM with Microsoft Exchange Server

LDAP Site Defaults Search Properties

For the **Maximum Number of Search Results**, enter a value equaling *(number of registered users + 10).*

LDAP Site Defaults Idle Timeout Properties
10.3 Registering the MXM with Microsoft Exchange Server

Setting Up the Exchange Server Configuration in the MXM Administrator

Finally, you have to set up the Exchange Server configuration for the MXM in the MXM Administrator.

➤ To set up the Exchange Server configuration in the MXM

1. In the Main view, expand the Templates group. Right-click Desktop (or other node type to be registered in the LDAP Server), point to Property, then MXM, and then click LDAP. In the Create an Entry in Server list, choose Exchange and then click Apply.

![Image of MXM Administrator's interface]

Template’s LDAP Properties

2. Click Show LDAP Servers. The LDAP Servers View appears.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Server Name</th>
<th>Host Address</th>
<th>Host Port</th>
<th>Refresh Connection Interval</th>
<th>Default Directory</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILS</td>
<td>Default_ILS</td>
<td>209</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange</td>
<td>Default_Exchange</td>
<td>209</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MRS</td>
<td>Default_MRS</td>
<td>509</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDS</td>
<td>Default_NDS</td>
<td>509</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MXM2000</td>
<td>Default_MXM</td>
<td>209</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDS</td>
<td>Default_SiteServer_ILS</td>
<td>1002</td>
<td>0</td>
<td>DefaultDomain</td>
<td>Default User</td>
<td>**********</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LDAP Servers View
3. Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - 389
- Refresh Connection Interval - number of seconds. This value must be greater than 0 (“0” indicates that there is no connection with the LDAP server). The recommended value is 30 (seconds).
- Default Directory - Folder as created in the Exchange Server, reflecting the assigned organization (“o”), organizational unit (“ou”) and additional levels in the hierarchy (“cn”, or common name). For example, “cn=recipients, ou=Site_Name, o=Default_Organization_Name”.
- Domain - Domain of the Exchange Server.
- User - Valid user in the Exchange Server domain, with access rights to its MXM default directory
- Password - Password as defined in the Exchange Server.

To edit an entry, click in the relevant cell(s), then delete and type.
10.4 Registering the MXM with Windows 2000 Active Directory

The MXM supports Microsoft Windows 2000 Active Directory, which sets up directories in schemas. The schemas are made up of sublevels called classes. Each class is made up of uniquely named attributes.

In the Active Directory Console, you must expand its schema by creating a new class titled “MXMNode” and then create new attributes for the MXM with specific names.

This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in an Active Directory Server. To perform the tasks, you must open the Active Directory Console. Then, follow the series of procedures in this section.

Adding an Administrator with Full Configuration Rights

To extend the schema, you have to give full control (read and write permissions) to a user from the Schema Admin group. As a result, this user becomes an Administrator.

Then, add a new Active Directory schema snap-in.

These tasks are basic Active Directory functions. If necessary, refer to the Active Directory documentation for instructions.
Adding the MXM Attributes

You have to add specific attributes, or characteristics, for MXM objects to the snap-in.

➢ To add MXM attributes to the snap-in

1. In the **Active Directory Schema** snap-in on the left side of the Active Directory Console, right-click the **Attributes** folder and then click **Create Attribute**.

![Create New Attribute dialog box](image)

*Creating New MXM Attributes*

2. In the Create New Attribute dialog box, type identical names in the **Common Name** and the **LDAP Display Name** boxes.

   In the **Unique X500 Object ID** box, type the OID of the attribute.

   The table following this procedure contains the required attribute names and their respective OIDs. Enter them as they appear in the table.

3. In the **Syntax** list, select **Case Insensitive String**.

4. Click **OK**.
5. Repeat this procedure for all the attributes in the following table.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXMTelephonyStateDescription</td>
<td>1.2.840.113556.1.8000.35.1.10.2</td>
</tr>
<tr>
<td>MXMUserType</td>
<td>1.2.840.113556.1.8000.35.1.10.3</td>
</tr>
<tr>
<td>MXMBChannelNum1</td>
<td>1.2.840.113556.1.8000.35.1.10.4</td>
</tr>
<tr>
<td>MXMBChannelNum2</td>
<td>1.2.840.113556.1.8000.35.1.10.5</td>
</tr>
<tr>
<td>MXMBChannelNum3</td>
<td>1.2.840.113556.1.8000.35.1.10.6</td>
</tr>
<tr>
<td>MXMBChannelNum4</td>
<td>1.2.840.113556.1.8000.35.1.10.7</td>
</tr>
<tr>
<td>MXMBChannelNum5</td>
<td>1.2.840.113556.1.8000.35.1.10.8</td>
</tr>
<tr>
<td>MXMBChannelNum6</td>
<td>1.2.840.113556.1.8000.35.1.10.9</td>
</tr>
<tr>
<td>MXMRestricted56k</td>
<td>1.2.840.113556.1.8000.35.1.10.10</td>
</tr>
<tr>
<td>MXMVideoSupport</td>
<td>1.2.840.113556.1.8000.35.1.10.11</td>
</tr>
<tr>
<td>MXMAudioSupport</td>
<td>1.2.840.113556.1.8000.35.1.10.12</td>
</tr>
<tr>
<td>MXMInCall</td>
<td>1.2.840.113556.1.8000.35.1.10.13</td>
</tr>
<tr>
<td>MXMH323Alias</td>
<td>1.2.840.113556.1.8000.35.1.10.14</td>
</tr>
<tr>
<td>MXMDeskTopUserDataNotes</td>
<td>1.2.840.113556.1.8000.35.1.10.15</td>
</tr>
</tbody>
</table>
Adding the MXMNode Class

You must now create an MXMNode class, to which you will later add the attributes you created in the previous section.

➤ To create the MXMNode class

1. In the Active Directory Schema snap-in on the left side of the Active Directory Console, right-click the Classes folder and then click Create Class.

![Create New Schema Class](image)

Creating the MXMNode Class

2. In the Create New Schema Class wizard, type **MXMNode** in the Common Name and the LDAP Display Name boxes.

3. In the Unique X500 Object ID box, type `1.2.840.113556.1.8000.35.1.10.1` as the OID of the attribute.

4. In the Parent Class box, enter **organizationalPerson**.

5. In the Class Type list, select **Structural**.

6. Click Next.
10.4 Registering the MXM with Windows 2000 Active Directory

Adding MXM Attributes to MXMNode Class

7. Next to the **Optional** list, click **Add**.

Selecting MXM Attributes for the MXMNode Class

8. In the Select Schema Object dialog box, select all the new MXM attributes and click **OK**.
9. Right-click the MXMNode Class object on the left side of the Active Directory Console, and then click Properties. In the Properties dialog box, click the Relationship tab.

MXMNode Class Relationship

10. Opposite the Possible Superior box, click Add.
11. In the Select Schema Object dialog box, select an Organizational Unit and then click **OK**.

*Selecting an Organizational Unit for the MXMNode Class*

The MXMNode class is now contained inside the selected Organizational Unit.
10.4 Registering the MXM with Windows 2000 Active Directory

Granting Full Control for the MXMNode Class to an Active Directory User

To work with the newly created MXMNode class, create an Active Directory User account with Administrator privileges.

1. Right-click the MXMNode Class object on the left side of the Active Directory Console, and then click Properties. In the Properties dialog box, click the Security tab.

2. In the Names list, select the user and then select Full Control in the Allow column. Click OK.

Granting Full Control Privileges to an Active Directory User
10.4 Registering the MXM with Windows 2000 Active Directory

Setting the Properties of the MXM Attributes

In this procedure, you must assign specific properties to all the MXM attributes.

➤ To set the properties of the MXM attributes

1. In the Attributes folder, right-click an MXM attribute and then click Properties.

![Setting MXM Attribute Properties](image)

2. In the Description box, enter the identical name of the attribute.

3. Select the following options:
   - Show objects of this class while browsing
   - Replicate this attribute to the Global Catalog

4. Click OK.
10.4 Registering the MXM with Windows 2000 Active Directory

Creating an Organizational Unit for Your MXM

At this time, create a new Organizational Unit which will be your MXM’s working folder in the LDAP server.

➤ To create your MXM’s Organizational Unit

1. Expand the Active Directory Users and Computers snap-in on the left side of the Active Directory Console. Right-click the LDAP Server object, point to New and then click Organizational Unit.

2. In the Name box, type MXMWorkingFolder.

3. Click OK.
10.4 Registering the MXM with Windows 2000 Active Directory

Setting Up the LDAP Configuration in the MXM Administrator

Finally, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1. In the MXM Administrator, click the LDAP Servers View button.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Server Name</th>
<th>Host Address</th>
<th>Host Port</th>
<th>Refresh Connection Interval</th>
<th>Default Directory</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange</td>
<td>Exchange</td>
<td>Default_Exchange_Server</td>
<td>389</td>
<td>0</td>
<td>cn=Microsoft.objectClass=RTPeer</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>NSD</td>
<td>NSD</td>
<td>Default_NS_D_Server</td>
<td>389</td>
<td>0</td>
<td>ou=MXM,dc=servername,dc=com</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>W2K2000</td>
<td>W2K</td>
<td>Default_W2K_Server</td>
<td>389</td>
<td>0</td>
<td>cn=organisation.Unt,dc=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>ILS</td>
<td>ILS</td>
<td>Default_ILS</td>
<td>389</td>
<td>0</td>
<td>cn=Microsoft.objectClass=RTPeer</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>ILS</td>
<td>ILS</td>
<td>Default_ILS</td>
<td>389</td>
<td>0</td>
<td>cn=Microsoft.objectClass=RTPeer</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>ILS</td>
<td>ILS</td>
<td>Default_ILS</td>
<td>389</td>
<td>0</td>
<td>cn=Microsoft.objectClass=RTPeer</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
<tr>
<td>ILS</td>
<td>ILS</td>
<td>Default_ILS</td>
<td>389</td>
<td>0</td>
<td>cn=Microsoft.objectClass=RTPeer</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td></td>
</tr>
</tbody>
</table>

**LDAP Servers View**

2. Make sure that the following information appears in the table in the W2K row:
   - Host address - Exact host name or IP address of the LDAP server.
   - Port - 389
   - Refresh Connection Interval - number of seconds. This value must be greater than 0 ("0" indicates that there is no connection with the LDAP server). The recommended value is 30 (seconds).
   - Default Directory - Path as created in the Active Directory tree, reflecting the assigned organizational unit ("ou") and domain controls. For example, "ou=MXMWorkingFolder,dc=servername,dc=com".
   - Domain - keep this space blank.
   - User - Active Directory User with Administrator rights, as defined in "Granting Full Control for the MXMNode Class to an Active Directory User" on page 199. For example, "su,cn=users,dc=server_name,dc=com".
   - Password - Password for this user as defined in the Active Directory application.

To edit an entry, click in the relevant cell(s), then delete and type.
10.5 Registering the MXM with Novell Directory Services (NDS)

The MXM is compatible with Novell NDS® scalable LDAP directory services. The NDS sets up directories in schemas and hierarchies.

NDS hierarchies are made up of sublevels called classes. Each class is made up of uniquely named objects.

We recommend that you register your MXM and its registered users either during NDS installation or while the MXM is shut down. You must expand its schema by creating a new class titled “MXMNode” and then create new attributes for the MXM with specific names.

This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in an NDS LDAP Server. Follow the series of procedures.
Creating MXM Attributes

First, you have to add specific attributes, or characteristics, for MXM objects.

➤ To create MXM attributes

1. Run the NDS management application.
2. In the **Object** menu, click **Schema Manager**.
3. In the Schema Manager, click **Attributes**.

4. To make a new attribute, click **Create**. The Create Attribute wizard appears.
5. In the **Attribute Name** box, type the exact name of the attribute and click **Next**.
6. In the **Syntax** List, select a value that describes the way that item may be written or requested in the directory service. For working with the MXM, select **Case Ignore String** and click **Next**.

**Selecting a Syntax**
7. As flags, select **Single valued** and **Public read**. Click **Next**.

![Create Attribute](image)

**Selecting Flags**

8. Click **Next** until the last page of the wizard, keeping the default values for the new attribute. In the last page, click **Finish**.

9. Repeat steps 3 - 8, setting identical properties as specified, for the following attribute names.

<table>
<thead>
<tr>
<th>MXMIPAddress</th>
<th>MXMBChannelNum2</th>
<th>MXMRestricted56k</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXMTelephonyStateDescription</td>
<td>MXMBChannelNum3</td>
<td>MXMVideoSupport</td>
</tr>
<tr>
<td>MXMUserType</td>
<td>MXMBChannelNum4</td>
<td>MXMAudioSupport</td>
</tr>
<tr>
<td>MXMNotes</td>
<td>MXMBChannelNum5</td>
<td>MXMInCall</td>
</tr>
<tr>
<td>MXMBChannelNum1</td>
<td>MXMBChannelNum6</td>
<td></td>
</tr>
</tbody>
</table>
Creating the MXMNode Class

You must now create an MXMNode class based on the default super class named User. Attribute flags and rules will be inherited from the super class.

**CAUTION** Do not make changes to the NDS default schemas. Otherwise, the LDAP functions of the MXM may be affected.

➢ To create the MXMNode class

1. In the Object menu, click Schema Manager. Click Create to open the Create Class wizard.

2. In the Class Name box, type **MXMNode** as the exact name of the class and click Next.

![Create Class](image)

**Entering Class Name**

3. As the Class flag, select **Effective Class** (for creating instances from this class) and then click Next.
10.5 Registering the MXM with Novell Directory Services (NDS)

**Selecting Class Flag**

4. From the **Available Classes** list, choose **User** as the existing class from which the new class will inherit attributes. Click **Next**.

**Inheriting Attributes from Existing Classes**
5. In the **Available Attributes** list, do not add mandatory attribute(s) for the new class. By default, the class already includes the attributes **CN**, **Object Class** and **Surname**. Click **Next**.

![Create Class](image)

**Selecting Mandatory Attributes**

6. Choose optional attribute(s) for the new class. From the **Available Attributes** list, choose all the attributes that you created earlier in this procedure (named **MXM**...). Click **Next**.
Selecting the Optional Attributes

7. For the naming attributes, click **Next** without adding more attributes. For the Container Classes, click **Finish** without adding more classes.

8. Restart the server and then run the NDS management application again.

Creating an MXM Container

A separate container on the NDS Services tree keeps the MXMNode objects apart from the other NDS objects.

➤ **To create a separate MXM container**

1. Select the organization or organizational unit to which you want to place the MXMNode class and its objects.

2. Right-click, point to **New** and then click **Organizational Unit**.

3. Type **MXM** as the Organization Unit’s name and click **OK**.
Setting Up the LDAP Group Object Configuration

The LDAP Group contains the class and attribute mappings and security policies for one or more LDAP servers. If you plan to use the same configuration on more than one LDAP server, it’s easier to set up one LDAP Group object and assign it to each LDAP server in the LDAP Group Server List Properties.

To set up the LDAP Group Object configuration

1. In the container that holds the NetWare Server object, double-click LDAP Group.

2. In the LDAP Properties General tab, select Allow Clear Text Passwords. This option enables the exchange of passwords over nonencrypted connections, and is required for the MXM’s normal operation with the NDS Service.

3. Click the Attribute Map tab, where you will map the NDS schema names of the new MXM attributes (created in the section, “Creating MXM Attributes” on page 204) to corresponding LDAP names.
4. Click **Add**. In the Attribute Mapping dialog box, choose a new MXM attribute from the **NDS Attribute** list. Enter that same name into the **LDAP Attribute** box and click **OK**.

Repeat this step for all new MXM attributes.

**Mapping the MXM Attributes to LDAP Attributes**

The new MXM attributes are now part of the LDAP Group configuration.

5. Click **OK** and restart the server and then run the NDS management application again.
Adding a Trustee for the MXMNode Container

To use the MXMNode container, you have to set up a user with rights for creating and updating objects in the container. Other than the administrator with Super User privileges, who has full rights on the whole NDS Service tree, it is recommended to designate an MXM user as a Trustee, who has rights for creating and deleting objects in the MXMNode container.

To add a trustee for the MXMNode container

1. Right-click the MXMNode organizational unit, point to Trustees of this object and then click Add Trustees.
2. Browse the NDS tree to find the MXM user that will be the trustee and click OK.
3. For this user’s Entry Rights and Attribute Rights, select Create and Delete (if you want, you can select additional rights).
4. Click OK.
Setting Up the LDAP Configuration in the MXM Administrator

Finally, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1. In the MXM Administrator, click the **LDAP Servers View** button.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Server Name</th>
<th>Host Address</th>
<th>Host Port</th>
<th>Refresh Connection Interval</th>
<th>Default Directory</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNS</td>
<td>Default_LNS</td>
<td>389</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>NDS</td>
<td>Default_NDS</td>
<td>389</td>
<td>0</td>
<td>Default</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>MVMX2000</td>
<td>MVMX2000</td>
<td>389</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>ILX</td>
<td>Default_ILX</td>
<td>389</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>LNS</td>
<td>Default_LNS</td>
<td>389</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>Exchange</td>
<td>Exchange</td>
<td>389</td>
<td>0</td>
<td>Default</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>MVMX2000</td>
<td>MVMX2000</td>
<td>389</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>Site Server</td>
<td>Default_Site Server</td>
<td>1102</td>
<td>0</td>
<td>0</td>
<td>Domain</td>
<td>Default</td>
<td>User</td>
<td>Password</td>
</tr>
</tbody>
</table>

**LDAP Servers View**

2. Make sure that the following information appears in the table:
   - **Host address** - Exact host name or IP address of the LDAP server.
   - **Port** - 389
   - **Refresh Connection Interval** - number of seconds. This value must be greater than 0 ("0" indicates that there is no connection with the LDAP server). The recommended value is 30 (seconds).
   - **Default Directory** - Path as created in NDS Tree, reflecting the assigned organization ("o") and organizational unit ("ou"). For example, "ou=MXM, o=vcon".
   - **Domain** - keep this space blank.
   - **User** - Valid user in the Exchange Server domain, with access rights to its MXM default directory. For example, "su, ou=MXM, o=vcon".
   - **Password** - Password as defined in the NDS.

To edit an entry, click in the relevant cell(s), then delete and type.
10.6 Registering the MXM with ILS on Windows 2000

Site Server ILS on Windows 2000 is a service used for publishing H.323 videoconferencing and telephony users and IP multicast conferences on the network. Site Server ILS may be installed during Microsoft Windows 2000 Server setup.

When registering the MXM with Site Server ILS and subsequent listing of users, Site Server ILS’ default configuration is suitable.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with Site Server ILS, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1. In the MXM Administrator, click the LDAP Servers View button.

2. Make sure that the following information appears in the table:
   - Host address - Exact host name or IP address of the LDAP server.
   - Port - 1002
   - Refresh Connection Interval - number of seconds. This value must be greater than 0 (“0” indicates that there is no connection with the LDAP server). The recommended value is 30 (seconds).
   - Default Directory - Path as created in the Site Server directory tree, reflecting the assigned object class. For example, “objectClass=RPerson”.
   - Domain, User, Password - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Server Name</th>
<th>Host Address</th>
<th>Host Port</th>
<th>Refresh Connection Interval</th>
<th>Default Directory</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILS</td>
<td>ILS Server</td>
<td>Default_IIS_Server</td>
<td>1002</td>
<td>0</td>
<td>objectClass=RPerson</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>Exchange</td>
<td>Exchange</td>
<td>Default_Exchange</td>
<td>1002</td>
<td>0</td>
<td>ou=Microsoft,ou=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>NDS</td>
<td>NDS Server</td>
<td>Default_NDS_Server</td>
<td>1002</td>
<td>0</td>
<td>ou=Microsoft,ou=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows</td>
<td>Default_Windows</td>
<td>1002</td>
<td>0</td>
<td>ou=Microsoft,ou=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>ILS</td>
<td>ILS Server</td>
<td>Default_IIS_Server</td>
<td>1002</td>
<td>0</td>
<td>objectClass=RPerson</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>Exchange</td>
<td>Exchange</td>
<td>Default_Exchange</td>
<td>1002</td>
<td>0</td>
<td>ou=Microsoft,ou=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows</td>
<td>Default_Windows</td>
<td>1002</td>
<td>0</td>
<td>ou=Microsoft,ou=Default</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
<tr>
<td>Site Server</td>
<td>Site Server</td>
<td>Default_Site_Server</td>
<td>1002</td>
<td>0</td>
<td>objectClass=RPerson</td>
<td>Default_Domain</td>
<td>Default_User</td>
<td>**********</td>
</tr>
</tbody>
</table>
10.7 Registering the MXM with Netscape Directory Server

Netscape Directory Server provides an embeddable, extensible directory for users of a company’s extranet or e-commerce site.

This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in a Netscape Directory Server. Follow the procedure below (for more details about setting up Organizational Units, see the Netscape Directory Server user documentation).

➤ To set up the MXM’s configuration in the Netscape Directory Server

1. Run the Netscape Console.

2. From the folder tree in the left pane of the console, open the Directory Server.

Netscape Console
3. In the Directory Server, expand the tree.

4. Create a new Organizational Unit (for example, companyname.co.il).

5. Set access permissions for one user that has full read-write privileges for the LDAP configuration.

6. Add the organization’s users under the Organizational Unit. Create relevant branches in accordance to your organization’s departmental structure or other organizational criteria.

*Netscape Directory Server*
Setting Up the LDAP Configuration in the MXM Administrator

After registering with the Netscape Directory Server, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1. In the MXM Administrator, click the **LDAP Servers View** button.

2. Make sure that the following information appears in the table:

   — Host address - Exact host name or IP address of the LDAP server.
   — Port - 389
   — Refresh Connection Interval - number of seconds. This value must be greater than 0 (“0” indicates that there is no connection with the LDAP server). The recommended value is 30 (seconds).
   — Default Directory - Path as created in Network Directory Server, reflecting the assigned organization (“o”) and organizational unit (“ou”). For example, “ou=MXM, o=yourcompany.com”.
   — Domain, User, Password - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.
11 INITIATING VIDEOCONFERENCES FROM THE MXM ADMINISTRATOR

11.1 Administrator-Initiated LAN Dialing

As a system administrator with Super User or Monitor/View privileges, you can initiate a point-to-point videoconference by connecting two end points listed in the Administrator’s Main View. Calls may also be initiated to end points in neighboring zones.

➤ To initiate a point-to-point call through the Administrator

1. Select the parties for the videoconference.
2. Right-click and then click Initiate point-to-point call.
3. Make any changes required in the call properties. Otherwise, leave the default settings. For a description of the properties, see “Setting Point-to-Point Videoconference Properties” on page 220.
4. Click Initiate Call.

![Initiate Point-to-Point Call](image)

Initiating a Point-to-Point Videoconference
Setting Point-to-Point Videoconference Properties

If necessary, change point-to-point videoconference properties before connecting the two end points.

- **Call Name**: Name of the videoconference. This name will identify this call in the CDR.
- **Party #1; Party #2**: The two end points in the videoconference.
- **Initiating Entity**: End point that dials to initiate the videoconference.
- **Call Bandwidth**: Maximum bandwidth allocated for the videoconference.
- **Call Status Display in Node Status View**: Select **Show Call Status in Tab** to display the call status in the Node Status View in a specific tab. The name or description listed here is also listed on the tab.
- **Select Don’t show Call Status in Node Status View** if you don’t want to monitor the videoconference in the Node Status View.

## 11.2 Administrator-Initiated ISDN Dialing

To initiate an ISDN videoconference through the Administrator:

1. Select the initiating party of the videoconference.
2. Right-click and then click **Initiate ISDN call**.
3. Set the call properties, including the ISDN numbers of the receiving party. For a description of the properties, see “Setting ISDN Videoconference Properties” on page 221.
4. Click **Initiate Call**.

If the call is successful, a notification, “In ISDN Call: [n] kbps” appears in the Main View next to the calling station’s entry, where n indicates the call’s bandwidth.
11.2 Administrator-Initiated ISDN Dialing

Initiating an ISDN Videoconference

Setting ISDN Videoconference Properties

Set ISDN videoconference properties before initiating the call.

**Call Name**  
Name of the videoconference. This name will identify this call in the CDR.

**Initiating End Point**  
End point that dials to initiate the videoconference.

**Phone Numbers**  
The ISDN phone numbers to dial. Enter numbers corresponding to the number of lines and amount of bandwidth that the call will require.

**Bonding**  
Click to make this conference a Bonding call. Bonding combines multiple ISDN lines into a single channel, effectively strengthening the signal.

**Restricted**  
Select if the connection is over a Restricted network, which uses 56K switches (instead of 64K).

**Loopback**  
Click to initiate a call to the end point’s own ISDN lines. A loopback tests if the ISDN lines are functioning normally.
11.3 Administrator-Initiated Hang Up

As a system administrator with Super User privileges, you can hang up open calls that include selected users or users within a selected group. For example, if more than one user in the Sales Administrative group are involved in videoconferences but you have to terminate all of that group’s calls, select the Sales Administrative group object.

Although administrators with Monitor/View privileges may initiate videoconferences, they cannot hang up calls.

To hang up calls through the Administrator

1. Select the end point(s) or group object that includes the users that you want to disconnect.

2. In the toolbar, click the Hang Up Calls button.

All calls involving the selected users are therefore disconnected.
12 Setting Up Multipoint Videoconferences Managed by a VCB

The VCB is available only for licensed users of the VCON Conference Bridge Option. If you want to add this option to your MXM, please contact your local VCON distributor.

12.1 Overview of the VCON Conference Bridge

The VCON Conference Bridge (VCB) is an MCU that enables:

- Initiation and management of an ad-hoc videoconference, which is a multipoint videoconference that was expanded from a point-to-point conference by one of the conference's parties.
- End points to dial into a predefined multipoint videoconference.
- Simultaneous multicast streaming of active conferences to multiple participants.
12.1 Overview of the VCON Conference Bridge

The conference’s video may be displayed by one of the following methods:

- **Voice-Activated Switching** The participants see the video of the participant whose audio signal is strongest. For example, the non-speaking participants see the person speaking.

- **Continuous Presence** Several participants in a multipoint conference are viewed and heard simultaneously.

For instructions on installing the VCB, see “Installing the VCON Conference Bridge” on page 16.

The VCB provides the following features and capabilities:

- Up to 64 concurrent participants, depending on the audio codec used by the sessions.
  - Up to 64 participants (8x8, 4x16, 2x32, 1x64, or mixture) in all sessions using G.711 audio.
  - Up to 32 participants (4x8, 2x16, 1x32, or mixture) in all sessions using G.722 audio or mixed G.711/G.722.

- Up to 1.5 Mbps data rate per participant in Voice-activated Switching
  Up to 384 Kbps data rate per participant in Continuous Presence.

- Dial-in conference initiation.

- Simultaneous streaming of active multicast conferences.

- Support for sessions including H.323 end points/devices and SIP User Agents (through the MXM's embedded SIP proxy server).

- Multi-point sessions can be joined (cascaded) onto other sessions, contingent on similar data rates, display types, and audio/video algorithm.
  - VCB to VCB
  - VCB to other

- G.722 audio support with transcoding (G.711).

- Dynamic resource allocation pool – Unallocated ports may be used as overflow for configured sessions.
12.2 Logging in a New VCB

➤ To register a VCB to the MXM

1. In the VCB computer’s Windows desktop, click Start, point to Programs, VCON and VCB, and then click Update MXM Address.

2. Enter the IP address of the MXM and click OK.

Entering the MXM’s IP Address

If the MXM is in Open Mode, the VCB automatically logs in, and appears under the VCON Conference Bridges object. Services appear under the VCB. To edit VCB properties, see “Setting VCB Properties” on page 227. To edit Services properties, see “Setting VCB Services Properties” on page 232.

If the MXM is in Closed Mode for MCUs, a Login Request notification will appear on the Administrator tree after several seconds. To complete the Setup process, proceed to step 3.

3. Expand the Login Request item.

Login Request Notification for VCB
4. Right-click the VCB name and then click **Grant Login Permission**.

A message appears, asking if you want to register the VCB now.

![VCB Registration Request](image)

**VCB Registration Request**

5. Click **OK** if you want to manually set the VCB’s properties, such as Firewall ports. The New VCB Wizard appears. The original property values are the default values defined in the VCON Conference Bridge template (see “Setting Up Templates” on page 54).

If you click **Cancel**, the VCB does not log in, but remains under the Login Requests object until you delete it (and the VCB stops trying to log in). See “Deleting a Login Request” on page 38.

6. Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see “Setting VCB Properties” on page 227.

7. When you finish the last page, click **Finish**.

8. In the Create VCB Services dialog box, you can choose to add VCB Services now or to add them later.

![Decision to Add VCB Services Now or Later](image)
12.3 Setting VCB Properties

I want to add the services now
Set up the VCB Services during this registration process.

In the Number of Services to Add box, type the number of VCB Services that you want to set up.

Set up the new services now
Select to set up the configurations for the new services now.

The New VCB Service wizard appears. Set properties as required. For more information about the VCB Service properties, see “Setting VCB Services Properties” on page 232.

Create the Services Using the Template Settings
Select to set up the configurations for the new services based on the VCB Service template.

The new services will appear automatically in the Main View under the VCON Conference Bridge object.

I Will Add the Services Later
Select to add the VCB to the Main View without services at this time. You may add services later.

Click OK.

In the Main View, the VCB appears under the VCON Conference Bridges object. If you added services in Step 8, they appear under the VCB.

12.3 Setting VCB Properties

In step 6 of “Logging in a New VCB” on page 226, the Add Wizard provided the chance to change various VCB properties. VCB Properties define network and location information for the VCB. This section describes these properties.

Any changes will take effect for the next VCB session.
12.3 Setting VCB Properties

General

The **General** tab contains identity information of the VCB.

![VCB - General Properties](image)

### VCB - General Properties

In the **General** Properties tab, the following properties appear:

- **Description**: Identity of the VCB. This name will appear in the Main View after the login process is finished.

- **H.323 Address**
  - **Alias**: The VCB’s alias name.
  - **Type**: The type of address used by the VCB for registering with the MXM.

- **Network Address**: IP address of the VCB.

- **Build Number**: Version information for the VCB.
License

The License tab shows the details of your VCB license key. If you need to increase these numbers, contact your local VCON distributor.

![VCB - License Properties](image)

**Licensed Ports**
Maximum number of concurrent participants that may be serviced by in this VCB.

**Ports in Call**
Number of participants that are engaged in active videoconferences managed by this VCB.

**License Key**

**Export Key**
To purchase a license for more ports, click Export Key to create a license file for the VCB on its host computer. Send the file to your local VCON distributor. You will then receive an updated license key.

**Show Key**
Click to view the key code for the current VCB installation.

**New Key**
After receiving a new license file from your VCON distributor, click this button, browse to select the file and click Open. When prompted to apply the license code, click OK. To implement the license change and close the dialog box, click OK again.
12.3 Setting VCB Properties

Firewall

In the Firewall tab, enter the allocation of ports for communication through your organization’s firewall.

![Firewall Properties](image)

**VCB - Firewall Properties**

- **RTP & RTCP Port Range**
  
  The MXM allocates a range of ports for video and audio during videoconferences. The value indicates the lowest port number allowed.

  This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

- **H.245 Port Range**
  
  The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences. The value indicates the lowest port number allowed.

  This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

- **Defaults**
  
  Click this button to return to the default settings.
Product Info

The **Product Info** tab provides information about the VCB’s manufacturer and model. In addition, you can enable or disable the exchange functionalities supported for multipoint videoconferences through the VCB.

---

**Vendor ID**

Identity of the manufacturer.

**Product ID**

Manufacturer's identity of the product.

**Version ID**

Manufacturer's version identification of the product.

**Location**

Physical location of the VCB.

**Add New Services to this Group**

If a new VCB service is added to this VCB’s configuration, it will automatically be included in the MCU permission group selected here. To avoid adding services to permission groups automatically, select **No Group**.
12.4 Setting VCB Services Properties

VCB Services define the usage of resources used during a multipoint videoconference managed by the VCB.

After the VCB's installation and restart of the VCB's computer, you can add or edit service entries under the Video Conference Bridge object. One directory (E.164) number is created for each service type.

➤ To add VCB Services

1. Right-click the VCB and then click New Service. The New VCB Service wizard appears.

2. Change properties according to your ad-hoc videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click Next. For explanations about the various properties, see the following subsections.

3. When you finish the last page, click Finish.

The following subsections describe the VCB Service properties.
12.4 Setting VCB Services Properties

General

In the **General** page, enter identity information of the new VCB Service.

![General Properties](image)

**VCB Service - General Properties**

In the **General** Properties tab, the following properties appear:

- **Directory Number**: Number to be dialed for using this service.
- **Description**: Name of the service. This name will appear in the Main View after the login process is finished.
- **H.323 Address**
  - **Alias**: The service’s alias.
  - **Type**: The type of address used by the VCB for registering the service with the MXM.
  - **Additional IDs page**: Click this link to view any additional IDs that have been configured for this service.
- **Network Address**: IP address of the VCB.
Ad-Hoc Conference

A point-to-point conference becomes an ad-hoc conference when additional end points are "invited" by one of the parties and they join the session. In the **Ad-hoc Conference** page, define if the selected VCB Service can be used for expanding to ad-hoc conferences.

**VCB Service - Ad-hoc Conference Properties**

- **Use this service as an ad-hoc conference resource**
  
  This service is available for use when expanding to an ad-hoc videoconference.

- **Use this service exclusively for ad-hoc conferences**
  
  This service is available only for use in ad-hoc videoconferences, and unavailable for point-to-point sessions.

- **Ad-hoc Resources page**
  
  Click this link to open the MXM’s Ad-hoc Resources Properties, in which you can also select other VCB Services that may be used for ad-hoc videoconferences (see “Ad-hoc Resources” on page 81).
Session

In the **Session** page, define the configuration for multipoint sessions initiated with this service.

### Participants

**Limit Number of Participants to**

The maximum number of concurrent calls allowed in this session. Selecting this option also enables you to reserve ports for the defined number of users.

- The VCB supports up to 64 concurrent participants, depending on the audio codec used by the sessions.

  - Up to 64 participants (8x8, 4x16, 2x32, 1x64, or mixture) in all sessions using G.711 audio
  - Up to 32 participants (4x8, 2x16, 1x32, or mixture) in all sessions using G.722 audio or mixed G.711/G.722

If this option is not selected, the number of users that can participate in this session is limited to the number of free ports. However, no ports are reserved specifically for this session.
### 12.4 Setting VCB Services Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reserve VCB Ports</strong></td>
<td>Only available if the <strong>Limit Number of Participants</strong> option is selected.</td>
</tr>
<tr>
<td></td>
<td>The VCB reserves an equal number of ports as the number of maximum users in this session. For example, if the session is limited to a maximum of 8 participants, the VCB will reserve 8 ports. None of those ports will be available for other sessions.</td>
</tr>
</tbody>
</table>

#### Switching Mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voice Activated Switching</strong></td>
<td>The participants see the video of the participant whose audio signal is strongest. For example, the non-speaking participants see the person speaking.</td>
</tr>
<tr>
<td><strong>Continuous Presence</strong></td>
<td>Several participants in a multipoint conference are viewed and heard simultaneously.</td>
</tr>
</tbody>
</table>

#### Video

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td>The video codec (<strong>H.261, H.263</strong>) used in the multipoint conference.</td>
</tr>
<tr>
<td></td>
<td>Continuous Presence only supports H.261.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>The size of the transmitted video images:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CIF</strong> (Common Interchange Format), or normal size</td>
</tr>
<tr>
<td></td>
<td>• <strong>QCIF</strong> (Quarter Size Common Interchange Format), or quarter size</td>
</tr>
<tr>
<td></td>
<td>In Continuous Presence, the local side transmits QCIF video and receives CIF video.</td>
</tr>
</tbody>
</table>

#### Bandwidth

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bandwidth available for each party in the multipoint conference.</td>
</tr>
</tbody>
</table>

Click **Default** to restore the system’s default Session configuration.
12.4 Setting VCB Services Properties

Multicast

In the **Multicast** page, enable this service to support VCON's Interactive Multicast.

![Multicast Properties](image)

**VCB Service - Session Properties**

- **Enable Multicast for this Session**: Select to enable this service to be used for Interactive Multicast sessions.
- **Session Name**: Type a name to identify this service's Interactive Multicast session.
- **Session Description**: Type a name or description of the Interactive Multicast.
- **Advanced**: Click this button to display additional properties (described below).
- **Broadcast to Address**: The destination IP address for the Interactive Multicast session. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0 to 239.255.255.255**.
- **Media Packets TTL**: The maximum number of routers (hops) that the Multicast session's packets may pass through.

---

*VCON MXM Administrator's Guide 237*
12.4 Setting VCB Services Properties

**SDP Rate**
Session Description Protocol Rate - The interval at which announcements and descriptions of the Multicast session are sent out on the Internet Multicast backbone (Mbone), for Participants and passive third-party viewers.

**SDP TTL**
The maximum number of routers (hops) that the SDP announcement for this session may pass through.

**Defaults**
Click this button to return to the Multicast default settings.

**Advanced**
In the Advanced page, define the delay period before changing the displayed video during a voice-activated switching multipoint conference. The displayed video changes only after the source of the new sound or voice is steady for the defined period. A delay period is necessary to prevent quick incoherent display changes that may be caused by sudden noises (such as a sneeze) rather than a steady speaker.

![VCB Service - Advanced Properties](image)
QoS

The QoS page contains properties for controlling the type of Quality of Service that will be used for transmitting packets during a multipoint conference that’s initiated using this VCB service.

Set QoS properties as follows:

**Priority Type (QoS)**

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

- **No Priority**: Network transfers packets using normal Best-effort (or Routine) packet transmission.
- **IP Precedence**: Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.
- **Diffserv**: Network transfers packets according to specific needs of the sending application.
12.4 Setting VCB Services Properties

Priority Values

For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix D, “QoS Priority Values.”

To reset the Priority default values, click Restore QoS Defaults.

LDAP

The LDAP page provides information about the VCB service’s registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes’ LDAP Properties, see “LDAP” on page 109.

Additional ID

In addition to its directory (E.164) number, a VCB service may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the Additional ID page, you may enter these, if applicable. For more information about adding Additional IDs, see “Additional IDs” on page 111.
12.5 Expanding to an Ad-hoc Videoconference

To expand from a point-to-point videoconference to an ad-hoc videoconference, one of the parties must invite the additional parties. This procedure depends on the party’s videoconferencing application:

**vPoint**
1. Enter an additional contact’s user number (E.164) or address into the Manual Dialer's address box.
2. Click **Invite**.
   -or-
1. Open the Dialer and locate the contact that you want to invite.
2. Right-click the contact and then click **Invite**.

**MeetingPoint 4.6, Falcon**
Use the **Invite** command. For further instructions, refer to the *MeetingPoint 4.6 User’s Guide*, or the *Falcon IP User’s Guide*.

**Other applications**
Enter the defined Ad-hoc Conference code (default is *77) followed by the directory number of the additional party. For example, to invite end point 2345, enter *772345*. 
13 CUSTOMIZING THE MXM ADMINISTRATOR

In the MXM Administrator application, you may customize the application according to your personal preferences. A set of defined window, table, and layout properties for the Administrator application is called a workspace. This chapter explains the following customization tasks:

- Defining the Main View Options
- Setting Up the Workspace
- Customizing the Toolbar
- Customizing the Status Views

13.1 Defining the Main View Options

You can customize the following elements of the Main View through the Options dialog box.

- Tree Styles - the appearance of the table format of the Main View.
- Item Attributes - the appearance (font, color, and so on.) of the various objects, such as end points and login requests.

**Tree Styles**

The Tree Styles Options control the appearance of tables in the main Administrator application window.

**To set Main View table properties**

1. In the View menu, click Options. The Options dialog box appears with the Tree Styles tab open.
2. Change the appropriate properties. For descriptions of these properties, see “Tree Styles Properties” on page 244.
3. Click OK to complete the change. If you want to discard the change, click Cancel.
13.1 Defining the Main View Options

Tree Styles Options

Tree Styles Properties

Set the Tree Styles properties according to your viewing preferences.

Enable Word Wrap

Select this option to cause text in each column to continue automatically on the next line, after it reaches the end of each line. The line width is determined by the column borders.

If this option is not selected, sections of long phrases or names, that are not within the column borders, are not seen. However, a tooltip appears over those names.

Show Column Headers

Select this option to display the column names that identify the information that appears in the Main View.

Main View Column Headers

Show Lines Between Columns

Select this option to display the vertical borders between columns of the Main View.

Show Lines Between Items

Select this option to display the horizontal borders between items.
13.1 Defining the Main View Options

### Highlight Entire Row
Select this option to highlight the entire row when you select an item. In this case, you can click anywhere on the row.

Deselect this option to highlight only the item name when you select it. In this case, you must click the name to highlight it.

### Display Large Images
Select this option to view the workspace’s details and images at a larger size.

### Animated Expand/Collapse
Select this option to expand and collapse the levels of the System tree in a graded, stuttering motion. To control the speed, drag the speed slider towards the left for faster motion or towards the right for slower motion.

Deselect this option to expand and collapse the levels in one swift motion.

### Item Attributes
In the **Item Attributes** tab, you can customize the way entries are indicated in the Main View. For example, you can change the color of the characters in order to differentiate between VCON end points, MCUs, hunting groups and so on. Also, you can assign sounds to indicate occurrences such as login requests.

To use the factory-set indication styles, do not make any changes. Keep **Use Default Attributes** selected for all entries.

#### To customize the indications for entries in the Main View
1. In the **View** menu, click **Options**. Click the **Item Attributes** tab.
2. From the **Item** list, select the entry type you want to customize.
3. Deselect **Use Default Attributes**.
13.1 Defining the Main View Options

4. Customize items, according to your own specifications, as follows:

*Font Style*

**Color**
Click and choose another color from the palette. If you want, you can also create colors that don't appear on the original palette.

**Inverse Background Color**
Select to add a highlight background to the item in the Main View.

**Bold**
Select to display the item name in bold letters in the Main View.

**Play Sound**
If you want, associate a sound with the item. Click this button to browse and locate Wave (\wav\) files. For example, you can find login request indication files in the \Vcon\Administrator folder. Otherwise, you can use a wav file from another source.

5. Click **OK**.
13.2 Setting Up the Workspace

Several options are available for customizing the MXM Administrator’s workspaces in accordance with your operating preferences.

Defining Workspace Options

The Options dialog box Workspaces tab contains options for storing the data and appearance that are associated with a specific Workspace.

➤ To define Workspace options

1. In the View menu, click Options. The Options dialog box opens to the Workspaces tab.
2. Change the appropriate properties. For descriptions of the properties, see “Workspace Properties” on page 247.
3. Click OK to complete the change. If you want to discard the change, click Cancel.

Workspace Properties

Set Workspace properties as follows:

- **Save the active workspace when exiting**
  - Select this option to automatically save all the current Workspace properties whenever you close the Workspace or the Administrator application.

- **Reload the last used workspace when starting**
  - Select this option to open the previously used Workspace whenever you start the Administrator application.

- **Workspace Persistence**
  - Persistence information includes the customization properties defined for the workspace and the data about devices and other nodes that are defined within that workspace.

  - Select **Save Persistence Information to a file** to store all of the current workspace’s data in a file located in the Administrator application’s root directory (Default is C:\Program Files\Vcon\Admin).

  - Select **Save Persistence Information to the registry** to store all of the current workspace’s data in the system Registry
13.2 Setting Up the Workspace

**Maximum inactive time for change level login**

For administrators with “Change” privileges, this is the maximum amount of time that the MXM administrator remains idle. When this interval passes, a message asks you to disconnect or stay connected. If you do not respond, the administrator disconnects from the system.

*Workspace Options*
Managing Workspaces

The MXM Administrator application provides functions for managing and storing workspaces. These functions include:

- Saving a workspace
- Renaming a workspace
- Deleting a workspace
- Opening a workspace
- Reorganizing the Workspace list.

Saving a Workspace

A workspace may be saved in different formats:

- As a file - this is advantageous if you may log in to the MXM and use the same workspace from other computers.
- As information stored in the system registry - this is advantageous if more than one administrator may log in to the MXM from the same computer.

➤ To save a workspace as a file

In order to save workspaces as files, the Save persistence information to a file option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the File menu, point to Workspaces and click Save Workspace Now. The Save Workspace dialog box appears.

2. To create a new workspace file, type the name in the File Name box and click Save. The system automatically adds a .paw extension to the filename.

- or -

To update a previous workspace file, double-click the name of the file from the list. Then, click Yes to confirm.
13.2 Setting Up the Workspace

➤ To save a workspace in the system registry

In order to save workspaces in the registry, the **Save persistence information to the registry** option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the **File** menu, point to **Workspaces** and click **Save Workspace As**. The Save Workspace dialog box appears.

2. Click the **New (Insert)** button.

3. Type the name of the new workspace.

4. Click in the free space of the dialog box. A confirmation request appears.

5. Click **Yes** to save the new workspace.

![Save Workspace dialog box]

*Saving a Workspace to the Registry*
Renaming a Workspace

The procedure for renaming a workspace depends on whether you save workspaces to files or to the registry.

➤ To rename a workspace file

In order to rename a workspace file, the Save persistence information to a file option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the File menu, point to Workspaces and click Open Workspace. The Open Workspace dialog box appears.

2. Click the workspace file that you want to rename. After 1 second, click again. The filename is highlighted for editing.

3. Type the new name and then click outside the new name area. The workspace file is now renamed.

➤ To rename a workspace that is stored in the registry

In order to rename a workspace in the registry, the Save persistence information in the registry option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the File menu, point to Workspaces and click Open Workspace. The Open Workspace dialog box appears.

2. Double-click the workspace that you want to rename. The name is highlighted for editing.

3. Type the new name and then click below the list.

4. Click Done to exit the dialog box.
13.2 Setting Up the Workspace

Opening a Workspace

The procedure for opening a workspace depends on whether you save workspaces to files or to the registry.

➤ To open a workspace file

In order to open a workspace file, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Double-click the file that you want to open. The Login To [MXM name] dialog box appears.
3. Type the required password and then click **Login**. The workspace opens in the Administration window.

➤ To open a workspace from the registry

In order to open a workspace from the registry, the **Save persistence information in the registry** option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Click the workspace that you want to open and then click **Open**. The Login To [MXM name] dialog box appears.
3. Type the required password and then click **Login**. The workspace opens in the Administration window.
13.2 Setting Up the Workspace

Deleting a Workspace

The procedure for deleting a workspace depends on whether you save workspaces to files or to the registry.

➤ To delete a workspace file

In order to delete a workspace file, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Right-click the workspace file that you want to delete and then click **Delete**. Click **Yes** to confirm.

   The workspace file is deleted from the system.

➤ To delete a workspace from the registry

In order to delete a workspace from the registry, the **Save persistence information in the registry** option of the Options dialog box must be selected. For more details, see “Defining Workspace Options” on page 247.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Click the workspace that you want to delete and then click the **Delete** button.

   The workspace is deleted from the system. No confirmation is requested.
3. Click **Done** to exit the dialog box.
You can set the appearance and the buttons of the toolbars according to your preferences.

**Defining the Toolbar Display**

By default, the toolbars are docked in the Administrator window below the menu bar. You can choose any or all toolbars to be part of the application display. In addition, you can select among a number of other appearance options.

**To define the toolbar display**

1. In the **View** menu, click **Customize**. The Customize dialog box opens to the **Toolbars** tab.

2. To display a particular toolbar on the screen, select it in the **Toolbars** list. To hide a toolbar, deselect it.

3. Set the toolbar display properties according to your preferences. The toolbar display changes as you change each setting. For a description of these properties, see “**Toolbar Display Properties**” on page 255.

   To return a toolbar to its default formation, select it in the **Toolbars** list and then click **Reset**.

4. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

If you want to change the buttons on the toolbars, click **Apply** to implement the toolbar display property changes. Then, click the **Commands** tab.
13.3 Customizing the Toolbar

Customizing Toolbar Display Properties

**Toolbar Display Properties**

Set toolbar display properties as follows:

**Toolbars**

In this list, select any or all of the various toolbars that will appear in the Administrator application window. Only toolbars that are marked with a ✓ will appear.

**Show Tooltips**

Select this option to display tool tips when you hold the pointer over a button for about 1 second.

**Cool Look**

Select this option to cause each button to display a raised effect when the pointer points it.

When deselected, the buttons are static with clear borders.

**Large Buttons**

Select this option to increase the size of the buttons by 400% (4x).
13.3 Customizing the Toolbar

Adding and Removing Toolbar Buttons

You can control the contents of each toolbar by adding or removing buttons, or moving buttons among the various toolbars.

➤ To control the contents of the various toolbars

1. In the View menu, click Customize. The Customize dialog box opens to the Toolbars tab.
2. Click the Commands tab.
3. To add a button to any toolbar, select a category from the Categories list. Drag the appropriate button to any toolbar in the Administrator window that you want.

To remove a button from any toolbar, drag the button to the Customize dialog box.

To move a button to another toolbar, drag the button to the new location.

Customizing Toolbar Button Contents
Creating a Custom Toolbar

You can add a toolbar other than the standard ones provided by the Administrator application.

➤ To add a custom toolbar

1. In the View menu, click Customize. The Customize dialog box opens to the Toolbars tab.
3. Type the name of the new toolbar and click OK. The new toolbar appears in the Administrator window and its name appears in the Toolbars list.
4. Click the Commands tab.
5. Switching Categories according to your preference, drag any number of toolbars to the new toolbar.
6. Click OK to close the dialog box.
13.4 Customizing the Status Views

According to your preferences, you can customize the way that the Administrator displays information in the various status view tables. Design functions are available for:

- Displaying the various views
- Style formats for table elements or types of information.
- Style formats for printed tables.

Setting Table On-Screen Display Properties

This section provides instructions for customizing the on-screen display of the Administrator application’s various table views. You can control the appearance of table elements such as gridlines and column heads, colors, and current cell.

The display properties affect only the active table view. To set the display properties of another specific table, you must enter that particular view.

To set table on-screen display properties

1. In the View toolbar, click the table view that you want to format.

2. In the View menu, click Display Properties. The Display Settings dialog box appears.

3. Set the display properties according to your preferences. For a description of these properties, see “Table Display Settings” on page 259.

   In the Preview area of the dialog box, you can preview the effects of your changes.

4. Click OK to implement the settings.
Table Display Settings

Set the table display properties as follows:

- **Titles and Gridlines**: Select **3D Buttons** to display column and row titles inside borders.
  
  Select **Vertical Lines** to display borders between columns.
  
  Select **Horizontal Lines** to display borders between rows.
  
  Select **Mark Current Row** and/or **Mark Current Column** to provide a 3-D pressed appearance to the selected row/column heading.
13.4 Customizing the Status Views

**Color**

Click any item in the Color list and then click the required color from the adjacent palette.

- **Grid lines** are the borders between columns and rows.

- **Fixed lines** are rows that are in a specific location permanently. They cannot be sorted.

- **Tracking Line** is the border that is being dragged during a Resize Column/Row action.

- **Background** represents the empty area behind and around the table.

**User Properties**

In the **Value** list, select the option that determines the appearance of the adjacent **Attribute**.
13.4 Customizing the Status Views

Style Formats for Table Elements or Types of Information

You can customize the display styles of various table elements, such as column headers and standard cells. For example, you can change the font style and colors of particular information that must be quickly recognizable.

The style formats affect only the active table view. To set the style formats of another specific table, you must enter that particular view.

➤ To change the formatting of a table element

1. In the View toolbar, click the table view that you want to format.

2. In the Format menu, click Styles. The Styles dialog box appears.

3. In the Names list, click the element that you want to format and then click Change.

   A style formatting dialog box appears for the selected element. By default, the Font tab is open.

4. Set the style properties according to your preferences. For a description of these properties, see “Style Format Properties” on page 262.

5. Click OK to complete the change. If you want to discard the change, click Cancel.

Table Element Styles Dialog Box
13.4 Customizing the Status Views

Style Format Properties

The following categories make up a table element style:

- Font
- Color
- Borders
- Align

Font Properties

For the table’s text, you can select the font, its size, and any special characteristics such as **Bold** or **Underlined**.

![Font Properties](image)

Color Properties

In the style changing dialog box, click the **Color** tab.

- To change the color of the table element, click a color in the **Foreground** group.
- To change 3-D effect (such as raised, pressed, or normal flat) of the table element, select one of the options in the **3-D Effect** group.
13.4 Customizing the Status Views

Color Properties

Borders Properties

1. In the style changing dialog box, click the **Borders** tab.
2. In the **Border** group, select the side(s) of the cells that you want to change.
3. In the **Type** group, select a type of line and/or thickness. If necessary, select a different color from the **Color** list.
Align Properties

To change Align properties of the selected table element, click the Align tab in the style changing dialog box.

- In the **Horizontal** group, select left, center or right text alignment in the cells.
- In the **Vertical** group, select top, center, or bottom text alignment in the cells.
- Select **Wrap Text** to display cell text on a new line if the text exceeds the cell’s borders.
- Select **Auto Size** to set the size of the columns automatically according to the column’s content.
13.4 Customizing the Status Views

Showing and Hiding Columns

By default, some of the Node Status View table's columns always appear and some appear only if the node is connected to ISDN. In the Show/Hide Columns dialog box, you can change these settings to display or hide the columns of your choice.

This feature is applicable only to the Node Status View.

➤ To show and hide columns

1. In the Format menu, click **Show/Hide Columns**. The Show/Hide Columns dialog box appears.

   ![Show/Hide Columns Dialog Box]

   *Show/Hide Columns Dialog Box*

2. In the **Column Name & State** list, choose the column whose display status you want to change.
3. Select Properties as follows:

**Auto Hide the Column**  
The column is displayed if relevant to the node's current status, and hidden in other situations. If deselected, the column is constantly displayed or not displayed according to the **The Column is Visible** option below.

**The Column is Visible**  
The column is displayed in the Table View on the screen. If deselected, the column is hidden.

**Default**  
Click Default to return to the default Table View, according to the nodes listed in the table.

4. Click OK to implement the new settings.
14 Remote Upgrade of Videoconferencing Devices Software

After your organization receives new versions or patches of certain VCON videoconferencing software applications, you can then install them on all registered end points that require the specific applications. The MXM's Remote Software Upgrade utility supports the following software products:

- vPoint 5.0
- VCON Conference Bridge
- MXM Administrator
- IPNexus

The definition of a software upgrade progress requires the setting of five sets of properties. The Software Upgrade Wizard's steps enable you to:

- Select the application and version - Versions page (see “Selecting a Software Version” on page 270).
- Copy the upgrade to a target location in your network or on an FTP server - Upload page (see “Setting a Target Location for the Upgrade” on page 271)
- Set temporary alias and password for end points to access the upgrade file (for users not defined as "Administrators" on their computers) - Login page (see “Setting Up User Login” on page 274)
- Schedule the time for upgrading all or selected end points - Run page (see “Setting the Upgrade Schedule” on page 275)
- Confirm the upgrade task's properties and initiate the upgrade - Confirmation page (see “Confirm Upgrade Definition” on page 277).

The MXM enables you to monitor the software versions status for applicable end points throughout the network, making sure that all end points are working with the latest or most suitable software versions.
14.1 Defining a Software Upgrade

The Software Upgrade Wizard enables you to define properties such as application version, upload location, and scheduling.

➤ To set up the software upgrade

1. Make sure that the upgrade file is in an accessible location, such as a CD-ROM.

2. In the MXM Administrator, open the MXM menu and choose Update Software. The Software Update Wizard appears.


4. Set properties according to your upgrading specifications. When you finish each page of the wizard, click Next. For explanations about the various Property pages, see “Setting Software Upgrade Properties” on page 269.

5. When you finish the last page, click Finish.

The Software Upgrade task is set up and the upgrade process will proceed as defined.
14.2 Setting Software Upgrade Properties

The Software Upgrade Wizard guides you through the task of defining the upgrade process. The Wizard’s steps enable you to:

- Select the application and version
- Upload the upgrade to an accessible target location in your network or on an FTP server
- Set login parameters for providing access to the software upgrade file
- Schedule the time for upgrading all or selected nodes that require the specific software application
- Confirm the upgrade task’s properties.
14.2 Setting Software Upgrade Properties

Selecting a Software Version

When you open the Software Upgrade Wizard, the Version page opens first.

Define whether this upgrading task will be New or an Update:

**New**

- Click **Browse** to locate and select the application+version upgrade file. VCON supplies an XML file with its upgrades that define its version identification, installation requirements, and other information.

**Update**

- If an update was previously performed, select the appropriate application description from this list. The description provides identification information for the required application version.

After selecting the upgrade file, the installation information appears on the Version Page.

---

*Selecting Software Upgrade Application*
Setting a Target Location for the Upgrade

In the Software Upgrade Wizard’s Upload page, set the location from which the upgrade is accessible for the relevant registered nodes.

**File Server**
Select to upload the upgrade file to either a **Network Drive** or **FTP** location. Depending on your choice, specify the exact access information in the relevant areas in the dialog box.

**Network Drive**
Select a folder on your organization’s network for the upgrade file. Click **Browse** in the Network Drive area, then locate and select the location.

**FTP**
Type the path of a folder on an FTP server for the upgrade file.

Enter the login information (**Name**, **Password**, and **IP Address**) that the administrator must enter to upload the upgrade file to the FTP location.

The FTP option is not applicable for upgrades from vPoint 5.0 to 5.1.
Setting Network Location for the Upgrade
14.2 Setting Software Upgrade Properties

Setting FTP Location for the Upgrade
14.2 Setting Software Upgrade Properties

Setting Up User Login

In the Login page, set the login parameters for providing access to the software upgrade file.

Setting Up User Login

**Impersonation**
Provide a **Name**, **Password**, and **Domain** of a Windows NT/2000/XP user that has Administrator privileges. This allows the server to perform the upgrade for client users that do not have sufficient privileges on their computers or the network.

**Parameters**
Switches used to modify the installation command.

**FTP**
*For upgrading through an FTP server*
Provide a **Name** and **Password** for the MXM to use on behalf of the nodes in order to access the upgrade file.
14.2 Setting Software Upgrade Properties

Setting the Upgrade Schedule

In the Run Page, define the time for upgrading all registered nodes that require the specific software application.

![Software Update Wizard 4/5](image)

**Setting the Upgrade Schedule**

**End User Confirmation**

**User Confirmation Required**

- Select **Always** to notify the node user that a newer version of the application is available, and to ask if the MXM should perform the upgrade now.

- Select **Only When In a Call** to wait for users engaged in videoconferences to hang up before notifying them that the software upgrade is available.

- Select **Never** to perform the upgrade without asking for the node user’s permission.
14.2 Setting Software Upgrade Properties

**Confirmation Question**
Type the text that should appear in the Upgrade request on the node’s screen (for example, “**Do you want to upgrade to the newest software version?**”).

If this box is blank, a default text appears.

**Make this the default version when a new endpoint logs in**
Select to make this upgrade task the default for all new nodes (of the relevant node type) that register with the local MXM.

**Update**
Set the time to run the upgrade process.

**Run Now (all users)**
Select to initiate the upgrade process immediately after you finish defining it.

The MXM starts the task of upgrading the software of all relevant logged in nodes. For offline nodes, their upgrade will be available the next time they log in to the MXM.

**Schedule (all users)**
Select to set a time period for initiating the upgrade process on all logged-in nodes (of the relevant node type). If offline nodes log in during this period, their applications will be updated too.

**Run Later**
Select if you want to run this upgrade process at a later, undefined time. When you exit the last page of this Wizard, this upgrade task, although defined, will not run until you initiate it a later time.

**Schedule Window**
This area is available if you selected **Schedule (all users)** above.

In the **From** and **To** lines, set the time period for performing the upgrade process.

In the **Date** box, choose a date.

In the **Time** box, highlight the hour, minute, and/or seconds, and then press the up or down arrow buttons until the correct time appears.
Confirm Upgrade Definition

In the Confirmation page, confirm the upgrade task’s properties. A summary describes the Property values that you set in the previous pages of the Software Upgrade Wizard.

Summary of Upgrade Task Definition

Click **Finish** to activate the upgrade task in the MXM’s zone. If you defined a new upgrade task (see “Selecting a Software Version” on page 270), the MXM copies the upgrade file to the target location (defined in the Upload page - see page 271).
14.3 Selecting Nodes to Upgrade

If you schedule the software upgrade to Run Later (see “Setting the Upgrade Schedule” on page 275) at an undefined time, you can select specific nodes at a convenient time and run the upgrade process.

➤ To select nodes and run the upgrade process

1. In the Main View, select the specific nodes.
2. Right-click and then click Update Software. The Update Software Wizard appears.
3. Set the Upgrade properties according to your specifications. For descriptions of the properties, see the next section, “Node Software Upgrade Properties”.
4. Click OK to start the upgrade process on the selected nodes.

Node Software Upgrade Properties

For node types whose software may be updated through the MXM, you can view and set upgrade properties for individual nodes.

➤ To access the Software Upgrade properties of individual nodes

1. In the Main View, select the specific end points.
2. Right-click the node(s), point to Property and Software Update, and then click the specific properties. The node’s Properties dialog box opens to the property type that you clicked.
   -or-
   Double-click the node, and then browse to the Software Update properties. Click the specific properties that you need.

The Software Upgrade Property pages are:

- Update Version
- Impersonation
- Update FTP
- Update Parameters
- Update Run
14.3 Selecting Nodes to Upgrade

**Update Version**

The **Update Version** tab displays the name(s) of the required videoconferencing application for the end point and the currently installed videoconferencing application.

The **Required Version** is the version (as defined in the Software Upgrade task) that the end point will receive when an upgrade takes place. To change the version or the defined upgrade task, select it from the list.

![Software Upgrade Properties - Update Version](image)
14.3 Selecting Nodes to Upgrade

**Impersonation**

In the **Impersonation** tab, set the login parameters for providing access to the software upgrade file.

![Software Upgrade Properties - Impersonation](image)

**Impersonation**

**Name, Password, Domain**

The Name, Password, and Domain of a Windows NT/2000/XP user that has Administrator privileges. This allows the server to perform the upgrade for client users that do not have sufficient privileges on their computers or the network.

**Parameters**

Switches used to modify the installation command.
Update FTP

The Update FTP tab contains the login parameters for providing access to the software upgrade file if it's located on an FTP server.

![Software Upgrade Properties - Update FTP]

**Name, Password**

The MXM uses these to log onto the FTP server, on behalf of the end points.

The FTP option is not applicable for upgrades from vPoint 5.0 to 5.1.
Update Parameters

In the Update Parameters tab, define node-specific properties for software upgrade procedures.

**Software Upgrade Properties - Update Parameters**

**Restrictions**

**Ignore Selected End Points**
Select to prevent the software upgrade of the selected nodes.

**End User Confirmation**

**User Confirmation Required**
- Select **Always** to notify the node user that a newer version of the application is available, and to ask if the MXM should perform the upgrade now.
- Select **Only When In a Call** to wait for users engaged in videoconferences to hang up before notifying them that the software upgrade is available.
- Select **Never** to perform the upgrade without asking for the node user’s permission.
Confirmation Question  The text box displays the text that should appear in the Upgrade request on the end point’s screen (for example, “Do you want to upgrade to the newest software version?”).

If this box is blank, a default text appears.

Update Run

In the Update Run tab, define the time for upgrading the selected node's videoconferencing software.

Software Upgrade Properties - Update Run

Update

Run Now  Select to initiate the upgrade process after you finish defining it.

The MXM starts upgrading the software in all relevant logged in nodes. For nodes engaged in calls, their upgrade occurs after hangup. For offline nodes, their upgrade occurs the next time they log in to the MXM.

Schedule  Select to set a time period for initiating the upgrade process on all logged-in end points (of the relevant node type). If offline end points log in during this period, their applications will be updated too.
14.4 Monitoring Software Upgrade Status

Schedule Window

This area is available if you selected Schedule above.

From, To

In these lines, set the time period for performing the upgrade process.

In the Date box, choose a date.

In the Time box, highlight the hour, minute, and/or seconds, and then press the up or down arrow buttons until the correct time appears.

14.4 Monitoring Software Upgrade Status

In the Main View, you can see which end points received the upgrades and which ones did not.

❑ Next to each applicable end point, an icon indicates if that end point is working with the latest available software version.

❑ The Event Log shows if the end point's software was upgraded.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Software agent will now run install, process=C:\DOCUME\T</td>
</tr>
<tr>
<td>3103</td>
<td>Sending software upgrade message to Endpoint: Endpoint N</td>
</tr>
<tr>
<td>3111</td>
<td>Unrecognized Version for logged Endpoint: Endpoint Number</td>
</tr>
</tbody>
</table>

Event Log Details

❑ The Main View’s “Systems with an outdated version” filter displays only end points that have not been upgraded yet (see “Filtering the Main View” on page 29).

“Systems with an Outdated Version” Filter
15 Least Cost Routing of Gateway Calls

Least cost routing automatically connects an outgoing ISDN or IP-to-ISDN call with the least expensive gateway service to the target location at that time of day. Depending on the locations of the registered gateways, long-distance calling costs can be reduced significantly.

For example, suppose that a user in Hong Kong wants to videoconference with someone in Canada. If the call is initiated over a LAN through a registered gateway located in the USA, the initiator in Hong Kong is charged for a call from the USA to Canada, instead of from Hong Kong to Canada.

If the most efficient service is not available, least cost routing will try to pass the call through the next most-efficient service, or it will give the caller a busy signal.

In the MXM Administrator, you can check and compare the costs of IP-to-ISDN calls from the MXM’s zone to destinations using registered gateway services. This allows you to apply the most cost-efficient connections for these calls.

Setting up and using least cost routing requires a combination of procedures in the MXM Administrator:

1. In the MXM's ISDN Call Routing Properties, set the location of the MXM and define the prefixes required for dialing (see “Setting ISDN Call Routing Properties” on page 286).

2. In the appropriate Gateway's Call Routing Properties, set the location of the gateway and enter the costs for dialing through it (see “Setting Gateway Call Routing Properties” on page 288).

3. Select registered end points and access their MXM ISDN Call Routing Properties. Select the preference of using Least Cost Routing rules or Bandwidth rules for routing calls (see “Setting Preference of Using Least Cost Routing or Bandwidth Rules” on page 288).

4. Before initiating a gateway call from a registered end point, test the Least Cost Routing rules to select the least expensive gateway and service available (“Testing for the Optimal Gateway Service” on page 290).
15.1 Setting ISDN Call Routing Properties

One of the factors that determine the costs of ISDN calls is the location of the end points on the network. You must enter this information in the MXM’s System Properties in order to test and implement least cost routing.

In addition, you must enter the prefixes required by the local telephone company or ISDN provider for dialing international and long distance destinations.

➤ To set the location and define the prefixes

1. Right-click the local MXM object, point to Property and then ISDN Call Routing, and click System Location. The System Location tab appears.

2. Enter the country and area code in which the local MXM is located and click Apply.

3. Click the Dialing Prefixes tab.

4. Click the New Prefix button.

5. Type the prefix and press <Enter>.

6. To enter more prefixes, repeat steps 1 and 2 as many times as required.

7. Click OK to implement the settings and close the dialog box.

Local MXM Location
15.1 Setting ISDN Call Routing Properties

Gateway Dialing Prefixes for Local MXM Network
15.2 Setting Gateway Call Routing Properties

In the registered gateways’ Call Routing Properties, enter the physical location of the gateway and define the cost rates for using the gateway’s services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see “Testing for the Optimal Gateway Service” on page 290).

For the complete Call Routing procedure, see “Call Routing” on page 120.

15.3 Setting Preference of Using Least Cost Routing or Bandwidth Rules

The MXM provides various rules for deciding how to route calls through gateways:

- Least Cost Routing Rules
- Bandwidth Rules (nodes’ Properties Services tab - see “Gateway Services” on page 105)

When gateway calls are initiated, the MXM applies the rules in accordance to the ISDN Call Routing properties of the initiating end point. These settings are located in nodes’ MXM Properties.

➤ To select the preferred set of rules

1. Select the nodes that will be affected by the rule preference.
2. Right-click, point to Properties and then MXM, and click ISDN Call Routing. The ISDN Call Routing tab appears.
15.3 Setting Preference of Using Least Cost Routing or Bandwidth Rules

H.323 End Point - ISDN Call Routing Properties

3. Select **Use least cost routing rules when this end point makes a call.**
   This selection allows the MXM to apply least cost routing to the end points’ gateway calls.

4. Select a preference for applying rules:
   - **Bandwidth rules precede least cost routing rules**
     When initiating a gateway call, the MXM first searches for gateway services that meet the criteria defined in the initiating end point’s Service properties.
   - **Least cost routing rules precede bandwidth rules**
     When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.

5. To implement the changes and close the dialog box, click **OK.**
15.4 Testing for the Optimal Gateway Service

The ISDN Dialing Simulator enables you to find the most cost-efficient gateway services available for registered end points. The results are based on gateway services that meet the criteria defined in:

- The end points’ ISDN Call Routing Properties (see page 106)
- The end points’ Gateway Services Properties (see page 105)
- The gateways’ Call Routing Properties (see page 120).

For example, suppose that you allocate a maximum bandwidth of 256K for calls from Hong Kong to Canada. The initiating end point is allowed to use bandwidths equal or lower than the requested one. In addition, least cost rules were enabled for the end point. After you enter the required information in the Simulator, it will display a table of gateway services available to the end point and their costs, sorted by cost. The MXM initiates dialing through the cheapest route first, trying all routes, if necessary, until the call connects successfully.

➤ To test the least-cost-routing rules

1. Right-click the node that will initiate the call and then click Test Least Cost Routing Rules. The ISDN Dialing Simulator appears.

2. Based on the information that you enter, the simulator will provide possible gateway services and their costs for calling your destination. Enter the following details:

   - **Dialing End Point**: The initiator of the call.
   - **Dialed ISDN Address**: The phone number of the destination node.
   - **Call Bandwidth**: The maximum bandwidth required for the call.

   Click **End Point Routing Properties** to view or change the end point’s ISDN routing properties before testing.
3. Click **Dial**. The available registered gateway services appear in the table. The most cost-efficient service appears first in the table, followed by lesser efficient ones until the most expensive service, which appears at the bottom of the table.

### ISDN Dialing Simulator

<table>
<thead>
<tr>
<th>Number</th>
<th>Location</th>
<th>In Gateway</th>
<th>Bandwidth</th>
<th>Dialed Number</th>
<th>Provider</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>None</td>
<td>10.0.10.90</td>
<td>128</td>
<td>71441629823366</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>70</td>
<td>None</td>
<td>10.0.10.90</td>
<td>64</td>
<td>70441628823366</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>72</td>
<td>None</td>
<td>10.0.10.90</td>
<td>256</td>
<td>72441628823366</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>73</td>
<td>None</td>
<td>10.0.10.90</td>
<td>384</td>
<td>73441628823366</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

*ISDN Dialing Simulator*
16 MANAGING SIP NETWORKS

The Session Initiation Protocol (SIP) is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. The MXM supports management of SIP end points (called User Agents) within its network, in a similar manner as for H.323 end points.

By employing proxy interfaces (H.323 Gatekeeper for H.323 end points, SIP Proxy for SIP user agents), the MXM provides similar services to systems of either protocol. Administrators can initiate calls between two SIP user agents and between a SIP user agent and an H.323 end point. The MXM provides gateway-like services when connecting calls between H.323 and SIP networks.

The MXM’s SIP system server combines the roles of an SIP Proxy, SIP Redirect Server, and SIP Registrar.

16.1 SIP User Agents

SIP user agents are end points, such as SIP phones and Windows XP Messenger applications, that initiate and receive communication and collaboration over a SIP network. They can initiate requests (UAC client) and respond to requests (UAS server). User agents communicate with other user agents directly or through a server.

For communication between two SIP user agents using Windows XP Messenger, the MXM supports the following:

- Video conversation
- Instant messaging
- Asking for remote assistance
- Application sharing
- Voice conversation
- Sending file or photo
- Whiteboard

For communication between a SIP user agent using Windows XP Messenger and an H.323 end point or other SIP user agent, the MXM supports the following:

- Video conversation
- Voice conversation
16.2 SIP Servers

SIP user agents logged into the MXM may also use the supported telephony functions by entering the appropriate TUI number before the destination address (see “Dial Plan” on page 73):

- Call Pickup and Specific Pickup
- Call Forwarding
- Simplified Gateway Dialing

Additionally, a SIP user agent may also be the recipient of a call transfer or ad-hoc conference although it cannot initiate these functions.

16.2 SIP Servers

The MXM fulfills a multi-faceted role in managing SIP user agents. Its SIP server functions interchangeably as an SIP Proxy, SIP Redirect Server, and SIP Registrar. This section discusses each role.

SIP Proxy

The SIP Proxy relays requests from user agents to other servers or user agents within the network. The SIP Proxy also “forks” requests to several destinations sequentially or in parallel.

It also retains information for billing/accounting purposes.

The SIP Proxy is represented in the MXM Administrator under the System Servers branch of the Main View. Its Properties configuration indicates the same types of information as the local MXM gatekeeper, except that it does not have a zone prefix assigned to it.

SIP Proxy’s Location in the Main View
SIP Redirect Server

A SIP Redirect Server responds to SIP client requests and either informs them of the requested server's address or forwards the calls. The forwarding requests can travel in several hops until they reach the final destination.

To determine user or routing policies, a SIP Redirect server contacts a location server (in the MXM), thereby providing users with more than one method to locate users.

SIP Registrar

A SIP Registrar receives login requests from SIP user agents and stores this information in a location service. The MXM handles the login requests according to its Security policy, such as Open/Closed mode, and License limits (see “Security Properties” on page 85). After the login information is stored, the Registrar sends the appropriate response back to the user agents.

When the SIP Redirect server has to route a SIP request to a user it queries the location service for the destination’s current location. Using the data received from the location service, the SIP Redirect server then routes the SIP request (or provides routing information) to the destination.
16.3 Logging in New SIP User Agents

If the MXM is in Open Mode for SIP user agents, any user agent that attempts to register is automatically logged in (see “Security Mode” on page 85).

If the system is in Closed Mode, a SIP user agent must be granted login permission by an administrator with Super User privileges. During this process, the administrator must define or confirm the user agent’s MXM properties, as for H.323 end points (see “Granting Login Permission” on page 36).
16.4 Setting the MXM SIP Advanced Settings

If a SIP user agent and an H.323 end point are engaged in a conversation, the multimedia information sent by the H.323 end point takes longer to reach the SIP user agent than the transmission in the opposite direction. To enable the MXM to synchronize their conversation, the MXM collects all information sent by the H.323 end point and routes it to the SIP user agent before the user agent transmits again. The period of collecting transmitted data is called the OLC timeout.

➤ To set the SIP channels’ timeout

1. In the Administrator window, right-click the MXM node at the top, point to Property and H.323 _SIP, and then click Advanced Settings.

2. If necessary, change the following properties or keep the default values:

   **Collect OLCs Regular Timeout**
   The maximum period that the MXM collects information transmitted by H.323 devices (except gateways) in order to synchronize a SIP-H.323 conversation.

   **Collect OLCs Slow Timeout**
   The maximum period that the MXM collects information transmitted by H.323 gateways in order to synchronize a SIP-H.323 conversation.
16.5 Registering a Windows XP Messenger SIP User Agent to the MXM

To register with the local MXM, a Windows XP Messenger (XP) user must perform the following procedure.

To register into the MXM

1. In the Windows XP Messenger application, open the Tools menu and click Options. Click the Accounts tab.
2. Define the following:
   - **Sign in with this account**: Select Communications Service.
   - **Sign-in name**: Enter a user name using the following syntax: 
     
     \[alias]@[IP address of SIP Proxy]

     The SIP Proxy may be located in the same computer as the MXM Server.
3. Click **Advanced**. In the Communications Service Connection Configuration dialog box, define the following:

- **Configure settings**: Select this method to configure the user agent system’s connection to a communications service.
- **Server name or IP address**: Enter the IP address of the SIP Proxy.
- **Connect using**: Select either **TCP** or **UDP**, depending on the network’s specifications.

4. Click **OK** in both open dialog boxes to implement the configuration.
16.6 Dialing Unlisted Users in Windows XP Messenger

MXM end points (H.323) and SIP user agents other than Windows XP Messenger are not listed in the Windows XP Messenger address book. To dial these users, you must enter an MXM directory number (E.164), IP address, or alias in the Windows XP Messenger manual dialer.

For communication between a Windows XP Messenger and an H.323 end point or other SIP user agent, the MXM supports the following:

- Video conversation
- Voice conversation

To dial unlisted users from Windows XP Messenger

1. In the Actions menu, click Start a Video (or Voice) Conversation and then the Other tab.
2. Enter the following information:
   - Enter e-mail address
   - Enter the destination’s e-mail address, MXM directory number (E.164) or alias.
   - Service
   - Make sure that Communications Service is chosen.
3. Click OK.

Dialing an Unlisted User
17 Configuring ALG Proxy Servers

VCON’s SecureConnect family of products provides connectivity for videoconferencing networks within organizations that are protected by NAT and firewalls.

- The **ALG** (Application Level Gateway) **Proxy Server** translates H.323 messages between firewall-protected LANs or NATs and the public WAN. It also routes management channels across network boundaries. The VCON ALG Proxy translates private IP addresses to public ones and conversely, from public to private addresses. It also relays every packet towards the correct destination according to its mapping configuration. Network interface cards (NIC) connect the private LAN and public networks.

  Throughout this guide, the name, “ALG Proxy,” refers to the ALG Proxy Server.

- The **Advanced Encryption Server** authenticates the various clients and assigns public encryption keys to them. The AES encrypts videoconferences and other data transmissions across public or private networks.

- The **Encryption Client** is an application which may be installed on PC-based devices such as end points, MCUs and other servers within your organization. The Encryption Client operates as a virtual network card, and encrypts all data transmissions from devices in which this client application is installed. The Encryption Client applies the encryption to signaling and media streams immediately as they leave the Client’s host.

For detailed descriptions and illustrations of the SecureConnect system, its components, and typical topologies of networks which apply SecureConnect components, please see the *SecureConnect Family Getting Started Guide*. 
17.1 Setting ALG Proxy Properties in the MXM Administrator

Following the installation of the ALG Proxy, it registers with the MXM (or other gatekeeper) specified during the installation process. This allows you to view and define configuration properties in the MXM Administrator. The ALG Proxy appears in the Main View under the object ALG Proxy Servers.

➤ To define ALG Proxy properties

1. In the Main View, double-click an ALG Proxy. The Properties dialog box appears.

2. Define the properties according to your network’s specifications, or keep the default settings.

3. To implement the changes and proceed to another tab in the dialog box, click Apply and then the appropriate tab.

4. To implement all the changes and close the dialog box, click OK.

The following sections describe the properties.
17.1 Setting ALG Proxy Properties in the MXM Administrator

**General**

The **General** tab contains identity information of the ALG Proxy.

![ALG Proxy - General Properties](image)

**ALG Proxy - General Properties**

- **Directory Number**: Internal directory number (E.164 number) assigned to the ALG Proxy.
- **Description**: Identity of the server. This name appears in the Main View.
- **Network Address**: IP address of the server.
- **Build Number**: Version information for the server software.

Changing the server’s IP address must be done through its setup program. The address cannot be changed from the MXM.
Server Settings

In the **Server Settings**, enable or disable the operation of the ALG Proxy system. This tab also displays connection status, the installed network adapter MAC address, and the IP addresses of the ALG Proxy’s NICs.

---

**Enable ALG Proxy Server Operation**
Select to enable communication between the private LAN and the public WAN.

**Status**
Connection to the server is open or disconnected.

**MAC**
Name and MAC address of the installed network adapter.

**IP Address**
IP address of the NICs on the LAN and WAN sides, respectively.
17.1 Setting ALG Proxy Properties in the MXM Administrator

License

The License tab shows the details of your ALG Proxy license key. If you need to increase these numbers, contact your local VCON distributor.

![ALG Proxy - License Properties]

**Licensed Ports** Number of concurrent calls that this ALG Proxy supports.

**License Key**

**Export Key** To purchase a license for more ports, click Export Key to create a license file for the ALG Proxy on its host computer. Send the file to your local VCON distributor. You will then receive an updated license key.

**Show Key** Click to view the key code for the current ALG Proxy installation.

**New Key** After receiving a new license file from your VCON distributor, click this button, browse to select the file and click Open. When prompted to apply the license code, click OK. To implement the license change and close the dialog box, click OK again.
Encryption Settings

The Encryption Settings are required if an Advanced Encryption Server is installed in the configuration.

**ALG Proxy - Encryption Settings Properties**

- **Connect to the Advanced Encryption Server**
  - Select to connect this device to the Advanced Encryption Server.

- **Encryption Server Address**
  - The IP address of the Advanced Encryption Server.

- **User Account**
  - Client username required for logging in to the Advanced Encryption Server.

- **User Password**
  - Password associated with the User Account. It’s required for logging in to the Advanced Encryption Server.

- **WorkGroup**
  - User Group (defined in Advanced Encryption Server) that this ALG Proxy is assigned to.
Proxy Timeouts

In the Proxy Timeouts tab, define intervals for the sending of various control messages to the network.

**ALG Proxy - Server Timeouts Properties**

- **Remove RAS messages from queue**
  Amount of time until an unanswered Registration Admission Status (RAS) request to the MXM is discarded.

- **Refresh TCP connections interval**
  Frequency for sending Keep Alive messages over the TCP/IP connection, if applicable.

- **Refresh UDP connections interval**
  Frequency for sending Keep Alive messages over the UDP connection, if applicable.
Firewall/Network Settings

In the Firewall/Network Settings tab, define controls over permitted traffic through your network’s firewall.

**Enable Multicast Traversal**

The ALG Proxy provides built-in support for VCON’s Interactive Multicast. However, to enable the transmission of standard broadcast multicasts (such as that used in the VCB and other videoconferencing vendors), select this option. The source of the multicast must be located in the LAN side of the network.

**Signalling Ports Start At**

The first port in the firewall through which the system routes TCP/IP and UDP signals.

This port must be identical to the lowest port of the 3–port range of pinholes opened in the firewall configuration (see the SecureConnect Family Getting Started Guide for more details).

**Media Ports Lower/Higher Boundary**

The range of ports in the firewall through which the system routes data.

**MXM/Gatekeeper Address**

The address from which this ALG Proxy receives MXM or gatekeeper management.
17.1 Setting ALG Proxy Properties in the MXM Administrator

Located on the WAN/LAN side of the ALG Proxy Server

Select **WAN** if the MXM/gatekeeper is located in the public network.

Select **LAN** if the MXM/gatekeeper is located in a private network.

**QoS**

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets through this ALG Proxy.

These settings override the local QoS settings of any end points communicating through this ALG Proxy.

![ALG Proxy - QoS Properties - Default Settings](image)

**ALG Proxy - QoS Properties - Default Settings**
Set QoS properties as follows:

**Priority Type (QoS)**

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

**No Priority**  
Network transfers packets using normal Best-effort (or Routine) packet transmission.

**IP Precedence**  
Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.

**Diffserv**  
Network transfers packets according to specific needs of the sending application.

**Priority Values**

**Video, Audio and RTCP Priority**  
For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix D, “QoS Priority Values”.

To reset the Priority default values, click **Restore QoS Defaults**.
A  **vPoint™ END POINT PROPERTIES**

From the MXM Administrator application, the administrator may view and control various properties of vPoint™ end points. vPoint is the videoconferencing application used by VCON’s ViGO, and may also be used as a software-only application with various cameras.

For explanations about end point MXM Properties, see “Setting End Point MXM Properties” on page 97 to 111.

For explanations about end point Software Upgrade Properties, see “Node Software Upgrade Properties” on page 278 to 284.

A.1 **Conversation Properties**

The Conversation Properties dialog box may be used for viewing and controlling the Video and Data settings of vPoint end points.

**Video**

In the **Video** tab, you may control certain video features that improve the quality of the video transmission from the selected vPoint end point.

![vPoint End Point - Video Properties](image-url)
A.1 Conversation Properties

**Display**

**Clearer Picture/ Smoother Motion**

This control enables you to define the relationship between clear, sharp images and smooth uninterrupted motion during the video transmission. If the picture is clearer, the motion may be slower and more broken. If the motion is smoother, the picture may be less clear.

Drag the slider until you are satisfied with the image sharpness and the smoothness of motion. There are 30 possible settings on the slider – 1 represents the clearest picture but the most uneven motion; 30 represents the smoothest motion but the most blurry picture.

**Video Format**

The type of video format in which the current video meeting is broadcast. This setting affects the viewing quality for the remote party, and may only be changed during a call. The possible options are:

- **Normal (CIF)**
  
  Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

  All VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

- **Quarter Size (QCIF)**
  
  Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF).

  QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.
**Data**

In the **Data** tab, select **Automatically Start Data When Application Starts** to enable data receiving capability immediately AND to automatically enable it when vPoint starts again. In such a case, Microsoft® NetMeeting® runs minimized on the Windows Desktop and the end point user can use NetMeeting's data sharing features during the videoconferences.
A.2 Calls Properties

The Calls Properties dialog box may be used for viewing and controlling incoming and outgoing call properties of vPoint end points.

Incoming Calls

In the Incoming Calls tab, customize how the vPoint end point indicates and accepts incoming calls.

![vPoint End Point - Incoming Calls Properties]

_When Idle_

**Auto answer**  Select to turn automatic acceptance of calls on. If the system is idle when a videoconferencing call arrives, the session starts automatically.

_As Interactive Multicast Chair_

If the selected user's system supports VCON's Interactive Multicast, it may sometimes be the Chair of multicast videoconferences. If another party tries to call it while it chairs a conference, that call may be accepted or rejected according to the selected option:

- **Manually join IP point-to-point calls**  Enable the selected user to either join or reject callers to an ongoing Multicast conference.
A.2 Calls Properties

Auto join IP point-to-point calls
Enable the selected user to automatically join callers to an ongoing Multicast conference.

Auto reject all incoming calls
Enable the selected user to automatically reject incoming calls to an ongoing Multicast conference.

Outgoing Calls
In the Outgoing Calls tab, define properties for calls initiated by the selected vPoint end point.

Make Audio-only Call
The next call does not transmit video - the parties will only be able to hear each other. To send video, this option must not be selected.

Maximum Number of Recent Addresses
The maximum number of recently dialed addresses that can appear in the vPoint Manual Dialer's Call Log.
A.2 Calls Properties

Ringing

In the **Ringing** tab, define the sounds used by the selected end point to indicate incoming and outgoing videoconference calls.

![vPoint End Point - Ringing Properties](image)

**Ringing Settings**

**No Sound**
Select to disable all audio ringing. Only the Incoming Call and Outgoing Call messages visually indicate calls.

**Multimedia Speakers**
Select to enable ringing sounds to indicate calls.

**Incoming Ring/Outgoing Ring**
Filenames of the sounds that indicate incoming and outgoing calls.
3rd Party Viewer

In the 3rd Party Viewer tab, define the settings for transmission of an Interactive Multicast videoconference through third-party viewers.

**CAUTION** The default settings of this tab should be edited with caution.

-vPoint End Point - 3rd Party Viewer Properties-

**Announcement Frequency**  
The interval between announcements of Multicast sessions in the third-party viewer's schedule.

**Video Broadcast Format**  
The video coding standard that all parties viewing the Multicast sessions must be capable of using - H.261 and H.263. H.263 provides better video quality, especially at low bitrate transmissions.

However, video systems that do not support H.263 will not be able to receive an H.263 broadcast.

**Audio Broadcast Format**  
The audio coding standard that all parties viewing the Multicast sessions must be capable of using.
A.2 Calls Properties

**G.711 U-law/A-law**
This standard gives the lowest quality results, but all third-party viewing systems will be able to receive the broadcast.

Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local VCON technical support representative.

**G.722**
This standard gives the best quality. Select it if you know that the third-party viewing systems support it and if you think that the connection will be over high bandwidths.

**G.728**
This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the third-party viewing systems support it and if you think that the connection will be over low bandwidths.

**Video Refresh Timeout**
The maximum number of seconds required until the video broadcast is synchronized for all viewers. If the refresh value is low, the quality is lowered. If the refresh value is high, it will take a longer time to see the video display when the viewers connect. Use the default setting as a guide.

**Defaults**
Return all options to the original preset third-party viewer settings.
Interactive Multicast

In the **Interactive Settings** tab, set the default configuration for this end point's Interactive Multicast broadcasts.

![Interactive Multicast Configuration Screen]

**vPoint End Point - Interactive Multicast Properties**

**Session's Password**

To restrict entry into the Interactive Multicast videoconferences that the end point initiates, define a security password. If you want to allow anyone who calls the end point to join the conference, leave this box blank.

The default Broadcasting settings are recommended for most Multicast conditions.

**Configure Bandwidth Rate in the Bandwidth Control page**

Click the link to jump to the MXM Properties - Bandwidth Control topic, where you can set the Default Bandwidth for multicast sessions.

**Max. Participants**

The maximum number of Participants allowed in a Multicast initiated and chaired by this end point.
A.2 Calls Properties

**Video Format**
The video coding standard that all parties in the Multicast are capable of using - H.261 and H.263. H.263 provides better video quality, especially at low bitrate transmissions.

However, some video systems do not support H.263. If at least one Participant's system does not support H.263, or you are not sure, select H.261.

**Audio Format**
The audio standard that all parties in the Multicast are capable of using.

- **G.711 U-law/A-law**
  This standard gives the lowest quality results, but it must be selected if you want 3rd Party viewers to be able to join a multicast session. Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local VCON technical support representative.

- **G.722**
  This standard gives the best quality. Select it if you know that the remote parties support it and if you think that the connection will be over high bandwidths.

- **G.728**
  This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the remote parties support it and if you think that the connection will be over low bandwidths.

If you select either G.728 or G.722, and a remote party's system does not support it, that party will not be able to participate in the session.

**Broadcast IP Address**
The destination IP address for the Interactive Multicast. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.

**Video port**
The ID of the port used for the video connection.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video control port</strong></td>
<td>The ID of the port used for transferring control and synchronization information about the video transmission.</td>
</tr>
<tr>
<td><strong>Time to Live</strong></td>
<td>The maximum number of routers that the Session's packets may pass through.</td>
</tr>
<tr>
<td><strong>Audio port</strong></td>
<td>The ID of the port used for the audio connection.</td>
</tr>
<tr>
<td><strong>Audio control port</strong></td>
<td>The ID of the port used for transferring control and synchronization information about the audio transmission.</td>
</tr>
</tbody>
</table>

- Participants must use the same video, audio and control ports. Make sure that the ports you choose are available for every participant.

| **Defaults** | Click to return to the original settings. These settings help you connect to the Interactive Multicast through the default ports and/or IP address that was defined automatically by your system. |
A.3 User Data Properties

The User Info settings provide identification of the vPoint end point user. This includes the following information:

- First Name
- Company or organization
- Last Name
- E-mail address
A.4 Communication Properties

The Communication Properties dialog box may be used for viewing and controlling various network settings of vPoint end points.

LAN

The LAN Properties contain the vPoint end point's identification configuration on the local network. Additional capabilities are provided for holding videoconferences over the connected network.

vPoint End Point - LAN Properties

**IP Address**

The selected end point’s IP address.

**DNS Name**

The selected computer's name if it resides in a network that employs a DNS server (*DNS* stands for Domain Naming System, which enables computers on a network to be referred to by name in addition to IP Addresses).

**Gatekeeper IP**

The IP address of the MXM or gatekeeper from which this end point receives gatekeeper services.

**Go to General and Bandwidth Control Pages for More Settings**

Click the General link to display the selected user’s MXM General Properties (see “General” on page 97).

Click the Bandwidth Control link to display the selected user’s MXM Bandwidth Control Properties (see “Bandwidth Control Properties” on page 101).
A.4 Communication Properties

Allow Adaptive Bandwidth Adjustment

Enables videoconferences to precede at reduced bandwidth if the network is congested. Deselecting this option maintains a constant quality to the session, but it may cause network problems.

Enable Lip Synchronization Mechanization

Enables adjustment of the video and the audio if they are out of sync with each other.

Automatic Buffering Control

☑ Enables the system to automatically control the amount of buffering required to maintain the consistency of the video and audio transmission. For example, if video packets are delayed for 1 or 2 seconds, the system will automatically synchronize the transmission so that the delay does not disturb the visible video.

☑ Deselect this option only if the automatic buffering is not sufficient — for example, if the quality of the video meeting is poor or there is a noticeable delay.

Enable NAT

If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for the selected user.

NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

Enable Selection of Local IP Address

Enables the end point to receive its IP address configuration from the LAN's DHCP server. A DHCP server automatically assigns IP addresses to computers as they log on to the network, eliminating the need to assign IP addresses manually and locally.
Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization’s firewall.

![Firewall Properties](image)

**vPoint End Point - Firewall Properties**

**RTP & RTCP Port Range**

The MXM allocates a range of ports for video and audio during videoconferences.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

**H.245 Port Range**

*Applicable to vPoint and Falcon 3.0 end points only*

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences.

This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.
A.4 Communication Properties

Login

In the Login tab, define how the end point logs into an MXM.

vPoint End Point - Login Properties

Login Automatically with the Current User Name and Password

The end point automatically logs in to the MXM during vPoint's startup using the current User Name and Password. If this option is selected, the user does not have to enter login details during vPoint startup.

Change User Password

New Password that replaces the current one.

Confirm Confirmation of the new password.

If the Password boxes are blank, the current password remains valid.
A.5      **Hardware Properties**

The Hardware Properties dialog box may be used for viewing and controlling various Audio and Camera settings of vPoint end points.

**Audio**

In the Audio Settings for ViGO, you can define the audio configuration to be used during videoconferences.

**ViGO**

![Configuration Mode](image)

**vPoint Properties - Audio (ViGO)**

**Configuration Mode**

Select a mode for manual or automatic audio settings.

- **Manual** Select to choose audio settings one by one. Select this option if the selected end point has a PTZ camera or other optional hardware.

- **Private** Select to automatically select settings for headset audio.

- **Speaker** Select to automatically select settings for tower audio (if connected) or speaker audio (if a tower is not connected).
A.5 Hardware Properties

*Audio Origin*

Active if Configuration Mode is **Manual**.

Select an available audio input source. The selected end point can speak or send audio through one, two, or all three possible sources.

- **Desktop**
  - Select to use the camera’s built-in microphone.

- **Camera**
  - Select to use the supplied headset.

- **Headset**
  - Select to use a microphone that’s connected to the Line Level Audio In connector on the ViGO rear panel. The source may be from a connected VCR or other external audio device.

- **Aux/Line In**
  - Select to use a microphone that’s connected to the Line Level Audio In connector on the ViGO rear panel. The source may be from a connected VCR or other external audio device.

*Enhanced Audio*

- **Acoustic Echo Canceller**
  - Select to prevent the remote party from hearing themselves from their own speakers. This condition occurs if the speaker output is received by the selected end point’s microphone and sent back to the remote party.

- **Automatic Gain Control**
  - Select to ensure that the remote parties hear the selected end point normally regardless of the speaker’s distance from the microphone.

- **Automatic Noise Suppression**
  - Select to mute surrounding noise. The result is that the remote parties only hear what the speaker says into the microphone.

*Speaker*

Active if Configuration Mode is **Manual**.

This end point emits audio through one or both of the following devices:

- **Tower Speaker**
  - Select to emit audio from the ViGO tower’s built-in speaker.

- **Headset/External**
  - Select to emit audio from the headset or from another device connected to the Speaker connector on the ViGO’s side panel.

*Volume level*

- **Enable Speaker**
  - Select to control the volume of the selected end point’s speaker. Drag the slider accordingly.

- **Enable Microphone**
  - Select to control the volume through the selected end point’s microphone.
**Software Only**

In the Audio Settings for the vPoint software-only application (not connected to ViGO), you can define the audio configuration to be used during videoconferences.

---

**Microphone Origin**

**Sound Card Microphone**

Use a microphone that’s connected to the Line Level Audio In connector on the installed videoconferencing card.

**USB Camera Microphone**

Use the camera’s built-in microphone.

**Enhanced Audio**

**Acoustic Echo Canceller (AEC)**

Select to cancel the echo created when your microphone picks up audio from your speakers.

AEC is not available if you are using a **USB Camera Microphone**.

**Environment**

Select **Quiet, Medium, or Noisy**, as applicable, according to your surroundings. This setting controls the automatic adjustment to compensate for surrounding noise levels, so that they don't affect the outgoing audio.
A.5 Hardware Properties

Volume level

Enable Speaker  Select to control the volume of the selected end point’s speaker. Drag the slider accordingly.

Enable Microphone  Select to control the volume through the selected end point’s microphone.

Camera

The Pan/Tilt/Zoom Camera properties are applicable if a Pan/Tilt/Zoom-type (PTZ) camera is connected to the selected system. If a PTZ camera is not used, None appears as the PTZ camera type in the dialog box’s top list and no communication port is required.

Pan/Tilt/Zoom camera type  The manufacturer and/or model of the PTZ camera.

Camera’s communication port  The name of the computer port to which the camera is connected.

Allow the remote side to control camera settings  Select to permit a remote party in a video meeting to control the positioning of the selected user’s PTZ camera. If a PTZ camera is not used, this option is not relevant.
A.6 Advanced Properties

The Advanced Properties dialog box may be used for viewing end point system information and controlling various QoS, Intras, advanced Video, advanced Data, and advanced Audio settings of vPoint end points.

System Info

The System Info tab displays information about the VCON videoconferencing system that’s installed in the selected end point. If you contact VCON Technical Support (see “VCON Technical Support” on page vi before the Table of Contents) about a problem associated with this end point, include this information with your request.

![vPoint Properties - System Information]

**Software**
- **Application Version**: Version number of the vPoint application running on the end point’s computer.
- **Operating System**: Operating system that’s installed on the end point’s computer.
- **Multicast installed**: Indicates if the end point’s videoconferencing system includes VCON’s Interactive Multicast feature.
### A.6 Advanced Properties

**Hardware**

**Board Type**
Videoconferencing system installed in the end point’s computer.

**ViGO Model**
Model name of the end point’s ViGO (if applicable).

**Hardware ID**
Unique identification number for the videoconferencing card’s installation. This number is for VCON Technical Support use.

**QoS**

The QoS tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the specified vPoint end point.

#### vPoint Properties - QoS (Default Settings)

Set QoS properties as follows:

**Priority Type (QoS)**

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

- **No Priority**
  Network transfers packets using normal Best-effort (or Routine) packet transmission.

- **IP Precedence**
  Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.
To reset the Priority default values, click **Restore QoS Defaults**.

### Intras

During videoconferences, vPoint end points send periodic intras (full video frames) in order to synchronize the video display at the receiving party. You may define the interval between the transmission of intras from a specific vPoint end point.

```
\begin{figure}
\centering
\includegraphics[width=\textwidth]{vPoint_Properties_Intras.png}
\caption{vPoint Properties - Intras}
\end{figure}
```

**Send Intra Interval**

Type the length of the interval (in seconds) between intra transmissions.
Advanced Video

The Advanced Video tab permits you to enable usage of H.261 and H.263 for video transmission and to control the bandwidth thresholds for switching between the two standards, if applicable.

Transmit H.261/H.263

Enable H.261/H.263 at Maximum

Select to enable the use of the specified video format coding from the specific vPoint end point. In the box, type the maximum transmission rate at which the specific coding may be used.

For example, for H.263 the default maximum transmission rate is 256 kbps. At higher rates, the H.263 coding is not available.

Enable CIF

Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

All VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.
To reset the advanced Video default values, click **Restore Defaults**.

### Advanced Audio

In the **Audio** tab, select the supported audio algorithms for transmitting audio from the specified end point. In addition, you can enter the audio transmit speed for all algorithms supported by the end point.

To reset the advanced Audio default values, click **Restore Defaults**.

![vPoint Properties - Advanced Audio](image-url)
B MEETINGPOINT® END POINT PROPERTIES

From the MXM Administrator application, the administrator may view and control various properties of MeetingPoint® 4.5 (and higher) end points. MeetingPoint is the videoconferencing application used by VCON’s Escort and Cruiser.

Many of the properties described in this appendix are supported by the MediaConnect 9000’s Advanced Configuration.

B.1 Conversation Properties

The Conversation Properties dialog box may be used for viewing and controlling the Video and Data settings of MeetingPoint end points.

Video

You may control certain video features that improve the quality of the video transmission from the selected MeetingPoint end point.
B.1 Conversation Properties

**Video Window**

**Always on Top**
Select to keep the Video windows and their subapplications (such as Camera Controller) always on top of all open windows, even if another application is selected. When this command is not selected, a selected application may hide the Video windows.

**Display**

**Clearer Picture/Smother Motion**
This control enables you to define the relationship between clear, sharp images and smooth uninterrupted motion during the video transmission. If the picture is clearer, the motion may be slower and more broken. If the motion is smoother, the picture may be less clear.

Drag the slider until you are satisfied with the image sharpness and the smoothness of motion. There are 30 possible settings on the slider – 1 represents the clearest picture but the most uneven motion; 30 represents the smoothest motion but the most blurry picture.

**Video Format**

The type of video format in which the current video meeting is broadcast. This setting affects the viewing quality for the remote party, and may only be changed during a call. The possible options are:

**Normal (CIF)**
Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

All VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

**Quarter Size (QCIF)**
Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF).

QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.
**Display Mode**

This setting is applicable if the end point is a MediaConnect 8000 system. The display mode determines how local video, remote video and software applications (such as MeetingPoint) are displayed at this end point.

**Single Monitor**  Video and applications on the SVGA monitor only.

**Dual Monitor**  Video on the TV monitor, applications on the SVGA monitor.

**Triple Monitor**  Local video on one TV monitor, remote video on the second TV monitor, and applications on the SVGA monitor.

**Attributes**

**Use H.261 for ISDN when possible**  Select if you are sure of gaining a connection at a higher bitrate—for example, if you are dialing 3 or more ISDN channels.

The default codec recommendation is H.263, which includes techniques for improved video performance over low bitrates.
B.1 Conversation Properties

Data

The **Data** tab provides several options for preparing to share data during videoconferences.

**MeetingPoint End Point - Data Properties**

**Data Applications**

**Use MeetingPoint Data Applications**
- Select if you want the selected user to use MeetingPoint’s standard data sharing features. Selecting this option can save you time and computer memory.

**Use NetMeeting Data Application**
- Select if you want the selected user to use the full Microsoft NetMeeting data sharing application.

If you change the data sharing method, the change only takes effect after the end point exits and start MeetingPoint again.

It is recommended to select a common data sharing method for all logged-in users.
**File Transfer**

**Default Directory**
This box shows the path of the folder that receives files transferred to the selected computer during a video meeting.

**Application Sharing**

**Auto Collaborate**
Select to automatically enable a remote party to work (instead of observing passively), together with the selected user, in a shared application.

**Setting**

**Enable Full Data Bandwidth**
This feature permits temporary increases in bandwidth during a video meeting. This speeds up the transfer of large amounts of data. The system temporarily uses the bandwidth allocated for video transmission for the transfer of data. This results in the prevention of video transmission until data transfer is complete.

**Always use Data in Interactive Multicast Sessions**
Select to open a data connection automatically whenever the selected user initiates an Interactive Multicast video meeting as the chair.
B.2 Calls Properties

The Calls Properties dialog box may be used for viewing and controlling incoming call and multicast (if applicable) properties of MeetingPoint end points.

Incoming Calls

In the **Incoming Calls** tab, customize how the MeetingPoint end point indicates and accepts incoming calls.

**MeetingPoint End Point - Incoming Calls Properties**

**When Idle**

**Auto answer**  
Select to enable the selected user to automatically accept all calls when its system is not in a video meeting.

**As Interactive Multicast Chair**

If the end point supports VCON's Interactive Multicast, it may sometimes be the Chair of multicast video meetings. If another party calls it while it chairs a meeting, that call may be accepted or rejected according to the selected option:

**Manually join IP point-to-point calls**  
Select to enable the selected user to either join or reject callers to an ongoing Multicast meeting.
B.2 Calls Properties

**Auto join IP point-to-point calls**
Select to enable the selected user to automatically join callers to an ongoing Multicast meeting.

**Auto reject all incoming calls**
Select to enable the selected user to automatically reject incoming calls to an ongoing Multicast meeting.

**Ringing**
You can define the method to notify the selected user that a call is coming in or going out.

![MeetingPoint End Point - Ringing Properties](image)

*Ringing Settings*

**No Sound**
Select to receive calls and to call out with no accompanying ringing sound.

**Internal Speaker**
Select if you want the ringing to originate from the computer’s standard speaker.
B.2 Calls Properties

**Multimedia Speakers**
Select if you want the ringing to originate from connected external speakers.

**Incoming Ring/Outgoing Ring**
If the end point is using external speakers, ringing sounds other than the defaults may be used. If applicable, the appropriate filenames appear in these boxes.

### 3rd Party Viewer

This tab is only available for end points with the Interactive Multicast option.

The Calls Properties **3rd Party Viewer** tab contains options for transmission of an Interactive Multicast video meeting through third-party viewers.

**MeetingPoint End Point - 3rd Party Viewer Properties**

**Settings**

**Announcement Frequency**
In this list, click the number of minutes as an interval between announcements of the Multicast video meeting in the third-party viewer’s schedule. Persons subscribing to the third-party viewer can see the announcement when they are online.
3rd Party Viewer Format

The default third-party viewer settings are recommended for most Multicast broadcasting conditions. Change them ONLY if the remote systems’ specifications differ from the default values.

Video Broadcast Format
In this list, click a format that all parties in the meeting are capable of using.

Audio Broadcast Format
In this box, click the audio standard that all parties in the meeting are capable of using.

For third-party-compatible video meetings, the above settings are used instead of the Broadcast Format settings in the Interactive Multicast tab.

Video Refresh Timeout
In this list, click the maximum number of seconds required until the video broadcast is synchronized for all viewers.

Restore Defaults
Click this button to return to the original preset third-party viewer settings.
Interactive Multicast

This tab is only available for end points with the Interactive Multicast option.

In the Call Properties Interactive Multicast tab, define the default configuration for Interactive Multicast video meetings.

MeetingPoint End Point - Interactive Multicast Properties

Broadcast

The default Broadcast settings are recommended for most Multicast broadcasting conditions. Change them ONLY if your network’s specifications require different settings (for example, if your organization has a firewall).

Session’s Password

If you want to restrict entry into the Interactive Multicast video meetings that the end point initiates, define a security password. In this box, type the characters that make up the password.

If you want to allow anyone who calls the end point to join the multicast meeting, leave this box blank.
### B.2 Calls Properties

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Bandwidth Rate in the Bandwidth Control page</strong></td>
<td>Click the link to jump to the MXM Properties - Bandwidth Control topic, where you can set the Default Bandwidth for multicast sessions.</td>
</tr>
<tr>
<td><strong>Video Format</strong></td>
<td>In this box, click the video coding standard that all parties in the meeting are capable of using.</td>
</tr>
<tr>
<td><strong>Audio Format</strong></td>
<td>In this box, click the audio standard that all parties in the meeting are capable of using.</td>
</tr>
<tr>
<td><strong>Broadcast to IP Address</strong></td>
<td>In this box, type the destination IP address for an Interactive Multicast video meeting. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of <strong>224.0.0.0</strong> to <strong>239.255.255.255</strong>.</td>
</tr>
<tr>
<td><strong>Video Port</strong></td>
<td>In this box, type the ID of the port used for the video connection.</td>
</tr>
<tr>
<td><strong>Video Control Port</strong></td>
<td>In this box, type the ID of the port used for transferring control and synchronization information about the video transmission.</td>
</tr>
<tr>
<td><strong>Audio Port</strong></td>
<td>In this box, type the ID of the port used for the audio connection.</td>
</tr>
<tr>
<td><strong>Audio Control Port</strong></td>
<td>In this box, type the ID of the port used for transferring control and synchronization information about the audio transmission.</td>
</tr>
<tr>
<td><strong>Time to Live (TTL)</strong></td>
<td>In this list, click the maximum number of routers that the packets sent from your system may pass through.</td>
</tr>
<tr>
<td><strong>Audio Packet Size</strong></td>
<td>In the box, enter the number of bits that make up a packet carrying audio.</td>
</tr>
</tbody>
</table>
B.3 User Data Properties

The End Point User Data property dialog boxes may be used for viewing and entering identification, business and location information about the selected user. This information is optional and does not affect the functioning of the MXM and the communication within its network.

MeetingPoint End Point - General User Properties

MeetingPoint End Point - Location Properties
B.4 Communication Properties

The Communication Properties dialog box may be used for viewing and controlling various LAN settings of MeetingPoint end points.

LAN

This tab contains configuration information for holding video meetings over the connected LAN.

### MeetingPoint End Point - LAN Properties

- **IP Address**: The selected end point’s IP address.
- **DNS Name**: The selected computer's name (*DNS* stands for Domain Naming System, which enables computers on a network to be referred to by name in addition to IP Addresses.
- **Gatekeeper IP**: The IP address of the MXM or gatekeeper from which this end point receives gatekeeper services.
- **Go to General and Bandwidth Control Pages for More Settings**: Click the General link to display the selected user’s MXM General Properties (see “General” on page 97) or the Bandwidth Control link to display the selected user's MXM Bandwidth Control Properties.
### B.4 Communication Properties

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Adaptive Bandwidth Adjustment</strong></td>
<td>Select this option to enable reduction of the allotted bandwidth if the network is congested.</td>
</tr>
<tr>
<td><strong>Enable Lip Synchronization Mechanization</strong></td>
<td>Select this option to enable adjustment of the video and the audio if they are out of sync with each other (see the MeetingPoint User Guide, Appendix B, “Monitoring the Conversation State”).</td>
</tr>
<tr>
<td><strong>Automatic Buffering Control</strong></td>
<td>☐ Select this option to enable the system to automatically control the amount of buffering required to maintain the consistency of the video and audio transmission. For example, if video packets are delayed for 1 or 2 seconds, the system will automatically synchronize the transmission so that the delay does not disturb the visible video. ☐ Deselect this option only if the automatic buffering is not sufficient — for example, if the quality of the video meeting is poor or there is a noticeable delay.</td>
</tr>
<tr>
<td><strong>Do not show Network Congestion dialog box</strong></td>
<td>Select this option if you do not want to notify the selected end point when its calls are transmitted at a lower bandwidth because of network congestion.</td>
</tr>
</tbody>
</table>
| **Enable NAT**                               | If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for the selected user.  
NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.  
This feature is applicable only to MeetingPoint 4.6 end points and higher. |
Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization’s firewall.

**MeetingPoint End Point - Firewall Properties**

**RTP & RTCP Port Range**

The MXM allocates a range of ports for video and audio during videoconferences.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.
B.4 Communication Properties

Login

In the **Login** tab, define how the end point logs into an MXM.

*MeetingPoint End Point - Login Properties*

**Login**

The end point automatically logs in to the MXM during vPoint's startup using the current User Name and Password. If this option is selected, the user does not have to enter login details during vPoint startup.

**Automatically with the Current User Name and Password**

If the Password boxes are blank, the current password remains valid.

**Change User Password**

**New**

Password that replaces the current one.

**Confirm**

Confirmation of the new password.
Connection

In the **Connection** list, select the type of external communication line (LAN or ISDN) the selected system will use. Selecting **None** enables the end point to videoconference only on the connected LAN.

This dialog box is applicable only to VCON Cruisers and MediaConnect 8000s that are set up for ISDN connection.

*MeetingPoint End Point - Connection Properties*
B.5 Telephony Properties

The Telephony Properties dialog box may be used for viewing and controlling various ISDN settings.

These properties are only applicable only to VCON Cruisers and MediaConnect 8000s that are set up for ISDN connection.

**Phone Numbers**

The **Phone Numbers** tab lists the end point’s ISDN phone numbers, if applicable.

---

**MeetingPoint End Point - Phone Numbers Properties**

**Number of ISDN Lines to be Used**

The number of ISDN lines the selected system uses. The number of available lines depends on the number of BRIs (Basic Rate Interface) on the videoconferencing card. Each BRI supports up to two phone lines of 64 kbps each (56 kbps in Restricted networks):

- Cruiser 150 - Up to 2 ISDN lines (1 BRI)
- Cruiser 384/MediaConnect 8000 - Up to 6 ISDN lines (3 BRI)

**Phone Numbers**

The ISDN numbers of each line. Do not include your own country’s international code or your local area code.
Switch Type

The **Switch Type** tab contains information about the ISDN switch type used by the selected end point.

### MeetingPoint End Point - Switch Type Properties

**Your Location**

The country in which the selected user is located.

**Switch Type**

If applicable, the most common switch type for the user’s country appears automatically. If a different switch type is being used (according to your ISDN carrier), select it from the list.

**Check this Box if you Have Restricted 56K Access**

In some areas (such as the United States, Canada, Korea and Japan), the main ISDN network is Restricted (data rate of 56K). If applicable to the selected user, select this option.
SPID Numbers

If the selected ISDN Switch Type supports Service Profile Identifiers (SPID), the SPID Numbers tab lists them for the ISDN lines. A SPID number relates to the capabilities of the end point on the ISDN line. This information may be obtained from the end point's ISDN carrier.

**MeetingPoint End Point - SPID Properties**

**Number of SPIDs**
Select the number of SPID numbers that were specified by your ISDN carrier.

**SPID Numbers 1,2,3,4,5,6**
Type the SPID numbers as your ISDN carrier specifies. If your ISDN provider gave the selected end point only one SPID number, enter it in **SPID 1**.
**MSN**

The **MSN** tab is relevant if the connected ISDN network supports Multiple Subscriber Numbering (MSN).

**MeetingPoint End Point - MSN Properties**

Select **MSN Support** to use MSN capabilities. In the MSN Address boxes, type the exact MSN numbers for the end point.
Subaddressing

Subaddressing is applicable if the selected system shares an ISDN BRI line with other equipment (such as other computers, fax machines, standard telephones, and so on). In such a case, the computer has an additional series of numbers and/or letters added to the end of its phone number.

MeetingPoint End Point - Subaddressing Properties

**Sub-Addressing**

Phone number followed by an “|” character, and the series of numbers and/or letters making up the subaddress.
Dialing

The Dialing Information area displays the **Country** that the selected user is in, the area code, and the appropriate digits for dialing an outside line (**External**), a **Long Distance** call, or an **International** call.

If the user needs to dial a specific digit to receive an external line, you must type that digit before the digits required for a long distance or international call.

For example, if you must dial 9 to receive an external line, and then 01 to dial long distance, type **901** in the Long Distance box.
B.6 Hardware Properties

The Hardware Properties dialog box may be used for viewing and controlling various Audio and Camera settings of MeetingPoint end points.

Audio

The Audio settings vary, according to the VCON videoconferencing product installed in the selected end point.

Escort/Cruiser 150 Audio

![Escort Demo Properties (Escort)](image)

**Default Audio Device**

**Private**

Select for listening to audio through the handset. In the **Private** list, click the type of handset being used (default is **Handset 1.0**).

**Speaker**

Select for listening to audio through speakers connected to the computer. In the **Speaker** list, click the type that is most suitable to the speakers installed.
## Microphone Origin

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always use Desktop camera microphone</td>
<td>Select to use the camera’s built-in microphone at all times.</td>
</tr>
<tr>
<td>Always use “Line-level” AUD IN audio input</td>
<td>Select to use a microphone that’s connected to the Line Level Audio In port of the end point’s videoconferencing card.</td>
</tr>
<tr>
<td>Switch audio when Camera is switched</td>
<td>Select to always use the microphone of the selected camera. If you switch to a second camera, that camera’s microphone is used.</td>
</tr>
</tbody>
</table>

## Volume Level

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Speaker</td>
<td>Select to control the volume of the selected end point’s speaker. Drag the slider accordingly.</td>
</tr>
<tr>
<td>Enable Microphone</td>
<td>Select to control the volume through the selected end point’s microphone. Drag the slider accordingly.</td>
</tr>
</tbody>
</table>
**B.6 Hardware Properties**

**ViGO**

### Configuration Mode

Select a mode for manual or automatic audio settings.

- **Manual**
  
  Select to choose audio settings one by one. Select this option if the selected end point has a PTZ camera or other optional hardware.

- **Private**
  
  Select to automatically select settings for headset audio.

- **Speaker**
  
  Select to automatically select settings for tower audio (if connected) or speaker audio (if a tower is not connected).

### Audio Origin

Active if Configuration Mode is **Manual**.

Select an available audio input source. The selected end point can speak or send audio through one, two, or all three possible sources.

- **Desktop Camera**
  
  Select to use the camera’s built-in microphone.

- **Headset**
  
  Select to use the supplied headset.
**B.6 Hardware Properties**

**Aux/Line In**
Select to use a microphone that’s connected to the Line Level Audio In connector on the ViGO rear panel. The source may be from a connected VCR or other external audio device.

**Enhanced Audio**

**Acoustic Echo Canceller**
Select to prevent the remote party from hearing themselves from their own speakers. This condition occurs if the speaker output is received by the selected end point’s microphone and sent back to the remote party.

**Automatic Gain Control**
Select to ensure that the remote parties hear the selected end point normally regardless of the speaker’s distance from the microphone.

**Automatic Noise Suppression**
Select to mute surrounding noise. The result is that the remote parties only hear what the speaker says into the microphone.

**Speaker**

Active if Configuration Mode is **Manual**.

The selected end point emits audio through one or both of the following devices:

**Tower Speaker**
Select to emit audio from the ViGO tower’s built-in speaker.

**Headset/External**
Select to emit audio from the headset or from another device connected to the Speaker connector on the ViGO’s side panel.

**Volume level**

**Enable Speaker**
Select to control the volume of the selected end point’s speaker. Drag the slider accordingly.

**Enable Microphone**
Select to control the volume through the selected end point’s microphone.
Cruiser 384/MediaConnect 8000

Cruiser 384 - Audio Properties

Audio Origin

**Tabletop Microphone**
Select to use a tabletop microphone. Applicable to MediaConnect 8000.

**Camera Microphone**
Select to use the camera’s built-in microphone. Applicable to Cruiser 384.

**Aux/Line-in**
Select to use a microphone that’s connected to the Line Level Audio In connector on the installed video system board. The source may be from a connected VCR or other external audio device.

If this option is selected, the only available Mixing Mode is **No Mixing**.
### Mixing Mode

Using the following table as a guide, select the setup that best suits the end point’s audio requirements.

<table>
<thead>
<tr>
<th>Mixing Mode</th>
<th>Audio Origin</th>
<th>Microphone</th>
<th>Aux/Line in</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Mixing</td>
<td></td>
<td>All parties hear audio only from the microphones.</td>
<td>All parties hear audio from their remote sides and from the connected auxiliary equipment (such as VCR or 2-way speaker).</td>
</tr>
<tr>
<td>Playback</td>
<td></td>
<td>All parties hear audio only from a connected VCR.</td>
<td>Not available.</td>
</tr>
<tr>
<td>Playback + Narration</td>
<td></td>
<td>The remote party hears audio from both the connected VCR and the microphones.</td>
<td>Not available.</td>
</tr>
<tr>
<td>Record</td>
<td></td>
<td>If the video meeting is being recorded, the audio is recorded from the video meeting to the VCR.</td>
<td>Not available.</td>
</tr>
<tr>
<td>External Phone</td>
<td></td>
<td>Enable a telephone party (using Plain Old Telephone Service, or POTS) to hear audio and to be heard by you and the other participants.</td>
<td>Not available.</td>
</tr>
</tbody>
</table>
## Enhanced Audio

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Echo Cancellation</strong></td>
<td>Select to prevent the remote party from hearing themselves from their own speakers. This condition occurs if the speaker output is received by the local microphone and sent back to the remote party.</td>
</tr>
<tr>
<td><strong>Automatic Gain Control</strong></td>
<td>Select to ensure that the remote party hears the local side normally regardless of the person’s distance from the microphone.</td>
</tr>
<tr>
<td><strong>Automatic Noise Suppression</strong></td>
<td>Select to mute surrounding noise. The result is that the remote party only hears what the local person says into the microphone.</td>
</tr>
</tbody>
</table>

### Volume level

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Speaker</strong></td>
<td>Select to control the volume of the selected endpoint’s speaker. Drag the slider accordingly.</td>
</tr>
<tr>
<td><strong>Enable Microphone</strong></td>
<td>Select to control the volume through the selected endpoint’s microphone.</td>
</tr>
</tbody>
</table>
Camera

The Pan/ Tilt/Zoom Camera properties are applicable if a Pan/Tilt/Zoom-type (PTZ) camera is connected to the selected system. If a PTZ camera is not used, None appears as the PTZ camera type in the dialog box’s top list and no communication port is required.

*MeetingPoint End Point - Camera Properties*

**Camera**

**Pan/Tilt/Zoom camera type**

The manufacturer and/or model of the PTZ camera.

**Camera’s communication port**

The name of the computer port to which the camera is connected.

**Camera Control**

**Allow the remote side to control camera settings**

Select to permit a remote party in a video meeting to control the positioning of the selected user’s PTZ camera. If a PTZ camera is not used, this option is not relevant.
B.7 Advanced Properties

The Advanced Properties dialog box may be used for viewing end point system information and controlling various QoS, Intras, advanced Video, advanced Data, and advanced Audio settings of MeetingPoint end points.

System Info

This tab displays information about the VCON videoconferencing system that’s installed in the selected end point. If you contact VCON Technical Support (see “VCON Technical Support” on page vi before the Table of Contents) about a problem associated with this end point, include this information with your request.

---

**MeetingPoint End Point - System Information**

**Software**

**Application Version**

Version number of the MeetingPoint application running on the end point’s computer.

**Operating System**

Operating system that’s installed on the end point’s computer.

**Multicast installed**

Indicates if the end point’s videoconferencing system includes VCON’s Interactive Multicast feature.
Hardware

Board Type  Videoconferencing system installed in the end point’s computer.

Hardware ID  Unique identification number for the videoconferencing card’s installation. This number is for VCON Technical Support use.

QoS

The QoS tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the specified MeetingPoint end point.

MeetingPoint End Point - QoS Properties - Default Settings

Set QoS properties as follows:

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority  Network transfers packets using normal Best-effort (or Routine) packet transmission.
### B.7 Advanced Properties

<table>
<thead>
<tr>
<th><strong>IP Precedence</strong></th>
<th>Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diffserv</strong></td>
<td>Network transfers packets according to specific needs of the sending application.</td>
</tr>
</tbody>
</table>

#### Priority Values

**Video, Audio and RTCP Priority**

For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix C, “QoS Priority Values”.

To reset the Priority default values, click **Restore QoS Defaults**.
Intras

During videoconferences, MeetingPoint end points send periodic intras (full video frames) in order to synchronize the video display at the receiving party. You may define the interval between the transmission of intras from a specific MeetingPoint end point.

**MeetingPoint End Point - Intras Properties**

**Send Intra Interval**
Type the length of the interval (in seconds) between intra transmissions.
B.7 Advanced Properties

Advanced Video

The advanced Video tab permits you to enable usage of H.261 and H.263 for video transmission and to control the bandwidth thresholds for switching between the two standards, if applicable.

MeetingPoint End Point - Advanced Video Properties

Transmit H.261/H.263

**Enable H.261/H.263 at Maximum**

Select to enable the use of the specified video format coding from the specific MeetingPoint end point. In the box, type the maximum transmission rate at which the specific coding may be used.

For example, for H.263 the default maximum transmission rate is 256 kbps. At higher rates, the H.263 coding is not available.

**Enable CIF**

CIF (Common Interchange Format) provides a higher resolution at a lower frame rate. If a higher bandwidth is available, CIF provides excellent video quality.

**Enable QCIF**

QCIF (Quarter Size Common Interchange Format) should be used if only low bandwidth is available, or if the remote party in a videoconference does not support CIF.
B.7 Advanced Properties

**Video Transmit**

- **maximum packet size**
  
Enter the maximum video packet size (in bytes) which the specified end point may transmit.

To reset the advanced Video default values, click **Restore Defaults**.

**Advanced Audio**

In the **Audio** tab, select the supported audio algorithms for transmitting audio from the specified end point. In addition, you can enter the audio transmit speed for all algorithms supported by the end point.

To reset the advanced Audio default values, click **Restore Defaults**.

*MeetingPoint End Point - Advanced Audio Properties*
C  FALCON™ END POINT PROPERTIES

From the MXM Administrator application, the administrator may view and control various properties of Falcon™ end points. In the Falcon Properties dialog box, the properties are divided into various categories:

- **MXM**
  Properties defining how the Falcon operates as parts of the MXM videoconferencing network (see “Setting End Point MXM Properties” on page 97).

- **Network**
  LAN, Firewall, H.323, QoS, Phone Numbers, Switch Type, SPID Numbers

- **Video**
  Dual Monitor, Far End Camera Control

- **Audio**
  Audio Input, VCR Audio Mix, automatic adjustments

- **Options**
  General, Version

Properties cannot be changed while the Falcon is engaged in a videoconference.
C.1 Network Configuration

This section explains how to set up the Falcon’s network and connections configuration. Network options may be edited at any time.

LAN Connection and Registration

The LAN tab includes the Falcon’s address and information about its connection to the LAN (Local Area Network).

![Falcon LAN Properties]

**Obtain an IP Address from a DHCP server**
Select to enable Falcon to receive its network configuration from the LAN’s DHCP server and enter it automatically in the LAN tab.

If this option is not selected, the LAN properties must be entered manually.

**IP Address**
IP address of the Falcon.

If Falcon receives an address automatically, it is a temporary address which is liable to be changed when the network’s users’ IP addresses are updated periodically.

If you manually enter an IP address here, the address remains permanently.

**Subnet Mask**
Your company’s subnet mask.
Firewall

In the Firewall tab, enter the allocation of ports for communication through your organization’s firewall.

---

**DNS Server & WINS Server**

- **Domain**
  - DNS domain name of your company (for example, `yourcompany.com`).

- **Default Gateway**
  - IP address of the network’s Gateway router. The gateway helps Falcon send and receive calls between subnets.

---

**Falcon Firewall Properties**

**RTP & RTCP Port Range**

- The MXM allocates a range of ports for video and audio during videoconferences.

  - This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.
C.1 Network Configuration

Use the same port number for RTP reception and transmission

H.245 Port Range

**Applicable to vPoint and Falcon 3.0 end points only**

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences. This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

**H.323 Management**

In the **H.323** tab, you can define how the Falcon operates within a managed H.323 videoconferencing network.

**Gatekeeper IP**

Enter the IP address of the gatekeeper which manages the Falcon. This may be either the MXM’s gatekeeper or another one used by your organization.
If the Falcon is logged in to a non-VCON gatekeeper, the Falcon’s status in the Main View is “Logged In to Management Server.”

**NAT IP**

If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for your computer.

NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

**Enable Lip Synchronization Mechanism**

Select this option to synchronize the audio and video of a LAN conversation.

**Automatic Buffering Control**

Buffer Control adjusts the video streams for the available dynamic bandwidth of IP networks.

Select this option to make the buffer control automatic. Deselect it to make it adjustable during LAN conversations.
QoS

The QoS tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the Falcon.

*Falcon QoS Properties*

**Priority Type (QoS)**

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

**No Priority**  
Network transfers packets using normal Best-effort (or Routine) packet transmission.

**IP Precedence**  
Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.

**Diffserv**  
Network transfers packets according to specific needs of the sending application.
C.1 Network Configuration

**Priority Values**

**Video Priority**

For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or DiffServ. For a list of Priority levels, see Appendix D, “QoS Priority Values.”

To reset the Priority default values, click **Restore QoS Defaults**.

**Phone Numbers**

The **Phone Numbers** tab lists the Falcon’s ISDN numbers of each line. Do not include your own country’s international code or your local area code.

![Falcon ISDN Phone Numbers](image)

*Falcon ISDN Phone Numbers*
Switch Type

In the Switch Type tab, the ISDN switch type used by the Falcon appears. If a different switch type is being used (according to the ISDN carrier), select it from the list.

*Falcon ISDN Switch Type*
C.1 Network Configuration

SPID Numbers

If the selected ISDN Switch Type supports Service Profile Identifiers (SPID), this tab lists them for the ISDN lines. A SPID number relates to the capabilities of the end point on the ISDN line. This information may be obtained from the Falcon's ISDN carrier.

Falcon SPID Numbers

**SPID numbers**  Type the SPID numbers as your ISDN carrier specifies. If your ISDN provider gave you only one SPID number, enter it in SPID 1.
C.2 Video Properties

The Video tab provides options for controlling the display of video in the Falcon IP.

### Falcon Video Properties

**Dual Monitor**
Falcon supports the use of two monitors to display both parties on full screens during videoconferences. One monitor displays remote video and the other monitor displays local video. Select this option only if two TV monitors are connected.

**Camera Control by Far End**
Far End Camera Control (FECC) enables the remote party to control the local party's camera, so that they see views that are convenient for them. FECC provides control over the pan/tilt/zoom positioning and the adjustment of brightness, color, contrast and hue.

**Minimum time between two intras**
During videoconferences, Falcon end points send periodic intras (full video frames) in order to synchronize the video display at the receiving party. Type the length of the interval (in seconds) between intra transmissions.

**Enable H.323 Annex Q**
Select to operate Far End Camera Control (FECC) based on ITU H.323 Annex Q Recommendations.
C.3 Audio Properties

In the Audio tab, you can select and activate various audio properties in the selected Falcon.

*Falcon Audio Properties*

**Audio input**

**Tabletop Mic**
To use the supplied tabletop microphone or other audio device connected to the Falcon’s MIC connector, select Tabletop Mic.

**Line Level**
To use the microphone or audio device (such as VCR, mixer, etc.) connected to the Falcon’s VCR AUD IN connector, select Line Level.

**VCR audio mix**
Mixing options determine how the audio from a VCR connected to the Falcon is mixed and sent to the remote party or recorded to a VCR cassette. Select the appropriate VCR Audio Mix option:

**No Mix**
Both parties hear each other’s audio only.

**VCR Record**
Both parties hear each other’s audio while a VCR records both of them.
C.3 Audio Properties

**VCR Playback**
Both parties hear each other’s audio and the audio from a video cassette.

Falcon supports advanced features that improve audio quality for different types of videoconferencing environments.

**Acoustic Echo Cancellation (AEC)**
Select to prevent the remote party from hearing themselves from their own speakers (selected by default). This condition occurs if the speaker output is received by the selected end point's microphone and sent back to the remote party. You should deselect AEC only if an external AEC device is in use.

**Automatic Gain Control (AGC)**
Select to ensure that the remote parties hear the selected end point normally regardless of the speaker's distance from the microphone. AGC improves audio for big rooms.

**Automatic Noise Suppression (ANS)**
Select to mute surrounding noise. The result is that the remote parties only hear what the speaker says into the microphone.

The gain level is the boost in signalling power when the audio signal is increased. Depending on your microphone or other audio input, you may adjust the gain to a suitable level. Use the Gain Levels table below as a guide for choosing an appropriate level.

**Microphone Gain Level**
Gain level for the microphone.

**Line In Gain Level**
Gain level for the Line In input (for example, from a VCR).

**Gain Levels**

<table>
<thead>
<tr>
<th>Level</th>
<th>Gain in decibels</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>12 dB</td>
</tr>
<tr>
<td>1</td>
<td>10 dB</td>
</tr>
<tr>
<td>2</td>
<td>8 dB</td>
</tr>
<tr>
<td>3</td>
<td>6 dB</td>
</tr>
<tr>
<td>4</td>
<td>4 dB</td>
</tr>
<tr>
<td>5</td>
<td>2 dB</td>
</tr>
<tr>
<td>6</td>
<td>0 dB</td>
</tr>
<tr>
<td>7</td>
<td>-2 dB</td>
</tr>
</tbody>
</table>
C.4 Options

General Options

The General Options tab contains several options for defining how the selected Falcon operates.

Falcon General Options

**Auto Answer**
Select to enable the selected Falcon to accept all incoming calls automatically (unless it is already engaged in a call).

Select **Mute outgoing audio for auto-answered call** if you don’t want the remote party to hear your outgoing audio at the start of an auto-answered videoconference.

**View Active Keys**
Select to display a graphic of the remote control on the selected Falcon's monitor. The graphic shows which functions are available and their respective keys at any given time.

**Remote Access**
Select to enable remote management (through a Web browser) of the selected Falcon's configuration from another terminal.

This setting does not affect management through the Property dialog box in the MXM Administrator.
C.4 Options

**Instant All**  
Select to enable the selected Falcon to dial all ISDN numbers of a remote party at the same time and then synchronize. This may help speed up the connection.

**Force G.722**  
Select to enable the selected Falcon to transmit audio according to G.722 standard, producing high audio quality. The remote device must also support G.722. If the remote device is also Falcon, this option must also be selected on it.

**Accept Multicast Floor Anytime**  
If this option is selected, the end point automatically receives the Floor every time the Chair grants it during Multicast calls, therefore skipping the confirmation message.

**Language**  
Select the language of the selected Falcon's interface. All menus and options appear in the selected language.

**Version**

The **Version** tab displays hardware and software version information for the Falcon. If you contact VCON's Technical Support about this unit, provide the information on this page.

If the Falcon model changes (among LAN only, 1-BRI, 3-BRI models), enter the new Software Key that you received from your VCON distributor.

![Falcon Version Information](image)

*Falcon Version Information*
Security

The **Security** tab enables you to set restrictions on the use of the Falcon IP and to protect it from unauthorized use, such as configuration changes and unpermitted videoconferencing calls.

**Falcon Security Properties**

**Security Mode**

- **Dual**
  - IP and ISDN calls and configuration are permitted.

- **ISDN only**
  - Only ISDN calls and configuration are permitted. IP calls are unavailable and configuration is disabled.

- **LAN only**
  - Only IP calls and configuration are permitted. ISDN calls are unavailable and configuration is disabled.
### C.4 Options

**Lock System**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock system user interface</td>
<td>Select to prevent access to Falcon functions and menus by unauthorized persons. Videoconferencing users will be unable to dial or receive calls, or change any configuration properties. A password is required to gain access to videoconferencing and configuration settings.</td>
</tr>
<tr>
<td>Enter password to unlock user interface</td>
<td>A password prevents unauthorized Falcon users from changing the system’s configuration, initiating videoconferences, and/or accepting videoconference calls. The password is mandatory for locking the system completely from all of the actions stated above.</td>
</tr>
<tr>
<td>Ban user from making calls</td>
<td>Select to prevent users from initiating calls.</td>
</tr>
<tr>
<td>Disable user configuration changes</td>
<td>Select to prevent unauthorized changes to the system configuration. The system's configuration is then disabled to videoconferencing users.</td>
</tr>
</tbody>
</table>
The tables in this appendix list the available priority values for Quality of Service (QoS) configuration. The MXM Administrator application supports QoS configuration of VCON vPoint, MeetingPoint 4.5 (and higher), and Falcon end points.

### D.1 IP Precedence Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Routine</td>
</tr>
<tr>
<td>1</td>
<td>Priority</td>
</tr>
<tr>
<td>2</td>
<td>Immediate</td>
</tr>
<tr>
<td>3</td>
<td>Flash</td>
</tr>
<tr>
<td>4</td>
<td>Flash Override</td>
</tr>
<tr>
<td>5</td>
<td>Critic/ECP</td>
</tr>
<tr>
<td>6</td>
<td>Internetwork Control</td>
</tr>
<tr>
<td>7</td>
<td>Network Control</td>
</tr>
</tbody>
</table>
## D.2 DiffServ Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>Probability Timely Forwarding 0</td>
</tr>
<tr>
<td>001000</td>
<td>Probability Timely Forwarding 1</td>
</tr>
<tr>
<td>010000</td>
<td>Probability Timely Forwarding 2</td>
</tr>
<tr>
<td>011000</td>
<td>Probability Timely Forwarding 3</td>
</tr>
<tr>
<td>100000</td>
<td>Probability Timely Forwarding 4</td>
</tr>
<tr>
<td>101000</td>
<td>Probability Timely Forwarding 5</td>
</tr>
<tr>
<td>110000</td>
<td>Probability Timely Forwarding 6</td>
</tr>
<tr>
<td>111000</td>
<td>Probability Timely Forwarding 7</td>
</tr>
<tr>
<td>101110</td>
<td>Expedited Forwarding</td>
</tr>
<tr>
<td>001010</td>
<td>Forward Class 1 Low Drop</td>
</tr>
<tr>
<td>001100</td>
<td>Forward Class 1 Mid Drop</td>
</tr>
<tr>
<td>001110</td>
<td>Forward Class 1 High Drop</td>
</tr>
<tr>
<td>010010</td>
<td>Forward Class 2 Low Drop</td>
</tr>
<tr>
<td>010100</td>
<td>Forward Class 2 Mid Drop</td>
</tr>
<tr>
<td>010110</td>
<td>Forward Class 2 High Drop</td>
</tr>
<tr>
<td>011010</td>
<td>Forward Class 3 Low Drop</td>
</tr>
<tr>
<td>011100</td>
<td>Forward Class 3 Mid Drop</td>
</tr>
<tr>
<td>011110</td>
<td>Forward Class 3 High Drop</td>
</tr>
<tr>
<td>100010</td>
<td>Forward Class 4 Low Drop</td>
</tr>
<tr>
<td>100100</td>
<td>Forward Class 4 Mid Drop</td>
</tr>
<tr>
<td>100110</td>
<td>Forward Class 4 High Drop</td>
</tr>
</tbody>
</table>
E  USING ACCORD® MGC™ WITH THE MXM

The Accord® MGC™ operates under a different configuration model than most other MCUs being used in the videoconferencing sector. This appendix provides instructions for setting up the MGC’s configuration for operation in conjunction with the MXM. In addition, this appendix includes instructions for setting up an Accord Meeting Room for ad-hoc videoconferences.

This appendix only provides information directly related to the integrated operation of the Accord MGC with the MXM. For additional information about using the MGC, see the MGC’s accompanying user documentation.

E.1  MGC Configuration

Network Services Configuration

Create a new Network Service, or if you’re editing an existing configuration, choose the one that you want to change.

➢ To set up Network Service properties

1. Run the Accord MGC management application.

2. In the left pane, browse through the tree to MCU Configuration, Network Services, and Network Services-H.323.
3. Create a new Network Service or choose the existing one allocated for use with your MXM.

4. In the **Setting** tab, enter the following information:

   **Subnet Mask**  
   IP subnet mask used by the connected network.

   **Default Router**  
   IP address of the default router used by the connected network.

   **External Gatekeeper**  
   Select this option. The MXM is an external gatekeeper in relation to the MGC.
Network Services - Setting Configuration for MXM

5. In the **Gatekeeper** tab, enter the following information:

- **External IP address** of the MXM.
- **Port** 1719 should be the defined port.
- **Prefix** Prefix that must be dialed in addition to all of the MGC’s Meeting Rooms’ directory numbers (or “node number”). This number must be within the permitted directory number range (see “Dial Plan” on page 73) and be the same number of digits.

For example, if the prefix is “1234” and the Meeting Room’s directory number is 1095, then a user must dial “12341095” to enter the videoconference.
6. The **Span** tab displays a list of H.323 cards in the MGC. You must enter a Circuit ID and unique alias for each H.323 card. Click the plus (+) button to add a new card configuration.

7. Enter the following information:
   - **Circuit ID**: Unique number for the H.323 card in the MGC.
   - **IP Address**: IP address for the H.323 card.
   - **Alias**: Enter one H.323 ID alias for this card (must be unique in the MXM).

8. Click **OK**.
E.1 MGC Configuration

Network Services - Gatekeeper Configuration for MXM

Adding a New H.323 Card Configuration
H.323 Card Configuration

After setting up the Network Services configuration, assign the appropriate Circuit IDs to the H.323 cards in the MGC.

➤ To assign a Circuit ID to an H.323 card

1. In the left pane, open the Cards object. Select the slot of the H.323 card.
2. Right-click the card, and then click Properties. The Card Settings dialog box appears.
3. In the H.323 Network Parameters tab, enter the Circuit ID for this card.
4. Click OK.

Following Network Services and H.323 card configuration, make sure that the Circuit IDs, IP addresses, and Service Type correspond in both configurations.
E.2 Adding an Accord Meeting Room

A Meeting Room is a hunting group of MCU services provided by the Accord MGC or other Accord hunting groups. A multipoint videoconference managed by the MGC must be associated with a Meeting Room.

If you will use the MGC to manage ad-hoc videoconferences, you must define this ability in a Meeting Room configuration.

To set up Meeting Rooms in the MGC, see the Accord MGC user documentation.

➤ To add an Accord Meeting Room to the Main View

1. Right-click the MXM object, point to Add Node, and click New Accord Meeting Room. The New Accord Meeting Room wizard appears.

2. Change properties according to your multipoint videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click Next. For explanations about the various properties, see the following section.

3. When you finish the last page, click Finish.


E.3 Setting Meeting Room Properties

In step 2 of “To add an Accord Meeting Room to the Main View” in the previous section, the wizard provided the chance to change various Meeting Room properties. This section describes these properties.

General

The General page contains identity information of the new Meeting Room.

In the General page, enter the following information:

- **Directory Number**: Assign a directory number for the Meeting Room.
- **Description**: Type an identity for the Meeting Room. This description does not affect the operation of the system.
Ad-hoc Conference

A point-to-point conference becomes an ad-hoc conference when additional endpoints are "invited" by one of the parties and they join the session. In the Ad-hoc Conference page, you can make this Meeting Room available for use in ad-hoc conferences. This availability may be in addition to basic multipoint videoconferencing or exclusive for ad-hoc conferences.

**Accord Meeting Room - Ad-hoc Conference Properties**

Enable ad-hoc videoconferencing using this Meeting Room as follows:

- **Use this service as an ad-hoc conference resource**
  Select to make this Meeting Room available for use when expanding to an ad-hoc videoconference.

- **Use this service exclusively for ad-hoc conferences**
  Select to make this Meeting Room available only for use in ad-hoc videoconferences, and unavailable for point-to-point sessions.

- **Ad-hoc Resources page**
  Click this link to open the MXM’s Ad-hoc Resources Properties, in which you can also select which Meeting Rooms may be used for ad-hoc videoconferences (see “Ad-hoc Resources” on page 81).
E.3 Setting Meeting Room Properties

**Hunting Group**

In the Hunting Group Properties page, you can place specific H.323 cards (installed in the MGC) and/or other Accord hunting groups in the hunting group. Only selected cards may manage multipoint videoconferences that require this Meeting Room’s services. The cards may be identified either by their prefixes or by their aliases.

![New Accord Meeting Room - Hunting Group Properties](image)

Select any number of cards from the list to be in the hunting group.

- To place all cards in the hunting group, click **Select All**.
- To clear all the selections, click **Clear All**.
**LDAP**

The **LDAP** page provides information about the Meeting Room’s registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes’ LDAP Properties, see “LDAP” on page 109.

A Meeting Room that’s defined exclusively for ad-hoc videoconferences does not appear in the online directory.

**Additional ID**

In addition to its directory (E.164) number, a Meeting Room may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see “Additional IDs” on page 111.
E.4 Adding an Accord Gateway

If your organization is employing an Accord gateway for IP-to-ISDN videoconferences, prepare it for registration in the MXM by defining an appropriate Network H.323 Service configuration in the Accord MGC. This configuration must include the MXM's IP address (in the Gatekeeper IP parameter), a prefix, and a span of cards that will be registered to the MXM. After the cards reset, they automatically register to the MXM.

Also, an Accord hunting group, which includes the span of cards configured in the Accord MGC, may be automatically created in the MXM Administrator's Main View. If the span includes ONLY one card, you have to manually create an Accord Hunting Group which includes this single card.

Unlike the Accord cards, the gateway does not initiate a registration request with the MXM. You have to add the Accord Gateway node and its services to the Main View manually.

To provide access to the Accord Gateway services, you then have to assign an Accord Hunting Group to each registered Accord gateway.

The setup of the Accord Gateway configuration for use in the MXM's network requires the following tasks:

- Adding the Accord Gateway to the Main View (see the following procedure)
- Creating a new Accord Hunting Group or placing the gateway in an existing one (see “Resources” on page 408).
- Adding gateway services to the Accord Gateway (see “Adding Accord Gateway Services” on page 409).

➤ To add an Accord Gateway to the Main View

1. In the Main View's toolbar, click the New Accord Gateway button. The New Accord Gateway Wizard appears.

2. Change properties according to your videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click Next. For explanations about the various properties, click the Related Topics icon below.

3. When you finish the last page, click Finish.
E.5 Setting Accord Gateway Properties

In step 2 of “Adding an Accord Gateway” on page 404, the New Accord Gateway wizard provided the chance to change various gateway properties. This section describes these properties.

General

The General page contains identity information of the Accord gateway.

Define the following information:

**Description**

Identity or name of the Accord gateway.
Dialing

Dialing conventions vary among gateways, according to the manufacturer's design and configuration. Refer to your gateway's documentation for the specific delimiters or other characters that are required to access the gateway's services.

The values entered in this page must be identical to the dialing configuration of the gateway.

New Accord Gateway - Dialing Properties

- **Delimiter between Service Number and First Number**: Type the character, if applicable, that the MXM adds before the first ISDN number. For Accord gateways, the default delimiter should be an asterisk (*).

- **Delimiter between Phone Numbers**: Type the character, if applicable, that the MXM adds between each ISDN number to be dialed. For Accord gateways, the default delimiter should be a semi-colon (;).
### E.5 Setting Accord Gateway Properties

<table>
<thead>
<tr>
<th><strong>Dialing sequence is terminated with</strong></th>
<th>Type the character, if applicable, that the MXM must enter at the end of the dialing string. For Accord gateways, by default, this box should be blank.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send the Service Alias when dialing to this Gateway</strong></td>
<td>Video gateways support multiple services. If the gateway's dialing syntax requires the inclusion of the service number, select this option.</td>
</tr>
<tr>
<td><strong>Treat H.323 messages sent from this Gateway as if they were sent from its service</strong></td>
<td>Select this option if the gateway does not define services. The MXM will handle messages sent through the gateway as H.323 64K Voice messages.</td>
</tr>
</tbody>
</table>
E.5 Setting Accord Gateway Properties

Resources

To provide access to the Accord gateway services, you then have to place Accord cards (as set up in the Accord MGC's configuration) in one or more Accord hunting groups. MXM nodes must dial the hunting group prefix in order to receive these services.

In the **Resources** page, select the hunting group for this gateway. If the hunting group already exists, it appears in the **Select Group** list. To add a new hunting group, perform the following procedure.

![](image)

**New Accord Gateway - Resources Properties**

To add a new hunting group

1. If the hunting group does not appear in the **Select Group** list, click the Add New Hunting Group button. The New Accord Hunting Group Wizard appears.

2. Enter a **Directory Number** (E.164) and a **Description**.

   The E.164 number must be identical to the Network H.323 Service prefix as defined in the cards' configuration in the Accord MGC.

   To go to the next page, click **Next**.
3. In the Hunting Group Properties page, select the Accord services (cards) that will belong to this hunting group.

4. Click **Finish**. The new hunting group now appears in the Accord gateway's Resources Properties.

To delete a hunting group, select it in the list and click the Remove Accord Hunting Group button.

**Call Routing**

In the **Call Routing** page, enter the physical location of the gateway and define the cost rates for using the gateway’s services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see “Testing for the Optimal Gateway Service” on page 290).

For a description of the Call Routing page, see “Call Routing” on page 120.

**E.6 Adding Accord Gateway Services**

The Accord Gateway does not initiate registration of itself and its services with the MXM. Therefore, you have to manually add the Accord Gateway's services under the Accord Gateway node in the Main View.

Make sure to choose only services that are defined as ISDN services in the Accord MGC.

➤ **To add an Accord Gateway Service**

1. In the Main View's toolbar, click the New Gateway Service button. The New Gateway Service Wizard appears.

2. Define properties (**Directory Number** and **Bandwidth**) of the service as they are defined in the Accord MGC configuration (for descriptions of the properties, see “Setting Gateway Service Properties” on page 123). When you finish each page of the wizard, click **Next**.

3. When you finish the last page, click **Finish**.
**F Upgrading Falcon Software**

This appendix explains how to upgrade your Falcon to the latest software version through the MXM Administrator application. The utility is called the Falcon Upgrade program.

The latest software version is supplied by your local VCON distributor on either a CD-ROM, or from VCON’s website (http://www.vcon.com/support/downloads.shtml).

**CAUTION** Make sure that you do not restart a Falcon until the instructions specifically tell you to do so.

- Before you begin an upgrade, make sure that you initiate it during a quiet period of the network. Heavy network traffic may interfere with the procedure and cause upgrade failures.
- Make sure that the possibility of electrical failure is at a minimum.
- Make sure that the computer from which the upgrade will run (same as the MXM Administrator application’s computer) fills the following requirements:
  - Windows XP, 2000, NT, 95/98/ME. If it uses Windows NT, Service Packet 5.0 is necessary as well.
  - Microsoft Internet Explorer 5.0 or later must be installed.
  - It should not run other programs at the same time as the Falcon upgrade program.
- Decide whether the upgrade process should begin automatically, or if the Falcon user should be able to accept or reject it before it begins.
  - If the Falcon systems will be upgraded when the users are not working, the procedure should be automatic.
  - If the upgrade is going to take place during working hours, you might require user approval, to prevent disturbing an important call.
### F.1 Running the Upgrade Program

#### Falcon User Instructions

1. **Set up Falcon for remote access**
   - (Menu/Options; see “Web-Based Remote Management” in the *Falcon IP User’s Guide*).

#### MXM Administrator User Instructions

1. **Click Start/Programs/FalconIP Tools/FalconIP Upgrade.**
   - The upgrade program starts.

#### Falcon Upgrade Program Window

1. **To see the IP address of the Falcon unit,** press <Status> and open the LAN tab.

2. **In the IP Address box in the Falcon Upgrade program window,** enter the IP address of the Falcon.

3. **Click Upgrade.**

4. **Browse the CD-ROM or the location folder you received and double-click the zip file containing the new version.** When asked to confirm the upgrade, click **Yes.**
The Falcon monitor displays a progress bar after the upgrade begins.

The upgrade process begins. The bar at the bottom of the window shows the actual progress of the upgrade.

---

**CAUTION** The entire procedure takes about 30 minutes. Do not try to initiate videoconferences with the Falcon or change its configuration during this process. Do **not** restart Falcon until the upgrade process is complete!
F.2 Applying the New Upgrade

**Falcon User Instructions and Screens**

1. When the progress bar shows that Step 4 of 4 is complete, wait for the remote PC user to inform you that the upgrade is complete, and then restart Falcon.

2. When the system restarts, a message appears.

   ![Upgrade](image)

   Press <OK> to accept the upgrade.

   Falcon now transfers your old configuration parameters and Phone Book to the new version and starts the Post-Upgrade procedures.

**MXM Administrator User Instructions**

1. When the process is complete, a message appears, saying that the upgrade is complete.

   ![Upgrade](image)

   Click OK. Restart the Falcon unit, or tell the Falcon user to restart it.

2. Wait for confirmation from the Falcon user that upgrade was successful; that Falcon passed through the Post-Upgrade procedures without problems and that the Guide Screen opened.

**CAUTION** If you do not press <OK> now on the Falcon unit, the system will restart in Installer Mode (see “Installer Mode” on page F415).
The upgrade process has been successfully completed. Now Falcon begins the Post-Upgrade procedures.

After you press the OK button on the remote control, a message appears on the TV monitor.

Do not turn off, restart, or use Falcon at this point. Wait a few minutes until the next message appears.

Falcon then restarts itself and runs through the usual opening process. Wait until the Falcon’s Guide Screen appears.

After the Guide Screen appears, Falcon is ready for use!

If for some reason the upgrade was not successfully completed, Falcon enters Installer Mode after it restarts. This mode allows you to rerun the upgrade process until it is successfully completed. You will know that you are in Installer Mode because the TV monitor displays a different background.
A possible reason for unsuccessful installation is a mistaken IP address for the Falcon.

1. Press <Menu>. The Set Network - LAN dialog opens.
2. Keep the same IP address or assign another static IP address. Press <OK>.
3. Rerun the upgrade process from the Falcon Upgrade Program. Be sure to enter the correct IP address for the Falcon.

**F.5 Software Key Upgrade**

To upgrade to Falcon Model 3.0, contact your local reseller for details on purchasing a software key.

➤ **To change models with the software key**

1. Contact your local VCON reseller with a request to purchase the software key for a model upgrade.

   After VCON processes your order, you will receive the new software key.

2. Turn on the Falcon and press <Menu>. The Menu opens.

   ![Falcon Menu](image)

   3. Select **Version**. The Version dialog box appears.

4. Press the down arrow key until **Software Key** is highlighted.

5. Enter the software key that you received.

6. Press <OK> to apply the changes and then restart the Falcon.
G  **SETTING UP THE IPNEXUS CONFIGURATION**

The IPNexus Server, an optional module of the MXM, provides your organization with a secure, private, instant collaboration service. The tools include instant messaging, application sharing, file transfer, group polling, screen capturing, and e-mailing.

Based upon your network and firewall configuration, you have total control of the level of accessibility from inside and outside your network.

The IPNexus Server must be installed on a computer that has a static IP address. The IPNexus Server may be on the same computer as the FTP server and/or MXM.

For installation instructions, see “Installing the IPNexus Server” on page 17.

To enable IPNexus clients to share files and applications, an FTP server is also required on your network.

The configuration setup includes the following tasks:

1. Creating an IPNexus User type.
2. Create an IPNexus folder on the web server.
3. Enable web sharing for the IPNexus folder.
4. Assign full control permissions in the IPNexus folder to the IPNexus User type.
5. Modify the IPNexus Server properties in the associated MXM.

The series of procedures described in this chapter are suggestions aimed at persons without prior experience in setting up FTP directories and Web sites. If you have done this previously, you may perform the above steps using procedures familiar to you.
G.1 Creating an IPNexus User Type

In the web server, create a specific user type that is associated with IPNexus Clients who log in to the IPNexus server.

1. In the Windows desktop, right-click **My Computer** and click **Manage**. The Computer Management Console appears.
2. In the Console tree, browse to the **System Tools>Local Users and Groups>Users** folder.
3. Right-click **Users** and click **New User**.

![Sample New User Entry]

*Sample New User Entry*
4. In the New User dialog box, enter the following properties:

**User Name**
The user name required to access the FTP site.

**Password**
The password required to access the FTP site.

**User must change password at next logon**
Deselect this option.

**User cannot change password**
Select this option. The password must only be controlled by the system administrator.

**Password never expires**
Select this option. There is no defined time limit for this password and this setting overrides the **Maximum Password Age** defined in other Group Policy settings.

5. Click **Create**.

---

**G.2 Installing Internet Information Services (IIS)**

Setting up the FTP and Web servers for IPNexus requires that Internet Information Services (IIS) be installed on the IPNexus Server’s host computer. Verify if IIS is installed; if not, install it (Windows 2000 Server CD-ROM is required).

➢ **To verify if IIS is installed on the IPNexus Server computer, and install if necessary**

1. Open the Windows Control Panel. Double-click **Add/Remove Programs**.
2. In the left toolbar, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard, verify if **Internet Information Services (IIS)** is checked. If not, select it and click **Details**.
4. Verify if **File Transfer Protocol (FTP) Server** is checked. If not, select it and click **OK**.
5. In the Windows Components Wizard, click **Next** to proceed with the installation of IIS.
G.3 Creating an IPNexus Folder for FTP/Web Access

Create a shared access folder on the FTP/Web Server. All files and applications shared between IPNexus clients will be uploaded to this location.

To create the IPNexus folder

1. On the FTP/Web Server computer, browse to C:\inetpub\ftproot and create a new folder. Give it a name — for example, ipnexus.
2. Right-click the new folder and then click Sharing.
3. In the Sharing tab, select Share This Folder and click Apply.
4. Click Permissions. The Permissions for [share name] appears.
5. In the Share Permissions tab, click Add. The Select Users, Computers or Groups dialog box appears.
6. Select the IPNexus User type that you created in the previous section. Click Add and then click OK.
7. In the Permissions dialog box, select the IPNexus User type and then select Full Control. This provides full read and write privileges to this folder.
G.4 Creating a Virtual FTP Directory

The path location of the IPNexus folder is hidden from the system’s clients. Create a virtual FTP directory that enables clients to locate, access and post files on the FTP site.

➤ To create a Virtual FTP Directory

1. Open the Windows Control Panel. Double-click **Administrative Tools** and then **Internet Services Manager**. The Internet Information Services window appears.

2. In the left pane, expand the tree. Right-click **Default FTP Site**, point to **New** and click **Virtual Directory**. The Virtual Directory Creation wizard opens. Click **Next**.

3. Enter an alias for the User Name defined in “Creating an IPNexus User Type” on page 418. Click **Next**.

4. Enter the path of the FTP/Web access folder that will contain uploaded FTP content (defined in “Creating an IPNexus Folder for FTP/Web Access” on page 420). Click **Next**.

5. Select **Read** and **Write** access permissions. Click **Next**.

6. Click **Finish** to close the wizard.
G.5 Creating a Virtual Web Directory

To enable web sharing on the IPNexus Server, create another virtual directory (like the one created in the previous section).

➢ To set up web sharing

1. Open the Windows Control Panel. Double-click Administrative Tools and then Internet Services Manager. The Internet Information Services window appears.

2. In the left pane of the Internet Information Services window, right-click Default Web Site, point to New and click Virtual Directory. The Virtual Directory Creation wizard opens. Click Next.

3. Enter an alias for the User Name defined in “Creating an IPNexus User Type” on page 418. Click Next.

4. Enter the path of the FTP/Web access folder that will contain uploaded FTP content (defined in “Creating an IPNexus Folder for FTP/Web Access” on page 420). Click Next.

5. Select appropriate access permissions and click Next.

6. Click Finish to close the wizard.

7. In the left pane of the Internet Information Services window, expand Default Web Site, right-click the new Virtual Directory, and click Properties.

8. Click the Documents tab.

9. Deselect Enable Default Document and click OK twice to implement the change and exit the Properties dialog box.

G.6 Setting FTP Properties in the MXM

Data collaboration with IPNexus requires access to an FTP site where clients can send and receive data (files, shared applications, etc.). In the MXM Administrator, specify the information about the FTP site that was set up for this purpose.

➢ To define the FTP access properties in the MXM

1. In the MXM Administrator, double-click the IPNexus Server listed under the System Servers object.

2. In the Properties dialog box, click the FTP tab.
G.6 Setting FTP Properties in the MXM

3. Enter the following properties:

- **FTP Address**: IP address of the FTP server.
- **Read/Write Access User Names & Passwords**: User name and password required to access the FTP site. This name must be entered by all IPNexus Clients when they log in to the FTP site. We recommend use of the same user name and password for both Read and Write.
- **Additional Path Data**: Specific subfolder and path under the FTP root folder that will serve the IPNexus Server's clients.
- **Mapping to HTTP Server**: If selected, the IP-Nexus Server uses the same folder as the FTP site and as a website. For example, a downloadable file in the folder may be accessed through addresses such as:

  - `ftp://username:password@11.22.33.44/widget.pdf`.

From the IPMessenger window, users can then download this file by clicking an HTTP link, if provided, or to follow a provided FTP link.

![IPNexus Server Properties (IPNexus)](image)

4. Click **OK**. The IPNexus Server is now set up.
G.7 Setting Options Properties in the MXM

The **Options** tab contains various options for the IPNexus Server's activity.

![IPNexus Server Properties (IPNexus)]

### IPNexus Server - Options Properties

**Server Port**

The port through which the IPNexus Server and its clients communicate. This port must correspond with the clients' Port Code ID property.

**Turn Debug On**

Select to receive and display debugging information, in order to troubleshoot.
G.8 Setting Up WebSharing

This section explains how to set up WebSharing for an FTP Server located on the same computer as the IPNexus Server.

➤ To set up WebSharing

1. Inside the FTP folder that you created in “Creating an IPNexus Folder for FTP/Web Access” on page 420, create a subfolder named `applets`.

   For example, `C:\Inetpub\ftproot\ipnexus\applets`

2. From `C:\Program Files\IPNexus Server`, copy the `webshare.class` file to the `applets` subfolder created in the previous step.

3. In the MXM Administrator, double-click the IPNexus Server under the System Servers object and then click the FTP tab.

4. In the Webshare Drive box, enter the pathname of the folder that you created for FTP/Web access.

   For example, `C:\Inetpub\ftproot\ipnexus`

5. Add user accounts on both the IPNexus host, and the FTP server (if they are not the same system). Both these accounts must have the same User Name and Password. Place these accounts in the Power User Group.

6. On the IPNexus Server, click Start, point to Settings, Control Panel, Administrative Tools and click Services. A list of Services appears.

7. Double-click IPNexus Service to display its Properties.

8. Change the logon name and password to the same logon name and password defined in the FTP server and click OK.

   If the accounts are set up correctly, a message, “The new logon name will not take effect until you stop and restart the service,” appears. Click OK to close the Properties dialog box.

9. In the Services list, right-click IPNexus Service and click Stop. After a few seconds, start the service again.
INDEX

A
Accord Gateway
adding, 404
properties
General, 405
Accord Meeting Room, 399
properties
Additional IDs, 403
Ad-hoc Conference, 401
General, 400
Hunting Group, 402
LDAP, 403
Accord MGC configuration, 393—398
adding
Accord Gateway, 404
Accord Meeting Room, 399
Ad-hoc Permission Group, 142
Administrative group, 64
Administrator, 33—35
gateway, 113
gateway service, 115, 123
Gateway Service hunting group, 125
hunting group, 57—63
MCU Service Permission Group, 138
neighbor gateway, 179, 180
neighbor MCU, 179, 180
node, 36—39
non-registered device, 164
Short Dial Number, 66
SIP user agent, 296
VCB, 225
VCB services, 226
zones, 166
Additional IDs properties
Accord Meeting Room, 403
dial points, 111
hunting groups, 63
MCU service, 137
Short Dial Numbers, 67
VCB service, 240
zones, 166
Ad-hoc Conference properties
Accord Meeting Room, 401
MCU services, 136
MXM Server, 80
VCB services, 234
Ad-hoc Permission Group, 104
adding, 142
initiating ad-hoc conference from neighboring zones, 154
properties
General, 143
Ad-hoc Resources properties, 81
ad-hoc videoconferences, 6
dialing code, 76, 241
expanding to, 241
Administrative group, 64
Administrator, 6
adding, 33—35
administration levels, 34
password, 34
properties, 33—35
Administrator application, MXM, 2, 25—31
minimum system requirements, 10
Advanced Encryption Server, 301
properties, 306
Advanced properties, VCB services, 238
Advanced properties, zones, 162
ALG Proxy, 301
license key, 305
properties
Encryption Settings, 306
Firewall/Network Settings, 308
General, 303
License, 305
Server Settings, 304
Server Timeouts, 307
ALG Proxy Server. See ALG Proxy
**Index**

**B**
- Bandwidth control
  - end points, 101
  - gateway services, 124
  - inter-zone calls, 173
  - MCU, 130
  - MCU services, 135
  - zones, 153
  - Bandwidth routing rules, 107, 159, 289

**C**
- Call forward, 100
  - between zones, 160, 175, 176
  - MXM Server properties, 80
  - no answer
    - dialing code, 75
    - end points, 101
  - on busy
    - dialing code, 75
    - end points, 101
  - through gateway, 117
  - through hunting group, 59
  - through MCU, 131
  - unconditional, 75
- Call pickup
  - dialing code, 75
  - permissions, 103
- Call routing properties, 288
  - Accord gateway, 409
  - gateway, 120
- Call transfer
  - between zones, 160, 175, 176
  - dialing code, 76
  - through gateway, 117
  - through MCU, 131
- CDR
  - enabling billing, 93
  - for inter-zone calls, 152
- Change login properties, 98
- child gatekeeper, 162, 169, 172
- Closed mode, 36, 86
  - end points, 95
  - MCUs, 127
  - VCBs, 225

**D**
- Dedicated Service, 141
  - for end point, 104
  - for end points in neighboring zones, 155
  - MCU Service, 136
- Defined Zones search, 91, 167
- deleting
  - login request, 37, 38, 114, 128, 226
  - nodes, 44
- DGK. See Directory Gatekeeper
- dialing between zones, 165—168
- dialing prefix, 286
- Dialing Prefixes, 83
- dialing unlisted users in Windows XP Messenger, 300
- DiffServ values, 392
- Directory Gatekeeper, 169—172
  - configuration, 172
  - diagram, 170
  - inter-zone dialing, 167, 169
  - Zone Settings, 162, 172
  - directory numbers, 43, 165

**E**
- E.164 number, 43
- editing nodes, 36—44
- Empty Capability Set
  - through gateway, 118
  - through MCU, 132
  - to neighboring zones, 160
- Encryption Client, 301
  - minimum system requirements, 11
- Encryption Settings properties, ALG Proxy, 306
- end points, 1, 6, 95
  - Open mode login, 36
  - password, 98
end points (cont.)
properties
  Additional IDs, 111
  Bandwidth control, 101
  Call Forwarding, 100
  Gateway Services, 105
  General MXM, 97
  ISDN Call Routing, 106, 288
  LDAP, 109
  MCU Services, 104
  MXM, 97—111
  Pickup permissions, 103
  Product info, 108
  Status, 99
setup, 95—96
end points, Falcon
ISDN connection status, 27
properties
  Audio, 385
  Network, 376—383
  Options, 387
  Security, 389
  Version, 388
  Video, 384
end points, MeetingPoint
properties
  Advanced, 368—373
  Calls, 342—347
  Communication, 349—353
  Conversation, 337—341
  Hardware, 360—367
  Telephony, 354—359
  User Data, 324
end points, vPoint
properties
  Advanced, 331—335
  Calls, 314—316
  Communication, 323—326
  Conversation, 311—313
  Hardware, 327—330
  User Data, 322
Event Log, 25, 31, 49—54
filtering records, 51—54

F
Falcon end points. See end points, Falcon
Falcon Upgrade program, 411
filtering
  Event Log, 51—54
  Main View, 29
Find items, 39—41
  in Main View, 39
  in other Views, 41
firewall, 6
properties
  ALG Proxy, 308
  routing video data through firewall ports, 308
Firewall properties, VCB, 230
Firewall/Network Settings properties, ALG Proxy, 308
Forward Facility messages
  between zones, 160
  through gateway, 117
  through MCU, 132

G
Gatekeeper
  Directory Gatekeeper, 169—172
  MXM, 1, 6
  Open mode, 36
  redundancy, 161
gateway, 6, 113
  adding, 113
  adding neighbor gateway, 179, 180
  cost rates, 121
Least Cost Routing, 120
login, 113
properties
  call routing, 120, 288, 409
  General, 116
  ISDN dialing, 118
  Product info, 117
Gateway Service hunting groups, 125
  adding, 125
  adding services, 118
  calls from neighboring zones, 156
  end points receiving services, 105
Index

Gateway Service hunting groups (cont.)
  properties
    General, 126
    Hunting Group, 126
  sharing services with other zones, 177

gateway services, 75
  adding, 115, 123
  Least Cost Routing, 285—291
  properties
    Bandwidth control, 124
    General, 123
  sharing with other zones, 177

Gateway Services tab
  end points properties, 105
  zone properties, 156

General properties
  Accord Gateway, 405
  Accord Meeting Room, 400
  Ad-hoc Permission Group, 143
  ALG Proxy, 303
  end points, 97
  Gateway Service hunting groups, 126
  gateway services, 123
  gateways, 116
  hunting groups, 58
  MCU, 129
  MCU Service Permission Groups, 139
  MCU services, 134
  Short Dial Numbers, 66
  VCB, 228
  VCB services, 233
  zones, 150

hunting groups>properties (cont.)
  Gateway Service hunting groups, 126
    General, 58
    Hunting Group, 60
    LDAP, 62

I
  ILS, MXM configuration, 183—186
    in MXM Administrator, 185
  impersonation, 274
    properties, 280
  Information Request Messages (IRQ)
    gateway, 118
    MCU, 132
  initiating
    hang up videoconference, 222
    point-to-point (ISDN) videoconference, 220
    point-to-point (LAN) videoconference, 219
  installation
    Falcon, 411—416
    IPNexus Client, 18
    IPNexus Server, 17
    MXM Administrator, 15
    MXM Server, 13
    remote software upgrade, 267—284
    VCON Conference Bridge, 16
  Installer Mode, Falcon, 415
  Internet Location Server. See ILS, MXM configuration
  Invite
    dialing code, 76, 241
  IP Precedence values, 391
  IPNexus, 4
    Client
      installation, 18
      minimum system requirements, 12
      license, 88
    Server
      installation, 17
      minimum system requirements, 12
      software upgrade, 267

H
  H.450.3
    between zones, 160, 175, 176
    through gateway, 117
    through MCU, 131
  hunting groups, 6
    adding, 57—63
    gateway services, 125
    properties, 57—63
      Additional IDs, 63
      Call Forwarding, 59
ISDN Call Routing properties
  end points, 106, 288
  MXM, 82, 286
  zones, 158
ISDN connection status, 27
ISDN dialing, gateway properties, 118
Item Attributes, 245

K
  key, license
    ALG Proxy, 305
    MXM, 19, 88
    VCB, 229

L
  LDAP, 6
  LDAP directories, 181—182
    MXM configuration
      in ILS, 183—186
      in Microsoft Exchange Server, 187—191
      in NDS, 203—214
      in Netscape Directory Server, 216—218
      in Site Server ILS, 215
      in Windows 2000 Active Directory, 192—202
  LDAP Group object configuration, 211
  LDAP properties
    Accord Meeting Room, 403
    end points, 109
    hunting groups, 62
    MCU services, 137
    MXM Server, 77, 166
    Short Dial Numbers, 67
    VCB services, 240
  LDAP Servers View, 25, 31
    MXM configuration in ILS, 185
    MXM configuration in Microsoft Exchange Server, 190
    MXM configuration in NDS, 214, 215
    MXM configuration in Netscape Directory Server, 218
    MXM configuration in Windows 2000 Active Directory, 202

Least Cost Routing, 285—291
  cost rates, 120, 121, 288, 409
  rules, 107, 159, 289, 290
  license key
    ALG Proxy, 305
    MXM, 19, 88
    VCB, 229
  License properties, ALG Proxy, 305
  License properties, VCB, 229
  Lightweight Directory Access Protocol. See LDAP directories
  login, 6
    Closed mode, 36, 86, 95, 149
    deleting request, 37, 38, 114, 128, 226
    duplicate user, 96
    end points, 95—96
    gateway, 113
    granting permission, 36, 45
    MCU, 127
    new MXM, 21
    Open mode, 36, 86, 95, 148
    rejecting, 37, 38, 114, 128, 226
    SIP user agents, 296
    VCB, 225
    zones, 148
  Login page, Software Upgrade, 274
  Login Status View, 25, 30, 45

M
  Main View, 25—29
    customizing, 243—245
    filtering, 29
    finding items, 39
  MCU, 6, 127
    Accord MGC configuration, 393—398
    adding neighbor MCU, 179, 180
    Closed mode, 127
    login, 127
    Open mode, 36, 127
    properties
      Bandwidth control, 130
      General, 129
      Product Info, 131
Index

MCU Service Permission Groups, 138
  adding, 138
  adding services, 132, 231
  end points receiving services, 104, 154
  properties
    General, 139
    Permission Group, 140, 144
  sharing services with other zones, 178
MCU services, 133
  editing, 133
  properties
    Additional IDs, 137
    Ad-hoc conference, 136
    Bandwidth control, 135
    General, 134
    LDAP, 137
  sharing with other zones, 177
MCU Services tab
  end point properties, 104
  zone properties, 154
MeetingPoint end points. See end points, MeetingPoint
Microsoft Exchange Server, MXM
  configuration, 187—191
    in MXM Administrator, 190
Monitor System administration level, 34
monitoring network status, 44—54
Multicast Location Requests, 91, 149, 167
Multicast properties, VCB services, 237
Multicast through ALG Proxy, 308
Multipoint Control Unit. See MCU multipoint videoconferences, 223
MXM, 1
  Administrator application, 2, 25—31
    customizing, 243—264
    minimum system requirements, 10
    software upgrade, 267
Gatekeeper, 1
  installation, Administrator, 15
  installation, Server, 13
  license key, 19, 88
  login to MXM Administrator, 21
  minimum system requirements, 9
  running application, 20
MXM (cont.)
  Server properties, 69—94
    Ad-hoc Resources, 81
    Advanced settings, 92
    Bandwidth control, 79
    Billing, 93
    Call Settings, 80
    Connection, 70
    Dial Plan, 73—76, 165
    Dialing Prefixes, 83
    Event Log, 50, 94
    ISDN Call Routing, 82, 286
    LDAP settings, 77, 166
    License, 87
    Non-registered devices, 89
    Security Mode, 85, 148, 166
    System Info, 72
    System Location, 82
    Zone settings, 90, 148, 167
MXM attributes, 204—206
MXM container, 210
MXM Node, 6
MXM Server, installing, 13
MXM Transfer Model
  between zones, 160, 175, 176
  through gateway, 117
  through MCU, 131
MXMNode class, 207—210

N
NAT (Network Address Translation), 7, 324, 350
NDS, MXM configuration, 203—214
  create MXM attributes, 204—206
  create MXM container, 210
  create MXMNode class, 207—210
  in MXM Administrator, 214, 215
  LDAP Group object, 211
  trustee, 213
neighbor node, 7
  search properties, 90, 148, 167
neighboring gatekeeper, Open mode, 36
neighboring MXM, Open mode, 36
neighboring zones, 7, 147—180
Index

Netscape Directory Server, MXM configuration, 216—218
   in MXM Administrator, 218
Network Address Translation. See NAT.
Node Status View, 25, 30, 46—48
   nodes, 7
      adding, 36—39
      changing numbers, 43
      deleting, 44
      editing, 36—44
      editing multiple, 42
      setting properties, 38, 42
   templates, 54
non-registered devices
   adding, 164
   allowing calls with end points, 102
   allowing in multipoint videoconferences, 130, 135
   Make Permanent, 164
   MXM Server properties, 89
Novell Directory Services. See NDS, MXM configuration

O
   OLCs timeout, 92, 297
online directories. See LDAP directories
Open mode, 36, 86
   end points, 95
   MCUs, 127
   VCBs, 225
   zones, 148, 166

P
   parent gatekeeper, 162, 169, 172
   password
      Administrator, 34
      end point, 98
   permanent non-registered devices. See non-registered devices
   Permission Group properties, 140, 144
   point-to-point (ISDN) videoconference
      hang up, 222
      initiating, 220
      properties, 221
point-to-point (LAN) videoconference
   hang up, 222
   initiating, 219
   properties, 220
Product Info properties
   end points, 108
   gateways, 117
   MCU, 131
   VCB, 231
   zones, 159
Q
   QoS
      ALG Proxy, 309
      DiffServ values, 392
      Falcon end point, 380
      IP Precedence values, 391
      MeetingPoint end point, 369
      VCB, 239
      vPoint end point, 332
   Quality of Service. See QoS
R
   Redundancy properties, 161
   rejecting login, 37, 38, 114, 128, 226
   replacing license key
      ALG Proxy, 305
      MXM, 19, 88
      VCB, 229
   Requirements, minimum, 9—12
   Run page, Software Upgrade, 275
S
   searching for items, 39—41
   SecureConnect, 5, 301—309
      description, 301
   Server Settings properties, ALG Proxy, 304
   Server Timeouts properties, ALG Proxy, 307
   services, 7
   Session Initiation Protocol. See SIP
   Session properties, VCB services, 235
   Setup, MXM, 13
Index

Short Dial Number, 66
  adding, 66
  properties
    Additional IDs, 67
    Call Forwarding, 67
    General, 66
    LDAP, 67
SIP, 293
SIP Proxy, 293, 294
  OLCs timeout, 92, 297
  registering Windows XP Messenger user, 298
SIP Registrar, 295
SIP user agents, 293
  adding, 296
  login, 296
  Open mode, 36
Site Server ILS, MXM configuration, 215
Software Upgrade
  defining, 268
  properties, 278—284
    Impersonation, 280
    Update FTP, 281
    Update Parameters, 282
    Update Run, 283
    Update Version, 279
Wizard, 268—277
  Confirmation page, 277
  Login page, 274
  Run page, 275
  Upload page, 271
  Versions page, 268, 270
Specific Pickup, dialing code, 75
status monitoring, 44—54
Status properties, 99
Super User administration level, 34
Support, Technical, vi
system tree, 26

T
TCP/IP
  MXM connection port, 71
  refreshing connections interval, 307
  routing signals through firewall, 308
Technical Support, vi
templates, 7, 54
Test Least Cost Routing Rules, 290
toolbars, 254—257
Tree Styles, 243
trustee, 213

U
UDP
  refreshing connections interval, 307
  routing signals through firewall, 308
Unconditional forwarding, 100
dialing code, 75
Update FTP properties, 281
Update Parameters properties, 282
Update Run properties, 283
Update Version properties, 279
upgrading Falcon, 411—416
upgrading videoconferencing software
  Confirmation page, 277
  defining upgrade task, 268
  Login page, 274
  properties, 278—284
    Impersonation, 280
    Update FTP, 281
    Update Parameters, 282
    Update Run, 283
    Update Version, 279
  Run page, 275
  Software Upgrade Wizard, 268—277
  Upload page, 271
  Versions page, 268, 270
Upload page, Software Upgrade, 271
V

 vca file, 21

 VCB, 3, 223
 adding to MXM, 225
 Closed mode, 225
 installing, 10, 16
 license, 88
 license key, 229
 login, 225
 minimum system requirements, 10
 on same computer as MXM, 9
 Open mode, 225
 properties
 Firewall, 230
 General, 228
 License, 229
 Product Info, 231
 setup, 225—240
 software upgrade, 267
 software upgrade indication, 28
 VCB services, 232
 adding, 226
 Dedicated Service for end point, 104
 Dedicated Service for end point in neighboring zone, 155
 in ad-hoc permission group, 142, 144
 properties
 Additional IDs, 240
 Ad-hoc Conference, 234
 Advanced, 238
 General, 233
 LDAP, 240
 Multicast, 237
 QoS, 239
 Session, 235
 VCON Conference Bridge Option, 223
 VCON Conference Bridge. See VCB
 Versions page, Software Upgrade, 268, 270
 videoconference
 hang up, 222
 initiating (ISDN), 220
 initiating (LAN), 219

 View
 Event Log, 25, 31, 49—54
 filtering records, 51—54
 finding items in other views, 41
 LDAP Servers, 25, 31
 Login Status, 25, 30, 45
 Main, 25, 25—29
 Node Status, 25, 30, 46—48
 View System Properties administration level, 34
 Voice-activated Switching, 224, 236
 vPoint
 end points. See end points, vPoint
 software upgrade, 267

 W

 Windows 2000 Active Directory, MXM configuration, 192—202
 adding MXM attributes, 193—194
 adding MXMNode class, 195—196
 creating organizational unit, 201
 granting full control for the MXMNode class, 192
 in MXM Administrator, 202
 MXM attributes properties, 200
 Windows 2000 Active Directory, MXM configuration granting full control for the MXMNode class, 199
 Windows XP Messenger
 dialing unlisted users, 300
 supported features, 293
 Workspace
 customizing, 243—264
 display properties, 258—260
 Main View, 243—245
 table styles, 261—264
 toolbars, 254—257
 workspaces, 247
 deleting, 253
 filtering, 29
 Item Attributes, 245
 Main View, 25, 25—29
 opening, 252
 renaming, 251
Workspace (cont.)
  saving, 249—250
  toolbars, 254—257
  Tree Styles, 243

Z
zone prefix, 152, 166
  dialing to non-VCON gatekeepers, 152, 168
  in LDAP entries, 166
Zone Settings properties, 151, 167, 168
zones, 7, 147—180
  adding manually, 149, 166
  calls between zones, 152, 167
  CDR records, 152
  Closed mode, 166
  Directory Gatekeeper, 169
    configuration, 172
zones>Directory Gatekeeper (cont.)
  diagram, 170
  inter-zone dialing, 167, 169
  Zone Settings, 162, 172
  inter-zone dialing, 165—168
  login, 148
Open mode, 36, 166
properties
  Additional IDs, 160
  Advanced, 162
  Bandwidth control, 153, 173
  Gateway Services, 156
  General, 150
  ISDN Call Routing, 158
  MCU Services, 154
  Product Info, 159
  Redundancy, 161
  Zone Settings, 151, 167, 168
  zone prefix, 152, 166