

Toshiba Magnia® SG30 Appliance Server User's Guide

If you need assistance, use one of the following:

❖ www.support.toshiba.com

View the latest support bulletins, download software upgrades, and view detailed installation instructions.

❖ www.applianceservers.toshiba.com

View the latest SG30 information

❖ InTouch® Center

Calling within the United States (800) 457-7777

Calling from outside the United States (949) 859-4273

Model: SG30

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. There is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ❖ Reorient or relocate the receiving antenna.
- ❖ Increase the separation between the equipment and receiver.
- ❖ Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- ❖ Consult the dealer or an experienced radio/TV technician for help.

NOTE

Only peripherals complying with the FCC Class B limits may be attached to this device. Operation with non-compliant peripherals or peripherals not recommended by Toshiba is likely to result in interference to radio and TV reception. Shielded cables must be used between the external devices and the unit's printer port. Changes or modifications made to this equipment not expressly approved by Toshiba or parties authorized by Toshiba could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- ❖ This device may not cause harmful interference.
- ❖ This device must accept any interference received, including interference that may cause undesired operation.

Contact:

Toshiba America Information Systems, Inc.
9740 Irvine Blvd.
Irvine, CA 92618-1697
(949) 583-3000

EU-Declaration of Conformity

Toshiba declares that the product: SG30 conforms to the following standards:
Toshiba erklärt, daß das Produkt: SG30 folgenden Normen entspricht:
Toshiba déclarent que le produit cité ci-dessous: SG30 est conforme aux normes suivantes:
Toshiba declaran que el producto: SG30 cumple los siguientes estándares:

Toshiba dichiara, che il prodotto: SG30 è conforme alle seguenti norme:
Toshiba intygar att produkten: SG30 överensstämmer med följande normer:

Supplementary Information:	The product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC.
Weitere Informationen:	Das Produkt entspricht den Anforderungen der Niederspannungs-Richtlinie 73/23/EG und der EMC-Richtlinie 89/336/EG.
Informations complémentaires:	Ce produit est conforme aux exigences de la directive sur les basses tensions 73/23/CEE et de la directive EMC 89/336/CEE.
Información complementaria:	El Producto cumple los requisitos de baja tensión de la Directiva 73/23/CEE y la Directiva EMC 89/336/CEE.
Ulteriori informazioni:	Il prodotto é conforme ai requisiti della direttiva sulla bassa tensione 73/23/EG e la direttiva EMC 89/336/EG.
Ytteligare information:	Produkten uppfyller kraven enligt lågspänningsdirektiver 73/23/EEC och EMC-direktiv 89/336/EEC.

EMC-emission:	EN55022	1994	Class B
	EN61000-3-3	1995	
EMC-immunity:	EN61000-4-2	1995	10V/m, 80-1000MHz, 1kHz 80% AM 10V/m, 895-905MHz, 200Hz 50% PM AC-line: 1kV / 2kV, Polarity; +/- 10V emf, 0.15-80MHz, 80% AM 30% 10ms, 60% 100ms, >95% 5000ms
	EN61000-4-3	1998	
	EN61000-4-4	1995	
	EN61000-4-5	1995	
	EN61000-4-6	1996	
	EN61000-4-11	1994	
Safety:	EN60950	1992	
	A1	1993	
	A2	1993	
	A3	1993	
	A4	1995	
	All	1997	

This product is carrying the CE-Mark in accordance with the related European Directives. Responsible for CE-Marking is Toshiba Europe, Hammfeldamm 8, 41460 Neuss, Germany.

FCC Requirements

The following information is pursuant to FCC 47 CFR, Part 68 and refers to internal modems.

Installation

When you are ready to install or use the modem, call your local telephone company and give them the following information:

- ❖ The telephone number of the line to which you will connect the modem.
- ❖ The FCC registration number of the modem.
- ❖ The ringer equivalence number (REN) of the modem, which is 0.6B.

The modem connects to the telephone line by means of a standard jack called the USOC RJ11C.

Type of service

Your modem is designed to be used on standard-device telephone lines. Connection to telephone company-provided coin service (central office implemented systems) is prohibited. Connection to party lines service is subject to State tariffs. If you have any questions about your telephone line, such as how many pieces of equipment you can connect to it, the telephone company will provide this information upon request.

Telephone Company Procedures

The goal of the telephone company is to provide you with the best service it can. In order to do this, it may occasionally be necessary for them to make changes in their equipment, operations or procedures. If these changes might affect your service or the operation of your equipment, the telephone company will give you notice, in writing, to allow you to make any changes necessary to maintain uninterrupted service.

If Problems Arise

If any of your telephone equipment is not operating properly, you should immediately remove it from your telephone line, as it may cause harm to the telephone network. If the telephone company notes a problem, they may temporarily discontinue service. When practical, they will notify you in advance of this disconnection. If advance notice is not feasible, you will be notified as soon as possible. When you are notified, you will be given the opportunity to correct the problem and informed of your right to file a complaint with the FCC. In the event repairs are ever needed on your modem, they should be performed by Toshiba America Information Systems, Inc. or an authorized representative of Toshiba America Information Systems, Inc.

Disconnection

If you should ever decide to permanently disconnect your modem from its present line, please call the telephone company and let them know of this change.

Fax Branding

The Telephone Consumer Protection Act of 1991 makes it unlawful to use a computer or other electronic device to send any message via a telephone fax machine unless such message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity or individual sending the message and the telephone number of the sending machine or such business, other entity or individual.

In order to program this information into your fax modem, you should complete the setup for your fax software before sending a message.

Special Instructions for a Field Representative

This product may be partially assembled by another manufacturer covered in Volume 1 of the Follow-Up Service Procedures with the exception of specific components.

The final assembly manufacturer's Field Representative shall verify that sub-assembly products shipped from the manufacturing plant are delivered in a carton bearing one 6mm blue dot as the identification marking.

Detailed inspection of sub-assemblies is performed at the manufacturing plant of the basic List and is not required during final assembly as described in Volume 1.

In case of non-compliance, as described in Volume 1, the manufacturer shall be instructed in writing to remove UL Listing Marks from each unit, or to hold the shipment pending appeal to a Reviewing Office.

Instructions for IC CS-03 certified equipment

- 1 **NOTICE:** The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

- 2 The user manual of analog equipment must contain the equipment's Ringer Equivalence Number (REN) and an explanation notice similar to the following:

The Ringer Equivalence Number (REN) of this device is 0.6.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

- 3 The standard connecting arrangement (telephone jack type) for this equipment is jack type(s): USOC RJ11C.

Copyrights

This guide is copyrighted by Toshiba America Information Systems, Inc. with all rights reserved. Under the copyright laws, this guide cannot be reproduced in any form without the prior written permission of Toshiba. No patent liability is assumed, however, with respect to the use of the information contained herein.

©2003 by Toshiba America Information Systems, Inc. All rights reserved.

Additional copyright information may be found in [Open Source License Information](#) on page 336.

Export Administration Regulation

This document contains technical data that may be controlled under the U.S. Export Administration Regulations, and may be subject to the approval of the U.S. Department of Commerce prior to export. Any export, directly or indirectly, in contravention of the U.S. Export Administration Regulations is prohibited.

Caution

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instruction.

Toshiba Battery Co. Ltd. model CR2032

Sony Electric Corp. model CR2032

Hitachi Maxell Ltd. model CR2032

Matsushita Electric Corp. model CR2032

Important Safety Instructions

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- 1 Do not use this product near water, for example, near a bath tub, wash bowl or kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- 2 Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- 3 Do not use the telephone to report a gas leak in the vicinity of the leak.
- 4 Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions. SAVE THESE INSTRUCTIONS.

▲CAUTION Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

Disclaimer

The information contained in this manual, including but not limited to any instructions, descriptions and product specifications, is subject to change without notice.

TOSHIBA CORPORATION AND TOSHIBA AMERICA INFORMATION SYSTEMS, INC. (TOSHIBA) PROVIDE NO WARRANTY WITH REGARD TO THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO ANY OF THE FOREGOING. TOSHIBA ASSUMES NO LIABILITY FOR ANY DAMAGES INCURRED DIRECTLY OR INDIRECTLY FROM ANY TECHNICAL OR TYPOGRAPHICAL ERRORS OR OMISSIONS CONTAINED HEREIN. IN NO EVENT SHALL TOSHIBA BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES, WHETHER BASED ON TORT, CONTRACT OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

Some states do not allow the exclusion of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

SG30 Software License Information

The Magnia SG30 uses the Red Hat® 8 distribution of Linux. Copies of the binary software packages or the source for these packages can be obtained from Red Hat FTP site at <ftp://ftp.redhat.com>. Further information about these packages can be obtained from the Red Hat Web site at <http://www.redhat.com>.

The software installed on the Magnia SG30 is a modular operating system made up of hundreds of individual software components, each of which was written and copyrighted individually. Each component has its own applicable end user license agreement ("EULA"). Most of the software programs are licensed pursuant to a EULA that permits you to copy, modify, and redistribute the software in both source and binary code forms. All of the software and documentation developed or created by or for TOSHIBA are proprietary products of TOSHIBA and are protected by copyright laws, international treaty provisions, and other applicable laws.

The following EULAs are provided in accordance with their terms. The full text of the documents can be found at the Web sites listed here for ease of reference.

Apache

Copyright ©2000 The Apache Software Foundation. All rights reserved.

[http:// www.apache.org/LICENSE.txt](http://www.apache.org/LICENSE.txt)

The BSD License

Copyright ©1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

<http://www.xfree86.org/3.3.6/COPYRIGHT2.html#6>

The DES License

Copyright ©1995-1997 Eric Young (eay@cryptsoft.com) All rights reserved. See Appendix in the user guide.

GNU Lesser General Public License

<http://www.gnu.org/copyleft/lesser.html>

GNU Library General Public License

<http://www.gnu.org/copyleft/library.html#SEC3>

GNU General Public License

<http://www.gnu.org/copyleft/gpl.html>

MIT License

Copyright ©1985-2001 Massachusetts Institute of Technology. All rights reserved.

<http://www.opensource.org/licenses/mit-license.html>

Open Content License

<http://www.opensource.org/licenses/cpl.html>

Open LDAP

Copyright ©1998-2001 the Open LDAP Foundation and portions Copyright ©1992-1996 Regents of the University of Michigan. All rights reserved.

<http://www.OpenLDAP.org/license.html>

Open SSL

Copyright ©1998-2000 The Open SSL Project. All rights reserved. See Appendix in the user guide.

<http://www.openssl.org>

Open SS Leay

Copyright ©1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved. See Appendix in user guide.

The Q Public License

<http://opensource.org/licenses/qtpl.html>

W3C IPR Software Notice

Copyright © 1994-2001 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.

<http://www.w3.org/Consortium/Legal/copyright-software-19980720>

Xfree86

Copyright © 1994-2001, The Xfree86 Project, Inc. All Rights Reserved.

<http://www.xfree86.org/>

This product includes software developed by: the Apache Group for use in the Apache HTTP server project and the Apache Software Foundation (<http://www.apache.org/>); the University of California, Berkeley and its contributors; the Open SSL Project for use in the Open SSL Toolkit (<http://www.openssl.org/>); Eric Young (eay@cryptsoft.com).

THE SOFTWARE PROGRAMS THAT ARE INSTALLED OR ANY OTHER SOFTWARE DISTRIBUTED TO YOU AT ANY TIME IN CONNECTION WITH THE MAGNIA SG30 (COLLECTIVELY THE “SOFTWARE”), AND THIS MANUAL AND ANY OTHER DOCUMENTATION DISTRIBUTED TO YOU AT ANY TIME IN CONNECTION WITH THE MAGNIA SG30 AND ALL INFORMATION CONTAINED THEREIN (COLLECTIVELY “DOCUMENTATION”) ARE PROVIDED BY TOSHIBA “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE, AND AS TO THE ACCURACY AND COMPLETENESS OF THE DOCUMENTATION, IS WITH YOU. IN NO EVENT WILL TOSHIBA BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE DOCUMENTATION OR ANY INFORMATION CONTAINED THEREIN OR THE USE THEREOF, OR ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE SOFTWARE TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF TOSHIBA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

If you would like to receive a copy of the source code for software licensed pursuant to an end user license agreement that requires that a distribution of the object code shall be accompanied by an offer to provide the source code, please contact product support at the number listed in the accompanying manual.

THE SOFTWARE PROGRAMS THAT ARE INSTALLED OR ANY OTHER SOFTWARE DISTRIBUTED TO YOU AT ANY TIME IN CONNECTION WITH THE MAGNIA SG30 (COLLECTIVELY THE “SOFTWARE”), AND THIS MANUAL AND ANY OTHER DOCUMENTATION DISTRIBUTED TO YOU AT ANY TIME IN CONNECTION WITH THE MAGNIA SG30 AND ALL INFORMATION CONTAINED THEREIN (COLLECTIVELY “DOCUMENTATION”) ARE PROVIDED BY TOSHIBA AMERICA INFORMATION SYSTEMS, INC. (“TAIS”) “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE, AND AS TO THE ACCURACY AND COMPLETENESS OF THE DOCUMENTATION, IS WITH YOU. IN NO EVENT WILL TAIS BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE DOCUMENTATION OR ANY INFORMATION CONTAINED THEREIN OR THE USE THEREOF, OR ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE SOFTWARE TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF TAIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

If you would like to receive a copy of the source code for software licensed pursuant to an end user license agreement that requires that a distribution of the object code shall be accompanied by an offer to provide the source code, please contact TAIS product support at the number listed in this manual.

Magnia is a trademark Toshiba America Information Systems, Inc. and/or Toshiba Corporation.

Ethernet is a registered trademark of Xerox, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Red Hat is a registered trademark of Red Hat, Inc.

Other product names and trademarks belong to the individual companies concerned.

Trademarks

Magnia is a registered trademark and InTouch is a service mark of Toshiba America Information Systems, Inc. and/or Toshiba Corporation.

Apple and Macintosh are registered trademarks of Apple Computer, Inc.

Ethernet is a registered trademark of Xerox, Inc.

Microsoft, Outlook, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

RealNetworks and RealPlayer are trademarks of RealNetworks, Inc.

Red Hat is a registered trademark of Red Hat, Inc.

Intel is a registered trademark and Celeron is a trademark of the Intel Corporation.

WinZip is a registered trademark of WinZip computing, Inc.

America Online is a registered trademark of America Online, Inc.

Wi-Fi is a registered trademark of the Wireless Capability Ethernet Alliance.

Other product names and trademarks belong to the individual companies concerned.

Table of Contents

How to use this guide	19
Other documentation.....	19
Safety icons.....	19
Other icons used.....	20
Service options.....	20
Maintenance contracts	21
Chapter 1: Getting Started	22
What is the Magnia SG30?	22
Features	23
Unpacking the Magnia SG30	24
You will also need.....	24
Quick start procedure	24
Finding your way around	26
Front of the Magnia SG30.....	26
Back of the Magnia SG30	26
Turning on the Magnia SG30.....	28
Shutting down the Magnia SG30.....	29
Connecting the first client computer using the seven LAN ports.....	30
Configuring the first client computer.....	30
Before You Begin.....	31
Configuring the Magnia SG30.....	35
Security modes	35
Magnia SG30 locale.....	36
Internet connection information.....	37
Broadband connection	39
Dial-up connection	41
Connecting a printer to the Magnia SG30 (optional)	42
Configuring wireless access.....	43
Determining if wireless access point is installed	43
Configuring wireless features.....	44
Configuring Wired Equivalent Privacy (WEP) keys	45
Configuring access control.....	46

Using SSL	47
Advanced wireless configuration.....	49
Connecting and configuring other client computers using the seven LAN ports	50
Chapter 2: Setting Up Your Local Area Network	52
Planning your network.....	52
Network topologies.....	53
Wireless networking	55
Physical considerations.....	55
Connecting client computers	57
Dial-in access.....	57
Connecting to an existing corporate network	59
Manually Configuring Clients for the Magnia SG30	61
Manually configuring clients using the Windows 95, 98 and Windows Me operating system	61
Manually configuring clients with Windows NT 4.0, Windows 2000 and Windows XP operating systems.....	70
Configuring a Macintosh client	78
Network settings.....	78
User Accounts.....	79
Chapter 3: Establishing an Internet Connection.....	81
Connecting the Magnia SG30 to the Internet.....	81
Shared Internet access	81
Types of Internet connections	82
Internet connection information.....	83
Configuring for phone-based Internet service.....	83
Configuring for cable-based Internet service	85
Configuring for DSL-based Internet service.....	88
Client configuration to access the Internet	90
Dial-out modem usage	91
Internet performance enhancements	94
Internet content filtering	95
Internet security and the firewall.....	97

How the firewall works	97
Changing the firewall settings	98
Advanced firewall usage	99
Adding your own firewall rules.....	100
Chapter 4: Setting up Email Services	106
Types of email services supported.....	106
Local email	106
ISP Only	107
Internet email (mirrored host).....	108
Using Internet email	109
Setting up the Magnia SG30 for local email	109
Setting up the Microsoft® Outlook® application	110
How to modify your existing Outlook® Express client	112
Setting up the Magnia SG30 for Internet email	114
Domain hosted email (email mirroring)	114
Enabling Internet email for users	115
Summary of email user accounts	116
Sending email through an ISP	116
Client email setup	117
Advanced topics	117
Setting up automated email retrieval	117
Direct email delivery.....	119
Domain hosts and SMTP	119
When Internet email is checked.....	119
Chapter 5: VPN Configuration.....	121
Introduction.....	122
Interactions with Other Magnia SG30 Server Features	123
Remote client access to the VPN through the Internet	124
Configuring the PPTP VPN Software.....	124
Configuring a Client Computer.....	126
Connecting two VPNs in different locations.....	146
Configuring the IPsec Server to Server VPN Software	146
Connecting a Client to the VPN -- Automatically	151

Downloading the IPSec Setup Tool.....	151
Installing the IPSec Client VPN Setup Tool.....	153
How to Install the Certificate Authority	155
Using the Client Client IPsec Tool	158
Connecting a Client to the VPN -- Manually.....	163
Enabling the IPSec Client VPN Feature.....	164
Disabling IPSec Client VPN Access.....	166
Logging On and Using the VPN	166
Chapter 6: Managing the Server	167
Accessing the Administration Web site	167
Exploring the Administration Web site	168
Viewing overall server status.....	169
Viewing server health status	170
Viewing server status through the front panel LCD.....	173
Monitoring Overall Server Status with Toshiba Administrators.....	175
Managing user accounts	175
Predefined accounts	175
System security modes	176
User security levels	178
Creating user accounts	178
Changing user accounts	179
Deleting user accounts.....	179
Backing up your data.....	180
Types of backup	181
Performing a manual backup	181
Selecting backup location	185
Selecting Internet backup.....	187
Starting a manual backup	188
Scheduling an automatic backup	188
Canceling automatic backups	191
Viewing backup status.....	192
Encrypting backups.....	193
Restoring files from a backup.....	195
Selecting an archive.....	195

Selecting files to restore.....	197
Starting the restore	198
Extracting Files Under Windows	199
System Recovery CD	199
Using the second disk drive	200
Primary disk drive usage.....	200
Secondary disk drive usage.....	201
Installing a second disk drive	202
Secondary disk drive usage.....	204
Using an External USB Hard Disk.....	208
Connecting a USB HDD to the Magnia SG30.....	209
Disconnecting the USB HDD	211
Formatting the USB HDD	211
Checking the USB Drive	212
Configuring a Shared Printer.....	213
Software upgrades	214
Viewing available upgrades.....	214
Selecting an upgrade to install.....	215
Viewing installed upgrades	215
Manual software upgrades.....	215
Software upgrades auto-check.....	216
Managing the Intranet site.....	217
Adding your company logo.....	219
Choosing a style and color scheme	220
Adding a welcome message	222
Managing news items	223
Managing events.....	224
Managing documents and forms.....	226
Adding a document or form.....	226
Managing company links.....	229
Developing an Intranet from scratch	230

Chapter 7: Using the Network	231
Logging in to the network	231
Types of users	232
Notes for systems with Windows NT, Windows 2000 and Windows XP operating systems	232
Placing files on the network.....	233
Storing files on the server	234
Sharing files.....	234
Mapping drives using the Windows 95 and Windows 98 operating system.....	235
Mapping drives using the Windows Me operating system	236
Mapping drives using the Windows NT operating system	236
Mapping drives using the Windows 2000 operating system	236
Mapping drives using the Windows XP operating system	237
Technical information on file sharing	237
Sharing a printer.....	238
Connecting the printer to the Magnia SG30.....	238
Connecting a client computer to the network printer.....	239
Deleting print jobs from the print queue	241
Dial-in access	242
Exploring your intranet site	242
Chapter 8: Using Email Services	243
Client email setup and use	243
Internet email (domain hosted)	244
User information.....	245
Chapter 9: Using the VPN	247
Logging On and Using the VPN	247
Disconnecting VPN	248

Chapter 10: Using your Digital Central Intranet Site.....	249
Creating your own photo albums.....	250
Adding photos to the Digital Central photo album	250
Scenario 1: Copying existing digital photos onto your	
Digital Central site	251
Scenario 2: Copying photos from a digital camera to the	
Magnia SG30 with a personal computer as the interface	253
Viewing photo albums	254
Changing the photo album name	255
Removing individual photos from albums or removing albums entirely...	256
Adding/removing digital videos.....	257
Viewing digital videos.....	258
Pocket PC support.....	259
Using the digital music jukebox	259
Creating digital music from your personal music collection.....	261
Copying your personal digital music to your Digital Central site	261
Creating a Playlist	262
Changing the playlist order	265
Adding/removing songs from a playlist	266
Creating a playlist to match an entire album	267
Randomizing a playlist	268
Removing a playlist	268
Playing a playlist from your personal computer.....	269
Playing a playlist on your home stereo system	269
Playing a playlist on a Pocket PC device.....	273
Using the Monitoring System	273
Setting up your monitoring system.....	274
Adding more cameras.....	277
General recording	280
Manual recording	281
Scheduling and managing recordings.....	282
Viewing recordings.....	285
Using the Digital Central recording viewer	286
Deleting a recording from the playback listing.....	288

Connecting to Digital Central with a Pocket PC device	288
Accessing your photo album with your Pocket PC	289
Accessing digital music with your Pocket PC	290
Viewing your monitoring cameras using your Pocket PC	291
Chapter 11: Advanced Networking Features.....	292
Changing the Appliance / Workgroup Name	293
Turning off Workgroup Master Browser.....	295
Changing the Local IP Addresses.....	296
Turning off Network Address Translation.....	297
Resetting Default Networking Configuration	300
SNMP Support.....	301
Chapter 12: Advanced Features-Home Automation Interface	307
Introduction.....	307
Setup/Configuration.....	308
Connecting the Home Automation Controller.....	309
Configuring the Home Automation Controller.....	310
Configuring Lighting	312
Configuring Audio/Video.....	313
Security	315
Heating/Air conditioning	316
Controlling Home Automation Devices.....	317
Lighting.....	317
Audio/Video	318
Security	320
Heat / Air Conditioning	320
Viewing Log Information.....	321
Alarm System Program for Stargate Compatible Controllers	322

Chapter 13: If Something Goes Wrong	324
Problems when you turn on the Magnia SG30.....	324
Problems when you turn on a client computer	325
Internet problems	326
Other system problems	327
Email problems	330
If you need further assistance	331
Remote monitoring and maintenance	331
Toshiba Support Web site	331
Toshiba voice contact.....	331
Appendix A: Specifications.....	332
Basic overview	332
Operating systems supported	333
Appendix B: Privacy Statement for Magnia SG30.....	335
Contacting Toshiba.....	335
Appendix C: Open Source License Information	336
GNU GENERAL PUBLIC LICENSE.....	336
Preamble.....	336
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION	337
NO WARRANTY	338
END OF TERMS AND CONDITIONS.....	339
DES / SSL Library LICENSE.....	339
Open SSL Library LICENSE	340

Introduction

Thank you for purchasing the SG30. With this device you'll be able to quickly and easily install your own network.

For simple, pictorial installation instructions, use the Quick Start card. If you prefer to follow a written procedure, use the Quick Start card in conjunction with [Quick start procedure](#) on page 24.

How to use this guide

This guide introduces the features of the Magnia SG30 and explains how to set up, configure, and maintain your network. Chapters 1-5 (**Getting Started, Setting Up Your Local Area Network, Establishing an Internet Connection, Setting up Email Services, and VPN Configuration**) contain network setup and configuration procedures intended primarily for the network administrator. Chapter 6 (**Managing the Server**) presents many of the ongoing management and monitoring issues for the network administrator. Chapters 7-10 (**Using the Network, Using Email Services, Using the VPN, and Using Your Digital Central Intranet Site**) are for users of the network as well as the network administrator. Information on advanced features and a chapter on troubleshooting (**If Something Goes Wrong**) comprise chapters 11-13.

Other documentation

In addition to this user's guide, Toshiba provides:

- ❖ Quick Start card
- ❖ Warranty and service material
- ❖ End-User License Agreement and Registration Card

Safety icons

Read all safety instructions carefully. Make sure you understand them before using the SG30.

This guide contains the safety instructions that must be observed in order to avoid personal injury or damage to your Magnia SG30. The safety instructions have been

classified according to the seriousness of the risk, and the following icons highlight these instructions:

DANGER

Danger indicates a hazardous situation, which will result in death, serious personal injury, or substantial property damage if the safety instruction is ignored.

CAUTION

Caution indicate a serious situation, which will or can cause minor personal injury or property damage if the safety.

WARNING

Warning indicates a hazardous situation, which can result in death, serious personal injury, or substantial property damage if the safety instruction is ignored.

NOTE

Provides you with important but not hazard-related information..

It is extremely important that basic safety practices are followed when installing and maintaining the system.

Other icons used

Additional icons highlight other helpful or educational information:



TECHNICAL NOTE: This icon highlights technical information about the SG30.



HINT: This icon denotes helpful hints and tips.



DEFINITION: This icon indicates the definition of a term used in the text.

Service options

Toshiba offers a full line of warranty options and service programs. Refer to the warranty and service material included with the Magnia SG30 for more information, or go to our Web site at support.toshiba.com.

Toshiba also offers accessories to enhance server performance. These range from extra cables to more complex items like an extra hard disk drive or a wireless device.

Maintenance contracts

Periodic maintenance and inspection is essential to keeping the Magnia SG30 fully operational. Toshiba recommends taking out a maintenance contract for support of the SG30.

Toshiba also offers a Remote Health Monitoring Service. This service is designed to remotely monitor health information about your Magnia SG30. By monitoring your device remotely, Toshiba can ensure problems are identified early, often before they result in system downtime. To obtain more information, or to sign up, refer to the Services tab on the Magnia SG30 Administration Web site, or call Toshiba.

Chapter 1

Getting Started

This chapter provides a written quick start procedure. In addition to explaining how to connect the Magnia SG30 and install the software, it introduces the unit's features, and identifies each component.

What is the Magnia SG30?

The Magnia SG30 is a device that allows you to quickly connect computers to form a single system through a built-in wired or wireless network. It provides all the basic networking capability you need to support small groups, a home office, or small business, including: file sharing, printer sharing, Internet gateway, and local intranet.

The Magnia SG30 is:

- ❖ Simple to use and setup
- ❖ Dedicated to a limited, but specific purpose
- ❖ Extremely reliable

The Magnia SG30 provides the following networking features:

- ❖ **File sharing:** You can store files on the server's hard disk drives instead of on your local computer. These files are available to any other computer connected to the network. Files stored in your personal directory are accessible to your client computer only when you are logged on with your user account. Files can also be stored in a public directory that is accessible to all users.
- ❖ **Print sharing:** The same printer can serve all computers connected to the network.
- ❖ **Internet gateway:** All network computers can access the Internet through the Magnia SG30. You can surf the World Wide Web, send and receive email, and use other Internet services.
- ❖ **Wireless networking:** The optional internal wireless access point in the Magnia SG30 establishes a fast, secure wireless network for all your clients. Mobile systems such as notebook computers can be used anywhere, and even desktop computers become easier to manage and move because a wired networking infrastructure is no longer required.

- ❖ **Intranet service:** You can customize the content of your preinstalled intranet Web pages, which are stored in the Magnia SG30. The pages include: Welcome page (a good place for your mission statement), Company News (your own electronic newsletter), Upcoming Events (an electronic bulletin board), Docs and Forms (special procedures), and Company Links (your favorite Web links).
- ❖ **Scheduled Internet data backups:** The Magnia SG30 provides a feature allowing you to back up your data on an external FTP site of your choosing on a scheduled basis.
- ❖ **Digital Photo and Video Album:** Organizes your digital photos and digital movie files. Makes photos and movie files accessible from any computer connected to the server.
- ❖ **Digital Music Library:** Organizes and arranges your digital music library (in .mp3 and .wma formats). Makes your music library accessible to all computers connected to the server, and if you purchased the required additional equipment, your home stereo system.
- ❖ **Digital Video Camera Monitoring and Recording:** Provides recording and remote viewing capabilities from an optional video camera(s).

Features

In addition to being easy to set up and administer, your Magnia SG30 provides:

- ❖ **Firewall service:** You don't have to worry about someone accessing your computers illegally over the Internet. The Magnia SG30 comes with a built-in firewall to protect your data.
- ❖ **Scheduled data backup:** You can schedule automatic backups of your important data on a scheduled time frame of your choosing. It's a good idea to back up regularly, especially if the Magnia SG30's hard disk drives contain important information.
- ❖ **Data redundancy:** If you decide to purchase a second hard disk drive, you can use it to back up the primary drive. You can take a snapshot of your main hard disk every night, so that if anything goes wrong you can simply switch drives.
- ❖ **Health Monitoring Service:** For a small subscription fee, Toshiba administrators can monitor various health statistics of your Magnia SG30 from a remote location.
- ❖ **Software upgrades:** As software upgrades or new features become available, you can download and install them from the Internet quickly and easily.
- ❖ **Email:** The Magnia SG30 comes with local email services. Every user added to the system can exchange email with other local network users. You can also establish

Internet email services, and have your domain's email retrieved to the Magnia SG30, or clients can access an external email service directly through your server's Internet gateway.

Unpacking the Magnia SG30

1 Unpack the Magnia SG30 kit.

In addition to this guide, you should have:

- ❖ Magnia SG30
- ❖ Magnia SG30 Setup CD
- ❖ Power cable (black)
- ❖ Ethernet network cable
- ❖ Quick Start card
- ❖ Magnia SG30 Software License Information sheet
- ❖ Master End User License Agreement
- ❖ Limited Warranty booklet
- ❖ Magnia SG30 Product Registration

If any items are missing or damaged, notify your dealer immediately.

2 Write the Magnia SG30 serial and part numbers on the convenient peel-off label located on the Quick Start card.

3 Peel off the label and apply it to the side or base of the Magnia SG30. Avoid covering any ventilation holes.

For a detailed description of each component, see [Finding your way around](#) on page 26.

You will also need

- ❖ Network cables or wireless devices for connecting client computers to the Magnia SG30, and for connecting the Magnia SG30 to the Internet
- ❖ Printer cable if connecting a printer to the USB port

Quick start procedure

If you have already planned your network and are an experienced computer user, this section, along with the Quick Start card, should provide all the information you need.

Otherwise, read [Planning your network](#) on page 52 before installing the Magnia SG30, and begin the installation process with [Finding your way around](#) on page 26.

The basic steps for installing the Magnia SG30 are:

- 1 Unpack all components.
- 2 Assemble the additional components you will need: network cables or wireless network card for client computers, printer cable (if you're connecting a network printer), and telephone cable or Ethernet[®] cable (for connecting to the Internet).

- 3 Locate and identify all ports.

For more information, see [Finding your way around](#) on page 26.

- 4 Turn on the Magnia SG30.

- 5 Connect the first client computer.)

NOTE

Verify that your TCP/IP address is coming from the Magnia SG 30 (i.e., 192.168.1.x)

- 6 Connect a printer to the USB port on the Magnia SG30 (optional).
- 7 Connect the Magnia SG30 to your Internet connection (such as Ethernet connection from cable or DSL modems to the public Ethernet port).
- 8 Run the Client Setup Wizard on the client computer. (Insert the Toshiba Magnia SG30 Setup CD. The CD program runs automatically. Select the option **Connect this PC to your Magnia SG30.**)
- 9 Configure the Magnia SG30. (When you configure the first client computer, the Server Setup Wizard runs automatically after the Client Setup Wizard has finished.)

NOTE

After the Client Setup Wizard has finished the Applianceadmin password will now be the same password of the first user account that was added.

- 10 Connect the rest of the client computers and run the Client Setup Wizard on each.

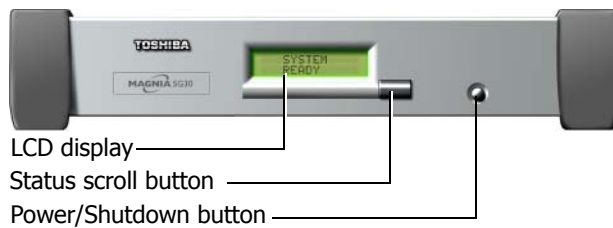
Before you use the Magnia SG30, remember to register it with Toshiba. If you're an experienced user, see [Features](#) on page 23.

The rest of this chapter explains each of these steps in more detail.

Finding your way around

This section explains the physical connections and screen displays of the Magnia SG30.

Front of the Magnia SG30



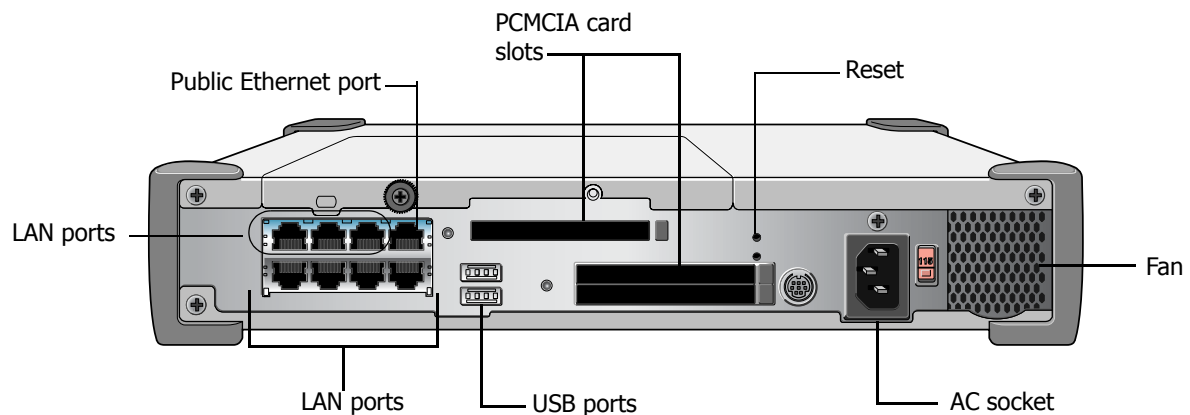
Locating the LCD display, status and power buttons

- ❖ The **LCD display** indicates that the Magnia SG30 is on, provides access to the public and private network IP addresses, and displays warnings if any of the hardware is at the point of failure.

You can configure the display to provide information about the status of your Magnia SG30 such as: modem status, the date and time the last backup was performed, the availability of software upgrades, and so on.

- ❖ The **Status scroll button** allows you to scroll through the information displayed on the LCD display.
- ❖ The **Power/Shutdown button** turns the Magnia SG30 on and off. When you turn off the Magnia SG30, a message prompts you to press the button again as confirmation.

Back of the Magnia SG30



Magnia SG30 ports

- ❖ The **public Ethernet port** connects the network to the Internet via a cable modem, DSL modem or an existing local area network (LAN). For more information about connecting the Magnia SG30 to a corporate network, see [Corporate environment](#) on page 55.
- ❖ The **LAN ports** provide a built-in switch for connecting the individual client computers. For more information about adding a computer to the network, see [Configuring the first client computer](#) on page 30. (All local LAN ports are auto-sensing for uplink connection, and can be used to connect hubs or switches for additional client connections).



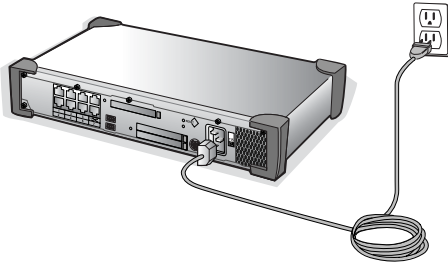
DEFINITION: The Magnia SG30 is a computer through which your local area network (LAN) connects to the Internet.

Each computer connected to the Magnia SG30 is called a client.

- ❖ An optional **PCMCIA modem card** allows the Magnia SG30 to dial out to the Internet, and a client computer to dial into the Magnia SG30. For more information about using the Magnia SG30 modem, see [Stand-alone with modem connection](#) on page 54.
- ❖ Installing an 802.11b/Wi-Fi™ wireless LAN PCMCIA card into a PCMCIA slot enables the Magnia SG30 to provide access to client computers that have 802.11b/Wi-Fi networking capability.
- ❖ The **reset button** resets the Magnia SG30 CPU and restarts the system. For information, see [Problems when you turn on the Magnia SG30](#) on page 324.
- ❖ The **AC socket** connects the Magnia SG30 to AC power (120 volt, 60 Hz line).
- ❖ The **fan** provides cooling to the power supply.
- ❖ The **USB ports** allow connection of selected USB devices to the Magnia SG30. For more information about adding a printer or other device to the network, see [Connecting a printer to the Magnia SG30 \(optional\)](#) on page 42.

Turning on the Magnia SG30

Place the Magnia SG30 where you can easily access the back panel. Connect the black power cable to the socket on the back of the Magnia SG30 and then to a wall outlet.



Connecting the power cable

The Magnia SG30 powers up in a few moments.

NOTE

The system starts as soon as it is plugged in.

If the Magnia Sg30 has been powered off, press the Power/Shutdown button on the front of the Magnia SG30 to turn on the unit. This process takes from 45 to 60 seconds. During this time, the LCD panel displays the message, “Magnia SG30” with an asterisk moving back and forth. When the system has finished loading, the LCD panel reverts to its Date/Time display, indicating it is ready for use. Now you can access the Administration Web site, file and printer sharing, Internet gateway and other services.

If the Magnia SG30 is shut down incorrectly, it may take several minutes to warm up. To avoid this delay, always make sure it is properly shut down.

During the startup process, the Magnia SG30’s LCD displays a “warming up” message. When the startup process is complete, the LCD displays a date and time message as follows:



Magnia SG30 system date and time message

The Magnia SG30 is ready for you to connect the first client computer.

Shutting down the Magnia SG30

As a general rule, you can leave the Magnia SG30 running at all times. If you plan to unplug the unit, make sure the system is shut down properly. Always use the Power/Shutdown button at the front of the unit, or the shutdown command in the Administration Web Site to turn off the Magnia SG30.



Shutting down the Magnia SG30

To shut down the Magnia SG30 using the Power/Shutdown button:

- 1** Press the Power/Shutdown button.
The LCD panel displays a confirmation message.
- 2** Press the Power/Shutdown button again within five seconds to confirm shutdown.
The LCD panel light turns off.

The appliance is now off and safe to unplug.

NOTE

When the Magnia SG30 is shut down, a small amount of power may still be supplied within the unit. This power preserves the last message on the LCD panel, "System Off, Push Power to Start."

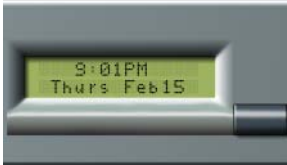
To shut down the system using the Administration Web Site:



- 1** From a client computer, click the **Admin** icon to start the Administration Web site.
- 2** Select the **System** tab, and click the **Shutdown** tab. Then select either:
 - ❖ **Shutdown the Appliance**
 - The system shuts down and turns itself off.
 - ❖ **Reboot the Appliance**

- The system shuts down, then restarts itself.

When the startup process is complete, the LCD panel displays the date and time.



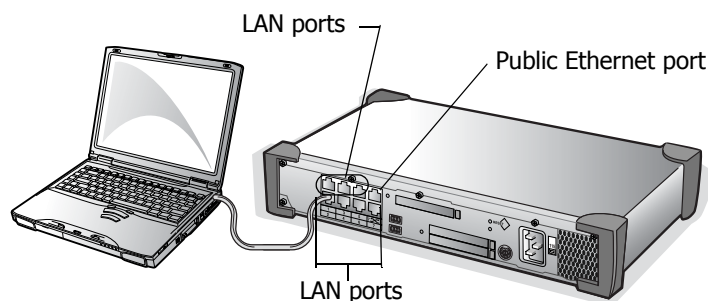
Magnia SG30 system date and time message

The method of shutting the system off described above (and shutting it down using the Administrative Web interface) is a “soft” shutdown, assuring the system software writes all data to disk before turning the power off. You can also shut the system down by pressing the front panel power button and holding it down for 10 seconds. This causes an immediate power off. This method is not recommended, as it turns power off without allowing the software to write all data to disk. As a result, data may be lost, and the system could even become inoperable.

Connecting the first client computer using the seven LAN ports

The first step in setting up your Magnia SG30 is to connect a client computer and configure the computer to access the server.

Using the network cable, connect a desktop or notebook computer to one of the seven LAN ports of the built-in switch on the back of the unit.



A client connected to the Magnia SG30

Configuring the first client computer

The Magnia SG30 Setup CD automatically sets up your client computer to access the Magnia SG30. Specifically, it:

- ❖ Sets up the network configuration
- ❖ Creates a user account on your PC and the server

- ❖ Maps drive G: on the PC to your personal directory on the Magnia SG30
- ❖ Maps drive H: on your PC to the public directory on the Magnia SG30
- ❖ Adds icons to the desktop on your PC for accessing the built-in Intranet and Digital Central Intranet

Before You Begin

The Magnia SG30 comes with three accounts already created and defined on the server. These accounts are defined for specific purposes. The first two of these accounts come from the factory with a default password of “toshiba.” However, both accounts will have their password changed to the first account’s password when the system is first set up.

NOTE

It is important that you remember the password of the first account you create using the Magnia SG30 Setup CD or Administration Web site, because this password will be used to access these predefined accounts.

applianceadmin— Because this account cannot be deleted, it can be used to gain access to the Administration Web site if other accounts have been deleted. It is a predefined level 3 account, meaning that it has full access to all administrative functions. While all other accounts are restricted to viewing files and directories belonging to that account, the applianceadmin account can view and access any file or directory belonging to any account on the server. The applianceadmin account cannot send or receive email.

telnetuser — Telnet is a method of accessing the Magnia SG30 internal Linux interface directly, without going through the Administration Web site. Only experienced Linux users should attempt this method of accessing the server. For security reasons, the only account allowed to log in via telnet is the telnetuser account (it serves no other purpose).

toshsupport — A third account called “toshsupport” is created when you sign up for Health Status Monitoring. This account is not enabled until you enable it in the Administration Web site. The password is calculated at that time and is known only to Toshiba support. Enabling this account will allow Toshiba support personnel access to your system to troubleshoot any problems you report. This access by Toshiba support personnel is restricted by you, and can only occur if and when you enable this account.

- ❖ To set your home page for Internet Explorer to the Magnia SG30 intranet, select the **General** tab from the **Tools** menu and type `http://myserver.loc` in the box labeled Home Page.

NOTE

The address `http://192.168.1.1` may also be used initially to access the intranet. The address can be changed by the user.

- ❖ To access the Administrative web site, type in the address `http://myserver.loc:8282`.

NOTE

The address `http://192.168.1.1:8282` may also be used.

- ❖ If you use the Magnia SG30 Setup CD, you'll find a desktop icon titled "Digital Central" that will take you to the Digital Central intranet site. Without the desktop icon, you can access the Digital Central intranet site by opening your Web browser and specifying `http://192.168.1.1/digital/` as the address.

Follow these steps:

- 1 If it's not on already, turn on the client computer. If it is on, close all other applications to avoid a potential loss of data.
- 2 Insert the Magnia SG30 Setup CD into the CD-ROM drive on the client computer.
The Setup CD menu appears.
- 3 Select **Connect this PC to your Magnia SG30**.

The setup wizard runs automatically and displays the Welcome screen. This wizard automatically configures your computer for access to the Magnia SG30.

NOTE

The Client Setup CD will automatically change your client computer's networking configuration. If you do not want to have your configuration modified by the Setup CD, click **Cancel**. Client computers/workstations that log into a Domain should not use this Setup CD. If you need to run the Server Setup Wizard manually, simply use your web browser on a client connected to the Magnia SG30 local network, and use the following URL: `http://192.169.1.1:8282/wizard`. For more information on connecting and configuring client computers, please see [Connecting client computers](#) on page 57

- 4 Click **Next**.

The setup wizard examines the system and briefly displays a setup screen.

- 5 When the setup wizard displays the User account information screen, enter your personal information.

The logon name is the name you will type every day to log in to your PC and to the network. Pick a name that is easy to remember. If you already have a user account set up on your client computer, you can use this account.

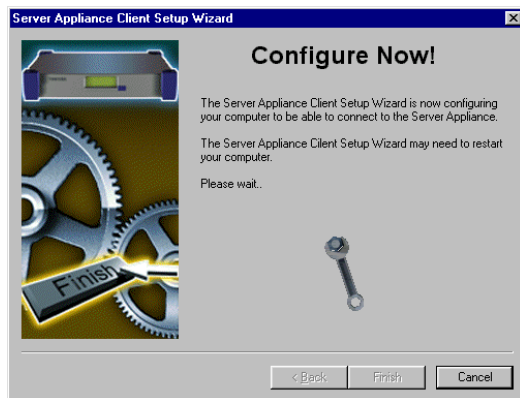
Logon names are conventionally *flastname* where “*f*” is the first initial of the first name, and “*lastname*” is the last name of the user. However, you may use any combination of letters and numbers you wish.

Your password can be any combination of letters and numbers. Make sure it's a name you will be able to remember, but not something like your birthday or nickname that others can easily guess.

NOTE

The Appliance admin account password changes to match the first user's password.

After you've entered the personal information, the Configure Now screen appears.



Sample Configure Now screen

- 6 Click **Next** to continue answering the questions about configuring the Magnia SG30's Internet connection.



Sample Final Setup screen

Your system may restart, after which the setup wizard automatically completes the network setup of your computer.

After restarting, the setup wizard displays the Client Setup Wizard screen, and the configuration process will complete without further interaction.

The first time you run the Client Setup Wizard, it automatically continues with the Server Setup Wizard Welcome screen. Steps for setting up the server are continued in the following section [Configuring the Magnia SG30](#) on page 35.

Configuring the Magnia SG30

The Client Setup Wizard from the previous section automatically continues with the Server Setup Wizard Welcome screen. The Server Setup Wizard performs the initial configuration of your server. Configuration choices you make during this server setup process can always be changed later through the server's Administration Web interface.

If you need to run the Server Setup Wizard manually, simply use your web browser on a client connected to the Magnia SG30 local network, and use the following URL: <http://192.169.1.1:8282/wizard/>.

The setup wizard will ask you to set these options:

- ❖ Security mode (“Ease-of-Use” or “High Security”)
- ❖ System date and time (Locale)
- ❖ Internet connection (Cable, DSL or telephone)

Click **Next** and follow the instructions on the screen to prepare the Magnia SG30.

Security modes

The security mode screen appears.



Sample Security Mode screen

The Magnia SG30 supports two security modes:

- ❖ Ease-of-Use mode allows you to create user accounts on the Magnia SG30 at any time by running the Client Setup Wizard. All user accounts have access to basic server management (administrative) functions using the Administration Web site.



DEFINITION: Each person who uses the network must have a user account set up for them. User accounts determine access to personal files, data, and server administration.

User accounts are level 1, 2 or 3.

Level 1 users have no special account privileges, level 2 users can access basic server management functions, and level 3 users have access to all network features.

- ❖ High Security mode requires you to set up new user accounts before you run the setup wizard on the client computer.

With High Security mode, you must assign access privileges (level 1, 2 or 3) for each user.

You may always change the server's security mode after your network computers are set up.

Magnia SG30 locale

The wizard automatically sets its date and time to that of the client computer you're using to set up the server.

Date and Time **TOSHIBA**

Please set the appliance date and time. If the date and time shown below are correct, simply press the Next button.

Date: [Month: July] [Day: 28] [Year: 2001]

Time: [Hour: 06] [Minute: 52] [AM/PM: PM]

Time Zone: [(GMT-8:00) Pacific Time (US & Canada); Los Angeles]

System Language: [English]

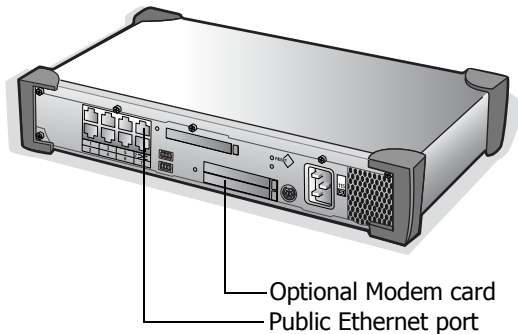
< Back Next >

Sample Date and Time screen

If these values are incorrect, enter the proper date, time, and time zone for the Magnia SG30.

Internet connection information

You have several options for connecting the Magnia SG30 to the Internet.



Options for connecting to the Internet

- ❖ Use the public Ethernet port for a broadband connection (such as cable or DSL) or a corporate LAN. See [Broadband connection](#) on page 39 for detailed instructions.
- ❖ If broadband access is not available, you may connect the server to a phone line and use a dial-up, phone-based ISP (Internet Service Provider). This requires that the optional PCMCIA modem card be installed in the server. See [Dial-up connection](#) on page 41 for detailed instructions.

NOTE

If you do not already have access to the Internet in some way, you will need to obtain an account with an Internet Service Provider.

To configure your Magnia SG30 to access the Internet through your broadband or dial-up connection, select **Yes**. If you do not wish to set up the system for Internet access at this time, select **No** and click **Next**. (You can always configure your Internet access using the Administration Web interface at a later time.) If you select **No**, your server setup is complete.

To configure Internet access:

1 Enter the Internet connection information such as:

- ❖ Server name
- ❖ Primary and secondary DNS
- ❖ User ID and password

If you're unsure how to configure your Internet connection, ask your Internet Service Provider (ISP) to help you.

NOTE

The setup wizard automatically takes you through setting up the Magnia SG30 only once.

To change the configuration, use the Administration Web site. To access the site, click the Admin icon on your desktop.

If you selected Yes, the Internet connection choice screen appears. Note that the modem option will not appear if the optional PCMCIA modem is not installed.



Sample Internet Connection choice screen

2 Select what type of Internet access you will be using.

Broadband access support includes:

- ❖ Cable modem or corporate network connection
- ❖ DSL with Ethernet modem (DSL modems connected with USB are not supported)

For broadband connections, continue to [Broadband connection](#) on page 39.

Alternatively, you can select phone-based access to the Internet using the modem port. Continue at [Dial-up connection](#) on page 41.

Broadband connection

For a broadband connection, the following screen appears.

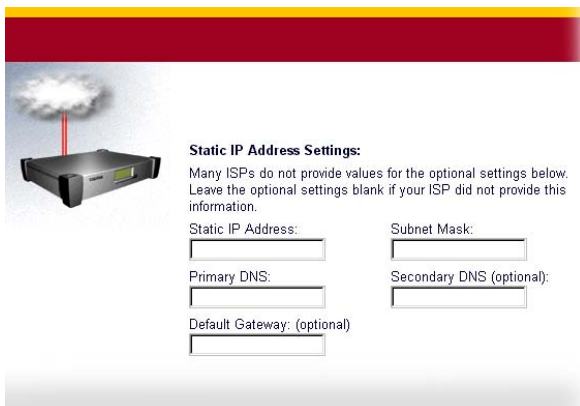
A screenshot of a web-based configuration interface. On the left is a small image of a black router with a cloud icon above it. To the right of the image, the text reads: "Which of the following does your Internet Service provider (ISP) provide?". Below this text are two radio button options. The first option is "DHCP" and is selected. Below it is a paragraph of text explaining DHCP: "Dynamic Host Configuration protocol (DHCP) is used by many ISPs to dynamically assign you an IP address. If your ISP did not provide you with an IP address, then select this option. An IP address looks something like 192.168.123.123." The second option is "A static IP address" and is not selected. Below it is a paragraph of text: "The next page will prompt you for your static IP address and other related settings."

Sample ISP address type screen

1 Select ISP address type.

Determine whether your ISP uses a fixed IP address (provided by your ISP) or is set up to assign the addresses whenever your computer connects. If you don't know, try the **DHCP** option or call your ISP for assistance.

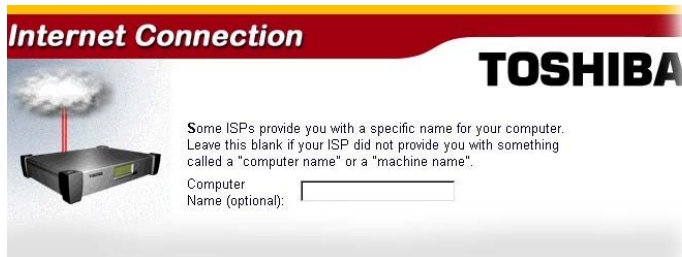
If you select **Static IP**, you will be asked to enter your IP address and subnet mask. These are sets of numbers joined with periods, like 192.168.123.12, and 255.255.255.0. You will also need to enter the primary DNS, which is an IP address like the above examples.

A screenshot of a web-based configuration interface for static IP settings. On the left is a small image of a black router with a cloud icon above it. To the right of the image, the text reads: "Static IP Address Settings: Many ISPs do not provide values for the optional settings below. Leave the optional settings blank if your ISP did not provide this information." Below this text are five input fields arranged in two columns. The first column contains three fields: "Static IP Address:", "Primary DNS:", and "Default Gateway: (optional)". The second column contains two fields: "Subnet Mask:" and "Secondary DNS (optional)".

Sample ISP Static IP address screen

- 2 Enter the secondary DNS and Gateway addresses, if your ISP provides them. Otherwise, leave these fields blank. Click **Next** to continue.

If you selected DHCP on the ISP address type screen, the computer name screen appears. This screen assigns the Magnia SG30 a specific computer name that is used only when communicating with your ISP's DHCP server.

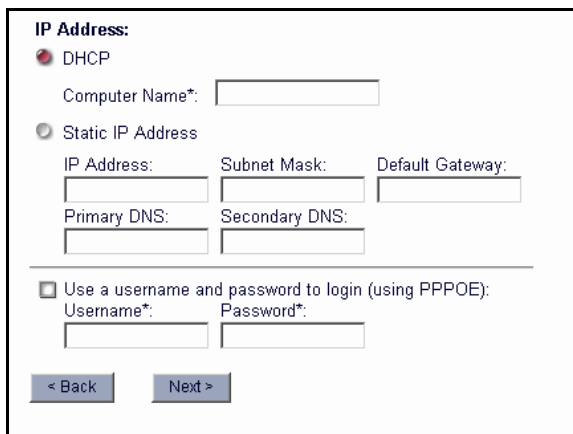


Sample computer name screen

- 3 If your ISP has provided a specific computer name, type the name in the computer name field. Otherwise, leave the field empty.

If you leave the computer name field empty, the server automatically assigns a computer name.

When configuring broadband using DSL, you can also enter a username and password. This is used if your ISP uses PPPoE for its connection protocol.

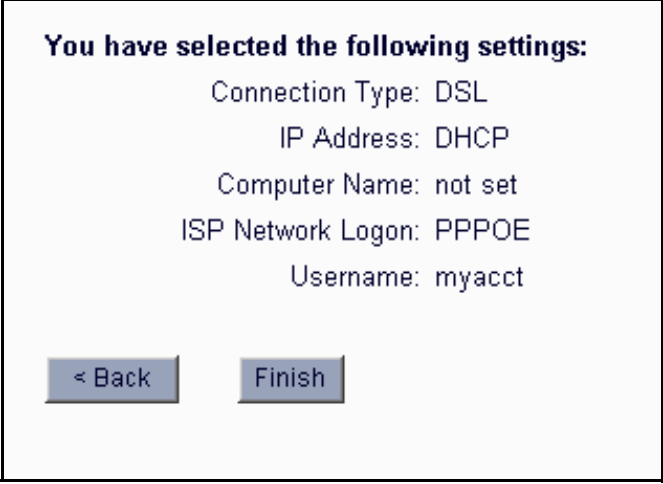
The image shows a web-based configuration screen for "IP Address:". It has two radio buttons: "DHCP" (which is selected) and "Static IP Address". Under "DHCP", there is a "Computer Name*" label and a text input field. Under "Static IP Address", there are three input fields for "IP Address:", "Subnet Mask:", and "Default Gateway:". Below these are two input fields for "Primary DNS:" and "Secondary DNS:". At the bottom, there is a checkbox labeled "Use a username and password to login (using PPPOE):". If this checkbox is checked, there are "Username*" and "Password*" labels, each followed by a text input field. At the very bottom are two buttons: "< Back" and "Next >".

Sample username and password screen

DSL configuration also allows you to select the idle connect timeout value. Don't change the idle connect timeout value from the default "Never" unless you pay for DSL connect time by the minute.

- 4 Click **Next** to continue.

A verification screen appears.



You have selected the following settings:

Connection Type: DSL
IP Address: DHCP
Computer Name: not set
ISP Network Logon: PPPOE
Username: myacct

< Back Finish

Sample verification screen

- 5 If all entries are correct, click **Next** to save your settings.
- 6 Click **Finish** to end the server setup process.

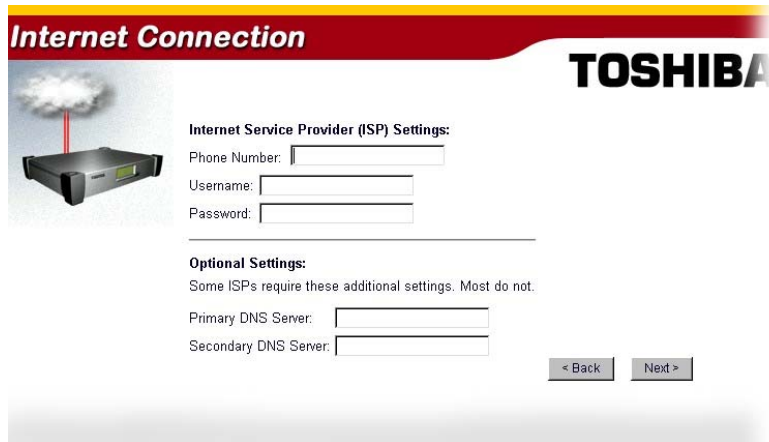
Dial-up connection

NOTE

Some phone-based ISPs require special software to access their networks. These ISPs include America Online[®], and any free ISP that requires advertisements to be downloaded and displayed on your client computer while connected. These ISPs cannot be used with the Magnia SG30.

If you purchased the Magnia SG30 with the optional modem, you can configure the system for modem based Internet access.

- 1 The setup wizard requests information specific to phone-based access. Enter this information, including the phone number you use to connect to your ISP and the account name and password used to validate access.



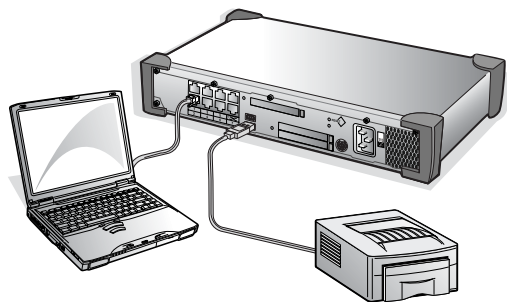
Sample Dial-up connection configuration screen

- 2 When you have completed your dial-up entries, a verification screen appears. If all entries are correct, select **Next**.

Connecting a printer to the Magnia SG30 (optional)

An important feature of the Magnia SG30 is that it allows all users on the network to share the same printer, rather than having a printer connected to each individual computer. Each user can submit print jobs, which will be queued on the Magnia SG30 to be printed in the order received.

Connect the printer's data cable to the Magnia SG30's USB printer port. (If your printer uses a parallel cable instead of USB, a USB to parallel converting cable can be purchased and used to connect with the Magnia SG30).



A printer connected to the USB port

The Magnia SG30 supports both the direct connect USB printer connection, or a network printer connection. If you have a network printer, you can configure the Magnia SG30 to send print jobs to this network printer instead of connecting it directly to the server. If you are connecting a printer directly to the Magnia SG30's USB printer port, you don't need

to configure the printer on the Magnia SG30. If the printer is a network printer, connected to a local network connection, you will have to configure the Magnia SG30 to redirect print jobs to the printer. See [Configuring a Shared Printer](#) on page 213.

Whether you have a network printer or a USB printer, you will need to install the printer on each of the client computers using the Add Printer Wizard. See [Connecting the printer to the Magnia SG30](#) on page 238.

Configuring wireless access

The Magnia SG30 offers a built-in wireless access point option. This option enables you to use the server as a wireless access point for your local network. With this option, you can provide both wireless 11-Mbit and wired 100-Mbit local network access.

Wireless clients can easily access your network, with all of the same features and capabilities as clients directly wired to the seven internal LAN ports. Using the wireless access point option provides immediate, easy and fast expansion of your network with unparalleled flexibility.

If you purchased your Magnia SG30 without the wireless access point option, you can purchase it as a customer-installable feature from Toshiba.

Determining if wireless access point is installed

To determine if the wireless access point option has been installed on your Magnia SG30, open the Administration Web interface, and click the **Network** tab. If wireless access point is not installed, a status screen appears showing the option is not present.



Sample Wireless Access Point not installed screen

If wireless access point is installed, a configuration page appears that enables you to configure the wireless features.

Configuring wireless features

When the wireless access point option is installed in the Magnia SG30, wireless access should be possible using the configured defaults. However, it is recommended that you review the wireless configuration and modify it as necessary.

- 1 Open the Administration Web site, click the **Network** tab, then select **Wireless**.

The wireless configuration screen appears.



Sample Wireless configuration screen

- 2 Select the **Enable Wireless Access Point** check box to enable wireless access. Clear the check box to disable wireless access.
- 3 In the **Network Name** box, enter your network name (sometimes known as the ESSID).

Each wireless client is configured using the same network name. If there is more than one wireless access point, the network name determines which access point each wireless client uses.

- 4 In the **Channel** box, select which radio frequency to use for wireless communications.

This same frequency must also be specified in each wireless client's configuration.

- 5 Select the **Enable Data Encryption** check box to encrypt information sent between wireless clients and the Magnia SG30. Clear the check box to disable encryption.

This feature is known as Wired Equivalent Privacy (WEP).

- 6 If you enabled data encryption in step 5, click the **Configure** hyperlink next to the **Enable Data Encryption** check box to set up or modify the required encryption keys (passwords).

See [Configuring Wired Equivalent Privacy \(WEP\) keys](#) on page 45 for further instructions.

- 7 Select the **Enable Access Control** check box to specify the wireless clients that can access your network, using each client's unique network card MAC address.

This security feature allows only the specified clients to access the network through the wireless access point. See [Configuring access control](#) on page 46 for further instructions.

- 8 Select the **Enable SSL (Secure Sockets Layer)** check box to use HTTPS (Secure Hyper Text Transfer Protocol) to encrypt your usage of the Administration Web Site and the Digital Central Web Site.

The primary purpose of this feature is to add another layer of security to help prevent an unauthorized user on your wireless network from changing settings in the Administration Web Site or Digital Central Web Site.

There are additional advanced wireless configuration options. To view and modify these options, click the **Advanced Settings** hyperlink next to the **Enable Wireless Access Point** check box.

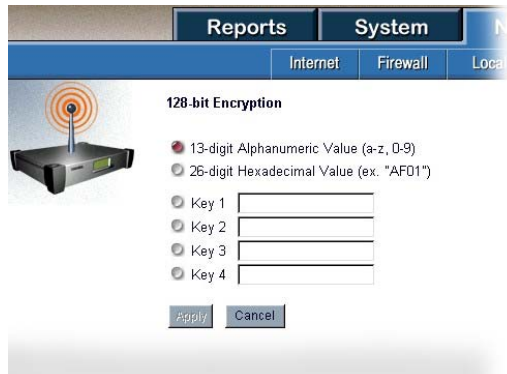
Configuring Wired Equivalent Privacy (WEP) keys

Encryption keys are passwords that are used to ensure privacy when transferring wireless data. To use WEP encryption in your wireless network, all wireless client computers must have the encryption feature installed and enabled, and they must use the same encryption key as the Magnia SG30.

This feature enables you to configure up to four keys, then select which key to enable. This makes it convenient to change the key periodically, without disrupting service while configuring new keys.

- 1 Open the Administration Web site, click the **Network** tab, then click the **Configuration** link next to the **Enable Data Encryption** box.

The following screen appears.



Sample Configure Wired Equivalent Privacy encryption keys screen

- 2 Select either **13-digit Alphanumeric Value** or **26-digit Hexadecimal Value** format for the encryption keys.

The default is alphanumeric. Typically, there is no reason to change this setting.

- 3 Enter up to four encryption keys in the **Key** fields as follows.
 - ❖ When your wireless interface supports 64-bit encryption and you selected alphanumeric format in step 2, enter a five-digit alphanumeric value using letters a through z and numbers 0 through 9 (for example, SECU1).
 - ❖ When your wireless interface supports 64-bit encryption and you selected hexadecimal format in step 2, enter a ten-digit hexadecimal value.
 - ❖ When your wireless interface supports 128-bit RC4 encryption and you selected alphanumeric format in step 2, enter a 13-digit alphanumeric value using letters a through z and numbers 0 through 9 (for example, SECURITY12345).
 - ❖ When your wireless interface supports 128-bit RC4 encryption and you selected hexadecimal format in step 2, enter a 26-digit hexadecimal value.
- 4 Select the key you wish to enable at this time.
- 5 Click **Apply** to save the changes.

Configuring access control

You can control wireless access to your network by specifying each wireless client's MAC address. MAC addresses are 16-digit hexadecimal identification numbers assigned to networking devices, such as adapters, at the factory. Each adapter has a unique MAC

address that cannot be changed. The MAC address is usually printed on a label on the back of the adapter.

Limiting network access to specific MAC addresses provides additional security and improves network performance by filtering extraneous traffic.

- 1 Open the Administration Web site, click the **Network** tab, then select **Wireless**.
- 2 Make sure the **Enable Access Control** check box is selected, then click the **Configuration** link next to it.

The MAC address configuration screen appears.



Sample MAC Address Configuration screen

- 3 To add a new MAC address to the list, enter the 16-digit value in the **New MAC Address** field, then click **Add**.
- 4 To delete a MAC address from the list, click the address you wish to delete, then click **Delete**.
- 5 Click **Apply** to save the changes, otherwise click **Cancel**.

Using SSL

By enabling SSL (Secured Sockets Layer), the main URLs for the Administration Web Site and the Digital Central Web site will be redirected to an HTTPS (Secure HTTP) Web site. HTTPS will encrypt your connections to these sites, thus making your communication more secure. In particular, your user name and password, which you enter to access certain sensitive settings, will be encrypted. This adds one more layer of wireless security should an unauthorized user access your wireless network.

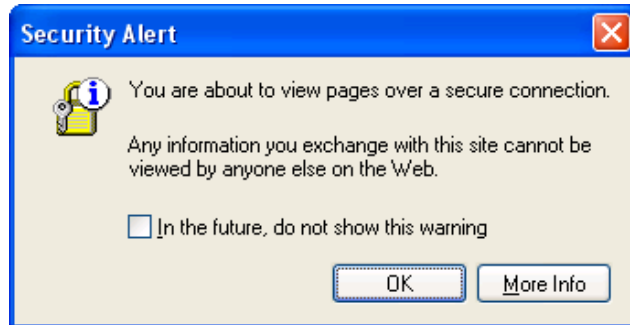
The next time you request either Web site once SSL is enabled, you will be redirected to the corresponding HTTPS Web site. The Administration Web Site, <http://myserver:8282/>,

will redirect to <https://myserver:8383/>. The Digital Central Web Site, <http://myserver/digital/>, will redirect to <https://myserver/digital/>.

NOTE

When you change to SSL, the wireless connection momentarily shuts off.

Whenever you access a secured Web site, you might see the following Security Alert message box. You can simply click Yes to proceed to the Web site.



Security Alert - Entering a secured Web site

You will also be presented with a second security alert which indicates that the Magnia SG30 is not on your list of trusted certificate authorities.



Security Alert - your Magnia SG30 is not on your trusted list

You can simply click **Yes** to proceed to the Web site. However, to avoid this alert in the future, the Microsoft Internet Explorer browser will allow you to click **View Certificate**, and then click **Install Certificate...** and follow the wizard instructions from there. See your browser's documentation or help text for help with this on your browser.

Advanced wireless configuration

The wireless access point feature provides several advanced configuration options. These options should not typically be modified. However, if you are an experienced wireless network administrator managing a multiple access point environment, you may wish to modify these settings.

- 1 Open the Administration Web interface, click the **Network** tab, select **Wireless**, then click the **Advanced Settings** link.

The Advanced Configuration screen appears.



Sample Advanced Configuration screen

Select the **Reject clients using the network name ANY** box (this is the default) to reject connections from wireless clients with a network name (ESSID) of “ANY.” If you clear this check box, the Magnia SG30 accepts connections from wireless clients with a network name of “ANY,” in addition to wireless clients with a network name that matches the configured local network name. (See [Configuring wireless features](#) on page 44 for information on configuring the local network name.)

The **Distance between access points** option prevents overlap of access point service regions when multiple access points are used. This value should not be changed unless the Magnia SG30 is part of a network of wireless access points.

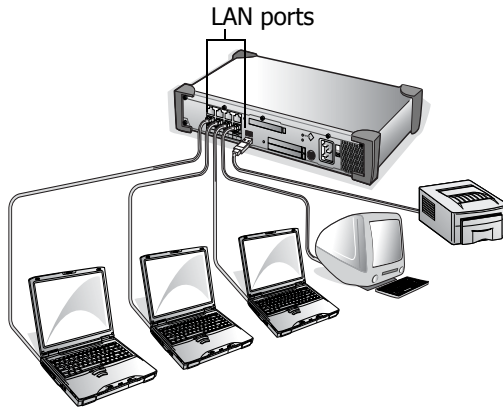
The **Multicast Rate** option applies to multicast environments, which exist in some corporate networks that have multiple access points. Typically, this value should not be changed, as the default multicast rate of 2 Mbit/s is supported by all wireless network interfaces. However, you may want to use higher multicast rates when all of the following conditions exist:

- ❖ Your network environment includes wireless Turbo PC Cards only
- ❖ The physical placement of access points was based on the objective of creating a high-performance wireless infrastructure with maximum data throughput, regardless of the total number of access points required to build such a network
- ❖ All locations where wireless devices are operated have been verified with the Client Manager tool to provide a communications quality that is rated “Excellent” or “Good”

Connecting and configuring other client computers using the seven LAN ports

When you've finished configuring the Magnia SG30:

- 1 Connect the other client computers, each to one of the LAN ports on the Magnia SG30.



An example of a typical local network

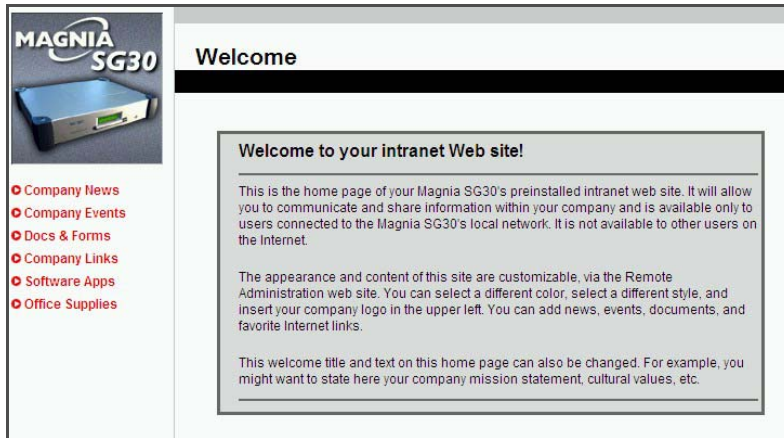
The client computers connected to the Magnia SG30 can use different versions of the Windows® operating system. You can also connect Macintosh computers to the Magnia SG30.

- 2 For PCs, use the Magnia SG30 Setup CD to configure each additional client computer.

To configure a PC manually, see [Manually Configuring Clients for the Magnia SG30](#) on page 61 for more information.

To configure a Macintosh, see [Configuring a Macintosh client](#) on page 78 for more information.

Once setup is complete, the client computer starts your Web browser and displays the Administration Web site if you are the first user, or it displays the preinstalled intranet site if you are a subsequent user.



Sample Intranet home page

This intranet site is fully customizable via the Administration Web site. For more information, see [Managing the Intranet site](#) on page 217.

The Magnia SG30 maintains an internal intranet for the exclusive use of the computers connected to the Magnia SG30. The intranet is not available to outside systems.



HINT: Before using the Magnia SG30 or accessing any external Internet services, Toshiba recommends that you purchase a virus detection program. Viruses have become a danger to all operating systems and can lurk anywhere. They can range from small annoyances to truly destructive events. A virus detection program on your client computers automatically check the files you download from the Internet. You'll need to periodically update this program, but as long as you've got the latest version, your clients should be virus-free.

For more information about setting up client computers and user accounts, see [Managing user accounts](#) on page 175.

Chapter 2

Setting Up Your Local Area Network

This chapter describes the basic configuration options for setting up your Local Area Network (LAN) and connecting to the Internet. This chapter is for the network administrator.

The Client Setup CD is used to modify your client computer's network configuration to match that of the Magnia SG30 [Connecting client computers](#) on page 57. If your client computer is already configured for use with another network (such as a corporate LAN), or if you wish to manually configure your client for Magnia SG30 access, See "Manually Configuring Clients for the Magnia SG30" on page 61. To configure a Macintosh, see [Configuring a Macintosh client](#) on page 78.

For information concerning additional configuration options, and management of the Magnia SG30 through the Administration Web site, See "Managing the Server" on page 167.

Planning your network

This section describes how to set up your Magnia SG30 for the first time.



DEFINITION: A server is the central computer to which other computers connect so that they can share services, such as printing, hard disk space, and the Internet.

In a network, the individual computers connected to the server are called client computers, or clients.

Before you can actually connect your network, you need to:

- ❖ Plan what equipment to use, including any wireless accessories that may be needed
- ❖ Select appropriate locations for the Magnia SG30 and client computers

- ❖ Plan and route cabling to the locations of each client device. (Ethernet cable length and path is key to planning the physical location)
- ❖ Plan and execute wireless area coverage (optional).
- ❖ Ensure that adequate power is available to run the equipment
- ❖ Consider making standby power available for the Magnia SG30 (optional)
- ❖ Take into consideration the location of connections to the telephone or cable system for access to the Internet

If wireless is used, consider distances of the Magnia SG30 to wireless clients. Wireless access may be usable up to 300 feet, though the usable distance can be greatly reduced by walls and other interference caused by machinery or other electronic devices. For best results, the Magnia SG30 should be located in a central position as close to wireless client computers as practical.

NOTE

Wireless security should be taken seriously. The Magnia SG30 supports WEP as well as MAC address filtering. You should also consider enabling SSL for the Administration Web site and Digital Central. For more information, refer to [Configuring wireless access](#) on page 43.

A single Magnia SG30 supports up to seven client computers directly connected to its internal LAN ports. Additional client computers can be connected using an additional hub accessory or through the wireless option.

Connecting to the Internet requires that you subscribe to an Internet Service Provider (ISP). There are many service providers to choose from.

Network topologies



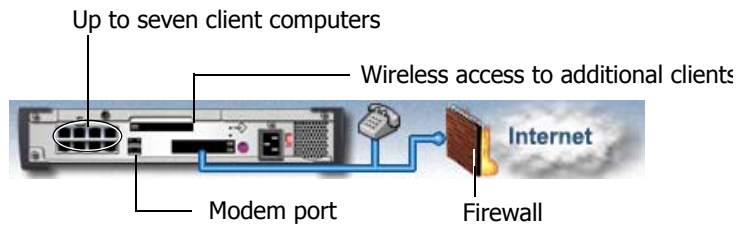
DEFINITION: A topology is the physical layout of the network, including how the devices are connected.

The Magnia SG30 supports several network topologies, including:

- ❖ Stand-alone with modem connection
- ❖ Stand-alone with broadband connection
- ❖ Corporate environment

Stand-alone with modem connection

This is a widely used topology. It has these characteristics:



Modem connection

- ❖ The Magnia SG30 is used as the sole (stand-alone) server within the network.
- ❖ The modem port allows dialing out to the Internet.
- ❖ The firewall is automatically on, but can be turned off.



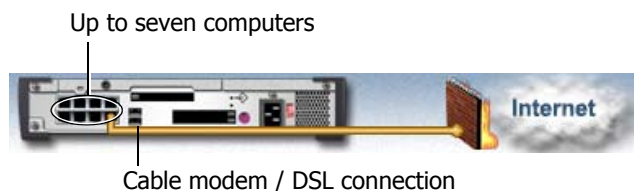
DEFINITION: Firewall is a term for the security procedures used to prohibit unauthorized users from gaining access to the resources on the network.

For more information about firewalls, see [Internet security and the firewall](#) on page 97.

For this topology, connect a standard telephone cable to the modem port and to the RJ11 port on the telephone or wall jack.

Once you have configured the Magnia SG30 with your Internet Service Provider's dial-up settings, any client computer can request Internet content, such as a Web page or email, and the Magnia SG30 will automatically dial out to the Internet.

Stand-alone with broadband connection



Broadband connection

The Magnia SG30 can connect to broadband communications through the public Ethernet port.

Using an RJ45 cable, connect the Magnia SG30's public Ethernet port to a cable modem or Digital Subscriber Line (DSL) modem.

Corporate environment

In this topology, the Magnia SG30's public Ethernet port is connected to a corporate LAN.



Direct connection to a LAN

Direct connection to the corporate LAN is via DHCP client or static IP address.



DEFINITION: DHCP (Dynamic Host Configuration Protocol) is a TCP/IP protocol that enables PCs and client computers to get temporary IP addresses from centrally-administered servers.

You perform the initial setup through the private (Magna SG30) network. Assuming the corporate LAN can be considered a trusted and secure environment, you can turn off the Magnia SG30 firewall. This way, the preinstalled intranet and Administration Web site can be accessed from clients connecting via the corporate LAN.

Wireless networking

Wireless communications provide the ability to connect client computers to the Magnia SG30 and the network to the Internet without using cables.

The Magnia SG30 can be purchased with a built-in wireless capability, so that the server acts as the wireless access point for your wireless network. If the Magnia SG30 contains the wireless access point option, simply configure it for use (see “Configuring Wireless Access” in Chapter 1). Make sure clients systems that are to be part of the wireless network have a wireless 802.11b PC Card or PCI card installed.

Physical considerations

Locate your Magnia SG30 in a safe place, away from work and recreation areas.

Environment

- ❖ Place the server in a clean, dust-free, and well-ventilated place
- ❖ Place the server on a level and steady surface

- ❖ Operate the Magnia SG30 under the following temperature and humidity conditions:

Ambient temperature: 50° F to 95° F (10° C to 35° C)

Relative humidity: 30% to 80% Rh (no condensation)

⚠CAUTION Avoid exposing the Magnia SG30 to condensation during use and storage. Condensation can corrode components and short-circuit electrical circuits if the unit is on.

To avoid damage from condensation when the room temperature is too high or too low, wait about an hour to allow the Magnia SG30 to adjust to the ambient conditions of the room before turning it on.

Other considerations

Never place the Magnia SG30 upside down or in any of the following places:

- ❖ Where it will be exposed to direct sunlight
- ❖ Where it will be exposed to vibration or shock
- ❖ Near any devices that generate a strong magnetic field or produce radio frequency noise—such as a radio, TV, large motor, or loudspeaker
- ❖ Where the temperature and humidity change constantly, near an air-conditioning vent, fan, or heat source
- ❖ Near liquids or corrosive chemicals

⚠CAUTION If debris or liquid gets in the Magnia SG30, shut it down, set the Power/Shutdown button to Off, and unplug the power cable from the AC outlet. Do not turn the unit back on. Contact an authorized Toshiba service provider immediately.

Cleaning the Magnia SG30

If the Magnia SG30's exterior case is dirty or stained, clean it with a soft cloth. If necessary, moisten the cloth with water. Never use harsh chemicals to clean the case.

Power requirements

Before plugging the power cable into a wall outlet, make sure the AC power source and the over-current protector (circuit breaker current rating) are sufficient to handle the requirements of the Magnia SG30.

To ensure a continuous supply of power, Toshiba recommends the use of an Uninterruptable Power Supply (UPS).

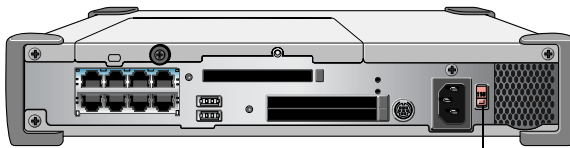
⚠ WARNING

To ensure proper grounding of the Magnia SG30 and avoid a possible fire hazard, only use the power cable provided.

Set the power supply setting on the back of the Magnia SG30 to match your local voltage requirement.

NOTE

The default value for the voltage is 115V.



Power supply setting

Power supply setting

Connecting client computers

The [Quick start procedure](#) on page 24 explains the basics of connecting and configuring client computers for the local network if you have already set it up.

You can connect clients to the Magnia SG30 and configure them quickly and easily using the Magnia SG30 Client Setup CD. This is the recommended method of setting up client computers for your private network.

The Client Setup CD will modify your client computer's network configuration to match that of the Magnia SG30. If your client computer is already configured for use with another network (such as a corporate LAN), you may wish to manually configure your client for Magnia SG30 access.

If you need to set up client computers without using the Client Setup CD, see [Manually Configuring Clients for the Magnia SG30](#) on page 61. To configure a Macintosh, see [Configuring a Macintosh client](#) on page 78.

Dial-in access

The Magnia SG30 has an optional modem that allows users to log in to the network from remote locations (such as their homes) over a phone line. If you would like to allow users to connect via modem, you must first connect the Magnia SG30 to a working phone line.

- 1 Connect a telephone cable from the modem port to the telephone jack.

- 2 At the remote location, connect the computer to the telephone line.

Configuring the Magnia SG30

To perform this procedure, you must be logged in with a user name that has level 3 access. To enable Dial-In access:

- 1 Click the **Admin** icon on the client computer's desktop to access the Administration Web site.
- 2 Click the **Network** tab.
- 3 In the Network section of the tab, select **I want to: Enable Dial-In**.
- 4 Click **Enable/Disable Users**.
- 5 Click **Apply**.

The dial-in screen appears.



Sample Dial-in screen

- 6 Select the **Dial-In Enabled** check box next to a user account to enable dial-in access for that user. To disable access, clear the check box.
- 7 Click **Apply** to save your changes. Otherwise, click **Cancel**.

Configuring the client computer

Even with the Dial-In service enabled, you must grant dial-in access to each user name individually. By default no users can dial in. To allow a user to dial in to the Magnia SG30:

- 1 Click the **Admin** icon on the client computer's desktop to access the Administration Web site.
- 2 In the Users section of the System page, check the **Dial-In Access** option on that user's account configuration page

To perform this procedure, you must be logged in with a user name that has level 3 access.

After the user name has had "Dial-In Access" privileges granted, all other user name and password rules still apply to the client computer. This means that both the client computer that the user is dialing in from and the Magnia SG30 must have the same user name and password.

Once connected to the Magnia SG30 by modem, users can do anything that they were able to do when connected locally including access public and personal files, make backup copies, and print to the network printer.

Connecting to an existing corporate network

Instead of connecting the Magnia SG30 to the Internet, you can connect it to another local network. This is useful if the other network has Internet access, or if you need to transfer files between the Magnia SG30 and the corporate LAN.

Using a suitable cable, connect the corporate LAN to the Magnia SG30's public Ethernet port.



Locating the Ethernet ports on the Magnia SG30

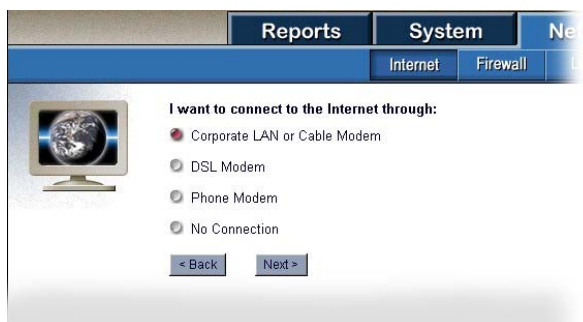
NOTE

Do not connect the LAN to any of the private ports. This action may affect LAN performance. Use only the "public" port for LAN connection.

Configure the Magnia SG30 to the corporate LAN option. If you do this when setting the server up for the first time, you can select this option through the Server Setup Wizard.

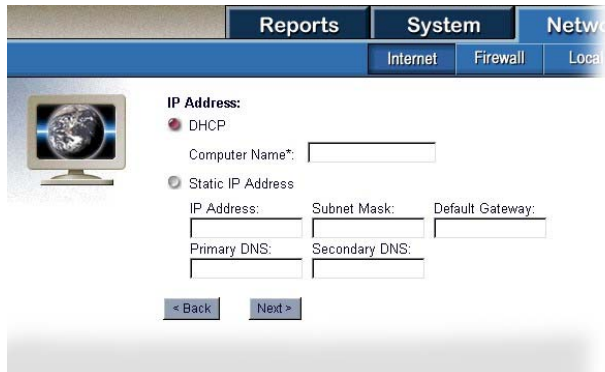
If you have already set up your system, use the Administration Web site to configure the Magnia SG30.

- 1 Click the **Network** tab. Make sure the Internet menu has been selected.
- 2 A screen appears confirming your Internet connection type and configuration. Select the Internet Connection **Configure** option.



Sample Configuring the Internet connection screen

- 3 Select the **Corporate LAN** or **Cable Modem** option. Click **Next**.

A screenshot of a web-based configuration interface. At the top, there are tabs for 'Reports', 'System', and 'Network'. Under the 'Network' tab, there are sub-tabs for 'Internet', 'Firewall', and 'Local'. The 'Local' sub-tab is selected. On the left, there is a small icon of a computer monitor. The main area is titled 'IP Address:' and contains two radio button options: 'DHCP' (which is selected) and 'Static IP Address'. Below the 'Static IP Address' option, there are input fields for 'IP Address:', 'Subnet Mask:', 'Default Gateway:', 'Primary DNS:', and 'Secondary DNS:'. At the bottom, there are two buttons: '< Back' and 'Next >'.

IP Address:
☒ DHCP
Computer Name*:
☐ Static IP Address
IP Address: Subnet Mask: Default Gateway:
Primary DNS: Secondary DNS:
< Back Next >

Sample Configuring the LAN option screen

- 4 Enter your specific network information: specify either **DHCP** or **Static IP** address.

Once you have set up access for the corporate LAN, all client computers attached to the Magnia SG30 will be able to use the LAN's Internet access.

To grant access to the Magnia SG30's files and shared printer to client computers on the corporate LAN, you must turn off the appliance firewall.

To do this:



- 1 From a client computer, click the **Admin** icon to open the Administration Web site.
- 2 Click the **Network** tab.
- 3 Select the **Firewall** menu.

A screenshot of a web-based configuration interface. At the top, there are tabs for 'Reports', 'System', and 'Network'. Under the 'Network' tab, there are sub-tabs for 'Internet', 'Firewall', 'Local', and 'Dial-Up'. The 'Firewall' sub-tab is selected. On the left, there is a small icon of a firewall device. The main area is titled 'I want to set:' and contains two radio button options: 'Firewall on (recommended)' and 'Firewall off'. The 'Firewall off' option is selected. To the right of the 'Firewall on (recommended)' option is a link that says 'Customize'. At the bottom, there is an 'Apply' button.

I want to set:
☐ Firewall on (recommended) [Customize](#)
☒ Firewall off
Apply

Sample Firewall screen

- 4 Select **Firewall off**, then click **Apply**.

Computer systems on the corporate LAN can now access the Magnia SG30 as long as the users have corresponding accounts on the Magnia SG30.

Manually Configuring Clients for the Magnia SG30

This section explains how to manually configure clients to run with the Magnia SG30.

To configure the client using the Windows 95, 98 or Windows Me operating system, see [Manually configuring clients using the Windows 95, 98 and Windows Me operating system](#) on page 61.

To configure the client using the Windows NT, Windows 2000, or Windows XP operating systems, see [Manually configuring clients with Windows NT 4.0, Windows 2000 and Windows XP operating systems](#) on page 70.

Manually configuring clients using the Windows 95, 98 and Windows Me operating system

To access the Magnia SG30, you need to configure:

- ❖ The network card
- ❖ Network settings
- ❖ Web browser

Have your original operating system installation CD available. Many of the settings require this CD to complete the configuration.

NOTE

Some of the steps may require restarting the client computer. Therefore, before starting the configuration, shut down any other software that is currently running to avoid conflicts or loss of data.

Determining if your system has a network interface card (NIC)

If the client computer has no NIC (sometimes also called a network adapter), the first step is to install one. You need to have ready both the driver diskette that came with the card and your Windows® operating system setup CD.

There are three ways to determine if the computer already has a NIC installed:

- ❖ Physical signs
- ❖ Desktop signs
- ❖ Control Panel signs

Looking for physical signs

Check for a PCI network adapter card (if using a desktop computer) or a network adapter PC Card in the PC Card slot of a notebook computer.

Check the documentation that came with your computer. It may indicate that the network feature is built in. If it is, there will be an RJ45 port on the side of the computer for connecting the network cable.

Your computer may also come with wireless networking capability. Check the documentation.

Looking for the Network Neighborhood icon

Look for an icon for Network Neighborhood (or My Network Places). If one appears, your system has a NIC installed.

Looking for Network Adapters in Control Panel

- 1 From the **Start** menu, click **Settings**, then click **Control Panel** to display the Control Panel.

For the Windows® Me operating system, the Control Panel may not automatically display all the operating system options. To locate and view the required icons, click the blue underlined hyperlink **view all Control Panel options**.

- 2 Double-click **System**, and then **Device Manager** in the System Properties dialog box.

In the list of devices, the item Network Adapters should appear. If it does not, there is no network adapter installed.

- 3 If Network Adapters does appear in the list of devices, double-click the words **Network Adapters**.

If the computer is configured for networking through its modem, the Dial-Up Adapter should be listed. If the Dial-Up Adapter is the only network adapter installed on the client computer, you must install a network adapter card.

If any of the devices listed as a part of the Network Adapters group has an exclamation point, that device may not be physically working or may need to be reconfigured. Click the device name and then click **Remove**.

If any of the devices listed as a part of the Network Adapters group has a red "X," that device may be disabled. Click the device name and then click **Properties**. A new dialog box appears named appropriately for your network adapter card. The **General** page should contain a Device status message that says, "The device is disabled." If so, click the gray box beside **Original Configuration (Default)** in the **Device Usage** section of the dialog box.

If any other message appears, consult the documentation supplied with the network adapter card and install the card according to the manufacturer's instructions.

- 4 If the System Properties dialog box is still displayed, click **OK** to close the dialog box.

Configuring the PCMCIA socket

If you are using a PC Card network adapter on a portable computer, you may need to configure the computer's PCMCIA socket. Check the status of the PCMCIA socket using the System Properties dialog box.

- ❖ The item PCMCIA Sockets should appear in the list of devices.

If it does, double-click the words **PCMCIA Sockets**.

If it does not, there is no driver for the PCMCIA socket installed on the computer. You will need to consult the documentation for the computer to configure the PCMCIA socket before you can use a PCMCIA network adapter.

- ❖ If any of the devices listed under PCMCIA Sockets as a part of the Network Adapters group has an exclamation point, that device may not be physically working or may need to be reconfigured. Click the device name and then click **Remove**. Restart the computer and follow the instructions on screen to configure the PCMCIA socket.

If no instructions appear on the screen, consult the computer's documentation for information on installing and configuring the PCMCIA socket.

- ❖ If any of the devices listed as a part of the PCMCIA Sockets group have a red "X," that device may be disabled. Click the device name and then click **Properties**. A new dialog box will appear named appropriately for your PCMCIA socket. The **General** page should contain a Device status message that says, "The device is disabled." If so, click the gray box beside **Original Configuration (Default)** in the **Device Usage** section of the dialog box. Click **OK** to continue.

If any other message appears, consult the documentation for the computer and configure the PCMCIA socket according to the manufacturer's instructions.

For systems with the Windows® 95 operating system, follow the directions on the PC Card Wizard.

Installing the network card using Windows 95 or 98 operating systems

- 1 Click **Start, Settings, Control Panel** and double-click **Network**.

The Network Properties dialog box appears.

If there is no adapter (or only the Dial-Up Adapter) listed in the box labeled "The following network components are installed:" continue with these steps to install your network adapter card.

- 2 On the **Configuration** tab of the Network Properties dialog box, click **Add**.
- 3 When the Select Network Component Type dialog box appears, click **Adapter** in the list, then click **Add**.

- 4 When the Select Network Adapter dialog box appears, either locate the manufacturer and adapter from the provided list and click **OK** or, if you have the driver disk handy, click **Have Disk** and follow the prompts.
- 5 For systems with the Windows® 98 operating system, when your network adapter card has been installed, you may be returned to the Network Properties dialog box. If this happens and you are not prompted to restart your computer, click **OK** and allow the client computer to restart.

The steps for completing the installation depend on the requirements of the network interface. Follow the instructions for each prompt. When installation is complete, you will need to restart the computer.

Before restarting the computer, make sure that the Ethernet cable is properly connected to both the network adapter card and the Magnia SG30. After the computer restarts, you will be ready to continue with your client configuration network settings.

Installing the NIC using the Windows Me operating system

- 1 Click **Start**, **Settings**, **Control Panel** and double-click **Add New Hardware**.

The Add New Hardware Wizard appears.

- 2 Follow the prompts of the Wizard accepting all defaults.

You should allow the Windows® Me operating system to search for your network interface card. If it does not find your particular card, or any errors occur, consult the installation instructions supplied with your network adapter card.

The procedure that the wizard follows depends on the requirements of the network adapter you are attempting to install. Follow the instructions for each prompt. When installation is complete, you will need to restart the computer.

Before restarting the computer, make sure that the Ethernet cable is properly connected to both the network adapter card and the Magnia SG30. After the computer restarts, you will be ready to continue with your client configuration network settings.

Operating system networking settings

Once you have a properly installed network interface card, you need to make additional network settings so that the client computer can communicate with the Magnia SG30. You may need your Windows® operating system setup disk to complete this process.

Determine network settings

To determine the client computer network settings:

- 1 Click **Start** then **Run**.

- 2 In the Run dialog box, type `winipcfg` in the Open box, and click **OK**.

If you get a message that says “Cannot find the file ‘winipcfg’...”, you may need to install TCP/IP, see step 3 below.

If the IP Configuration window appears, click **Release All**, then click **Renew All**.

If the Default Gateway field does not contain the text “192.168.1.1” you must configure your network settings.

- 3 Click **Start**, then **Programs**.

- ❖ For Windows® 95 or Windows® 98 operating systems:
click **MS-DOS Prompt**.

- ❖ For the Windows® Me operating system:
select **Accessories** then click **MS-DOS Prompt**

- 4 When the MS-DOS® Prompt window opens, type:
`ping 192.168.1.1` and press **Enter**.

If the words “Request timed out” or “Bad command or file name” appear in the window, you must configure your network settings.

- 5 Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon.

The Network Properties dialog box appears.

Installing TCP/IP

If there is no listing for TCP/IP in the box labeled “The following network components are installed:” continue with these steps to install TCP/IP.

- 1 Click **Add**.
- 2 When the Select Network Component Type dialog box appears, click **Protocol** in the box labeled Click the type of network component you want to install: then click **Add**.
- 3 In the Manufacturers list, click **Microsoft**. In the Network Protocols list, click **TCP/IP**, then click **OK**.

TCP/IP should now be included in the list labeled The following network components are installed: on the Network Properties dialog box.

- 4 Click **OK** and follow the prompts.
- 5 Restart the client computer to complete installation of TCP/IP.
- 6 Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon.

The Network Properties dialog box appears.

- 7 Click the **Identification** tab. If the **Workgroup** box does not contain the word "SAWORKGROUP," your network settings must be configured.

Configuring network settings

- 1 Click **Start, Settings, Control Panel** and double-click the **Network** icon.
The Network Properties dialog box appears.
- 2 Click the **Configuration** tab.
- 3 In the list labeled The following network components are installed: click the **TCP/IP** item that is associated with the network adapter card you wish to use for connecting to the Magnia SG30, then click **Properties**.
- 4 When the TCP/IP Properties dialog box appears, click the **IP Address** tab.

NOTE

If Specify IP Address is selected and you have numbers in the "IP Address" box or the "Subnet Mask" box, write them down now.

- 5 Select the **Obtain an IP Address Automatically** option.
- 6 Click **OK** on the TCP/IP Properties dialog box to close it.
- 7 Click the **Identification** tab.
- 8 Verify that the computer name displayed is unique for your network. If it is not a unique name, change it to one that will not be used by any other computer.
- 9 In the Workgroup box, type in SAWORKGROUP (all upper case letters) to completely replace any text that was there before.
- 10 Click **OK** on the Network Properties dialog box to close it.
- 11 Restart the computer.

Configuring Internet Explorer to connect to the Magnia SG30

Although you may use any Internet browser to access your Magnia SG30, this section explains how to configure Microsoft® Internet Explorer.

Determining the version of Internet Explorer

The intranet and Administration Web sites on the Magnia SG30 require Internet Explorer version 4.0 or newer. To determine the version of Internet Explorer on your client computer:

- 1 Start Internet Explorer.

- 2 From the **Help** menu, click **About Internet Explorer**.

The version number displays on the About Internet Explorer dialog box.

Running Internet Explorer for the first time

The first time Internet Explorer runs on a computer, it starts with a program called the “Internet Connection Wizard.” If this program displays, simply provide the following answers to the questions:

- 1 On the Welcome page, select the item I want to set up my Internet connection manually or I want to connect through a local area network and click **Next**.
- 2 For the question “How do you connect to the Internet?” select **I connect through a local area network (LAN)** and click **Next**.
- 3 For “Automatic Configuration,” check the item **Automatic discovery of proxy server (recommended)** and click **Next**.
- 4 For the question “Do you want to set up an Internet mail account now?” check the answer **No**, then click **Next**.
- 5 On the page titled Completing the Internet Connection Wizard, click **Finish**.

Setting Internet Explorer options

- 1 From the **Tools** menu, select **Internet Options...**
- 2 When the Internet Options dialog box appears, select the **Connections** tab.
- 3 If the Dial-up Settings are not disabled (gray), select the option **Never dial a connection**.
- 4 To set your home page for Internet Explorer to the Magnia SG30 intranet, select the **General** tab and type `http://myserver.loc` in the box labeled Home Page.

NOTE

The address `http://192.168.1.1` may also be used to access the intranet.

- 5 Click **OK** on the Internet Options dialog box to save your settings.

User accounts

As the server for your local area network, the Magnia SG30 requires accounts with user names and passwords for each of your users. To log in to the Magnia SG30, you must first be logged in to your client computer as that same user.

NOTE

The user name and password must match on both computers.

Creating a new user name and password

Use this procedure if you don't already use a user name and password when you log in to the operating system.

- 1 Click **Start** then **Shut Down**.
- 2 When the Shut Down Windows dialog box appears, select the option to restart the computer and click **Yes**.

When the operating system restarts it should prompt you for a user name and password.

- 3 Type the user name and password that you wish to use to connect to the Magnia SG30. The operating system may require you to confirm the password.

WARNING

Your user name and password must be single words (no spaces) and capitalization must be the same every time you use the name and password.

- 4 If no prompt appears for a user name and password, click **Start, Settings, Control Panel** and double-click the **Passwords** icon.

The Passwords Properties dialog box appears.

- 5 Click **Change Windows Password**. In the Change Windows Password dialog box, type the password you wish to use in both of the boxes for the new password.
- 6 Click **OK**.
- 7 Click **OK** again to close the Passwords Properties dialog box
- 8 Click **Start** then **Shut Down**. When the Shut Down Windows dialog box appears, select the option to restart the computer and click **Yes**.

Using your current user name and password

Use this procedure if you already have a user name and password that you wish to use when you log in to the Magnia SG30.

- 1 If you haven't already done so, restart the operating system.
- 2 Type the user name and password that you wish to use to connect to the Magnia SG30. The operating system may require you to confirm the password.
- 3 Start Internet Explorer or your preferred Internet browser application. Type in the address `http://myserver.loc:8282`.

NOTE

The address `http://192.168.1.1:8282` may also be used.

4 From the Administration Web site, click the **System** tab.

5 Once the System page displays, click **Users**.

The Enter Network Password dialog box appears.

6 If you are the first user to be added to the network, type the user name `applianceadmin` and the password `toshiba`.

If you are not the first user, type your user name and password you wish to use when you log in to the Magnia SG30.

7 Click **New Account**.

If you are logged in as a level 1 or 2 user, the New Account button does not appear.

8 If you are logged in as a level 3 user, type the user name in the account name box exactly as you did when you logged in to your client computer.

9 In the Password box, type the password exactly as you did to log in to your client computer.

10 Type the information requested in the boxes labeled First Name, Last Name, and Title for the new user.

11 Set the Account Level as appropriate for the new user.

For the first connection only

If this is the first time any client computer has been configured to work with your Magnia SG30, you must configure the Magnia SG30 itself.

To do so, start Internet Explorer or your preferred Internet browser application and type in the address `http://myserver.loc:8282/wizard`

NOTE

The address `http://192.168.1.1:8282/wizard` may also be used.

Adding links to the desktop

For convenient access to the Magnia SG30 intranet and Administration Web site, you may add links to the desktop of the client computer. To do so:

1 Click the right mouse button anywhere on the desktop to display the Desktop menu.

2 Select **New**, then **Shortcut** to display the Create Shortcut dialog box.

3 In the Command line box, type `http://myserver.loc` and click **Next**.

NOTE

The address `http://192.168.1.1` may also be used.

- 4 On the Select a Title for the Program page, type `Appliance Server Intranet` in the box labeled Select a name for the shortcut.
- 5 Click the right mouse button anywhere on the desktop to display the Desktop menu.
- 6 Select **New** then **Shortcut** to display the Create Shortcut dialog box.
- 7 In the Command line box type `http://myserver.loc:8282` and click **Next**.

NOTE

The address `http://192.168.1.1:8282` may also be used.

- 8 On the Select a Title for the Program page, type `Appliance Administration` in the box labeled Select a name for the shortcut.

Manually configuring clients with Windows NT 4.0, Windows 2000 and Windows XP operating systems

The Windows NT, Windows 2000, and Windows XP operating systems are very similar in the way they implement networking. They differ from the Windows 95, 98, and Me operating systems in that they require a user to log in. Also, all setup and configuration must be performed by an administrator level user.

NOTE

Be aware that an administrative user on the client computer may not be an administrator on the Magnia SG30. Both computers maintain their own user lists.

This section explains how to configure clients with the Windows 95, Windows 98, or Windows Me operating systems to run with the Magnia SG30.

To access the Magnia SG30, you need to configure:

- ❖ The network card
- ❖ Network settings
- ❖ Web browser

Have your original operating system installation CD available. Many of the settings require this CD to complete the configuration.

NOTE

Some of the steps may require restarting the client computer. Therefore, before starting the configuration, shut down any other software that is currently running to avoid conflicts or loss of data.

Many of the settings require your original installation CD for the operating system. Make sure that you are logged into the client computer as a system administrator before you begin.

Determining if your system has a network interface card (NIC)

If the client computer has no NIC, the first step is to install one. You need to have ready both the driver disk that came with the card and your Windows® operating system setup disk.

Checking for an existing NIC

Here are some ways to check whether the client computer already has a network adapter installed:

- ❖ Check the PCI or PCMCIA (for notebooks) sockets for a network adapter. If you do not find a network adapter card, you will be unable to configure the computer as a client of the Magnia SG30 at this time. If you have not overlooked an existing network adapter, you must purchase one that is compatible with your computer.
- ❖ From the **Start** menu on the taskbar, select **Settings, Control Panel**, and double-click the **Network** icon.

If the message “Windows NT Networking is not installed” appears, you must install a network adapter.

If the Network Properties dialog box appears, click the **Adapters** tab. If there are no adapters listed in the Network Adapters box, you must install a network adapter.

Installing the NIC with the Windows NT® operating system

- 1 Click **Start, Settings, Control Panel**, and double-click the **Network** icon.
- 2 If the message “Windows NT Networking is not installed. Do you want to install it now?” appears, click **OK**.
- 3 Follow the prompts, accepting all default values presented after you have correctly identified your network adapter card. Select to enable DHCP when (and if) asked. You will need both your Windows NT Setup Disk and your network adapter setup disk.
- 4 Restart the client computer.

The steps for completing the installation depend on the requirements of the network interface. Follow the instructions for each prompt. When installation is complete, you will need to restart the computer.

Before restarting the computer, make sure that the Ethernet cable is properly connected to both the network adapter card and the Magnia SG30. After the computer restarts, you will be ready to continue with your client configuration network settings.

Installing the NIC with the Windows 2000 operating system

- 1 Click **Start, Settings, Control Panel**, and double-click the **Add New Hardware** icon.

The Add New Hardware Wizard appears.

- 2 Follow the prompts of the Wizard accepting all defaults.

Allow the operating system to search for your network adapter card. If it does not find your network adapter card as expected, or any errors occur, consult the installation instructions supplied with the network adapter card.

- 3 Follow the instructions on screen.

The steps for completing the installation depend on the requirements of the network interface. Follow the instructions for each prompt. When installation is complete, you will need to restart the computer.

Before restarting the computer, make sure that the Ethernet cable is properly connected to both the network adapter card and the Magnia SG30. After the computer restarts, you will be ready to continue with your client configuration network settings.

Installing the NIC with Windows XP Virtual Private Networking Adapter

To configure your network settings:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 If not in the Classic View, select the **Switch to Classic View** from the left frame.
- 4 Double-click **Network Connections**.
- 5 Select **Create a New Connection** from the left frame. If prompted, enter the area code and close the dialog box. The New Connection Wizard appears.
- 6 Click **Next**. The Network Connection Type page appears.
- 7 Select **Connect the network at my workplace**, and click **Next**.
- 8 Enter the IP address for your Magnia SG30 and click **Next**.
- 9 Click **Finish**.

Networking settings

Once you have a properly installed network adapter card, you need to make additional network settings so that the client computer can communicate with the Magnia SG30.

You may need your Windows® operating system setup disk to complete this process.

NOTE

With the Windows NT, Windows 2000, and Windows XP operating systems, if a network adapter was previously properly installed and was subsequently removed, you may believe that the network adapter card is working, when in fact it is not present. If you complete the steps to establish your network settings, and these continue to fail, verify that the network adapter card is still physically installed in the client computer.

Determining network settings

To determine your client computer network settings:

- 1 Click **Start**, then select **Programs**.
- 2 For the Windows NT® operating system, click **Command Prompt**.
For the Windows® 2000 operating system, select **Accessories**, then click **Command Prompt**.
- 3 When the Command Prompt window opens, type `ping 192.168.1.1` and press Enter.
If the words “Request timed out” or “Bad command or file name” appear in the window, you must configure your network settings.
- 4 While the Command Prompt is open, type `ipconfig /all` and press Enter.
If the words “DHCP Server.....:192.168.1.1” do not appear, or the words “Bad command or file name” appear, you must configure your network settings.
- 5 Click **Start**, **Settings**, **Control Panel**, and double-click the **Network** icon.
The Network Properties dialog box appears.
- 6 Click the **Protocol** tab.

Installing TCP/IP

If there is no listing for TCP/IP in the Network Protocols box, continue with these steps to install TCP/IP.

- 1 Click **Add**.
- 2 When the Select Network Component Type dialog box appears, select **TCP/IP Protocol** in the Network Protocol box, then click **Add**.

- 3 Follow the prompts and accept all defaults.
- 4 Restart the client computer to complete installation of TCP/IP.

Determining if configuration is required

- 1 Click **Start, Settings, Control Panel** and double-click the **Network** icon.
The Network Properties dialog box appears.
- 2 Click the **Identification** tab.
- 3 If the Workgroup box does not contain the word “SAWORKGROUP,” your network settings must be configured.

Configuring your network settings

- 1 Click **Start, Settings, Control Panel**, and double-click the **Network** icon.
The Network Properties dialog box appears.
- 2 Click the **Protocols** tab.
- 3 In the Network Protocols list, select **TCP/IP Protocol**, then click **Properties**.
- 4 When the TCP/IP Properties dialog box appears, click the **IP Address** tab.
- 5 From the drop-down Adapter list, select the adapter that you wish to use for connecting to the Magnia SG30.

NOTE

If Specify IP Address is selected, and you have numbers in the IP Address box or the Subnet Mask box, write them down now.

- 6 Select the option **Obtain an IP Address Automatically**.
- 7 Click **OK** to close the TCP/IP Properties dialog box.
- 8 Click the **Identification** tab.
- 9 Verify that the computer name displayed is unique for your network.
- 10 If it is not a unique name, click **Change** and change it to one that will not be used by any other computer.

NOTE

Write down the existing Domain or Workgroup name.

- 11 In the Workgroup box, click **Change** and type in SAWORKGROUP (all uppercase letters) to completely replace any text that was there before.

NOTE

Make sure you select the Workgroup box, not the Domain box.

- 12 Click **OK** to close the Network Properties dialog box.

- 13 Restart your computer.

Configuring Internet Explorer to connect to the Magnia SG30

Although you may use any Internet browser to access your Magnia SG30, this section explains how to configure Internet Explorer.

Determining the version of Internet Explorer

The intranet and Administration Web sites on the Magnia SG30 require Internet Explorer version 4.0 or newer. To determine the version of Internet Explorer on your client computer:

- 1 Start Internet Explorer.
- 2 From the **Help** menu, click **About Internet Explorer**.

The version number displays on the About Internet Explorer dialog.

Running Internet Explorer for the first time

The first time Internet Explorer is run on a computer, it starts with a program called the "Internet Connection Wizard." If this program appears, simply provide the following answers to the questions:

- 1 On the Welcome page, select the item **I want to set up my Internet connection manually** or **I want to connect through a local area network** and click **Next**.
- 2 For the question "How do you connect to the Internet?," select the answer **I connect through a local area network (LAN)** and click **Next**.
- 3 For "Automatic Configuration," check the item **Automatic discovery of proxy server (recommended)** and click **Next**.
- 4 For the question "Do you want to set up an Internet mail account now?" check the answer **No**, then click **Next**.
- 5 On the page titled "Completing the Internet Connection Wizard," click **Finish** to continue.

Setting Internet Explorer options

- 1 From the **Tools** menu, select **Internet Options....**

- 2 When the Internet Options dialog box appears, select the **Connections** tab.
- 3 If the Dial-up Settings are not disabled (gray), select the option **Never dial a connection**.
- 4 To set your home page for Internet Explorer to the Magnia SG30 intranet, select the **General** tab and type `http://myserver.loc` in the box labeled Home Page.

NOTE

The address `http://192.168.1.1` may also be used to access the intranet.

- 5 Click **OK** on the Internet Options dialog box to save your settings.

User accounts

As the server for your local area network, the Magnia SG30 requires accounts with user names and passwords for each of your users. To log in to the Magnia SG30 as a specific user, you must first be logged on to your client computer as that same user.

NOTE

The user name and password must match on both computers.

Creating a new user name and password

Use this procedure if you don't already use a user name and password when you log in to the operating system.

- 1 Click **Start, Programs, Administrative Tools (Common)** and select **User Manager**.
- 2 When the User Manager window appears, open the **User** menu and select **New User....**
- 3 Complete the information on the New User dialog box.

The user name and password must be those that you wish to use to log in to the Magnia SG30. Capitalization matters.

⚠CAUTION

Be aware of the settings for: User must change his Password at Next Logon, Password never expires, and User Cannot Change Password.

If the password changes on the client computer, it must also be changed on the Magnia SG30.

- 4 When you have completed your data entry, click **OK**.
- 5 Open the **User** menu and select **Exit** to close the User Manager window.
- 6 Click **Start**, then **Shutdown**.

- 7 When the Shut Down Windows dialog box appears, select **Close all programs and log on as a different user**.

Using your current user name and password

Use this procedure if you already have a user name and password that you wish to use when you log in to the Magnia SG30.

- 1 If you haven't just done so, restart the operating system.
- 2 Once it has restarted, type the user name and password that you wish to use to connect to the Magnia SG30.
- 3 Start Internet Explorer or your preferred Internet browser application. Type in the address `http://myserver.loc:8282`.

NOTE

The address `http://192.168.1.1:8282` may also be used.

- 4 From the Administration Web site, click the **System** tab.
- 5 Once the System page displays, click **Users**.
The Enter Network Password dialog box appears.
- 6 If this will be the first user added to the system, type the user name `applianceadmin` and the password `toshiba`.
If this is not the first user, type the user name and password of the level 3 user you wish to log in to the Magnia SG30 as.
- 7 Click **New Account**.
If the user you are logged in as is not a level 3 user, the New Account button does not appear.
- 8 In the Account Name box, type the user name exactly as you did to log in to the client computer.
- 9 In the Password box labeled Password, type the password exactly as you did to log in to your client computer.
- 10 Type the information requested in the boxes labeled First Name, Last Name, and Title for the new user.
- 11 Set the Account Level as appropriate for the new user.

For the first connection only

If this is the first time any client computer has been configured to work with your Magnia SG30, you must now configure the Magnia SG30 itself. To do so, start Internet Explorer

or your preferred Internet browser application. Type in the address
`http://myserver.loc:8282/wizard`

NOTE

The address `http://192.168.1.1:8282/wizard` may also be used.

Adding links to the desktop

For convenient access to the Magnia SG30 intranet and Administration Web site, you may add links to the desktop of the client computer. To do so:

- 1 Right-click anywhere on the desktop to display the Windows[®] Desktop menu.
- 2 Select **New**, then **Shortcut** to display the Create Shortcut dialog box.
- 3 In the Command line box type `http://myserver.loc` and click **Next**.

NOTE

The address `http://192.168.1.1` may also be used.

- 4 On the Select a Title for the Program page, type
Appliance Server Intranet in the box labeled
Select a name for the shortcut.
- 5 Right-click anywhere on the desktop to display the Desktop menu.
- 6 Select **New**, then **Shortcut** to display the Create Shortcut dialog box.
- 7 In the Command line box type `http://myserver.loc:8282` and click **Next**.

NOTE

The address `http://192.168.1.1:8282` may also be used.

- 8 On the Select a Title for the Program page, type Appliance Administration in the box labeled
Select a name for the shortcut.

Configuring a Macintosh client

Unlike client computers running Microsoft[®] Windows[®] operating systems, Macintosh client computers already have the network adapter installed. To connect your Macintosh client to the Magnia SG30 is a simple task of setting some network configurations.

Network settings

To configure your Macintosh:

- 1 From the Apple menu, select Control Panels, then select AppleTalk.

- 2** When the AppleTalk dialog box appears, ensure that Connect via: is set to Ethernet built-in.
- 3** Close the AppleTalk dialog box.
- 4** From the Apple menu, select Control Panels, then TCP/IP.
- 5** When the TCP/IP dialog box appears, ensure that Connect via: is set to Ethernet built-in.
- 6** Set Configure to Using DHCP Server.
- 7** Close the TCP/IP dialog box.
- 8** From the Finder application in the Special menu, select Restart to restart the computer.

User Accounts

As the server for your local area network, the Magnia SG30 requires accounts with user names and passwords for each of your users. To log in to the Magnia SG30 as a specific user, you must first be logged in to your client computer as that same user.

NOTE

The user name and password must match on both computers.

Using your current user name and password

If you are setting up an existing user:

- 1** Start your web browser.
- 2** In the URL address line, type `http://Myserver.loc` and press Enter.



HINT: You can also use the address `http://192.168.1.1`.

- 3** From the Toshiba Appliance Administration page, click the System tab. Once the System page displays, click Users.

The Enter Network Password dialog box appears.

- 4** If this will be the first user added to the system, type the user name `applianceadmin` and the password `toshiba`.

If this is not the first user, enter the user name and password of the level 3 user with which you wish to log in.

Creating a new user name and password

If you are setting up for a new user:

- 1 Click **New Account**.

If the user you are logged in as is not a level 3 user, the New Account button does not appear.

- 2 In the Account Name box, type the user name exactly as you did to log in to your client computer.
- 3 In the Password box, type the password exactly as you did to log in to your client computer.
- 4 Type the information requested in the boxes: First Name, Last Name, and Title for the new user.
- 5 Set the Account Level as appropriate for the new user.

Accessing Public and Private Folders

- 1 From the Apple menu, select Chooser.
- 2 When the Chooser dialog box appears, click **Active for your AppleTalk option**.
- 3 Click **AppleShare** and in the Select-a-file-server list, select your Magnia SG30.

If the name of your Magnia SG30 has been changed from the default Myserver, substitute the new name.



TECHNICAL NOTE: If you are using “Dave” peer-to-peer networking software available from Thursby Software Systems, Inc., you may also connect to the Magnia SG30 by selecting Dave Client.

This software allows Macintosh computers to communicate with computers running Microsoft Windows. It also works with the Magnia SG30. Dave will not interfere with the networking.

- 4 Click **OK**.
- 5 When the Connect to file server dialog box appears, click **Registered User:** and type your user name and password in the spaces provided.
- 6 Click **Connect** to continue.
- 7 When the Select the items you want to use: dialog box appears, click **Public** and the one listed with your user name.
- 8 Click **OK** and close the Chooser dialog box.

Chapter 3

Establishing an Internet Connection

The Internet connection can be established during initial configuration of the Magnia SG 30 by using the Magnia SG 30 Setup CD. It can also be established through the Administration web site if the network administrator opted to not configure with the Setup CD, or if the network administrator wishes to change the initial configuration.

The following sections of this chapter use the Administration Web interface to either setup the Internet connection, or modify the initial Internet configuration. The Administration Web site is accessed by clicking the Admin icon on the client computer's desktop. For further information on using the Administration web site, see [Accessing the Administration Web site](#) on page 167

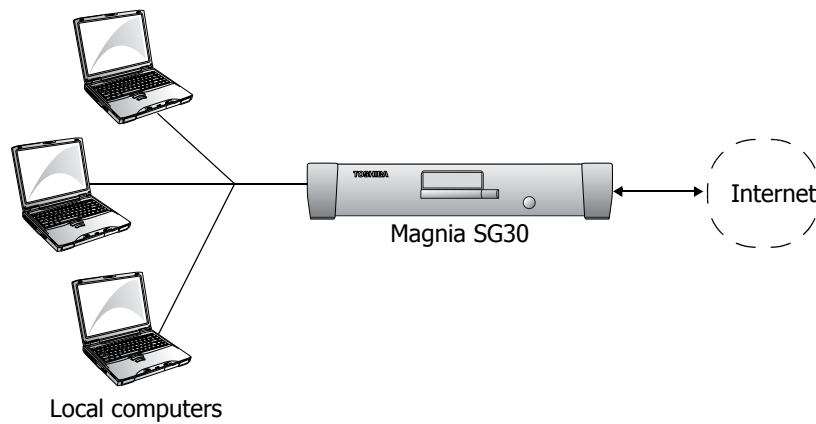
To establish an Internet Connection during initial setup of the Magnia SG 30, see [Connecting the first client computer using the seven LAN ports](#) on page 30 and continue with [Configuring the first client computer](#) on page 30. The setup procedures continue with [Configuring the Magnia SG30](#) on page 35 where the initial Internet configuration is completed. The setup and configuration of the client computers and the Internet connection is done automatically by using the Magnia SG30 Setup CD.

Connecting the Magnia SG30 to the Internet

Shared Internet access

The Magnia SG30 supports phone-based access to the Internet through its optional modem card, or broadband access through its built-in public Ethernet port. When the Magnia SG30 is connected to the Internet, all client computers connected to it can also access the Internet. This shared Internet access allows all the client computers on your local network to use a single Internet access line. While you may have several client computers accessing the Internet, it appears to your ISP as if there is only one computer

connected. The Magnia SG30 takes care of routing Internet traffic to the correct client computer.



Internet data routing

Types of Internet connections

The Magnia SG30 can connect to the Internet in several ways:

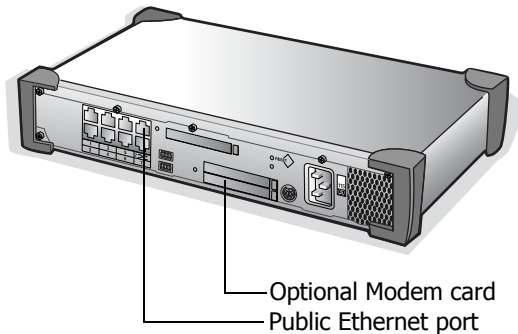
- ❖ Through a phone line (at modem speeds of up to 56,000 baud)
- ❖ Through a cable modem
- ❖ Using a DSL (Digital Subscriber Line)

Each method has its advantages, such as speed or economy, although the final consideration will be what your Internet Service Provider (ISP) offers, and what kind of wiring is available and cost effective in your locale.

When you have decided on the connection to use, contact your local Internet Service Provider and open an account. Once your ISP has supplied you with your account information and the appropriate connection hardware, you may proceed to the following section to connect to the Internet.

Internet connection information

You have several options for connecting the Magnia SG30 to the Internet.



Options for connecting to the Internet

- ❖ Use the public Ethernet port for a broadband connection (such as cable or DSL) or a corporate LAN.
- ❖ If broadband access is not available, you may connect the server to a phone line and use a dial-up, phone-based ISP (Internet Service Provider). This requires that the optional PCMCIA modem card be installed in the server. .

⚠ WARNING

Changing networking options and configurations will restart the networking connections to all clients connected to the Magnia SG30. Ongoing work may be interrupted, and data could be lost. To avoid this, reconfigure networking options only when the Magnia SG30 is not being actively used by client computers or for other system operations, such as backups.

Configuring for phone-based Internet service

Many businesses start with a traditional phone-based connection to the Internet. If you purchased an Magnia SG30 with the modem option, you can connect the Magnia SG30 to a phone line using its 56K modem port. When configuring your Magnia SG30 for a phone-based Internet connection, you will need information such as:

- ❖ Phone number (if using a dial-up ISP connection)
- ❖ Account number or name
- ❖ Password

- ❖ Primary and Secondary DNS (optional, depending on whether the ISP requires this. Most do not).

NOTE

Some phone-based ISPs require special software to access their networks. These ISPs include America Online, and any free ISP that requires advertisements to be downloaded and displayed on your client computer while connected. These ISPs cannot be used with the Magnia SG30.

To configure your system for phone-based access to the Internet:

- 1 Connect your phone line to the modem card at the back of the Magnia SG30.
- 2 From a client computer, click the **Admin** icon to start the Administration Web site. Select the **Network** tab.



A screen describing your current configuration appears.

- 3 Click the **Configure** hyperlink next to the Internet Connection section.

This takes you to the screen where you can select the type of Internet connection to use.

- 4 Select the **Phone Modem** option and click **Next**.

The ISP information screen appears.

Internet Service Provider (ISP) Settings:

Phone Number:

Username:

Password:

Optional Settings:

Primary DNS Server:

Secondary DNS Server:

Sample ISP information screen

- 5 Type in your ISP's phone number, account, and password. The optional setting section allows you to enter your ISP's DNS server information. This is not usually required, because most phone-based ISPs provide this information to your server automatically when it connects. However, if your ISP gives you this information, type it here. The check box to log in to network is used only in rare circumstances.

- 6 When you have finished entering the information, click **Next**.

A confirmation screen showing your current settings appears.



Sample Connection settings screen

- 7 If these settings are correct, click **Finish**.

NOTE

Your configuration changes are not made permanent until you click Finish.

Once configured for dial-up phone access, the Magnia SG30 will dial your ISP and connect to the Internet whenever any client computer connected to it (and properly configured) attempts to access the Internet. This can happen when a client computer accesses a Web site, checks email, accesses an FTP site, or runs a program that attempts to access the Internet (such as RealNetworks™ RealPlayer™).

Once the Magnia SG30 connects to the Internet using a dial-up service, it will typically remain connected for 20 minutes after the last Internet access. If you wish to disconnect the phone sooner than this, you can do so manually. For more information, see [Hanging up or disabling the modem](#) on page 92.

NOTE

The Magnia SG30 provides “dial on demand” service to the Internet. This means that any time any client software accesses any Internet site, the Magnia SG30 will dial out to make a connection. Most client computers have many types of software that automatically make Internet connections. As a result, the Magnia SG30 may dial out to the Internet when it appears that no one is accessing a web browser or other Internet service.

Configuring for cable-based Internet service

As digital cable service becomes more widely available, Internet access using a cable modem is becoming increasingly widespread. This method can provide always connected and extremely fast (broadband) access to the Internet. You can connect the Magnia SG30 to a cable modem using its public Ethernet port. When configuring your Magnia SG30 for a cable-based Internet connection, you will need information such as:

- ❖ Whether your ISP (cable company) has provided a specific IP address (static IP), or whether your Magnia SG30 will obtain a new IP address each time it connects (DHCP).
If you don't know, use DHCP or call your ISP.
- ❖ If your ISP has given you a static IP, you will also need the following information:
 - ❖ IP address
 - ❖ Subnet mask
 - ❖ Primary DNS Server
 - ❖ Secondary DNS Server (optional)
 - ❖ Default gateway (optional)
- ❖ The Magnia SG30 establishes a default computer name to be used with the public Ethernet port. Some cable ISPs require that you assign your computer a name that they specify. If your ISP does this, you will need the specific computer name in addition to the static IP information indicated above.

To configure your system for cable-based access to the Internet:

- 1 Connect your cable modem to the public Ethernet port at the back of the Magnia SG30 using a standard Ethernet (CAT5) cable.

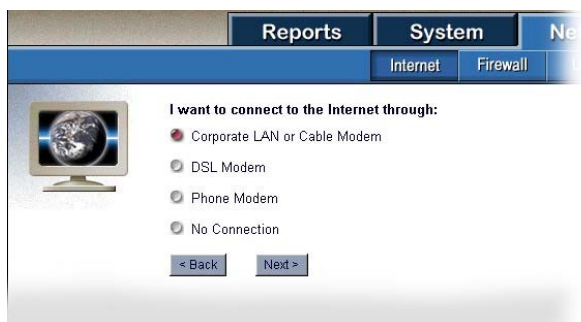


- 2 From a client computer, click the **Admin** icon to start the Administration Web site. Select the **Network** tab.

A screen describing your current configuration appears.

- 3 Click the **Configure** hyperlink next to the Internet Connection section.

This takes you to the screen where you can select the type of Internet connection to use.



Sample Cable connection configuration screen

- 4 Select the **Cable** option and click **Next**.

The ISP information screen appears.



The screenshot shows the 'ISP Information' screen in the Magnia SG30 configuration utility. The interface has a top navigation bar with 'Reports', 'System', and 'Network' tabs. Under 'Network', there are sub-tabs for 'Internet', 'Firewall', and 'Local'. On the left, there is a small globe icon. The main area is titled 'IP Address:' and has two radio buttons: 'DHCP' (unselected) and 'Static IP Address' (selected). Below the radio buttons, there is a 'Computer Name:' text box. Under the 'Static IP Address' section, there are three rows of input fields: 'IP Address' (66.100.107.106), 'Subnet Mask' (255.255.252.0), and 'Default Gateway' (66.100.104.1). Below these are 'Primary DNS' (66.100.104.95) and 'Secondary DNS' (66.100.104.99). At the bottom, there are '< Back' and 'Next >' buttons.

Sample ISP information screen

- 5 If your ISP assigns an IP address each time you connect, select the **DHCP** option. If your ISP has assigned you a specific IP address, select **Static IP Address**, and type in the additional information.

The Magnia SG30 automatically assigns a computer name. You can change this if your ISP uses DHCP and requires a specific name for your computer.

- 6 When you have finished entering the information, click **Next**.

A confirmation screen showing your current settings appears.



The screenshot shows the 'Connection Settings' confirmation screen. It has the same top navigation bar as the previous screen. On the left, there is a small globe icon. The main area is titled 'You have selected the following settings:'. Below this, it lists the selected settings: 'Connection Type: Corporate LAN / Cable Modem', 'IP Address: Static IP (66.100.107.106)', 'Subnet Mask: 255.255.252.0', 'Primary DNS: 66.100.104.95', 'Secondary DNS: 66.100.104.99', and 'Default Gateway: 66.100.104.1'. At the bottom, there are '< Back', 'Finish', and 'Test' buttons.

Sample Connection settings screen

- 7 If these settings are correct, click **Test**.

The Magnia SG30 will use the settings to connect to the Internet through the cable modem. It will then attempt to contact several well-known Internet sites.

- 8 When the Magnia SG30 reports that this process is successful (which may take a minute or two), click **Finish**.

NOTE


Your configuration changes are not made permanent until you click Finish.

Configuring for DSL-based Internet service

DSL (Digital Subscriber Line) service is available from various ISPs. It can provide always connected and extremely fast (broadband) access to the Internet. You can connect the Magnia SG30 to a DSL modem using its public Ethernet port. When configuring the Magnia SG30 for a DSL Internet connection, you will need information such as:

- ❖ Whether your ISP has provided a specific IP address (static IP), or whether your server will obtain a new IP address each time it connects (DHCP). If you don't know, use DHCP or call your ISP.
- ❖ Whether your ISP uses PPPoE (PPP over Ethernet) to connect to its network. If so, you may need to enter an account name and password.
- ❖ If your ISP has given you a static IP, you will also need the following information:
 - ❖ IP address
 - ❖ Subnet mask
 - ❖ Primary DNS Server
 - ❖ Secondary DNS Server (optional)
 - ❖ Default gateway (optional)
- ❖ The Magnia SG30 establishes a default computer name to be used with the public Ethernet port. Some ISPs require that you assign your computer a name that they specify. If your ISP does this, you will need the specific computer name in addition to the static IP information indicated above.

To configure your system for DSL-based access to the Internet:

- 1 Connect the DSL modem to the public Ethernet port at the back of the Magnia SG30 using a standard Ethernet (CAT5) cable.
-  2 From a client computer, click the **Admin** icon to start the Administration Web site. Select the **Network** tab.

A screen describing your current configuration appears.

- 3 Click the **Configure** hyperlink next to the Internet Connection section.

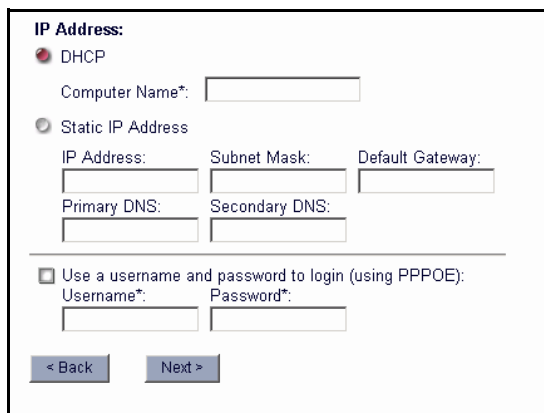
This will take you to the screen where you can select the type of Internet connection to use.



Sample DSL connection configuration screen

- 4 Select **DSL Modem** and click **Next**.

The ISP information screen appears.

A screenshot of a web-based configuration interface for ISP information. The title is 'IP Address:'. There are two radio button options: 'DHCP' (which is selected) and 'Static IP Address'. Below the 'DHCP' option is a text field labeled 'Computer Name*'. Below the 'Static IP Address' option are three text fields: 'IP Address:', 'Subnet Mask:', and 'Default Gateway:'. Below these are two more text fields: 'Primary DNS:' and 'Secondary DNS:'. At the bottom, there is a checkbox labeled 'Use a username and password to login (using PPPoE):'. Below this checkbox are two text fields: 'Username*:' and 'Password*:'.

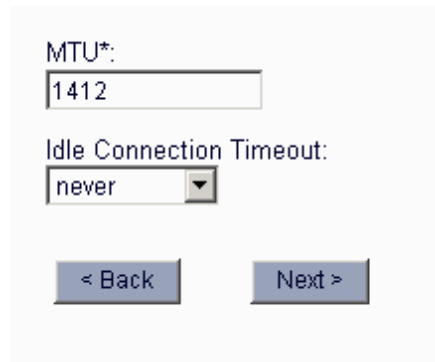
Sample ISP information screen

- 5 If your ISP assigns an IP address each time you connect, select the **DHCP** option. If your ISP has assigned you a specific IP address, select **Static IP Address**, and type in the additional information. You will need to determine whether your ISP requires PPPoE to connect to its network and, if so, obtain an account name and password.

The Magnia SG30 will automatically assign a computer name. You can change this if your ISP requires a specific name for your computer.

- 6 When you have finished entering the information, click **Next**.

A screen displays allowing you to modify some DSL specific configuration items.

A screenshot of a web-based configuration interface for DSL settings. It features two input fields: the first is labeled 'MTU*' and contains the value '1412'; the second is labeled 'Idle Connection Timeout:' and has a dropdown menu currently set to 'never'. Below these fields are two buttons: '< Back' on the left and 'Next >' on the right.

Sample DSL modification screen

You may specify an idle connection timeout value. By default, the timeout is “Never”, which means your DSL connection will not be dropped unless your ISP disconnects it or you shut down the Magnia SG30. Selecting a timeout value tells the Magnia SG30 to disconnect from your ISP when there has been no Internet access for the specified time. It is recommended that you leave the default of “Never” unless you are using a DSL connection with an ISP that charges based on connection time.

You may also specify the MTU (maximum transmission unit) for the connection. This number specifies the size of the data packets being sent out across the broadband connection. Accept the default for this value and do not change it unless you are familiar with broadband network performance tuning.

- 7 When you have finished entering the information, click **Next**.

A confirmation screen showing your new settings appears.

- 8 If these settings are correct, click **Finish**.

NOTE

Your configuration changes are not made permanent until you click Finish.

Client configuration to access the Internet

We strongly recommend that you use the Magnia SG30 Setup CD to configure your local client computers. If you do this, your client computers will automatically be configured to use the Magnia SG30 as their gateway to the Internet. No further configuration changes should be necessary.

If you choose to configure your client computers manually to access the Magnia SG30 (without the Setup CD), see [Manually Configuring Clients for the Magnia SG30](#) on page 61 for complete instructions.

Dial-out modem usage

The optional modem on the Magnia SG30 can be used for either dial-out access to the Internet through an ISP, or dial-in access to the local network. While you can configure the modem for use in both these ways, the modem cannot handle both incoming and outgoing connections at the same time. Configuring the modem for outgoing Internet connectivity can keep it busy for significant periods.

Please note that the features described below may not appear on your Administration Web site if you have not configured an Internet connection using the modem.

Viewing modem status

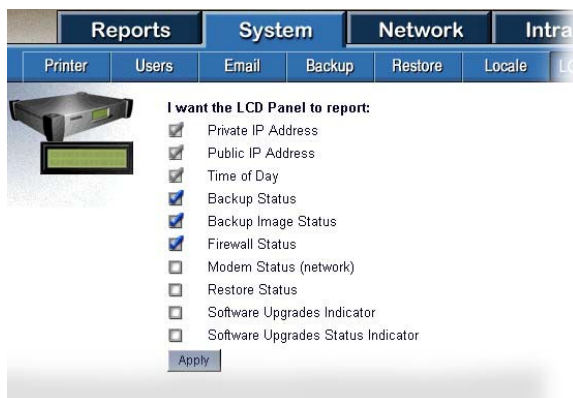
Checking modem status can help you to identify why the modem is currently in use, or to troubleshoot problems connecting to ISPs. You can see what the modem is currently doing in several ways.

The quickest way to view the current status is on the LCD screen. To make sure modem messages have been turned on for the LCD:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site. Select the **System** tab.
- 2 Select the **LCD panel** menu item.

The LCD configuration screen appears.



Sample LCD configuration screen

- 3 If the **Modem Status** item is not selected, select it, then click **Apply**.

Modem messages should now appear on the LCD panel.

Common modem messages displayed on the LCD panel and their meanings are listed below:

Message	Explanation
Modem Ready	The modem is currently hung up, and ready to dial out on request, or to accept dial-in networking calls.
Dialing <number>	The modem is currently dialing the number indicated.
Connect Error	The modem attempted to connect to the ISP, but failed. Reasons may include being unable to negotiate a baud rate, or being disconnected by the ISP's host computer.
No Carrier	The Magnia SG30 dialed a phone number which answered, but the modem on the other end did not respond.
Busy	The modem dialed a number that was busy.
No dialtone	The modem did not detect a dial tone when it attempted to dial out.
No Answer	The modem dialed a number which did not answer.
Logging in	The Magnia SG30 is in the process of logging in to the ISP's network.
Failed to log in	When the Magnia SG30 attempted to log in to the ISP's network, the log in failed. Check the account/password. Alternatively, the ISP's network may be down.
Remote Hangup	The ISP's host computer disconnected the line.
Dialin	The modem is currently connected to a dial-in networking session.

You can also view the current status of the modem from the Administration Web site. From a client computer, click the **Admin** icon, click the **Network** tab, and select the **Internet** menu item. The current modem status is displayed on the Internet page just above the Hangup and Connect buttons.

You can also view a history of the modem messages by clicking the **View Log** hyperlink to the right of the modem status item. This log can be helpful if you are having difficulty connecting to an ISP and wish to see what happened during a connection session.

Hanging up or disabling the modem

The modem can be connected to the Internet for a variety of reasons. Any client computer attached to the local network can cause the modem to dial out when it accesses the Internet through a Web browser, email, FTP or other program (including running programs like RealPlayer). Also, some internal server programs can cause a dial-out to the Internet to manage the internal server cache of Internet information used to speed client access.

Once connected to the Internet, the modem generally waits for 20 minutes after the last Internet access before hanging up automatically.

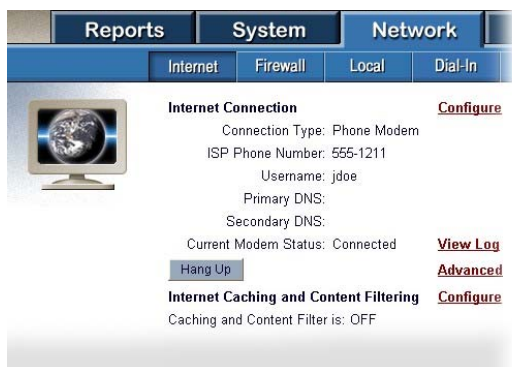
Usually, you can let the Magnia SG30 manage the modem for you, and you do not need to manually intervene and either hang up or dial. However, if you wish to stop the modem from dialing out, or to terminate a current active connection, you can do so from the Administration Web site.

To access the modem management features:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Click the **Network** tab, and select the **Internet** menu item.

The Internet connection screen appears, containing a Hangup button.



Sample Modem hangup screen

- 3 Click **Hang Up** to disconnect the current session and hang up the modem.

NOTE

Be careful when hanging up the modem, because you could disconnect ongoing sessions for other client computers accessing the network, downloading files, or retrieving email.

The modem may redial and attempt to access the Internet because of ongoing network activity from other client computers, or because of internal server cache activities.

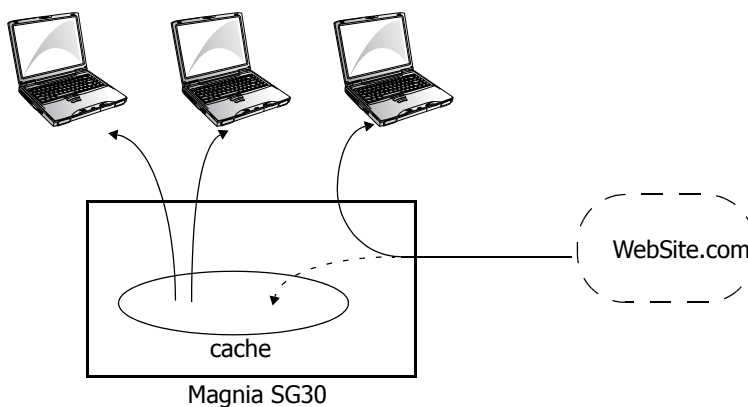
Manually connecting the modem

Under normal circumstances, the modem will automatically dial whenever it needs to access the Internet to service any internal or client computer request. However, you can manually force the modem to connect using the current configuration. This may be useful when you are working to resolve a connection problem.

To manually force a dialout to your ISP, go to the Administration Web site, click the **Network** tab, and select the **Internet** menu option. Click **Connect**. This will cause the modem to dial out and connect to your ISP using the current configuration.

Internet performance enhancements

The Magnia SG30 includes special caching software that helps improve Internet access performance. It does this by keeping copies of frequently accessed Web pages and graphics locally. Delivering Web content to your browser from this cache is much faster than downloading the content from the Internet each time. This can help improve performance by removing much of the effect of slow Internet connections and slow Web site response. In addition, because this cache is shared with all local network users, content saved because of one client computer's Web site access can be used to improve access to that site for all client computers across the entire local network.



Internet performance enhancements

By default, the local caching of Web pages is turned on to increase Internet access performance.

To turn on Internet Caching:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **Network** tab and click the **Internet** menu item.
- 3 Select **Configure** next to the Internet Caching and Content Filtering item.



Sample Enabling network cache screen

- 4 If the option for **Caching and Content Filtering** is turned off, click the option to turn it on and click **Apply**.

Web content caching is now turned on.

Internet content filtering

The Magnia SG30 can also restrict access to specific Web sites, or to sites that contain certain phrases or words in their domain name. This feature can be useful when you wish to regulate access to areas of the Internet by users of your local network.

To use this feature, you must first turn on Internet Caching on Content Filtering. See the instructions outlined in the previous section (Internet Performance Enhancements) to turn this feature on.

Click **Customize** on the screen that allows you to turn on the caching and content filtering.

You will be presented with a screen showing the current content filtering options. When you first configure your system, this list will be empty.

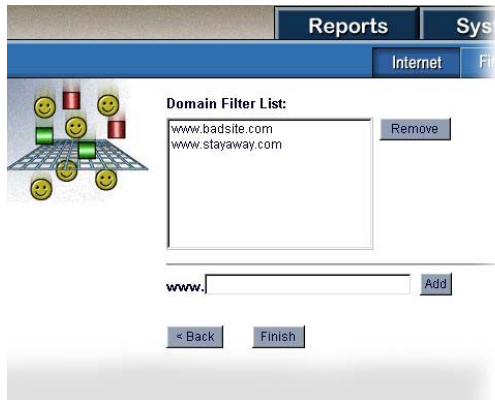


Sample Internet content filtering screen

You have a choice of two filtering methods - domain name filtering or keyword filtering. Use of these methods is outlined in the following sections.

Domain name filtering

To block access to a specific domain, click the **Change** hyperlink next to the Domain filter rule section of the screen. This will present a new screen that allows you to edit the list of blocked domain names (initially empty).



Sample Domain name filtering screen

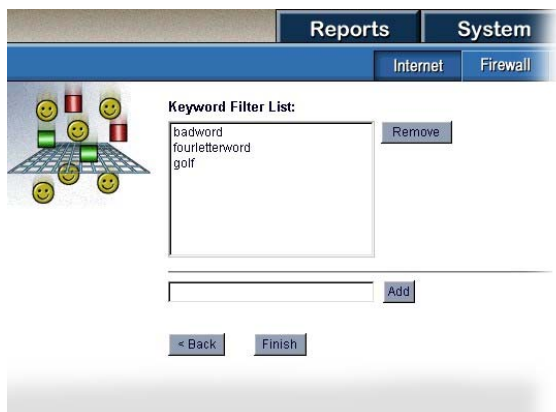
To block a domain, type its name in the fields at the bottom of the screen. You don't need to type the "www." prefix, which is added automatically. After typing the domain name, click **Add** to include the domain name in the list of filtered domains.

If you add a domain to the list and wish to remove it later, come to this screen, select the domain name and click **Remove**. The domain is no longer blocked.

Keyword filtering

To block a number of potential domains or Web sites, you can use a keyword as a filter. Access to any domain or URL containing the keyword will be blocked.

To block access to domains or URLs based on keyword, click the **Change** hyperlink next to the Keyword filter rule section of the screen. This will present a new screen that allows you to edit the list of keywords used to block domain names (initially empty).



Sample Keyword filtering screen

To add a new keyword to use for blocking, type it in the fields at the bottom of the screen. After typing the keyword, click **Add**, to include it in the list of keywords.

If you add a keyword to the list and wish to remove it later, come to this screen, select the keyword and click **Remove**. The keyword is removed from the list and is no longer used to block or filter URLs.

Note that use of filtering keywords can have the effect of blocking sites or URLs unintentionally. For example, the keyword “sex” would block sites such as www.sexton.org or www.essex.com, or URLs such as [//www.AnotherMedicalDictionary.org/article=pectusexcavatum](http://www.AnotherMedicalDictionary.org/article=pectusexcavatum). These kinds of URLs may be generated automatically by some Web sites. As a result, keyword blocking may filter access in unintended ways, and should be used with caution.

Internet security and the firewall

The Magnia SG30 serves as a gateway between your local network (LAN) and the Internet. Whether through a broadband connection using the built-in Ethernet port, or through the built-in modem connection for dial-up Internet access, all your local network’s traffic for the Internet is channeled through the server’s gateway. This provides much more efficient access to the Internet.

The Magnia SG30 incorporates a firewall into the Internet gateway feature to prevent unauthorized access to your network.



DEFINITION: Firewall is the term for a security measure implemented in both hardware and software that prohibits unauthorized users on the Internet from gaining access to the resources on your network.

This firewall is designed to protect your local network while allowing efficient access to the Internet for your users. It prohibits access to your local computer network, and protects your proprietary data and files.

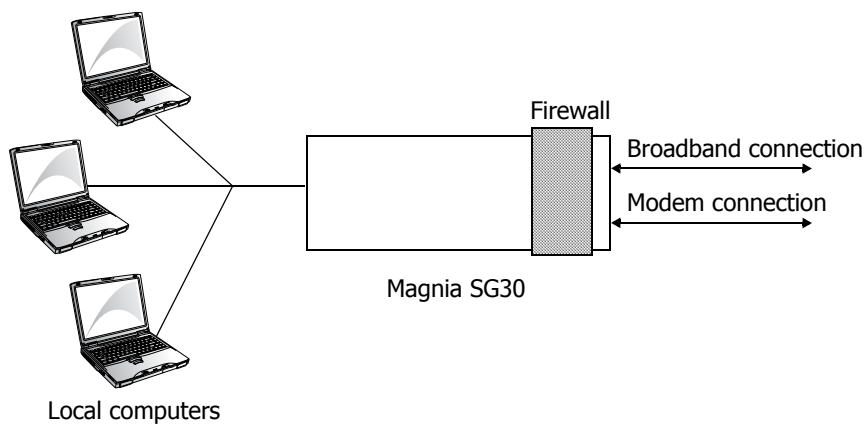
How the firewall works

The primary purpose of a firewall is to provide a single point of entry where a defense can be implemented, allowing access to the Internet from within the organization while controlling access from the Internet to the Magnia SG30.

The firewall works by refusing nearly all direct access to your Magnia SG30 from the Internet. No one may access any application, file, or resource within your firewall from the Internet, but any application (from the local network) may access the Internet and conduct bidirectional access transparently.

All access to the Internet is channeled through a single access point on the server, called the gateway. The firewall incorporated into this gateway is a set of programs designed to deny access to your network from the outside unless access has been granted. By refusing access to your local network resources, the firewall prevents potentially damaging use of your local network computers by outside sources.

The server's firewall is active for all connections made on the public Ethernet port (used for broadband connections to the Internet) as well as all communications on the modem port (used for dial-up Internet connections). This logically separates the server from "remote" access equipment, but does not restrict access by local network clients.



Firewall diagram

The firewall feature is set up to provide maximum protection for your network, and should meet most network needs without change. However, you may occasionally need to enable special access to your local network by allowing additional outside network traffic to pass through the firewall. For this reason, a variety of special-case firewall configuration options are available.

Changing the firewall settings

Your Magnia SG30 has the firewall enabled by default. You can customize the firewall configuration using the Administration Web site.



Sample Firewall screen

Turning off the firewall opens the system to any kind of network access through the broadband Ethernet port (and the modem when using a dial-up ISP). This means access to the Magnia SG30 through these ports will be regulated only by user account access privileges.

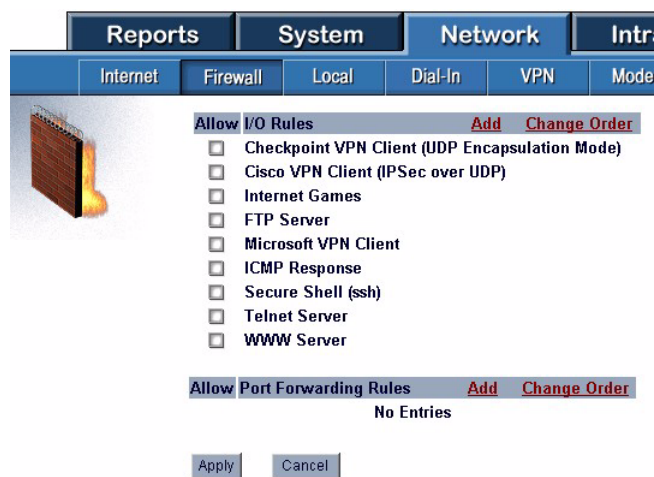
NOTE

Lowering the firewall is not recommended for any Magnia SG30 connected to the Internet.

Advanced firewall usage

Under some circumstances, you may wish to keep the firewall up, but open it to specific features. These features might include access to server features (such as the FTP server) from the Internet, or allowing additional access to a client for special purposes such as multi-user Internet-based gaming.

Click the **Customize** hyperlink on the firewall configuration page to display a list of special applications or communication types that you can allow through your firewall.



Sample Advanced firewall usage screen

The Cisco® and Checkpoint® VPN check boxes allow a client connected to the private network of the appliance server to successfully use their Cisco or Checkpoint VPN client software to tunnel through the appliance server and across the Internet to their VPN server. Not all VPN configurations are supported; only the configurations listed in parentheses are supported. If the VPN client does not work, try again after disconnecting the appliance server and connecting and configuring the client machine directly to the Internet connection used by the appliance server. This will ensure that your VPN server supports your client VPN configuration and that your VPN server and Internet connection are working.

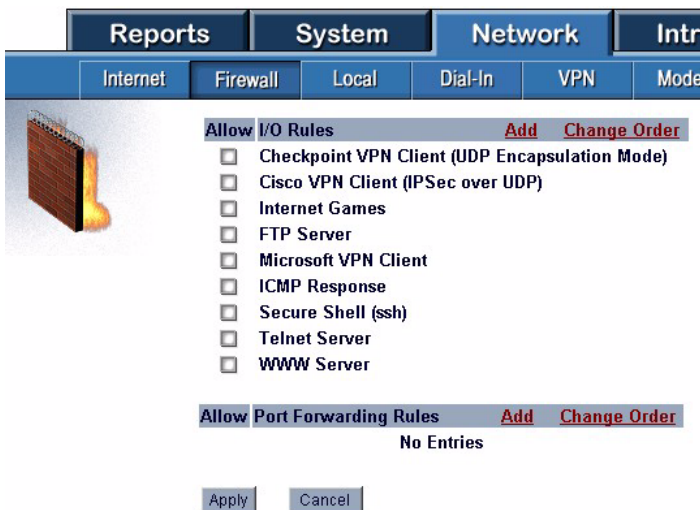
The **Internet Games** check box allows all UDP traffic from port 1024 and higher into the appliance server.

To enable one of the listed features to pass through your firewall, select the check box next to that feature. To disable access, clear the check box.

Other special firewall rules appear on this screen, and can be checked to open the firewall for other types of applications such as FTP, telnet, ssh, and Internet gaming.

Adding your own firewall rules

The Magnia SG30 also allows you to enter your own firewall rules. This can be done by clicking the **Add** hyperlink in either the I/O Rules or Port Forwarding Rules section of the firewall rules listing.



Sample FW Advanced screen

⚠ WARNING

Creating firewall rules should only be attempted by experienced users familiar with firewalls. Incorrect firewall rules can unintentionally block all access to the system, rendering the Magnia SG30 unusable.

When you click the Add button on the I/O Rule list, a screen allowing you to create a new I/O firewall rule displays.

Sample Add IO Rule screen

This screen contains a number of fields necessary for special handling of specific network traffic when opening a hole in the firewall.

Field	Description	Possible Values
Rule Name	This is a text name that helps you easily identify the rule in the future, when editing, sorting or deleting a rule.	Any string up to 30 characters.
Direction	This field allows you to identify whether this rule applies to inbound or outbound network connections. Select the direction from the drop down box.	INPUT, OUTPUT, FORWARD
Protocol	A firewall rule is applied to specific types of network traffic, such as TCP, UDP and other protocols. Select the protocol for this rule from the drop down box.	tcp, udp, any
Interface	The interface field specifies which of the networking interfaces to which this rule will apply. The public (WAN) interface is the external interface, and is the usual interface to which rules are applied. Select the interface from the drop down box.	External, internal, PPP dialin, any
Destination	IP This field allows you to specify that this firewall rule will apply to network traffic destined for a specific IP address. Enter the IP address in the field, or select from the drop down box.	Select either the Public IP / Private IP of the SG30 or input an IP address.

Field	Description	Possible Values
Destination Mask	Allows you to specify the network mask for the destination IP.	Four-byte representation of the network mask for the destination IP. (for example, 255.255.255.0)
Destination Port	This field further narrows the scope of a firewall rule to apply only to traffic on a specific port. Enter a port number range. For a single port, enter the port number in both boxes (e.g. 80, 80).	Can be a single port or a range of ports (1-65535). If these fields are blank then a setting of ANY port will be used.
Source IP	Allows you to specify that the firewall rule will apply to network traffic coming from a specific IP address. Enter the IP address in the field, or select it from the drop-down list.	Select either the Public IP / Private IP of the SG30 or enter an IP address.
Source Mask	The network mask for the source IP of the packet.	Four byte representation of the network mask for the source IP. (for example, 255.255.255.0)
Source Port	The source port for the packet.	Can be a single port or a range of ports (1-65535). If these fields are blank then a setting of ANY port will be used.
Action	Action to take for the packet when it is matched.	Accept or Deny

Port Forwarding rules require slightly different information. When you click the Add button on the Port Forwarding Rule list, a screen allowing you to create a new Port Forwarding firewall rule displays.



Sample Add Port Forwarding Rule screen

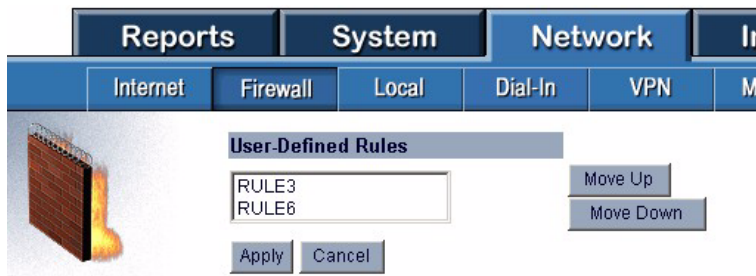
Field	Description	Possible Values
Rule Name	This is a unique name for the custom rule that will be displayed on the main customization page.	Any string up to 30 characters.
Protocol	A firewall rule is applied to specific types of network traffic, such as TCP, UDP, and other protocols. Select the protocol for this rule from the drop-down list.	tcp, udp
Incoming Port	This is the port that the incoming packets are originally destined for.	1-65535
New Destination IP	This is the IP address that these packets will be forwarded to.	Any private IP address behind the firewall.
New Destination Port	This is the port on the new destination IP where the packets will be sent.	1-65535, if this entry is blank then the port will be the same as the incoming port.

The Change Order hyperlink is used to change the relative sort order of the rules. Port forwarding and I/O rules are sorted separately, so there is a separate hyperlink for each of the rule categories.

The firewall rule order can only be changed for user-defined rules. Sort order may be important depending on the nature of the rules that are defined. Firewall rules are processed in a top-down sequence. This means that when the Magnia SG30 receives a packet, it will start at the top of the list of firewall rules and process them one at a time until a match is made for the packet. As soon as a match is made it will process the packet based on that rule. Therefore, if a packet potentially matches two different iptables rules, then the first rule matched will be executed for the packet.

Custom firewall rules are initially process in the order entered. The current processing order can be seen on the advanced firewall page, which lists all custom and optional firewall rules.

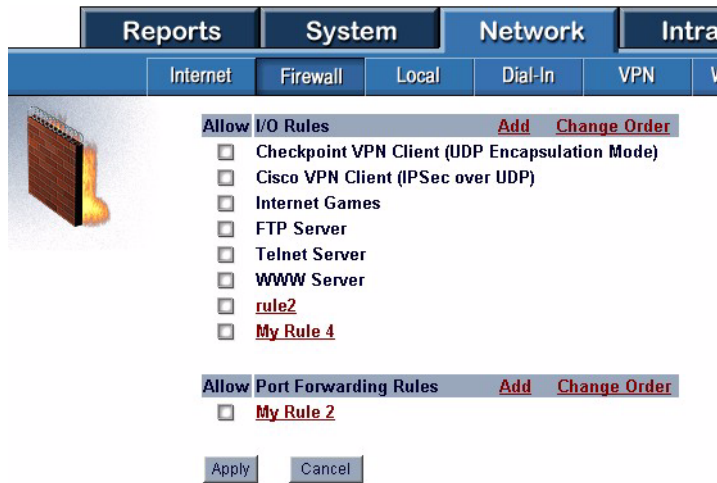
To change the order for either the I/O Rules or the Port Forwarding Rules, click the **Change Order** hyperlink on this page. The resulting screen will list the rules that can be sorted.



Sample Change Order screen

All custom rules are listed on this screen. To select a rule to move in the sequence, click on it to highlight it. Then, move it up and down the list of rules using the Move Up and Move Down buttons. When the order of rule execution is correct, click Apply to save your changes.

Once your custom rule has been defined, it is added to the list of custom rules which appears on the advanced firewall screen.



Sample Advanced with Custom Rules screen

NOTE

Creating new firewall rules does not automatically activate them. You must still check the rule and click Apply to activate it.

Chapter 4

Setting up Email Services

The Magnia SG30 has a built-in mail server capable of sending and receiving email between all the client computers and accounts on your local network, as well as to and from the Internet. The Magnia SG30 can act as the email gateway for your company's connection to the Internet.

NOTE

The Magnia SG30 comes with a built-in administrative account, named "applianceadmin." This account is not capable of sending or receiving email.

Types of email services supported

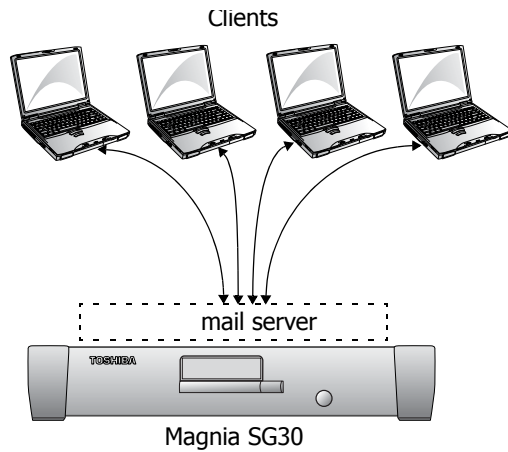
The Magnia SG30 supports several different methods of transmitting and receiving email. You should understand these methods, and choose the one that is right for you.

Local email

The Magnia SG30 comes preconfigured to support local email transmission. This allows any user with an account on the server to exchange email with any other user of the server.

Using this feature, client computers are configured to use the Magnia SG30's mail server, and messages are sent to and held in the server until the recipient checks his/her email.

No email to or from the Internet is supported in this configuration.



Local email diagram

Using Magnia SG30 local email

The Magnia SG30 is set up to support local email automatically. All accounts that are created on the system are capable of sending and receiving local email.

To use the Magnia SG30 to host local email traffic, you do not need to change any server settings.

Because all email programs use a domain (like `mycompany.com`) to address email, the local mail service of the Magnia SG30 established a local domain. This domain is `myserver.loc`. Each user account on the Magnia SG30 is set up with local email so that you can send email to `acct@myserver.loc` where `acct` is the user's account name.

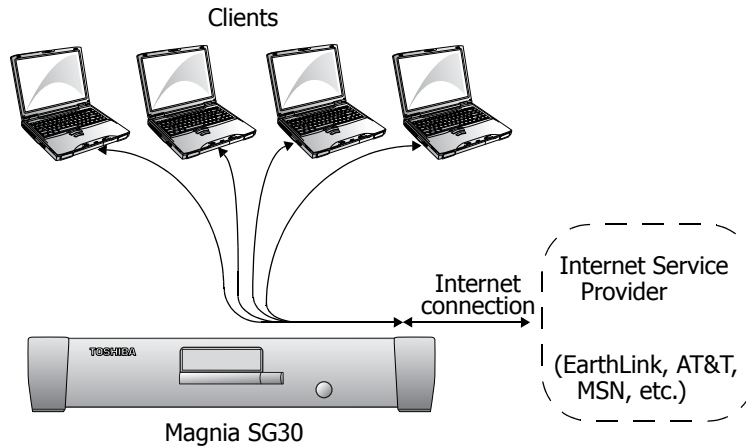
For more information, see [Setting up the Magnia SG30 for local email](#) on page 109.

ISP Only

If you already have an email service with an ISP, you can continue to use this from your client computers. In this mode, your client computers communicate directly with your ISP, sending and receiving email to and from the ISP's mail servers. If you choose to access email in this manner, simply set up your mail clients such as Outlook[®] Express (or keep their existing setup) as defined by your ISP.

When setting client computers up in this way, you are not using the Magnia SG30 mail server, and are simply using its shared Internet gateway to access your existing ISP email accounts.

This option also applies whenever you establish domain-hosted email which you access directly, either through a Web-based interface or directly from your email clients on your computer.



ISP connection email diagram

For more information, see [Sending email through an ISP](#) on page 116.

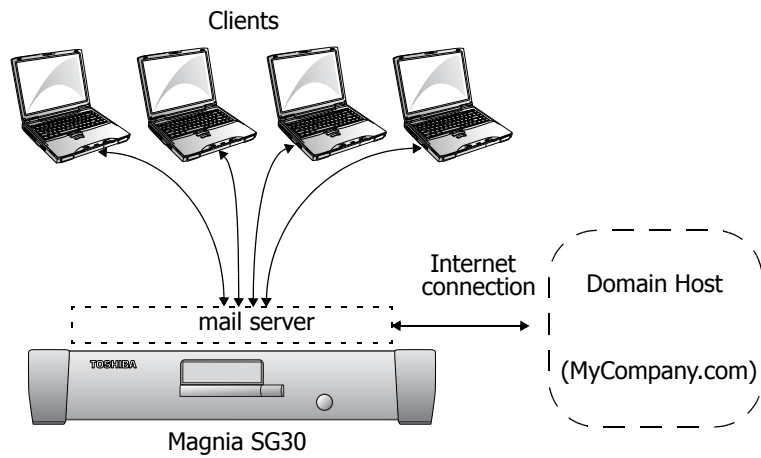
Internet email (mirrored host)

The Magnia SG30 email server is also capable of sending and receiving mail via an established mail server on the Internet. This is commonly used if you wish to establish your own domain on the Internet (`mycompany.com`) and have an Internet hosting company host your email services (`user@mycompany.com`).

You can have the Magnia SG30's email server mirror your domain's email locally. The advantage of doing this is that local email (messages destined for someone with an account on the Magnia SG30) goes directly to the local recipient—it will not be transmitted to the Internet and then sent back to your local network. Messages for recipients who aren't local to your network are sent to your domain host's server for transmission.

Alternatively, when you establish a domain with hosted email, you can set up your client computers to access the hosting site's servers directly. In this case, you are using the

Magnia SG30 in essentially the same way as described in the “ISP Only” section (above).



Mirrored email from host

For more information, see [Setting up the Magnia SG30 for Internet email](#) on page 114.

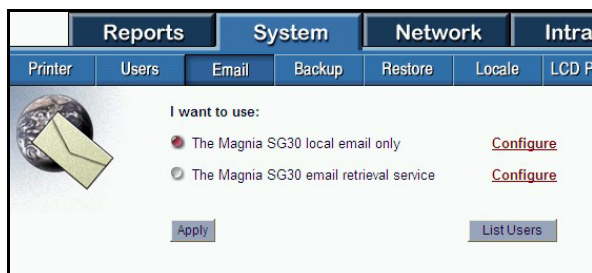
Using Internet email

If you establish your own domain on the Internet and can send and receive mail from this domain, you can configure the Magnia SG30 email server to automatically download email from this domain, and to send its mail to Internet users through this domain.

NOTE

The Magnia SG30 email server places a 10 MB limit on emails (including their attachments). Individual mail messages larger than this will be rejected. This limit does not apply to the ISP-only email option.

Setting up the Magnia SG30 for local email



Sample Local email setup screen

Because this is the way the system is configured when you first setup the Magnia SG30, there is no need to change these settings to use local email. However, if you had previously configured the server for Internet email, you can go to this screen to select local email only.

All user accounts are automatically set up for local email. To see this, click **List Users** on the email management screen (depicted above). This will present a list of all user accounts and their corresponding email addresses.

NOTE

Changing from Internet to local email only will clear all the Internet email information on the server, such as POP or SMTP addresses, user accounts and passwords.

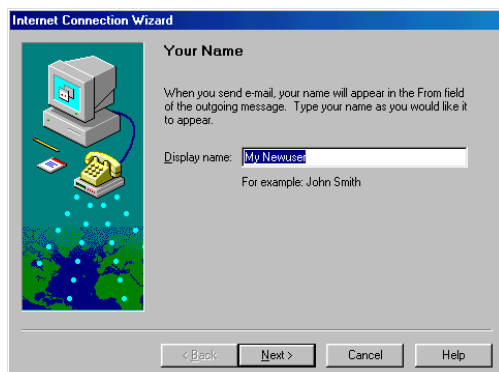
Please note that all accounts are set up with email addresses that use the Magnia SG30 user account name as the email address. For example, you could send local email to a user with the account name “jsmith” using the address jsmith@myserver.loc.

If you change the name of the Magnia SG30 (server name setting in the Local Networking area of the Administrative Web interface), this will also automatically change the local domain name used for email accounts. For example, if you change the name of the server from “myserver” to “centralserver,” local email addresses will change from jsmith@myserver.loc to jsmith@centralserver.loc.

Setting up the Microsoft® Outlook® application

If you have an existing Microsoft® Outlook® client and wish to modify it to work with your Magnia SG30, see [How to modify your existing Outlook® Express client](#) on page 112.

If you have never set up your email, the Microsoft® Outlook® Internet Connection Wizard starts automatically when you run the Outlook® or Outlook® Express applications. The wizard's first screen is similar to that below:



Sample Internet Connection Wizard, Your Name screen

Fill in the name to be used to identify the current configuration. This can be the same as your user account name.

Local email

On the Internet E-mail Address screen, enter `username@myserver.loc` where *username* is the name of your user account on the Magnia SG30.

User information

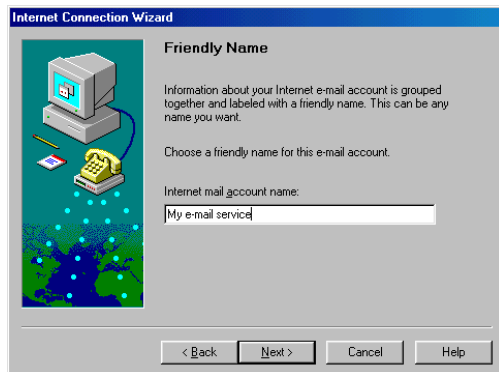
In the Mail Logon screen, enter your user name and password as created on the Magnia SG30. This is all you need to send and receive email.



Sample Internet Mail Logon screen

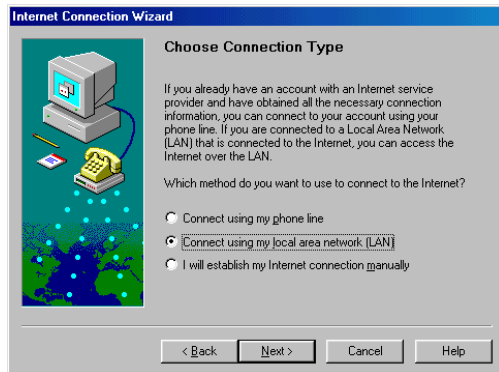
Completing the setup

On the following screen, enter a name which identifies the configuration, then click **Next**. This name can be anything you like.



Sample Friendly Name screen

On the following screen, select **Connect using my local area network (LAN)**.



Sample Choose Connection Type screen

How to modify your existing Outlook[®] Express client

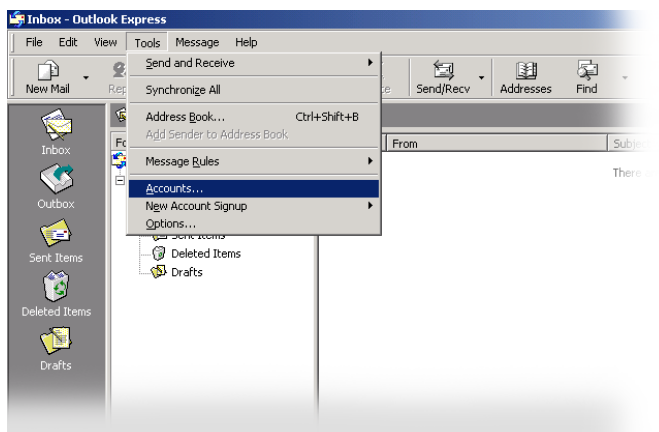
Follow these instructions if your Microsoft[®] Outlook[®] Express client was set up before you installed the Magnia SG30.

NOTE

If you plan to continue accessing your existing Internet email provider (ISP or hosted domain) directly, you don't need to change your Outlook[®] Express configuration.

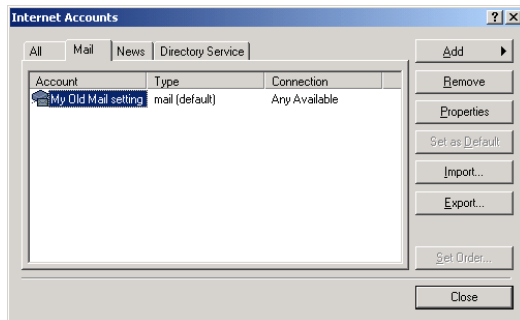
If your Outlook[®] Express Client has been setup to work directly with your ISP, you can take the following simple steps to redirect the client to use the Magnia SG30 email server.

- 1 Start Outlook[®] Express.
- 2 From the **Tools** menu, select **Account**.



Sample Outlook Express screen; selecting Accounts from the Tools menu

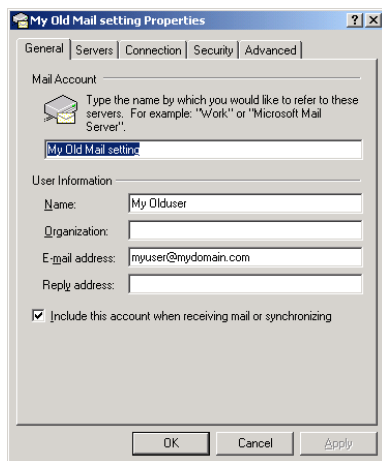
- 3 In the next window, select the **Mail** tab, and click **Properties**.



Sample Outlook Internet Accounts screen

The email setting property window appears.

- 4 Click **Properties** to modify your email settings.
- ❖ The My Old Mail setting field is for your information. Here you can enter anything you wish.



Sample Outlook My Old Mail setting Properties screen

- ❖ In the Name field, enter the name you want to appear on the Recipients mailbox. This may be any name you wish.
- ❖ The Organization field is optional.
- ❖ In the E-mail address field, enter your ISP email address.

If you are using local email only, enter your local email address (account name).

- 5 Click the **Servers** tab.

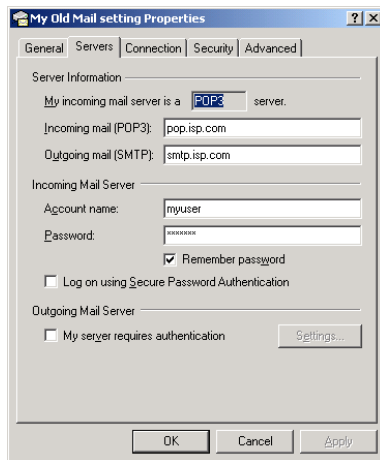
- 6 In the Server window:

- ❖ Change the Incoming mail (POP3) and Outgoing mail (SMTP) fields to mail.

- ❖ Change Account Name and Password to the values created on your Magnia SG30.

NOTE

If the domain name of your Magnia SG30 is changed, your email setting must also be changed to use the new domain name.



Sample Outlook My Old Mail setting Properties screen

- 7 Click **Apply** and **OK**.

Setting up the Magnia SG30 for Internet email

When you establish your own domain on the Internet you can have mail rerouted to that domain. Your server can then download the email from your domain. Many domain-hosting services also allow you to send email out to the Internet through your domain.

Domain hosted email (email mirroring)

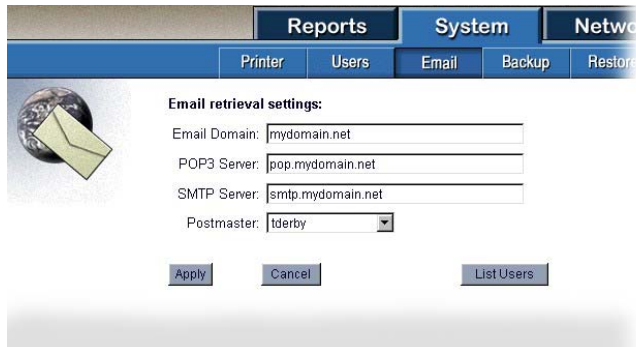
To configure your system to mirror the contents of your domain hosted email:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Click the **System** tab, and select the **Email** menu item.

- 3 Select the **E-mail** option for the email retrieval service, and click the **Configure** hyperlink.

The email configuration screen appears.

The image shows a web-based configuration interface for email settings. At the top, there are tabs for 'Reports', 'System', and 'Network'. Below these, there are sub-tabs for 'Printer', 'Users', 'Email', 'Backup', and 'Restore'. The 'Email' sub-tab is selected. On the left, there is a graphic of a globe with an envelope. The main area is titled 'Email retrieval settings:' and contains four input fields: 'Email Domain:' with the value 'mydomain.net', 'POP3 Server:' with the value 'pop.mydomain.net', 'SMTP Server:' with the value 'smtp.mydomain.net', and 'Postmaster:' with a dropdown menu showing 'tderby'. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'List Users'.

Sample Email retrieval settings screen

- 4 Enter the domain name, POP3 server name, SMTP server name and postmaster account.
 - ❖ E-mail Domain—The domain name which you have established and which is used to host your Internet email.
 - ❖ POP3 Server—The address of the server from which the Magnia SG30 will download incoming email. The ISP hosting your domain should provide this address.
 - ❖ SMTP Server—The address of the server to which the Magnia SG30 will send your outgoing Internet email. The ISP hosting your domain should provide this address.

Enabling Internet email for users

Once you have configured the Magnia SG30's email server to send and receive Internet mail through your domain, you must configure each user account to access their corresponding account on your domain.

Each user account is automatically created with local email configured.

To enable Internet email:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab.
- 3 Select the **Email** menu option.
- 4 Click **List Users**.

- 5 To enable Internet email access, type in the email account name and password for the user.

This account is the email account established on your domain, and may not correspond exactly to the account for the user on your Magnia SG30. For example, the Magnia SG30 might have an account `jsmith` that will use the ISP domain email account of `jsmith7`.

- 6 Click **Apply** to save the updated information.

Summary of email user accounts

To see a summary of the accounts on the Magnia SG30 and how they are mapped to ISP/domain hosted Internet accounts:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab.
- 3 Select the **Email** menu option.
- 4 Click **List Users**.

The Internet user account summary will appear.

Magna SG30 account names are shown on the left, and the corresponding email address is shown on the right.

If no Internet domain email account is entered for a local server user account, that account will be limited to local email.

Sending email through an ISP

The configuration described above enables the Magnia SG30 email server to both send and receive email from your own domain.

Some domain hosting services only support retrieving mail (POP3), but do not support relaying email out to the Internet (SMTP). In this case, you have two options:

- ❖ Choose not to use the Magnia SG30 for email mirroring – configure your client computers to interact with the domain host's email server directly.
- ❖ Use the Magnia SG30 email server for incoming email mirroring only. Send outgoing mail through your ISP servers.

If you choose not to use the Magnia SG30 for email mirroring, configure your client computers to access email as directed by your ISP.

To use the Magnia SG30's email server to mirror the incoming email from your domain, but send mail through your ISP, simply change the SMTP server specified in the Magnia SG30 email configuration to your ISP's SMTP email server. This will allow mail for users local to the Magnia SG30 to stay local (it won't go to the Internet and back), but will still send email destined for remote users through your ISP and on to the final user.

By going to the email section of the System tab, you can type in the address of your ISP's SMTP server. Outgoing Internet email will then be routed through your ISP.

Client email setup

Once you have set up the Internet email address, the network users need to have their Web browsers configured to read email from that location. For a presentation of these procedures and the creation of a user name and password to complete the users setup [See "Client email setup and use" on page 243.](#)

Advanced topics

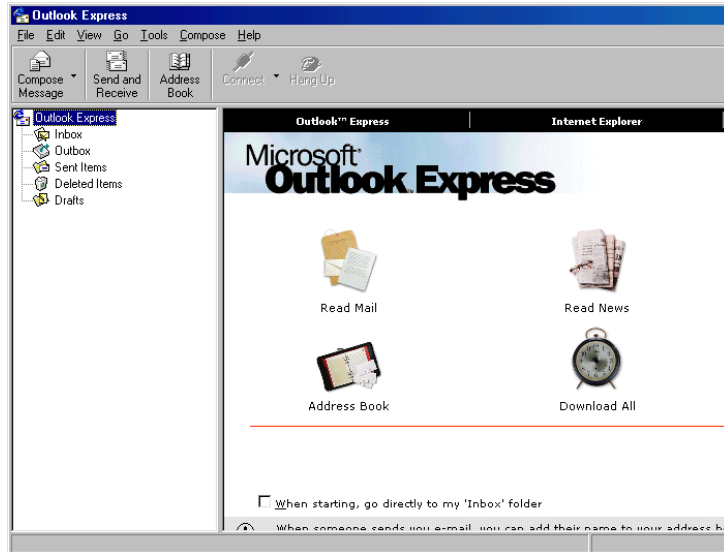
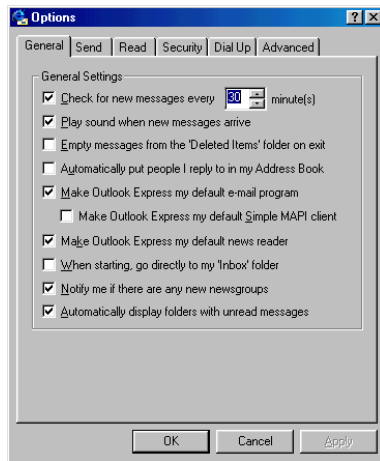
This section contains additional topics dealing with email delivery and hosting.

Setting up automated email retrieval

NOTE

If you have a broadband connection to your ISP, such as cable or DSL, skip this section.

If you are using the modem in the Magnia SG30 to provide a phone-based connection to your ISP, the email clients in your network can initiate a dial-up connection every time they ask for new email. To minimize the number of dial-ups, you can specify a time interval between checks for new email.

1 Start Outlook® Express.*Sample Outlook Express window - set up automated email***2** From the **Tools** menu, select **Options**.**3** Select the **General** tab.*Sample Options screen, General tab***4** Select **Check for new messages every Minutes**.

Because you can always refresh your list of email by selecting **Send/Receive**, Toshiba recommends that you increase the interval at which the clients check for mail to at least 60 minutes.

Direct email delivery

The Magnia SG30 is capable of delivering email directly to the target user. The configurations described earlier in this chapter all have the Magnia SG30 direct mail to another server (either the domain host's email server or the ISP's email server) for relaying to the final recipient.

If you leave the SMTP server field blank, as shown in the example below, the Magnia SG30 will attempt to deliver Internet email directly to the target user's server, bypassing ISP and other servers.

While this technique can be used in some cases to bypass intermediate servers, some ISPs block SMTP delivery to any server but their own. If you attempt to use this configuration and have difficulties, contact your ISP to see if it allows SMTP traffic to other email servers.

Domain hosts and SMTP

Many domain-hosting services require some form of authentication before they will accept SMTP connections. Three common methods are:

- ❖ Access through an ISP— if your domain is hosted by your ISP, you are authorized to access the domain's SMTP servers by accessing them through your ISP.
- ❖ SMTP access following POP3— some domain hosting services will relay messages sent to the domain's servers for a few minutes following a successful POP3 log in.

In this case, you may need to do a Receive or Send/Receive from your email client to trigger the POP3 log in before you can send mail out.

- ❖ SMTP authentication— some domain hosting services allow you to log in to their SMTP services using SMTP-based authentication. The Magnia SG30 does *not* support this form of SMTP access authentication.

When Internet email is checked

If the Magnia SG30 is set up for Internet email, it contacts the domain or ISP for incoming email whenever any user sends or receives email.

Whenever any client checks incoming email, this will trigger a connection with the domain email site or ISP email servers to download all emails pending for any user on the system. Likewise, sending an email will trigger a check for incoming email for all accounts.

All emails are sent to the Internet as soon as the Magnia SG30 receives them. If Internet access is provided through a dial-up connection, sending any email, or checking for email will initiate a dial-out session.

Chapter 5

VPN Configuration

This chapter contains an introduction to the Virtual Private Network (VPN), how to use the VPN, and how the VPN interacts with Magnia SG30 features.

The Magnia SG30 provides three types of VPNs.

- ❖ The PPTP VPN is designed to support roaming or distant client computers connected to the Magnia SG30 through the Internet.
- ❖ The IPSec server to server VPN is designed to connect two SG30s at different locations together across the Internet.
- ❖ The IPSec client to server VPN is designed to connect a client to the Magnia SG30; this can provide added local wireless security, or a connection for roaming and distant client computers connected to the Magnia SG30 through the Internet.

NOTE

If you are setting up the Magnia SG30 in a corporate LAN environment, and want to use VPN services, check with your network administrator for necessary setup and configuration information.

VPN enables you to create a secure connection through the Internet to the private network created by the Magnia SG30 Server. The VPN offers access to Magnia SG30 features when you:

- ❖ Work at home. VPN enables you to use your home Internet connection to access the company server files, print, email, client shares, and other Magnia SG30 features.
- ❖ Are on the road. You can access your company's local network and server.
- ❖ Are a remote user. Workers in remote locations can access information and programs on your company's local network.
- ❖ Have two or more offices you want to connect in a secure manner.

When a client computer is connected to the Magnia SG30 using VPN, the client is capable of accessing virtually all of the same features as a computer that is connected directly to the LAN. The following actions are available for all clients using VPN:

- ❖ File sharing - access personal and shared directories

- ❖ Printing - print to the shared printer
- ❖ Email - retrieve and send email messages
- ❖ Intranet - access the built-in Intranet Web site and shared areas on local client computers
- ❖ System administration - the system administrator can access the Administration Web site and manage the network from a remote site.

Introduction

The VPN software on the Toshiba Magnia SG30 enables you to access your local area network (LAN) through the Internet. This means that in addition to the dial-in capabilities of the Magnia SG30, network access is available any place a client computer has an Internet connection.

While the VPN connections utilize Internet access, they are designed to be secure. The client connection VPN software uses Point-to-point Tunneling Protocol (PPTP) and Remote Access Server (RAS) protocols, or the IPsec protocol. The server-to-server connection uses IPsec (IP Security). These are standard Windows-based security features that enable information transmitted using the VPN to remain secure.

- ❖ Communications over the VPN connection are encrypted and validated to prevent unauthorized access or tampering with data.
- ❖ PPTP is available and easily configurable on all Windows operating systems, including Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, and Windows XP. Macintosh operating systems are not supported at this time.
- ❖ The VPN is compatible with the firewall application. Your firewall remains active while VPN is enabled, keeping your server and LAN safe.

The VPN is engineered for reliability, ease-of-use, and total compatibility with the Magnia SG30. Through tight interface and networking integration, the VPN provides easy access to all of the features of the Magnia SG30 server, as well as access to all systems on the local network. Since the VPN connection enables access inside the firewall, remote users appear to be connected to the server's LAN as if they were locally connected.

Because remote users can fully access the system using VPN, the firewall is active to maintain your local network security.



Using your Magnia SG30's PPTP VPN to connect remotely to your local network

⚠ WARNING

In order to connect to the VPN, client systems must be running a Windows operating system.

Interactions with Other Magnia SG30 Server Features

There are limitations and conditions for certain Magnia SG30 server features when using the following:

- ❖ Modem connections
- ❖ Firewall
- ❖ Backup/Restore
- ❖ Account Management

Modem Connections

VPN is a feature designed for use with broadband Internet connections. As a result, it is incompatible with configurations where the Magnia SG30 uses a dial-out ISP connection. If you attempt to enable VPN on a Magnia SG30 configured to use a modem-based dial-out ISP, you will receive a message indicating that the VPN cannot be enabled with the current Internet connection. If you enable the VPN with a broadband Internet connection, and then decide to change the Magnia SG30 Internet configuration to use a dial-out ISP connection, the VPN will be disabled.

Firewall

The VPN feature does not require any manual changes to your firewall. When you use the VPN, your firewall remains enabled, protecting your local network and server. Enabling the VPN opens a communication port in the firewall that is used only by the VPN software. This opening is secure because the VPN software is the only system software that responds to activity transmitted through this port. The port is automatically closed when the VPN is disabled.

Backup/Restore

The backup and restore features are fully operational when using the VPN. You can access these features, modify schedules, and start manual backups from a client accessing the server through a VPN connection. However, the Magnia SG30 cannot see shared drives on a client computer accessing the network through the VPN. This prevents backups from being configured on shared drives which are located on a client computer accessing the server through the VPN.

Account Management

When connecting to the Magnia SG30 using the VPN feature, it is possible to gain access to the Magnia SG30 local network using one account while retaining access rights based on another account. This happens when a user attempts to log on to the VPN using a different account than used when normally logging on to Windows. To avoid this confusion, always connect to the VPN using the same Windows account.

Remote client access to the VPN through the Internet

Configuring the PPTP VPN Software

Setting Up VPN

Your Magnia SG30 already has the VPN software installed. However, before it can be used, you must configure it. During configuration, user accounts must be given access to the VPN. Then, a client setup diskette must be created to use when setting up VPN access on client computers.

Enabling the VPN Feature

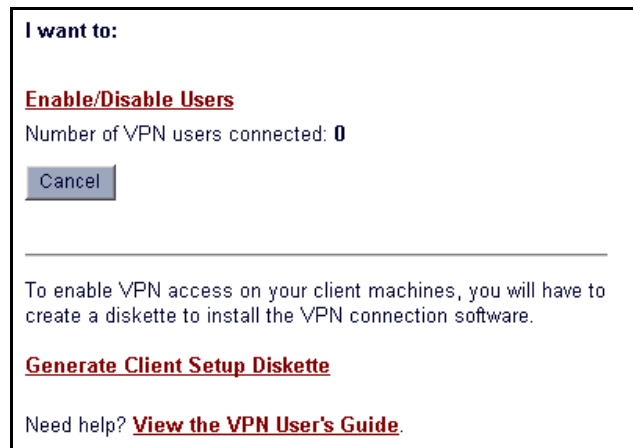
- 1 Go to the Administrative Web site.
- 2 Select the **Network** tab and click on the **VPN** menu item.

- 3 Check the **PPTP VPN Access** check box and click **Apply** to turn on the VPN feature.



Sample Network tab screen

- 4 Click the **Configure** hyperlink to configure the VPN service.
- 5 Click on the **Enable/Disable Users** hyperlink to enable specific users accounts to access this feature.



Sample Administrative Web site VPN screen



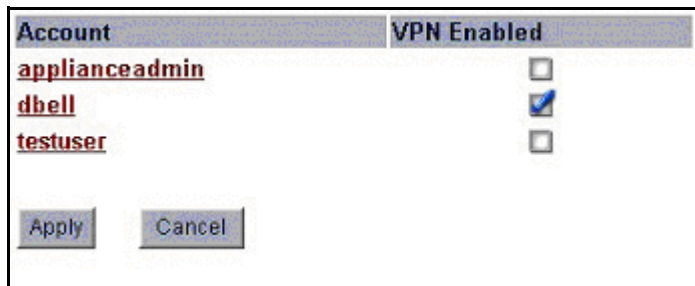
TECHNICAL NOTE: VPN access can be enabled or disabled by the system administrator at any time without losing other VPN configuration settings.

User Access

Users do not automatically have access to VPN. Each user must be given permission. To enable VPN access for individual users follow these steps:

- 1 Go to the Administrative Web site.

- 2 Open the main VPN page and select the **Enable/Disable Users** hyperlink.



Account	VPN Enabled
applianceadmin	<input type="checkbox"/>
dbell	<input checked="" type="checkbox"/>
testuser	<input type="checkbox"/>

Apply Cancel

Sample Administrative Web site VPN screen

- 3 On the displayed screen, check the boxes next to the users to which you are granting VPN access. You may change these settings at any time.
- 4 Click **Apply**.

The screen used to generate a client setup diskette displays.

Configuring a Client Computer

External computers that connect to the Magnia SG30 server through the VPN are called "client" computers. Each client computer must be configured to connect with the server.

In all Microsoft® Windows operating systems, Virtual Private Networking is implemented as a feature of Dial-Up Networking. In order to configure your computer for VPN, Dial-Up Networking must be installed on your computer even if you have no intention of using the modem to dial an ISP.

In addition to Dial-Up Networking, you must have at least one working network adapter installed. This adapter can be a Dial-Up, Ethernet, or any networking adapter that has a connection to the Internet. It is not required that your client computer be connected to the Internet for configuration. It is however, required that your client computer be connected to the Internet to actually use VPN.



TECHNICAL NOTE: The process of setting up a client for VPN takes approximately 5 minutes, and includes one restart of your computer.

Configuration Requirements

To communicate via VPN with a Microsoft Windows client over the Internet, your Magnia SG30 must have:

- ❖ Enabled VPN support
- ❖ At least one user account with VPN enabled for the client to use when connecting

- ❖ A static public IP address.

⚠ WARNING

If your server's IP address or workgroup changes, the program used to create a Client Setup Diskette must be downloaded again so it contains the correct IP address. If you are using a client setup diskette that was configured on a Magnia SG30 using a DHCP IP address, a warning message will display during setup. At that point, you can select to reconfigure your server or continue with configuration.

To communicate via VPN with a Microsoft Windows client over the Internet, the client computer must be:

- ❖ Running Windows 95/98/Me/NT/2000/XP operating system (Macintosh operating systems are not supported at this time)
- ❖ Connected to the Internet via a broadband or dial-up connection
- ❖ A computer that is not directly connected to the Magnia SG30 server.



TECHNICAL NOTE: Installing on a client system running Window 95 may require you install the Dial Up Networking 1.3 Performance and Security Update. To verify whether this upgrade is needed, see [Verifying that the upgrade is needed](#) on page 132.

Generating a Client Setup Diskette

Once your Magnia SG30 is set up to accept VPN connections from specified users, you need to configure the client computers, such as laptops or remote desktops, to access the server. The client configuration program must be downloaded from the Magnia SG30 to a diskette.

To create a VPN Setup Diskette:

- 1 Go to the Administrative Web site.

- 2 Open the main VPN page and select the **Generate Client Setup Diskette** hyperlink.

A page describing the client setup procedure displays.



Sample VPN Diskette Image Download screen

- 3 Follow the instruction on the page to create a diskette.



TECHNICAL NOTE: Additional Client Setup Diskettes can be created later. See [Generating Additional Client Setup Diskettes](#) on page 128 for more information.

Generating Additional Client Setup Diskettes

Clients, such as laptops or remote desktops, must be configured to have access to the server using VPN. If you want to make additional Client Setup Diskettes:

- 1 Go to the Magnia SG30 Administration Web site.
- 2 Select the Network tab, then click **VPN**.
- 3 Click the **VPN Administration** option.
- 4 Click **Generate Client Setup Diskette**.

To enable VPN access on your client machines, you will have to create a diskette to install the VPN connection software.

Generate Client Setup Diskette

Sample Generate Client Setup Diskette screen

5 Click **Generate Client Setup Diskette**.

You will be asked where to place the downloaded program. Select any location.



TECHNICAL NOTE: The downloaded program is most commonly placed on a diskette so that it may be used directly on a client. The downloaded program may be placed on your hard drive for later use or it can be emailed as an attachment.



A downloaded program used to configure a client computer will contain the server's current IP address. If your server's IP address changes, or the server uses DHCP, the program used to create a Client Setup Diskette must be downloaded again so it contains the correct IP address. Any clients previously configured must be reconfigured with the new IP address.

Running the Client Configuration Diskette

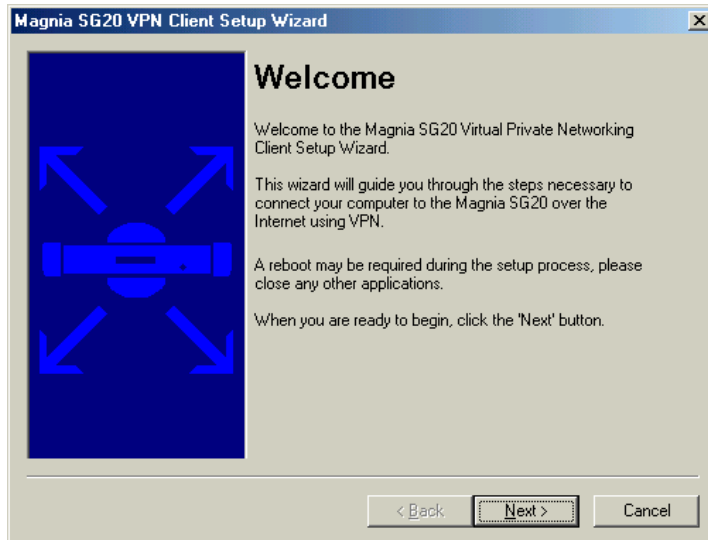


TECHNICAL NOTE: The VPN Client Setup Wizard is designed to properly configure your client systems, and should be used under normal circumstances. If this is not possible, instructions on how to manually setup a client system are provided at the end of this chapter. Please refer to the section which corresponds to your operating system.

1 Insert the client configuration diskette into the client computer.

- 2 Double-click the setup executable called **SG30VPNSetup.exe** (this is the program downloaded when **Generate VPN Disk** was selected).

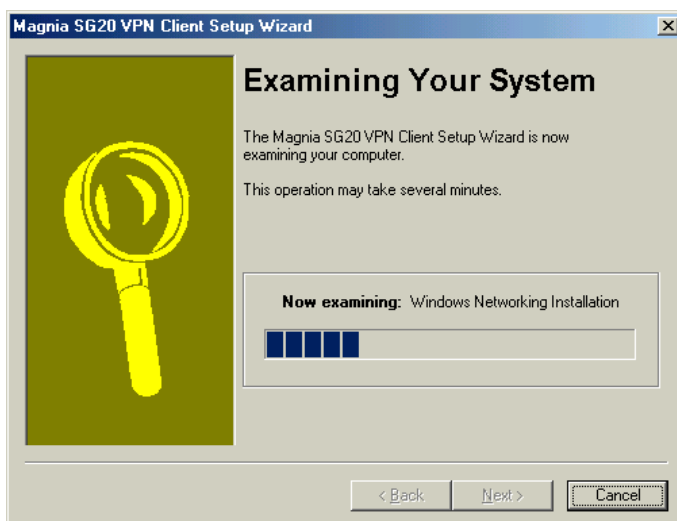
The VPN Client Setup Wizard opens.



Sample VPN client Setup Wizard Welcome screen

- 3 Click **Next** to begin.

The setup wizard examines your system for the proper settings and Internet connection.



Sample Examining Your System screen

When your settings are verified, the VPN Client Setup program installs and configures PPTP and RAS.

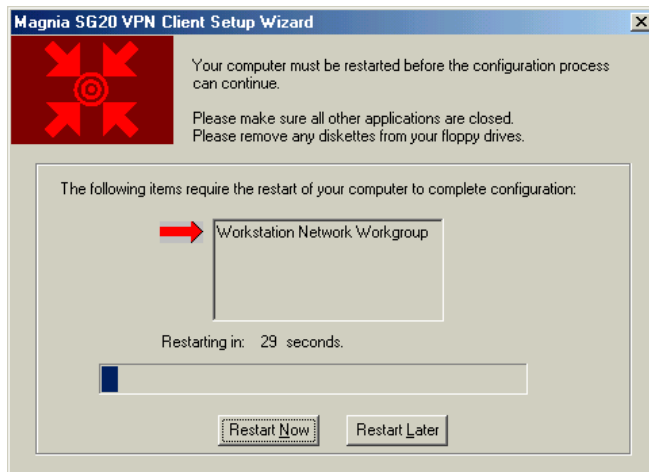


TECHNICAL NOTE: If you are running a client configuration diskette on a Windows NT system, additional dialog boxes not shown in this section may appear. These dialog boxes are not part of the VPN setup process. You will be unable to select them with your mouse. You can close the extra dialog boxes by simply pressing the Enter key.



TECHNICAL NOTE: TVPN setup may request that you insert your Windows CD so that PPTP and RAS can be installed and configured. See [Introduction](#) on page 122 for information about these technologies.

After PPTP and RAS configuration are complete, the wizard will prompt you to restart the computer.



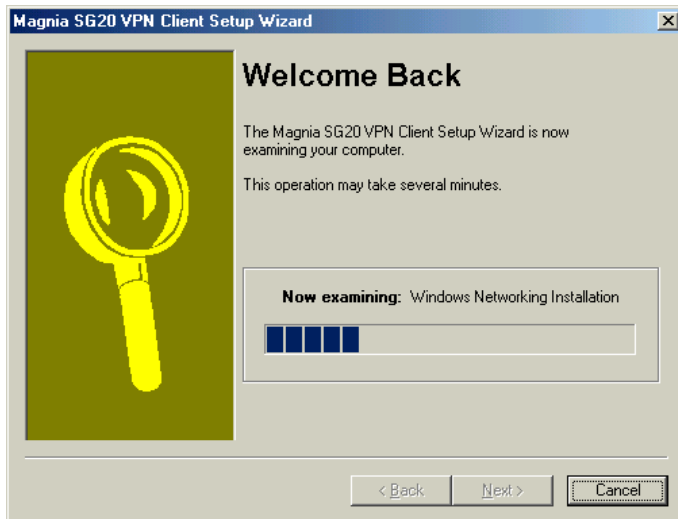
Sample Computer Restart screen

- 4 Remove the diskette before restarting.
- 5 Click **Restart Now** to restart the computer. If no selection is made, the computer will restart automatically.



TECHNICAL NOTE: If Restart Later is selected, the VPN setup will not be complete and the VPN setup wizard will resume after your next restart.

After restarting, the VPN setup program runs again to complete the final configuration.



Sample Welcome Back screen

When configuration is complete, the client computer is ready to use the VPN.

Manually Configuring a Client running Windows 95/98/Me

Windows 95 VPN Support Download

Windows 95 did not originally ship with an option for VPN support. The Dial-Up Networking 1.3 upgrade is available from the Microsoft Internet site.

WARNING

When connecting to a VPN server over a dial-up ISP connection the following error message may be displayed:

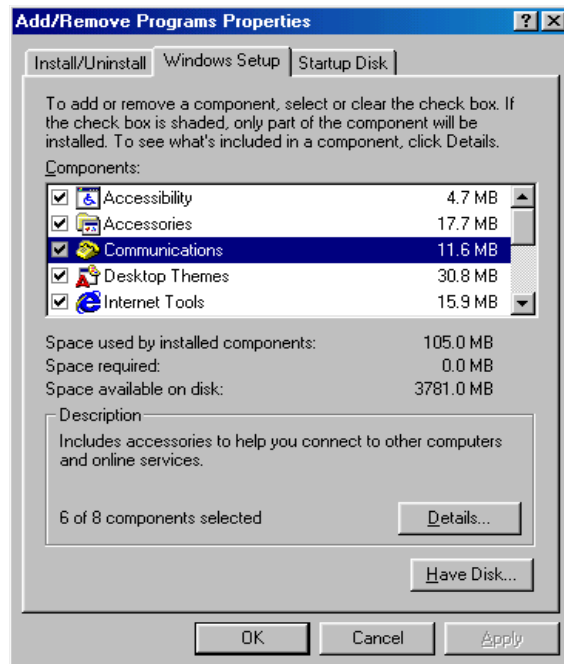
error 645: The Microsoft Dial-Up adapter is in use or not responding properly, disconnect other connections and try again.

This error is caused by a bug in Windows which may corrupt the Windows registry when a VPN adapter is configured manually. It may be resolved quickly by removing the VPN adapter from the client computer and running the Magnia SG30 VPN Client Setup program.

Verifying that the upgrade is needed

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.

- 3 Double-click the **Add/Remove** icon.
The Add/Remove Programs dialog box displays.
- 4 Click the tab labeled **Windows Setup**.
- 5 Select **Communications** from the list labeled **Components**.



Sample Add/Remove Programs dialog box, Windows Setup tab

- 6 Scroll to the bottom of the Components list and find the component named **Virtual Private Networking**. If this item exists, the Dial-Up Networking 1.3 upgrade has already been installed on your computer. Skip the next section and proceed to Installing the VPN adapter. If the item is not in the list, following the steps in the next section to install the upgrade.

Installing Dial-Up Networking Version 1.3

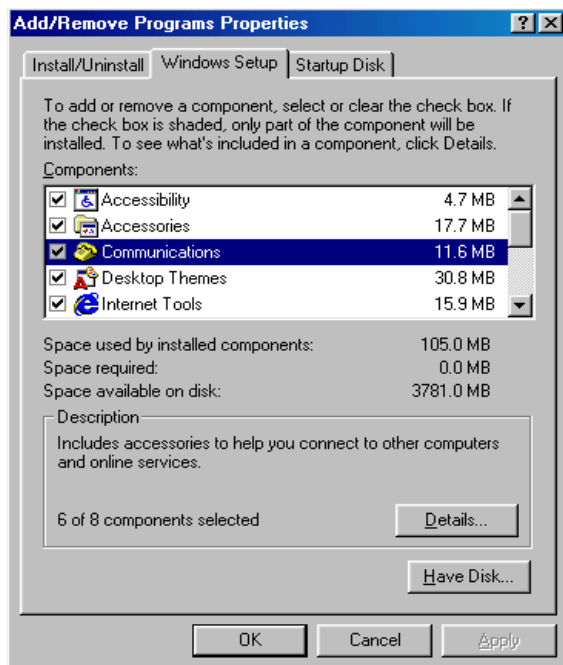
- 1 Download the file MSDUN13.EXE from the Microsoft Internet Web site.
- 2 Run the program MSDUN13.EXE following all instructions and prompts.
- 3 Restart your computer and proceed to the next section.

Installing the VPN adapter

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 Double-click the **Add/Remove Programs** icon.

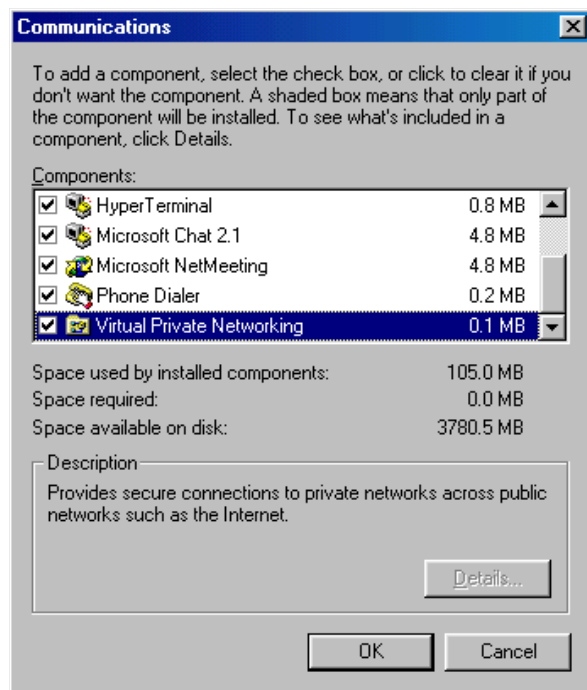
The Add/Remove Programs dialog box displays.

- 4 Click the tab labeled **Windows Setup**.
- 5 Select **Communications** from the list labeled **Components**.



Sample Add/Remove Programs dialog box, Windows Setup tab

- 6 Click the **Details...** button to display the Communications dialog box.



Sample Communications dialog box

- 7 Select the component named **Virtual Private Networking** by clicking on the check box.
- 8 At this time you may be prompted for your Windows Setup Disk to provide some of the drivers needed for Virtual Private Networking. If so, insert the Windows Setup Disk and follow any instructions and prompts to install the drivers.

Configuring Network Settings

Once you have properly installed the VPN adapter, the only remaining network setting that is required for your client computer to communicate with the Magnia SG30 using VPN is the workgroup name.

WARNING

Once you complete the setup of your network settings, you will be required to restart your computer. Be sure to exit all other applications before proceeding.

To configure your network settings:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 Double-click the **Network** icon.
The Network Properties dialog box displays.
- 4 Click the **Identification** tab.
- 5 Verify that the computer name displayed is unique for your network. If it is not a unique name, change it to one that will not be used by any other computer.
- 6 In the field named **Workgroup**, type in the word **SAWORKGROUP** in all upper case letters to completely replace any text that was there before.

WARNING

If you or your Network Administrator has changed the workgroup on the Magnia SG30 from the default “SAWORKGROUP”, you will need to type the new workgroup name.

- 7 Click **OK** to complete the setup.

Windows will now require you to restart your computer.

Dial-Up Networking Phone Book Entry

The Microsoft Windows implementation of Virtual Private Networking is tied to the Dial-Up Networking feature of the operating system. You must configure a phone book entry to connect to your Magnia SG30 via VPN.

To create a phone book entry for the Magnia SG30 VPN.

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Programs>Accessories>Communications>Dial-Up Networking**.



TECHNICAL NOTE: If Dial-Up Networking is not in the menu, try opening My Computer. Open the folder named Windows Control Panel and double-click the Dial-Up Networking icon.

The Dial-Up Networking window displays.

- 3 Double-click the **Make New Connection** icon.

The Make New Connection Wizard is displayed.

- 4 Type in a name to identify the VPN Phone Book Entry in the text box labeled **Type in a name for the computer you are dialing**.
- 5 Select the device labeled **Microsoft VPN Adapter** from the **Select a device** drop-down list.
- 6 Click the **Next** button.

The Wizard now needs the public IP Address of your Magnia SG30. The public IP address may be viewed on the LCD of your Magnia SG30 by clicking the scroll button next to the LCD display. The public IP Address is labeled **Public Address**.

- 7 Type the public IP Address of your Magnia SG30 in the field labeled **Host name or IP Address**.
- 8 Click the **Next** button.

The Wizard displays an information only page which allows you to cancel the process or complete the creation of the phone book entry.

- 9 Click the **Finish** button to complete the creation of the phone book entry.



HINT: The icon for your newly created phone book entry can be dragged to the desktop of your computer as a quick and convenient shortcut.

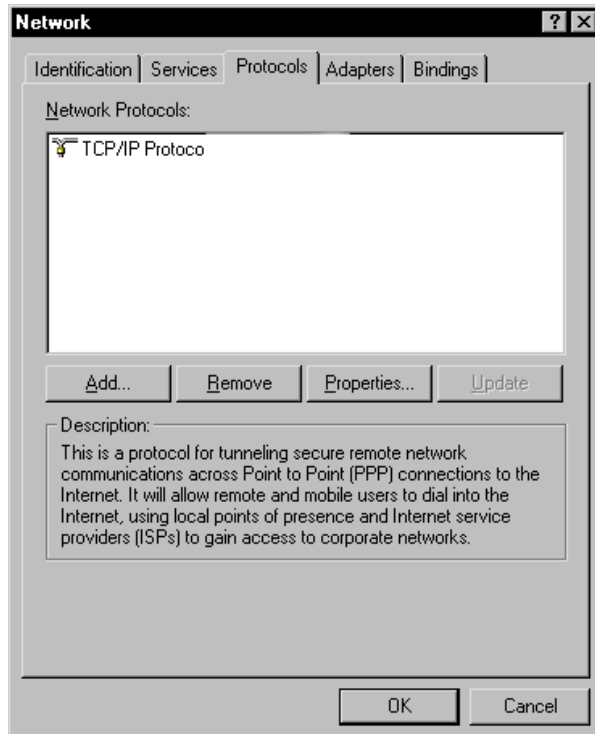
Manually Configuring a Client running Windows NT

Virtual Private Networking Adapter

When connecting a client computer running Windows NT to the Magnia SG30, you must first install the Virtual Private Networking Adapter. During this installation, you will be required to use your Windows operating system setup disk.

To install your VPN Adapter:

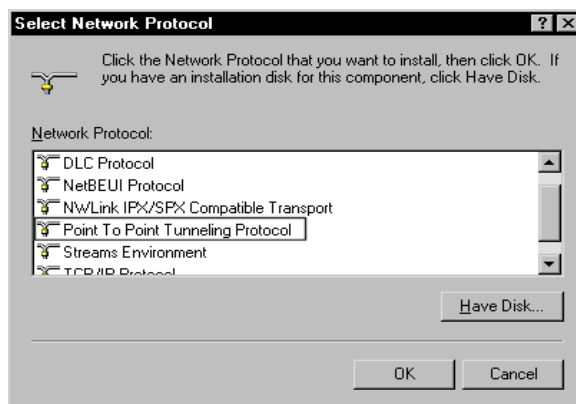
- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 Double-click the **Networking** icon.
The Networking dialog box displays.
- 4 Click on the tab labeled **Protocols**.



Sample Networking dialog box

- 5 Click the **Add** button.

The Select Network Protocol dialog box displays.



Sample Select Network Protocol dialog box

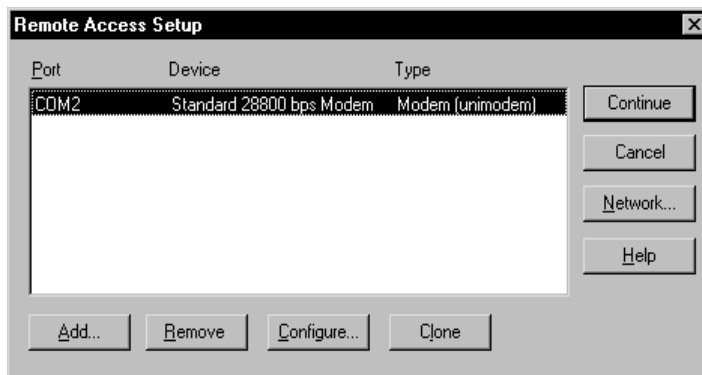
- 6 From the **Network Protocol** list, select the item named **Point To Point Tunneling Protocol**, then click the **OK** button.

A dialog box asking the **Number of Virtual Private Networks** displays.



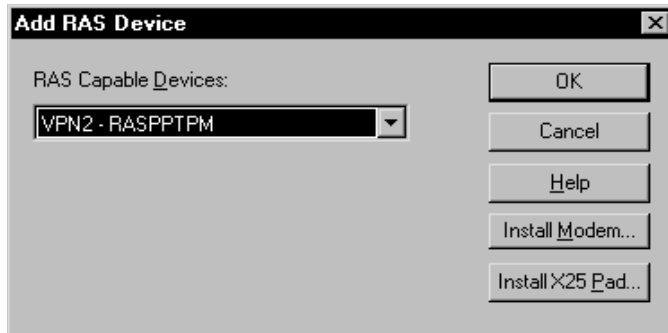
Sample Number of Virtual Private Networks dialog box

- 7 The text box should have the number **1** in it.
- 8 Click the **OK** button and a confirmation dialog box displays.
- 9 Click the **OK** button to display the Remote Access Setup dialog box.



Sample Remote Access Setup dialog box

- 10 Click the **Add** button to display the Add RAS Device dialog box.



Sample Add RAS Device dialog box

- 11 Select the item labeled **VPN-RASPPTPM** in the drop-down list labeled **RAS Capable Devices**, then click the **OK** button.

After configuration is complete, Windows NT will restart.

Configuring Network Settings

Once you have a properly installed the VPN adapter, the only remaining network setting that is required for your client computer to communicate with the Magnia SG30 using VPN is the workgroup name.

WARNING

Once you complete the setup of your network settings, you will be required to restart your computer. Be sure to exit all other applications before proceeding.

To configure your network settings:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 Double-click the **Networking** icon.
- 4 Click the **Identification** tab.
- 5 Verify that the computer name displayed is unique for your network. If it is not a unique name, change it to one that will not be used by any other computer.
- 6 In the field named **Workgroup**, type in the word **SAWORKGROUP** in all upper case letters to completely replace any text that was there before.

WARNING

If you or your Network Administrator has changed the workgroup on the Magnia SG30 from the default “SAWORKGROUP”, you will need to type the new workgroup name.

- 7 Click **OK** to complete the setup.

Windows will now require you to restart your computer. The Network Properties dialog box displays.

Dial-Up Networking Phone Book Entry

The Microsoft Windows implementation of Virtual Private Networking is tied to the Dial-Up Networking feature of the operating system. You must configure a phone book entry to connect to your Magnia SG30 via VPN.

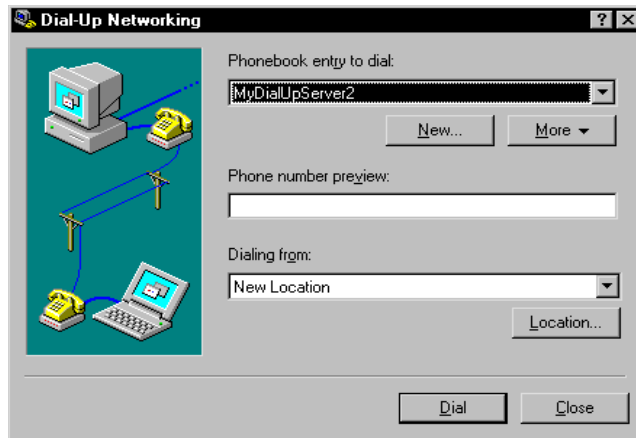
To create a phone book entry for the Magnia SG30 VPN:

- 1 On the Windows Desktop, double-click the **My Computer** icon.

The My Computer window opens.

- 2 Double-click the **Dial-Up Networking** icon.

The Dial-Up Networking dialog box displays.

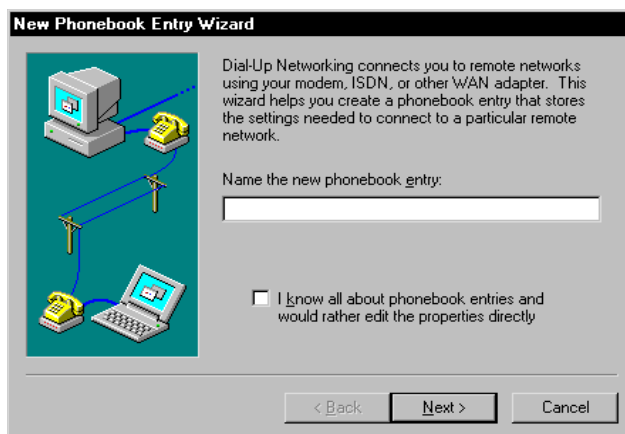


Sample Dial-Up Networking dialog box

- 3 Click the **New** button.

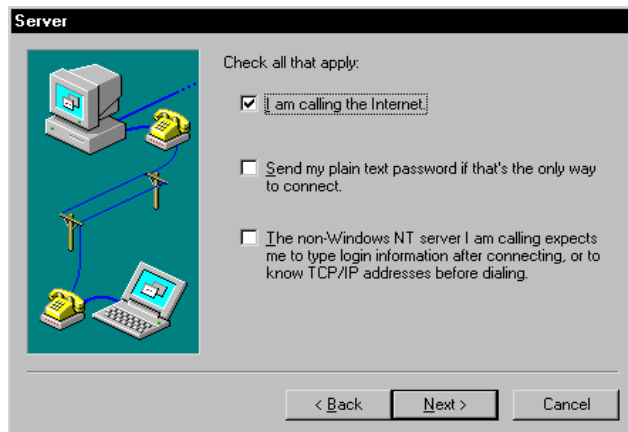
The New Phonebook Entry Wizard displays.

- 4 In the text box labeled **Name the new phonebook entry**, type a name to identify the Magnia SG30 VPN phonebook entry, then click the **Next** button.



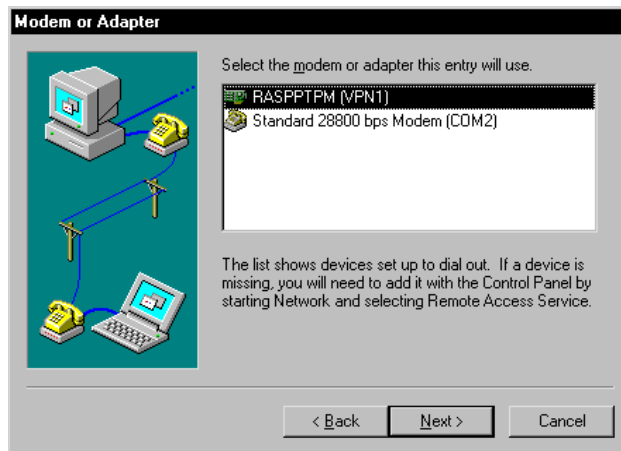
Sample New Phonebook Entry Wizard

- 5 When the Server page displays, check the box labeled **I am calling the Internet**, then click the **Next** button.



Sample Server page

- 6 When the Modem or Adapter page displays, select the list item labeled **RASPPTPM (VPN1)**, then click the **Next** button.



Sample Modem or Adapter page

The Wizard now needs the public IP Address of your Magnia SG30. The public IP address may be viewed on the LCD of your Magnia SG30 by clicking the scroll button next to the LCD display. The public IP Address is labeled **Public Address**.



Sample Phone Number page

- 7 Type the public IP Address of your Magnia SG30 in the field labeled **Phone number**, then click the **Next** button to complete the wizard.

Manually Configuring a Client running Windows 2000

Configuring Network Settings

Once you have a properly installed the VPN adapter, the only remaining network setting that is required for your client computer to communicate with the Magnia SG30 using VPN is the workgroup name.

WARNING

Once you complete the setup of your network settings, you will be required to restart your computer. Be sure to exit all other applications before proceeding.

To configure your network settings:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 Double-click the **Network and Dial-Up Connections** icon.

The Network and Dial-Up Connections dialog box displays.

- 4 Click the **Advanced** menu, then click **Network Identification**.
- 5 Click the button labeled **Properties**.

The Identification Changes dialog box displays.

- 6 In the text box labeled **Workgroup**, type in the word **SAWORKGROUP** in all upper case letters to completely replace any text that was there before.

⚠ WARNING

If you or your Network Administrator has changed the workgroup on the Magnia SG30 from the default "SAWORKGROUP", you will need to type the new workgroup name.

- 7 Click **OK** to close the Identification Changes dialog box.
- 8 Click **OK** to close the System Properties dialog box.

Windows will now require you to restart your computer.

Dial-Up Networking Phone Book Entry

The Microsoft Windows implementation of Virtual Private Networking is tied to the Dial-Up Networking feature of the operating system. You must configure a phone book entry to connect to your Magnia SG30 via VPN.

To create a phone book entry for the Magnia SG30 VPN:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Dial-Up Networking**.

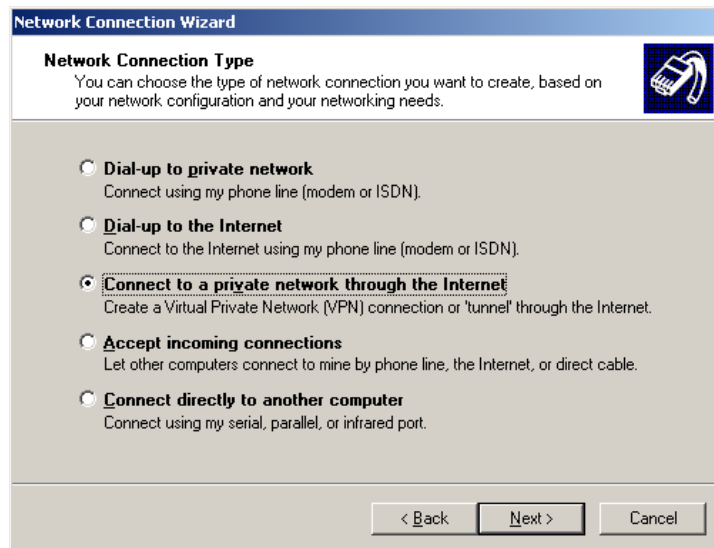
The Dial-Up Networking window displays.

- 3 Double-click the **Make New Connection** icon.
- 4 When the Make New Connection Wizard displays, click the **Next** button to begin.



Sample Network Connection Wizard's Welcome screen

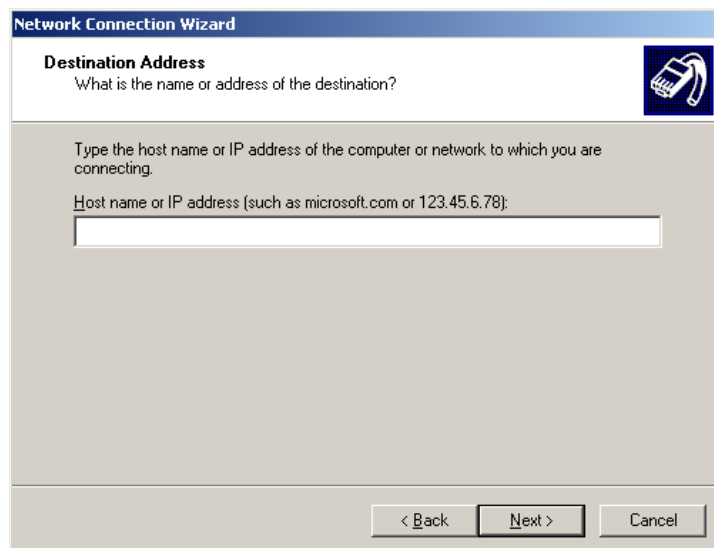
- 5 Identify the connection type as VPN by selecting the **Connect to a private network through the Internet** option, then click the **Next** button.



Sample Network Connection Type screen

The Wizard now needs the public IP Address of your Magnia SG30. The public IP address may be viewed on the LCD of your Magnia SG30 by clicking the scroll button next to the LCD display. The public IP Address is labeled **Public Address**.

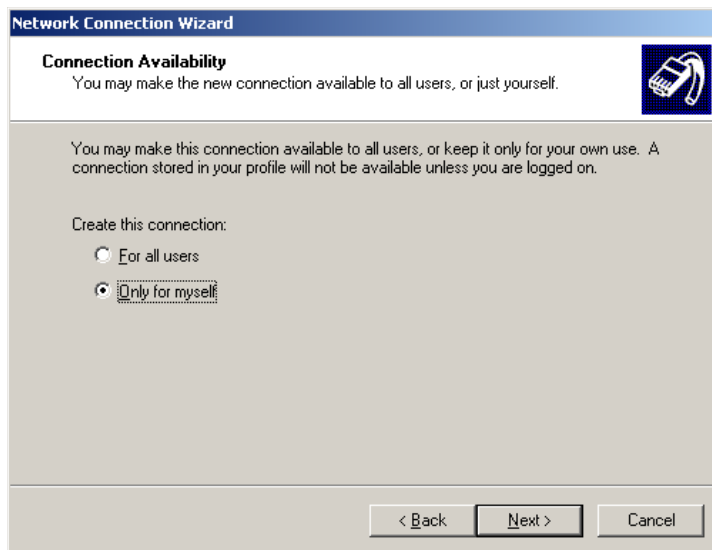
- 6 Type the public IP Address of your Magnia SG30 in the field labeled **Host name or IP address**, then click the **Next** button.



Sample Destination Address screen

Windows 2000 will need to know if you intend this connection to be used by all users or keep it for your own use.

- 7 Select the appropriate choice then click the **Next** button.



Sample Connection Availability screen

- 8 In the text box provided, type a name to identify the VPN Phone Book Entry.



Sample Finish screen

- 9 Click the **Finish** button to complete the creation of the phone book entry.



HINT: The icon for your newly created phone book entry can be dragged to the desktop of your computer as a quick and convenient shortcut.

Manually Configuring a Client running Windows XP Virtual Private Networking Adapter

To configure your network settings:

- 1 Open the Windows Start Menu on the Windows Taskbar.
- 2 Select **Settings>Control Panel** to display the Windows Control Panel.
- 3 If not in the Classic View, select the **Switch to Classic View** from the left frame.
- 4 Double-click **Network Connections**.
- 5 Select **Create a New Connection** from the left frame. If prompted, enter the area code and close the dialog box. The New Connection Wizard appears.
- 6 Click **Next**. The Network Connection Type page appears.
- 7 Select **Connect the network at my workplace**, and click **Next**.
- 8 Enter the IP address for your Magnia SG30 and click **Next**.
- 9 Click **Finish**.

Connecting two VPNs in different locations

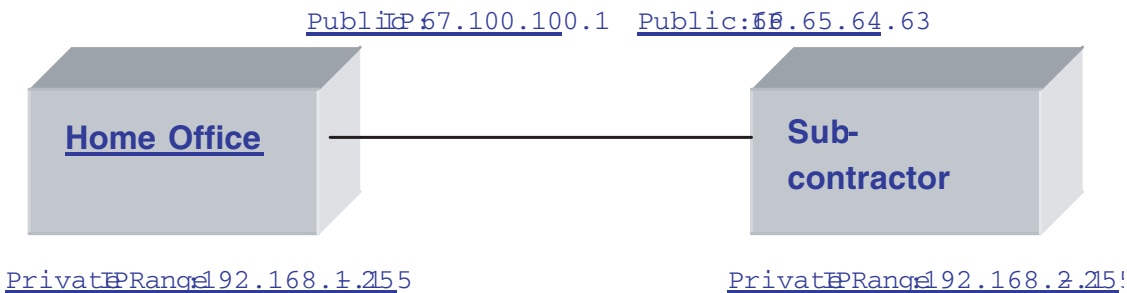
Configuring the IPSec Server to Server VPN Software

If you have two Magnia SG30's in different locations, and you wish to connect them, both need to be configured using the IPSec server to server software configuration. Each server needs to know the IP address information concerning the remote server in order to complete the connection.

Because IPSec is based on establishing a configuration between two predefined IP addresses, both Magnia SG30 Internet connections must be assigned static IPs from your ISP. If you are not sure if this is the case, contact your ISP for more information.

In order to connect two Magnia SG30s using an IPSec VPN connection, the private networks of both systems must have different subnet ranges. The default private address range shipped with the Magnia SG30 starts with 192.168.1.1 through 192.168.1.255. To change the private subnet range, go to the Administrative Web interface, select the Network tab, and click on the Local menu item. Use the Advanced button to change the

private network IP range (for more information, refer to [Advanced Networking Features](#) on page 292).



Enabling the IPsec VPN Feature

The IPsec VPN feature is turned off by default. In order to use this feature, you must first enable it, and then configure at least one connection to another Magnia SG30 with IPsec VPN enabled. Both servers must have the IPsec VPN enabled and configured in order to establish a connection.

- 1 Go to the Administrative Web site.
- 2 Select the **Network** tab, and then click on the **VPN** menu item.
- 3 Check the **IPsec Server to Server VPN Access** check box, and then click **Apply** to turn on the VPN feature.
- 4 Click the **Configure** hyperlink to configure the VPN. This will display the list of existing IPsec configurations you have created. The first time you enter this screen, the list will be empty.
- 5 You can add your first (and subsequent) IPsec connection definitions by clicking the Add button. This will display the IPsec configuration screen.

Local (left) IP Address:	66.100.105.238
Local (left) Next Hop:	66.100.104.1
Local (left) Private Network:	192.168.1.0
Local (left) Private Subnet Mask:	255.255.255.0
Local (left) Firewall:	yes
Connection Name:	<input type="text"/>
Remote (right) IP Address:	<input type="text"/>
Remote (right) Next Hop:	<input type="text"/>
Remote (right) Private Network:	<input type="text"/>
Remote (right) Private Subnet Mask:	<input type="text"/>
Remote (right) Firewall:	yes <input type="button" value="v"/>
Shared Key:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Sample IPSec Configuration screen

The top part of the IPSec configuration screen displays the information describing the local side of the VPN connection. This is read only information; you cannot change the IP information (it is picked up from your local IP address information).

The bottom part of the screen is where you describe the Magnia SG30 to which you will be connecting. Complete the following fields:

- ❖ **Connection Name:** A name of your choosing. This name is used to identify the IPSec connection configuration.
- ❖ **Remote IP Address:** IP address of the public port for the remote Magnia SG30. This can be viewed on the LCD screen or report pages of the web administration, and is labeled “Public IP”.
- ❖ **Remote Private Address:** IP address of the remote Magnia SG30 private network. By default, this is 192.168.1.1, but can be changed in the advanced networking screen of the web administration user interface.
- ❖ **Remote Next Hop:** This is the IP address of the remote ISPs gateway server. This can be obtained from the ISP that provides the Internet connection for the remote server.
- ❖ **Remote Private Subnet Mask:** The subnet mask for the remote Magnia SG30’s private network. By default, this is 255.255.255.0, but can be changed on the Advanced Networking screen.
- ❖ **Remote Firewall:** Defines whether the remote Magnia SG30 has its firewall up. This should normally be left set to “Yes”.
- ❖ **Shared key:** The shared key is a password you choose and enter in both Magnia SG30s. The same key must be entered on each of the Magnia SG30’s IPSec configuration in order to authenticate and authorize the connection.

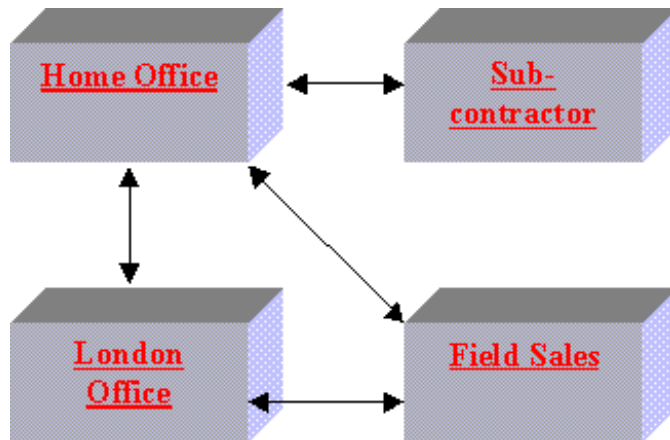
6 When you have finished entering the information, click **Apply** to save your settings.

IPSec VPN Use

Whenever an IPSec configuration is entered, a corresponding IPSec configuration must be entered on the other Magnia SG30. The shared key must be the same on both systems.

You can add additional IPSec connection definitions, by returning to the IPSec VPN screen and clicking the **Add** button. You can create a network of Magnia SG30’s between several remote offices. In the example below, connections can be established between

the Home Office, Sales Office, the London Office, but a remote sub-contractor can only contact the Home Office Magnia SG30.



Sample IPsec VPN Usage screen

While the shared key for a specific connection must be the same on each of the systems that are on either end of the VPN connection, different keys can be used for connections for different machines. In the example above, the Home Office shared key for a connection to Field Sales must be the same as the key entered on the Field Sales connection for the Home Office. However, the Home Office shared key to the Subcontractor may be a completely different key.

When multiple IPsec VPN configurations are entered, they are all active and multiple connections can be made simultaneously. In the example above, this means that client computers connected to the Home Office Magnia SG30 local network would be able to access the local networks of the Subcontractor, Field Sales and London Office servers.

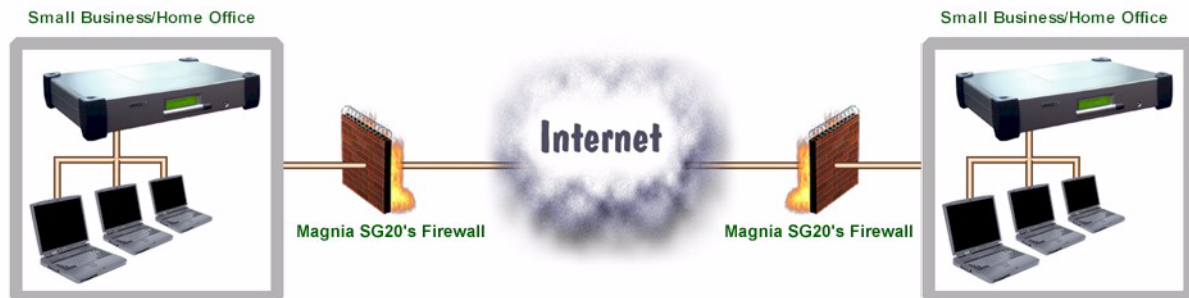
IPsec VPN connections are made automatically. Once defined, these connections will service any requests for access to computers on a remote network. It will appear much as if the remote Magnia SG30 and its clients are part of the local network.

IPsec VPN connections are made as soon as the system boots, and remain connected until the system is shut down (or the configuration is manually disabled).

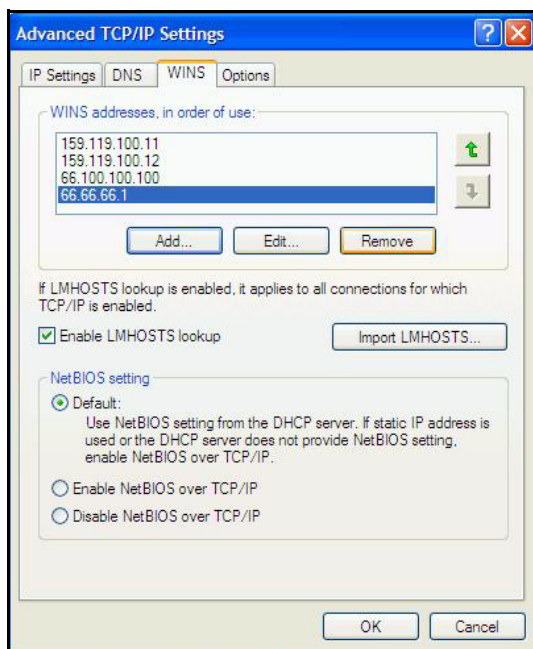
Client Configuration

Once the VPN connection is established between the two Magnia SG30s, any client on one Magnia SG30 private network can gain access to the other server's private network. However, in order to browse another private network, or use computer names to reference the other server or clients, a client computer must be configured to include the

other server's IP address as a WINS server. This allows the client to use both the WINS services of both the local server and the services of the remote server.



Client WINS settings are made on the WINS Configuration tab of the TCP/IP Properties window for network configuration.

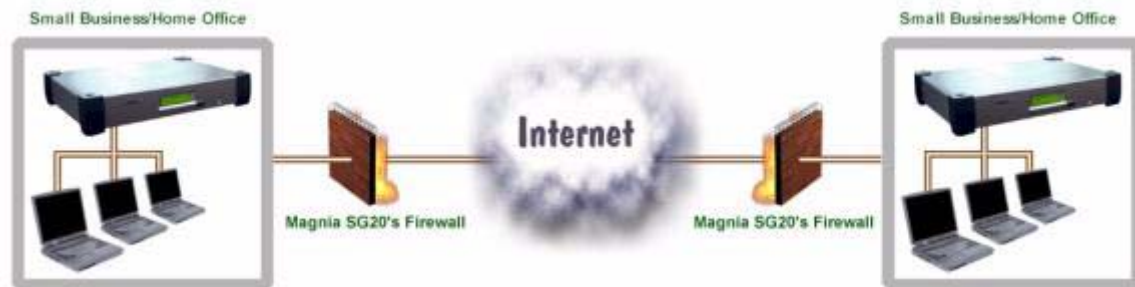


WINS Configuration Tab

User Accounts

When you establish an IPSec VPN connection to another Magnia SG30's local network, you are able to access that network's local clients, and the resources of the remote Magnia SG30 (such as file and printer sharing). For this reason, it is important to coordinate user accounts to assure proper access permissions (or restrictions) are in place. In order for a user to access another Magnia SG30 (or clients connected to the

Magnia SG30), there must be a matching user account on both server systems (with the same password).



Connecting a Client to the VPN -- Automatically

Because the process of configuring a Windows client for IPSec access can be complicated, the Magnia SG30 provides a tool which will configure your system for you. This is bundled with the certificate of authority created and provided by the Magnia SG30.

Downloading the IPSec Setup Tool

To obtain the certificate and the IPSec client tool for installation on a client computer:

- 1 Go to the Administrative Web interface.
- 2 Click the Network tab.
- 3 Click on the VPN menu item.

The main screen for VPN displays.

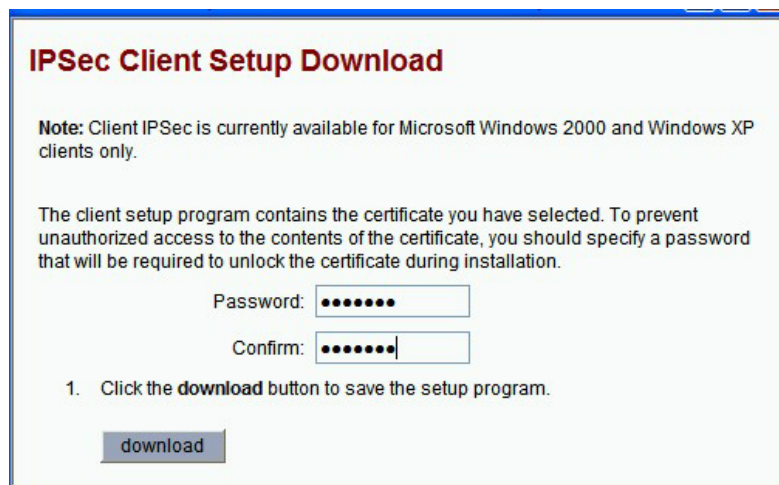
- 4 Click on the Configure hyperlink to the left of the IPSec Client VPN option to display the list of certificates.



Sample VPN Certificate List

- 5 Select a certificate by clicking on the hyperlink name of the certificate.

A dialogue screen will display allowing you to download the IPSec VPN Client Setup utility.



Sample VPN Certificate Download screen

- 6 Enter a password. This password is associated with the certificate being downloaded, and must be entered when the certificate is installed on the client computer. This extra security helps assure that certificates do not fall in to the wrong hands.

NOTE

A new password is entered each time the certificate is downloaded from the server. This means that if you download a certificate more than once, and enter different passwords, you will need to track which copy of the certificate used each password.

- 7 After entering a password, click the Download button, and a single file named ipsec_setup.exe will be downloaded to your client computer. This file is the

installation and setup program for the IPsec Client VPN and contains the certificate of authority. Distribute this file only to users you wish to have VPN access to your Magnia SG30.

NOTE

The downloaded file contains the X.509 Public Key certificate and the user's private key required for certification generated by the MAGNIA SG30. Be sure to use a Client PC connected directly to the private LAN port of the MAGNIA SG30 with a LAN cable. If the tool is downloaded using an unsecured wireless LAN or hub, it is possible that the information may be viewed or captured by a third party.

Installing the IPsec Client VPN Setup Tool

The Client Client IPsec Setup tool can only be used on a PC on which running Windows2000 or WindowsXP.

Two types of IP connections between a Client PC and the Client MAGNIA SG30 are available: local connection (wireless) and remote connection.

Local connections are used for connecting a Client PC to a private network using the MAGNIA SG30 (typically through a wireless connection). When the Client PC is connected the MAGNIA SG30, the connection between the MAGNIA SG30 and the Client PC will be secured by the IPsec encryption.

Remote connections are used for connecting a Client PC to the MAGNIA SG30 via the Internet. When a Client PC is connected to a private network with the MAGNIA SG30 via the Internet, the connection between the MAGNIA SG30 and the Client PC will be secured by the IPsec encryption.

NOTE

You must log on as the Administrator to install the Client IPsec Tool.

To install the Client IPsec tool on a Client PC:

- 1 Double-click the file ipsec_setup.exe (which was previously downloaded from the Magnia SG30).

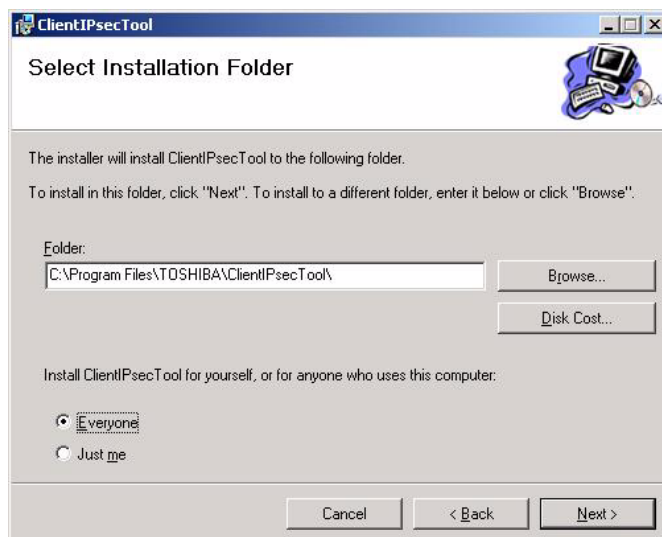
The Welcome screen displays.



Sample Welcome to the Client IPsec Tool Setup Wizard screen

- 2 Click Next.

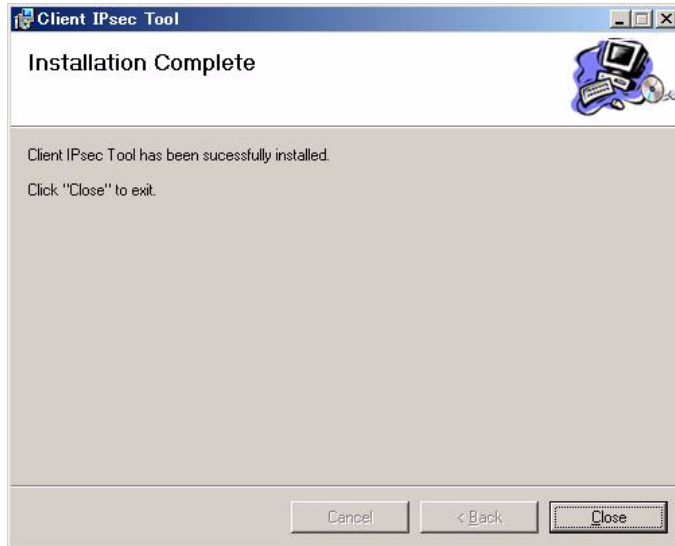
The Select Installation Folder screen displays.



Sample Select Installation Folder screen

- 3 The Client IPsec tool must be installed for all users. Select "Everyone" and then click Next.

The Installation Complete screen displays.



Sample Installation Complete screen

- 4 Click Close.

A confirmation message displays.

- 5 Click OK.

Uninstallation of Client IPsec VPN Tool

The IPsec Client VPN tool is installed and runs on your computer at all times. If you wish to uninstall the Client IPsec tool from a PC, use Add/Remove Programs in the Windows Control Panel.

How to Install the Certificate Authority

The IPsec Client Setup includes an X.509 Public Key Certificate Authority (CA), which authenticates the client computer with the Magnia SG30. This process is similar to using an encrypted password to verify you are authorized for access, but is automatic, once the certificate has been installed on the system.

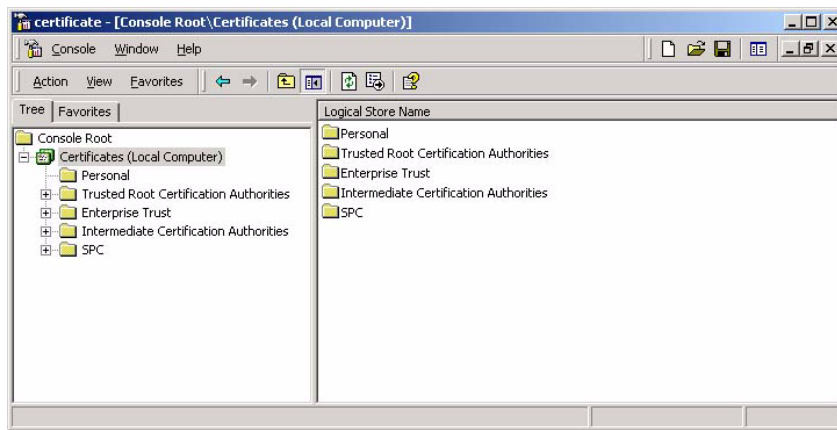
In order to begin communication with the Magnia SG30, the certificate must first be installed. Once it has been installed, it does not need to be installed again unless the certificate has been disabled and a new one issued.

The certificate is generated by the MAGNIA SG30 and is downloaded together with the Client IPsec tool as part of the IPsec Client Setup program. When the Client IPsec tool is installed, the CA will be stored in the Client IPsec target installation folder.

Installation of the certificate requires use the Microsoft Management Console (MMC). To install the certificate on the client, make sure you have first run the ipsec_setup.exe program. Then, install the certificate using the following steps:

- 1 Open a Windows Explorer window and browse to the installation directory of the MAGNIA Client IPsec software (default is C:\Program Files\Toshiba\Client IPsec Tool). Double click on the file “certificate.msc” to launch the Microsoft Management Console..

A Certificate screen displays.



Sample Certificate screen

- 2 Click the “_” mark on the side of Certificates (local Computer) to expand the tree.
- 3 Right-click on Certificates (local Computer) – Personal, and click All Tasks – Import.

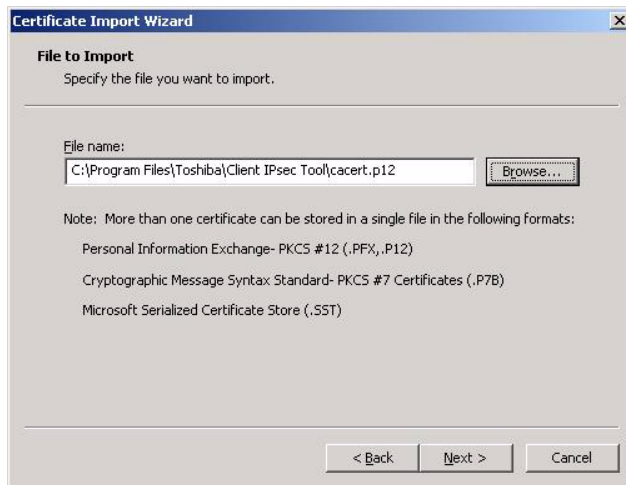
The Welcome to the Certificate Import Wizard screen displays.



Sample Welcome to the Certificate Import Wizard screen

4 Click Next.

The Certificate Import Wizard screen displays.



Sample Certificate Import Wizard screen

5 The CA file is stored in the folder where the Client IPsec tool has been installed under the name cacert.p12. Click the Browse button to select the CA file.

The default installation folder is C:\Program Files\Toshiba\Client IPsec Tool.

6 After selecting the CA file to be imported, click Next.

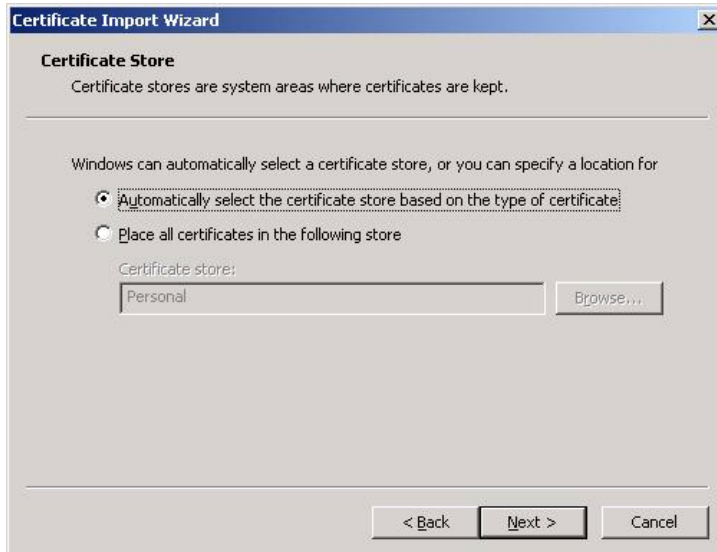
An Enter Password screen displays.



Sample Certificate Import Wizard - Enter Password screen

- 7 Enter the same password you entered when the Client IPsec tool was downloaded, and click Next.

The Certificate Store screen displays.



Sample Certificate Import Wizard - Certificate Store screen

- 8 Select Automatically select the certificate store based on type of certificate, and then click Next.

The Completing the Certificate Import Wizard screen displays.

- 9 Click Finish.

NOTE

When exiting from the Microsoft Management Console (MMC), a prompt message, 'Save console setting to certificate.msc?' will appear. You may click Yes or No as appropriate.

If the operating system running on the Client PC is Windows XP and when you click Yes, the system will ask you want to save as the MMC Version 2.0 format. You may click either Yes or No as appropriate.

Using the Client Client IPsec Tool

Start the Client Client IPsec tool as follows:

- 1 Click Start, point to Programs, and then click MAGNIA Client IPsec VPN – Client IPsec Tool.

Once activated, the Client Client IPsec tool will display an icon on the taskbar.

NOTE

When setup is completed, the Client IPsec tool will automatically start when the computer is booted.

Menu

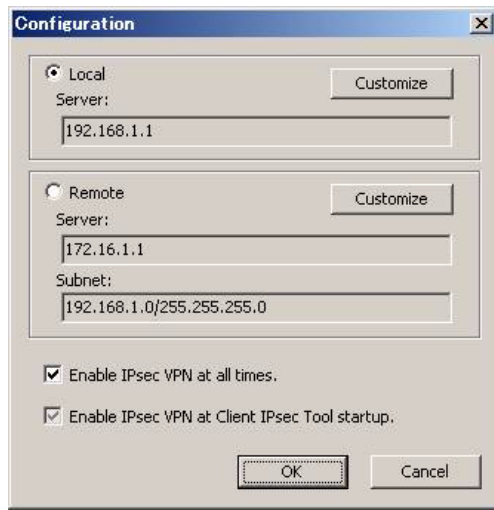
Click the icon on the task tray to display the following menu items.

Menu Item	Description
Help	Displays explanations of individual items in the menu and Configuration dialog box.
Configuration	Displays the Configuration dialog box.
IPsec VPN	Activates the IPsec communication. (When the IPsec is active, this item is checked.)
Exit	Closes the Client IPsec tool.

Configuration Dialog Box

This dialog box allows you to:

- ❖ Select of the connection type.
- ❖ Change of the IP address the Magnia SG30 server.
- ❖ Select whether the IPSec connection is established automatically and is up at all times.
- ❖ Select whether the IPSec connecton is established automatically when the IPSec VPN tool is run.



Sample Configuration screen

Types of Connection

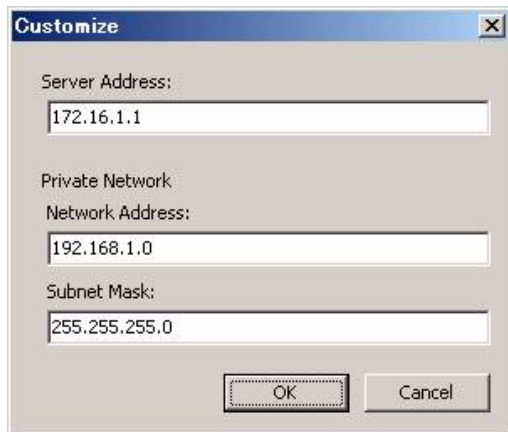
Two types of connections, local or remote, are available to be selected at the time of connection. Changes in the type of connection will not take effect until the computer reboots.

Connection Type	Description
Local	Select this connection type if your PC is a Client PC connected to a private network using the MAGNIA SG30.
Remote	Select this connection type if your PC is a Client PC connected to the MAGNIA SG30 via the Internet.
Default	Local connection.

Server address

The client computer must know the IP address of the Magnia SG30 in order to establish a connection. The IP address of the Magnia SG30 at the time the certificate was generated is used by default, and under normal circumstances, these values do not need to be changed. If the Magnia SG30 has been reconfigured with new IP addresses, it may be necessary to change them, so that the client knows how to find the server.

To change the address of the MAGNIA SG30, click the Customize button. This will display a dialog box allowing you to change the local or public IP addresses assigned to the Magnia SG30 public and private Ethernet connections.

A screenshot of a Windows-style dialog box titled "Customize". It contains three text input fields. The first field is labeled "Server Address:" and contains the text "172.16.1.1". The second field is labeled "Private Network" and "Network Address:" and contains the text "192.168.1.0". The third field is labeled "Subnet Mask:" and contains the text "255.255.255.0". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Sample Customize screen

Enable/Disable IPsec VPN

If the Enable IPsec VPN at all times check box is selected, the IPsec VPN will remain active even after the Client IPsec tool is exited, allowing the existing setting of the IPsec VPN to remain active whenever the Client PC is rebooted.

If the check box is not selected, the IPsec VPN will be disconnected when the Client IPsec tool is exited.

Selection Type	Description
Enable	When the tool is exited, the IPsec policy being set will be retained. When the tool is started next time, the IPsec VPN will be automatically activated in accordance with the preserved information. It is also possible, if the present IP address of the Client IP should differ from that in the preserved setting, to revise the IPsec VPN setting automatically to the present IP address.
Disable	When the tool is exited, the IPsec policy being set will be deleted.
Default	Enable.

Enable/Disable IPsec VPN at Client IPsec Tool setup

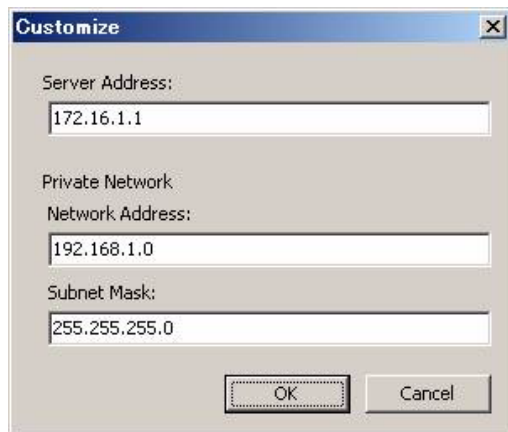
Select whether or not the IPsec VPN is automatically enabled when the tool is started.

Selection Type	Description
Enable	When the tool is started, the IPsec VPN will be automatically activated.
Disable	The IPsec VPN will not be activated automatically when the tool is started. You will be required to enable the IPsec VPN manually by selecting IPsec VPN on the menu.
Default	Enable.

Customize Dialog Box

This dialog box allows you to:

- ❖ Change the IP address of the MAGNIA SG30.
- ❖ Change the private network address of the MAGNIA SG30.



Sample Customize dialog box

Local connection

Selection Item	Description
Server Address	Enter the IP address of the private LAN port of the MAGNIA SG30.
	IP address: XXX.XXX.XXX.XXX (XXX representing a number between 0 and 255.)

NOTE

When making the setting for local connection, it is only the IP address of the MAGNIA SG30 that can be changed.

Remote connection

Selection Item	Description
Server Address	Enter the IP address of the public Ethernet port of the MAGNIA SG30.
	IP address: XXX.XXX.XXX.XXX (XXX representing a number between 0 and 255.)
Network Address	Enter the network address of the private network using the MAGNIA SG30.
	XXX.XXX.XXX.XXX (XXX representing a number between 0 and 255.)
Subnet Mask	Enter the subnet Mask of the private network using the MAGNIA SG30.
	XXX.XXX.XXX.XXX (XXX representing a number between 0 and 255.)

IPsec VPN Menu

This menu item selects whether the Client IPsec VPN should be enabled or disabled.

If the displayed menu item is checked, the data communication between the Client PC and the MAGNIA SG30 will be secured by the IPsec encryption. All communications will be encrypted until the IPsec VPN is cancelled.

If the displayed menu item is not checked, the IPsec VPN has been cancelled.

Exiting from the Client IPsec Tool

You can exit the Client Client IPsec tool by either of the following methods:

- 1 Select Exit on the menu of the Client IPsec tool.
- 2 Log off Windows.

If the Enable IPsec VPN at all time is selected on the Customize dialog box, the IPsec VPN will remain active even after the tool is exited. If the Enable IPsec VPN at all times is not selected, the IPsec communication will be disconnected when the tool is exited.

Connecting a Client to the VPN -- Manually

The third form of VPN connection supported by the Magnia SG30 provides secure communications between a client computer and the server. This is ideal for adding additional security for local clients accessing the server through the wireless interface. In addition, it can also be used to connect a client to the server through an Internet connection, similar to the PPTP VPN option.

The IPSec client VPN has the advantage of being usable for either local service, or for remote access (PPTP is designed only for remote access). However, the PPTP VPN is

supported on most Windows operating systems, and the IPsec VPN is supported only on Windows 2000 and Windows XP.

The IPsec connection between a client PC and the MAGNIA SG30 requires configuration of both the MAGNIA SG30 and Client PC.



TECHNICAL NOTE: In order for IPsec Client VPN to make connections to the server over the Internet, the Magnia SG30 must have a static IP address for its public (Internet) interface. DHCP is not supported.

Enabling the IPsec Client VPN Feature

To enable client IPsec VPN connections, you must first enable the feature on the Magnia SG30 and create client certificates that can be used to validate individual client access.

To enable the IPsec Client VPN feature:

- 1 Go to the Magnia SG30 Administrative Web interface.
- 2 Click the Network tab.
- 3 Click on the VPN menu item.

The displayed VPN screen allows you to select the type of VPN you wish to enable.

- 4 Click on the check box next to the IPsec Client VPN option, and then click Apply.

This will enable the Client IPsec VPN feature (though no clients can yet access the system).



Sample VPN main screen

To enable specific clients to access the Magnia SG30 using the IPsec Client VPN, you must first create and install certificates of authority. This is also done using the Magnia SG30 Administrative Web interface.

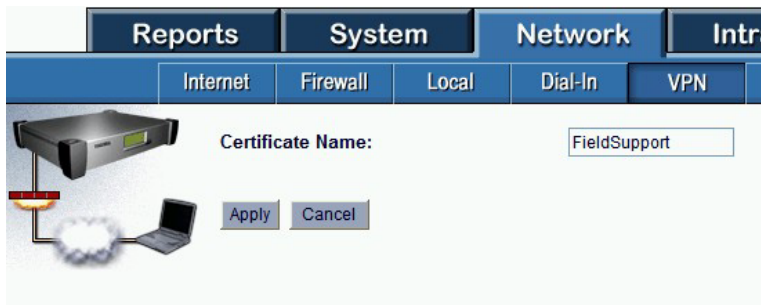
- 1 In the VPN screen of the Administrative Web interface, click the Configure option next to the IPsec Client VPN option.

This will display a screen listing the current certificates. When you first enable the IPsec Client VPN feature, this list will be empty.

You can create as many certificates as you like, and provide them to users in whatever manner you like. Multiple users could use a single certificate, such as an entire remote office or category of employee. Alternatively, you can provide a single certificate for each user.

- 2 Click the Add button to add a new certificate.

The displayed screen allows you to enter a new certificate name.



Sample VPN Add Certificate screen

- 3 Click Apply to create the new certificate.

When the certificate has been created, you will be returned to the screen listing current certificates. By default, new certificates are enabled for use.



Sample VPN Certificate List

Disabling IPSec Client VPN Access

Once you have enabled IPSec Client VPN access, you can disable it in two ways:

- ❖ Disable the IPSec Client VPN feature completely. If you disable the Client VPN feature completely, no IPSec client access will be allowed, even though individual certificates may be enabled (this does not affect PPTP VPN client access).
- ❖ Disable individual certificates. By disabling individual certificates, you can revoke the ability of any client using that certificate to access the system using the IPSec VPN feature. Other clients using different certificates will still have access to the server.

To turn off the IPSec Client VPN feature completely:

- 1 Go to the Administrative Web interface.
- 2 Click the Network tab.
- 3 Click on the VPN menu option.
- 4 Uncheck the IPSec Client VPN option.
- 5 Click Apply to save your change.

To disable specific certificates:

- 1 Go to the Administrative Web interface VPN screen.
- 2 Click on the Configure hyperlink next to the IPSec Client VPN option.
This will present the list of existing certificates.
- 3 Uncheck the check box next to any certificate you wish to disable.
- 4 Click the Apply button when finished.

Logging On and Using the VPN

When setup is complete, the client will have a new Dial-up Networking icon on the desktop and in the dial up networking window. For procedures to log on and use the VPN. See “Using the VPN” on page 247.

Chapter 6

Managing the Server

This chapter describes many of the management activities for maintaining your Magnia SG 30. To administer to the network, requires accessing the Administration Web site as described in the following section. After introducing how to access the administration web site, see [Viewing overall server status](#) on page 169 for a discussion of how to access and monitor the information describing the overall health and status of the SG30.

Outside monitoring services by Toshiba qualified administrators are also available for your Magnia SG30 if you would like additional assistance. For more information [See “Monitoring Overall Server Status with Toshiba Administrators” on page 175.](#)

Following that section, is a description of how to perform various management functions beginning with [Managing user accounts](#) on page 175. [Managing user accounts](#) on page 175 is followed by sections on backing up data, restoring files, and other management activities.

If the system goes down, a system recovery CD is available to reformat the Magnia SG 30 hard drive and reinstall all of the factory software. For more information see [System Recovery CD](#) on page 199

Through the Administration Web site you can modify the contents of the preinstalled Intranet and customize its look and feel. For more information [See “Managing the Intranet site” on page 217.](#)

Accessing the Administration Web site


The Magnia SG30 doesn't support the connection of a monitor or keyboard. Instead, you use your Web browser on one of the client computers to access both the built-in Intranet Web site and the Administration Web site, which stored on the Magnia SG30's hard disk drive.

If you used the Magnia SG30 Setup CD to set up the client computer, an icon on the desktop labeled “Admin” provides access to the Administration Web site.



To access the Administration Web site, click the **Admin** icon on the client computer's desktop. If the client computer does not have this icon, direct your browser to the following URL: `http://myserver:8282` (you can also use `http://192.168.1.1:8282`).

Be patient when accessing the Administration Web site. Like any other Web site, it may take a few seconds to load.



Status	Topic	Details
Overall appliance health		Health Warning
Number of print jobs queued		0
Backup last performed on		No backup performed
The firewall is		On
Primary hard disk usage		6% used, 31.045GB free
Second hard disk usage		No disk installed
External hard disk usage		No disk connected
Wireless network is		Not installed
The current system time is		3/29/2003 6:25 AM

Copyright © 2003 Toshiba Inc., All rights reserved.

Sample Administration Web site

Access to the Administration Web site is restricted to level 2 and 3 user accounts. When the Magnia SG30 is set up in Ease-of-Use mode (default), all accounts are at least Level 2. Some areas of the Administration Web site are restricted to Level 3 users. If you attempt to enter these areas, you will be prompted for a login password. Once you have logged in, you will be able to access all areas of the Administration Web site. If your server is set for High Security mode, user accounts are created as Level 1 accounts by default. Most user accounts will not be able to access the Administration Web site.

Exploring the Administration Web site


The Administration Web site has five tabs, which link to additional Web pages, allowing you to manage a variety of areas for your server. Click each tab to view its page. The Quick Help Box explains how to use each page.

- ❖ **Reports:** This tab provides current information about several features of the network and Magnia SG30: overall status, software upgrades, users, Internet access and configuration, system health, email, and backup.
- ❖ **System:** This tab lets you configure a variety of system related areas: print queues, adding, deleting and changing user accounts, setting up and configuring local or Internet email services, configuring or performing backups, restoring files from previous backups, changing the server's Date/Time, configuring what messages appear on the LCD panel, configuring the second disk, and shutting down the system.
- ❖ **Network:** This tab provides access to pages for configuring network-related parameters including: local network, Firewall, wireless networking, modem configuration, dial-in configuration and Internet connection.

- ❖ **Intranet:** This tab lets you configure the preestablished company Intranet functions: company news, upcoming events, common documents for download, and favorite links. You can also use this tab to adjust the look and feel of the Intranet.
- ❖ **Services:** This tab presents additional services available for the Magnia SG30.

Viewing overall server status

You can obtain information about the general operation and status of your Magnia SG30 from the Administration Web site. A general system report is displayed when you first enter the Administration Web site, as shown below.



Status	Topic	Details
	Overall appliance health	Health Warning
	Number of print jobs queued	0
	Backup last performed on	No backup performed
	The firewall is	On
	Primary hard disk usage	6% used, 31.045GB free
	Second hard disk usage	No disk installed
	External hard disk usage	No disk connected
	Wireless network is	Not installed
	The current system time is	3/29/2003 6:25 AM

Copyright © 2003 Toshiba Inc., All rights reserved.

Example of the System Status Report

Items on this screen include:

- ❖ **Overall appliance health:** The Magnia SG30 monitors internal information on system operation and health.
- ❖ **Number of print jobs queued:** This function reports the number of print jobs currently waiting in the Magnia SG30's print queue.
- ❖ **Backup last performed:** This reports the last time a successful backup was performed. It does not cover snapshots made to the second hard disk drive. The status will initially be "yellow" and will not change until a backup is performed.
- ❖ **Firewall is on/off:** This indicates whether the firewall is on, protecting the local network and server from Internet attacks.
- ❖ **Hard disk usage:** This reports on the amount of disk space used on the primary and secondary hard drives (if configured).
- ❖ **Current system time:** This shows the system time at which this page was displayed.
- ❖ **Wireless Access Point:** This reports on the current status of the internal wireless access point.

More information about the options in the System status report can be viewed by clicking on the given hyperlinks (underlined words).

The green bullets to the left of each item can indicate whether there are cautions or problems with the system. In this example, the Backup item is yellow because no backups have been taken. The firewall item is also yellow, because the firewall has been turned off (which is a potential security risk).

The hyperlinks in each item can be used to display more information.

More detailed information is presented on the following menu tabs:

- ❖ Upgrades — This screen displays the list of software upgrades that have been installed on the server.
- ❖ Users — This screen displays a list of current user accounts, along with summary information about each.
- ❖ Internet — This screen lists networking information, including the type of connection, MAC address of the WAN Ethernet port, and all the IP addresses currently used by the system.
- ❖ Health — The status of the various self-monitoring features of the server is displayed on this screen.
- ❖ Email — A listing of the current email mailboxes and their sizes is displayed on this screen, as well as the current system mail queue (pending mail to be sent).
- ❖ Backup — This screen lists the most recent backups taken of the server.

You can also view the system status information by displaying it on the Magnia SG30's LCD screen. For more information, see [Viewing server status through the front panel LCD](#) on page 173.

Viewing server health status

The Magnia SG30 has been integrated using high quality, reliable components. You should not experience a problem during the normal life of the unit. However, in the unlikely case that there is a problem, the Magnia SG30 contains a number of self-monitoring capabilities that allow the system to detect potential problems before they permanently damage the system. In this way, the system can help you identify problems and get them resolved before the system crashes or data is lost.

The health monitoring subsystem can be viewed using the Administration Web site. A summary of your server's health is displayed on the default reports page when you first access this server Web site.

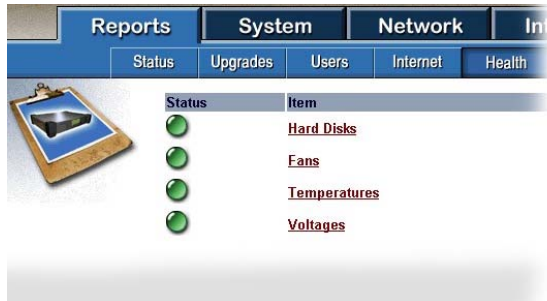
To view the “health” (current operational status) of the Magnia SG30, select the **Reports** tab, and click the **Health** tab.



Example of the System Status Report

This indicator will normally show that the Magnia SG30 is in good health, as indicated above. If a problem is detected, the bullet on the left will turn yellow, and the status will change from “Good” to “Warning.”

To view more detailed information about the server’s health, and the types of status being monitored, select the Health menu item in the Reports tab. A more detailed summary of the system’s health will appear.



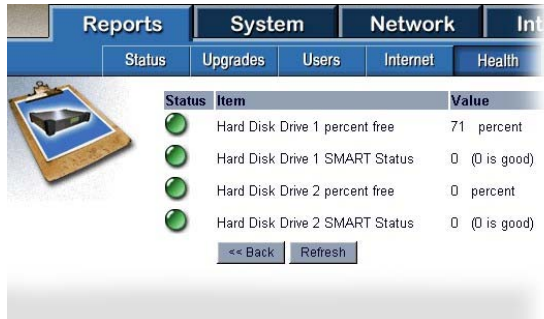
Example of the System Health Report

You can view even more detailed information by clicking the hyperlinks for any of the topics.

Hard drive status

The Magnia SG30 hard drives are “SMART” drives. They have built in capabilities to self-monitor performance. They use this information to detect subtle changes in performance and predict if the drive is likely to fail in the future. If a failure is predicted for a drive, this will be displayed in the health status section of the Administration Web site as well as the LCD.

If the health status system indicates there is a problem with a hard drive, stop using the server immediately. If possible, perform a backup of the current user files on the hard drive, and contact Toshiba or your supplier to obtain a replacement disk.



Status	Item	Value
●	Hard Disk Drive 1 percent free	71 percent
●	Hard Disk Drive 1 SMART Status	0 (0 is good)
●	Hard Disk Drive 2 percent free	0 percent
●	Hard Disk Drive 2 SMART Status	0 (0 is good)

Example of the Disk Drive report

Fan status

The Magnia SG30 uses several internal fans to assure that it is cooled properly. These fans are monitored to make sure they are operating properly. If one of the fans slows below an acceptable RPM, or stops spinning, the health monitoring system will detect the failure and alert you on the LCD panel and in the Administration Web site.

If a fan fails, it does not mean there is an immediate problem with your Magnia SG30 – if the room is cooled and the unit is properly ventilated, the server can continue operation for some time. However, if a fan fails, it is best to perform a backup of all user data, and contact Toshiba or your supplier to have the unit repaired or replaced.

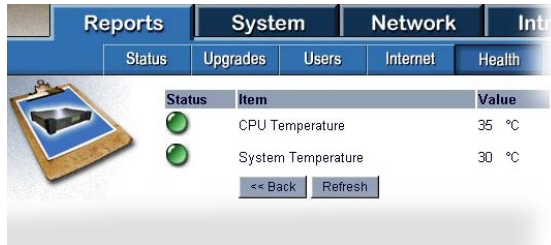
If you choose to continue running the unit when a fan failure is displayed, carefully monitor the temperature of the unit to make sure it does not go too high.

Temperature status

As with all computers, the Magnia SG30 can generate some heat, and needs to be properly ventilated and cooled. Overheating can cause the unit to fail.

The Magnia SG30 monitors its internal temperature in two different locations. One location monitors general internal temperature. The other monitors the main CPU, which generates the most heat within the system. Because the Magnia SG30 is designed to operate in a variety of conditions, the internal temperature can rise well above normal office temperature before it is considered dangerous to the server's components.

If the internal temperature rises above an acceptable level, the problem will be displayed on the LCD as well as in the Administration Web site. As with all health status screens, a problem condition is shown with the bullet on the left of an item changing color to yellow.



Status	Item	Value
●	CPU Temperature	35 °C
●	System Temperature	30 °C

Example of the Temperature Status report

If the health system indicates that internal temperature is too high, check to make sure the unit is in a well-ventilated area. It may be helpful to move the server to another room that is cooler. Also check to make sure the ventilation holes in the sides of the unit are not blocked. If a fan failure is causing the unit to overheat, this will be shown in the fan status.

Voltage status

The Magnia SG30 has a robust power supply that should perform well for the entire life of the unit. However, if there is a problem, the health monitoring system will detect any significant change in the power flow to a variety of system components. Problem warnings will appear on the LCD and in the Administration Web site.

Some variation in voltage is normal in systems. The Magnia SG30 is preconfigured to detect abnormal variations, which will cause the bullet to the left of the voltage item to turn yellow.

If the voltages on your system appear to be consistently or repeatedly abnormal, contact Toshiba for service.

Viewing server status through the front panel LCD

In addition to viewing status of your server through the Administration web site, the LCD panel on the front of the server can display a variety of information about your Magnia SG30. The default display shows the date and time. Several messages may be displayed simultaneously, in which case some messages appear only when you scroll through the list of messages.

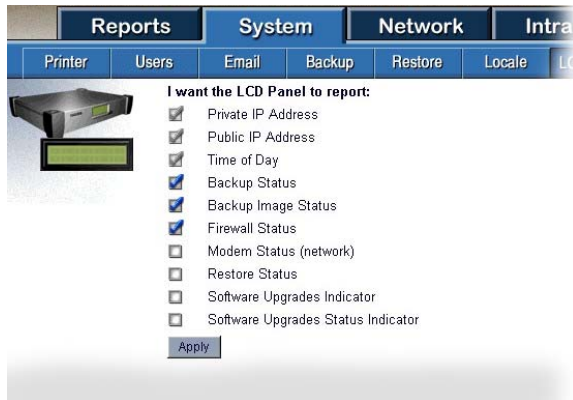
You can press the Status scroll button on the front of the appliance to view the Internet IP address and other current status information.

Urgent messages will display on the LCD panel immediately: they don't require use of the scroll button.

To set the LCD to display the status of certain system conditions:

- 1 From the Administration Web site, select the **System** tab, and click the **LCD Panel** tab.

The LCD options screen appears.



Sample System LCD options screen

- 2 Select which options you want to display on the LCD and click **Apply**.

Some of the information on the LCD panel is always displayed and cannot be turned off. This information includes:

- ❖ **Software Version:** The software version number is displayed on the LCD panel in case it is requested by Toshiba Support.
- ❖ **Private address:** This private TCP/IP address is set for the local network Ethernet interface (7 port hub).
- ❖ **Public address:** This public TCP/IP address is set for the public (Internet) Ethernet port.
- ❖ **Time of day:** This default display is frequently used to show the system is ready.

Other information can be displayed on the LCD panel. This optional information includes:

- ❖ **Firewall status:** This displays the status of firewall operation.
- ❖ **Software upgrades indicator:** Information displays when a new software upgrade is available for downloading.
- ❖ **Software upgrades status indicator:** Information displays showing whether a software upgrade installation was successful.
- ❖ **Backup status:** This indicates whether the last backup was successful, and the time at which the last backup was performed.
- ❖ **Backup image status:** This shows the last time the second hard disk was used to take a snapshot of the primary hard drive.
- ❖ **Restore status:** Information displays on the progress of a restore operation from a previous backup.

- ❖ **Modem status:** Information displays on the status and settings of the modem.

Monitoring Overall Server Status with Toshiba Administrators

One of the best ways to keep your Magnia SG30 continually up and running is with the Health Monitoring Service. Qualified administrators monitor your Magnia SG30 and address any health-alert conditions.

Here's how it works:

- ❖ After signing up for the Health Monitoring Service via the Administration Web site, your Magnia SG30 will send daily reports about its health to Toshiba. Information includes hard disk statistics, system temperature, system fan speed, etc. No personal data is sent.
- ❖ In the unlikely event that your Magnia SG30 has a component that shows signs of failure, an alert is sent to qualified administrators at Toshiba.
- ❖ A Toshiba administrator can then contact you to help proactively remedy the error and keep your Magnia SG30 up and running.

To sign up for the service, see the "Health" section of the "Services" tab in your Magnia SG30's Administration Web site.

Managing user accounts

This section describes how to add, modify, or delete user accounts on your Magnia SG30. User accounts are used to control access to the server. Access to specific areas of the system, and specific files, are regulated by the user account. User accounts also determine access permissions to administrative functions of the server.

Predefined accounts

The Magnia SG30 comes with three accounts already created and defined on the server. These accounts are defined for specific purposes. The first two of these accounts come from the factory with a default password of "toshiba." However, both accounts will have their password changed to the first account's password when the system is first set up.

NOTE

It is important that you remember the password of the first account you create using the Magnia SG30 Setup CD or Administration Web site, because this password will be used to access these predefined accounts.

applianceadmin— Because this account cannot be deleted, it can be used to gain access to the Administration Web site if other accounts have been deleted. It is a predefined level 3 account, meaning that it has full access to all administrative functions. While all other accounts are restricted to viewing files and directories belonging to that account, the applianceadmin account can view and access any file or directory belonging to any account on the server. The applianceadmin account cannot send or receive email.

telnetuser — Telnet is a method of accessing the Magnia SG30 internal Linux interface directly, without going through the Administration Web site. Only experienced Linux users should attempt this method of accessing the server. For security reasons, the only account allowed to log in via telnet is the telnetuser account (it serves no other purpose).

toshsupport — A third account called “toshsupport” is created when you sign up for Health Status Monitoring. This account is not enabled until you enable it in the Administration Web site. The password is calculated at that time and is known only to Toshiba support. Enabling this account will allow Toshiba support personnel access to your system to troubleshoot any problems you report. This access by Toshiba support personnel is restricted by you, and can only occur if and when you enable this account.

System security modes

When you set up the first account on the Magnia SG30, you also setup basic configurations for the server, including whether to use Ease-of-Use mode, or High Security mode. Your choice at this time will affect the type of accounts that are created on the system, and who is allowed to create these accounts.

Ease-of-Use mode — The client setup CD can create new accounts automatically when setting up a client. All new accounts are set (by default) as level two users, giving them partial access to the Administration Web site.

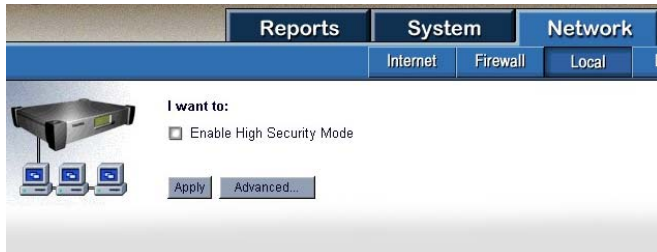
NOTE

this is the default mode if you are performing the setup manually.

- ❖ **High Security Mode** — The client setup CD cannot create new accounts. The setup CD can only set up client computers using accounts that already exist on the Magnia SG30. This requires that a user with a level 3 account (see explanation below) create accounts on the system prior to using the setup CD.

To determine what security mode the system is currently in, or to change it, go the Administration Web site, click the Network tab, and select the Local Network menu item. If the Enable High Security Mode item is checked, the server is in high security mode. If it is unchecked, the server is in Ease-of-Use mode.

To change the mode check (or uncheck) the Enable High Security Mode item, and click **Apply**.



Sample Local network security screen

NOTE

When accessing the Administration Web site, you may be asked to log in with a level 3 account and password before accessing the more secure features of this site.

The local network security screen also allows you to specify whether you wish to require client computers to have a matching account on the Magnia SG30 in order to access its file and printer sharing features. In its default configuration, the Magnia SG30 requires all users to have an account on the server in order to access files or to use its printer. You can change this configuration to allow any client computer connected to the Magnia SG30 local network to access the public file share, and the shared printer. Such unrestricted access without an account only applies to the public share and the printer. Users without an account will be able to access the public share and printer, but will not be able to access personal account directories.

To change access permissions to the public share and printer:

- 1 Access the Administration Web site.
- 2 Click the **Network** tab.
- 3 Select the **Local** menu option.
- 4 To enable access to the public areas of the Magnia SG30 without an account, click the “Enable Unrestricted Access to Public File Shares” checkbox.
- 5 Click **Apply** to save the setting.

User security levels

NOTE

Choose your degree of security wisely. Set the mode to avoid any unauthorized use of, or access to, important data files or admin screens.

Each user is assigned a security level by default. In high security mode, all users are created at level 1 by default. In ease of use mode, all users are created at level 2 by default.

In either case, the level of an individual user account can be changed in the user account management section of the Administration Web site.

You can apply one of three security levels to each user:

Level 1— These users cannot configure the Magnia SG30 from their client computers (no remote administration privileges), but have access to the public folder and their personal folders on the Magnia SG30. They can also use the shared printer and access the Internet and other general features of the Magnia SG30.

Level 2— These users have limited access to administrative functions (access to part of the Administration Web site) as well as access to public and personal folders and other general Magnia SG30 features.

Level 3— This user has full access to all administrative functions (full remote administration privileges).

Creating user accounts

When you run the Client Setup Wizard, it creates a user account for the system you are installing. You can create other user accounts through the Administration Web site.



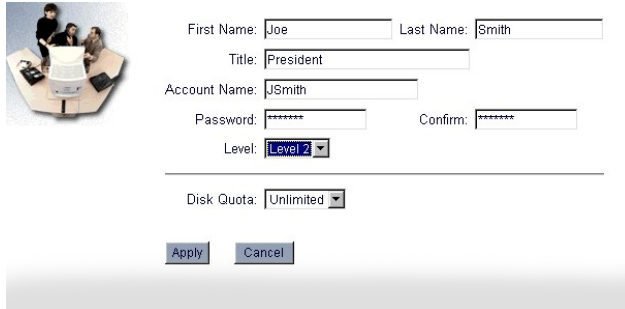
1 From a client computer, click the **Admin** icon to start the Administration Web site.

2 Select the **System** tab and click the **Users** menu item.

At this point you may be asked to enter your level 3 user account and password before the user account management page will display

3 Click **New Account**.

- 4 Assign a user name in the Account Name field, and enter the remaining information.



The screenshot shows a web form for creating a new user account. On the left is a small graphic of three people at a computer. The form fields are: First Name (Joe), Last Name (Smith), Title (President), Account Name (JSmith), Password (masked with asterisks), Confirm (masked with asterisks), Level (a dropdown menu showing 'Level 2'), and Disk Quota (a dropdown menu showing 'Unlimited'). At the bottom are 'Apply' and 'Cancel' buttons.

Sample Creating new accounts screen

You can select an access level for the account at this time. If you do not wish to use the default shown, you can select that the account have level 1, 2 or 3 access.

If you have enabled disk quotas, a drop-down box will appear, allowing you to select a quota. To specify something other than the default of unlimited, click the drop-down box and select a limit.

Changing user accounts

You can change user account information and limits at any time after the account has been created. To change an account:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **Users** menu item.

The list of existing users will be presented.

NOTE

To change user accounts, you must be a level 3 user. To validate this, you are asked to enter a level 3 account name and password before user account administrative pages can be accessed.

- 3 Select the user account you wish to change.

This will present the same screen as for new user accounts, in which you can change any account characteristic.

- 4 Modify the account's details as required.

Deleting user accounts

You can delete user accounts that are no longer in use. Deleting old user accounts can free up space and close security holes in your system.

When you delete a user account, the Magnia SG30 performs the following actions:

- ❖ The account and all accompanying account information are removed from the system.
- ❖ The account's personal directory and all files contained in it are moved to the directory "deletedUsers." To reclaim the space from these files, you must browse to this location using network neighborhood and manually delete them. Use the account "applianceadmin" to browse and delete the deleted account's directories.
- ❖ The account's mail file will be deleted. Any pending (undelivered messages) will be removed.

To delete an account from the server:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **Users** menu item.
The list of existing users will be presented.
- 3 Select the name of the account you wish to delete.
The user account information appears.
- 4 Click **Delete**.

Backing up your data

NOTE

Backing up data is extremely important to maintain smooth operations, especially if the Magnia SG30 contains business or important personal information, such as tax or banking details. Hardware breakdowns and power outages can occur at any time. Take the time to back up important files in case of an emergency.

One of the most important features of the Magnia SG30 is the number of backup options available and the ease with which you can back up your data. From the Administration Web site, you can choose the following:

- ❖ Files to back up
- ❖ Place to store the files (on a second hard disk drive or on an Internet backup service)

- ❖ A schedule for when a backup is to occur



HINT: Backing up data and system files uses up valuable space very rapidly. Toshiba recommends that you invest in one of the following: a second hard disk drive to expand the Magnia SG30 capacity, an external backup device such as a tape drive, or subscription to an online Internet backup service.

The Magnia SG30 provides several built-in methods of performing backups. You can also perform backups of the server's files by accessing them from a client with a separately purchased backup device, such as a tape drive.

Types of backup

There are three types of backup:

- ❖ **Full backup** — All user files and selected system files are automatically included in full backups.
- ❖ **Incremental backup** — Selects only those files that have changed since the last backup. This can be useful when full backups are taking too much space to perform frequently.
- ❖ **Partial Backup** — With partial backups, you select a specific set of file to backup.

Backups can be performed to three locations.

- ❖ **Local client** — If you have a client computer on the network that has extra space on its hard disk drive, this client can be used to store backups.
- ❖ **Additional hard disk drive** — The Magnia SG30 can have a second drive configured for extra storage, as well as an additional USB disk drive. Backups may be targeted to either of these added storage locations.
- ❖ **Internet location** — The Magnia SG30 offers the ability to store backups off site at an Internet FTP location. To use this option, you must have an FTP site available, such as one provided by a commercial Internet based backup service, or through a corporate FTP site. Because the speed of Internet backups is limited by the speed of your Internet connection, this option is appropriate for smaller backups of selected, business critical files.

Performing a manual backup

Backups can be performed automatically or can be scheduled to execute automatically.

To perform a manual backup:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **Backup** menu item.

The System Backup screen appears.



Sample System backup screen

- 3 Select the manual backup option, and click **Next**.

NOTE

You may be asked to enter a level 3 account and password before proceeding. For security reasons, backing up and restoring data are operations restricted to level 3 user accounts.

Selecting backup type

First determine whether the backup is to be a partial, incremental or full backup.

- ❖ Full backups will save all user files from all of the user account personal directories, the public directory, all user data from the Intranet, and optionally, system files can be saved. Including system files in a full backup saves information about user accounts, networking configurations and your Intranet content. If anything should happen to your system, restoring a full backup with system files included should restore nearly all of the server's configuration options and customizations, as well as all of your user data. It is recommended that you periodically perform a full backup to assure you have copies of all your files in case something happens to the server system.

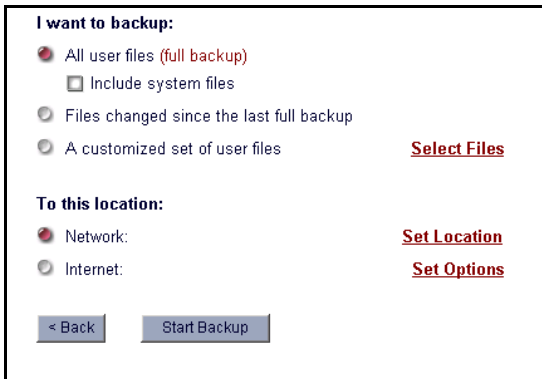
While full backups are the most complete and offer the best protection, they can be very large (even though they are compressed to minimize their size). As you place more and more data on your Magnia SG30, the backup files can become quite large. Consequently, you may not wish to perform full backups every time.

- ❖ As an alternative to a full backup, you can perform a partial backup. In this case, you select only specific files for inclusion in the backup. This can reduce time required for the backup process, as well as space required for the backup file. This method works if you have a subset of files which are most critical and need to be backed up more frequently than other files on the system.

- ❖ The incremental backup method provides another way of performing backups without the size and time requirements of full backups. Once you have performed a full backup, subsequent incremental backups can be performed which will backup only files that have been modified since the last backup. The incremental backup method, used in conjunction with periodic full backups, can provide a great combination of reliability, completeness and efficiency.

Once you have decided which type of backup to perform, select one of the following options from the **I want to back up** section of the screen.

For a full backup, select **All user files**. For incremental backup, select **Files changed since the last full backup**. For a partial backup, select **A customized set of user files**.

A screenshot of a web-based backup configuration screen. The title is "I want to backup:". There are three radio button options: "All user files (full backup)" which is selected, "Files changed since the last full backup", and "A customized set of user files". Below the first option is a checkbox labeled "Include system files". To the right of the third option is a red hyperlink "Select Files". Under the heading "To this location:", there are two radio button options: "Network:" and "Internet:". To the right of "Network:" is a red hyperlink "Set Location", and to the right of "Internet:" is a red hyperlink "Set Options". At the bottom left are two buttons: "< Back" and "Start Backup".

Sample Backup choices screen

If you select the full backup or incremental backup methods, no further action is necessary for backup file selection.

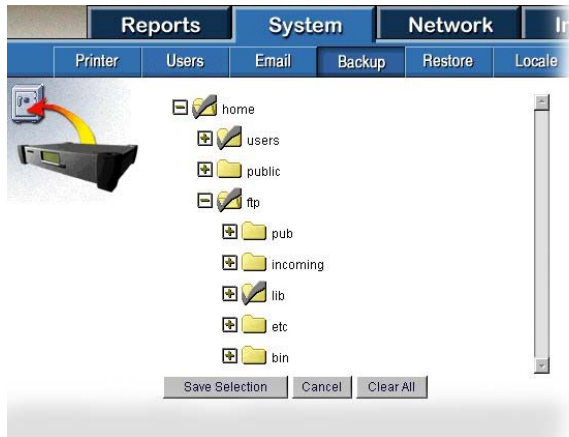
If you select the partial backup method, you must select the list of files to include in the backup. Click the **Select Files** hyperlink. This will take you to the file selection screen.

Selecting files for backup

To select specific files for a partial backup, select the **Customized set of user files** option, and then click the **Select Files** hyperlink. This will take you to a screen that will allow you to view and select files and directories on your Magnia SG30 disk. You can backup files from a variety of directories:

- ❖ FTP — This directory contains the Magnia SG30 FTP files, including upload or download files. Don't bother to back up this directory unless you are using the FTP feature.
- ❖ Intranet — This directory contains files for a custom Intranet (not the same as the preinstalled, built-in Intranet accessed by the icon the Setup CD places on your desktop). Don't bother backing up this directory unless you have created a customized Intranet by placing your own HTML pages here.

- ❖ **Public** — This directory is the public directory accessible to all accounts and client computers. Back up the contents of this directory if you or any other of the network's users are placing files here.
- ❖ **Users** — This directory contains all of the individual account directories for each Magnia SG30 user. You should back up some or all of this directory.



Sample Selecting files for backup screen

There are several types of icons you will see on the screen.



This icon (red check) indicates that the specified directory, and all subdirectories and files it contains, are selected for backup. Clicking this icon deselects the directory and its contents.



This icon (gray check) indicates that the specific directory, and some specified subdirectories or files have been selected for backup. Click it to select all files in the directory, including any that may be added in the future.



This icon indicates that this file has been selected for backup. Click it to deselect it.



This icon indicates that this file has not been selected for backup. Click it to select it for backup.



This icon indicates that the specified directory can be expanded out to view subdirectories and files it contains. Click this icon to expand the view.



This icon indicates that the specified directory has an expanded view of its contents below. Click it to hide the expanded view.

The example screen below illustrates the use of the backup file selection screen.



Selecting backup files

In this example, the users and owner directories have a gray check because not all of their contents have been selected for backup (the AccountsPayable file has not been selected). The guest directory has a red check because its entire contents were selected.

When a directory has a red check, all files and subdirectories it contains are included in a backup, including files or directories added at a later time. For example, if you click the users directory twice, which changes the icon to a red check, save this file selection, any backup in the future that uses this file selection will include all user files and directories, even ones added after the file selection list was first created.

Once you have established a custom list of files for a backup, this list can be used for subsequent backups. The Magnia SG30 will remember your list of files selected, and use this each time you do a backup until you change this list.

Selecting backup location

Once you have selected the files that will be included in the backup, you can select where the backup will be placed. You have two options. You can place the backup file on a local client computer that has been configured with a shared directory. This includes a second hard drive or USB external hard drive connected to your Magnia SG30. You can also place the backup on an Internet site (after signing up for this service).

Placing your backup files on a local computer can be very convenient, and because the local computer is accessed through the high speed LAN, this method can accommodate large backups. Using a local client as a holding place for your backup has the disadvantage of not preserving your data in case of fire or theft.


Placing your backup files on an Internet FTP site is a great way of making sure you store critical information off site quickly and easily. It has the disadvantage of being limited by the bandwidth of your Internet connection.

To designate a local client computer as a backup location, click **Set Location** next to the Network option.

The Magnia SG30 surveys your network to find available shared directories on client computers. This may take a few seconds. When completed, the screen will show the clients in your network. If a computer symbol appears with a plus sign in a box, click the plus sign to list the computers in the workgroup.

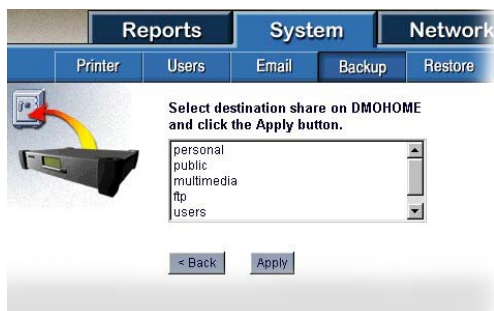


Sample Client system list screen

Click the local computer to use for the backup location. A red checkmark  will appear on the folder symbol to the left of the computer name.

If the shared file on the desired computer requires an account and password to gain access, enter them in the spaces provided at the bottom of the screen.

After clicking **Next**, the following screen will list the shared directories available on the selected local computer.



Sample Available directories screen

Select the shared directory to use for the backup, and click **Apply**. This share will now be used for all future backups to a local computer (until you change this setting).

If you have an external USB HDD and wish to place backup images on this device, simply select the Magnia SG30 as the target client. The "ExtDisk" share, representing the USB HDD, will appear. Select this as the target for your backups.



Sample USB HDD backup selection screen

Selecting Internet backup

You can perform backups to an Internet based FTP site. If you have access to an FTP site, you can automatically configure your backups to be placed on this site. The advantages to doing this include:

- ❖ Files are stored off site, protecting them from fire and theft
- ❖ Encryption technologies protect the security of your data

If you have access to an FTP site, you can select the Internet backup site as the location for your backups by going to the Administration Web site main backup screen and selecting Internet Backup as the location.

Click **Set Options** to enter the URL of the FTP site, along with your account name and password.

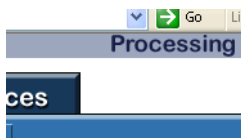
A screenshot of a web form for configuring an FTP backup account. The form is enclosed in a black border. It contains three labeled input fields: 'FTP Site:', 'Username:', and 'Password:'. Each label is followed by a text input box. At the bottom left of the form are two buttons: 'Apply' and 'Cancel'.

Sample Backup account configuration screen

After entering the account name and password, click **Apply**. When this process is complete, you can use the Internet location for any backup, including manual, incremental, automatic or full.

Starting a manual backup

Once you have selected the type of backup to perform, the files to include (if a partial backup), and the location for the backup, you can begin the actual backup process. Click **Start Backup**. The backup will begin, as indicated by the “Processing” indicator in the upper-right hand corner of the screen.



Example of a Processing indicator

When complete, a dialog box will be displayed confirming that the backup has completed successfully.



Sample Backup complete dialog box

Scheduling an automatic backup

You can schedule backups to be run automatically using the settings you specify in the main backup configuration screen. Configurations for manual and automatic backups are stored separately. Configuring a manual backup will not effect your automatic backup configurations and establishing an automatic backup configuration will not disturb a configuration for a manual backup.

To establish automatic backups:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.

- 2 Select the **System** tab and click the **Backup** menu item.

The System Backup screen appears.

I want to:

- ☐ Perform a manual backup
- ☒ Schedule regular backups
- ☐ View current backup schedule
- ☐ Manage previous data archives
- ☐ Manage advanced options

Next >

Selecting the Schedule regular backups option

- 3 Select the **Schedule regular backups** item on the initial backup screen, and click **Next**.
- 4 From the next screen, select the type of backup and the location of backup as described above.



Sample Configure backup options screen

- 5 When finished, click **Next**.

You will be presented with the backup-scheduling screen.

- 6 From this screen, you can schedule daily, weekly or monthly backups.

- ❖ To schedule backups to be performed once a day, click the Daily option. Complete the backup schedule by entering in the time you want the backup to begin.



Example of Daily backup option

- ❖ To schedule backups to be performed the same day of the week, click the Weekly option. You can select weekly backups performed on specific days of the week. For example, backups could be performed every Sunday and Wednesday morning at 2:00 AM.

Backup Time:

02 00 AM

Recurrence Pattern:

☐ Daily
☒ Weekly
☐ Monthly

☒ Sun ☐ Mon ☐ Tue ☒ Wed
☐ Thu ☐ Fri ☐ Sat

Finish Cancel

Example of Weekly backup option

- ❖ To schedule backups to be performed once a month, click the **Monthly** option. You can specify monthly backups that will be performed on the same day of each month. In the example below, an automatic backup will be performed on the 3rd of each month.

Backup Time:

12 00 AM

Recurrence Pattern:

☐ Daily
☐ Weekly
☒ Monthly Day 3 of every 1 month(s)

Finish Cancel

Example of Monthly backup option

- 7 Once finished establishing the schedule, click **Finish**.

Your automatic backup configuration and schedule is saved and will be run automatically.

Canceling automatic backups

If you have configured an automatic backup using this method, it will be run as scheduled until you delete the configuration and cancel the backups.

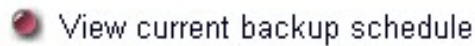
To cancel automatic backups:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **Backup** menu item.

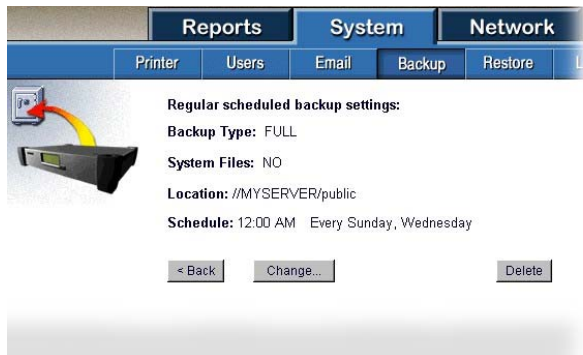
The System Backup screen appears.

- 3 On the backup screen, select the **View current backup schedule** item.



Selecting the View backup schedule item

The next screen displays the current backup schedule, and also contains buttons allowing you to change or delete the automated backup configuration.



Sample View backup schedule screen

- 4 To delete the current backup configuration, click **Delete**.

The configuration is deleted, and automatic backups will no longer be executed.

Viewing backup status

Backup status can be seen in several places on the system. The easiest and most obvious location is in the Administration Web site, which initially displays the summary report page. This summary report page will show when the last backup was performed.



Sample View backup status screen

To see more detail about the backup status, click the **Backup** hyperlink on this report page, or select the Backup menu item on the Reports tab. This detailed backup report

will list the last several backups performed, and give more detailed information about each of them.

Status	Date	Location/Archive (Size)
	Jan 17, 2001 3:43 PM	//TESTMACHINE/TEST/CUSTOM.backup- 154315-17Jan2001.tbk (9.59 MB)
	Jan 17, 2001 1:57 PM	//SASVR_/public/CUSTOM.backup- 135754-17Jan2001.tbk (9.59 MB)
	Jan 15, 2001 5:23 PM	//SASVR_/public/FULL.S.backup- 172338-15Jan2001.tbk (10.7 MB)

Sample View backup status detail screen

The status column shows a bullet that will be green if the backup was successful, or yellow if there was a problem. The date and time of the backup is listed in the next column. The last column gives the name of the computer on which the backup was placed the name of the file, and the size of the backup file in megabytes.

The name of the backup file is created from the type of backup, and the time and date it was performed. For example, the backup file name CUSTOM.backup-172338-17Jan2001 means the backup was performed on January 17, 2001 at 5:23 in the afternoon, and was a custom backup of selected files.

The last method of viewing backup status is from the LCD panel. If the LCD has been configured to show status on the LCD, it will display the status of the last backup (success or failure). This can be useful as a quick check to make sure scheduled backups are being performed regularly and successfully.

Encrypting backups

Security is always a consideration when performing any type of backup. Placing backups on local computer drives or on the Internet backup site can mean making files more easily accessible to others, and can increase the chances of unauthorized access to your private data.

In order to secure your backup data, the Magnia SG30 offers the ability to encrypt the contents of a backup. This encryption is powerful, and is extremely difficult to reverse without your password.

In order to encrypt your backups, you must enable this feature and specify a password.



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.

- 2 Select the **System** tab and click the **Backup** menu item.

The System Backup screen appears.

I want to:

- ☐ Perform a manual backup
- ☐ Schedule regular backups
- ☐ View current backup schedule
- ☐ Manage previous data archives
- ☒ Manage advanced options

Selecting Manage advanced options

- 3 Select the **Manage advanced options** item and click **Next**.
- 4 Select backup encryption by unchecking the **I do not want to encrypt my backup archives** option. You must then also enter a password, which will be used for all backups.

Enter an encryption password:

If you opt to encrypt your backups, please write down the password in a private and secure place for possible later use.

Password: Confirm:

OR

☐ I do not want to encrypt my backup archives.

Sample Backup encryption password screen

- 5 Click **Apply** when you have entered your password.

NOTE

When you enable encryption of backup archives, all backups performed from that point on will be encrypted. This includes full, partial and incremental as well as manual and automatic backups.

NOTE

Do not forget your password. If you forget your password, there is no way to retrieve the information in your encrypted backup archives. Write your password down and place it in a secure location.

Restoring files from a backup

Once you begin making regular backups, you may find circumstances when it would be useful to restore files from the backups. These circumstances might range from restoration of a single file which was accidentally deleted to restoring all the files after a system or a disk has been replaced.

Selecting an archive

To restore one or more files to your system:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **Restore** menu item.

The System Restore screen appears.

Sample System restore screen

- 3 Select the backup archive from which you wish to restore files.
If your backup archive files have been placed on a local client computer, select the **Network** option.

If you wish to restore files from an archive on an Internet based archive, select the **Internet** option (this will show “not available” if you have not signed up for this service).
- 4 To select the actual archive, click the **Select Archive** hyperlink next to the Network or Internet option (whichever you have selected).

- 5 Select the system from which the backup archives reside, entering an account and password if needed. (This selection is equivalent to the configuration you originally established when you specified where the backups should be placed).

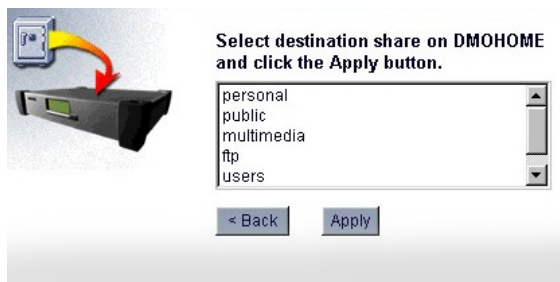
The following screen appears, displaying a list of backups.



Sample Select client screen

- 6 Enter your Login ID and password, and click **Next**.

The following screen appears, displaying a list of shared directories on the client computer.



Sample Shared directories screen

- 7 Select the directory containing the backup archive you wish to use, and click **Next**.

The following screen displays a list of available archives.

- 8 Select the archive to use for the restore from the drop-down list of backup archive file names.

To assist in selecting the correct archive, the file name incorporates the type of archive and the date it was created.

- 9 When you have selected the archive to use, click **Finish**.

Selecting files to restore

You can restore all files from the archive, or selected individual files.

Selecting all files

To restore all files in the selected archive:

- ❖ Click the **All files from the archive** option.

I want to restore from the above selected archive:

☒ All files from the archive:

☐ Include system files

☐ Selected file(s) from the archive:

[Select Files](#)

Selecting all files from the archive

If the Include system files option box is grayed out as shown above, the archive did not include system files. If it is not grayed out, you can restore system files from this backup archive.

NOTE

Restoring system files deletes the current Magnia SG30 configuration and restores the configuration as of the time you executed the backup.

Do not select this unless you wish to reestablish the server configuration taken at that time. Items such as network configuration and user accounts will be replaced.

Selecting individual files

To select individual items from the archive:

- ❖ Click the **Selected file(s) from the archive** option.

I want to restore from the above selected archive:

☐ All files from the archive:

☐ Include system files

☒ Selected file(s) from the archive:

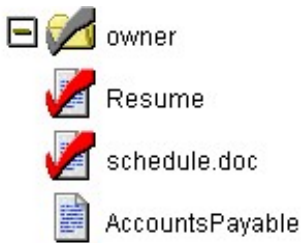
[Select Files](#)

Start Restore

Selecting individual files from the archive

- ❖ After selecting this option, click the **Select Files** hyperlink to select the specific files to restore.

The next screen will allow you to select files for restoration (using the same method used to select files for backup). Only files or directories that were included will appear in this list.



Selecting specific files from the archive

- ❖ Click the files and directories you wish to restore.
- ❖ When completed, click **Save Selection**.

The selection of files to be restored will be saved.

When you have completed selecting a full restore, or selecting file to restore, you can begin the restoration operation.

Starting the restore

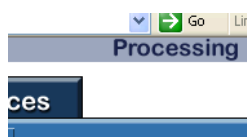
Once you have selected the archive from which you wish to restore files, and selected the files to restore, you can begin the restore. After selecting file for restore, or the backup archive to use, you will return to the main restore screen.

To start the restore:

- 1 Click **Start Restore** at the bottom of the screen.

The processing indicator will appear in the upper-right corner of the screen, indicating the system is extracting the files from the backup archive.

This process can take some time, even when only one or two files are being restored. This is because the entire archive must be copied down to the local system before the selected files are extracted. If the backup was a full backup, it could be very large, and the restore time long.



Example of a Processing indicator

When the file restore is completed, the specified files have been returned to their original location on the Magnia SG30. Their original account ownership and modification date are preserved.

Extracting Files Under Windows

It is possible to extract individual files from a Magnia SG30 backup archive using tools available from third parties. This method allows you to access files from Magnia SG30 backup archives without using the Magnia SG30. This may be useful if you need to extract data files quickly when the server is not available.

Magnia SG30 backup archives are Linux “tar” files that have been compressed using “gzip.” A popular product that can handle both of these formats is WinZip®.

Extracting a file using WinZip in a Windows® operating system

To extract a file using WinZip in a Windows® operating system:

- 1 Change the file name extension from “.tbk” to “.tar.gz.”
- 2 Run WinZip to decompress the backup archive – it will produce a file with a “.tar” extension.
- 3 Run WinZip again on the file created with the “.tar” file name extension. Use WinZip to extract the specific file or files you require.

This technique will only work if the backup was not encrypted. Encrypted backup archives must be restored using the Magnia SG30 software.

System Recovery CD

A system recovery CD is available to restore the Magnia SG30 hard drive to the original factory image. The recovery CD will reformat the Magnia SG30 hard drive and then reinstall all of the factory software.

Before running the System Recovery CD:

- ❖ **Remove the secondary hard disk if it is installed in the Magnia SG30 before booting from the Recovery CD.** If the second drive is not removed before the recovery process begins, all data on the second hard drive will be lost.
- ❖ Disconnect all USB devices from the SG30 except for a USB CDROM which will be used to perform the system recovery.

To perform the system recovery:

- 1 Shutdown the Magnia SG30 and unplug the power cord.

- 2 Attach a USB 1.1 CDROM drive to one of the Magnia SG30 USB ports and power on the CDROM drive. (The CDROM drive can be a CDRW drive as well)
- 3 Insert the Magnia SG30 System Recovery CD into the USB CDROM drive.
- 4 Reconnect the power cord to the Magnia SG30.

The LCD panel will display "Magnia SG30".

- 5 Press and hold the LCD scroll button until the LCD panel displays "Alternate Boot" and then release the LCD scroll button.

The SG30 should begin booting from the USB CDROM drive within 10-15 seconds. In a minute, the LCD panel will display the following confirmation message: "Press SCROLL to continue install".

- 6 Press and hold the LCD scroll button for approximately 2 seconds. If you do not press the LCD scroll button within 20 seconds, the Magnia SG30 will power off and you will need to repeat steps 1-5. This step provides a safety mechanism to avoid inadvertent reinstallation of the Magnia SG30.

The LCD panel should now display "Installing SG30 Please Wait...".

When installation is complete, the Recovery CD will be ejected from the CDROM drive and the SG30 will reboot.

During the reboot, the SG30 will complete the installation by auto-configuring itself. The LCD panel should display "Configuring SG30 Please Wait..."

The Magnia SG30 will reboot one final time after the configuration process is completed and the system is now ready for use.

The entire recovery process will take approximately about 30 minutes to complete.

Using the second disk drive

The Magnia SG30 can be purchased with either one or two drives. These drives are the only user serviceable parts in the system. If you purchased a server with a single drive, you can purchase a second drive from Toshiba at a later time to upgrade your system.

Primary disk drive usage

Your primary disk drive has a size of 40 GB or more (depending on the configuration purchased). However, not all of this space is usable for general file storage. Several hundred megabytes are set aside and used for system files and other requirements to support the various features of the server. The remaining space is available for you to use as general file storage.

Secondary disk drive usage

A second disk drive can be used in two different ways, depending on your network needs.

- ❖ A second disk drive can be configured to contain periodic snapshots of your primary disk drive.

This snapshot mechanism makes a complete copy of the entire primary disk drive on a periodic basis. If something goes wrong with your primary disk drive, you can move the secondary disk drive in to the primary disk drive's slot, reboot the server, and the system will resume operation with all files intact as of the last time a snapshot was taken.

NOTE

This process is commonly referred to as mirroring.

However, it should not be confused with RAID mirroring, where all files are constantly mirrored on a second disk drive. The SG30 copies files on a regularly scheduled basis, not continuously. If you set the snapshot for once a day at 12:00, then you will need to reenter all data entered since 12:00.

You can specify when you would like to take a snapshot of the system. The process of copying all files from one disk drive to the other can have an effect on server performance, and can take several hours (on a large, full disk). Therefore, the recommended schedule is to have the disk drive snapshot operation automatically performed once every night at midnight.

If you use the second disk drive for snapshots, it must be at least the same size as your primary disk drive.

- ❖ You can also configure the second disk drive as extra file storage.

If you do this, the second disk drive will appear as the directory "2ndDisk," and can be reached by browsing in network neighborhood. The second disk drive is configured as a generally available disk drive – any account can place files on it and access its contents (similar to the public directory).

Second disk drives are automatically configured for snapshots as the default, unless you change the configuration.

Viewing second disk status



To view the status of the second disk, click the **Admin** icon to start the Administration Web site. The main report page will display an item showing the current status of the second disk. If the second disk is being used for extra space, a status line similar to the one below will appear:



Second hard disk usage 5% used, 17.40GB free

Example of viewing second disk status

If the second drive has been configured for snapshots, the status shows when the last snapshot was taken.



Second hard disk usage Mirror completed:
Jan 20, 2000 at 3:26
PM

Example of viewing second disk status - mirrored device

Installing a second disk drive

If you originally purchased your Magnia SG30 with a single drive, you can purchase and add a second drive to the system. Because Magnia SG30 disk drives are pre-configured at the factory, you need only insert the disk drive in the primary or secondary disk drive bay.

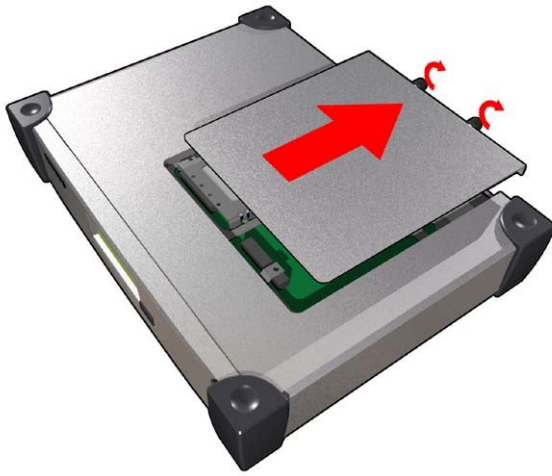
NOTE

Only disk drives purchased from Toshiba as Magnia SG30 accessories are supported in the Magnia SG30.

To install a second disk drive:

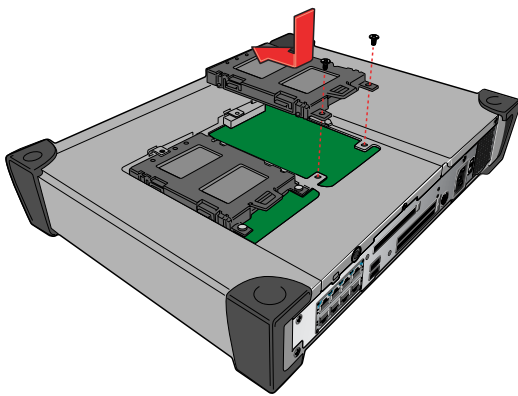
- 1 Turn off all client computers connected to the Magnia SG30.
- 2 Turn off the Magnia SG30 by pressing the Power/Shutdown button on the front of the unit, or by using the system shutdown feature of the Administration Web site, and disconnect the power cable.
- 3 Undo the two thumbscrews on the rear of the Magnia SG30.

- 4 Slide back the top of the case.



Removing the cover

- 5 Locate the slot for the disk drive. Facing the unit from the front, the primary disk drive slot is on the right, and the secondary disk drive slot is on the left.
- 6 If you are replacing a primary disk drive:
- ❖ Remove it by unscrewing the two thumbscrews.
 - ❖ Slide the disk drive back and lift it out.
 - ❖ Remove the drive from the disk drive from the drive cage by unscrewing the four mounting screws.
 - ❖ Continue at step 8.
- 7 If you are adding a new disk drive, mount the new disk drive to the drive cage using the screws.



Mounting the disk in the drive cage

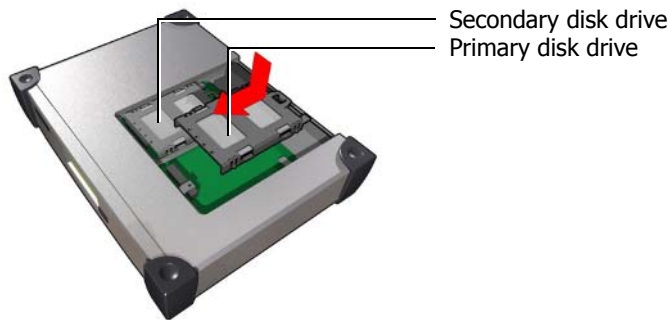
- 8 Install the new disk drive in the chassis.
(Again, facing the machine from the front, the primary drive is on the right, and the

secondary drive is on the left.)

Place the disk drive on the rails and slide it forward.

Ensure that the disk drive connectors engage firmly with the chassis connectors.

Secure the disk drive with the two thumbscrews (do not over tighten).



Installing the disk drive

9 Close the top of the case and secure it with the two thumbscrews.

10 Plug in the power cable, reconnect the client computers, and turn on the Magnia SG30 and the client computers.

If you added a second disk drive, the Magnia SG30 will recognize the drive.

11 Configure the disk drive.

- ❖ To configure the disk drive as a backup device or as additional storage, see [Configuring the second disk drive for snapshots](#) on page 205.
- ❖ To configure the disk drive as a primary disk drive replacement, see [Installing the second disk drive as the primary disk drive](#) on page 207.

Secondary disk drive usage

A second disk drive can be used in two different ways, depending on your network needs.

1 A second disk drive can be configured to contain periodic snapshots of your primary disk drive.

This snapshot mechanism makes a complete copy of the entire primary disk drive on a periodic basis. If something goes wrong with your primary disk drive, you can move the secondary disk drive to the primary disk drive's slot. The system will resume operation with all files intact as of the last time a snapshot was taken. For

more information, see [Installing the second disk drive as the primary disk drive](#) on page 207.

NOTE

This process is commonly referred to as mirroring. However, it should not be confused with RAID mirroring, where all files are constantly mirrored on a second disk drive, which can significantly affect performance.

You can specify when you would like to take a snapshot of the system. The process of copying all files from one disk drive to the other can have an effect on server performance, and can take several hours (on a large, full disk). Therefore, the recommended schedule is to have the disk drive snapshot operation automatically performed once every night at midnight.

If you use the second disk drive for snapshots, it must be at least the same size as your primary disk drive.

- 2 You can also configure the second disk drive as extra file storage.

If you do this, the second disk drive will appear as the directory “2ndDisk,” and can be reached by browsing in network neighborhood. The second disk drive is configured as a generally available disk drive – any account can place files on it and access its contents (similar to the public directory).

Second disk drives are automatically configured for snapshots as the default, unless you change the configuration.

Configuring the second disk drive for snapshots

To configure a second disk drive:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **2nd Disk** menu item.

If the second disk drive has been installed properly and is recognized, the following screen appears.



Sample Configuring a second disk screen

- 3 To configure the Magnia SG30 to perform snapshots every night, accept the defaults and click **Apply**.

For another configuration, select a different daily schedule and click **Apply**.

⚠ WARNING

Switching from one configuration to another (changing from “extra space” to “snapshots,” or vice versa), will wipe out whatever information is on the second disk drive.

If you have used the second disk drive as extra space, configuring it for snapshots will wipe out any files you may have placed on the disk drive.

To disable snapshots at any time, return to this page, and uncheck the **Enable scheduled snapshot** box. The configuration will remain, but snapshots will no longer be taken.

You can take a snapshot at any time by clicking the **Take Snapshot** hyperlink. If you perform a manual snapshot, it will display a confirmation when the snapshot is complete.

Configuring the second disk drive for extra space

To configure the second disk drive to be used as extra space:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **System** tab and click the **2nd Disk** menu item.
- 3 Select the **Extra local disk space** option, and click **Apply**.

My second hard disk is currently configured as:

☒ Extra local network disk space

☐ A snapshot image of my main hard disk

☐ Enable scheduled snapshot at:

1:00 AM Every 1 Days

Apply Changes

Selecting the Extra local network disk space option

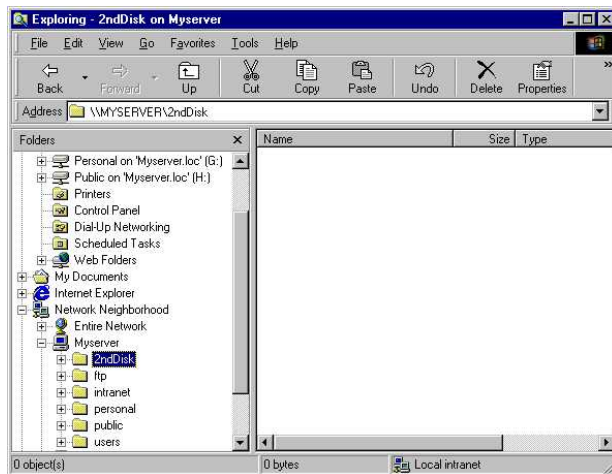
The disk drive will be reformatted and made available for general use.

⚠ WARNING

Switching from one configuration to another (changing from “extra space” to “snapshots,” or vice versa), will wipe out whatever information is on the second disk drive.

If you have used the second disk drive as extra space, configuring it for snapshots will wipe out any files you may have placed on the disk drive.

To access the second disk drive, you can use the Windows® Explorer to browse to the Magnia SG30, and locate the directory named “2ndDisk.” Files can be placed in this directory, and the directory itself can be mapped as a logical disk drive under the operating system for easier access.



Example of viewing the second disk using Windows® Explorer

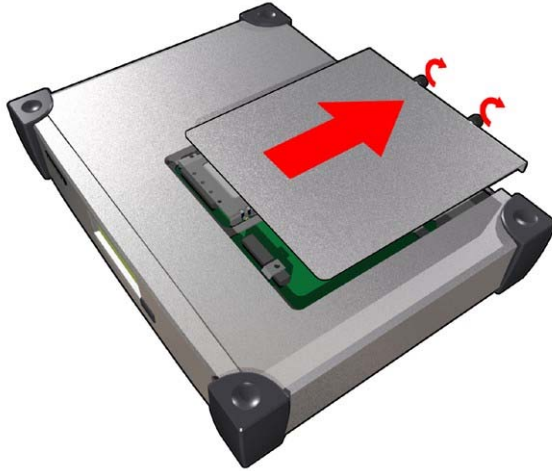
Installing the second disk drive as the primary disk drive

If you have been using the second disk drive snapshot feature, you can move the second disk drive to the primary slot and use it as the primary disk drive. This can be useful if the primary disk drive has experienced a problem. After switching the second disk drive in to the primary slot, you can continue operations with the system as of the last time a system snapshot was taken.

To install the second disk drive as the primary disk drive:

- 1 Turn off the Magnia SG30 by pressing the Power/Shutdown button on the front of the unit, or by using the system shutdown feature of the Administration Web site, and disconnect the power cable.

- 2 Remove the top cover by unscrewing the two thumbscrews at the rear of the appliance and sliding the cover back.



Removing the cover

- 3 Release the secondary disk drive by loosening the thumbscrews, then remove the disk drive by sliding it back and lifting it out.
- 4 Release the primary disk drive by loosening the thumbscrews, then remove the disk drive by sliding it back and lifting it out.
- 5 Set the primary disk drive aside.
- 6 Place the secondary disk drive in the primary disk drive's mounting rails and slide it forward. Ensure that the disk drive's connectors engage firmly with the chassis connectors. Secure the disk drive with the two thumbscrews (do not over tighten).
- 7 Replace the cover, reconnect the power cable and turn the unit back on.

You can now use the second disk as the primary disk.

Using an External USB Hard Disk

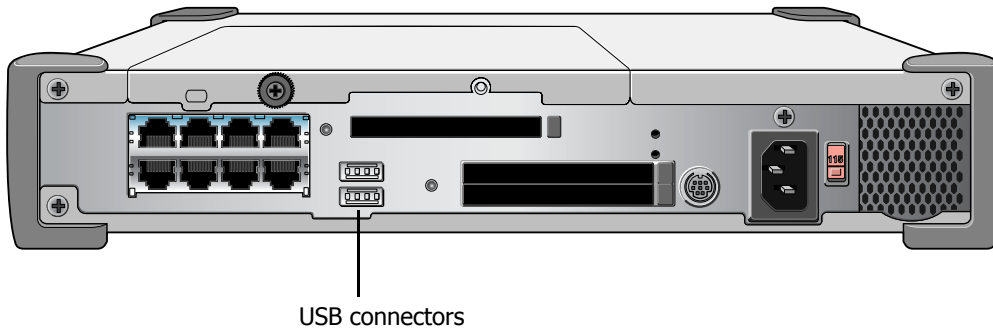
The Magnia SG30 allows you to connect an external USB hard disk (HDD) to one of its USB ports in the back. This extra disk can be formatted and used for extra storage on the system. Because it is also portable, an external USB hard disk can be removed and taken to other systems for use. The external USB HDD can also be used for storage of backup images.



TECHNICAL NOTE: The server must be powered off before connecting an external USB hard disk.

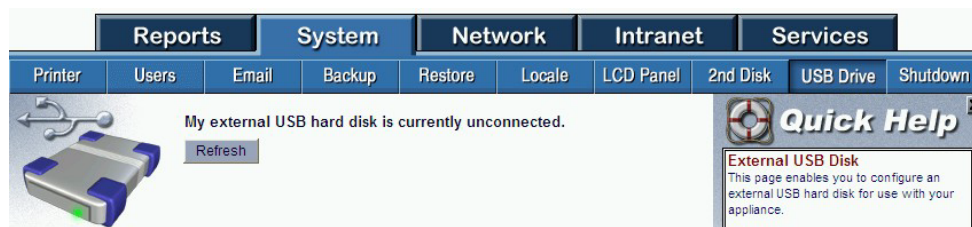
Connecting a USB HDD to the Magnia SG30

To connect a USB hard disk to the Magnia SG30, plug its USB cable in to one of the USB connectors in the back of the Magnia SG30. The HDD can be connected to either of the USB connections.



Connecting a USB HDD to the SG30

- ❖ After connecting the USB HDD, plug it in and turn it on if there is an on/off switch.
- ❖ To view the USB HDD status, go to the Administrative Web interface, select the System tab, and click on the USB Drive menu item. If no HDD has been detected, the screen will inform you that no USB drive is present.



Sample USB drive not present screen

- ❖ If the USB drive is powered on and connected, you can click the Refresh button to scan for the USB drive again. The screen will repaint and confirm that the drive has been detected.



Sample USB HDD not mounted screen

- ❖ If the drive has been previously formatted, you can immediately mount the drive for use (many USB HDDs come pre-formatted). If the drive is not formatted or does not mount, try formatting it first (see section below). The process of mounting a disk drive makes it available for use in a specific directory.

⚠ WARNING

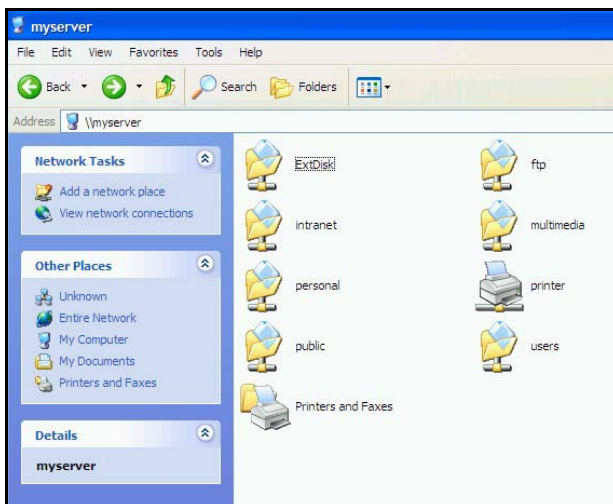
Never unplug or power off a mounted USB HDD without first either shutting down the Magnia SG30 or unmounting the drive through the Administrative Web interface.

- ❖ Once the drive has been mounted, the USB Drive screen will show its current status, including the amount of space used.



Sample USB HDD mounted screen

- ❖ The external USB HDD is made available on its own directory share called “ExtDisk”, which can be reached by browsing the network to your server.



Sample USB HDD browser directory screen

Once you mount a USB HDD, the Magnia SG30 will look for it each time it boots. If it finds the USB HDD available during the boot, it will automatically mount it. This allows you to format and mount the USB HDD as extra storage once, and then use it with no further configuration, even when the system is restarted.

Disconnecting the USB HDD

To disconnect a USB HDD, you must first unmount the drive (if the drive is not mounted, it can be physically disconnected without further configuration). While the drive is mounted, it may be in use, or have data cached inside the computer. Disconnecting the drive without unmounting it can cause loss of data.

To unmount the USB HDD, go to the Administrative Web interface, selected the System tab and click on the USB Drive menu item. If the drive is mounted, a button will appear on the screen labeled “unmount”. Click this button and wait for the confirmation that the USB drive has been unmounted successfully.



Sample USB HDD mounted screen

The USB drive can also be safely removed by shutting the server down. Please see the section “Shutting Down the Magnia SG30” in Chapter 3.

Once the USB drive is unmounted (or the Magnia SG30 is shut down), turn off or unplug the USB HDD and disconnect the USB cable from the back of the Magnia SG30.

Formatting the USB HDD

While some USB HDDs come pre-formatted, it may be necessary to format the hard disk for use on the Magnia SG30. If there is any problem mounting a new USB HDD, or if you wish to use a USB HDD previously used elsewhere, you can format it for use using the Administrative Web interface. Once it has been formatted, it should not be necessary to format the disk again.

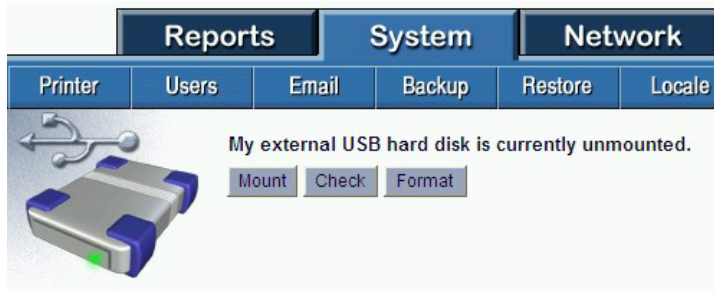
⚠ WARNING

Formatting the USB disk drive will erase all data contained on it. There is no way to retrieve this data once the format has begun.

To format the HDD:

- 1 Connect the HDD to the Magnia SG30, and then use a web browser to go to the Administrative Web interface.

- 2 Select the System tab, and click on the USB Drive menu item. The screen should confirm that the USB drive is present, but not mounted. If the drive is mounted, it must be unmounted before a format can be accomplished.



Sample USB HDD not mounted screen

- 3 Click the Format button. A warning dialog displays.



Sample format warning message

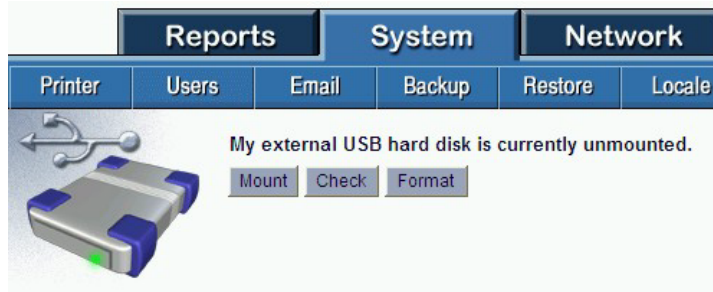
Depending on the size and speed of your hard disk, a format may take a few minutes. Do not shut down the Magnia SG30 or disconnect the USB drive during until this operation is complete.

Checking the USB Drive

While USB drives are very reliable, under rare circumstances, there may be file system or data integrity issues that need repair. This usually happens when the drive has been disconnected without unmounting it, or when a power failure may have shut the system down improperly.

The Magnia SG30 provides an option to check and possibly repair any damage to the USB HDD file system. To access this option, go to the Administrative Web interface, select the System tab, and click on the USB Drive menu item. If the drive is mounted, click the Unmount option.

The USB Drive screen displayed when the drive is unmounted displays a “Check” button. Click this button to perform a file system inspection and repair. Depending on the size of the HDD, and the amount of data on it, this operation could take some time.

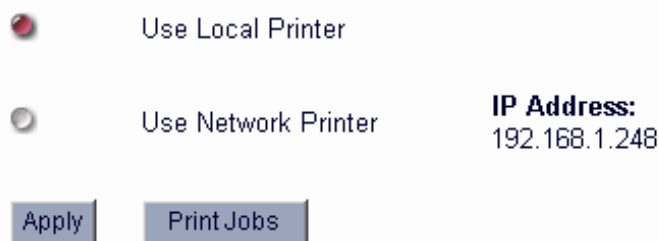


Sample USB HDD not mounted screen

Configuring a Shared Printer

The Magnia SG30 will act as a print server for a local parallel printer or a networked attached printer. Configuring a printer in this way allows you to share a single printer for all client computers in your local network. The Magnia SG30 will accept print jobs from the client computers, and queue them to be sent to the shared printer.

Configuration of the shared printer is simple. A direct connect parallel printer is supported by default. Simply connect the printer to the Magnia SG30 parallel port and configure your clients for its use.



Sample shared printer screen

To use a network printer:

- 1 Connect the printer to one of the ports of the built in Ethernet switch.
- 2 Access the Administrative Web site.
- 3 Click the **System** tab, and then select the **Printer** menu option.
- 4 Select “Use Network Printer”.

- 5 Note the IP address of the network printer, and click **Apply** to save the settings.

When configuring a network printer connected through Ethernet, be sure to configure the printer for a static IP, and make sure this IP address matches the one displayed on the Printer configuration screen in the Web Administration site.

Software upgrades

The Magnia SG30 has a built in feature that allows you to stay on top of fixes and features released by Toshiba for your server. The Software Upgrades feature allows you to quickly identify software upgrade packages that can be applied to your server. It will track which packages have already been installed, as well as automatically notifying you when a new package is available.

Because Toshiba may release important fixes and new features using this process, it is recommended that you periodically check and install recommended upgrades (see [Software upgrades auto-check](#) on page 216).

Viewing available upgrades

To view the list of available software packages available for upgrade:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Click the **Services** tab, and select the **Upgrades menu** item.

A list of upgrade categories available for your Magnia SG30 appears.



Sample List of upgrade categories screen

This list of upgrades needs to be refreshed whenever you check it. To check the list of upgrades and identify any new upgrades available on the Toshiba upgrades Internet site, click **Check for New Upgrades** at the bottom of the screen. The list is updated with the latest upgrades, organized by category.

- 3 To view the list of available upgrades in a specific category, click the hyperlink for that category.

A screen displays the upgrades that are available for installation on your system.

Selecting an upgrade to install

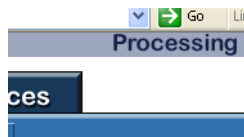
To install an upgrade:

- 1 Select the upgrade category, then click the hyperlink for the upgrade you wish to install.

A screen displays more detail about the selected upgrade.

- 2 Click the **Install Upgrade** button to install the upgrade.

It can take some time to download the upgrade package and install it. During this operation, the “Processing...” indicator will appear in the upper-right corner of the screen.



Example of a Processing indicator

Viewing installed upgrades

You can view a report of Installed upgrades by going to the Administration Web site, clicking on the Reports tab, and selecting the Upgrades menu item. A list of software upgrade packages you have already installed will appear. You can also view this list from the Software Upgrades screen by clicking **Advanced**, and selecting the **View upgrade report** option.



Sample Viewing software upgrades screen

Manual software upgrades

If you do not have Internet access, you may be able to obtain the upgrade on a diskette or CD.

To install a local copy of a software upgrade package:



- 1** From a client computer, click the **Admin** icon to start the Administration Web site.
- 2** Click the **Services** tab, and select the **Upgrades menu** item.
- 3** Click **Advanced**.

A list of advanced features appears.

Toshiba Software Upgrades:

- ☐ View upgrade report
- ☒ Perform a manual upgrade
- ☐ Configure auto-check

Selecting the Perform a manual upgrade feature

- 4** Select **Perform a manual upgrade**, and click **Next**.

The install selected upgrade screen appears.



Sample Install selected upgrade screen

- 5** Enter the location of the package, including the file name (e.g. C:\TEMP\KUPD.RPM).
Alternatively, you can use **Browse** to locate and specify the upgrade file.
- 6** Click **Install Selected Upgrade**.

The package will be installed.

Software upgrades auto-check

The Magnia SG30 software upgrades feature has the ability to automatically check for new upgrade packages. This system will automatically notify you via the LCD panel when a new upgrade becomes available.

To enable this feature:



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Click the **Services** tab, and select the **Upgrades menu** item.
- 3 Click **Advanced**.
A list of advanced features appears.
- 4 Select **Configure auto-check**, and click **Next**.



Selecting the Configure auto-check feature

- 5 The next screen allows you to turn on the Auto-check feature.



Sample of the Configure auto-check screen

- 6 To enable Auto-check, select the **Auto-check on** option.
To disable Auto-check, select the **Auto-check off** option.
- 7 Click **Apply** to save your settings.

The Auto-check feature has been set accordingly.

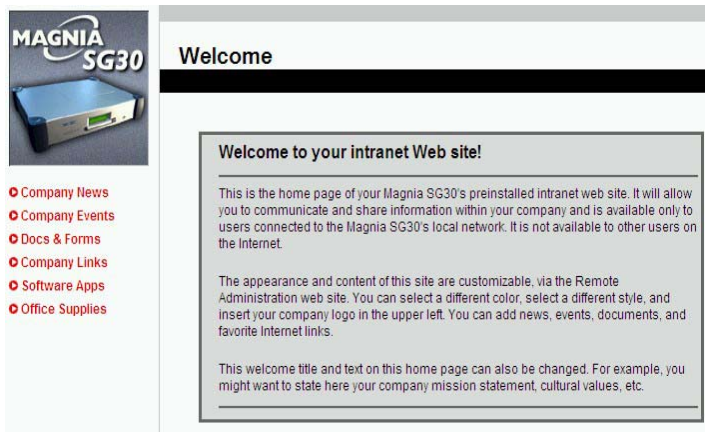
Managing the Intranet site

This section introduces the productivity enhancements Toshiba has built into the preinstalled Intranet on your Magnia SG30 Appliance Server.

Three basic types of features combine to help you manage your work more efficiently. The preinstalled Intranet site, stored on your Magnia SG30, contains a number of pages which let you:

- ❖ Communicate with employees and provide easy access to office resources such as standard documents and forms
- ❖ Gain easy and convenient access to specific Internet sites that offer additional services

You control the appearance and content of these pages.



Sample Preinstalled Intranet as supplied screen

The preinstalled Intranet is viewable by everyone connected to your Magnia SG30 local network. It is not viewable through the Internet by users who are not connected to your local network unless you turned off your firewall. (For more information, see [Internet security and the firewall](#) on page 97.)

Each time you use the Magnia SG30 Setup CD to connect a client computer to your Magnia SG30, an icon labeled Intranet is created on the client computer's desktop. This icon will launch the browser to display the preinstalled Intranet.

Through the Administration Web site you can modify the contents of the preinstalled Intranet and customize its look and feel.



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Select the **Intranet** tab. The Web pages under this tab allow you to control your Intranet.



Sample Intranet Appearance screen

All users with a Level 2 or Level 3 access can view the Intranet tab Web pages and modify the preinstalled Intranet. If you need to keep certain users from being able to modify the Intranet, you must first enable High Security mode for your Magnia SG30. Then change the users' access level to Level 1.

- 1 In the **Local Network** section of the **Network** tab in your Magnia SG30's Administration Web site, make sure that High Security mode is enabled.
- 2 In the **Users** section of the **System** tab, modify the access level in the user accounts.

Level 1 users cannot access the Administration Web site at all but, like other users, they can view the Intranet itself.

No matter how you customize your preinstalled Intranet, it will always have links or buttons to the same set of six pages:

- ❖ Company News
- ❖ Events
- ❖ Documents and Forms
- ❖ Company Links
- ❖ Software Applications
- ❖ Office Supplies

The rest of this chapter discusses how to manage these pages. If you want to develop your own Intranet with a different set of pages, see [Developing an Intranet from scratch](#) on page 230.

Adding your company logo

If your company or organization has a logo, you can display it in the upper-left corner of your preinstalled Intranet. You'll need a version of your logo in any graphic format your browser is able to show. For best results, create a logo that is 140x140 pixels or smaller. Anything larger than this will be cropped so that it will fit properly in the Intranet logo space.

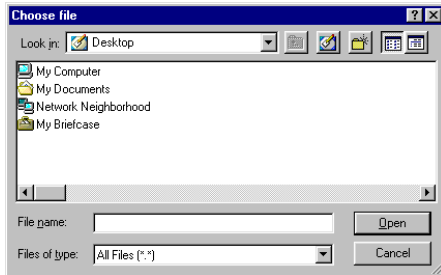
After you have created your logo file, follow these steps to add it to your Intranet.



- 1 From a client computer, click the **Admin** icon to start the Administration Web site.
- 2 Click the **Intranet** tab to view the Appearance page. (Shown above.)

3 Click **Browse...**

A Choose File dialog box appears.



Sample Intranet Appearance - choose file dialog box

4 Navigate to your logo file, select the file and click **Open**.

The Choose File dialog box closes and the path to your company logo will appear in the edit box to the left of the Browse... button.

5 Click **Apply**.

A message box will appear stating that the operation completed successfully.

6 Click **OK**.

Your company logo will appear to the right just as it will on your preinstalled Intranet.

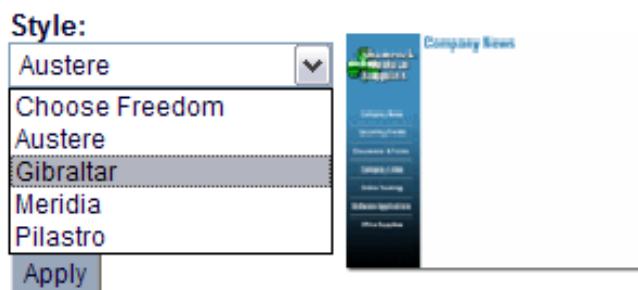
To re-select the original Magnia SG30 logo, browse to your Magnia SG30 using network neighborhood and go to the "intranet" shared folder, and select the file named "companylogo.gif".

Choosing a style and color scheme

Your preinstalled Intranet can take on many appearances. Preview and select the style that best suits you on the Intranet tab's Appearance page.



1 Click the down arrow next to the current style to display a drop-down list of the available styles for your preinstalled Intranet.



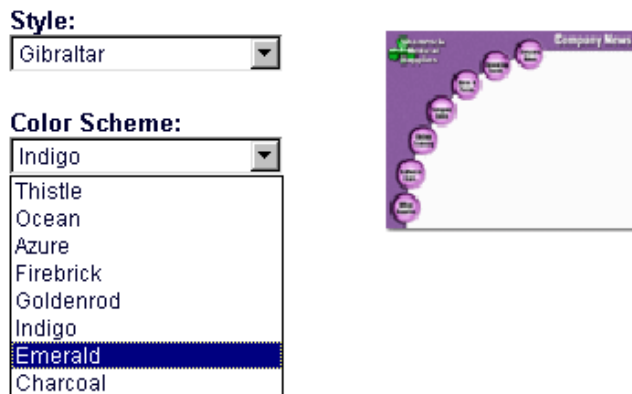
Sample Intranet Appearance - list of Intranet styles

- 2 Select a style and view its thumbnail to the right. Repeat until you find the style you like best.

As you choose a different style, the picture to the right will show you a miniature version of what your preinstalled Intranet will look like.

- 3 Click the down arrow next to the current color scheme to display a drop-down list of available colors for your preinstalled Intranet.

Some styles will have a limited set of colors from which to choose.



Sample Intranet Appearance - list of color schemes

- 4 Select a color and view its effect on the thumbnail to the right. Repeat until you find the color scheme you like best.

As you choose a different color scheme, the picture to the right will show you a miniature version of what your preinstalled Intranet will look like.

- 5 When you have found a style and color scheme that suits you, click **Apply**.

A message box may appear warning you about browser caching anomalies. Sometimes browsers will display the graphics from the previous Intranet style or color scheme.

If you experience this while browsing your Intranet, try the solutions offered on the message box:

- ❖ Click **Refresh** while viewing the Intranet page.
- ❖ Press Ctrl + F5 while viewing the Intranet.
- ❖ Close and restart the browser.
- ❖ Clear the browser's cache, then close and restart the browser.

- 6 Click **OK** on the browser cache warning box.

A message box will appear stating that the operation completed successfully.

7 Click **OK**.

You can now view your preinstalled Intranet's new style! Click the **Intranet** desktop icon from a client computer that was setup using the Magnia SG30 Setup CD.

Adding a welcome message

You can provide your own welcome message on your preinstalled Intranet's homepage.



Sample Intranet Welcome message screen

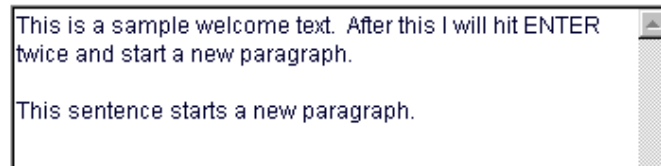
1 Enter your title text in the **Welcome Title** box.

If your title is very long, it will simply wrap on the Intranet homepage.

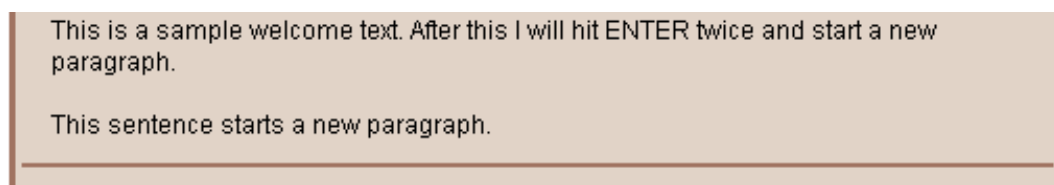
2 Enter your message text in the **Welcome Text** box.

To create a new paragraph on your Intranet's homepage, press Enter twice in a row.

Certain HTML tags are supported. If you know how to use HTML tags, feel free to try them. To create a new paragraph, use the paragraph tag `<p>`.

Welcome Text:

Sample Intranet Welcome - message entry



Sample Intranet Welcome - message display

3 Click **Apply**.

A message box will appear stating that the operation completed successfully.

4 Click **OK**.

You now have a fully customized Intranet homepage. To view it, click the **Intranet** desktop icon from a client computer that was setup using the Magnia SG30 Setup CD.

Managing news items

Your preinstalled Intranet has a Company News page. This page enables you to keep network users informed about current developments, company policy and so on. The items may be of specific interest to the network users, or more general—it's up to you.

You can add, remove, and modify news items on this page of your Intranet.

Start by selecting the **News** page under the **Intranet** tab of the Magnia SG30 Administration Web site.

Adding a news item

1 Click **New**.

A page appears that allows you to create your own news item.



Sample Intranet News - new item entry screen

2 Change the date to whatever date is appropriate for your news item.**3** Type your news headline in the box under **News Title**.**4** Type or paste your news story into the multi-line box under **News Text**.

It's all right if you have more text than will fit this box.

5 Click **Apply**.

A message box will appear stating that the operation completed successfully.

6 Click **OK**.

You now have a news item that will appear on your Intranet's Company News page.

To view it, click the **Intranet** desktop icon from a client computer that was setup using the Magnia SG30 Setup CD.

Modifying a news item

- 1 To modify an existing news item, open the Administration Web site, select the **Intranet** tab, then select **News**.
- 2 Click the title of the news item you want to modify.
- 3 When the edit/entry screen for this news item displays you can change the date, title, or text as necessary.
- 4 Click **Apply**.

A message box appears stating that the operation completed successfully.

- 5 Click **OK**.

Deleting a news item

- 1 To delete an existing news item, open the Administration Web site, select the **Intranet** tab, then select **News**.
- 2 Click the title of the news item you want to delete.

A screen listing all current news items appears.

- 3 Click **Delete**.

A confirmation box appears.

- 4 Click **OK**.

The news item is deleted.

Managing events

Your preinstalled Intranet has a button or link called **Upcoming Events** (or just **Events** for some styles). You can add, remove, and modify events on this page of your Intranet.

Start by going to the **Events** page under the **Intranet** tab of the Magnia SG30 Administration Web site.

Adding an event

- 1 Click **New**.

A page appears that allows you to create your own event notice for your Intranet.



Creating an event

- 2 Change the date for your event.

Today's date appears as the default date.

- 3 Type the title of your event in the box under **Event Title**.

- 4 Type or paste your event information into the multi-line box under **Event Text**.

It's all right if you have more text than will fit in this box.

- 5 Click **Apply**.

The message "Operation completed successfully" appears.

- 6 Click **OK**.

The notice of your event will appear on your Intranet's Events page.



To view the event, click the **Intranet** desktop icon from a client computer that was set up using the Magnia SG30 Setup CD.

Deleting or modifying an event

- 1 To modify or delete an existing event, open the Administration Web site, select the **Intranet** tab, then select **Event**.

- 2 Click the title of the event to modify or delete.

The Events page appears.

- 3 To delete the event, click **Delete**.

A confirmation box appears.

- 4 To modify the event information, change the date, title or text.

- 5 Click **Apply**.

The message “Operation completed successfully” confirms the modification.

- 6 Click **OK**.

Managing documents and forms

Your preinstalled Intranet has a button or link called **Docs & forms**. It opens the Documents page, on which you can store copies of your company’s important documents and forms.

Start by displaying the **Documents** page under the **Intranet** tab of the Magnia SG30 Administration Web site.

Adding a document or form

- 1 Click **New**.

A page appears allowing you to upload your document.

A screenshot of a web form for uploading a document. On the left is a small image of a scanner. To the right, there are several input fields and buttons. The 'Document Title:' field contains 'Expense Report Form'. The 'Current File Name:' field is empty. The 'Upload Document:' field contains 'C:\My Documents\Expe' and has a 'Browse...' button next to it. At the bottom are 'Apply' and 'Cancel' buttons.

Document Title:
Expense Report Form

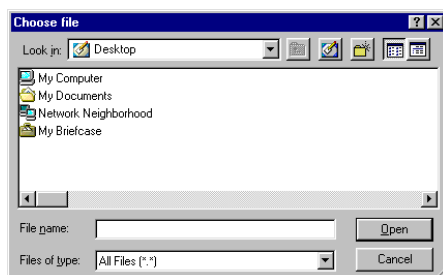
Current File Name:

Upload Document:
C:\My Documents\Expe

An example of a form ready to be uploaded

- 2 Type the document description in the box under **Document Title**.
- 3 Click **Browse...**

A Choose file dialog box appears.



Sample Choose File dialog box

- 4 Using this dialog box, locate the document you want to make available on the Documents page, select the document and click **Open**.

This document can be a text file or form, such as a form created using Microsoft Office, or it can be a PDF (Portable Document Format) file.

The Choose file dialog box closes and the path to your document appears in the edit box to the left of the Browse... button.

- 5 Click **Apply**.

The message "Operation completed successfully" confirms the modification.

A link to your document or form is now available on your Intranet site. Any network user can download this form by clicking on the link.



To download the file, click the **Intranet** desktop icon from a client computer that was set up using the Magnia SG30 Setup CD.

As an alternative, many browsers let users copy the document to their hard disk by right-clicking on the document title link and selecting a menu item that reads something like **Save Target As....**

NOTE

No network users will be able to modify or delete the documents from the preinstalled Intranet. Document attributes (name, etc.) can only be modified and the links deleted from the Documents page using the Magnia SG30 Administration Web site's Intranet tab.

Modifying a document or form

This procedure is for modifying a document or form, changing its title or changing where the Intranet software looks for it on the hard disk.

To modify the contents of a document or form, edit the file using the program you originally used to create it, then re-post the document to the Intranet.

To change the title or re-upload a document:

- 1 Click the title of the document.

The Documents page appears.

- 2 Type a different document title or use **Browse...** to specify a different document location.

- 3 Using the Choose File dialog box, locate the document or form.

- 4 Select the document name and click **Open**.

The Choose File dialog box closes and the path to the document appears in the edit box to the left of the Browse... button.

- 5 Click **Apply**.

The message "Operation completed successfully" confirms the modification.

- 6 Click **OK**.

Your preinstalled Intranet's Documents page now contains the updated information.

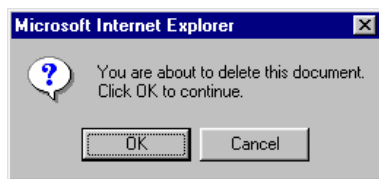
Deleting a document or form

- 1 Select the title of the document or form you want to delete.

The Documents page appears.

- 2 Click **Delete**.

A confirmation box appears.



Sample Document or form - delete confirmation dialog box

- 3 Click **OK**.

The document or form has been deleted from the preinstalled Intranet's Documents page.

Managing company links

Your preinstalled Intranet has a button or link called **Company Links**. You can add, remove, and modify important Web site links using this page of your Intranet.

Start by going to the **Links** page under the **Intranet** tab of the Magnia SG30 Administration Web site.

Adding a link

- 1 Click **New**.

A page appears that allows you to create your own link for your Intranet.



Creating a link

- 2 Type the description of your link in the box under **Link Title**.
- 3 Type or paste the Internet address of the link into the box under **Link URL**.

A Link URL (Uniform Resource Locator) is the standard way of specifying the location of a Web page. You can enter any URL that your browser can interpret (for example, <http://www.toshiba.com> or simply toshiba.com)



HINT: The easiest way to get the Internet address is to open a new browser window and browse to the Web page to which you want to create a link. Once you reach that page, highlight and copy the address from your browser's address box and paste it into the box under the Link URL prompt.



An example of a browser's address box

- 4 Click **Apply**.

A message box will appear stating that the "Operation completed successfully."

- 5 Click **OK**.



You now have a link that will appear on your Intranet's Company Links page. To view it, click the **Intranet** desktop icon from a client computer that was setup using the Magnia SG30 Setup CD.

Modifying a link

- 1 To modify an Intranet link, click the title of the link you want to modify.

An edit URL screen appears.

- 2 Change the title or URL as necessary.

- 3 Click **Apply**.

A message box will appear stating that the operation completed successfully.

- 4 Click **OK**.

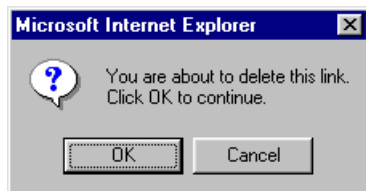
Deleting a link

- 1 Click the title of the link you want to delete.

The following page will appear.

- 2 Click **Delete**.

A confirmation box appears.



Sample delete confirmation box

- 3 Click **OK**.

A message box will appear stating that the operation completed successfully.

Developing an Intranet from scratch

If you've outgrown the preinstalled Intranet or simply want to develop your own Intranet pages, the Magnia SG30 lets you do that. Enter `http://myserver/Intranet/` to direct your browser to a second Intranet Web site that the Magnia SG30 provides for just such a purpose.

The "applianceadmin" account has complete read and write control over the source code for this Web site. Using Network Neighborhood, locate the Intranet share under myserver, which contains the source code for this placeholder page.

Chapter 7

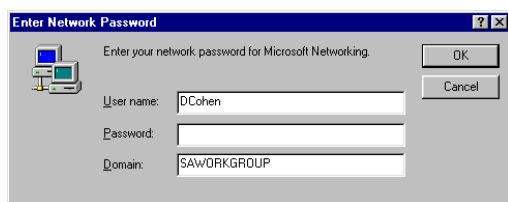
Using the Network

A network is a group of computers connected together so that they can share services such as printers, files, disk space and backup. Your Magnia SG30 provides networking services to all the computers connected through the private Ethernet® LAN ports on its back panel, or through the optional built-in wireless network. These computers are called “clients.”

After your client computer has been connected to the Magnia SG30, it needs to be configured with the Magnia SG30 Setup CD. Your network administrator may do this for you. Then each time you start your computer you can automatically connect to the Magnia SG30. The process of connecting to the server is called “Logging in.”

Logging in to the network

When you start your computer, you will be asked for a user name and password to connect to the server. Both your client computer and the Magnia SG30 check your user name and password entries to make sure that you are an authorized user of the system. Therefore, the user name and password for your client computer must match the user name and password registered with the Magnia SG30 exactly.



Sample login screen

The various Microsoft® Windows® operating systems manage user names differently.

The Microsoft® Windows® 95, Windows® 98, and Windows® Me operating systems each maintain their user names in separate files on the computer's hard disk. They do not have elaborate security, and therefore allow you to cancel the login process by clicking **Cancel** or pressing the **Escape** key on the keyboard. If you cancel the login process on the Windows® 95, 98, or Me operating system, you will have access to the client computer

only, you will not be logged in to the Magnia SG30 and, therefore, will not have use of its resources.

The Windows NT®, Windows® 2000, and Windows® XP operating systems have sophisticated security and user management features. They will not allow you to access the client computer without entering a user name and password.

Types of users

Your Magnia SG30 categorizes user accounts by different types of administrative access permissions, identified by their access (or security) level.

- ❖ Level 1 users cannot use the Administration Web site to configure the Magnia SG30. This access level is only used if your Magnia SG30 is configured in High Security mode.
- ❖ Level 2 users have limited access to the Administration Web site but lack security clearance to change sensitive settings. The Magnia SG30 is preset to Ease-of-Use mode, in which Level 2 is the default security level.
- ❖ Level 3 users have full access to all functions on the Administration Web site. The network administrator is a level 3 user, and is automatically assigned to the first user that is set up on the Magnia SG30.

Notes for systems with Windows NT, Windows 2000 and Windows XP operating systems



TECHNICAL NOTE: If you have a pre-existing network setup, you should consider manually configuring clients.

See “Manually Configuring Clients for the Magnia SG30” on page 61. rather than using the Setup CD.

The Windows NT, Windows 2000, and Windows XP operating systems also have different types of users. This is important because, when you log in to your client computer, you are actually logging in to the Magnia SG30 as well. Furthermore, your user name has a user type associated with it on both the client computer and the Magnia SG30.

Both operating systems have a default user name called “administrator” that has been granted administrator rights and can change sensitive settings.

The Magnia SG30 Setup CD can only be run by a user name that has administrator rights. On Windows 2000 and Windows XP, it creates a user account with administrative rights. On Windows NT, the account created does not have administrative rights.

As a result, your user name and password on your client computer may have administrator rights in the Windows NT/Windows 2000/Windows XP operating systems, but the same user name and password on the Magnia SG30 may not.

Equally, your user name and password may lack administrator rights on your client computer, but have level 3 access rights on the Magnia SG30.

Placing files on the network

When you store data on your local computer, this information is usually stored in files on the computer's hard disk. Later, when you want to work on the information again, you open these files and can modify, print, or use the data. Information stored on your local computer is normally accessible only when you are using your computer.

The Magnia SG30 can act as a central file server, allowing you to save files on the Magnia SG30 instead of your local computer. Saving files on your server can have several advantages:

- ❖ **Extra Storage:** If the hard disk on your local computer is almost full, you can save information to the Magnia SG30. The Magnia SG30's hard disk becomes an extension of your computer, providing extra storage when needed.
- ❖ **Data Backup:** Because the information on your Magnia SG30 is centrally located, copies of everyone's work can be copied to a remote location, such as the Internet. This type of data backup provides an extra sense of security. If something happens to your disk or a file is accidentally deleted, you can retrieve the file from the backup copy. The Magnia SG30 can even act as a backup device itself.
- ❖ **File Sharing:** A public area is provided on the Magnia SG30's hard disk where you can place files that need to be shared with other computers on the network. This "scratch pad" area makes it easy to transfer information between network users.

Each user account created on the Magnia SG30 has its own folder in which to place files. This folder is private, and cannot be viewed by other users (except for the network administrator, who can view any files, including those in private account folders). These folders are named after the user account. For example, the account "jsmith" would have a private folder named "jsmith."

An additional public folder is provided on the server. Anyone can create, modify, or delete files in this folder.

When your client computer is configured for access to the network, the setup wizard automatically creates your account's private folder as a special mapped disk drive. It also

maps a second hard disk drive to the public folder on the Magnia SG30. These drives look just like the C: drive on your computer, but have a different letter.

You can access these drives from your computer using My Computer, Windows Explorer or by browsing any file selection dialog in an application.

If your computer has not been set up using the Magnia SG30 Setup CD, you can still access the files on the Magnia SG30 using Network Neighborhood (or My Network Places). By browsing using this utility, you can see the Magnia SG30 (named "Myserver" as the default name).



Double-click the Myserver icon to show the folders available for access, including your private folder and the public folder.

Storing files on the server

Storing files on the server is easy. Simply copy files from the folder in your local client computer to the Magnia SG30. You can also access these files directly with applications such as word processors, spreadsheets, database applications, and other programs, by simply specifying that the files reside on the private or public drive.

To gain access to the files on the Magnia SG30, you must be logged in to your local client computer, and your login account must match the account established on the Magnia SG30. If you used the setup wizard, these accounts were established automatically. However, if you have multiple user accounts on your client computer, the account you use when you log in determines which files you see on the Magnia SG30.

Sharing files

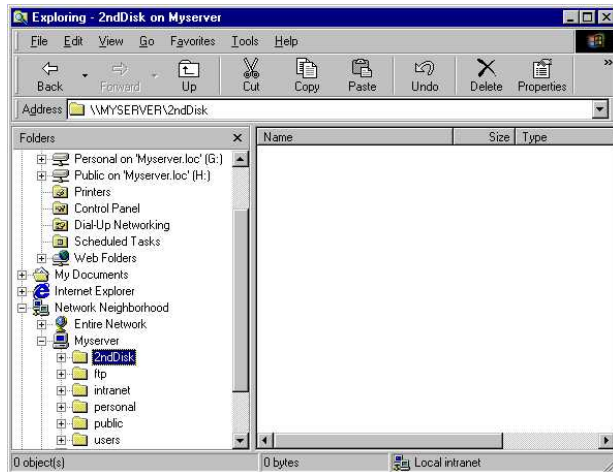
A basic use of the Magnia SG30 is for file sharing. Each client computer connected to the Magnia SG30 can access not only its own hard disk drive(s), but also two special areas on the Magnia SG30's hard disk drive. The two areas are:

- ❖ \public, which is used to store shared files and documents to which all network users have access
- ❖ \personal, which is used to store personal files and documents to which only the individual client computer has access

To view these areas:

- 1 Open the Windows[®] Network Neighborhood folder (or My Network Places folder).

2 Select the Magnia SG30.

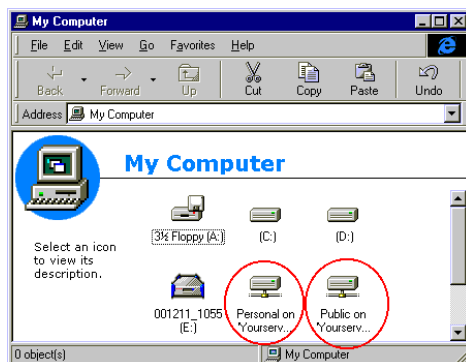


Sample Network Neighborhood window

The default name for the Magnia SG30 is “Myserver.”

3 Locate the \personal and \public drive in your local My Computer folder.

These folders are mapped drives that point to an area on the Magnia SG30.



Sample My Computer window

To map drives to these areas without using the Magnia SG30 Setup CD, follow the instructions based on your operating system.

Mapping drives using the Windows 95 and Windows 98 operating system

- 1 Double-click the **Network Neighborhood** icon on the Desktop.
- 2 In the Network Neighborhood window, double-click the Magnia SG30 icon (usually labeled “Myserver”).
- 3 Click the folder labeled **Personal**.

- 4 From the **File** menu, select **Map Network Drive...**
- 5 Select from the drop-down list the drive letter you wish to map to your personal folder on the Magnia SG30, select the **Reconnect at logon** check box, and click **OK**.
- 6 Repeat steps 3-5 to map the folder labeled **Public**.

Mapping drives using the Windows Me operating system

- 1 Double-click the **My Network Places** icon on the Windows Desktop.
- 2 The Network Places window appears.
- 3 From the **Tools** menu, select **Map Network Drive....**
- 4 In the box labeled **Drive**, select from the drop-down list the letter you wish to map to your personal folder on the Magnia SG30.
- 5 In the box labeled **Path**, type `\\Myserver\personal`.

If the name of your Magnia SG30 has been changed from the default "Myserver," substitute the new name.
- 6 Check the **Reconnect at logon** check box, and click **OK**.
- 7 Repeat steps 1-6 to map the public drive. For the path name type `\\Myserver\public`.

Mapping drives using the Windows NT operating system

- 1 Double-click the **Network Neighborhood** icon on the Desktop.
- 2 In the Network Neighborhood window, double-click the Magnia SG30 icon (usually labeled "Myserver").
- 3 Click the folder labeled **Personal**.
- 4 From the **File** menu, select **Map Network Drive... .**
- 5 Select from the drop-down list the drive letter you wish to map to the personal folder on the Magnia SG30, check the **Reconnect at logon** check box, and click **OK**.
- 6 Repeat steps 1-5 for the folder labeled **Public**.

Mapping drives using the Windows 2000 operating system

- 1 Double-click the **My Network Places** icon on the Desktop.

The Network Places window appears.

- 2 From the **Tools** menu, select **Map Network Drive...**
- 3 In the box labeled **Drive**, select from the drop-down list the letter you wish to map to the personal folder on the Magnia SG30.
- 4 In the box labeled **Path**, type \\Myserver\personal.

If the name of your Magnia SG30 has been changed from the default “Myserver,” substitute the new name.
- 5 Check the **Reconnect at logon** check box, and click **OK**.
- 6 Repeat steps 1-5 to map the public drive. For the path name type \\Myserver\public.

Mapping drives using the Windows XP operating system

- 1 Click **Start**.
- 2 Select **My Computer**.
- 3 From the **Tools** menu, select **Map Network Drive...**
- 4 In the box labeled **Drive**, select from the drop-down list the letter you wish to map to the personal folder on the Magnia SG30.
- 5 In the box labeled **Path**, type \\Myserver\personal.

If the name of your Magnia SG30 has been changed from the default “Myserver,” substitute the new name.
- 6 Check the **Reconnect at logon** check box, and click **OK**.
- 7 Repeat steps 1-5 to map the public drive. For the path name type \\Myserver\public.

Technical information on file sharing

The Magnia SG30 uses the Server Message Block (SMB) file sharing protocol for file sharing services. This protocol is supported by the Windows 95/98 and Windows Me operating systems, as well as by the Windows NT, Windows 2000, and Windows XP operating systems. If you are using an Apple® Macintosh®, you can either configure it to access the Magnia SG30 using AppleTalk or use a commercial product, such as “Dave” to obtain SMB access. For more information about configuring a Macintosh, see [Configuring a Macintosh client](#) on page 78.

The network administrator can set limits on how much disk space a single account can use.

If your Magnia SG30 has a second hard disk drive, your network administrator can make its disk available for general public storage in addition to the private folders established with all accounts. For more information, see [Using the second disk drive](#) on page 200.

Sharing a printer

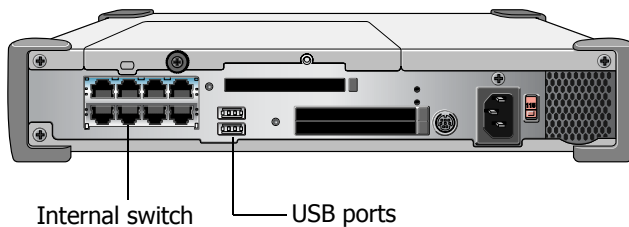
Another important feature of the Magnia SG30 is that it allows all users to share a single network printer. In some cases, the network printer can replace individual printers. In other cases, the network printer is an additional higher-speed and higher-resolution device.

Print jobs sent to this single network printer are stored in a queue on the Magnia SG30 and are processed on a first-come first-served basis. You can even send print jobs to the shared network printer from a remote location when you are connected to the local network through a dial-in or VPN connection.

The Magnia SG30 supports a printer connected directly to its USB printer port, or a network enabled printer connected to your local LAN (connected to the 7 port built-in switch).

Connecting the printer to the Magnia SG30

If you plan to use a printer with a USB connection, the printer must be connected to the printer USB port on the back of the Magnia SG30. If the printer is a network printer supporting a LAN network connection, it should be plugged in to the internal switch. Normally your network administrator does this when setting up the LAN.



Magnia SG30 printer port

NOTE

Make sure the power for the printer is turned on before you attempt to configure the network to use it.

Connecting a client computer to the network printer

Although the screen displays vary slightly between the different Microsoft Windows operating systems, the way you configure the network printer is much the same. You will probably need the device driver diskette or CD that came with the printer, as well as your original Microsoft Windows Setup Disk.

General Windows procedure

Follow these steps to connect your client computer to the Magnia SG30 printer.

- 1 From the Windows **Start** menu, select **Settings**, then **Printers**.

The Printers folder appears on your desktop.

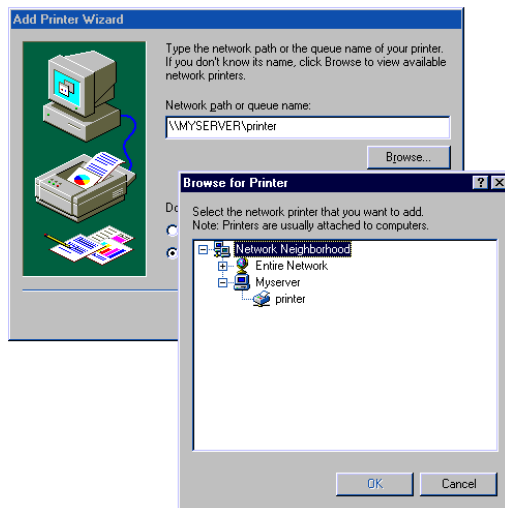
- 2 Double-click the **Add Printer** icon. It should be the first icon displayed.

- 3 When the Add Printer Wizard appears set these options:

❖ For **Is the printer attached to your computer?** select the setting **Network printer**.

❖ For **Network path or queue name**, type \\Myserver\printer.

- If the name of your Magnia SG30 has been changed from the default “Myserver,” substitute the new name.



Sample Add Printer Wizard screen

❖ For **Manufacturer** and **Printer**, select from the lists provided.

- To use your device driver diskette, click **Have Disk**, and follow the directions on screen.

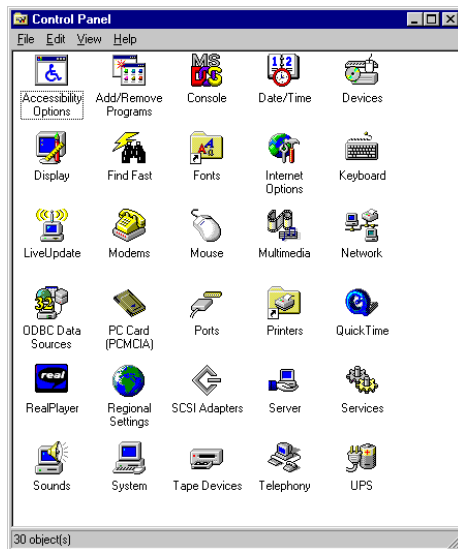
- 4 Print a test page to verify that the printer is configured correctly.

Procedures for the Windows 98 operating system

This example uses the Windows 98 operating system. The process is very similar on other Windows operating systems.

- 1 Click **Start**, **Settings**, then **Control Panel**.

The Control Panel window opens.



Sample Control Panel

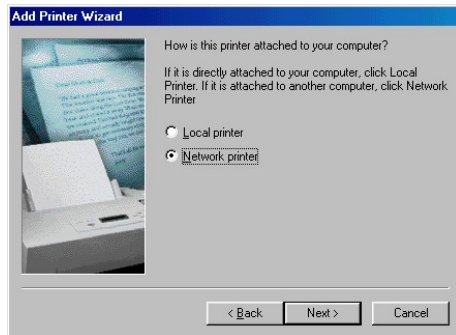
- 2 Double-click **Printers**.

The Printers window opens, listing the network printer and any local printer connected to your computer.



Sample Printers window

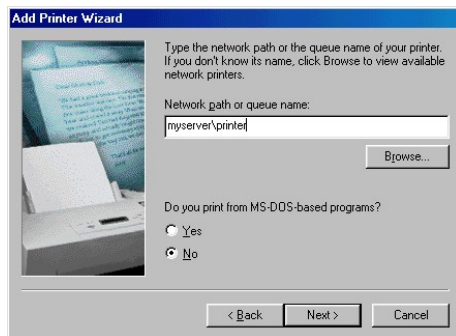
- 3 Double-click the **Add Printer** icon, and select the **Network printer** option.



Sample Add Printer Wizard screen

- 4 Type the name of your Magnia SG30 (the default is “Myserver”) or use **Browse** to find the server and printer.

The name of the shared network printer on the Magnia SG30 is “printer.”



Sample Add Printer Wizard screen

The Windows Add Printer Wizard continues with the printer driver installation process.

- 5 Install the driver on your client computer as you would for any printer connected locally.

Once your client computer has been configured for the printer, you may use the network printer just like any printer connected directly to your computer.

Deleting print jobs from the print queue

Should you send a print job to the network printer by mistake, you can cancel the print job by using the Administration Web site (provided you are a level 2 or 3 user).



- 1 Click the **Admin** icon on your desktop.

The Administration Web site opens.

- 2 Click the **System** tab and the **Printer** page.

The Administration Web site displays the printer information.



Sample printer status screen

- 3 Select the print job(s) to delete, and click **Delete Selected Jobs**.

The selected print job(s) are removed from the printer queue.

Dial-in access

The Magnia SG30 has an optional modem that allows you to log in to the network from remote locations (such as your home) over a phone line—provided your network administrator has enabled this option and granted your user name Dial-In Access privileges.

All the other user name and password rules apply to the remote client computer. This means that the computer you are dialing in from must have the same user name and password as your account on the Magnia SG30.

Once connected by modem, you can do anything that you are able to do when connected locally including accessing public and personal files, printing to the network printer, and making backup copies of your files to the Magnia SG30.

Exploring your intranet site

The Magnia SG30 maintains an internal intranet for the exclusive use of the systems in the local area network. It is not available to outside systems.



To access the Magnia SG30's intranet, click the **Intranet** icon.

The intranet home page opens in your Web browser.

Your company may customize and use the intranet site for whatever purpose it wishes. For more information, see [Managing the Intranet site](#) on page 217.

Chapter 8

Using Email Services

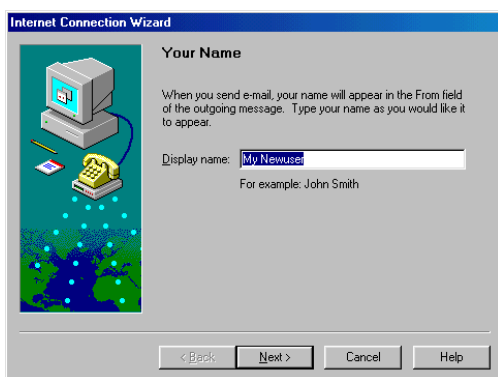
This chapter describes the final setup and use for email services using Magnia SG30 client computers.

Client email setup and use

Once you have set up the Internet email address, the network users need to have their Web browsers configured to read email from that location.

On the client computer, start the Internet Connection Wizard by clicking **Start**, pointing to **Programs**, then **Internet Explorer**, and clicking **Connection Wizard**.

The Internet Connection Wizard dialog box appears. Follow the instructions on screen. After completing each instruction, click **Next** to go to the next screen.

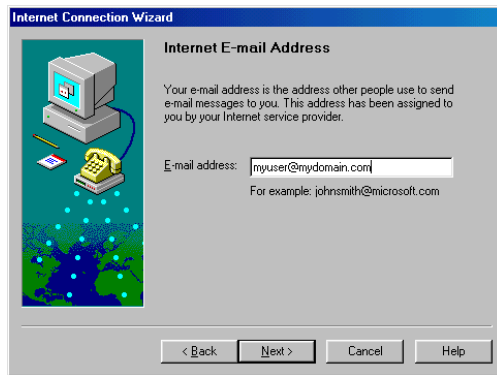


Sample Internet Connection Wizard's Your Name screen

On your Magnia SG30, you select either **Local Mail** or **Local and Internet Mail**. Your Magnia SG30 allows users to send and receive local mail at all times. For more information, see [Setting up the Magnia SG30 for local email](#) on page 109.

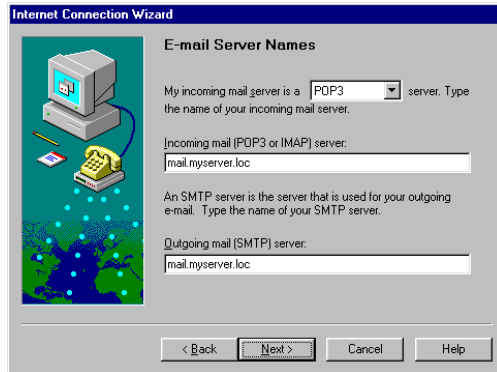
Internet email (domain hosted)

On the Internet E-mail Address screen, enter `username@domainname` where *username* is the name of your account on the ISP mail server and *domainname* identifies your registered domain, such as `mydomain.com`.



Sample Internet Email Address screen

For incoming mail POP3 and outgoing mail SMTP type `mail.servername.loc` where *servername* is the name of the ISP mail server. Your Magnia SG30 will direct all of your outgoing mail to your ISP.



Sample E-mail Server Names screen

NOTE

Some companies that host email domains do not allow you to send email through their mail servers. If this is the case with your email domain hosting service, you can configure your SMTP server name with the name of your ISP's outgoing email server (obtain this server name from your ISP).

User information

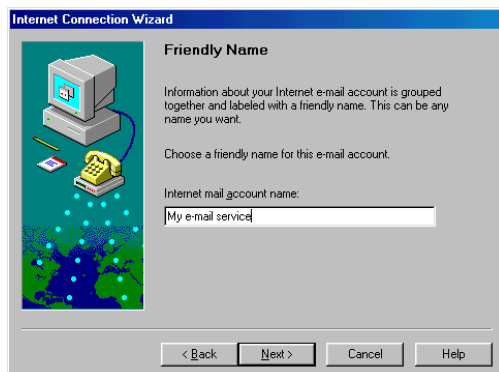
In the Mail Logon screen, enter your user name and password as created on the Magnia SG30. This is all you need to send and receive email.



Sample Internet Mail Logon screen

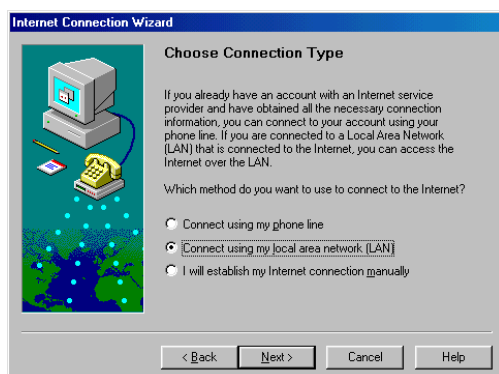
Completing the setup

In the next window, enter a friendly name that identifies the configuration. This name can be anything you like.



Sample Friendly Name screen

On the Choose Connection Type screen, select **Connect using my local area network (LAN)**.



Sample Choose Connection Type screen

A final screen should appear to show you have successfully entered all of the information required to set up your account.

Chapter 9

Using the VPN

This chapter presents how to log on and use the Virtual Private Network (VPN). For information on configuring a VPN, [See “VPN Configuration” on page 121.](#)

Logging On and Using the VPN

When setup is complete, the client will have a new Dial-up Networking icon on the desktop and in the dial up networking window.



Sample Dial-up Networking icon on desktop

To connect to the Magnia SG30 server from the client using VPN:

- 1 Log on to the client computer using the same account information as you use with your Magnia SG30 server.

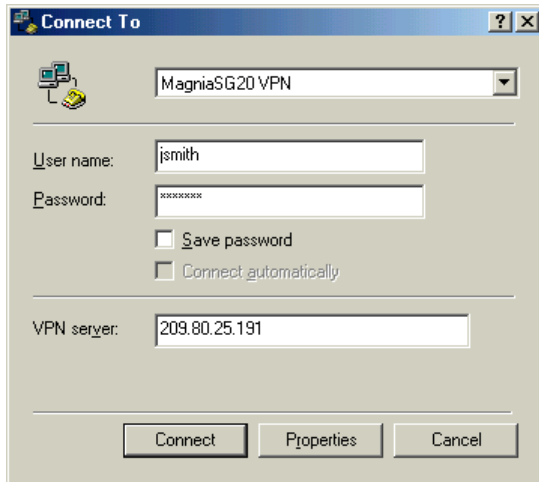


TECHNICAL NOTE: If you are logged on under another account, or if you are not logged on, you may be prompted for an additional log on.

- 2 Open your Web browser and log on to the Internet.

- 3 Once you are logged on to the Internet, double-click the **VPN** icon to establish the VPN connection.

A screen containing your current log on displays.



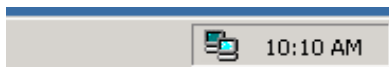
Sample VPN Connect To screen

- 4 Enter your password.
- 5 Click **Connect**.

The VPN connection is established. Once connected, you can access the Magnia SG30 features using the same methods you use on locally connect computers.

Disconnecting VPN

- 1 Double-click the VPN connection icon found in the system tray.



Sample VPN connection icon

- 2 Click **Disconnect**.

VPN is disconnected, but your computer is still connected to the Internet.

Chapter 10

Using Your Digital Central Intranet Site

Your Magnia SG30 includes entertainment and monitoring features to take advantage of its internal storage space.

Specifically, the Magnia SG30 comes with Digital Central, an intranet that provides the capability for:

- ❖ **Digital Photo and Video Album** — organizes your photos and digital movies and makes them accessible from any computer connected to the Magnia SG30.
- ❖ **Digital Music Jukebox** — makes your personal digital music library (in .mp3 and .wma file formats) accessible to all connected computers and potentially to your home stereo system (if you purchase the required additional equipment).
- ❖ **Digital Video Monitoring and Recording** — provides recording and remote viewing capability. With the specified optional camera(s) (purchased separately) you can make your Magnia SG30 a centralized monitoring system that allows you to view household and exterior activity from any computer connected to the Magnia SG30. You can also record activity when you are away for later viewing.

You can also access your Digital Central site from specified wireless devices such as Toshiba wireless notebook computers or properly equipped Pocket PC handhelds. With the wireless network connected computers, you can enjoy your digital music, your photos, or monitor the cameras from wherever the wireless network connection allows.

If you use the Magnia SG30 Setup CD, you'll find a desktop icon titled "Digital Central" that will take you to the Digital Central Intranet site. Without the desktop icon, you can access the Digital Central Intranet site by opening your Web browser and specifying <http://192.168.1.1/digital/> as the address. The following provides detailed information on how to enjoy the Magnia SG30 Digital Central Intranet.

Creating your own photo albums



Digital Central is capable of organizing and displaying your digital photos and digital videos. The advantage of using your Magnia SG30 for storing pictures in a central location is that the pictures are now available to all computers and compatible Pocket PC devices connected to your network. The Virtual Private Network (VPN) software, enables you to share your electronic pictures to remote computers through the Internet.

The photo and digital video album is compatible with Toshiba digital cameras (and most other digital cameras, provided the pictures can be converted to .jpeg/.jpg format). The process of placing pictures on the Magnia SG30 is simple. You copy images to the photo album in the same way as you copy images from your digital camera onto your personal computer. Simply copy or transfer the folder containing the images from your computer to a specific folder on your Magnia SG30. Once there, the images automatically appear on your Digital Central site and are available to your entire network.

This section explains how to:

- ❖ Add photos to the Digital Central photo album
- ❖ View photo albums
- ❖ Change the name of photo albums
- ❖ Remove individual photos and complete photo albums
- ❖ Add/remove digital videos
- ❖ View digital videos

Adding photos to the Digital Central photo album

Before you can add digital photos to your Magnia SG30, the photos (.jpeg/.jpg format only) must exist either on a personal computer that is connected to the Magnia SG30 or on a digital camera that has the capability to copy its photos to a mapped drive on your personal computer. Both of these methods are illustrated below:



Photos on personal computer transferred to Magnia SG30



Photos transferred from digital camera to personal computer, then transferred to Magnia SG30

Both scenarios require that a drive on the personal computer is mapped to the Magnia SG30's public folder dedicated for Digital Central use. A drive was automatically created for you if you used the Magnia SG30 Setup CD to configure your personal computer to connect to the Magnia SG30. If you set up your client computer manually and didn't map the network locations to logical mapped drives, then refer to [Sharing files](#) on page 234.

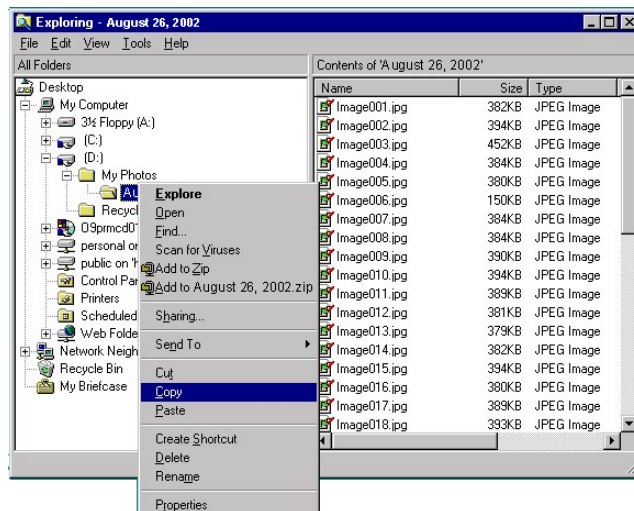
Instructions for both scenarios are given below. Scenario 2 is specific to Toshiba digital cameras but is likely to be very similar for other digital cameras. For more information, refer to your camera's documentation.

Scenario 1: Copying existing digital photos onto your Digital Central site

- 1 Using the file manager application on your personal computer (Windows® Explorer or Macintosh equivalent) locate the folder containing the images that you wish to place on your Digital Central site.

- 2 Right-click the folder.

A submenu appears.



An example of how to copy a folder of photo images from the personal computer

- 3 Select **Copy**.

The folder and its contents are copied to temporary storage.

- 4 Select the drive mapped from your personal computer to your Magnia SG30's public folder during the Magnia SG30 setup process.

This mapped drive should appear in your file manager application with a label similar to: "Public on 'Myserver' G:"

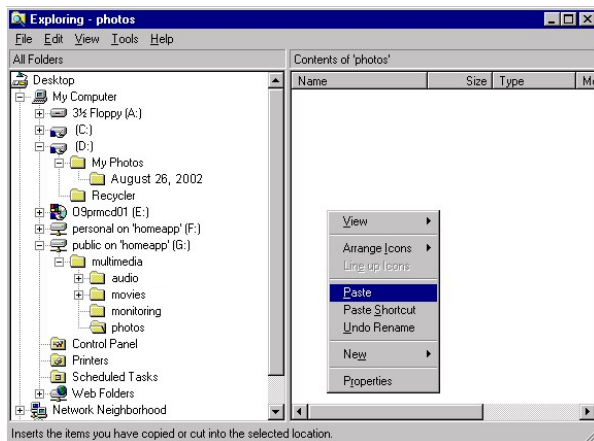
NOTE

If you changed the name of your Magnia SG30 from the default “Myserver” to something else, this mapped drive label will also have changed. In this example, we changed the name “Myserver” to “Homeapp.” Also, this mapped drive may not be “G:.”

Whatever the name or the drive letter, a mapping on your personal computer should exist to the Magnia SG30 and the contents of this mapped folder should have a subfolder “multimedia\photos.” Copy the folders containing the digital photos to this subfolder.

5 Right-click the drive.

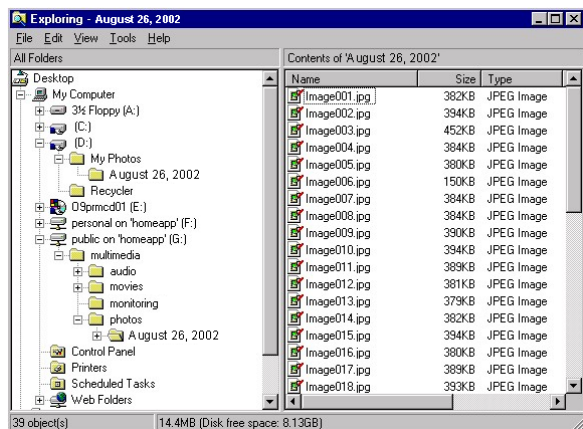
A submenu appears.



An example of how to copy a folder of photo images from the personal computer

6 Select **Paste**.

The folder and its contents are copied from temporary storage into the selected folder.



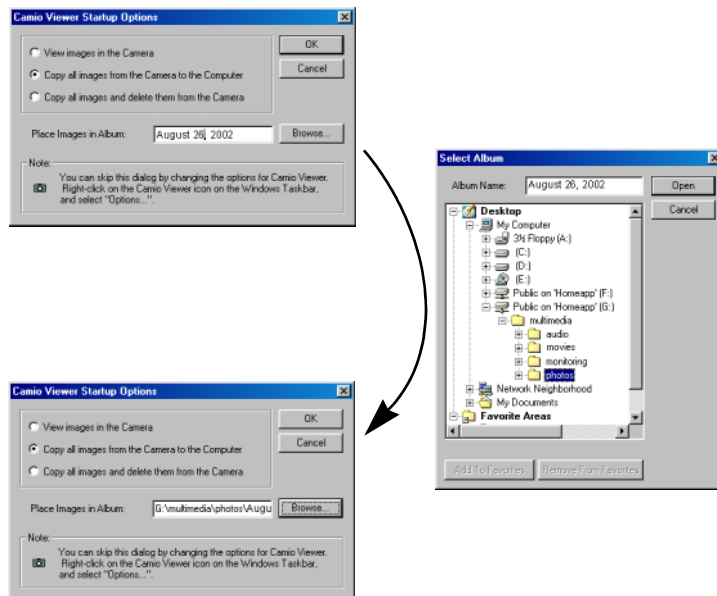
An example of files pasted into a folder

Your photo album is now in the correct place for Digital Central to automatically detect and display it.

Scenario 2: Copying photos from a digital camera to the Magnia SG30 with a personal computer as the interface

Most digital cameras provide software allowing you to copy your photos from your camera to a drive on your computer. This example uses the software that comes with the Toshiba PDR-M70 digital camera. Other cameras will use different software. Please see your digital camera owner's manual for details.

- 1 Connect your digital camera to your PC using the PC synchronization software and hardware that came with the camera.
- 2 If your digital camera software supports naming and placement of the new photo folder, change the default folder placement to the "multimedia\photos" folder on your mapped Magnia SG30 public drive.



An example of how to copy photos from your camera to a drive on your computer

You can now view this photo album within Digital Central from any connected computer or supported Pocket PC device on your network, or you can add more photo albums.

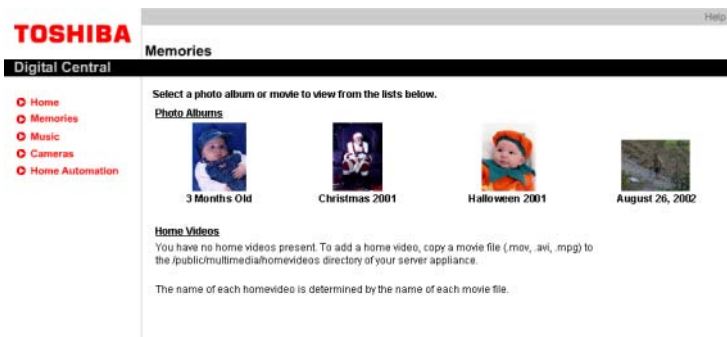
Viewing photo albums

To view a photo album:



- 1 Go to the Digital Central Web site and click the **Memories** main navigation button.

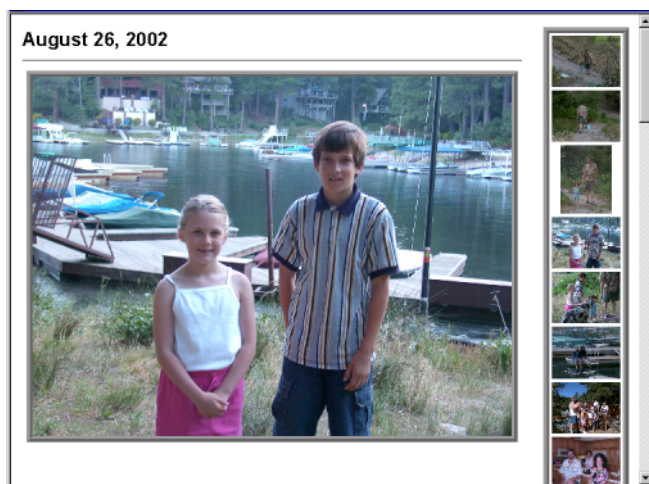
A sample, or thumbnail photo, representing the first photo in each photo album will appear in the main page along with the photo album's title. In the following figure, there are four photo albums available to view:



Sample Digital Central photo album

- 2 Select the photo album you wish to view by clicking the appropriate thumbnail photo.

A new window appears with a large image of that photo in the main frame and the remaining photos within the album listed in thumbnail form down the right side. To view other images within the main frame, click the corresponding thumbnail photo. Photos are listed down the right side in alphabetical order.

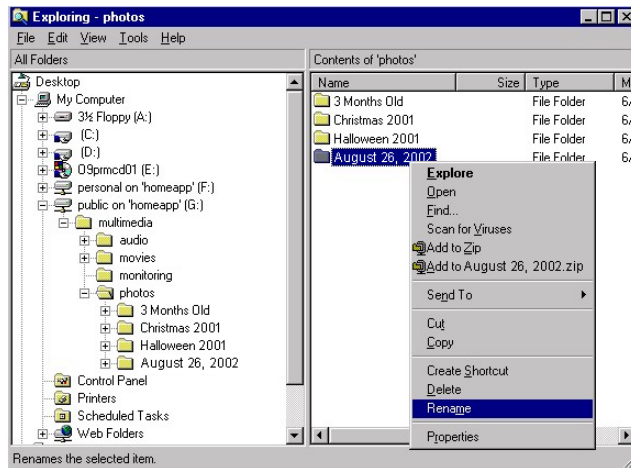


Sample Digital Central photo

Changing the photo album name

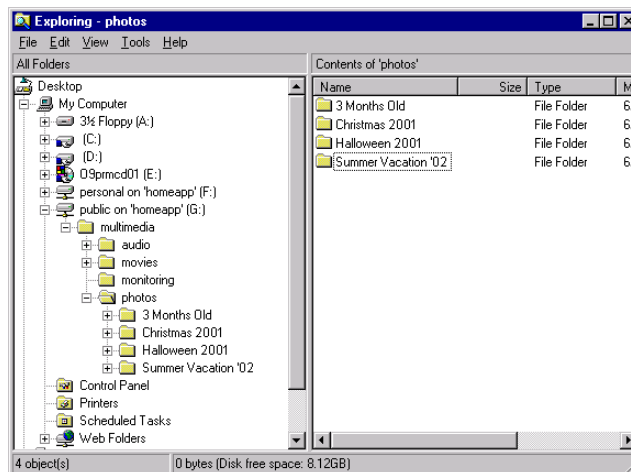
Digital Central uses the file system folder name on the Magnia SG30 for the photo album name. Therefore, change the folder name to change the photo album name.

- 1 Through the file manager application (Windows® Explorer or Macintosh® equivalent), go to the mapped drive containing the multimedia\photos subfolder.
- 2 Right-click the folder for which you wish to change the name and select **Rename**.



An example of selecting the album to rename

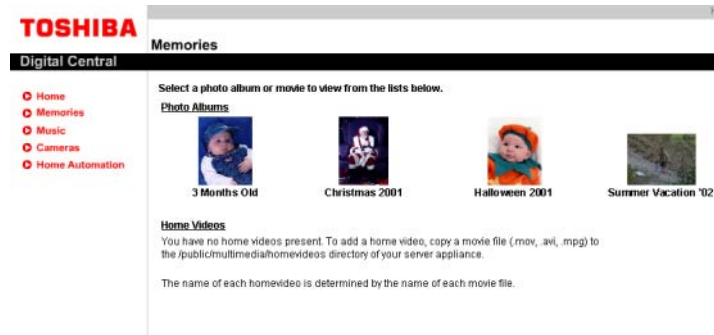
- 3 Type in the new name of the folder and click the mouse to save it.



An example of changing the album name to "Summer Vacation '01"

- 4 To see the changes in Digital Central, click the **Memories** navigation button to refresh the photo album listings.

The changed album name will appear.



Album name changed to "Summer Vacation '01"

Removing individual photos from albums or removing albums entirely

Like renaming photo albums, removing individual photos from a Digital Central photo album or removing entire photo albums requires use of the file manager application on a computer that is connected to the Magnia SG30:

- 1 In the file manager application, go to the mapped drive containing the multimedia\photos subfolder.
- 2 Select the individual file, set of files, or folder you wish to delete.
- 3 Right-click the mouse and select **Delete**.
- 4 To see the changes in Digital Central, click the **Memories** navigation button to refresh the photo album listings.

If you removed a folder from the Magnia SG30 file system, the album will no longer appear on the Digital Central site.

Similarly, if you removed a single photograph from the file system, it will no longer appear in the photo album from which you deleted it.

Adding/removing digital videos

NOTE

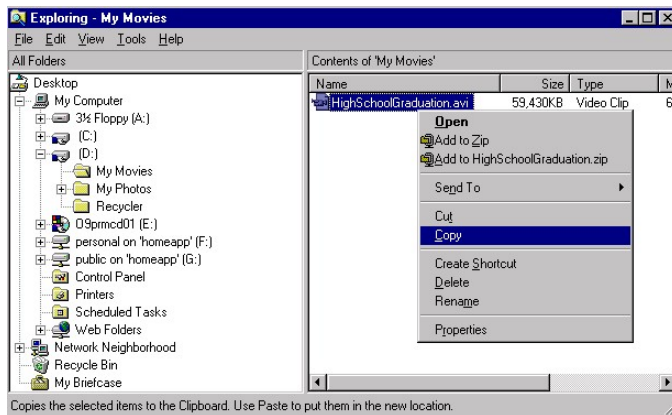
Please observe all copyright laws that you agree to when you purchase any media.

NOTE

The process for adding digital videos to your Magnia SG30 assumes you have the mechanisms in place to copy the video files from your digital video recorder to a personal computer and that this personal computer is connected to the Magnia SG30.

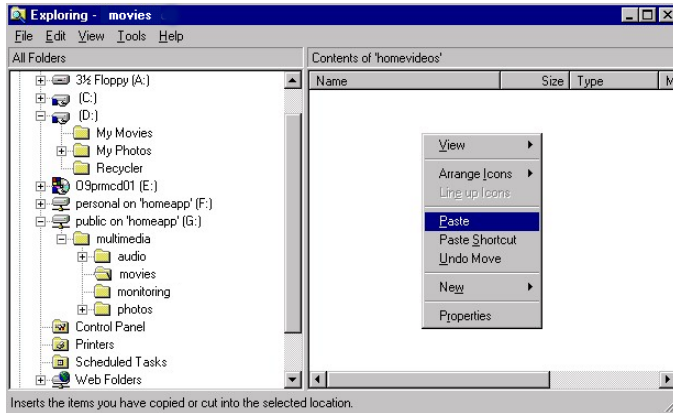
The digital video file must be in .mpeg, .mov or .avi format.

- 1 Using your PC's file manager application, select the digital video file you wish to move to Digital Central, right-click the file and select **Copy**.



An example of copying a video file from a personal computer

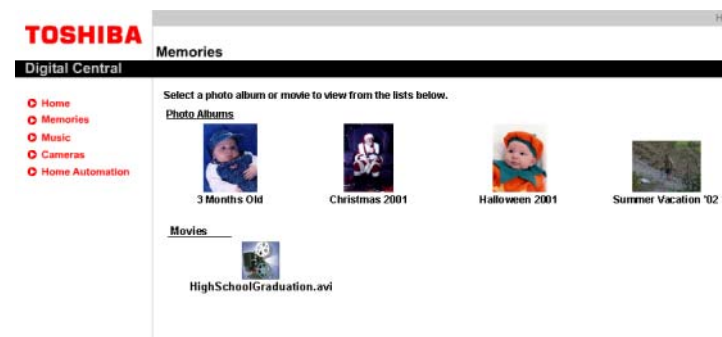
- 2 Locate the drive mapped from your personal computer to your Magnia SG30's public folder during the Magnia SG30 setup process. Go to the folder multimedia/movies and paste the digital video file by right-clicking it and selecting **Paste**.



An example of pasting a video file from a personal computer

The digital video file is now available on the Digital Central site for viewing.

- 3 Click **Memories** to refresh the photo and video album.



Sample video file in Digital Central

To remove any digital video files from Digital Central:

- 1 Use the file manager application to go to the mapped drive on the Magnia SG30 and locate the multimedia/movies folder.
- 2 Right-click the file you wish to delete and select **Delete**.
- 3 Click the **Memories** navigation button in Digital Central.

The file will no longer be listed.

Viewing digital videos

To view digital videos on your personal computer from Digital Central, you need to have the appropriate media player installed. An example of a media player is Real Player,[®]

which is installed to view the videos that are preinstalled on the Magnia SG30. You can install Real Player from the Setup CD. Another example is Microsoft® Windows Media™ Player, which was probably preinstalled by the computer manufacturer. Refer to your digital video recorder help manual and/or your personal computer help manual for details.

- 1 Click the **Memories** navigation button to see a list of available digital videos to choose from.
- 2 Select the video you wish to view by clicking the icon above the name of the video.

If you have the appropriate media player installed on your personal computer, the video will start playing.



Viewing the video file from any computer connected to your Magnia SG30 Appliance Server

Pocket PC support

You may also view your digital photos using a supported handheld device connected to the Magnia SG30 network. Please see [Connecting to Digital Central with a Pocket PC device](#) on page 288 for more details.

Using the digital music jukebox



Your Magnia SG30 via Digital Central includes the capability to store and organize digital music (.mp3 and .wma formats). Your Digital Central site allows your centralized music collection to be played from any wired or wireless connected computer or supported Pocket PC device as well as through a standard audio stereo system (if you have purchased the Voyetra® Turtle Beach® AudioTron™ digital music player or equivalent accessory).

Digital Central digital music jukebox not only centralizes your music to be played on any compatible device or system, but also allows you to create selections of music (called

playlists) from a single album or several different albums. These playlists can be permanently saved for playback later.



Digital Central's versatile digital music capability

The Magnia SG30's central, internal storage allows different playlists to be stored. The efficient network capabilities permit different playlists to be played on the network simultaneously.

This section provides instructions on:

- ❖ Creating digital music in .mp3 or .wma format from your personal music collection (taking care to observe the copyright laws)
- ❖ Making your personal digital music available to your Digital Central site
- ❖ Creating a playlist
- ❖ Changing the play order of a playlist
- ❖ Adding/removing songs from a playlist
- ❖ Creating a playlist to match an entire album
- ❖ Randomizing a playlist order
- ❖ Removing a playlist
- ❖ Playing a playlist from your personal computer
- ❖ Playing a playlist from your home stereo system
- ❖ Playing a playlist from a Pocket PC device

Creating digital music from your personal music collection

There are various third party tools that allow you to create a digital copy of your favorite CDs using your personal computer. These third party tools can create digital music in various formats. The Magnia SG30 supports two of the most popular formats — .mp3 and .wma.

NOTE

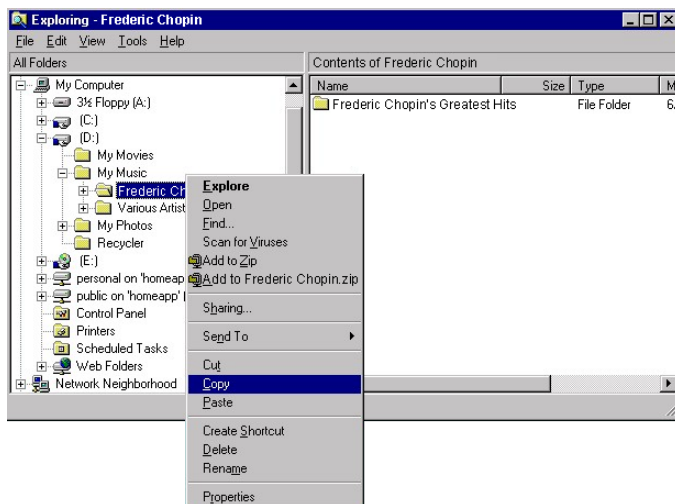
Please observe all copyright laws that you agree to when you purchase any media.

Once you have created copies of your music, you can place these copies in the Magnia's centralized storage to make them accessible over your network. See the next section for details.

Copying your personal digital music to your Digital Central site

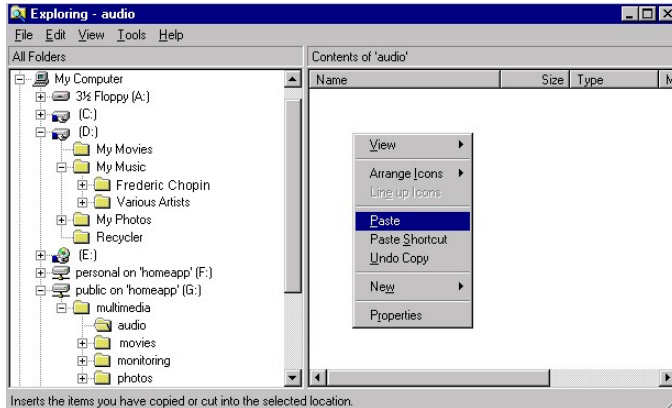
Once you have created or purchased your digital music, you need to copy it to a predefined folder on your Magnia SG30 so that your Digital Central site can access it. The drive containing this folder should be mapped to your personal computer during the Magnia SG30 Setup process.

- 1 In your computer's file manager application (Windows® Explorer or Macintosh equivalent) select the digital music albums you wish to store on the Magnia SG30. Right-click the folders and select **Copy**.



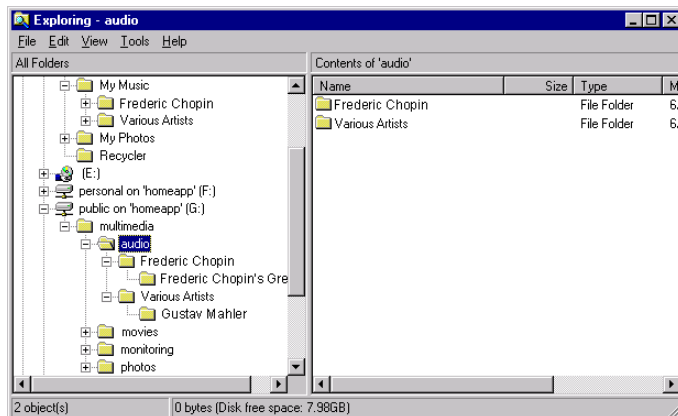
An example of copying music files from a personal computer to your Magnia SG30

- 2 Locate the drive mapped from your personal computer to the Magnia SG30's public folder. Select the subfolder **multimedia\audio**, right-click the mouse and select **Paste**.



All music folders need to be in the 'public\multimedia\audio' folder in the Magnia SG30

- 3 Repeat this process for each album you wish to place in your Digital Central jukebox.



Sample view showing two albums

Your personal digital music is now accessible to Digital Central and you are ready to create your playlists.

Creating a Playlist

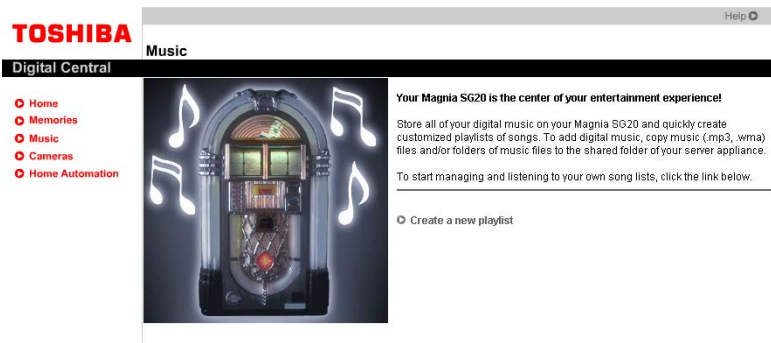
A playlist is a selection of songs from one or more of the personal albums you have available on your Magnia SG30. Once created, these playlists are available to the various devices connected to your network, including your personal computers, home stereo system, and supported Pocket PC devices.

To create a playlist:

- 1 Click the **Music** navigation button in Digital Central.

If you have not created a playlist before, a generic graphic will appear describing your jukebox capability. If you have created a playlist before, a list of existing playlists will appear.

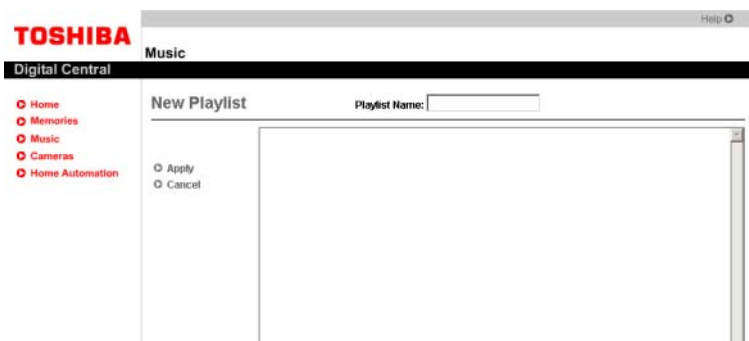
- 2 In either case, click the link **Create a new playlist**.



Creating your own playlist

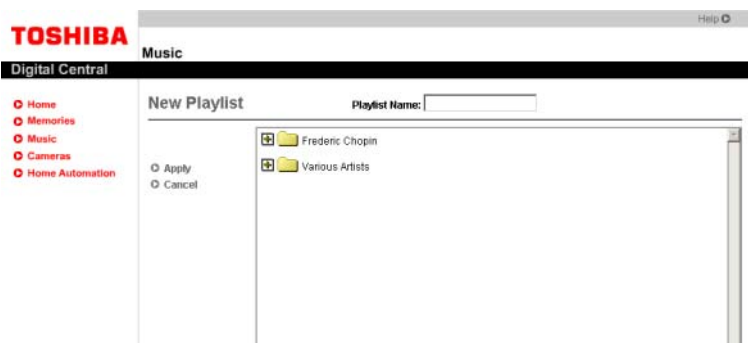
A New Playlist page will appear with a Playlist Name box in the upper-left corner. In the main viewing area, you select the songs you wish to include in the playlist. The left side of the screen provides Apply and Cancel buttons.

If the main viewing area is blank, as shown below, that means there are no digital songs available in your Magnia SG30's \multimedia\audio folder.



An empty main area means there are no songs in your Magnia SG30's 'public\multimedia\audio' folder

- 3 If the main area displays one or more folders, there is music to choose from on your Magnia SG30. Select the folders of interest and then select the various songs you wish to include in the playlist. You may choose an unlimited number of songs as well as an unlimited number of albums.



An example of Digital Central displaying the available digital music

4 Enter the name of this playlist.

This name will appear on all supported and connected devices.



Select songs for your playlist by clicking the CD symbol next to the song

5 Click **Apply** to save your playlist.

The playlist will now appear in the main playlist management screen. If you place your mouse pointer over the playlist name, the list of songs that are in the playlist will appear.



New playlists appear in the Manage Playlist page

Changing the playlist order

The default play order of songs within a saved playlist is alphabetical. You may wish to modify your playlist to your own playlist order. To do this:

- 1 Click the **Music** navigation button in Digital Central and select the playlist for which you wish to change the play order by clicking the check box on the left side of the playlist name.
- 2 Click the **Edit Playlist** button on the left side of the screen.

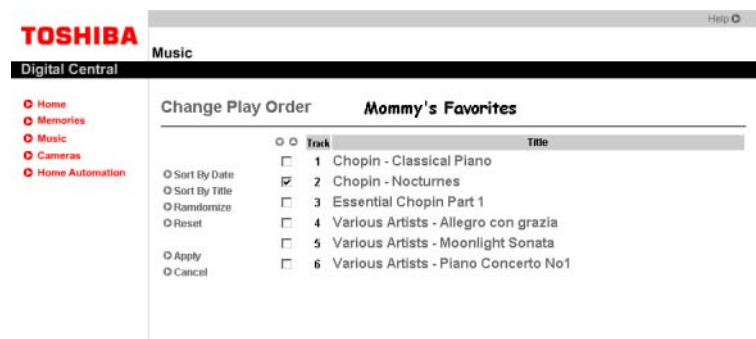


Selected playlist appears in the Edit Playlist page

- 3 Click **Change order of this playlist**.

The list of songs within the playlist will appear with “Sort by Date,” “Sort by Title,” “Randomize,” and “Reset” options on the left side. You may choose to do any of these by clicking the appropriate button.

- 4 To move an individual song or selected songs up or down the playlist order, select the song or songs you wish to move via the check boxes on the left side of the song.
- 5 Click the up or down arrows as appropriate. Repeat this for all songs you wish to move up or down the play order.



The song “A Spoonful of Sugar” was moved up two songs

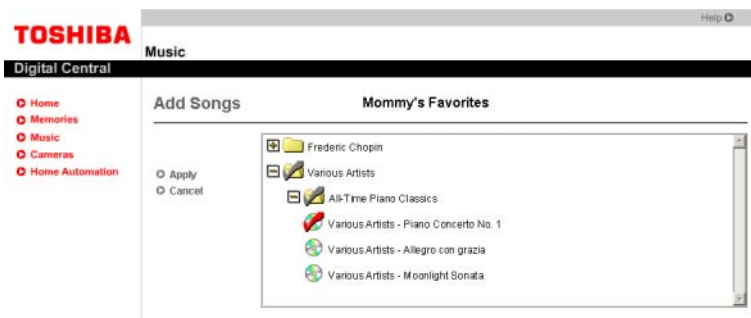
- 6 After the playlist is to your satisfaction, click the **Apply** button on the left side of the screen.

- 7 Click **Ok** to confirm you want to change the playlist order.

Adding/removing songs from a playlist

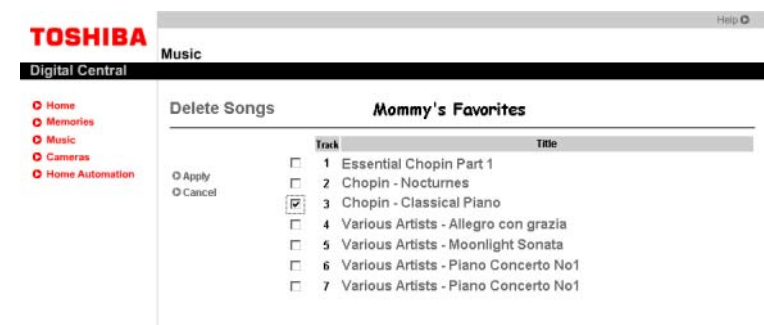
- 1 Click the **Music** navigation button in Digital Central and select the playlist you wish to modify by clicking the check box on the left side of the playlist name.
- 2 Click the **Edit playlist** button on the left side of the screen.
- 3 Click either **Add Song** or **Delete Song** as required.
- 4 If you are adding a song, the Add Songs screen appears. Go through the various folders and select the song or songs you wish to add. When you have finished, click **Apply**.

The songs you selected will be at the end of the playlist order. See [Changing the playlist order](#) on page 265 for instructions on how to move these new songs around in the playlist.



Adding a song to an existing playlist

- 5 If you are deleting a song, the list of songs within the playlist will appear. Select the songs you wish to remove by clicking the check box on the left side of the songs. When you have checked all of the songs you wish to remove, click **Apply** to save these changes.



Removing a song from a playlist

NOTE

Removing songs from playlists doesn't remove the actual songs from your Magnia SG30 \multimedia\audio folder.

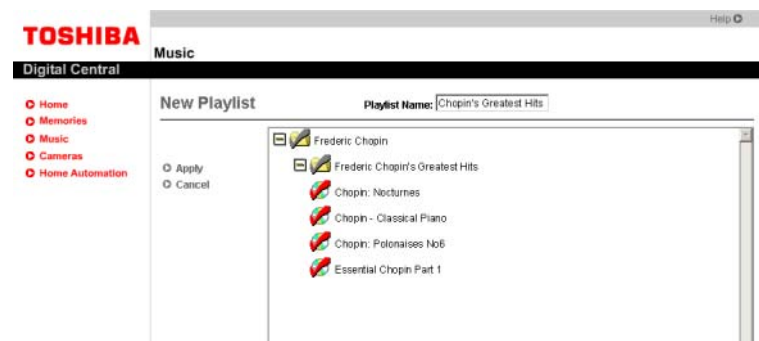
Creating a playlist to match an entire album

You may want to play a digital album in its entirety as it exists on the original CD. Most "ripping" tools, however, save the songs on an album in alphabetical order, not the original order.

Your Digital Central Jukebox remedies this by allowing you to change the order of playlist by date, which simulates the actual song order on your CD since the "ripping" tool you used most likely created the digital copy in order as it appears on the CD and kept the date when the music file was created.

To create a playlist to match an entire album:

- 1 Select **Create a new playlist** in the Manage Playlist page.
- 2 Select an entire album by clicking the folder that matches the album title. You will notice all songs get automatically selected.
- 3 Name the playlist.
- 4 Save the playlist by clicking **Apply**.



Clicking a folder name automatically selects all songs within the album/folder

- 5 Select the newly created playlist by clicking the check box on the left side of the playlist name, and then click **Edit Playlist**.
- 6 Click **Change Order**.
- 7 Click **Sort by Date**.

8 Click **Apply**.

Your new playlist is now in the same song order as the original CD.

Randomizing a playlist

With the randomize feature, you can choose all of your favorite songs and let the Magnia SG30 randomly create a playing order. To do this:

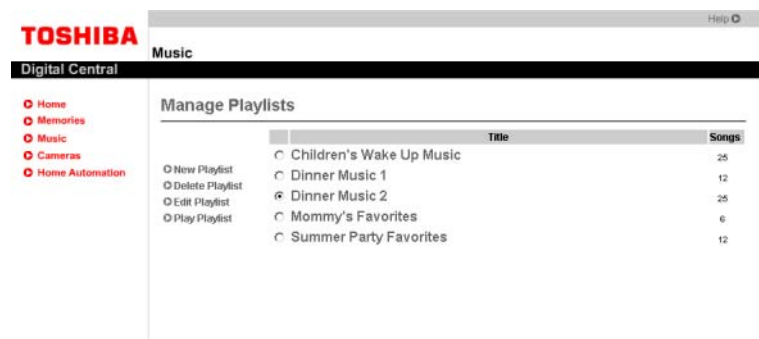
- 1 Select the playlist you wish to randomize by clicking the check box on the left side of the playlist name.
- 2 Click the **Edit Playlist** button on the left side of the screen.
- 3 Click **Change Order**.

The songs within the playlist will appear.

- 4 Click the **Randomize** button on the left side of the list of songs. (You may use this button whenever you want to change the random song order again in the future.)
- 5 Click **Apply** to save the changes.

Removing a playlist

- 1 Go to the **Manage Playlist** page, which is the default page when you click the **Music** navigation button in Digital Central.
- 2 Select the playlist you wish to remove by clicking the check box on the left side of the playlist name.
- 3 Click **Delete**.



Removing a playlist

- 4 Click **Yes** on the confirmation box that pops up.

Playing a playlist from your personal computer

You can play your digital music playlists from most devices that are connected to your network via either a wire or wireless connection. To take advantage of your personal computer's speaker system, the Digital Central playlist will utilize most media players that are installed on your computer's operating system.

To play a playlist in two ways:

Method 1

- 1 Go to the **Manage Playlist** page, which is the default page when you click the **Music** navigation button in Digital Central.
- 2 Select the name of the playlist you wish to play.

The playlist will start to play in your default media player.

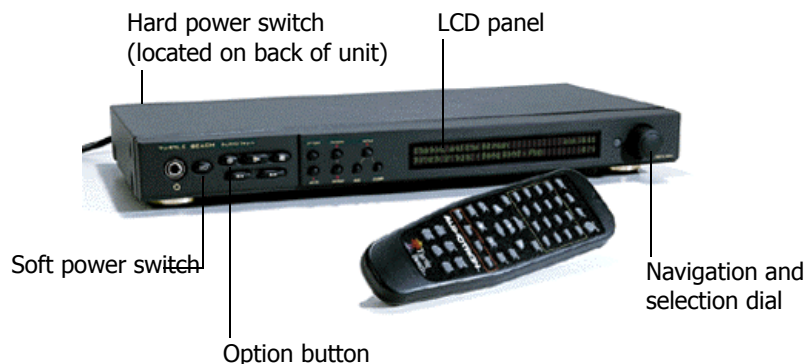
Method 2

- 1 Go to the Manage Playlist page and select the playlist you wish to play by clicking the check box next to the playlist name.
- 2 Click the **Play Playlist** button on the left side of the page.

Playing a playlist on your home stereo system

To play your playlist on your home stereo system, you need an Ethernet-connected digital music player. For example, the AudioTron player, or equivalent player, can be used to deliver .mp3 or .wma music files from your Magnia SG30 to your home stereo system.

Before proceeding to configure your Turtle Beach player to communicate with your SG30 Appliance Server, it is recommended that you familiarize yourself with the components and features of the system as shown below:



AudioTron player that connects Digital Central to your home stereo system



TECHNICAL NOTE: Toshiba has no control over the AudioTron unit. The configuration process may change at any time. The configuration steps documented below are accurate at the time of this publication, but may change in the future.

To connect your AudioTron player to your network:

- 1** Before connecting the Ethernet cable, connect the power cable to a power source, again making sure the unit is not yet connected to the SG30 via the Ethernet cable. After connecting the power cable, press the Hard power switch on the back of the unit (indicated with a "|" on the switch), and then press the Soft power switch until the front panel lights come on.
- 2** Verify the LCD panel reads "Searching for Network" and displays an incremental counter. This counter may continue for up to 120 seconds before stopping the search.
- 3** Turn off DHCP on the unit by first pressing the Options button once. The LCD panel should read "Select Option" on the first line, and "Check for New Music Files?" on the second line. Rotate the Navigation and Selection Dial clockwise until the LCD second line reads "Configure DHCP." Press the Navigation and Selection Dial to select this option.

The first line on the LCD should read "Configure DHCP" and the second line should read "Disable/Enable." Rotate the Navigation and Selection Dial clockwise until "Disable" blinks, and then press the Navigation and Selection Dial. DHCP is now disabled.

- 4** Set the IP address to 192.168.1.252. Make sure the LCD panel first line reads "Select Option". If it does not, press the Options button. Rotate the Navigation and Selection Dial until the second line reads "Configure IP address" and then press the Navigation and Selection Dial.

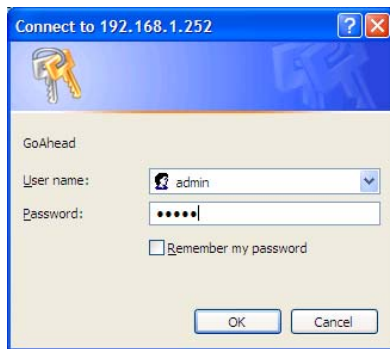
To change the IP Address, rotate the Navigation and Selection Dial until the number you want is displayed on the LCD panel, and then press the Dial to move onto the next number series. The 192 and 168 should already be defined correctly. Simply press the dial until the third number series blinks. Rotate the dial until "1" is selected. Press the dial again to advance to the fourth number series. Once "252" is selected, press the dial again to advance the cursor to "Save." Press the dial once more to save your new IP address.

- 5 Connect the unit to the SG30. Turn off the power using the Hard Power switch on the back of the unit and then connect the Ethernet cable to the AudioTron and the other end to an available port on the SG30. Press the Hard Power switch and then the Soft Power switch to power on the unit.

The unit is now ready for final configuration.

- 6 Next you will set the UserID and Password. The Turtle Beach AudioTron unit comes with a web interface for userID configuration. Using a computer properly connected to the SG30, open your Web browser and type in the URL, **http://192.168.1.252**.

You will be prompted for a password.



Sample password prompt

- 7 Enter **admin** for both the User name and Password, and click **OK**.

The AutoTron Configuration site appears.



Sample AutoTron Configuration site

- 8 Click the **Configuration** link on the left-hand side of the page.

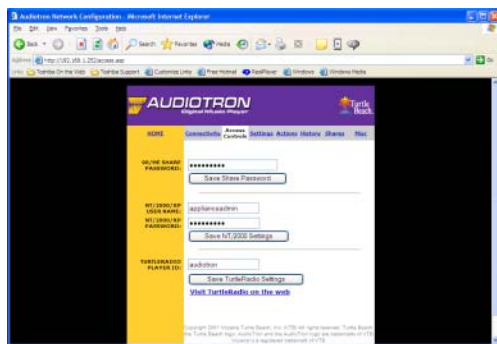
The Default Configuration page appears.



Sample AutoTron Default Configuration page

- 9 Click the **Access Controls** link on the top menu.

The Interface to Change User Name and Password page appears.



Sample AutoTron Change User Name and Password page

- 10 Change the NT/2000/XP user name to **applianceadmin**.
- 11 Change the password to the appropriate password for this SG30 administration account (the default “Toshiba” automatically changes to the password of the first user connected to the SG30). After entering the password, click **Save NT/2000 Setting**.

The unit is now configured to the SG30. To verify the connection, place .mp3 or .wma files in the **public\multimedia\audio** directory (refer to [Using the digital music jukebox](#) on page 259 for details). Turn off the Turtle Beach AudioTron unit and then power it back on using the Hard Power switch, followed by the Soft Power switch. The LCD panel should read “Myserver” and that it has found a number of songs.

Playing a playlist on a Pocket PC device

Wireless Pocket PC devices that use the Microsoft® Pocket PC operating system are capable of connecting to Digital Central, allowing you to play your digital music. The requirements are that the wireless Pocket PC devices use 802.11b as their wireless technology and have Player installed.



TECHNICAL NOTE: Player for PocketPC only plays .wma files and does not support .mp3 format.

For more details on how to play your Digital Central playlists from a Pocket PC device, please see [Accessing digital music with your Pocket PC](#) on page 290.

Using the Monitoring System



Digital Central has the ability to view and record from monitoring video cameras that can be purchased separately. Once the cameras are installed, you can view video from them on any computer within your network, on a remote computer (hotel, work, etc., if you purchase the optional VPN software), or on a wireless Pocket PC device that meets Digital Central's requirements.

This section gives instructions on:

- ❖ Setting up your monitoring system
- ❖ General recording
- ❖ Manual recording
- ❖ Scheduling and managing recordings
- ❖ Stopping a scheduled recording while it is active
- ❖ Removing a scheduled recording
- ❖ Viewing recordings
- ❖ Using the Digital Central recording viewer
- ❖ Saving a scheduled recording before automatic deletion
- ❖ Manually deleting a recording

Setting up your monitoring system

Your Magnia SG30 Digital Central site will initially have no cameras installed. When you click the **Cameras** navigation button, the following screen appears:



An example of Digital Central with no cameras installed

The Magnia SG30 Digital Central site can manage up to four cameras. Toshiba has verified the use of Axis® 2100 cameras, and the Axis® 2400 Video Server.

The Axis 2100 cameras are directly connected to the Magnia SG30 using standard Ethernet cable connected to the Magnia SG30 built-in switch.

The Axis 2400 Video Server is used to connect many standard coaxial cameras to the Magnia SG30 by converting the signal from analog to digital for communication over a standard Ethernet cable to the Magnia SG30 built-in switch.

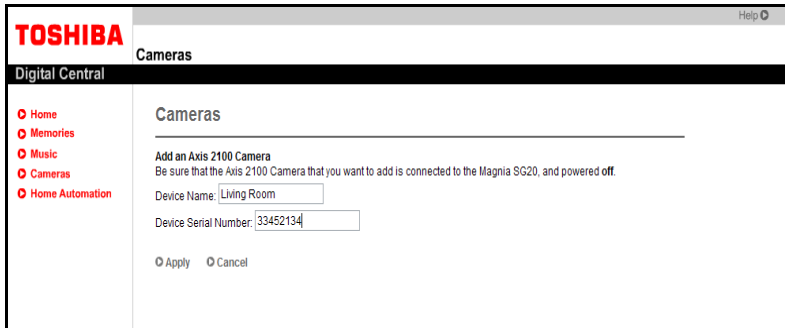
Both Axis camera systems are similar to use and their setup is covered in this chapter.

Setting up Axis 2100 cameras

- 1 Click **Configure Cameras** on the default page in the **Cameras** section.
- 2 Under “Currently Installed Devices” you should see the message “You have no devices configured.” Make sure that the camera is connected via an Ethernet cable to your Magnia SG30 but that the camera is not plugged into any power outlet.
- 3 For the device type, click **2100 Camera>Camera**.
- 4 Click **Apply**.
- 5 Enter the camera name (any name you like — this name will be used as a label for viewing and for recording).

6 Enter the serial number of the Axis 2100 camera.

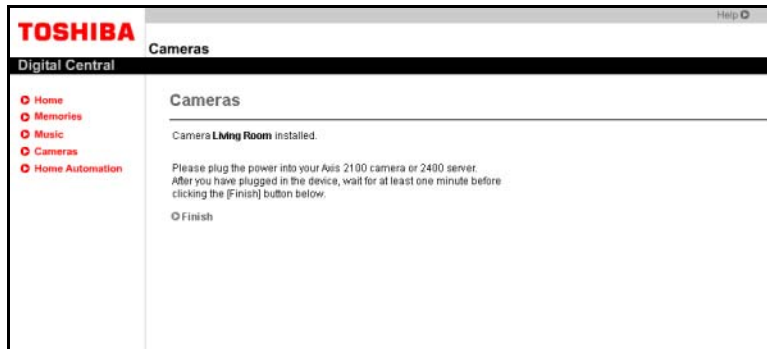
This serial number should be present on the bottom of the camera and labeled Ser. No.



The screenshot shows the Toshiba Digital Central interface. On the left is a navigation menu with options: Home, Memories, Music, Cameras (highlighted), and Home Automation. The main content area is titled 'Cameras' and contains the following text: 'Add an Axis 2100 Camera', 'Be sure that the Axis 2100 Camera that you want to add is connected to the Magnia SG20, and powered off.', 'Device Name: Living Room', and 'Device Serial Number: 33452134'. At the bottom of the main area are 'Apply' and 'Cancel' buttons.

Sample configuration for an Axis 2100 camera

7 Click **Apply** to save.

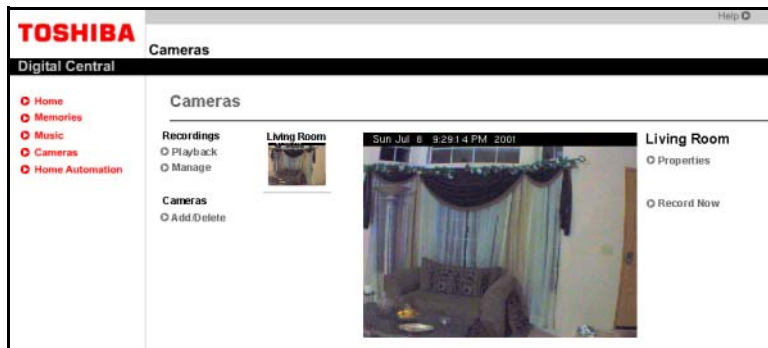


The screenshot shows the same Toshiba Digital Central interface. The main content area now displays a confirmation message: 'Camera Living Room installed.' followed by instructions: 'Please plug the power into your Axis 2100 camera or 2400 server. After you have plugged in the device, wait for at least one minute before clicking the [Finish] button below.' and a 'Finish' button.

Sample message to plug in camera and wait one minute

8 Now plug in the power supply to your camera. Wait for one minute before you click the **Finish** button. Another minute or two may pass while the camera completes its configuration.

Your camera should now be installed with a live main viewing screen and a thumbnail still picture for navigation when two or more cameras are installed.



Sample newly installed camera is now viewable

You may now configure the camera for brightness, color, focus, etc.

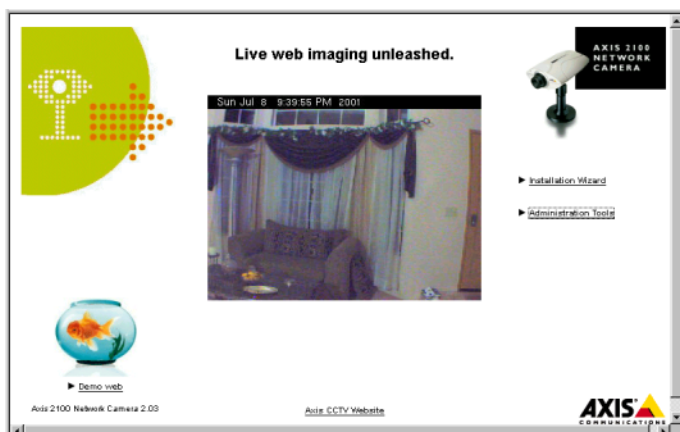
Configuring the Axis 2100 camera

The Axis 2100 camera has manual focus capability as well as the ability to change brightness, color, compression ratio, and more. The manual focus is located on the camera itself and you can access the properties of the camera from the Properties link provided in the right side of the main viewing page. This link goes to the Axis configuration page and is not part of the Digital Central site. To go there:

- 1 Click the **Cameras** main navigation button in Digital Central.
- 2 Bring up the camera you wish to change the properties of by clicking on the thumbnail of the camera.
- 3 Select the **Properties** link.

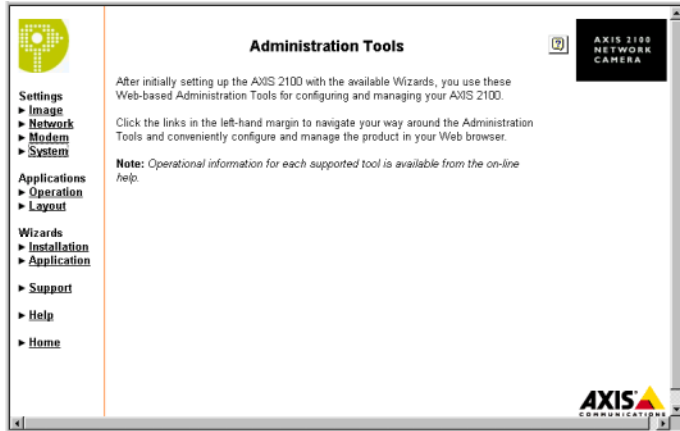
The Axis main Web site for that specific camera will appear.

- 4 Select **Administrative Tools**.



Configuring the Axis 2100 via their administration site

The following administration page is provided by Axis. Use this page to configure the image, set the date/time of the camera, enable the date/time to be displayed on the actual video, etc. Please see the Axis manual for details.

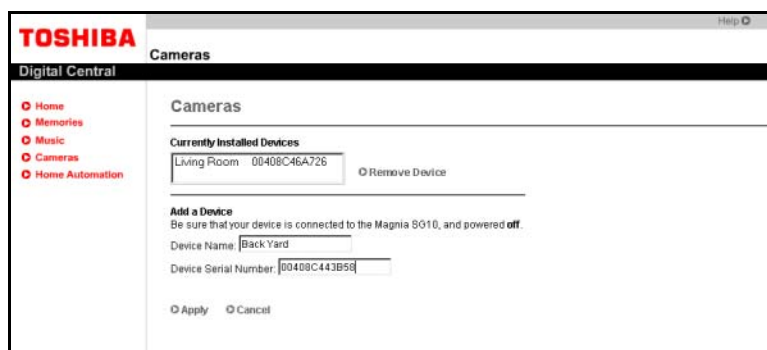


Sample Axis 2100 camera configuration page

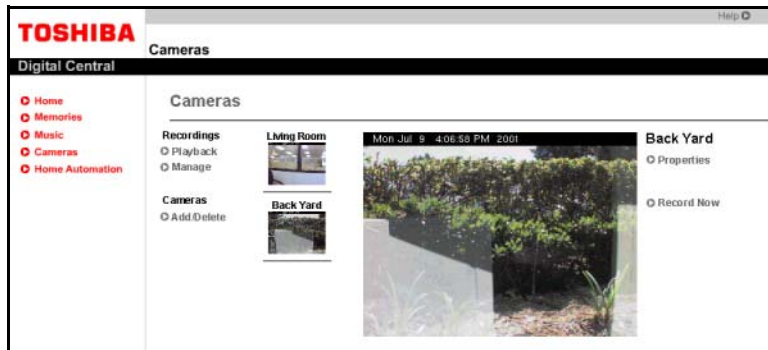
Adding more cameras

Your Digital Central site can have up to four Axis 2100 cameras installed. To add a camera:

- 1 Click Cameras on the Digital Central Web site left menu.
- 2 Click the **Add/Remove** link on the left side of the page.
- 3 Follow the installation instructions for the applicable camera setup described earlier in this chapter.



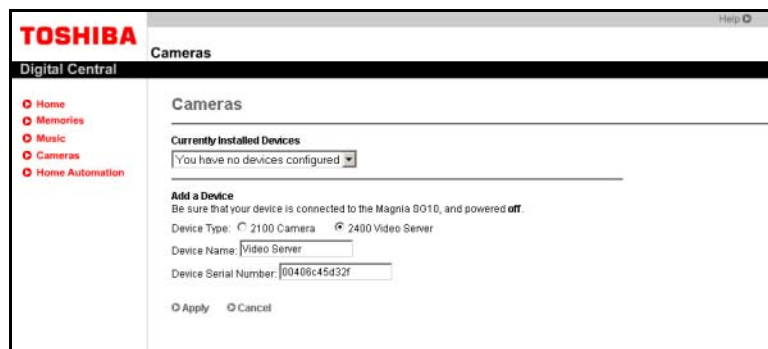
An example of installing additional cameras



Click the new thumbnail picture to view the second installed camera

Setting up your Axis 2400 video server

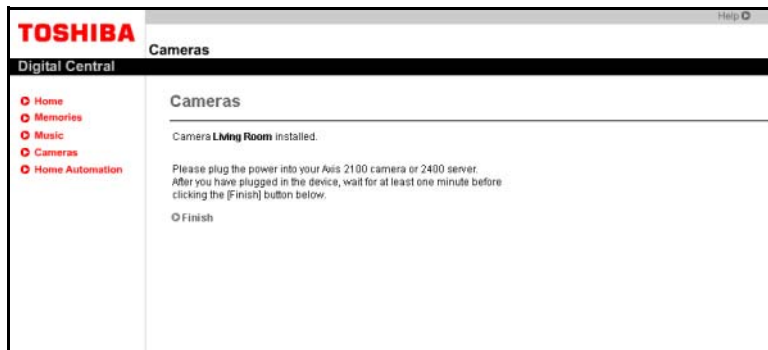
- 1 Make sure the video server's power is turned off.
- 2 Connect the video server's Ethernet cable to an appropriate port on the Magnia SG30.
- 3 Click the **Cameras** link on the Digital Central Web site left menu.
- 4 Click the **Configure Cameras** link on the default page in the Cameras section.
- 5 Select the **Axis 2400 Video Server** as the device type.



Selecting the Axis 2400 video server in the Setup page

- 6 Click **Apply**.
- 7 Type in a name for the video server (this name is used for labeling purposes).
- 8 Type in the serial number of the video server.
- 9 Click **Apply**.

- 10 Plug in the video server to a power supply and wait one minute.

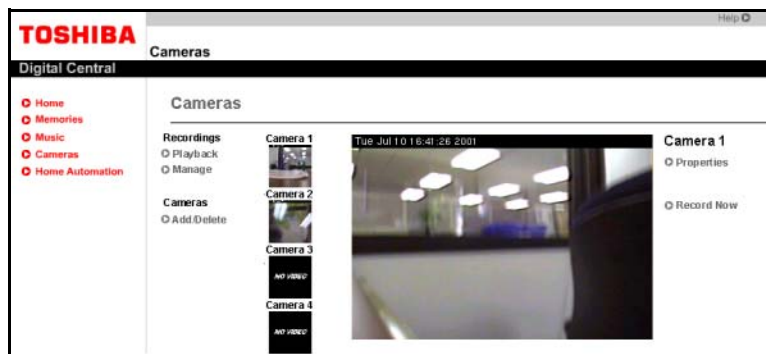


Completing the video server setup

- 11 Click **Finish**.

You can connect a maximum of four cameras to the video server at one time.

Unlike when individual Axis 2100 cameras are installed, the video server will display generic names for the cameras connected to it. In the following example, two cameras have been installed:



Video server successfully installed with two cameras attached

Note the generic “Camera 1,” “Camera 2,” “Camera 3” and “Camera 4” labels. Also note that Camera 3 and Camera 4 are not installed and hence a “No Video” message is displayed.

Configuring your Axis 2400 video server

You can reach the Axis video server administration page by selecting the **Properties** link on the right side of the Digital Central camera viewing page. The administration page is not part of Digital Central but comes from Axis directly. From this page you can make date/time and other generic image settings. You must make camera-specific settings on

each camera individually, since the Axis Video Server can work with almost all types of monitoring camera.



Sample Axis 2400 Video Server administration page

General recording

Your Digital Central site can create digital recordings from your monitoring system. This recording capability includes both manual and scheduled recordings.

Recording works by your camera system creating individual .jpeg images and storing them on your Magnia SG30. Digital Central includes a viewing tool that automatically recreates the video by loading these stored images in the sequence that they were recorded. During playback, you may fast forward, go frame-by-frame, jump to the end, etc.

For both manual and scheduled recordings, you can set various frame rates (how often the video image is updated). The options are full motion, one frame every second, one frame every three seconds, etc. The lower the frame rate, the less storage space the recording requires. For example, if you record at full motion for 10 minutes, the video will require approximately 45 megabytes. If you record for the same 10 minutes but use one frame every three seconds, the video will require only three megabytes. Of course, the video playback will be of higher quality for the full motion rate, but this quality comes at the price of greatly increased storage requirements.

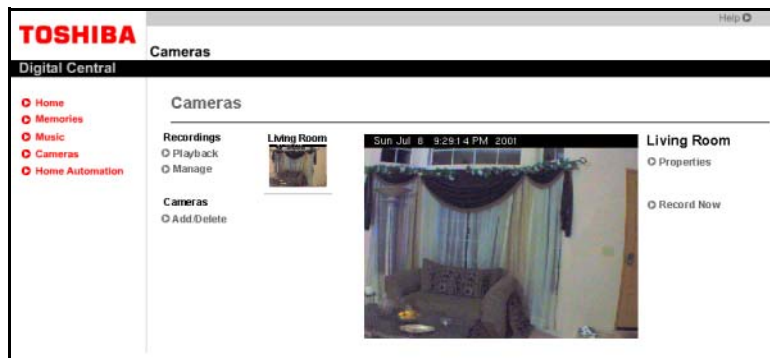


TECHNICAL NOTE: Recordings can consume a considerable amount of disk space on your Magnia SG30. As a precaution, recordings will not start if the disk is over 95% full. Recordings in progress will also monitor remaining disk space and will stop when the disk is approximately 95% full.

Manual recording

To create a manual recording:

- 1 Click the **Cameras** navigation button in Digital Central.
- 2 Select the camera you wish to record from by clicking its thumbnail image on the left side of the main camera page.
- 3 Select the **Record Now** link on the right side of the page.



Creating a manual recording

The Record pop-up window should appear. The file name field is optional. If you don't provide a file name, one will be provided in the format, "7/17/2002 6:24 AM". This name identifies a folder under your appliance server's public share in the folder path multimedia\monitoring\<camera name>\manual\, where <camera name> is the name of your camera. When you provide a recording name, the recording's folder in the manual folder will be named exactly the same as the name you provided. However, when you use the default file name in the format, "7/17/2002 6:24 AM", the folder under your appliance server's public share will look like multimedia\monitoring\<camera name>\manual\1026883492\ (The large number used for the folder name allows the timestamp used for the default recording name to be displayed in the appropriate language format.) The .jpeg files that make up your recording are contained in this folder.

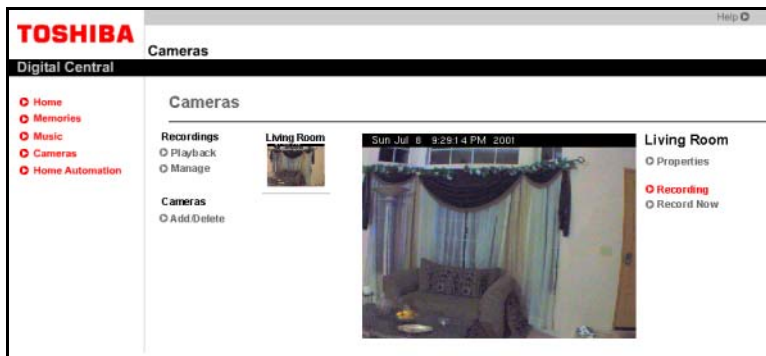
- 4 Select the frame rate for this recording:
Full Motion will give the highest quality recording but also requires the most disk space.
1 Frame Per Second, the default, is preferred for most monitoring situations since it doesn't require much disk space.
1 Frame Every 10 Seconds may meet some monitoring objectives and uses least disk space.

5 Select the duration of the recording.

The maximum is eight hours in manual record mode. If you need 24 hour recording, use the scheduled recording feature under Manage Recordings.

6 Press **Start**.

The manual recording starts and the pop-up window closes. To confirm the recording is actually happening, a red Recording caption appears on the right side of the main viewing window.



A red Recording caption appears during manual recordings

When the recording is completed for the duration that you selected, the Recording caption will NOT automatically disappear. You must refresh the page to get an updated recording status. If you wish to stop a manual recording before your specified duration has elapsed, click the **Stop Recording** caption.

Another method of verifying a recording is active is to go to the Manage Recording page. From here you can manage both manual and scheduled recordings. See the next section for more detail.

Scheduling and managing recordings

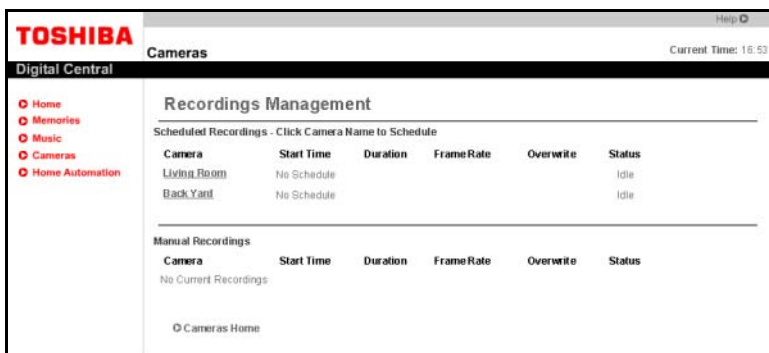
You may schedule a recording for any or all of your installed cameras and manage all recording activity (scheduled and manual) from the Digital Central recording manager. To schedule a camera for recording:

1 Click the **Cameras** navigation button in Digital Central.

2 Select **Manage**, which is on the left side of the page under the label Recordings.

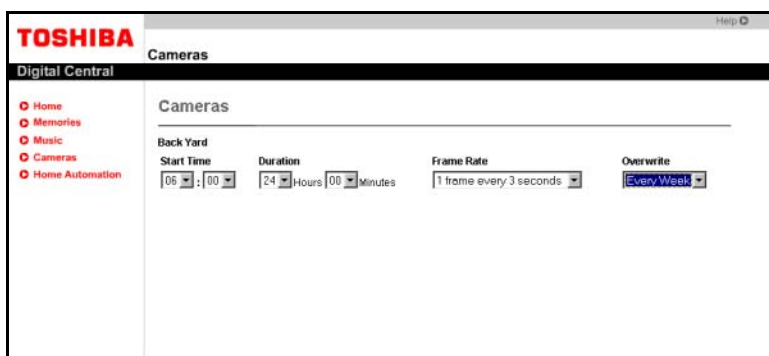
A list of the installed cameras with current schedule information will appear. Any manual recording activity will also be listed.

- 3** Select the camera you wish to schedule a recording from by clicking the name of the camera.



Sample Recording management system

- 4** The start date is the current date and cannot be changed. Select the start time by clicking the hour and minute drop down boxes. A 24-hour clock is used here (for example, 20:00 hours is equivalent to 8:00 p.m.).



Sample of scheduling a recording

- 5** Select the duration.

If you want to record 24 hours per day for every day, simply select 24 hours. If you want the recordings to occur from 8:00 a.m. to 5:00 p.m., select a duration of 9 hours and a start time of 08:00, etc.

- 6** Select the desired frame rate.

For scheduled recordings, full motion is not available. A rate of one frame per second requires 1.3 GB for every 24 hours of recording. A rate of one frame every three seconds requires approximately 430 MB for every 24 hours of recording.

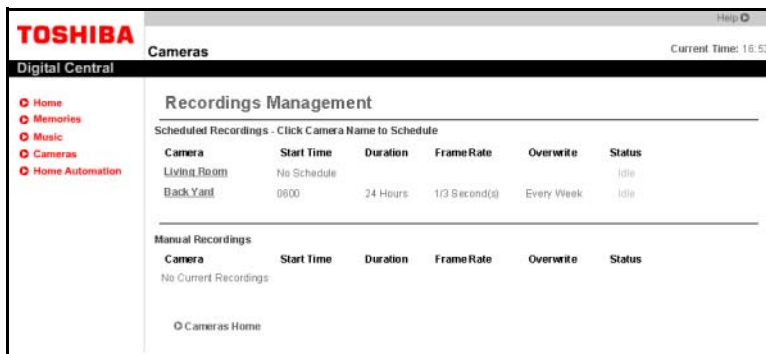
- 7** Select the overwrite frequency.

This can be either every day or every week. If you select every day, you can view the recordings when you come home if you find a need to (for example, something missing, etc.). The recording will automatically be deleted the following day to save

disk space. If you select every week, a recording will be saved for seven days before it is deleted. This will result in much more disk space being used however.

8 Click **Apply**.

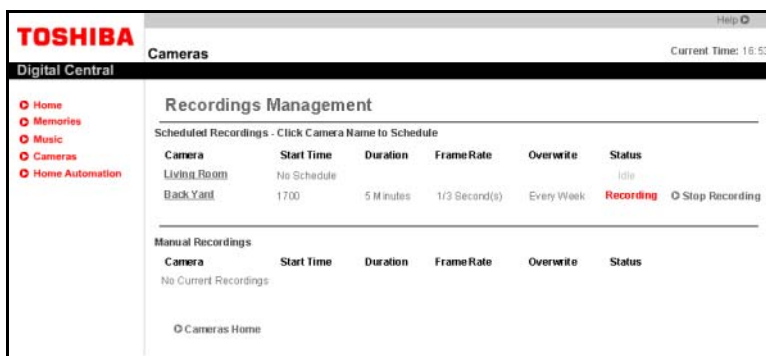
The scheduled recording is now saved. The Recording Management page will display the recording as well as the current status.



Sample scheduled recording and its status

Stopping a scheduled recording while it is active

- 1 Click the **Cameras** navigation button in Digital Central.
- 2 Select the **Manage** link on the left side of the page.
- 3 Go to the active Scheduled Recording and click **Stop Recording**.



Sample of canceling an active scheduled recording

This will only cancel the current recording and the schedule will be resumed the next day. To permanently cancel a scheduled recording, please see the next section.

Removing a scheduled recording

- 1 In the main Cameras page, click the **Manage** link under the Recordings label.
- 2 Select the recording you wish to remove.
- 3 Click the **Remove Recording** button in the lower-right corner.

Viewing recordings

To view manual and/or scheduled recordings, it is best to learn the naming convention used.

Default recording names

The default format is:

Month/Day/Year hours:minutes AM/PM

For example, "7/17/2002 6:24 AM" lets you know the recording started on July 17th, 2002 at 6:24 in the morning. If you browse the appliance server's public share, you'll see a folder named something like "1026883492". This is not very informative, so it's best to view the file system details of the folder, such as the create date or last modified date. This will let you know when the recording was made.

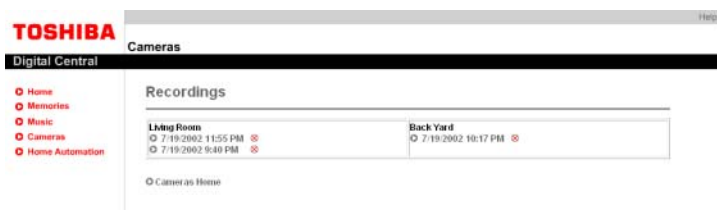
The default name format of a scheduled recording is the same as a manual recording.

Playing back a recording

Knowing the naming convention makes management and viewing of the actual recording much easier. To view a recording:

- 1 Click the **Cameras** navigation button in Digital Central.
- 2 Select the **Playback** link under the Recordings label on the left side of the page.

A list of all available recordings is displayed and grouped by the camera name. In the following example page, there are two manual recordings under the camera "Living Room" and one scheduled recording under the camera "Back Yard."



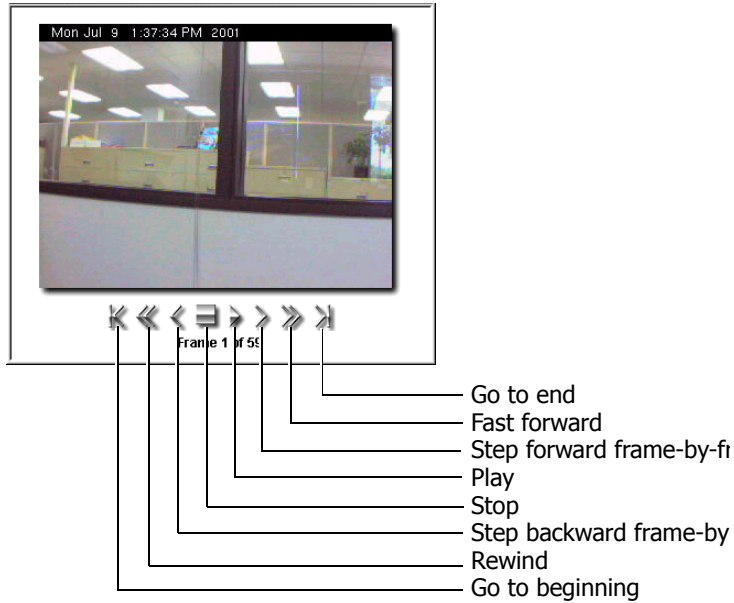
All available recordings are listed

- 3 Select the recording you wish to view by clicking the name of the recording.

The recording will play via the Digital Central site. You may fast forward, rewind, go to the end, go to the front, stop, and step forward and backward through the recording. See the next section for details.

Using the Digital Central recording viewer

The Digital Central recording viewer has the following capabilities:



Sample Digital Central recording viewer

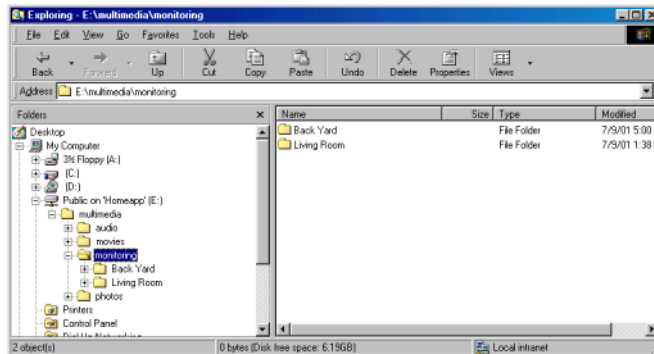
Also displayed on the viewer are the total number of frames and the name of the frame that is being viewed.

Playback on this viewer is in actual time, even though the recorded frame rate may vary from full motion to one frame every 10 seconds.

Saving a scheduled recording before it gets automatically deleted

You may sometimes need to save a scheduled recording for later viewing. To do this, you need to change the folder name of the actual images residing on your Magnia SG30 file system. To access this file system, you need to be a valid user on the Magnia SG30 (which is created via the Setup CD, or can be created via the Magnia SG30 Administration Web site). The Setup CD also creates a drive mapping from your local computer to the public drive of your Magnia SG30. If this has occurred, then:

- 1 In your computer's file manager application, locate the public drive and click through until you select the \multimedia\monitoring folder.

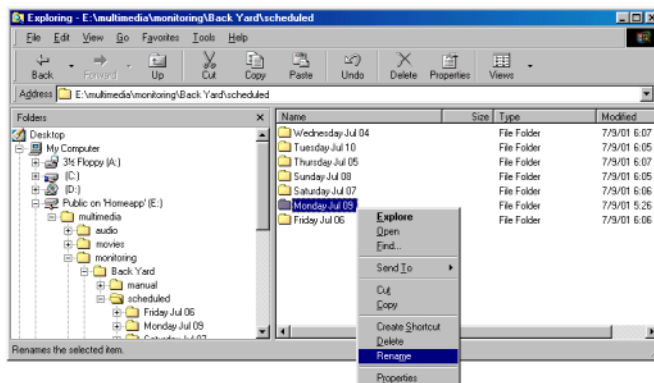


Example of how to access the Magnia SG30 file system

- 2 Double-click the folder name that represents the camera from which you have a scheduled recording that you would like to save.
- 3 Double-click the folder **scheduled**.

You should see a list of folders for the days that have been recorded. In this example, weekly overwrite was used since there are a week's worth of recordings.

- 4 Select the folder you wish to save by right-clicking it.
A submenu appears.
- 5 Select **Rename** from the options.

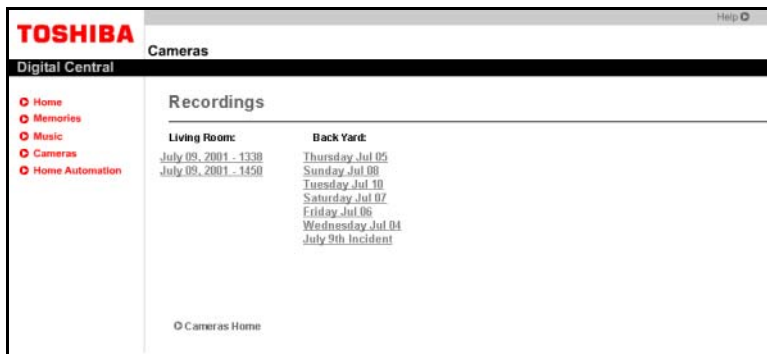


Renaming the folder will protect it from being automatically deleted

6 Type in a new name for this recording.

By changing the name from the default, you are ensuring that Digital Central will not delete it. In this example, we named it “July 9th Incident”.

The renamed recording will still be available via the Digital Central interface and it will not be automatically deleted.



A renamed folder will not be automatically deleted from the system



TECHNICAL NOTE: Recordings can consume a considerable amount of disk space on your Magnia SG30. As a precaution, recordings will not start if the disk is over 95% full. Recordings in progress will also monitor remaining disk space and will stop when the disk is approximately 95% full.

Deleting a recording from the playback listing

To delete a manual or scheduled recording, click the **Playback** link to see the list of current recordings for each camera.

- ✖ Click the delete icon, to the right of the recording you wish to delete.

Connecting to Digital Central with a Pocket PC device

If you have a Pocket PC device that meets the following requirements:

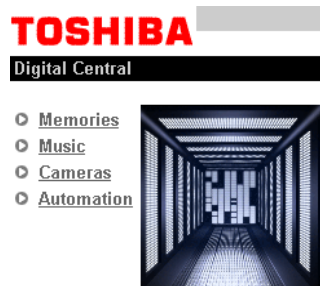
- ❖ Incorporates the Microsoft® PocketPC operating system
- ❖ Has Windows Media™ Player 7.1 or above installed
- ❖ Has 802.11b wireless capability (and the 802.11b wireless access card for your Magnia SG30)

you can use it to access your Digital Central site. In this way, you have mobile access within your home environment not only to the photo album, digital music jukebox, and monitoring cameras, but also to the Internet in general via your Magnia SG30's Internet connection.

Once your Pocket PC device is successfully connected to your Magnia SG30 via the 802.11b wireless interface:

- 1 Tap the Internet Explorer icon on your Pocket PC device.
- 2 Type in the URL <http://192.168.1.1/digital/> and tap **Return**.

A special version of Digital Central that was specifically designed for the Pocket PC interface will appear:



Sample Pocket PC version of Digital Central

From this main page, you can access the majority of Digital Central's features.

Accessing your photo album with your Pocket PC

To access your photo album and view various pictures:

- 1 Tap the **Memories** navigation button on the Pocket PC Digital Central main page.
- 2 Tap the thumbnail image for the folder you wish to view.



Photo albums are represented by thumbnail images

- 3 Once in the folder, view any picture by tapping on its thumbnail image.
- 4 To go back to the Pocket PC Digital Central main page, tap anywhere on the **Digital Central** caption at the top of the screen.

Accessing digital music with your Pocket PC

If you have Windows Media™ Player 7.1 or later installed on your Pocket PC device, you can use it to play your digital music collection (.wma files only). Use a headset for best sound quality.

You can also create new playlists and modify existing ones on your Pocket PC device.

To listen to an existing playlist:

- 1 Tap the **Music** navigation button in the Pocket PC Digital Central main page.



Create a playlist or listen to an existing playlist

- 2 Tap **Manage Playlist**.



Play, edit, or remove a playlist via your Pocket PC

- 3 Tap the playlist you wish to listen to.
- 4 Tap **Play**.

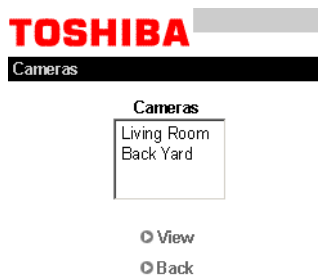
Windows Media™ Player will pop up and start to play your music.

Viewing your monitoring cameras using your Pocket PC

If you installed a monitoring system for your Digital Central site, you can access the images from the cameras using your Pocket PC device. Full-motion playback isn't available on your Pocket PC Digital Central camera site. Instead, the images are updated every three seconds; you will receive clear, wireless snapshot access to your camera monitoring system.

To view images from your Digital Central monitoring system:

- 1 Tap the **Cameras** navigation button on your Pocket PC Digital Central main page.
- 2 Select which camera you would like to view.
- 3 Tap **Play**.



An example of how to access your monitoring cameras from your Pocket PC device

The images from the selected camera will appear on your Pocket PC device.

- 4 Tap the **Back** button to select other cameras installed on your system.

Chapter 11

Advanced Networking Features

The Magnia SG30 is designed to be easy to set up and use in most environments. It configures the system for network use in a way that will meet most requirements small business or home use. Some specific features are set up as the default and should not be changed under normal circumstances. Some of these settings include:

- ❖ Local IP Address Range
- ❖ DHCP server for the local LAN
- ❖ Network Address Translation for shared access to the Internet gateway
- ❖ Changing the server name (appliance name) or workgroup

However, in some networking environments, there may be a need to adjust some of these networking parameters. These adjustments can make the Magnia SG30 work more flexibly and in a wider variety of environments. Such environments may include:

- ❖ Using multiple SG30 systems in a small business network
- ❖ Using the SG30 as a component in a corporate network
- ❖ Using the SG30 as a router / local workgroup server

Making some of these adjustments is recommended only for users experienced in advanced networking techniques. Some of these changes may create situations where your client computers can no longer communicate with the Magnia SG30 using their default networking configuration. You can also create configurations where the Setup CD will not longer be able to create matching client configurations. Use care in making changes as described in this chapter.

⚠ WARNING

Changing networking options and configurations will restart the networking connections to all clients connected to the Magnia SG30. Ongoing work may be interrupted, and data could be lost. To avoid this, reconfigure networking options only when the Magnia SG30 is not being actively used by client computers or for other system operations, such as backups.

NOTE

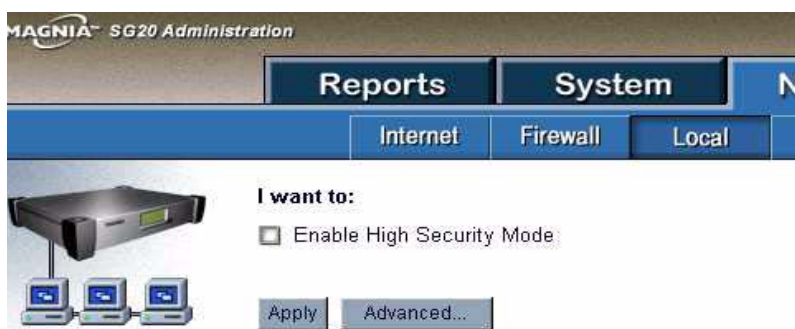
Some Digital Central features (such as camera and MP3 player connections) depend on the default networking setup. Changing settings in this area may effect the ability of these features to operate properly.

Changing the Appliance / Workgroup Name

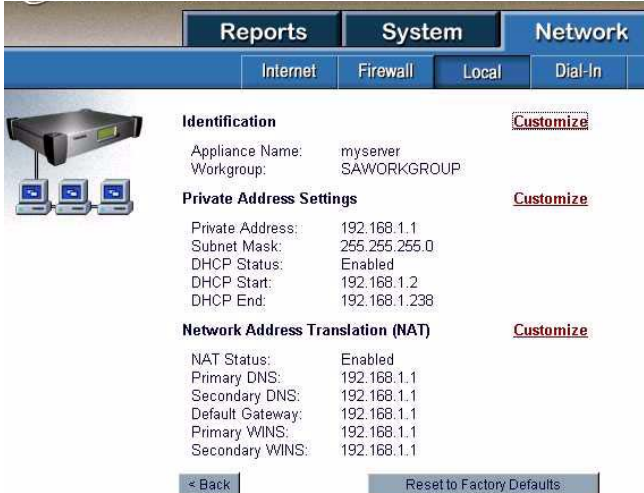
The Magnia SG30 comes preconfigured with the internal server name of “myserver”. This server name is used when accessing the server by browsing the network, or when accessing the server’s Web Administration site or Intranet sites. Changing the server name will allow you to access the server using a different name. This may be necessary when connecting more than one Magnia SG30 to the same network.

To change the server name:

- 1 Go to the Administrative Web site and click on the **Network** tab. Select the **Local** menu item.



- 2 Click on the Advanced button. The screen displayed contains a general status of the advanced networking options



The screenshot shows the 'Network' tab in the Magnia SG20 Administration interface. It contains three main sections: Identification, Private Address Settings, and Network Address Translation (NAT). Each section has a 'Customize' link. The Identification section shows 'Appliance Name: myserver' and 'Workgroup: SAWORKGROUP'. The Private Address Settings section shows 'Private Address: 192.168.1.1', 'Subnet Mask: 255.255.255.0', 'DHCP Status: Enabled', 'DHCP Start: 192.168.1.2', and 'DHCP End: 192.168.1.238'. The Network Address Translation (NAT) section shows 'NAT Status: Enabled', 'Primary DNS: 192.168.1.1', 'Secondary DNS: 192.168.1.1', 'Default Gateway: 192.168.1.1', 'Primary WINS: 192.168.1.1', and 'Secondary WINS: 192.168.1.1'. There are 'Back' and 'Reset to Factory Defaults' buttons at the bottom.

- 3 Click on the **Customize** hyperlink next to the Identification item on the screen. On the next screen, enter the new name and click the **Apply** button.



The screenshot shows the 'Identification' section of the Magnia SG20 Administration interface. It features a warning message: 'Warning: Changing these settings may adversely affect the operation of Digital Central!'. Below the warning are two input fields: 'Appliance Name:' with the value 'myserver' and 'Workgroup:' with the value 'SAWORKGROUP'. There is an 'Apply' button at the bottom.

When you change the appliance name using this method, both the server's computer name and its domain name will be changed. The Magnia SG30 will be accessed by this new name when:

- ❖ Browsing the network
- ❖ Accessing the Administrative Web site
- ❖ Accessing local email addresses

Remember that when you change the appliance name you must also change any links previously established on clients that point to the appliance by name. This includes mapped drives and URL links such as those created by the Setup CD.

The Magnia SG30 workgroup name is preset to SAWORKGROUP. This allows all client computers access to the server and other clients as part of the same networking group and facilitates network browsing.

If necessary, changing the name of the workgroup assigned to the Magnia SG30 can be done using the same method as changing the Appliance Name (see section above). Using the same Identification page of the Advance local networking screen, you can change both the appliance name and the workgroup name.

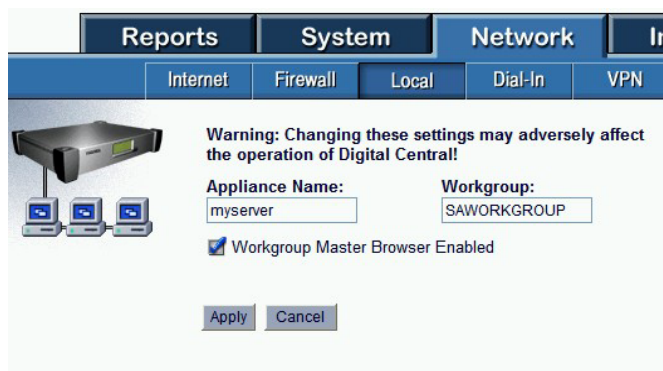
Changing the workgroup name will effect where the server appears on the network neighborhood.

Turning off Workgroup Master Browser

Because the Magnia SG30 is designed to manage its own network out of the box, it is preconfigured to act as the master browser for its private LAN. The server fills all file sharing browsing requests for its workgroup.

If the Magnia SG30 is connected to a corporate network that has its own Windows based servers **and** the workgroup name of the Magnia SG30 is set to the same workgroup as those Windows servers, there may be a conflict that will disrupt network file browsing on clients. In this situation, it may be useful to turn off the master browsing feature of the Magnia SG30.

To turn off the workgroup master browser feature for the Magnia SG30, go to the Administrative Web interface, select the Network tab, and click on the Local menu item. Click on the Advanced button to display the advanced network settings, and then click on the Customize hyperlink next to the Identification area. This screen contains a check box for Workgroup Master Browser, which can be un-checked.



Sample Advanced Network Settings screen

Changing the Local IP Addresses

NOTE

If you change the Private IP address range, then the Administrative screen (at 192.168.1.1:8282) is no longer active. It will be located at the new address as : 8282 The private IP address range cannot match the public WAN port address.

The Magnia SG30 comes with the local network (for client computers connected to the built in switch) set up in the following way:

- ❖ Magnia SG30 local IP is 192.168.1.1
- ❖ DHCP server is on
- ❖ Subnet mask is 255.255.255.0
- ❖ DHCP range is from 192.168.1.2 through 192.168.1.238

These settings can be changed in the following way:

- ❖ A new IP address range can be defined (including a new IP address for the Magnia SG30)
- ❖ A new address can be defined for the local Magnia SG30 port
- ❖ A new subnet can be defined
- ❖ DHCP can be turned on or off (allowing clients to use static IP addresses)

To adjust these settings, go to the Administrative Web site, click on the **Network** tab, and select the **Local** menu option. Click on the **Advanced** button. The screen displaying the current advanced network settings will appear. Click on the **Customize** hyperlink next to the Private Address Settings section.



Reports System **Network**

Internet Firewall Local Dial-up

 Warning: Changing these settings may adversely affect the operation of Digital Central!

Private IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

☒ Enable DHCP Server

DHCP Start Address: 192.168.1.2 DHCP End Address: 192.168.1.238

Apply Cancel

This screen allows you to enter the private IP address for the server (192.168.1.1 by default). You can also change the subnet mask for the current subnet used for the local switch.

Under normal circumstances, the Magnia SG30 local network is managed with a DHCP server, providing DHCP addresses to all clients connected to the built in switch. Typically, this is the best arrangement. However, if the local network needs to be managed with static IPs, disabling the DHCP server can do this.

Disable the DHCP server by unchecking the **Enable DHCP Server** check box.

After modifying the local network settings, click the **Apply** button to apply the new settings.

NOTE

Changing these settings may reset the networking connection between the server and your client. As a result, your client may no longer be connected to the Magnia SG30 after you click the Apply button, and the screen will not refresh to show the new settings. In this case:

1. Click **Start**, then **Run**.
2. Type `Command`.
3. Type `ipconfig /release` and press **Enter**.
4. Type `ipconfig /renew` and press **Enter**.

Turning off Network Address Translation

The Magnia SG30 is preconfigured as a transparent gateway to the Internet. One of its features is the ability to share a single connection to the Internet among all of its local client computers. This is done with the Network Address Translation (NAT) feature. When NAT is turned on (the default setting), the Magnia SG30 combines all Internet transactions using its own public IP address. This allows all the clients on the local network to communicate using the single public IP address assigned to the server. This means the Magnia SG30 requires only a single address for communication with the ISP.

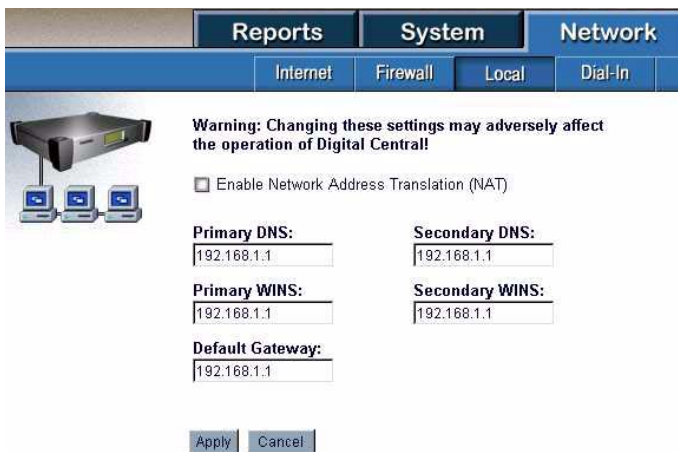
When NAT is on, the local clients are not separately visible to the Internet – systems on the Internet (or a corporate LAN) can only see the Magnia SG30. In some circumstances, such as a corporate network, it may be desirable to have the Magnia SG30 manage its own subnet of IP addresses, which can then be visible to the external (public) network. This is accomplished by turning NAT off.

When NAT is turned off, the Magnia SG30 becomes a router that manages networking traffic between its public and private interfaces. In this case, it is important that the IP addresses assigned to the local clients be part of an assigned subnet compatible with the network connected on the public port. It does not matter whether the private IPs are static or dynamic (DHCP) as long as they are part of a unique, routable address range.

NAT can be turned off when a specific subnet has been assigned for the SG30 as a router, such as:

- ❖ The public port is connected to a business broadband account using cable or DSL and has an assigned set of IP addresses that constitute a subnet.
- ❖ The public port is connected to a corporate network that has allocated a set of IP addresses specifically for the Magnia SG30 private network.

To turn off NAT, go to the administrative web site, click on the **Network** tab, and select the **Local** menu item. Click on the **Advanced** button on the local network screen. When the advanced networking summary page is displayed, click on the **Customize** hyperlink next to the Network Address Translation section.



The screenshot shows the 'Network' tab selected in the top navigation bar. Below it, the 'Local' sub-tab is active. A warning message states: 'Warning: Changing these settings may adversely affect the operation of Digital Central!'. A checkbox labeled 'Enable Network Address Translation (NAT)' is present. Below this, there are five input fields: 'Primary DNS:', 'Secondary DNS:', 'Primary WINS:', 'Secondary WINS:', and 'Default Gateway:'. All five fields contain the IP address '192.168.1.1'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

If NAT is on, the Network Address Translation screen displays only the single check box (it will be checked) to enable or disable the feature. To turn NAT off, uncheck the box. When the box is unchecked, fields to set a variety of IP addresses will appear, including:

- ❖ Primary DNS
- ❖ Primary WINS
- ❖ Default Gateway
- ❖ Secondary DNS
- ❖ Secondary WINS

All these IP addresses must be filled in with appropriate values for the network. The default values set the Magnia SG30 as the server providing these services. These defaults can be retained unless there is a specific alternate server to be used for one of these services.

Configuring Multiple Magnia SG30s on a Single Network

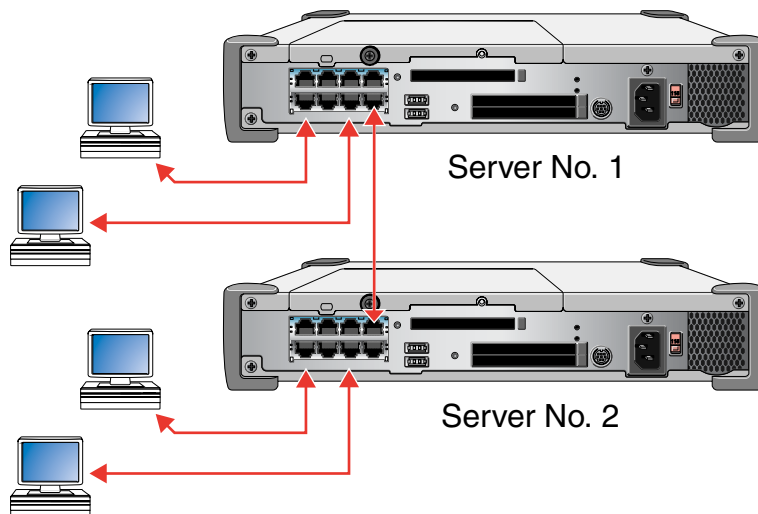
One possible use of the advanced networking options is to allow multiple Magnia SG30s to exist in a single small business network. In this case, all clients require access to both servers, but some server functions may need to be disabled on one of the two servers.

Before connecting the two servers, make the following configuration changes on the servers:

- 1 Turn off DHCP on the second server.
- 2 On the server with DHCP turned on, make sure there are at least two IPs not assigned in the range (for example, start the IP range at 192.168.1.3).
- 3 Assign each server private port an IP from the local IP range. For example, the first server may be 192.168.1.1, and the second one may be 192.168.1.2.
- 4 Change the server name of the second server so the two servers have different names (for example, myserver and myserver2).

The client computers can be connected to either of the built in switches.

Once the servers have been configured, connect them using ports on their built in switches. An example of this configuration is shown below:



Connecting two Magnia SG30 servers using the built-in switch

The two Magnia SG30s are connected using connectors in the built in switch. Care should be taken to connect from the private port on the first system to a private port on the other.

Once set up, the two servers are peers on the same network. The first server will act as the DHCP server for the clients, which will be able to access the two Magnia SG30s by their names (myserver and myserver2) or IP addresses (192.168.1.1 and 192.168.1.2).

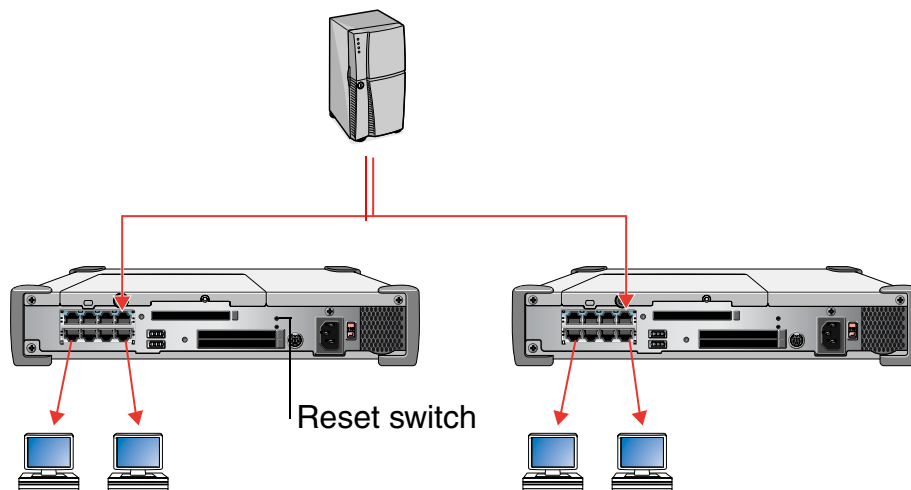
The clients can be configured to access either of the systems as their Internet gateway, email server, DNS server, etc.

Configuring a Magnia SG30 as a Router

It is possible to set up the Magnia SG30 as a router servicing a local subnet. All clients in that subnet look to the Magnia SG30 as their gateway to the corporate LAN. The clients and Magnia SG30 shares could be visible to the other systems in the corporate LAN.

To set up a network in this configuration, a Magnia SG30 is connected to a corporate LAN (or a DSL/Cable connection to the Internet) using the public port. A routable subnet is then configured / purchased for the Magnia SG30. The following configuration steps should be taken:

- 1 Turn NAT off
- 2 A local IP range is established for the private clients (DHCP could remain active).
- 3 An IP from the private subnet is entered for the server private port.
- 4 An IP from corporate LAN is used for the public port (or DHCP can be used)
- 5 Lower the Magnia SG30 firewall only if the Magnia SG30 shares are to be accessed from a corporate network (do not lower firewall if connected directly to the Internet through a connection such as DSL or Cable).
- 6 The subnet IPs is adjusted based on the size of the subnet being routed by the SG30.



Resetting Default Networking Configuration

If you ever need to reset your advanced networking settings back to their default factory released condition, you can do so. Go to the Administrative Web site and click on the

Network tab, then select the Local menu item. On this screen, select the **Advanced** button.

The advanced networking screen has a button labeled Reset to Factory Defaults. By clicking on this button, you will reset the advanced networking configurations to their original defaults.

These include:

- ❖ NAT on
- ❖ DHCP on
- ❖ Local IP address range 192.168.1.2 through 192.168.1.238
- ❖ Server private address 192.168.1.1

NOTE

There is also a reset switch on the back of the SG30 that can be used to return the network settings to their default factory values..

SNMP Support

The Magnia SG30 contains an SNMP management agent that is capable of sending standard SNMP v.2 alerts, and responding to SNMP agent queries with information about the current state of the server. The Simple Network Management Protocol (SNMP) allows remote network management consoles (NMC) to query and set configuration values on a hardware device. This enables network management staff to control and monitor many network devices from a single location. This feature is intended for use in large scale, managed network environments.

SNMP Agent Services

The version of SNMP supported is SNMP v.2c. The Magnia SG30 server appliance has an SNMP Agent that will respond to configuration information queries. The SNMP Agent on the server appliance only supports “Get” requests from the NMC. “Set” requests are not supported. In other words, you can query device settings but not change them through SNMP. To change settings on the Server Appliance, the device’s Administration Website should be used.

SNMP can also alert the NMC when a system problem or specific system state is encountered. This is accomplished through the use of SNMP traps. The SNMP agent will send a message to the NMC when specific criteria are met.

The triggering of SNMP agent traps on the server appliance is tied in to the server’s health monitoring feature. Most of the information available using the Magnia SG30 health monitoring system can be viewed using SNMP. Alerts sent from the Magnia SG30

for health conditions can be sent as SNMP traps. Generating traps is optional and is not required to query configuration information.

When SNMP is enabled, port 161 (or a user-defined port) will automatically be opened in the server appliance's firewall. When SNMP is disabled after being enabled, the port will automatically be closed.

Security Warning

If the server appliance is connected to an external network or the Internet, turning on the SNMP service can expose your machine to internal and external threats if not configured correctly. By default, SNMP is set to “off” and the community string is not set. Enabling SNMP is not recommended unless you are familiar with securing an SNMP enabled machine and/or network, some examples are:

- ❖ The community string should consist of a long string of alphanumeric characters.
- ❖ If SNMP traffic is to be sent outside a secure corporate environment, make sure it is tunneled in a VPN such as IPSec.
- ❖ Blocking Ports 161 and 162 on the corporate external Internet firewall.

Enabling SNMP

To enable the SNMP service, go to the Administrative Web site, and click on the Network tab. Select the SNMP menu item. This displays a screen that allows you to turn the SNMP service on and off.

In addition, the SNMP page contains links to a readme file with online instructions, as well as two MIBs for use with NMCs.

To enable SNMP, select the SNMP On option, and click Apply. Once SNMP has been enabled, it is important to click on the Customize button to configure the remaining SNMP options.

Configuring SNMP

Once SNMP has been turned on, clicking on the Customize hyperlink will present you with a screen with configuration options for the SNMP service.

Simple Network Management Protocol (SNMP) Settings:

SNMP community string:

SNMP Port to use:

Enable Traps: ☐

Trap server community string:

Port to use for SNMP traps:

Address to report traps to:

System location:

System contact:

Below is a description of each of the fields on this screen.

Value	Default	Comments	Required
SNMP Read-Only Community String	No default	This is the community string that the SNMP agent uses. If a request from a Network Management Console is received with this community string, the information will be returned to the requesting console. The first time you enable SNMP you will have to fill in this value.	Yes
SNMP Port to Use	161	This is the port that the SNMP Agent will listen to and respond through. The default is the standard value for SNMP, but it can be changed if the NMC has been customized for a different port.	Yes
Enable Traps	Unchecked	If this box is checked, Traps will be sent to the NMC.	Yes
Port to use for SNMP Traps	162	This is the port at the IP Address that trap messages will be sent to.	If "Enabled Traps" is set, this field is required.
Address to Report Traps To	No default	This is the IP Address that trap messages will be sent to.	If "Enabled Traps" is set, this field is required.

System Location	My Server	Can be used to indicate the location in the network of the Magnia Server. This is a documentary text string.	No
System Description	Toshiba Magnia SG30	Can be used to indicate the function of the server in the network. This is a documentary text string.	No
System Contact	"Not Configured"	Can be used to indicate the person or department responsible for the server. This is a documentary text string.	No

After configuring all SNMP options, click the **Apply** button to save the changes.

If the firewall is enabled when you save your changes, the configured port (161 by default) will be opened in the firewall. When the Magnia SG30 user interface has finished applying your changes, a pop-up message displays.

Disabling SNMP

To disable SNMP services, go to the Administration Web site, click on the **Network** tab, and select the **SNMP** menu item. On this screen, select the SNMP Off option, and click **Apply**.

When you save these changes, the Magnia SG30 will stop the SNMP daemon. If the firewall is enabled, the configured port (161 by default) will be closed in the firewall. When the web server has finished applying your changes, a pop-up message displays.

SNMP Values

The general values supported by the SNMP agent are those defined in SNMP v.2c that defines the protocol and MIB structure elements using the existing SNMP v.1 administration structure. This is the agreed SNMP v.2 standard.

The standard SNMP values that can be queried are grouped as follows:

- ❖ System information: Overall information about the system
- ❖ Interfaces: information about each of the interfaces from the system to a sub network.
- ❖ IP: information related to the implementation and execution experiences of IP on this system.
- ❖ TCP: information related to the implementation and execution experiences of TCP on this system.
- ❖ UDP: information related to the implementation and execution experiences of UDP on this system.

- ❖ DOT3(transmission): information about the transmission schemes and access protocols at each interface.
- ❖ SNMP: information related to the SNMP implementation on the device

Magnia SG30 specific SNMP values are described in more detail in the online readme file. A summary of the values is listed below:

- ❖ Current operational state
- ❖ Timezone
- ❖ Current system language
- ❖ Backup location
- ❖ Type of backup
- ❖ Current security mode
- ❖ WEP enabled status (wireless)
- ❖ Firewall enabled status
- ❖ Pop3 email status
- ❖ Firewall state
- ❖ PPTP enabled status
- ❖ Description of telnet enabled state
- ❖ Gateway enabled state
- ❖ Wireless “Any” access enabled state

Traps that are sent appear as alerts on the Administrative Web interface and LCD panel, and are listed below:

- ❖ CPU Fan Speed
- ❖ System Fan Speed
- ❖ 5 Volt
- ❖ 5 Volt Standby
- ❖ 12 Volt
- ❖ 3 Volt
- ❖ Core Voltage 1 (CPU)
- ❖ Core Voltage 2 (CPU)
- ❖ CPU Temperature
- ❖ System Temperature

- ❖ HDD Full
- ❖ HDD SMART Status

Chapter 12

Advanced Features- Home Automation Interface

Introduction

The Magnia SG30 server appliance is an ideal centralized resource for all home-computing needs. It provides central storage, automatic, built-in networking, wireless access and a central shared gateway to the Internet.

In addition to acting as a central server for your computing needs, the Magnia SG30 can also provide a portal for you to access and control home automation devices such as lights, thermostats and security systems. With the proper home automation equipment configured, you can view the status of your home from any computer connected to your home data network. You can also change the state of most enabled devices, such as turning lights on and off, controlling temperature settings, and turning alarm systems on or off. The Magnia SG30 provides an easy to use connection between your household computers and your home automation devices.

With the Magnia SG30 Home Automation interface, you can allow access to your home automation network to any client computer that can connect to your home data network.

For example:

- ❖ **Local clients:** You can control home automation devices through any client computer connected to your Magnia SG30.
- ❖ **PDAs:** The Magnia SG30 support for PDA access allows you to control your home automation devices through the special PDA interface.
- ❖ **Wireless:** By enabling wireless access, you can roam throughout your home with a notebook computer or wireless PDA and have complete access to your home automation devices.

- ❖ **VPN Access:** When the VPN option is enabled, you can securely access your home network from any Internet connection. This allows unparalleled access and control of your home.

By using your Magnia SG30 Home Automation interface, you are merging your home automation and home data networks, making life easier, more efficient, and even more entertaining.

NOTE

The Magnia SG30 Home Automation Interface supports PDA access. Because of the difference between computer and PDA screen size and features, some screens may appear different than the ones shown in this chapter. However, the general features and abilities remain the same.

The Home Automation Interface described in this section of the manual is designed to work with a third party vendor's Home Automation equipment. If you are interested in obtaining Home Automation features which can be accessed using your Magnia SG30, please contact a dealer / installer of compatible Home Automation equipment.

Setup/Configuration

The Magnia SG30 Home Automation subsystem is designed to be connected to an existing home automation installation. It is assumed that the Home Automation controller and all automated devices are already installed and operational at the time the Magnia SG30 is set up to communicate with the Home Automation controller. Typically, a professional installer would perform this installation and setup.

Once the Home Automation system is installed and running, the Magnia SG30 can be connected to the controller, to allow activation and configuration of the Magnia SG30 Home Automation interface.

The Magnia SG30 does not actually control home automation devices, but rather communicates with existing home automation controllers (for example, when you use the digital central interface to turn a light on, the SG30 sends the "light on" command to the currently installed home controller, which in turn will turn the light on.) The SG30 currently supports a number of home controllers, including the following:

- ❖ JDS Stargate Lite
- ❖ JDS Time Commander Plus
- ❖ JDS Comit
- ❖ JDS Comit Star

The Magnia SG30 Home Automation interface supports a wide variety of the most common automation devices. Specific supported devices appear in selection menus as

you configure the system. Other devices may be used, as long as they are 100% compatible with a device listed in one of the configuration menus. Devices supported include:

- ❖ RCS RS485 Thermostats
- ❖ Caddox NX8e Security Panel
- ❖ Leviton 2 way lamp module
- ❖ LCD Multi-menu key pad
- ❖ JDS Infrared Xpander

Be sure to check the user interface for a complete list of supported devices, as this may change with software updates.

Once your Home Automation controller and devices are installed and configured, some configuration of the Magnia SG30 is required. This configuration will tell the Magnia SG30 what type of controller and what devices you have. Check with your installer to see if this has been configured.

The Magnia SG30 assumes that the home controller and devices are already installed and configured (since the SG30 simply provides an extension to the interface to the home controller unit, such as a wireless notebook or PDA).

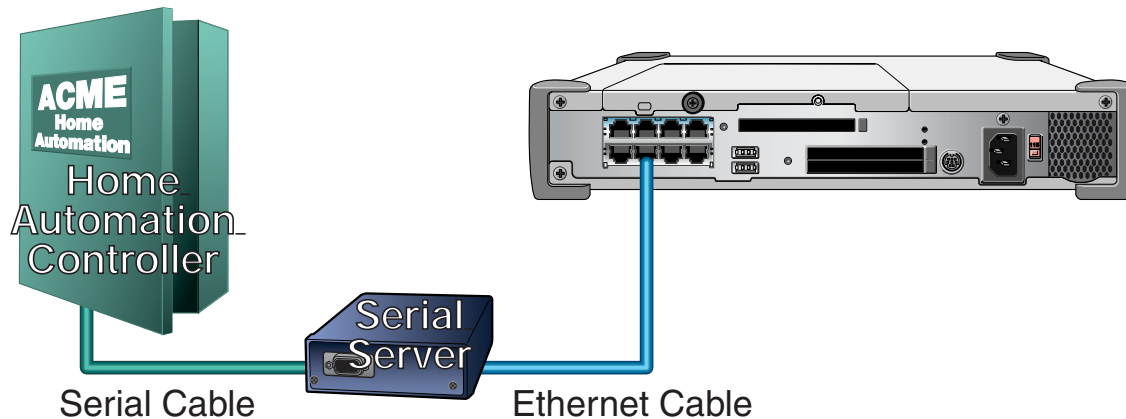
Prior to configuring the SG30, make sure complete information is available regarding:

- ❖ Type of lighting device (X10, Extended X10)
- ❖ X10 address (as configured in the controller)
- ❖ IR codes programmed in the controller, and the devices for these codes

Connecting the Home Automation Controller

The home automation controller should be connected to the Magnia SG30 using the supported Atop Single Port Serial Server or compatible device. This device provides a connection between the home automation controller's serial port and an Ethernet port on

the Magnia SG30. The serial server's Ethernet cable should be connected to the Magnia SG30's local network (one of the sockets in the built in Ethernet switch).



The serial server should be configured with a static IP address for connection to the Magnia SG30 local network. This address must be within the subnet range of the Magnia SG30 local network, but must be outside the local network's DHCP range. With the default configuration, this could be any address from 192.168.1.241 through 192.168.1.254. Recommended values to prevent collision with other Digital Central options are 192.168.1.253 or 192.168.251. The serial server comes with a setup program that will allow you to configure it with the selected address.

Configuring the Home Automation Controller

The first step in configuring your Magnia SG30 Home Automation interface is selecting the home automation controller installed in your home. Make sure you have a client computer connected to your Magnia SG30, and configured so that it can access the built-in Digital Central web site.

To configure the automation interface:

- 1 Enter the following URL in your web browser: <http://myserver/digital> to display the Magnia SG30 Digital Central web site. (If you have changed the name of your server, replace the name "myserver" in the URL with your server's new name).

NOTE

The Digital Central web site may work with several different web browsers, but it has been designed to work best with Internet Explorer 4.1 and above. Also, the PDA interface is supported for general use of the home automation module, but it is not supported for configuring the home automation module (i.e. a notebook or desktop computer must be used).

Once connected to the Digital Central web site, a menu on the left allows you to select various options.

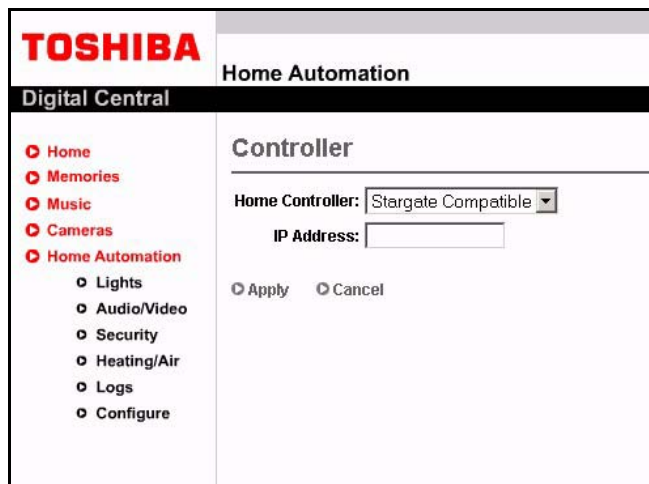
- 2 Expand the Home Automation item, and select the Configuration sub-menu.

The main configuration page appears.



- 3 Select the Home Controller option.

The Controller page appears allowing you to select the controller installed in your home, and enter its IP address.



- 4 Select the controller from the drop down list of supported controllers.
- 5 Enter the IP address of the serial server in the text box. Make sure this is the address assigned earlier to your serial server using its configuration program.
- 6 Click **Apply**.

Once completed, you can configure the Magnia SG30 to recognize the specific devices you have connected to your home automation controller.

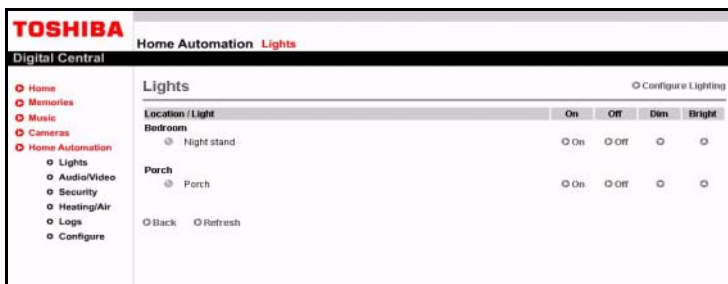
Configuring Lighting

Any X10 or Extended X10 device such as the supported Leviton lamp module typically controls lighting. This type of device can turn lights on and off, and may be able to dim or brighten a light. Make sure you know how your lights were configured in the home automation controller (their X10 addresses) before attempting to configure them in the Magnia SG30. X10 addresses entered in the Magnia SG30 configuration are a combination of the House Code and Unit code (such as A1 or B3).

To configure lights:

- 1 Select Home Automation.
- 2 Select the Configuration sub-menu item and then click the **Lighting** configuration option.

The Lighting Configuration page appears, which lists all lights currently configured (this list is blank until you enter devices).



- 3 Click **Add Lighting Devices** to add a new light.

The Add a Lighting Device screen appears, which allows you to enter information about a new lighting device.

TOSHIBA Home Automation

Digital Central

Add a Lighting Device

Name:

Type:

House: Unit:

Location:

- 4 By completing the applicable information on this screen, you can tell the Magnia SG30 about a lighting device configured in your home automation controller. This includes:

- ❖ **Name of device:** Enter any name that will help you identify the light later. Examples might be Desk lamp or Standing Lamp.
 - ❖ **Type:** The type of device, generally X10 or Extended X10.
 - ❖ **X10 Address:** This is an address that is derived from the house code and unit code of the X10 device. For example, if the device's house code was "A", and the unit code was "4", its address in the Magnia SG30 will be A4.
 - ❖ **Location:** Select a location from the drop down list. Before you enter the first device, this list is empty. After you enter locations, you can select from these locations in the drop-down, or enter new locations by clicking on the "New Location" button. The location helps you identify where the device is – it is usually a room or area of the house such as "Living Room". Establishing locations can help you sort and view your devices more easily elsewhere in Digital Central.
- 5** When you have completed entering the information for the new lighting device, click **Apply** to save the information.

After you have entered your lighting devices, you can edit the information later by going to the Lighting Configuration screen and clicking the **Edit** option next to the lighting device you wish to change.

You can also delete lighting devices on this screen by clicking the **Delete** option next to the lighting device to be deleted.

Configuring Audio/Video

The Magnia SG30 is capable of interfacing and controlling audio and video equipment that has been programmed in the home automation controller via an infrared (IR) extender such as the supported JDS Infrared Xpander.

Specific IR codes are entered into the controller, and can then be referenced and used to control specific devices. IR codes are entered into the controller with specific numbers. For example, a television may have its IR codes entered into the controller so that On could be IR code 1, Off could be IR code 2, Channel up could be IR code 3, and so on. IR numbers must be unique, so if there were a second TV in the home, its IR codes would be different (for example, On could be 20, Off could be 21, and so on).

NOTE

When configuring multi-function devices (such as a TV/VCR or a Tape/CD/Tuner combination device), you may need to create a separate configuration for each function (for example, one configuration for the TV, and one of the VCR).

To configure the SG30, you need the codes currently programmed in your home controller. For the SG30 to communicate with your home controller for IR command, the SG30 will have to have the identical information input into its database.

To access this IR code information, use the software provided with the existing home controller. The following example applies to the Stargate system.

To configure Magnia SG30 access to your IR extenders and control your audio/video equipment:

- 1 Select Home Automation in Digital Central.
- 2 Select the Configuration sub-menu item and click the Audio/Video configuration option.

The Audio/Video Configuration screen appears, which lists all audio and video devices currently configured (this list will be blank until you enter some devices).

- 3 Click **Add A/V device** to add a new piece of audio or video equipment with IR control.

The Add New Audio/Video Device screen appears, which allows you to enter information for a new device.

TOSHIBA Home Automation Configure

Digital Central

Home Automation

- Home
- Memories
- Music
- Cameras
- Home Automation
 - Lights
 - Audio/Video
 - Security
 - Heating/Air
 - Logs
 - Configure

Add an Audio/Video Device

Device Name:

Symbol	Description	IR#	Symbol	Description	IR#
Ⓢ	Power	<input type="text"/>	↵	Enter	<input type="text"/>
▲	Volume Up	<input type="text"/>	●	Select	<input type="text"/>
▼	Volume Down	<input type="text"/>	0	0	<input type="text"/>
⏻	Mute	<input type="text"/>	1	1	<input type="text"/>
⬆	Channel Up	<input type="text"/>	2	2	<input type="text"/>
⬇	Channel Down	<input type="text"/>	3	3	<input type="text"/>
▶	Play	<input type="text"/>	4	4	<input type="text"/>
■	Stop	<input type="text"/>	5	5	<input type="text"/>
⏸	Pause	<input type="text"/>	6	6	<input type="text"/>
⏭	Skip	<input type="text"/>	7	7	<input type="text"/>
⏩	Fast Forward	<input type="text"/>	8	8	<input type="text"/>
⏮	Rewind	<input type="text"/>	9	9	<input type="text"/>
☰	Menu	<input type="text"/>			<input type="text"/>
⬆	Menu Up	<input type="text"/>			<input type="text"/>
⬇	Menu Down	<input type="text"/>			<input type="text"/>
⬅	Menu Left	<input type="text"/>			<input type="text"/>
➡	Menu Right	<input type="text"/>			<input type="text"/>

Ⓢ Apply Ⓢ Cancel

By completing this screen, you tell the Magnia SG30 about an A/V device with IR codes configured in your home automation controller. This includes:

- ❖ **Name of device:** Enter any name that will help you identify the device later. Examples might be Living Room TV or Stereo Downstairs.
- ❖ **IR Codes:** For each supported operation, enter the IR code programmed into the home automation controller for that device. Not all devices support all operations (for example, there is no fast forward on a TV). Leave the IR code for unsupported operations blank.

- 4 When you have completed entering the information for the new A/V device, click **Apply** to save the information.

After you have entered your A/V devices, you can edit the information later from the Audio/Visual Configuration screen by clicking the **Edit** option next to the A/V device you wish to change.

You can also delete A/V devices on this screen by clicking the **Delete** option next to the device to be deleted.

Security

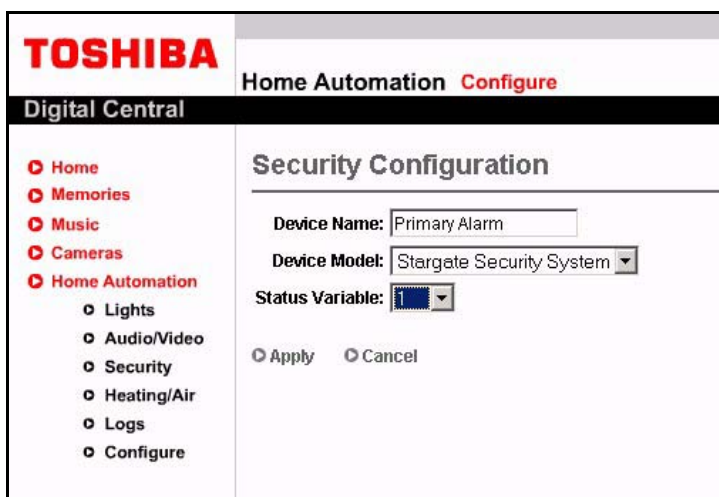
The Magnia SG30 can interact with a home security system, such as the supported Caddox NX8E security controller. You can view current alarm system status, as well as turn the alarm system on and off through the Digital Central Home Automation interface.

To configure the Magnia SG30 to access your security controller:

- 1 Select Home Automation in Digital Central.
- 2 Select the Configuration sub-menu item and click on the Security Configuration option.

The Security Configuration screen appears, which allows you to enter:

- ❖ the name of the alarm (a text label which you assign)
- ❖ a device model
- ❖ the status variable (a number programmed into your Home Automation controller, which must be obtained from your installer).



The screenshot shows the Toshiba Digital Central Home Automation interface. The top bar features the Toshiba logo and the text 'Home Automation Configure'. Below this is a 'Digital Central' header. On the left is a navigation menu with options: Home, Memories, Music, Cameras, Home Automation (selected), Lights, Audio/Video, Security, Heating/Air, Logs, and Configure. The main area is titled 'Security Configuration' and contains three fields: 'Device Name' with the text 'Primary Alarm', 'Device Model' with a dropdown menu showing 'Stargate Security System', and 'Status Variable' with a dropdown menu showing a blue icon. At the bottom of the main area are 'Apply' and 'Cancel' buttons.

- 3 After selecting your security controller, click **Apply**. This will configure the Magnia SG30 to connect to your security controller and allow you to access its functions.

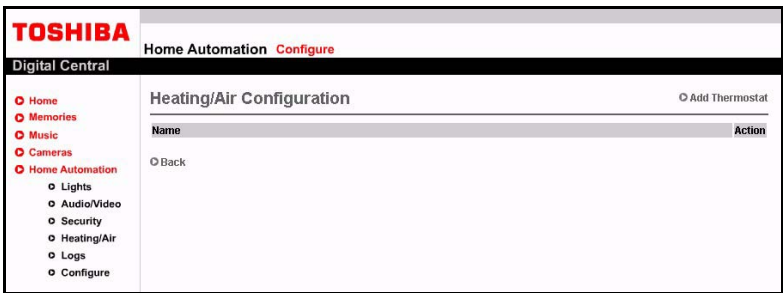
Heating/Air conditioning

The Magnia SG30 supports accessing and controlling home thermostats that are connected to your home automation controller. With the Heating/Air Conditioning option configured, you can view current temperatures, as well as adjust thermostat settings to control heating and air conditioning. You can control multiple thermostats (for example, upstairs, downstairs) if installed. The Magnia SG30 supports several models of thermostats, such as the RCS Thermostat 485.

To configure Magnia SG30 access to your thermostats and control heating/air conditioning equipment:

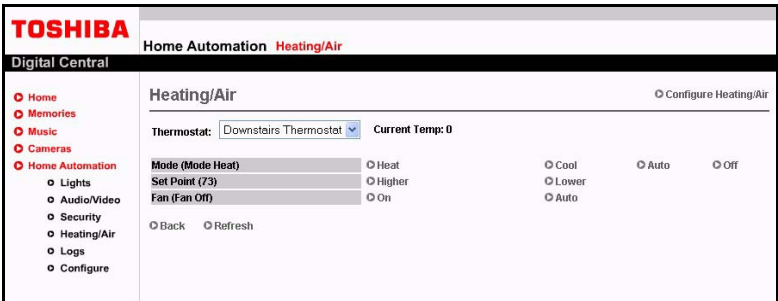
- 1 Select Home Automation in Digital Central.
- 2 Select the Configuration sub-menu item and click on the Heating/Air configuration option.

The Heating/Air Configuration screen appears, which lists all thermostats currently configured (this list will be blank until you enter devices).



- 3 Click **Add thermostat**.

The Add New Thermostat screen appears, which allows you to enter information for a new thermostat.



By completing this screen, you tell the Magnia SG30 about a thermostat configured in your home automation controller. Information includes:

- ❖ **Name of device:** Enter any name you wish that will help you identify the thermostat later. Examples might be Upstairs Thermostat or Downstairs Thermostat.
 - ❖ **Thermostat model:** Select the model of the thermostat from the drop down list.
 - ❖ **Address:** The location of the thermostat programmed into your Home Automation controller and must be obtained from your installer. Each thermostat has a unique location assigned to it.
 - ❖ **Location:** Text field allowing you to enter an easily identified location of the device.
- 4 Click **Apply** to complete the configuration.

Controlling Home Automation Devices

The Magnia SG30 Digital Central Home Automation interface allows you to view the status of all your connected home automation devices through any computer that can reach your Magnia SG30 server. Through this interface, you can adjust heating and air conditioning, lighting, security panel settings and audio/video equipment. Because you can access your home automation through the Internet, dial up modem, or wirelessly, you have tremendous flexibility and control using the Digital Central interface.

Lighting

Through the Magnia SG30 Digital Central interface, you can view and change the lighting throughout your home. To view the state of the lights connected to your home automation controller, use a web browser on a client computer or PDA to access your Magnia SG30 Digital Central web site. Enter the following URL in your web browser: `http://myserver/digital`. (If you have changed the name of your server, replace the name "myserver" in the URL with your server's new name).

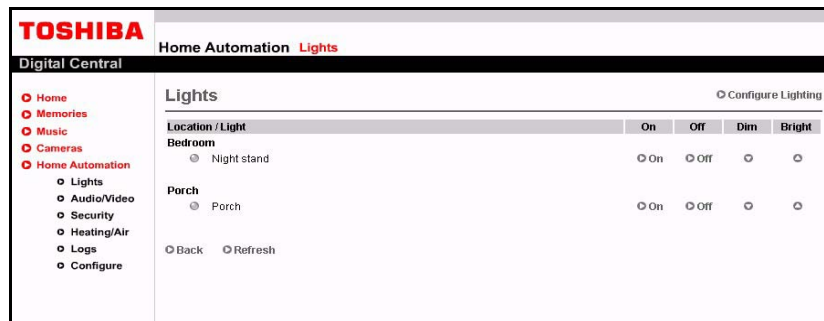
NOTE

If you have difficulty accessing the Digital Central web site using this URL, you can try using the server's IP address: `http://192.168.1.1/digital`. If you have changed the local IP address, use the server's new IP address.

All lights that are configured for home automation via the SG30 Lighting Configuration page will be displayed in Digital Central. The list of lights will be grouped by the zones they were assigned during configuration (for example, Den, Living Room, and so on.). The groups (or zones) are listed in alphabetical order.

Each light in a specific zone is identified by the name you gave it during configuration (for example, Front Standing Light). Next to this name is an indicator of whether the light is

currently on or off (bright yellow indicator for "on", gray for "off"). This is how you can tell the state of your lights from remote locations (via VPN).



For each light, there are four options: On, Off, Dim, Bright.

- ❖ To turn the light on, press the On button next to the light you wish to turn on.
- ❖ The same process is used for turning the light off.

The dim and bright features only apply to certain electrical switch plates that support these functions. If the switch plate that the light is plugged into does not support dim and bright, then pressing these buttons will have no effect on the light. If these features are supported, the dim and bright buttons will decrease or increase the light until it is either completely off or at its brightest level.

When a light has been dimmed and subsequently turned off, the next time the light is turned on, it will be in the same dimmed state. To return the light to it brightest, press the Bright button.

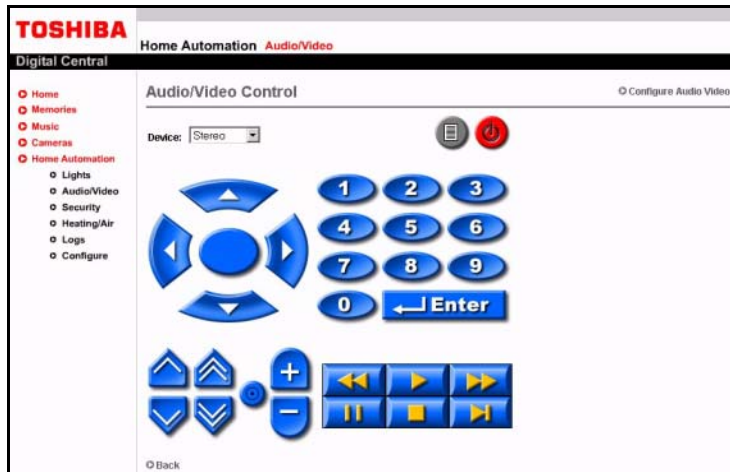
Audio/Video

The Magnia SG30 Digital Central interface allows you to directly manipulate Audio/Video equipment that is controlled through an Infrared (IR) interface (if configured on your home automation controller). To control IR configured equipment, use a web browser on a client computer or PDA to access your Magnia SG30 Digital Central web site.

The interface for controlling audio and video equipment via Digital Central was designed to replicate the use of a normal remote control as much as possible. The same interface is used no matter which device you are controlling (for example, the interface does not change when you move from a DVD player to a stereo).

- ❖ To control an audio or video device, click **Audio/Video** from Home Automation. A drop-down list of available audio/video devices displays in the left hand side of the main audio/video page. The list is in alphabetical order and will default to the device

with the highest alphabetical name (for example, Bedroom TV will come before Den TV.)



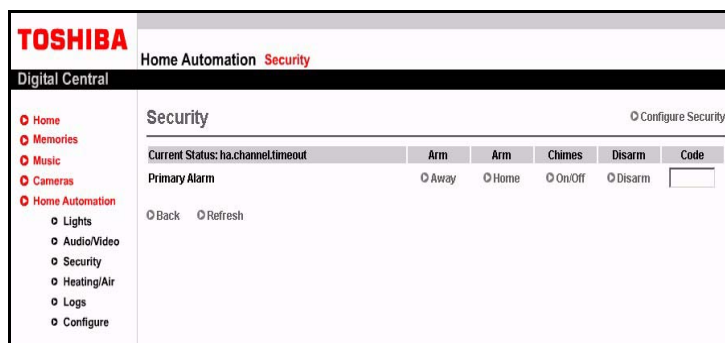
- ❖ To select a device, click on the device you wish to control. All the buttons on this interface will happen instantaneously upon your click (just like what happens when you click on a remote). For example, the power on, volume up or down, menu, and so on, will all invoke the respective command upon a click.
- ❖ Like some remotes, the **Enter** command is required to actually complete certain commands. For example, when changing to channel "24", if you click on "2" then "4", some TV's will immediately change the channel. On other TV's, either a third digit (for example, "0" "2" "4") must be entered, or a certain time must elapse before the channel is actually changed. This behavior is dependent on the audio/video device and its IR interface.
- ❖ The unique item regarding the Digital Central interface is the Vol++ and Vol-- buttons. These buttons are designed to compensate for the fact that commands sent via a computer or PDA wirelessly to the SG30, which is then sent to the home controller, then to the IR repeater, will take slightly longer to get to the target device than a regular remote controller. The volume control for some devices are very finely tuned and to turn the volume up or down noticeably on such devices would involve many clicks on the Digital Central interface.

The Vol++ and Vol-- buttons send 5 volume up or volume down commands in a single click. This makes volume control very usable whether the audio or video device has a finely defined volume control or not. If your audio/video device is not finely defined (if the maximum volume value is 10 vs. 100), then you most likely will never need to use these buttons.

Security

Through the Magnia SG30 Digital Central interface, you can view and change the security settings of your security system. To view the current state of your security system connected to your home automation controller, use a Web browser on a client computer or PDA to access your Magnia SG30 Digital Central web site.

The security panel is accessed by clicking the **Security** link under Home Automation. The Digital Central interface will tell you if your alarm system is Ready, Faulted, Armed and Home or Armed and Away. This interface is designed to look and act very similar to the actual security control panel.



Because the supported security systems may vary, please consult the manual that came with your system. The interface provided on Digital Central acts as if a security panel was being used (for example, clicking the number 1 on Digital Central will result in the same action as if you pressed 1 on the actual security panel).

You will need your pass codes to turn off the alarm system. The codes you enter through the Digital Central interface are secure (they are encrypted before they are sent to the SG30 (via Secure Sockets Layer (SSL)) and then forwarded to the home controller. They are not saved on either the client computer or PDA or the SG30.

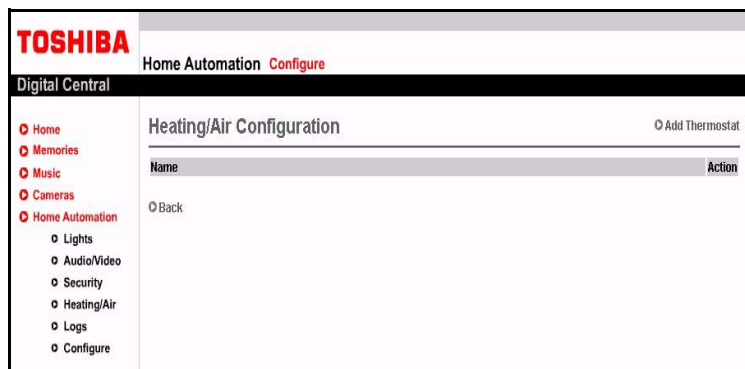
- ❖ To arm your alarm system, click either the **Home** or **Away** button (just as you do with the actual alarm panel).
- ❖ To disarm the alarm, type your pass code in the edit box, and click the **Disarm** button.
- ❖ To turn on or off the chime (door open/closed) click the **Chime** button.

Heat / Air Conditioning

The Magnia SG30 Digital Central interface allows you to control your heating and air conditioning units that are controlled through a thermostat configured in your home automation controller. To control thermostat settings, use a web browser on a client computer or PDA to access your Magnia SG30 Digital Central web site.

The heating and air conditioning interface provided on Digital Central act similar to the actual thermostat in your home. The main difference is that if you have multiple thermostats, you need to select which thermostat you wish to remotely control via the drop down list on the main heating and air screen.

- ❖ To get to the heat and air screen, click the **Heating/Air** link in Home Automation.
- ❖ In the upper left hand corner of this main page, you can select which thermostat to control. If you have only one thermostat installed, then it should be the only one listed.

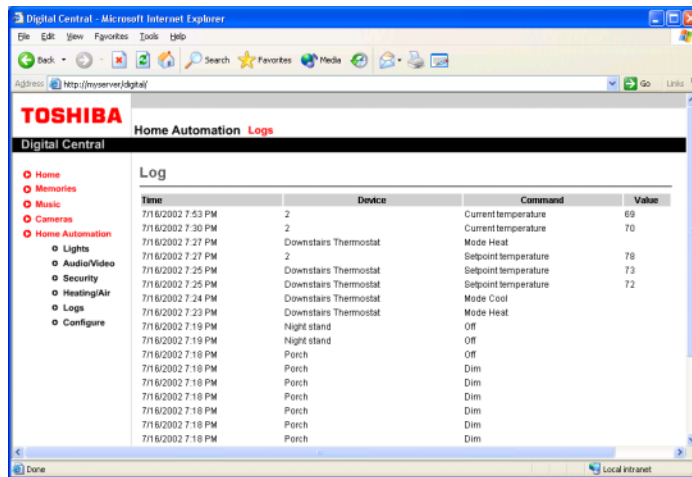


Please see your thermostat manual for detailed instructions since the buttons and commands provided on Digital Central should act identically to the actual buttons provided on the thermostat itself.

Viewing Log Information

A log of the last 30 commands sent through your home automation controller, whether from Digital Central or the interface provided with the home automation controller unit itself (for example, keypads, other software, and so on). This log is provided for auditing purposes so that you know exactly what actions and/or commands are being processed by your home controller.

❖ To access this log, click on the **Log** link in Home Automation.



Alarm System Program for Stargate Compatible Controllers

A special program is required for Stargate compatible controllers that enable them to report alarm system status. Without this program, the home security section of the Magnia SG30 Home Automation interface cannot function. This program can be loaded in to Stargate compatible controllers using the Windows Event Manager program provided with the controller.

This program is provided for Home Automation installers and other Home Automation professionals as a reference.

EVENT: disarm

If

ASCII-In: Match "DISARM1234" [COM1]

Then

SEC: Disarm partition [Partition 1]

End

EVENT: disarmed

If

Partition Not ARMED [Partition 1] TRANSITION

Then

(V: security) LOAD with 1

End

EVENT: armed away

If

Partition ARMED [Partition 1] TRANSITION
Then

(V: security) LOAD with 2
End

EVENT: armed home

If

Partition ARMED & in Home Mode [Partition 1] TRANSITION
Then

(V: security) LOAD with 3
End

EVENT: faulted

If

Partition has alarm condition [Partition 1] TRANSITION
Then

(V: security) LOAD with 1
End

Chapter 13

If Something Goes Wrong

Some problems you may encounter when using your Magnia SG30 are relatively easy to identify and solve. Others may require help from your dealer or Toshiba.

Problems when you turn on the Magnia SG30

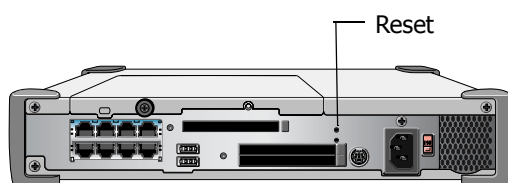
The LCD panel remains dim and does not brighten.

Make sure you attached the power cable properly at both ends.

Unplug the Magnia SG30 and plug it back in again.

The LCD display brightens, but does not display the “Magnia SG30” message.

The initial power to the Magnia SG30 did not fully trigger the warming up process. You should unplug the Magnia SG30, and then plug it back in. If the problem repeats itself, use a pen or paperclip to push the reset button that resides inside the tiny reset hole on the back panel of the Magnia SG30.



The system reset button is just inside the tiny hole labeled Reset

The “Magnia SG30” message does not go away.

It should normally show this message for 30 seconds to a minute. However, if the Magnia SG30 was powered off abruptly and not shut down as expected, then the warming up message could take up to five minutes.

It is also possible that your primary hard disk drive cannot be recognized. If you recently inserted a new hard disk drive or adjusted your hard disk drive(s), check your hard disk drive connection(s). You might want to remove and reinsert your hard disk drive(s).

The Magnia SG30 does not display the expected “Magnia SG30” and date/time messages.

Make sure you attached the power cable properly.

Unplug the Magnia SG30 and plug it back in again.

One or more clients configured for DHCP cannot access the Magnia SG30. Such clients might include a PC, a PocketPC device, or a TurtleBeach AudioTron.

Since the DHCP server on the Magnia SG30 was just restarted, some clients may not know it's time to request a new IP address. To resolve this issue, wait until the appliance server is fully booted, then reboot any client device that is not able to communicate with the appliance server. For the Audiotron, use the power switch in the back of the unit.

Problems when you turn on a client computer

A client computer reports that it has found a new hardware device.

You need to run the Client Setup Wizard to configure your client computer to work with the Magnia SG30. Insert the Magnia SG30 Setup CD and see [Connecting the first client computer using the seven LAN ports](#) on page 30.

A client computer reports that it cannot acquire a DHCP address.

The Magnia SG30 may be turned off. It must be turned on and finished warming up before you turn on a client computer. You should check to see if the Magnia SG30 is powered on.

Check your cables between the client machine and the Magnia SG30. Make sure the client machine is connected to one of the seven local network ports. (Remember that the eighth port is for expansion and cannot be connected directly to a client machine without a cross-over cable).

If you have changed the local network IP address range and subnet mask through the advanced networking feature, verify the size of the IP range and the number of connected client devices. The Magnia SG30 reserves a certain number of IP addresses for internal use. As a result, you may run out of available IP addresses faster than you might think. To test this, try disconnecting or releasing the IP for another client, and then have the first client attempt to acquire an IP address.

A client computer reports that it cannot connect to a drive that is shared from the Magnia SG30.

The user name and password used to login to the client machine might be invalid for the Magnia SG30 local network login. (If a successful login with a user name and password was not achieved on the client machine, then the server's local network cannot be accessed.) Check that the user name and password used to login to the client machine match a user account on the Magnia SG30.

If the user name is not listed on the Administration Web site's Users page (which is under the System tab), then you may wish to run the Client Setup Wizard to configure your client computer to work with the Magnia SG30. Insert the Magnia SG30 Setup CD and see [Connecting the first client computer using the seven LAN ports](#) on page 30.

The client computer displays a message indicating that it cannot reconnect to the Magnia SG30 or the server is unavailable.

The Magnia SG30 may be turned off. It must be turned on before you turn on a client computer.

I get a message about a missing shortcut.

You may have received this message, "The drive or network connection that the shortcut 'netconnectwizard.lnk' refers to is unavailable. Make sure that the disk is properly inserted or the network resource is available, and then try again."

The client computer could not connect properly to the server. Run the Magnia SG30 Setup CD again.

I can't find my files that I placed on the Magnia SG30.

The files are in a private folder, and you cannot view it from your current logged in account. Log out and log back in with the proper login account name.

Internet problems

I can't connect to America Online (AOL).

Because of the proprietary nature of America Online's authentication and communications, AOL is not supported as an ISP.

If you wish to connect to AOL, you can do so by establishing another ISP connection to the Internet. Once connected to the Internet, you can use AOL's software.

My Internet connection is very slow.

Many factors contribute to the speed with which you can surf the Internet. They include: connection speed, time of day (when everyone else is surfing, your access can be slow) and popularity of the site. If accessing a particular site is very slow, try later.

My browser can't find the URL address I typed in.

Make sure you separated the domain names of the address with the forward slash (/). Check the spelling of each name and the syntax of the address carefully. A single incorrect letter, missed period ("dot") or other mistake makes it impossible for your browser to locate the site.

My browser can't find a site I bookmarked.

The World Wide Web is constantly changing. A site you bookmarked yesterday may not be available today or its server may be down for temporary repair. Try again later.

My browser can't find any Internet site.

Test to see if your browser can find the Magnia SG30 intranet (<http://192.168.1.1/>).

If you can see this site, then check your cables and connectivity from the Internet port on back of the Magnia SG30. Verify your Internet settings on the Administration Web site's Internet page under the Network tab.

Contact your Internet Service Provider for further assistance.

My browser can't find the Magnia SG30 intranet.

If your browser cannot find the Magnia SG30 intranet, try browsing to "<http://192.168.1.1/>" instead of "<http://myserver/>" or "<http://myserver.loc>" and instead of using the desktop icon provided by the Magnia SG30 Setup CD. If this works, your server's name may have been changed from "myserver." To see what your server's name is, browse to the Magnia SG30 Administration Web site using "<http://192.168.1.1:8282/>." Click **Advanced** on the Network tab's Local Network page. The initial factory setting for the Magnia SG30's name is "myserver." If this has changed, all Magnia SG30 Setup CD desktop icons created before the name change will need to be updated to reference the new name.

If you cannot browse to the intranet using "<http://192.168.1.1/>," then the Magnia SG30 may be turned off. It must be turned on and finished warming up before you can access the intranet.

You should check to see if the Magnia SG30 is turned on.

Check your cables between the client machine and the Magnia SG30. Make sure the client machine is connected to one of the seven local network ports. (Remember that the eighth port is for expansion and cannot be connected directly to a client machine without a cross-over cable.)

Reboot your client machine. If the client machine was powered on before the Magnia SG30 was finished warming up, then your client machine might not be recognized and assigned a valid IP address (Internet Protocol address) by the Magnia SG30. Rebooting the client machine will fix this.

Other system problems

A client machine can no longer access anything.

The client machine may have lost its IP address. Reboot the client machine and try again.

The Magnia SG30 Administration Web site is difficult to navigate due to scroll bars.

Check your screen area (a.k.a. screen resolution) and use of large fonts. For best viewing, set your screen area to at least 800 by 600 pixels. Set it higher if you use large fonts.

To change your screen area and font size in the operating system:

- 1 Click **Start**, **Settings**, then **Control Panel**.

The Control Panel window opens.



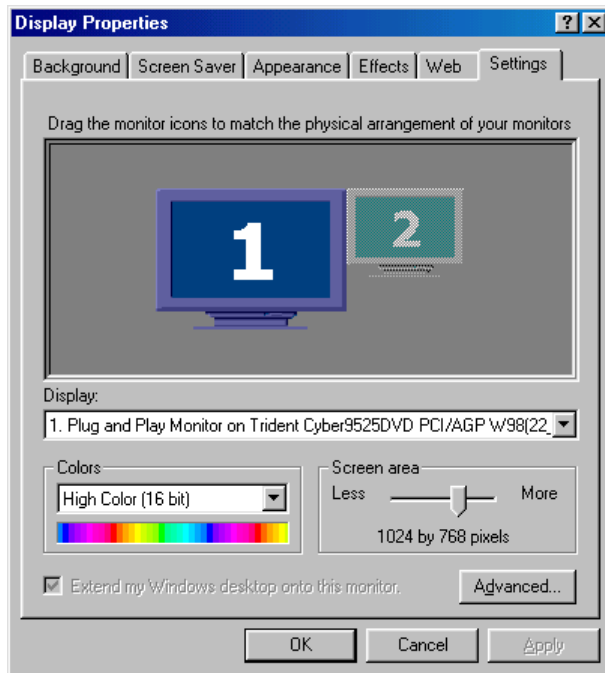
The control panel window

- 2 Double-click **Display**.

The Display window opens.

3 Click the **Settings** tab.

The Settings tab appears something like the following depending on your operating system.



The Settings tab (Windows[®] 98 operating system version shown)

4 Increase your screen area by dragging the slider to the right.

5 To reduce your font size, click **Advanced....**

A new window will appear with a drop list of font size choices. Choose “Small Fonts” for best results.

How do I install virus detection on my system?

Virus detection software is widely available for your client computers. The server is merely a portal, and does not examine, filter, or block the emails passing through it. To obtain virus protection, install it on your client computers.

How do I change my Microsoft[®] Outlook[®] application settings on the server?

The Outlook[®] application is not on the server. It is on the client computer. The server runs under the Linux operating system, and does not use the Outlook[®] application. The settings should be changed on each of the client computers on your local network.

Will the Magnia SG30 work if the client computers are running Linux?

The Magnia SG30 may work flawlessly, but Toshiba has not tested Linux as an operating system for the client computers. Moreover, Toshiba is unable to support customers using Linux on their Magnia SG30 networks.

Email problems

I can receive emails but I cannot send

Check with your ISP. With some ISPs you need to ask them to open SMTP port (PORT 25) for you (for example, AT&T).

Remove information for SMTP from Remote Admin/System tab/E-mail and click **Apply**. By doing so, your Magnia SG30 becomes the primary server for sending emails. This technique works in many environments and ISPs. However, some ISPs will block SMTP traffic. Check with your ISP if you have problems using this configuration.

Check with your ISP and ask them for their Mail Server SMTP information; enter that address in your Server / e-mail / SMTP configuration and click **Apply**. This should fix the problem. For example, if EarthLink is your ISP, you might enter mail.earthlink.net for your SMTP configuration and click **Apply**.

When I send emails to outside recipients, they are returned with the error message “550 User Unknown” or “553 User Unknown.”

Check the email address of the recipient and verify it is typed correctly.

From your Exchange or Netscape Messenger click “Send/Receive” once and then attempt to resend the mail. Some domain hosting services require that you log in using POP3 (Receive) before sending email.

I can send mail but I cannot receive emails

Check and verify you have entered correct User Name and Password. Go to Remote Admin/System/Users, click the user who is not able to receive emails, “Verify ISP E-mail Acct” and “Password” fields. Try reentering the User account and Password.

If you need further assistance

If you have followed the recommendations in this chapter and are still having problems, you may need additional technical assistance. This section contains the steps to take to ask for help.

Remote monitoring and maintenance

This is a subscription service from Toshiba in which qualified Toshiba personnel will assist you with the administration of your Magnia SG30. Toshiba will also monitor the health of your Magnia SG30 as part of this service.

Toshiba Support Web site



- 1** From a client computer, click the **Admin** icon to start the Administration Web site.
- 2** Click the **Services** tab.
- 3** Click **Support** on the menu bar to view the Support page.
- 4** Click the **Toshiba Support Web Site** link, and follow the instructions that appear on the screen.

Toshiba voice contact

Before calling Toshiba, make sure you have:

- ❖ Your Magnia SG30's serial number
- ❖ Information about what you were doing when the problem occurred
- ❖ Exact error messages and when they occurred

For technical support, call the Toshiba InTouch Center:

Within the United States at (800) 457-7777

Outside the United States at (949) 859-4273

Appendix A: Specifications

This appendix describes the Magnia SG30 specifications at the time this user's guide was published. The most current specifications are available on the Toshiba America Information Systems' Web site at applianceserver.toshiba.com.

Basic overview

CPU	Intel® Celeron-T™ 1.2 GHz 100 MHz local bus clock speed
Cache	32 KB
Second level cache	256 KB
Memory	128 MB, 256 MB, 512 MB, 1 GB PC133 unbuffered ECC SDRAM Two 168-pin DIMM sockets
Ethernet LAN interface	10Base-T/100Base-TX Ethernet Seven private RJ45 connectors
Wireless LAN interface (optional)	IEEE 802.11b using PCMCIA card Three Type II PCMCIA slots
WAN interface	One public WAN RJ45 connector
USB 1.1 ports	Two USB 1.1 ports for expansion
Serial port	9-Pin serial, with adapter
Hard disk drive	40 GB 2.5-inch EIDE drive, 4200 rpm -or- 80 GB 2.5-inch EIDE drive, 4200 rpm Optional second hard disk drive
LCD display	Backlit 16 character x 2 line display
Power and frequency	100/240 VAC, 50/60 Hz Maximum power consumption: 110 Watts
Dimensions (w x h x d)	13.5 x 2.6 x 10.3 inches (344 x 68 x 264 mm)
Weight	11.0 lb. (5 kg)

Environmental conditions, Operating	Temp.: 50 - 95°F (10 - 35°C) Humidity: 30% - 80%
Environmental conditions, Non operating	Temp.: -22 - 158°F (-30 - 70°C) Humidity: 20% - 90%
Certifications	Product Safety UL 1950 CSA 950 72/23/ECC (Low Voltage Directive) for CE Mark EMI FCC Part 15, Class B ICES-003 Class B 89/336/EEC (EMC Directive) (EN 55022 Class B) for CE Mark Modem FCC Part 68 R&TTE UL/cUL CTR21 Industry Canada
Cooling fans	One constant speed fan for power supply One fan for remaining components
BIOS	AMI
Hardware monitors	Hard disk drivesTemperature, fan speed, and voltages



TECHNICAL NOTE: This product is not designed for continuous 24-hour operation. If you use this product for this purpose, please contact the manufacturer.

Operating systems supported

The server uses the Red Hat[®] Linux operating system to control the overall environment. The Magnia SG30 provides easy and reliable compatibility with attached computers using all major operating systems, including:

- ❖ Windows NT[®]
- ❖ Windows[®] 95

- ❖ Windows[®] 98
- ❖ Windows[®] 98 Second Edition
- ❖ Windows[®] 2000
- ❖ Windows[®] Millennium Edition
- ❖ Windows[®] XP
- ❖ Apple[®] (Macintosh[®] System 9 and above)



TECHNICAL NOTE: These operating systems cannot replace the Linux operating system in the server.

Linux components

- ❖ Based on Red Hat Linux distribution
- ❖ Linux kernel
- ❖ Gateway/proxy services
- ❖ Samba file services
- ❖ Apache Web server
- ❖ DHCP services
- ❖ DNS/NAT services
- ❖ Sendmail mail services

Appendix B: Privacy Statement for Magnia SG30

Toshiba America Information Systems has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses our information gathering and dissemination practices for the Magnia SG30 product.

The Magnia SG30 Administration Web site contains links to www.toshibapc.com, www.csd.toshiba.com, and other Internet Web sites. These links will sometimes pass the product name, such as "Magnia SG30", and the product serial number to enhance navigation and/or simplify data input. For example, the "Register Now!" link in the Administration Web site passes both of these values so that the user is taken directly to the Magnia SG30 Internet product registration page and so the serial number can be pre-filled in the serial number field to help avoid registration errors.

Our www.csd.toshiba.com site's product registration form requires you to give us your name, company (if for business use), model number, serial number and purchase date. Your contact information is used to contact you about your product. Users may opt-out of receiving mail regarding product information and updates by clicking a box on the product registration form. We may use product registration data to benefit your overall experience on our Internet site, www.csd.toshiba.com.

See our privacy statement for www.csd.toshiba.com for further information about our Internet privacy practices.

The Magnia SG30 offers various services that may require the user to provide information via a sign-up or registration form. When this is the case, only the information provided on the form is sent. No other user data is retrieved from the Magnia SG30.

The Magnia SG30 contains a Health Monitoring Service. The sign-up form for this service requires you to give your name, company (if for business use), model number, serial number, and contact information. Your contact information is used to contact you in regards to this service. For users that purchase the Health Monitoring Service, various statistics about your Magnia SG30 can be sent to www.toshibapc.com on a daily basis. These statistics include all of the information found under the Magnia SG30 Administration Web site's health report plus information regarding your last successful backup and backup type. No backup data or any other user data is sent.

The Magnia SG30 contains a feature that automatically checks for software upgrades. This feature is enabled by default for the benefit of our customers. To make this feature work, the product name will occasionally be sent to www.toshibapc.com so that a list of possibly needed software upgrades can be downloaded. This auto-checking feature can be disabled via the Magnia SG30 Administration Web site under the Services tab's Upgrades page.

The Magnia SG30 contains Web links to other Internet sites. Toshiba is not responsible for the privacy practices or the content of such Web sites.

Your information may be shared with third party contractors for the purposes of performing services for Toshiba America Information Systems.

Contacting Toshiba

If you have any questions about this privacy statement, you can contact Toshiba support.

Copyright© 2001 Toshiba America Information Systems, Inc. All rights reserved.

Appendix C: Open Source License Information

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.

59 Temple Place / Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software— to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

- 0 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program,” below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification.”) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

- 1 You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

- 2 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

- 3 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special

exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4 You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 6 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

- 7 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- 8 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

- 10 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED

TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

DES / SSL Library LICENSE

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Open SSL Library LICENSE

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Glossary



TECHNICAL NOTE: Some features defined in this glossary may not be available on your computer.

Acronyms

AC	Alternating current
DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Service Domain Name System
DSL:	Digital Subscriber Line
ECC:	Error-Correcting Code
FTP:	File Transfer Protocol
HTML:	HyperText Markup Language
IMAP:	Internet Message Access Protocol
I/O:	Input/Output
IP:	Internet Protocol
ISP:	Internet Service Provider
ISDN:	Integrated Services Digital Network
LAN:	Local Area Network
LCD:	Liquid Crystal Display
MB:	Megabyte
NIC:	Network Interface card
PCMCIA:	Personal Computer Memory Card International Association
POP:	Post Office Protocol

<i>SMTP:</i>	Simple Mail Transfer Protocol
<i>TCP/IP:</i>	Transmission Control Protocol/Internet Protocol
<i>UPS:</i>	Uninterruptible Power Supply
<i>URL:</i>	Uniform Resource Locator
<i>VPN</i>	Virtual Private Network
<i>WWW:</i>	World Wide Web

A

access point: A device that connects to a computer or network hub for the purpose of communicating with wireless-enabled computers. See also *wireless communications*

Administration Web site: The Web site that is stored on the Magnia SG30 and accessed from a client computer.

alternating current (AC): Electric current that reverses its direction at regular intervals. This type of power is usually supplied to residential and commercial wall outlets.

B

backup: A copy of a file, usually on removable disk or tape, kept in case the original is lost or damaged. Backup copies should be made of all your important files.

bandwidth: The amount of data that can be transmitted per second over a communications channel. Bandwidth is measured in bits per second (bps) for digital devices and in cycles per second (cps) for analog devices.

broadband: A type of data transmission in which a single medium (wire) can carry several channels at once.

C

CD-ROM (Compact Disc Read Only Memory): A high-capacity (approximately 600 MB) storage medium that uses laser optics instead of magnetic means for reading data. The system can read data from these discs, but cannot write data to the discs.

client: In a network, a computer that accesses shared resources provided by the server.

client: A computer connected to a server.

Client Setup Wizard: A program, found on the Setup CD, that configures the network software on the client computers.

configuration: (1) The set of components in a computer system (such as memory, printers, and disk drives). (2) How parts of the system are set up. For example, the configuration of the serial port includes the baud rate, parity, data bits, and stop bits.

D

device: A component attached to the computer. Internal devices are mounted on the chassis. External devices are connected to the computer via a port.

device driver: A program that controls the operation of a specific device such as the screen, CD-ROM drive, or printer. The operating system loads many device drivers when you turn the computer on.

download: To receive a file from another computer through a modem. See also *upload*.

DSL (Digital Subscriber Line): A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. DSL speeds are tied to the distance between the customer and the telephone company's central office.

E

Ethernet: A local area network (LAN) standard for hardware, communications, and cabling. It links network nodes in a bus topology using coaxial cable, or in a star topology using fiber-optic cable or twisted-pair cable. Normally, all nodes share the total bandwidth, which is 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet). With switched Ethernet, each sender and receiver pair have the full bandwidth.

F

file: A collection of related information (such as the information required for a program or document) saved on disk with a unique name. See also *document*.

firewall: A security system that prevents computers in an organization's network from communicating directly with computers outside the network. It consists of a computer system which controls access to the organization's network and routes incoming and outgoing messages. See also proxy server.

G

gateway: a computer through which other computers can access the Internet.

gateway address: The default address of a network or Web site that provides a single domain name and point of entry to the site.

H

hardware: The physical, electronic, and mechanical components of a computer system, including devices such as a screen, disk drive, printer, mouse, and processor.

hub: A central connecting device in a network that joins communications lines together in a star configuration. A switching hub also routes messages and packets among the computers connected to the network.

HyperText Markup Language (HTML): A special coding scheme used to prepare text and graphics for access over the World Wide Web.

I

Integrated Services Digital Network (ISDN): A worldwide communications network for delivering telephone and data services. It uses two types of communications channel: a B channel, which carries voice, graphics and data at 64 Kbps, and a D channel, which carries control information for signalling at 16 Kbps. A basic ISDN installation typically provides two B channels and one D channel.

Internet: The collection of computers located throughout the world that are connected over telephone lines to provide electronic mail and other services.

intranet: World Wide Web pages designed to serve a limited group of people, such as the employees of a particular company.

IP address: The Internet Protocol address is a unique number for the server and each client computer on a network.

L

LAN (Local Area Network): A collection of computers (located geographically close to each other) connected together in a network.

light-emitting diode (LED): A semiconductor device that emits light when it receives an electric current. Used for indicators like disk activity lights.

liquid crystal display (LCD): A type of display that uses a liquid substance between two transparent electrode panels. By selectively turning the electrodes on and off, the LCD creates the images you see on the screen.

M

map: A method of associating objects or of translating one set of values into another. For example, the association of logical drive letters with the actual physical devices.

modem: A device for transmitting computer information over telephone lines. A modem converts (modulates) digital information for transmission and also converts (demodulates) information it receives back to digital format. Many modems also interpret and execute commands received from the computer.

N

network: A collection of interconnected, individually controlled computers, together with the hardware and software used to connect them. A network allows users to share data and peripheral devices such as printers, and to exchange electronic mail.

network interface card: An expansion board you insert into a computer so the computer can be connected to a network.

O

off line: Not currently connected to or under the control of the computer. Used to refer to equipment such as disk drives and printers.

on line: A functional state in which a device is ready to receive or transmit information.

operating system: A set of programs that controls how the computer works. Operating system functions include creating programs and data files, and controlling the flow of information between the processor, memory, and devices. Examples of operating systems used by computers are Windows[®] 98, and Windows NT[®].

P

password: A unique string of characters used to identify a specific user or group of users for security purposes. A password prevents unauthorized use of the computer.

POP (Post Office Protocol): A protocol used to retrieve email from a mail server. Most email applications (sometimes called an email client) use POP, although some can use the newer IMAP (Internet Message Access Protocol).

portal: A Web site or service that offers a broad array of resources and services, such as email, forums, search engines, and online shopping malls.

protocol: A set of rules and conventions that makes it possible to transfer information between computers. If you're transmitting a file, both modems must use the same protocol—just as two people talking on the telephone must speak the same language to communicate effectively.

proxy server: (1) An application that forms part of a firewall by breaking the connection between the sender and receiver. It intercepts requests for information, decides whether they should be fulfilled, and passes them on to an internal server. It therefore prevents outsiders from obtaining internal addresses and details about a private network. Also called proxy. (2) A server that stores frequently requested data, such as popular Web pages, to reduce network (or Internet) access.

Q

Quick Setup Wizard: A program that configures the bare essential settings for the Magnia SG30 and connects the server to the Internet.

R

radio frequency interference (RFI): All computer equipment generates radio frequency signals. The FCC regulates the amount of RFI a computing device can leak past its shielding. A Class A device is suitable for office use. Class B is a more stringent classification applying to equipment for home use. Toshiba desktop and notebook computers are Class B devices; Toshiba servers are Class A.

reboot: See *boot*, *restart*.

Remote Web Site: A Toshiba Web site used to configure the Magnia SG30 from a geographically remote location.

RJ11 (Registered Jack 11): A modular telephone connector used on most telephone networks and direct-connect modems.

RJ45 (Registered Jack 45): A network connector that holds up to eight wires. RJ45 plugs and sockets are used in 10BaseT Ethernet and Token Ring Type 1 devices.

router: A device that routes data packets from one local area network (LAN) or wide area network (WAN) to another.

S

server: A computer or program that provides information or shared resources in response to external requests from clients. For example, a file server stores on its hard disks the programs and data files for all the computers in a local area network (LAN). *See also Client*.

Setup CD: A CD used to load and configure software.

Soft modem: A modem with functionality that is dependant on software rather than hardware and is easily reconfigured for updates and feature changes.

subnet mask: The method for grouping IP networks into multiple subgroups, or subnetworks. The mask is a binary pattern that is matched up with the IP address. It turns part of the host ID address field into a field for subnetworks.

T

TCP/IP: A set of procedures (protocol) for connecting dissimilar systems.

Topology: In a network, the pattern of interconnection between computers and servers; for example, the Magnia SG30 and its connected client computers are in a star configuration.

U

Uninterruptible Power Supply (UPS): A device connected between a piece of electrical equipment, such as a computer system, and the AC power source to protect against transient power conditions and short-term power outages. A UPS unit contains a power-level sensor and a battery. If the sensor detects a loss of power, it switches over to the battery giving you time to save data and close down the system.

upload: To send a file to another computer through a modem. *See also download*.

V

VPN (Virtual Private Network): VPN enables you to create a secure connection through the Internet to access the company server files, print, email, client shares, and other Magnia SG30 features.

W

WAN (Wide Area Network): A collection of geographically separate local area networks connected over the telephone lines

wireless communications or *wireless network:* A network of computers and servers that does not rely on a physical cable to connect the client computers to the server. Instead, each client computer is capable of transmitting a radio signal, which is apprehended by an access point connected to the Magnia SG30. See also *access point*.

wizard: A helpful online tutor that guides you through common procedures or processes, as in hardware wizard.

World Wide Web (www): The international network of home pages linked together over the Internet by hypertext jumps. A user of the Web can jump from page to page regardless of the location of each page.

Index

Numerics

802.11b wireless capability 288

A

AC socket 26
 access
 dial-in 242
 folders 234
 remote 242
 accessing the Internet 22
 accessing your local area network through the Internet 122
 accessories
 server 20
 account management and VPN 124
 accounts, user 67, 76
 Administration Web site
 accessing 167
 exploring 168
 Administrative Web site 126
 appliance server
 problems
 power 324
 archive files 195
 assistance 331
 Toshiba Web site 331
 automatic
 backup 188
 backup, canceling 191
 email retrieval 117
 avi 257
 Axis 2100 camera 276
 Axis 2400 video server 278, 279

B

back panel

AC socket 26
 expansion port 26
 fan 26
 LAN port 26
 modem port 26
 printer port 26
 public ethernet port 26
 backup
 automatic 188
 daily 190
 data 180
 directory
 FTP 183
 Intranet 183
 public 184
 user 184
 encrypting 193
 files 183, 195
 full 181
 incremental 181
 location 185, 187
 Internet client 181
 local client 181
 manual 181, 188
 monthly 191
 partial 181
 selecting
 full 182
 incremental 183
 partial 182
 viewing
 schedule 192
 status 192
 weekly 190
 backup/restore and VPN 124
 broadband connection 39

C

cable modem
 configuring 85

- IP address 86
- cables 24
- cleaning the Magnia SG30 56
- client
 - defined 231
 - local data backup 181
- client computer
 - configuring 30, 58
 - configuring Internet access 90
 - connecting 30, 57
 - connecting a network printer 239
 - dial-in access 57
 - first LAN connection 78
 - problems 325
- client computers
 - configuring 50
 - connecting 50
- client email
 - Outlook Express 112
 - setup 117, 243
- company logo 219
- configuration requirements for VPN 126
- configuring
 - client computer 30, 58
 - clients 50
 - Internet Explorer 66, 75
 - Internet service
 - cable 85
 - LAN
 - manual 61
 - Macintosh 78
 - Magnia SG30 58
 - network settings 66, 74
 - PCMCIA socket 63
 - wireless access 43
- configuring a client computer
 - VPN 126
- configuring the VPN 124
- connecting
 - a network printer 239
 - a printer 238

- client computer 57
- client computers 30
- connecting a printer 42
 - general Windows procedure 239
- connecting clients 50
- connecting to the internet 37, 83
- connection
 - start up 25
- contracts
 - maintenance 21
- Control Panel
 - finding network adapters 62
- creating
 - user accounts 178
 - user name and password 68, 76

D

- daily data backup 190
- data backup 233
- data redundancy 23
- data, backup 180
 - daily 190
 - full 181
 - incremental 181
 - Internet 181
 - local 181
 - partial 181
- desktop
 - adding links 69, 78
- DHCP
 - problems 325
- dial-in access 242
- dial-out modem, using 91
- dial-up
 - access, configuring 84
- digital camera 250
- digital music 259
- Digital Music Jukebox 249
- Digital Photo 249
- digital photos 250
- digital video album 250

- digital videos 250
- direct email delivery 119
- disabling the modem 92
- disconnecting VPN 248
- disk
 - primary drive 200
 - second drive 200
 - view 202
- display
 - problems 324
- documents
 - archive 195
 - backup 183
 - restore 195
 - selecting 197
- domain
 - email 114
- domain host
 - email 114, 244
 - ISP 119
 - SMTP authentication 119
 - SMTP,POP3 119
- Domain name
 - blocking 96
 - filtering 96
- drive
 - hard, view status 171
 - primary disk 200
 - second disk 200
 - view 202
- drives, mapping with
 - Windows 2000 236
 - Windows 95 236
 - Windows 98 236
 - Windows NT 236
- drives,mapping with
 - Windows Me 236
- DSL internet service, configuring 88

E

- email 24

- and POP3 server 115
- and SMTP server 115
- and your ISP 116
- client setup 117, 243
- direct delivery 119
- domain 114, 115
- domain host 244
- Internet
 - checking 119
 - mirrored host 108
- ISP 107
- local 106
- mirroring
 - domain host 114
- Outlook Express 112
- setup 117, 243
 - auto retrieval 117
- user 116
- Web site 170
- enabling the VPN 124
- encrypting
 - for backup 193
 - wireless data 45
- enhancing Internet performance 94
- events
 - intranet management 224
- expansion port 26
- extra storage 233

F

- fan 26
 - status 172
- features 22
 - data redundancy 23
 - email 24
 - firewall service 23
 - Health Monitoring Service 23
 - Internet data backup 23
 - software upgrades 23
- file sharing 22, 233
 - technical information 237

files

- archiving 195
- backup 183
- extra storage 233
- network 233
- personal 234
- problems 326
- public 234
- restoring 195
- sharing 22, 233, 234
- storing on the server 234
- viewing 234
- Windows
 - extracting 199

firewall

- changing settings 98
- function 97
- Internet security 97
- purpose 97
- service 23

firewall, advanced usage 99

firewalls and VPNs

- VPNs and firewalls 123

folders

- public 233

front panel

- LCD display 26
- power/shutdown button 26
- status scroll button 26

FTP directory, backing up 183

G

generating a client setup diskette for VPN 127

generating additional client setup diskettes

- VPN 128

H

hanging up the modem 92

hard drive

- status 171

health

- Web site 170

Health Monitoring Service 23

help 331

high security, mode 176

I

icons

- other 20
- safety 20

installing

- a NIC 64
- TCP/IP 65, 73

installing a NIC for

- Windows 2000 72

installing NIC for

- Windows NT 71

installing the NIC for Windows ME 63

Internet

- configuring for phone 83

connecting

- phone service 83

connection

- broadband 39
- settings 35

connection types 82

email

- check 119
- mirrored host 108

filtering content 95

performance 94

shared access 82

Web site 170

internet

- connecting 37, 83

Internet access

- configuring client computers 90
- configuring for cable 85
- configuring for DSL 88

Internet data backup 23, 181

Internet Explorer

- configuring 66, 75
- determining version 75

- identifying the version 66
- running 67
- setting options 67, 75
- start up 75
- starting 67

Internet gateway 22

Internet security, firewall 97

Intranet

- directory, backup 183

intranet

- color scheme 220
- company logo 219
- exploring 242
- managing 217
 - events 224
 - news 223, 224
- users 219

Intranet service 23

IP address

- cable 86

ISP

- domain host, authentication 119
- email 107, 116

J

jpeg 250

jpg 250

K

keywords

- blocking 96
- filtering 96

L

LAN

- connecting to existing network 59
- first connection 78
- manual configuration with Windows 95, 98
 - and Me 61
- port 26
- setting the first connection 68, 69

LCD

- viewing information 173

LCD panel

- backup view 193
- modem messages 92

links adding to the desktop 69

Linux

- client computer 329
- components 334

local data backup 181

local email 106

logo, your company on intranet 219

M

Macintosh

- configuring 78
- folders
 - private 80
 - public 80
- network settings 78
- user accounts 79

maintenance

- remote
 - monitoring 331

maintenance contracts 21

manual

- backup 181, 188
- software upgrades 215

manual recording 281

manually configuring a VPN client running
Windows 2000 142

manually configuring a VPN client running
Windows 95/98/Me 132

manually configuring a VPN client running
Windows NT 136

mapping drives

- Windows 2000 236
- Windows 95 236
- Windows 98 236
- Windows Me 236
- Windows NT 236

Microsoft Outlook, setup 110

mirrored host, Internet, email 108

modem

- connecting manually 93
- dial-in access 242
- disabling 92
- FCC requirements 3
- hanging up 92
- LCD panel messages 92
- phone-based service 84
- remote access 242
- using dial-out 91
- viewing status 91

modem connections

- VPN 123

modem port 26

modes, security 35

monthly data backup 191

mov 257

mp3 259, 261

mpeg 257

N

network

- conditions 56
- connecting to an existing LAN 59
- defined 231
- determining network settings 64
- files 233
- logging in 231
- physical conditions 55
- planning 52
- topology 53, 54
- using 231

network adapter

- finding 61, 62
- NIC 61

network card

- see network adapter 63

network printer, connecting 239

network settings 73

- configuring 66, 74

determining 73

operating system 64

network users

Windows NT and 2000 232

networking

wireless 55

NIC

checking for 61, 71

installing for Windows Millennium Edition
63

O

operating system

network settings 64

operating systems 333

options

- service 20
- warranty 20

other icons 20

Outlook Express

and client email 112

P

PCMCIA socket, configuring 63

PDR-M70 253

personal files 234

photo folder 253

playlist 262, 263, 265

PocketPC operating system 288

Point-to-point Tunneling Protocol (PPTP) 122

POP3

- domain host authentication 119
- server, email 115

port

LAN 26

power

- problems 324
- requirements 56

power down 29

power on 28

print jobs

deleting 241

- printer
 - add printer wizard 239
 - connecting 42, 238
 - deleting print jobs 241
 - sharing 238

- printer port 27

- printers
 - sharing 22, 240

- problems
 - power 324

- public
 - files 234
 - folder 233
 - folders accessing 234

- public directory, backup 184

- public ethernet port 27

R

- registration 25

- remote
 - monitoring
 - maintenance 331

- remote access 242

- Remote Access Server (RAS) 122

- remove
 - processor 124, 248

- restore
 - start 198

- restore files
 - selecting 197

- running the client configuration diskettes for VPN 129

S

- safety icons 20

- second
 - disk drive 200
 - view 202

- security 176
 - ease-of-use mode 176
 - user 178, 232
 - types 232

- security modes 35

 - ease-of-use 36

 - high security 36

- select

 - data backup

 - incremental 183

 - restore 197

- server

 - storing files 234

- server accessories 20

- service options 20

- service programs 20

- setting up 25

 - email

 - auto retrieval 117

 - client 117, 243

 - local 109

 - firewall settings 98

 - Internet connection 35

 - Microsoft Outlook 110

 - network settings 73

 - system date and time 35, 36

 - the system mode 35

- settings

 - network 73

- SG30VPNSetup.exe 130

- shared Internet access 82

- sharing

 - a printer 238

 - general Windows procedure 239

 - files 233, 234

 - printers, Windows 98 240

- sharing files 22

- sharing printers 22

- shortcut

 - problems 326

- shutting down 29

- SMTP

 - and domain host authentication 119

 - server email 115

- software

- manual upgrades 215
- upgrade 214
- software upgrades 23
- start up
 - configuring 25
- starting Internet Explorer 67
- startup
 - restore 198
- status
 - fan 172
 - hard drive 171
 - temperature 172
 - view backup 192
 - voltage 173
- synchronization software 253
- system
 - mode setting 35
 - requirements, power 56

T

- TCP/IP, installing 65, 73
- telnet user, managing 31, 176
- temperature
 - status 172
- Turtle Beach AudioTron digital music player
 - 259, 269

U

- upgrade
 - software 214
 - manual 215
 - Web site 170
- upgrades
 - software 23
- user
 - account 76
 - creating 178
 - deleting 179
 - directory backup 184
 - email 115
 - summary 116
 - intranet 219

- levels 232
- name
 - creating 68, 76
 - using 77
- name and password
 - using 68
- password
 - creating 68, 76
 - using 77
- security 178
- telnet
 - managing 31, 176
- types 232
- Web site 170
- user access to VPN 125
- user account 67
 - changing 179
 - file storage 233
 - managing 175

V

- Video Album 249
- video cameras 273
- Virtual Private Network (VPN) 121
- virus detection 329
- voltage status 173
- VPN
 - configuration requirements 126
 - configuring 124
 - configuring a client computer 126
 - disconnecting 248
 - enabling 124
 - generating a client setup diskette 127
 - generating additional client setup diskettes 128
 - giving users access to 125
 - manually configuring a VPN client running windows 2000 142
 - manually configuring a VPN client running Windows 95/98/Me 132
 - manually configuring a VPN client running

- Windows NT 136
 - running the client configuration diskettes 129

- VPN and account management 124
- VPN and backup/restore features 124
- VPN and modem connections 123
- VPN Client Setup Wizard 130

W

- warranty options 20

- Web site

- Toshiba 331
- view status 169
 - backup 170
 - email 170
 - fan 172
 - hard drive 171
 - health 170
 - Internet 170
 - temperature 172
 - users 170
 - voltage 173

- viewing status
 - upgrades 170

- weekly, data backup 190

- Windows 2000

- mapping drives 236

- Windows 95

- mapping drives 236

- Windows 98

- mapping drives 236

- Windows Me

- mapping drives 236

- Windows Media Player 288

- Windows NT

- 4.0 and 2000
 - manual LAN configuration 70
 - mapping drives 236

- Windows, file extracting 199

- wireless access

- configuring 43

- configuring advanced features 49

- determining if installed 43

- encrypting data 45

- limiting 46

- wireless networking 55

- wizards

- add printer 239

- client setup 32

- wma 259, 261