



SmartServer 2.2 User's Guide



Echelon, LON, LONWORKS, LonTalk, Neuron, LONMARK, 3120, 3150, LNS, LonMaker, and the Echelon logo are trademarks of Echelon Corporation registered in the United States and other countries. LonPoint and LonSupport are trademarks of Echelon Corporation.

Other brand and product names are trademarks or registered trademarks of their respective holders.

Smart Transceivers, Neuron Chips, and other OEM Products were not designed for use in equipment or systems which involve danger to human health or safety or a risk of property damage and Echelon assumes no responsibility or liability for use of the Smart Transceiver or Neuron Chips in such applications.

Parts manufactured by vendors other than Echelon and referenced in this document have been described for illustrative purposes only, and may not have been tested by Echelon. It is the responsibility of the customer to determine the suitability of these parts for each application.

ECHELON MAKES NO REPRESENTATION, WARRANTY, OR CONDITION OF ANY KIND, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE OR IN ANY COMMUNICATION WITH YOU, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR ANY PARTICULAR PURPOSE, NONINFRINGEMENT, AND THEIR EQUIVALENTS.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Echelon Corporation.

Printed in the United States of America.
Copyright ©1997–2013 by Echelon Corporation.
Echelon Corporation
www.echelon.com

Table of Contents

Preface	X
Purpose	xii
Audience	xii
Requirements	xii
SmartServer 2.2 Upgrade Requirements	xiii
SmartServer Documentation.....	xiii
Related Reading	xiv
Content	xiv
For More Information and Technical Support	xv
Using the SmartServer Help Files	xvi
Viewing the SmartServer 2.2 ReadMe	xvi
Using Technical Support	xvii
1 Introduction	19
Introduction	20
What's New in the SmartServer 2.2 Software	21
LONWORKS Connections in Standalone Mode.....	21
Increased Device and Data Point Limits.....	21
Maintenance Network Management Mode	22
Static Repeating Mode	22
Enhanced XMPP Client.....	22
OpenLNS Server and OpenLNS CT Support.....	22
i.LON Vision 2.2	22
Cross Browser Support.....	22
New Languages	23
SmartServer Limits	23
SmartServer Compatibility with Network Management Services and Tools	23
2 Installing the SmartServer 2.2 Products	25
Installation Overview	26
Installing Echelon SmartServer Software	26
Installing Echelon SmartServer 2.2 Enterprise Services	31
Installing Echelon i.LON Vision Software	32
Installing Echelon NodeBuilder Resource Editor	32
Installing a BACnet Interface.....	35
3 Configuring and Managing the SmartServer	37
SmartServer Configuration and Management Overview	38
Connecting the SmartServer	39
Configuring the SmartServer	42
Configuring TCP/IP Properties	42
Configuring SOAP/HTTP Service Properties	47
Configuring Time Properties	49
Configuring Security Properties	51
Using HTTPS/SSL	54
Enabling and Disabling Secure Access Mode	54
Performing a Secure Access Reset	55
Securing SmartServer Web Pages	55
Rebooting the SmartServer	56
Creating Modem Connections	57
Selecting Modem Type	58
Configuring Dial-in Connections	59
Configuring Dial-out Connections.....	60

Creating Dial-Out Connections	61
Adding Host Devices.....	65
Adding a Remote SmartServer to the LAN	69
Adding an OpenLNS Server to the LAN.....	70
Troubleshooting the LNS Proxy Web Service.....	73
Adding an E-mail (SMTP) Server to the LAN.....	74
Adding a Time (SNTP) Server to the LAN	76
Adding an IP-852 Configuration Server to the LAN	79
Adding a Web Connection Target Server to the LAN	80
Selecting a Network Management Service.....	83
Using the SmartServer as an RNI and IP-852 Router.....	83
Using the SmartServer as an IP-852 Router.....	84
Activating IP-852 Routing on the SmartServer	85
Adding a SmartServer to an IP-852 Channel.....	87
Configuring the SmartServer as an IP-852 Router	87
Using an IP-852 Channel	92
Using the SmartServer as an RNI.....	94
Configuring the SmartServer as a Remote Network Interface.....	95
Configuring the SmartServer RNI Properties	98
SmartServer RNI Limits	100
Switching Between the SmartServer RNI and Local Network Interface ..	100
Connecting the SmartServer with RNI vs. IP-852.....	101
Managing the SmartServer.....	102
Viewing System Information and Performance.....	103
Using the SmartServer Flash Memory.....	108
Viewing System Health Monitoring	109
Testing Connections	110
Upgrading an i.LON e3 plus Internet Server to the SmartServer	112
Downgrading the SmartServer 2.2 Firmware to the 1.0 Version.....	114
Downgrading the SmartServer Firmware to i.LON 100 e3 Version	116
Migrating an e3 Network Configuration to the SmartServer	116
Restoring a SmartServer to Factory Default Settings.....	119
Replacing the SmartServer	121
Activating the SmartServer v40 Interface.....	122
4 Using the SmartServer Web Interface	125
Using the SmartServer Web Interface	126
Using General and Driver Modes	131
Accessing SmartServer Functional Blocks in General and Driver Modes	132
Accessing Data Points in General and Driver Modes.....	133
Opening SmartServer Applications	135
Using the SmartServer Web Interface to Open SmartServer Applications	136
Using OpenLNS CT to Open SmartServer Applications	138
Adding Data Points to SmartServer Applications.....	138
SmartServer Data Point Names and Organization.....	142
Internal SmartServer Data Points (formerly NVLs)	142
External LONWORKS Device Data Points (formerly NVEs)	142
Virtual Data Points (formerly NVVs).....	143
Constant Data Points (formerly NVCs)	143
Managing Network Objects	144
Managing Network Objects.....	145
Managing Channel Objects	147
Managing Device Objects	150
Managing Functional Block Objects	153
Managing Data Point Objects.....	156
Issuing Network Management Commands	158

Using Device Templates.....	161
Creating Device Templates	161
Creating Devices from Templates	164
Creating External Data Points from Device Templates	166
Deleting Templates on a SmartServer	170
Duplicating Functional Blocks and Data Points	171
Creating a Duplicate Functional Block.....	171
Creating a Duplicate Dynamic Data Point	173
Adding Connections	174
Creating Web Connections.....	174
Creating LONWORKS Connections	177
Configuring Connections	180
Deleting Connections	182
Validating Connections.....	183
Adding File Attachments	185
Deleting File Attachments.....	186
Retrieving File Attachments.....	187
Viewing Connections	187
Checking Error Messages and Viewing the System Log	189
Configuring Global Settings	190
Using Custom Device and Functional Block Icons	193
5 Using the SmartServer as a Network Management Tool.....	195
Network Management Overview	196
Network Management Scenarios	196
Using the SmartServer as a Standalone Network Manager.....	196
Using the SmartServer as a Standalone OpenLNS Network Tool.....	197
Using the SmartServer as a Synchronized OpenLNS Network Tool	198
Designing a LONWORKS Network.....	199
Creating and Configuring a LONWORKS Network.....	199
Creating LONWORKS Networks from the SmartServer Tree	200
Creating LONWORKS Networks from the OpenLNS Tree	202
Configuring a LONWORKS Network.....	204
Switching the SmartServer to a Different OpenLNS Network Database ..	218
Switching to LNS Mode,Synchronizing to OpenLNS Network Database	222
Switching a Network from LNS Mode to Standalone Mode	226
Creating and Configuring LONWORKS Channels	226
Creating a LONWORKS Channel	226
Configuring LONWORKS Channels	227
Creating and Configuring LONWORKS Devices	231
Creating LONWORKS Devices	231
Configuring LONWORKS Devices	233
Using OpenLNS and LNS Plug-ins.....	239
Viewing LONWORKS Devices	242
Changing the Channel of Devices	246
Creating and Configuring LONWORKS Routers	247
Creating LONWORKS Routers.....	247
Configuring LONWORKS Routers	250
Creating and Configuring Functional Blocks.....	253
Creating Functional Blocks	253
Configuring Functional Blocks.....	254
Viewing Functional Blocks	256
Creating, Configuring, and Connecting LONWORKS Data Points.....	257
Creating LONWORKS Data Points	258
Configuring LONWORKS Data Points	259
Viewing LONWORKS Data Points	267

Connecting LONWORKS Data Points with LONWORKS Connections	270
Designing a Modbus Network	270
Creating and Configuring Modbus Channels	270
Creating Modbus Channels	270
Configuring Modbus Channels	271
Creating and Configuring Modbus Devices	273
Creating Modbus Devices	274
Configuring Modbus Devices	276
Viewing Modbus Devices	277
Creating and Configuring Modbus Data Points	278
Creating Modbus Data Points	278
Configuring Modbus Data Points	280
Viewing Modbus Data Points	283
Designing an M-Bus Network	286
Creating and Configuring M-Bus Channels	286
Creating M-Bus Channels	287
Configuring M-Bus Channels	287
Creating and Configuring M-Bus Devices	289
Creating M-Bus Devices	289
Configuring M-Bus Devices	290
Viewing M-Bus Devices	292
Creating and Configuring M-Bus Data Points	294
Creating M-Bus Data Points	294
Configuring M-Bus Data Points	295
Viewing M-Bus Data Points	296
Using the Virtual Channel	298
Installing LONWORKS Networks	300
Acquiring the Neuron ID	301
Automatically Acquiring the Neuron ID	301
Manually Acquiring the Neuron ID	305
Selecting Devices	307
Installing Devices with Smart Network Management	307
Enabling Smart Network Management	307
Installing Devices	308
Checking Device Status	309
Installing Routers	311
Detaching the OpenLNS Server from the Network	313
Maintaining LONWORKS Networks	313
Loading Device Applications	313
Replacing Devices	317
Automatically Replacing Devices	317
Manually Replacing Devices	320
Decommissioning Devices	321
Testing Devices	323
Setting Devices Offline	323
Querying Devices	324
Winking Devices	326
6 Alarming	329
Alarming Overview	330
Using the Alarm Generator Application	330
Opening an Alarm Generator Application	331
Selecting a Data Point	334
Selecting a Compare Point	334
Selecting a Data Point	335
Entering a Constant Value	335

Selecting and Configuring a Comparison Function	336
Using a Binary Comparison Function	336
Using an Analog Comparison Function	337
Selecting SNVT_alarm Output Data Points	340
Using the Alarm Notifier Application	342
Opening an Alarm Notifier Application	342
Selecting and Configuring Input Points.....	345
Configuring Alarm Conditions.....	347
Configuring E-mail and Data Point Destinations	349
Configuring the Alarm Summary and History Log Files.....	352
Automatically Transferring Alarm Logs	353
Viewing the Alarm Summary and Alarm History Logs.....	353
Using the Alarm Notifier: Summary Web Page	353
Using the Alarm Notifier: History Web Page	354
7 Scheduling	357
Scheduling Overview	358
Creating an Event Scheduler	358
Planning Your Schedule	359
Configuring the Real-Time Clock	359
Opening an Event Scheduler Application.....	363
Selecting Data Points	367
Creating Daily Schedules	370
Defining Schedules	370
Creating Events in the Daily Schedule	372
Copying and Deleting Schedules	375
Creating the Exception Schedule.....	375
Creating One-Time Exceptions.....	375
Creating Exceptions in the Event Scheduler.....	379
Creating Exception Groups	387
Editing and Deleting Exceptions in the Event Scheduler	389
How the Scheduler Works with Daylight Savings Time	392
Creating Sunrise and Sundown Events.....	392
Demonstrating Sunrise and Sundown Events	395
Using the Event Calendar	403
Opening the Event Calendar.....	403
Viewing Exceptions in the Event Calendar	406
Creating Exceptions in the Event Calendar.....	407
Editing Exceptions in the Event Calendar.....	408
Deleting Exceptions in the Event Calendar	409
8 Data Logging.....	411
Data Logging Overview.....	412
Creating a Data Logger	412
Opening a Data Logger Application	413
Selecting and Configuring a Log File	416
Selecting and Configuring Data Points	417
Setting Alarm Limits.....	420
Automatically Transferring Alarm and Data Logs	421
Creating a Web Connection for Logger Extraction.....	421
Creating the Web Connection in LNS Mode	422
Creating the Web Connection in Standalone Mode.....	422
Attaching a Log File	425
Triggering Log Transfer	426
Example 1: Scheduling a Log transfer	426
Example 2: Using Case Logic for Log transfer.....	428

Viewing Extracted Data Log Files	429
Viewing Data Logs	430
Viewing Data Logs with the SmartServer Web Pages	430
Manually Transferring Data Logs.....	432
Viewing Data Points.....	432
9 Connecting Legacy Devices Using SmartServer Inputs and Outputs..	437
Connecting Legacy Devices Overview	438
Connecting Pulse Meters	438
Opening the Pulse Counter Application.....	438
Configuring the Pulse Counter Application	441
Connecting Digital Input Devices.....	442
Connecting Digital Output Devices	444
10 Using Analog Functional Blocks	447
Analog Functional Block Overview	448
Creating an Analog Functional Block.....	448
Opening an Analog Functional Block Application	449
Selecting Input Points	452
Selecting and Configuring a Mathematical or Logical Operation	453
Selecting and Configuring a Mathematical Operation	454
Selecting and Configuring a Logical Operation.....	454
Selecting an Output Point	456
11 Using Type Translators	459
Type Translator Overview	460
Creating a Type Translator.....	460
Opening a Type Translator	461
Selecting Input and Output Points	464
Selecting or Creating a Type Translation	465
Selecting a Pre-Defined Type Translation	465
Creating a Custom Type Translation	469
Integrating M-Bus Devices With a Type Translator.....	475
Deleting a Type Translation	479
Specifying a Delay.....	479
12 Using the SmartServer with OpenLNS CT	481
Introduction	482
Installing the SmartServer with OpenLNS CT	482
Synchronizing the SmartServer with a OpenLNS CT drawing	484
Changes Requiring Manual SmartServer Synchronization	486
Changes Requiring OpenLNS CT Synchronization	488
Opening SmartServer Applications with OpenLNS CT	488
Connecting the SmartServer to External Devices	490
Binding External Network Variables.....	490
Polling External Network Variables	499
Troubleshooting SmartServer-OpenLNS CT Synchronization	503
Appendix A Troubleshooting the SmartServer	505
Troubleshooting	506
Appendix B Using the SmartServer Console Application.....	509
Using the Console Application	510
Console Command List	510
Interrupting the Boot Process.....	518
The Bootrom State	518

Updating the Bootrom.....	518
Appendix C Securing the SmartServer.....	521
Securing the SmartServer Overview	522
Updating SmartServer Security Settings	522
Setting Access Restrictions.....	523
Users and Groups.....	523
Locations.....	525
Realms	526
Aliases	527
Sample WebParams.dat file	528
Securing Folders and Files.....	529
Securing Folders	529
Securing Files	530
Examples for Securing a SmartServer.....	530
Example 1	531
Example 2 (recommended for single user group)	531
Example 3	531
Example 4	532
Example 5	532
Example 6	533
Example 7 (recommended for multiple user groups).....	533
Appendix D Manually Managing and Deploying SmartServers	541
Introduction	542
Manually Backing Up the SmartServer Firmware	542
Manually Upgrading the SmartServer Firmware.....	542
Manually Restoring the SmartServer Firmware	544
Manually Copying Device Templates to a SmartServer.....	545
Manually Deploying a Pre-Configured SmartServer in a Single Network	545
Manually Deploying Pre-Configured SmartServers in Multiple Networks	547
Manually Deploying a Network Configuration on Multiple SmartServers.....	549
Appendix E Software License Agreements.....	553

Preface

The SmartServer is a low-cost, high-performance controller, network manager, router, remote network interface, and Web server that connects LONWORKS[®], BACnet, Modbus, and M-Bus devices to corporate IP networks or the Internet.

Purpose

This document describes how to configure the SmartServer and use its applications to manage control networks.

Audience

This guide is intended for system designers and integrators with an understanding of control networks.

Requirements

Requirements for the running the SmartServer 2.2 software are listed below:

- 64-bit and 32-bit Microsoft® Windows 8®, 64-bit and 32-bit Microsoft Windows 7® or 32-bit Microsoft Windows® XP.
- Intel® Pentium® III 1.3 GHz processor or faster, and meeting the minimum Windows requirements for the selected version of Windows (Pentium IV 1.5 GHz or faster if running Echelon Enterprise Services 2.2).
- 2 GB RAM minimum.
- 50 to 830 megabytes (MB) free hard-disk space, plus the minimum Windows requirements for the selected version of Windows.

- The i.LON Vision 2.2 software requires 44 MB of free space.
- If you install Echelon Enterprise Services 2.2 from the SmartServer 2.2 DVD, you need an additional 270 MB of free space. Echelon Enterprise Services 2.2 is required for maintaining synchronization between the SmartServer and OpenLNS network databases, adding the data points of external devices in OpenLNS managed networks to the SmartServer's built-in applications and to your custom SmartServer 2.2 Web pages, and managing OpenLNS networks with the SmartServer Web interface.

If you are running Echelon Enterprise Services 2.2 with a SmartServer operating in LNS mode, OpenLNS Server or LNS Turbo Editions (3.25) or later must be installed on the OpenLNS Server or LNS Server computer and on remote OpenLNS clients running EES 2.2. See the *Echelon Enterprise Services 2.2 User's Guide* for more information on installing Echelon Enterprise Services 2.2.

- You must have the SmartServer 2.0 Programming Tools to create custom C/C++ apps and drivers (also called freely programmable modules [FPMs]), and to translate the SmartServer Web interface into a number of different languages (language localization). To build and upload custom apps and drivers, order the SmartServer 2.0 Programming Tools 2.0 DVD (Echelon model number 72111-409). To order this DVD, contact your Echelon sales representative.
- If you install Adobe® Reader 9.1 from the SmartServer 2.2 DVD, you need an additional 204 MB of free space. You need Adobe Reader or another PDF viewer to view the SmartServer 2.2 documentation.
- DVD-ROM drive.
- 1024x768 or higher-resolution display with at least 256 colors.
- Mouse or compatible pointing device.
- If you are running Echelon Enterprise Services 2.2 with a SmartServer operating in LNS mode, LNS Turbo Editions (3.25) or newer is required.
- Microsoft Internet Explorer 8 or higher, or Mozilla Firefox 18 or higher, Google Chrome 24 or higher or Apple Safari 6.0 or higher.

- Terminal emulator such as PuTTY.

SmartServer 2.2 Upgrade Requirements

You must have a SmartServer 2.0 license for each SmartServer 1.0 (a SmartServer running the Release 4, 4.01, or 4.02 firmware) or i.LON e3 plus Server to be upgraded to SmartServer 2.2 (a SmartServer running the Release 4.06 firmware). Upgrades from earlier i.LON releases are not supported due to their smaller memory not being sufficient for the SmartServer firmware.

You can use the i.LON AdminServer Web application included with Echelon Enterprise Services 2.2 to automatically upgrade your licensed SmartServers. For more information on using the i.LON AdminServer to upgrade your SmartServers, see Chapter 2 of the *Echelon Enterprise Services 2.2 User's Guide*.

Note: To upgrade i.LON e3 plus Servers or SmartServers that have previously been downgraded to the i.LON 100 e3 version firmware to the SmartServer 2.2 (Release 4.06) firmware, you must first manually upgrade them to the SmartServer 1.0 (Release 4.02) firmware via FTP as described in Chapter 3 of this guide.

SmartServer Documentation

The documentation for the SmartServer is provided as Adobe Acrobat PDF files and online help files. You can download the latest SmartServer documentation, including the latest version of this guide, from Echelon's Website at www.echelon.com/support/documentation/manuals/cis.

This user's guide, the online help files, and the following documents comprise the SmartServer documentation suite:

- *Echelon Enterprise Services 2.2 User's Guide*. Describes how to use the i.LON AdminServer to rapidly and automatically deploy and install LONWORKS networks and how to use the LNS Proxy Web service to manage OpenLNS networks.
- *SmartServer 2.2 Hardware Guide*. Describes how to assemble, mount, and wire the SmartServer hardware.
- *SmartServer 2.2 Power Line Repeating Network Management Guide*. Describes how to install a PL-20 repeating network and how to use the SmartServer to prepare, maintain, monitor and control, and connect the network.
- *SmartServer 2.2 Programmer's Reference*. Describes how to configure the SmartServer using XML files and SOAP calls. This allows you to create your own applications that you can use to configure the SmartServer.
- *SmartServer 2.0 Programming Tools User's Guide*. Describes how to write custom built-in applications called Freely Programmable Modules (FPMs) and deploy them on the SmartServer. FPMs let you implement custom functionality and tailor the SmartServer to meet your needs.
- *SmartServer 2.2 Quick Start Guide*. Contains all the information you will need to connect the SmartServer hardware, install the SmartServer software, and configure the SmartServer using the SmartServer configuration Web pages.
- *i.LON Vision 2.2 User's Guide*. Describes how to create custom Web pages for monitoring and controlling LONWORKS networks and other control networks.
- *IP-852 Channel User's Guide*. Describes how to configure an IP-852 channel with the Echelon LONWORKS[®]/IP IP-852 Configuration Server. You will need this information if you plan to use the SmartServer as an IP-852 router.
- *Rapid Deployment Example for EES*. Describes how to assemble and install a demo board that you can use to test the new automatic network installation feature.

- *SmartServer XMPP Client Developer's Guide*. Describes how to use XMPP to enable the SmartServer and client applications to communicate bi-directionally when they are located behind firewalls.

Related Reading

The following additional documents may be useful if you are using certain features of the SmartServer. You can download these documents from Echelon's Web site at www.echelon.com/docs.

- *LNS[®] Programmer's Guide*. Describes how to write OpenLNS applications that take advantage of the network design, installation, maintenance, and control/monitoring capabilities provided by the SmartServer.
- *OpenLDV[™] Programmer's Guide, xDriver Supplement*. Describes how an LNS or OpenLDV application can use the xDriver software to manage communications with multiple LONWORKS networks over a TCP/IP network. The xDriver software is used to communicate with the SmartServer when it is functioning as a Remote Network Interface (RNI).
- *OpenLNS Commissioning Tool User's Guide*. Describes how to use the OpenLNS Commissioning Tool (OpenLNS CT), which you can use to install the SmartServer in a LONWORKS network.
- *NodeBuilder FX User's Guide*. Describes how to use the NodeBuilder tool to develop and test the applications for Neuron-hosted devices.

Content

This guide includes the following content:

- *Introduction*: Provides an introduction to the SmartServer, summarizes the new features in the release of the SmartServer software, describes the SmartServer built-in applications, and summarizes how data points are named and organized on the SmartServer.
- *Installing the SmartServer Products*. Describes how to install the Echelon SmartServer 2.2 software, Echelon Enterprise Services 2.2, the Echelon i.LON Vision 2.2 software, and Echelon NodeBuilder Resource Editor 4.02.
- *Configuring and Managing the SmartServer*. Describes how to connect your SmartServer to a TCP/IP network. Describes how to use the Setup Web pages to configure the SmartServer's properties, which you should do before using any of its built-in applications. Describes how to reboot the SmartServer. Explains how to connect host devices such as remote SmartServers, OpenLNS Servers, time servers, e-mail servers, and Web Connection Target servers to your local SmartServer. Explains how to configure your SmartServer as an IP-852 router and as a remote network interface (RNI), and how to add dial-up connections to your SmartServer. Describes how to manage your SmartServer, including how to view the SmartServer's system information, view and configure the SmartServer's system health monitoring, backup and upgrade the SmartServer firmware, restore the SmartServer to its factory default settings, copy an i.LON 100 e3 server network configuration to the SmartServer, and replace a SmartServer.
- *Using the SmartServer Web Interface*. Describes how to use the navigation pane in the new Web interface to access the SmartServer setup Web pages, switch between General and Driver modes, open the SmartServer built-in applications, add data points to SmartServer built-in applications, manage network objects, manage devices, and use device templates. Explains how to configure the Web interface and check error messages.
- *Using the SmartServer as a Network Management Tool*. Describes how to use the SmartServer to design, install, and maintain LONWORKS, M-Bus, and Modbus control networks. Describes how to create networks, channels, devices (application devices and routers), functional blocks, and data points. Explains how to synchronize the SmartServer to an OpenLNS network database. Explains the differences between LNS and standalone network management and how to switch between the

two network management service modes. Describes how to use the new device discovery feature to automatically acquire the Neuron IDs of the devices on the network. Describes how to use the smart network management feature to install networks. Details how to upgrade, replace, decommission and test devices with the SmartServer.

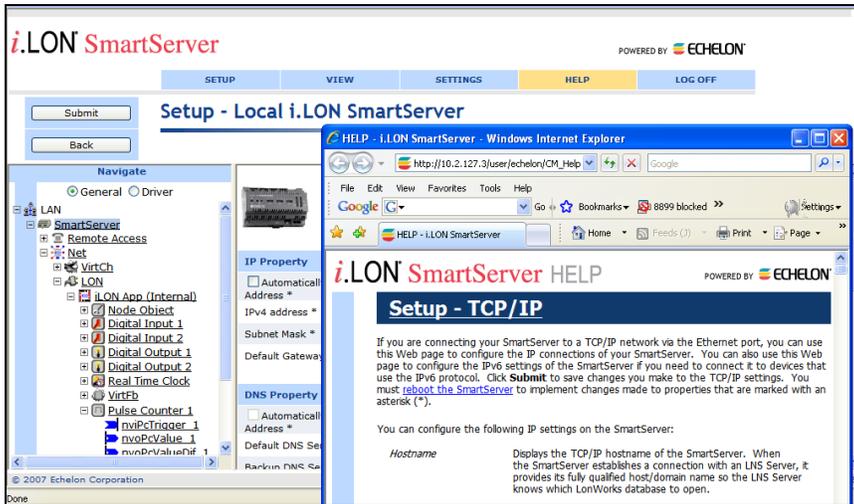
- *Alarming.* Describes how to use the Alarm Generator and Alarm Notifier applications on the SmartServer. You can use the Alarm Generator to generate alarms based on monitored conditions, and you can use the Alarm Notifier to send e-mails and update data points based on alarm conditions.
- *Scheduling.* Describes how to use the Scheduler application on the SmartServer to schedule daily, weekly, and monthly updates to the data points on your network. Describes how to overlap events, and how to start or stop events based on the calculated sundown and sunrise times.
- *Data Logging.* Describes how to use the Data Logger on the SmartServer to record data point updates. Describes how to create historical and circular data loggers. Describes how to automatically transfer data log files to a remote server and extract them to a .csv or XML file. Explains how to view data logs using the **Data Logger: View** Web page, and how to monitor and control data points using the **View – Data Points** Web page.
- *Connecting Legacy Devices Using the SmartServer Inputs and Outputs.* Describes how to use the inputs and outputs on the SmartServer to connect legacy devices to it. Describes how to use the pulse counter inputs on the SmartServer to connect electric, gas, and water meters. Explains how to use the digital inputs and output on the SmartServer to connect legacy digital input and output devices such as switches, push buttons, drive contractors, and alarm bells.
- *Using Analog Functional Blocks.* Describes how to use the Analog Functional Block application on the SmartServer to perform mathematical and logical operations on a set of input points and store the result in an output point, which can be used to control one or more actuator devices.
- *Using Type Translators.* Describes how to use the Type Translator application on the SmartServer to connect devices with different data types. It describes how to use and create scalar-based translations to directly convert an input data point with one type to an output data point with another type. It explains how to use and create rule-based translations that merge multiple input points to create one output point, split one input point to create multiple output points, and split a structured data point into its individual fields.
- *Using the SmartServer with OpenLNS CT.* Describes how to install the SmartServer with OpenLNS CT and the LonMaker Turbo Integration Tool, maintain synchronization between the SmartServer and a OpenLNS CT drawing, and launch the SmartServer’s built-in applications from a OpenLNS CT drawing. Describes how to link the network variables of external devices in a OpenLNS CT drawing (formerly referred to as “NVEs”) to the SmartServer’s built-in applications and custom SmartServer Web pages after synchronizing the SmartServer to an OpenLNS network database.
- *Appendices:* Provides information for troubleshooting and managing the SmartServer; using the SmartServer console application; and using the *i.LON 100 Web Server and Security Parameters* program to secure built-in and custom SmartServer Web pages. Includes the SmartServer 2.2 and i.LON LNS Server software license agreements.

For More Information and Technical Support

If you need help using the SmartServer, you can use the online help files, view the SmartServer 2.2 ReadMe, or read the SmartServer 2.2 documentation. If none of these sources, answer your questions, you can contact technical support if you have purchased support services from Echelon or an Echelon support partner.

Using the SmartServer Help Files

If you need more information on how to use a particular SmartServer Web page, you can click **Help** to open a new window with context-sensitive help for that Web page.



If you need help with a particular dialog in the SmartServer Web interface, you can click the “?” icon in the upper-right hand corner of the dialog to open a new window with context-sensitive help for that dialog.



Viewing the SmartServer 2.2 ReadMe

The SmartServer 2.2 ReadMe provides descriptions of known problems, if any, and their workarounds. To view the SmartServer 2.2 ReadMe, click **Start**, point to **Programs**, point to **Echelon SmartServer 2.2 Software**, and then select **SmartServer 2.2 ReadMe First**. You can also find additional information about the SmartServer online at www.echelon.com/ilon.

Using Technical Support

If you have technical questions that are not answered by this document, the SmartServer 2.2 online help, or the SmartServer 2.2 ReadMe document, you can contact technical support. Free e-mail support is available or you can purchase phone support from Echelon or an Echelon support partner. See www.echelon.com/support for more information on Echelon support and training services.

You can also view free online training or enroll in training classes at Echelon or an Echelon training center to learn more about developing devices. You can find additional information about device development training at www.echelon.com/training.

You can obtain technical support via phone, fax, or e-mail from your closest Echelon support center. The contact information is as follows (check www.echelon.com/support for updates to this information):

Region	Languages Supported	Contact Information
The Americas	English Japanese	Echelon Corporation Attn. Customer Support 550 Meridian Avenue San Jose, CA 95126 Phone (toll-free): 1.800-258-4LON (258-4566) Phone: +1.408-938-5200 Fax: +1.408-790-3801 lonsupport@echelon.com
Europe	English German French Italian	Echelon Europe Ltd. Suite 12 Building 6 Croxley Green Business Park Hatters Lane Watford Hertfordshire WD18 8YH United Kingdom Phone: +44 (0)1923 430200 Fax: +44 (0)1923 430300 lonsupport@echelon.co.uk
Japan	Japanese	Echelon Japan Holland Hills Mori Tower, 18F 5-11.2 Toranomom, Minato-ku Tokyo 105-0001 Japan Phone: +81.3-5733-3320 Fax: +81.3-5733-3321 lonsupport@echelon.co.jp
China	Chinese English	Echelon Greater China Rm. 1007-1008, IBM Tower Pacific Century Place 2A Gong Ti Bei Lu Chaoyang District Beijing 100027, China Phone: +86-10-6539-3750 Fax: +86-10-6539-3754 lonsupport@echelon.com.cn

Region	Languages Supported	Contact Information
Other Regions	English Japanese	Phone: +1.408-938-5200 Fax: +1.408-328-3801 lonsupport@echelon.com

Introduction

This chapter introduces the SmartServer, summarizes the new features in the release of the SmartServer 2.2 software, and describes the SmartServer built-in applications.

Introduction

The SmartServer 2.2 is a low-cost, high-performance, controller, network manager, router, network interface, and Web server that connects LONWORKS, BACnet, M-Bus, and Modbus devices to corporate IP networks or the Internet. It features a built-in Web server that allows Web access to all the data managed and controlled by the SmartServer.

The SmartServer includes built-in applications for alarming, scheduling, logging, translating, and performing arithmetic, logical and statistical functions on data types. It also includes a Web binder for bridging multiple LONWORKS domains. The SmartServer also includes built-in I/O for reading pulse meters and digital inputs, and for switching local loads. All data points and built-in I/O are accessible through either the LONWORKS or Web interfaces.

The SmartServer can be used with the included Echelon Enterprise Services 2.2 (EES 2.2) for rapidly deploying and managing SmartServers and integrating the SmartServer with OpenLNS CT and other OpenLNS network tools.

EES 2.2 includes the i.LON AdminServer, which is a Web application that you can use to upgrade SmartServers, backup and restore SmartServers, and create and deploy i.LON templates. For example, you can backup or upgrade multiple SmartServers at the same time, or you can create a template of one SmartServer and deploy that template on multiple SmartServers simultaneously. In addition, when you deploy a template, you can have the SmartServer automatically or semi-automatically install the devices in the SmartServer or OpenLNS network database included in the template. This automatic network installation feature is supported for single-channel networks containing up to approximately 20 devices.

EES 2.2 also includes the LNS Proxy Web service, which enables the SmartServer to directly communicate with OpenLNS network databases on OpenLNS Server computers. This means that you can use the SmartServer Web interface as a standalone OpenLNS network management tool to design, install, monitor/control, and maintain LONWORKS networks, or you can synchronize the SmartServer with an OpenLNS network database and use the SmartServer to monitor and control the network.

The SmartServer can also be used as a standalone network manager without a connection to an OpenLNS Server. You can use the SmartServer in standalone mode to manage a small, single-channel TP/FT-10 or PL-20 network that does not require OpenLNS management or LONWORKS connections. In standalone mode, the SmartServer serves as a network manager that can directly load, commission, set online/offline, wink, test, and reset the devices attached to its channel without sending the network management commands through OpenLNS.

The SmartServer can be used as a Remote Network Interface (RNI), allowing you to use an OpenLNS or OpenLDV based application, such as OpenLNS CT, to access to a single LONWORKS network remotely. The SmartServer includes optional IP-852 routing, which you can use to access multiple LONWORKS networks remotely (you can order IP-852 routing for new SmartServer units or activate it later). The SmartServer can also be used with the LonScanner™ Protocol Analyzer to capture, analyze, characterize, and display ISO/IEC 14908-1 Control Network Protocol (CNP) packets either locally or remotely via the Internet.

The SmartServer includes an optional programming feature that you can use to create and run custom built-in applications and drivers on the SmartServer called Freely Programmable Modules (FPMs). The SmartServer also provides a SOAP/XML Web services interface for integration with custom enterprise applications.

The SmartServer operates on 100 – 240 VAC high-voltage models that are available for TP/FT-10 and PL-20 channels. An optional built-in 56K V.90 analog modem can be ordered with the TP/FT-10 models.

What's New in the SmartServer 2.2 Software

The SmartServer 2.2 software includes the following new features:

- *LONWORKS Connections in Standalone Mode.* Create peer-to-peer bindings in standalone networks with repeating for rapid response to external events.
- *Increased Device and Data Point Limits in Standalone Mode.* Install up to 300 devices and use up to 2,000 data points in a standalone network.
- *Maintenance Network Management Mode.* Rapidly commission networks by disabling data point heartbeats and polling messages.
- *Static Repeating Mode.* Optimize the performance of power line repeating channels by disabling the periodic verification of repeating paths.
- *Enhanced XMPP Client.* Use real-time bi-directional communication between SmartServers and enterprise applications located behind firewalls. The SmartServer's built-in XMPP client now supports connections where the IP address changes because of lease timeouts, and it is now compatible with Openfire.
- *OpenLNS Server and OpenLNS CT Support.* Integrate the SmartServer in networks managed with an OpenLNS Server. Use the SmartServer with networks managed with the OpenLNS Commissioning Tool (OpenLNS CT).
- *i.LON Vision 2.2.* Rapidly create custom SmartServer Web pages with the i.LON Vision 2.2 standalone Web publishing tool.
- *Cross Browser Support.* View SmartServer 2.2 built-in and custom Web pages using Chrome and Safari in addition to previously supported browsers (Internet Explorer and Firefox).
- *New Languages.* View SmartServer 2.2 built-in and custom Web pages in Chinese, Korean, and Japanese in addition to previously supported languages (English, French, and German).

Note: To use the new SmartServer 2.2 features on a SmartServer 1.0 (a SmartServer currently running the Release 4, 4.01, or 4.02 firmware) or on an i.LON e3 plus Server, you must have a SmartServer 2.0 license for each SmartServer 1.0 to be upgraded to a SmartServer 2.2 (a SmartServer running the Release 4.06 firmware).

LONWORKS Connections in Standalone Mode

You can create LONWORKS connections in standalone networks. This enables devices on a power line repeating networks to send and receive event-driven updates. Previously, if you selected the Standalone network management you could only bind devices using Web connections, which use polling to transmit and receive data. For example, a presence sensor in a street lighting network can now detect a car and send the event to an outdoor lighting controller (OLC) to illuminate a street light and transmit the event to street lights further down the network.

For more information on creating LONWORKS connections in a standalone network, see *Connecting LonWorks Data Points with LonWorks Connections* in Chapter 5.

For more information on using LONWORKS connection in a power line repeating network, see the *Power Line Repeating Network Management Guide*.

Increased Device and Data Point Limits

You can now install up to 300 devices and use up to 2,000 data points in a standalone network. The previous limit for standalone networks was 200 devices and 1,000 data points.

Maintenance Network Management Mode

You can speed up network commissioning using the new maintenance network management mode. The **Network Management Mode** box in the **Setup - LON Network Driver** Web page includes a new **Maintenance** option. When this option is selected, the SmartServer does not send out heartbeat and polling messages. This increases the available bandwidth by freeing up the consumption from checking data point heartbeats, sending poll requests, and receiving poll message responses. This management mode is ideal for power line repeating networks. See the *Power Line Repeating Network Management Guide* for more information.

Static Repeating Mode

You can optimize the performance of power line repeating networks using the new static proxy chains. The **Repeating** box in the **Setup - LON Channel Driver** Web page includes a new **On (Static Proxy Chains)** option. When this option is selected, the power line channel uses repeating, but the SmartServer does not continuously try to discover and optimize the repeating chains used to communicate messages from the SmartServer to the devices on the network. This increases the available bandwidth on the power line repeating network for operational traffic. See the *Power Line Repeating Network Management Guide* for more information.

Enhanced XMPP Client

You can use the Extensible Messaging and Presence Protocol (XMPP) to enable bi-directional communication between SmartServers and enterprise applications located behind firewalls. For SmartServer 2.2, the SmartServer XMPP client supports connections where the source or destination IP address changes because of an IP lease timeout. In addition, the SmartServer XMPP client has new configuration options that make it compatible with the Openfire XMPP server. For more information on using the SmartServer XMPP client, see the *SmartServer 2.2 XMPP Client Developer's Guide*.

OpenLNS Server and OpenLNS CT Support

SmartServer 2.2 supports the new OpenLNS Server when running in LNS mode. This enables the SmartServer to remain synchronized with an OpenLNS database in a system managed with an OpenLNS Server (for example, lighting systems and other building applications where an OpenLNS Server is used to manage the network configuration). SmartServer 2.2 is compatible with the OpenLNS Commissioning Tool and other OpenLNS tools.

i.LON Vision 2.2

You can rapidly create custom SmartServer 2.2 Web pages with the i.LON Vision 2.2 standalone Web publishing tool.

With i.LON Vision 2.2, you can create custom Web pages for monitoring and controlling the data points on your SmartServer 2.2—without any knowledge of HTML, JavaScript, or Web programming. The i.LON Vision 2.2 toolkit provides many objects that you can use to read and write values to data points, including basic read/write objects; SVG objects (for example, sliders, gauges, and thermometers); application objects that expose some of the SmartServer's built-in applications to your end users; and a custom JavaScript object for implementing your own custom objects.

i.LON Vision 2.2 features quick Web page creation as you can switch between the edit and publish views of your Web pages without long delays. This means that you can create or edit a custom Web page and instantly see the results when you publish it.

Cross Browser Support

You can view the SmartServer 2.2 built-in and custom Web pages using Chrome and Safari in addition to previously supported browsers (Internet Explorer and Firefox).

New Languages

You can view the SmartServer 2.2 built-in and custom Web pages in Chinese, Korean, and Japanese in addition to previously supported languages (English, French, and German).

You can work with the SmartServer in any one-byte or two-byte character language by translating the **.properties** file in the **/web/nls/echelon** folder on the SmartServer flash disk. You can perform this language localization using either the demo version of the SmartServer 2.0 Programming Tools included on the SmartServer 2.2 DVD or using the full version on the SmartServer 2.0 Programming Tools included on the SmartServer 2.0 Programming Tools DVD. For more information on ordering the SmartServer 2.0 Programming Tools DVD, contact your Echelon sales representative. See the *SmartServer 2.0 Programming Tools User's Guide* for more information on how to localize the language of the SmartServer Web interface.

SmartServer Limits

The SmartServer 2.2 has the following limits:

- Up to 4,096 address table entries.
 - Up to 32 simultaneous outgoing transactions.
 - Up to 1,024 network variable aliases.
 - The number of devices and data points supported by the SmartServer in OpenLNS managed networks depends on the available memory on the flash disk.
 - The SmartServer can support up to 300 devices and 2,000 data points in standalone networks. This limit may be lower depending on the number of data points and custom apps on the SmartServer.
 - The SmartServer's App device can support up to 3,000 dynamic network variables, but the SmartServer may run out of memory before this limit is reached. The practical limit depends on the sizes of the defined dynamic network variables. You can check the available memory on your SmartServer using the **Setup - System Info** Web page. To access this Web page, right-click the SmartServer icon in the navigation pane in the left frame, point to **Setup**, and then click **System Info** in the shortcut menu. Alternatively, you can click **Setup** and then click **System Info**.
-

SmartServer Compatibility with Network Management Services and Tools

You can integrate the SmartServer 2.2 in systems managed by OpenLNS and LNS Turbo Edition Servers (version 3.25 or newer). In addition, the SmartServer 2.2 is compatible with the OpenLNS Commissioning Tool (CT), other OpenLNS tools, the LonMaker tool, and other LNS tools. For simplicity when describing network management services and Echelon network tools hereafter, this document references only OpenLNS Server and OpenLNS CT. For more information on integrating the SmartServer 2.2 with OpenLNS CT, see Chapter 12, *Using the SmartServer with OpenLNS CT*.

Installing the SmartServer 2.2 Products

This chapter describes how to install the Echelon SmartServer 2.2 products including the SmartServer 2.2 software, SmartServer 2.0 Programming Tools Demo, Echelon Enterprise Services 2.2, i.LON Vision 2.2, and Echelon NodeBuilder Resource Editor 4.02.

Installation Overview

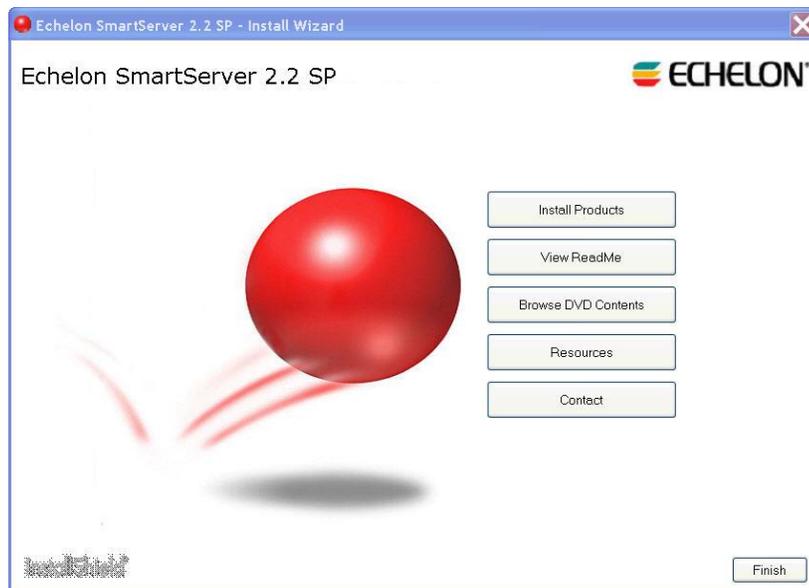
The following sections describe how to install the following SmartServer products:

- Echelon SmartServer 2.2 software.
- Echelon i.LON Enterprise Services 2.2.
- Echelon i.LON Vision 2.2 Software.
- Echelon NodeBuilder Resource Editor 4.02.

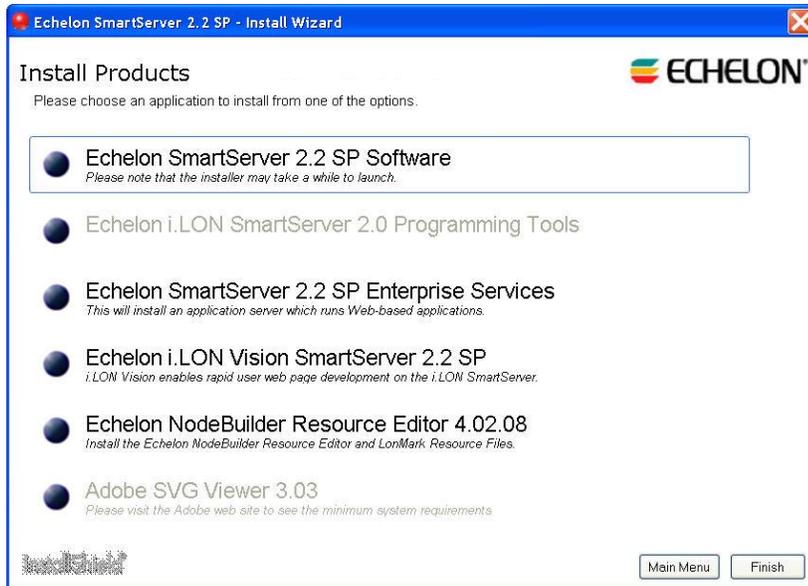
Installing Echelon SmartServer Software

To install the SmartServer 2.2 software, follow these steps:

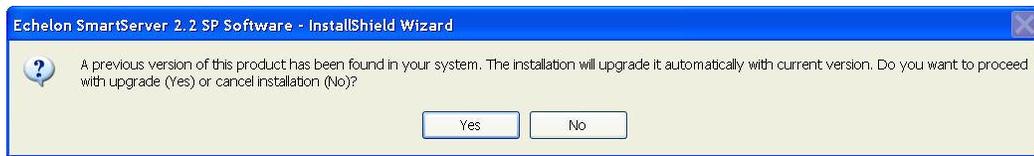
1. Download the SmartServer 2.0 SP4 (SmartServer 2.2) to your computer and click on the downloaded executable(153-0547-01a_SmartServer_2_SP4_downloader.exe). A WinZip Self-Extractor will pop up and if you click the Unzip button, it will unzip and automatically open the Echelon SmartServer 2.2 SP main menu.



2. Click **Install Products**. The **Install Products** dialog opens.



3. Click **Echelon SmartServer 2.2 SP Software**. If SmartServer 1.0 software (Release 4.0, 4.01, or 4.02) is installed on your computer, the following dialog opens prompting you to confirm that you want to upgrade to the SmartServer 2.2 software. Click **Yes** to upgrade.



4. A dialog opens prompting to close all applications currently running on your computer. Close any applications running on your computer, and then click **OK**.



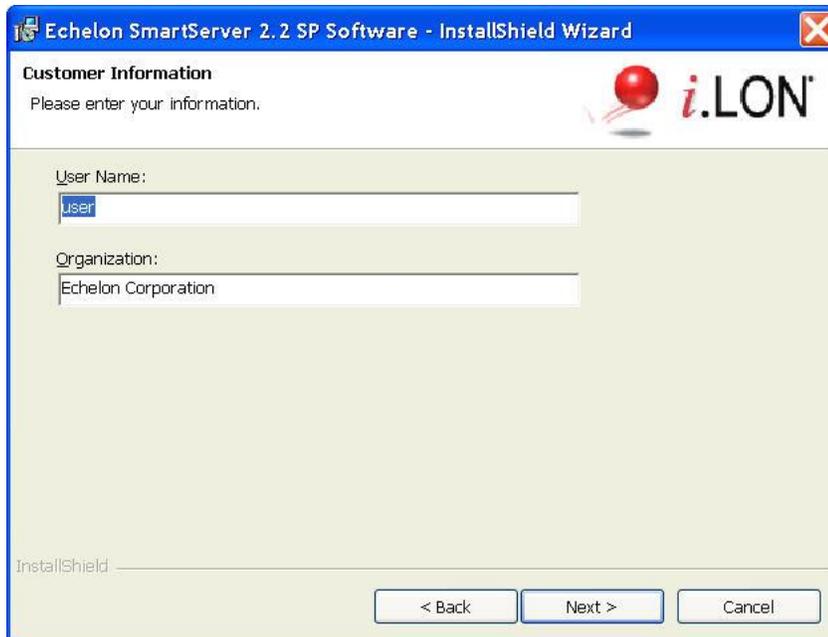
5. The Welcome window of the SmartServer 2.2 SP software installer opens. The original product name was *i.LON SmartServer*, so *i.LON* may appear on some of the screens.



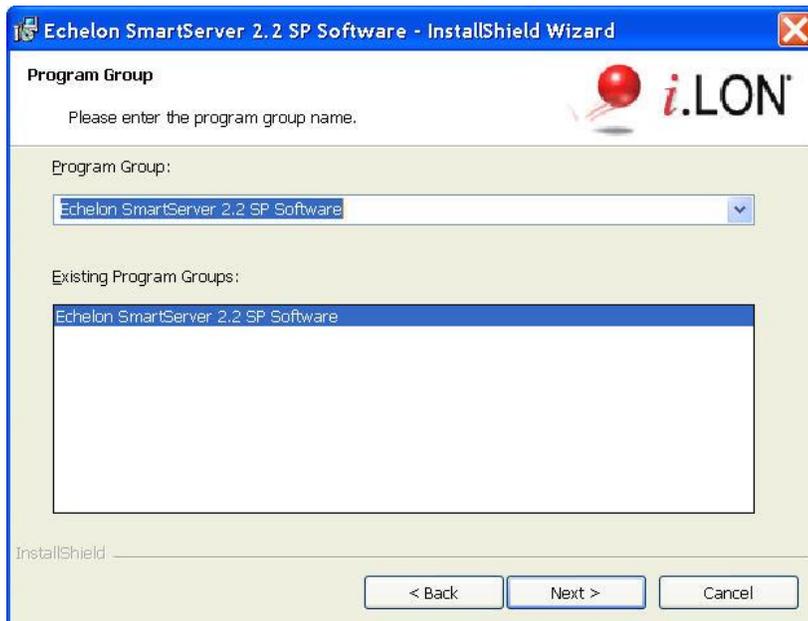
6. Read the information on the Welcome window and click **Next**.
7. The License Agreement window appears.



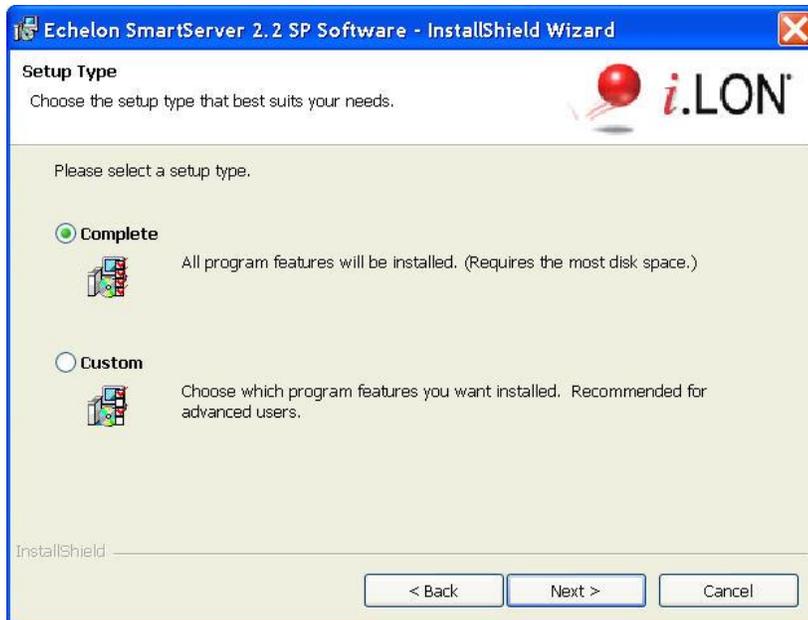
8. Read the license agreement (you can read a printed version of the license agreement in Appendix E, *Software License Agreements*). If you agree with the terms, click **Accept the Terms** and then click **Next**. The Customer Information window appears.



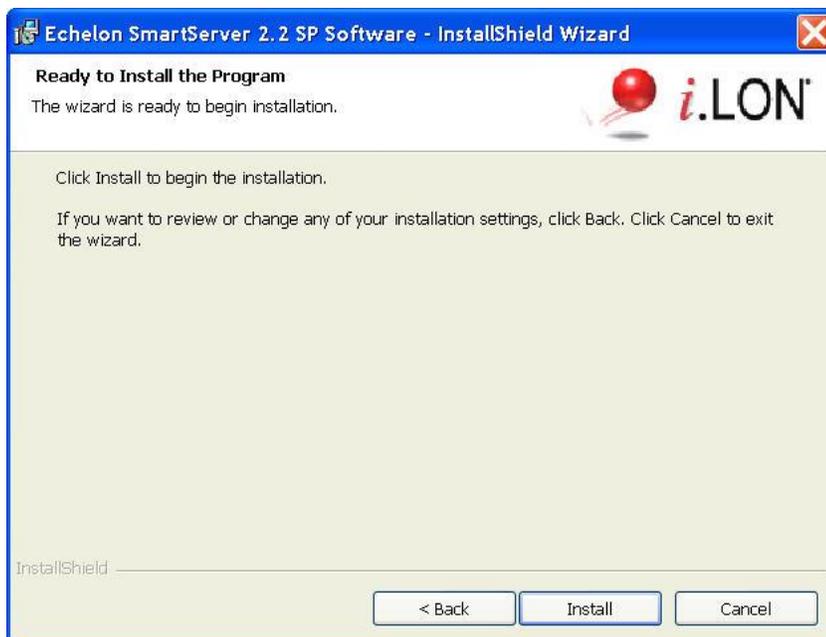
9. Enter your name and company name in the appropriate fields. The name and company may be entered automatically based on the user currently logged on and whether other Echelon products are installed on your computer. Click **Next**. The Program Group window appears.



10. Enter or select a program group in the **Start** menu to use for starting the SmartServer applications and accessing the SmartServer images and documentation. The default program group is **Echelon SmartServer 2.2 SP Software**. By default, the SmartServer 2.2 SP software, SmartServer 2.2 SP image (iLon100 4.06), and documentation will be installed in the **LonWorks\iLon100 LonWorks** folder. The Setup Type window appears.



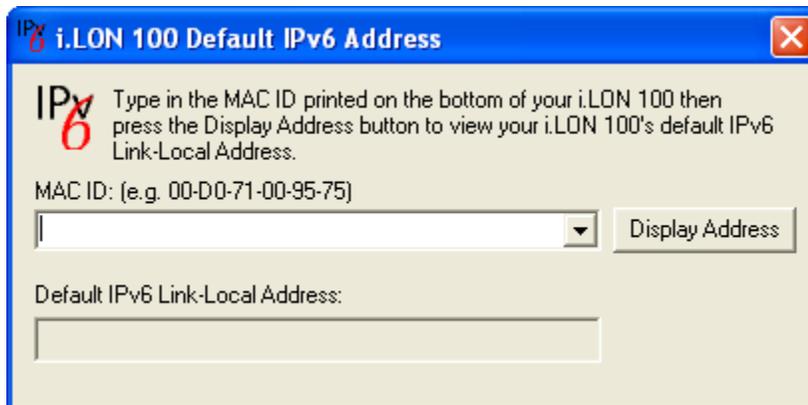
11. Select the type of installation to be performed. It is recommended that you select **Complete**. Click **Next**. The Ready to Install window appears.



12. Click **Install** to begin the SmartServer software installation. The installer first checks whether OpenLDV 4.0 is installed on your computer. If OpenLDV 4.0 is not installed on your computer, the SmartServer 2.2 SP software installer will automatically install it before installing the SmartServer 2.2 software.
13. After the SmartServer 2.2 SP software has been installed, a window appears stating that the installation has been completed successfully. The window also provides you with an option to view the SmartServer 2.2 SP ReadMe, which contains information that is not included in this user's guide, and an option to view the default IPv6 link local address of your SmartServer.



14. Click **Finish**. If you need to reboot your computer, a window will appear prompting you to select to reboot your computer now or later.
15. The SmartServer 2.2 ReadMe file appears. When you finish reading the SmartServer 2.2 ReadMe, close the window.
16. If you chose to display the default IPv6 link local address (you can open this dialog by clicking **Start**, pointing to **Programs**, pointing to **Echelon SmartServer 2.2 Software**, and then clicking **SmartServer 2.2 Default IPv6 Address**.), enter the MAC ID address of your SmartServer in the **MAC ID** box (the MAC ID is located on the bottom of your SmartServer hardware device), and then click **Display Address** to show the default IPv6 address.
17. To use this IPv6 address to access your SmartServer you need to enable IPv6 on your SmartServer as described in *Configuring TCP/IP Properties* in Chapter 3.



Installing Echelon SmartServer 2.2 Enterprise Services

The Echelon Enterprise Services 2.2 (EES 2.2) includes the i.LON Admin Server used for managing and deploying SmartServers, and the LNS Proxy Web service and Tomcat 6 Server used for communication between the SmartServer and OpenLNS or LNS network databases. You need to install EES 2.2 in order to synchronize the SmartServer to an OpenLNS or LNS network database, and add the data points of external devices in OpenLNS or LNS managed networks to the SmartServer's built-in applications.

If you are using LNS mode, or if you are using EES to convert binary log files to CSV format, you must install either an OpenLNS Server or an LNS Server. The OpenLNS Server is included with the OpenLNS Commissioning Tool and other OpenLNS tools. The LNS Server is included with the LonMaker Integration Tool and other LNS tools. If you do not have either server, you can download the OpenLNS Server from www.echelon.com/openlns.

To install the Echelon i.LON Enterprise Services, click the Echelon SmartServer 2.2 SP – Install Wizard button in the taskbar to return to the SmartServer 2.2 installer, click **Echelon SmartServer 2.2 SP Enterprise Services** in the **Install Products** dialog, and then follow the on-screen instructions. See the *Echelon Enterprise Services 2.2 User's Guide* for more information on installing the EES 2.2 software.

After the Echelon Enterprise Services has been installed, the Tomcat 6 Server starts and an EES tray tool  is added to the notification area of your desktop. If you have installed an OpenLNS Server or LNS Server, the LNS Proxy Web service is enabled and ready for setup on your SmartServer. For instructions on setting up and troubleshooting the LNS Proxy Web service, see *Adding an OpenLNS Server to the LAN* section in Chapter 3, *Configuring and Managing the SmartServer*.

For more information on using the i.LON Admin Server and using the EES tray tool, see the *Echelon Enterprise Services 2.2 User's Guide*.

Installing Echelon i.LON Vision Software

You can install the i.LON Vision 2.2 software to create custom 2.2 SmartServer Web pages for monitoring and controlling your networks.

To install the i.LON Vision 2.2 software, click the Echelon SmartServer 2.2 SP – Install Wizard button in the taskbar to return to the SmartServer 2.2 installer, click **Echelon i.LON Vision SmartServer 2.2 SP** in the **Install Products** dialog, and then follow the on-screen instructions. See the *i.LON Vision 2.2 User's Guide* for more information on installing this software.

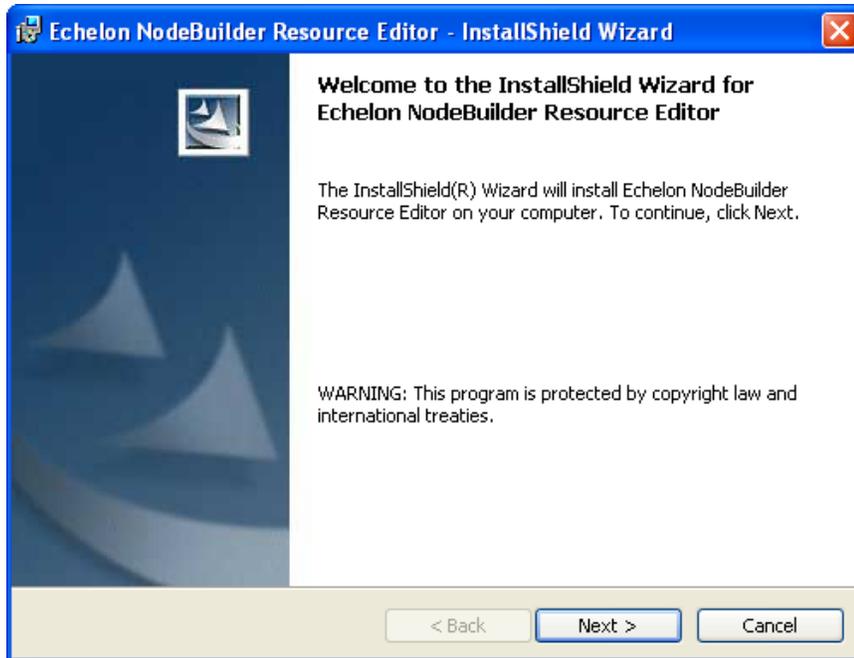
Installing Echelon NodeBuilder Resource Editor

You can install Echelon NodeBuilder Resource Editor 4.02 and LonMark Resource Files 14 to view, create, and modify device resource files.

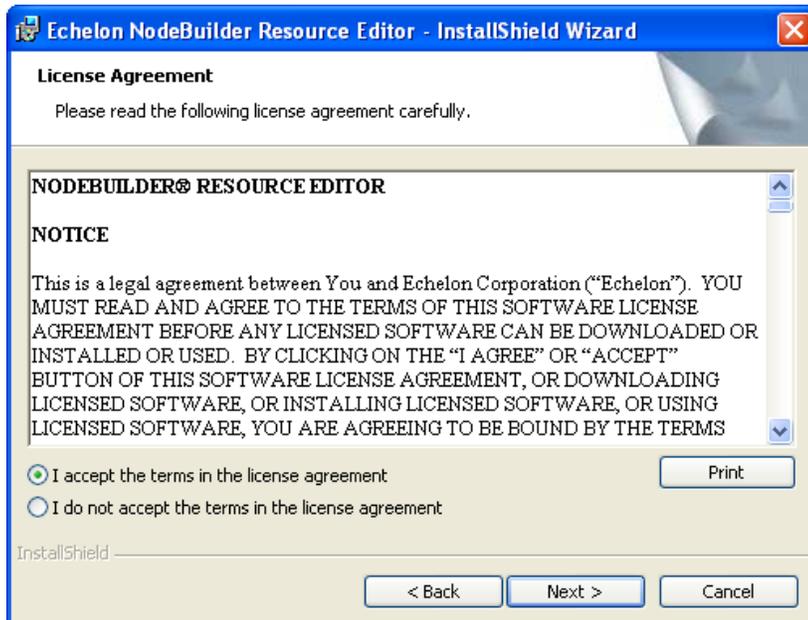
To use the new fast data log transfer feature, the device resource files for the subject data points must be installed on your computer running EES 2.2. You must also install an OpenLNS Server or LNS Server to use the new fast data log transfer feature. If you installed an OpenLNS Server, you already have the version 14 Standard Resource File Set. You can manually copy any user-defined device resource files to the **LonWorks\types\user\<company>** folder to your EES 2.2 computer. If you send binary data logs from your SmartServer to be converted to **CSV** format and the device resource files for the subject data points are not present, the conversion will fail.

To install the Echelon NodeBuilder Resource Editor, follow these steps:

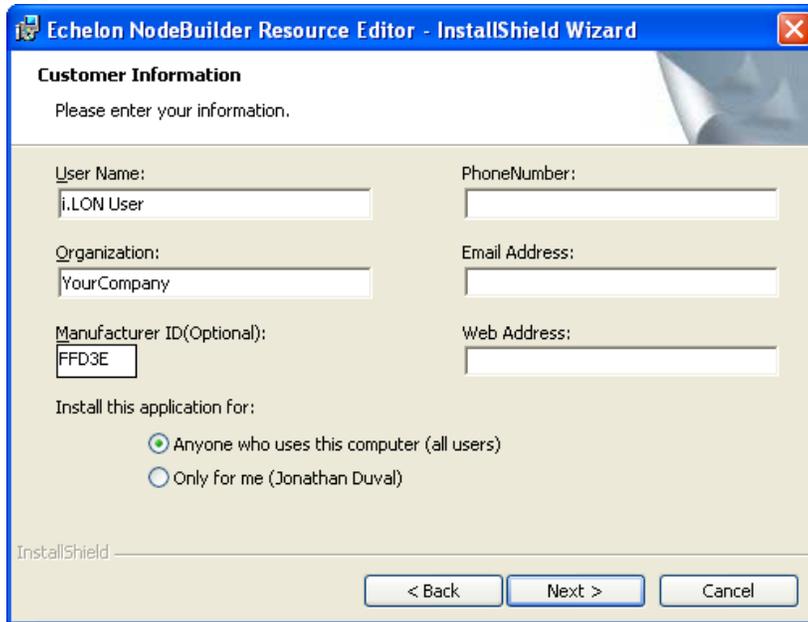
1. Click the Echelon SmartServer 2.2 SP – Install Wizard button in the taskbar to return to the SmartServer 2.2 installer, click **Echelon NodeBuilder Resource Editor** in the **Install Products** dialog.
2. The Welcome window of the NodeBuilder Resource Editor installer opens.



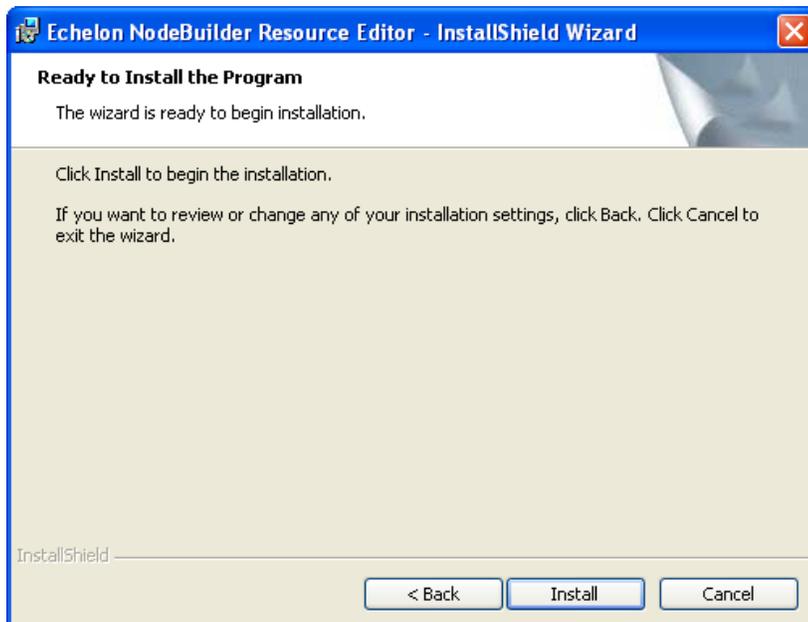
3. Read the information on the Welcome window and click **Next**. The License Agreement window appears.



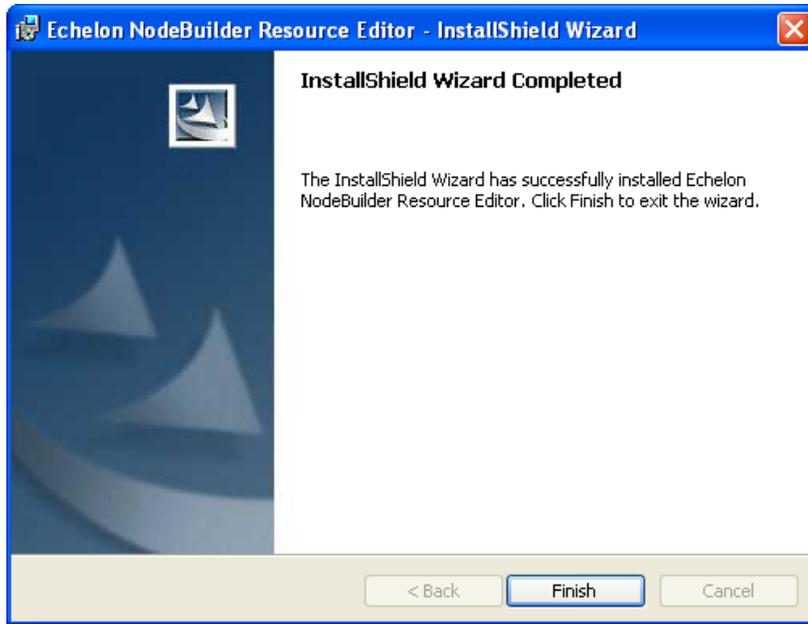
4. Read the license agreement. If you agree with the terms, click **Accept the Terms** and then click **Next**. The Customer Information window appears.



5. Enter your name, company name, phone number, e-mail address, and company Web site address in the appropriate fields. Optionally, you can enter your company's 5-digit manufacturer ID in hexadecimal format in the **Manufacturer ID** box (if you do not have a manufacturer ID, you can get a temporary manufacturer ID from LonMark at www.lonmark.org/mid). You can enter this information so that it can automatically be entered when you create resource files with the NodeBuilder Resource Editor. Click **Next**. The Ready to Install window appears.



6. Click **Install** to begin the NodeBuilder Resource Editor installation. After the NodeBuilder Resource Editor has been installed, a window appears stating that the installation has been completed successfully.



7. Click **Finish**.
8. If you installed the NodeBuilder Resource Editor on a computer that has not had any other Echelon software previously installed on it, you need to register the Echelon resource files in the resource catalog. To do this, follow these steps:
 - a. Start the NodeBuilder Resource Editor. To do this, click **Start**, point to **Programs**, point to **Echelon NodeBuilder Resources**, and then click **NodeBuilder Resource Editor**. The **Echelon NodeBuilder Resource Editor** opens
 - b. Click **File**, and then select **Add Folder**.
 - c. Browse to the **C:\Lonworks\types\user\echelon** directory, and then click **OK**.
 - d. Click **File**, and then select **Refresh Catalog**.

Installing a BACnet Interface

You can purchase and install a BACnet interface for the SmartServer. The BACnet interface is a custom app for the SmartServer provided by ConnectEx, Inc. It provides an interface that is compatible with all common BACnet AWS/OWS workstations. For more information on the BACnet interface for the SmartServer, contact [ConnectEx](#).

Configuring and Managing the SmartServer

This chapter describes how to connect your SmartServer to a TCP/IP network. It describes how to use the Setup Web pages to configure the SmartServer's properties.

It explains how to add dial-up connections to your SmartServer if an Ethernet connection is not readily available. It explains how to connect host devices such as remote SmartServers, OpenLNS Servers, e-mail servers, time servers, IP-852 Configuration Servers, and Web Connection Target servers to your local SmartServer. It describes how to configure your SmartServer as an IP-852 router and as a remote network interface (RNI). It describes how to manage your SmartServer, including how to view its performance; view its system health monitoring configuration, test its connections; replace it; activate the V40 interface on it; and migrate an i.LON 100 e3 server network configuration to a SmartServer.

SmartServer Configuration and Management Overview

You can connect and configure your SmartServer before using it to manage, monitor, and control your networks. To connect the SmartServer you assemble, mount, and wire the SmartServer as described in the *SmartServer Hardware Guide*, use an Ethernet cable to connect it to a TCP/IP network, and then open the SmartServer Web interface.

After you connect your SmartServer, you can use the SmartServer's Setup Web pages to set its IP address, SOAP/HTTP services, real-time clock, and security settings. After you configure the security settings, you can disable the **Setup - Security** Web page so that other users cannot modify the security settings. If you change TCP/IP properties marked with an asterisk (*) or security properties marked with a double-asterisk (**) you need to reboot your SmartServer to implement the changes.

You can create dial-up connections for your SmartServer if an Ethernet connection is not readily available. You can use the built-in analog modem on the SmartServer (certain hardware models only) or connect the SmartServer to an external GSM modem. If you create a dial-out connection, you can connect your SmartServer to other host devices via that connection.

You can connect a number of host devices to your SmartServer by adding them to the SmartServer's LAN or dial-up connections. You can add remote SmartServers, OpenLNS Servers, time (SNTP) servers, e-mail (SMTP) servers, IP-852 Configuration Servers (if you are not using the standard port on the SmartServer for IP-852 routing [1628]), and Web Connection Target servers (Web server that can receive SOAP/HTTP requests).

- Adding a remote SmartServer lets you connect the devices on your SmartServer to the devices on that remote SmartServer, and it lets you manage that remote SmartServer and the network attached to it from the Web interface of your local SmartServer.
- An OpenLNS Server lets you use the LNS Proxy Web service to synchronize the SmartServer to an OpenLNS network database; add the data points of external devices in OpenLNS managed networks to the SmartServer's built-in applications and your custom SmartServer Web pages; and maintain and manage the OpenLNS network databases in an OpenLNS Server.
- An e-mail server lets the SmartServer send out e-mail notifications when alarm conditions occur.
- A time server lets you synchronize the date and time on the SmartServer and the other host devices on the LAN to a common base.
- An IP-852 Configuration Server lets you create and manage IP-852 channels.
- A Web Connection Target server lets you send data logs, alarm logs, an event scheduler log, or any user-defined file from your SmartServer to a central enterprise system.

After you configure your SmartServer, you can select a network management service mode. You can run your SmartServer with OpenLNS network management services or you can use the SmartServer as a standalone network manager.

- In **LNS mode (LNS Auto or LNS Manual)**, the SmartServer uses an OpenLNS Server or LNS Server to manage the network. You must use LNS mode if your network is managed by an OpenLNS Server or an LNS Server. Using LNS mode requires you to install the Echelon Enterprise Services 2.2 from the SmartServer 2.2 DVD, install an OpenLNS or LNS Server, and then add an LNS Server to the LAN.
- In **Standalone** mode, the SmartServer directly manages the network. You must use standalone mode if an OpenLNS Server or LNS Server is not available for your network. You can use standalone mode to install and operate a small, single-channel network that does not require OpenLNS services or connections to other network management tools. Networks running in standalone mode are limited to a maximum of 300 devices (for FT-10 networks, you need to attach a physical layer repeater to the network to exceed the 64-device limit posed by the physical channel).

You can configure your SmartServer as an IP-852 router (if IP-852 routing is activated on your SmartServer) to integrate the network attached to your SmartServer into a single large LONWORKS network that runs over a high-speed IP backbone. You can also configure your SmartServer as an IP-852 router or as a remote network interface (RNI) to connect an OpenLNS or OpenLDV-based application to a LONWORKS network remotely via a TCP/IP connection.

You can manage your SmartServer by viewing its performance with the **Setup – System Info** Web page; viewing the configuration of its system health monitoring with the **systemhealth.conf** file on the SmartServer flash disk; testing its connections with the **Setup – Verify** Web page; backing it up to protect your network configuration and your custom SmartServer Web pages; upgrading the firmware when service packs become available; restoring the SmartServer from a backup or restoring it to its factory default settings with the SmartServer Web pages or the console application; replacing your SmartServer if there is a hardware failure; and activating the V40 interface so that you can add dynamic functional blocks to the **i.LON App (Internal)** device. You can also migrate an i.LON 100 e3 server network to the SmartServer.

This chapter describes how to perform the following tasks:

1. Connect the SmartServer.
2. Configure the SmartServer.
3. Create modem connections.
4. Add host devices to the LAN.
5. Select a network management service.
6. Configure the SmartServer as an IP-852 router or an RNI.
7. Manage the SmartServer.

Connecting the SmartServer

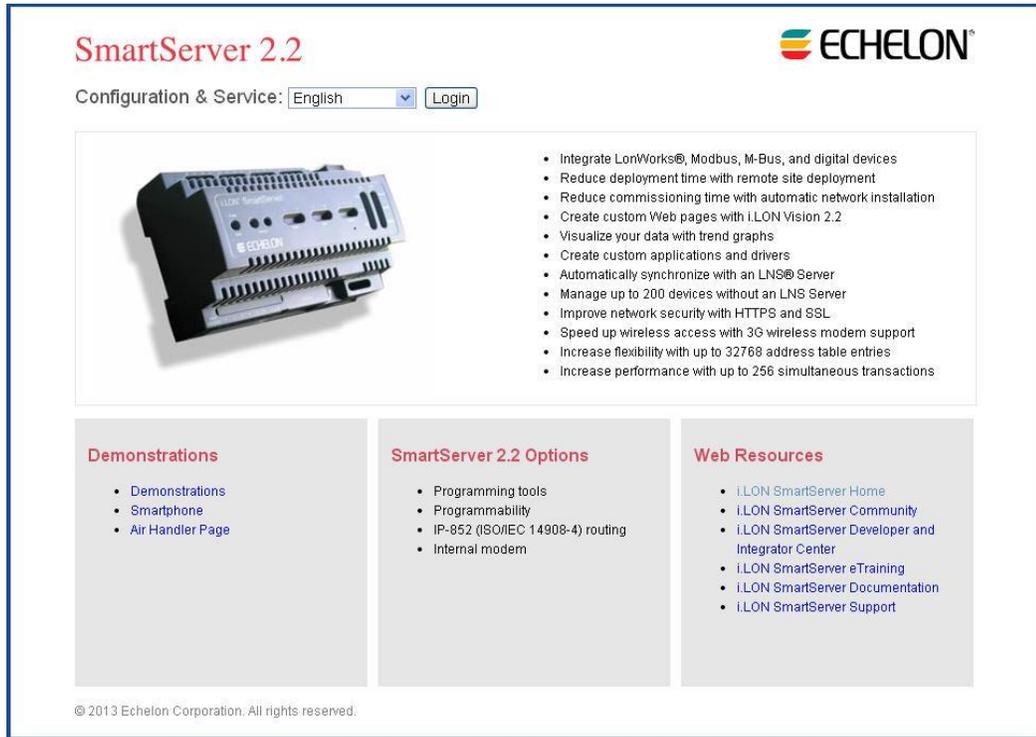
After you install the SmartServer software on your computer, you need to connect your SmartServer to a TCP/IP network. To connect your SmartServer, follow these steps:

1. Assemble, mount, and wire the SmartServer as described in the *SmartServer Hardware Guide*. Open the SmartServer Web pages using IPv4 or IPv6.
2. If you are using IPv4 to open the SmartServer Web pages, follow these steps:
 - a. If your computer is not on the same subnet as the SmartServer (192.168.1.x by default), open a Windows command prompt with administrator privileges on your computer and enter the following command:

```
route add 192.168.1.0 mask 255.255.255.0 %computername%
```

Note: To open the command prompt with administrator privileges, click **Start**, type **cmd** in the search box, right-click the **cmd.exe**, and then select **Run as Administrator**. If you receive a “The parameter is incorrect” error after entering the route command, replace **%computername%** with the IP address of your computer.
 - b. Open a Web browser and enter the IP address of your SmartServer. The default address is <http://192.168.1.222>.
3. If you are using IPv6 to open the SmartServer Web pages, follow these steps:
 - a. Enable the IPv6 interface on your computer. For more information on doing this on a Windows 7 computer, see <http://windows.microsoft.com/en-us/windows7/ipv6-frequently-asked-questions>.
 - b. Set up a DNS entry to create a hostname for the SmartServer. When setting up the DNS entry, use the default IPv6 address shown by the installation wizard (see step 18 in *Installing Echelon SmartServer Software* in Chapter 2)
 - c. Create the hostname for the SmartServer.

4. The SmartServer 2.2 home page opens.



5. In the **Configuration & Service** box, select the language to be used for the SmartServer Web interface. The SmartServer includes English (the default), German, French, Chinese, Korean, and Japanese languages, but you can work with the SmartServer in any one-byte or two-byte character language by translating the **.properties** file in the /web/nls/echelon folder on the SmartServer flash disk.

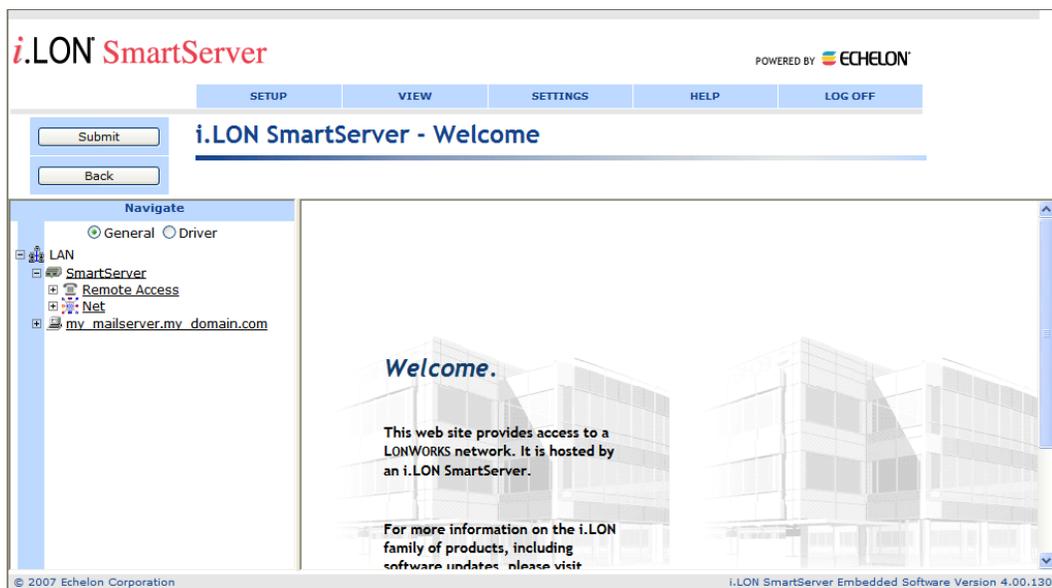
You can perform this language localization using either the demo version of the SmartServer 2.0 Programming Tools included on the SmartServer 2.2 DVD or using the full version on the SmartServer 2.0 Programming Tools included on the SmartServer 2.0 Programming Tools DVD. For more information on ordering the SmartServer 2.0 Programming Tools DVD, contact your Echelon sales representative.

See the *SmartServer 2.0 Programming Tools User's Guide* for more information on how to localize the language of the SmartServer Web interface.

6. Click **Login**. A Login dialog opens.



7. Enter the **User name** and **Password** for logging on to your SmartServer, which are both `ilon` by default, and then click **OK**. The **SmartServer - Welcome** Web page opens.



The navigation pane on the left side of the SmartServer Web pages provides a hierarchal view of the LAN on which your local SmartServer resides. The top level of the navigation pane shows the LAN icon, which represents the SmartServer's Ethernet connection. The host devices on the LAN are then listed one level below the LAN icon. When you initially connect your SmartServer, your local SmartServer and a sample e-mail server are the only host devices on the LAN. The remote access (modem) connections and the network attached to your local SmartServer are listed one level below the local SmartServer icon.

You can connect other host devices to your local SmartServer via its Ethernet connection or a dial-up modem connection. The host devices you can connect to your local SmartServer include OpenLNS Servers, e-mail (SMTP) servers, time servers (SNTP), IP-852 Configuration Servers, Web Connection Target servers, and remote SmartServers. See *Adding Host Devices* later in this chapter for more information on how to do this.

Configuring the SmartServer

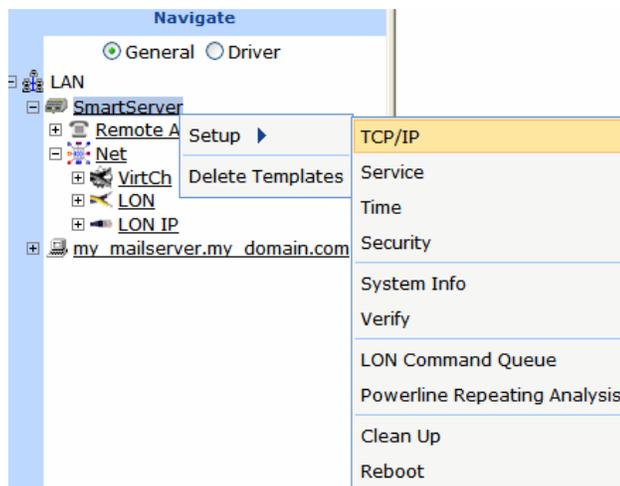
After you can connect your local SmartServer to a TCP/IP network, you can use the SmartServer's Setup Web pages to configure its TCP/IP, SOAP/HTTP, time, and security properties. When you change the TCP/IP and security properties of the SmartServer, you may be required to reboot your SmartServer. The following sections describe how to perform the following configuration tasks for a SmartServer.

- Configure TCP/IP properties.
- Configure SOAP/HTTP properties.
- Configure time properties.
- Configure security properties.
- Reboot the SmartServer.

Configuring TCP/IP Properties

If you are connecting your SmartServer directly to a TCP/IP network via the Ethernet port, you must configure the SmartServer's TCP/IP connection properties. To configure the TCP/IP properties, follow these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **TCP/IP** on the shortcut menu.



Alternatively, you can click **Setup** and then click **TCP/IP** to configure the TCP/IP properties on your local SmartServer.

2. The **Setup – Local SmartServer (TCP/IP)** Web page opens.

Setup - Local i.LON SmartServer



Hostname

IP Property	Value
<input checked="" type="checkbox"/> Automatically obtain IP Address *	
IPv4 address *	<input style="width: 40px;" type="text" value="10"/> <input style="width: 40px;" type="text" value="2"/> <input style="width: 40px;" type="text" value="124"/> <input style="width: 40px;" type="text" value="111"/>
Subnet Mask *	<input style="width: 40px;" type="text" value="255"/> <input style="width: 40px;" type="text" value="255"/> <input style="width: 40px;" type="text" value="128"/> <input style="width: 40px;" type="text" value="0"/>
Default Gateway *	<input style="width: 40px;" type="text" value="10"/> <input style="width: 40px;" type="text" value="2"/> <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="1"/>
DNS Property	Value
<input type="checkbox"/> Automatically obtain IP Address *	
Default DNS Server *	<input style="width: 40px;" type="text" value="0"/>
Backup DNS Server *	<input style="width: 40px;" type="text" value="0"/>

- Configure the following IPv4 properties. You must reboot the SmartServer to implement changes made to properties that are marked with an asterisk (*).

Hostname

Displays the TCP/IP hostname of the SmartServer. When the SmartServer establishes a connection with an OpenLNS Server, it provides its fully qualified host/domain name so the OpenLNS Server knows which LONWORKS database to open.

By default, the hostname is **SmartServer**. The URL of the SmartServer is the hostname followed by the DNS suffix. For example, if the hostname is SmartServerAlpha and the domain suffix is ABCcorp.com, the URL would be SmartServerAlpha.ABCcorp.com.

Set a unique hostname if you want to have the DHCP server register the hostname with the DNS server, or when you want to manually register with the DNS server administrator.

The hostname must start with a letter and it may include numbers, letters, and hyphens, but it cannot include underscores or spaces. The maximum hostname length is 19 characters.

IP Property

If you modify any of the following IP properties, you must reboot your SmartServer to implement the changes.

Automatically Obtain IP Address Enables the SmartServer to obtain its IP address, subnet mask, and default gateway from the local network's DHCP server. As soon as the DHCP server is contacted, the SmartServer reboots and implements the new IP address. If the DHCP server cannot be contacted, the IP address, subnet mask, and gateway are temporarily set to the following addresses:

- IP address: 192.168.1.222
- Subnet mask: 255.255.255.0
- Gateway: 192.168.1.222

Selecting this option makes the subsequent **IPv4 Address**, **Subnet Mask**, and **Default Gateway** properties unavailable.

If you plan to use the SmartServer as an IP-852 router, you must ensure that the SmartServer uses a fixed IP address. See the *DHCP* section in Chapter 4 of the *IP-852 Channel Users Guide* for more information on this issue.

IPv4 Address Enter the static IPv4 address used by the SmartServer. Make sure that the IP address you enter is not in a range reserved by a local DHCP server. The default IPv4 address is **192.168.1.222**.

Note: If you are using a modem connection, enter a static IP address that is outside the range of the SmartServer's Ethernet connection.

This property is unavailable if you select **Automatically Obtain IP Address**.

Subnet Mask Enter the subnet mask used by the SmartServer. The default subnet mask is **255.255.255.0**.

This property is unavailable if you select **Automatically Obtain IP Address**.

Default Gateway Enter the IP address of the gateway used by the SmartServer. The default IP address is **192.168.1.222**.

This property is unavailable if you select **Automatically Obtain IP Address**.

DNS Property If you modify any of the following DNS properties, you must reboot your SmartServer to implement the changes.

Automatically Obtain IP Address Enables the SmartServer to obtain its DNS Server Address from the local network's DHCP server. If the DHCP server cannot be contacted, this property is temporarily set to **0.0.0.0**. As soon as the DHCP server is contacted, the SmartServer will reboot itself to implement the new DNS Server IP address.

Selecting this option makes the subsequent **Default DNS Server** and **Backup DNS Server** properties unavailable.

Default DNS Server Enter the IP address of the primary DNS server used to resolve OpenLNS Server names, DNS server names, hostnames, and so on. An IT department typically provides this information. The default IP address of the default DNS server is **0.0.0.0**.

This property is unavailable if you select **Automatically Obtain IP Address**.

Backup DNS Server Enter the IP address of the secondary DNS server used to resolve names. The default IP address of the backup DNS server is **0.0.0.0**.

This property is unavailable if you select **Automatically Obtain IP Address**.

4. Select the **Advanced** check box to configure IPv6 properties. The IPv6 properties appear on the Web page.

<input checked="" type="checkbox"/> Advanced	
IPv6 Property	Value
<input type="checkbox"/> Enable IPv6 Interface *	
Link Local Address (Autoconfigured)	fe80::2d0:71ff:fe02:a18
Global Address (Autoconfigured)	
Current Default Gateway	
<input type="checkbox"/> Use additional Static Address *	
IPv6 Address *	:/64
Default Gateway *	
IPv6 DNS Property	Value
<input type="checkbox"/> Automatically obtain IP Address *	
Default DNS Server *	
Backup DNS Server *	

5. Configure the following IPv6 properties. You must reboot the SmartServer to implement changes made to properties that are marked with an asterisk (*).

IPv6 Property

Enable IPv6 Interface

Enables the SmartServer to connect to devices and servers that use IPv6. This option is selected by default.

Link Local Address (auto configured)

Displays the IPv6 link local address assigned to the SmartServer. The link local address can only be accessed by IPv6 devices on the local network to which the SmartServer is attached. If a router is present between your computer and the SmartServer you will not be able to use this address to communicate with the SmartServer. Both addresses are automatically configured by the SmartServer when the IPv6 interface is enabled.

Note: To use this local IPv6 link local address, you need to append the ‘%’ character and the number of your computer’s network card to the IPv6 address. You can obtain this number by entering the **ipconfig** in the Windows command prompt. The network interface is normally named “Ethernet adapter Local Area Connection”, and the card number is the number after the ‘%’ character in your computer’s IPv6 address.

For example, if your SmartServer’s IPv6 address is FE80::2D0:71FF:FE03:0122 and your computer’s IPv6 address is FE80::213:72FF:FE98:a649%5, enter the following in your Web browser to access the SmartServer via IPv6:

http://FE80::2D0:71FF:FE03:0122%5

<i>Global Address (auto configured)</i>	Displays the IPv6 global address assigned to the SmartServer. The global address is accessible to IPv6 devices outside the local network to which the SmartServer is attached.
<i>Current Default Gateway</i>	Displays the default gateway used by SmartServer for IPv6 addressing.
<i>Use Additional Static Address</i>	Enables you to manually assign the SmartServer an additional IPv6 address and gateway in the properties below, in addition to the default link local address and global address displayed on the Web page. If you select this option, you must reboot your SmartServer to implement any changes.
<i>IPv6 Address</i>	<p>Enter an additional IPv6 address for the SmartServer to use. The addresses must conform to IPv6 addressing standards or an error will occur when you click Submit. The following provides two example IPv6 addresses:</p> <p>2002:1234:0000:0000:02d0:71ff:fe00:00aa 2002:1234::2d0:71ff:fe00:aafe::fefe:dddd</p> <p>The IPv6 Address field also supports an optional prefix length specifier, which must be a “/” followed by a decimal integer between 0 and 128. If it is omitted, it will default to 64. The following provides an IPv6 address with the prefix length specifier 64:</p> <p>2002:1234::2d0:71ff:fe00:aa/64</p> <p>For more details on IPv6 addressing, see “<i>RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture</i>” online at: http://www.faqs.org/rfcs/rfc3513.html. Section 2.2 of the RFC describes the addressing formats shown above in more detail, and section 2.3 of the RFC provides more details on prefix specifiers.</p>
<i>Default Gateway</i>	Enter an additional IPv6 address for the SmartServer to use as a gateway.

IPv6 DNS Property

<i>Automatically Obtain IP Address</i>	<p>Enables the SmartServer to obtain its DNS Server IPv6 address from the local network’s DHCP server. If the DHCP server cannot be contacted, this property is temporarily set to 0.0.0.0. As soon as the DHCP server is contacted, the SmartServer will reboot itself to take on the new DNS Server IP address.</p> <p>Selecting this option makes the subsequent Default DNS Server and Backup DNS Server properties unavailable.</p>
<i>Default DNS Server</i>	<p>Enter the IPv6 address of the primary DNS server used to resolve OpenLNS Server names, DNS server names, hostnames, and so on. An IT department typically provides this information.</p> <p>This property is unavailable if you select Automatically Obtain IP Address.</p>
<i>Backup DNS Server</i>	<p>Enter the IPv6 address of the secondary DNS server used to resolve names.</p> <p>This property is unavailable if you select Automatically Obtain IP Address.</p>

TCP/IP Property

Ethernet Media Speed

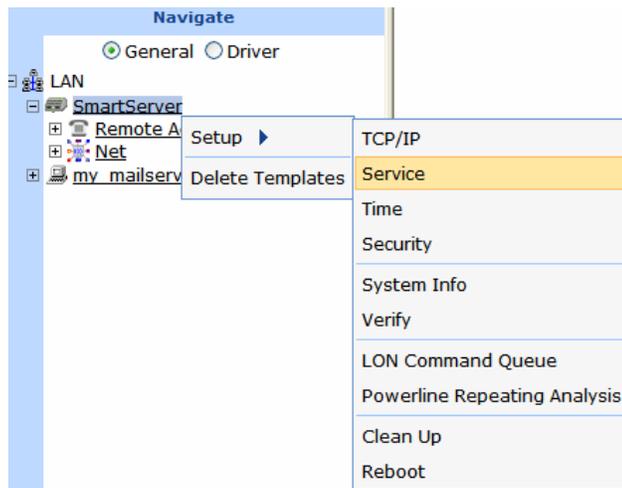
You can select the Ethernet speed (10 or 100 MB per second) and mode (full-duplex or half-duplex) of the SmartServer. You have five choices:

- **Automatic.** The SmartServer employs autonegotiation to determine the Ethernet speed and mode to use based upon the device with which it is communicating. This is the default.
 - **100 MB Full-Duplex.** Data streams in both directions simultaneously at 100 MB/s.
 - **100 MB Half-Duplex.** Data streams in one direction at a time at 100 MB/s
 - **10 MB Full-Duplex.** Data streams in both directions simultaneously at 10 MB/s.
 - **10 MB Half-Duplex.** Data streams in one direction at a time at 10 MB/s
6. Click **Submit** to save the changes. If you change the IP address and want to continue to have Web access to your SmartServer you must change your computer's TCP/IP settings to place it on the same subnet as the SmartServer.
 7. If you modified a property marked with an asterisk (*), you must reboot your SmartServer. See the *Rebooting the SmartServer* section later in this chapter for more information on how to do this.

Configuring SOAP/HTTP Service Properties

You can configure your SmartServer's SOAP/HTTP service properties, following these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **Service** on the shortcut menu.



Alternatively, you can click **Setup** and then click **Service** to configure the SOAP/HTTP properties on your local SmartServer.

2. The **Setup – Local SmartServer (Service)** Web page opens.

Setup - Local i.LON SmartServer



Hostname
SmartServer

i.LON SmartServer Property	Value
Logical ID	030000197B82
SOAP Path	/WSDL/iLON100.WSDL
HTTP Port (Web Server / SOAP)	80
Retry Time (defaults to 120 s)	120.0 Seconds
Format values in WebBinder SOAP messages using	Data Point Format
<input type="checkbox"/> Maximum Age	Seconds

* For i.LON SmartServer Destination Servers, SOAP Authentication Parameters may be configured in the webparams.dat file

3. Configure the following SOAP/HTTP service properties.

Hostname

Displays the TCP/IP hostname of the SmartServer. When the SmartServer establishes a connection with an OpenLNS Server, it provides its fully qualified host/domain name so the OpenLNS Server knows which LONWORKS database to open.

By default, the SmartServer's hostname is **SmartServer**. The URL of the SmartServer is the hostname followed by the DNS suffix. For example, if the hostname is SmartServerAlpha and the domain suffix is ABCcorp.com, the URL would be SmartServerAlpha.ABCcorp.com.

Set a unique hostname if you want to have the DHCP server register the hostname with the DNS server, or when you want to manually register with the DNS server administrator.

The hostname must start with a letter and it may include numbers, letters, hyphens, and underscores, but it cannot include spaces. The maximum hostname length is 19 characters.

SmartServer Property

Logical ID

Displays the user-specified identifier used to manage the SmartServer. By default, the logical ID is set to the Neuron ID of the SmartServer's **i.LON App** device. You can change the logical ID to any value containing one or more 2-digit hex pairs (00-FF). For example, 00, 00FF, and 00FF00 are legal logical IDs.

SOAP Path

The path on the SmartServer to which SOAP messages should be transmitted. This is typically the location of the WSDL or ASMX file on the server where it receives SOAP messages. The default path is **/WSDL/iLON100.WSDL** (the default location of this file on a SmartServer).

You can password protect the SmartServer's WSDL using the **i.LON Web Server Security and Parameters** program, or by manually

configuring the **webparams.dat** file located at the root level of the SmartServer 's flash disk. See *Appendix C* for more information on protecting the WSDL using the **i.LON Web Server Security and Parameters** program.

HTTP Port (Web Server/SOAP)

The port the your local SmartServer uses to serve HTTP requests (SOAP and WebDAV). The default value is **80**, but you may change it to any valid port number. Contact your IS department to ensure your firewall is configured to allow access to the server on this port.

Retry Time

Set the amount of time (in seconds) after which the local SmartServer will not resend failed Web Connection connection messages to the Web Connection destination. The default value is **120** seconds.

The local SmartServer automatically attempts to resend failed Web Connection connection messages to the Web Connection destination every 45 seconds.

Format Values in Web Connection SOAP Messages Using

Select the format used for communicating data point values to the Web Connection destination. You have two choices:

- **Data Point Format.** Data point values are transmitted in the format defined by their SNVT, UNVT, SCPT, or UCPT.
- **Raw HEX.** Data point values are transmitted in raw hex.

Maximum Age

Specify the maximum age (in seconds) to be written to the target data points on the Web Connection destination when the local SmartServer sends updated values to them.

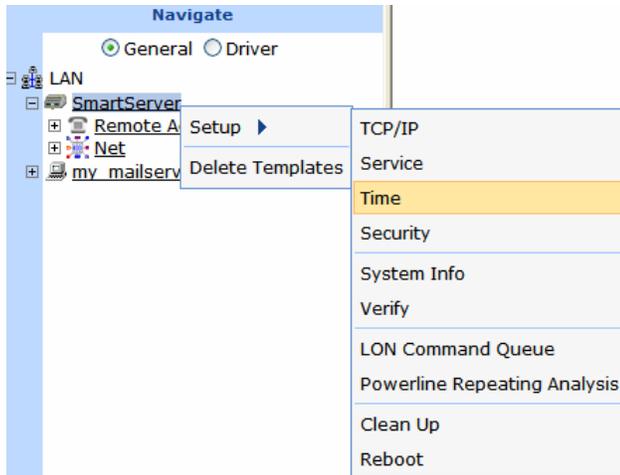
If the Web Connection destination cannot communicate with the parent device of the target data point, the Web Connection destination caches the updated value it received from the local SmartServer. When the device goes online, the cached value is written to the target data point provided that time the value has been cached is less than the maximum age. If the value has been cached longer than the maximum age, the value is not written to the target data point.

4. Click **Submit** to save the changes. Click **Back** to leave all fields unchanged.

Configuring Time Properties

You can configure the SmartServer's real-time clock, following these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **Time** on the shortcut menu.



Alternatively, you can click **Setup** and then click **Time** to configure the time settings on your local SmartServer.

2. The **Setup – Time** Web page opens.

Setup - Time	
Property	Value
Default Time Server	0.0.0.0:123
Backup Time Server	0.0.0.0:123
Last Time Sync	Unknown
Timezone	(GMT-08:00) Pacific Time (US & Canada) ▼
Date and Local Time	2007 Nov 28 15 : 38 : 08 <input type="button" value="Refresh"/>

3. Configure the following time settings:

Default Time Server Displays the IP address of the designated default SNTP time server. See *Adding a Time (SNTP) Server* for how to add a time server to the LAN and select it as the default.

Backup Time Server Displays the IP address of the designated backup SNTP time server. See *Adding a Time (SNTP) Server* for how to add a backup time server to the LAN.

Last Time Sync Displays the last time in which the SmartServer synchronized its clock with the default SNTP time server. The amount of time varies between 1 to 15 minutes, depending on the difference in time between the SmartServer's clock and the SNTP time server. As the difference approaches 75 ms or less, the interval will keep increasing until it reaches the maximum of 15 minutes.

Time Zone Select the time zone in which the SmartServer is located.

Date and Local Time Displays the time and date currently stored in the SmartServer's real time clock. You may need to refresh the Web page to view the current time. You can manually enter a different time and/or date.

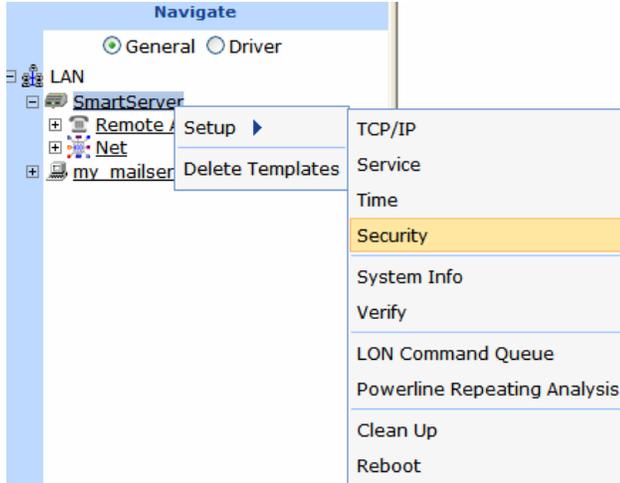
Note: If you have configured an SNTP time server, changes to the time and date will be overwritten the next time the SmartServer is synchronized with the SNTP time server.

4. Click **Submit** to save the changes. Click **Back** to leave all fields unchanged.

Configuring Security Properties

You can configure the SmartServer's security properties, including enabling HTTPS to further secure your SmartServer's Web pages. To set the SmartServer's security settings, follow these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu.



Alternatively, you can click **Setup** and then click **Security** to configure the security settings on your local SmartServer.

2. The **Setup – Security** Web page opens.

Setup - Security	
General	Value
<input checked="" type="checkbox"/> Enable this Page without Security Access	
FTP/Telnet User Name	<input type="text" value="ilon"/>
FTP/Telnet Password	<input type="button" value="Change Password"/>
Service	Port
<input checked="" type="checkbox"/> Enable FTP	<input type="text" value="21"/> *
<input checked="" type="checkbox"/> Enable Web Server **	<input type="text" value="80"/> **
<input checked="" type="checkbox"/> Enable SSL Web Server **	<input type="text" value="443"/> **
<input checked="" type="checkbox"/> Enable Downlink RNI Connections	<input type="text" value="1628"/> *
<input checked="" type="checkbox"/> Enable Telnet	<input type="text" value="23"/> *
<input checked="" type="checkbox"/> Enable Remote Dial-In	Not Applicable
<input checked="" type="checkbox"/> Enable Remote Reboot	Not Applicable
<input checked="" type="checkbox"/> Enable LonScanner Connections	<input type="text" value="1629"/> *
<input type="checkbox"/> Capture all Packets on LonScanner Connections	

3. You can configure the following security settings if secure access mode is enabled on the SmartServer (it is enabled by default), or if the **Enable This Web Page Without Security Access** check box is selected. If secure access mode is currently disabled, you can re-enable secure access using the console application, or you can perform a secure access reset. See the next section, *Enabling and Disabling Secure Access*, for more information.

For properties marked with an asterisk (*), you must first select the check box or button on the left to configure them. If the check box is cleared, the property is unavailable. You must reboot the SmartServer to implement changes made to properties that are marked with a double asterisk (**).

General

Enable This Page Without Security Access Reset Enables the security settings on this Web page to be modified regardless if secure access is disabled. This check box is selected by default.

You can clear this option to prevent users with access to your SmartServer from modifying your security settings when secure access mode has been disabled.

For more information on secure access mode, see *Enabling and Disabling Secure Access* in the next section.

FTP/Telnet User Name Displays the user name for FTP/Telnet access to your SmartServer. The default user name is **ilon**. You can enter a different user name, which may be up to 20 characters long and contain letters, numerals, and the underscore character. Change the user name if your SmartServer is accessible from the Internet.

FTP/Telnet Password The default password is **ilon**. You can click **Change Password** to enter a new password for FTP/Telnet access to your SmartServer. In the **New Password** box, enter your new password, which may be up to 20 characters long and contain letters, numerals, and the underscore character. Re-enter the password in the **Re-enter Password** field. Change the password if your SmartServer is accessible from the Internet.

Service

Enable FTP Enables FTP access to the SmartServer. If you select this option, enter the port the SmartServer will use for FTP communication in the **Port** column. This option is selected by default and the port is set to **21**.

Enable Web Server Enables HTTP access to the SmartServer. If you select this option, enter the port the SmartServer will use for HTTP communication in the **Port** column.

This option is selected by default and the port is set to **80**.

If you will be using HTTPS to secure your SmartServer Web pages, clear this option to disable HTTP access.

If you clear this option, you will not be able to access the SmartServer Web pages via HTTP after a reset. To re-enable HTTP access, perform a security access reset. This will reset this option.

<i>Enable SSL Web Server</i>	<p>Enables HTTPS access to the SmartServer. HTTPS is a combination of the Hypertext Transfer Protocol and a cryptographic protocol such as SSL, which is used by the SmartServer 2.2. Using HTTPS/SSL, you can help protect your SmartServer from unauthorized access and secure your SmartServer's data.</p> <p>If you select this option, enter the port the SmartServer will use for HTTPS communication in the Port column. This option is selected by default and the port is set to 443.</p> <p>To use HTTPS/SSL to secure your SmartServer, you must create a self-signed SSL certificate or obtain a direct-signed SSL certificate and install it on your SmartServer. For more information on acquiring and installing an SSL certificate on your SmartServer, see the next section, <i>Using HTTPS/SSL</i>.</p>
<i>Enable Downlink RNI Connections</i>	<p>Enables the SmartServer to be used as a Remote Network Interface (RNI). This allows an OpenLNS application running on your computer to access an OpenLNS Server remotely. This option is selected by default and the port on which the SmartServer listens for downlink requests is set to 1628.</p> <p>For more information on using the SmartServer as an RNI, see <i>Using the SmartServer as an RNI</i> later in this chapter.</p>
<i>Enable Telnet</i>	<p>Enables Telnet access to the SmartServer's console application. This option is selected by default and the port is set to 23.</p> <p>For more information on the SmartServer console application, see Appendix B, <i>Using the SmartServer Console Application</i>.</p>
<i>Enable Remote Dial-in</i>	<p>Enables an OpenLNS Server to dial-in to the SmartServer. This option is selected by default.</p> <p>See <i>Adding an OpenLNS Server to the LAN</i> later in this chapter for more information.</p>
<i>Enable Remote Reboot</i>	<p>Enables the SmartServer to be rebooted remotely via the Setup - Reboot Web page. This option is selected by default.</p>
<i>Enable LonScanner Connections</i>	<p>Enables the SmartServer to be connected to the LonScanner Protocol Analyzer tool, which you can use to monitor and diagnose network traffic. This option is selected by default and the port is set to 1629. If you select this option, enter the port number to use to connect to the protocol analyzer in the Port column.</p> <p>For more information on the protocol analyzer, see the <i>LonScanner Protocol Analyzer User's Guide</i>.</p>
<i>Capture all Packets on LonScanner Connections</i>	<p>Enables packets directly transmitted to the internal devices on the SmartServer to be viewed with the LonScanner Protocol Analyzer tool. These packets will still not be sent on the physical network. This option is cleared by default.</p> <p>For more information on the protocol analyzer, see the <i>LonScanner Protocol Analyzer User's Guide</i>.</p>

LonTalk Authentication

Raw MD5 Authentication Key

You can enter an MD5 authentication key to be used for authentication when using the SmartServer as an RNI. This value must match the one specified in the LONWORKS Interfaces control panel application. This box is unavailable if you are using a Text Secret Phrase for authentication.

Note: Changing the key here is generally not necessary, as it is automatically updated when modified in the LONWORKS Interfaces control panel application (provided that the previous key was known by the control panel, or was the default key [all zeros]).

For more information on using the SmartServer as an RNI and on the LONWORKS Interfaces application, see *Using the SmartServer as an RNI* in this chapter

Text Secret Phrase

You can enter a text secret phrase instead of using a Raw MD5 authentication key for authentication when using the SmartServer as an RNI. This box is unavailable if you are using a raw MD5 authentication key for authentication.

4. Click **Submit** to save the changes. Click **Back** to leave all fields unchanged.
5. If you modified a property marked with a double asterisk (**), you must reboot your SmartServer. See the *Rebooting the SmartServer* section later in this chapter for more information on how to do this.

Using HTTPS/SSL

By default, the SmartServer includes a self-signed SSL certificate for the “SmartServer 2.2” hostname. The name of an SSL certificate cannot match the host name; therefore, a warning will appear in your Web browser each time you open your SmartServer if HTTPS is enabled. This SSL certificate is included for demonstration purpose only and cannot provide secure communication.

To use HTTPS/SSL on a SmartServer, you must replace the default SSL certificate with one that has been issued for that SmartServer (each SmartServer requires its own certificate). You can either create a self-signed certificate and install it into your Web browser, or you can buy a direct-signed certificate from an accredited certificate authority. The SmartServer does not support intermediate certificates; therefore, make sure that the certificate authority issues direct signed certificates.

After receiving an SSL certificate for your SmartServer, save the private key as **private_key.pem** and save the certificate as **server_cert.pem**, and then upload both files to the **/config/certs** folder on your SmartServer flash disk.

Enabling and Disabling Secure Access Mode

You can control whether the security settings on your SmartServer can be modified via the **Setup – Security** Web page. You do this by enabling and disabling secure access mode via the console application.

To re-enable secure access temporarily, enter the `enable secureaccess` command. Users will be able to access the security settings until your SmartServer is rebooted. To keep secure access mode enabled after the next reboot, enter the `enable secureaccess always` console command (this is the default secure access mode setting).

To disable secure access temporarily, enter the `disable secureaccess` command on the console application. Users will not be able to access the security settings until your SmartServer is rebooted. You can keep secure access mode disabled after the next reboot by entering the `disable secureaccess always` command. You must also clear the **Enable This Page Without Security Access Reset** option on the **Setup - Security** Web page to ensure that the security settings are protected; otherwise, users will still be able to access them even when secure access mode is disabled.

See Appendix B, *Using the SmartServer Console Application*, for more information on the `enable secureaccess` and `disable secureaccess` console commands.

Performing a Secure Access Reset

If you have disabled secure access on your SmartServer and you do not have access to the console application, but you do have access to the SmartServer hardware, you can perform a security access reset to re-enable secure access. To do this, follow these steps:

1. To ensure maximum security, disconnect your computer and SmartServer from the LAN.
2. Remove the SmartServer from the TCP/IP network and attach it to the computer using an Ethernet cable or a local server hub. This step is optional, but it is likely needed because performing a security access reset temporarily resets the SmartServer's IP address to 192.168.1.222.
3. Press and hold the service pin on the SmartServer hardware.
4. Reboot the SmartServer while holding down the service pin. You can reboot using the SmartServer hardware or the SmartServer Web pages.
 - To reboot using the SmartServer hardware, use a small wire such as a paper clip to press the reset switch located just below the Output LEDs on top of the SmartServer.
 - To reboot using the SmartServer Web pages, right-click the SmartServer icon in the navigation pane in the left frame, point to **Setup**, select **Reboot** from the shortcut menu, and then click **Reboot** in the **Setup – Reboot** dialog.
5. Continue holding the service pin. In approximately 10 seconds, all the LEDs on the SmartServer will illuminate.
6. Approximately 30 seconds from when the reboot began, the service LED will illuminate solid yellow. At this point you can release the service pin.
7. The SmartServer enters secure access mode and its IPv4 address, subnet mask, and gateway are temporarily changed to **192.168.1.222**, **255.255.255.0**, and **192.168.1.222**, respectively (IPv6 addresses are not changed during this process). They are returned to their specified IP addresses after the SmartServer is rebooted.

Note: The IPv4 address change could place the SmartServer on a subnet with which your computer cannot communicate. If this occurs, you can either modify your computer's IP configuration and place it on the 192.168.1.* subnet, or enter the following command in the Windows Command Prompt window with administrator privileges:

```
route add 192.168.1.0 mask 255.255.255.0 %computername%
```

To open the command prompt with administrator privileges, click **Start**, type `cmd` in the search box, right-click the `cmd.exe`, and then select **Run as Administrator**. If you receive a "The parameter is incorrect" error after entering the route command, replace `%computername%` with the IP address of your computer.

This command allows your computer to communicate with the SmartServer even when they are not on the same subnet. This command does not persist through computer reboots, but you can add it to the startup script for your computer or add the `-p` option to the route add command listed above.

Securing SmartServer Web Pages

You can secure the Web pages on your SmartServer using the **iLON Web Server Security and Parameters** program. Using this tool, you add security realms for to the `webParams.dat` file located at the root of the SmartServer's flash disk. A realm defines which files (Web pages) and folders on the SmartServer can be accessed by which users from which IP addresses.

To secure a SmartServer Web page, you create a realm for that Web page's `.htm` file, which is located in the SmartServer's root/web/user/echelon folder, and define which users can access it from which

locations. After you create a realm, you use the tool to create or update a **webParams.dat** file, and you then transfer the file via FTP to the SmartServer's root directory.

After transferring the **webParams.dat** file to the SmartServer's root directory, users must enter the user name and password that you defined to access the Web page. You can secure all the Web pages on your SmartServer by creating a realm for the main.htm file in the root/web/user/echelon folder.

For more detailed information on securing Web pages using the **i.LON Web Server Security and Parameters** program, see Appendix C, *Securing the SmartServer*.

Rebooting the SmartServer

You must reboot your SmartServer if you change TCP/IP properties in the **Setup – Local SmartServer** Web page that are marked with an asterisk (*), change the security properties in the **Setup – Security** Web page that are marked with a double asterisk (**), change the country/region of the SmartServer's internal analog modem, or add an IP-852 routing or programming license to your SmartServer.

Rebooting executes the SmartServer's shutdown and startup scripts, stopping and re-loading the SmartServer's modules in an orderly fashion. The reboot process takes approximately 5 to 10 minutes depending on the complexity of your network configuration. While the SmartServer is rebooting, the LEDs on the hardware will flash. Once the reboot is complete, the green Power/Wink LED will stay on solidly.

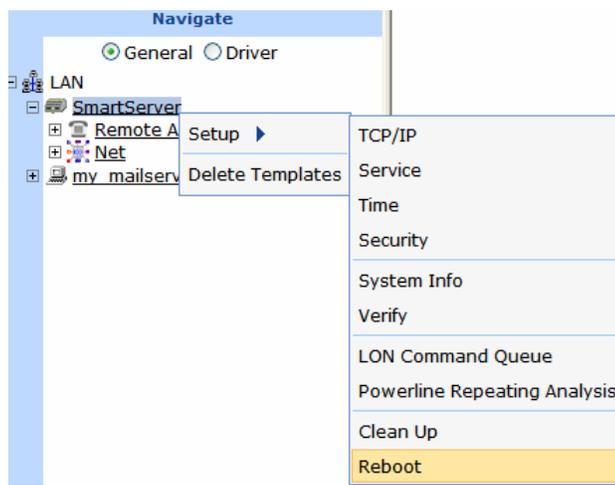
If your SmartServer is not behind a firewall, the **SmartServer - Welcome** Web page will open automatically once the reboot is complete. If your SmartServer is behind a firewall, you may need to close and then re-open your Web browser.

If DHCP is enabled, this page may not redirect the Web browser to the **SmartServer - Welcome** Web page properly. This because the new address from the DHCP server is unknown. If this is the case, issue the `show all` command from the console application, or ask your network administrator to determine the new IP address of the SmartServer. See Appendix B, *Using the SmartServer Console Application*, for more information on the console application.

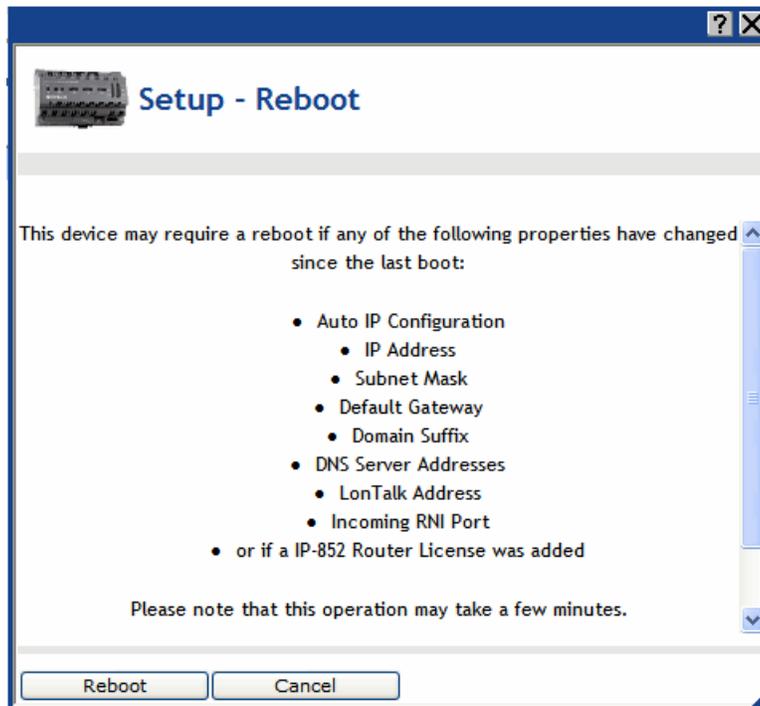
If your DHCP server has the capability to dynamically propagate newly assigned device IP address and target name to the DNS server (as is the case with the WIN2K DHCP server), you should be able to connect to the SmartServer after reset using its fully qualified hostname.

To reboot the SmartServer, follow these steps:

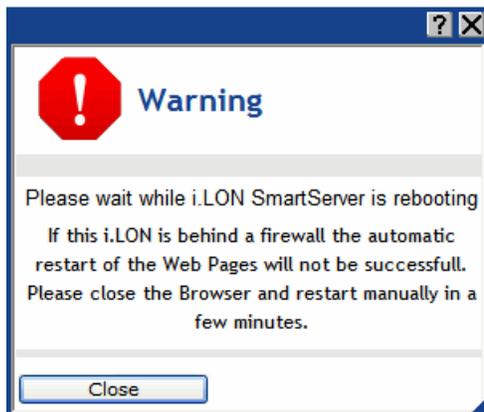
1. Right-click the SmartServer to be rebooted, point to **Setup**, and then select **Reboot** from the shortcut menu.



2. The **Reboot** dialog opens.



3. Click **Reboot**. The following warning opens:



It takes approximately 5 to 10 minutes for the SmartServer to finish rebooting. When the SmartServer has finished rebooting, this dialog closes and the **SmartServer - Welcome** Web page opens automatically. If your SmartServer is behind a firewall, you may need to close and then re-open your Web browser.

Creating Modem Connections

You can use modem connections to access a SmartServer remotely and to connect it to a TCP/IP network so that it can communicate with host devices such as remote SmartServers, OpenLNS Servers, e-mail servers, time servers, IP-852 Configuration Servers, and Web Connection Target servers. Modem connections are useful for networks in remote locations where an Ethernet connection is not readily available. To use a modem connection, your SmartServer must either contain an internal analog modem or be connected to a third-party external GSM modem via its RS-232 serial port. In order for your SmartServer to connect to host devices via modem, you must add and configure one or more dial-out connections to the modem. The dial-out connections you can create consist of analog, GPRS, and persistent GPRS.

To create modem connections for your SmartServer, you do the following:

1. Select the modem type (internal analog modem or external GSM modem).
2. Configure the modem for dial-in connections to the SmartServer.
3. Configure the modem for dial-out connections to host devices connected to the SmartServer.
4. Create and configure dial-out connections.

For more information on connecting an external GSM modem to the SmartServer's RS-232 serial port, see the SmartServer *Hardware Guide*.

Selecting Modem Type

You can select whether the SmartServer uses its built-in analog modem (applicable models only) or an external GSM modem, including the ETM9300-1, ETM9440-3, and Siemens MC55 external 3G wireless serial modems now supported by the SmartServer. To do this, follow these steps:

1. In the navigation pane directly under the SmartServer icon, click **Remote Access**. The **Setup - Modem** Web page opens.

Property	Value
Modem	Internal Analog
Modem Country / Region *	Europe / North America

* Reboot required if changed

2. Set the following properties:

Modem

Select the modem to be used by the SmartServer. You have the following choices:

- Internal Analog (default for applicable models).
- External ETM 9300-1.
- External ETM 9440-3.
- External GSM Multitech MTCBA-G-F1.
- External GSM Multitech MTCBA-G-F4 (Europe).
- External GSM Multitech MTCBA-G-F4 (US).
- External Janus Terminus Terminal (GSM864Q).
- External GSM Siemens/Cinterion 35 to 45 Series.
- External GSM Siemens/Cinterion 75 Series.
- External GSM Siemens/Cinterion MC55i.

Note: Many GSM service provider contracts do not include provisions for establishing data-only connections. Contact your GSM provider to ensure that you have data-only connections activated for your GSM contract.

For information on connecting an external GSM modem to the SmartServer, see the SmartServer *Hardware Guide*.

Modem

Country/Region

If you are using the SmartServer's **Internal Analog** modem, select the country in which the SmartServer is located. **Note:** You must reboot your SmartServer to implement changes to this property.

PIN Number

If you are using an **External GSM** modem, enter the PIN (maximum 30 characters) to be sent to the external modem in order for it to transmit or receive calls.

3. Click **Submit**.

Configuring Dial-in Connections

You can enable the SmartServer to be accessed remotely via a dial-in connection. To do this, follow these steps:

1. In the navigation pane directly under the **Remote Access** modem icon, click the **Dial-In** modem icon.

Property	Value
User Name for Incoming Calls	ilon
Password for Incoming Calls	Change Password
Local IP Address for Incoming Calls	192 . 168 . 2 . 2
PPP Authentication for Incoming Calls	PAP

2. Set the following properties:

User Name for Incoming Calls

Enter the user name (maximum 30 characters) that a caller must provide to connect to the SmartServer via modem. The default user name is **ilon**. Change this name for enhanced security.

Password for Incoming Calls

Click **Change Password** to enter and then re-enter the password (maximum 30 characters) that the caller must provide to connect to the SmartServer via modem. The default password is **ilon**. Change this password for enhanced security.

Local IP Address for Incoming Calls

Enter the IP address that will be assigned to incoming calls by the SmartServer. The default IP address is **198.162.2.2**.

Note: The local IP address must be outside the range of the SmartServer's Ethernet IP connection. For example, do not use 192.168.1.0 to 192.168.1.255 for the local IP address if you are using the SmartServer's default IPv4 address (192.1.168.222).

In addition, do not enter **0** or **254** in the last field of the IP address because other services may need to use these values. In addition, do not enter **255** in the last field of the IP address because the modem will not be able to ping the SmartServer.

PPP Authentication for Incoming Calls

Select the PPP (Point-to-Point Protocol) authentication type to validate the identity of a remote client. You have three choices:

- **None.** No PPP authentication is used for incoming calls.
- **PAP** (Point-to-Point Access Protocol). PAP uses unencrypted ASCII encoding to transmit user names and passwords over the network. Because PAP is considered insecure, only use it if CHAP is not available, or if the user name and password that the user submitted to PAP must be sent to another program without encryption. This is the default.
- **CHAP** (Challenge Handshake Authentication Protocol). CHAP uses a three-way handshake to validate a remote client when the connection is established and may validate it again anytime afterwards. This is the recommended PAP authentication type.

3. Click **Submit**.

Configuring Dial-out Connections

You can enable the SmartServer to connect to a TCP/IP network via a dial-out modem connection so that it can connect to other host devices. To do this, specify the phone number or GPRS service to be used by your SmartServer's modem to dial out. To configure the dial-out connections, follow these steps:

1. In the navigation pane directly under the **Dial-in** modem icon, click the **Dial-Out** modem icon. The properties that you can set depend on whether the SmartServer is using its internal analog modem or an external GSM modem.
2. If you are using an **Internal Analog** modem, set the following properties:

Property	Value
Dialing Type	<input checked="" type="radio"/> Tone <input type="radio"/> Pulse
Dialing Prefix	<input type="text"/>
Delay after Prefix	<input type="text" value="0"/> Seconds

Dial Tone Waiting

Dialing Type

Select whether the SmartServer's modem will dial using touch-tone or pulse dialing. The default dialing type is **Tone**.

Dialing Prefix

Enter a prefix (maximum 30 digits) if the SmartServer is connected to a phone system that requires a code to be dialed to reach an outside line. By default, this field is blank.

Delay After Prefix

If you entered a dialing prefix, enter the delay (in seconds) between the prefix and the phone number being dialed. The default delay is **0** seconds.

You must reboot the SmartServer for changes to this property to take effect

Dial Tone Waiting

Enables the modem to wait for a dial tone before dialing out.

- If you are using an **External GSM** modem, set the following properties:

Access Point Name (APN) Set the APN (maximum 64 characters), which is required by most GPRS service providers. The APN can be a valid IP address, or a valid hostname and domain suffix pair.

Quality of Service (QoS) Set the QoS string (maximum 30 characters), which is required by most GPRS providers.

QoS refers to the control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from an application program.

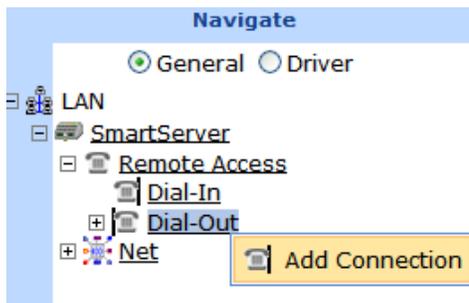
- Click **Submit**.

Creating Dial-Out Connections

You can create a dial-up connection for each phone number or GPRS service to which the SmartServer is connected. The SmartServer contains two sample dial-out connections: **Frenet** and **T-Online**. You can configure these connections by expanding the **Dial-Out** modem icon and then clicking them, or you can create new dial-out connections. You can delete these sample connections if you do not plan on using them.

To create a new dial-up connection, follow these steps:

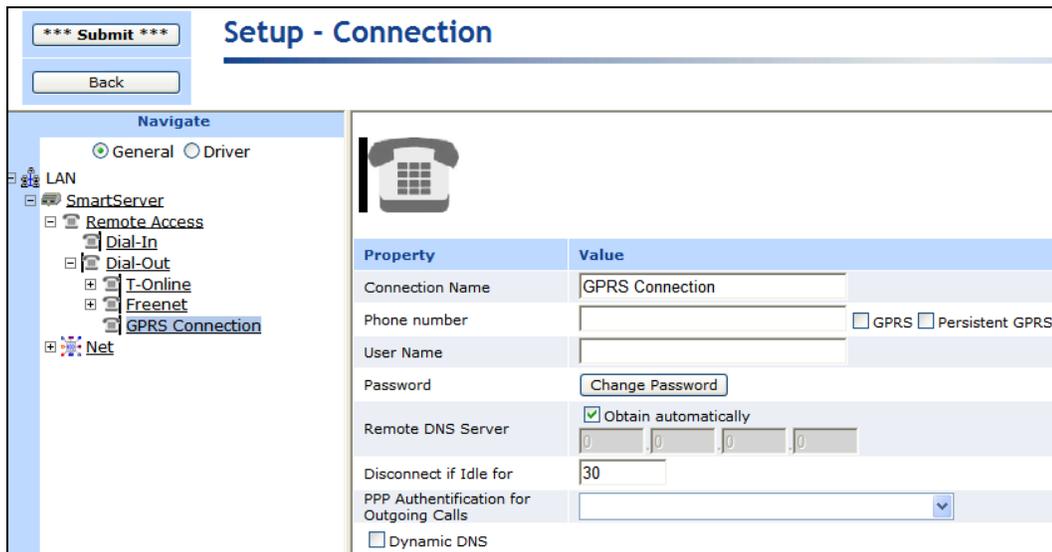
- In the navigation pane, right-click the **Dial-Out** modem icon and then click **Add Connection** on the shortcut menu.



- The **Enter Name** dialog opens. Enter a name for the connection and then click **OK**.



3. The **Setup – Connection** Web page opens and the connection is added to the bottom of the **Dial-Out** tree.



4. Click **Submit**.
5. Set the following properties for the dial-out connection:

Connection Name Enter a name for the dial-out connection (maximum 30 ASCII characters), such as the name of the ISP. The name may not include the '&', '<', and '>' characters.

Phone Number

Enter the phone number to call when this dial-out connection is used.

If you are using an external GSM modem, you can select the following options to enable a GPRS connection with this number:

- *GPRS*. Uses the GPRS protocol to transmit data instead of an analog phone call. A connection will be established whenever the SmartServer attempts to contact a server with the dial-up connection. Once the transaction with the server is complete, the connection will be dropped. See the documentation for your GSM modem for more information about the GPRS protocol.
- *Persistent GPRS*. Uses the GPRS protocol to transmit data, but the GSM modem requests a network connection as soon as the SmartServer boots, and keeps it open as long as the ISP allows it.

Note: Many GPRS service providers require a phone number that must be dialed when establishing a connection, such as *99***1#. Consult your ISP for details on configuring the properties of your GPRS connections.

Note: To use the Firefox Web browser to access the SmartServer Web pages via GPRS, you must modify your user agent string in the Web browser. To do this, follow these steps:

1. Enter **about:config** in the address bar of the Firefox Web browser.
2. In the **Filter** box, enter **general.useragent.extra.firefox**.
3. Double-click the **general.useragent.extra.firefox** preference name.
4. Enter the following value in the **Enter String Value** dialog:

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

5. Click **OK**.

User Name

Enter the user name (maximum 30 ASCII characters) to be used by the SmartServer when connecting to an ISP. The user name may not include the '&', '<', and '>' characters. This field is blank by default.

Password

Click **Change Password** to enter and then re-enter the password (maximum 30 ASCII characters) to be used by the SmartServer when connecting to an ISP. The password may not include the '&', '<', and '>' characters. This field is blank by default.

Remote DNS Server

Enter the IP address of the DNS server to be used when using this dial-out connection. Select the **Obtain Automatically** check box to obtain the DNS server address from the PPP server when establishing the connection.

Disconnect if Idle for

Enter the length of time (between 0.0 and 6553.5) seconds that the connection may be idle before it is disconnected. Once a PPP connection is established, it will not be released until it has been idle for this amount of time. This means that if data is being constantly sent over a PPP connection, the connection will never be dropped and any data that needs to use a second PPP connection may never be sent.

PPP Authentication for Outgoing Calls

The default time is **30.0** seconds.

Select the PPP authentication type to be used when connecting to an ISP. You have three choices:

- **Automatic.** The SmartServer automatically selects the authentication type to be used when connecting to the ISP. This is the default.
- **PAP** (Point-to-Point Access Protocol). PAP uses unencrypted ASCII encoding to transmit user names and passwords over the network. Because PAP is considered insecure, only use it if CHAP is not available, or if the user name and password that the user submitted to PAP must be sent to another program without encryption.
- **CHAP** (Challenge Handshake Authentication Protocol). CHAP uses a three-way handshake to validate a remote client when the connection is established and may validate it again anytime afterwards. This is the recommended PAP authentication type.

Dynamic DNS

Enables you to use a DNS server that has a dynamic IP address. The SmartServer only supports www.dyndns.org as a dynamic DNS (DDNS) provider. You must set up an account on this site and set up the DDNS hostname.

For example, consider a case where the SmartServer should be accessible via the hostname “ilon100example.dyndns.org” when a persistent GPRS connection is established. The user needs to use the account with the name <UserName> and the password <Password>. In this case, perform the following steps:

1. Set up a user account at www.dyndns.org with the user name <UserName> and password <Password>.
2. Set up a dynamic DNS entry for the host “ilon100example.dyndns.org”.
3. Set up a persistent GPRS connection with this DDNS.
4. Test these settings by opening the following Web page: <http://ilon100example.dyndns.org>. You should receive the normal SmartServer Web pages via GPRS.

6. If you enabled dynamic DNS by selecting the **Dynamic DNS** checkbox, set the following properties:

Host name (complete)	<input type="text"/>
User name	<input type="text"/>
Password	<input type="button" value="Change Password"/>

Hostname

Enter the hostname of the SmartServer that is registered at www.dyndns.org. You only need to set this property if you are enabled dynamic DNS service.

User Name

Enter the user name (maximum 30 ASCII characters) defined for the DDNS server at www.dyndns.org. You only need to set this field if you are using dynamic DNS service. The user name may not include the ‘&’, ‘<’, and ‘>’ characters. This property is blank by default.

Password

Click Change Password to enter and then re-enter the password (maximum 30 ASCII characters) defined for the DDNS server at www.dyndns.org. You only need to set this property if you are using dynamic DNS service. The password may not include the '&', '<', and '>' characters. This property is blank by default.

7. If you enabled a persistent GPRS connection for the phone number you entered by selecting the **Persistent GPRS** check box, you can select the **GPRS Check** checkbox to set the following properties:

<input checked="" type="checkbox"/> GPRS Check	
Host name (complete)	<input type="text"/>
Check Interval	<input type="text"/> Minutes
Retry Time (defaults to 120 s)	<input type="text"/> Seconds
Retry Count	<input type="text"/>
Verify Mode	Default

Hostname (complete) Enter the hostname or IP address of the Web server provided by the ISP for the GPRS connection.

Check Interval Enter the amount of time after which the SmartServer connects to the ISP automatically.

Retry Time Set the interval (in seconds) that network messages wait for confirmation before being re-sent over the network. The default time retry time is **120** seconds.

Retry Count Set the number of times a network message is re-sent when no confirmation is received.

Verify Mode Select the method in which the SmartServer simulates internet activity in order to verify that the GPRS connection is active. You have the following three choices:

- **Default.** The SmartServer pings the IP address of the Web server, and it opens a TCP connection to the HTTP port (80) of the Web server. If either check succeeds, the GPRS connection is active.
- **Ping Host.** The SmartServer pings the IP address of the Web server. This is similar to the 'ping' command in Linux or Windows.
- **Check HTTP Connection.** The SmartServer opens a TCP connection to the HTTP port (80) of the Web server.

If the GPRS connection is lost, the SmartServer restarts the modem.

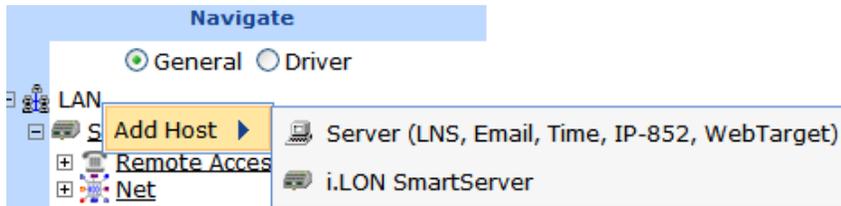
Once you have created and configured a dial-out connection, you can add host devices to the connection (remote SmartServers, OpenLNS Servers, e-mail servers, time servers, IP-852 Configuration Servers, and Web Connection Target servers). For information on how to do this, see the next section, *Adding Host Devices*.

Adding Host Devices

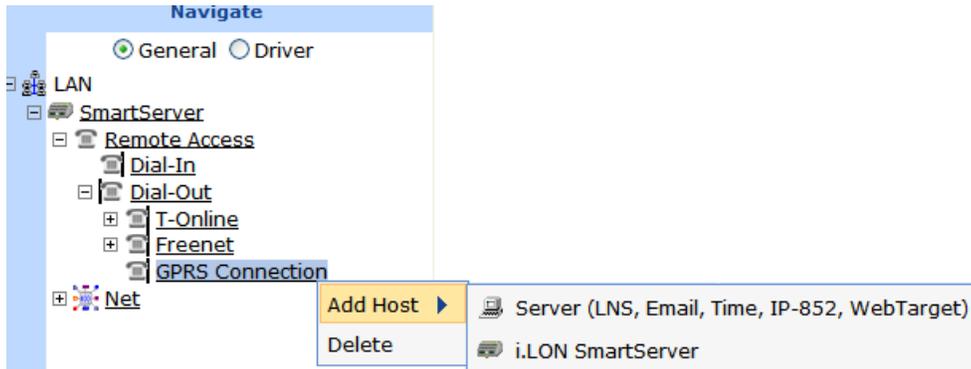
You can connect host devices to your local SmartServer through the SmartServer's Ethernet connection, or through a dial-up connection that you have added to the SmartServer's built-in analog

modem (applicable models) or an external GSM modem connected to the SmartServer's RS-232 serial port. The host devices you can add to the LAN consist of remote SmartServers, OpenLNS Servers, e-mail servers, time servers, IP-852 Configuration Servers, and Web Connection Target servers (Web servers that can process SOAP requests).

To add a host device to the SmartServer's Ethernet connection, right-click the **LAN** icon (the first icon at the top of the navigation pane in the left frame), point to **Add Host**, and then select **Server** or **SmartServer**. Select **Server** to add an OpenLNS Server, e-mail server, time server, IP-852 Configuration Server, or Web Connection Target server to the LAN. Select **SmartServer** to add a remote SmartServer to the LAN.

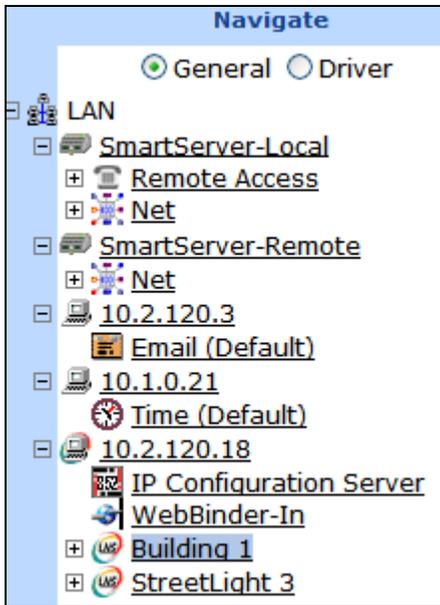


To add a host device to a dial-up connection on the SmartServer, you right-click the icon representing the dial-out connection to which the host device is to be added, point to **Add Host**, and then select **Server** or **SmartServer**.



When you add a host device, it appears one level below the LAN or dial-out connection in the navigation pane. In addition, if you add a remote SmartServer to the LAN, the network attached to it is listed one level below its SmartServer icon. If you add an OpenLNS Server to the LAN, its networks (OpenLNS network databases) are listed one level below its LNS Server icon. If you add an e-mail, time, IP-852 configuration, or Web Connection Target server to the LAN, An icon representing the specific host device is listed one level below its generic server icon.

You can add multiple services to a given host device. For example, the OpenLNS Server you add to the LAN might also serve as an IP-852 Configuration Server and a Web Connection Target server.



The LAN, the host devices on the LAN, and the networks available on the host devices are further described as follows:

- | | | |
|----------------------------|---|--|
| LAN |  | The LAN icon corresponds to the SmartServer's 10/100-BaseT Ethernet connection. This connection is always the first icon shown in the navigation pane, and it cannot be deleted |
| Host Devices |  | Host devices represent the various servers on the LAN. Host devices include your local SmartServer and may include remote SmartServers, OpenLNS Servers, e-mail (SMTP) servers, time servers (SNTP), IP-852 Configuration Servers, and Web Connection Target servers. |
| <i>Local SmartServer</i> |  | Your local SmartServer is always the second icon shown in the navigation pane, and it cannot be deleted. From this icon, you can configure your local SmartServer; access the SmartServer's built-in applications; and manage, monitor, and control the devices connected to your local SmartServer. The remote access (dial-up) connections and the network attached to your local SmartServer are listed one level below the local SmartServer icon. |
| <i>Remote SmartServers</i> |  | You can add remote SmartServers to the LAN and manage them from your local SmartServer. You can also create Web connections between the data points on your local SmartServer to the data points on the remote SmartServers (called <i>peer-to-peer connections</i>).

Remote SmartServers are represented by SmartServer icons that include the IP addresses or hostnames of their respective remote SmartServers. |

<i>OpenLNS Servers</i>		<p>You must add an OpenLNS Server to the LAN in order to add the data points of external devices to the SmartServer's built-in applications and to your custom SmartServer Web pages. In addition, you need to add an OpenLNS Server to the LAN in order to keep your local SmartServer synchronized with an OpenLNS network database and use OpenLNS network management services to manage the network attached to your local SmartServer. You can also create Web connections between your local SmartServer and OpenLNS Servers (called <i>LNS uplink connections</i>).</p> <p>OpenLNS Servers are represented by LNS Server icons that include the IP addresses of their respective OpenLNS Servers.</p>
<i>E-mail server</i>		<p>You can use an SMTP server to have the SmartServer send e-mail messages to a technician, maintenance company, or other personnel when a data point is an alarm condition. You must also add Alarm Generator and Alarm Notifier functional blocks to the SmartServer's i.LON App (Internal) device for the SmartServer to send e-mail notifications.</p> <p>SMTP servers are represented by a server icon that includes the IP address or hostname of the server and an SMTP icon listed directly below it.</p>
<i>Time server</i>		<p>You can use an SNTP server to synchronize the time and date of the SmartServer and the other host devices on the LAN to a common base.</p> <p>SNTP servers are represented by a server icon that includes the IP address or hostname of the server and an SNTP icon listed directly below it.</p>
<i>IP-852 Configuration Server</i>		<p>You can add an IP-852 Configuration Server to the LAN to enable a SmartServer with IP-852 routing activated and other IP-852 devices such as OpenLNS Servers and i.LON 600 LONWORKS/IP servers to communicate with each other over a high-performance backbone channel.</p> <p>An IP-852 Configuration Server is represented by an IP-852 server icon that includes the IP address of the IP-852 Configuration Server.</p> <p>Note: You only need to add an IP-852 Configuration Server if you do not plan on using the default port on the SmartServer (1628) used for receiving messages from the IP-852 Configuration Server.</p>
<i>Web Connection Target Server</i>		<p>You can add an Web Connection Target Server to send data logs, alarm logs, event scheduler logs, or any user-defined file from your SmartServer to a central enterprise system via a Web connection (called an <i>enterprise connection</i>).</p>
Networks		<p>You can manage the channels, devices, functional blocks, and data points on the network attached to your local SmartServer, the networks attached to remote SmartServers on the LAN, and in the networks in the OpenLNS Servers on the LAN.</p>
<i>SmartServer Network</i>		<p>By default, the network attached to a SmartServer is represented by the SmartServer network icon, and it is named Net. Once you synchronize your SmartServer to an OpenLNS network database, this icon changes to an OpenLNS network icon () and is re-named to the name of the OpenLNS network database.</p>
<i>OpenLNS network (Database)</i>		<p>By default, the networks in an OpenLNS Server are represented by OpenLNS network icons that include the names of their respective OpenLNS network databases. Networks originally created in the SmartServer tree are represented by SmartServer network icons () in the OpenLNS tree.</p>

Adding a Remote SmartServer to the LAN

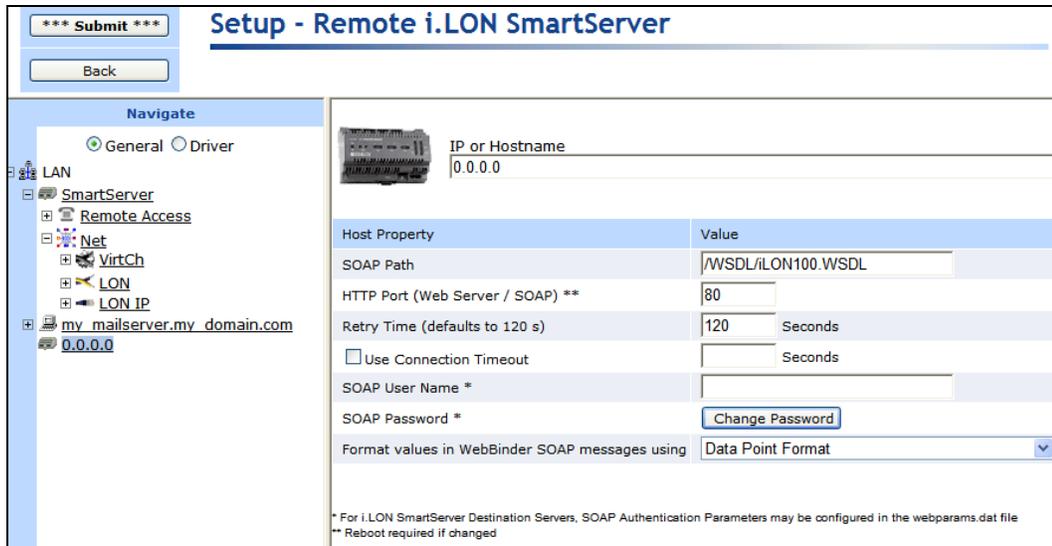
You can add another SmartServer to the LAN, and then manage the remote SmartServer and manage, monitor, and control the network attached to it from the Web interface of your local SmartServer. In addition, you can create Web connections between the data points on your local SmartServer to those on the remote SmartServer. The Web connections will keep the values of the data points synchronized. For more information on creating and using Web connections, see *Creating Web Connections* in Chapter 4, *Using the SmartServer Web Interface*.

To add a remote SmartServer to the LAN, follow these steps:

1. Verify that the remote SmartServer has a unique hostname relative to the LAN—the remote SmartServer cannot have the same hostname as the local SmartServer. To change the hostname of a SmartServer, do the following:
 - For a SmartServer in an LNS managed network, change the SmartServer’s hostname with OpenLNS CT or another OpenLNS tool.
 - For a SmartServer in a standalone managed network, change the hostname in its **Setup – Local SmartServer** TCP/IP Web page or the console application.
2. Right-click the **LAN** icon or a dial-out connection icon, point to **Add Host**, and then click **SmartServer** on the shortcut menu.



3. The **Setup – Remote SmartServer** Web page opens, and a SmartServer icon is added one level below the LAN icon at the bottom of the navigation pane or one level below the dial-out connection icon.



4. Configure the following properties for the remote SmartServer:
 - IP or Hostname* Enter the IP address or hostname of the remote SmartServer. The default

hostname is **SmartServer**.

Host Property

<i>SOAP Path</i>	Enter the path on the remote SmartServer to which SOAP messages should be transmitted. This is typically the location of the WSDL or ASMX file on the SmartServer where it receives SOAP messages. The default path is /WSDL/iLON100.WSDL (the default location of the WSDL file on a SmartServer).
<i>HTTP Port (Web Server/SOAP)</i>	<p>Enter the port that the remote SmartServer uses to serve HTTP requests (SOAP and WebDAV). The default value is 80, but you may change it to any valid port number. Contact your IS department to ensure your firewall is configured to allow access to the server on this port.</p> <p>Select the SSL option to create a secure Web connection. Enter the port number to use for the SOAP interface. The default port used for SSL is 443, but you may change it to any valid port number.</p>
<i>Retry Time</i>	<p>Set the amount of time (in seconds) after which the remote SmartServer will stop attempting to resend failed Web Connection connection messages. The default value is 120 seconds.</p> <p>The remote SmartServer automatically attempts to resend failed Web Connection connection messages every 45 seconds.</p>
<i>Use Connection Timeout</i>	<p>Set the maximum period of time (in seconds) that the remote SmartServer waits for a response to a SOAP request from the local SmartServer's Web server before the transaction is canceled and a timeout error is thrown.</p> <p>By default, the connection timeout is 2 seconds—even if this check box is cleared. If you select this check box, the default timeout is 120 seconds.</p>
<i>SOAP User Name</i>	<p>Optionally, you can enter a user name to be used for logging in to the remote SmartServer.</p> <p>Alternatively, you configure the user name and password using the iLON Web Server Security and Parameters program, or by manually configuring the webparams.dat file located at the root level of the SmartServer's flash disk. See <i>Appendix C</i> for more information on using the iLON Web Server Security and Parameters program.</p>
<i>SOAP Password</i>	If you create a user name, click Change Password to enter the password to be used for logging in to the remote SmartServer.
<i>Format Values in Web Connection SOAP Messages Using</i>	<p>Select how data point values are formatted in SOAP messages sent to this remote SmartServer via Web connections. You have two choices:</p> <ul style="list-style-type: none">• Data Point Format. Data point values are formatted based on the SNVT, UNVT, SCPT, or UCPT defined for the data point.• Raw HEX. Data point values are transmitted in raw hexadecimal format.

5. Click **Submit** to save the changes.

To delete a remote SmartServer, right-click the SmartServer icon representing the remote SmartServer, click **Delete** on the shortcut menu, and then click **Submit**.

Adding an OpenLNS Server to the LAN

You can add an OpenLNS Server or LNS Server to the LAN and then use the LNS Proxy Web service to synchronize your SmartServer an OpenLNS network database, add the data points of external

devices in OpenLNS managed networks to the SmartServer's built-in applications and to your custom SmartServer 2.2 Web pages, and use OpenLNS network management services to manage the network attached to your local SmartServer.

You can also create Web connections between your local SmartServer and an OpenLNS Server on the LAN (called *LNS uplink connections*). When the value of a data point on your local SmartServer changes, an uplink connection to the destination OpenLNS Server is initiated and the data point value is transmitted to that OpenLNS Server. For more information on creating and using Web connections, see *Creating Web Connections* in Chapter 4, *Using the SmartServer Web Interface*.

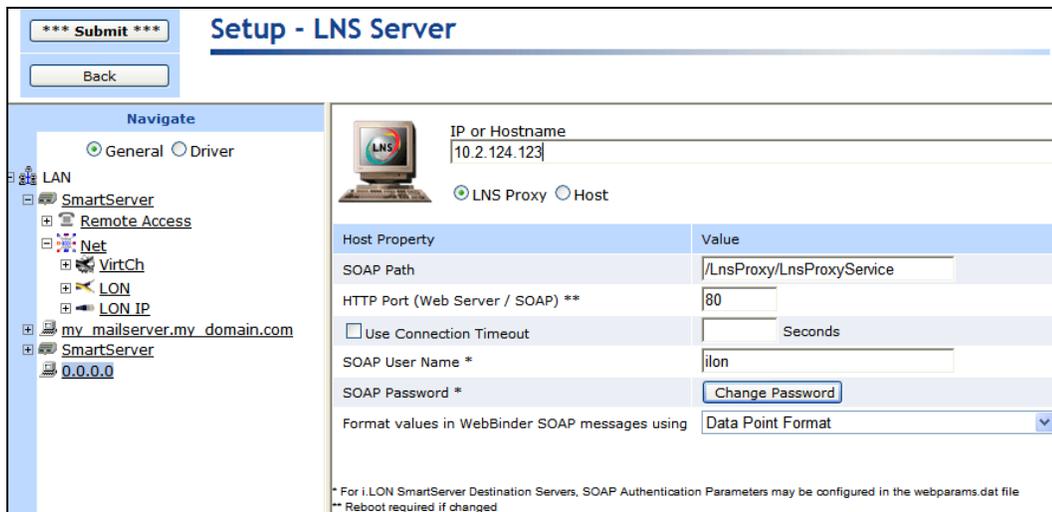
To add an OpenLNS Server or LNS Server to the LAN, follow these steps:

1. Verify that EES 2.2 and an OpenLNS Server or LNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Right-click the **LAN** icon or a dial-out connection icon, point to **Add Host**, and then click **Server (LNS, Email, Time, IP-852, WebTarget)** on the shortcut menu.



Note: If IP-852 routing is activated and enabled on the SmartServer and the IP-852 Configuration Server is installed on the OpenLNS Server computer, click the IP-852 Configuration Server icon (IP-852), click **LNS Proxy**, and then skip to step 5 in order to configure the properties of the OpenLNS Server.

3. The **Setup – Host** Web page opens, and a server icon is added one level below the LAN icon at the bottom of the navigation pane or one level below the dial-out connection icon.
4. Enter the IP address or hostname of the OpenLNS Server or LNS Server and then click **LNS Proxy**. The server icon on the tree becomes an LNS Server icon and the **Setup – OpenLNS Server** Web page opens.



5. Configure the following OpenLNS Server properties:

Host Property

<i>SOAP Path</i>	Enter the path on the OpenLNS Server to which SOAP messages are transmitted via the LNS Proxy Web service. The default path is /LnsProxy/LnsProxyService .
<i>HTTP Port (Web Server/SOAP)</i>	Enter the port on the SmartServer used for accessing the LNS Proxy Web service. The default port is 80 . Contact your IS department to ensure your firewall is configured to allow access to the server on this port. Note: If you modify this property, you need to reboot the SmartServer to implement the change.
<i>Use Connection Timeout</i>	Set the maximum period of time (in seconds) that the LNS Proxy Web service waits for a response to a SOAP request from the local SmartServer's Web server before the transaction is canceled and a timeout error is thrown. By default, the connection timeout is 2 seconds if this option is cleared. If you select this option, the default timeout is 120 seconds.
<i>User Name</i>	Optionally, enter a user name to be used by the SmartServer for accessing the LNS Proxy Web service. The default user name is ilon .
<i>SOAP Password</i>	Optionally, you can click Change Password to change the password used by the SmartServer for accessing the LNS Proxy Web service. The default password is ilon .
<i>Format Values in Web Connection SOAP Messages Using</i>	Select how data point values are formatted in SOAP messages sent to this OpenLNS Server via Web connections. You have two choices: <ul style="list-style-type: none"> • Data Point Format. Data point values are formatted based on the SNVT, UNVT, SCPT, or UCPT defined for the data point. • Raw HEX. Data point values are transmitted in raw hexadecimal format.

6. Click **Submit** to save the changes. Click **Back** to leave all fields unchanged.
7. If you are using Internet Explorer 7, enable your Web browser to access the LNS Proxy Web service on the OpenLNS Server computer. To do this, follow these steps:
 - a. Add the locations of your local SmartServer and the OpenLNS Server on which the LNS Proxy Web service is installed as trusted sites. To do this, click **Tools**, click **Internet Options**, click the **Security** tab, click **Trusted Sites**, and then click **Sites**. Clear the **Require Service Verification** check box.

By default, the IP address of your local SmartServer appears in the **Add this Website to the Zone** box. Click **Add** to add the IP address of your local SmartServer. Enter the IP address of the LNS Proxy Web service in the **Add this Website to the Zone** box, click **Add**, click **Close**, and then click **OK**.
 - b. Enable your Web browser to access sites over other domains. To do this with Internet Explorer 7, click **Tools**, click **Internet Options**, click the **Security** tab, and then click **Custom**. Under the **Miscellaneous** category, select **Enable or Prompt for the Access data sources across domains** property.

Note: If you are using Internet Explorer 7 and you do not complete step 2, the **Cannot Access Remote Host** dialog appears when you try to expand the LNS Server icon or synchronize the SmartServer to an OpenLNS network database. If you are using Internet Explorer 8, Chrome, or Firefox, you do not need to complete this step.
5. You can now expand the LNS Server icon to show the networks, channels, devices, functional blocks, and data points on your OpenLNS Server. It may take a minute to show the networks on an OpenLNS Server after you initially expand the LNS Server icon.

You can configure the object in the OpenLNS tree and the changes are automatically transmitted to the OpenLNS Server. In addition, when you modify an OpenLNS network database with another OpenLNS client such as OpenLNS CT, the OpenLNS tree will be updated because the SmartServer polls the OpenLNS network database and processes the changes.

For more information on using the SmartServer to manage the objects in an OpenLNS network database, see Chapter 5, *Using the SmartServer as a Network Integration Tool*.

6. You can now operate the SmartServer in LNS mode and select an OpenLNS or LNS network database to be synchronized to your SmartServer. See *Configuring a LonWorks Network* in Chapter 5 for more information on how to do this.
7. You now add the external network variables and configuration properties in the OpenLNS tree to an embedded application on a SmartServer (your local SmartServer or a remote SmartServer that you have added to the LAN). See *Adding Data Points to SmartServer Applications* in Chapter 4, *Using the SmartServer Web Interface*, for more information on adding external network variables and configuration properties to the SmartServer's built-in applications.

To delete an OpenLNS Server, right-click the OpenLNS Server, click **Delete** on the shortcut menu, and then click **Submit**.

Troubleshooting the LNS Proxy Web Service

If you cannot synchronize the SmartServer to an OpenLNS or LNS network database, Echelon Enterprise Services 2.2 (EES 2.2) may not have been installed or configured correctly, or a firewall may be blocking access. Follow these steps to correct the problem:

1. Verify that the SmartServer and the LNS Proxy Web service are using the same HTTP port on the OpenLNS Server computer for SOAP communication. To do this follow these steps:
 - a. Open the **Setup – OpenLNS Server** Web page. To do this, click the LNS Server icon in the tree view on the left side of the SmartServer Web interface.
 - b. The port used by the SmartServer to communicate with the LNS Proxy Web service is specified in the **HTTP Port (Web Server / SOAP)** property. The default port is **80**.
 - c. Right-click the Enterprise Services tray icon in the notification area on the desktop of the OpenLNS Server computer, and then click **Options** on the shortcut menu.
 - d. The port used by the LNS Proxy Web service on the OpenLNS Server computer is listed in the **Port Number** property in the **Connection** tab. The default port is **80**.
2. Verify that the EES tray tool icon is red, meaning that EES 2.2 is running. If the icon is gray and the ToolTip states “SmartServer Enterprise Services OFF”, EES 2.2 is not running. To start EES 2.2, right-click the Enterprise Services tray icon and click Start Service on the shortcut menu.
3. If you selected the **LNS Auto** network management service in the **Setup – LON Network Driver** Web page and a firewall is blocking access to the LNS Proxy Web Services, do the following on both your OpenLNS Server computer and your remote OpenLNS client (if being used):
 - a. Open the HTTP port to be used for the LNS Proxy Web Services. To do this, open the Control Panel, click **Security Center**, click **Services**, click **Windows Firewall**, click the **Exceptions** tab, and then click **Add Port**. Enter LNS Proxy (or some other meaningful name) in the **Name** box, enter the selected HTTP port in the **Port** box, and then click **OK**.
 - b. If you are using a third-party firewall, add the Tomcat 6 executable as an exception. The full path of the Tomcat 6 executable is **LonWorks\iLON\EnterpriseServices\Appserver\bin\tomcat6.exe** by default.
 - c. Try to expand the LNS Server icon in the navigation pane on the left side of the SmartServer Web interface. If you cannot expand the OpenLNS Server, either proceed to step 4, or open the **Setup – LON Network Driver Web** page and change the **Network Management Service** property to **LNS Manual**.

- Browse to **http://<OpenLNS Server Computer IP Address>/EES/AdminService/v4.0/index.htm**, which is the IP address of the i.LON AdminServer tool that is installed on your OpenLNS Server computer by EES 2.2. For example, if the IP address of your OpenLNS Server computer is 10.2.124.30, enter **http://10.2.124.30/EES/AdminService/v4.0/index.htm**.

Note: Browse from a computer that is on the same side of the firewall as the SmartServer and the computer used to access the SmartServer Web pages.

- If the i.LON AdminServer tool opens, the SmartServer should be able to communicate with the LNS Proxy Web Service. Use the Add or Remove Programs Control Panel application to verify that the version of EES 2.2 matches the SmartServer firmware version. The SmartServer firmware version is displayed at the bottom right side of the SmartServer Web pages. You can also view this information by clicking **Setup** and then clicking **System Info** in the SmartServer Web pages, or right-clicking the local SmartServer and clicking **System Info** on the shortcut menu.
- If the i.LON AdminServer tool does not open, un-install and then re-install EES 2.2. In addition, verify that there are no port conflicts with any other applications.

Adding an E-mail (SMTP) Server to the LAN

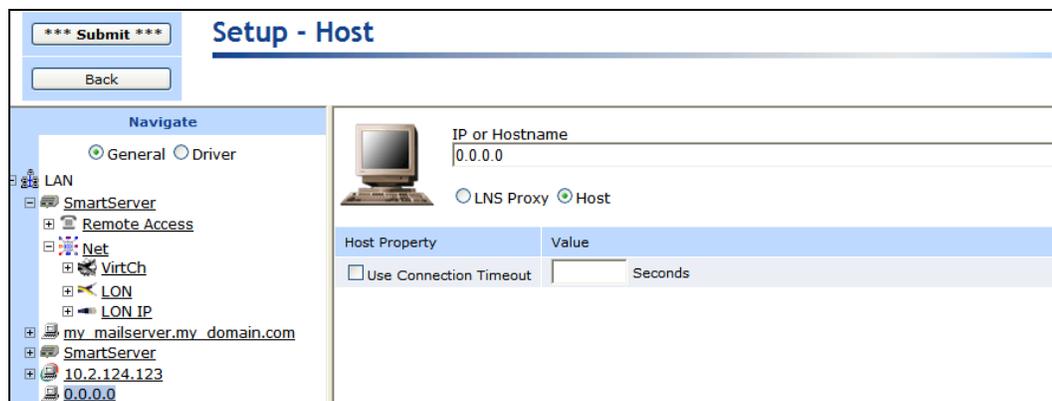
You can add an e-mail (SMTP) server to the LAN to have the SmartServer automatically send e-mail notifications when a data point is an alarm condition. You must also add Alarm Generator and Alarm Notifier functional blocks to the SmartServer's **i.LON App (Internal)** device and configure them for the SmartServer to send e-mail notifications. See Chapter 6, *Alarming*, for more information on configuring the SmartServer's alarming applications.

To add an e-mail server to the LAN, follow these steps:

- Right-click the **LAN** icon or a dial-out connection icon, point to **Add Host**, and then click **Server (LNS, Email, Time, IP-852, WebTarget)** on the shortcut menu, or if you are adding the time service to an existing server on the LAN, skip to step 4.

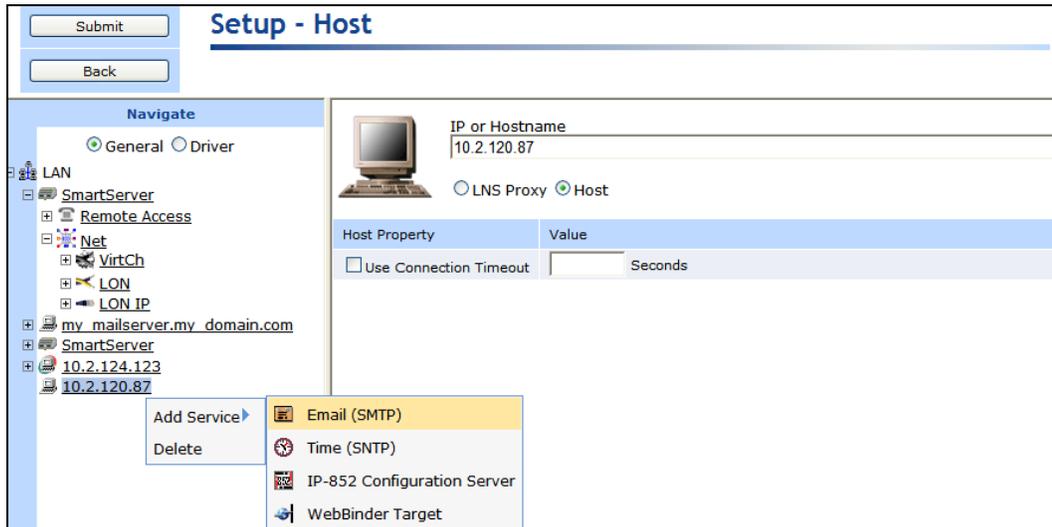


- The **Setup – Host** Web page opens, and a server icon is added one level below the LAN icon at the bottom of the navigation pane or one level below the dial-out connection icon.

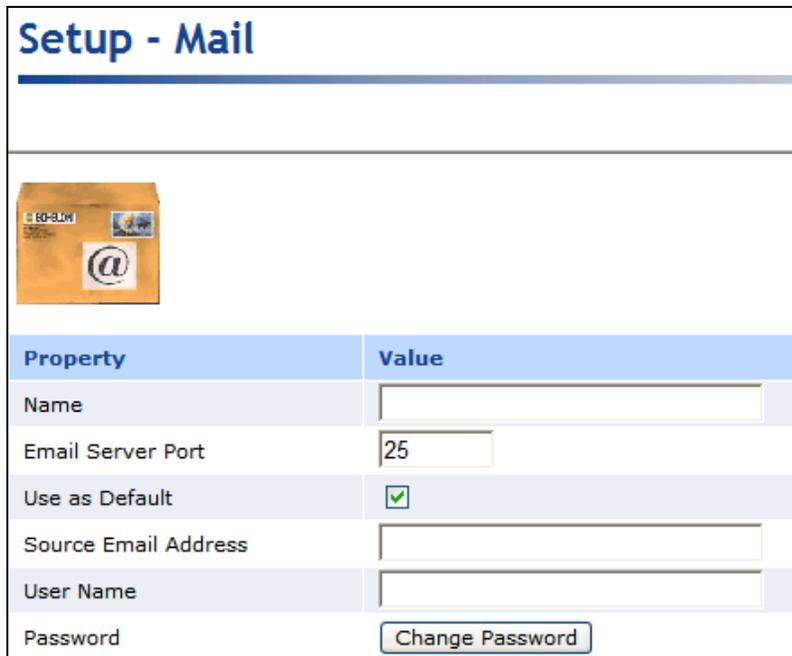


- Enter the IP address or hostname of the e-mail (SMTP) server.

- Optionally, select the **Use Connection Timeout** option and enter the maximum period of time (in seconds) that the e-mail (SMTP) server waits for a response to a SOAP request from the local SmartServer's Web server before the transaction is canceled and a timeout error is thrown. By default, the connection timeout is 2 seconds if this option is cleared. If you select this option, the default timeout is **120** seconds.
- Click **Submit**. The server icon in the tree is updated with the IP address or hostname you entered.
- Right-click the new server icon, point to **Add Service**, then and click **E-Mail (SMTP)** on the shortcut menu.



- The **Setup – Mail** Web page opens.



- Configure the following e-mail (SMTP) server properties:

Property

Name Enter a name for the SMTP server. This field is blank by default.

<i>E-mail Server Port</i>	Enter the port used by the SmartServer to send e-mail messages. The default value is 25 . Contact your IS department to verify that your firewall will allow you to access the e-mail server on this port.
<i>Use as Default</i>	Makes the e-mail server the default e-mail service for the SmartServer. If this is the first e-mail service created on the SmartServer this option will be set by default. If another e-mail service is currently designated as the default and this check box is selected, the default designation will be removed from the first e-mail service when you click Submit .
<i>Source E-mail Address</i>	Enter the string that will appear in the From field of e-mail messages sent through this service (<i>for example</i> lonfloor1@echelon.com). This field is blank by default.
<i>User Name</i>	If the SMTP server requires authentication, enter the user name for logging in to the SMTP server. The SmartServer and the SMTP server will automatically negotiate the authentication mechanism to be used (PLAIN, LOGIN, or CRAM-MD5). The SmartServer does not support the POP before SMTP authentication mechanism.
<i>Password</i>	If the SMTP server requires authentication, click Change Password to enter the password for logging in to the SMTP server.

9. Click **Submit** to save the changes.

To delete an e-mail (SMTP) server, right-click the generic server icon if the sever is used exclusively for the e-mail service, or right-click the e-mail service icon if the server is used for other services, click **Delete** on the shortcut menu, and then click **Submit**.

Adding a Time (SNTP) Server to the LAN

You can add a time (SNTP) server to the LAN to synchronize the date and time on the SmartServer and all other devices on the LAN to a common base. This ensures that message packets overcome the latencies posed by large IP networks and reach their destinations. The time (SNTP) server you add must be running at the specified location. For more information on time and frequency services and a list of available public time (SNTP) servers, go to <http://ntp.isc.org/bin/view/Servers/WebHome>.

Tip: You can install Tardis2000, a shareware program available at www.kaska.demon.co.uk, and synchronize it to another SNTP server or the local time on your computer. If you synchronize it to the local time on your computer, you can then use the loopback address of your local computer (127.0.0.1) as an SNTP server on your SmartServer.

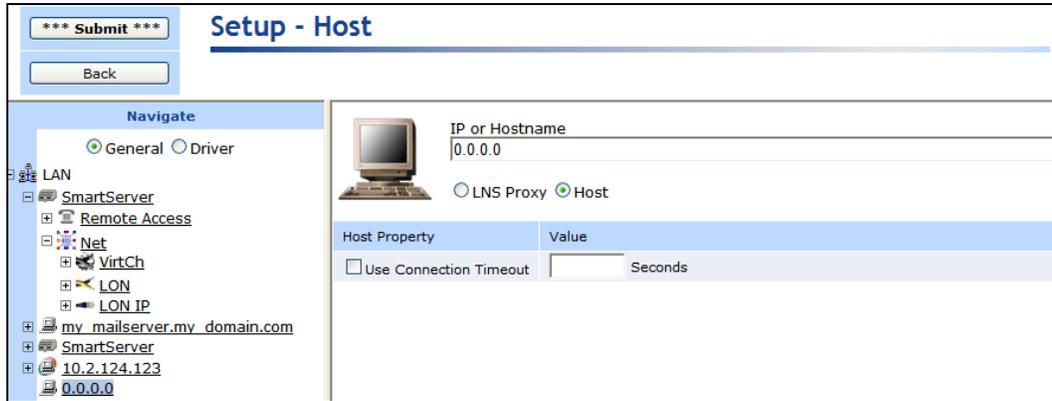
Note: If you are using the SmartServer as an IP-852 router and using a channel timeout for that IP-852 channel, you can let the IP-852 Configuration Server manage the SNTP time server configuration on the SmartServer. See the *IP-852 Channel User's Guide* for details on this. If the IP-852 Configuration Server sets a time server on the SmartServer, that time server will automatically show up in the SmartServer Web pages, and will override any time server configurations you have made with the SmartServer Web pages.

To add a time (SNTP) server to the LAN, follow these steps:

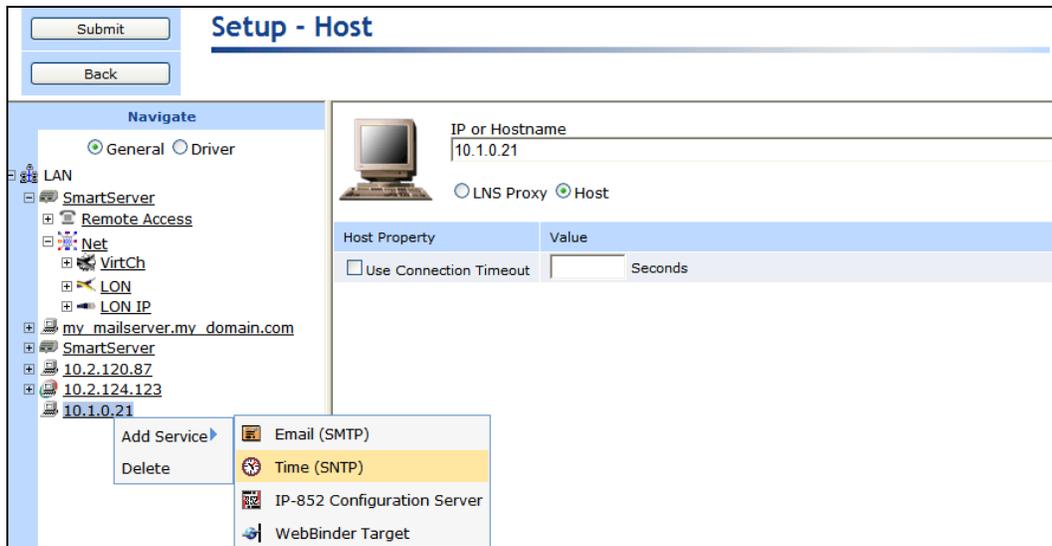
1. Right-click the **LAN** icon or a dial-out connection icon, point to **Add Host**, and then click **Server (LNS, Email, Time, IP-852, WebTarget)** on the shortcut menu, or if are you adding the time service to an existing server on the LAN, skip to step 4.



2. The **Setup – Host** Web page opens, and a server icon is added one level below the LAN icon at the bottom of the navigation pane or one level below the dial-out connection icon.



3. Enter the IP address or hostname of the time (SNTP) server.
4. Optionally, select the **Use Connection Timeout** option and enter the maximum period of time (in seconds) that the time (SNTP) server waits for a response to a SOAP request from the local SmartServer’s Web server before the transaction is canceled and a timeout error is thrown. By default, the connection timeout is **2** seconds if this option is cleared. If you select this option, the default timeout is **120** seconds.
5. Click **Submit**. The server icon in the tree is updated with the IP address or hostname you entered.
6. Right-click the server icon, point to **Add Service**, then and click **Time (SNTP)** on the shortcut menu.



7. The **Setup – TimeService** Web page opens.

Setup - TimeService



Property	Value
Time Server Port	123 (not configurable)
Time Synchronization Mode	Automatic ▼
Time Synchronization Interval	12 Hours ▼
Use as	<input checked="" type="radio"/> Default <input type="radio"/> Backup

8. Configure the following time (SNTP) server properties:

Property

- | | |
|--------------------------------------|---|
| <i>Time Server Port</i> | The port used by the SmartServer to receive time data. This default value is 123 , and it cannot be changed. Contact your IS department to make sure that your firewall is configured to allow you to access the time server on this port. |
| <i>Time Synchronization Mode</i> | <p>Select the frequency in which the SmartServer is synchronized to the SNTP server. You have four choices:</p> <ul style="list-style-type: none"> • Automatic. The SmartServer is synchronized every 1 to 15 minutes and remains within 100ms of the SNTP server. This is the default, and it can be used for both LAN and dial-out (modem and GPRS) connections. • Sync when dial-up is active. The SmartServer clock is synchronized when a dial-out connection is established. This option can only be used for dial-out connections (modem and GPRS). • Fixed interval. The frequency in which the SmartServer is synchronized is based on the value in the Synchronization Interval property. This option can only be used for Ethernet connections. • Disabled. The SmartServer is not synchronized with the SNTP server. |
| <i>Time Synchronization Interval</i> | Set how often the SmartServer clock is synchronized with the SNTP server. This option is only available if Fixed Interval is the selected synchronization method. The default synchronization interval is 12 hours . |
| <i>Use As</i> | Select whether this time server is the Default or the Backup time server. If this is the first time service created on the SmartServer, this option is set to Default . If another time service is currently designated as the default and you select Default , the default designation will be removed from the other time server when you click Submit . |

9. Click **Submit** to save the changes.

To delete a time (SNTP) server, right-click the generic server icon if the sever is used exclusively for the time service, or right-click the time service icon if the server is used for other services, click **Delete** on the shortcut menu, and then click **Submit**.

Adding an IP-852 Configuration Server to the LAN

If you licensed and activated IP-852 routing on your SmartServer but you are not using the standard port on the SmartServer for it (1628), you can add an IP-852 Configuration Server to the LAN. Adding an IP-852 Configuration Server to the LAN enables a SmartServer with IP-852 routing activated to communicate with other IP-852 devices over a high-performance IP-852 backbone channel. The other IP-852 devices may include other SmartServers with IP-852 routing licensed, i.LON 600 IP-852 routers, OpenLNS Servers, LNS Servers, and OpenLNS or LNS tool computers.

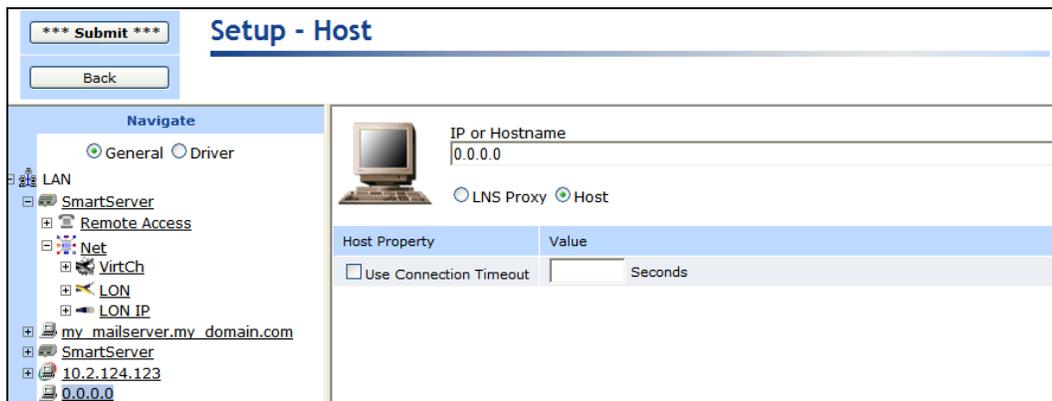
Note: If you are using the standard port for IP-852 routing, you can skip this section and use the **IP-852 Configuration Server** program to add the SmartServer to an IP-852 channel. The IP-852 Configuration Server stores the configuration of the IP-852 channel, including the IP addresses of all the IP-852 devices installed on the channel. You will initially configure the IP-852 channel with the IP-852 Configuration Server, and the IP-852 Configuration Server must be running anytime you change the configurations of the IP-852 devices on the IP-852 channel. You can run the IP-852 Configuration Server on any computer with access to the IP network containing the IP-852 channel. The software required to run the IP-852 Configuration Server is included with the SmartServer software. For more information on the IP-852 Configuration Server and using this program, see the *IP-852 Channel User's Guide*.

To add an IP-852 Configuration Server to the LAN, follow these steps:

1. Right-click the **LAN** icon, point to **Add Host**, and then click **Server (LNS, Email, Time, IP-852, WebTarget)** on the shortcut menu, or if are you adding the IP-852 Configuration Server to an existing server on the LAN, skip to step 4.



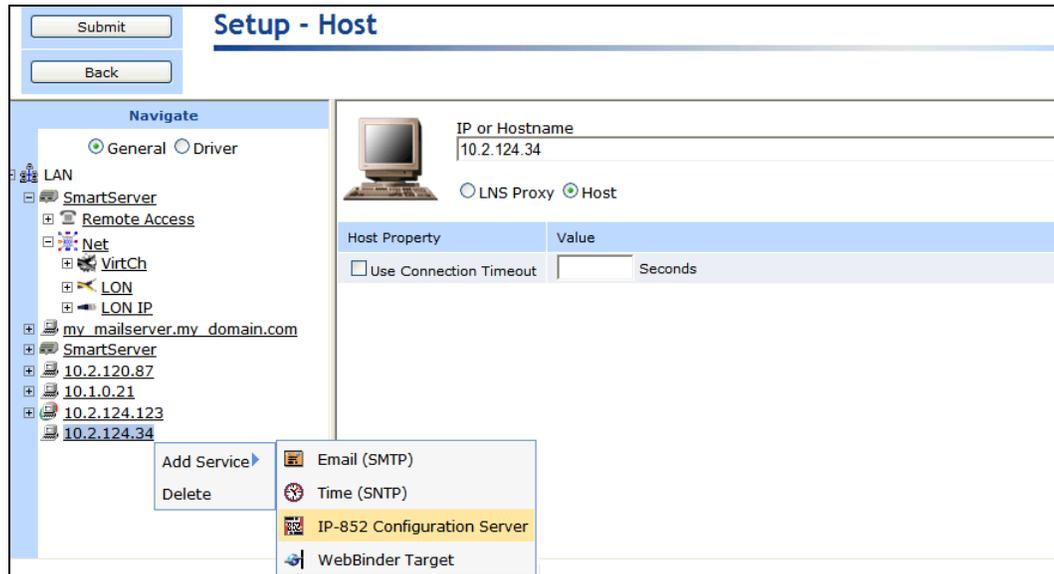
2. The **Setup – Host** Web page opens, and a server icon is added one level below the LAN icon at the bottom of the navigation pane.



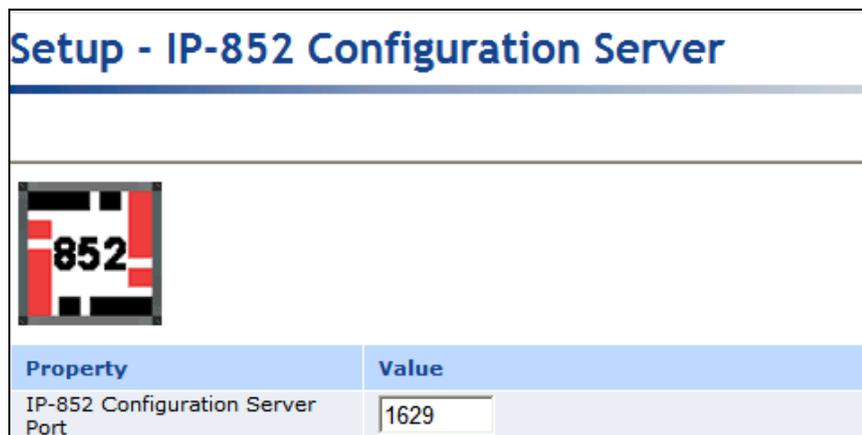
3. Enter the IP address or hostname of the IP-852 Configuration Server.
4. Optionally, select **Use Connection Timeout** and enter the maximum period of time (in seconds) that the IP-852 Configuration Server waits for a response to a SOAP request from the local

SmartServer's Web server before the transaction is canceled and a timeout error is thrown. By default, the connection timeout is 2 seconds if this option is cleared. If you select this option, the default timeout is 120 seconds.

5. Click **Submit**. The server icon in the tree is updated with the IP address or hostname you entered.
6. Right-click the new server icon, point to **Add Service**, then and click **IP-852 Configuration Server** on the shortcut menu.



7. The IP-852 Configuration Server Property Web page opens. Enter the port used by the IP-852 Configuration Server to receive messages form the SmartServer in the **IP-852 Configuration Server Port** box. The default port is 1629.



8. Click **Submit** to save the changes.

To delete an IP-852 Configuration Server, right-click the generic server icon if the sever is used exclusively for the IP-852 Configuration Server, or right-click the IP-852 Configuration Server icon if the server is used for other services, click **Delete** on the shortcut menu, and then click **Submit**.

Adding a Web Connection Target Server to the LAN

You can add a Web Connection Target server (a Web server that can process SOAP requests) to the LAN. This enables you to create Web connections between the local SmartServer and the Web Connection target, which are referred to *enterprise connections*. With enterprise connections, you can send data logs, alarm logs, event scheduler logs, or any user-defined file from your local SmartServer

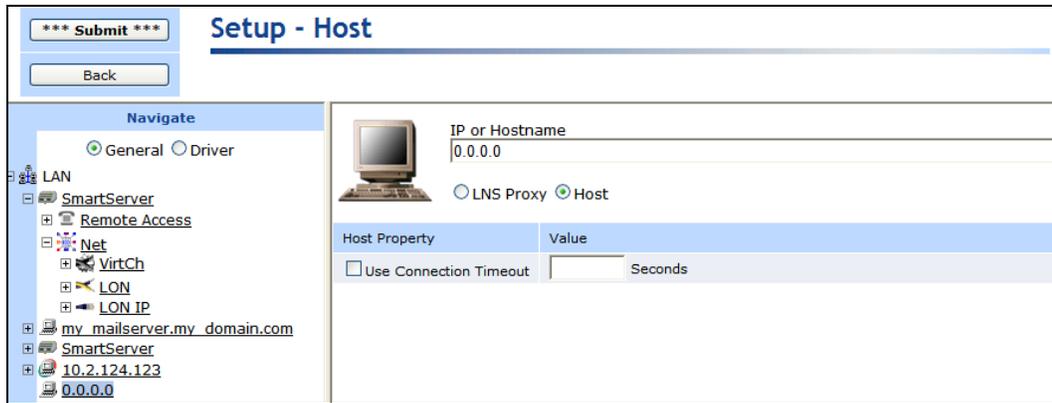
to a central enterprise system. For more information on creating and using Web connections, see *Creating Web Connections* in Chapter 4, *Using the SmartServer Web Interface*.

To add a Web Connection Target server to the LAN, follow these steps:

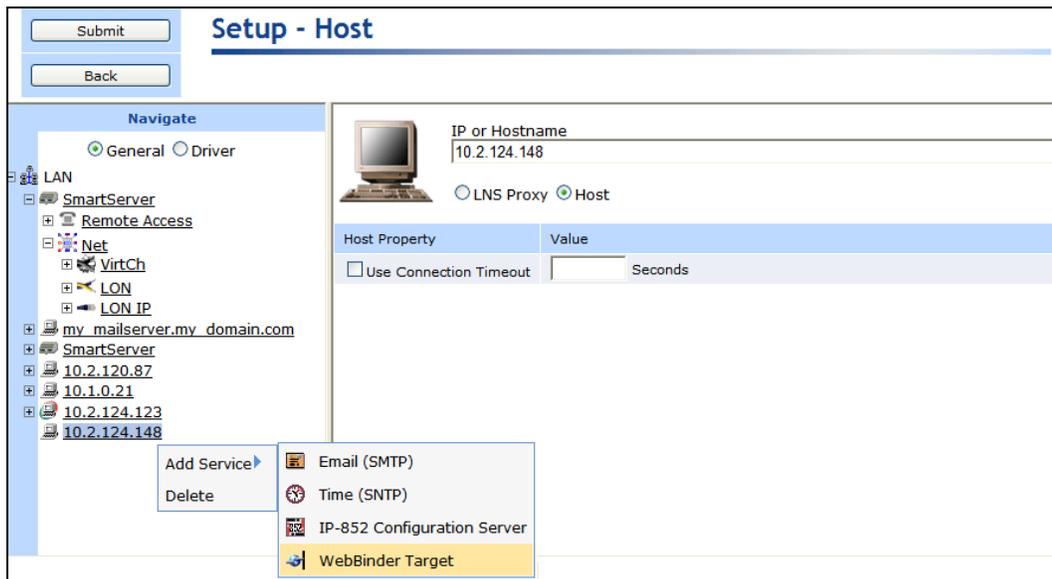
1. Right-click the **LAN** icon or a dial-out connection icon, point to **Add Host**, and then click **Server (LNS, Email, Time, IP-852, WebTarget)** on the shortcut menu, or if are you adding the Web Connection Target to an existing server on the LAN, skip to step 4.



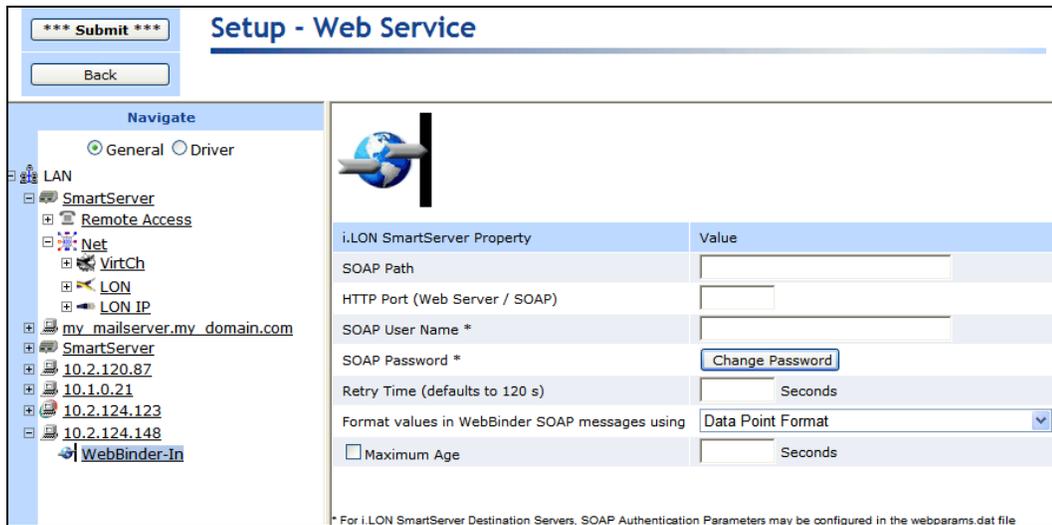
2. The **Setup – Host** Web page opens, and a server icon is added one level below the LAN icon at the bottom of the navigation pane or one level below the dial-out connection icon.



3. Enter the IP address or hostname of the Web Connection Target server and then click **Submit**. The server icon in the tree is updated with the IP address or hostname you entered.
4. Right-click the server icon, point to **Add Service**, then and click **Web Connection Target** on the shortcut menu.



5. The **Setup – Web Service** Web page opens.



6. Configure the following properties for the Web Connection Target server:

**SmartServer
Property**

- | | |
|--|--|
| <i>SOAP Path</i> | Enter the path on the Web Connection Target server to which SOAP messages should be transmitted. This is typically /LnsProxy/LnsProxyService (the location of the SOAP path to the Echelon Enterprise Service running on your computer) . |
| <i>HTTP Port (Web Server/SOAP)</i> | Enter the port that the Web Connection Target server uses to serve HTTP requests (SOAP and WebDAV). The default value is 80 , but you may change it to any valid port number. Contact your IS department to ensure your firewall is configured to allow access to the server on this port.

Select SSL to create a secure Web connection. Enter the port number to use for the SOAP interface. The default port used for SSL is 443 , but you may change it to any valid port number. |
| <i>SOAP User Name</i> | Optionally, you can enter a user name to be used for logging in to the Web Connection Target server. |
| <i>SOAP Password</i> | If you create a Web Connection Target server, click Change Password to enter the password to be used for logging in to the Web Connection Target server. |
| <i>Retry Time</i> | Set the amount of time (in seconds) after which the Web Connection Target server will stop attempting to resend failed Web Connection connection messages. The default value is 120 seconds.

The Web Connection Target server automatically attempts to resend failed Web Connection connection messages every 45 seconds. |
| <i>Format Values in Web Connection SOAP Messages Using</i> | Select how data point values are formatted in SOAP messages sent to this Web Connection Target server via Web connections. You have two choices: <ul style="list-style-type: none"> • Data Point Format. Data point values are formatted based on the SNVT, UNVT, SCPT, or UCPT defined for the data point. |

- **Raw HEX.** Data point values are transmitted in raw hexadecimal format.

Maximum Age

Specify the maximum age (in seconds) to be written to the target data points on the Web Connection destination when the local SmartServer sends updated values to them.

If the Web Connection destination cannot communicate with the parent device of the target data point, the Web Connection destination caches the updated value it received from the local SmartServer. When the device goes online, the cached value is written to the target data point provided that time the value has been cached is less than the maximum age. If the value has been cached longer than the maximum age, the value is not written to the target data point.

7. Click **Submit** to save the changes.

To delete a Web Connection Target server, right-click the generic server icon if the sever is used exclusively for the Web Connection Target service, or right-click the Web Connection Target server icon if the server is used for other services, click **Delete** on the shortcut menu, and then click **Submit**.

Selecting a Network Management Service

You can manage a LONWORKS network using OpenLNS or LNS network management services or using the SmartServer as a standalone network manager. To select a network management service, follow these steps:

1. Click **Driver** at the top of the navigation pane on the left side of the SmartServer Web interface, and then click the **Net** network near the top of the SmartServer tree.
2. The **Setup - LON Network Driver** Web page opens.
3. In the **Network Management Service** property, select one of the following options.

- **LNS Auto** or **LNS Manual.** In LNS mode, the SmartServer manages the network using an OpenLNS or LNS Server.

Note: To use the SmartServer in LNS mode, you must have done the following: installed the SmartServer with OpenLNS CT or LonMaker Integration Tool, or another OpenLNS or LNS application; installed EES 2.2; and added an OpenLNS Server or LNS Server to the LAN (the LNS Server should contain the OpenLNS or LNS network database in which the SmartServer was installed).

For more information on configuring the SmartServer to run in LNS mode, see *Automatically Synchronizing the SmartServer to an OpenLNS Network Database* and *Manually Synchronizing the SmartServer to an OpenLNS Network Database* in Chapter 5.

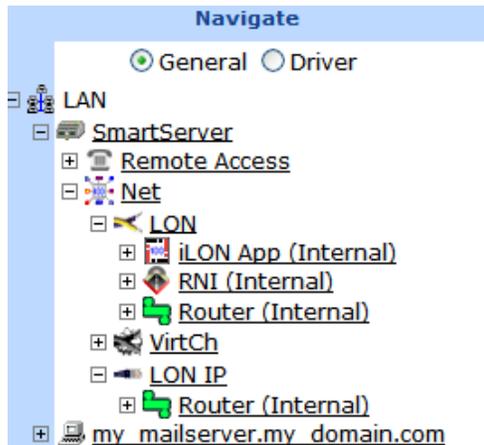
- **Standalone.** In **Standalone** mode, the SmartServer manages the network. You can use standalone mode to install and operate a small, single-channel network that does not require OpenLNS or LNS services or connections to other network management tools. Networks running in standalone mode are limited to a maximum of 300 devices (for FT-10 networks, you need to attach a physical layer repeater to the network to exceed the 64-device limit posed by the physical channel).

See *Using Standalone Mode* in Chapter 5 for more information on configuring the SmartServer to run in standalone mode.

Using the SmartServer as an RNI and IP-852 Router

You can configure your SmartServer as an IP-852 router (if IP-852 routing is activated on your SmartServer) to integrate the network attached to your SmartServer into a single large LONWORKS

network that runs over a high-speed IP-852 backbone. You can also configure your SmartServer as an IP-852 router or as an RNI to connect an OpenLNS, LNS, or OpenLDV-based application to a LONWORKS network remotely via a TCP/IP connection. The SmartServer's IP-852 connection is represented by router icons (🚚) that are listed under both its internal **LON** and **LON IP** channels below the network icon in the tree. The LON IP channel only appears in the tree if an IP-852 router license is installed on your SmartServer. The SmartServer's RNI connection is represented by an RNI device icon (🏠) that is listed under the **LON** channel.



Using the SmartServer as an IP-852 Router

You can activate the IP-852 routing service on your SmartServer to enable the network attached to your SmartServer to be integrated with the networks attached to other IP-852 routers into one large network that runs over a high-speed IP-852 backbone. With IP-852 routing, you can use an OpenLNS, LNS, or OpenLDV application to access the networks attached to IP-852 routers remotely and use LONWORKS connections to bind the devices on the networks together, regardless of the distance between the networks. You just need to make sure that your SmartServer and the other IP-852 routers are on the same IP-852 channel as the OpenLNS or LNS Server and the computer running the OpenLNS, LNS, or OpenLDV application.

To use your SmartServer as an IP-852 router, an IP-852 license must be installed on your SmartServer. The Professional models of the SmartServer include an IP-852 router license. If an IP-852 license is not pre-installed on your SmartServer, you can order one (Echelon model number 72160) from the Echelon Web site at www.echelon.com/products/cis/activate.

To use your SmartServer as an IP-852 router, you do the following:

1. Activate IP-852 routing if an IP-852 license is not pre-installed on your SmartServer.
2. Add your SmartServer to an IP-852 channel using the IP-852 Configuration Server application.
3. Configure your SmartServer as an IP-852 router using an OpenLNS or LNS application such as OpenLNS CT or the SmartServer (from the OpenLNS tree using the LNS Proxy Web service).
4. Use your SmartServer on the IP-852 channel.

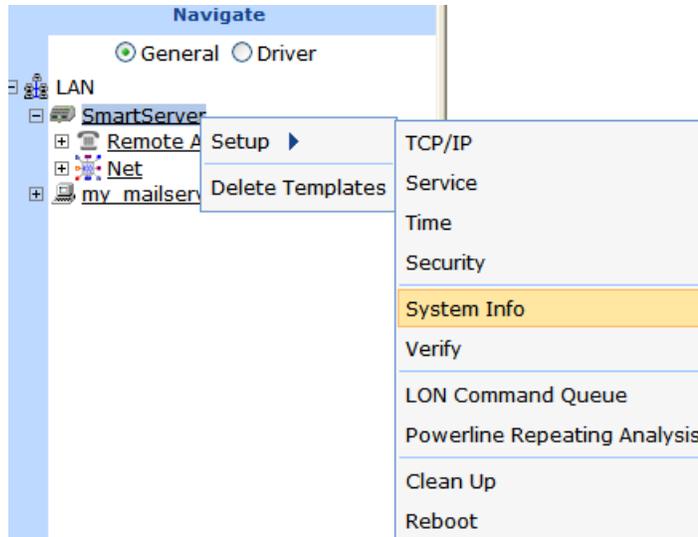
Notes:

- The IP-852 router on the SmartServer does not support routing between devices using IPv6. However, you can use the IP-852 router with IPv4 devices simultaneously with other SmartServer applications that are using IPv6.
- IP-852 routing cannot be used on a power line repeating channel.
- The SmartServer's capabilities are not restricted when using IP-852 routing. All the other application features of the SmartServer are available when it is operating as an IP-852 router.

Activating IP-852 Routing on the SmartServer

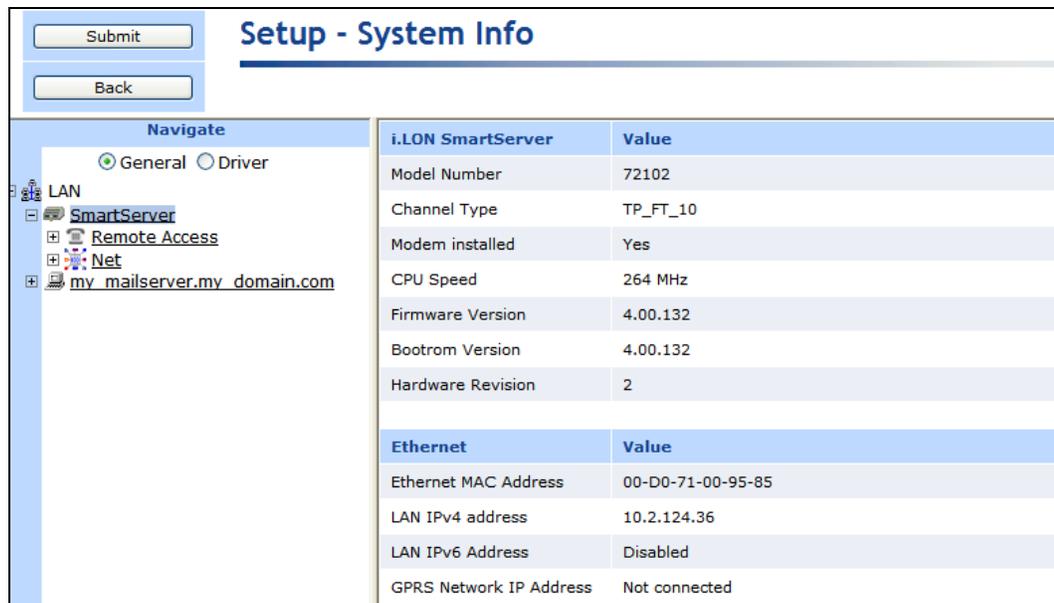
To activate IP-852 routing on your SmartServer follow these steps:

1. Right-click the **SmartServer** icon, point to **Setup**, and then click **System Info** on the shortcut menu.



Alternatively, you can click **Setup** and then click **System Info**.

2. The **Setup - System Info** Web page opens.

A screenshot of the 'Setup - System Info' web page. At the top left, there are 'Submit' and 'Back' buttons. The page title is 'Setup - System Info'. On the left, the 'Navigate' menu is open, showing 'General' selected and 'Driver' unselected. The 'SmartServer' icon is highlighted, and the context menu is open, showing 'Setup' and 'Delete Templates'. The main content area displays a table of system information. The table has two sections: 'i.LON SmartServer' and 'Ethernet'.

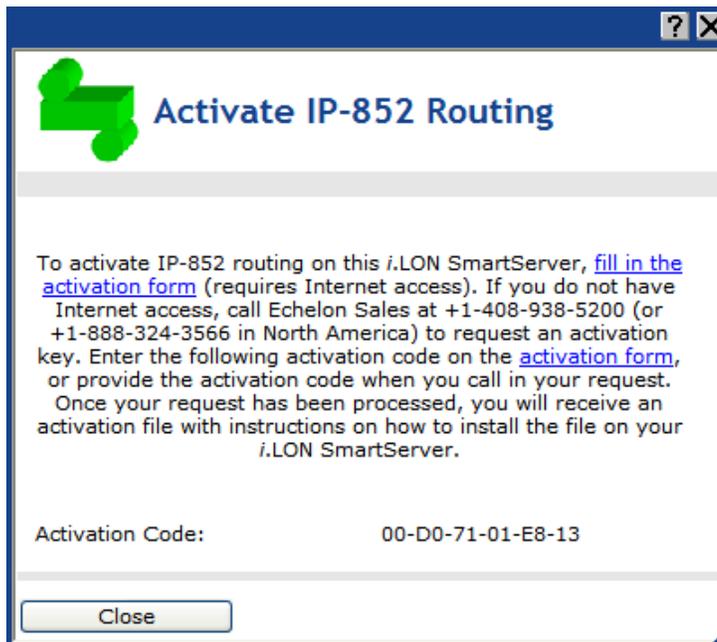
i.LON SmartServer	Value
Model Number	72102
Channel Type	TP_FT_10
Modem installed	Yes
CPU Speed	264 MHz
Firmware Version	4.00.132
Bootrom Version	4.00.132
Hardware Revision	2

Ethernet	Value
Ethernet MAC Address	00-D0-71-00-95-85
LAN IPv4 address	10.2.124.36
LAN IPv6 Address	Disabled
GPRS Network IP Address	Not connected

3. Verify whether IP-852 routing has been licensed on your SmartServer. To do this, scroll down to the **LonTalk Statistics** property header.
 - If IP-852 routing has been licensed, network traffic statistics appear in their respective properties. Skip to step 6.
 - If IP-852 routing has not been licensed, “Not Licensed” appears in all the properties.

Setup - System Info				
Navigate		LonTalk Statistics	Current Value	Packets / Sec
<input checked="" type="radio"/> General <input type="radio"/> Driver		LonTalk-Side Packets sent	Not Licensed	Not Licensed
LAN		LonTalk-Side Packets received	Not Licensed	Not Licensed
<input checked="" type="checkbox"/> SmartServer		LonTalk-Side Packets lost	Not Licensed	Not Licensed
<input type="checkbox"/> Remote Access		IP-Side Packets sent	Not Licensed	Not Licensed
<input type="checkbox"/> Net		IP-Side Packets received	Not Licensed	Not Licensed
<input type="checkbox"/> my_mailserver.my_domain.com		IP-Side Packets stale	Not Licensed	Not Licensed
		IP Configuration Packets sent	Not Licensed	Not Licensed
		IP Configuration Packets Received	Not Licensed	Not Licensed
		Seconds since Last Clear	Not Licensed	Not Licensed
		Time last Cleared	Not Licensed	Not Licensed
		Last Refresh	Not Licensed	Not Licensed

- Click any **Not Licensed** link in the IP-852 router properties. The **Activate IP-852 Routing** dialog opens.



- Follow the instructions on the dialog to obtain your license and activate IP-852 routing on your SmartServer.
- If you do not plan on using the standard local port for IP-852 routing (1628), follow the steps in *Adding an IP-852 Configuration Server* to add the IP-852 Configuration Server to the SmartServer.
- Add the SmartServer to a new or existing IP-852 channel with the IP-852 Configuration Server program. For instructions on using this program to add a SmartServer to an IP-852 channel, see the next section, *Adding a SmartServer to an IP-852 Channel*.
- A **LON IP** channel and a router are added underneath the network icon, and the IP-852 routing service on the SmartServer is activated.

Adding a SmartServer to an IP-852 Channel

You can use the IP-852 Configuration Server application to add a SmartServer to an IP-852 channel. To do this, follow these steps:

1. Start the IP-852 Configuration Server application. Click **Start** on the taskbar, point to **Programs**, point to **Echelon IP-852 Configuration Server**, and then click **IP-852 Configuration Server**. The IP-852 Configuration Server main dialog opens.
2. Verify that the IP-852 Configuration Server is attached to your IP network. To do this, you confirm that the IP network is enabled and verify the IP address of the IP-852 Configuration Server computer is correct.
3. To confirm that the IP network is enabled, check that the **Network** status box displays “Enabled”. If “Enabled” is not displayed, click **Network** and then select **Enabled**. The IP-852 Configuration Server should correctly detect and display the IP address of your computer in the **Channel Description** box.
4. To verify the IP address of the IP-852 Configuration Server computer, click **Network** and then select **Settings**. Confirm that the IP address of the IP-852 Configuration Server computer is shown in the **Local IP Address or Hostname** box.
5. If you are adding the SmartServer to a new IP-852 channel, click **Channel** and then click **New Channel**. Configure the channel following the *IP-852 Channel User’s Guide*.
6. Right-click the IP-852 channel to which the SmartServer is to be added, and select **New Device** on the shortcut menu. An IP-852 device is added to the channel.
7. Enter a descriptive name for the new IP-852 device.
8. Right click the new IP-852 device and select **Device Properties**. The **New Device Properties** dialog appears with the **IP Address** tab selected.
9. Enter the IP address of the SmartServer in the **IP Address or Hostname** box and then click **Apply**. This is the same IP address that you assigned to the SmartServer using the Setup Web pages. If you enter a hostname, it must be registered with a DNS server that is available to the IP-852 Configuration Server computer.
10. Click the **iLON Time Zone** tab and set the time zone corresponding with the geographical area in which the SmartServer resides and then click **OK**.
11. The IP-852 Configuration Server adds the SmartServer to the IP-852 channel and updates the configuration of the SmartServer automatically.

For more information on using the IP-852 Configuration Server application, see the *IP-852 Channel User’s Guide*.

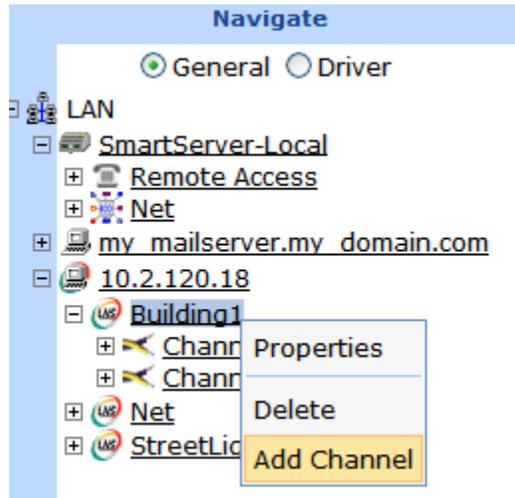
Configuring the SmartServer as an IP-852 Router

You can configure your SmartServer as an IP-852 router using an OpenLNS or LNS application such as OpenLNS CT or the SmartServer (from the OpenLNS tree using the LNS Proxy Web service). For information on using OpenLNS CT to configure your SmartServer as an IP-852 router, see Chapter 2 of the *IP-852 Channel User’s Guide*.

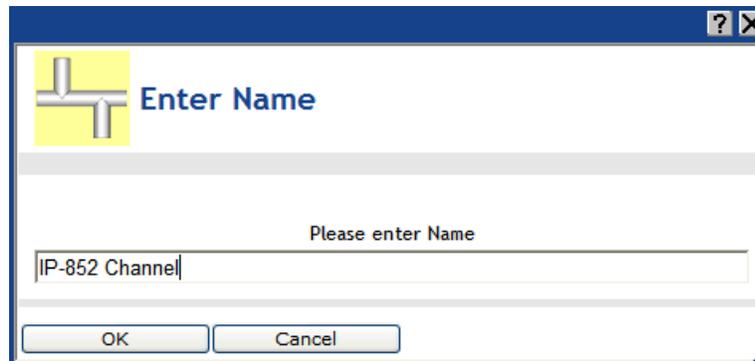
To use the OpenLNS tree on the SmartServer to configure your SmartServer as an IP-852 router, follow these steps:

1. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User’s Guide* for how to perform these installations.
2. Verify that an OpenLNS Server computer containing the OpenLNS network database in which the SmartServer is to be used as an IP-852 router has been added to the LAN. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on how to do this.

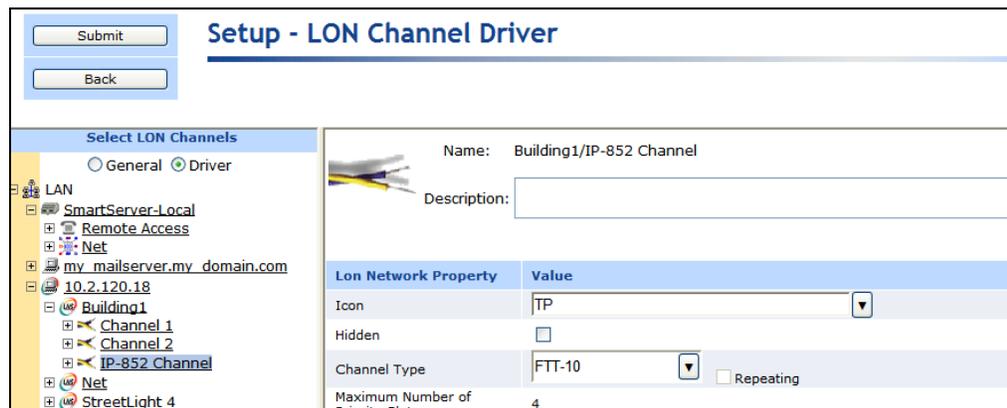
3. Expand the LNS Server icon, and then enter the **User Name** and **Password** for logging in to the OpenLNS Server via the Echelon Enterprise Services 2.2. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon in the notification area of your computer, and then click **Options** on the shortcut menu.
4. Create an IP-852 channel in the OpenLNS tree. To do this follow these steps:
 - a. Right-click the OpenLNS network icon and then click **Add Channel** on the shortcut menu.



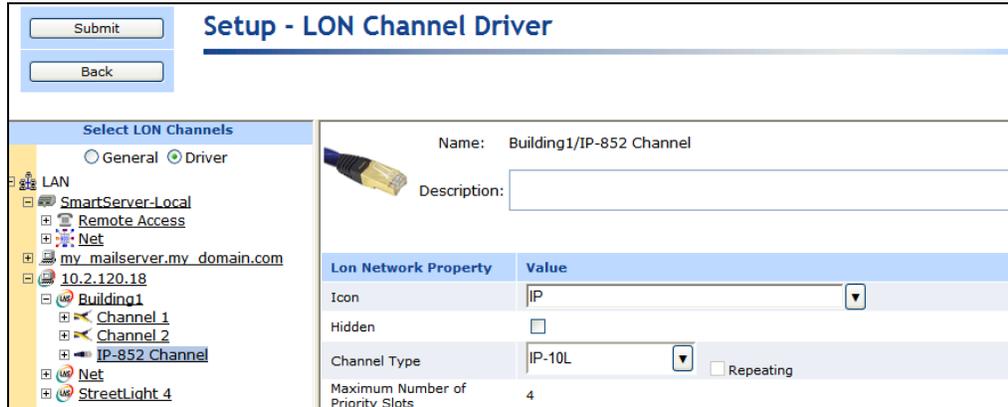
- b. The **Enter Name** dialog opens. Enter a descriptive name for the IP-852 channel such as “IP-852 Channel”, click **OK**, and then click **Submit**.



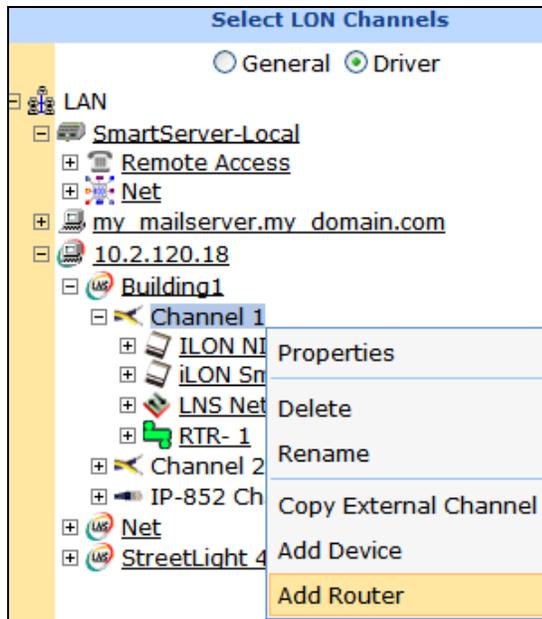
- c. Click the channel created in step b and then click **Driver**. The **Setup – LON Channel Driver** Web page opens.



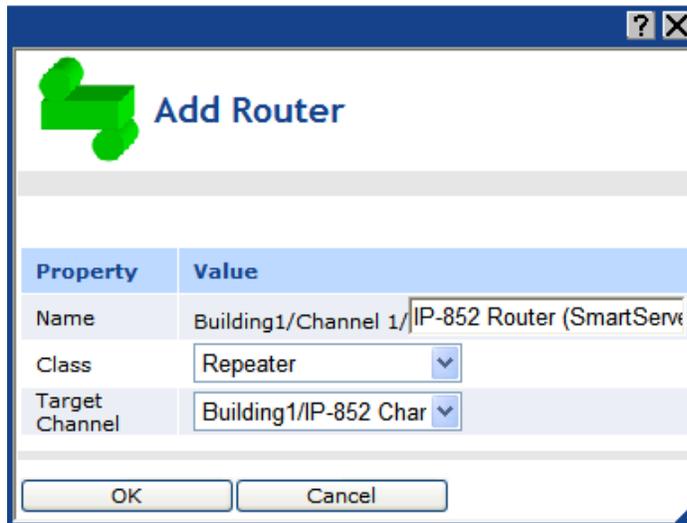
- d. In the **Icon** property, select the **IP** icon; in the **Channel Type** property, select **IP-10L** (if using a local IP network) or **IP- 10W** (if using a wide area IP network); and then click **Submit**.



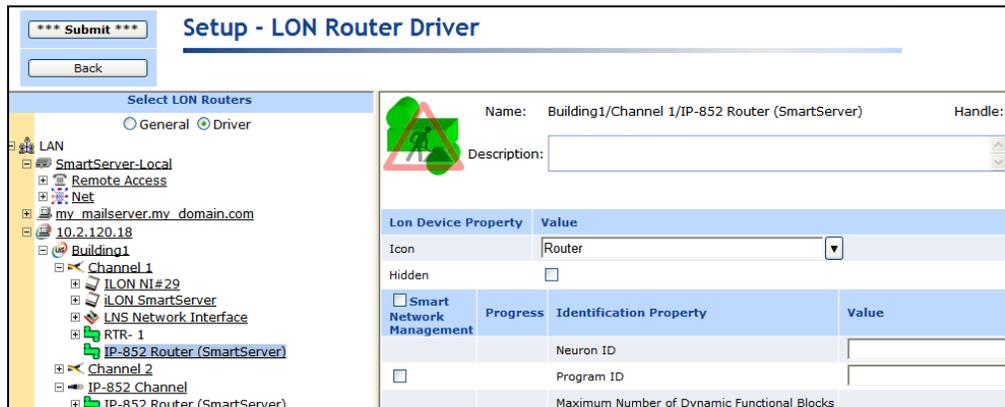
5. Add a router between the LONWORKS channel closest to the OpenLNS network interface and the IP-852 channel. To do this follow these steps:
- Right-click the LONWORKS channel closest to the OpenLNS network interface and then click **Add Router** on the shortcut menu.



- The **Add Router** dialog opens. Enter a descriptive name for the IP-852 router on the SmartServer such as “IP-852 Router (SmartServer)”, select the IP-852 channel created in step 4 in the **Target Channel** property, and then click **OK**.



- c. The **Setup – LON Router Driver** Web page opens, and router icons are added under the LONWORKS channel (near side) and the IP-852 Channel (far side) in the OpenLNS tree.



- d. Click **Submit**.
6. Commission the near side of the SmartServer's IP-852 router. To do this, follow these steps:
 - a. In the **Neuron ID** property on the **Setup – LON Router Driver** Web page, click **Use Service Pin**.

Setup - LON Router Driver

Name: Building1/IP-852 Channel/IP-852 Router (SmartServer) Handle: 65

Description:

Lon Device Property		Value
Icon		Router
Hidden		<input type="checkbox"/>

<input type="checkbox"/> Smart Network Management	Progress	Identification Property	Value
		Neuron ID	<input type="text" value="000000000000"/> <input type="button" value="Use Service Pin"/>
<input type="checkbox"/>		Program ID	<input type="text" value="8000010101000000"/>
		Maximum Number of Dynamic Functional Blocks	0
		Maximum Number of Dynamic Data Points	0
		Geographical Position	<input type="text"/>

- b. The **LON Device Identification** dialog opens. Press the service pin on your SmartServer, click **OK** to return to the **Setup – LON Router Driver** Web page.

Service pin messages for the **i.LON App (Internal)** and **i.LON NI (Internal)** devices also appear with the one for the **Router (Internal)** device if the **Show Messages with Identical Program ID Only** check box is cleared. However, the Neuron ID of the IP-852 router is selected by default because its program ID matches the one fetched from the IP-852 Router device.

LON Device Identification

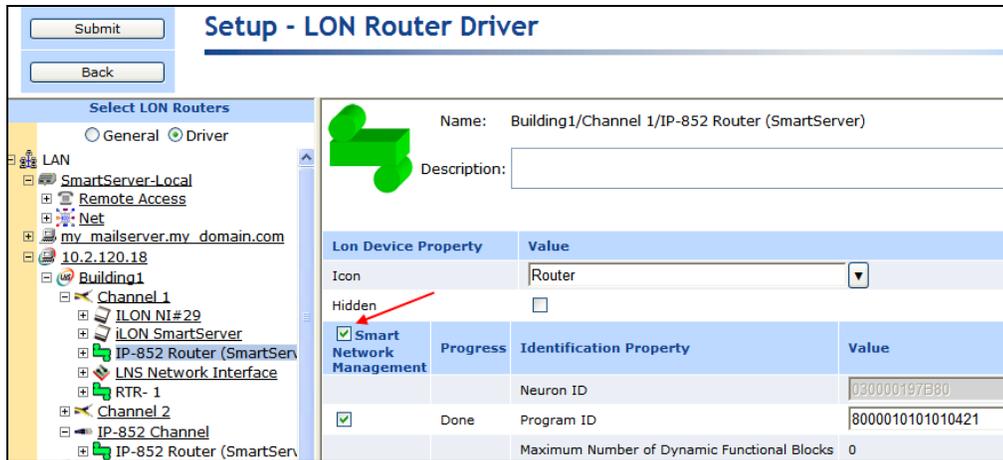
Property	Value						
Incoming Service Pin Messages	<table border="1"> <tr> <td>030000197B82</td> <td>900001012881040C</td> </tr> <tr> <td>030000197B84</td> <td>9000010102810401</td> </tr> <tr> <td>030000197B80</td> <td>80000101010421</td> </tr> </table>	030000197B82	900001012881040C	030000197B84	9000010102810401	030000197B80	80000101010421
030000197B82	900001012881040C						
030000197B84	9000010102810401						
030000197B80	80000101010421						

Show Messages with Identical Program ID only

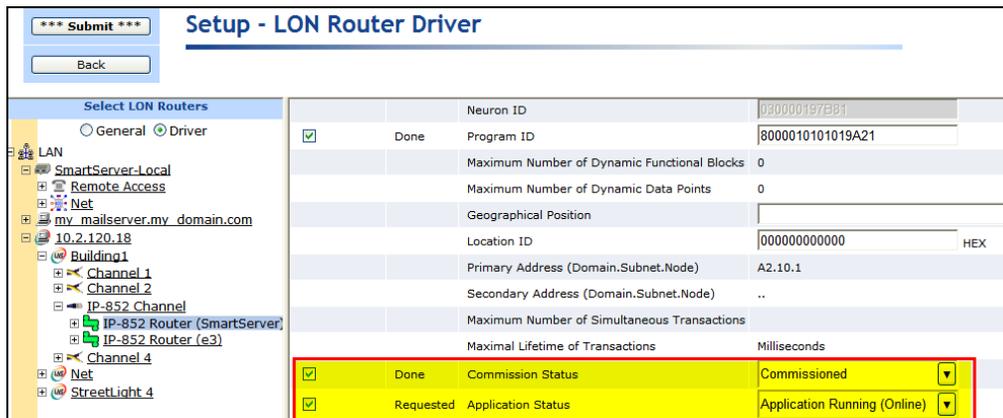
Neuron ID or LUID

Program ID

- c. Click **Submit**.
7. Select **Smart Network Management** at the top of the Web page and then click **Submit**. This automatically commissions the IP-852 router and starts the router application.



Alternatively, you can scroll down to the **Commission Status** property, and either select the individual Smart Network Management property option to the left or select **Commissioned** from the list to the right. In the **Application Status** property, select the individual Smart Network Management property option to the left or select **Application Online (Running)** from the list to the right. Click **Submit**.



- You can repeat steps 5–6 to add and commission another i.LON IP-852 router (SmartServer, i.LON e3 Server, or i.LON 600 IP-852 Router) between the IP-852 channel and another LONWORKS channel. The i.LON IP-852 router to be added and commissioned must already have been added to the IP-852 channel with the IP-852 Configuration Server application.

Note: You must add the i.LON IP-852 router to the IP-852 channel you created in step 4 and commission the near side of the router (the router icon below the IP-852 channel).

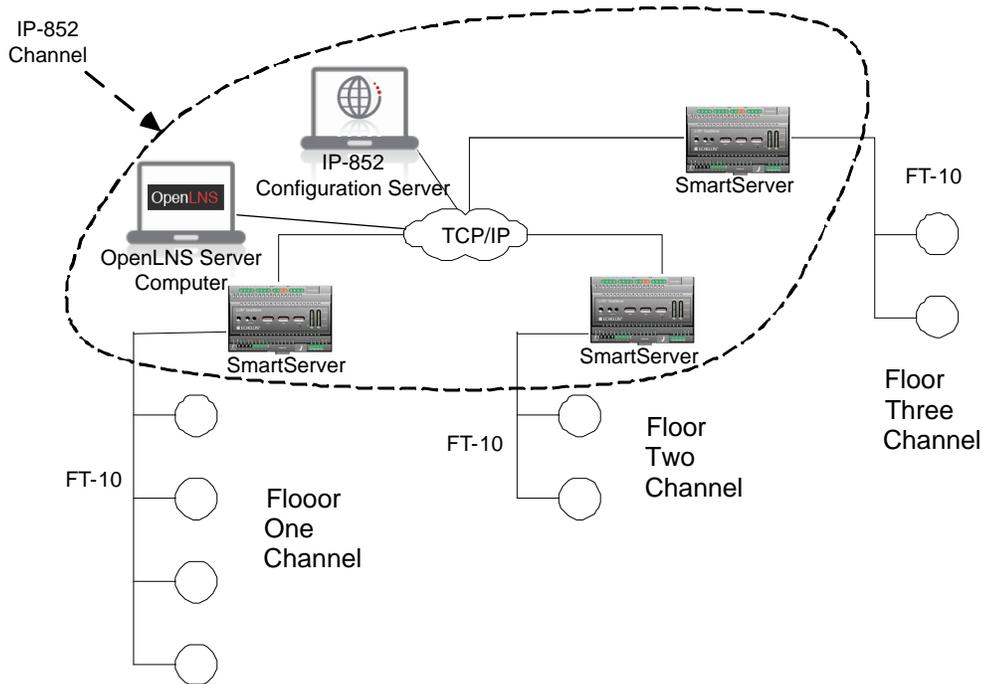
- After you have added and commissioned the i.LON IP-852 router, you can use the OpenLNS tree to create LONWORKS connections between the devices attached your SmartServer and the devices attached to the i.LON IP-852 router created in step 7. See *Connecting LONWORKS Data Points with LONWORKS Connections* in Chapter 5, *Using the SmartServer as a Network Management Tool*, for more information on creating LONWORKS connections.

Using an IP-852 Channel

An IP-852 channel uses the IP addresses on a shared IP network to form a “virtual wire” connecting IP-852 devices. IP-852 devices use this virtual wire in the same way they use traditional dedicated twisted pair wiring.

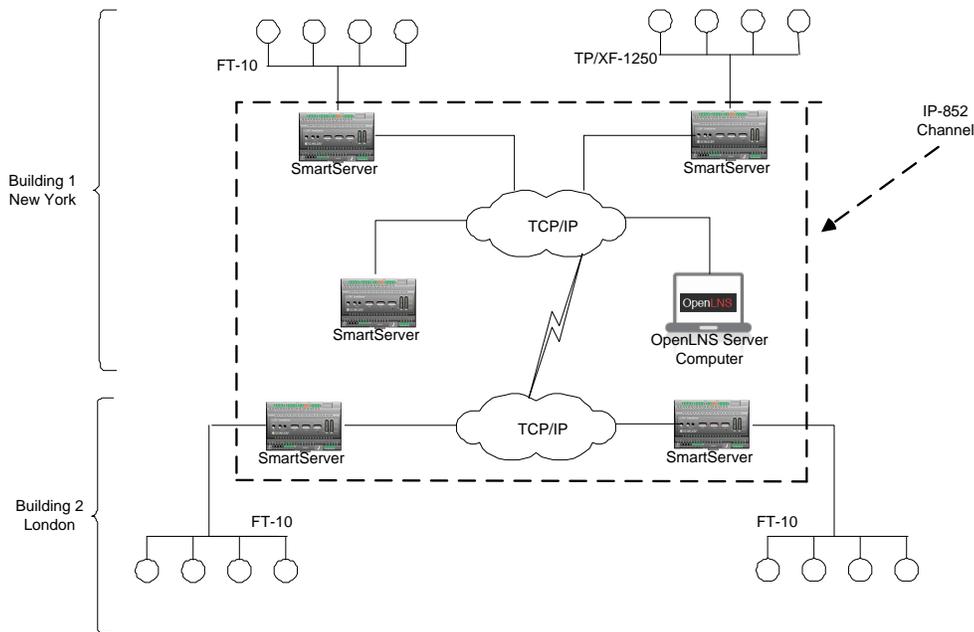
The concept of an IP-852 channel is similar to a Virtual Private Network (VPN). Each IP-852 device in the system is aware of its peers and each IP-852 device keeps peer information in its routing tables

so it can forward LONWORKS packets to the correct IP address. The following figure shows a typical IP-852 channel configuration.



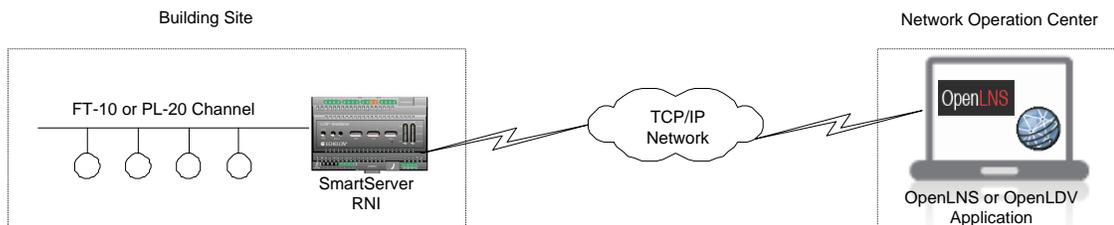
This example demonstrates a network in which three SmartServers are used to create an IP-852 channel connecting three TP/FT-10 channels, each of which connects the devices installed on a different floor in a building. The circled portion of the diagram represents the IP-852 channel—the virtual, IP-based connection between the three SmartServers, the OpenLNS Server, and the IP-852 Configuration Server. An OpenLNS, LNS, or OpenLDV application can use this IP-852 channel to communicate with the devices on all three of the TP/FT-10 channels connected to each of the three SmartServers, and monitor and control the entire building.

A complete installation may contain many IP-852 devices attached to one IP-852 channel. Because the IP-852 channel can exist on any IP network, a system may now span the entire globe as easily as it once spanned a single building, as shown in the following figure.



Using the SmartServer as an RNI

You can use the SmartServer as a Remote Network Interface (RNI). This enables you to connect an OpenLNS, LNS, or OpenLDV-based application to a LONWORKS network remotely via a TCP/IP connection. This means that you do not need to install a local network interface (for example, PCLTA-10, PCLTA-20 and 21, PCC-10, or U10) on the computer running the OpenLNS, LNS, or OpenLDV-based application to connect it to the LONWORKS network. The following figure demonstrates how the SmartServer can be used as an RNI to connect a computer running an OpenLNS, LNS, or OpenLDV-based application to a LONWORKS network.



To use the SmartServer as an RNI, you must configure the RNI settings for the SmartServer on the computer running the OpenLNS, LNS, or OpenLDV-based application with the LONWORKS Interfaces application. Once you have done this, the SmartServer will appear in the list of available network interfaces you can use with your OpenLNS and OpenLDV-based applications.

Note: If you are using either LNS or OpenLDV, you need to install OpenLDV 4.0 on your computer to create the remote network connection. You can download OpenLDV 4.0 from the Echelon support Web site at www.echelon.com/support. OpenLDV 4.0 is included with OpenLNS.

This section describes the following:

- How to configure your SmartServer as an RNI using the LONWORKS Interfaces application.
- How to configure the RNI properties on the SmartServer.
- Limits on the SmartServer when operating as an RNI.
- How to switch the network interface to an RNI or a local network interface.
- Differences between using an RNI and IP-852 routing to connect an OpenLNS, LNS, and OpenLDV-based application to a LONWORKS network.

Configuring the SmartServer as a Remote Network Interface

You can use the LONWORKS Interfaces Control Panel application to configure your SmartServer as an RNI. You can then reference this RNI with your OpenLNS, LNS, or OpenLDV-based application to connect the application to the LONWORKS network attached to the SmartServer. A separate entry is required for each SmartServer you plan to use as an RNI and connect to the OpenLNS or LNS Server.

If you are managing a large application on a single OpenLNS or LNS workstation and will be using many SmartServers (more than 50), you can create an external lookup extension to improve performance. See the *OpenLDV Programmer's Guide, xDriver Supplement* for more information on doing this.

To use the LONWORKS Interfaces application to configure your SmartServer as an RNI, follow these steps:

1. Click **Start** on the taskbar, open the **Control Panel**, and then double-click the **LONWORKS Interfaces** application. The LONWORKS Interfaces application's opens and the **RNI** tab is selected.
2. Click **Interface**, point to **Add**, and then either click **RNI Interface** or click **New Interface** and then click **RNI** in the **Select Interface Type** dialog.
3. The **Add Network Interface Wizard** dialog opens.

The screenshot shows the 'Add Network Interface' dialog box. It has a blue title bar with the text 'Add Network Interface' and a close button. The dialog is divided into three sections: 'Name', 'IP Address / Hostname', and 'Authentication'. The 'Name' section has a text box with 'X.Default' and a dropdown menu set to 'Default'. The 'IP Address / Hostname' section has a text box and a 'Port' field set to '1628'. The 'Authentication' section has a dropdown menu set to 'Use MD5 Key' and a text box containing '00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00'. At the bottom are 'OK' and 'Cancel' buttons.

4. Enter the following properties for the RNI:

Name

Enter a unique name for the RNI to be configured on the SmartServer. This will be used as a lookup key to access the proper registry entry each time xDriver initiates a connection to this RNI.

The name you specify will be appended to the name of the RNI's xDriver

profile (for example, "X.Default" is the name of the default profile). If you enter "myRNI" for example, the name of your RNI by default will be "X.Default.myRNI".

Optionally, select the xDriver profile to be used by your RNI. Typically, you will use the **Default** Profile; however, you can select a different profile. An xDriver profile represents a set of configuration parameters that determine how xDriver manages a group of connections. The profile that xDriver uses for each connection is determined on a session-by-session basis.

*IP Address/
Hostname*

Specifies the hostname or IP address of the RNI. This is the same IP address that you assigned to the SmartServer using the Setup Web pages. If you enter a hostname, it must be registered with a DNS server that is available to the computer on which the LONWORKS Interfaces application is running

You may enter a hostname (for example, myilon.mynet.com), IPv4 address (for example, 192.168.1.1), or IPv6 address (for example, FEDC:BA98:7654:3210:0123:4567:89AB:CDEF). You may enter any valid IPv6 notation in addition to the preferred form shown above.

If you enter an IPv6 address, the address you enter must conform to the IPv6 addressing standards. The following provides two example IPv6 addresses:

2002:1234:0000:0000:02d0:71ff:fe00:00aa

2002:1234::2d0:71ff:fe00:aa

For more information about IPv6 addressing, see "RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture" at www.faqs.org/rfcs/rfc3513.html. Section 2.2 of the RFC describes the addressing formats shown above in more detail.

In the **Port** box, enter the port number on which the SmartServer should listen for messages when it is used as an RNI. The default port is **1628**.

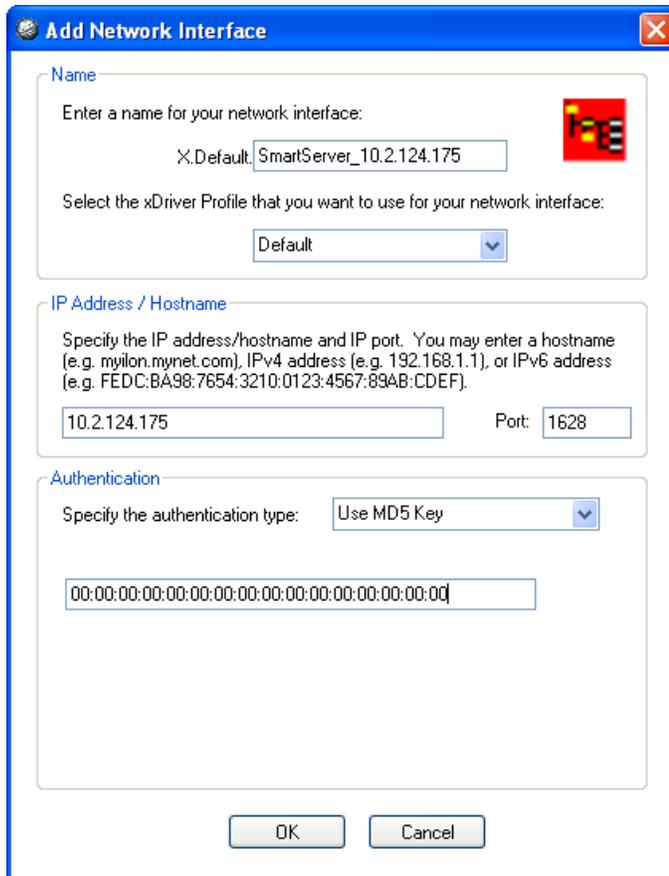
Authentication

Specify how connections between the SmartServer RNI and the OpenLNS Server are authenticated. Using authentication prevents the RNI or OpenLNS Server from responding to unauthorized messages during an xDriver session. You have the following two choices:

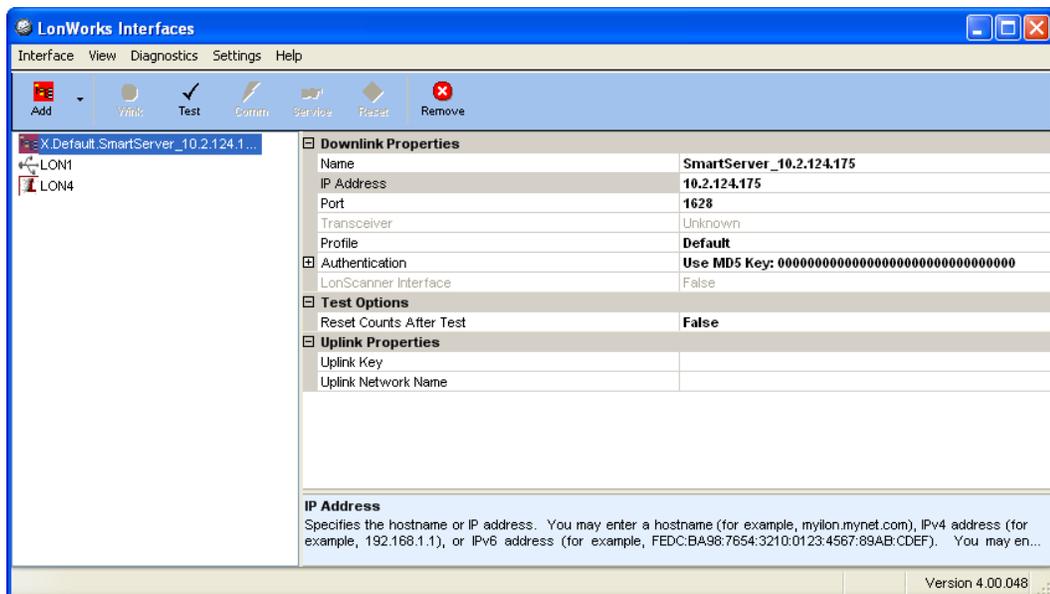
- **Use MD5 Key.** Enter a 32-character hexadecimal string representing a 128-bit MD5 key. The 32 characters must be entered in colon-separated pairs. For example:
A9:04:87:49:F4:BF:89:59:03:10:C5:47:BD:45:94:D7.

This key must match the MD5 authentication key configured into the device. Setting the authentication key to all 0s causes xDriver to use the pre-defined, default factory authentication key for the SmartServer RNI device. For security reasons, do not use the default authentication key. This is the default authentication type.

- **Use Secret Phrase.** Enter a 16 to 63 character string that matches the text secret phrase configured into the SmartServer RNI device.



5. Click **OK** to create the RNI.
6. The SmartServer is now configured as an RNI. The name you entered for the SmartServer RNI device appears in the list view on the left side of the user interface.



7. Optionally, you can continue configuring the RNI by editing the properties on the right side of the user interface. See the LONWORKS Interfaces on-line help for more information on configuring the RNI.

8. Using the SmartServer Web interface, verify that the SmartServer is enabled for RNI connections. Right-click the SmartServer host device, point to **Setup**, and then click **Security**. The **Security** Web page opens. In the **Service** section, confirm that the **Enable Downlink RNI Connections** check box is selected.
9. You can now use the RNI configured on your SmartServer to connect an OpenLNS, LNS, or OpenLDV application to a LONWORKS network, just as you would with any other local LONWORKS network interface.

Note: You may have multiple SmartServers configured as RNIs that are all connected to the same channel. This is a valid configuration; however, if your OpenLNS, LNS, or OpenLDV application uses the RNI on any of those SmartServer to connect to the channel, the application cannot commission any of the other SmartServers that are also configured to operate as RNIs. This is because the SmartServer being commissioned would be assigned the same network address as the SmartServer used to access the channel. To avoid this, either program your application to assign the SmartServer being commissioned a different network address, or you disable the RNI on the SmartServer being commissioned. You can disable the RNI by clearing the **Enable Downlink RNI Connections** option in the **Service** section of the **Security** Web page.

Configuring the SmartServer RNI Properties

You can configure the SmartServer's RNI properties using the SmartServer Web pages following these steps.

1. Click **Driver** at the top of the tree.
2. Expand the network icon, expand the SmartServer's internal **LON** channel, and then click the **RNI (Internal)** device. The **Setup – LON RNI Driver** Web page opens.

i.LON SmartServer POWERED BY ECHELON

Setup - LON RNI Driver

Select LON RNI Devices

General Driver

- LAN
 - SmartServer
 - Remote Access
 - Net
 - LON
 - iLON App (Internal)
 - RNI (Internal)
 - Router (Internal)
 - VirtCh
 - LON IP
 - my_mailserver.my_domain.com



Name: Net/LON/RNI Handle: -5

Description:

Lon Device Property		Value
Icon		RNI
Hidden		<input type="checkbox"/>
Smart Network Management		Value
<input type="checkbox"/>	Progress	
	Identification Property	
	Neuron ID	030000046c53
<input type="checkbox"/>	Program ID	4c354d6970000000
	Maximum Number of Dynamic Functional Blocks	0
	Maximum Number of Dynamic Data Points	0
	Geographical Position	
	Location ID	000000000000 HEX
	Primary Address (Domain.Subnet.Node)	.0.0
	Secondary Address (Domain.Subnet.Node)	.0.0
	Maximum Number of Simultaneous Transactions	256
	Maximal Lifetime of Transactions	0 Milliseconds
<input type="checkbox"/>	Unknown	Commission Status
		Commissioned
<input type="checkbox"/>	Unknown	Application Status
		Application Running (Online)
<input type="checkbox"/>		Reset
RNI Property		Value
	Port	1628
	Maximum Number of Simultaneous Receive Transactions	16

3. Scroll to the **RNI Property** header and configure the following properties:

Port

Displays the port used by the SmartServer to listen for LonTalk packets when it is being used as an RNI. The default port is **1628**.

Maximum Number of Simultaneous Receive Transactions Enter the maximum number of receive transactions that the RNI application can receive at one time. This value may range from 1 to 32,768. The default value is **16**. You can increase this value if you observe buffer overflows. You can decrease this value if you observe that the SmartServer's memory is low.

A receive transaction entry is required for any incoming message which uses either repeating or acknowledged messaging service (a receive transaction is not required for messages using unacknowledged service). A receive transaction entry is also required for each unique source address/destination address/priority attribute.

Each receive transaction entry contains a current transaction number. A message is considered to be a duplicate if its source address, destination address, and priority attribute vector into an existing receive transaction and the message's transaction number matches the entry's transaction number.

Receive transaction entries are freed after the receive timer expires. The receive timer duration is determined by the destination device and varies as a function of the message addressing mode. For group addressed messages, the receive timer is determined by the address table. For Neuron ID addressed messages, the receive timer is fixed at eight seconds. For other addressing modes, the non-group receive timer in the configuration data structure is used.

4. Click **Submit** to save your changes.

SmartServer RNI Limits

The capabilities of the RNI on the SmartServer depend largely on the software running on the host computer. When configured as an RNI, the SmartServer has the following limits:

- Up to 32,768 address table entries.
- Up to 256 simultaneous outgoing transactions.
- Up to 32,768 simultaneous incoming transactions.
- Up to 1,024 network variable aliases.
- Up to 256 groups, with up to 15 used for incoming messages.
- Up to 4,096 dynamic network variables.
- Output messages can be sent to up to 256 different destination addresses within each 24-second interval. Multiple messages can be sent to each of those destination addresses within the interval.
- One RNI link at a time.

See *Introduction to LONWORKS® Platform* for more information about these limits. This guide is available on the Echelon Web site at www.echelon.com/docs.

Switching Between the SmartServer RNI and a Local Network Interface

You can switch the network interface used by an OpenLNS, LNS, or OpenLDV application to communicate with a LONWORKS network. You can switch to either the RNI configured on the SmartServer or a local network interface such as a PCLTA-20 or 21, PCLTA-10, PCC-10, or U-10.

If your SmartServer is configured as an RNI and want to switch to a local LONWORKS network interface, but you want to leave the SmartServer attached to the network, you must disable the RNI

application on the SmartServer before opening the network with the new network interface. You can disable the RNI using the SmartServer Web interface or the console application.

- To use the SmartServer Web interface to disable the RNI, right-click the SmartServer host device, point to **Setup**, and then click **Security**. The **Setup – Security** Web page opens. In the **Service** section, clear the **Enable Downlink RNI Connections** check box. To restart the RNI application later, select the **Enable Downlink RNI Connections** check box.
- To use the console application to disable the RNI, enter the following command:

```
deactivate 4
```

“4” is the index of the RNI application. You can obtain the index of the applications on the SmartServer by entering the following command:

```
listapp
```

Confirm that you want to disable the RNI application. Disabling the RNI application may cause the SmartServer to reboot. To restart the RNI application later, enter the following command:

```
activate 4
```

See *Appendix B* for more information about the console application.

If you are using a local LONWORKS network interface and you want to switch the network interface to the RNI configured on the SmartServer, you must physically remove the local network interface device from the network.

Connecting the SmartServer with RNI vs. IP-852

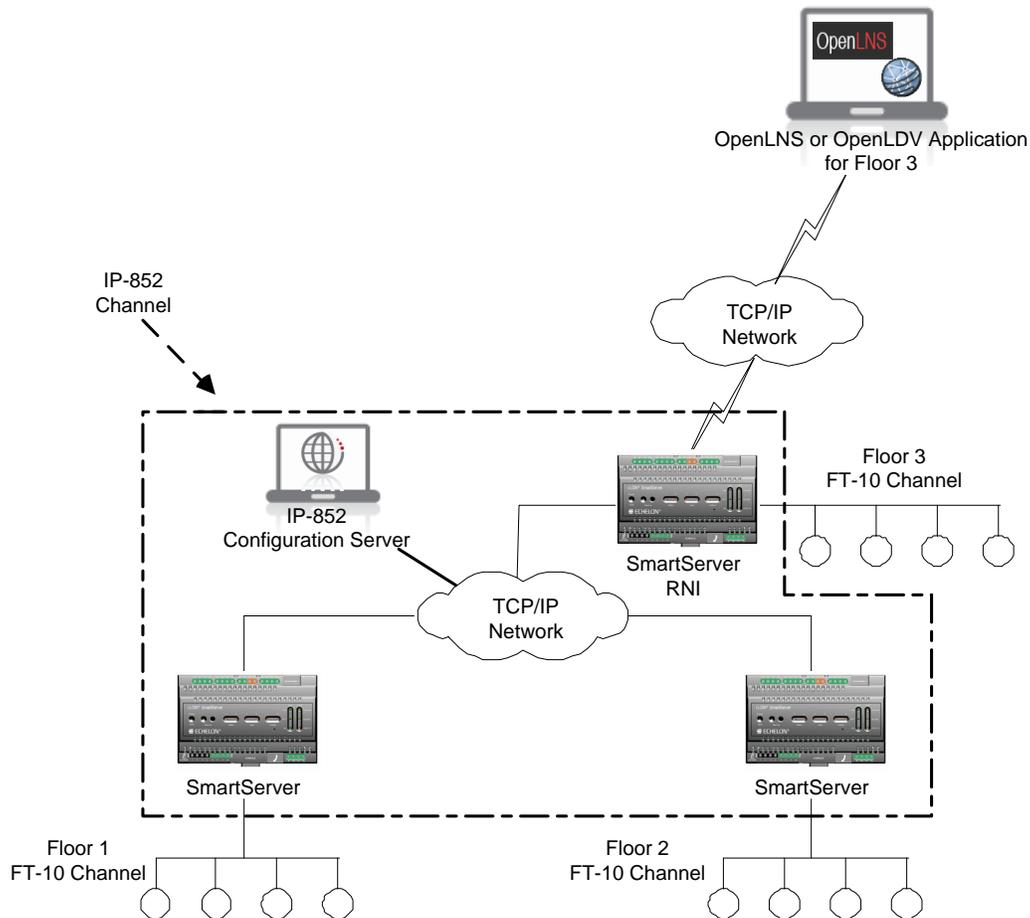
You can use the SmartServer to connect an OpenLNS, LNS, and OpenLDV-based application to a LONWORKS network over an IP network. You can create this remote connection by either configuring the SmartServer as an RNI or activating IP-852 routing on the SmartServer and adding it to the same IP-852 channel on which the computer running the OpenLNS, LNS, or OpenLDV application resides.

If you use the SmartServer as an RNI, it means that you are using it as a network interface to establish a point-to-point connection between an OpenLNS, LNS, or OpenLDV-based application and the LONWORKS channel to which your SmartServer is attached. This approach is simpler than using IP-852 routing and is an option if you are only using a single SmartServer on one channel.

If you need to connect multiple TP/FT-10 or PL-20 channels over an IP network so that a single application could connect to the devices on each channel, then you can use IP-852 routing on the SmartServer. In addition, you can use IP-852 routing if you have multiple SmartServers on multiple channels, and you want to connect the channels. This may be especially useful if each SmartServer needs to connect to the same OpenLNS or LNS Server.

In addition, you can use a SmartServer as an RNI and as an IP-852 router simultaneously. For example, consider a building with multiple floors, where the devices in the rooms on each floor are connected by an FT-10 channel, and each floor has a SmartServer installed to manage those devices. You could create an IP-852 channel to connect all three floors and control them with a central application. This would be the best way to perform control of the building over a long period of time. However, you may need another entry point into the network at some point, to perform maintenance on a certain part of the building. In this case, you could configure the SmartServer as an RNI for a specific floor to be accessed by an OpenLNS, LNS, or OpenLDV application. This would prevent you from having to re-configure the IP-852 channel with the Configuration Server, which you may want to avoid doing if you do not plan on making the new entry point a long-term part of the network.

The following figure demonstrates a SmartServer on an IP-852 channel being configured as an RNI for a specific floor (Floor 3) of a building. This enabled an OpenLNS, LNS, or OpenLDV application to connect to the devices on Floor 3 without having to re-configure the IP-852 channel with the Configuration Server. In this example, the SmartServer for Floor 3 is involved in two separate TCP/IP connections: (1) the IP-852 connection with the other SmartServers, and (2) the RNI connection with the application for Floor 3.



Note: The SmartServer’s capabilities are not restricted when using either the RNI or IP-852 routing function. All the other application features of the SmartServer are available when it is operating as an RNI or as an IP-852 router.

Managing the SmartServer

You can manage the connections, performance, and configuration of your SmartServer. This section describes how to perform the following management tasks with your SmartServer:

1. View system information and performance with the **Setup – System Info** Web page.
2. View system health monitoring with the **systemhealth.conf** file on the SmartServer flash disk.
3. Test connections with the **Setup – Verify** Web page.
4. Upgrade an i.LON 100 e3 plus Server to the SmartServer.
5. Downgrade the SmartServer 2.2 firmware to the SmartServer 1.0 version.
6. Downgrade the SmartServer 2.2 firmware to the i.LON 100 e3 version.
7. Migrate an i.LON 100 e3 Server network configuration to the SmartServer.
8. Restore the SmartServer to its factory default settings.
9. Replace the SmartServer.
10. Activate the V40 interface on the SmartServer (in Standalone mode only).

Note: You can manually upgrade, backup/restore, and deploy SmartServers via FTP instead of using the i.LON AdminServer. For more information on manually managing and deploying SmartServers, see Appendix D, *Manually Managing and Deploying SmartServers*.

To upgrade i.LON e3 plus Servers or SmartServers that have previously been downgraded to the i.LON 100 e3 version firmware to the SmartServer 2.2 (Release 4.06) firmware, you must first

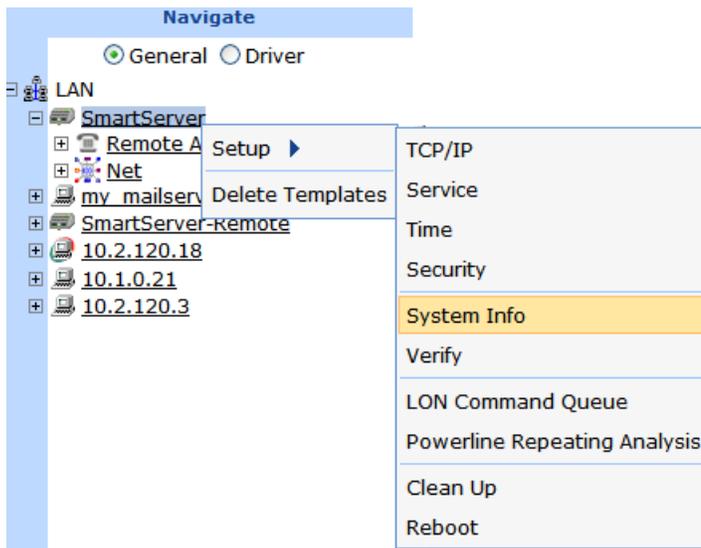
manually upgrade them to the SmartServer 1.0 (Release 4.02) firmware via FTP and then use the i.LON AdminServer to upgrade them to the SmartServer 2.2 firmware. For more information on how to do this, see *Upgrading an i.LON e3 plus Internet Server to the SmartServer* later in this section.

Viewing System Information and Performance

You can use the **Setup – System Info** Web page to view the SmartServer’s system information, including its hardware and firmware versions; Ethernet addresses; general performance statistics; performance as an IP-852 router (if IP-852 routing is activated on your SmartServer); and FPM license status.

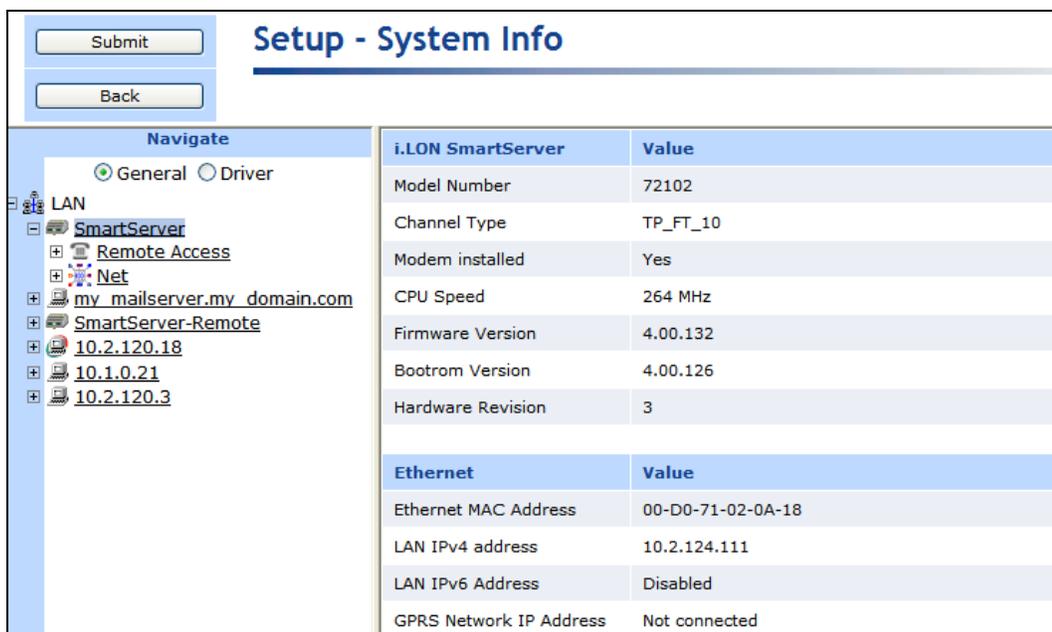
To view the SmartServer’s system information, follow these steps:

1. Right-click the **SmartServer** icon, point to **Setup**, and then click **System Info** on the shortcut menu.



Alternatively, you can click **Setup** and then click **System Info**.

2. The **Setup – System Info** Web page opens.



3. The following system information related to your SmartServer's hardware and firmware and its Ethernet connections are displayed in the dialog:

SmartServer This section displays information about the SmartServer hardware and firmware. This information may be requested by Echelon support when diagnosing a problem with the SmartServer.

Model Number The SmartServer's model number.

Channel Type The channel type of the SmartServer. For free topology models of the SmartServer, this is TP_FT_10. For power line models, this is PL_20N (or PL-20C if CENELEC is enabled).

Modem Installed Indicates whether the SmartServer has an internal modem.

CPU Speed The CPU speed (in MHz) of the SmartServer.

Firmware Version The firmware version of the SmartServer.

Bootrom Version The bootrom version of the SmartServer.

Hardware Revision The hardware version of the SmartServer, which is one of following values:

- 1 - Release 1 hardware
- 2 - e3 hardware
- 3 - SmartServer hardware

Ethernet This section lists the Ethernet addresses currently used by the SmartServer.

MAC Address The unique 12-digit hexadecimal Ethernet MAC address assigned to the SmartServer. A MAC address consists of a Block ID and a Device ID. The Block ID (the first set of six digits) identifies the manufacturer. The Device ID (the second set of six digits) identifies the model and manufacturer date.

LAN IPv4 Address The IPv4 address currently assigned to the SmartServer.

LAN IPv6 Address The IPv6 address currently assigned to the SmartServer. This field will be empty if IPv6 is not enabled on your SmartServer.

GPRS Network IP Address The IP address used by the SmartServer for GPRS network connections. If a GPRS connection has not been set up on your SmartServer, "Not Connected" appears in this field.

4. You can scroll down to view the following properties related to the SmartServer's general performance:

Setup - System Info				
Navigate		General Statistics	Current Value	Recommended Limit
<input type="button" value="Submit"/> <input type="button" value="Back"/>				
<input checked="" type="radio"/> General <input type="radio"/> Driver		Flash Disk Activity: Moving Average	0 Erases / Minute	78 Erases / Minute maximum
LAN		Flash Disk Activity: Last 3 Minutes	20 Erases / Minute	Not Applicable
<input checked="" type="checkbox"/> SmartServer		Flash Disk Activity: Last 1 Hour	6 Erases / Minute	Not Applicable
<input type="checkbox"/> Remote Access		Flash Disk Activity: Since Startup (5 Days)	6 Erases / Minute	Not Applicable
<input type="checkbox"/> Net		Spare Flash Blocks	93 available / 94 total	8 Blocks Available minimum
<input type="checkbox"/> my_mailserver.my_domain.com		Free Disk Space / Total Disk Space	18356 kB / 63866 kB	1024KB Free Space Minimum
<input type="checkbox"/> 10.2.124.108		Free Memory (RAM)	22798 kB	Not Applicable
		CPU Utilization	15.00 %	Not Applicable
		Data Point Message Failures: Last 2 minutes	0 per Minute / 0 total	1 Failure / minute Maximum
		Data Point Message Failures: Last 10 Minutes	0 per Minute / 0 total	1 Failure / minute Maximum
		Data Point Message Failures: Last 1 day	0 per Minute / 0 total	1 Failure / minute Maximum
		Last Refresh	2013-02-13 12:04:39	Not Applicable
		Battery Level	Ok	Not Applicable

General Statistics

This section lists the current usage and recommended limits (where applicable) for the SmartServer's flash memory usage, CPU utilization, data point message failures, and time of last refresh.

For more information on how the SmartServer uses flash memory, see the next section, *Using the SmartServer Flash Memory*.

Flash Disk Activity: Moving Average

The long term moving average of the number of flash block erases/minute (using a two day sliding window). When this value exceeds the recommended limit (78 erases/minute), the value will be shown in red and a warning message will be displayed at the top of the Web page.

Flash Disk Activity: Last 3 Minutes

The number of flash disk erases/minute over the last 3 minutes.

Flash Disk Activity: Last 1 hour

The number of flash disk erases/minute over the last 1 hour.

Flash Disk Activity: Since Startup

The number of flash disk erases/minute since the SmartServer was last rebooted.

Spare Flash Blocks

The number of available spare flash blocks remaining. Initially, the SmartServer hardware contains up to 94 spare flash blocks that are used to accommodate block failures. However, it is normal for a small number of flash blocks to initially be marked as failed by the flash manufacturer, and additional blocks may fail after extended use, so the number of available spare blocks on your SmartServer may vary. This does not adversely affect the normal operation of the flash disk, as long as some spare blocks are available.

When the number of spare flash blocks falls below the recommended limit (18 blocks), this value will be shown in red and a warning message will be displayed at the top of the Web page. If a flash block on the SmartServer fails and there are no spare blocks remaining, the flash disk may become unreliable. The SmartServer should be replaced before this happens.

Free Disk Space/Total Disk Space

The current available disk space, and the total possible disk space in the SmartServer (in KB). The SmartServer hardware has a 64MB flash disk, and initially has approximately 28 MB of free disk space. If you go below the recommended limit of 1,024KB of free disk space, this value will appear in red and a warning message will appear at the top of the Web page.

- Free Memory (RAM)** The current available RAM (in KB) on the SmartServer. The SmartServer FT initially has approximately 35 MB of free RAM. The SmartServer PL has approximately 27MB of free RAM.
- CPU Utilization** The percentage of time the SmartServer’s processor is working. This property is a primary indicator of processor activity. If your SmartServer seems to be running slowly, this property may display a higher percentage.
- Data Point Message Failures: Last 2 Minutes** The rate and number of data point message failures over the last 2 minutes.
Data point message failures occur when the SmartServer’s data server passes data point updates to an application. This problem can be caused by high-network traffic, misconfigured applications, or overactive remote applications attempting read or write to the SmartServer’s data points.
- Data Point Message Failures: Last 10 Minutes** The rate and number of data point message failures over the last 10 minutes.
- Data Point Message Failures: Last 1 Day** The rate and number of data point message failures over the last day.
- Last Refresh** The last time the SmartServer Web interface was refreshed.
- Battery Level** Indicates the status of the SmartServer’s real-time clock battery (OK or LOW). The LOW value means that the SmartServer’s internal battery can no longer reliably maintain system time during a power outage.

The battery has a service life of 10 years. The SmartServer firmware checks the battery voltage level on startup and reports any battery failures within 10 minutes of the failure. When a failure is detected an error is written in the event log and in the System Logger.

You can monitor the current voltage level of the battery using the **Net/VirtCh/iLON System/VirtFb/BatteryLevel** data point, which has a **SNVT_lev_percent** format. The default value is **100.0** percent; if the battery fails, the value is set to **0.0** percent.

5. You can further scroll down to view the properties related to the SmartServer’s performance as an IP-852 router (if IP-852 routing is activated on the SmartServer) and the SmartServer’s FPM license status.

The screenshot shows the 'Setup - System Info' page. On the left is a 'Navigate' sidebar with a tree view containing 'General', 'Driver', 'LAN', 'SmartServer', 'Remote Access', 'Net', 'my_mailserver.my_domain.com', 'SmartServer-Remote', '10.2.120.18', '10.1.0.21', and '10.2.120.3'. The main content area is a table with two sections: 'LonTalk Statistics' and 'FPM Information'.

LonTalk Statistics	Current Value	Packets / Sec
LonTalk-Side Packets sent	454	0.04
LonTalk-Side Packets received	10917	0.97
LonTalk-Side Packets lost	0	0.00
IP-Side Packets sent	0	0.00
IP-Side Packets received	0	0.00
IP-Side Packets stale	0	0.00
IP Configuration Packets sent	0	0.00
IP Configuration Packets Recieved	0	0.00
Seconds since Last Clear	11235	Not Applicable
Time last Cleared	2007-12-06 14:36:08	Not Applicable
Last Refresh	2007-12-06 17:43:23	Not Applicable

FPM Information	Current Value
FPM Licensed	Activated

LonTalk Statistics

If you are using the SmartServer as an IP-852 router, the following properties display the total number and rate (per second) of packets sent and received on the LON and LON IP sides of the IP-852 channel since the SmartServer began operating as an IP-852 router.

If “Not Licensed” appears in all the fields, an IP-852 routing license is not installed on your SmartServer. You can click any of the **Not Licensed** links in this section to activate IP-852 routing on your SmartServer. Alternatively, you can order an IP-852 routing license (Echelon model number 72160) from the Echelon Web site at www.echelon.com/products/cis/activate.

<i>LonTalk-Side Packets Sent</i>	Packets transmitted from the SmartServer’s internal LON channel to its IP-852 router.
<i>LonTalk-Side Packets Received</i>	Packets received on the SmartServer’s internal LON channel from its IP-852 router.
<i>LonTalk-Side Packets Lost</i>	Packets received from the IP-852 router that were lost on the SmartServer’s internal LON channel.
<i>IP-Side Packets Sent</i>	Packets the SmartServer has transmitted from its IP-852 router to the IP-852 channel.
<i>IP-Side Packets Received</i>	Packets the SmartServer’s IP-852 router has received from the IP-852 channel.
<i>IP Packets Data Stale</i>	Expired packets received by the SmartServer’s IP-852 router from the IP-852 channel.
<i>IP Configuration Packets Sent</i>	Packets sent by the SmartServer’s IP-852 router to the IP-852 Configuration Server on the IP-852 channel.
<i>IP Configuration Packets Received</i>	Packets received by the SmartServer’s IP-852 router from the IP-852 Configuration Server on the IP-852 channel.
<i>Seconds Since Last Clear</i>	Total number of seconds that have elapsed since the SmartServer was last rebooted.
<i>Seconds Since Last Clear</i>	Displays when the SmartServer was last rebooted.
<i>Last Refresh</i>	Displays when you last refreshed your browser.

Custom App (FPM) Information

This section indicates whether you can deploy and run custom apps—also called Freely Programmable Modules (FPMs)—on your SmartServer. A custom app is a custom embedded application or driver that customizes the functionality of your SmartServer.

You can create custom apps with the Echelon i.LON Programming Tools. A trial version of the SmartServer 2.0 Programming Tools is available on the SmartServer 2.2 DVD. To build custom apps and upload them to your SmartServer, you need to order the SmartServer 2.0 Programming Tools DVD (Echelon model number 72111-409). To order this DVD, contact your Echelon sales representative.

For more information on writing and deploying custom apps, see the *SmartServer 2.0 Programming Tools User’s Guide*.

FPM Licensed

Indicates whether custom app programmability is licensed on your SmartServer. If “Activated” appears in this field, custom app programmability is licensed on your SmartServer. If “Not Licensed” appears in this field, a programming license is not installed on your SmartServer. A programming license must be installed on your SmartServer in order to deploy and use custom apps on it.

You can click the **Not Licensed** link to activate custom app programmability on your SmartServer. Alternatively, you can order an programming license (Echelon model number 72161) from the Echelon Web site at www.echelon.com/products/cis/activate.

Using the SmartServer Flash Memory

The SmartServer uses flash memory to store data associated with its applications. This non-volatile memory appears to the SmartServer applications as a logical disk drive (also called a *flash disk*). The flash disk is extremely reliable and will last a long period of time, but it has some limitations that may affect the lifetime and runtime configuration of the SmartServer.

The SmartServer flash memory is physically composed of 4,096 blocks of 16 KB each (these are not the same as disk blocks/sectors, which are much smaller). Of the 4,096 blocks, 4,000 are mapped to the logical disk driver, 2 are required for overhead, and the remaining ones (up to 94) are spares.

Once a flash block has been written to, it must be completely erased before it can be written to again. As the SmartServer applications write data to the logical flash disk, physical flash blocks are erased as needed to allow data to be stored. Each flash block can be erased a limited number of times before it fails, and flash manufacturers specify a minimum expected value for this limit. When a flash block fails, it is permanently marked as failed and no longer used by the SmartServer. The spare flash blocks allow for a limited number of block failures to occur without affecting the reliability of the flash disk.

The amount of time it takes for the flash blocks on the SmartServer to reach their erase limit depends on how much and how often data is written to the flash disk. Writes to the logical flash disk cause erases of physical flash blocks, but there is no simple formula to precisely describe this relationship. The flash erase rates reported by the SmartServer apply to the entire flash memory, not to individual flash blocks. The SmartServer contains a sophisticated flash file system that distributes flash erases across all available blocks, in order to optimize the flash life. Over time, the actual number of erases of each block will remain approximately equal, thus maximizing the life span of all flash blocks. According to the flash manufacturers' rated limits, all flash blocks should last at least 10 years if the total block erase rate averages no more than 39 erases per minute for that entire time. Exceeding this limit may cause the flash disk to wear out sooner.

The block erase limit specified by the flash manufacturers is very conservative. Empirical testing of at least some flash parts indicates that a typical limit under normal conditions may be at least 10 times longer, which translates to a much longer life for the SmartServer flash disk, and/or erase rates much greater than 39 erases per minute. Informally, flash manufacturers will confirm these findings, but they cannot be guaranteed. You can trade off expected life span for increased erase rates.

The configuration of your SmartServer may have a significant impact on the number of flash erases per minute. You can monitor both the rate at which you are erasing the flash blocks on your SmartServer and how many spare disk blocks are available. You can do so using the information on this Web page. If the number of spare block falls below 8 blocks, you should replace the SmartServer.

Short-term increases or decreases in the rate of flash block erases value are not meaningful to the life span of the flash memory. Only long-term, sustained rates are truly significant. However, if you are trying to adjust your data logging to determine the affect this has on the erase rate, a long-term number is not very helpful. To accommodate these different needs, this Web page reports four different values for the flash block erase rate.

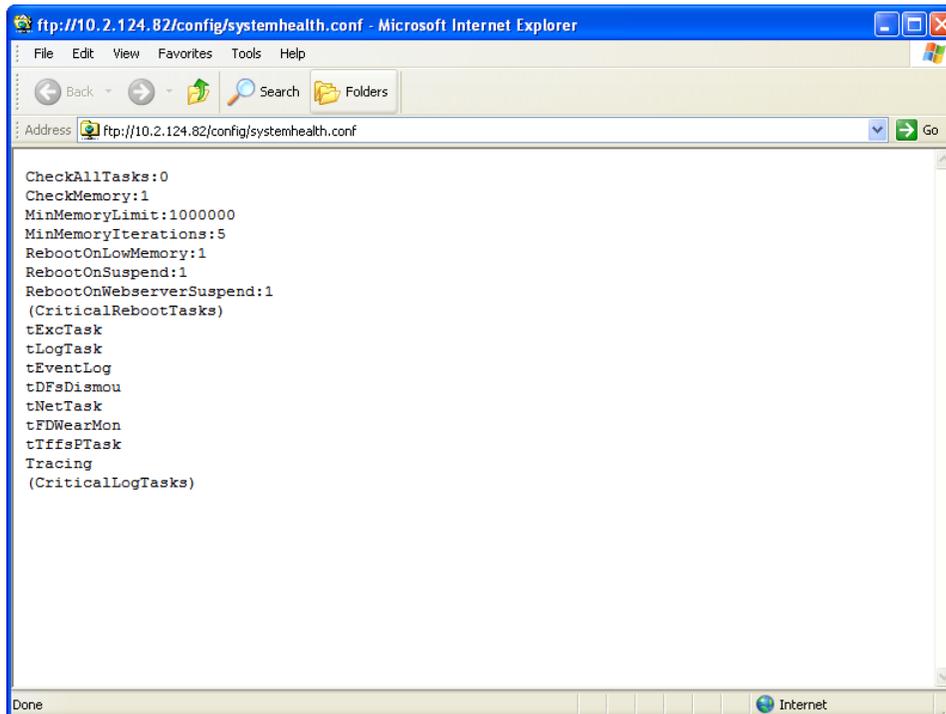
The most important one is computed using a two-day moving average, which will reflect only sustained erase rates. However, this average is slow to respond to changes in the rate, and it may take

up to five days before the value fully reflects a sustained change in the erase rate. The three minute and one hour values provide more immediate feedback by using shorter time windows, but they may show jumps in their values due to short-term activity (for example, transferring a file via FTP to the SmartServer). The final value is the rate since the last reboot, which may respond to rate changes even slower than the two-day average, but provides a very long-term view.

Viewing System Health Monitoring

You can view and configure the **systemhealth.conf** configuration file in the /config folder on the SmartServer flash disk. This file lists the inputs that determine how the SmartServer's system health is monitored. It lists the tasks to be monitored by the SmartServer, the memory limits to be checked, and the actions to be performed by the SmartServer. To view and configure the **systemhealth.conf** file, follow these steps:

1. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the local SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click Security. The **Setup – Security** Web page opens.
 - b. In the **General** property, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - c. In the **Service** property, verify that the **Enable FTP** check box is selected.
2. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example).
3. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
4. Browse to the /config folder on the SmartServer flash disk.
5. To view the **systemhealth.conf** configuration file, double-click it. The **systemhealth.conf** configuration file opens in a new browser.



The screenshot shows a Microsoft Internet Explorer browser window with the title bar "ftp://10.2.124.82/config/systemhealth.conf - Microsoft Internet Explorer". The address bar contains "ftp://10.2.124.82/config/systemhealth.conf". The main content area displays the following configuration text:

```
CheckAllTasks:0
CheckMemory:1
MinMemoryLimit:1000000
MinMemoryIterations:5
RebootOnLowMemory:1
RebootOnSuspend:1
RebootOnWebserverSuspend:1
(CriticalRebootTasks)
tExcTask
tLogTask
tEventLog
tDFsDismou
tNetTask
tFDWearMon
tIffsPTask
Tracing
(CriticalLogTasks)
```

The status bar at the bottom of the browser window shows "Done" and "Internet".

6. You can view the following inputs related to the monitoring of the SmartServer’s system health:
- | | |
|----------------------------------|---|
| <i>CheckAllTasks</i> | Defines whether the general task check is performed. A value of 1 will cause the system health monitoring to perform the general task check. If RebootOnSuspend is set to 1, the system is rebooted on failure. The default value is 0 . |
| <i>CheckMemory</i> | Defines whether the memory check is performed. A value of 1 causes the memory check to be performed. The default value is 1 . |
| <i>MinMemoryLimit</i> | Defines the size of the largest available free block to be checked. The default value is 1000000 . |
| <i>MinMemoryIterations</i> | Defines the number of consecutive iterations for which the memory has to be below MinMemoryLimit for the memory check test to fail. The default value is 5 . |
| <i>RebootOnLowMemory</i> | Determines the action taken when the memory check fails. If this property is set to 1 , the system will be rebooted. The default value is 1 . |
| <i>RebootOnSuspend</i> | Determines the action taken when the general task check fails. If this property is set to 1 , the system will be rebooted. The default value is 1 . |
| <i>RebootOnWebServer Suspend</i> | Determines the action to be taken when a Web task is suspended or non-existent. If this property is set to 1 , the system will be rebooted. The default value is 1 . |
| <i>CriticalRebootTasks</i> | Lists critical tasks. If any of these tasks are suspended or non-existent, the system is rebooted. |
| <i>CriticalLogTasks</i> | List of critical tasks. If any of these tasks are suspended or non-existent, an entry is made to the system log and a trace is produced on the console. |
7. To configure the **systemhealth.conf** configuration file, you can copy it to your computer and open it with a text editor such as Notepad. The parameters in the configuration file can be listed in any order; however, they must precede the list of critical tasks. You must keep the “CriticalRebootTasks” and “CriticalLogTasks” tags in the file.
8. When you are done configuring the **systemhealth.conf** configuration file, save it, and then upload it via FTP to /config folder on the SmartServer flash disk, overwriting the existing **systemhealth.conf** file.

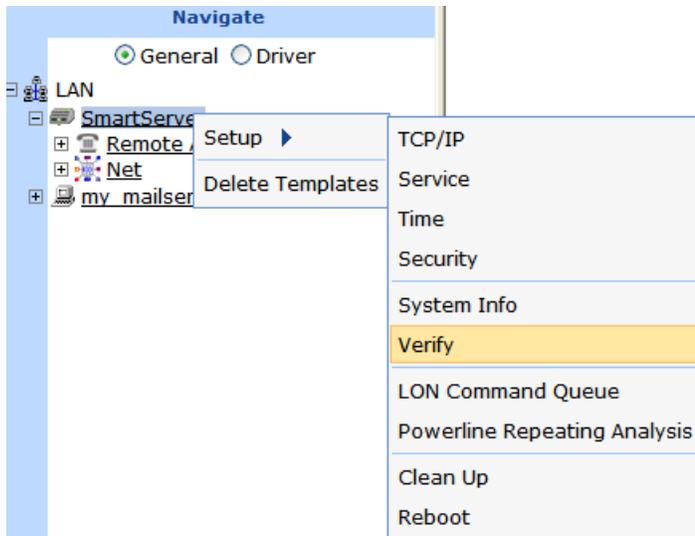
Testing Connections

You can use the **Setup – Verify** Web page to test that the Ethernet and dial-up connections between a SmartServer and the other host devices on the LAN are functioning properly. You can test a SmartServer’s connections to remote SmartServers, OpenLNS Servers, e-mail (SMTP) servers, time (SNTP) servers, and Web Connection Target servers. You can also test a turnaround connection to the selected SmartServer, and test IP-852 configuration and persistent GPRS connections.

When initiating a remote test from this Web page, the SmartServer will dial out to each dial-up connection that contains one or more host devices. If the SmartServer needs to break communication with your computer during that communication, do not refresh your internet browser during the process. Testing of dial-up connections while dialed in to the SmartServer will fail, because the Web page will not be able to maintain communication with the SmartServer after the modem disconnects and dials to another location.

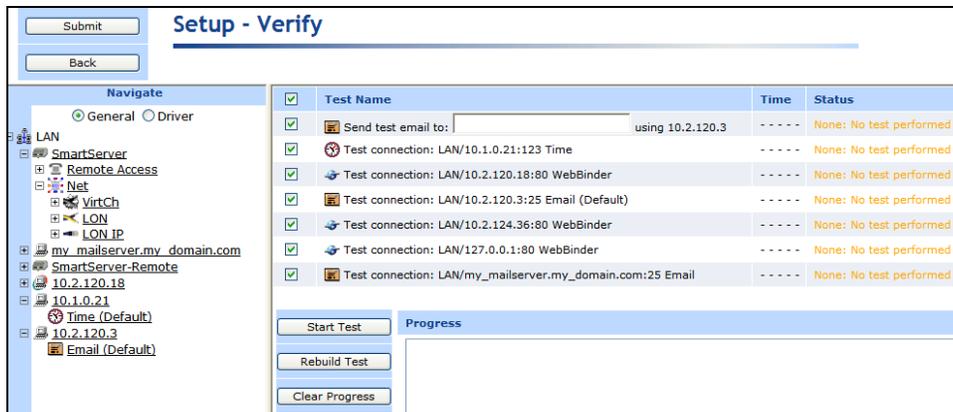
To test a SmartServer’s connections, follow these steps:

1. Right-click the **SmartServer** icon, point to **Setup**, and then click **Verify** on the shortcut menu.

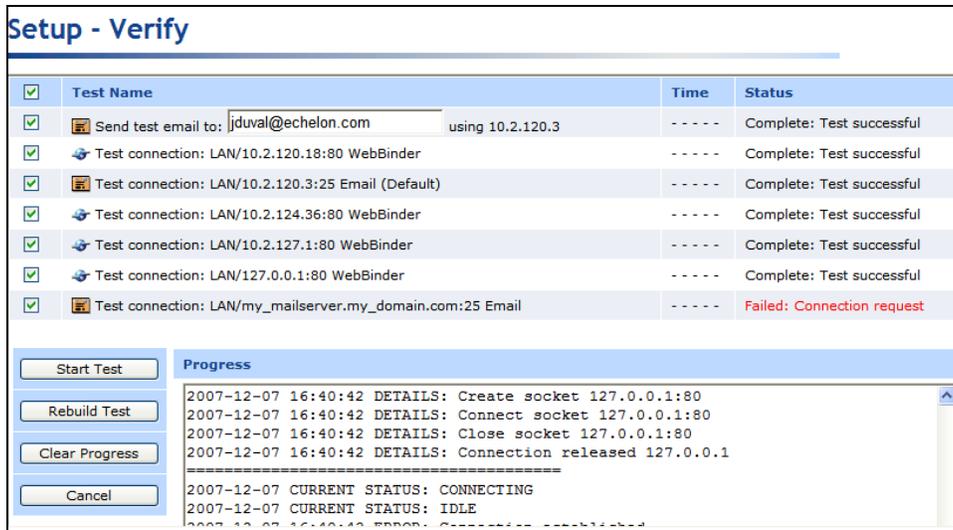


Alternatively, you can click **Setup** and then click **Verify**.

2. The **Setup - Verify** Web page opens. This Web page lists the connections that have been configured for the selected SmartServer including IP-852 routing and persistent GPRS settings.



3. Select the connections to be tested. The tests for all connections are selected by default.
4. Click **Start Test** to begin testing the selected connections.
5. The **Progress** box lists the verification events in the order they occur. The result of the connection test is listed in the **Status** column. Any problems establishing communications with any of the selected servers will be reported. To stop all ongoing tests anytime, click **Cancel**. To re-start the previous set of tests, click **Rebuild Test** and then click **Start Test**. To clear the data in the progress box, click **Clear Progress**.



Upgrading an i.LON e3 plus Internet Server to the SmartServer

You can upgrade an i.LON 100 e3 plus Server to the SmartServer 2.2 firmware so that you can implement the new features provided by SmartServer 2.2. This upgrade entails manually upgrading the firmware on your i.LON 100 e3 plus Server to the SmartServer 1.0 software, which preserves the configurations of the built-in applications and NVEs on your i.LON 100 e3 plus Server, and then using the i.LON AdminServer to automatically upgrade to the SmartServer 2.2 firmware.

To perform the upgrade, follow these steps:

1. Install the SmartServer 2.2 software from the SmartServer 2.2 DVD as described in *Installing Echelon SmartServer 2.2 Software* in Chapter 2. This installs the latest SmartServer 1.0 and SmartServer 2.2 images to the **LonWorks\iLon100\images** folder on your computer.
2. Install EES 2.2 from the SmartServer 2.2 DVD. Also install OpenLNS Server if you plan on using the SmartServer 2.2 in an OpenLNS managed network. See *Installing Echelon SmartServer 2.2 Enterprise Services* and *Installing Echelon OpenLNS Server* in Chapter 2 for how to perform these installations.
3. Backup the i.LON 100 e3 plus Server via FTP. To do this follow these steps:
 - a. Verify that you have the correct user name and password to access your i.LON 100 e3 Server via FTP and that FTP access is enabled on your i.LON e3 Server. To do this, follow these steps:
 - i. Click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - ii. Under **Property**, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - iii. Under **Service**, verify that the **Enable FTP** check box is selected.
 - b. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your i.LON 100 e3 Server (ftp://192.168.1.222, for example).
 - c. Enter the FTP/Telnet user name and password for accessing your i.LON 100 e3 Server via FTP.
 - d. Copy all the folders in the root directory of the i.LON 100 e3 Server flash disk except for the alarmLog and data folders to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions. If you copy Data Logger and Alarm Notifier log files to the SmartServer flash disk, the SmartServer will replace them with empty files.

4. Update the bootrom following these steps:
 - a. Connect a serial cable between your computer and the i.LON 100 e3 plus Server console port.
 - b. Start a terminal emulator such as *PuTTY*. Set the serial interface settings to 9600 bps, 8 bits, no parity, 1 stop bit, and no flow control. See Appendix B, *Using the SmartServer Console Application*, for more information on the console interface.
 - c. Open the SmartServer 2.2 (Release 4.06) bootrom images folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer 2.2 Software**, select **i.LON Image Folder**, and then open the **BootROM 4.03** folder. Alternatively, you can browse to the file path of the SmartServer 2.2 bootrom image folder, which is **LonWorks\iLon100\images\BootROM 4.03** by default.
 - d. Upload via FTP the updated **bootrom.upd** file to the root directory of your i.LON 100 e3 plus Server.
 - e. Reboot the i.LON 100 e3 plus Server by entering the `reboot` command in the console application. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The i.LON 100 e3 plus Server will reboot to the bootrom state, halting all applications.
 - f. Enter the `update bootrom` command in the console application. If the bootrom file name is different than the default (**bootrom.upd**), specify the actual file name as an additional parameter.

Note: Do not interrupt the bootrom update process. Doing so will render the i.LON 100 e3 plus Server unable to boot. If this happens, you will need to ship your SmartServer back to Echelon to be repaired.
 - g. After the bootrom update has been completed, reboot your i.LON 100 e3 plus Server by entering the `reboot` command in the console application.
5. Format the SmartServer flash disk using the bootrom console following these steps:
 - a. Enter the `reboot` command in the SmartServer console application.
 - b. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - c. Enter the `format` command in the bootrom application. Your i.LON 100 e3 plus Server is automatically rebooted.

See Appendix B, *Using the SmartServer Console Application*, for more information on using the bootrom and console applications.
6. If the devices on your network have user-defined network variable types (UNVTs) or user-defined configuration property types (UCPTs), copy the devices’ custom resource file sets (**.ENU**, **.fmt**, **.fpt**, **.ls**, and **.typ** files) from the `lonworks/types` folder in the e3 backup to a `lonworks/types/User/<YourCompany>` folder on the i.LON 100 e3 plus Server flash disk.
7. Open the SmartServer images folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer 2.2 Software**, and select **i.LON Image Folder**. Alternatively, you can browse to the file path of the SmartServer 1.0 image folder, which is **LonWorks\iLon100\images\iLon100 4.02** by default.
8. Copy all the folders and files in the **LonWorks\iLon100\images\iLon100 4.02** folder on your computer to the root directory of the i.LON 100 e3 plus Server flash disk.
9. Copy the **ItConfig**, **Config**, and **Web/user/<Custom>** folders from the e3 plus backup to the root directory of the i.LON 100 e3 plus Server flash disk. The **ItConfig** folder contains the LONWORKS connections and other LONWORKS data in your network; the **Config** folder contains

the network configuration files; and the **Web/user/<Custom>** folder contains your custom Web pages.

Note: Do not copy any of the factory e3 Web pages in the **/web/user/echelon** folder; otherwise, you will replace all the SmartServer 2.2 configuration Web pages with the e3 pages, which will no longer be functional. Do not copy any other folder under the **/web** directory.

10. Reboot your i.LON 100 e3 plus Server by entering the `reboot` command in the console application. This automatically converts your e3 network configuration to the SmartServer format.
11. If you are using the SmartServer in an OpenLNS managed network, logically replace the i.LON 100 e3 Server with the SmartServer in the OpenLNS application. If you are using OpenLNS CT, right-click the i.LON100 device shape, point to **Commissioning**, and then click **Replace** on the shortcut menu. Follow the device replacement procedures described in Chapter 7 of the *OpenLNS Commissioning Tool User's Guide*.

When selecting the device interface definition to be loaded, select the **ILON100_FTT_V12.XIF**, **ILON100_PLC_V12.XIF**, **ILON100_FTT_V40.XIF**, or **ILON100_PLC_V40.XIF** based on your SmartServer model.

12. If you are using the SmartServer in an OpenLNS managed network, synchronize the SmartServer to the OpenLNS network database after your SmartServer has finished rebooting. See *Configuring a LonWorks Network* in Chapter 5 for more information on how to do this.
13. Use the i.LON AdminServer to automatically upgrade your SmartServer's firmware to the SmartServer 2.2 (Release 4.06) format. For more information on how to do this, see Chapter 2 of the *Echelon Enterprise Services 2.2 User's Guide*.
14. You can use i.LON Vision 2.2 to automatically upgrade all your existing e3 custom Web pages previously built with i.LON Vision 1.0 and Contribute 3.0/3.1/CS3/CS4 to the SmartServer 2.2 format. See *Upgrading e3 Web Pages to SmartServer 2.2 Pages* in Chapter 3 of the *i.LON Vision 2.2 User's Guide* for more information on how to do this.
15. Open the SmartServer 2.2 Web pages and test that your system is functioning properly. Verify that your external devices and their network variables appear in the navigation pane in the left side of the SmartServer Web interface and that their names match those in the OpenLNS network database. Verify that the SmartServer's built-in applications are configured correctly.

Note: If you have integrated any custom SOAP/XML applications with your i.LON e3 plus server, you must re-build them using the version 4.0 namespace. This is because the i.LON e3 plus server and the SmartServer use different SOAP/XML interfaces. See the *SmartServer Programmer's Reference* for more information on creating custom SOAP/XML applications for your SmartServer.

Downgrading the SmartServer 2.2 Firmware to the 1.0 Version

You can downgrade the firmware on your SmartServer 2.2 to the SmartServer 1.0 (Release 4.02) version via FTP. To downgrade the firmware on your SmartServer, follow these steps:

1. Backup the SmartServer via FTP. To do this follow these steps:
 - a. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - i. Click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - ii. Under **Property**, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - iii. Under **Service**, verify that the **Enable FTP** check box is selected.
 - b. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (`ftp://192.168.1.222`, for example).

- c. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
 - d. Copy all the folders in the root directory of the SmartServer flash disk except for the alarmLog and data folders to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions. If you copy Data Logger and Alarm Notifier log files to the SmartServer flash disk, the SmartServer will replace them with empty files.
2. Format the SmartServer flash disk using the bootrom console following these steps:
 - a. Enter the `reboot` command in the SmartServer console application.
 - b. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - c. Enter the `format` command in the bootrom application. The SmartServer will automatically reboot.

See Appendix B, *Using the SmartServer Console Application*, for more information on using the bootrom and console applications.

3. Update the bootrom on the SmartServer following these steps:
 - a. Connect a serial cable between your computer and the i.LON 100 e3 plus Server console port.
 - b. Start a terminal emulator such as *PuTTY*. Set the serial interface settings to 9600 bps, 8 bits, no parity, 1 stop bit, and no flow control. See Appendix B, *Using the SmartServer Console Application*, for more information on the console interface.
 - c. Open the SmartServer 1.0 (Release 4.02) bootrom images folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer 2.2 Software**, select **i.LON Image Folder**, and then open the **BootROM 4.02** folder. Alternatively, you can browse to the file path of the SmartServer 2.2 bootrom image folder, which is **LonWorks\iLon100\images\BootROM 4.02** by default.
 - d. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (`ftp://192.168.1.222`, for example).
 - e. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
 - f. Copy the **bootrom.upd** file in the LonWorks\iLon100\images\BootROM 4.02 folder on your computer to the root directory of the SmartServer flash disk.
 - g. Enter the `update bootrom` command in the SmartServer console application. If the bootrom file name is different than the default (**bootrom.upd**), specify the actual file name as an additional parameter.

Note: Do not interrupt the bootrom update process. Doing so will render the SmartServer unable to boot. If this happens, you will need to ship your SmartServer back to Echelon to be repaired.
 - h. After the bootrom update has been completed, enter the `reboot` command in the SmartServer console application.
4. If the devices on you network have user-defined network variable types (UNVTs) or user-defined configuration property types (UCPTs), copy the devices’ custom resource file sets (**.ENU**, **.fmt**, **.fpt**, **.ls**, and **.typ** files) from the lonworks/types folder in the SmartServer 2.2 backup to a **lonworks/types/User/<YourCompany>** folder on the SmartServer flash disk.
5. Open the SmartServer images folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer 2.2 Software**, and the select **i.LON Image Folder**. Alternatively, you can browse to the file path of the SmartServer 1.0 image folder, which is **LonWorks\iLon100\images\iLon100 4.02** by default.

6. Copy all the folders and files in the **LonWorks\iLon100\images\iLon100 4.02** folder on your computer to the root directory of the SmartServer flash disk.
7. Reboot your SmartServer by entering the `reboot` command in the console application.

Downgrading the SmartServer Firmware to i.LON 100 e3 Version

You can downgrade the firmware on your SmartServer to the i.LON 100 e3 version via FTP. To downgrade the firmware on your SmartServer, follow these steps:

1. If the SmartServer 2.2 software is installed on your computer, uninstall it.
2. Install the i.LON 100 e3 software from the i.LON 100 e3 CD.
3. If you have not already installed i.LON 100 e3 SP3 or i.LON 100 e3 SR3 on your computer, download and install i.LON 100 e3 SP3 from www.echelon.com/downloads.
4. Format the SmartServer flash disk using the bootrom console following these steps:
 - a. Enter the `reboot` command in the SmartServer console application.
 - b. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - c. Enter the `format` command in the bootrom application. The SmartServer will automatically reboot.

See Appendix B, *Using the SmartServer Console Application*, for more information on using the bootrom and console applications.

5. Update the bootrom on the SmartServer following these steps:
 - a. In the browser of an FTP client such as Core FTP, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (`ftp://192.168.1.222`, for example).
 - b. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
 - c. Copy the **bootrom.upd** file in the **LonWorks\iLon100\images\BootROM 3.03** folder on your computer to the root directory of the SmartServer flash disk.
 - d. Enter the `update bootrom` command in the SmartServer console application. If the bootrom file name is different than the default (**bootrom.upd**), specify the actual file name as an additional parameter.

Note: Do not interrupt the bootrom update process. Doing so will render the SmartServer unable to boot. If this happens, you will need to ship your SmartServer back to Echelon to be repaired.
 - e. After the bootrom update has been completed, enter the `reboot` command in the SmartServer console application.
6. When the reboot is complete, format the SmartServer flash disk again as described in step 4. After the reboot is done, the SmartServer will be running the e3 bootrom.
7. Copy either the e3 SR3/SP3 firmware in the **LonWorks\iLon100\images\iLon100 3.03** folder on your computer or an existing e3 firmware backup to the root directory of the SmartServer flash disk.
8. Reboot the SmartServer using the `reboot` command in the SmartServer console application. When the reboot is complete, the SmartServer will be running the e3 firmware.

Migrating an e3 Network Configuration to the SmartServer

You can move a network configuration from an i.LON 100 e3 Server to the SmartServer. Integrating the SmartServer with an existing network configuration lets you implement the new network

management, monitoring, and control features provided by the SmartServer, and it enables you take advantage of the SmartServer's increased memory and improved performance.

1. Install the SmartServer 2.2 software from the SmartServer 2.2 DVD as described in *Installing Echelon SmartServer 2.2 Software* in Chapter 2. This installs the latest SmartServer 1.0 and SmartServer 2.2 images to the **LonWorks\iLon100\images** folder on your computer.
2. Install Echelon Enterprise Services 2.2 and OpenLNS Server from the SmartServer 2.2 DVD. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for more information.
3. Backup the i.LON 100 e3 Server via FTP. To do this follow these steps:
 - a. Verify that you have the correct user name and password to access your i.LON 100 e3 Server via FTP and that FTP access is enabled on your i.LON e3 Server. To do this, follow these steps:
 - i. Click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - ii. Under **Property**, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - iii. Under **Service**, verify that the **Enable FTP** check box is selected.
 - b. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your i.LON 100 e3 Server (ftp://192.168.1.222, for example).
 - c. Enter the FTP/Telnet user name and password for accessing your i.LON 100 e3 Server via FTP.
 - d. Copy all the folders in the root directory of the i.LON 100 e3 Server flash disk except for the **alarmLog** and **data** folders to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions. If you copy Data Logger and Alarm Notifier log files to the SmartServer flash disk, the SmartServer will replace them with empty files.
4. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the local SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - b. In the **General** property, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - c. In the **Service** property, verify that the **Enable FTP** check box is selected.
5. Format the SmartServer flash disk and then downgrade the firmware to the latest SmartServer 1.0 firmware image (Release 4.02) to preserve the configurations of the NVEs and built-in applications (for example, Scheduler and Data Logger) on your i.LON 100 e3 Server. The SmartServer 1.0 firmware image is installed on your computer when you installed the SmartServer 2.2 software as described in step 1.

To format your SmartServer and then downgrade to the SmartServer 1.0 firmware image, follow these steps:

- a. Connect a serial cable between your computer and the i.LON 100 e3 plus Server console port.
- b. Start a terminal emulator such as *PuTTY*. Set the serial interface settings to 9600 bps, 8 bits, no parity, 1 stop bit, and no flow control. See Appendix B, *Using the SmartServer Console Application*, for more information on the console interface.
- c. Enter the `reboot` command in the SmartServer console application.

- d. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - e. Enter the `format` command in the bootrom application. Your SmartServer is automatically rebooted.
 - f. Open the SmartServer **images** folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer Software**, and then select **SmartServer Images Folder**. Alternatively, you can browse to the file path of the SmartServer 1.0 image folder, which is **LonWorks\iLon100\images\iLon100 4.02** by default.
 - g. Copy the following folders and files in the **LonWorks\iLon100\images\iLon100 4.02** folder on your computer to the root directory of the SmartServer flash disk: **lonWorks**, **modules**, **web**, and **iLonSystem**.
6. Copy the **ItConfig** and **Config** folders from the e3 backup to the root directory of the SmartServer flash disk. The **ItConfig** folder contains the LONWORKS connections and other LONWORKS data in your network. The **Config** folder contains the network configuration files.
 7. Copy the XIF files of the external devices on the network from the **lonworks/import** folder on your computer to the **lonworks/import/User/<YourCompany>** folder on the SmartServer flash disk. Note that you may need to create the **User/<YourCompany>** folder on the SmartServer flash disk before copying the device XIF files.
 8. If the devices on your network have user-defined network variable types (UNVTs) or user-defined configuration property types (UCPTs), copy the devices’ custom resource file sets (**.ENU**, **.fmt**, **.fpt**, and **.typ** files) from the **lonworks/types** folder in the e3 backup to a **lonworks/types/User/<YourCompany>** folder on the SmartServer flash disk.
 9. Reboot your SmartServer using the SmartServer Web pages or the SmartServer console application.
 - To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.
 - To reboot your SmartServer using the SmartServer console application, enter the `reboot` command. For more information on using the SmartServer console application, see *Appendix B*.
 10. If your SmartServer has a different IP address than the i.LON 100 e3 server and you intend on using the SmartServer as an RNI to connect an OpenLNS or OpenLDV-based application to the LONWORKS network attached to it, configure your SmartServer as an RNI using the LONWORKS Interfaces Control Panel application. For more information on how to do this, see *Configuring the SmartServer as a Remote Network Interface* earlier in this chapter.
 11. Open the network being migrated to the SmartServer using OpenLNS CT or other OpenLNS application. If you are using the SmartServer as an RNI and your SmartServer is using a different IP address than the i.LON 100 e3 server, change the network interface to the new SmartServer RNI created in step 10.
 12. Logically replace the i.LON 100 e3 Server with the SmartServer in the OpenLNS application. If you are using OpenLNS CT, right-click the i.LON100 device shape, point to **Commissioning**, and then click **Replace** on the shortcut menu. Follow the device replacement procedures described in Chapter 7 of the *OpenLNS Commissioning Tool User’s Guide*.
 13. Synchronize the SmartServer to the OpenLNS network database. See *Configuring a LonWorks Network* in Chapter 5 for more information on how to do this.
 14. Use the i.LON AdminServer to automatically upgrade your SmartServer’s firmware to the SmartServer 2.2 (Release 4.06) format. For more information on how to do this, see Chapter 2 of the *Echelon Enterprise Services 2.2 User’s Guide*.

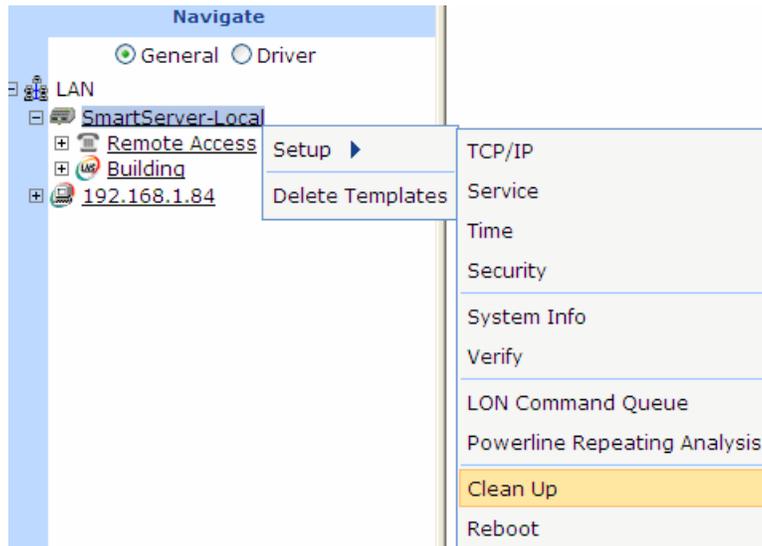
15. At the end of the upgrade process, the i.LON AdminServer will display the following error message: “Failed I/O error: Connection refused: connect; nested exception is java.net.ConnectException”. As a result, you cannot open the SmartServer 2.2 Web pages until you reboot the SmartServer with the console application.
16. Reboot your SmartServer by entering the `reboot` command in the console application. For more information on the SmartServer console application, see Appendix B, *Using the SmartServer Console Application*.
17. When the reboot has been completed, you can open the SmartServer 2.2 Web pages.

Restoring a SmartServer to Factory Default Settings

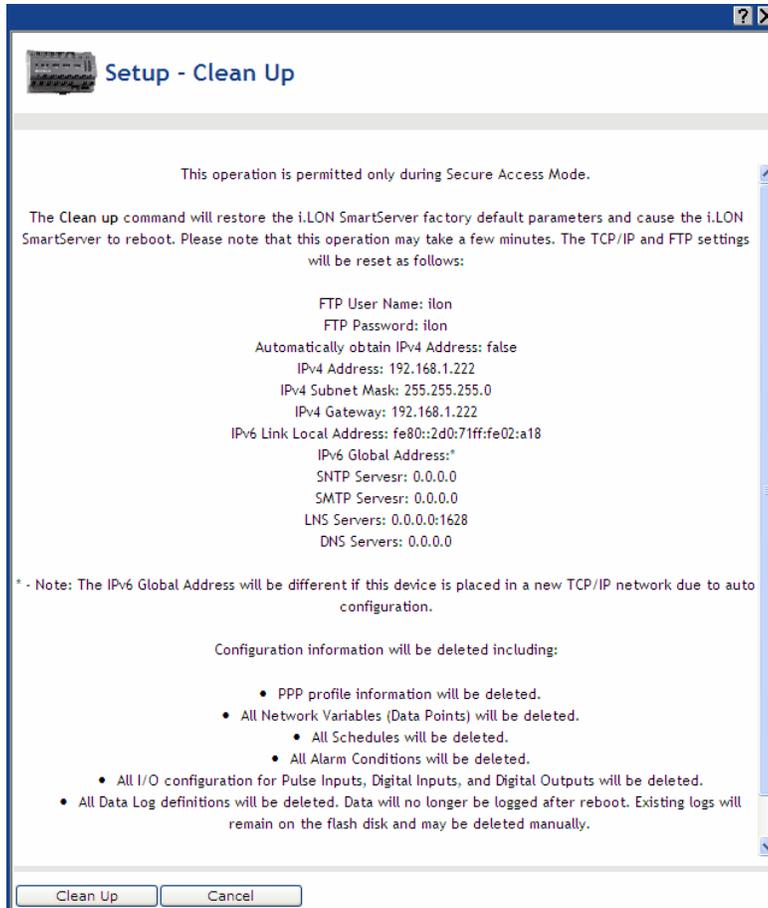
You can restore your SmartServer to its factory default settings with the SmartServer Web pages or the console application. To perform a factory default reset, secure access mode must be enabled on your SmartServer (see *Enabling and Disabling Secure Access Mode* in this chapter for more information on enabling secure access on your SmartServer).

To restore your SmartServer to its factory default settings with the SmartServer Web pages, follow these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **Cleanup** on the shortcut menu.



2. The **Setup – Cleanup** dialog opens.



3. Click **Cleanup** to proceed with the resetting of the SmartServer to its factory default settings.

To restore your SmartServer to its factory default settings with the console application, enter the `factorydefaults` command, or enter the `factorydefaults keepipaddr` command to reset the SmartServer but keep its basic IPv4 and IPv6 IP addresses.

Performing a factory default reset, resets your SmartServer to the following configuration:

FTP/Telnet User Name	ilon
FTP/Telnet Password	ilon
Automatically Obtain IP address	False
IPv4 Address	192.168.1.222
IPv4 Subnet Mask	255.255.255.0
IPv4 Gateway	192.168.1.222
IPv6 Link Local Address	fe80::2d0:71ff:fe02:a18
IPv6 Global Address	different if SmartServer is placed on a new TCP/IP network
Web Server Port	80
Hostname	SmartServer
Domain Suffix	[blank]
DNS Servers	0.0.0.0
Time (SNTP) Servers	0.0.0.0
Time Zone	(GMT-08:00) Pacific Time (US & Canada); Tijuana
Network Management Service	LNS Auto (No Host)

OpenLNS Servers	0.0.0.0:1628
Incoming RNI Port	1628
LonTalk Address	Unconfigured
E-mail (SMTP) Servers	0.0.0.0
Source E-mail Address	[blank]
CENELEC Enabled	False (PL models only)

In addition, all the XML configuration files on the SmartServer, as well as the contents of the **/PulseBackup** (pulse count data), **/AlarmLog** (alarm log data), and **/data** (data log data) directories, are backed up to the **/config/software.bak** directory.

Also, the device templates currently stored in the **/config/template** directory are moved to a **/config/template.bak** directory. To use these templates again, copy them from the **/config/template.bak** directory to your computer, and then copy them from your computer back to the **/config/template** folder.

If you did not use the `factorydefaults keepipaddr` command in the console application, you must set the TCP/IP properties of your SmartServer again. To do this, place your computer on the same 192.168.1.* subnet as your SmartServer, or enter the following command in the Command Prompt window (change “192.168.1.0” to the appropriate prefix for your subnet):

```
route add 192.168.1.0 mask 255.255.255.0 %computername%
```

Open the command prompt with administrator privileges. To do this, click **Start**, type **cmd** in the search box, right-click the **cmd.exe**, and then select **Run as Administrator**. If you receive a “The parameter is incorrect” error, replace `%computername%` with the IP address of your computer.

If you entered the `factorydefaults keepipaddr` command in the console application, the IPv4 and IPv6 addresses are not reset to their defaults and you do not need to set the TCP/IP properties of your SmartServer again.

Replacing the SmartServer

You can replace the SmartServer using an OpenLNS application such as OpenLNS CT if there is a hardware failure. To replace the SmartServer, follow these steps:

1. Close any OpenLNS application that is currently accessing the network containing the SmartServer to be replaced.
2. Backup the SmartServer via FTP as described in *Backing Up the SmartServer Firmware* in this chapter.
3. Format the flash disk of the old SmartServer using the bootrom console. To do this, follow these steps:
 - a. Enter the `reboot` command in the SmartServer console application.
 - b. When the console reads “Press the ‘!’ key to stop auto-boot”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - c. Enter the `format` command in the bootrom application.
4. Remove the old SmartServer hardware, and then attach the replacement SmartServer hardware to the physical network.
5. Follow step 3 to format the flash disk of the replacement SmartServer using the bootrom console.
6. After the replacement SmartServer has rebooted, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example) in the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP.

7. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
8. Copy all the folders in the SmartServer backup directory to the root directory of the SmartServer flash disk.
9. Enter the `reboot` command in the SmartServer console application.
10. After the replacement SmartServer has rebooted, enter the `show` command in the SmartServer console application and verify that the replacement SmartServer has the same IP address, subnet mask, and gateway as the old SmartServer.
11. If you are using the SmartServer as an RNI, you need to use the **Setup – Security** Web page to verify that the replacement SmartServer has the same MD5 authentication key as the old SmartServer. If the replacement SmartServer is initially configured to use the default key (all zeros), this will occur automatically when connecting to the RNI.
12. Use an OpenLNS application to re-open the network containing the old SmartServer.
13. Logically replace the old SmartServer in the OpenLNS application. If you are using OpenLNS CT, right-click the SmartServer device shape, point to **Commissioning**, and then click **Replace** on the shortcut menu. Follow the device replacement procedures described in Chapter 7 of the *OpenLNS Commissioning Tool User's Guide*.
14. The new SmartServer will now function in the same manner as the old one.

Activating the SmartServer v40 Interface

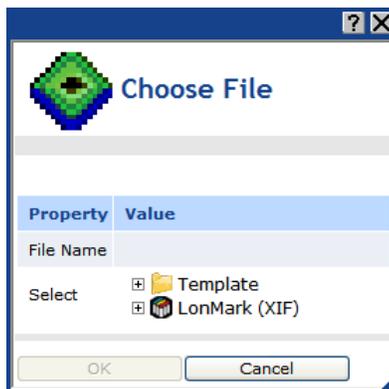
If you are using the SmartServer in standalone mode, you can activate the new v40 interface on your SmartServer. The v40 interface features a dynamic interface with a capacity of 500 dynamic functional blocks. By default, the SmartServer uses the v12 interface, which has a static device interface. This static interface limits the number of applications (functional blocks) that you can create on your SmartServer (10 data loggers, 40 schedulers, 40 alarm generators, 40 alarm notifiers, 40 type translators, 20 analog functional blocks, and 40 Web servers). You can activate the v40 interface if you need to exceed the limits posed by the static interface provided by the v12 interface.

To activate the v40 interface on your SmartServer, follow these steps:

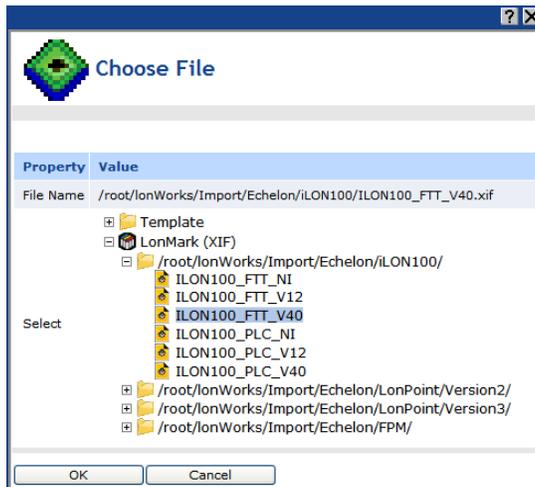
1. Verify that the **Network Management Service** property in the **Setup – LON Network Driver** Web page is set to **Standalone**. To open the **Setup – LON Network Driver** Web page, click **Driver** above the navigation pane in the left frame of the SmartServer Web interface, and then click the **Net** network icon in the SmartServer tree.
2. Expand the network icon in the SmartServer tree, expand the **LON** channel, and then click the **i.LON App (Internal)** device. The **Setup -LON Device Driver** Web page opens.
3. In the **Template** property near the bottom of the Web page, click the box to the right.



4. The **Choose File** dialog open.

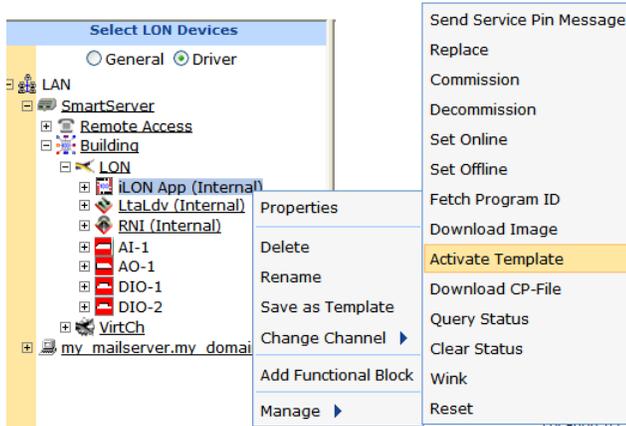


5. In the **Choose File** dialog, expand the **LonMark (XIF)** folder, expand the **//lonWorks/Import/Echelon/iLON100** folder, select the **ILON100_FTT_V40** XIF file or **ILON100_PLC_V40** XIF file, and then click **OK** to return to the **Setup -LON Device Driver** Web page.



6. Click **Submit**.

7. Activate the v40 interface. To do this, right-click the **i.LON App (Internal)** device, point to **Manage**, and then click **Activate Template** on the shortcut menu. The v40 interface is activated on the SmartServer. You can now add dynamic functional blocks to the **i.LON App (Internal)** device.



Alternatively, you can activate the v40 interface by clearing and then selecting **Smart Network Management** to the left of the **Template** property in the **Setup -LON Device Driver** Web page and then clicking **Submit**.

Using the SmartServer Web Interface

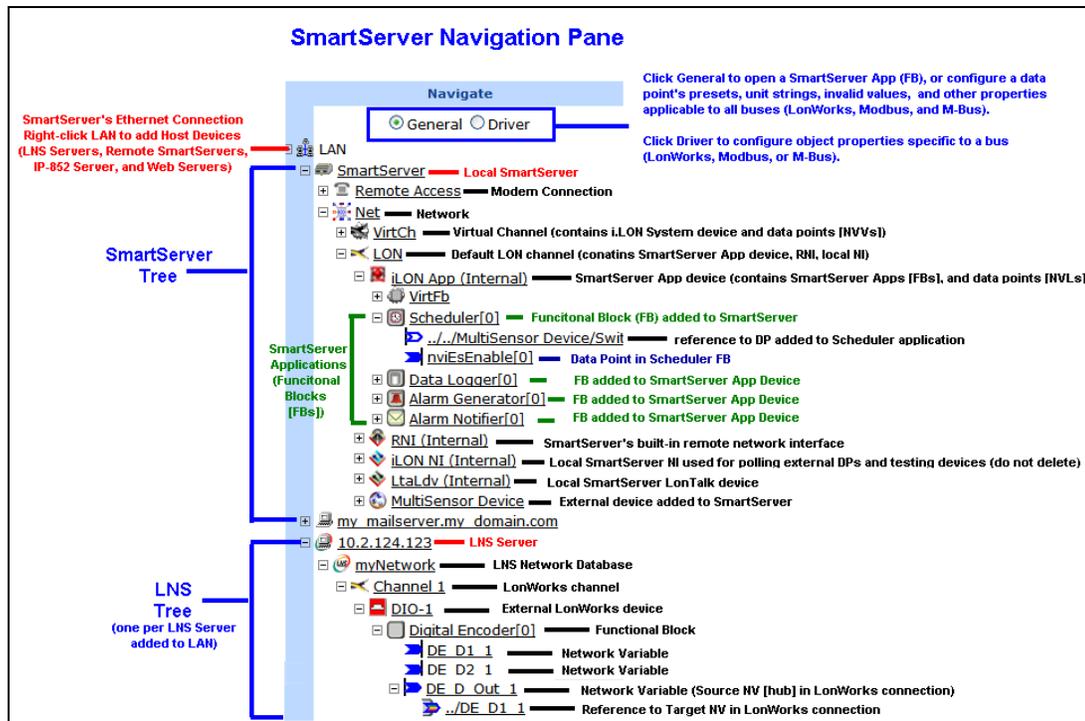
This chapter describes how to use the navigation pane in the Web interface to access settings, change modes, open SmartServer applications, add data points to SmartServer applications, manage icons, manage devices, duplicate functional blocks and data points, and use templates. In addition, it explains how to configure the Web interface and check error messages.

Using the SmartServer Web Interface

The SmartServer Web interface includes a dynamic navigation pane that you use to operate the SmartServer. The tree appears in the left frame of the SmartServer Web pages and represents the LAN on which your local SmartServer resides.

The following graphic serves as a quick reference (cheat sheet) for using the SmartServer navigation pane. It is based on a SmartServer that has initially been set to its factory default settings, and then has had four SmartServer applications (functional blocks), one external device, and an OpenLNS Server added to it. A data point has been added to the Scheduler application. The items displayed in the navigation pane will vary based on many factors, including whether your SmartServer is operating in Standalone or LNS mode, whether IP-852 routing is activated on your SmartServer, the network objects that you have added, deleted, or hidden, and so on. The icons used to represent some network objects will change if you use the SmartServer is LNS mode. For example, the network icon in the SmartServer tree will change to an OpenLNS network database icon when you synchronize the SmartServer to an OpenLNS network database, and the SmartServer App device icon will change to a generic device icon.

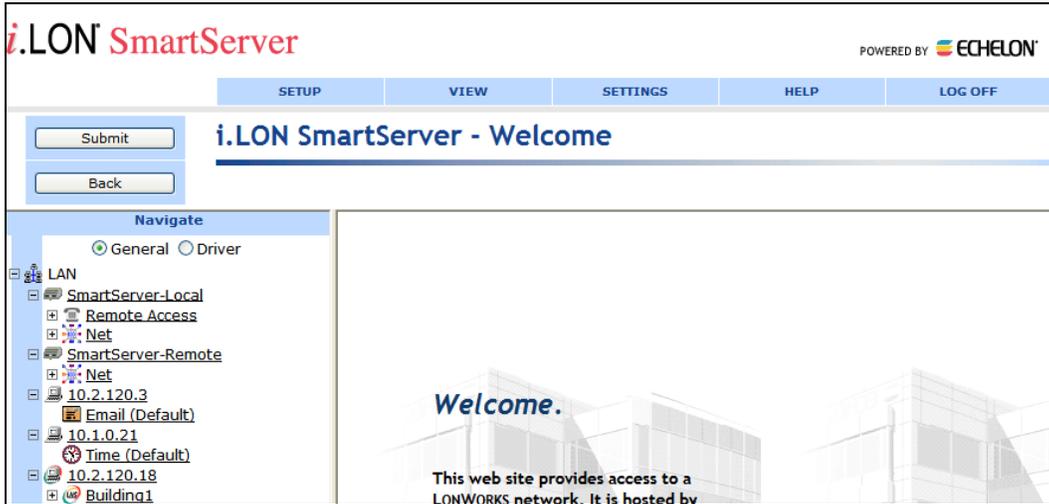
This section describes the items in the navigation pane, and the subsequent sections explain how to use the navigation pane to perform tasks such as using the **General** and **Driver** modes, opening the SmartServer's applications and adding data points to them, the commands you can perform on the network objects in the navigation pane, and setting options for configuring the navigation pane.



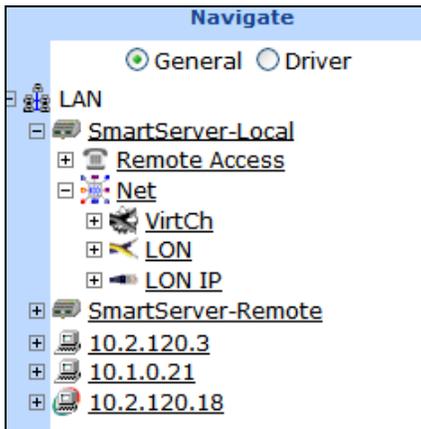
Note: The icon used to represent the SmartServer App device (🔴) was updated in the SmartServer 2.2 release. All other screen shots in this document, and all other documents in the SmartServer 2.2 document suite, display the original icon for the SmartServer App device (🔴).

The host devices accessible from your local SmartServer's Ethernet connection are listed under **LAN**. Host devices include your local SmartServer and may include remote SmartServers, OpenLNS Servers (if you install Echelon Enterprise Services 2.2 from the SmartServer 2.2 DVD), e-mail (SMTP) servers, time (SNTP) servers, IP-852 Configuration Servers, and Web Connection Target servers.

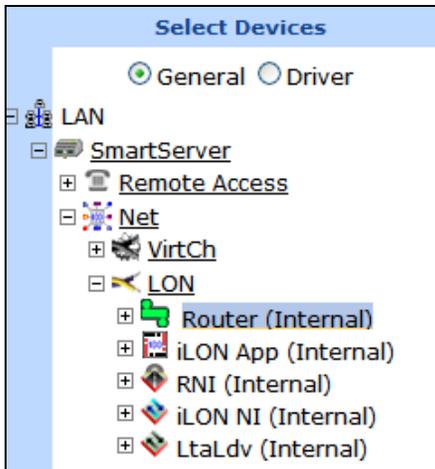
The connections and networks are then listed below their respective host devices. Connections include the remote access (modem) connections under the local SmartServer and the e-mail, time, IP-852 Configuration Server, and Web Connection Target servers under their respective servers.



Networks include their channels, devices, functional blocks, and data points, which are listed in that order following the LONWORKS network hierarchy. You expand an item in a network to show its child objects. For example, when you initially open the SmartServer pages, you can expand the SmartServer network **Net** item to show the **VirtCh** and **LON** channel items (a **LON IP** channel icon will also be shown under the **Net** item if IP-852 routing is activated on your SmartServer).



You can expand the **LON** channel to display the SmartServer's internal devices.

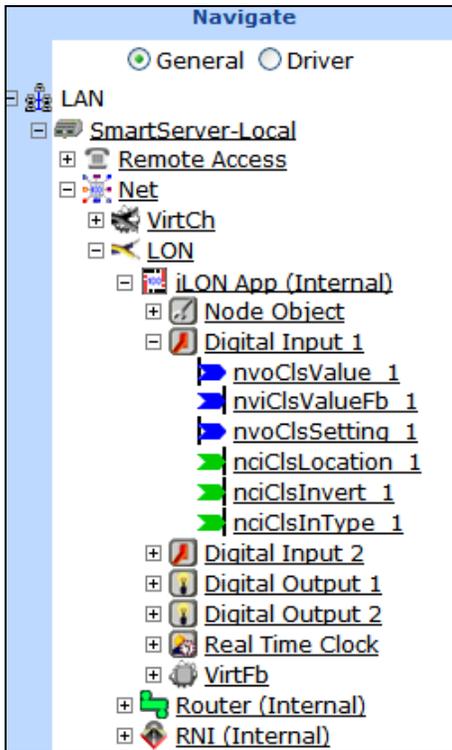


These internal SmartServer devices are described as follows:

Icon	Device Name	Description
 (formerly )	iLON App (Internal)	Contains all of the SmartServer's built-in applications such as the Scheduler, Alarm Generator, Alarm Notifier, and Data Logger. See Chapters 6–11 for more information on using the SmartServer's applications.
	Router (Internal)	The SmartServer's built-in IP-852 router. If IP-852 routing is activated on your SmartServer, you can integrate the network attached to your SmartServer into a single large LONWORKS network that runs over a high-speed IP-852 backbone. See <i>Using the SmartServer as an IP-852 Router</i> in Chapter 3 for more information.
	RNI (Internal)	The SmartServer's built-in remote network interface (RNI). The RNI is used for connecting OpenLNS or OpenLDV-based applications to a LONWORKS network remotely over a TCP/IP network. See <i>Using the SmartServer as an RNI</i> in Chapter 3 for more information.
	iLON NI (Internal)	The SmartServer's local network interface. It is used by the SmartServer polling external data points (NVEs) and for testing and winking external devices.
	LtaLdv (Internal)	The SmartServer's network interface when used as a standalone network manager. In standalone mode, the LtaLdv device sends network management commands to external devices (for example, download application, commission, set online, and so on), and queries devices to verify that they are online. In a power line repeating network, the LtaLdv device also manages the repeating chains.

You can expand the **iLON App (Internal)** device to show its functional blocks, which represent the SmartServer's built-in applications, and then expand a functional block to show the data points (network variables and configuration properties) that are statically defined in the functional block. Network variables are represented with blue data point items.

Input network variables are marked with lines to right of their data point icons and their names have “nvi” prefixes. Output network variables are marked with lines to the left of the data point icons and their names have “nvo” prefixes. Configuration properties are represented with green data point icons that have lines to right of their icons, and their names have “nci” prefixes.

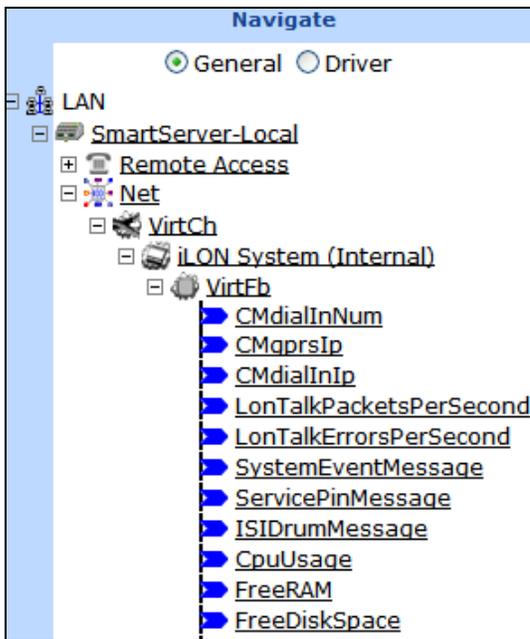


The following table lists and describes the various data point icons that you may observe in the navigation pane:

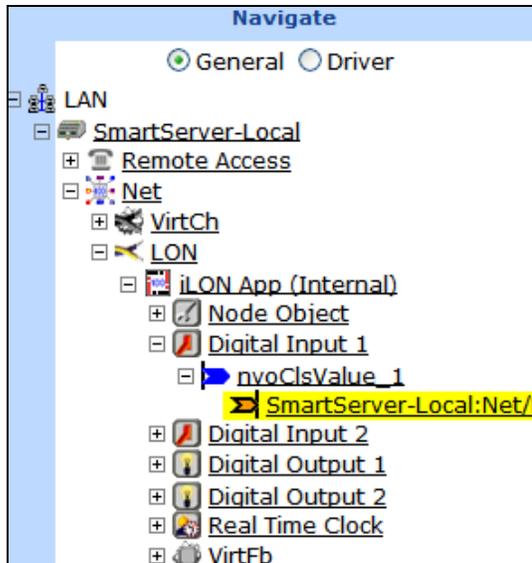
Icon	Name	Description
	Dp_Cfg	Configuration property
	Dp_In	Input data point
	Dp_Out	Output data point
	Dp_In_Out	Data point with undefined direction
	Dp_In_Ref	Reference to input data point added to SmartServer application. Displayed directly below application’s functional block.
	Dp_Out_Ref	Reference to output data point added to SmartServer application. Displayed directly below application’s functional block.
	Dp_In_Out_Ref	Reference to data point added to SmartServer application. Displayed directly below application’s functional block.
	Dp_In_Webbinding	Reference to the target input/output data point in a Web connection. Displayed directly below the source data point in the connection.
	Dp_Out_Webbinding	Reference to the target input/output data point in a Web connection. Displayed directly below the source data point in the connection.
	Dp_In_Webbinding_Attach	Reference to the target input/output data point in a Web connection, and the Web connection

	Dp_Out_Webbinding_Attach	Includes a file attachment. Displayed directly below the source data point in the connection.
	Dp_In_LonConnection	Reference to the target input/output network variable in a LONWORKS connection. Displayed directly below the source network variable (hub) in the connection.
	Dp_Out_LonConnection	
	FbRef	Reference to a SmartServer application to which the data point has been added. Displayed directly below a data point that has been added to a SmartServer application (functional block).

You can expand the **VirtCh** channel icon to display the SmartServer's other internal device, which is the **i.LON System (Internal)** device. This device contains data points that provide valuable system information related to the SmartServer. You can expand the **i.LON System (Internal)** device, and then expand the **VirtFB** virtual functional block to show data points representing the SmartServer's free RAM, free disk space, CPU usage, battery level, software version number, and other system information.



The networks may also have a number of connections. These connections include Web connections and LONWORKS connections, which are represented by target data points that are listed under their respective source data points in the connections.



Above the tree in the left pane, a message box displays the current action to be performed such as “navigate” or “select devices”. Below the message box are buttons that you use to select in which mode to operate the SmartServer (**General** or **Driver**). The color of the bar to the left of the tree indicates the current mode (it is blue in **General** mode, and orange in **Driver** mode). See *Using General and Driver Modes* in this section for more information. Above the left frame, the SmartServer reports error and warning messages. You can configure the organization and appearance of the navigation pane by clicking **Settings**.

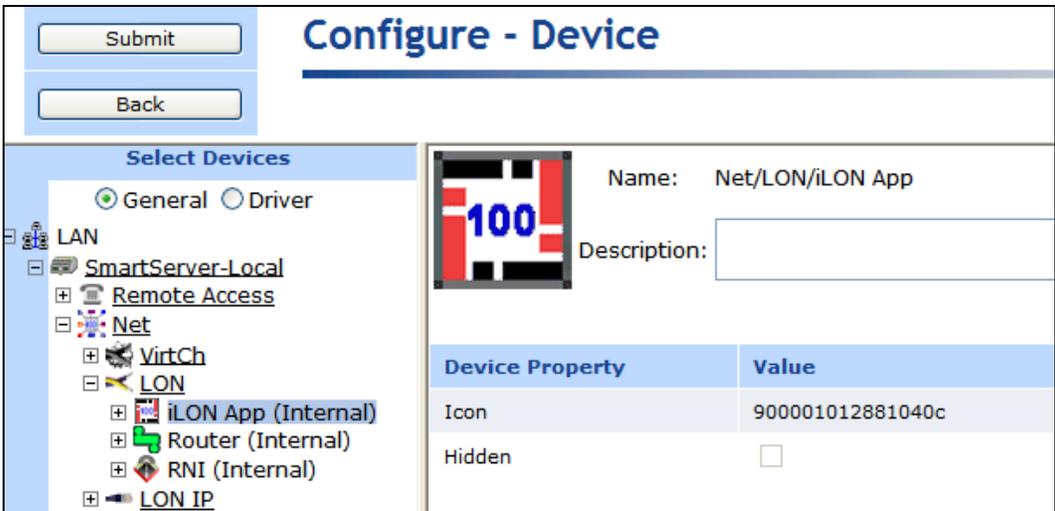
This section helps you learn the new web interface by showing you how to perform the following tasks:

- Use General and Driver modes.
- Open SmartServer applications.
- Add data points to SmartServer applications.
- Manage network objects.
- Issue network management commands on devices.
- Create Web connections.
- Create LONWORKS connections.
- Use device templates.
- Duplicate functional blocks and data points.
- Check error messages and view the system log.
- Configure global settings.
- Use custom device and functional block icons.

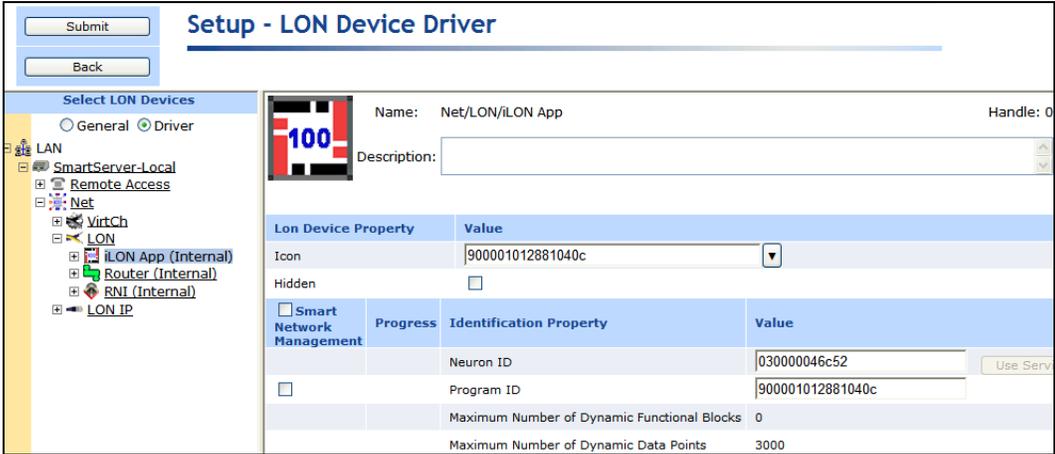
Using General and Driver Modes

You can use the SmartServer in **General** or **Driver** mode to configure the properties of the networks, channels, devices, functional blocks, and data points (network variables and configuration properties) in your systems. The mode you select depends on whether you are modifying the general properties of an object or the properties that pertain to a specific bus—LONWORKS, Modbus, or M-Bus.

Using a LONWORKS device for example, you use **General** mode to open the **Configure – Device** Web page. You can only use this Web page view the name of the device, enter an optional description for the device, view the icon used to represent the device in the tree, and view whether the device is hidden or shown in the tree. This is also true for Modbus and M-Bus devices.



You can click **Driver** to open the **Setup – LON Device Driver** Web page. You can use this Web page to manage the device completely, from acquiring its Neuron ID and changing its configuration and application state to selecting an application image to download to the device and activating a new device interface (XIF) file for the device.



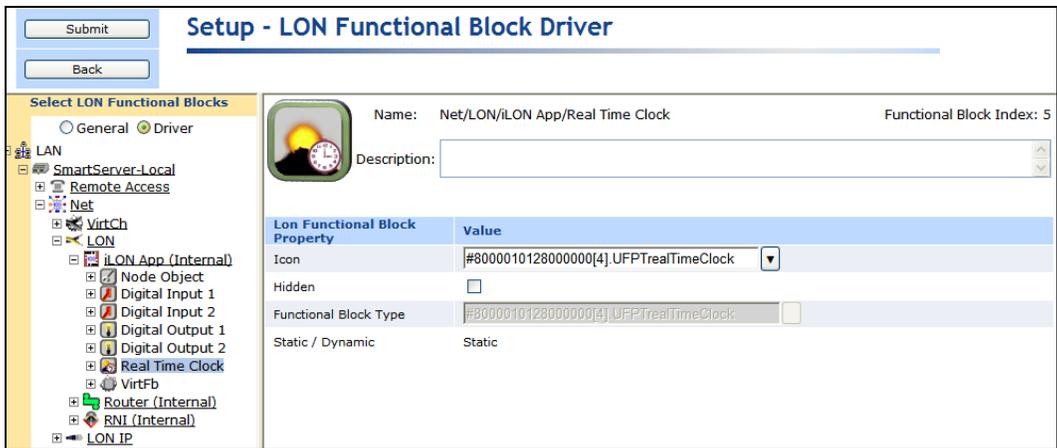
The use of these modes is similar for networks, channels, and functional blocks not representing the SmartServer’s applications as you use **Driver** mode to configure these objects. However, it is slightly different for functional blocks representing the SmartServer applications and data points.

Accessing SmartServer Functional Blocks in General and Driver Modes

In **General** mode, you can click a functional block representing a SmartServer application to open the Web page for that application. For example, you can configure the SmartServer’s real-time clock by clicking **General** and then clicking the **Real-Time Clock** functional block under the **iLON App (Internal)** device. The functional blocks for the SmartServer’s Digital Input, Digital Output, and Real-Time Clock applications are shown in the tree by default. The functional blocks for all other SmartServer applications (Alarm Generator, Alarm Notifier, Data Logger, Pulse Meter, and Scheduler) are initially hidden in the tree. See *Opening SmartServer Applications* in this chapter for more information.

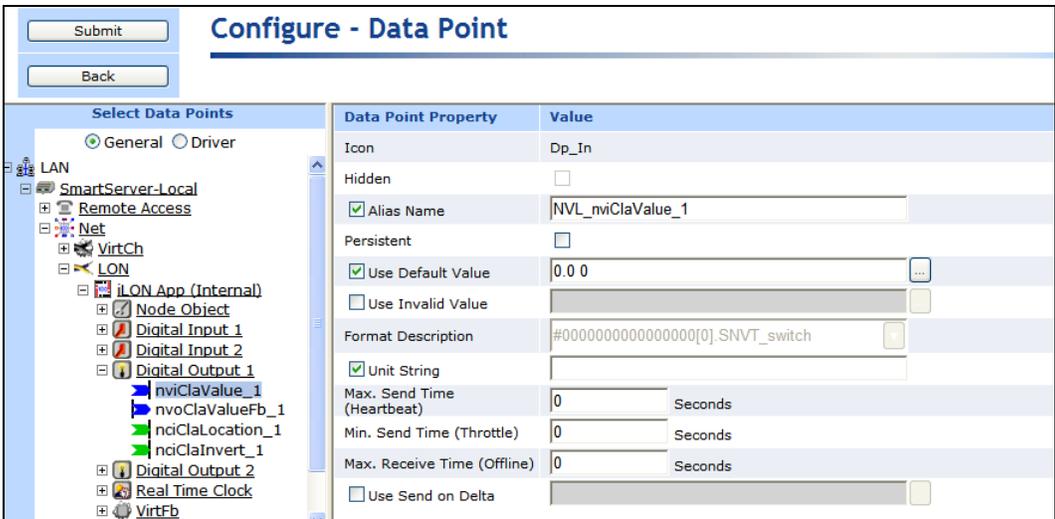


If you click a functional block representing a SmartServer application in **Driver** mode, the **Setup - LON Functional Block Driver** page for that functional block opens. You can only use this Web page to view the name and index of the functional block, enter an optional description for the functional block, modify the icon used to represent the functional block in the tree, select whether the functional block is hidden or shown in the tree, and view whether the functional block is static or dynamic.

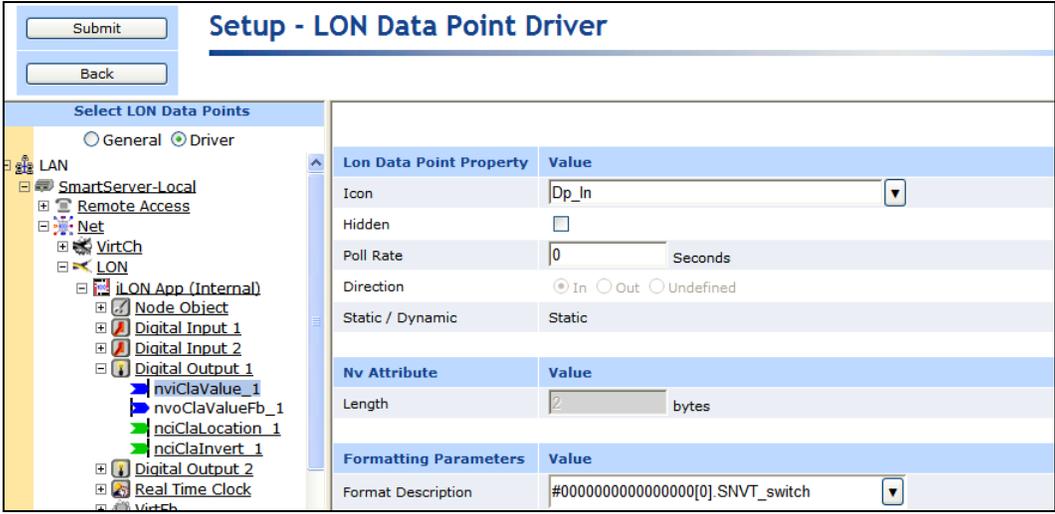


Accessing Data Points in General and Driver Modes

In **General** mode, you can click a LONWORKS, Modbus, or M-Bus data point to open the **Configure - Data Point** Web page. You can use this Web page to view or configure the following data point properties that are applicable to all buses: alias name, whether a constant, format description (view only), default and invalid values, whether its unit string is made available to applications, network performance configuration properties (heartbeat, throttle, offline, and send on delta), presets, and unit strings used for the fields of structured data points.



If you click **Driver**, the **Setup – LON Data Point Driver** Web page will open for that data point. You can use this Web page to view or configure the following properties for that LONWORKS DATA point: poll rate, direction, whether it is static or dynamic, length, and format description (program ID, data type, and format).



Now if you click a Modbus data point with **Driver** mode selected, the **Setup – Modbus Data Point Driver** Web page open for that data point. You can use this Web page to view or configure the following properties for that Modbus data point: poll rate, direction, register type, data access type, whether the data point is read-write or read-only, addressing properties, and data type/formatting properties.

Submit

Setup - MODBUS Data Point Driver

Back

Select MOD-Bus Data Points

General Driver

- LAN
- SmartServer-Local
- Remote Access
- Net
 - LON
 - VirtCh
 - LON IP
 - Modbus
 - ABB_ACH550-UH
 - VirtFb
 - Speed**
 - OutputFreq
 - Current
 - Torque
 - Power
 - DCBusVol
 - OutputVol
 - DriveTemp
 - CvtB-rt

Name: Net/Modbus/ABB_ACH550-UH/VirtFb/Speed

Description: SPEED

MOD-Bus Data Point Property	Value
Icon	Dp_In_Out
Hidden	<input type="checkbox"/>
Poll Rate	10 Seconds
Direction	<input type="radio"/> In <input type="radio"/> Out <input type="radio"/> Undefined
MOD-Bus data register type (Function #)	Hold Register (Functions 3 & 16 multi-write)
Data Point value is	Read/Write
Data Addressing Parameters	
Length	2 bytes

Opening SmartServer Applications

The SmartServer includes the following set of built-in apps that let you monitor and control devices:

- *Alarm Generator and Alarm Notifier.* The SmartServer can trigger alarms based on inputs from the devices it is attached to. In response to an alarm condition, the SmartServer can be configured to update LONWORKS, Modbus, and M-Bus data points; log the conditions to one or more data logs; or send out e-mails or SOAP messages notifying recipients of the alarms and the conditions that triggered them. You can configure alarms to shut off automatically when certain conditions are met or they can be configured to require manual clearance in the SmartServer Web pages. The alarming applications are described in Chapter 6, *Alarming*.
- *Scheduler.* The SmartServer can be used to update any data points based on the time-of-day, day-of-week, and date. These schedules can drive the inputs to any data point including LONWORKS, Modbus, and M-Bus data points. The Event Scheduler includes an astronomical position sensor that you can use to calculate the position of the sun based on the location of the SmartServer and the time-of-day. This is useful for calculating whether it is light or dark outside without using an external light-level sensor, and it is ideal for applications such as street lighting, where lights need to turn on at sundown and turn off at sunrise. This application is described in Chapter 7, *Scheduling*.
- *Data Logger.* The SmartServer can log LONWORKS, Modbus, and M-Bus data points. These logs can be downloaded automatically using the new fast data log transfer feature, or they can be downloaded manually using File Transfer Protocol (FTP), retrieved using a SOAP/XML Web service, or displayed with the **Data Logger: View** Web page. This application is described in Chapter 8, *Data Logging*.
- *Pulse Meter, Digital Input, Digital Output.* The SmartServer contains two built-in pulse metering inputs, two built-in digital inputs, and two built-in digital relay outputs. You can use these inputs and outputs to connect legacy devices to the SmartServer. You can use the Pulse Metering application to have the SmartServer count pulses or to measure the pulse frequency from pulse output devices. You can use the Digital Input and Digital Output applications to monitor and control simple sensors and actuators that can be connected to the SmartServer such as switches, push buttons, alarms, and drive contractors. These applications are described in Chapter 9, *Connecting Legacy Devices to the Local iLON Inputs and Outputs*.
- *Analog Functional Block.* The SmartServer contains an Analog Functional Block application that you can use to perform a variety of arithmetic and logical operations on a set of data points, and then store the result of the operation in an output data point. This application is described in Chapter 10, *Using Analog Functional Blocks*.

- *Type Translator*. The SmartServer can translate data from one data type to another. This is useful for integrating devices with incompatible data types, including devices on different busses (LONWORKS, Modbus, and M-Bus). For example, you can use type translation to translate a **SNVT_temp_f** data point to a **SNVT_temp** data point, convert the **SNVT_scene.function** and **SNVT_scene.scene_number** fields of a scene controller to the **SNVT_switch.value** and **SNVT_switch.state** fields of a switch, and connect an M-Bus data point to a LONWORKS data point. This application is described in Chapter 11, *Using Type Translators*.

You can open the built-in applications on the SmartServer with the SmartServer Web pages, or you can open them with OpenLNS CT if you are using OpenLNS network management services (you cannot use another network management tool such as OpenLNS CT to access a network when the SmartServer is managing the network in standalone mode).

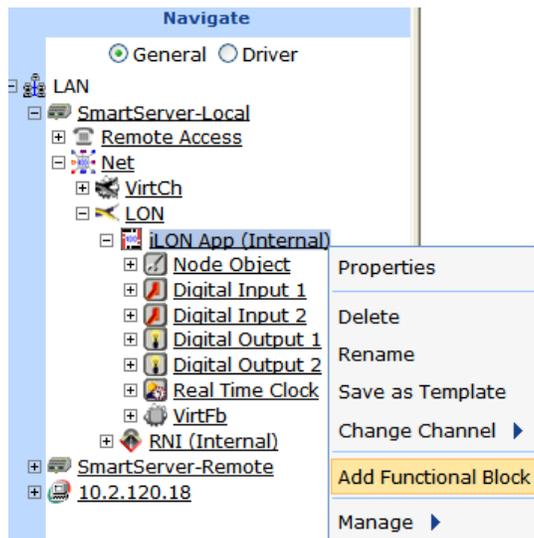
Using the SmartServer Web Interface to Open SmartServer Applications

In the e3 release, the built-in applications on the i.LON 100 server were all accessible from the **Configure** menu, which has since been removed. The built-in applications on the SmartServer are represented by functional block icons that are listed directly under the **i.LON App (Internal)** device in the tree.

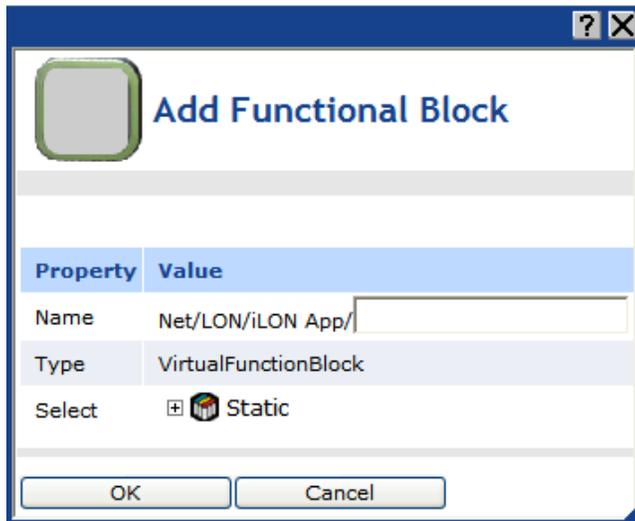
To open an application, click **General** and then click the functional block icon corresponding to the application to be opened. For the Alarm Generator, Alarm Notifier, Analog Functional Block, Data Logger, Pulse Meter, Scheduler, and Type Translator applications, you must first create an instance of their functional blocks. After you create the functional block instance, the functional block appears below the **i.LON App (Internal)** device in the tree, and you can then click the functional block to open the corresponding application.

To create an instance of an application's functional block and open the application using the SmartServer Web pages, you do the following:

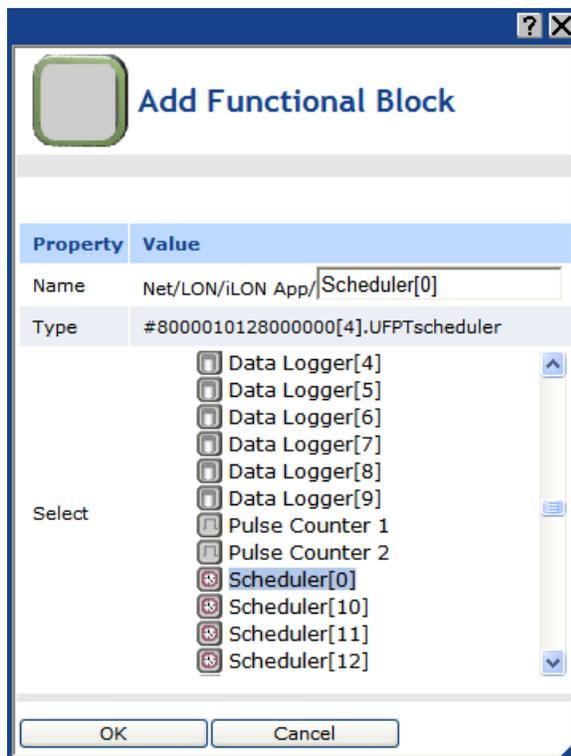
1. Click **General** at the top of the navigation pane in the left frame of the SmartServer Web interface. If **Driver** is selected, the **Setup - LON Functional Block Driver** Web page for the functional block will open when you are done creating the functional block instead of the corresponding SmartServer application.
2. Expand the **Net** network item and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



4. The **Add Functional Block** dialog opens.

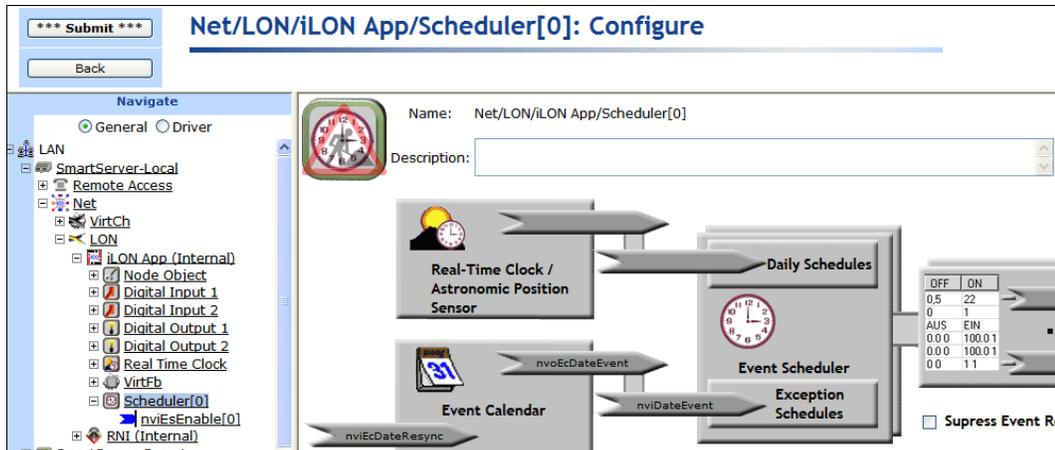


5. Select the functional block representing the application to be opened.
 - If the SmartServer is using the static v12 interface, expand **Static**, select an application, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, expand **Dynamic**, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile (UFPT) of the SmartServer application to be opened, enter a name for the functional block such as “Data Logger”, and then click **OK**. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

- A functional block representing the selected application and all the data points statically defined for the functional block are added under the **iLON App (Internal)** device network object at the bottom, and the application opens in the application frame to the right. The construction symbol overlaid onto the application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



- Click **Submit**.

Note: You can click **View** to open the **Alarm Notifier: Summary**, **Alarm Notifier: History**, **Data Logger: View**, and the **View - Data Points** Web pages.

To open an application from an existing functional block instance, follow these steps:

- Click **General**. If **Driver** is selected when you click a functional block, the **Setup - LON Functional Block Driver** Web page for the functional block opens instead of the corresponding SmartServer application.
- Click the functional block representing the SmartServer application to be opened. The application opens in the application frame to the right.

See the next section for how to add data points to SmartServer applications.

Using OpenLNS CT to Open SmartServer Applications

You can create an instance of a SmartServer application's functional block and open the application using OpenLNS CT. Using this method to open a SmartServer application is comparable to launching an OpenLNS plug-in. You right-click the functional block shape representing the SmartServer application to be configured, and then click **Configure** on the shortcut menu. For more information, see *Opening SmartServer Applications with OpenLNS CT* in Chapter 12, *Using the SmartServer with OpenLNS CT*.

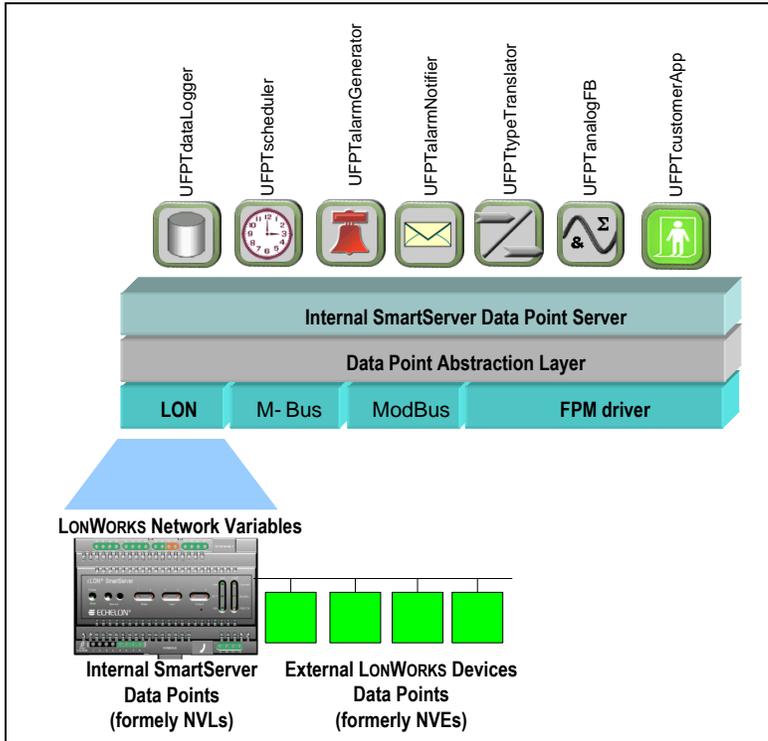
Adding Data Points to SmartServer Applications

The applications on the SmartServer work with the network variables from LONWORKS devices, and also work with data elements from M-Bus and Modbus devices. For example, an Event Scheduler can schedule an M-Bus or Modbus register just as easily as it can schedule a LONWORKS network variable.

This flexibility enables the SmartServer to integrate legacy devices from other field busses. The integration of other field busses with a LONWORKS network is accomplished by the SmartServer's data server. The data server is a software component that *abstracts* any data element of any bus into a *data point*. It enables the SmartServer applications to operate on these abstractions without regard of the device driver.

The following figure illustrates that the SmartServer applications monitor and control the data points abstracted by the internal SmartServer data server. The data server abstracts the network variables on

LONWORKS devices and abstracts the registers of Modbus and M-Bus devices. The LONWORKS network variables that data server abstracts includes those on the SmartServer’s application device [**iLON App (Internal)**] and those on the external LONWORKS devices connected to the SmartServer.



You can directly add data points to the SmartServer’s applications using the SmartServer Web interface. The data points that you can add include the data points of external devices and the data points of the internal SmartServer devices (formerly referred to as NVLs).

External devices are physical application devices that are connected to the SmartServer. External devices are either stored in an OpenLNS database and managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application (the data points of these devices were formerly referred to as “NVEs”), or they are stored on the SmartServer’s internal database (the XML files in the /config/network folder on the SmartServer flash disk) and managed with the SmartServer operating in Standalone mode.

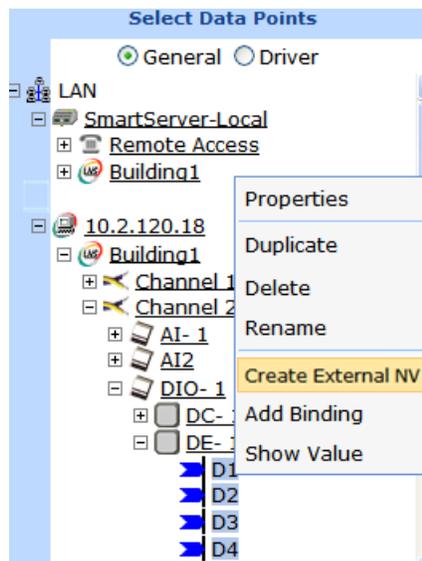
An internal device refers to one of the 16 virtual devices that can be stored on the SmartServer. One of these internal devices is the SmartServer automated systems device [the **iLON App (Internal)** device], which contains the SmartServer’s built-in built-in applications. Ten of the internal devices are reserved for the custom built-in applications (called *custom apps* or *Freely Programmable Modules* [FPMs]) that you can write and deploy on your SmartServer using the full version of SmartServer 2.0 Programming Tools. The other five internal devices on the SmartServer are the **iLON System (Internal)** device, which contains all the virtual data points (formerly referred to as NVVs); the IP-852 router; the local network interface [**iLON NI (Internal)**], which is used to poll external data points (NVEs), and to test and wink external devices; the RNI; and the LonTalk device. You can add the data points in the **iLON App (Internal)** device, the **iLON System (Internal)** device, and the internal FPM application devices to the SmartServer applications.

To add data points to the SmartServer applications, follow these steps:

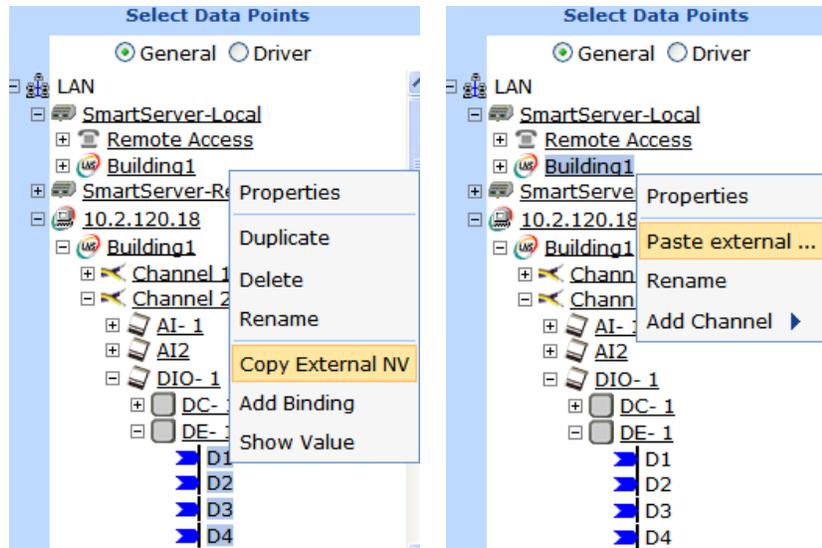
1. If you are operating the network in LNS mode and you are adding the network variables or configuration properties of an external device that is stored in an OpenLNS database and managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application (these data points were formerly referred to as “NVEs”), you must first copy the network variables or configuration properties from the OpenLNS tree to the tree of the target SmartServer (your local SmartServer or

a remote SmartServer you have added to the LAN) via the LNS Proxy Web service. To do this, follow these steps:

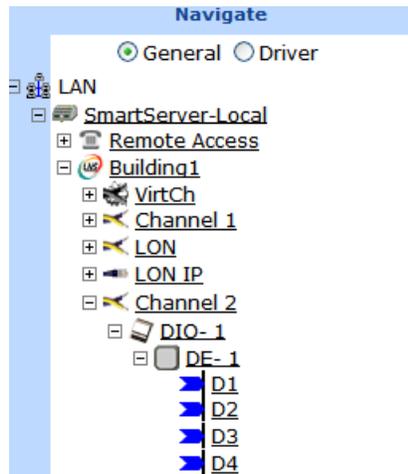
- a. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
- b. Verify that you have added an OpenLNS Server to the LAN that contains the OpenLNS network database in which the network variable or configuration property is stored. In addition, verify that you have synchronized the target SmartServer with the OpenLNS network database containing the external network variables or configuration properties you are copying. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on adding an OpenLNS Server to the LAN and synchronizing the SmartServer to an OpenLNS network database.
- c. Expand the LNS Server item, and then enter the **User Name** and **Password** for logging in to the OpenLNS Server via the Echelon Enterprise Services 2.2. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon (🔴) in the notification area of your computer, and then click **Options** on the shortcut menu.
- d. In the OpenLNS tree, expand the OpenLNS network database, channel, device, and functional block containing the network variable to be copied to the local SmartServer, right-click the network variable, and then select **Create External NV** on the shortcut menu. To copy multiple network variables, click one, and then either hold down CTRL and click all others to be copied or hold down SHIFT and select another to select the entire range, right-click one of the selected network variables, and then click **Create External NV** on the shortcut menu.



Note: If you have one or more remote SmartServers on the LAN, the **Create External NV** option is not available in the shortcut menu of the network variable in the OpenLNS tree. Instead, right-click the network variable in the OpenLNS tree, select **Copy External NV** on the shortcut menu, right-click any object in the network tree of the target SmartServer, and then click **Paste External** on the shortcut menu.



- e. The data points and their parent channel, device, and functional block are added to the network tree of the target SmartServer.



- f. Click **Submit**.
2. Verify that you have created an instance of the functional block that represents the application to which data points are to be added.
 3. Click **General** at the top of the navigation pane in the left frame of the SmartServer Web interface.
 4. From the navigation pane, click the functional block representing the application to which data points are to be added. The application opens in the details pane to the right.
 5. If you are adding the data point to an Alarm Notifier, Data Logger, Scheduler, Analog Functional Block, or Type Translator, open the **Data Points** Web page where you add references to the external data points.
 6. From the SmartServer tree, click the data point to be added to the application. The data point is added to the application, a reference to the data point () is added to the bottom of the application's functional block tree, a reference to the functional block is added directly below the selected data point (), and you can begin monitoring and controlling the data point with the application.

SmartServer Data Point Names and Organization

Data point names are based on the LONWORKS networks hierarchy, using the following naming convention: *network/channel/device/functional block/data point*. The data point name also conveys the location of the data point in the navigation pane on the left side of the SmartServer Web interface.

Note: You can revert the organization of the navigation pane so that data points are listed by source device as they were in the e3 release of the i.LON 100 server. To do this, click **Settings** to open the **Global Settings** dialog. In the **Tree Mode** property, select **Alias Name** and then click **Close**. Data points with alias names defined for them will be listed in the tree. The internal SmartServer data points and virtual data points have pre-defined alias names; therefore, they will automatically appear in the tree. By default, external device data points do not have pre-defined alias names unless you have migrated your LONWORKS network from an i.LON 100 e3 server to the SmartServer. As a result, external device data points do not appear in the navigation pane in Alias Name mode unless you define an alias name for them. You can define an alias name for a data point in its **Configure - Data Point** Web page, which you can access by clicking **General** and then clicking the data point in the navigation pane.

The following sections describe how data points are named and organized in the SmartServer.

Internal SmartServer Data Points (formerly NVLs)

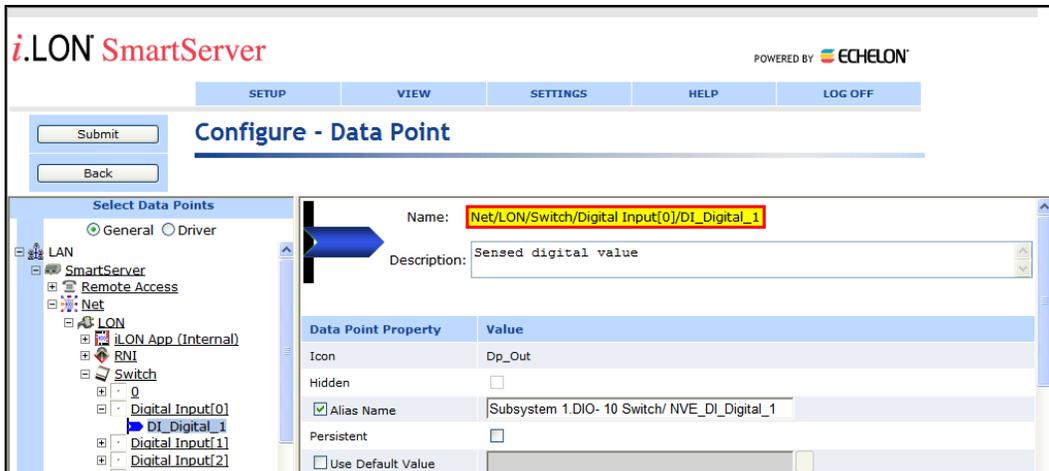
The internal data points on the SmartServer are located under a *<network>/LON/iLON App (Internal)/<functional block>* object and named accordingly. For example, the name of the **nvoClaValueFb_1** data point of the first digital relay output on the SmartServer is “Net/LON/iLON App/Digital Output 1/nvoClaValueFb_1”. This means that you can locate the **nvoClaValueFb_1** data point in the navigation pane by expanding (in the listed order) the network object, the **LON** channel, the **i.LON App (Internal)** device, and then the **Digital Output 1** functional block.

The screenshot shows the SmartServer web interface. At the top, it says "i.LON SmartServer" and "POWERED BY ECHELON". Below that are navigation tabs: "SETUP", "VIEW", "SETTINGS", "HELP", and "LOG OFF". The main heading is "Configure - Data Point". There are "Submit" and "Back" buttons. On the left is a "Select Data Points" tree view showing a hierarchy: LAN > SmartServer > Remote Access > Net > LON > iLON App (Internal) > Digital Output 1 > nvoClaValueFb_1. A blue arrow points from this data point in the tree to the main configuration area. The main area shows the "Name" field with the value "Net/LON/iLON App/Digital Output 1/nvoClaValueFb_1" highlighted in red. Below the name is a "Description" field with the text "Feedback. Reports the level being sent to the attached device." At the bottom is a table of "Data Point Property" and "Value".

Data Point Property	Value
Icon	Dp_Out
Hidden	<input type="checkbox"/>
<input checked="" type="checkbox"/> Alias Name	iLON100/NVL/static/DO/Output1/State/ NVL_nvoCl
Persistent	<input type="checkbox"/>
<input type="checkbox"/> Use Default Value	

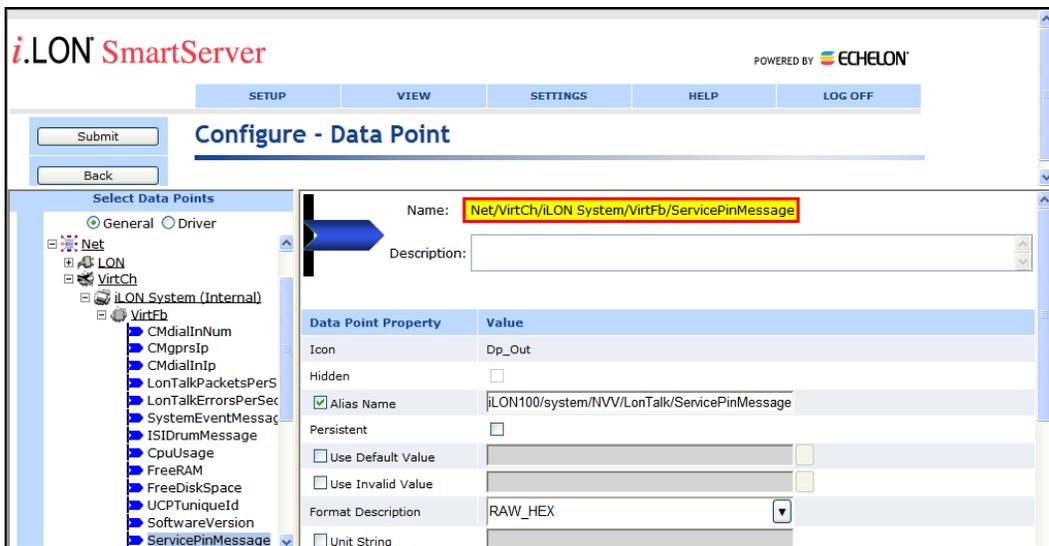
External LONWORKS Device Data Points (formerly NVEs)

The external data points on the device attached to the SmartServer are located under a *<network>/<channel>/<device>/<functional block[index]>* object and are named accordingly. For example, the name of a **DI_Digital_1** data point on an external switch device connected to the SmartServer could be “Net/LON/Switch/Digital Input[0]/DI_Digital_1”.



Virtual Data Points (formerly NVVs)

Interoperable Self-Installation (ISI) data points and data points containing connection manager and LonTalk statistics are located under the `<network>/VirtCh/iLON System (Internal)/VirtFB` object and are named accordingly. For example, the `ServicePinMessage` data point is named “Net/VirtCh/iLON System/VirtFb/ServicePinMessage”.



Constant Data Points (formerly NVCs)

Constant data points are located under a `<network>/LON/iLON App (Internal)/<functional block>` object and are named “CompareDP”. The functional block represents the SmartServer embedded application in which the constant data point is used. For example, a constant data point used in an Alarm Generator could be named “Net/LON/iLON App/Alarm Generator[0]/CompareDP”.

The screenshot shows the i.LON SmartServer web interface. At the top, there is a navigation bar with buttons for SETUP, VIEW, SETTINGS, HELP, and LOG OFF. Below this is a 'Configure - Data Point' page. On the left, there is a 'Select Data Points' tree view showing a hierarchy of objects: General, Driver, Net, LON, iLON App (Internal), Node Object, Digital Input 1, Digital Input 2, Digital Output 1, Digital Output 2, Real Time Clock, Streetlight Scheduler, Alarm Generator[0], nviAgEnable[0], nvoAgAlarmFlag[0], nviAgLatchEnbl[0], Net/LON/Luminaire/, and CompareDP. The 'CompareDP' object is selected and highlighted in blue. The main configuration area shows the Name field set to 'Net/LON/iLON App/Alarm Generator[0]/CompareDP' and the Description field set to 'AG constant created by web interface'. Below these fields is a table of Data Point Properties:

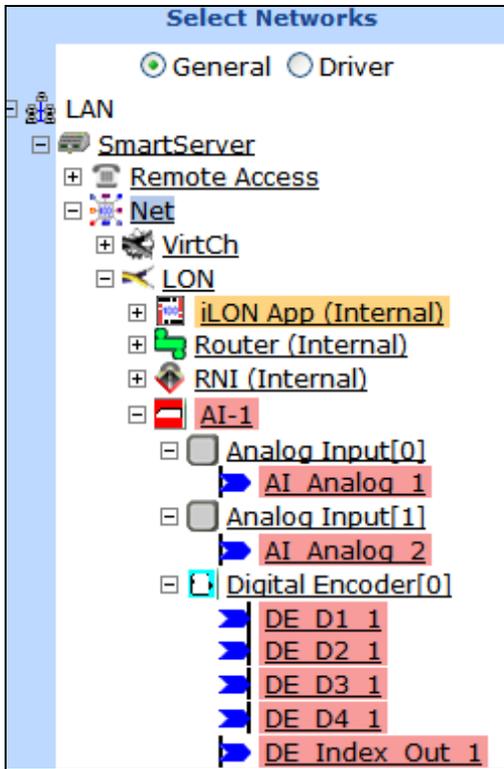
Data Point Property	Value
Icon	Dp_In
Hidden	<input checked="" type="checkbox"/>
Alias Name	<input checked="" type="checkbox"/> iLON100/system/NVC/AG/NVC_AGconstant[0]
Persistent	<input checked="" type="checkbox"/>
Use Default Value	<input checked="" type="checkbox"/> 60
Use Invalid Value	<input type="checkbox"/>
Format Description	#0000000000000000[0] SNVT_temp_f

Managing Network Objects

You can use the navigation pane to configure, duplicate, create, copy/delete, rename, and save templates of the objects in the networks attached to your local SmartServer, in networks attached to the remote SmartServers on the LAN, and in the OpenLNS network databases on the OpenLNS Servers on the LAN. You can perform the following actions on the network objects in a SmartServer or OpenLNS tree:

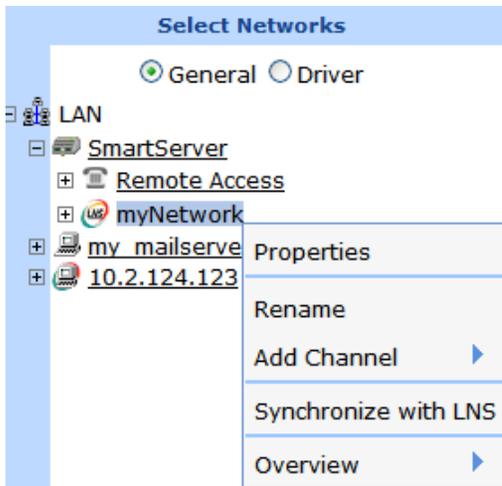
- Click an object to open its respective configuration (**General**) or **Driver** Web page in the application frame.
- Expand an object to display its child objects. For example, you can expand a network to show the channels on the network or expand a channel to show the devices attached to that channel. You can collapse an object to hide its child objects.
- Right-click an object to open a shortcut menu. The options available in the shortcut menu depend on the selected object. The following sections list the available options in the shortcut menu for each type of network object.

Note: Items in the SmartServer tree have special highlighting to indicate different states. Currently selected items are marked blue; offline devices and data points are marked red; uncommissioned devices are marked orange; and items that are out of sync with the OpenLNS network database are marked yellow. Items that are in sync with the OpenLNS network database are clear.

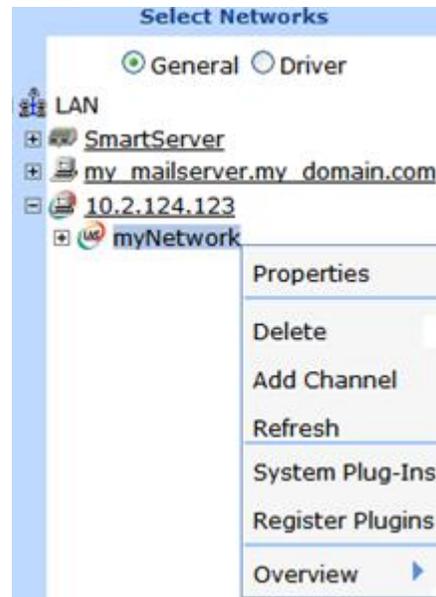


Managing Network Objects

The shortcut menu for networks has the following options:



SmartServer Tree



OpenLNS Tree

Properties

In **General** mode, opens the **Configure - Network** page. You can use this page to enter an optional description of the network, and view the object used to represent the network in the tree, and view whether the network is

hidden or shown in the tree.

In **Driver** mode, opens the **Setup - LON Network Driver** page. You can use this page to switch between LNS or standalone management services, select the network management mode (OnNet or OffNet), select an OpenLNS network database to be synchronized to the SmartServer network, manually synchronize the SmartServer network to an OpenLNS network database (if you create, delete, rename a network object other than a data point, or you configure an OpenLNS network database while the SmartServer is offline), and set the domain length and ID.

You can also use this page to enter an optional description of the network, and change the icon used to represent the network in the tree, and select whether the network is hidden or shown in the tree.

Paste External

This option is only available in the SmartServer tree when there are one or more remote SmartServers on the LAN, and it only appears after you have used the **Copy External** *<object>* on an object in the OpenLNS tree. Adds an object copied from the OpenLNS tree and all of its parent and child objects to the network tree of the target SmartServer.

If you click this command after copying a channel or device in the OpenLNS tree and there are one or more devices on the channel that do not already exist in the local SmartServer's internal database, the **Omit FBs?** dialog opens. By default, only the device is copied to the SmartServer tree. Click **Omit FBs** to accept the default and copy only the device, or click **Copy All** to also copy the functional blocks and data points on the device to the SmartServer tree. The time required to complete the copy operation depends on the number of functional blocks and data points on the device.

If you click **Copy All** to copy the device and all of its functional blocks and data points to the SmartServer tree, and there are more items than can be cached by your Web browser, the **Automatic Submit?** dialog opens. Click **Auto Submit** to continue copying the items to the SmartServer tree, or click **Lose Changes** to stop the copy operation. If you click **Auto Submit**, additional copies from the OpenLNS tree will be sent to the local SmartServer tree when a batch is ready.

For example, you can copy a device and paste it to a channel branch in a SmartServer tree. The device, its parent channel (if different than the selected channel), and optionally its functional block and data points are added to the network tree. You can then use the target SmartServer to manage the objects.

Note: The target SmartServer must be synchronized with the OpenLNS network database in which the copied object is stored in order to perform this operation.

Rename

This option is only available in the SmartServer tree. Opens the **Enter Name** dialog where you can enter a new name for the network. You can only rename the network when the SmartServer is operating in Standalone mode.

Delete

This option is only available in the OpenLNS tree. Permanently removes the OpenLNS network database from the OpenLNS Server on which it is stored.

Add Channel

In the SmartServer tree, opens a shortcut menu from which you select the type of channel to create on the network (**LON**, **MODBUS**, **M-BUS**, or **Virtual**) and then enter a name for the channel in the **Enter Name** dialog.

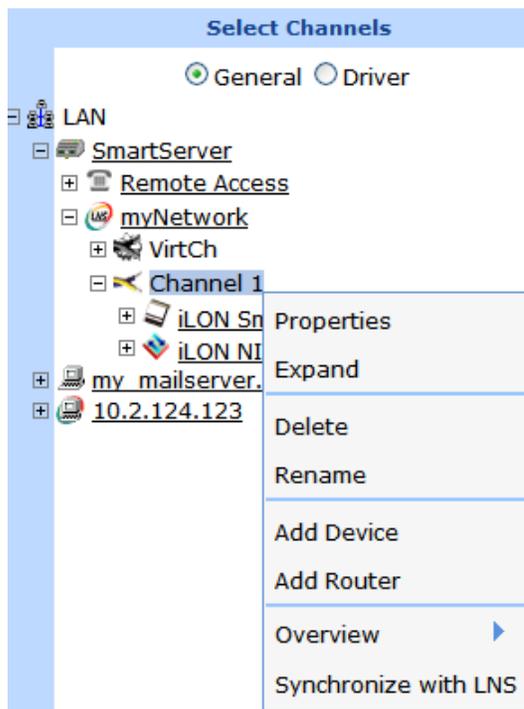
In the OpenLNS tree, opens the **Enter Name** dialog where you enter a name

for the LONWORKS channel being created. See *Creating and Configuring LONWORKS Channels* in Chapter 5 for more information.

<i>Synchronize with LNS</i>	This option is only available in the SmartServer tree. Opens the SmartServer Resync dialog where you can manually synchronize the SmartServer's internal database (the XML files in the /config/network folder on the SmartServer flash disk) to an OpenLNS network database. See <i>Manually Synchronizing the SmartServer to an OpenLNS network database</i> for more information.
<i>Refresh</i>	This option is only available in the OpenLNS tree. Updates the channels, devices, functional blocks, and data points displayed under the network.
<i>System Plug-ins</i>	This option is only available in the OpenLNS tree. Opens the Launch Plug-in dialog where you can start plug-ins that are registered for the device or functional block. See <i>Using LNS Plug-ins</i> in Chapter 5 for more information on starting plug-ins.
<i>Register Plug-ins</i>	This option is only available in the OpenLNS tree. Opens the Register Plug-in dialog where you can view the plug-ins that are registered and unregistered in the network, and register plug-ins so you can launch them. See <i>Using LNS Plug-ins</i> in Chapter 5 for more information on registering plug-ins.
<i>Overview</i>	Opens a shortcut menu that includes options for opening Overview Web pages for the channels, devices, and connections (Web connections in the SmartServer tree or LONWORKS connections in the OpenLNS tree) in the network, and an option for opening the Lon Command Queue Web page. See Chapter 5 for more information on using the Overview Web pages and the Lon Command Queue Web page.

Managing Channel Objects

The shortcut menu for channels has the following options:



Properties

In **General** mode, opens the **Configure - Channel** page. You can use this page to enter an optional description of the channel, view the icon used to represent the channel in the tree, and view whether the channel is hidden or shown in the tree.

In **Driver** mode, opens a Web page for configuring the channel's driver-specific properties (LONWORKS, Modbus, or M-Bus). The following describes the properties you can set on a channel for each driver type:

- **LONWORKS.** Opens the **Setup - LON Channel Driver** Web page. You can use this page to change the channel type (FT, IP, PL, RF, or TP), enable repeating on PL-20 channels, enable and set a round-trip delay time, set the minimal offline time for devices, set an offline delay for devices, and modify advanced properties (transmit timer and recount tries).
- **Modbus.** Opens the **Setup - Modbus Channel Driver** Web page. You can use this page to change the channel type (TCP/IP, RS-485, or RS-232), select the baud rate, select the transmission mode, and select the size of start and parity bits, and set a stop bit.
- **M-Bus.** Opens the **Setup - M-Bus Channel Driver** Web page. You can use this page to change the channel type (RS-485 or RS-232) and select the baud rate.

You can also a channel's **Driver** Web page to enter an optional description of the channel, change the icon used to represent the channel in the tree, and select whether the channel is hidden or shown in the tree.

Expand

Displays the devices attached to the channel in the navigation pane.

Delete

Removes the channel and all of its devices, functional blocks, and data points from the network. If the SmartServer is synchronized with an OpenLNS network database, this also deletes the channel and all of its devices, functional blocks, and data points from the OpenLNS network database.

Rename

Opens the **Enter Name** dialog where you can enter a new name for the channel.

Create External Channel

This option is only available in the OpenLNS tree when there are no remote SmartServers on the LAN. Adds the channel, all of its child devices, and optionally the devices' child functional blocks and data points to the local SmartServer tree (if the local SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the objects are added to the local SmartServer tree, they can be managed with the local SmartServer.

When you click this command and there are one or more devices on the channel that do not already exist in the local SmartServer's internal database, the **Omit FBs?** dialog opens. By default, only the device is copied to the SmartServer tree. Click **Omit FBs** to accept the default and copy only the device, or click **Copy All** to also copy the functional blocks and data points on the device to the SmartServer tree. The time required to complete the copy operation depends on the number of functional blocks and data points on the device.

If you click **Copy All** to copy the device and all of its functional blocks and data points to the SmartServer tree, and there are more items than can be cached by your Web browser, the **Automatic Submit?** dialog opens. Click **Auto Submit** to continue copying the items to the SmartServer tree, or click

Lose Changes to stop the copy operation. If you click **Auto Submit**, additional copies from the OpenLNS tree will be sent to the local SmartServer tree when a batch is ready.

Copy External Channel

This option is only available in the OpenLNS tree when there are one or more remote SmartServers on the LAN. Copies the channel and all of its children devices. The copied objects can then be pasted to a target SmartServer using the **Paste External** shortcut command on any network object in the target SmartServer tree (if the target SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the copied objects are pasted to the SmartServer tree, they can be managed with the target SmartServer.

Paste External

This option is only available in the SmartServer tree when there are one or more remote SmartServers on the LAN, and it only appears after you have used the **Copy External** <object> on an object in the OpenLNS tree. Adds an object copied from the OpenLNS tree and all of its parent and child objects to the network tree of the target SmartServer.

If you click this command after copying a channel or device in the OpenLNS tree and there are one or more devices on the channel that do not already exist in the local SmartServer's internal database, the **Omit FBs?** dialog opens. By default, only the device is copied to the SmartServer tree. Click **Omit FBs** to accept the default and copy only the device, or click **Copy All** to also copy the functional blocks and data points on the device to the SmartServer tree. The time required to complete the copy operation depends on the number of functional blocks and data points on the device.

If you click **Copy All** to copy the device and all of its functional blocks and data points to the SmartServer tree, and there are more items than can be cached by your Web browser, the **Automatic Submit?** dialog opens. Click **Auto Submit** to continue copying the items to the SmartServer tree, or click **Lose Changes** to stop the copy operation. If you click **Auto Submit**, additional copies from the OpenLNS tree will be sent to the local SmartServer tree when a batch is ready.

For example, you can copy a device and paste it to a channel branch in a SmartServer tree. The device, its parent channel (if different than the selected channel), and optionally its functional block and data points are added to the network tree. You can then use the target SmartServer to manage the objects.

Note: The target SmartServer must be synchronized with the OpenLNS network database in which the copied object is stored in order to perform this operation.

Add Device

Opens the **Add Device** dialog in which you create a new device from a XIF or device template (.XML file). See *Creating and Configuring LONWORKS Devices* in Chapter 5 for more information.

Add Router

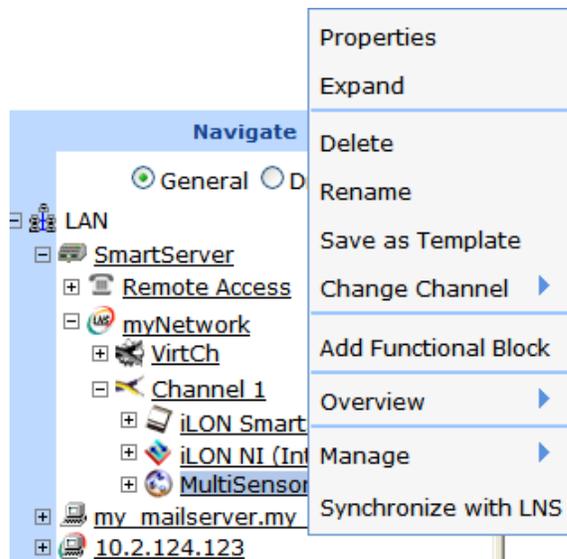
This option is only available for LONWORKS channels. Opens the **Add Router** dialog in which you enter a name for the router, select the router type, and select the target channel to be connected to the far side of the router. See *Creating and Configuring LONWORKS Routers* in Chapter 5 for more information.

Note: To add a router to a LONWORKS channel in a SmartServer tree, the SmartServer must be operating in LNS mode (**LNS Auto** or **LNS Manual**).

<i>Overview</i>	Opens a shortcut menu that includes options for opening Overview Web pages for the devices, functional blocks, and bindings (Web connections in the SmartServer tree or LONWORKS connections in the OpenLNS tree) in the network, and an option for opening the Lon Command Queue and Power Line Repeating Analysis Web page. See Chapter 5 for more information on using the Overview Web pages and the Lon Command Queue and Power Line Repeating Analysis Web pages.
<i>Synchronize with LNS</i>	This option is only available in the SmartServer tree when the SmartServer is synchronized to an OpenLNS network database. Transmits changes made to the channel to the OpenLNS network database, and updates the SmartServer's internal database with changes made to the channel with OpenLNS CT, OpenLNS tree, or other OpenLNS application. This option is only available in the SmartServer tree. Note that this synchronization does update the LON driver properties of the channel (for example, timing parameters, description) in the SmartServer's internal database.
<i>Refresh</i>	This option is only available in the OpenLNS tree. Updates the devices, functional blocks, and data points displayed under the channel in the OpenLNS tree.

Managing Device Objects

The shortcut menu for devices has the following options:



<i>Properties</i>	<p>In General mode, opens the Configure Network page. You can use this page to enter an optional description of the device, view the icon used to represent the device in the tree, and view whether the device is hidden or shown in the tree.</p> <p>In Driver mode, opens a Web page for configuring the device's driver-specific properties (LONWORKS, Modbus, or M-Bus). The following describes the properties you can set on a device for each driver type:</p> <ul style="list-style-type: none"> • LONWORKS. Opens the Setup - LON Device Driver Web page. You can use this page to manage and self-install the device. The network management tasks you can perform from this page include acquiring the device's Neuron ID, configuring the device, setting the device application online or offline, selecting an application image file and device interface to download to the device, and resetting the device (see
-------------------	--

Creating and Configuring LONWORKS Devices in Chapter 5 for more information). You can self-install the device using the Smart Network Management feature on this page (see *Installing Devices with Smart Network Management* in Chapter 5 for more information).

- **Modbus.** Opens the **Setup - Modbus Device Driver** Web page. You can use this page to view and set the logical address of the device and view and set the maximum number of data elements on the device.
- **M-Bus.** Opens the **Setup - M-Bus Device Driver** Web page. You can use this page to change the baud rate, set the primary and/or secondary address, and view and set the manufacturer ID, medium, and version.

You can also a device's **Driver** Web page to enter an optional description of the device, change the icon used to represent the device in the tree, and select whether the device is hidden or shown in the tree.

Expand

Expands the device to show all of the static and dynamic functional blocks defined for the device, and expands the functional blocks to show all of the static and dynamic network variables and configuration properties in the functional blocks. Deleted functional blocks, network variables, and configuration properties are not displayed.

Delete

Removes the device and all of its functional blocks, data points, and bindings from the channel.

If the SmartServer is synchronized with an OpenLNS network database, selecting this option opens the **Keep LNS Copy?** dialog. In this dialog, click **Yes** to delete the external device only from the SmartServer's internal database, or click **No** to delete the external device from both the SmartServer's internal database and the OpenLNS network database to which the SmartServer is synchronized.

If any data points in the device to be deleted are bound, a dialog appears prompting you to confirm that you want to delete the device even though it has bound data points.

Rename

Opens the **Enter Name** dialog where you can enter a new name for the device.

Save as Template

Opens the **Save as Template** dialog where you can save an .XML file documenting the current properties of the device and the child functional blocks and data points currently displayed under the device. You can then create new devices from this template. See *Using Device Templates* later in this section for more information.

Change Channel

Opens a shortcut menu in which you can select a different channel on the network where the device is to be moved logically.

Create External Device

This option is only available in the OpenLNS tree when there are no remote SmartServers on the LAN. Adds the device, its parent channel, and optionally all of its children functional blocks and data points to the local SmartServer tree (if the local SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the objects are added to the local SmartServer tree, they can be managed with the local SmartServer.

When you click this command, the **Omit FBs?** dialog opens. By default, only the device is copied to the SmartServer tree. Click **Omit FBs** to accept the default and copy only the device, or click **Copy All** to also copy the functional blocks and data points on the device to the SmartServer tree. Note that the time required to complete the copy operation depends on the

number of functional blocks and data points on the device.

If you click **Copy All** to copy the device and all of its functional blocks and data points to the SmartServer tree, and there are more items than can be cached by your Web browser, the **Automatic Submit?** dialog opens. Click **Auto Submit** to continue copying the items to the SmartServer tree, or click **Lose Changes** to stop the copy operation. If you click **Auto Submit**, additional copies from the OpenLNS tree will be sent to the local SmartServer tree when a batch is ready.

*Create Ext. Dev.
(use Template)*

This option is only available in the OpenLNS tree when there are no remote SmartServers on the LAN. Opens the **Choose File** dialog, in which you select a device template that is used to copy specific data points in the device interface to the local SmartServer. See *Creating External Data Points from Device Templates* later in this section for more information.

*Copy External
Device*

This option is only available in the OpenLNS tree when there are one or more remote SmartServers on the LAN. Copies the device and all of its children functional blocks and data points. The copied objects can then be pasted to a target SmartServer using the **Paste External** shortcut command on any network object in the target SmartServer tree (if the target SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the copied objects are pasted to the SmartServer tree, they can be managed with the target SmartServer.

Paste External

This option is only available in the SmartServer tree when there are one or more remote SmartServers on the LAN, and it only appears after you have used the **Copy External <object>** on an object in the OpenLNS tree. Adds an object copied from the OpenLNS tree and all of its parent and child objects to the network tree of the target SmartServer.

If you click this command after copying a channel or device in the OpenLNS tree and there are one or more devices on the channel that do not already exist in the local SmartServer's internal database, the **Omit FBs?** dialog opens. By default, only the device is copied to the target SmartServer tree. Click **Omit FBs** to accept the default and copy only the device, or click **Copy All** to also copy the functional blocks and data points on the device to the target SmartServer tree. The time required to complete the copy operation depends on the number of functional blocks and data points on the device.

If you click **Copy All** to copy the device and all of its functional blocks and data points to the target SmartServer tree, and there are more items than can be cached by your Web browser, the **Automatic Submit?** dialog opens. Click **Auto Submit** to continue copying the items to the SmartServer tree, or click **Lose Changes** to stop the copy operation. If you click **Auto Submit**, additional copies from the OpenLNS tree will be sent to the target SmartServer tree when a batch is ready.

Note: The target SmartServer must be synchronized with the OpenLNS network database in which the copied object is stored in order to perform this operation.

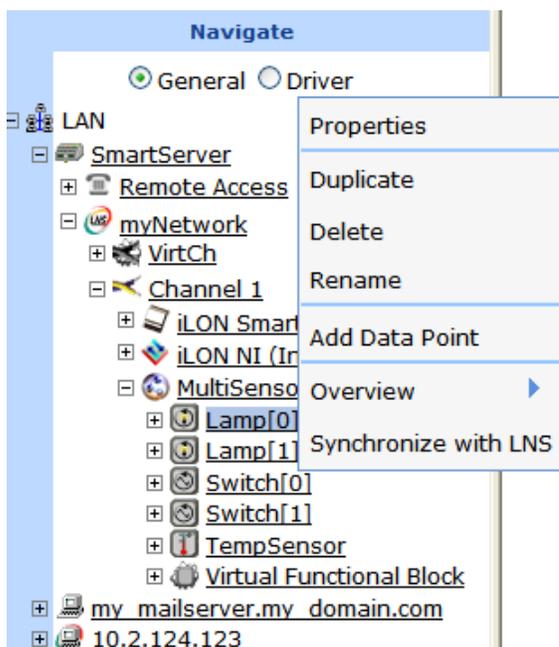
*Paste Ext. Dev.
(use Template)*

This option is only available in the SmartServer tree, and it only appears after you have used the **Copy External Device** option on a device in the OpenLNS tree. Opens the **Choose File** dialog, in which you select a device template that is used to copy specific data points in the device interface to the local SmartServer. See *Creating External Data Points from Device Templates* later in this section for more information.

<i>Add Functional Block</i>	Opens the Add Functional Block dialog in which you select a static functional block defined by the device interface (XIF) file, or create a dynamic functional block from a standard functional profile template (SFPT) or user-defined functional profile template (UFPT).
<i>Overview</i>	Opens a shortcut menu that includes options for opening Overview Web pages for the functional blocks, data points, and connections (Web connections in the SmartServer tree or LONWORKS connections in the OpenLNS tree) in the network. See Chapter 5 for more information on using the Overview Web pages.
<i>Manage</i>	This option is only available for LONWORKS devices. Opens a shortcut menu from which you can select the following network management commands: Send Service Pin Message, Replace, Commission, Decommission, Set Online, Set Offline, Fetch Program ID, Download Image, Activate Template, Download CP File, Query Status, Clear Status, Wink, Reset, and Self-Install. See <i>Issuing Network Management Commands</i> later in this chapter for more information on using these commands.
<i>Synchronize with LNS</i>	Transmits changes made to the device in the SmartServer tree to the OpenLNS network database, and updates the SmartServer's internal database with changes made to the device with OpenLNS CT, OpenLNS tree, or other OpenLNS application. This option is only available in the SmartServer tree. Note that this synchronization does update the LON driver properties of the device (for example, commission status, application status) in the SmartServer's internal database.
<i>Refresh</i>	This option is only available in the OpenLNS tree. Updates the functional blocks and data points displayed under the device in the OpenLNS tree.

Managing Functional Block Objects

The shortcut menu for functional block icons has the following options:



Properties In **General** mode, opens the SmartServer embedded application corresponding to the selected functional block. If the functional block does

not represent a SmartServer embedded application, it opens the **Configure - Functional Block** page. You can use this page to enter an optional description of the functional block, view the icon used to represent the functional block in the tree, and view whether the functional block is hidden or shown in the tree.

In **Driver** mode, opens a Web page for configuring the functional block's driver-specific properties (LONWORKS, Modbus, or M-Bus). The following describes the properties you can set on a device for each driver type:

- **LONWORKS.** Opens the **Setup - LON Functional Block Driver** page. You can use this page to enter an optional description of the functional block, view the icon used to represent the functional block in the tree, view whether the functional block is hidden or shown in the tree, and view the functional profile template used by the functional block.
- **Modbus.** Opens the **Setup - Modbus Functional Block Driver Web** page. This page provides the same options available in the **General properties** Web page (change the icon and select whether the functional block is hidden or shown in the tree).
- **M-Bus.** Opens the **Setup - M-Bus Functional Block Driver Web** page. This page provides the same options available in the **General properties** Web page (change the icon and select whether the functional block is hidden or shown in the tree).

You can also a functional block's **Driver** Web page to enter an optional description of the functional block, change the icon used to represent the functional block in the tree, and select whether the functional block is hidden or shown in the tree.

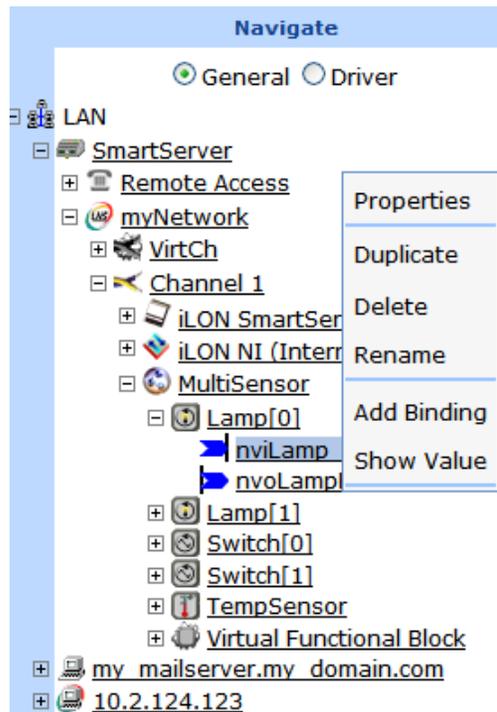
<i>Duplicate</i>	Opens the Duplicate Functional Block dialog where you can create a copy of the selected functional block that has the same configuration and driver properties as the source. This is useful for quickly adding pre-configured SmartServer applications (such as a Scheduler or an Alarm Notifier) to the SmartServer and expediting the network design process. See <i>Creating a Duplicate Functional Block</i> in this chapter for more information.
<i>Delete</i>	For the SmartServer App Device's [i.LON App (Internal)] functional blocks in the SmartServer tree, deletes the XML configuration of the functional block, and hides the functional block in the tree. For all other functional blocks, removes the functional block and all of its data points from the parent device tree. If the SmartServer is synchronized with an OpenLNS network database, this also deletes the functional block and all of its data points from the OpenLNS network database.
<i>Rename</i>	Opens the Enter Name dialog where you can enter a new name for the functional block.
<i>Create External FB</i>	This option is only available in the OpenLNS tree when there are no remote SmartServers on the LAN. Adds the functional block and all of its network variables and configuration properties to the local SmartServer tree (if the local SmartServer is synchronized with the OpenLNS database in which the objects are stored). After the objects are added to the local SmartServer tree, they can be managed with the local SmartServer.
<i>Copy External FB</i>	This option is only available in the OpenLNS tree when there are one or more remote SmartServers on the LAN. Copies the functional block and all of its network variables and configuration properties. The copied objects can then be pasted to a target SmartServer using the Paste External shortcut

command on any network object in the target SmartServer tree (if the target SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the copied objects are pasted to the SmartServer tree, they can be managed with the target SmartServer.

- Paste External* This option is only available in the SmartServer tree, and it only appears after you have used the **Copy External** <object> on an object in the OpenLNS tree. Adds an object copied from the OpenLNS tree and all of its parent and child objects to the network tree of the target SmartServer.
- For example, you can copy a data point and paste it to a functional block branch in a SmartServer tree. The data point, and its parent channel, device, and functional block (if different than the selected functional block and its parent channel and device) are added to the network tree. You can then use the target SmartServer to manage the objects.
- Note:** The target SmartServer must be synchronized with the OpenLNS network database in which the copied object is stored in order to perform this operation.
- Add Data Point* Opens the **Add Data Point** dialog in which you select a static network variable defined by the device interface (XIF) file, or create a dynamic network variable from a standard or user-defined network variable/configuration property type (SNVT, SCPT, UNVT, or UCPT).
- Overview* Opens a shortcut menu that includes options for opening Overview Web pages for the data points and bindings (Web connections in the SmartServer tree or LONWORKS connections in the OpenLNS tree) in the network. See Chapter 5 for more information on using the Overview Web pages.
- Synchronize with LNS* Transmits changes made to the functional block in the SmartServer tree to the OpenLNS network database, and updates the SmartServer's internal database with changes made to the functional block with OpenLNS CT, OpenLNS tree, or other OpenLNS application. This option is only available in the SmartServer tree. This synchronization updates the LON driver properties of the functional block (for example, description) in the SmartServer's internal database.
- Refresh* This option is only available in the OpenLNS tree. Updates the data points displayed under the functional block in the OpenLNS tree.

Managing Data Point Objects

The shortcut menu for data point icons has the following options:



Properties

In **General** mode, opens the **Configure - Data Point** Web page. You can use this page to enter an alias name, select whether the data point is constant, enable and set default and invalid values, view the type/format, set network performance configuration properties (heartbeat, throttle, offline, and send on delta), set presets, and modify the unit strings of the individual fields of structured data points.

You can also use the **Configure - Data Point** Web page to enter an optional description of the data point, view the icon used to represent the data point in the tree, view whether the data point is hidden or shown in the tree.

In **Driver** mode, opens a Web page for configuring the data point's driver-specific properties (LONWORKS, Modbus, or M-Bus). The following describes the properties you can set on a device for each driver type:

- **LONWORKS.** Opens the **Setup - LON Data Point Driver** page. You can use this page to set the poll rate, view and/or set the data point direction, view whether the data point is static or dynamic, view and/or change the length, and view and/or change the type/format.
- **Modbus.** Opens the **Setup - Modbus Data Point Driver** Web page. You can use this page to set the poll rate, access type, addressing properties, and the format and type parameters).
- **M-Bus.** Opens the **Setup - M-Bus Data Point Driver** Web page. You can use this page to change the poll rate, format and type parameters, and the length.

You can also use a data point's **Driver** Web page to enter an optional description of the data point, change the icon used to represent the data point in the tree, and select whether the data point is hidden or shown in the tree.

<i>Duplicate</i>	Opens the Duplicate Data Point dialog where you can create a copy of the selected data point (if it is a dynamic type) that has the same configuration and driver properties as the source. See <i>Creating a Duplicate Dynamic Data Point</i> in this chapter for more information.
<i>Delete</i>	Removes the data point from its functional block. If the SmartServer is synchronized with an OpenLNS network database, this also deletes the data point from the OpenLNS network database.
<i>Rename</i>	Opens the Enter Name dialog where you can enter a new name for the data point.
<i>Create External NV</i>	<p>This option is only available in the OpenLNS tree when there are no remote SmartServers on the LAN. Adds the network variable and its parent channel, device, and functional block to the local SmartServer tree (if the local SmartServer is synchronized with the OpenLNS database in which the objects are stored). After the objects are added to the local SmartServer tree, they can be managed with the local SmartServer.</p> <p>You must use this option (or the Copy External NV and Paste External options) in order to use the SmartServer's built-in applications to monitor and control the data points of external devices that are managed with OpenLNS CT or other OpenLNS application.</p>
<i>Copy External NV</i>	<p>This option is only available in the OpenLNS tree when there are one or more remote SmartServers on the LAN. Copies the data point and its parent channel, device, and functional block. The copied objects can then be pasted to a target SmartServer using the Paste External shortcut command on any network object in the target SmartServer tree (if the target SmartServer is synchronized with the OpenLNS database in which the copied objects are stored). After the copied objects are pasted to the SmartServer tree, they can be managed with the target SmartServer.</p> <p>You must use this option (or the Create External NV option) in order to use the SmartServer's built-in applications to monitor and control the data points of external devices that are managed with OpenLNS CT or other OpenLNS application.</p>
<i>Paste External</i>	<p>This option is only available in the SmartServer tree, and it only appears after you have used the Copy External <object> on an object in the OpenLNS tree. Adds an object copied from the OpenLNS tree and all of its parent and child objects to the network tree of the target SmartServer.</p> <p>For example, you can copy a functional block and paste it to a device branch in a SmartServer tree. The functional block, its parent channel and device (if different than the selected device and its parent channel), and its data points are added to the network tree. You can then use the target SmartServer to manage the objects.</p> <p>Note: The target SmartServer must be synchronized with the OpenLNS network database in which the copied object is stored in order to perform this operation.</p>
<i>Add Connection</i>	Opens the Configure – Web Connection Web page where you can bind the selected data point to one or more target data points in the Web Connection Destination frame to the right. In the SmartServer tree, you can use this option to create Web connections. In the OpenLNS tree, you can use this option to create LONWORKS connections.
<i>Show Value</i>	Opens a dialog showing the name, status, and current value of the data point.
<i>Synchronize with</i>	Transmits changes made to the data point in the SmartServer tree to the

LNS

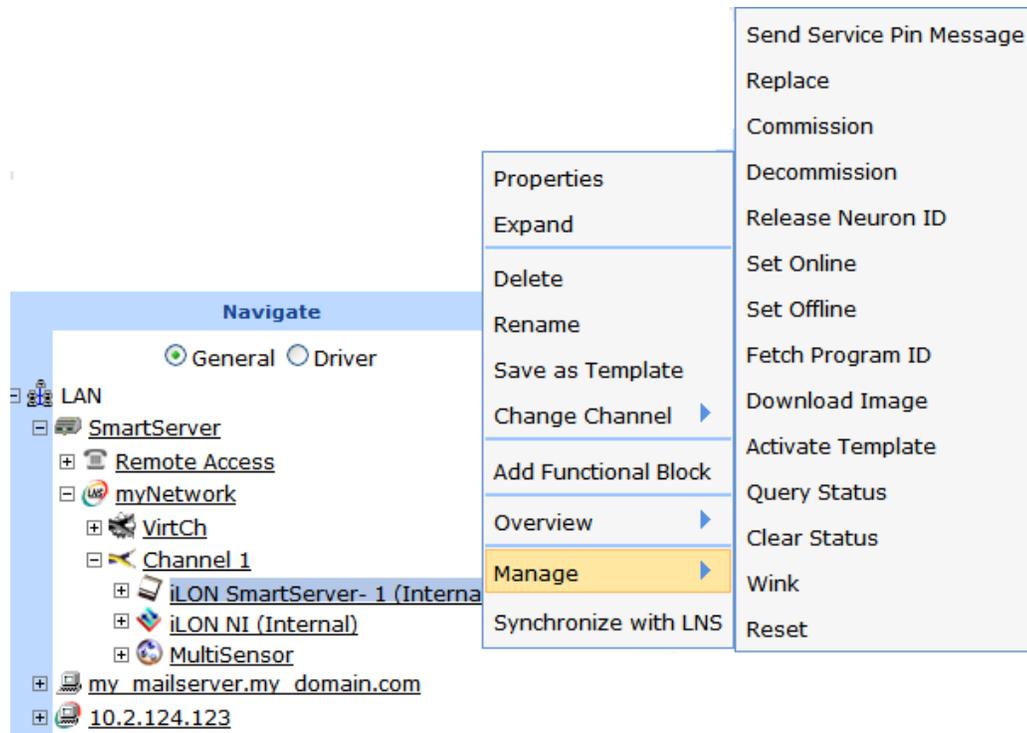
OpenLNS network database, and updates the SmartServer's internal database with changes made to the data point with OpenLNS CT, OpenLNS tree, or other OpenLNS application. This option is only available in the SmartServer tree. Note that this synchronization does update the LON driver properties of the data point (for example, format description) in the SmartServer's internal database.

Issuing Network Management Commands

You can use the SmartServer tree or the OpenLNS tree to manage the SmartServer device, the LONWORKS devices connected to the SmartServer, and the LONWORKS devices in OpenLNS network databases (provided that you install the Echelon Enterprise Services 2.2 and add an OpenLNS Server computer to the LAN). You can issue the following network management commands for the devices in the SmartServer tree and the OpenLNS tree: Send Service Pin Message (internal devices only), Replace, Commission, Decommission, Set Online, Set Offline, Fetch Program ID, Download Image, Activate Template, Download CP File, Query Status, Clear Status, Wink, Reset, and Self-Install (routers only).

To manage a device from the SmartServer tree or OpenLNS tree, follow these steps.

1. Expand the parent network and channel icons to show the device to be managed.
 - For devices in the SmartServer tree, expand the network, and then expand the LONWORKS channel to which the device is attached.
 - For devices in an OpenLNS network database, expand the LNS Server icon, expand the OpenLNS network database in which the device is stored, and then expand the LONWORKS channel to which the device is attached.
2. Select one or more devices to manage. To select one device, right-click the device, point to **Manage**, and then select a management command from the shortcut menu. To perform batch operations on two or more devices, click one device and then either hold down CTRL and click all other devices to be installed or hold down SHIFT and select another device to perform the management task on the entire range of devices, right-click one of the selected devices, point to **Manage**, and then select one of the following management commands from the shortcut menu:



Send Service Pin Message

This option is only available for the SmartServer’s 16 internal devices (SmartServer App device, SmartServer virtual device, IP-852 router, RNI, local network interface, LonTalk device, and 10 custom app devices). Sends a service pin message from the internal device. You can use this command to commission an internal device on the SmartServer, such as a custom app device, using an OpenLNS application such as OpenLNS CT.

This command is useful because if you press the service pin on the SmartServer hardware when commissioning an internal device, it sends service pin messages from all 16 of the internal devices defined on the SmartServer.

Replace

Opens the **Replace LON Device** dialog in which you manually enter the Neuron ID of a replacement device that has the same program ID of the selected device. See *Manually Replacing Devices* in Chapter 5 for more information.

Commission

Downloads network and application configuration data into the device.

Decommission

Temporarily uninstalls the device. Decommissioning devices is useful when optimizing, troubleshooting, or repairing a network. All the configuration data of a decommissioned device, including configuration properties and bindings, are preserved.

Release Neuron ID

Erases the Neuron ID defined for the device in the SmartServer or OpenLNS network database and decommissions the device. You can release the Neuron IDs of devices on a development SmartServer to create a template of that development SmartServer and deploy it on one or more target SmartServers, and automatically install the devices in the template.

Set Online

Places the device in the online state. The behavior in the online state depends on the device. A Neuron-hosted device, for example, will run its application.

<i>Set Offline</i>	Places the device in the offline state. The behavior in the offline state depends on the device. A Neuron-hosted device, for example, will not run its application. You can place devices offline to bring up a system incrementally.
<i>Fetch Program ID</i>	Retrieves the program ID stored in the device and enters it into the Program ID box in the device's Setup - LON Device Driver Web page.
<i>Download Image</i>	Downloads to the device the application image specified in the Image box on Setup - LON Device Driver Web page. The device must be a Neuron-hosted device, have writeable application memory, and come with an application file.
<i>Activate Template</i>	Loads onto the SmartServer the external device interface (XIF) file specified in the Template box on the Setup - LON Device Driver Web page.
<i>Download CP File</i>	Downloads to the device the configuration property files specified in the Configuration Property array on the Setup - LON Device Driver Web page.
<i>Query Status</i>	Tests the device to ensure that it is operating and configured correctly, and then opens the Query Status dialog, which reports the following device statistics: <ul style="list-style-type: none"> • Name • Unique ID • Transmission Errors • Transaction Timeouts • Receive Transaction Full Errors • Lost Messages • Missed Messages • Reset Cause • Version Number • Error Log • Neuron Model • Device State
<i>Clear Status</i>	Clears the statistics in the Query Status dialog.
<i>Wink</i>	Requests that the device generate an application-dependent audio or visual feedback such as a beep or a flashing service LED. The device must support the Wink function to use this command. This command is useful for identifying devices on the network.
<i>Reset</i>	Stops the device application, terminates all incoming and outgoing messages, sets all temporary settings to their initial values, and then restarts the device application. If the device was offline, it is placed online.
<i>Self-Install</i>	Configures an IP-852 router in the OpenLNS tree as a repeater and assigns default domain/subnet/node addresses to its interfaces. Only use this option if the LNS Proxy Web service is off and the SmartServer is not connected to a IP-852 Configuration Server. Once the SmartServer can communicate with an OpenLNS Server via the LNS Proxy Web service, the IP-852 router is synchronized to the OpenLNS network database and installed using OpenLNS network management services.

Note: You can also issue these network management commands from the **Setup - LON Device Driver** Web page. To access the **Setup - LON Device Driver** Web page, click **Driver** and then either click the device or right-click the device and select **Properties** from the shortcut menu. A

major advantage of using the **Setup - LON Device Driver** Web page to manage a device is that you can enable smart network management for one property or a set of properties. The SmartServer will then automatically issue the appropriate network management commands and set the device properties to the state considered to be desired. See Chapter 5, *Using the SmartServer as a Network Management Tool*, for more information on configuring devices with the **Setup - LON Device Driver** Web page and using smart network management to install and auto-manage devices.

Using Device Templates

You can configure a device in the SmartServer tree or OpenLNS tree, save it to a device template (.XML file) that is stored on the SmartServer flash disk or your computer, and then use the device template to create new devices that have a specific pre-defined configuration. You can also use device templates to automate the creation of external data points on the SmartServer (this feature provides the functionality offered by the i.LON 100 PointFactory Plug-in, which is compatible with the e2 and e3 releases of the i.LON 100 software).

This section describes how to perform the following tasks related to using device templates:

- Create device templates.
- Create devices from templates.
- Create external data points from a device template.
- Copy device templates to another SmartServer.
- Delete device templates on a SmartServer.

Creating Device Templates

You can save one device to a template at a time. The template will include the device, and it will include the functional blocks and data points currently displayed in the device tree. The template saves the current driver properties of the device and the functional blocks, and it saves the current configuration and driver properties of the data points.

Note: If you save the SmartServer's internal App device [**i.LON App (Internal)**] to a template, the configurations of the built-in applications (for example, Data Logger, Scheduler, and so on) will not be preserved in the template. The template will include the functional blocks on the SmartServer App device that were displayed in the SmartServer tree at the time the template was created and it will include their data points, but the actual applications will be unconfigured.

You can configure the SmartServer's built-in applications on a single source SmartServer, and then automatically or manually deploy that SmartServer App device configuration to one or more target SmartServers. You can automatically deploy the SmartServer App device configuration using the i.LON AdminServer (see Chapter 2 of the *Echelon Enterprise Services 2.2 User's Guide* for more information). You can manually deploy it by copying the SmartServer App device's XML file to the target SmartServers via FTP (see *Manually Deploying a Network Configuration on Multiple SmartServers* in Appendix D for more information on how to do this).

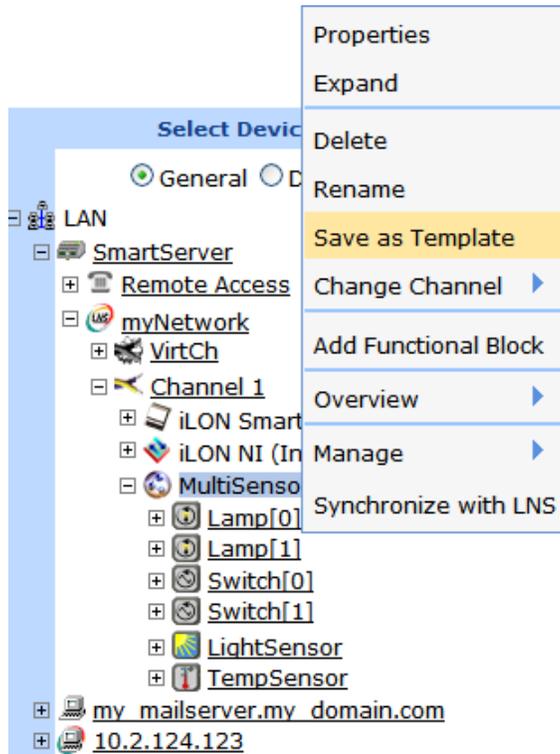
To create a device template, follow these steps:

1. To automatically install devices created from the device template, follow these steps:
 - a. Erase the Neuron ID of the source device. To do this, right-click the source device, point to **Manage**, and then click **Release Neuron ID** in the shortcut menu. This decommissions the source device.
 - b. Logically detach the network interface from the network. To do this, click **Driver**, click the network in the navigation pane, clear the **Use Network Interface** check box in the **Setup - LON Network Driver** Web page, and then click **Submit**. This prevents the SmartServer from associating a Neuron ID with the device template when you complete step d.
 - c. Open the source device's **Setup - LON Device Driver** Web page. To do this, click **Driver** and then click the source device in the navigation pane.

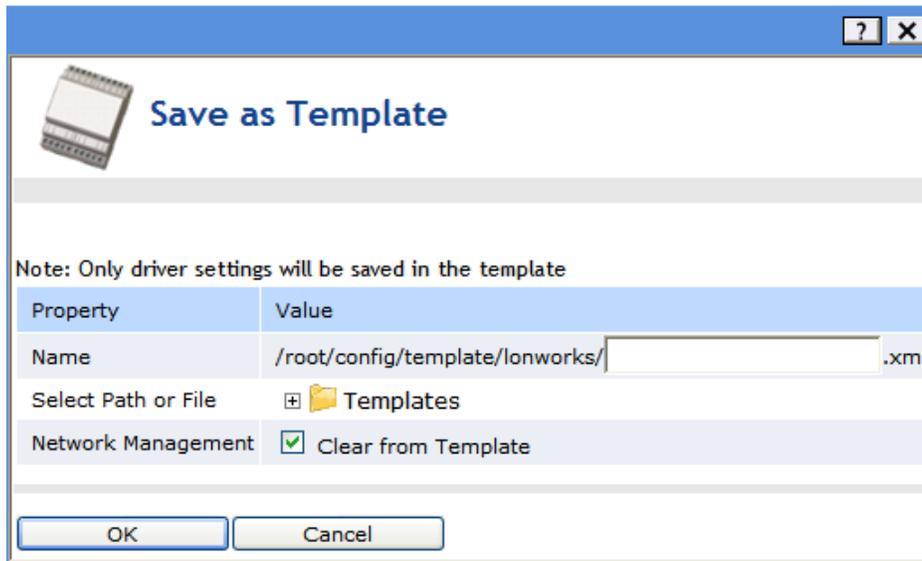
- d. Select **Neuron ID**. This enables the SmartServer to automatically acquire the Neuron ID of devices created from the device template using device discovery.
- e. Select **Smart Network Management** at the top of the Web page. This sets the network management commands required to commission the device and set it online.
- f. Click **Submit**.

Note: When you save your device as a template, clear **Clear from Template** in the **Network Management** property as described in step 7. This saves the network management commands you set in steps c-d in the device template. These network management commands will be executed when new devices created from the device template are instantiated.

2. Configure the general and driver properties of the device's data points. For example, you can set the data points' default values, persistent flags unit strings, and presets in the general properties, and you can set their poll rates in the driver properties. See *Configuring LONWORKS Data Points* in Chapter 5 for more information on setting these properties. The data points of the subsequent devices you add to the SmartServer using the device template will have the same property values by default
3. Right-click the device to be saved to a template and then click **Save as Template** on the shortcut menu.

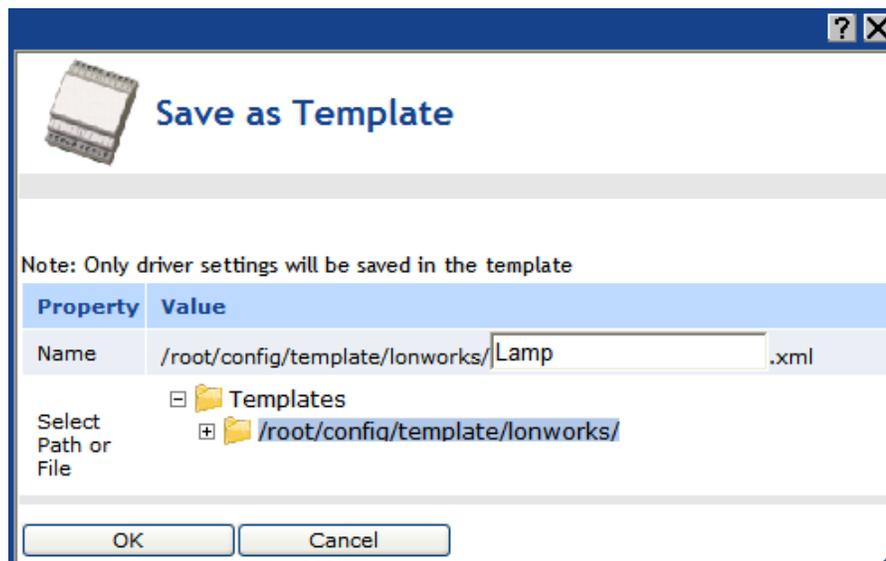


4. The **Save As Template** dialog opens.



5. In the **Name** property, enter a meaningful name for the template.
6. In the **Select Path or File** property, expand the **Templates** folder to show all the folders in the **/config/template** directory on the SmartServer flash disk or your computer. For device templates in the OpenLNS tree, the root directory refers to the **LonWorks\iLON\EnterpriseServices\repository\ees-Insproxy** folder on your EES 2.2 computer. Select the folder to which the template is to be saved or expand the folder and select an existing template file to be overwritten.

You can also select a folder and then enter a sub-directory. For example, if you are creating a template for a LONWORKS lamp device in the SmartServer tree, you can select the **/config/template/lonworks** directory and then enter **Lamp/** in the **Name** property to save the lamp template to its own **/config/template/lonworks/Lamp** sub-directory. The **Name** property will be updated with the specified full path of the template.



7. To enable devices created from the device template to be installed automatically clear **Clear from Template** in the **Network Management** property. This saves any network management commands currently issued for the source device (for example, commission, set online, reset, and so on) in the device template. These network management commands are executed when new

devices created from the device template are instantiated. See step 1 for configuring your device template for automatic installation.

This option is selected by default, meaning that network management commands are not saved in the template and therefore not executed on new devices when they are created from the device template.

8. Click **OK**. An .XML file documenting the driver properties of the device and its functional blocks, and the configuration and driver properties of the device's data points is created. The XML file is saved to the SmartServer flash disk or your EES 2.2 computer at the path specified in step 5. It may take a few minutes for the SmartServer to create the device template.

Note: The current values of the device's configuration properties are saved in the **Default Value** property on the configuration properties' **Configure – Data Point** Web pages.

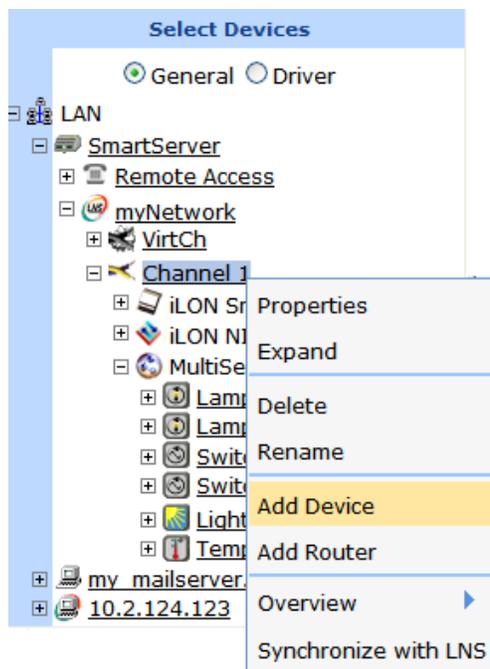
9. When the template has been created, a message appears above the application frame informing you that the template is ready.
10. Click **Submit**. You can now create new devices from the template you created as described in the next section.

Creating Devices from Templates

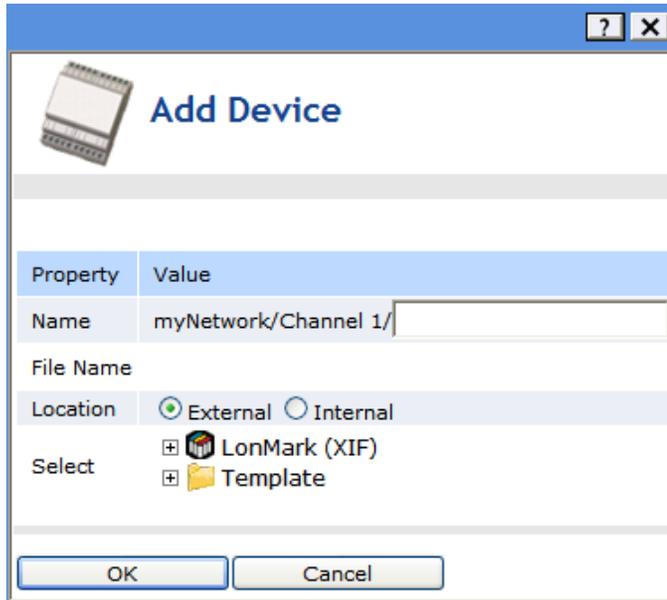
After you create a device template, you can use it to add new devices to the network in the SmartServer tree or OpenLNS tree. The new device and its functional blocks will have the same driver properties as the template, and the device's data points will have the same configuration and driver properties as the template. You can then further configure the device to meet the needs of the network and even create a new template that has a more specific configuration of that device.

To create a device from a template, follow these steps:

1. If you completed step 1 in the previous *Creating Device Templates* section to automatically install devices created from the device template, logically attach the network interface to the network. To do this, click **Driver**, click the network in the navigation pane, select the **Use Network Interface** check box in the **Setup – LON Network Driver** Web page, and then click **Submit**.
2. In the SmartServer tree, right-click the channel on which the new device is to be attached and then click **Add Device** in the shortcut menu.

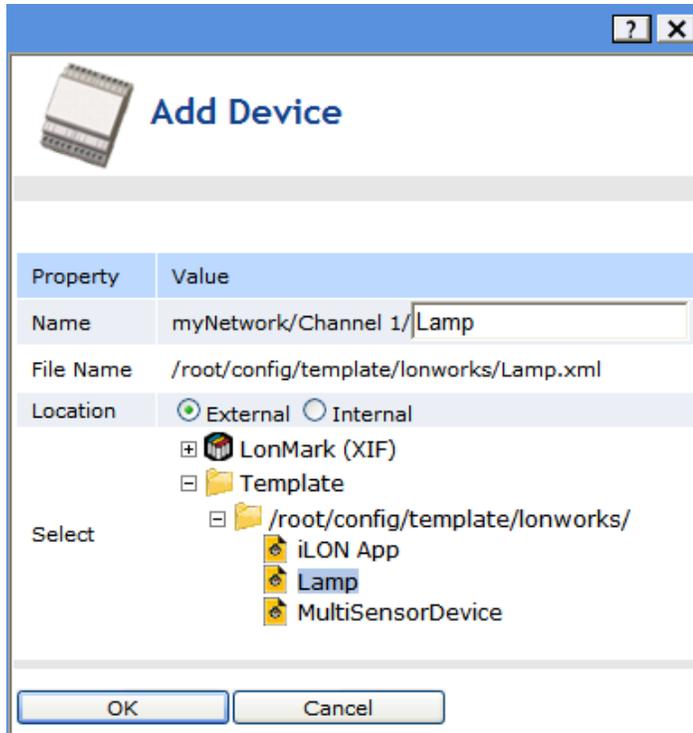


3. The **Add Device** dialog opens



4. In the **Name** property, enter a descriptive name for the device.
5. In the **Location** property, select whether you are creating an external device or an internal device (custom app device or SmartServer) from a template.
6. Expand the **Template** folder to show all the folders in the /config/template directory on the SmartServer flash disk. Expand the folder containing the template to be used to create the device and then click that template.

Note: The SmartServer includes the two pre-defined LONWORKS device templates that are stored in the /config/template/lonworks folder: a digital input (DI10) device and a SmartServer (i.LON App). In addition, it includes six pre-defined Modbus device templates that are stored in the /config/template/modbus folder: ABB_ACH550, BERG_UBN3060, LAE_LCD15, Schneider PM500, Socomec Diris40, and Wago_8DI_8DO_4AI_4AO_8DI_8DO.



7. Click **OK** to return to the SmartServer Web interface.
8. Click **Submit**. The new device and the functional blocks and data points included in the device template are added below the device's parent channel. The default driver properties of the device and its functional blocks match those of the selected template, and the default configuration and driver properties of the device's data points match those of the selected template. You can use these default settings or modify them as necessary.

Note: When you create a device from an LNS device template (**.XML** file), the configuration property values are set to the values saved in the template. This differs from creating a device from a XIF file, which sets the configuration property values to their defaults.

Creating External Data Points from Device Templates

You can copy an external device in the OpenLNS tree and then use a device template to paste specific data points to the SmartServer tree. You can use this feature to automatically create a large number of external data points on the SmartServer. This feature essentially provides the functionality of the i.LON 100 PointFactory Plug-in, which is compatible with the e2 and e3 releases of the i.LON 100 software.

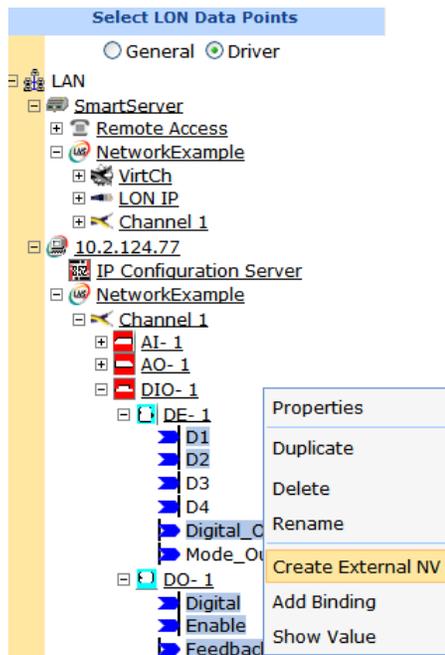
This feature is ideal for larger networks containing multiple devices of a single type. With it, you can use a single copy and paste to add multiple devices with the same program ID to the SmartServer and then select a device template that you previously created for the device. The SmartServer will then automatically copy the data points in the selected device template from the OpenLNS tree to the SmartServer's internal database. You can then use the SmartServer's built-in application and your custom Web page to monitor and control these external data points.

Example: A network is managed with OpenLNS CT or other OpenLNS application that has 100 of the same VAV controllers. Each VAV controller has the same set of six network variables that need to be monitored and controlled with the SmartServer. In this case, you can expand one of the VAV devices in the OpenLNS tree, copy the six desired network variables to the SmartServer, and then create a template of the device in the SmartServer tree. You can then select the 99 other VAV devices in the OpenLNS tree and then copy them to the SmartServer using the VAV device template you created.

You can expand any of the 99 VAV devices in the SmartServer to display the six network variables defined in the device template.

To create external data points on the SmartServer using a device template, follow these steps:

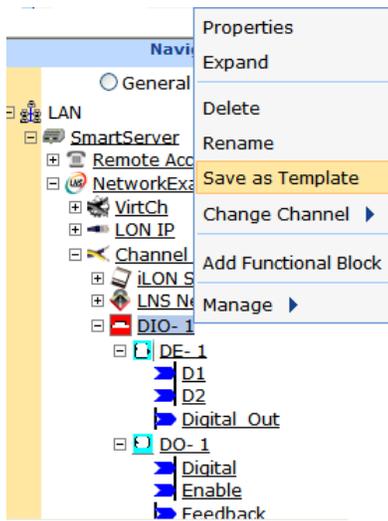
1. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Verify that you have added an OpenLNS Server to the LAN that contains the OpenLNS network database in which the external network variables are stored. In addition, verify that you have synchronized the target SmartServer with the OpenLNS network database containing the external network variables you are copying. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on adding an OpenLNS Server to the LAN and synchronizing the SmartServer to an OpenLNS network database.
3. Expand the LNS Server icon, and then, if prompted, enter the **User Name** and **Password** for logging in to the OpenLNS Server via the Echelon Enterprise Services 2.2. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon in the notification area of your computer, and then click **Options** on the shortcut menu.
4. In the OpenLNS tree, expand the OpenLNS network database, channel, device, and functional block containing the network variable to be copied to the SmartServer, right-click the network variable, and then select **Create External NV** on the shortcut menu. To copy multiple network variables, click one, and then either hold down CTRL and click all others to be copied or hold down SHIFT and select another to select the entire range, right-click one of the selected network variables, and then click **Create External NV** on the shortcut menu.



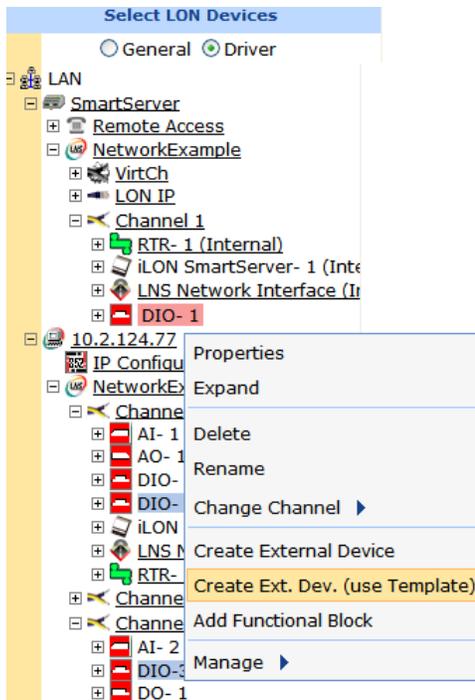
Note: If you have one or more remote SmartServers on the LAN, the **Create External NV** option is not available in the shortcut menu of the network variable in the OpenLNS tree. Instead, right-click the network variable in the OpenLNS tree, select **Copy External NV** on the shortcut menu, right-click any object in the network tree of the target SmartServer, and then click **Paste External** on the shortcut menu.

The data points and their parent channels, devices, and functional blocks are added to the network tree of the target SmartServer. The parent objects are only added if they do not already exist in the internal database of the target SmartServer.

- Click **Submit**.
- In the SmartServer tree, create a template of the external device as described in *Creating Device Templates* previously in this section.



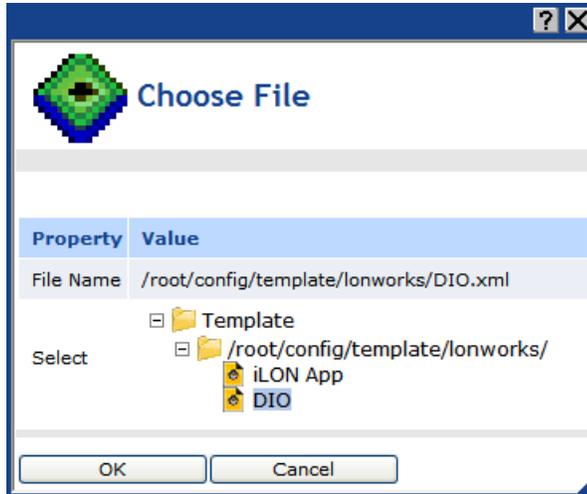
- In the OpenLNS tree, select one or more devices to be copied to the SmartServer. The selected devices must have the same program ID as the external device used for the device template created in step 7. To copy one device, right-click the device and then click **Create Ext. Dev. (use Template)** on the shortcut menu. To copy multiple devices, click one, and then either hold down CTRL and click all others to be copied or hold down SHIFT and select another to select the entire range, right-click one of the selected devices, and then click **Create Ext. Dev. (use Template)** on the shortcut menu.



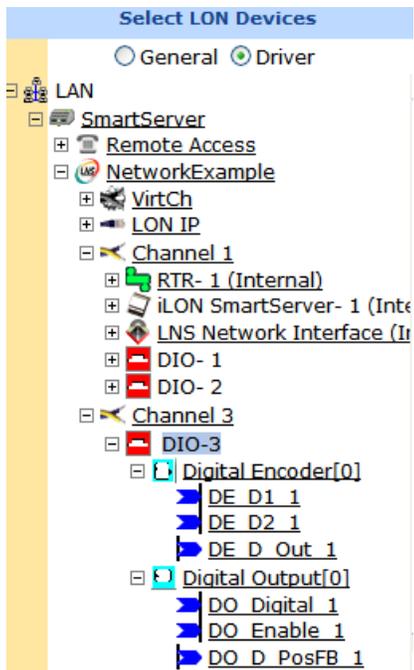
Note: If you have one or more remote SmartServers on the LAN, the **Create Ext. Dev. (use Template)** option is not available in the shortcut menu of the device in the OpenLNS tree. Instead, right-click the device in the OpenLNS tree, select **Copy External Device** on the shortcut

menu, right-click any object in the network tree of the target SmartServer, and then click **Paste Ext. Dev. (use Template)** on the shortcut menu.

8. The **Choose File** dialog opens. In the **Select** property, expand the **Template** folder, expand the folder and any sub-folders containing the device template created in step 7, click the device template, and then click **OK**.



9. Click **Submit**.
10. The devices and the functional blocks and data points in the device template are added to the network tree of the target SmartServer. You can expand one of the copied devices and verify that the functional blocks and data points in the device template appear in the device tree.

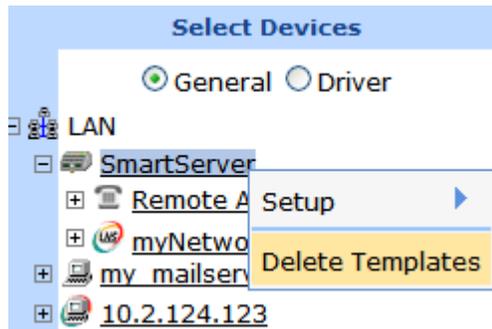


11. You can click a data point in **General** and **Driver** modes and verify that the configuration and LON driver property values are the same as those specified in the device template.

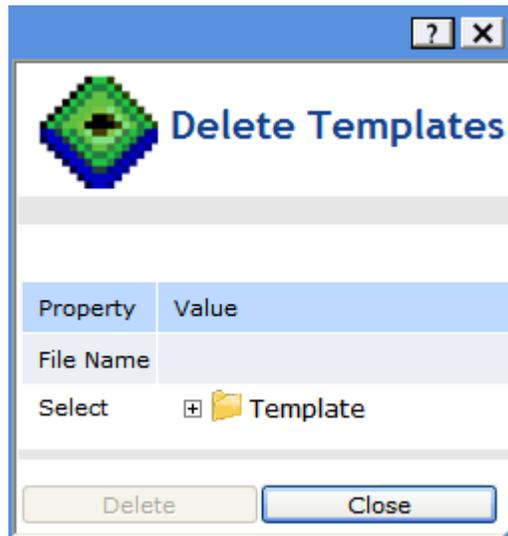
Deleting Templates on a SmartServer

You can remove the templates stored on the SmartServer flash disk or your EES 2.2 computer. This may be useful for maintaining an updated list of active templates or for freeing memory on the SmartServer flash disk. To delete a device template, follow these steps:

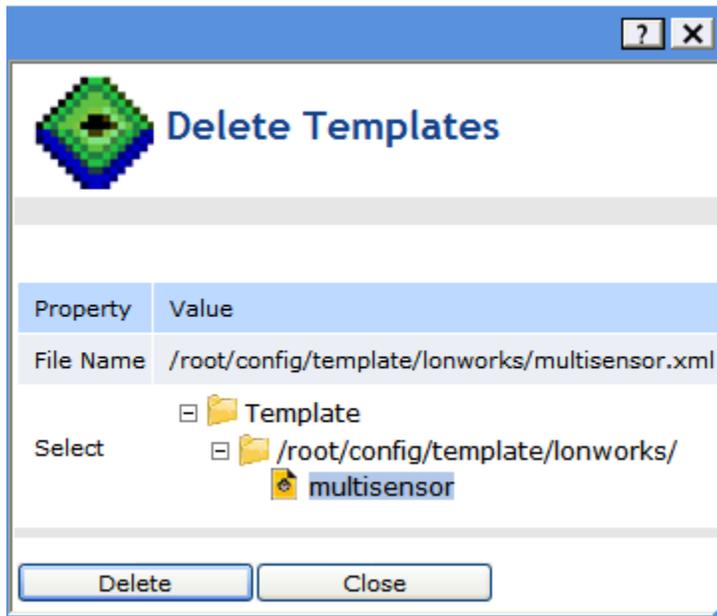
1. Right-click a SmartServer or an OpenLNS Server and select **Delete Templates** on the shortcut menu.



2. The **Delete Templates** dialog opens.



3. Expand the **Template** folder to show all the folders in the **/config/template** directory on the SmartServer flash disk. Expand the folder in which the template to be deleted is stored and then select the template. You can select multiple templates to be deleted by clicking one template and then either holding down CTRL and clicking the other templates to be deleted, or holding down SHIFT and selecting another template to delete the entire range of templates.



4. Click **Delete**. The .XML file documenting the selected device template is removed from the SmartServer flash disk or EES 2.2 computer.
5. Click **Close** to return to the SmartServer Web interface.
6. Click **Submit**.

Duplicating Functional Blocks and Data Points

You can create a new LONWORKS functional block or dynamic data point by duplicating an existing one. The new object will have the same configuration and driver properties as the source.

Duplicating is especially useful for quickly adding pre-configured applications to the SmartServer. In this case, you can use an existing application as a template for creating a new instance of the application. For example, you could add data points to a scheduler, create events in the daily and exception schedules, and then duplicate the Scheduler functional block. The events in the duplicate scheduler will occur at the same time as specified in the source and they will update the same data points. You could then further modify the duplicate scheduler to fit the specific application in which it is being used. This saves you the effort of adding the same data points to multiple schedulers and creating the same events in the daily and exception schedules.

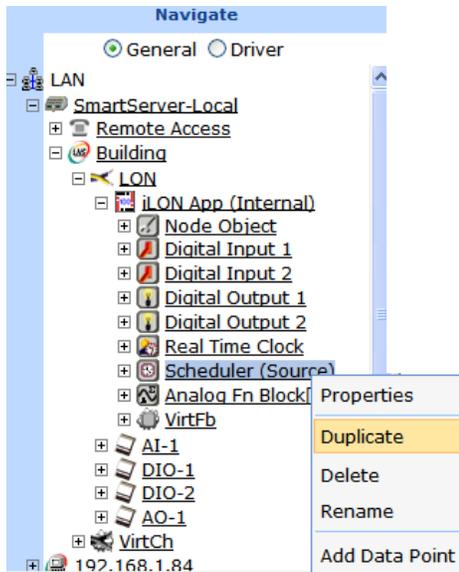
Creating functional blocks and data points from a duplicate can also help expedite the network design and configuration process. For devices with an array of a specific functional block, you can configure one functional block in the array, and then duplicate it to create one or more new instances that have the same configuration as the source functional block.

The following sections describe how to create new functional blocks and dynamic data points by duplicating existing ones.

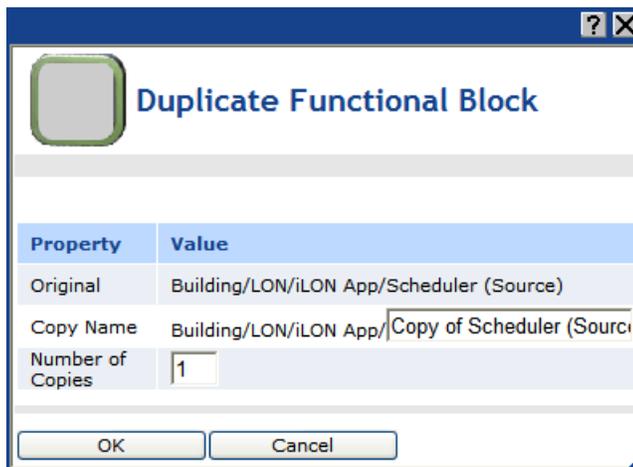
Creating a Duplicate Functional Block

To create a new functional block by duplicating an existing one, follow these steps:

1. Right-click the source functional block from which the copy will be created and then click **Duplicate** on the shortcut menu.



2. The **Duplicate Functional Block** dialog opens.



3. In the **Copy Name** property, enter a descriptive name for the functional block. The default name is **Copy of <original functional block name>**.
4. Select the number of copies of the functional block to be created. The default is **1** copy.
5. Click **OK**.
6. Click **Submit**. The selected number of functional blocks and their static and dynamic data points are added to the bottom of the parent device. If you created more than one functional block copy, an index is appended to the name of the functional block.

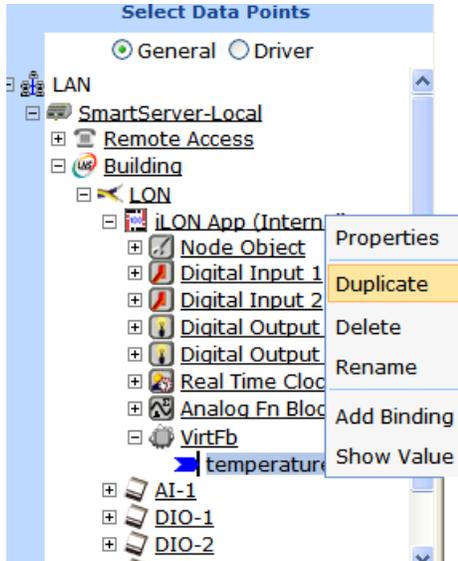
Note: You can only duplicate a static functional block if an instance of the object is available to be created. This means that you may have to delete an existing instance of a static functional block in order to create a new one from a copy. If a static instance is not available, an error message appears above the tree/application frame informing you that insufficient static objects are available, and that no driver copies were created. The SmartServer automatically deletes the duplicate functional block

To delete a static instance of a functional block, click **Settings**. In the **Global Settings** dialog, select **Functional Blocks** in the **Display Hidden** property and then click **Close**. All the functional blocks statically defined for the device in the SmartServer tree are shown. Select one or more static functional blocks, right-click one of the selected functional blocks, select **Delete** on the shortcut menu, and then click **Submit**.

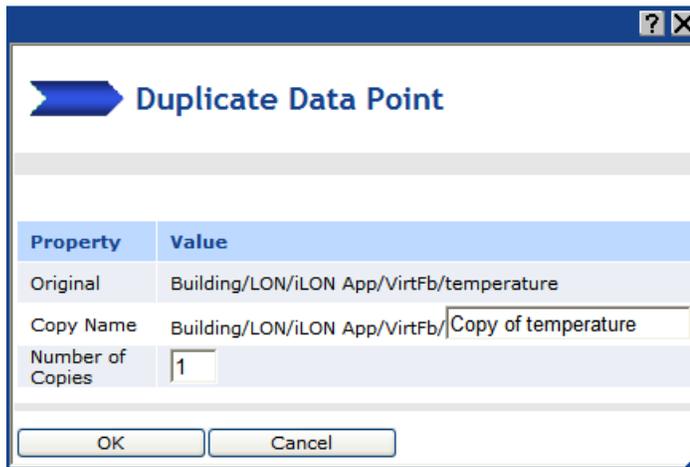
Creating a Duplicate Dynamic Data Point

To create a new dynamic data point by duplicating an existing one, follow these steps:

1. Right-click the source dynamic data point from which the copy will be created and then click **Duplicate** on the shortcut menu.



2. The **Duplicate Data Point** dialog opens.



3. In the **Copy Name** property, enter a descriptive name for the dynamic data point. The default name is **Copy of** <original data point name>.
4. Select the number of copies of the dynamic data point to be created. The default is **1** copy.
5. Click **OK**.
6. Click **Submit**. The selected number of dynamic data points are added to the bottom of the parent functional block. If you created more than one dynamic data point copy, an index is appended to the name of the dynamic data point.

Note: You cannot create duplicates of static data points. If you duplicate a static data point, an error message appears above the tree/application frame informing you that you cannot copy static data points.

Adding Connections

You can connect data points using *Web connections* and *LONWORKS connections*.

- Web connections bind the data points on your local SmartServer to other data points on your local SmartServer and to the data points on remote SmartServers, OpenLNS Servers, and Web Connection Target Servers that you have added to the LAN.
- LONWORKS connections bind the data points in the same network database. You can create LONWORKS connections in both OpenLNS managed networks and standalone networks.

Creating Web Connections

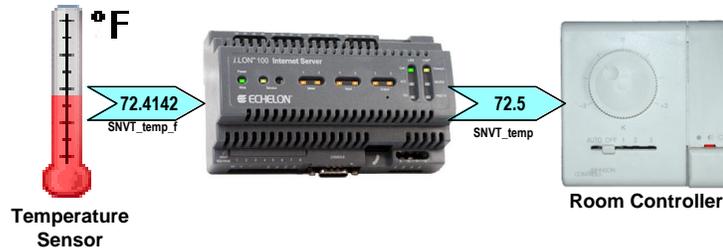
You can create Web connections to bind the data points on your local SmartServer to other data points on your local SmartServer and to the data points on remote SmartServers, OpenLNS Servers, and Web Connection Target Servers that you have added to the LAN. The Web connection will then keep the data points synchronized.

Web connections are independent of LONWORKS domain boundaries. You do not need an OpenLNS Server to create a Web connection between two SmartServers or between a SmartServer and a Web Connection Target server, and SmartServers connected via Web connections do not need to be in the same OpenLNS network database. You do need to add an OpenLNS Server to the LAN before creating Web connections between a SmartServer and an OpenLNS Server.

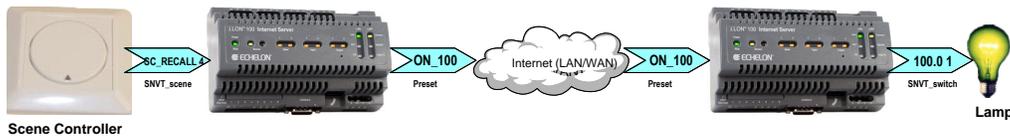
You can create four types of Web connections: internal connections, peer-to-peer connections, enterprise connections, and LNS uplink connections.

- An internal connections is a connection between two data points on a single SmartServer. Internal connections are useful for translating the data between two LONWORKS devices that have incompatible formats, as well as translating data between devices on different buses (LONWORKS, Modbus, and M-Bus).
- A peer-to-peer connection is a connection between two data points on separate SmartServers. Peer-to-peer connections provide an alternative solution to LONWORKS connections over an IP-852 channel for connecting devices over multiple networks; however, peer-to-peer bindings are much slower (40 data point updates per second) than LONWORKS IP-852 connections (1,000 updates per second). To create a peer-to-peer connection, you must first add a remote SmartServer to the LAN. See *Adding a Remote SmartServer to the LAN* in Chapter 3 for how to do this.
- An LNS uplink connection is a connection between a SmartServer and an OpenLNS Server. LNS uplink connections replace the LNS uplink feature that was used in the e3 release of the i.LON 100 server for data point connections between an i.LON server and an OpenLNS Server. To create an LNS uplink connection, you must first add an OpenLNS Server or LNS Server to the LAN. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for how to do this.
- An enterprise connection is a connection between a SmartServer and a Web Connection Target Server (a Web server that can process SOAP requests). Enterprise bindings are useful for sending a data log, an alarm log, an event scheduler log, or any user-defined file to a central enterprise system. To use an enterprise binding, you must first add a Web Connection Target Server to the LAN. See *Adding a Web Connection Target Server to the LAN* in Chapter 3 for how to do this.

Web connections can perform simple translations of scalar data points when the formats of the data points are incompatible. For example, you can create a Web connection with the **SNVT_temp_f** data point of a temperature sensor and the **SNVT_temp** data point of a room controller. The **SNVT_temp_f** uses a floating-point type and the **SNVT_temp** data point uses an integral data type (a signed long). In this case, the Web connection will translate the floating-point value stored in the **SNVT_temp_f** data point to the integral value required by the **SNVT_temp_p** data point. The following example demonstrates a scalar translation performed over an internal binding.

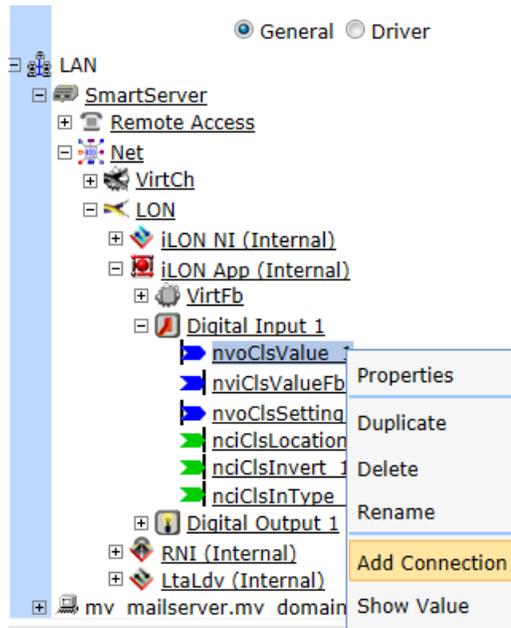


In addition, Web connections can translate structured data points (data points with multiple fields such as **SNVT_switch**) for which presets have been defined. For example, you can define an ON_100 preset for the **SNVT_scene** data point of a scene controller connected to one SmartServer and the **SNVT_switch** data point of a lamp connected to another SmartServer. You then create a Web connection with the data points of these devices. When the **SNVT_scene** data point is set to SC_RECALL 4, the source SmartServer sends the ON_100 preset to the destination SmartServer on the other end of the Web connection over the LAN. The destination SmartServer receives the ON_100 preset and then updates the **SNVT_switch** data point of the lamp to 100.0 1. The following example demonstrates a translation performed using presets over a peer-to-peer binding.



To create a Web connection, follow these steps:

1. Add Web Connection destinations (remote SmartServers, OpenLNS Servers, and Web Connection Target servers) to the LAN with which you want to create a web connection. See *Adding Host Devices* in Chapter 3 for more information on adding host devices to the LAN.
2. From the navigation pane in the left frame of the SmartServer Web interface, right-click a source data point and then click **Add Connection** in the shortcut menu.

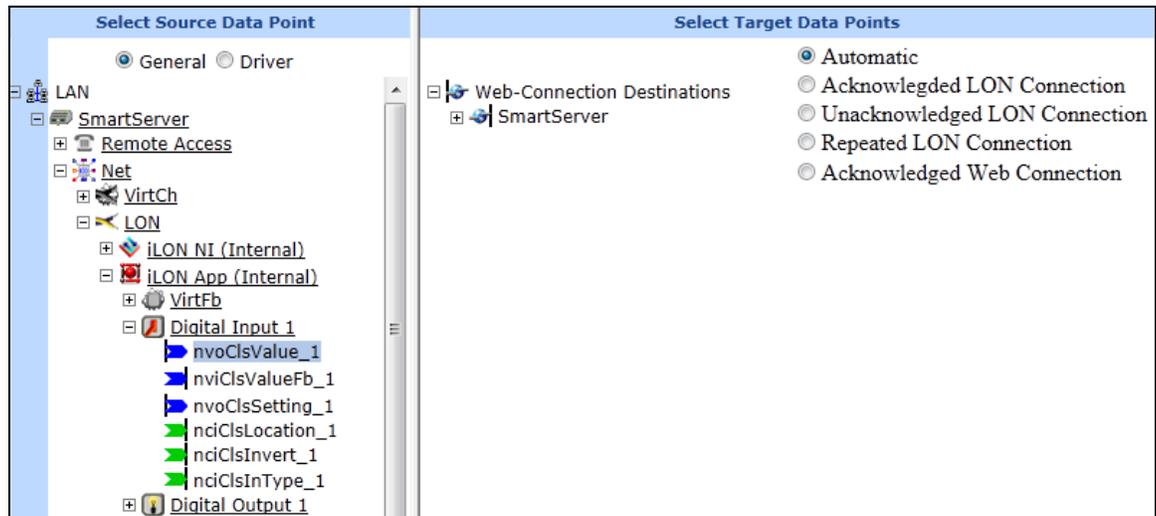


3. The **Configure – Web Connection** Web page opens and the hostnames of the local SmartServer and any remote SmartServers, OpenLNS Servers, and Web Connection Target servers that have been added to the LAN appear in the application frame to the right. The host devices in the right

frame are collectively referred to as *Web-Connection Destinations*. If a Webbinder Destination cannot be reached, a single child node called “Target” appears with the IP address of the SmartServer below the Web-Connection Destinations node.

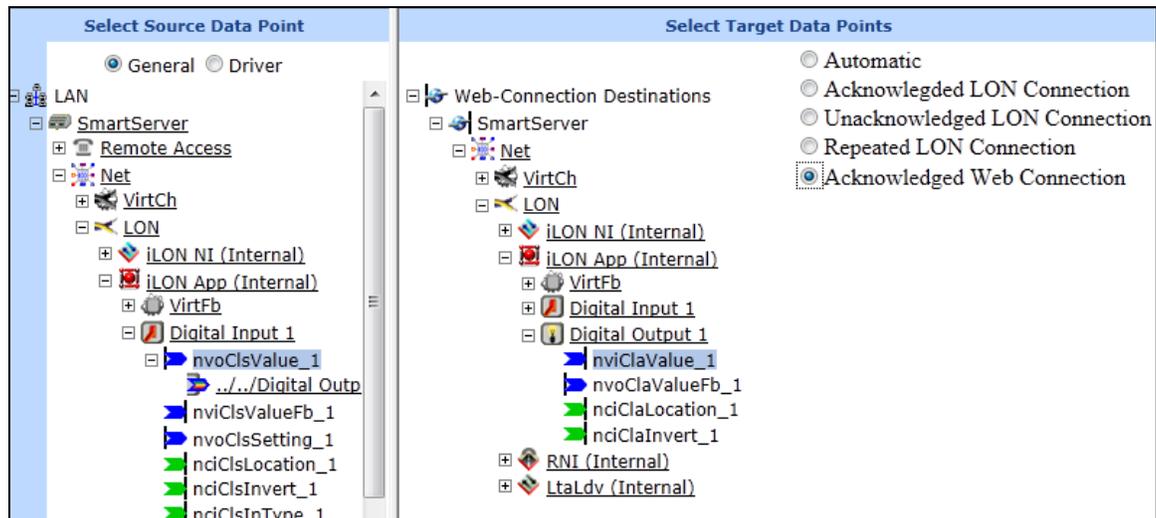
Note: If the IP address of a remote SmartServer is displayed instead of its hostname, the remote SmartServer may have the same hostname as another SmartServer on the LAN. SmartServers on the LAN must have unique hostnames (for example, a remote SmartServer cannot have the same hostname as the local SmartServer). To change the hostname of a SmartServer, do the following:

- For a SmartServer in an LNS managed network, change the SmartServer’s hostname with OpenLNS CT or another OpenLNS tool.
- For a SmartServer in a standalone managed network, change its hostname in the **Setup – Local SmartServer TCP/IP Web** page or its console application.



4. From the Web-Connection Destinations tree on the right frame, expand the Web Connection destination containing the target data points to be connected, expand the network, channel, device and functional block containing the desired target data point, and then click one or more compatible target data points.

References to the target data points (🚩) are added underneath the source data point in the local SmartServer tree in the left frame. Updates to the selected source data point will be propagated to the target data points listed underneath the source data point.



Repeat this step to connect the selected source data point to any other desired compatible target data points.

- If the target data point is not compatible with the source data point a warning message appears. You can delete the connection by right-clicking the reference to the target data point on the SmartServer tree in the left frame and clicking **Delete** on the shortcut menu. See *Deleting Connections* in this section for more information on how to do this.
 - You can also check whether a Web connection is valid by right-clicking the reference to the target data point on the SmartServer tree in the left frame and clicking **Validate** on the shortcut menu. The **Web Connection Validation Results** dialog opens and displays the results. See *Validating Connections* in this section for more information on using this dialog.
5. Select **Acknowledged Web Connection** for the service type. This means that the sending device expects to receive confirmation from the receiving device that a data point update was delivered. The sending application is notified when an update fails, but it is up to the developer of the sending device to handle the notification in the device application.
 6. Click **Submit**. Each time the value of the selected source data point is updated, the SmartServer now sends a request message to the Webbiner Destination. Upon receiving the request message, the Webbiner Destination updates the selected target data points to the value specified for the source data point in the request message.
 7. You can configure the Web connections you have created by clicking **Driver**, and then selecting one or more of the target data points under the source data point in the SmartServer tree. See *Configuring Connections* in this section for more information on how to do this.
 8. If you created an internal connection, peer-to-peer connection, or LNS uplink connection, you can add the source and target data points to the **View – Data Points** Web page and test that the Web connections are updating the data points accordingly.

If you created an enterprise connection, you can attach a data log, alarm log, event scheduler log, or any user-defined file stored on the SmartServer to the connection. To do this, you right-click the reference to the target data point on the SmartServer tree in the left frame and click **Add Attachment** on the shortcut menu. You can select the file to be attached to the connection in the **Select Attachment File** dialog. See *Adding File Attachments* in this section for more information on how to do this.

Note: If multiple source data points of Web connections use different dial-up connections, you must ensure that the source data points are not updated so frequently that the first PPP connection is never dropped. If data is being sent over a dial-up connection at a faster rate than the timeout for the connection, the connection will never be dropped, and a new connection can never be made. This can result in a situation in which the SmartServer will be unable to update a Web connection over a second dial-up connection. See *Creating Modem Connections* in Chapter 3 for more information on using dial-up connections.

Creating LONWORKS Connections

You can create LONWORKS connections in an LNS managed network or a standalone network to bind the network variables of LONWORKS devices that are in the same network database. Creating LONWORKS connections with the SmartServer is comparable to creating connections with OpenLNS CT. You select a hub network variable in the OpenLNS tree and then select one or compatible target network variables in the same network. Network variables must have the same type to be compatible. Once you create LONWORKS connection, the target data points will receive all updates from the hub (source) in the connection. This process of connecting network variables is called *binding*, and the logical connections are thought of as *virtual wires*.

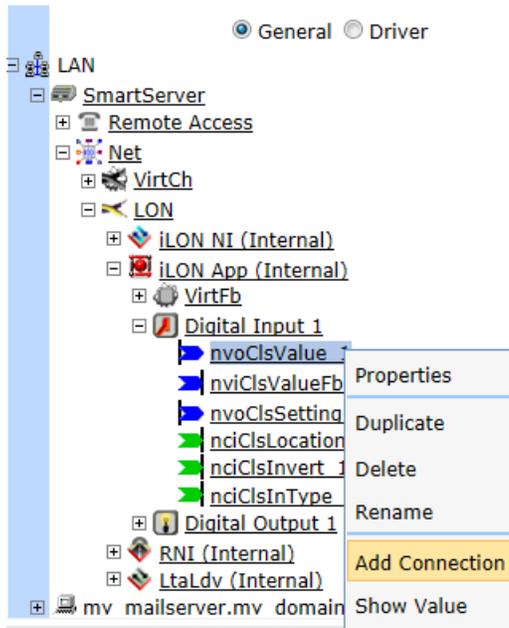
LONWORKS connections created with the SmartServer in LNS mode always use Subnet/Node ID addressing. You can use an OpenLNS application such as OpenLNS CT to select a different addressing mode such as group or broadcast for LONWORKS connections.

LONWORKS connections created in standalone mode are subject to different binding constraints to permit peer-to-peer connections in networks that using meshing. LONWORKS connections created in standalone mode must be defined from by selecting the output network variable on a device, and then one or more input network variables on other devices from the navigation pane. One networks using meshing, devices must include appropriate numbers of alias tables and address table entries. Acknowledged, Unacknowledged, and Repeated service are support if an output network variable is connected to a single input network variable. If an output network variable is connected to more than one input network variables on other devices, the only supported LonTalk services are Repeated and Unacknowledged.

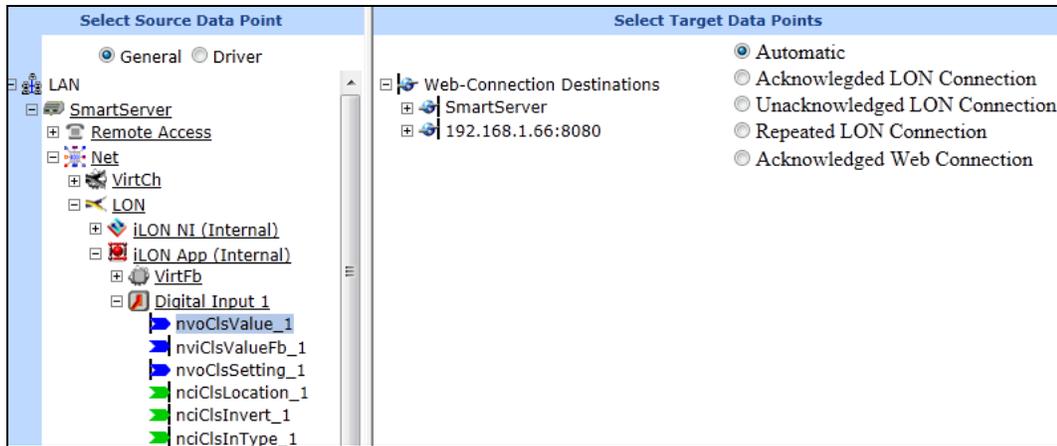
Standalone networks with meshing use group LonTalk addressing to update targets that can be reached directly. If the SmartServer determines some destination devices must be reached via repeating agents, the SmartServer will create special reverse proxy connections to the SmartServer that are repackaged in a new transaction that is broadcast through necessary agents to reach the remaining devices. This can create a flood of power line traffic which must considered when designing such systems. The reverse proxy support limits network variable updates to only include non-idempotent data—that is the updates must be limited to updates that can be received multiple times. For example, an update to set a light to a level is idempotent, whereas an update to increment the level of a light by 20% is not since multiple increments will result in a different level than a single increment.

To create a LONWORKS connection, follow these steps:

1. If your running the SmartServer in an OpenLNS managed network, do the following:
 - a. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
 - b. Verify that an OpenLNS Server has been added to the LAN in order to setup the LNS Proxy Web service on your SmartServer. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for how to add an OpenLNS Server to the LAN and setup the LNS Proxy Web service on your SmartServer.
2. From the SmartServer tree or OpenLNS tree in the left frame of the SmartServer Web interface, right-click a hub (source) network variable and then click **Add Connection** in the shortcut menu.

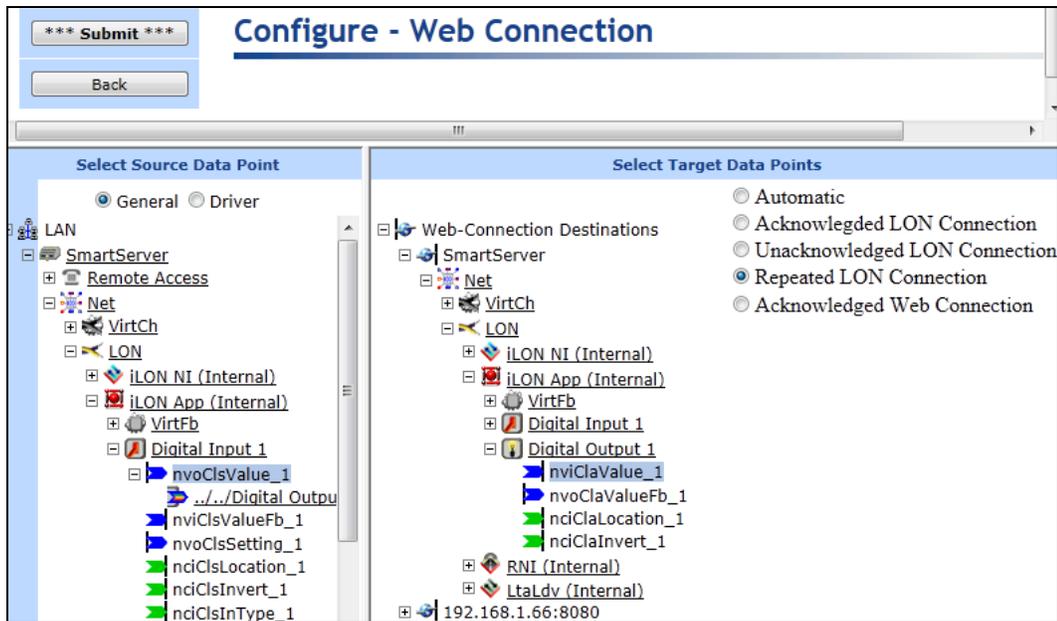


3. The **Configure – Web Connection** Web page opens and the hostname of the SmartServer or OpenLNS Server and the OpenLNS network database in which the hub network variable is stored appear under the Web Connection Destinations icon in the application frame to the right.



- From the Web-Connection Destinations tree on the right frame, expand the network, channel, device and functional block containing the desired target network variables to be connected, and then click one or more compatible target network variables.

References to the target LONWORKS network variables (📌) are added underneath the hub network variables in the tree in the left frame. Updates to the selected hub network variable will be propagated to the target network variables listed underneath the hub.



Repeat this step to connect the selected hub network variable to any other desired compatible target hub network variables.

- If the target network variable is not compatible with the hub network variable a warning message appears. You can delete the connection by right-clicking the reference to the target network variable on the OpenLNS tree in the left frame and clicking **Delete** on the shortcut menu. See *Deleting LONWORKS Connections* in this section for more information on how to do this.
- You can also check whether a LONWORKS connection is valid by right-clicking the reference to the target network variable on the OpenLNS tree in the left frame and clicking **Validate** on the shortcut menu. The **Web Connection Validation Results** dialog opens and displays the results. See *Validating LONWORKS Connections* in this section for more information on using this dialog.

5. Click **Submit**. When an event-driven update defined in the device application occurs, the hub network variable sends an updated value to the selected target network variables.
6. You can configure the LONWORKS connections you have created, including changing the messaging service used for the connection (Acknowledged, Repeated, or Unacknowledged). To do this, you click **Driver**, and then select one or more of the target network variables under the hub network variable in the OpenLNS tree. See *Configuring Connections* in this section for more information on how to do this.
7. You can add the hub and target network variables to the **View – Data Points** Web page and test that the LONWORKS connections are updating the target network variables accordingly.

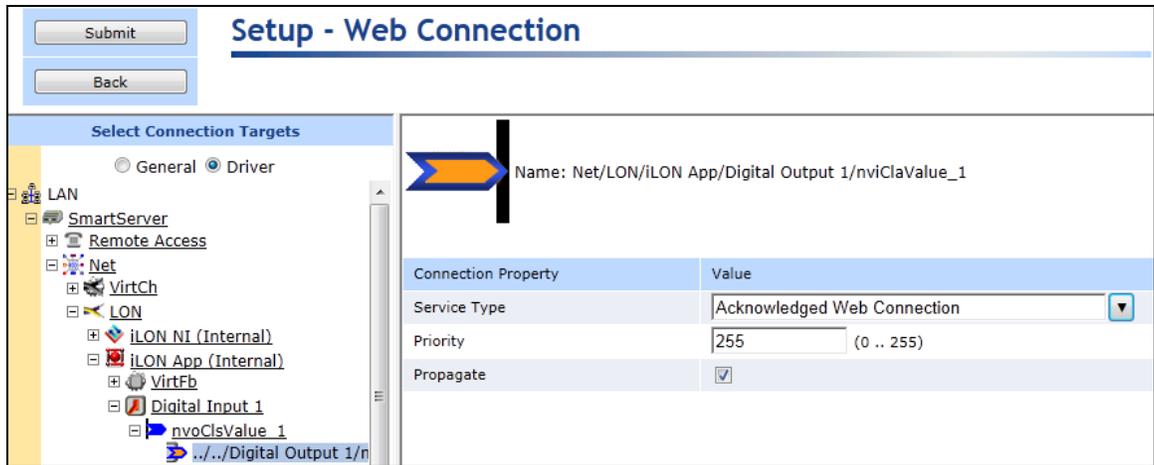
Note: LONWORKS connections created in the OpenLNS tree use the following connection options:

<i>Service Type</i>	Acknowledged (the default), Repeated, or Unacknowledged. See the next section, <i>Configuring LONWORKS Connections</i> , for how to select the service type.
<i>Addressing</i>	Subnet/Node ID.
<i>Priority</i>	Used if hub (source) network variable specifies priority.
<i>Authentication</i>	Used if target network variable has authentication enabled.
<i>Retry Count</i>	Calculated based on topology and service type.
<i>Repeat Count</i>	Calculated based on topology and service type.
<i>Repeat Timer</i>	Calculated based on topology and service type.
<i>Receive Timer</i>	Calculated based on topology and service type.
<i>Transaction Timer</i>	Calculated based on topology and service type.
<i>Broadcast Options</i>	Broadcast addressing is not used.
<i>Alias Options</i>	Network variable aliases are used to resolve selector conflicts.

Configuring Connections

You can configure a connection's service type, change the priority assigned to the connection for writing updated values to the target data point, and control whether updates to the source data point are transmitted to the target data point. To configure a connection, follow these steps:

1. Click **Driver**.
2. Select one or more of the target data points under the source data point in the SmartServer tree. To configure one Web connection, click the target data point in the Web connection to be configured. To configure two or more Web connection, click one target data point and then either hold down CTRL and click all other target data points in the Web connections to be configured or hold down SHIFT and select another target data point to configure the Web connections represented by the entire range of selected target data points.
3. The **Setup – Web Connection** Web page opens.



4. You can configure the following Web connection properties.

Name Displays the network path of the target data point in the following format: `<network>/<channel>/<device>/<functional block>/<data point>`. This field is read-only.

Connection Property

Service Type

Web Connections

Web connections use the **Acknowledged Web Connection** messaging service. This means that the sending device expects to receive confirmation from the receiving device that a data point update was delivered. The sending application is notified when an update fails, but it is up to the developer of the sending device to handle the notification in the device application.

Acknowledged service is very reliable; however, it can create excessive message traffic, especially when a single source or target data point is a member of numerous Web connections.

LONWORKS Connections

Select one of the following messaging service types for a LONWORKS connection. These message service types vary in reliability and resources consumed. Note that all LONWORKS connections created in the OpenLNS tree use subnet/node ID addressing. This means that a message packet travels from the sending device to the destination device using the 2-byte logical address of the destination device in the network.

- **Acknowledged LonConnection.** The sending device expects to receive confirmation from the receiving device or devices that a network variable update was delivered. The sending application is notified when an update fails, but it is up to the developer of the sending device to handle the notification in the device application.

While acknowledged service is very reliable, it can create excessive message traffic, especially for large fan-out or polled fan-in connections. When acknowledged messaging is used, every receiving device has to return an acknowledgment.

Acknowledged messaging can be used with up to 63 receiving devices, but an acknowledged message to 63 devices generates at least 63 acknowledgements—more if any retries are required due to lost

acknowledgements.

You cannot use acknowledged messaging in standalone networks for a connection that includes multiple input network variables. You can use acknowledged messaging in standalone networks with a single output network variable and a single input network variable.

- **Repeated LonConnection.** The sending device sends out a series of network variable updates, but does not expect any confirmation from the receiving device or devices. Repeated service with three repeats has a 99.999% success rate in delivering messages.

Repeated service provides the same probability of message delivery as acknowledged messaging with the same number of retries, with significantly lower network overhead for large multicast fan-out connections.

For example, a repeated message with three retries to 64 devices generates four packets on the network, whereas an acknowledged message requires at least 64 packets.

- **Unacknowledged LonConnection.** The sending device sends out the network variable update only once and does not expect any confirmation from the receiving device. This message service type consumes the least amount of resources, but is the least reliable.

Priority

Displays the priority assigned to the Web connection for writing updated values to the target data point. This value may range from 0 to 255 (highest to lowest priority). The default priority for a target data point is **255**.

You can assign the Web connection a higher priority for updating the data point. The priority you specify must be equal to or higher than the priority used by the last application that updated the data point.

Similarly, if this Web connection updates the target data point, the next application must specify a priority equal to or higher than the one you specified in order to write to the target data point.

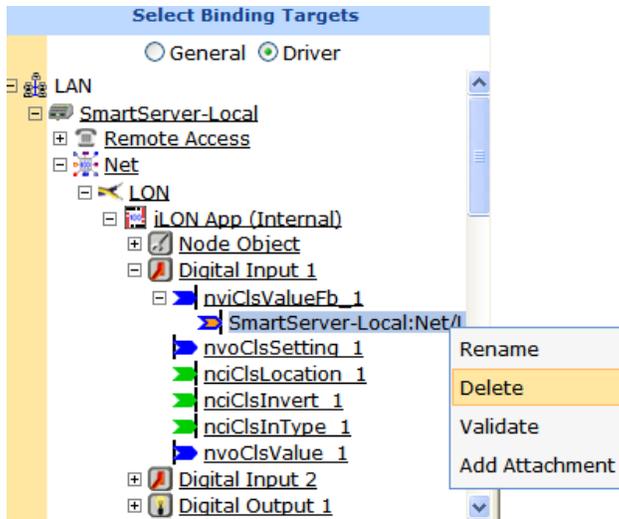
Propagate

Enables updates to the source data point in a Web connection to be transmitted to the target data point. This check box is selected by default. If you clear this check box, updates to the source data point are not transmitted to the target data point.

5. Click **Submit**.

Deleting Connections

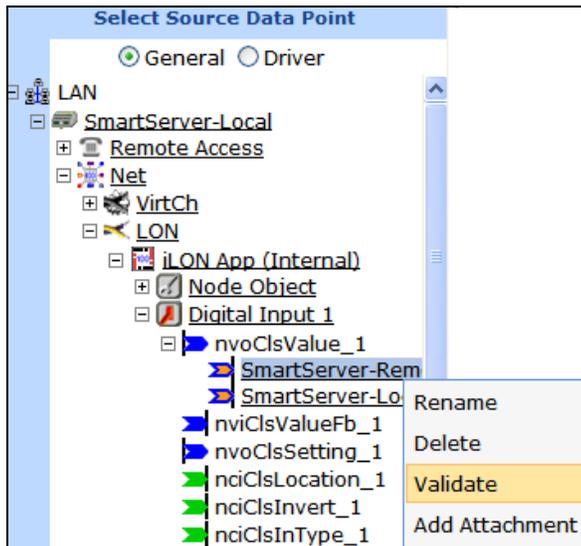
You can delete the connections you have created. To do this, right-click the target data point in the connection and then click **Delete** on the shortcut menu. The reference to the target data point and the connection are deleted. Click **Submit**.



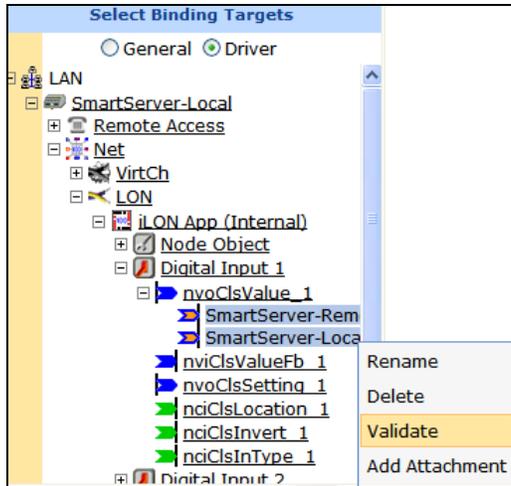
Validating Connections

You can validate the connections you have created. The validation process verifies that the types and formats of the bound data points are compatible. The Web Connection destination must be accessible to perform the validation. To validate a connection, follow these steps:

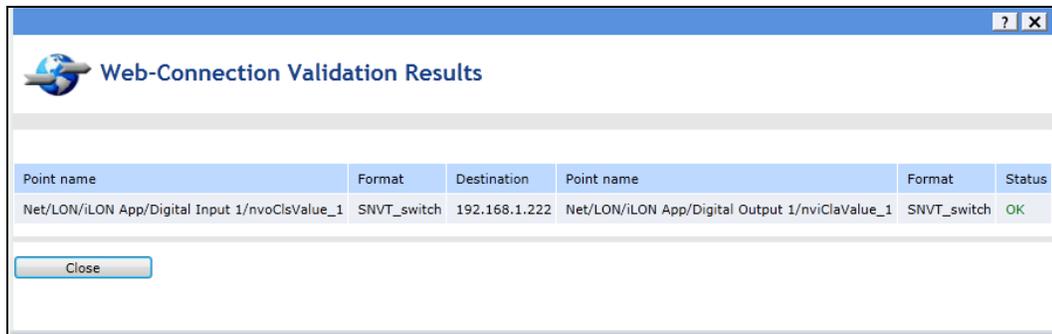
1. Right-click the target data point under the source data point in the SmartServer tree and then click **Validate** on the shortcut menu.



To validate multiple connections, you must first click **Driver** and then select the connections to be validated.



2. The **Web Connection Validation Results** dialog opens.



3. This dialog shows the following properties for all the selected Web connections:

<i>Point Name (Source Data Point)</i>	Displays the name of the source data point in the Web connection in the following format: <network>/<channel>/<device>/<functional block>/<data point>. This is also the location of the data point in the SmartServer tree.
<i>Format (Source Data Point)</i>	Displays the type and format of the source data point such as SNVT_switch or SNVT_temp_f .
<i>Destination</i>	Displays the IP address of the Webbinder Destination containing the target data point in the Web connection.
<i>Point Name (Target Data Point)</i>	Displays the name of the target data point in the Web connection in the following format: <network>/<channel>/<device>/<functional block>/<data point>.
<i>Format (Target Data Point)</i>	Displays the type and format of the target data point in the Web connection.
<i>Status</i>	Displays the results of the validation tests, which can be one of the following: <ul style="list-style-type: none"> • If the types and formats are compatible, OK is displayed. • If the formats are incompatible, Format Error is displayed.

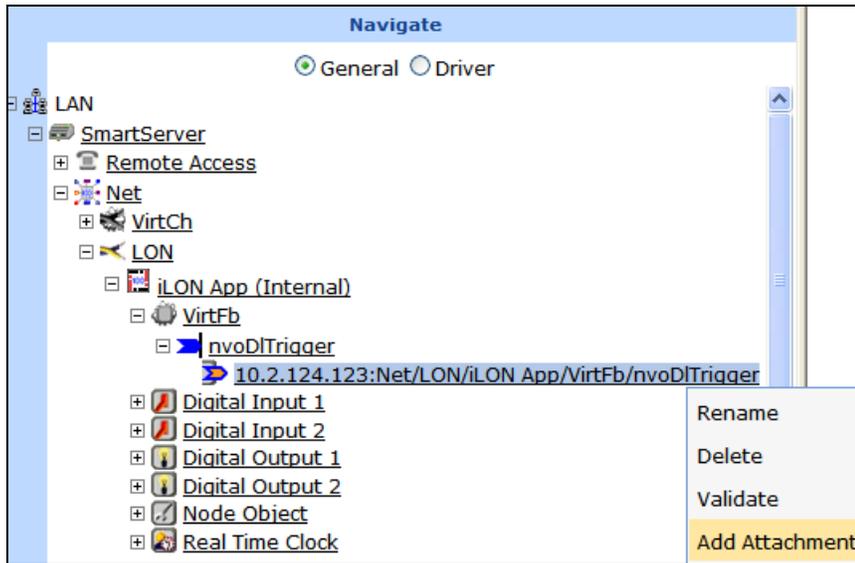
4. Click **Close** to return to the SmartServer Web interface.

Adding File Attachments

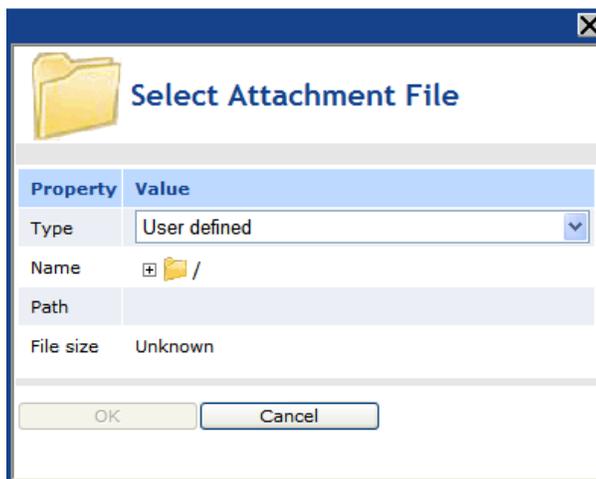
For Web connections between a SmartServer and a Web Connection Target server (a Web server that can process SOAP requests), which are referred to as *enterprise connections*, you can attach a file on your SmartServer to the request messages sent over the Web connection. You can send a data log, an alarm log, an event scheduler log, or any user-defined file stored on the SmartServer. Do not attach files to Web connections if the destination is a SmartServer or an OpenLNS Server (internal, peer-to-peer, and LNS uplink connections). These Web Connection Destinations will remove any attachments they receive via a Web connection.

To add an attachment to an enterprise connection, follow these steps:

1. Under the source data point icon, right click the reference to the target data point in the Web connection, and then click **Add Attachment** on the shortcut menu.

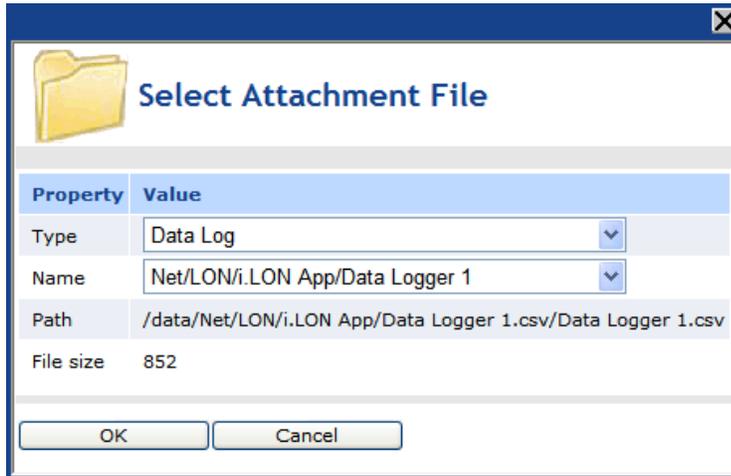


2. The **Select Attachment File** dialog opens.

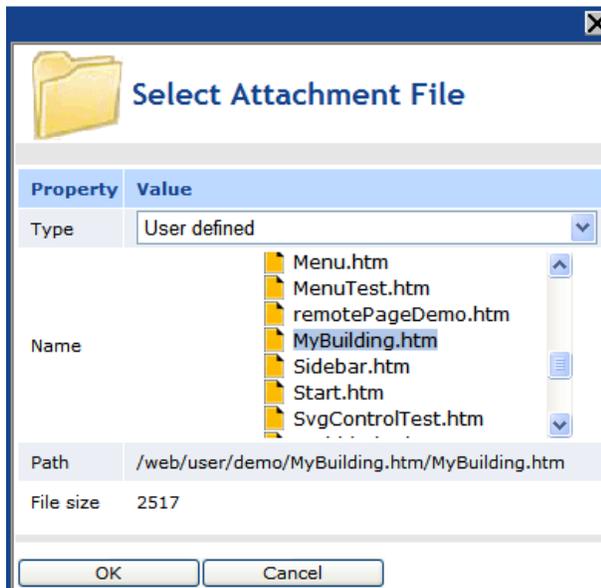


3. In the **Type** property select the type of file to be sent with the message request: **Alarm Log**, **Data Log**, **Event Log**, or **User Defined** (this is the default).
4. In the **Name** property, select the file to be attached.
 - If you select **Alarm Log**, **Data Log**, or **Event Log**, select the name of the log file to be attached. The names displayed are the locations of the logs on the SmartServer tree in the

following format: <network>/<channel>/<device>/<functional block>. The **Path** and **File Size** properties display the location of the selected log file on the root directory of the SmartServer flash disk and its size in KB.



- If you select **User Defined**, browse the root directory of the SmartServer flash disk and select a file to be attached. The **Path** and **File Size** properties display the location of the selected file and its size in KB.

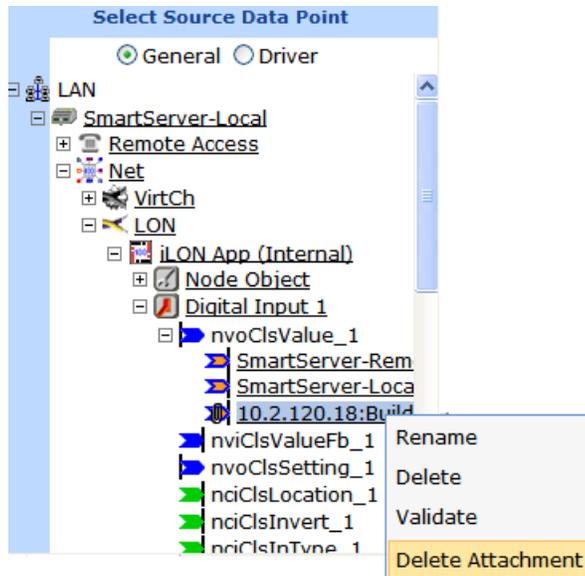


5. Click **OK**. An attachment icon (📎) is added to the target data point icon.
6. Click **Submit**.

Deleting File Attachments

You can delete the files that you have attached to an enterprise connection. To do this, follow these steps:

1. Right-click the target data point in the Web connection to which a file is attached, and then click **Delete Attachment** on the shortcut menu. The attachment icon is removed from the target data point.



2. Click **Submit**. The attachment to the enterprise connection is deleted.

Retrieving File Attachments

For sending file attachments, the Web Connection application on the SmartServer follows the Direct Internet Message Encapsulation (DIME) protocol specification, which is supported by Microsoft IIS with .NET V1.1 and WSE (Web Services Enhancements) 2.0.

DIME is a binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct. Each payload is described by a type, a length, and an optional identifier:

- Both URIs and MIME media type constructs are supported as type identifiers.
- The payload length is an integer indicating the number of octets of the payload.
- The optional payload identifier is a URI enabling cross-referencing between payloads.

DIME payloads may include nested DIME messages or chains of linked chunks of unknown length at the time the data is generated. DIME is strictly a message format: it provides no concept of a connection or of a logical circuit, nor does it address head-of-line problems.

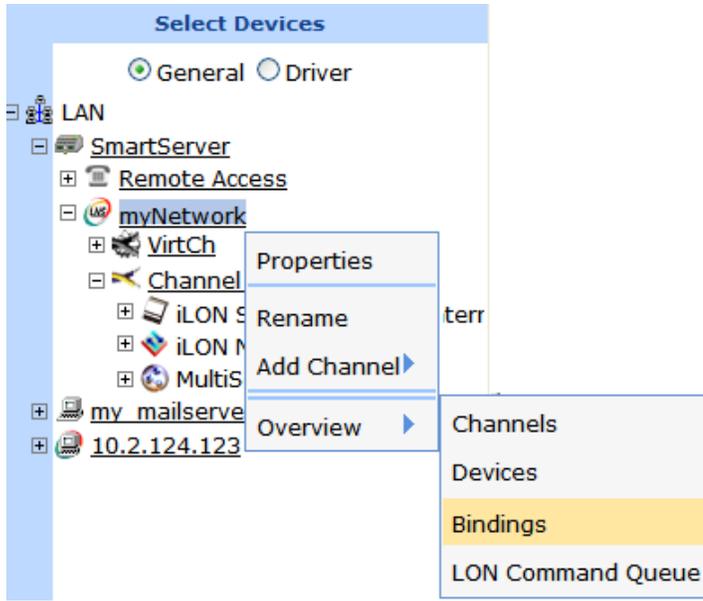
For more details on the DIME protocol specification, including information you will need when extracting file attachments from your Web connection, consult the following Web site:

www.gotdotnet.com/team/xml_wsspecs/dime/draft-nielsen-dime-01.txt.

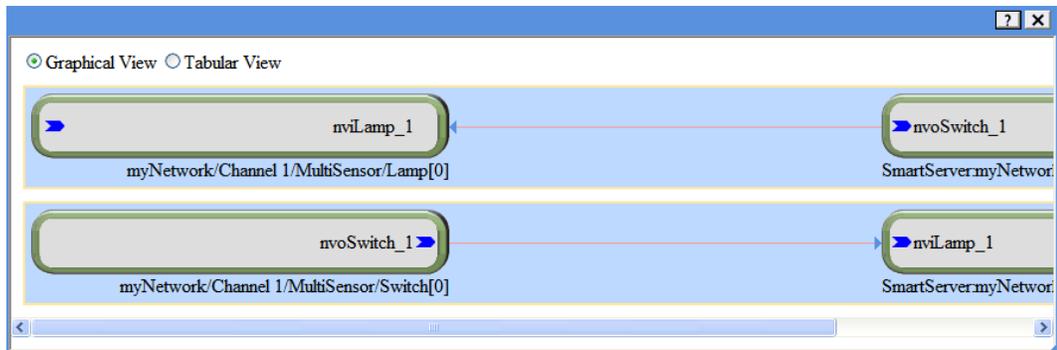
Viewing Connections

You can view all the connections in your in your network, or the connections on a specific channel, device, or functional block in a single graph or table. To do this, follow these steps:

1. Right-click a network, channel, device, or functional block in the SmartServer tree, point to **Overview**, and then click **Connections** in the shortcut menu.



2. The SmartServer gets all the Web connections on the subject network, channel, device, or functional block. This process may take a few minutes depending on the number of Web connections being collected.
3. A dialog opens graphically displaying all the functional blocks containing connected data points on the subject network, channel, device, or functional block. The functional blocks containing the source data points in the connections are displayed on the left side, and the functional blocks containing the target data points are displayed on the right. Multiple connections within single functional blocks are represented with different colors.



4. Select **Graphical View** to graphically display all the functional blocks containing connected data points. The functional blocks containing the source data points in the connections are displayed on the left side, and the functional blocks containing the target data points are displayed on the right. Multiple connections within single functional blocks are represented with different colors.

You can click a data point in this view to select it in the navigation pane on the left side of the SmartServer Web interface (provided that it is currently displayed in the navigation pane).

5. Select **Tabular View** to list all the connected source and target data points in a table. You can click a network variable to select it in the navigation pane (provided that it is currently displayed in the navigation pane).

Incoming	Point of Reference	Outgoing
../Switch[0]/nvoSwitch_1	myNetwork/Channel 1/MultiSensor/Lamp[0]/nviLamp_1	
	myNetwork/Channel 1/MultiSensor/Switch[0]/nvoSwitch_1	../Lamp[0]/nviLamp_1

This table contains the following columns:

- Incoming** Lists the names of all the source data points in the connections in the following format: *<functional block>/<data point>*.
- Point of Reference** Lists the names of the source or target data points connected to the data points listed next to them in the **Incoming** or **Outgoing** columns in the following format: *<network>/<channel>/<device>/<functional block>/<data point>*. If there is data point next to the point of reference in the **Incoming** column, then the point of reference is the target data point in the connection. Conversely, if there is a data point next to the point of reference in the **Outgoing** column, then the point of reference is the source data point in the connection.
- Outgoing** Lists the names of all the target data points in the connections in the following format: *<functional block>/<data point>*.

Checking Error Messages and Viewing the System Log

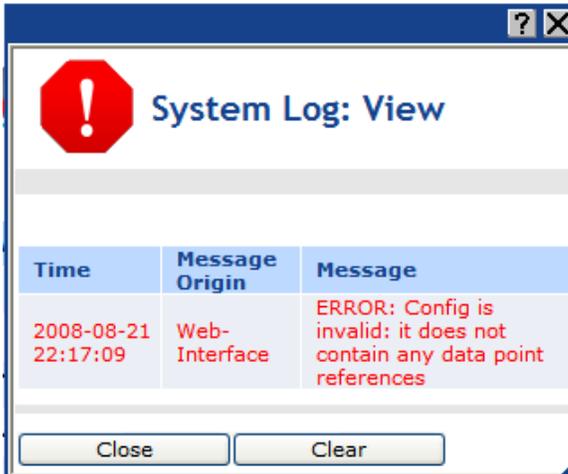
When an error or warning occurs on the SmartServer the SmartServer reports them just above the tree/application frame and records the error or warning in its system log. The error or warning is signified by an alarm bell and an informative message describing the error or warning. For errors, the alarm bell and message text are red; for warnings, they are orange. In addition, information messages that do not indicate any error may appear; these messages are marked with an arrow and black text.

The screenshot shows the SmartServer configuration interface. At the top, there are tabs for SETUP, VIEW, SETTINGS, HELP, and LOG OFF. Below the tabs, there is a "Configure - Data Point" window. On the left side of this window, there is a "Select Data Points" tree view showing a hierarchy: LAN > SmartServer-Local > Remote Access > Building > LON > iLON App (Internal) > Node Object > Digital Input 1 > nvoClsValue_1 > Copy of nvoClsValue_1. The main area of the "Configure - Data Point" window shows the configuration for the selected data point. The Name is "Building/LON/iLON App/Digital Input 1/Copy of nvoClsValue_11" and the Description is "Sensed digital value". Below this, there is a table of Data Point Properties:

Data Point Property	Value
Icon	Dp_Out
Hidden	<input type="checkbox"/>
Alias Name	<input checked="" type="checkbox"/> NVL_nvoClsValue_1
Persistent	<input type="checkbox"/>
Use Default Value	<input type="checkbox"/>
Use Invalid Value	<input type="checkbox"/>

At the top left of the configuration window, there is a red alarm bell icon and the message "ERROR: Cannot copy static Data Point".

You can open the system log and view all errors and warnings that have occurred since the SmartServer was last rebooted. To do this, click **View** and then **System Log**, or click the alarm bell or arrow (if visible).



By default, the errors (red) are warnings (orange) are listed in descending chronological order, but you can sort them by clicking a property header. This dialog displays the following properties for each error or warning message recorded by the SmartServer:

<i>Time</i>	A time stamp displaying the date and time when the error or warning was recorded.
<i>Message Origin</i>	The origin of the error or warning, which could be a bus (LON, M-Bus, Modbus, or custom driver), the SmartServer Web interface, the SmartServer system, or a SmartServer application.
<i>Message</i>	A description of the error or message.

Click **Close** to return to the SmartServer Web interface. Click **Clear** to delete all the current messages listed in the system log.

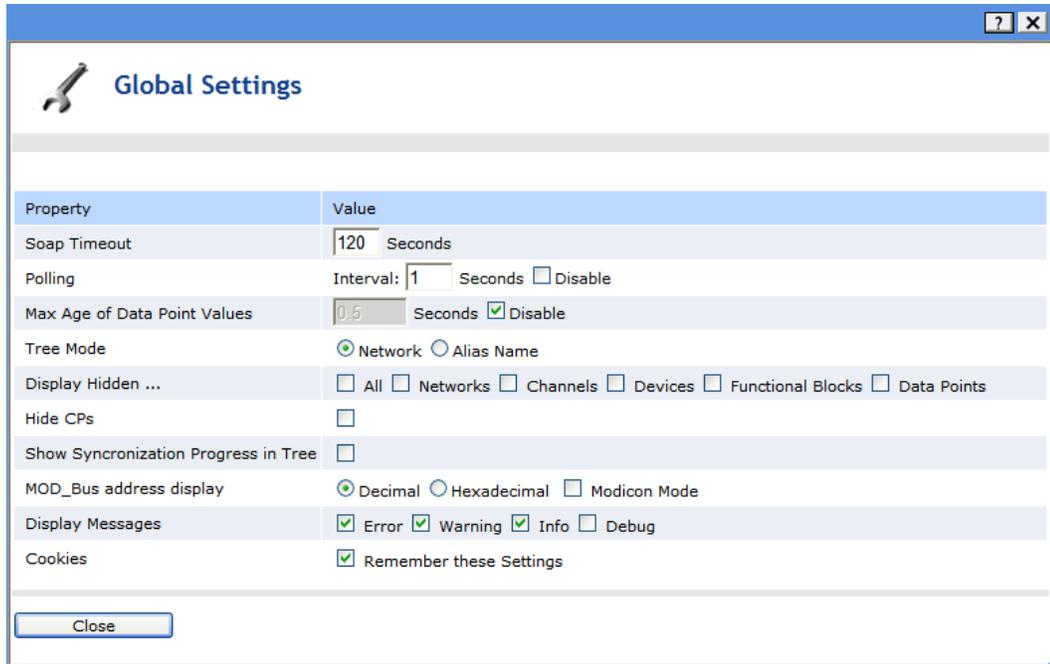
Note: You can change the type of messages logged by the SmartServer (error, warning, information, or debugging) in the **Global Settings** dialog. To open this dialog, click **Settings**. For more information on the **Global Settings** dialog, see the next section, *Configuring Global Settings*.

Configuring Global Settings

You can use this dialog to set the SmartServer's SOAP transaction timeout, set the frequency in which the SmartServer's built-in Web pages receive data point updates from the SmartServer's internal data server, change the organization of the icons in the tree from the current network hierarchy format to the data point location format used for the i.LON 100 e3 server, enable specific types of icons to always be shown in the SmartServer tree, enable a synchronization status bar for the network icon in the navigation pane, and set Modbus address display properties.

To configure the SmartServer's global settings, follow these steps:

1. Click **Settings**. The **Global Settings** dialog opens.



2. Configure the following properties:

SOAP Timeout Set the maximum period of time (in seconds) that the SmartServer waits for a response to a SOAP request before the transaction is canceled and a timeout error is reported. The default timeout is **120** seconds.

Polling Set how frequently (in seconds) the SmartServer's built-in Web pages poll the SmartServer's internal data server for data point updates. The default poll rate is **1** second. Select the **Disable** check box to disable the polling of data points by the SmartServer's built-in Web pages.

You can use this property to adjust the amount of LAN/WAN traffic that is generated by the SmartServer's built-in Web pages.

Max Age of Data Point Values Set the maximum period of time (in seconds) that data point values are cached in the SmartServer's internal data server before it polls the data points and returns updated values to the SmartServer's built-in Web pages. This enables you to control the amount of traffic that is generated on a specific channel by the SmartServer's built-in Web pages. If you enable this option, the default maximum age is **0.5** seconds.

The SmartServer compares the **Maximum Age** value to the amount of time a data point value has been cached in its internal data server, and then does the following:

- If **Maximum Age** is less than the period of time the data point value has been cached, the SmartServer's internal data server polls the data point and returns the updated value to the SmartServer's built-in Web pages.
- If **Maximum Age** is greater than the period of time the data point value has been cached, the SmartServer's internal data server returns the cached value to the SmartServer's built-in Web pages.
- If **Maximum Age** is set to **0**, the SmartServer's internal data server polls the data point and returns the updated value to the SmartServer's built-in Web pages regardless how current the data point is. This is the default value if the Maximum Age option is enabled.

Select the **Disable** check box to have the SmartServer’s internal data server return cached values to the Web pages regardless how old the data point values are. This is the default. If you clear this check box, the default maximum age is **0.5** seconds.

Tree Mode

Select how data points in the navigation pane in the left frame are organized. You have two choices:

- **Network.** Data points are organized by their parent objects using the following network hierarchy: network/channel/device/functional block/data point.
- **Alias Name.** Data points are alphabetized by their alias names, which correspond to their locations in the navigation pane. This is how data points were organized in the e3 release of the i.LON software. You can edit or create the alias name for a data point in its **Configure - Data Point** Web page, which you can access by clicking **General** and then clicking the data point in the tree. If you select this option, the data points are listed in the navigation pane as follows:
 - The data points on the **i.LON App (Internal)** device under the **LON** channel are listed in the tree with the “NVL” prefix.
 - The virtual data points on the **i.LON App (System)** device are listed in the tree with the “iLON System” prefix. In the e3 release of the i.LON 100 server, these data points were referred to as “NVVs”.
 - The data points of the external devices connected to the SmartServer do not have default alias names (unless you migrate a network from an i.LON 100 e3 server to the SmartServer). As a result, external data points are not listed in the navigation pane if this option is selected and alias names have not been created for them. In the e3 release of the i.LON 100 server, these data points were referred to as “NVEs”.

Displays Hidden

Shows all icons in the navigation pane of the selected type even if the **Hidden** property is enabled on individual icons of that type. The check boxes for all the icons are cleared by default.

Hide CPs

Hides all configuration properties currently displayed in the SmartServer tree. To re-display the configuration properties hidden by selecting this option, clear this check box.

Show Synchronization Progress in Tree

Adds a synchronization status bar to the right of the network icon in the SmartServer tree that displays the current ratio of items that have already been synchronized to the total number of items being synchronized (**myNetwork** 235/600). The number of items synchronized increases as the synchronization operations progresses. This check box is cleared by default.

MOD_Bus Address Display

Select the format used to display the logical address of the Modbus devices on the network: **Decimal** or **Hexadecimal**. The default format is **Decimal**.

Select **Modicon Mode** to enable device addressing to follow the Modicon standard, in which the device addresses begin with 1. If this check box is cleared, device addresses begin with 0. This check box is cleared by default.

Display Messages

Select the type of messages displayed in the SmartServer’s system log: **Error**, **Warning**, **Info**, or **Debug**. The **Error**, **Warning**, and **Info** check boxes are selected by default.

Cookies

Select **Remember these Settings** to save all the current settings in the **Global Settings** dialog. The settings will persist through browser refreshes, the closing and re-opening of the browser, and SmartServer reboots.

If you clear **Remember these Settings**, the changes you make to the settings in this dialog are not saved. This is the default.

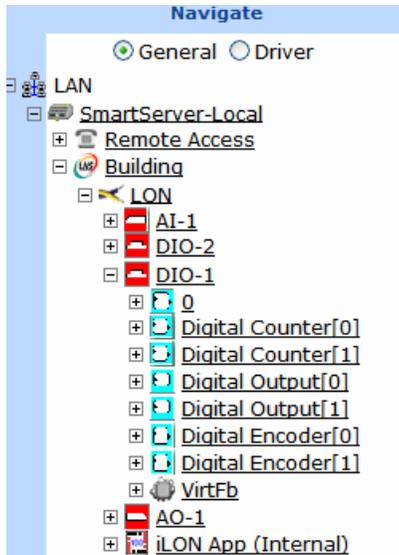
3. Click **Close** to return to the SmartServer Web interface.

Using Custom Device and Functional Block Icons

You can use custom icons (.gif images) to represent your devices and functional blocks in the SmartServer Web interface. Once you upload your custom device and functional blocks icons to the SmartServer flash disk and you create new devices and functional blocks from the SmartServer tree, your custom icons will automatically appear in the SmartServer tree and in the upper left-hand corner of the configuration and driver pages for those devices and functional blocks.

To use custom device and functional block icons in the SmartServer Web interface, follow these steps:

1. Create your custom device and functional blocks icons in **.gif** format. Name your device icons based on their program ID; name your functional blocks based on your company's manufacturer ID.
 - If you are creating a custom device icon, the name of the icon must be *<device program ID>.gif*. For example, the file name for An icon representing the Echelon LonPoint DIO-10v13 Device must be **80000105288A0403.gif**.
 - If you are creating a custom functional block icon, the name of the icon must be *<manufacturer ID>[scope selector]. <functional profile programmatic name>.gif*. For example, the file name for An icon representing the Digital Encoder functional block on the Echelon LonPoint DIO-10v13 Device must be **800001000000000[3].UFPTDigitalEncoder.gif**.
2. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the local SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click Security. The **Setup – Security** Web page opens.
 - b. In the **General** property, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - c. In the **Service** property, verify that the **Enable FTP** check box is selected.
3. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example).
4. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
5. Upload your custom icons to both the **/Web/images/tree** and the **/Web/images/app** folders on the SmartServer flash disk. The **/web/images/tree** folder stores the icons shown in the SmartServer tree. The **/web/images/app** folder stores the icons shown in the upper left-hand corner of an object's configuration and driver Web pages.
6. Create a new device or functional block and verify that your custom icon appears in the SmartServer tree.



7. Click the object and verify that your custom icon appears in the upper left-hand corner of the object's configuration or driver page.



8. You can also implement your custom icons on your existing devices and functional blocks. To do this, follow these steps:
 - a. Click **Driver**.
 - b. Click the device or functional block to be updated with your custom icon in the SmartServer tree. The Setup – Driver Web Page opens for the object.
 - c. In the **Icon** property at the top of the Web page, select your custom icon from the list.
 - d. Click **Submit**. The icon in the SmartServer tree and in the upper left-hand corner of the application frame should be updated with your custom icon.

Using the SmartServer as a Network Management Tool

This chapter describes how to use the SmartServer to design, install, and maintain LONWORKS, M-Bus, and Modbus control networks. It describes how to create and configure networks, channels, devices (application devices and routers), functional blocks, and data points. It explains how to synchronize the SmartServer to an OpenLNS network database. It explains the differences between LNS and standalone network management and how to switch between the two network management service modes. It describes how to use device discovery to automatically acquire the Neuron IDs of the devices on the network. It describes how to use the smart network management feature to install networks. It details how to upgrade, replace, decommission, and test devices with the SmartServer.

Network Management Overview

The SmartServer is a complete network management tool that you can use to design, install, maintain, and monitor/control LONWORKS, M-Bus, and Modbus control networks.

Designing LONWORKS, M-Bus, and Modbus control networks with the SmartServer entails creating, configuring, and maintaining channels, devices, routers, functional blocks, data points, and connections.

You install a network design by commissioning the devices on the network. Commissioning is a process in which you acquire or enter the Neuron ID of the device, and then write network configuration and application configuration data to the devices. Commissioning devices with the SmartServer is simple. You select one or more devices to commission and then use the Smart Network Management feature to have the SmartServer automatically commission the devices, download the application images (if necessary) to the devices, set the devices' applications online, load the device interface (XIF) files, and write the devices' default configuration property values.

After installing a network, you can use the SmartServer to perform network maintenance tasks such as upgrading, replacing, decommissioning, and testing devices, and manually synchronizing the SmartServer to an OpenLNS network database.

You can use the built-in applications on the SmartServer to monitor and control the network. The SmartServer includes applications for data logging, alarming, scheduling, performing arithmetic and logical calculations, and translating data types. To monitor and control a network, you copy data points representing for instance, the state or value of devices, to the various built-in applications on the SmartServer. You can then use the applications to perform monitoring and control tasks including the following: poll and record data point values; set data point value limits that trigger an alarm and e-mail alert when exceeded; and program data point values to be set to a specific value at a specific time.

The subsequent sections describe how to use SmartServer to design, install, and maintain a network. See chapters 6–11 in this guide for how to use the various SmartServer applications to monitor and control a network.

Network Management Scenarios

You can manage a LONWORKS network using the SmartServer Web interface. In this case, you can use the SmartServer as standalone network manager and design, install, and maintain your network in the SmartServer tree, or you can use the LNS Proxy Web service as an OpenLNS network tool and design, install, and maintain your network in the OpenLNS tree as you would with an OpenLNS network tool.

You can also design, install, and maintain a LONWORKS network with OpenLNS CT, LNS Proxy Web service, or another OpenLNS or LNS network tool and then synchronize the SmartServer with the OpenLNS network database. Synchronizing the SmartServer lets you copy network variables in the OpenLNS tree (OpenLNS network database) to the SmartServer tree (internal SmartServer database) so that you can use the SmartServer tree to monitor and control the network. Additionally, you can use the SmartServer tree as an OpenLNS network tool to install and maintain the network, if desired, or you can perform these tasks exclusively with your OpenLNS network tool.

The following sections further describe and illustrate the three ways you can use the SmartServer to manage a LONWORKS network: standalone network manager, standalone OpenLNS network tool, and synchronized OpenLNS tool.

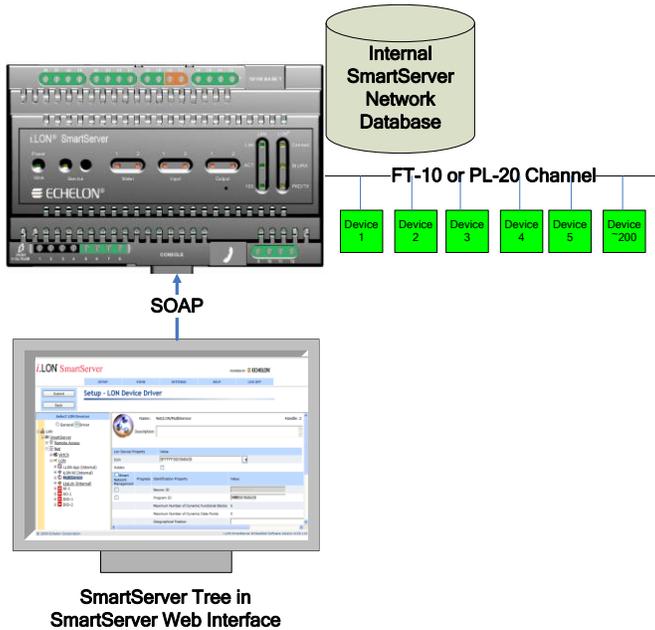
Using the SmartServer as a Standalone Network Manager

You can use the SmartServer as a standalone network manager for designing, installing, and maintaining a small (up to approximately 300 devices), single-channel network that does not require OpenLNS services or connections to other network management tools. In standalone mode, the

SmartServer transmits all network management commands to the devices attached to its channel, and network configuration changes are stored in XML files on the SmartServer's internal database (the **/config/network folder** on the SmartServer flash disk). In standalone mode, the network functions as a master-slave system, where the SmartServer is the master to the slave devices.

Note: For FT-10 networks, you need to attach a physical layer repeater to the network to exceed the 64-device limit posed by the physical channel.

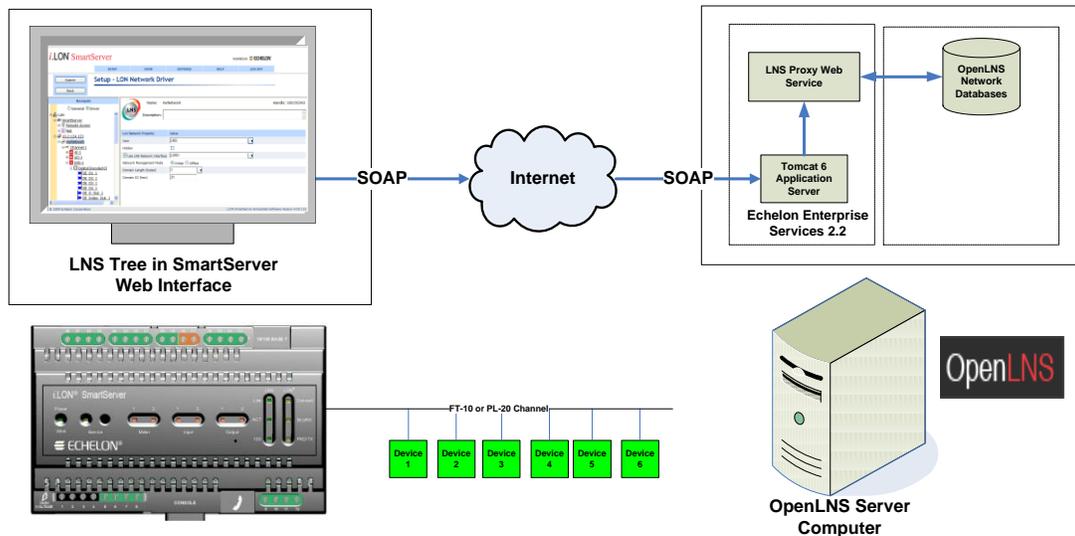
The following graphic demonstrates the SmartServer operating as a standalone network manager:



Using the SmartServer as a Standalone OpenLNS Network Tool

You can use the OpenLNS tree in the SmartServer Web interface as a complete OpenLNS network management tool for designing, installing, and maintaining your network. Using the OpenLNS tree as a network tool is comparable to using OpenLNS CT: you can create new networks, add devices and functional blocks to the network, configure the devices and functional blocks with LNS plug-ins, and then create network variable connections. The OpenLNS tree, however, does not provide the same graphical representation of your network and its data flow as does OpenLNS CT.

When you configure a network in the OpenLNS tree, the LNS Proxy Web service directly propagates the network configuration changes to the OpenLNS network database. The following graphic demonstrates the SmartServer operating as a standalone OpenLNS network tool:



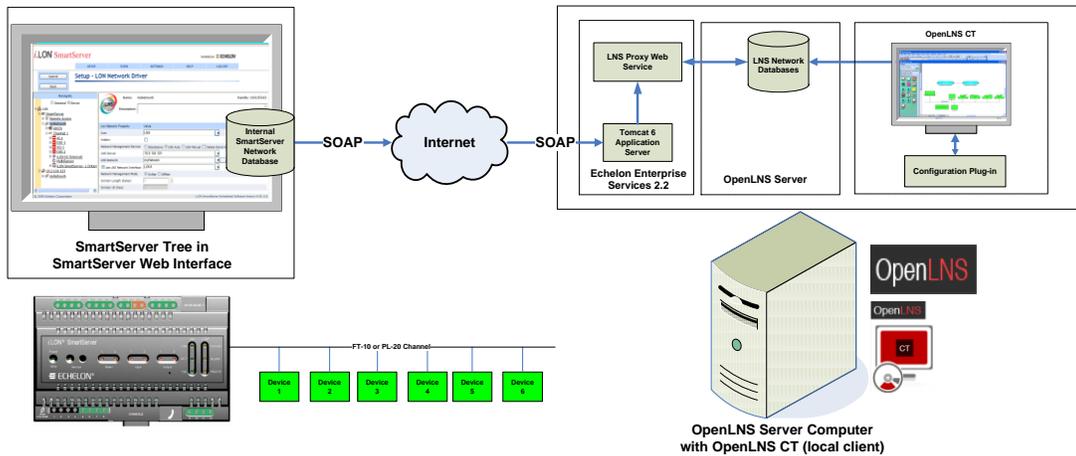
Using the SmartServer as a Synchronized OpenLNS Network Tool

You can design, install, and maintain a LONWORKS network with OpenLNS CT, LNS Proxy Web service, or another OpenLNS or LNS network tool and then synchronize the SmartServer with the OpenLNS network database. This lets you copy network variables in the OpenLNS network database to the SmartServer's internal database so that you can use the SmartServer tree to monitor and control the network (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information on copying data points to the SmartServer).

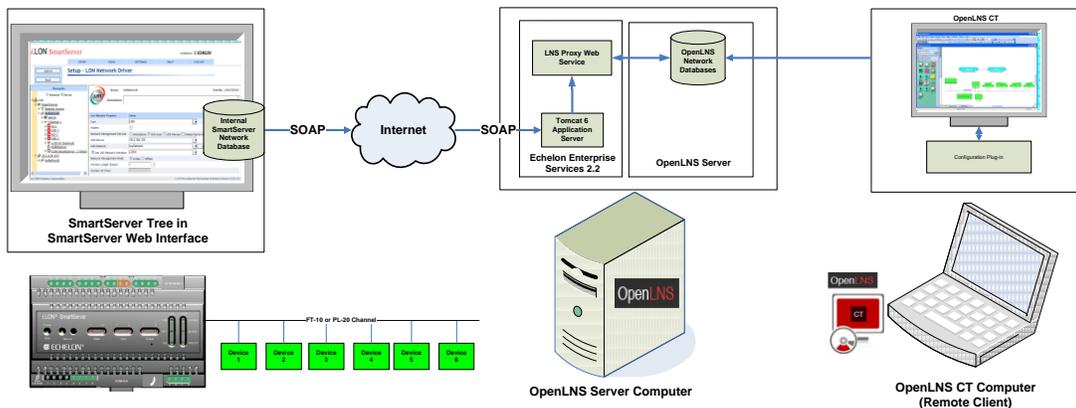
Once you synchronize the SmartServer to an OpenLNS network database, you can also use the SmartServer tree to make ad-hoc changes to the network design, and install and maintain the network using OpenLNS network management services. The SmartServer can automatically propagate the network configuration changes to the OpenLNS network database via the LNS Proxy Web service, or you can manually transmit the changes.

Note: You can only make network configuration changes with one network tool at a time to (for example, OpenLNS CT or the SmartServer). After you complete OpenLNS network management tasks with one network tool, you can then switch to another tool. In addition, if you perform OpenLNS network management tasks with OpenLNS CT or other OpenLNS network tool, you must clear the cache of the LNS Proxy Web service using the EES 2.2 tray tool to ensure that the OpenLNS objects in your network tool maintain synchronization with the LNS Proxy Web service (see Chapter 3 of the *Echelon Enterprise Services 2.2 User's Guide* for how to do this).

The following graphic demonstrates the SmartServer operating while synchronized to an OpenLNS network database:



You can also use OpenLNS CT as a remote OpenLNS client in this scenario as demonstrated in the following graphic:



Designing a LONWORKS Network

Designing a network with the SmartServer Web interface entails creating and configuring your network, and then creating and configuring channels, devices (application devices and routers), functional blocks, data points (network variables and configuration properties), and connections. If you are designing your network with the OpenLNS tree, you can configure your devices and functional blocks with LNS plug-ins.

The following sections describe how to create and configure LonWorks networks, channels, devices, routers, functional blocks, and data points; how to use LNS plug-ins to configure devices and functional blocks; and how to create network variable connections.

Creating and Configuring a LONWORKS Network

You can create a new LONWORKS network from the SmartServer tree or the OpenLNS tree. Doing so creates a new OpenLNS network database in the `/ilon/db` folder on your OpenLNS Server computer that you can then access with another OpenLNS client such as OpenLNS CT. After you create a new network, you can configure it and then add channels, devices, functional blocks, network variables to the network, and bind devices with LONWORKS connections.

If you are operating the SmartServer in LNS mode (**LNS Auto** or **LNS Manual**), you can keep the SmartServer and an OpenLNS network database synchronized. This entails updating the SmartServer with changes made to the OpenLNS network database by other OpenLNS clients such as OpenLNS CT.

Creating LONWORKS Networks from the SmartServer Tree

To create a new LONWORKS network from the SmartServer tree, follow these steps:

1. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Verify that an OpenLNS Server has been added to the LAN in order to setup the LNS Proxy Web service on your SmartServer. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for how to add an OpenLNS Server to the LAN and setup the LNS Proxy Web service on your SmartServer.
3. Click **Driver** and then click the network icon. The **Setup – LON Network Driver** Web page opens.

The screenshot shows the 'Setup - LON Network Driver' web page. On the left is a 'Navigate' tree with 'LAN' expanded, showing 'SmartServer', 'Remote Access', 'Net', 'my_mailserver.my_domain.com', and '10.2.124.77'. The 'Driver' tab is selected. The main area shows 'Name: Net' and 'Handle: 0'. Below is a table of properties:

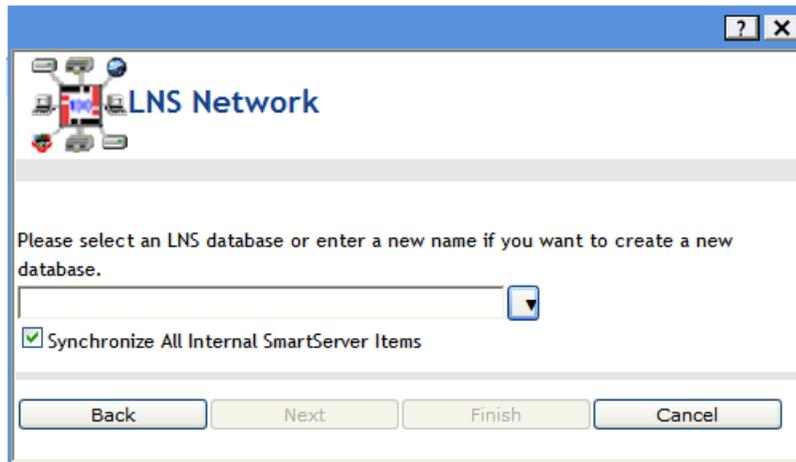
Lon Network Property	Value
Icon	iLonNS
Hidden	<input type="checkbox"/>
Network Management Service	<input type="radio"/> Standalone <input checked="" type="radio"/> LNS Auto <input type="radio"/> LNS Manual <input type="checkbox"/> Delete Items Hidden in LonMaker
LNS Server	[Dropdown menu]
LNS Network	[Dropdown menu]
<input type="checkbox"/> Use LNS Network Interface	[Dropdown menu]

A 'Synchronize' button is located to the right of the 'LNS Network' property.

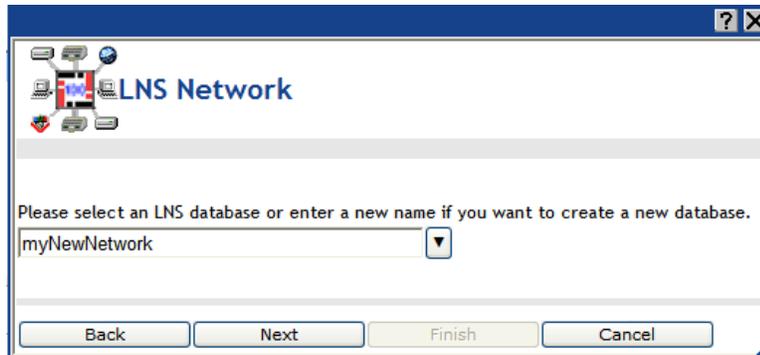
4. Verify that the Network Management Service property is set to LNS Auto or LNS Manual.
5. In the **LNS Server** property, select the OpenLNS Server on the LAN in which the OpenLNS network database is to be stored, if that OpenLNS Server is not already specified.

This screenshot is identical to the previous one, but the 'LNS Server' property in the table is now set to '10.2.124.77'.

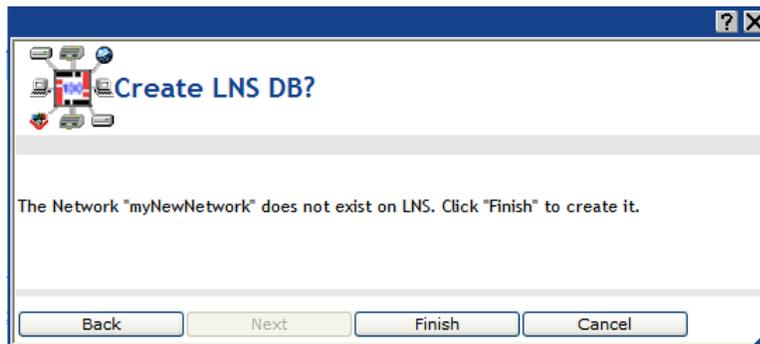
6. If the SmartServer is not currently synchronized to an OpenLNS network database, proceed with the following steps; otherwise, skip to step 8.
 - a. The **LNS Network** dialog opens.



- b. Enter a name (maximum 14 characters) for the OpenLNS network database that is unique to the selected OpenLNS Server (names are case-insensitive).

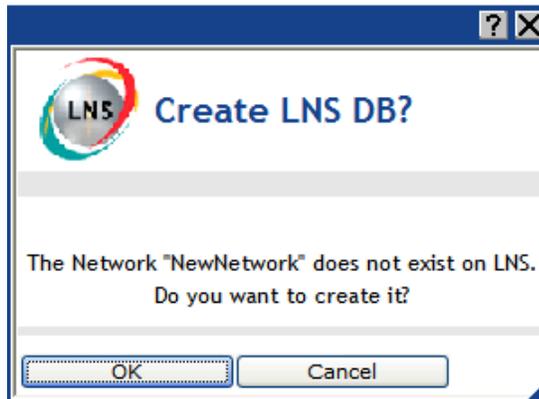


- c. Click **Next**. The **Create LNS DB?** dialog opens.



- d. Click **Finish** to confirm the creation of the new OpenLNS network database and return to the **Setup – LON Network Driver** Web page.
 - e. Click **Submit**.
 - f. The network icon changes to an LNS Server icon and the name of the network changes to the name specified in step b.
7. If the SmartServer is currently synchronized to an OpenLNS network database, follow these steps to create a new OpenLNS network database.
 - a. In the **OpenLNS Network** property, enter a name (maximum 14 characters) for the OpenLNS network database that is unique to the selected OpenLNS Server (names are case-insensitive). Changes made to the SmartServer tree will be transmitted to this OpenLNS network database.

- b. Click **Submit**. A dialog appears prompting you to confirm the creation of the new OpenLNS network database on the OpenLNS Server.

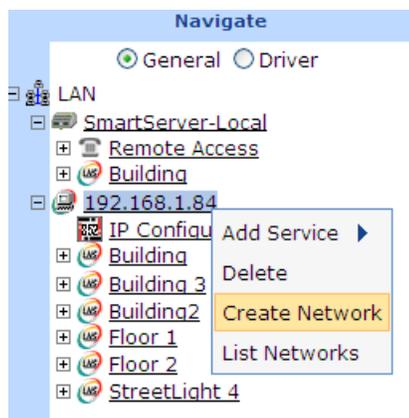


- c. Click **OK**. After the dialog closes, click **Submit**.
 - d. The name of the network changes to the name specified in step a.
8. If the **Network Management Service** property is set to **LNS Auto**, the SmartServer automatically begins synchronization with the new OpenLNS network database. If the **Network Management Service** property is set to **LNS Manual**, manually synchronize the SmartServer to the new OpenLNS network database following the steps described in *Manually Synchronizing the SmartServer to an OpenLNS network database* later in this chapter.

Creating LONWORKS Networks from the OpenLNS Tree

To create a new LONWORKS network from the OpenLNS tree, follow these steps:

1. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Verify that an OpenLNS Server has been added to the LAN in order to setup the LNS Proxy Web service on your SmartServer. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for how to add an OpenLNS Server to the LAN and setup the LNS Proxy Web service on your SmartServer.
3. Right-click the LNS Server icon and then click **Create Network** on the shortcut menu.



4. The **Create Network** dialog opens.



5. Enter the following network properties:

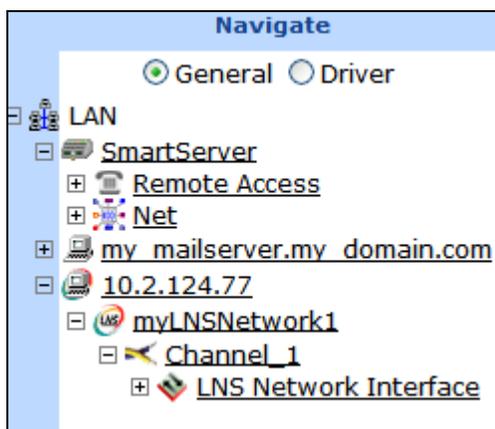
Name Enter a OpenLNS network database name that is unique to both the **Lm/DB** and **ilon/db** folders on your OpenLNS Server (network names are case-insensitive).

Domain Length (bytes) Specify the length (in bytes) of the domain ID. The domain is the top level of the LonTalk domain/subnet/icon addressing hierarchy. The domain length may be 1, 3, or 6 bytes. The default domain length is 3 bytes.

Domain ID (hex) Specify the domain ID in hexadecimal notation. The **Randomize** option is selected by default, and it makes this a read-only field that displays the random domain ID.

To specify a domain ID, clear the **Randomize** option and then enter the domain ID. If you enter an ID that has fewer bytes than that specified in the **Domain Length** box, the domain ID will be padded with leading zeroes.

6. Click **OK**. The network is added to the bottom of its parent LNS Server icon. You can expand the network and observe that a **Channel_1** has automatically been added below the network icon, and you can then expand **Channel_1** and observe that an **OpenLNS Network Interface** has automatically been added to it.



7. Click **Submit**.

To delete a OpenLNS network database in the OpenLNS tree, right-click the OpenLNS network database to be deleted, click **Delete** on the shortcut menu, click **OK** in the dialog that opens to confirm the deletion of the OpenLNS network database, and then click **Submit**. The OpenLNS network database is permanently removed from the OpenLNS Server and it is no longer available.

Configuring a LONWORKS Network

You can use the Driver properties to change the network management service, change the network management mode, select an OpenLNS network database to which the devices on the target SmartServer are synchronized, and modify the domain ID or length of the network. To configure the LONWORKS network driver properties, follow these steps:

1. Click a network icon or an OpenLNS network database icon in the SmartServer tree or the OpenLNS tree.
2. Click **Driver**. The **Setup – LON Network Driver** Web page opens.

3. Configure the following network driver properties:

<i>Name</i>	Displays the name of the network. This field is read-only.
<i>Handle</i>	Displays the handle of the network assigned by the OpenLNS Server. This field is read-only.
<i>Description</i>	Enter an optional description of the network. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Lon Network Property

Icon Displays the icon used to represent the network in the SmartServer or OpenLNS tree and in the application frame. You can change the icon for the network in the SmartServer tree by selecting a different icon and then clicking **Submit**.

You cannot change the icon used for networks in the OpenLNS tree.

Hidden Hides the network in the SmartServer tree or OpenLNS tree and in the application frame. If this network is not actively being used, you can hide it to simplify the web interface.

To show a hidden network icon, click **Settings**. In the **Global Settings** dialog, select the **Networks** check box in the **Display Hidden** property and then click **Close**.

Select the method for transmitting network messages and storing network configuration changes. You have three choices: **Standalone**, **LNS Auto**, or **LNS Manual**.

- **Standalone.** The SmartServer is the exclusive network manager. It transmits all network management commands to the devices attached to its channel, and network configuration changes are stored in XML files on the SmartServer's internal database (the **/config/network** folder on the SmartServer flash disk). In standalone mode, the network functions as a master-slave system, where the SmartServer is the master to the slave devices.

You can use standalone mode to install and operate a small, single-channel network that does not require OpenLNS services. Overall, a network operating in standalone mode has the following limitations:

- Network is limited to a maximum of 300 devices. For FT-10 networks, you need to attach a physical layer repeater to the network to exceed the 64-device limit posed by the physical channel.
- Network is limited to a single channel.
- Network cannot have a router attached to the channel.
- Network does not use OpenLNS management.
- Devices cannot be configured with LNS Plug-ins.
- Network cannot be connected to any other network management tool through the network interface or remote network interface.

Note: Switching a network from **LNS** to **Standalone** mode and clicking **Submit** opens the **Switching to Standalone** dialog. It takes approximately 1 minute for the SmartServer to switch to Standalone mode. When the SmartServer has finished switching to standalone mode, the dialog closes and you can begin using your SmartServer.

See *Using Standalone Mode* in this section for information on the files you need to copy to the SmartServer to install a network in standalone mode.

- **LNS Auto.** Network messages are routed through the selected OpenLNS Server. Network configuration changes are stored in the internal SmartServer database and they are transmitted to the OpenLNS network database specified in the **LNS Network** property. The SmartServer and the devices connected to it communicate in a peer-to-peer manner. This is the default.

Select this mode to have the SmartServer automatically synchronize with the selected OpenLNS network database via the LNS Proxy Web service (you can also manually initiate synchronization by pressing the **Synchronize** button in the **LNS Network** property). In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service. Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default).

See *Automatically Synchronizing the SmartServer to an OpenLNS Network Database* later in this section for more information using **LNS Auto** mode.

- **LNS Manual.** Similar to **LNS Auto** except that you have to manually synchronize the SmartServer with the selected OpenLNS network database. To do this, you press the **Synchronize** button in the **LNS Network** property.

When you press the **Synchronize** button, the SmartServer Web interface requests a list of objects to be synced from the SmartServer via SOAP and forwards the objects returned by the SmartServer to the LNS Proxy Web service. The LNS Proxy Web service returns a set of synced objects to the SmartServer Web interface, which forwards these objects back to the SmartServer.

This mode does not require the SmartServer to access to the LNS Proxy Web service port on the OpenLNS Server computer. Instead, the SmartServer Web interface serves as a proxy between the SmartServer and an OpenLNS Server. Select this mode if a firewall is blocking the SmartServer's access to the LNS Proxy Web service port on the OpenLNS Server computer (port 80 by default).

If the SmartServer is synchronized to an OpenLNS network database, but it will no longer have access to the OpenLNS Server after the network has been installed, you should select this mode. This will prevent the SmartServer from displaying repeated "Cannot Connect to OpenLNS Server" error messages.

See *Manually Synchronizing the SmartServer to an OpenLNS Network Database* later in this section for more information on manually synchronizing the SmartServer to an OpenLNS network database.

You can select the **Delete Items Hidden in LonMaker** check box to hide all functional blocks in the SmartServer tree that do not have corresponding functional block shapes in the LonMaker network drawing and delete their XML configurations from the SmartServer's internal database. This option is cleared by default.

This property is only available for networks in the SmartServer tree.

LNS Server

If you selected **LNS Auto** or **LNS Manual** in the **Network Management Services** property, select the IP address of the OpenLNS or LNS Server to be used for providing network management services.

This property is only available for networks in the SmartServer tree. You cannot change the OpenLNS Server used by an OpenLNS network database in the OpenLNS tree.

LNS Network

If you selected an OpenLNS Server in the **LNS Server** property, select the OpenLNS network database to be updated with the network configuration changes made by the SmartServer. Other OpenLNS clients such as OpenLNS CT can then be synchronized to the updated OpenLNS network database.

Note: If you open the OpenLNS network database with OpenLNS CT, you will observe that the OpenLNS CT drawing includes an additional i.LON Network Interface (i.LON NI) shape and LON IP channel and router shapes if IP-852 routing is activated on your SmartServer. You can delete the LON IP channel and router shapes to simplify your drawing. If

you delete these shapes, the corresponding items in the SmartServer tree are hidden. Do not delete the i.LON NI shape.

Click **Synchronize** to open the **SmartServer Resync** dialog and manually resynchronize the SmartServer with the selected OpenLNS network database. See the *Manually Synchronizing the SmartServer to an OpenLNS Network Database* section later in this chapter for more information.

This property is only available for networks in the SmartServer tree.

Use LNS Network Interface

To use an OpenLNS or LNS network interface, select this option and then select the network interface to be used for communication between the OpenLNS or LNS Server and the network.

If you are designing a network, you can clear this option to specify that the SmartServer is not attached to the network. This is the default.

Network Management Mode

Select when network configuration changes are propagated to devices. You have three choices:

- **OnNet.** Changes are sent immediately to the devices on the network. Select **OnNet** if you are installing an engineered network, or if you are designing and installing an ad-hoc network at the same time.
- **OffNet.** Changes are stored in the network database and then sent to the devices on the network when you place the SmartServer OnNet. Select **OffNet** if you are designing an engineered network.
- **Maintenance.** Same as **OnNet** except that the SmartServer does not send out heartbeat and polling messages. This increases the available bandwidth by freeing up the consumption from checking data point heartbeats, sending poll requests, and receiving poll message responses. Select **Maintenance** to speed up the network commissioning process. This mode is typically required for power line repeating networks.

Domain Length

You can change the length (in bytes) of the domain ID. The domain is the top level of the LonTalk domain/subnet/icon addressing hierarchy. The domain length may be 0, 1, 3, or 6 bytes. The zero-length domain, though, is reserved for the use of the OpenLNS architecture and cannot be used as the system's domain.

This property is not available for the network in the SmartServer tree when the SmartServer is operating in LNS mode (**LNS Auto** or **LNS Manual**).

Domain ID

You can change the domain ID in hexadecimal notation. If you enter an ID that has fewer bytes than that specified in the **Domain Length** box, the domain ID will be padded with leading zeroes.

This property is not available for the network in the SmartServer tree when the SmartServer is operating in LNS mode (**LNS Auto** or **LNS Manual**).

Use Authentication

Enables the SmartServer to send authenticated network management commands such as commissioning to the devices on the network. To enable authentication, select the **Use Authentication** check box, and specify a 6-byte or 12-byte key (12-digit or 24-digit hexadecimal string). To use a random authentication key, click **Generate Random Key**.

When the SmartServer commissions a device, it will set the device's key

to the specified authentication string. All network management commands sent to the device will then use authentication.

4. Click **Submit**.

Using Standalone Mode

You can use the SmartServer in standalone mode to install and operate a small, single-channel network that does not require OpenLNS services or connections to other network management tools.

To install a network with the SmartServer running in standalone mode, you must copy the device interface (XIF) files and resource files to the SmartServer flash disk. In addition, if you plan on upgrading the devices using the SmartServer, you must copy the devices' application image files to the SmartServer flash disk. Each of these files and where to store them on the SmartServer flash disk is described as follows:

- **Device interface (XIF) files.** Define the logical interface to a device. It can either be a device interface file (.xif extension) or a device template (.xml extension). The XIF specifies the number and types of functional blocks, and the number, types, directions, and connection attributes of data points. The program ID field is used as the key to identify each external interface. Each program ID uniquely defines the static portion of the interface.

Upload the XIF files provided by the device manufacturer to the **/LonWorks/import** folder on the SmartServer flash disk.

- **Resource files.** Defines the components of the device interface, including network variable types, configuration property types, format types, and functional profiles implemented by the device application. Resource files allow for the correct formatting of the data generated or configured by the device.

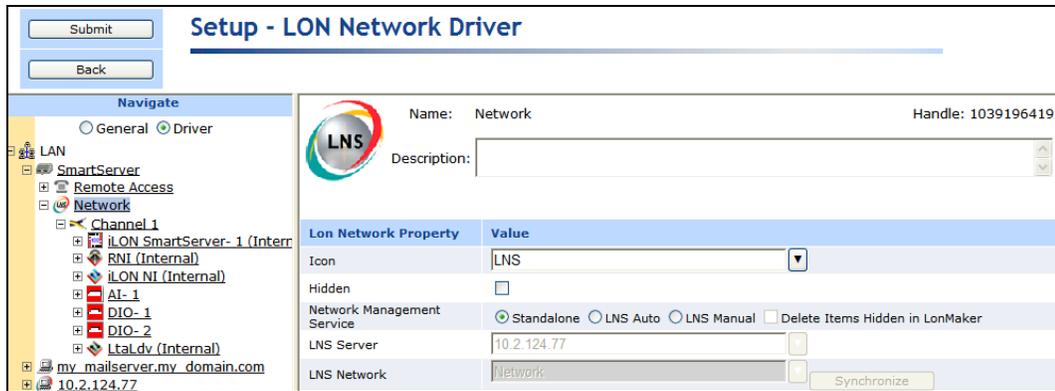
Upload the resource files provided by the device manufacturer to the **/LonWorks/types/user** folder. The standard, echelon, bas_controller, and mbus_integrator catalogs are pre-loaded in the SmartServer **/lonWorks/types** folder.

- **Application image files (.apb extension).** The application image is a file provided by the device manufacturer that determines how a device functions. It consists of the object code generated by the Neuron C compiler and includes other application-specific parameters such as self-identification data and program ID string. You can use the SmartServer to download the latest application image files (.apb extension) to the devices on the network.

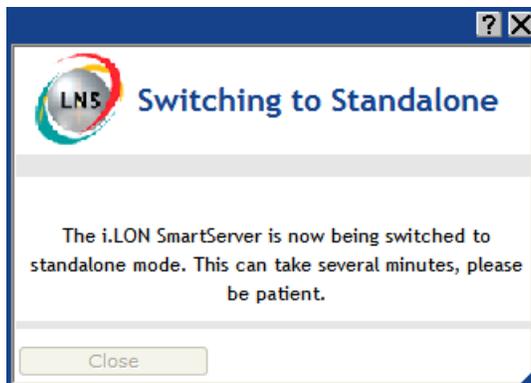
If you plan on upgrading the devices with the latest applications, upload the application image files provided by the device manufacturer to the **/LonWorks/import** folder on the SmartServer flash disk. If the device interface has also changed, also upload the updated XIF files provided by the device manufacturer.

After you are done copying the required resource, XIF, and application image files to the SmartServer, you can set the network to standalone mode, following these steps:

1. Click **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface, and then click the network icon in the SmartServer tree. The **Setup - LON Network Driver** Web page opens.
2. In the **Network Management Service** property, click **Standalone**. The **LNS Server** and **LNS Network** properties become unavailable.



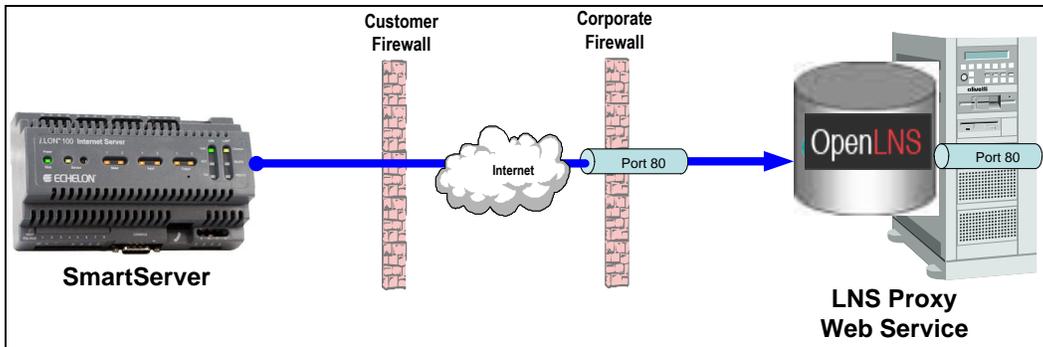
3. Optionally, in the **Domain Length** property, you can enter a different domain ID length, which may be 1, 3, or 6 bytes. The default is **6** bytes. The zero-byte domain is reserved and cannot be used as the network's domain.
4. Optionally, in the **Domain ID** property, you can enter a different domain ID in hexadecimal notation. If you enter an ID that has fewer bytes than that specified in the **Domain Length** box, the domain ID is padded with leading zeroes.
5. Click **Submit**. A dialog appears informing you that the SmartServer is being switched to standalone mode.



It may take up to a few minutes for the SmartServer to switch to standalone mode. When the SmartServer has switched to standalone mode, the dialog closes and you can continue using your SmartServer to manage the network.

Automatically Synchronizing the SmartServer to an OpenLNS network Database

You can synchronize the SmartServer to an OpenLNS network database automatically using **LNS Auto** mode. In **LNS Auto** mode, the SmartServer independently initiates communication with an OpenLNS network database via the LNS Proxy Web service, and directly sends network configuration changes made in the SmartServer tree to the OpenLNS network database. This mode requires the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default) to also be opened on any firewalls blocking the SmartServer's access to the OpenLNS Server computer. The following figure illustrates how the SmartServer communicates with the OpenLNS network databases in **LNS Auto** mode.



To synchronize the SmartServer to an OpenLNS network database using **LNS Auto** mode, follow these steps:

1. Verify that the SmartServer is connected to both the TCP/IP network and the LONWORKS network.
2. Commission the SmartServer with OpenLNS CT, OpenLNS tree, or another OpenLNS or LNS application. For more information on installing the SmartServer, see *Installing the SmartServer with OpenLNS CT* in Chapter 12.
3. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
4. Add an OpenLNS or LNS Server to the LAN. This OpenLNS Server must contain the OpenLNS network database in which the SmartServer was commissioned in step 2. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on how to do this.
5. Click **Driver** at the top of the navigation pane on the left side of the SmartServer Web interface, and then click the **Net** network near the top of the SmartServer tree.
6. The **Setup - LON Network Driver** Web page opens.

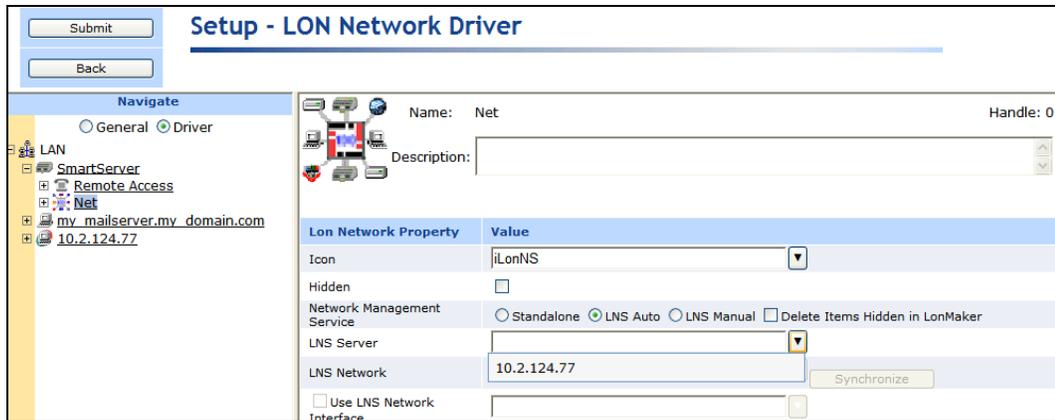
The screenshot shows the 'Setup - LON Network Driver' web interface. On the left is a 'Navigate' pane with a tree view showing 'LAN' > 'SmartServer' > 'Remote Access' > 'Net'. The main area has a 'Name: Net' and 'Handle: 0' field. Below is a table of properties:

Lon Network Property	Value
Icon	iLonNS
Hidden	<input type="checkbox"/>
Network Management Service	<input checked="" type="radio"/> Standalone <input checked="" type="radio"/> LNS Auto <input type="radio"/> LNS Manual <input type="checkbox"/> Delete Items Hidden in LonMaker
LNS Server	[Dropdown menu]
LNS Network	[Text field] <input type="button" value="Synchronize"/>
<input type="checkbox"/> Use LNS Network Interface	[Text field]

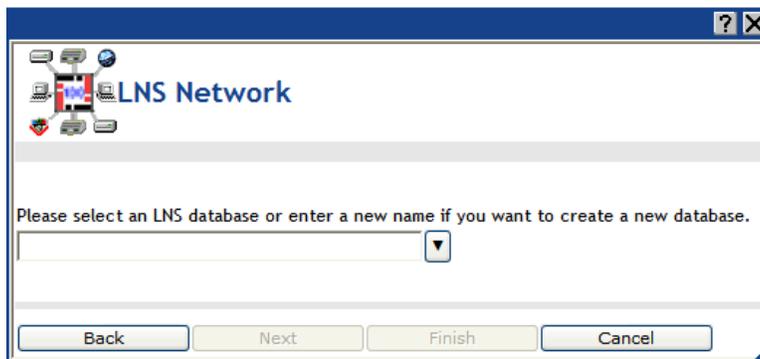
7. In the **Network Management Service** property, accept the default **LNS Auto** option. In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service, and automatically sends network configuration changes made in the SmartServer tree to the OpenLNS network database.

Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default). If a firewall is blocking access to the LNS Proxy Web service, select the **LNS Manual** option.

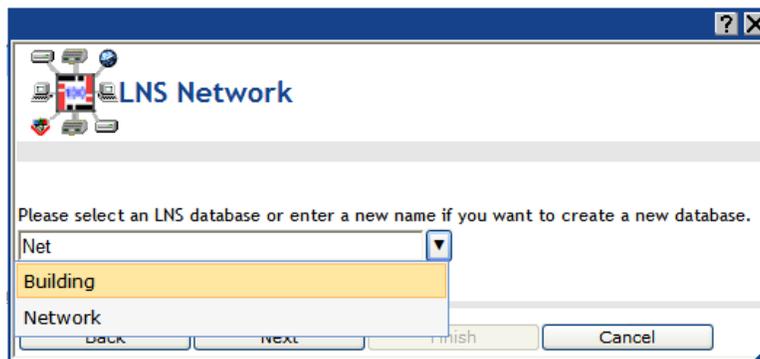
8. In the **LNS Server** property, select the IP address of the OpenLNS Server you added to the LAN in step 4.



9. A dialog for logging in to the LNS Proxy Web service opens. Enter the **User Name** and **Password** used by the SmartServer for logging in to the LNS Proxy Web service and then click **OK**. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon in the notification area of your computer, and then click **Options** on the shortcut menu.
10. The **LNS Network** dialog opens.



11. In the **LNS Network** dialog, select the OpenLNS network database to which the SmartServer is to be synchronized and then click **Finish**.



12. The **Use LNS Network Interface** option is selected and the network interface used for communication between the OpenLNS Server and the network is specified automatically. Accept these defaults if the OpenLNS Server is attached to the physical network and you want the SmartServer to communicate with the devices on the network through the selected network interface.

13. If **Use LNS Network Interface** is selected, the **Network Management Mode** property is set to **OnNet** automatically. This means that network changes are propagated to the network immediately. Click **OffNet** to store network changes in the selected OpenLNS network database and propagate them to the network when you place the SmartServer **OnNet**.

The screenshot shows the 'Setup - LON Network Driver' interface. On the left is a 'Navigate' tree with 'SmartServer' expanded to show 'LON'. The main area has 'Name: Building' and 'Handle: 0'. Below is a table of properties:

Lon Network Property	Value
Icon	LNS
Hidden	<input type="checkbox"/>
Network Management Service	<input checked="" type="radio"/> Standalone <input checked="" type="radio"/> LNS Auto <input type="radio"/> LNS Manual <input type="checkbox"/> Delete Items Hidden in LonMaker
LNS Server	10.2.124.77
LNS Network	Building <input type="button" value="Synchronize"/>
<input checked="" type="checkbox"/> Use LNS Network Interface	X.Default.10.2.124.53
Network Management Mode	<input checked="" type="radio"/> OnNet <input type="radio"/> OffNet
Domain Length (bytes)	1

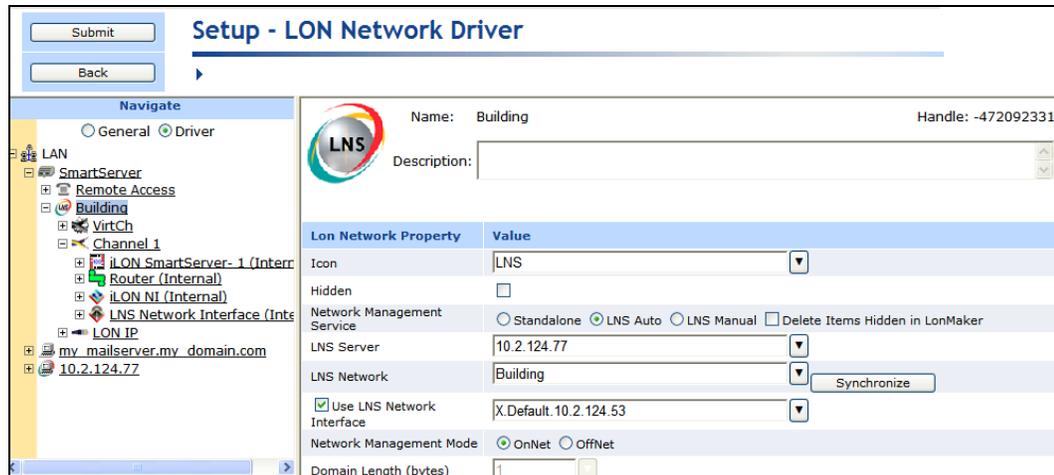
14. Click **Submit**. If you selected **LNS Auto** in the **Network Management Service** property, the name of the network changes to the name of the OpenLNS network database specified in step 11, the network icon changes to an LNS Server icon, and the synchronization automatically begins. During the synchronization process, items in the SmartServer tree that are out of sync with the OpenLNS network database are highlighted yellow. When all the items in the SmartServer tree are synchronized (not highlighted yellow), the synchronization is complete. You can continue to use the SmartServer Web interface during the synchronization.

The screenshot shows the 'Setup - LON Network Driver' interface after clicking 'Submit'. The 'LNS Network' is now 'Building' and the 'Network Management Mode' is 'OnNet'. The 'Handle' is now '-472092331'. The 'LNS Network' icon is now an LNS Server icon. The 'Synchronize' button is visible next to the 'LNS Network' field.

Notes:

- You can view the progress of the synchronization in the navigation pane. To do this, click **Settings** to open the **Global Settings** dialog, and then select the **Show Synchronization Progress in Tree** check box. This adds a synchronization status bar to the right of the network icon in the SmartServer tree that displays the current ratio of items that have already been synchronized to the total number of items being synchronized.
- You can view a log of the current synchronization in the SmartServer's console application. To view the sync log, enter the **trace 2** command. For more information on the SmartServer console application, see Appendix B, *Using the SmartServer Console Application*.

15. If you selected **LNS Manual** in the **Network Management Service** property, manually synchronize the network following the instructions in *Manually Synchronizing the SmartServer to an OpenLNS Network Database* later in this section.
16. After the synchronization, observe the following changes to the SmartServer's App device in the SmartServer tree: the SmartServer's App device is moved to the channel to which it was added in the OpenLNS CT drawing, OpenLNS tree, or other OpenLNS application, (for example, Channel 1); the name of the SmartServer's App device changes to the name of the SmartServer shape in your OpenLNS CT drawing, OpenLNS tree, or other OpenLNS application (for example, iLON SmartServer- 1); and the icon used for the SmartServer's App device in the SmartServer tree changes to a generic device icon.

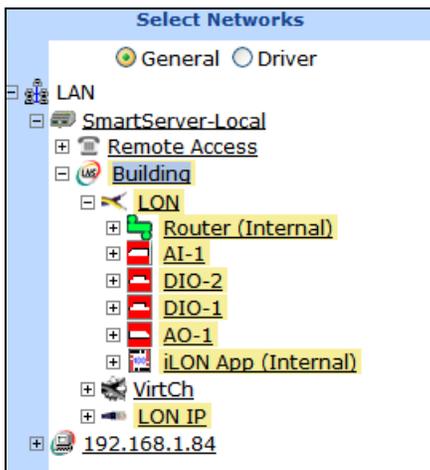
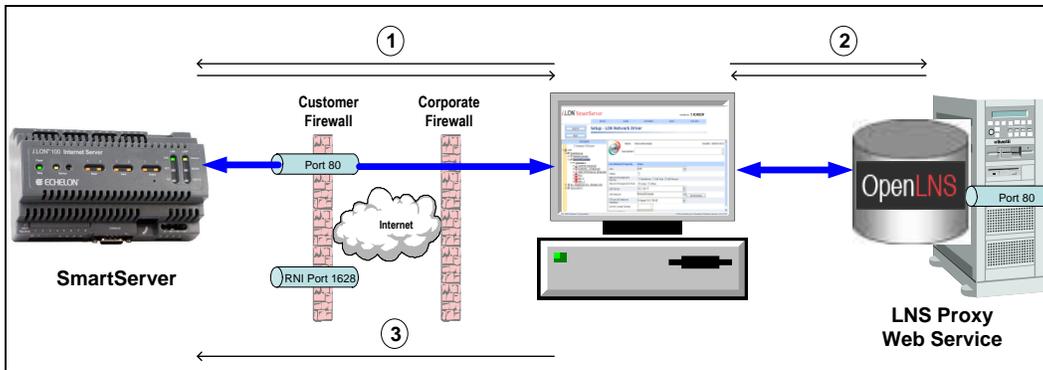


Manually Synchronizing the SmartServer to an OpenLNS Network Database

When a network in the SmartServer tree is using the **LNS Auto** network management service mode, the SmartServer automatically sends network configuration changes to the OpenLNS network database via the LNS Proxy Web service. Other OpenLNS or LNS clients such as OpenLNS CT can then be resynchronized to the updated OpenLNS network database. For more information on resynchronizing a OpenLNS CT drawing to an OpenLNS network database, see the *OpenLNS Commissioning Tool User's Guide*.

You can manually synchronize the SmartServer to an OpenLNS or LNS network database if you are using the **LNS Manual** network management service mode, or if you are using **LNS Auto** network management service mode and another OpenLNS client such as OpenLNS CT or OpenLNS tree makes changes to the OpenLNS network database that are not propagated to the SmartServer over the LonTalk channel. Manual synchronization in these cases is required because the network objects in the SmartServer tree lose synchronization with the OpenLNS network database. Objects that are not in sync with the OpenLNS network database are highlighted yellow in the SmartServer tree.

When you manually synchronize the SmartServer, the SmartServer Web interface requests a list of objects to be synced from the SmartServer via SOAP and forwards the objects returned by the SmartServer to the LNS Proxy Web service. The LNS Proxy Web service returns a set of synced objects to the SmartServer Web interface, which forwards these objects back to the SmartServer. Manually synchronizing the SmartServer does not require the opening of any ports on firewalls blocking the SmartServer's access to the OpenLNS Server computer. The following graphic illustrates how the SmartServer communicates with the OpenLNS network databases in **LNS Manual** mode.

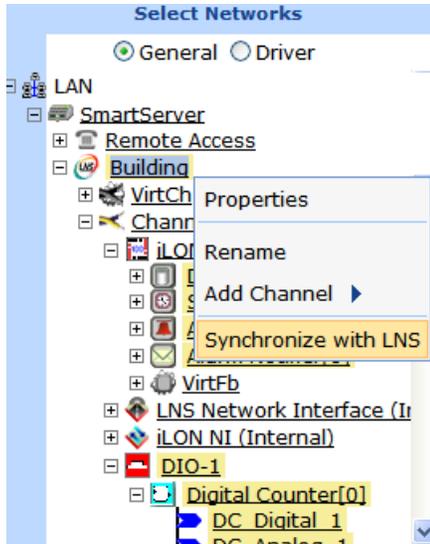


You can manually synchronize all items in the SmartServer tree that are out of sync at one time, or you can select individual items to be synchronized.

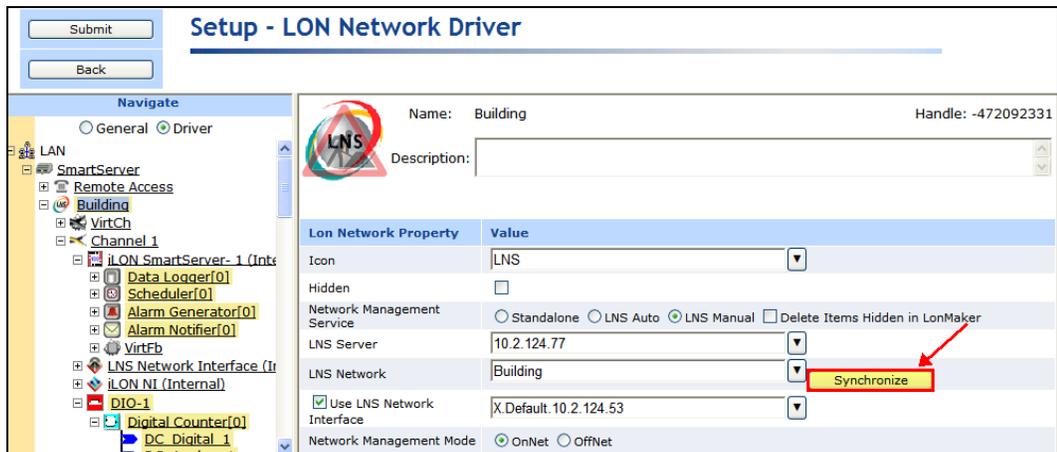
Manually Synchronizing All Items

If items in the SmartServer tree lose synchronization with the OpenLNS network database, you can manually synchronize all of them to the OpenLNS network database at one time following these steps:

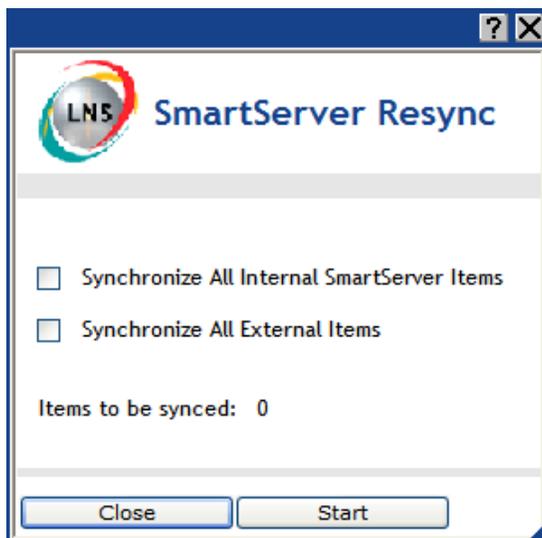
1. Right-click the network item in the target SmartServer tree, and then click **Synchronize with LNS** in the shortcut menu.



Alternatively, you can click **Driver**, click the network icon in the SmartServer tree to open the **Setup – LON Network Driver** Web page, and then click the **Synchronize** button in the **OpenLNS Network** property.



2. The **SmartServer Resync** dialog opens.



3. Set the following synchronization options:

Synchronize All Internal SmartServer Items

Synchronizes all internal items in the SmartServer's internal database, including hidden items, with the OpenLNS network database.

Internal items include the following:

- LONWORKS channels.
- The SmartServer's internal App device and its child functional blocks and data points.
- The SmartServer's internal IP-852 router.
- Internal devices created by custom apps and their child functional blocks and data points.

Selecting this option also transmits changes made to the LON driver properties of the internal items in the SmartServer tree to the OpenLNS network database, and it updates the SmartServer's internal database with changes made to the LON driver properties of the internal items with OpenLNS CT, OpenLNS tree, or other OpenLNS application.

This option is cleared by default, which means that the SmartServer sends only changes made to the internal items in the SmartServer tree to the OpenLNS network database. In addition, the SmartServer's internal database is updated only with the following changes made to internal items with OpenLNS CT:

- Renaming of devices or functional blocks.
- Addition of functional blocks to the SmartServer's internal App device that have stencils with no dynamic network variables on them.
- Deletion of the SmartServer App device's functional blocks.
- Addition or deletion of dynamic network variables on the SmartServer's internal App device while it is uncommissioned.

Note: Selecting this option may significantly increase the time required for the manual synchronization as all hidden internal items are synchronized.

Synchronize All External Items

Synchronizes all external items in the SmartServer's internal database with the OpenLNS network database.

External items include the following:

- LONWORKS channels.
- External devices and their child functional blocks and data points.
- Routers.

Selecting this option also transmits any changes made to the LON driver properties of the external items in

the SmartServer tree to the OpenLNS network database, and it updates the SmartServer's internal database with any changes made to the LON driver properties of the external items with OpenLNS CT, OpenLNS tree, or other OpenLNS application.

This option is cleared by default, which means that the SmartServer sends only changes made to the external items in the SmartServer tree to the OpenLNS network database. In addition, the SmartServer's internal database is updated only with any changes made to the names of external devices or functional blocks with OpenLNS CT.

4. Click **Start**.
5. The **Items to be Synced** property lists the number of items in the SmartServer tree to be updated. This number counts down as the synchronization operations progresses. When the synchronization operation has been completed, this number is 0. You can click **Close** anytime to return to the SmartServer Web interface and continue using the SmartServer during the synchronization.

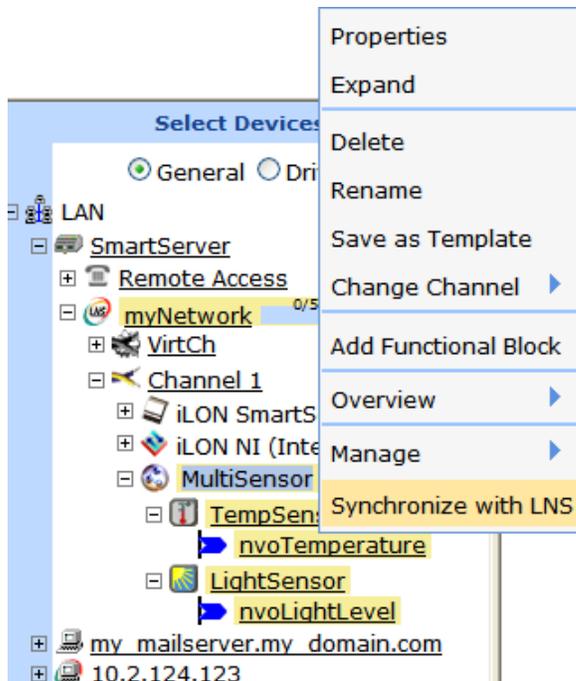
Notes:

- You can view the progress of the synchronization in the navigation pane. To do this, click **Settings** to open the **Global Settings** dialog, and then select the **Show Synchronization Progress in Tree** check box. This adds a synchronization status bar to the right of the network icon in the SmartServer tree that displays the current ratio of items that have already been synchronized to the total number of items being synchronized.
- You can view a log of the current synchronization in the SmartServer's console application. To view the sync log, enter the **trace 2** command. For more information on the SmartServer console application, see Appendix B, *Using the SmartServer Console Application*.

Manually Synchronizing Individual Items

If one or more items in the SmartServer tree lose synchronization with the OpenLNS network database, you can manually synchronize them to the OpenLNS network database. This synchronization operation automatically updates the LON driver properties of the selected items (for example, timing parameters of a channel, commission and application statuses of a device, format description of a data point) in the SmartServer's internal database.

To synchronize one item, right-click the item (channel, device, functional block, or data point) in the target SmartServer tree, and then click **Synchronize with LNS** in the shortcut menu to synchronize the item.



To synchronize multiple items at one time, click one item, either hold down CTRL and click all other items to be synchronized or hold down SHIFT and select another item to synchronize the entire range of items, and then click the **Synchronize with LNS** option in the shortcut menu.

Notes: Selecting the **Synchronize with LNS** option on a network item opens the **SmartServer Resync** dialog, where you can synchronize the entire network at one time.

Switching the SmartServer to a Different OpenLNS Network Database

You can change the OpenLNS or LNS network database to which a SmartServer is synchronized. You need to do this if you move the SmartServer to a new LONWORKS network or to another existing network, or if you want to create a new OpenLNS or LNS network database for an existing network.

When synchronizing the SmartServer to a new or existing OpenLNS network database, the current network configuration is merged into the new OpenLNS network database (this network configuration data is stored in the SmartServer's internal database [the XML files in the /config/network/<Current Network> folder on the SmartServer's flash disk]). This enables you to preserve the current configurations of the SmartServer's built-in applications in the new OpenLNS network database.

External devices that have been added to the SmartServer tree will also be merged into the new OpenLNS network database; therefore, you must delete all external devices that you do not want in the new database. If you do not delete these external devices, their shapes and the shapes of all their children functional blocks and data points will be added to the OpenLNS CT drawing. You will then need to manually delete these extra shapes from your OpenLNS CT drawing.

You must also delete all references to the data points of the deleted external devices that have been added to the SmartServer's applications. If you do delete these data point references, they will remain in the SmartServer's applications.

If you do not need to save the current configuration of the SmartServer's built-in applications, you can restore your SmartServer to its factory default settings before synchronizing it to a different OpenLNS network database. The SmartServer will automatically back up the current network configuration data and store it in the /config/network.bak/<Current Network> folder. This enables you to restore the applications to their previous configurations, if desired.

In summary, when synchronizing the SmartServer to a new or different OpenLNS network database, the changes made to the OpenLNS network database depend on whether the database is new (an empty

OpenLNS network database, which contains only the default “OpenLNS network Interface” and the default “Channel 1”) or if it is an existing database with other OpenLNS objects in it.

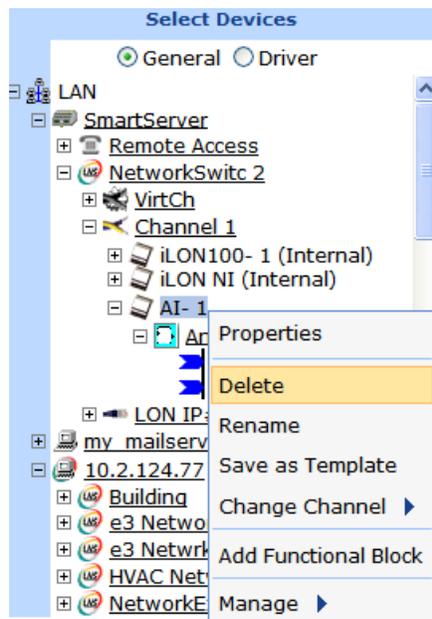
- If the OpenLNS network database is new (empty), the following changes are made to it:
 - The domain length and domain ID properties in the database are changed to those currently used by the network attached to the SmartServer;
 - The default “Channel 1” in the database is re-named to the name of the first LONWORKS channel on the SmartServer tree. The transceiver type in the database is changed to the one used on the first LONWORKS channel on the SmartServer.
 - All other LONWORKS channels and devices on the SmartServer tree are merged into the database.

Note: If there are any naming conflicts between the SmartServer and the OpenLNS network database, the OpenLNS network database has precedence. For example, if the **i.LON App (Internal)** device is named “iLON SmartServer- 1” in the OpenLNS network database, then it will be re-named to “iLON SmartServer- 1” in the SmartServer tree after the synchronization.

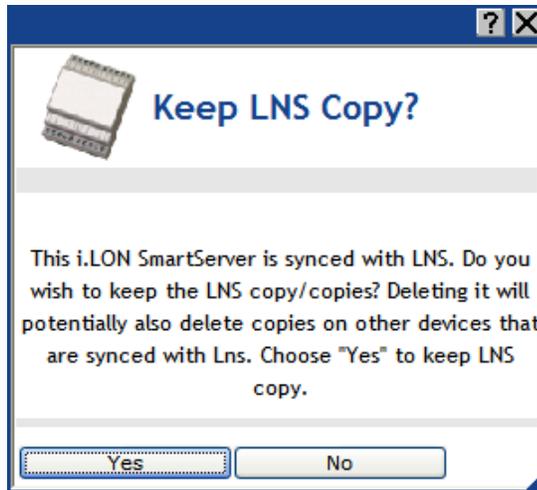
- If the OpenLNS network database is an existing OpenLNS network database with other LNS objects in (not empty), all the LONWORKS channels and devices on the SmartServer tree are merged into the database. The domain length and domain ID properties in the OpenLNS network database are not changed.

To synchronize the SmartServer to a new or existing OpenLNS network database, follow these steps:

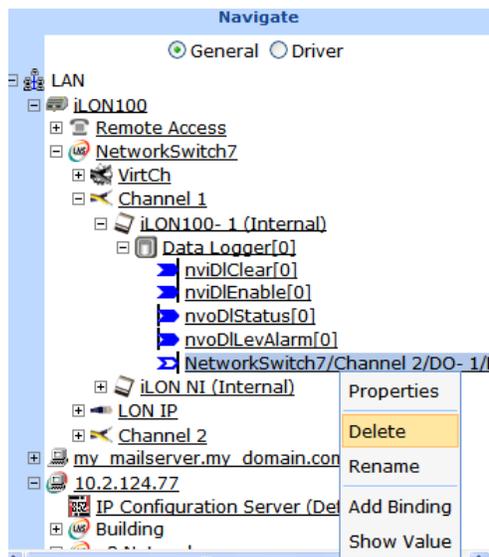
1. If you do not need to save the current configurations of the SmartServer’s built-in applications, restore your SmartServer to its factory default settings as described in *Restoring a SmartServer to Factory Default Settings* in Chapter 3.
2. To preserve the current configurations of the SmartServer’s built-in applications before synchronizing the SmartServer to a different OpenLNS network database, follow these steps:
 - a. Delete all external devices that you do not want in the new database. To do this, right-click the external device to be deleted or select multiple devices to be deleted in the SmartServer tree and then click **Delete** in the shortcut menu.



- b. The **Keep LNS Copy?** dialog opens.



- c. Click **Yes** to delete the external device only from the SmartServer's internal database. Click **No** to delete the external device from both the SmartServer's internal database and the OpenLNS network database to which the SmartServer is synchronized.
- d. Remove the data points of the deleted external devices from the SmartServer's built-in applications. To do this, expand the application's functional block in the SmartServer tree, select one or more data point references () to be deleted, right-click a data point reference, select **Delete** on the shortcut menu, and then click **Submit**.



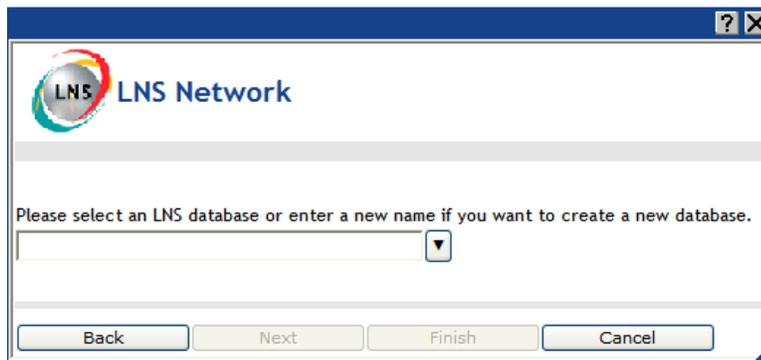
3. Decommission the SmartServer, the SmartServer's IP-852 router, and any commissioned internal FPM devices in the current OpenLNS network database with OpenLNS CT or other OpenLNS application.
4. Commission the SmartServer in the new or existing OpenLNS network database with OpenLNS CT or other OpenLNS application.

Note: The name of the channel on which the SmartServer is installed in the OpenLNS CT drawing must match that of the SmartServer's current parent channel in the SmartServer Web interface; otherwise, the synchronization process may corrupt your OpenLNS CT network design.

For example, if the SmartServer's internal automated systems device (i.LON App, i.LON SmartServer- 1, or some other user-defined name) is located under Channel 1 in the navigation

pane on the left side of the SmartServer Web interface, then you must drag the SmartServer device shape to Channel 1 in your OpenLNS CT drawing.

5. Click **Driver** at the top of the navigation pane, and then click the network icon. The **Setup – LON Network Driver** Web page opens.
6. If the target OpenLNS network database is located on a different OpenLNS Server, proceed with the following steps; otherwise, skip to step 7.
 - a. Add that OpenLNS Server to the LAN containing the target OpenLNS network database if it has not already been added.
 - b. In the **LNS Server** property, select the IP address of the target OpenLNS Server.
 - c. The **LNS Network** dialog opens.



- d. Select an existing OpenLNS network database or create a new one.
 - To select an existing OpenLNS network database, select the name of the OpenLNS network database from the list and then click **Finish**.
 - To create a new OpenLNS network database, enter a descriptive name (maximum 14 characters) that is unique to the selected OpenLNS Server, click **Next**, and then click **Finish** in the **Create LNS DB?** dialog. The new OpenLNS network database is created in the **ilon\db** folder on your computer.
7. In the **OpenLNS Network** property, either select an existing OpenLNS network database to be updated with the network configuration stored in the SmartServer's internal database (XML files in the /config/network folder on the SmartServer flash disk), or create a new OpenLNS network database.
 - To select an existing OpenLNS network database, select the name of the OpenLNS network database from the list and then click **Submit**.
 - To create a new OpenLNS network database, enter a descriptive name (maximum 14 characters) that is unique to the selected OpenLNS Server. The new OpenLNS network database is created in the **ilon\db** folder on your computer. Click **Submit**. A dialog appears prompting you to confirm the creation of the new OpenLNS network database on the OpenLNS Server. Click **OK**. After the dialog closes, click **Submit**.



8. If the **Network Management Service** property is set to **LNS Auto**, the SmartServer automatically begins synchronization with the new OpenLNS network database. If the **Network Management Service** property is set to **LNS Manual**, manually synchronize the SmartServer to the new OpenLNS network database following the steps described in *Manually Synchronizing the SmartServer to an OpenLNS network database* earlier in this chapter.
9. When the synchronization operation on the SmartServer has been completed, synchronize OpenLNS CT or other OpenLNS application to the OpenLNS network database. This updates OpenLNS CT or other OpenLNS application with the functional blocks on the SmartServer's internal App device that are displayed in the SmartServer tree.

Switching to LNS Mode and Synchronizing to an OpenLNS Network Database

You can switch the SmartServer from standalone to LNS mode (**LNS Auto** or **LNS Manual**) and then synchronize the network attached to the SmartServer to an OpenLNS database. To switch a network from standalone to LNS mode, you select an OpenLNS network database on an OpenLNS Server to be synchronized to the network. After the OpenLNS database has been updated, you can synchronize an OpenLNS application such as OpenLNS CT to the OpenLNS database and then use it to manage the network.

The changes made to the OpenLNS network database depend on whether it is empty (contains only the default "OpenLNS network Interface" and default "Channel 1").

- If the OpenLNS network database is empty, the following changes are made to it:
 - The domain length and domain ID properties in the database are changed to those currently used by the network attached to the SmartServer;
 - The default "Channel 1" in the database is re-named to the name of the first LONWORKS channel on the SmartServer tree, which is usually "LON".
 - The transceiver type in the database is changed to the one used on the first LONWORKS channel on the SmartServer.
 - All other LONWORKS channels and devices on the SmartServer tree are merged into the database.

Note: If there are any naming conflicts between the SmartServer and the OpenLNS network database, the OpenLNS network database has precedence. For example, if the **i.LON App (Internal)** device is named "SmartServer" in the OpenLNS network database, then it will be re-named as such in the SmartServer tree after the synchronization.

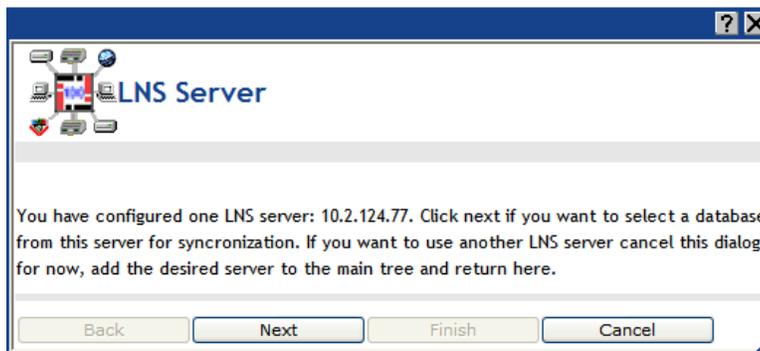
- If the OpenLNS network database is not empty, all the LONWORKS channels and devices on the SmartServer tree are merged into the database. The domain length and domain ID properties in the OpenLNS network database are not changed.

To switch the SmartServer from standalone to LNS mode (**LNS Auto** or **LNS Manual**) and synchronize the network in the SmartServer tree to an OpenLNS network database, follow these steps:

1. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Add an OpenLNS Server to the LAN. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on how to do this.
3. Click **Driver** and then click the network icon in the SmartServer tree. The **Setup - LON Network Driver** Web page opens.
4. In the **Network Management Service** property, select the **LNS Auto** option. In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service, and automatically sends network configuration changes made in the SmartServer tree to the OpenLNS network database.

Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default). If a firewall is blocking access to the LNS Proxy Web service, select the **LNS Manual** option.

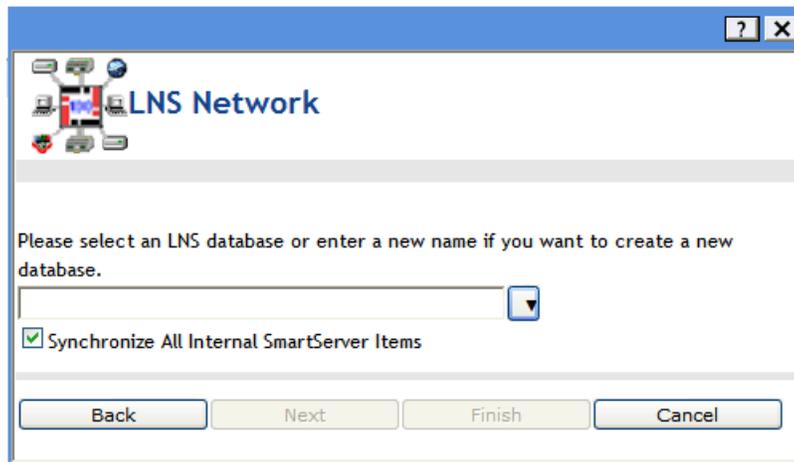
5. The **OpenLNS Server** dialog opens.



6. Click **Next**.
7. A dialog for logging in to the LNS Proxy Web service opens. Enter the **User Name** and **Password** used by the SmartServer for logging in to the LNS Proxy Web service and then click **OK**. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon in the notification area of your computer, and then click **Options** on the shortcut menu.



8. The **LNS Network** dialog opens.



9. In the **OpenLNS Network** property, either select an existing OpenLNS network database to be updated with the network configuration stored in the SmartServer's internal database (XML files in the /config/network folder on the SmartServer flash disk), or create a new OpenLNS network database.
 - To select an existing OpenLNS network database, select the name of the OpenLNS network database from the list and then click **Finish**.
 - To create a new OpenLNS network database, click the arrow to use the current network name for the OpenLNS network database or enter a different descriptive name (maximum 14 characters) that is unique to the selected OpenLNS Server, click **Next**, and then click **Finish** in the **Create LNS DB?** dialog. The new OpenLNS network database is created in the **ilon\db** folder on your computer.
10. If IP-852 routing is activated on your SmartServer, a dialog appears informing you that you need to reboot your SmartServer in order to use it as an IP-852 router. Click **Close**.



11. If you created a new OpenLNS network database in step 8, select the **Use OpenLNS Network Interface** option if the OpenLNS Server is attached to the physical network and you want the SmartServer to communicate with the devices on the network, and then select the network interface to be used for communication between the OpenLNS Server and the network.

If you selected an existing database in step 8, **Use OpenLNS Network Interface** is selected and the network interface is specified automatically.
12. If **Use OpenLNS Network Interface** is selected, the **Network Management Mode** property is set to **OnNet** automatically. This means that network changes are propagated to the network immediately. Click **OffNet** to store network changes in the selected OpenLNS network database and propagate them to the network when you place the SmartServer **OnNet**.
13. Click **Submit**.
14. If you selected **LNS Auto** in the **Network Management Service** property, synchronization automatically begins. If you selected **LNS Manual** in the **Network Management Service** property, manually synchronize the SmartServer to the new OpenLNS network database following the steps described in *Manually Synchronizing the SmartServer to an OpenLNS network database* earlier in this chapter.
15. If you are managing the network with OpenLNS CT, create a new OpenLNS CT drawing from the OpenLNS network database and then synchronize the OpenLNS CT drawing to the OpenLNS network database. See the *OpenLNS Commissioning Tool User's Guide* for more information on how to do this.
16. Commission the SmartServer and the external devices on the network with OpenLNS CT, OpenLNS tree, or another OpenLNS application. For more information on installing the SmartServer, see *Installing the SmartServer with OpenLNS CT* in Chapter 12.

Note: The SmartServer and the external device shapes already include their devices' Neuron IDs. Therefore, if you are using OpenLNS CT, you only need to right-click a device shape and clicking **Commission** in the shortcut menu to commission a device. You do not have to step through the New Device Wizard.
17. You now add the external network variables and configuration properties in the OpenLNS tree to the built-in applications on a SmartServer (your local SmartServer or a remote SmartServer that you have added to the LAN). See *Adding Data Points to SmartServer Applications* in Chapter 4 for more information on adding external network variables and configuration properties to the SmartServer's built-in applications.
18. If IP-852 routing is activated on your SmartServer, you need to reboot your SmartServer in order to use the SmartServer as an IP-852 router. You can reboot your SmartServer using the SmartServer Web pages or the SmartServer console application.
 - To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.

- To reboot your SmartServer using the SmartServer console application, enter the `reboot` command. For more information on using the SmartServer console application, see Appendix B, *Using the SmartServer Console Application*.

Switching a Network from LNS Mode to Standalone Mode

You can switch a network from LNS mode (**LNS Auto** or **LNS Manual**) to standalone mode; however the network configuration stored in the OpenLNS network database is not copied to the SmartServer. This is currently not supported. For instructions on setting a network to standalone mode, see *Using Standalone Mode* earlier in this section.

Creating and Configuring LONWORKS Channels

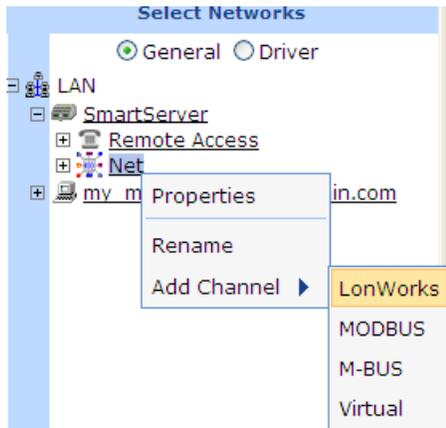
Channels are the physical media upon which devices communicate. Because the LonTalk protocol is media independent, you can use numerous types of media for channels in a network design such as twisted pair, power line, fiber optics, IP, and RF, and other types. Adding channels allows you to use different media within the same network, isolate network traffic for performance, isolate devices for reliability, and increase the number of devices beyond the limit of a specific transceiver. You can add LONWORKS, Modbus, M-Bus, and virtual channels to the network attached to a SmartServer and you can add LONWORKS channels to a network in an OpenLNS Server.

This section describes how to create and configure a LONWORKS channel. See *Designing a Modbus Network* and *Designing a M-Bus Network* later in this chapter for information on adding Modbus and M-Bus channels to the SmartServer. See *Using the Virtual Channel* later in this chapter for information on using the virtual channel on the SmartServer.

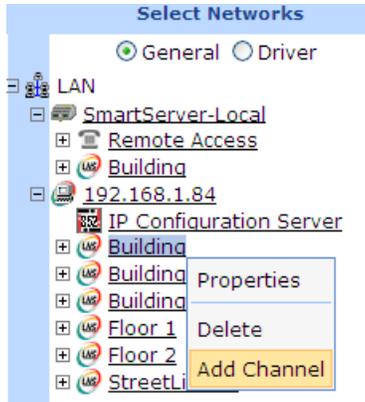
Creating a LONWORKS Channel

You can create a new channel with the SmartServer Web interface if the SmartServer is operating in LNS mode (**LNS Auto** or **LNS Manual**). You cannot add a second channel to the SmartServer if it is operating in Standalone mode. To create a LONWORKS channel, follow these steps:

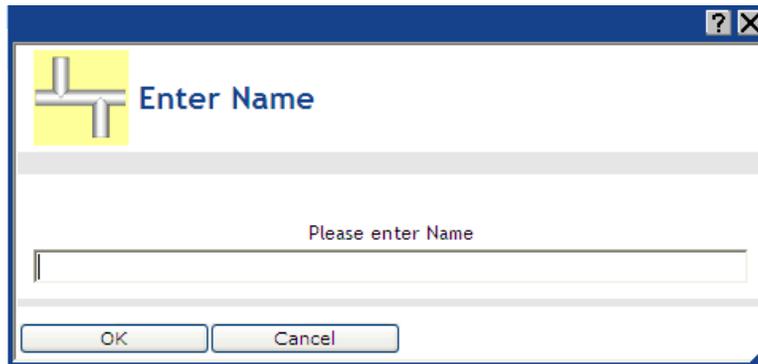
1. If you are adding a channel to the network in a SmartServer tree, right-click the network icon in the SmartServer tree, point **Add Channel**, and then click **LonWorks** in the shortcut menu.



If you are adding a channel to a OpenLNS network database in the OpenLNS tree, right-click the OpenLNS network database icon, and then click **Add Channel** in the shortcut menu.



2. The **Enter Name** dialog opens.

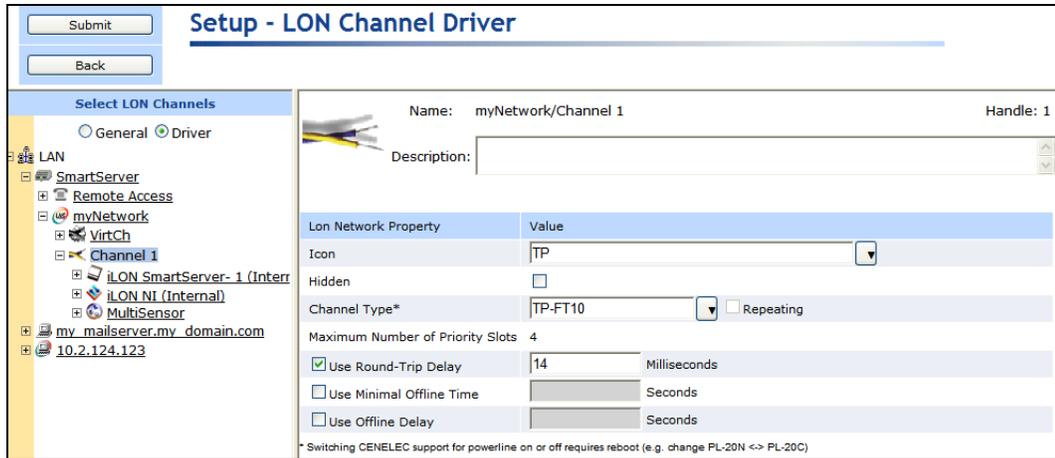


3. Enter a descriptive name for the LONWORKS channel that is unique to the network (channel names are case sensitive) and then click **OK**.
4. The channel is added to the bottom of the tree of its parent network or OpenLNS network database.
5. Click **Submit**.

Configuring LONWORKS Channels

You can use the driver properties to change the channel type, specify behavior of network messages on the channel, and set advanced timing properties. To configure the channel properties, follow these steps:

1. Click **Driver**.
2. Select one or more channels to configure.
 - To configure one channel, click the channel. Alternatively, you can right-click the channel and select **Properties** on the shortcut menu.
 - To configure two or more channels, click one channel and then either hold down CTRL and click all other channels to be configured or hold down SHIFT and select another channel to configure the entire range of channels. Alternatively, you can select multiple channels, right-click one of the selected channels, and then click **Properties** on the shortcut menu.
3. The **Setup - LON Channel Driver** Web page opens.



4. Configure the following channel properties:

- Name* Displays the network path of the channel in the following format: `<network>/<channel>`. This field is read-only.
- Handle* Displays the handle of the channel assigned by the OpenLNS Server. This field is read-only.
- Description* Enter an optional description of the channel. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Lon Network Property

Icon Displays the icon used to represent the channel in the SmartServer or OpenLNS tree and in the application frame. The default icon is TP or PL depending on your SmartServer hardware model. You can change the icon for the channel in by selecting a different icon and then clicking **Submit**.

Hidden Hides the channel in the SmartServer tree or OpenLNS tree. If this channel is not actively being used, you can hide it to simplify the web interface.

To show a hidden channel icon, click **Settings**. In the **Global Settings** dialog, select the **Channels** check box in the **Display Hidden** property and then click **Close**.

Channel Type Select the channel type from the list. The default channel is **TP-FT10** or **PL-20C** depending on your SmartServer hardware model.

If you select a PL channel, the **Repeating** box is available. If the SmartServer is managing a power line repeating network, select one of the following repeating modes:

- **Not Initialized.** Repeating is not initialized.
- **Off.** Repeating is initialized and disabled.
- **On (With Automatic Discovery and Optimization of Proxy Chains).** Enables the Enhanced LonTalk Proxy protocol to be used for transmitting messages to the devices attached to the power line. With this protocol, the SmartServer sends messages to the repeating devices (devices with a PL-3120® or PL-3150® Smart Transceiver that have been configured for repeating) closest to it and those

devices relay the messages to the repeating devices further down the power line until the message reaches the target device. In this mode, the SmartServer continuously attempts to discover and optimize the repeating chains used to communicate messages from the SmartServer to the devices on the network.

- **On (Static Proxy Chains).** Same as **On with Automatic Discovery**, except that the SmartServer does not continuously discover and optimize the repeating chains, which increases the available bandwidth on the power line repeating network for operational traffic.

Notes: To use power line repeating, application device repeating must be implemented on your LONWORKS devices by the device manufacturers. See your Echelon sales representative for more information.

To use power line repeating, you must also set the SmartServer to standalone mode. See the previous section, *Configuring a LONWORKS Network*, for how to do this. Power line repeating is not compatible with LNS mode.

For more information on managing a power line repeating network, see the *SmartServer 2.2 Power Line Repeating Network Management Guide*.

Maximum Number of Priority Slots

Displays the maximum number of priority slots available on the channel. Priority slots may be used by the critical devices on a network that use priority messaging.

With priority messaging, the device with the highest priority sends its packet before any other devices can send theirs. This is accomplished by assigning each priority device a time (priority) slot where it can transmit before all other lower priority and non-priority devices. These time slots consume network bandwidth; therefore, priority messaging should only be used for critical devices and data.

Use Round Trip Delay

Select this option to specify the expected longest round-trip time (in milliseconds) of a message (for example, message and response). This option allows expected traffic patterns to be input into the system so that the timer calculations can be affected accordingly.

If this option is cleared, the default round-trip delay, which is two packet cycles based on the average packet size, is used.

Minimal Offline Time

If a network message fails, a data point and its device are marked offline. You can select **Use Minimal Offline Time** so that all the data points on the offline device with pending network messages (read/write requests, polls, or heartbeats) are marked offline and network messages are not sent to them. This ensures that network performance is not impacted by an offline device. This check box is cleared by default.

You can also set the minimum period of time (in seconds) that the SmartServer waits before transmitting network messages to offline data points. During this period, an offline device transmits an OFFLINE status in response to data point requests. Once the **Minimal Offline Time** elapses, the SmartServer sends a read/write request to one offline data point. If the read/write request succeeds, the data point and its device are marked online, and all cached read/write requests for the offline data points on the device are executed.

The default **Use Minimal Offline Time** for a LONWORKS channel is **60** seconds.

Use Offline Delay Specify the period of time (in seconds) that the SmartServer waits before marking a data point and its parent device offline (red) in the SmartServer tree after the LON driver detects that the data point is offline.

For example, if you poll a data point every 5 minutes and you set **Use Offline Delay** to 1 hour, it takes 12 polls for the data point and its parent device to be marked offline—even though the LON driver detected that it could not communicate with the data point after the first poll.

5. Click **Advanced** to set the following timing properties for the channel:

Advanced	
Timing	Value
<input checked="" type="checkbox"/> Use Transmit Timer	512 ▼ Milliseconds
<input checked="" type="checkbox"/> Use Retry Count	3
<input checked="" type="checkbox"/> Use Number of Slots	0
<input checked="" type="checkbox"/> Use Slot Width	0 100 Milliseconds

Use Transmit Timer You can change the interval (in milliseconds) network messages wait for confirmation before being re-sent over the network. The default value is **96 ms** for FT-10 channels and **512 ms** for PL channels. If this option is cleared (it is cleared by default), the interval is calculated based on the network topology, specifically the transmission time for each channel that the message must cross. By default, the transmission time for each channel is determined by its type. However, this can be overridden with the **Use Round-Trip Delay** property.

For more information on configuring this property for a power line repeating network, see the *SmartServer 2.2 Power Line Repeating Network Management Guide*.

Use Retry Count You can change the number of times a network message is re-sent when no confirmation is received. The default value is **3** attempts for FT-10 channels and **5** attempts for PL-20 channels. If this option is cleared (it is cleared by default), a default value, which can range from 0 to 15 attempts, is calculated based on network topology. Typically, the default retry count is set to 3 attempts; however, if a message must pass through certain channel types, the default may be increased. For example, if a message must cross a PL-20 channel, the default retry count would be increased to 5 attempts.

For more information on configuring this property for a power line repeating network, see the *SmartServer 2.2 Power Line Repeating Network Management Guide*.

Use Number of Slots The **Use Number of Slots** and **Use Slot Width** properties are used to calculate how long the SmartServer waits before sending messages to the devices on the power line repeating network. These settings affect the traffic initiated by the SmartServer when it receives direct messages or events from the devices on the network.

Use Slot Width

Specify the maximum number of slots used for spacing packets on a power line repeating channel (the default value is **0**). You can specify the width of the slots in the **Use Slot Width** property (the default value is **0**).

If **Use Number of Slots** is set to n , then the SmartServer uses a random slot between 0 to $n-1$ for sending messages, and this slot is then multiplied by the value in the **Use Slot Width** box, and 100ms.

For example, if **Use Number of Slots** is **4** and **Use Slot Width** is **1**, the SmartServer would use a delay of either 0, 100, 200 or 300 ms for each message transmission.

6. Click **Submit**.

Creating and Configuring LONWORKS Devices

An *application device* consists of hardware (external devices only) and software that runs an application and communicates with other devices. You can add application devices to the network attached to a SmartServer or to a LONWORKS network database in an OpenLNS Server. To add an application device, you create a new device instance and then select the device name, template, and location relative to the SmartServer (internal or external). After you add an application device added to the network, you can configure it using its **Setup - LON Device Driver** Web page.

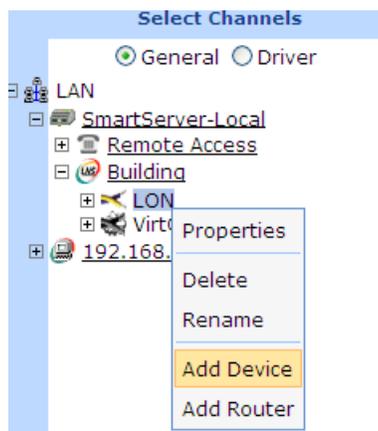
After creating and configuring an external application device, you can commission it. Commissioning associates the external device you created with the SmartServer to the physical device on the network. To commission a device, you acquire its Neuron ID by using Smart Network Management, pressing a service pin on the device, or manually entering it.

You do not have to commission devices until you are ready to install them. This is how you design an engineered system—you create and configure devices offsite, bring the network database onsite (if using OpenLNS network management services), and then commission the devices. Under the ad-hoc installation scenario, you define and commission the devices in one step while onsite. See *Installing LONWORKS Networks* in this chapter for more information on commissioning devices.

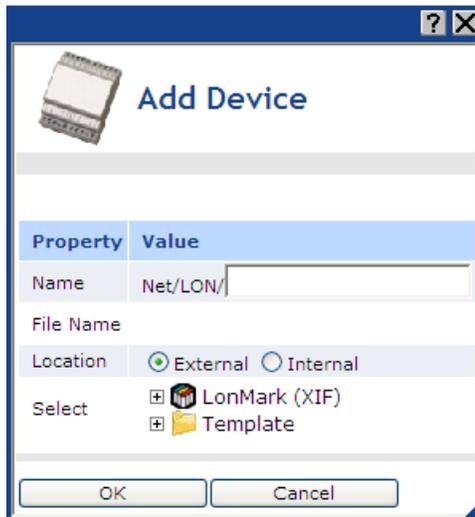
Creating LONWORKS Devices

To create a LONWORKS device, follow these steps:

1. If you are using the SmartServer in **Standalone** mode, copy the following files to the SmartServer flash disk:
 - Copy the device interface (XIF) files of the devices to be managed by the SmartServer to the **/LonWorks/import** folder on the SmartServer flash disk.
 - Copy the device resource files to the **/LonWorks/types/user** folder.
 - If you plan on upgrading the devices using the SmartServer, copy the devices' application image files to the **/LonWorks/import** folder.
2. Right-click a LONWORKS channel, and then select **Add Device** on the shortcut menu.



3. The **Add Device** dialog opens:



4. In the **Name** property, enter a descriptive name for the device that is unique to the network (device names are case sensitive).
5. If you are adding a device to a channel in the SmartServer tree, in the **Location** property, select the type of device you are creating: **External** or **Internal**.

- An **External** device is an application device that you can physically install on the network.
- An **Internal** device is an application that resides on the SmartServer, appears as a unique device on the LON network, and encapsulates the functional blocks and data points within an XIF or functional profile template. An internal device corresponds to one of the 10 custom app devices that you can create and deploy on a SmartServer. See the *SmartServer 2.0 Programming Tools User's Guide* for more information on custom apps.

These options are not available if you are adding a Modbus or M-Bus device to a channel in the SmartServer tree or if you are adding a LONWORKS device to a channel in the OpenLNS tree.

6. In the **Select** property, select the device interface file (.XIF or .XML extension) used by the device. The device's interface specifies the number and types of its functional blocks; number, types, directions, and connection attributes of its network variables; its configuration properties, and its program ID. The program ID is a 16-hex-digit number that uniquely identifies the device application. You can select a device interface file by expanding either the **LonMark (XIF)** or **Template** folder.

- **LonMark (XIF)**. This folder contains the .XIF files in the **/lonworks/import** directory on the SmartServer (if the device is located in the SmartServer tree) or the LonWorks **import** folder on the OpenLNS Server (if the device is located in the OpenLNS tree). The .XIF file contains all the functional blocks, network variables, and configuration properties programmatically defined for the device.

You can copy XIF files from the LONWORKS **import** folder on your computer to the **/LonWorks/import** folder on your SmartServer flash disk, and then use the XIF files for creating new devices in the SmartServer tree or changing the XIF files of existing devices. The file paths of the XIF files on your SmartServer and your computer must match in order to duplicate functional block and dynamic data points when operating the SmartServer in LNS mode (**LNS Auto** or **LNS Manual**).

Note: You can only select a XIF file if you are adding a LONWORKS device to a channel in the SmartServer or OpenLNS tree. If you are adding a Modbus or M-Bus device to a channel in the SmartServer tree, the **LonMark (XIF)** folder is not available.

- **Template.** This folder contains the .XML files in the `/config/template/lonworks` directory on the SmartServer. The .XML file contains all the functional blocks, network variables, and configuration properties shown on the navigation pane at the time the device template was created. The .XML file can contain dynamic functional blocks and dynamic network variables.

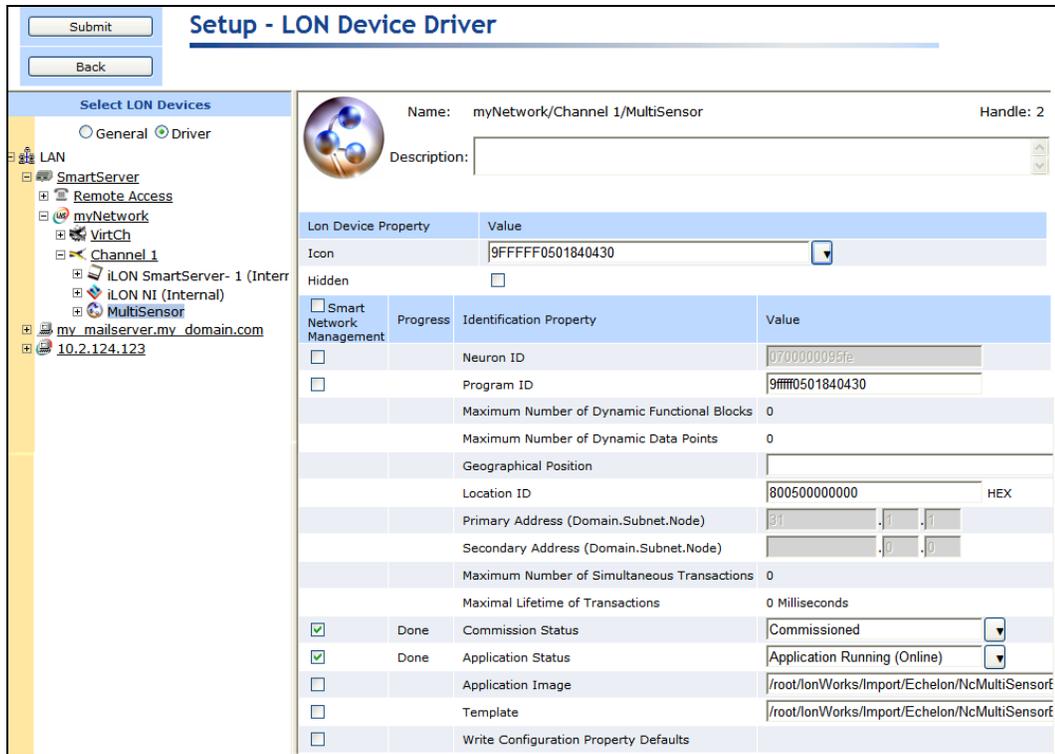
Note: You can only select a device template if you are adding a device to a channel in the SmartServer tree. If the device is located in the OpenLNS tree, the **Template** folder is not available.

7. The **File Name** property displays the full path of the LonMark device interface (.XIF file) or template (.XML file) selected for the device. If you selected a LONWORKS template, the program ID of the device is displayed.
8. Click **OK** to return to the SmartServer Web interface. The device is added underneath the icon of its parent channel. You must wait for the SmartServer to process the XIF file used for the device. The time it takes depends on the size of the XIF file. Once the XIF file has been processed, you can expand the device and its functional blocks to show the data points in the application device.
9. Click **Submit**.

Configuring LONWORKS Devices

You can use the device driver properties to install, configure, upgrade, and test devices. To configure the device properties, follow these steps:

1. Click **Driver**.
2. Select one or more devices to configure.
 - To configure one device, click the device. Alternatively, you can right-click the device and select **Properties** on the shortcut menu.
 - To configure two or more devices, click one device and then either hold down CTRL and click all other devices to be configured or hold down SHIFT and select another device to configure the entire range of devices. Alternatively, you can select multiple devices, right-click one of the selected devices, and then click **Properties** on the shortcut menu.
3. The **Setup - LON Device Driver** Web page opens.



4. Configure the following device properties:

- Name* Displays the network path of the device in the following format: `<network>/<channel>/<device>`. This field is read-only.
- Handle* Displays the handle of the device assigned by the OpenLNS Server. This field is read-only.
- Description* Enter an optional description of the device. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Lon Device Property

- Icon* Displays the icon used to represent the application device in the SmartServer tree or OpenLNS tree and in the application frame. The default icon is App for all devices except for the SmartServer’s application device (i.LON App).
You can create custom icons for your devices (See *Using Custom Device and Functional Block Icons* in Chapter 4 for how to do this).
You can change the icon for the device by selecting a different icon and then clicking **Submit**.
- Hidden* Hides the application device in the SmartServer tree or OpenLNS tree. If this device is not actively being used, you can hide it to simplify the web interface.
To show a hidden device icon, click **Settings**. In the **Global Settings** dialog, select the **Devices** check box in the **Display Hidden** property and then click **Close**.

Identification Property

Neuron ID

Displays the current Neuron ID of the application device. The Neuron ID is a unique 48-bit number that is manufactured into an external device or assigned to one of the SmartServer's 16 internal devices.

You can acquire the Neuron ID of external devices automatically by selecting the **Smart Network Management** option. When you select **Smart Network Management**, the SmartServer searches the physical network for uncommissioned devices and matches them based on program ID to device interface (XIF) files that are stored in the **LonWorks/import** folder on either the SmartServer flash disk or your computer.

You can manually acquire the Neuron ID of external devices by clicking **Use Service Pin** to open the **LON Device Identification** dialog, and then pressing a service pin on the device, scanning a bar code on the device, or manually entering it. Commissioning assigns a logical address (Subnet/Node ID) to the device.

Notes:

- You cannot change this property for internal devices.
- You can change the Neuron ID for an external device by releasing its Neuron ID or replacing the device. You can replace a device using the **Device - Overview Web page** or using the **Replace LON Device** dialog.
 - To release the Neuron ID of a device, select the device in the SmartServer tree or OpenLNS tree, right-click the device, point to **Manage**, and then click **Release Neuron ID** on the shortcut menu. This erases the Neuron ID defined for the device in the SmartServer or OpenLNS network database and decommissions the device.

You must release the Neuron IDs of devices on a development SmartServer if you plan on creating a template of that development SmartServer and deploying it on one or more target SmartServers, and automatically installing the devices in the template.

- To replace a device with the **Device - Overview Web page**, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface, right-click a network or channel, point to **Overview**, and then click **Devices**. Click **Scan** to discover the replacement device. When the replacement device is discovered its Neuron ID appears in the Neuron ID property, and the under construction triangle appears to the right of the generic device icon. In the **Replacement ID** property of the replacement device, select the name of the original device to be replaced. The **Replacement ID** property of the replacement device is updated with the name of the original device, and the **Replacement ID** property of the original device becomes unavailable. Click **Submit**.

Program ID

Displays the unique, 16-hex digit ID that uniquely identifies the device application in the following format: **FM:MM:MM:CC:CC:UU:TT:NN** [Format (F), Manufacturer ID (M), Device Class (C), Usage (U), Channel Type (T), Model Number (N)].

The program ID is assigned by the device manufacturer for an external device, and it is assigned the 16 internal devices on the SmartServer. You cannot change this property for external devices. Devices with the same program ID must have the same device interface.

You can select **Smart Network Management** to have the SmartServer fetch a device's program ID automatically. Alternatively, you can fetch the program IDs for one or more devices by selecting the devices, right-clicking one device, pointing to **Manage**, and then clicking **Fetch Program ID** in the shortcut menu.

<i>Maximum Number of Dynamic Functional Blocks</i>	<p>Displays the maximum number of dynamic functional blocks that you can add to the device.</p> <p>A dynamic functional block is a functional block that is not pre-loaded on a device. Devices that support dynamic functional blocks include controllers that do not have a static interface. For example, the v40 SmartServer interface, which has a dynamic interface, supports a maximum of 500 dynamic functional blocks.</p>
<i>Maximum Number of Dynamic Data Points</i>	<p>Displays the maximum number of dynamic network variables/data points that you can add to the device.</p> <p>A dynamic network variable/data point can be added to a functional block after the device has been commissioned. Devices that support dynamic network variables/data points include controllers and gateways with dynamic interfaces. For example, the v40 SmartServer interface, which has a dynamic interface, supports a maximum of 3000 dynamic network variables/data points.</p>
<i>Geographical Position</i>	<p>Displays the waypoint of the device. A waypoint is a set of coordinates (latitude and longitude) that identifies the device's location in physical space. Typically, waypoints are acquired with a GPS and then uploaded to the SmartServer using SOAP/HTTP messages over the console port.</p> <p>Alternatively, you can manually enter the waypoint in this field or enter a descriptive string that uniquely identifies the device location (for example, the light pole number of a luminaire in a street lighting network).</p>
<i>Location ID</i>	<p>Displays the 6-byte hexadecimal location string that documents the device's location within the network.</p>
<i>Primary Address (Domain.Subnet.Node)</i>	<p>Displays the domain ID of the network, and the subnet and node IDs assigned to the device by the OpenLNS Server when the device is created.</p> <p>The subnet/node ID is used for addressing messages. The subnet ID identifies the channel (subnet) on which the device resides, and the node ID identifies the device on that channel.</p> <p>The subnet/node IDs begin with an address of 1/1 and increase sequentially to 1/2, 1/3, and so on for devices on the same channel (subnet). For a second channel created on the network, the subnet/node IDs would begin with an address of 2/1 and increase sequentially to 2/2, 2/3, and so on.</p>
<i>Secondary Address (Domain.Subnet.Node)</i>	<p>If the device is a member of another network, displays the domain ID of that network and the device's subnet and node ID on it.</p>

<i>Maximum Number of Simultaneous Transactions</i>	Displays the maximum number of simultaneous transactions supported by the device application. If the device application exceeds this maximum value, then any attempt to begin a new transaction will fail
<i>Maximum Lifetime of Transactions</i>	Displays the timeout value (in milliseconds) for a transaction. This value represents the longest period of time a transaction can be active.
<i>Use Authentication</i>	<p>Enables authentication during initial installation. If enter the device's 6-byte or 12-byte authentication key (12-digit or 24-digit hexadecimal string) provided by the device manufacturer.</p> <p>When the SmartServer commissions the device, it will replace the manufacturer's initial authentication key with the authentication key specified for the network. All network management commands sent to this device will then use authentication.</p>
<i>Commission Status</i>	<p>Indicates the current device configuration: Commissioned, Uncommissioned, or Never Reached.</p> <p>To have the SmartServer automatically set the device configuration, select the Smart Network Management check box and click Submit.</p> <p>To manually commission or decommission one or more devices, select the devices, select Commission or Decommission from the list to the right, select the Smart Network Management check box to the left, and then click Submit.</p> <p>Alternatively, you can manually commission or decommission one or more devices by selecting the devices in the SmartServer or OpenLNS tree, right-clicking one device, pointing to Manage, and then clicking Commission or Decommission in the shortcut menu.</p>
<i>State</i>	<p>Indicates the current state of the device application: Application Running (Online), Application Stopped (Offline), or Never Reached.</p> <p>The behavior of a device in the Online state depends on the device. A device may run its application after it has been commissioned.</p> <p>The behavior of a device in the Offline state depends on the device. An offline Neuron-hosted device, for example, will not run its application after it has been commissioned. An offline device still receives data point updates, but it does not process or transmit updated data point values. Instead, the device transmits its default values. When a device is in the offline state, you can still place it online, wink it, and query its status. Resetting an offline device makes it go online, unless the device is in the hard offline state, in which case it will remain offline after a reset. You can keep devices offline and then place them online one at a time to bring up a system incrementally.</p> <p>To have the SmartServer automatically set the state of the device application, select Smart Network Management and click Submit.</p> <p>To manually set the application state for one or more devices, select the desired state from the list to the right, select Smart Network Management to the left, and then click Submit.</p> <p>Alternatively, you can set the application state for one or more devices by selecting the devices in the SmartServer or OpenLNS tree, right-clicking one device, pointing to Manage, and then clicking Set Online or Set Offline in the shortcut menu.</p>
<i>Application Image</i>	Displays the full path of the application image file (.apb) loaded on the device. For a Neuron-hosted device, the application image is device

firmware that consists of the object code generated by the Neuron C compiler from the user's application program and contains other application-specific parameters, including the following:

- Network variable fixed and self-identification data
- Network variable external interface data
- Program ID string
- Optional self-identification and self-documentation data
- Number of address table entries
- Number of domain table entries
- Number and size of network buffers
- Number and size of application buffers
- Number of receive transaction records
- Input clock speed of target Neuron Chip

To have the SmartServer automatically download to a device an application image file that matches the device's program ID, select the **Smart Network Management** check box and click **Submit**.

To manually download an application image file to one or more devices, select an application image file from the **Select File** dialog that appears when you click the box to the right, select the **Smart Network Management** check box to the left, and then click **Submit**. See *Upgrading Devices* for more information on selecting an application image file from this dialog.

Alternatively, you can manually download an application into or one or more devices by selecting the device or devices, right-clicking one device, pointing to **Manage**, and then clicking **Download Image** in the shortcut menu.

Template

Displays the full path of the device interface (.XIF or .XML file) loaded on the SmartServer. The device interface (XIF) is the logical interface to a device. A device's device interface specifies the number and types of functional blocks, and the number, types, directions, and connection attributes of data points. The program ID field is used as the key to identify each device interface. Each program ID uniquely defines the static portion of the interface. However, two devices with identical static portions may differ if dynamic data points are added or removed, or if the types of changeable data points are modified. Thus it is possible to have devices with the same program ID but different device interfaces.

To load an device interface file that matches the device's program ID onto the SmartServer, select the **Smart Network Management** check box and click **Submit**.

To manually load a device interface file onto the SmartServer, select a device interface file from the **Select File** dialog that appears when you click the box to the right, select the **Smart Network Management** check box to the left, and then click **Submit**. See the previous section, *Creating LONWORKS Devices*, for more information on selecting a device interface for a device.

Alternatively, you can load a device interface file for one or more devices onto the SmartServer by selecting the device or devices, right-clicking one device, pointing to **Manage**, and then clicking **Activate Template** in the shortcut menu.

Write Configuration

Writes the default configuration property values that are stored in the device interface specified in the **Template** property to the application device.

<i>Property Defaults</i>	To have the SmartServer write the default configuration property values to the device, select the Smart Network Management check box and then click Submit .
<i>Reset</i>	<p>Resetting a device stops the device application, terminates all incoming and outgoing messages, sets all temporary settings to their initial values, and then restarts the device application. If the device was in the soft offline state, it will be put online; if the device was in the hard offline state, it will remain offline.</p> <p>To have the SmartServer reset the device, select the Smart Network Management check box and then click Submit.</p> <p>Alternatively, you can reset one or more devices by selecting the device or devices, right-clicking one device, pointing to Manage, and then clicking Reset in the shortcut menu.</p>

5. Click **Submit**.

Using OpenLNS and LNS Plug-ins

OpenLNS and LNS plug-ins are applications that perform a specialized device or functional block-specific task. For example, a plug-in can provide user interfaces for reading and setting the configuration properties on a device. Many device manufacturers provide plug-ins that you can use to configure their devices. Any plug-in conforming to the OpenLNS or LNS plug-in guidelines may be used with the SmartServer Web pages. You can view and download free Echelon and third-party OpenLNS and LNS plug-ins at www.echelon.com/plugins.

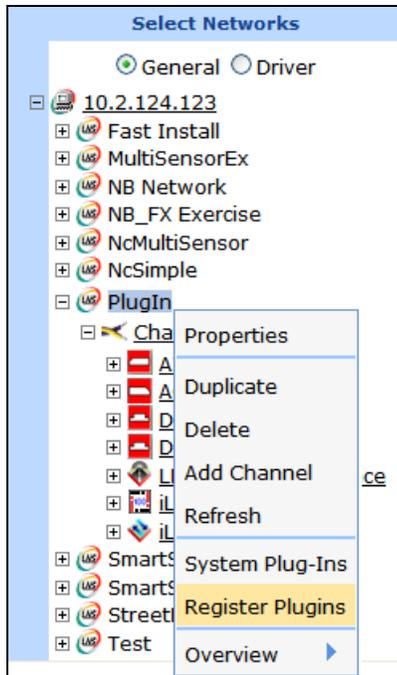
You can start plug-ins from the OpenLNS tree in the SmartServer Web interface on a local client (a computer that is running EES 2.2 and the OpenLNS Server). Starting an OpenLNS or LNS plug-in remotely is not supported; therefore, you cannot start plug-ins from the SmartServer tree in the SmartServer Web interface, or from a remote OpenLNS client (a separate computer that communicates with OpenLNS Server computer via the LNS Proxy Web service or the OpenLNS remote client interface).

OpenLNS or LNS plug-ins may also apply to entire systems instead of a device or functional block. System-wide plug-ins can provide generic services that may be used with multiple device types. For example, the *OpenLNS Browser* is a generic plug-in that can be used on any functional block to view and modify its network variables and configuration properties. If OpenLNS CT is installed on your computer, you can start the OpenLNS Browser using the **Browse** command. For more information on using the OpenLNS Browser, see the *OpenLNS Commissioning Tool User's Guide* or the LonMaker Browser on-line help.

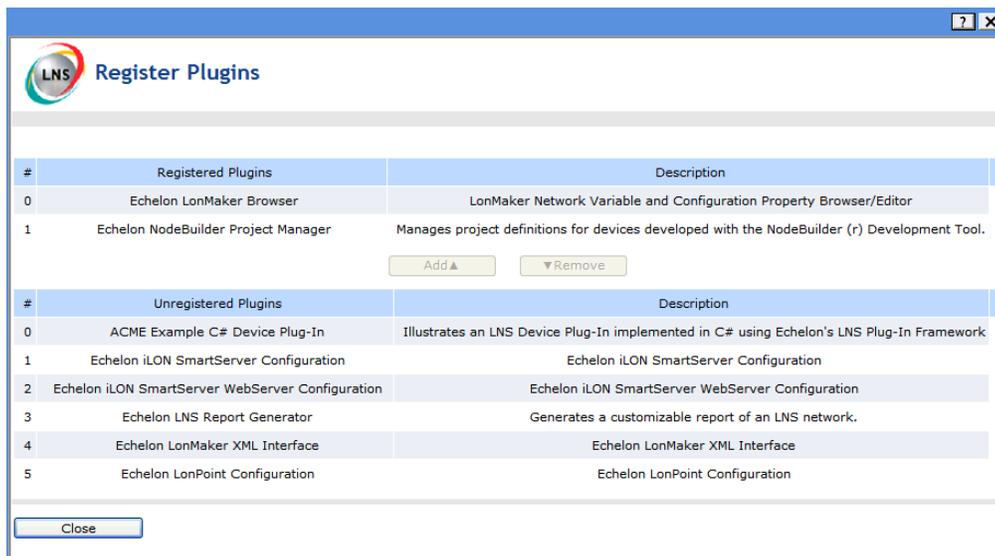
Each plug-in can implement multiple commands. For example, a plug-in may implement a **Configure** command for each functional block type used in a device. Each plug-in command may be associated with a device type, functional block type, a subsystem, or an entire network.

To use an OpenLNS or LNS plug-in, you must first register it from the subject network in the OpenLNS tree (this registers the plug-in with OpenLNS). After you register a plug-in, you can start the plug-in from the subject device or functional block in the LNS tree. To register and then start an OpenLNS or LNS Plug-in, follow these steps:

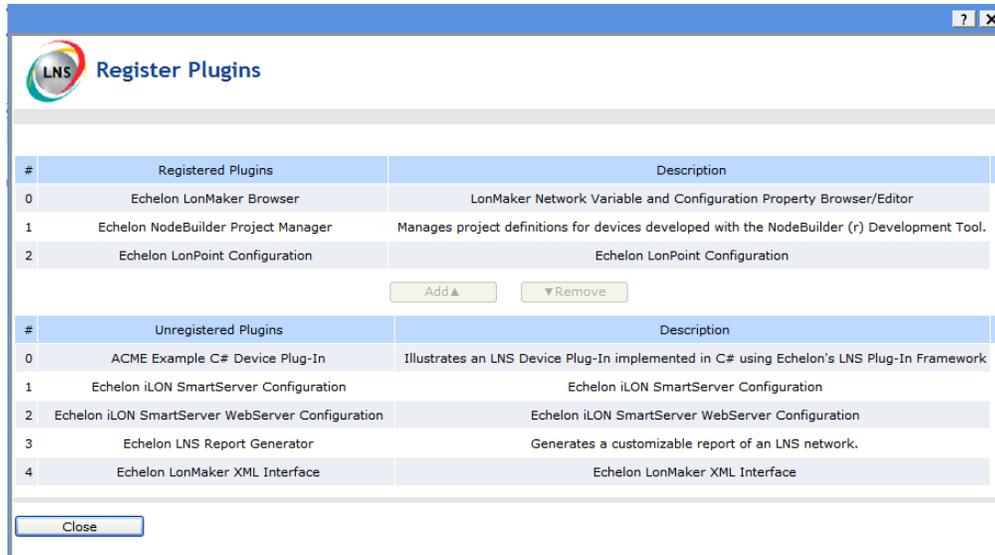
1. Verify that EES 2.2 and an OpenLNS Server or LNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Add an OpenLNS Server to the LAN following *Adding an OpenLNS Server to the LAN* in Chapter 3 of this document.
3. Right-click the subject network in the OpenLNS tree, and then click **Register Plug-ins**.



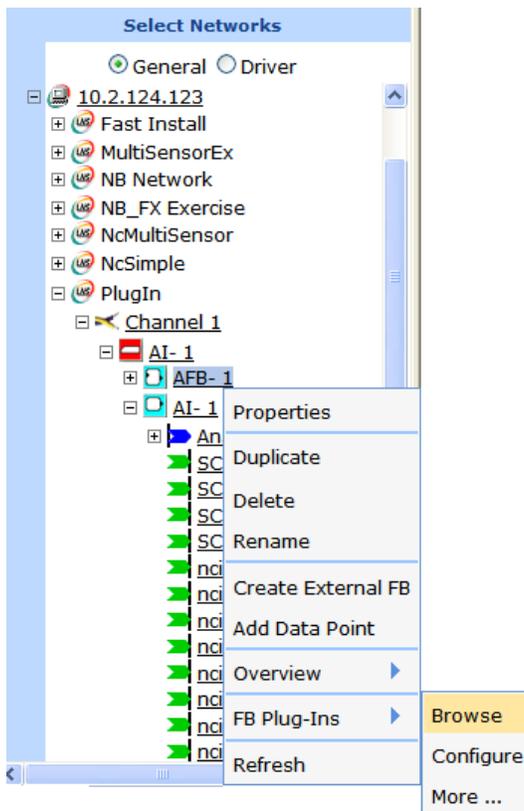
4. The **Register Plug-ins** dialog opens. This dialog lists the plug-ins installed on your computer that are currently registered or unregistered with OpenLNS.



5. Click the plug-in to be registered from the **Unregistered Plug-ins** list and then click **Add**.
6. The selected plug-in is moved to the **Registered Plug-ins** list.



- Click **OK** to register the plug-in with OpenLNS.
- Right-click the subject device or functional block in the OpenLNS tree, point to **Device Plug-ins** or **FB Plug-ins**, and then click **Browse** or **Configure** to start the plug-in that implements the selected command for the selected device or functional block. If you have installed OpenLNS CT, selecting **Browse** typically starts the OpenLNS Browser



You can click the **More** option to open the **Launch Plug-in** dialog and start other plug-ins that are registered for the same device or functional block.

- The plug-in that implements the selected command for the selected device or functional block starts. In this example, clicking **Browse** launches the OpenLNS Browser.

The screenshot shows a window titled "[PlugIn] LonMaker Browser - Untitled" with a menu bar (File, Edit, Browse, Help) and a toolbar. Below the toolbar is a table with the following columns: Subsystem, Device, Functional Block, Network Variable, Config Prop, Mon, and Value. The table contains 20 rows of configuration data for various subsystems and devices.

Subsystem	Device	Functional Block	Network Variable	Config Prop	Mon	Value
Subsystem 1	AI- 1	AFB- 1		SCPTmaxRcvT	N	0 0:00:20.000
Subsystem 1	AI- 1	AFB- 1		SCPTmaxSndT	N	0 0:00:05.000
Subsystem 1	AI- 1	AFB- 1		SCPTminSndT	N	0 0:00:00.000
Subsystem 1	AI- 1	AFB- 1		UCPTarbAluMode	N	ADD
Subsystem 1	AI- 1	AFB- 1		UCPTarbHysteresis	N	0
Subsystem 1	AI- 1	AFB- 1		UCPTarbLogicMode	N	RELAY
Subsystem 1	AI- 1	AFB- 1		UCPTarbMode	N	LOGIC
Subsystem 1	AI- 1	AFB- 1		UCPTdebounceT	N	0 0:00:00.015
Subsystem 1	AI- 1	AFB- 1		UCPTobjectMajorVer	N	2
Subsystem 1	AI- 1	AFB- 1		UCPTobjectMinorVer	N	0
Subsystem 1	AI- 1	AFB- 1		UCPTobjectType	N	3, 20005
Subsystem 1	AI- 1	AFB- 1		UCPTscaleParms	N	0, 0, 0, 0
Subsystem 1	AI- 1	AFB- 1		UCPTscalingEnbl	N	FALSE
Subsystem 1	AI- 1	AFB- 1	A_Out		II	89.6
Subsystem 1	AI- 1	AFB- 1	A_Out	SCPTovrValue	N	32
Subsystem 1	AI- 1	AFB- 1	A1		II	89.6
Subsystem 1	AI- 1	AFB- 1	A1	UCPTarbInputSrc	N	NV
Subsystem 1	AI- 1	AFB- 1	A1	UCPTarbSqrtEnbl	N	FALSE
Subsystem 1	AI- 1	AFB- 1	A1	UCPTconstInputFit	N	32
Subsystem 1	AI- 1	AFB- 1	A1	UCPTinputUsesMRT	N	TRUE

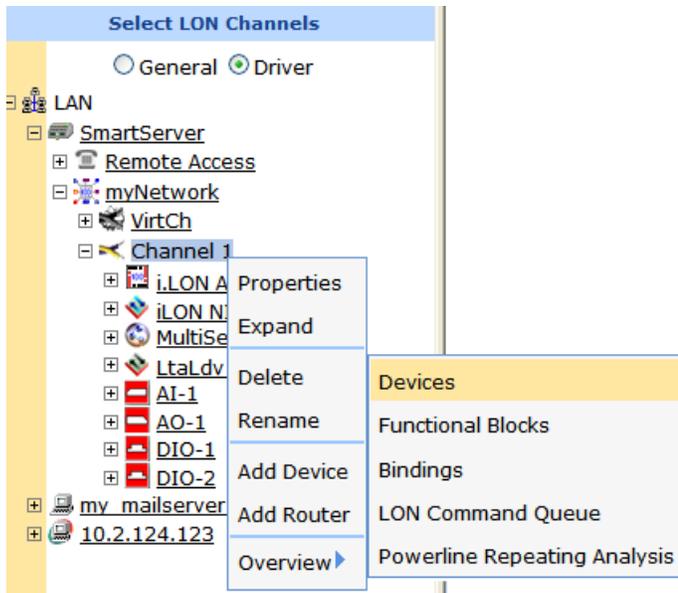
Viewing LONWORKS Devices

You can view and configure the all the LONWORKS devices in your network or on a specific channel using the **Overview – Devices** Web page. This Web page displays the statuses, subnet/node IDs, names, and Neuron IDs of the devices. You can also use this Web page to discover uncommissioned devices on the network, replace devices, and wink and test devices.

- In **General** mode, the **Overview – Devices** Web page displays the status, name, and parent channel for each device.
- In **Driver** mode, the **Overview – Devices** Web page displays the status, subnet/node ID, channel, name, Neuron ID, template (XIF or XML file), and location of each device, and you can use this Web page to re-name, upgrade, update the location string, wink, or test any device. In addition, you can use this Web page to install new devices that have been added to the network using the SmartServer's new device discovery feature, and you can replace devices that have failed using the new automatic device replacement feature.

To use the **Overview – Devices** Web page to view LONWORKS devices, follow these steps:

1. To configure, install, replace, or test devices, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click a LONWORKS network or channel in the SmartServer tree or OpenLNS tree, point to **Overview**, and then select **Devices**.



Note: You can select two or more channels and view all the devices on those channels in the same **Overview – Devices** page; however, the SmartServer’s performance may be impacted by trying to create large lists of objects.

3. The **Overview – Devices** Web page opens. For the LONWORKS channel on which the SmartServer is attached, this Web page by default displays the SmartServer's internal application device (**i.LON App**), local network interface used for polling external data points and testing external devices (**iLON NI**), LonTalk device (**LtaLdv**), and remote network interface (**RNI**), if being used.

	Subnet	Node	Channel	Device	Neuron ID	Replacement ID
0	1	3	Channel 1	i.LON App	03000028cd02	
1	1	4	Channel 1	iLON NI	03000028cd04	
2	1	5	Channel 1	MultiSensor	0700000095fe	
3	1	1	Channel 1	LtaLdv	03000028cd05	
4	1	6	Channel 1	AI-1	000256654500	
5	1	7	Channel 1	AO-1	000196794200	
6	1	8	Channel 1	DIO-1	00a145784600	
7	1	9	Channel 1	DIO-2	00a145791500	

4. You can sort the objects listed by clicking a property header.
5. View and /or configure the following properties:

Icon/Status Displays the icon used to represent the device in the SmartServer or OpenLNS tree and in the application frame. If the device is uncommissioned, offline, or not synchronized with the OpenLNS network database, this box is highlighted orange, red, or yellow, respectively.

Subnet Displays the channel (subnet) on which the device is attached. The **Node** property uniquely identifies the device on the subnet.

The subnet/node IDs begin with an address of 1/1 and increase sequentially to 1/2, 1/3, and so on for devices on the same channel

(subnet). For a second channel created on the network, the subnet/node IDs would begin with an address of 2/1 and increase sequentially to 2/2, 2/3, and so on.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

<i>Node</i>	<p>Displays the unique ID assigned to the device on the channel (subnet).</p> <p>This property is only displayed in Driver mode; it is not displayed in General mode.</p>
<i>Network</i>	<p>Displays the name of the device's parent network. This field is read-only. This property is only displayed if you opened this Web page by right-clicking the network icon.</p>
<i>Channel</i>	<p>Displays the name of the device's parent channel. This field is read-only.</p>
<i>Device</i>	<p>Displays the name of the device. In Driver mode, you can change the name. In General mode, this field is read-only.</p>
<i>Neuron ID</i>	<p>Displays the Neuron ID of the device. The Neuron ID is a unique 48-bit number that is manufactured into an external device or assigned to one of the SmartServer's 16 internal devices. This property is only displayed in Driver mode; it is not displayed in General mode.</p> <p>If the device is uncommissioned, 000000000000 is displayed. To get the Neuron ID of the device, select Auto-Assign Devices to Placeholders and then click Scan if the device is already attached to the network, or click the Continuously option if you are incrementally attaching the devices to the network.</p> <p>A message is broadcast to all the devices on the network that triggers the uncommissioned devices to identify themselves by their Neuron IDs. The SmartServer matches the uncommissioned devices on the network to the logical devices that you have added to the SmartServer or OpenLNS network based on program ID. The Neuron IDs of the uncommissioned devices appear in the Replacement ID properties, and under construction triangles appear to the right of their device icons.</p> <p>Click Submit to save the assignments of the discovered Neuron IDs to the devices.</p> <p>For more information on using the Overview – Devices Web page to get the Neuron IDs of uncommissioned devices, see <i>Automatically Acquiring the Neuron ID with Overview Devices Web Page</i> later in this chapter.</p>
<i>Replacement ID</i>	<p>Displays the Neuron ID of an uncommissioned device on the network that the SmartServer has discovered.</p> <p>This property is only displayed in Driver mode; it is not displayed in General mode.</p> <p>You can use the Overview - Devices Web page to replace devices quickly. You can attach a replacement device to the network, acquire its Neuron ID automatically using device discovery, and then assign the replacement device to the original device in the SmartServer or OpenLNS database. The SmartServer will then automatically exchange the configurations of the replacement and original devices, preserving the configuration of all the data points and configuration</p>

properties of the original device, and then commission the replacement device. For more information on using the **Overview – Devices** Web page to replace devices, see *Automatically Replacing Devices* later in this chapter.

Program ID Displays the unique, 16-hex digit ID that uniquely identifies the device application in the following format:
FM:MM:MM:CC:CC:UU:TT:NN [Format (F), Manufacturer ID (M), Device Class (C), Usage (U), Channel Type (T), Model Number (N)]. This field is read-only.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Template Displays the full path of the device interface (.xif or .XML file), which is the logical interface to the device. A device's interface specifies the functional blocks, network variables, configuration properties, and configuration property default values defined by the device's application.

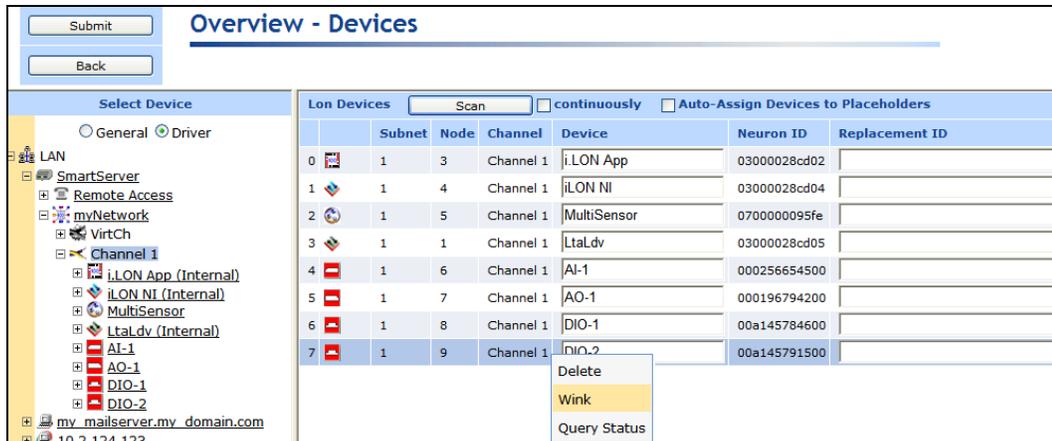
This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Geographical Position Displays the way point acquired or entered for the device. A way point is a set of coordinates (latitude and longitude) that identifies the device's location in physical space. This property is useful for outdoor lighting systems.

Typically, way points are acquired with a GPS receiver and then downloaded to the SmartServer using SOAP/HTTP messages over the console port.

Alternatively, you can enter a description of the device

6. Optionally, you can wink or test discovered devices. To do this, right-click anywhere in the device's row and then click **Wink** or **Query Status** on the shortcut menu.
 - You can wink a device to identify it on the network and verify that it is communicating properly. A device that supports the Wink command generates an application-dependent audio or visual feedback such as a beep or a flashing service LED when winked. Wink commands are typically used when installing or diagnosing multiple devices in a system, where a network tool may be needed to confirm the identity of a given device.
 - You can test a device to open the **Query Status** dialog and view network statistics such as the number of message transmission and receipt errors, transaction timeouts, and the number of missed or lost messages that indicate whether the device is operating and is configured correctly, and to view the current device configuration and application state. For more information on the **Query Status** dialog, see *Querying Devices* later in this chapter.

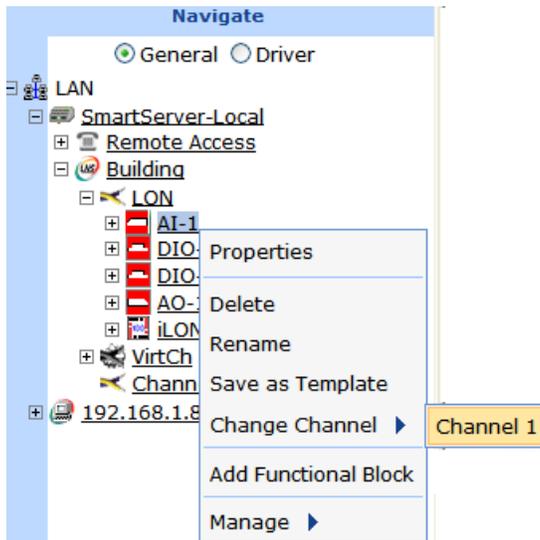


7. Click **Submit** to save any changes.

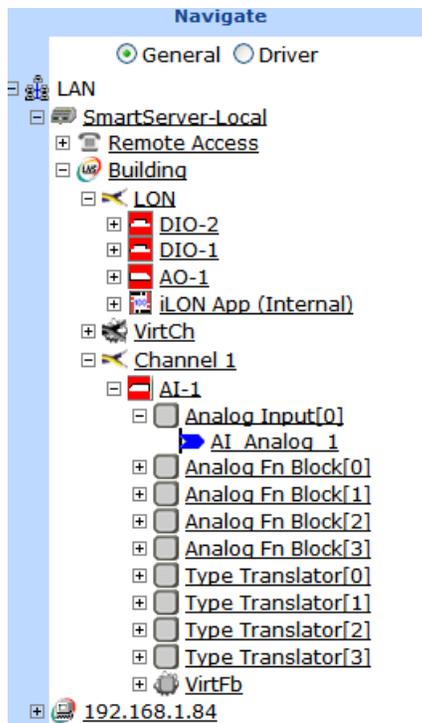
Changing the Channel of Devices

You can physically move a device to a different compatible channel and then logically move the device in the SmartServer or OpenLNS tree. You can move an application device, preserving the device's configuration and all of its connections, and you can move the near or far side of a router. To move a device to a different channel, follow these steps:

1. Physically remove the device from the source channel and attach it to the destination channel.
2. Right-click the device to be moved logically, point to **Change Channel**, and then click a compatible destination channel on the shortcut menu.



3. Click **Submit**.
4. The device and all of its children functional block and data points are logically removed from the source channel and they are added to the tree of the selected destination channel.



Creating and Configuring LONWORKS Routers

A *router* enables application devices on separate channels to communicate. The router may be a LonPoint router, an MPR-50 Multi-Port Router, a SmartServer with IP-852 routing, an i.LON 600 LONWORKS/IP Server, a SmartServer, or other compatible ISO/IEC 14908-1 (Control Network Protocol [CNP]) or ISO/IEC 14908-4 (IP-852) router.

You can use a single router to connect two channels or use multiple *redundant routers* between the same pair of channels. You can also use an MPR-50 Multi-Port Router to connect up to four TP/FT-10 free topology twisted-pair channels, or to connect one or more FT/TP-10 channels to a TP/XF-1250 high-speed backbone. See the *MPR-50 Multi-Port Router User's Guide* for more information on installing and using the MPR-50 Multi-Port Router.

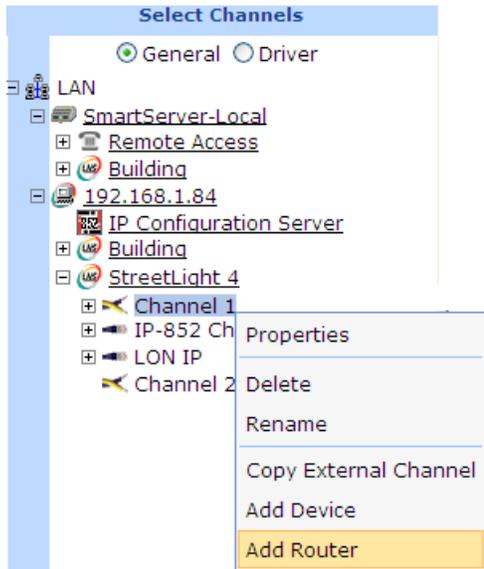
To add a router you first define the router and then commission it. To define a router, you enter the router name, specify the router type, and select the channel connected to the far side of the router. To commission a router, you associate the physical router on the network with the router you created with the SmartServer. See *Installing LONWORKS Networks* in this chapter for more information on commissioning devices.

Creating LONWORKS Routers

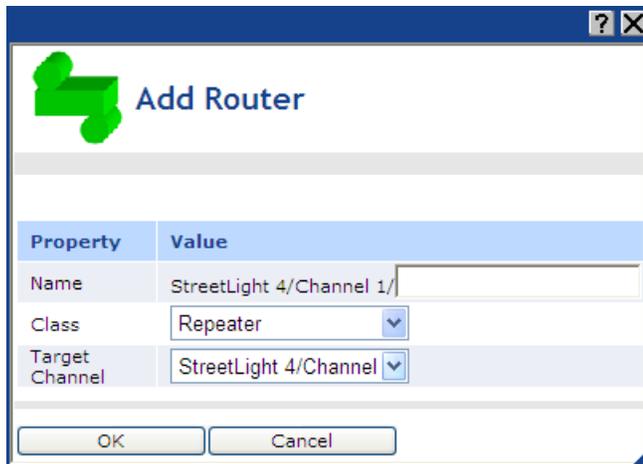
To create a LONWORKS router follow these steps:

1. If you are creating a router from the SmartServer tree, verify that the SmartServer has access to an OpenLNS network database. This means that an OpenLNS Server is on the LAN, you are operating the SmartServer in LNS mode (you cannot attach a router to a network that is being managed in standalone mode), and you have specified an OpenLNS Server and OpenLNS network database to be updated with network configuration changes made with the SmartServer. See *Creating and Configuring LONWORKS Networks* for more information on setting these properties.
2. Verify that there are at least two channels in the network to connect. If there is only one channel, you cannot create a router. See *Creating LONWORKS Channels* for how to add another channel to the network.

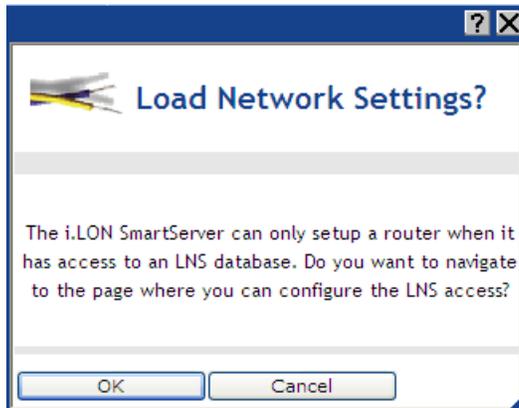
3. Right-click the LONWORKS channel to be attached to the near side of the router, and then select **Add Router** on the shortcut menu.



4. The **Add Router** dialog opens:



Note: If the SmartServer does not have access to an OpenLNS network database (an OpenLNS Server or LNS Server has not been added to the LAN, an OpenLNS Server and OpenLNS network database have not been specified, or the SmartServer is operating in standalone mode), the **Load Network Settings?** dialog opens when you attempt to create a router. Click **OK** to go to the **Setup – LON Network Driver** Web page to enable the SmartServer to access an OpenLNS network database. Click **Cancel** to stop the router creation process.



5. In the **Name** property, enter a name for the router that is unique to the network (router names are case sensitive).
6. In the **Class** property, select one of the following six router types:
 - **Configured.** The router determines which packets to forward based on internal routing tables. These routing tables contain one entry for each subnet and group in the application domain. Whenever a router receives a packet, it examines the source and destination subnet or group ID to determine whether to forward the packet. This is the most common type because it optimizes network traffic for both subnet/node ID and group addressed messages, and enables the channels on which devices are attached to be determined automatically. Configured routers also support the use of redundant routers (multiple routers connecting two channels), which provide for redundant message paths and greater system reliability.
 - **Learning.** Like a configured router, the router determines which packets to forward based on internal routing tables. Learning routers, though, have their routing tables stored in volatile memory; therefore, the router forwards packets addressed to all subnets in the application domain after being reset. Whenever a learning router receives a packet from one of its channels, it uses the source subnet ID to learn the network topology. It sets the corresponding routing table entries to indicate that the subnet in question is to be found in the direction from which the packet was received. A learning router always forwards all group-addressed messages.
 - **Repeater.** The router forwards all valid packets received on one channel to the other channel. Subnets cannot span non-permanent repeaters. You can use a non-permanent repeater to maintain flexibility in order to change the router type later. This is the default.
 - **Bridge.** The router forwards all valid packets that match the network domain. Subnets cannot span non-permanent bridges. You can use a non-permanent bridge to maintain flexibility in order to change the router type later.
 - **Permanent Repeater.** The router behaves like a repeater, except that you cannot change the router type after the router has been created. Subnets may span permanent repeaters. You can use permanent repeaters to preserve subnet IDs.
 - **Permanent Bridge.** The router behaves like a bridge, except that you cannot change the router type after the router has been created. Subnets may span permanent bridges. You can use permanent bridges to preserve subnet IDs.
 - Select **Unknown** to have the SmartServer automatically select the appropriate router type.
7. In the **Target Channel** property, select the channel to be attached to the far side of the router.
8. Click **OK**. Router icons are added underneath the channels on the near and far sides of the router. You can expand the router icon to show a reference to the opposite side of the router.
9. Click **Submit**.

Configuring LONWORKS Routers

You can use the driver properties to install, configure, and test routers. To configure the properties of a router, follow these steps:

1. Click **Driver**.
2. Select one or more routers to configure.
 - To configure one router, click the router. Alternatively, you can right-click the router and select **Properties** on the shortcut menu.
 - To configure two or more routers, click one router and then either hold down CTRL and click all other routers to be configured or hold down SHIFT and select another router to configure the entire range of routers. Alternatively, you can select multiple routers, right-click one of the selected routers, and then click **Properties** on the shortcut menu.
3. The **Setup – LON Router Driver** Web page opens.

Setup - LON Router Driver

Submit Back

Select LON Routers
 General Driver

LAN
 SmartServer-Local
 Remote Access
 Building
 192.168.1.84
 IP Configuration Server
 Building
 StreetLight 4
 Channel 1
 DIO-1
 iLON SmartServer- 1
 LNS Network Interface
 RTR- 1
 IP-852 Channel
 LON IP
 Channel 2

Name: StreetLight 4/Channel 1/RTR- 1
 Description:

Lon Device Property		Value
Icon		Router
Hidden		<input type="checkbox"/>
<input type="checkbox"/> Smart Network Management	Progress	Identification Property
		Value
		Neuron ID
		800000048C50
<input type="checkbox"/>		Program ID
		8000010101000000
		Maximum Number of Dynamic Functional Blocks
		0
		Maximum Number of Dynamic Data Points
		0
		Geographical Position
		Location ID
		800500000000 HEX
		Primary Address (Domain.Subnet.Node)
		65.1.7
		Secondary Address (Domain.Subnet.Node)
		..
		Maximum Number of Simultaneous Transactions
		Maximal Lifetime of Transactions
		Milliseconds
<input type="checkbox"/>	Unknown	Commission Status
		Commissioned
<input type="checkbox"/>	Unknown	Application Status
		Application Stopped (Offline)
<input type="checkbox"/>		Reset
Router Property		Value
	Far Side	StreetLight 4/IP-852 Channel/RTR- 1
	Class*	Configured
<input type="checkbox"/>	Use Authentication** **	

* Reset required if changed
 ** Only available in Secure Access mode

4. Configure the following router properties:

<i>Name</i>	Displays the network path of the router in the following format: <code><network>/<channel>/<router></code> . This field is read-only.
<i>Handle</i>	Displays the handle of the channel assigned by the OpenLNS Server. This field is read-only.
<i>Description</i>	Enter an optional description of the router. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Lon Device Property

- Icon* Displays the icon used to represent the router in the SmartServer tree or OpenLNS tree and in the application frame. The default icon is **Router**. You can change the icon for the router by selecting a different icon and then clicking **Submit**.
- Hidden* Hides the router in the SmartServer tree or OpenLNS tree. If this router is not actively being used, you can hide it to simplify the web interface.
- To show a hidden router icon, click **Settings**. In the **Global Settings** dialog, select the **Devices** check box in the **Display Hidden** property and then click **Close**.

Identification Property

- Neuron ID* Displays the current Neuron IDs for the respective side of the router. The Neuron ID is a unique 48-bit number that is manufactured into the router. The Neuron ID is acquired by using Smart Network Management, pressing a service pin on the router, or manually entering it. Commissioning assigns a logical address (Subnet/Node ID) to the router.
- You can click **Use Service Pin** to acquire the Neuron ID of the router.
- Program ID* Displays the program ID of the router as a set of hex digits. The program ID is manufactured into the router and cannot be changed.
- Select the **Smart Network Management** check box to have the SmartServer fetch the program ID of the router.
- Geographical Position* Displays the waypoint of the router. A waypoint is a set of coordinates (latitude and longitude) that identifies the router's location in physical space. Typically, waypoints are acquired with a GPS receiver and then uploaded to the SmartServer using SOAP/HTTP messages over the console port.
- Alternatively, you can manually enter the waypoint in this field or enter a description of the router location.
- Location ID* Displays the 6-byte location string that documents the router's location within the network.
- Primary Address (Domain.Subnet.Node)* Displays the domain ID of the network, and the subnet and node IDs assigned to the near and far sides of the router by the OpenLNS Server when the router is created.
- The subnet/node ID is used for addressing messages. The subnet ID identifies the channel (subnet) on which the router side resides, and the node ID identifies the router side attached to the channel.
- The subnet/node IDs begin with an address of 1/1 and increase sequentially to 1/2, 1/3, and so on for devices and router sides on the same channel (subnet). For a second channel created on the network, the subnet/node IDs for devices and router sides would begin with an address of 2/1 and increase sequentially to 2/2, 2/3, and so on.
- Secondary Address (Domain.Subnet.Node)* If the router is a member of another network, displays the domain ID of that network and the device's subnet and node ID on it.

<i>Commission Status</i>	<p>Indicates the current router configuration: Commissioned, Uncommissioned, or Never Reached.</p> <p>To have the SmartServer automatically set the router configuration, select Smart Network Management and click Submit.</p> <p>To manually select the configuration for one or more routers, select the desired configuration from the list to the right, select Smart Network Management to the left, and then click Submit.</p> <p>Alternatively, you can manually set the configuration for one or more routers by selecting the routers, right-clicking one router, pointing to Manage, and then clicking Commission or Decommission in the shortcut menu.</p>
<i>State</i>	<p>Indicates the current state of the router application: Application Running (Online), Application Stopped (Offline), or Never Reached.</p> <p>To have the SmartServer automatically set the state of the router application, select Smart Network Management and click Submit.</p> <p>To manually set the application state for one or more routers, select the desired state from the list to the right, select Smart Network Management to the left, and then click Submit.</p> <p>Alternatively, you can manually set the application state for one or more routers by selecting the routers from the SmartServer or OpenLNS tree, right-clicking one router, pointing to Manage, and then clicking Set Online or Set Offline in the shortcut menu.</p>
<i>Reset</i>	<p>Resetting a router stops the router application, terminates all incoming and outgoing messages, sets all temporary settings to their initial values, and then restarts the router application.</p> <p>To have the SmartServer reset the router, select Smart Network Management and then click Submit.</p> <p>Alternatively, you can manually reset or one or more routers by selecting the routers in the SmartServer or OpenLNS tree, right-clicking one router, pointing to Manage, and then clicking Reset in the shortcut menu.</p>

Router Property

<i>Far Side</i>	Displays the network path of the channel attached to the far side of the router in the following format: <code><network>/<channel>/<router></code> .
<i>Class</i>	You can change the router to one of the following six types: Configured , Learning , Repeater , Bridge , Permanent Repeater , or Permanent Bridge . If you change the router type, you must reboot the SmartServer to implement the change. See the previous section, <i>Creating LONWORKS Routers</i> , for more information on these router types.
<i>Use Authentication</i>	Enables authentication to be used for communication with this router. If the SmartServer is in secure access mode and authentication is enabled, you can enter a 16-digit hexadecimal MD5 authentication key. If you change the authentication key, you must reboot the SmartServer to implement the change.

5. Click **Submit**.

Creating and Configuring Functional Blocks

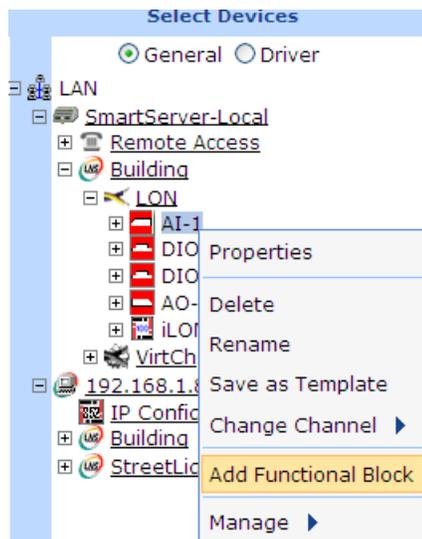
A *functional block* encapsulates a set of network variables and configuration properties that perform a specific device function. For example, a four-port digital input device could have functional blocks for each of its four switches. Each functional block would contain an output network variable representing the state or setting of a switch. In addition, each functional block could contain configuration properties that control how frequently the switch data is transmitted to other functional blocks. Ultimately, the task that the functional block performs in this example is transmitting the switch data to other functional blocks (another functional block receiving the switch data could then use it to turn a lamp on or off).

There are two types of functional blocks: static and dynamic. A *static functional block* is defined by the device application. Because static functional blocks are statically defined by the device application, creating a static functional blocks is simply a method for showing a functional block that has previously been hidden. Conversely, a *dynamic functional block* is not pre-loaded on the device; therefore adding a dynamic functional block actually does modify the device interface. Dynamic functional blocks are typically added to controllers that have a dynamic interface (the SmartServer with the v40 interface active, for example). To check whether a device supports dynamic functional blocks, click the device, click **Driver**, and view the **Maximum Number of Dynamic Functional Blocks** property.

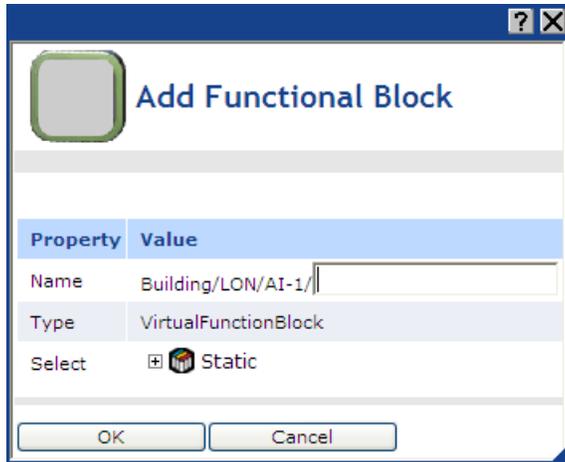
Creating Functional Blocks

To create a functional block, follow these steps:

1. Right-click a LONWORKS device, and then select **Add Functional Block** on the shortcut menu.



2. The **Add Functional Block** dialog opens:



3. In the **Name** property, enter a name for the functional block that is unique to its parent device (functional block names are case sensitive). Alternatively, you can accept the default programmatic name that appears after you select the functional block. For example, if you do not enter a name and then select an analog functional block, **Analog Fn Block** <instance number> appears in this field.
4. In the **Select** property, select the type of functional block to be created: **Static** or **Dynamic**. The **Dynamic** option is only available for devices with dynamic interfaces such as a SmartServer with the v40 interface active.
 - **Static**. Expand the static entry to show all the static functional blocks programmatically defined by the device's interface. Click the static functional block to be created. You can create multiple static functional blocks at once by clicking a static functional block, and then either holding down CTRL and clicking the other static functional blocks to be created, or holding down SHIFT and selecting another functional block to create the entire range of static functional blocks.
 - **Dynamic**. Expand the dynamic entry to show all the folders in the lonworks/types directory on the SmartServer (if you are adding a functional block to a device in the SmartServer tree) or on the OpenLNS Server (if you are adding a functional block to a device in the OpenLNS tree). Then expand a folder in a lonworks/types directory to show the functional profiles (SFPTs and UFPTs) available in that folder. Click the functional profile to be used for creating the functional block.
5. The **Type** property displays the functional profile that is valid for this functional block in the following format: #<device program ID>[scope selector]. <functional profile name>.
6. Click **OK**. The selected functional block is added underneath its parent device.
7. Click **Submit**.

Configuring Functional Blocks

You can use the driver properties to change the icon used to represent the functional block in the navigation pane and in the application frame and select whether the functional block is hidden in the tree. To configure the properties of a functional block, follow these steps:

1. Click **Driver**.
2. Select one or more functional blocks to configure.
 - To configure one functional block, click the functional block. Alternatively, you can right-click the functional block and select **Properties** on the shortcut menu.

- To configure two or more functional blocks, click one functional block and then either hold down CTRL and click all other functional blocks to be configured or hold down SHIFT and select another functional block to configure the entire range of functional blocks. Alternatively, you can select multiple functional blocks, right-click one of the selected functional blocks, and then click **Properties** on the shortcut menu.

3. The **Setup – LON Functional Block Driver** Web page opens.



4. Configure the following functional block properties:

- | | |
|-------------------------------|--|
| <i>Name</i> | Displays the network path of the functional block in the following format: <i><network>/<channel>/<device>/<functional block></i> . This field is read-only. |
| <i>Functional Block Index</i> | Displays the index number of the functional block within its associated device. This field is read-only. |
| <i>Description</i> | Enter an optional description of the functional block. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports. |

LON Functional Block Property

- | | |
|-------------------------|--|
| <i>Icon</i> | Displays the icon used to represent the functional block in the SmartServer tree or OpenLNS tree and in the application frame. The default icon is DefaultFB for all functional blocks that do not have icons defined for them. You create custom icons for your functional blocks (See <i>Using Custom Device and Functional Block Icons</i> in Chapter 4 for how to do this).

You can change the icon for the functional block by selecting a different icon and then clicking Submit . |
| <i>Hidden</i> | Hides the functional block in the SmartServer tree or OpenLNS tree. If this functional block is not actively being used, you can hide it to simplify the web interface.

To show a hidden functional block icon, click Settings . In the Global Settings dialog, select the Functional Blocks check box in the Display Hidden property and then click Close . |
| <i>Functional Block</i> | Displays the functional profile that is valid for this functional block in the |

<i>Type</i>	<p>following format: #<device program ID>[scope selector]. <functional profile name>. This field is read-only.</p> <p>For dynamic functional blocks, you can click the button to the right to open the Select Type dialog, where you can change the functional profile used by the functional block. See <i>Creating Functional Blocks</i> for selecting a functional profile for a dynamic functional block.</p> <p>The scope selector specifies the context in which the network variables and configuration properties within a functional block are interpreted. The scope selector may be any of the following values:</p> <ol style="list-style-type: none"> 0. Standard functional profile defined in the standard resource file set. 3. User-defined functional profile, defined in a manufacturer-specific resource file set. 4. User-defined functional profile, defined in a manufacturer and device class specific resource file set. 5. User-defined functional profile, defined in a manufacturer and device class/subclass specific resource file set. 6. User-defined functional profile, defined in manufacturer, and device class/subclass/model number specific resource file set.
<i>Static/Dynamic</i>	Indicates whether the functional block is static or dynamic. This field is read-only.

5. Click **Submit**.

Viewing Functional Blocks

You can use the **Overview – Functional Blocks** Web page to view the indexes, statuses, names, and types of the LONWORKS functional blocks in your network. If you open this Web page from the default **LON** channel in the SmartServer tree, this Web page displays the functional blocks in the SmartServer's internal application device (**i.LON App**) and virtual device (**i.LON System**) by default. To view functional blocks with this Web page, follow these steps:

1. To rename functional blocks, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click a LONWORKS channel or device in the SmartServer tree or OpenLNS tree, point to **Overview**, and then select **Functional Blocks**.

Note: You can select two or more channels or devices and view all the functional blocks on those channels or devices in the same **Overview – Functional Blocks** page; however, the SmartServer's performance may be impacted by trying to create large lists of objects.

3. The **Overview – Functional Blocks** Web page opens.
4. You can sort the objects listed by clicking a property header.
5. View and /or configure the following properties:

<i>Icon/Status</i>	Displays the icon used to represent the functional block in the SmartServer or OpenLNS tree and in the application frame. If the functional block is not configured or not synchronized with the OpenLNS network database, a symbol or yellow highlighting indicating the functional block's status appears to the right of the icon.
--------------------	---

<i>Functional Block Index</i>	Displays the index number of the functional block within its associated device. This field is read-only.
-------------------------------	--

This property is only displayed in **Driver** mode; it is not displayed in

General mode.

<i>Channel</i>	Displays the name of the functional block's parent channel. This field is read-only.
<i>Device</i>	Displays the name of the functional block's parent device. This field is read-only.
<i>Fb</i>	Displays the name of the functional block. In Driver mode, you can change the name. In General mode, this field is read-only.
<i>Functional Block Type</i>	Displays the functional profile that is valid for this functional block in the following format: #< device program ID >[scope selector]. <functional profile name>. This field is read-only.

For dynamic functional blocks, you can change the functional profile used by the functional block in the **Select Type** dialog that you can open from the functional block's **Setup – Functional Block Driver** Web page. To open this Web page, click the **Driver** option above the navigation pane on the left side of the SmartServer Web interface, and then click the data point.

The scope selector specifies the context in which the data points within a functional block are interpreted. The scope selector may be any of the following values:

- **0.** Standard functional profile defined in the standard resource file set.
- **3.** User-defined functional profile, defined in a manufacturer-specific resource file set.
- **4.** User-defined functional profile, defined in a manufacturer and device class specific resource file set.
- **5.** User-defined functional profile, defined in a manufacturer and device class/subclass specific resource file set.
- **6.** User-defined functional profile, defined in manufacturer, and device class/subclass/model number specific resource file set.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

6. Click **Submit** to save any changes.

Creating, Configuring, and Connecting LONWORKS Data Points

LONWORKS data points (network variables and configuration properties) allow an application device to send and receive data over the network to and from other devices. LONWORKS data points are data items (such as temperature, the state of a switch, or actuator position setting) encapsulated within functional blocks that a particular device application expects to receive from other physical devices (an *input network variable*) or expects to make available to other physical devices (an *output network variable*).

The SmartServer can support up to 3,000 LONWORKS data points. LONWORKS data points include data points defined on external devices (formerly referred to as NVEs) and the data points defined on the internal devices stored on the SmartServer including the SmartServer itself (formerly referred to as NVLs).

There are two types of LONWORKS data points: static and dynamic. A *static data point* is defined by the device application and is always available in the functional block. Most LONWORKS devices have

functional blocks that include static data points. Because static data points are statically defined by the device application, creating a static data point is simply a method for showing a data point that has previously been hidden or deleted. Conversely, a *dynamic data point* is not pre-loaded on the device; therefore adding a dynamic data point actually does modify the device interface. Some LONWORKS devices support dynamic data points (for example, the SmartServer with the v40 interface active). Other types of devices that support dynamic data points include controllers and gateways with dynamic interfaces. To check whether a device supports dynamic data points, click the device, click **Driver**, and view the **Maximum Number of Dynamic Data Points** property in the **Setup - LON Device Driver** Web page. Typically, you add dynamic data points to a functional block after the device has been commissioned.

You can create LONWORKS connections to bind the network variables in the OpenLNS tree via the LNS Proxy Web service, or in the SmartServer tree in standalone mode. Once you create LONWORKS connections, the target network variables will receive all updates from the hub (source) network variable in the connection.

You can also bind LONWORKS data points in the SmartServer tree using Web connections. The major difference between LONWORKS connections and Web connections is that LONWORKS connections propagate data point updates over a LONWORKS channel via the LonTalk Protocol or the LonTalk protocol tunneled through an IP-852 channel. Web connections propagate data point updates via SOAP/HTTP over a TCP/IP network. Web connections also provide an alternative solution to LONWORKS connections over an IP-852 channel for connecting devices over multiple networks; however, Web connections are much slower (40 data point updates per second) than LONWORKS IP-852 connections (more than 1,000 updates per second).

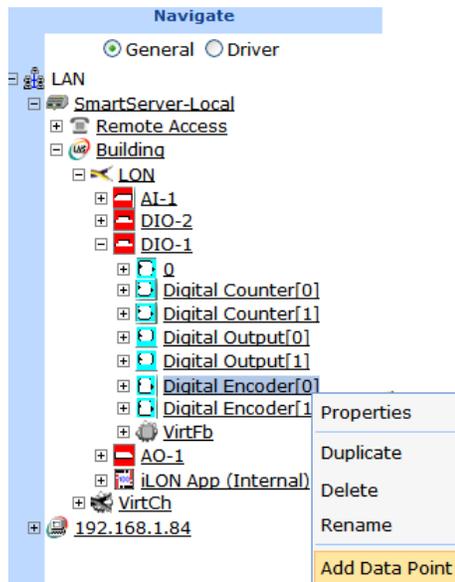
See *Creating Web Connections* in Chapter 4 for more information on binding data points in the SmartServer tree with Web Connections.

The following section describes how to create, configure, and connect LONWORKS data points.

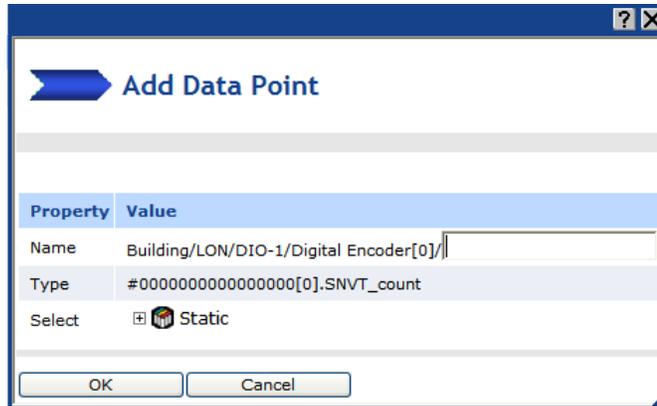
Creating LONWORKS Data Points

To create a LONWORKS data point, follow these steps:

1. Right-click a LONWORKS functional block, and then select **Add Data Point** on the shortcut menu.



2. The **Add Data Point** dialog opens:



3. In the **Name** property, enter a name for the data point that is unique to its parent functional block (data point names are case sensitive) or accept the default programmatic name that appears after you select the data point type. For example, if you do not enter a name and then select the first analog input data point for an analog functional block, **AFB_A1_1** appears in this field.
4. In the **Select** property, select the type of data point to be created: **Static** or **Dynamic**. The Dynamic option is only available for functional blocks representing the SmartServer's built-in applications, virtual functional blocks, and devices with dynamic interfaces such as the SmartServer with the V40 interface active.
 - **Static**. Expand the static node to show all the static data points programmatically defined for the functional block by the device's external interface. Click the static data point to be created.
 - **Dynamic**. Expand the dynamic node to show all the folders in the **lonworks/types** directory on the SmartServer (if you are adding a data point to a functional block in the SmartServer tree) or on the OpenLNS Server (if you are adding a network variable to a functional block in the OpenLNS tree). Expand a folder in the **lonworks/types** directory to show all the available resource files in that folder. Expand a resource file and then expand its configuration property types or network variable types to show all the available SNVTs, UNVTs, or built-in data types in that file. Click the SNVT, UNVT, or built-in data type to be used by the data point.
5. The **Type** property displays the data type (SNVT, UNVT, or built-in data type) used by the selected data point in the following format: `#<manufacturer ID>[scope selector].<type name>`.
6. Click **OK**. The data point is added underneath the icon of its parent functional block.
7. Click **Submit**.

Configuring LONWORKS Data Points

You can configure data points in both **General** and **Driver** modes. In **General** mode, you can click a LONWORKS data point to open the **Configure - Data Point** Web page. You can use this Web page to view or configure the following properties for that LONWORKS data point: alias name, whether a constant, default and invalid values, format description (read only), whether its unit string is made available to applications, network performance configuration properties (heartbeat, throttle, offline, and send on delta), presets, and unit strings used for the fields of structured data points.

In **Driver** mode, you can click a LONWORKS data point to open the **Setup – LON Data Point Driver** Web page. You can use this Web page to view or configure the following properties for that LONWORKS data point: poll rate, direction, whether it is static or dynamic, length, and format description. In addition you can change the icon used by the data point in the navigation pane and application frame and select whether the data point is hidden or shown in the tree.

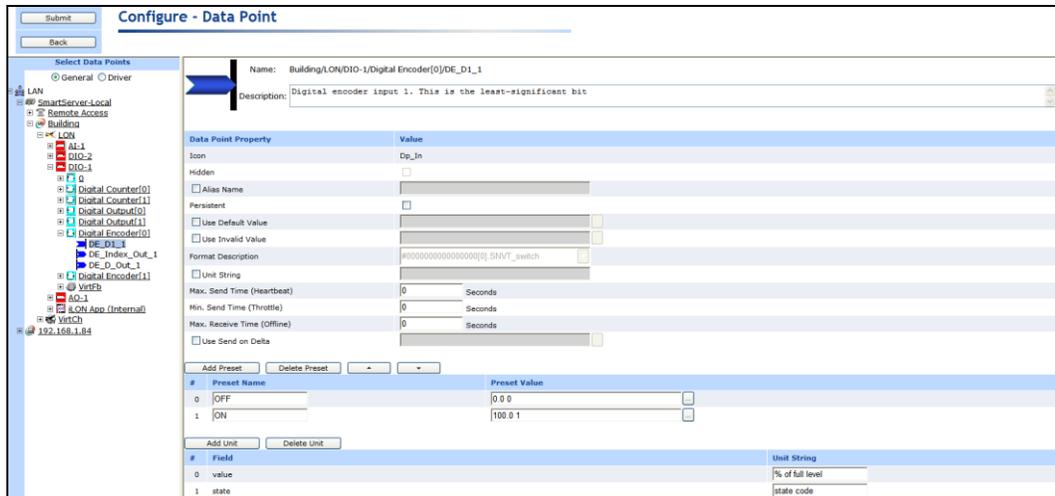
The following table summarizes the different properties you can set for LONWORKS data points in **General** and **Driver** modes.

General (Configure - Data Point Web page)	Driver (Setup – LON Data Point Driver Web page)
Name	Name, NV Index, Selector
Description	Description
Icon	Icon (read-only)
Hidden	Hidden (read-only)
Alias Name	Poll Rate
Persistent	Direction
Use Default Value	Static/Dynamic
Use Invalid Value	Authentication
Format Description (read-only)	Length
Unit String	Format Description
Max Send Time (Heartbeat)	
Min Send Time (Throttle)	
Max Receive Time (Offline)	
Use Send On Delta	
Presets	
Fields	

Configuring Data Point General Properties

To configure the general properties of a data point, follow these steps:

1. Click **General**.
2. Select one or more data points to configure.
 - To configure one data point, click the data point. Alternatively, you can right-click the data point and select **Properties** on the shortcut menu.
 - To configure two or more data points, click one data point and then either hold down CTRL and click all other data points to be configured or hold down SHIFT and select another data point to configure the entire range of data points. Alternatively, you can select multiple data points, right-click one of the selected data points, and then click **Properties** on the shortcut menu.
3. The **Configure - Data Point** Web page opens.



4. Configure the following data point properties:

Name Displays the network path of the data point in the following format: *<network>/<channel>/<device>/<functional block>/<data point>*. This field is read-only.

Description Enter an optional description of the functional block. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Data Point Property

Icon Displays the icon used to represent the data point in the SmartServer or OpenLNS tree. This field is read only.

You can change the icon by clicking **Driver**, clicking the data point in the tree, and selecting a different icon in the **Icon** property on the **Setup - <Driver> Data Point Driver** Web page.

Hidden Indicates whether the data point icon is hidden or shown in the SmartServer or OpenLNS tree. This field is read only.

You can hide the data point icon in the tree by clicking **Driver**, clicking the data point, and selecting the **Hidden** check box on the data point's **Setup - <Driver> Data Point Driver** Web page.

To show a hidden data point icon, click **Settings**. In the **Global Settings** dialog, select the **Data Points** option in the **Display Hidden** property and then click **Close**.

Alias Name Select this option to enable the data point alias name to be made available to the navigation pane, SmartServer built-in applications (for example, Alarm Notifier), and i.LON Vision objects. If you select this option, you can edit the default alias name or create an alias name by entering a unique string that describes the data point.

The alias name was the naming convention used for data points in the e3 release of the i.LON software. The data points in the tree were organized by their source devices.

- The data points on the **i.LON App (Internal)** device under the **LON** channel have default alias names that begin with the “NVL” prefix.
- The virtual data points on the **i.LON System (Internal)** device under

the **VirtCh** channel have default alias names that begin with the “iLON System” prefix. In the e3 release of the iLON software, these data points were referred to as “NVVs”.

- The data points of the external devices connected to the SmartServer do not have default alias names, and this property is initially disabled for these data points. In the e3 release of the iLON software, these data points were referred to as “NVEs”.

<i>Persistent</i>	Enables the current value stored in the data point to persist through a SmartServer reboot. Selecting this option enables the Use Default Value property and stores the current data point in it. Configuration properties are marked as persistent by default.
<i>Use Default Value</i>	Enables you to define a default value that the data point will use if the SmartServer is reset. To set a default value, select this option and enter a value. If this check box is cleared, the data point value will be set to 0 and its status will be set to AL_NUL when the SmartServer is reset.
<i>Use Invalid Value</i>	Enables you to define an invalid value that if reached, the data point status is set to AL_INVALID. You can have an Alarm Notifier send an alarm notification any time this occurs. See <i>Alarming</i> in Chapter 7 for more information on how to do this.
<i>Format Description</i>	<p>Displays the data point’s program ID; data type (SNVT, SCPT, UNVT, UCPT, or built-in data type); and format (for example, SI metric or US customary if the type has multiple formats such as SNVT_temp_p). The format description is displayed in the following format: #<manufacturer ID>[<scope selector>,<type name>].</p> <p>For data points with multiple formats such as SNVT_temp_p, you can change the format used for the data point in the Format Description property on the Setup - LON Data Point Driver Web page.</p> <p>For dynamic data points or data points with changeable types, you can change the data point’s type and/or format from the Setup - LON Data Point Driver Web page. To do this, click Driver and then click the box to the right of the Format Description property. The Select Types dialog opens and you can select a different type and/or format for the data point.</p>
<i>Unit String</i>	<p>For scalar and enumerated data points, displays the units of measures used by the data point. For example, the unit string of a SNVT_temp_f data point is ”degrees F.” The unit string is defined by resource files.</p> <p>For structured data points, displays the fields within the data point. Using a SNVT_setting data point for example, function, setting, and rotation is displayed in this property. You can edit the unit strings of the fields of a structured data point in the Fields property located at the bottom of this Web page.</p> <p>By default, the Unit String option is selected, meaning that the unit string is displayed on the SmartServer Web pages. You can edit the unit string and the revised unit string will appear in the SmartServer Web pages. You can clear Unit String to disable the appearance of the unit string.</p> <p>Note: To use the double quote (”) character in a unit string, you must escape it with another double quote. For example, to use a single double quote character to represent inches, enter two double quotes (”). If you do not escape the double quote, the Data Logger: View Web page may not display the data point value.</p>

*Max Send Time
(Heartbeat)*

This property applies to output data points. You can enter the maximum period of time (in seconds) that may elapse without an output data point receiving an updated value from the SmartServer. If this time period expires without the output data point receiving an updated value, the SmartServer will automatically send the output data point an updated value even if the value has not changed.

For example, if the value of a **SNVT_temp** data point is changing 1° every 10 seconds, but this property is set to 2 seconds, the SmartServer will update the data point every 2 seconds—regardless of the fact that the value is not changing more than once every 10 seconds.

An input data point connected to this output data point can use this value as a heartbeat, as it will be able to detect a failure if it does not receive an update within the specified time.

The default value is **0**, which means that the SmartServer will only update the output data point when its value changes. In addition, this default value disables the functionality of the **Max Receive Time** property.

Note: The heartbeat should be approximately a fourth of the **MaxReceiveTime** of any bound input data point located downstream. For example, if the heartbeat of the output data point is 5 seconds, the **MaxReceiveTime** of any bound input data point should be 20 seconds. This allows for lost messages.

*Min Send Time
(Throttle)*

This property applies to output data points. You can enter the minimum period of time (in seconds) that must elapse between updates transmitted by the output data point. Setting this property reduces network traffic by limiting the number of data point updates that are sent by the output data point.

For example, if the value of a **SNVT_temp** data point is changing 1° every 0.5 seconds, but this property is set to 2 seconds, the data point will only transmit the updated value every 2 seconds—regardless of the fact that the data point value is changing more frequently than that.

If the data point value changes more frequently than the specified throttle, only the first and last updates are propagated to the network. For example, if the throttle is set to 5 seconds, and 4 updates occur within a 5-second period, only the first and fourth updates will be propagated to the network.

The default value is **0**, which means that output data point will send an update every time its value changes.

*Max Receive Time
(Offline)*

This property applies to bound input data points. You can set the maximum period of time (in seconds) that may elapse without the input data point receiving additional updates from the data point to which it is connected. If this time period expires before the input data point receives another update, the input data point will use its default value and its status will be set to **AL_OFFLINE**. You can have an Alarm Notifier send an alarm notification any time this occurs. See *Alarming* in Chapter 7 for more information on how to do this.

The default value is **0**, which means that a bound input data point will not use its default value and its status will not be set to **AL_OFFLINE** if it does not receive additional updates.

Note: The **MaxReceiveTime** of an input data point should be approximately four times the heartbeat of any bound output data point located upstream. For example, if the **MaxReceiveTime** is 20 seconds,

*Use Send On
Delta*

the heartbeat of any output bound data point should be 5 seconds. This allows for lost messages.

This property applies to all data points. You can set the minimum amount of change required for a data point to send an updated value to all SmartServer applications in which the data point is a member. To set a send on delta value for this data point, select this option and enter a value.

For example, if you set this property to 1 for a structured data point (for example, **SNVT_switch** or **SNVT_setting**) or to a specific value for a scalar data point, the data point will send an update to the applications each time it changes by that value.

If this option is cleared, the SmartServer applications will use their default send on delta values for determining when a data point is to be updated. For example, the default send on delta value for the Web Connection application is for updates to be sent only if the value changes. This is to avoid instances such as a modem connection being created on every heartbeat.

The default for all the other SmartServers 100 applications is **0**, which means that the applications receive data point updates, regardless of whether the value changes.

Presets

You can use presets to define strings that represent specific values for a data point. Using presets enables you to integrate data points with varying types and structures into the SmartServer applications seamlessly.

For example, you can define a preset named ON for a **SNVT_switch** data point with a value of 100.0 1, and a preset named ON for a **SNVT_temp_f** data point with a value of 22. You could then add these data points to a Scheduler application and have it set both data points to ON at a specific time. In this case, the Scheduler does not need to know that **SNVT_switch** requires both a state and a value or that **SNVT_temp_f** requires a floating point value. Instead, the SmartServer's internal data server uses the presets to translate the strings into their required types and formats and updates the data points at the specified time. This example also demonstrates how you can use presets to drive multiple data points with differing types simultaneously.

To create a preset, click **Add Preset**. Enter the name for the new preset in the **Preset Name** box and then enter a valid value in the **Preset Value** box. This preset value will be applied to the data point when the specified preset name is called. You can also click the box to the right to open the **Edit Presets** dialog, where you can view the valid range of values for the data point and enter the preset values.

To remove a preset, select it and click **Delete Preset**.

For presets with multiple values, you can use the arrows to re-order which values are written to the data point when the preset name is received. For example, consider a **SNVT_switch** data point that has two values for the OFF preset (0.0 0 and 100.0 0), and the 0.0 0 value is listed before the 100.0 0 value. When the OFF preset is received, the 0.0 0 value will be written to the data point because it is the first one listed for that preset. If you want the 100.0 0 value to be written to the data point, click anywhere in the **Preset Name** or **Preset Value** header and then click an arrow to re-order the presets so that the 100.0 0 value is listed before the 0.0 0 value.

You can change the default presets for a given data type by modifying its template in the **/config/template/lonworks/dp folder** on the SmartServer flash disk. For example, you could change the default presets for the **SNVT_switch** data type by modifying the **/config/template/lonworks/dp/#0000000000000000.SNVT_switch.xml** file.

Fields

Structured data points (data points with multiple fields) such as **SNVT_switch**, **SNVT_alarm**, and **SCPT_maxRcvT** have default names and unit strings describing each field that are defined by resource files. You can edit the default names and unit strings.

Using a **SNVT_switch** data point for example, the data point will have fields named by default “Value” and “State” with unit strings of “% of full level” and “state code”, respectively. You could change the unit string used to describe the “State” field from the default “state code” to “occupied” for a restroom occupancy sensor

To edit the unit strings of the fields within a structured data point on an internal SmartServer device, click **Add Unit** to open the **Select Fields** dialog. Click the field with the unit string to be edited and then click **OK** to return to the **Configure - Data Point** Web Page, and then click **Submit**. The selected field is added under the **Fields** property at the bottom of the **Configure - Data Point** Web Page. You can then enter a brief description of the unit string to be used for that field in the **Unit String** box.

To edit the unit strings of the fields within a structured data point on an external device, enter a brief description of the units to be used for that field in the **Unit String** box.

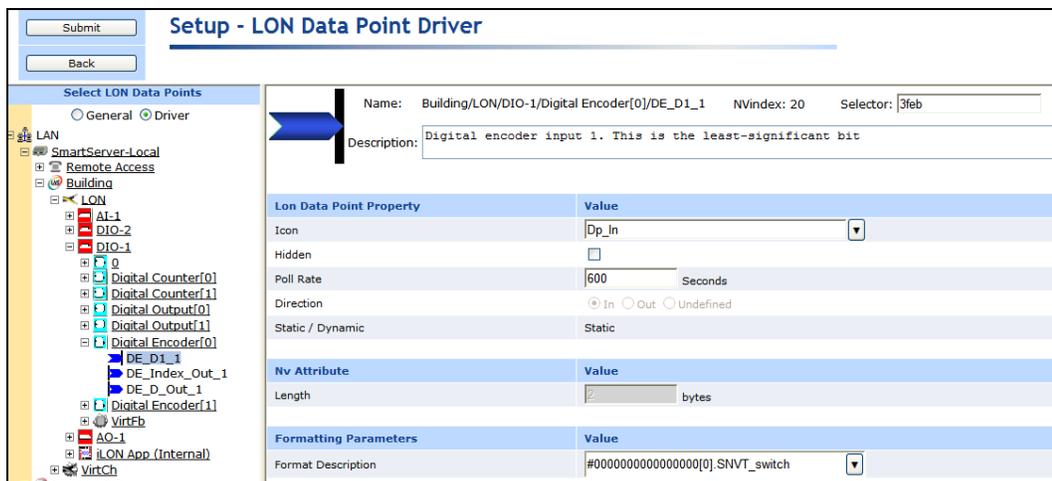
To reset the unit string used by a field to its default, click the field and then click **Delete Unit**.

5. Click **Submit**.

Configuring LONWORKS Data Point Driver Properties

To configure the driver properties of a data point, follow these steps:

1. Click **Driver**.
2. Click one or more data points to be configured.
3. The **Setup - LON Data Point Driver** Web page opens.



4. Configure the following data point properties:

<i>Name</i>	Displays the network path of the functional block in the following format: <code><network>/<channel>/<device>/<functional block>/<data point></code> . This field is read-only.
<i>NV Index</i>	Displays the index number of the data point within its device. This field is read-only.
<i>Selector</i>	Displays the value that uniquely associates the data point with its connections. If the data point is not a member of a connection, the selector is set to a value representing an unbound data point. For LONWORKS connections, a selector is a 14-bit number used to identify connected data points. When placing the data point in a LONWORKS connection, the SmartServer assigns the data point a value representing that connection. All data points in a given connection use the same selector. The OpenLNS Server shares a network variable selector among connections if the connections share one or more data points. You cannot change the value in the Selector property.
<i>Description</i>	Enter an optional description of the functional block. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

LON Data Point Property

<i>Icon</i>	Displays the icon used to represent the data point in the SmartServer or OpenLNS tree and in the application frame. You can change the icon for the data point by selecting a different icon and then clicking Submit .
<i>Hidden</i>	Hides the data point in the SmartServer tree or OpenLNS tree. If this data point is not actively being used, you can hide it to simplify the web interface. To show a hidden data point icon, click Settings. In the Global Settings dialog, select Data Points in the Display Hidden property and then click Close .
<i>Poll Rate</i>	The frequency in which the SmartServer's internal data server polls the data point. recommended typical minimum poll rate is 30 seconds; the maximum poll rate is 1 second. The default poll rate for network variables is 120 seconds if the network variable has been copied and pasted from the OpenLNS tree, or it is 600 seconds if the parent device has been manually added to a channel in the SmartServer tree. The default poll rate for configuration properties is 0 seconds, which means that means polling is disabled. You must set a poll rate for configuration properties to update their values. You can set poll rates for the data points of the external devices that are connected to the SmartServer. You can set poll rates for the data points of the internal SmartServer devices if you need to force updates in a specific SmartServer embedded application (for example, a data logger). Note: The actual poll rate for a data point is determined by calculating the greatest common divisor of all the poll rates set for the data point in the applications to which it has been added. For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 7 seconds, the

SmartServer's internal data server will poll the data point every 1 second.

Therefore, set poll rates in the SmartServer's applications that are the same for a given data point, or poll rates that are at least multiples of each other. For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 10 seconds, the SmartServer's internal data server will poll the data point every 5 seconds

<i>Direction</i>	Indicates whether the data point is an input data point or output data point. For dynamic data points, you can change the direction.
<i>Static/Dynamic</i>	Indicates whether the data point is static, dynamic, or has a changeable type (DDT_changeable). If the data point supports changeable types or is dynamic, you can change the type/and or format in the Format Description box.
<i>Use Authentication</i>	Enables the data point to use authenticated messaging.

NV Attribute

<i>Length</i>	Specifies the size (in bytes) of the data point.
---------------	--

Formatting Parameters

<i>Format Description</i>	Displays the SNVT, UNVT, SCPT, or UCPT used by the data point, and it specifies the format (for example, SI metric or US customary) used if the type has multiple formats such as SNVT_temp_f . The format description is displayed in the following format: #<manufacturer ID>[scope selector].<type name>.
---------------------------	---

For data points with multiple formats such as **SNVT_temp_f**, you can click the arrow to the right to select a different format defined for that data type from the list that appears. Using a **SNVT_temp_f** data point for example, you can click the arrow to change the format to **#US**, **#SI**, or **#US_Diff**.

For dynamic data points or data points with changeable types, you can click the box to the right to open the **Select Types** dialog, where you can change the data point's type and/or format. In the **Select Types** dialog, you expand the LonMark Resource directory, expand the **lonworks/types** folder, and then expand a LonMark resource file to show the network variable and configuration property types available in that file. You then expand the network variable or configuration property types to show the available data types, click the SNVT, UNVT, SCPT, or UCPT to be used for the data point, and then click **OK** to return to the **Setup – LON Data Point Driver** Web page.

Note: This **Select Types** dialog does not filter data types with the different lengths as the current data type of the selected data point.

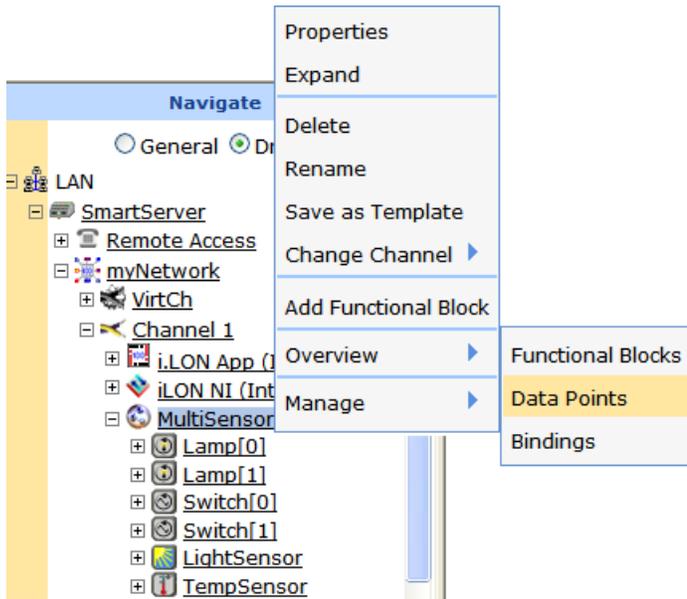
4. Click **Submit**.

Viewing LONWORKS Data Points

You can use the **Overview – Data Points** Web page to view or configure the indexes, statuses, names, types, unit strings, and poll rates of the LONWORKS data points within the devices and functional blocks in your network. To view LONWORKS data points with this Web page, follow these steps:

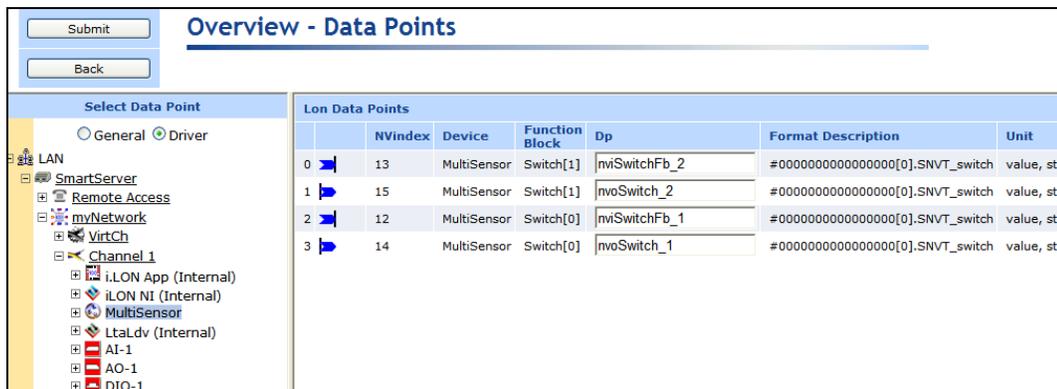
1. To rename or set the poll rates for data points, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.

- Right-click a LONWORKS device or functional block in the SmartServer tree or OpenLNS tree, point to **Overview**, and then select **Data Points**.



Note: You can select two or more devices or functional blocks and view all the data points on those devices or functional blocks in the same **Overview – Data Points** page; however, the SmartServer’s performance may be impacted by trying to create large lists of objects.

- The **Overview – Data Points** Web page opens.



- You can sort the objects listed by clicking a property header.
- View and /or configure the following properties:

- Icon/Status** Displays the icon used to represent the data point in the SmartServer or OpenLNS tree and in the application frame (input, output, or unspecified) . If the data point is offline or not synchronized with the OpenLNS network database, this box is red or yellow, respectively.
- NV Index** Displays the index number of the data point within its associated device. This field is read-only.
This property is only displayed in **Driver** mode; it is not displayed in **General** mode.
- Device** Displays the name of the data point's parent device. This field is

	read-only.
<i>Functional Block</i>	Displays the name of the data point's parent functional block. This field is read-only.
<i>Dp</i>	Displays the name of the data point. In Driver mode, you can change the name. In General mode, this field is read-only.
<i>Format Description</i>	<p>Displays the SNVT, UNVT, SCPT, or UCPT used by the data point, and it specifies the format (e.g., SI metric or US customary) used if the type has multiple formats such as SNVT_temp_f. The format description is displayed in the following format: <i>#<program ID>[scope selector].<type name></i>.</p> <p>For data points with multiple formats such as SNVT_temp_f, you can click the arrow to the right to select a different format defined for that data type from the list that appears. Using a SNVT_temp_f data point for example, you can click the arrow to change the format to #US, #SI, or #US_Diff.</p> <p>For static data points with changeable types or dynamic data points, you can change the data point's type and/or format in the Select Types dialog that you can open from the Format Description property in the data point's Setup – Data Point Driver Web page. To open this Web page, click the Driver option above the navigation pane on the left side of the SmartServer Web interface, and then click the data point.</p> <p>This property is only displayed in Driver mode; it is not displayed in General mode.</p>
<i>Unit</i>	<p>Displays the units of measures used by the data point. For example, the unit string of a SNVT_temp_f data point is “degrees F.” The unit string is defined by resource files. For structured data points, this displays the fields within the data point. Using a SNVT_setting data point for example, function, setting, rotation is displayed in this property.</p> <p>You can edit the unit strings in the data point's Configure - Data Point Web page. To open this Web page, click the General option above the navigation pane on the left side of the SmartServer Web interface, and then click the data point. The Unit String property is located in the upper portion of the Web page.</p> <p>This property is only displayed in Driver mode; it is not displayed in General mode.</p>
<i>Poll Rate</i>	<p>The frequency in which the SmartServer's internal data sever polls the data point. The typical minimum poll rate is 30 seconds; the maximum poll rate is 1 second.</p> <p>The default poll rate for external data points is 120 or 600 seconds. It is 120 seconds if the data point has been copied and pasted from the OpenLNS tree. It is 600 seconds if the parent device has been manually added to a channel in the SmartServer tree.</p> <p>The default poll rate for the data points of the SmartServer's internal devices (iLON App and iLON System) is 0 seconds, which means polling is disabled. You can set poll rates for the internal data points if you need to force updates in a specific SmartServer embedded application (e.g., a data logger).</p>

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Note: The actual poll rate for a data point is determined by calculating the greatest common divisor of all the poll rates set for the data point in the applications to which it has been added.

For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 7 seconds, the SmartServer's internal data server will poll the data point every 1 second.

Therefore, set poll rates in the SmartServer's applications that are the same for a given data point, or poll rates that are at least multiples of each other.

For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 10 seconds, the SmartServer's internal data server will poll the data point every 5 seconds.

6. Click **Submit** to save any changes.

Connecting LONWORKS Data Points with LONWORKS Connections

You can create LONWORKS connections in the SmartServer tree or OpenLNS tree to bind the network variables of LONWORKS devices that are in the same network. Creating LONWORKS connections with the SmartServer is comparable to creating connections with OpenLNS CT. You select a hub network variable in the OpenLNS tree and then select one or compatible target network variables in the same network. Network variables must have the same type to be compatible. Once you create LONWORKS connection, the target data points will receive all updates from the hub (source) in the connection. This process of connecting network variables is called *binding*, and the logical connections are thought of as virtual wires.

LONWORKS connections created with the SmartServer always use Subnet/Node ID addressing. You can use an OpenLNS application such as OpenLNS CT to select a different addressing mode such as group or broadcast for LONWORKS connections.

For more information on creating LONWORKS connections, see *Creating LONWORKS Connections* in Chapter 4.

Designing a Modbus Network

You can design a Modbus network with the SmartServer. This entails creating and configuring Modbus channels, devices, and data points. After you design a Modbus network, you can use the SmartServer applications to read and write to the holding registers on the Modbus devices. For more information on the Modbus protocol, go to www.modbus.org.

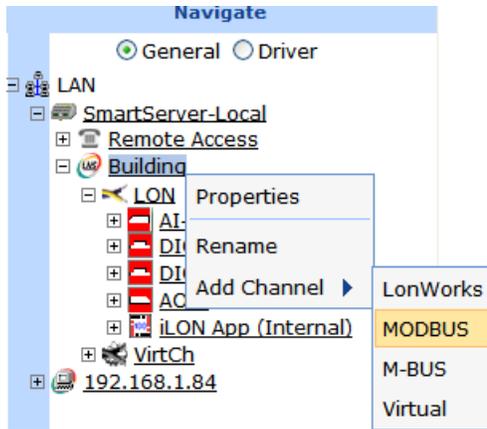
Creating and Configuring Modbus Channels

The SmartServer can interface with slave Modbus devices on TCP/IP, RS-232, and RS-485 channels. The RS-232 channel protocol is the Electronic Industries Association (EIA) standard for the interchange of serial binary data between two devices. The RS-485 channel protocol is a data protocol used for transmitting data over longer distances.

Creating Modbus Channels

To add a Modbus channel to the local SmartServer network, follow these steps:

1. Right-click the network icon, point to **Add Channel**, and then select **Modbus**.



2. The **Enter Name** dialog opens.

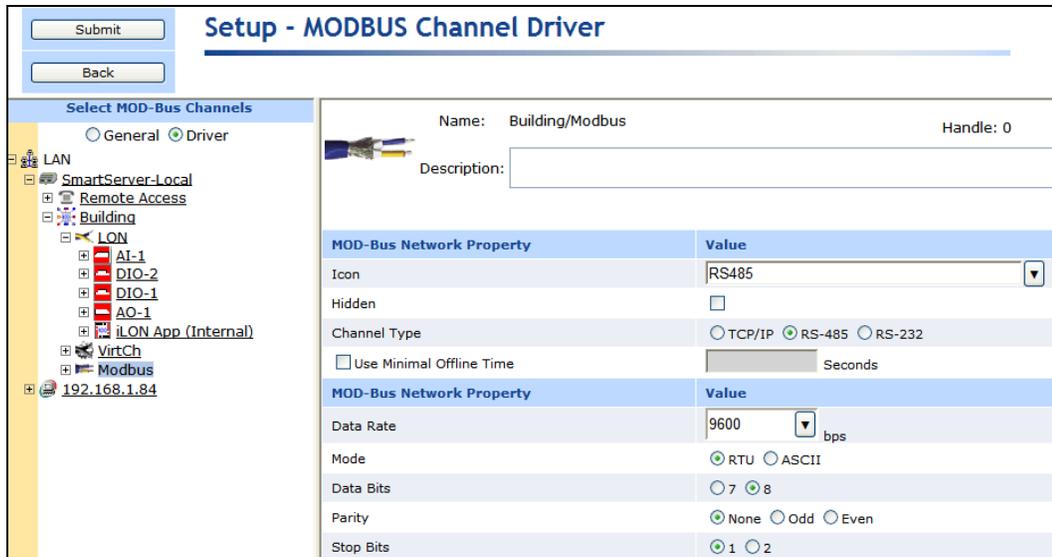


3. Enter a name for the Modbus channel that is unique to the network and then click **OK**.
4. The Modbus channel is added to the bottom of the SmartServer tree.
5. Click **Submit**.

Configuring Modbus Channels

You can use the Modbus driver properties to change the transmission mode and properties. To configure the Modbus channel properties, follow these steps:

1. Click **Driver**.
2. Select one or more Modbus channels to be configured. The **Setup - Modbus Channel Driver** Web page opens.



3. Configure the following Modbus channel properties:

Name Displays the network path of the Modbus channel in the following format: *<network>/<channel>*. This field is read-only.

Description Enter an optional description of the channel. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Modbus Network Property

Icon Displays the icon used to represent the Modbus channel in the SmartServer tree and in the application frame. The default icon is RS485. You can change the icon for the channel in by selecting a different icon and then clicking **Submit**.

Hidden Hides the Modbus channel in the SmartServer tree. If this channel is not actively being used, you can hide it to simplify the Web interface.

To show a hidden channel icon, click **Settings**. In the **Global Settings** dialog, select **Channels** in the **Display Hidden** property and then click **Close**.

Channel Type Select the channel type used for transmitting data between Modbus devices. You have the following three choices:

- **TCP/IP**. Modbus messages are enveloped in TCP/IP packets. TCP/IP allows for more versatile network systems, as Modbus connection can co-exists with other types of connections.
- **RS-485**. RS-485 is a balanced line, half-duplex system that allows transmission distances of up to 1.2 km. RS-485 allows for transmission over longer distances at higher speeds. This is the default.
- **RS-232**. RS-232 uses serial binary data for transmitting data between two devices.

Use Minimal Offline Time If a network message fails, a Modbus data point and its Modbus device are marked offline. You can select **Use Minimal Offline Time** so that all the Modbus data points on the offline Modbus device with pending network messages (read/write requests, polls, or heartbeats) are marked offline and

network messages are not sent to them. This ensures that network performance is not impacted by an offline Modbus device.

You can also set the minimum period of time (in seconds) that the SmartServer waits before transmitting network messages to offline Modbus data points. During this period, an offline Modbus device transmits an OFFLINE status in response to data point requests. Once the **Minimal Offline Time** elapses, the SmartServer sends a read/write request to one offline Modbus data point. If the read/write request succeeds, the Modbus data point and its Modbus device are marked online, and all cached read/write requests for the offline Modbus data points on the Modbus device are executed.

The default **Use Minimal Offline Time** for a Modbus channel is **60** seconds.

Modbus Network Property

<i>Data Rate</i>	Select the bit rate at which the SmartServer will communicate with the Modbus devices on the channel. The default value is 9600 Baud. See the documentation for your Modbus devices for more information on the bit rates they support.
<i>Mode</i>	Select the transmission mode used by the SmartServer for communicating with Modbus devices. You have the following two choices: <ul style="list-style-type: none">• RTU. Data is sent as two 4-bit, hexadecimal characters. RTU mode provides a higher throughput than ASCII mode at equivalent baud rates. This is the default.• ASCII. Data is sent as two ASCII characters. ASCII mode provides increased flexibility in regards to the timing sequence, as there can be up to a 1-second interval between character transmissions without communication errors occurring.
<i>Data Bits</i>	Select the data bit size for messages sent over the Modbus network. A data bit is a group of 5 to 8 bits that represents a single character of data for transmission over the network. Data bits are preceded by a start bit, and they are followed by an optional parity bit and one or more stop bits. The default value is 8 bits.
<i>Parity</i>	Select the parity bit size for messages sent over the Modbus network. A parity bit is an extra bit used to check for errors in groups of data bits transferred between devices. The default parity size is none .
<i>Stop Bits</i>	Select the number of stop bits used on the Modbus network. The default value is 1 stop bit.

4. Click **Submit**.

Creating and Configuring Modbus Devices

You can add Modbus devices to the local SmartServer network. Because of the many variations in Modbus devices, conduct compatibility testing before using the SmartServer with Modbus devices in your production systems. Modbus support with the SmartServer has been tested with the following devices:

- ABB ACH550*
- Berg UBN 3060*
- Berg UBN 315

- Berndt Contec LAE Electronic LCD 15*
- Cummins MOD-LON
- Dixel XW570K
- Honeywell 7800 series Burner controls with an S7810M Modbus Interface module
- Leibert system 3 AHU with and OpenComms interface module
- Schneider PM500*
- Socomec A40*
- Veris Industries H8035 Modbus Enercept kW/kWh meter
- Wago System 750*
- Yaskawa E7

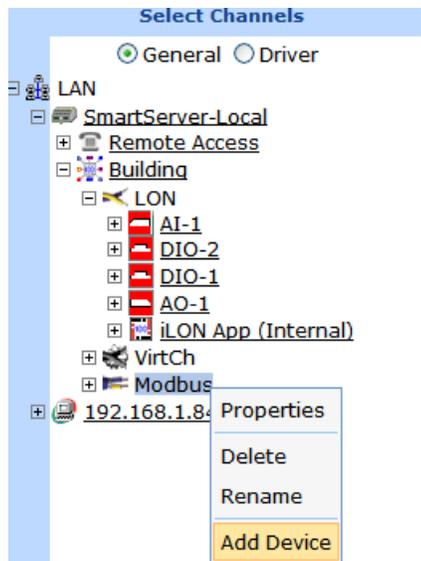
* Device has a pre-defined template file loaded on the SmartServer which you can use to add it to the SmartServer. See *Using Device Templates* in Chapter 4 for more information.

Each Modbus TCP/IP slave device must be added to a separate channel. Adding more than one Modbus TCP device to a Modbus TCP/IP channel generates unexpected results such as all points being mapped to the first device defined on the channel. These errors occur even if the Modbus TCP/IP addresses are unique.

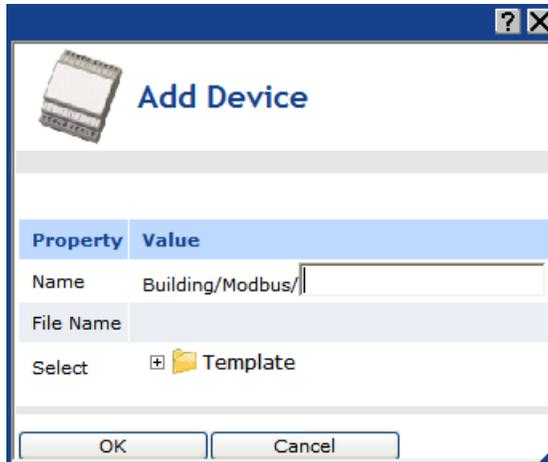
Creating Modbus Devices

To create a Modbus device, follow these steps:

1. Right-click a Modbus channel, and then select **Add Device** on the shortcut menu.

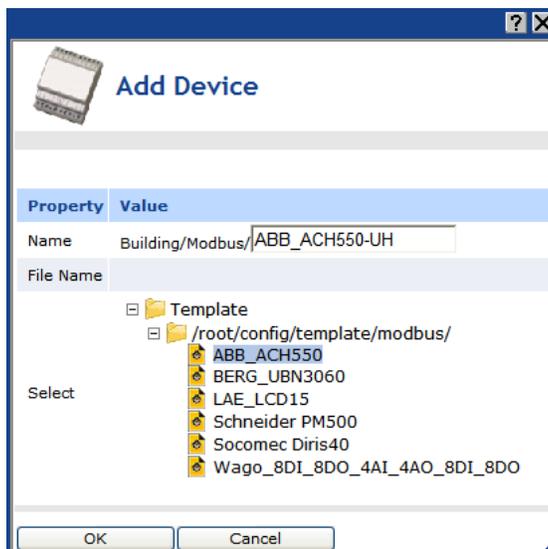


2. The **Add Device** dialog opens.

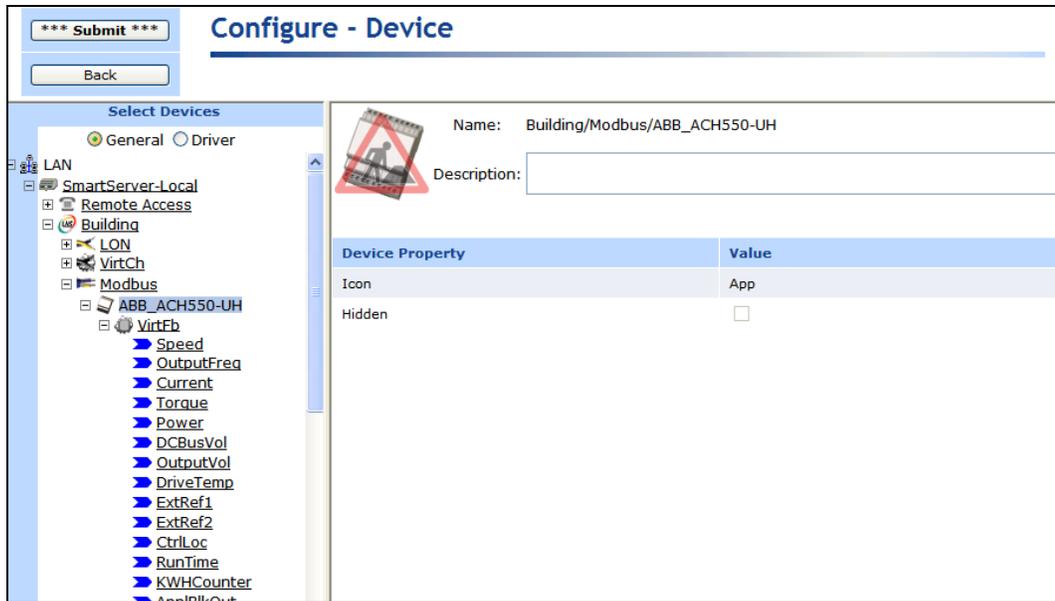


3. Enter the following device properties:

<i>Name</i>	Enter a name for the Modbus device that is unique to the network or leave this field blank to use the device name defined by the Modbus device template.
<i>File Name</i>	Displays the full path of the template (.XML file) selected for the Modbus device.
<i>Select</i>	Select the external interface for the Modbus device from the Template folder. To do this, expand the Template directory to show the config/template/modbus folder on the SmartServer. Expand this folder to show the pre-defined templates for Modbus devices that have been tested for SmartServer compatibility and any user-created templates. The user-created device templates include all the data points shown on the navigation pane at the time the Modbus device template was created. See <i>Using Device Templates</i> in Chapter 4 for more information on creating Device Templates.



4. Click **OK**. The Modbus device and a Virtual Functional Block containing all of the device's static data points are added to the bottom of the tree of the parent Modbus channel.

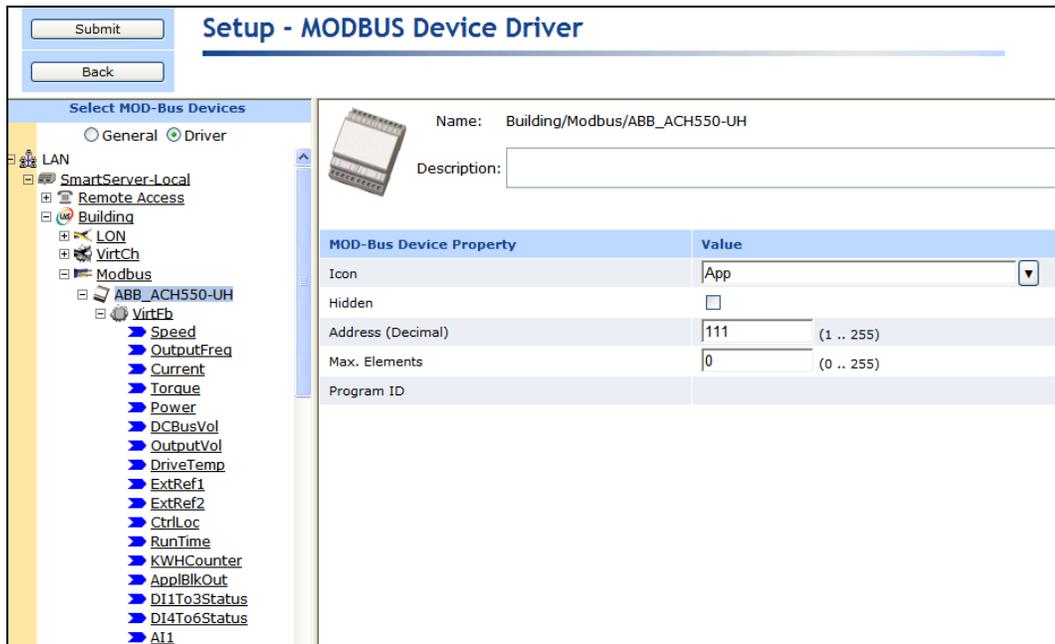


5. Click **Submit**.

Configuring Modbus Devices

You can use the driver properties to configure Modbus devices. To configure the device properties, follow these steps:

1. Click **Driver**.
2. Select one or more devices to be configured.
3. The **Setup - Modbus Device Driver** Web page opens.



4. Configure the following Modbus device properties:

Name Displays the network path of the router in the following format: *<network>/<channel>/<device>*. This field is read-only.

Description Enter an optional description of the Modbus device. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Modbus Device Property

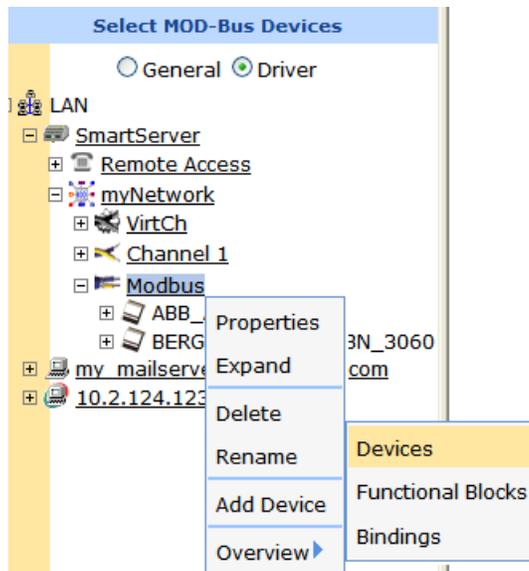
- Icon* Displays the icon used to represent the Modbus device in the SmartServer tree. The default icon is **App**. To change the icon for the Modbus channel, select a different icon and then click **Submit**.
- Hidden* Hides the Modbus device in the navigation pane. If the Modbus device is not actively being used, you can hide it to simplify the Web interface. To show hidden Modbus devices, click **Settings** to open the **Global Settings** dialog. In the **Display Hidden** property, select the **Devices** check box and then click **Close**.
- Address (Decimal)* Displays the logical address of the device on the Modbus network in decimal or hexadecimal format. You can select the format used to display the Modbus device address using the **Address Display** property in the **Configure Network** driver Web page.
- Max Elements* Displays the maximum number of data points that can be stored on the device.

5. Click **Submit**.

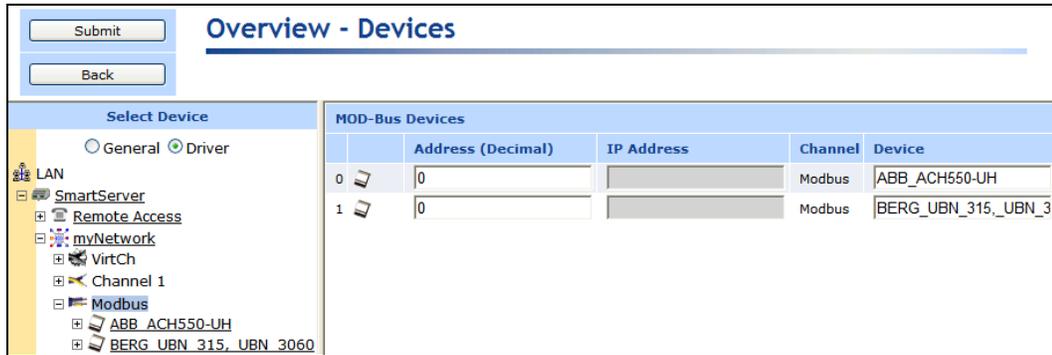
Viewing Modbus Devices

You can view and configure the all the Modbus devices in your network or on a specific channel using the **Overview – Devices** Web page. This Web page displays the status, logical address, IP address, parent channel, and name of each Modbus device. To view Modbus devices with the **Overview – Devices** Web page, follow these steps:

1. To configure the logical address, IP address, or name of the Modbus devices, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click the network or a Modbus channel in the SmartServer tree, point to **Overview**, and then select **Devices**.



3. The **Overview – Devices** Web page opens.



4. You can sort the objects listed by clicking a property header.
5. View and /or configure the following properties:

<i>Icon/Status</i>	Displays the icon used to represent the Modbus device in the SmartServer tree and in the application frame. If the device is offline, this box is highlighted red.
<i>Address (Decimal)</i>	Displays the logical address of the Modbus device in decimal or hexadecimal format. You can select the format used to display the Modbus device address using the Address Display property in the Global Settings dialog, which you can access by clicking Settings . This property is only displayed in Driver mode; it is not displayed in General mode.
<i>IP Address</i>	Displays the IP address of the of the Modbus device. This property is only available if the Modbus channel is using TCP/IP. This property is only displayed in Driver mode; it is not displayed in General mode.
<i>Channel</i>	Displays the name of the channel on which the Modbus device is attached.
<i>Device</i>	Displays the name of the Modbus device. In Driver mode, you can change the name. In General mode, this field is read-only.

6. Click **Submit** to save any changes.

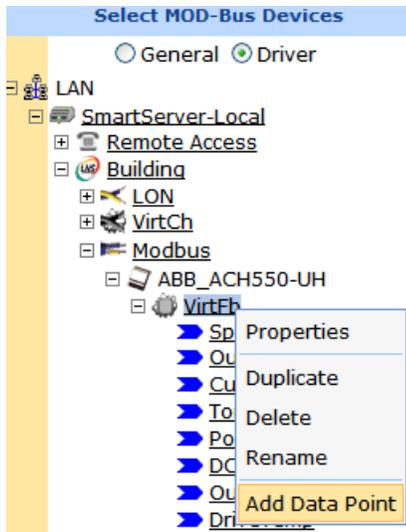
Creating and Configuring Modbus Data Points

You can dynamically add configuration properties to the Modbus devices on the network (you cannot add static data points).

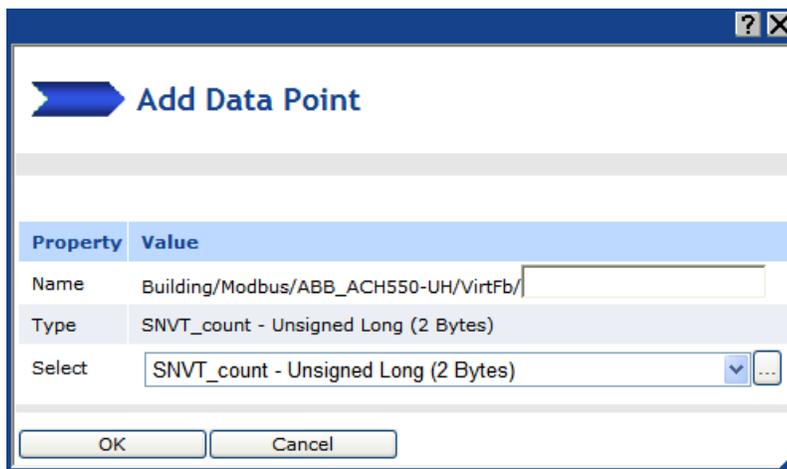
Creating Modbus Data Points

To add this type of dynamic data point to a Modbus device, follow these steps:

1. Right-click the virtual functional block of a Modbus device, and then select **Add Data Point** on the shortcut menu.

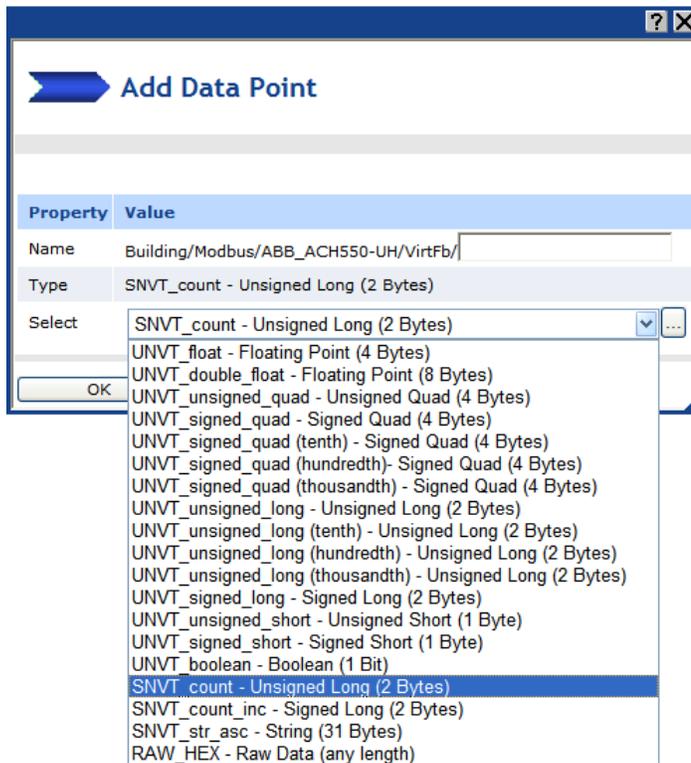


2. The **Add Data Point** dialog opens:



3. Enter the following data point properties:

<i>Name</i>	Enter a name for the data point.
<i>Type</i>	Displays the configuration property type of the currently selected data point.
<i>Select</i>	Either select one of the 19 SNVT, UNVT, or built-in types listed for the Modbus data point, or click the box to the right to select a different data point type in the Select Types dialog.



4. Click **OK**. The data point is added to the bottom of the tree of its parent virtual functional block.
5. Click **Submit**.

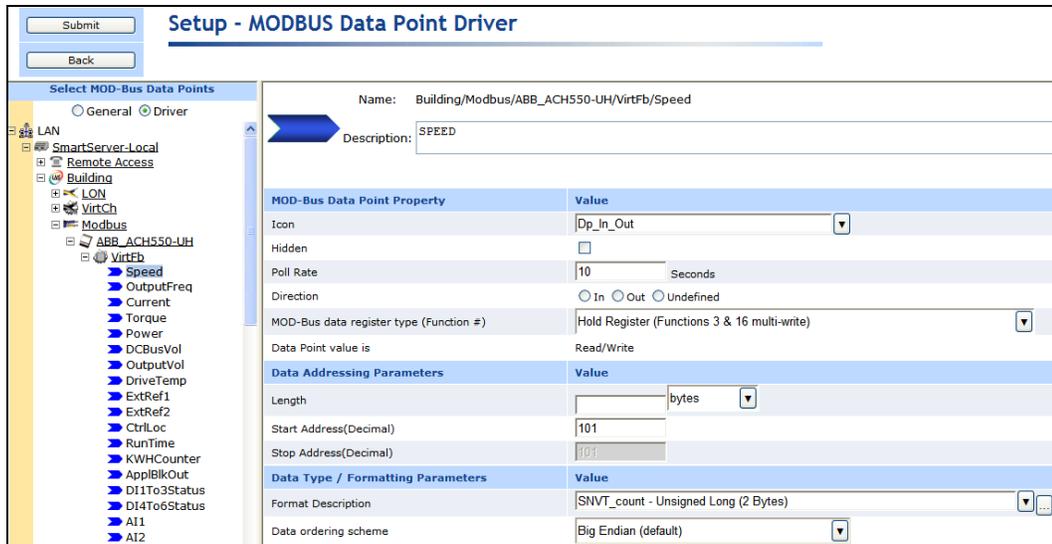
Configuring Modbus Data Points

You can configure Modbus data points using both the **General** and **Driver** modes. The following summarizes the data point configuration tasks you can perform in each mode:

- **General** mode. Enable and set default and invalid values; make the data point persistent; set the poll rate; set configuration properties (heartbeat, throttle, offline, and send on delta); and add or delete presets and fields. See *Configuring Data Point General Properties* earlier in this chapter for more information on modifying these properties.
- **Driver** mode. Change the icon of and hide the data point. Change the poll rate, access type, addressing properties, and the format and type parameters.

To configure the driver properties of a Modbus data point, follow these steps:

1. Click **Driver**.
2. Select one or more Modbus data points to be configured.
3. The **Setup - Modbus Data Point Driver** Web page opens.



4. Configure the following Modbus data point properties:

- Name* Displays the network path of the data point in the following format: *<network>/<channel>/<device>/<functional block>/<data point>*. This field is read-only.
- Handle* Displays the handle assigned to the Modbus data point. This field is read-only.
- Description* Enter an optional description of the Modbus data point. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Modbus Data Point Property

- Icon* Displays the icon used to represent the Modbus data point in the tree. You can change the icon for the Modbus data point by selecting a different icon and then clicking **Submit**.
- Hidden* Hides the Modbus data point in the navigation pane. If the Modbus data point is not actively being used, you can hide it to simplify the Web interface.

To show hidden Modbus data points, click **Settings** to open the **Global Settings** dialog. In the **Display Hidden** property, select **Data Points** and then click **Close**.
- Poll Rate* Set the frequency in which the SmartServer polls the data point. The recommended minimum poll rate is 30 seconds; the maximum poll rate is 1 second. Setting this value to 0 turns off polling. The default poll rate is **20** seconds.
- Direction* Specifies whether the Modbus data point is an Input data point (**In**), Output data point (**Out**), or **Undefined**.
- Modbus Data Access Type (Function #)* Select one of the following data access types based on the associated Modbus device:
 - **Coil Functions (Functions 1 & 5 single-write)**. For a single coil. Single bit, read-write data that has two states (on/off).
 - **Coil Functions (Functions 1 & 15 multi-write)**. For multiple coils.

Single bit, read-write data that has two states (on/off)

- **Discrete Input (Function 2).** Single bit, read-only data that has two states (on/off).
- **Input Register (Function 4).** 16-bit read-only data that can be interpreted as a numeric value, a bit map, or an ASCII character.
- **Hold Register (Functions 3 & 6 single-write).** For a single register. 16-bit write data that can be interpreted as a numeric value, a bit map, or an ASCII character.
- **Hold Register (Functions 3 & 16 multi-write).** For multiple registers. 16-bit write data that can be interpreted as a numeric value, a bit map, or an ASCII character. This is the default.

Data Point Value is

Indicates whether the value of the data point is read-only, or read-write. This is determined by the selected **Modbus Data Access Type**.

Data Addressing Parameters

Length

Enter the length of the data point. Enter a value and select whether it is measured in bits or bytes. The default is **2 bytes**.

Start Address (Decimal)

Enter the start address of the register to be used to read or write to the data point. If the **Length** property is configured to use bits, you can select the start and stop bits in the address.

The Modbus driver is configured to ensure that the start and stop addresses remain consistent with the **Length** property. This means that if **Length** property is changed, the **Start Address** and **Stop Address** properties are automatically updated to fit the desired length. Similarly, if the **Start Address** or **Stop Address** properties are changed, the **Length** property is updated accordingly.

Stop Address (Decimal)

Enter the stop address of the register to be used to read or write to the data point.

Data Type/ Formatting Parameters

Format Description

Displays the data type (SNVT, UNVT, or built-in type) of the data point. You can change the data type to any of the SNVT, UNVT, or built-in data types defined in the resource files on your computer.

Data Ordering Scheme

Select the ordering scheme to be used for interpreting Modbus data. You have the following four choices:

- **Big Endian.** The highest order byte of data is sent first and all subsequent bytes of data are arranged from highest to lowest order. This is the default.
- **Little Endian.** Lowest order byte of data is sent first, and each subsequent byte is arranged from lowest to highest order
- **Byte Swapped.** Data is first arranged from highest to lowest order, but every pair of bytes in the structure is interchanged.
- **Word Swapped.** Data is first arranged from highest to lowest order, but every pair of 16-bit words is swapped.

For example, consider a device that uses an unsigned 32-bit integer to report runtime accumulation. Selecting the data ordering scheme is required because the Modbus protocol leaves the interpretation of 32-bit integers to the discretion of the implementer.

In Big Endian format, the value of 120,000 hours (0x01D4C0 in hexadecimal format) would be represented as a value of: 00 01 D4 C0 in memory. This requires two adjacent Modbus registers (each holding 16 bits of data). If the device manufacture defines the unit runtime to be at register address 0x8, the Big Endian formatted response to a read function would return data 0x0001 0xD4C0 in that order.

Now suppose the manufacture states the U32 value is returned in Little Endian format. One interpretation of the value returned to the driver from the read function would be 0xC0D4 0x0100.

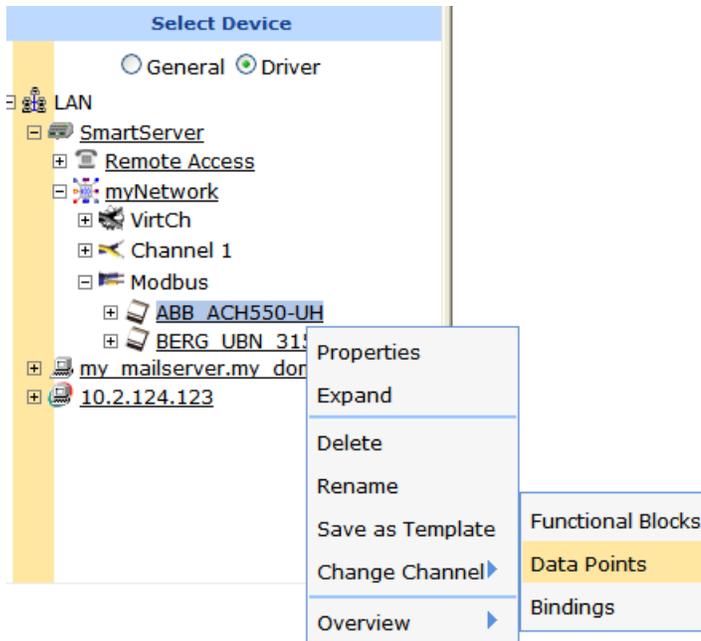
Alternatively, the manufacture may interpret Little Endian to be the ordering of registers and not bytes. In this case, the read function would return 0xD4C0 0x0001 and the driver would need to swap words to handle the value. If the device returned a value of 0x0100 0xC0D4A, a byte swapped format would need to be applied.

Viewing Modbus Data Points

You can view and configure all the data points on a Modbus device using the **Overview - Data Points** Web page. This Web page includes sortable columns for the addressing properties, register type, poll rate, and the format and type parameters of each data point on a Modbus device. This Web page is especially useful for setting the start addresses of the data points on a Modbus device.

To use the **Overview - Data Points** Web page to configure the data points on a Modbus device, follow these steps:

1. To configure the addressing properties, register types, names, poll rates, or descriptions of the Modbus data points, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click a Modbus device, point to **Overview**, and then click **Data Points** on the shortcut menu.



Note: You can select two or more Modbus devices or functional blocks and view all the data points on those devices or functional blocks in the same **Overview – Data Points** page; however, the SmartServer’s performance may be impacted by trying to create large lists of objects.

3. The **Overview - Data Points** Web page opens.

	Start Address	Length	MOD-Bus data register type (Function #)	Device	Function Block
0	101	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
1	102	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
2	103	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
3	104	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
4	105	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
5	106	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
6	108	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
7	109	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
8	110	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
9	111	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
10	112	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb
11	113	2 bytes	Coil (Functions 1 & 5 single-write)	ABB_ACH550-UH	VirtFb

4. By default, the Modbus data points are listed by the **Start Address** column in ascending order. You can sort the data points by clicking a property header. You can view and configure the following properties for each data point on the Modbus device:

Icon/Status Displays the icon used to represent the Modbus data point in the SmartServer tree and in the application frame. If the data point is offline, this box is highlighted red.

Start Address (Decimal) Displays the start address of the register to be used to read or write to the data point. If the **Length** property is configured to use bits, you can select the start and stop bits in the address.

If the value of the Modbus data point does not match the expected value, enter the data point’s physical address on the Modbus device, and verify

that the **Modicon Mode** check box in the **Modbus Address Display Property** in the **Global Settings** dialog is cleared (to access the **Global Settings** dialog, click **Settings**). If the current and expected values do not match, add 1 to the data point's physical address. If the values still do not match, subtract 1 from the data point's physical address.

The Modbus driver is configured to ensure that the start and stop addresses remain consistent with the **Length** property. This means that if **Length** property is changed, the **Start Address** property is automatically updated to fit the desired length. Similarly, if the **Start Address** is changed, the **Length** property is updated accordingly.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Length

Displays the length of the data point. Enter a value and select whether it is measured in bits or bytes. The default is **2 bytes**.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Modbus Data Register Type (Function #)

Displays the data access type of the Modbus device, which can be one of the following values:

- **Coil Functions (Functions 1 & 5 single-write)**. For a single coil. Single bit, read-write data that has two states (on/off).
- **Coil Functions (Functions 1 & 15 multi-write)**. For multiple coils. Single bit, read-write data that has two states (on/off)
- **Discrete Input (Function 2)**. Single bit, read-only data that has two states (on/off).
- **Input Register (Function 4)**. 16-bit read-only data that can be interpreted as a numeric value, a bit map, or an ASCII character.
- **Hold Register (Functions 3 & 6 single-write)**. For a single register. 16-bit write data that can be interpreted as a numeric value, a bit map, or an ASCII character.
- **Hold Register (Functions 3 & 16 multi-write)**. For multiple registers. 16-bit write data that can be interpreted as a numeric value, a bit map, or an ASCII character. This is the default.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Device

Displays the name of the Modbus data point's parent device.

Functional Block

Displays the name of the Modbus data point's parent functional block.

Dp

Displays the name of the Modbus data point. In **Driver** mode, you can change the name. In **General** mode, this field is read-only.

Format Description

Displays the data type (SNVT, UNVT, or built-in type) of the data point. You can select one of the 19 SNVT, UNVT, or built-in types listed for the Modbus data point.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Unit

Displays the units of measures used by the Modbus data point (for example, **speed, 1/10 Hz, 1/10 %**). The unit string is defined in the

template used by the Modbus device.

You can edit the unit strings in the data point's **Configure - Data Point** Web page. To open this Web page, click the **General** option above the navigation pane on the left side of the SmartServer Web interface, and then click the data point. The **Unit String** property is located in the upper portion of the Web page.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Poll Rate Displays the frequency in which the SmartServer polls the data point. The recommended minimum poll rate is 30 seconds; the maximum poll rate is 1 second. Setting this value to 0 turns off polling. The default poll rate for Modbus data points is **10** seconds.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Description Displays a description of the Modbus data point. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Tip: You can configure the data points on a Modbus device by creating one data point, and then duplicating it (right-click the data point and click **Duplicate** on the shortcut menu) to create the required number of data points. This enables the start addresses of the Modbus data points to be calculated automatically. You can then use the **Overview - Data Points** Web page to modify the start addresses, functions, format descriptions, and names of the duplicate Modbus data points accordingly. See *Creating a Duplicate Dynamic Data Point* in Chapter 4, *Using the SmartServer Web Interface*, for more information on duplicating data points.

7. Click **Submit** to save any changes.

Designing an M-Bus Network

You can design and operate an M-Bus network with the SmartServer. The M-Bus (Meter Bus) is a European standard for remote reading of meters. It can be used for supply meters, as well as sensors and actuators.

The SmartServer has an M-Bus driver that uses the M-Bus protocol (EN 1434-3) to communicate with M-Bus devices on the network. On an M-Bus network, the SmartServer functions as the master to the slave M-Bus devices. The M-Bus driver on the SmartServer conforms to the following serial parameters: **9600-8-None-1-None**.

Designing an M-Bus network entails creating and configuring M-Bus channels, devices, and data points. After you design an M-Bus network, you can use the SmartServer applications to read and write to the M-Bus devices. For more information on the M-Bus protocol, go to www.m-bus.com.

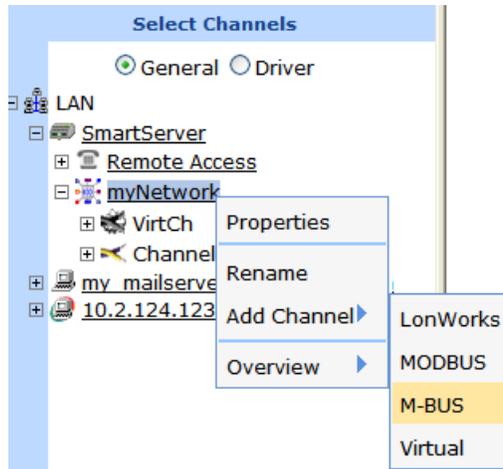
Creating and Configuring M-Bus Channels

The SmartServer can interface with slave M-Bus devices on RS-232, and RS-485 channels. The RS-232 channel protocol is the Electronic Industries Association (EIA) standard for the interchange of serial binary data between two devices. The RS-485 channel protocol is a data protocol used for transmitting data over longer distances.

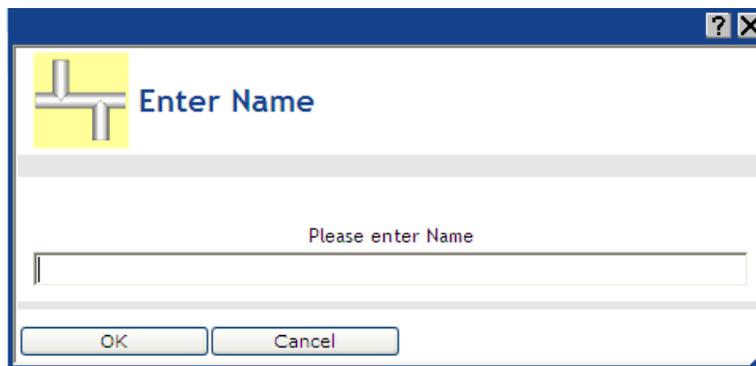
Creating M-Bus Channels

To add an M-Bus channel to the local SmartServer network, follow these steps:

1. Right-click the network icon, point to **Add Channel**, and then select **M-Bus**.



2. The **Enter Name** dialog opens.

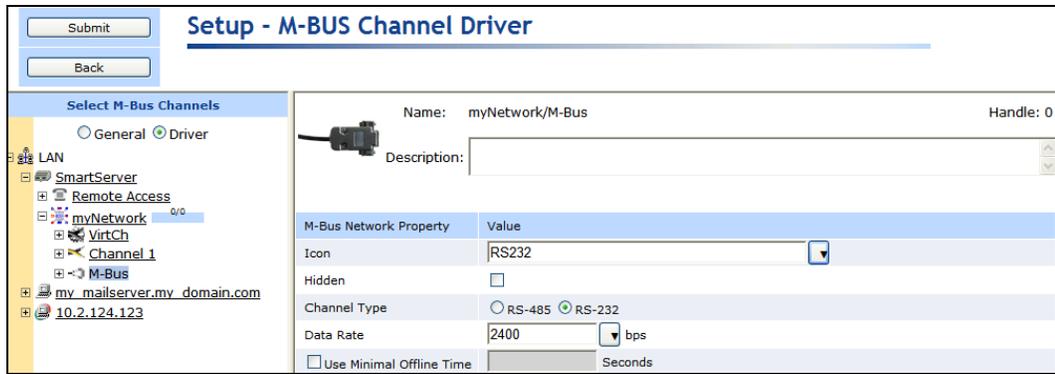


3. Enter a name for the M-Bus channel that is unique to the network and then click **OK**.
4. The M-Bus channel is added to the bottom of the SmartServer tree.
5. Click **Submit**.

Configuring M-Bus Channels

You can use the M-Bus driver properties to change the transmission mode and properties. To configure the M-Bus channel properties, follow these steps:

1. Click **Driver**.
2. Select one or more M-Bus channels to be configured.
3. The **Setup - M-Bus Channel Driver** Web page opens.



4. Configure the following M-Bus channel properties:

Name Displays the network path of the M-Bus channel in the following format: *<network>/<channel>*. This field is read-only.

Description Enter an optional description of the channel. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

M-Bus Network Property

Icon Displays the icon used to represent the M-Bus channel in the SmartServer tree and in the application frame. The default icon is **RS232**. You can change the icon for the channel in by selecting a different icon and then clicking **Submit**.

Hidden Hides the M-Bus channel in the SmartServer tree. If this channel is not actively being used, you can hide it to simplify the web interface.
To show a hidden channel icon, click **Settings**. In the **Global Settings** dialog, select the **Channels** check box in the **Display Hidden** property and then click **Close**.

Channel Type Select the channel type used for transmitting data between M-Bus devices. You have the following two choices:

- **RS-485**. RS-485 is a balanced line, half-duplex system that allows transmission distances of up to 1.2 km. RS-485 allows for transmission over longer distances at higher speeds.
- **RS-232**. RS-232 uses serial binary data for transmitting data between two devices. This is the default.

Data Rate Select the bit rate at which the SmartServer will communicate with the M-Bus devices on the channel. The default value is **2400** Baud.

See the documentation for your M-Bus devices for more information on the bit rates they support.

Use Minimal Offline Time If a network message fails, an M-Bus data point and its M-Bus device are marked offline. You can select **Use Minimal Offline Time** so that all the M-Bus data points on the offline M-Bus device with pending network messages (read/write requests, polls, or heartbeats) are marked offline and network messages are not sent to them. This ensures that network performance is not impacted by an offline M-Bus device.

You can also set the minimum period of time (in seconds) that the SmartServer waits before transmitting network messages to offline M-Bus

data points. During this period, an offline M-Bus device transmits an OFFLINE status in response to data point requests. Once the **Minimal Offline Time** elapses, the SmartServer sends a read/write request to one offline M-Bus data point. If the read/write request succeeds, the M-Bus data point and its M-Bus device are marked online, and all cached read/write requests for the offline M-Bus data points on the M-Bus device are executed.

The default **Use Minimal Offline Time** for an M-Bus channel is **60** seconds.

5. Click **Submit**.

Creating and Configuring M-Bus Devices

You can add M-Bus devices to the local SmartServer network. After you add M-Bus devices to the network, you can install them using an M-Bus specific installation tool. Consult the documentation provided with your M-Bus devices for more information on installing M-Bus devices.

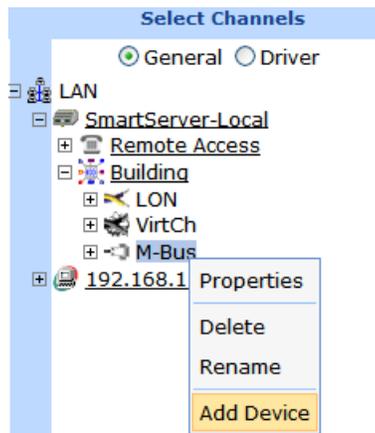
Because of the many variations in M-Bus devices, conduct compatibility testing before using the SmartServer with M-Bus devices in your production systems. The **ReadMe.htm** file in the **LonWorks\iLon100\driverSupport\M-Bus** folder on your computer lists the devices for which M-Bus support with the SmartServer has been tested.

After you create and configure an M-Bus device, you can use a type translator to integrate the data generated by the M-Bus device into a LONWORKS network. See *Integrating M-Bus Devices With a Type Translator* in Chapter 11 for more information on how to do this. The SmartServer includes three pre-defined rule-based type translations for converting water, power, and thermal measurements generated by M-Bus devices.

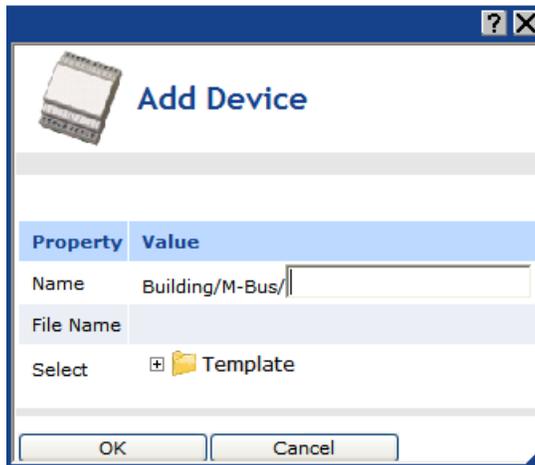
Creating M-Bus Devices

To create an M-Bus device, follow these steps:

1. Right-click an M-Bus channel, and then select **Add Device** on the shortcut menu.



2. The **Add Device** dialog opens.



3. Enter the following device properties:

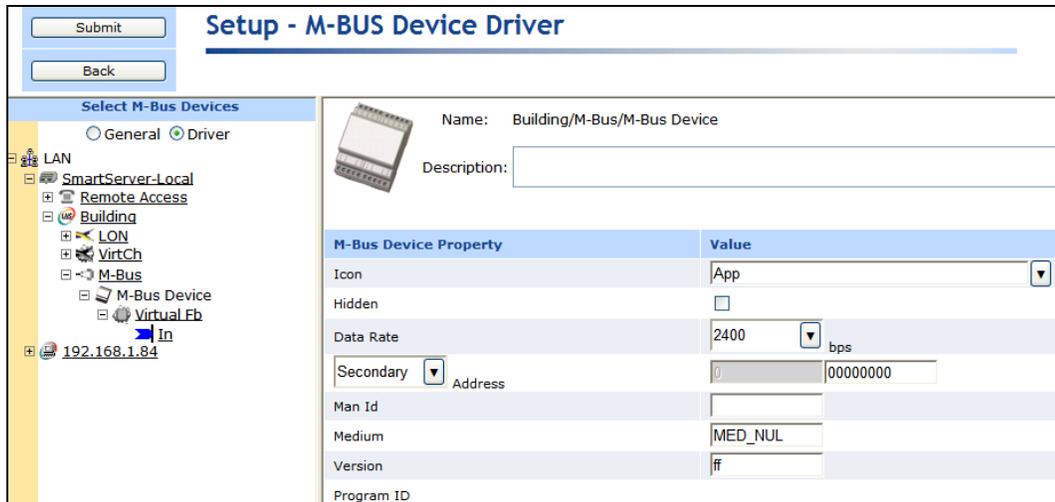
<i>Name</i>	Enter a name for the M-Bus device that is unique to the network.
<i>File Name</i>	Displays the full path of the template (.XML file) selected for the M-Bus device.
<i>Select</i>	Select the device interface for the M-Bus device from the Template folder. To do this, expand the Template directory to show the any user-created templates in the config/template folder on the SmartServer. The user-created device templates include all the data points shown on the navigation pane at the time the M-Bus device template was created. See <i>Using Device Templates</i> in Chapter 4 for more information on creating Device Templates.

4. Click **OK**. The M-Bus device and a Virtual Functional Block containing all of the device's static data points are added to the bottom of the tree of the parent M-Bus channel.
5. Click **Submit**.

Configuring M-Bus Devices

You can use the driver properties to configure M-Bus devices. To configure the device properties, follow these steps:

1. Click **Driver**.
2. Select one or more M-Bus devices to be configured.
3. The **Setup - M-Bus Device Driver** Web page opens.



4. Configure the following M-Bus device properties:

- Name* Displays the network path of the router in the following format: <network>/<channel>/<device>. This field is read-only.
- Description* Enter an optional description of the device. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

M-Bus Device Property

- Icon* Displays the icon used to represent the M-Bus device in the SmartServer tree. The default icon is **App**. To change the icon for the M-Bus channel, select a different icon and then click **Submit**.
- Hidden* Hides the M-Bus device in the navigation pane. If the M-Bus device is not actively being used, you can hide it to simplify the Web interface. To show hidden M-Bus devices, click **Settings** to open the **Global Settings** dialog. In the **Display Hidden** property, select the **Devices** check box and then click **Close**.
- Data Rate* Select the bit rate (bits per second [bps]) at which the M-Bus device communicates on the serial port. The default baud rate is **2400** bps. See the documentation for your M-Bus device for more information on supported bit rates.
- Address* Select whether to use primary or secondary addressing for the M-Bus device. Primary addressing is preferred because it makes replacing M-Bus devices more transparent. Each of these addressing methods is described as follows:
- **Primary**. The primary address is assigned by the network management tool used to install the M-Bus device (analogous to a LONWORKS subnet/icon address). Enter a primary address between 0 to 250 for the M-Bus device.
 - **Secondary**. The secondary address is manufactured into the device at the factory (analogous to a LONWORKS Neuron ID). Enter a secondary address between 0 to 99,999,999 for the M-Bus device.
- Man ID* Displays the device's manufacturer ID as a 3-byte string.

Medium

Displays the device's medium ID as a 1-byte enumeration that identifies the device functionality. The following is a list of possible medium IDs:

Value	Identifier	Notes
-1	MED_NUL	Invalid
0	MED_OTHER	Others
1	MED_OIL	Oil
2	MED_ELECTRICITY	Electricity
3	MED_GAS	Gas
4	MED_RETURN_TEMP	Return temperature
5	MED_STEAM	Steam
6	MED_HOT_WATER	Hot water
7	MED_WATER	Water
8	MED_HEAT_METER	Heat meter
9	MED_COMPRESSED_AIR	Compressed-air
10	MED_RES1	Reserved
11	MED_RES2	Reserved
12	MED_FLOW_TEMP	Flow temperature, outgoing/supply temperature
13	MED_RES3	Reserved
14	MED_SYS_BUS	System / Bus
15	MED_UNKNOWN	Unknown

Version

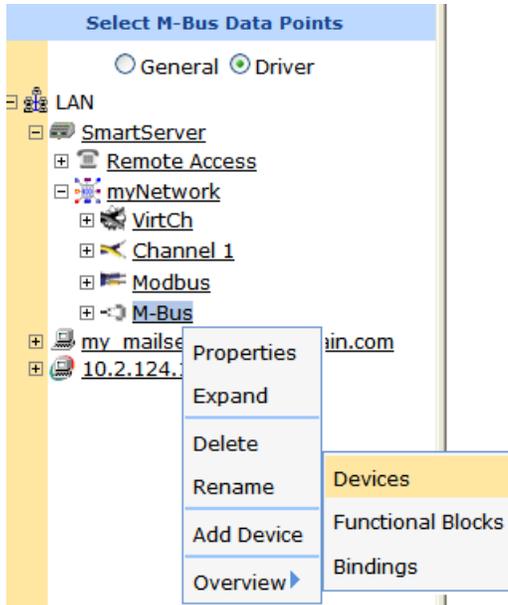
Specifies the generation or version of the device as 1-byte char. This value depends on the manufacturer.

5. Click **Submit**.
6. Create and configure a type translator to integrate the data generated by an M-Bus device into a LONWORKS network. See *Integrating M-Bus Devices With a Type Translator* in Chapter 11 for more information on how to do this.

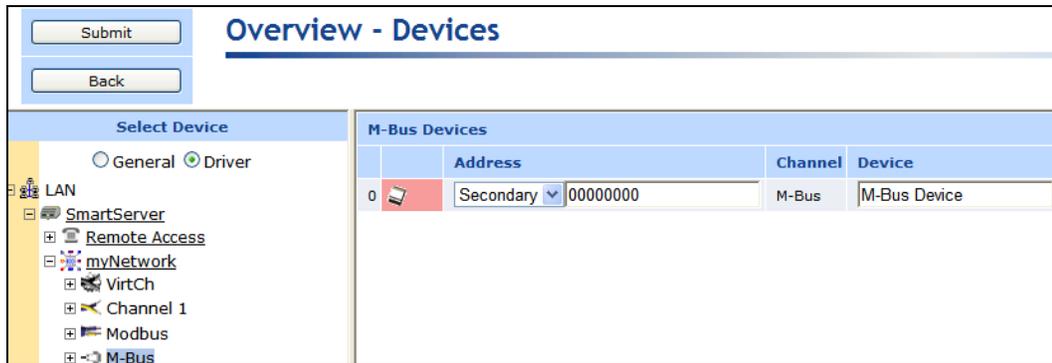
Viewing M-Bus Devices

You can view and configure the all the M-Bus devices in your network or on a specific channel using the **Overview – Devices** Web page. This Web page displays the primary or secondary address, parent channel, and name of each M-Bus device. To view M-Bus devices with the **Overview – Devices** Web page, follow these steps:

1. To configure the primary or secondary addresses, or names of the M-Bus devices, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click the network or a M-Bus channel in the SmartServer tree, point to **Overview**, and then select **Devices**.



3. The **Overview – Devices** Web page opens.



4. You can sort the objects listed by clicking a property header.

5. View and /or configure the following properties:

- Icon/Status* Displays the icon used to represent the M-Bus device in the SmartServer tree and in the application frame. If the device is offline, this box is highlighted red.
- Address* Displays whether the M-Bus device uses primary or secondary addressing. Primary addressing is preferred because it makes replacing M-Bus devices more transparent. Each of these addressing methods is described as follows:
 - **Primary.** The primary address is assigned by the network management tool used to install the M-Bus device (analogous to a LONWORKS subnet/icon address). Enter a primary address between 0 to 250 for the M-Bus device.
 - **Secondary.** The secondary address is manufactured into the device at the factory (analogous to a LONWORKS Neuron ID). Enter a secondary address between 0 to 99,999,999 for the M-Bus device.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

<i>Channel</i>	Displays the name of the channel on which the M-Bus device is attached.
<i>Device</i>	Displays the name of the M-Bus device. In Driver mode, you can change the name. In General mode, this field is read-only.

6. Click **Submit** to save any changes.

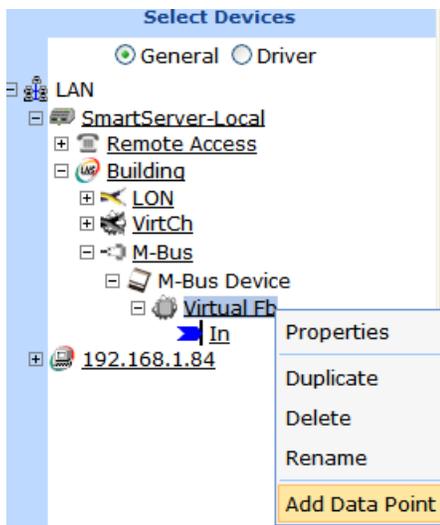
Creating and Configuring M-Bus Data Points

You can dynamically add configuration properties to the M-Bus devices on the network (you cannot add static data points).

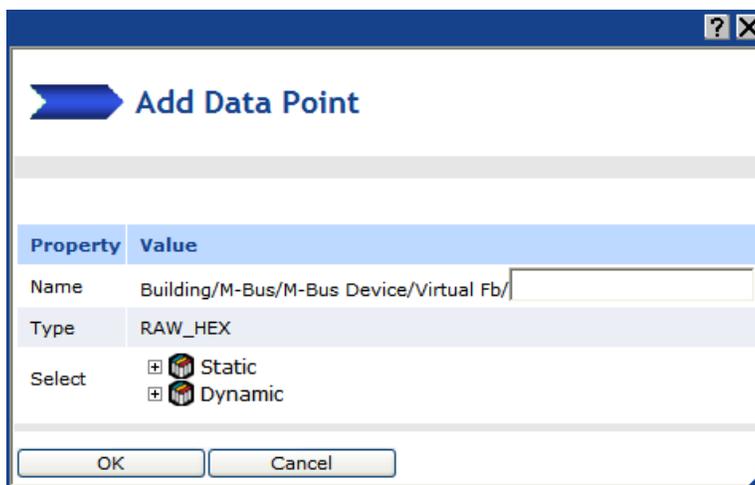
Creating M-Bus Data Points

To add this type of dynamic data point to an M-Bus device, follow these steps:

1. Right-click the virtual functional block of an M-Bus device, and then select **Add Data Point** on the shortcut menu.



2. The **Add Data Point** dialog opens:



3. Enter the following data point properties:

Name Enter a name for the data point.

- Type* Displays the configuration property type of the currently selected data point.
- Select* Select the type of data point to create: **Static** or **Dynamic**. The **Dynamic** option is only available for devices with dynamic interfaces.
- **Static**. Expand the static icon to show all the static data points programmatically defined by the device's external interface. Click the static data point to be created.
 - **Dynamic**. Expand the dynamic icon to show all the folders in the lonworks/types directory on the SmartServer or OpenLNS Server, and then expand a folder in a **lonworks/types** directory to show all the available resource files in that folder. Expand a resource file and then expand its configuration property types or network variable types to show all the available SNVTs, UNVTs, or built-in data types in that file. Click the SNVT, UNVT, or built-in data type to be used for creating the data point.
4. Click **OK**. The data point is added to the bottom of the tree of its parent virtual functional block.
 5. Click **Submit**.

Configuring M-Bus Data Points

You can configure M-Bus data points using both the **General** and **Driver** modes. The following summarizes the data point configuration tasks you can perform in each mode:

- **General** mode. Enable and set default and invalid values; make a data point persistent; set the poll rate; set configuration properties (heartbeat, throttle, offline, and send on delta); and add or delete presets and fields. See *Configuring Data Point General Properties* for more information on modifying these properties.
- **Driver** Mode. Change the icon of and hide the data point. Change the poll rate, format and type parameters, and the length.

To configure the driver properties of an M-Bus data point, follow these steps:

1. Click **Driver**.
2. Select one or more M-Bus data points to be configured.
3. The **Setup - M-Bus Data Point Driver** Web page opens.

Setup - M-BUS Data Point Driver

Submit Back

Select M-Bus Data Points
 General Driver

LAN
 SmartServer-Local
 Remote Access
 Building
 LON
 VirtCh
 M-Bus
 M-Bus Device
 Virtual Fb
 In
 Modbus DP
 192.168.1.84

Name: Building/M-Bus/M-Bus Device/Virtual Fb/Modbus DP
 Description:

M-Bus Data Point Property	Value
Icon	Dp_In
Hidden	<input type="checkbox"/>
Poll Rate	0 Seconds
Direction	<input checked="" type="radio"/> In <input type="radio"/> Out <input type="radio"/> Undefined
Format Description	#8000014600000000[4].UCPT_MBS1
Length	8

4. Configure the following M-Bus data point properties:

<i>Name</i>	Displays the network path of the functional block in the following format: <i><network>/<channel>/<device>/<functional block>/<data point></i> . This field is read-only.
<i>Description</i>	Enter an optional description of the functional block. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

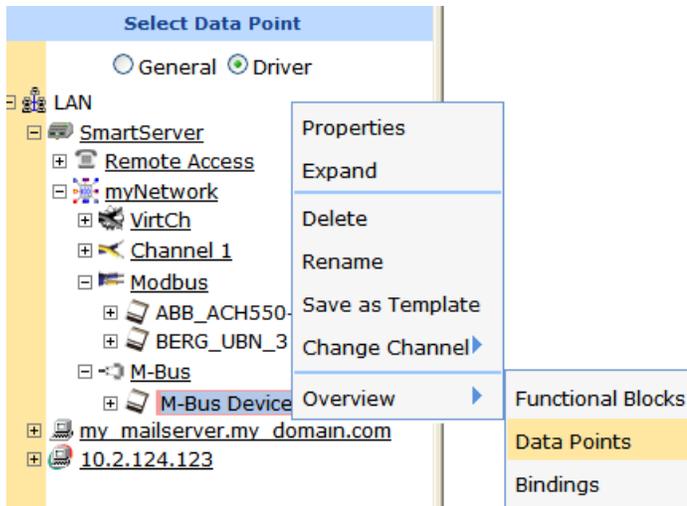
M-Bus Data Point Property

<i>Icon</i>	Displays the icon used to represent the M-Bus data point in the tree. You can change the icon for the M-Bus data point by selecting a different icon and then clicking Submit .
<i>Hidden</i>	Hides the M-Bus data point in the navigation pane. If the M-Bus data point is not actively being used, you can hide it to simplify the Web interface. To show hidden M-Bus data points, click Settings to open the Global Settings dialog. In the Display Hidden property, select the Data Points check box and then click Close .
<i>Poll Rate</i>	Set the frequency in which the SmartServer polls the data point. The typical minimum poll rate is 30 seconds; the maximum poll rate is 1 second. The default poll rate is 0 seconds, which means polling is disabled. Note: This value is independent of any poll rates set for the data point in the Configure - Data Point Web page or in a SmartServer application.
<i>Direction</i>	Specifies whether the M-Bus data point is an Input (In) data point, Output data point (Out), or Undefined .
<i>Format Description</i>	Displays the data type (SNVT, UNVT, or built-in type) of the data point in the following format: <i>#<manufacturer ID>[scope selector].<type name></i> . You can change the data type to any of the SNVT, UNVT, or built-in data types defined in the resource files on your computer.
<i>Length</i>	Displays the length (in bytes) of the data point.

Viewing M-Bus Data Points

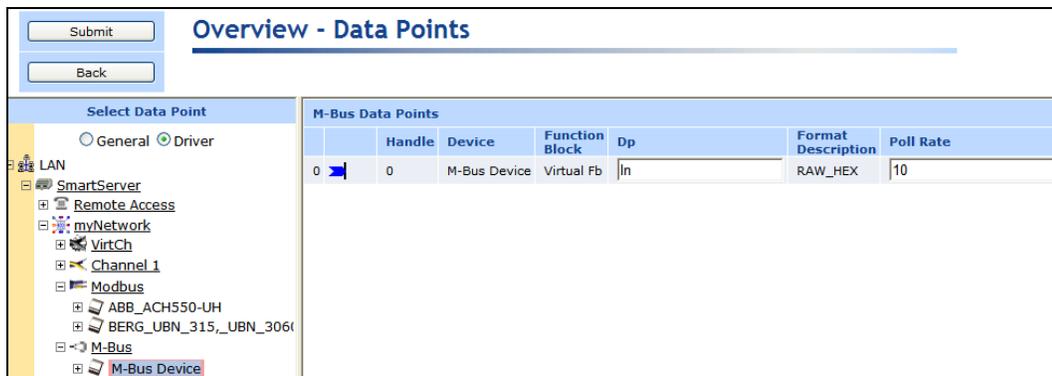
You can view and configure all the data points on an M-Bus device using the **Overview - Data Points** Web page. This Web page includes sortable columns for the name and poll rate of each data point on a M-Bus device. To use the **Overview - Data Points** Web page to configure the data points on a M-Bus device, follow these steps:

1. To configure the names or poll rates of the M-Bus data points, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click an M-Bus device, point to **Overview**, and then click **Data Points** on the shortcut menu.



Note: You can select two or more M-Bus devices or functional blocks and view all the data points on those devices or functional blocks in the same **Overview – Data Points** page; however, the SmartServer’s performance may be impacted by trying to create large lists of objects.

3. The **Overview - Data Points** Web page opens.



4. By default, the M-Bus data points are listed by the **Start Address** column in ascending order. You can sort the data points by clicking a property header. You can view and configure the following properties for each data point on the M-Bus device:

- Icon/Status* Displays the icon used to represent the M-Bus data point in the SmartServer tree and in the application frame. If the data point is offline, this box is highlighted red.
- Handle* Displays the handle assigned to the M-Bus data point by the SmartServer. This field is read-only, and is only displayed in **Driver** mode; it is not displayed in **General** mode.
- Device* Displays the name of the M-Bus data point’s parent device.
- Functional Block* Displays the name of the M-Bus data point’s parent functional block.
- Dp* Displays the name of the M-Bus data point. In **Driver** mode, you can change the name. In **General** mode, this field is read-only.
- Format Description* Displays the data type (SNVT, UNVT, or built-in type) of the data point in the following format: #<program ID>[<scope selector>].<type name>. You can click the button to the right to change the data type to any of the SNVT, UNVT, or built-in data types defined in the resource files in the

/lonworks/types folder on the SmartServer flash disk.

This property is only displayed in **Driver** mode; it is not displayed in **General** mode.

Poll Rate

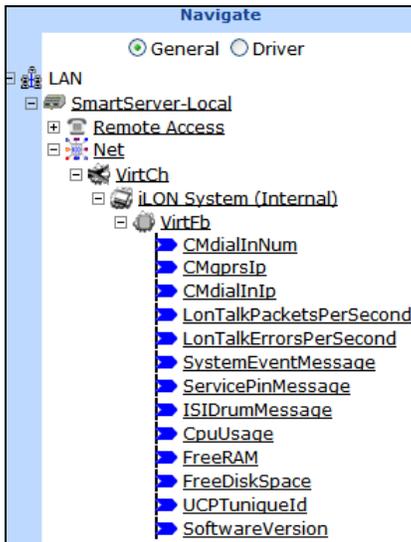
Displays the frequency in which the SmartServer polls the data point. The recommended minimum poll rate is 30 seconds; the maximum poll rate is 1 second. The default poll rate is 0 seconds, which means polling is disabled.

In **Driver** mode, you can change the poll rate. This property is not displayed in **General** mode.

7. Click **Submit** to save any changes.

Using the Virtual Channel

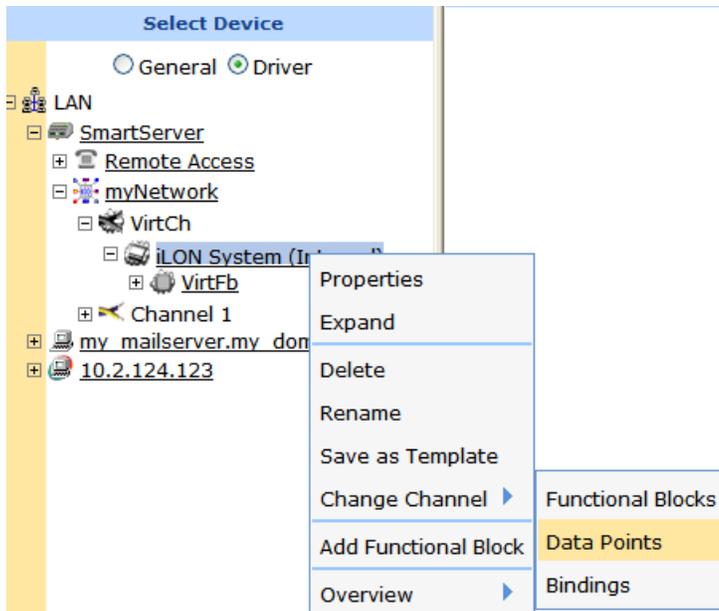
The virtual channel is the SmartServer's internal channel. It is used as a gateway for system information that is used by the data points on the SmartServer. You can expand this channel, expand the **i.LON System (Internal)** device, and then expand the **VirtFB** virtual functional block to show data points representing the SmartServer's free RAM, free disk space, CPU usage, battery level, software version number, last received service pin message, and other information.



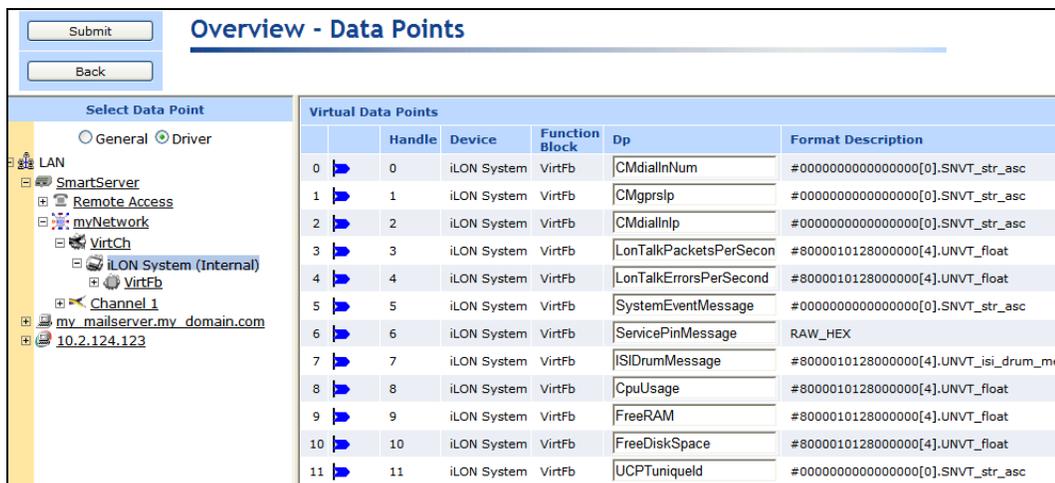
You can log the data points on the **i.LON System (Internal)** device, trigger alarms based on their values, and so on. For example, you could add the **FreeRAM** data point to a data logger and record its value once daily, or you could add this data point to alarm generator and trigger an alarm when it reaches a certain constant value. In addition, you can create a data point with a constant value on this channel and use this data point on other channels.

You can use the **Overview – Data Points** Web page to view or configure the names and poll rates of the Virtual data points on the SmartServer's internal systems device (**i.LON System**). To view the Virtual data points with this Web page, follow these steps:

1. To rename or set the poll rates for the Virtual data points, click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
2. Right-click the **i.LON System (Internal)** device or the **VirtFb** functional block below it in the SmartServer tree, point to **Overview**, and then select **Data Points**.



3. The **Overview – Data Points** Web page opens.



4. You can sort the objects listed by clicking a property header.
5. View and /or configure the following properties:
 - Icon/Status* Displays the icon used to represent the data point in the SmartServer tree and in the application frame (input, output, or unspecified) . If the data point is offline, this box is red.
 - Handle* Displays the handle assigned to the Virtual data point by the SmartServer. This field is read-only, and is only displayed in **Driver** mode; it is not displayed in **General** mode.
 - Device* Displays the name of the data point's parent device, which is **iLON System**. This field is read-only.
 - Functional Block* Displays the name of the data point's parent functional block, which is **VirtFb**. This field is read-only.
 - Dp* Displays the name of the data point. In **Driver** mode, you can change the name. In **General** mode, this field is read-only.

<i>Format Description</i>	<p>Displays the SNVT, UNVT, SCPT, or UCPT used by the data point, and it specifies the format (e.g., SI metric or US customary) used if the type has multiple formats such as SNVT_temp_f. The format description is displayed in the following format: #<program ID>[scope selector].<type name>.</p> <p>For data points with multiple formats such as SNVT_temp_f, you can click the arrow to the right to select a different format defined for that data type from the list that appears. Using a SNVT_temp_f data point for example, you can click the arrow to change the format to #US, #SI, or #US_Diff.</p> <p>For static data points with changeable types or dynamic data points, you can change the data point's type and/or format in the Select Types dialog that you can open from the Format Description property in the data point's Setup – Data Point Driver Web page. To open this Web page, click the Driver option above the navigation pane on the left side of the SmartServer Web interface, and then click the data point.</p> <p>This property is only displayed in Driver mode; it is not displayed in General mode.</p>
<i>Poll Rate</i>	<p>Displays the frequency in which the SmartServer polls the data point. The typical minimum poll rate is 30 seconds; the maximum poll rate is 1 second. The default poll rate is 0 seconds, which means polling is disabled.</p> <p>In Driver mode, you can change the poll rate. This property is not displayed in General mode.</p>

6. Click **Submit** to save any changes.

Installing LONWORKS Networks

You can use the SmartServer to install LONWORKS networks. The advantage of installing a network with the SmartServer is that it can install devices with minimal user input. To install a network, you only need to acquire the Neuron IDs of the devices to be installed, select the devices to be installed, and then enable the Smart Network Management option in the **Setup - LON Device Driver** Web page of one of the selected devices. The SmartServer will then automatically fetch the program IDs of the devices, download the appropriate device applications based on the program IDs, load and instantiate the device interface files based on the program IDs, commission the devices, reset the devices, and then start the device applications.

You can install networks under a number of installation scenarios. Installation scenarios include engineered system installation, ad-hoc installation, and a combination of both. The best scenario for a given network depends on many factors including the skill level of the installer, desired flexibility for the network, and the end-user requirements.

With an *engineered system*, you design a network offsite with OpenLNS CT, the SmartServer OpenLNS tree, or another OpenLNS application, or if you are installing a small network, you can design the network with the SmartServer tree in standalone mode. If you are using the SmartServer to install an engineered system, you can use the OpenLNS tree if you intend on using OpenLNS network management services, or you can use the SmartServer tree with the SmartServer operating in standalone mode. A network being run in standalone mode can support up to approximately 300 devices (for FT-10 networks, you need to attach a physical layer repeater to the network to exceed the 64-device limit posed by the physical channel). Once you are onsite, you can attach the SmartServer to the network and install the devices. The engineered system installation scenario makes installation quick, easy, and error-free because most of the time-consuming data entry and processing is done

offsite during the network design phase, yet it provides the flexibility to change the network configuration while onsite. This scenario is often used for building and industrial automation systems, in which the original network design closely matches the actual installation.

With an *ad-hoc system*, you both design and install the network onsite. Network configuration data is incrementally loaded into the physical devices as you add, configure, and install more devices with an OpenLNS tool or the SmartServer. If you use the SmartServer to install an ad-hoc system, you can add and install the devices either using the OpenLNS tree provided that an OpenLNS Server is attached to the LAN and the LNS proxy is enabled on it, or you can use the SmartServer tree with the SmartServer running in standalone mode. The ad-hoc system provides installers with the flexibility to make design decisions onsite. It is most appropriate for small, simple networks in which the details of the system to be installed are not known prior to arriving onsite.

You can also install a network under a combination of both engineered and ad-hoc system scenarios. For example, you can partially design a network offsite, install the devices onsite, and then incrementally add devices to the network design onsite and install them.

The following sections describe the steps required to install a network:

1. Acquiring the Neuron ID of the devices to be installed.
2. Selecting the devices to be installed.
3. Installing the devices using Smart Network Management.

Acquiring the Neuron ID

In order to install a device, you must first acquire its Neuron ID. The Neuron ID is a unique 48-bit number manufactured into the Neuron chip of the device. Acquiring the Neuron ID broadcasts the device's Neuron ID and program ID over the network so that a logical address (Subnet/Node ID) can be assigned to the device.

You can acquire the Neuron ID of a device automatically using device discovery or manually by either pressing a service pin on the device, manually entering a 12-digit hex string, or scanning in a bar code on the device.

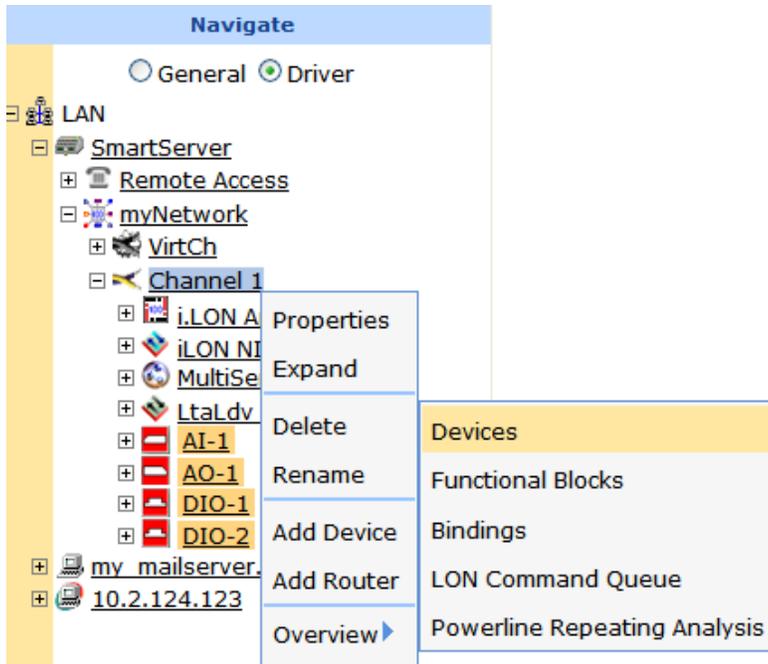
Automatically Acquiring the Neuron ID

You can automatically acquire the Neuron ID of uncommissioned LONWORKS device using device discovery. You can do this from the **Overview – Devices** Web page or from the **Setup – LON Device Driver** Web page.

Automatically Acquiring the Neuron ID with Overview - Devices Web Page

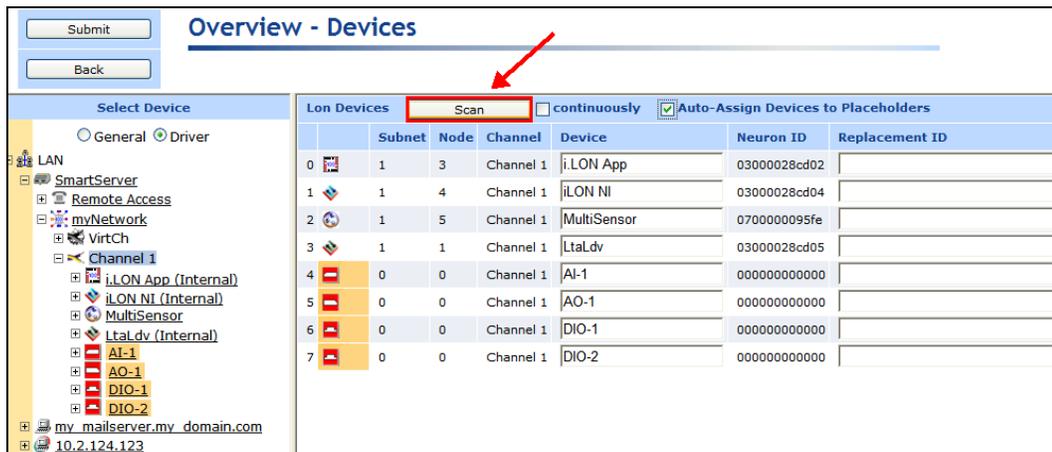
To automatically acquire the Neuron ID of a LONWORKS from the **Overview – Devices** Web page, follow these steps:

1. Verify that the devices for which you are acquiring the Neuron IDs are uncommissioned.
2. Click **Driver**.
3. Right-click a network or channel, point to **Overview**, and then click **Devices** on the shortcut menu.



4. The **Overview – Devices** Web page opens.
5. If you are installing an engineered system, observe that the device icons are shaded based on their current commission status (orange for uncommissioned; clear for commissioned). If you are installing an engineered system (you logically created the devices or “placeholders”), select the **Auto-Assign Devices to Placeholders** check box. This enables the SmartServer to match the discovered devices to the devices you have already logically created.
6. To discover ISI devices, click the button to the right of the **Scan** button to open the **LON Scan Settings** dialog, select the **Include ISI Drum Messages** check box, and then click **OK**.
7. Click **Scan** to discover all uncommissioned devices on the network if they are already attached to the network, or click the **Continuously** check box if you are incrementally attaching the devices to the network. A message is broadcast to the devices on the network that triggers the devices to identify themselves by their Neuron IDs. Click **Cancel Scan** to stop device discovery.

Note: If you are using Standalone mode, the device discovery process may take a few minutes.

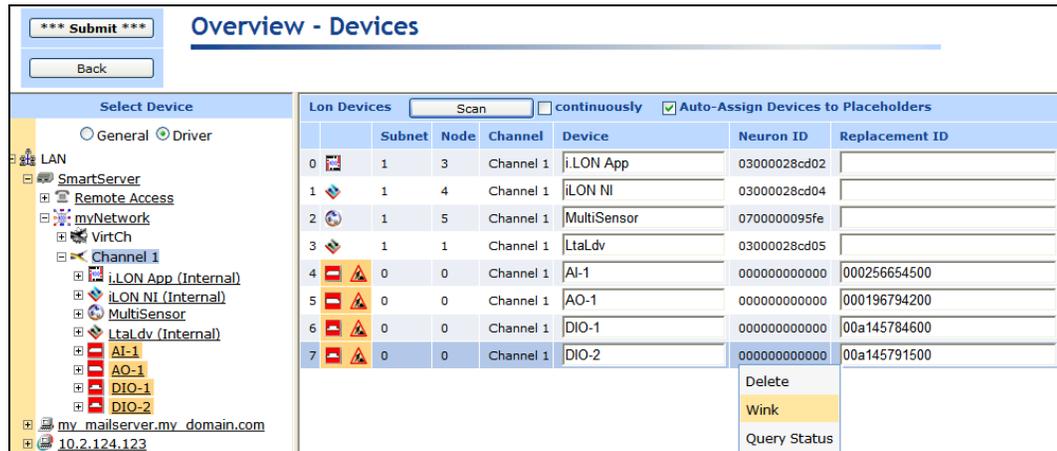


8. If you are discovering an engineered system, the Neuron IDs of the discovered devices appear in the **Replacement ID** property, and the under construction triangle appears to the right of the device icon. If you are discovering an ad-hoc system, the Neuron IDs of the discovered devices

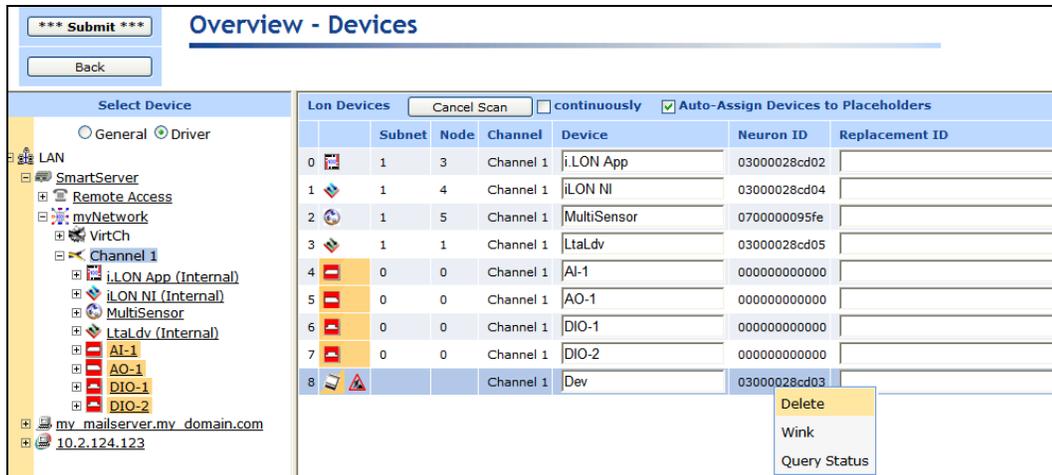
appear in the **Neuron ID** property, and the under construction triangle appears to the right of a generic device icon. By default, device names are based on the name of the XIF file. You can change the name in the **Device** box.



- Optionally, you can wink or test discovered devices. To do this, right-click anywhere in the device's row and then click **Wink** or **Query Status** on the shortcut menu.
 - You can wink a device to identify it on the network and verify that it is communicating properly. A device that supports the Wink command generates an application-dependent audio or visual feedback such as a beep or a flashing service LED when winked. Wink commands are typically used when installing or diagnosing multiple devices in a system, where a network tool may be needed to confirm the identity of a given device.
 - You can test a device to open the **Query Status** dialog and view network statistics such as the number of message transmission and receipt errors, transaction timeouts, and the number of missed or lost messages that indicate whether the device is operating and is configured correctly, and to view the current device configuration and application state. For more information on the **Query Status** dialog, see *Querying Devices* later in this chapter.



- Optionally, you can remove devices that you do not want to be assigned Neuron IDs or you do want to be created. To do this, right-click anywhere in the device's row and then click **Delete** on the shortcut menu.

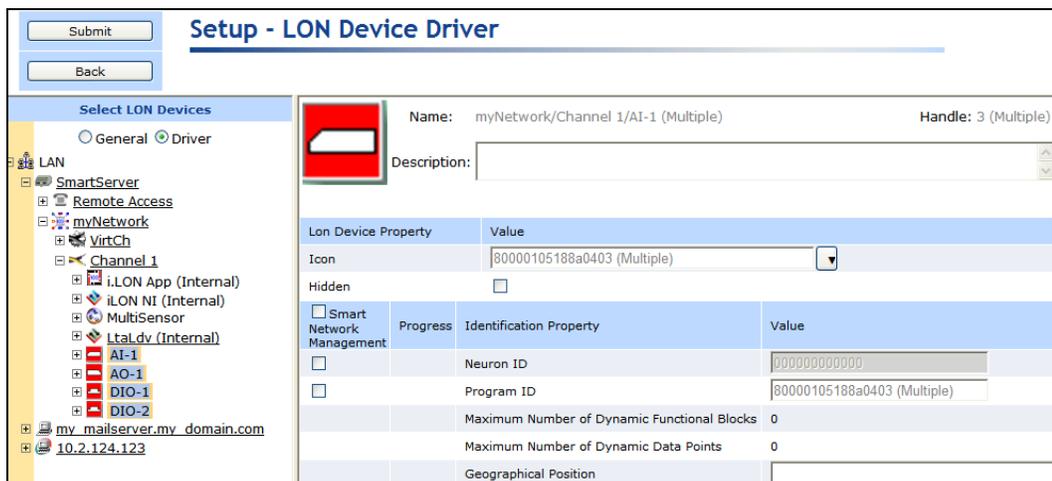


11. Click **Submit**.
12. Select the devices to be commissioned following the *Selecting Devices* section.

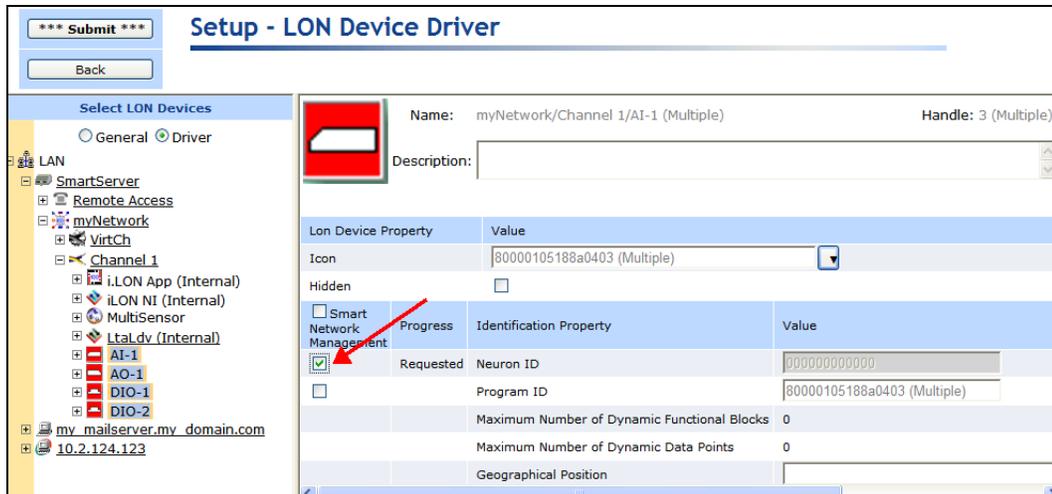
Automatically Acquiring the Neuron ID with LON Device Driver Web Page

To automatically acquire the Neuron ID of a LONWORKS from the **Overview – Devices** Web page, follow these steps:

1. Click **Driver**.
2. Click one or more devices to be installed in the SmartServer tree or OpenLNS tree.
 - To select one device, click that device.
 - To select multiple devices, click one device and then either hold down CTRL and click all other devices to be installed or hold down SHIFT and select another device to install the entire range of devices.
3. The **Setup - LON Device Driver** Web page opens.



4. Select the **Neuron ID** check box and then click **Submit**.



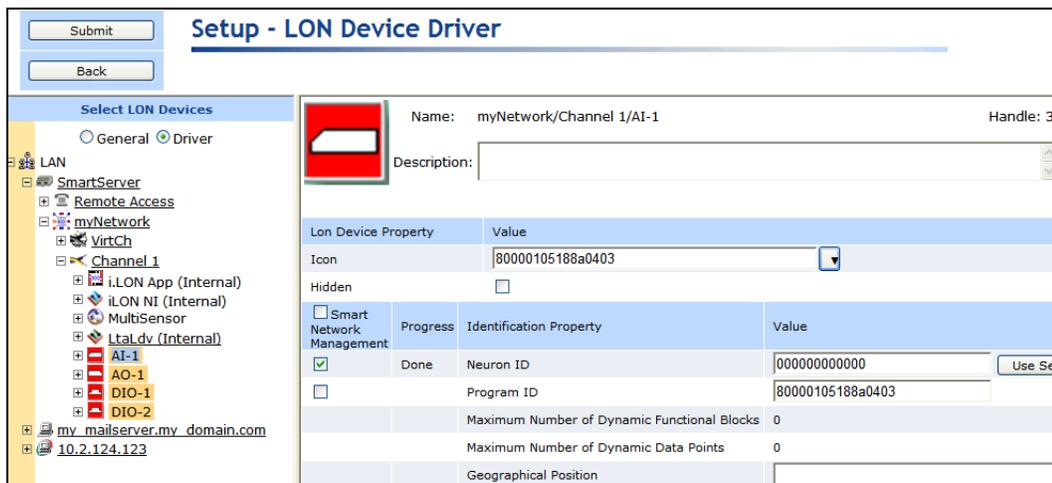
- The SmartServer discovers the selected uncommissioned devices if they are already attached to the network. The **Neuron ID** property in the **Setup - LON Device Driver** Web page for each device is populated as the device is discovered.

Note: If you are using Standalone mode, the device discovery process may take a few minutes.

Manually Acquiring the Neuron ID

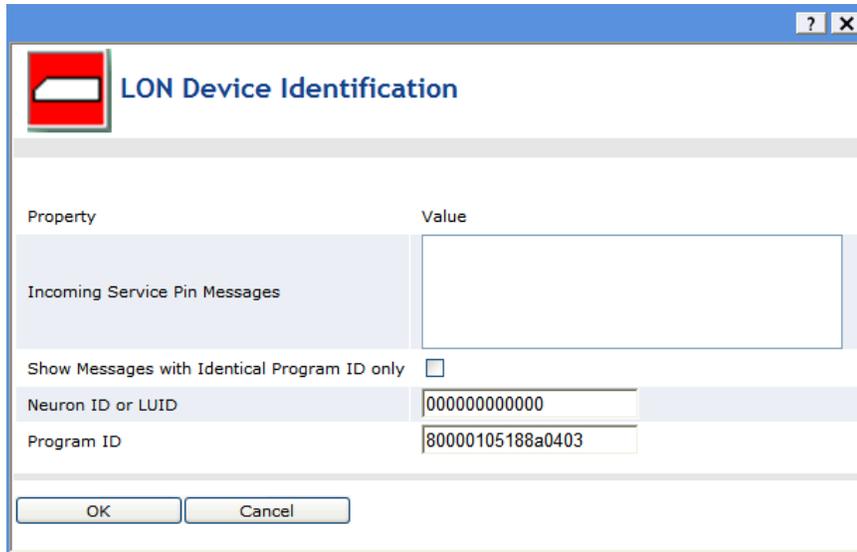
To manually acquire the Neuron ID of a LONWORKS device, follow these steps:

- Click **Driver**.
- Click the device to be installed in the SmartServer tree or OpenLNS tree. Select one device at a time because you cannot manually acquire multiple Neuron IDs in a single transaction.
- The **Setup - LON Device Driver** Web page opens.

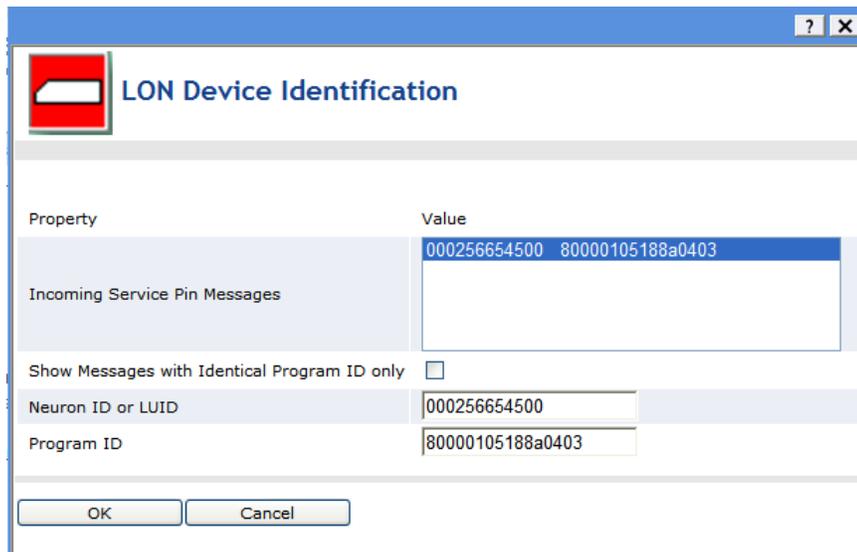


- Enter the Neuron ID in the **Neuron ID** box using the service pin, manual entry, or scanning method.
 - To use the service pin method, click **Use Service Pin** in the **Neuron ID** box and then proceed to step 5.
 - To use the manual entry method, enter the 12-digit hex string on the device in the **Neuron ID** box and then proceed to step 9.

- To use the scanning method, scan the Neuron ID bar code label on the device using a hands-free cordless scanner or a handheld gun-style laser, gun-style LED, and pen-style scanner to scan the bar code and then proceed to step 9.
5. If you are using the service pin method, the **LON Device Identification** dialog opens.



6. Optionally, you can select **Show Messages with Identical Program ID Only** to limit service pin messages to those devices that have the same program ID.
7. Press the service pin of the device. The Neuron ID and program ID of the device being installed are both entered into the **Incoming Service Pin Messages** box, and they are input into the **Neuron ID or LUID** and **Program ID** boxes, respectively. You can manually enter the device's Neuron ID in the **Neuron ID or LUID** box.



Note: If you are acquiring the Neuron ID of the SmartServer [the **i.LON App (Internal)** device], the SmartServer's IP-852 router [the **Router (Internal)** device], or the SmartServer's network interface [the **i.LON NI (Internal)** device] in the OpenLNS tree and **Show Messages with Identical Program ID Only** is cleared, you will receive service pin messages from all three of these internal SmartServer devices. You can ignore the extra service pin messages because the

service pin message from the actual device being commissioned is selected by default based on having a program ID matching the one fetched from the device.

8. Click **OK** to return to the **Setup - LON Device Driver** Web page.
9. Click **Submit**.
10. Select the devices to be commissioned following the *Selecting Devices* section.

Selecting Devices

After acquiring the Neuron IDs of the devices to be installed, you select those devices on the tree. To do this, follow these steps:

1. Click **Driver**.
2. Select one or more devices from the tree to be installed.
 - To select one device, click that device.
 - To select multiple devices, click one device and then either hold down CTRL and click all other devices to be installed or hold down SHIFT and select another device to install the entire range of devices.
3. The **Setup - LON Device Driver** Web page opens. Proceed to the next section, *Installing Devices using Smart Network Management*, to install the devices.

Setup - LON Device Driver

Submit Back

Select LON Devices

General Driver

LAN

- SmartServer
 - Remote Access
 - myNetwork
 - VirtCh
 - Channel 1
 - iLON App (Internal)
 - iLON NI (Internal)
 - MultiSensor
 - Ltal.dv (Internal)
 - AI-1
 - AO-1
 - DIO-1
 - DIO-2
- my mailservr.my_domain.com
- 10.2.124.123

Name: myNetwork/Channel 1/AI-1 (Multiple) Handle: 3 (Multiple)

Description:

Lon Device Property	Value
Icon	80000105188a0403 (Multiple)
Hidden	<input type="checkbox"/>
<input type="checkbox"/> Smart Network Management	
Progress	Identification Property
<input type="checkbox"/> ((multiple))	Neuron ID
	000256664500 (Multiple)
<input type="checkbox"/>	Program ID
	80000105188a0403 (Multiple)
	Maximum Number of Dynamic Functional Blocks
	0
	Maximum Number of Dynamic Data Points
	0
	Geographical Position

Installing Devices with Smart Network Management

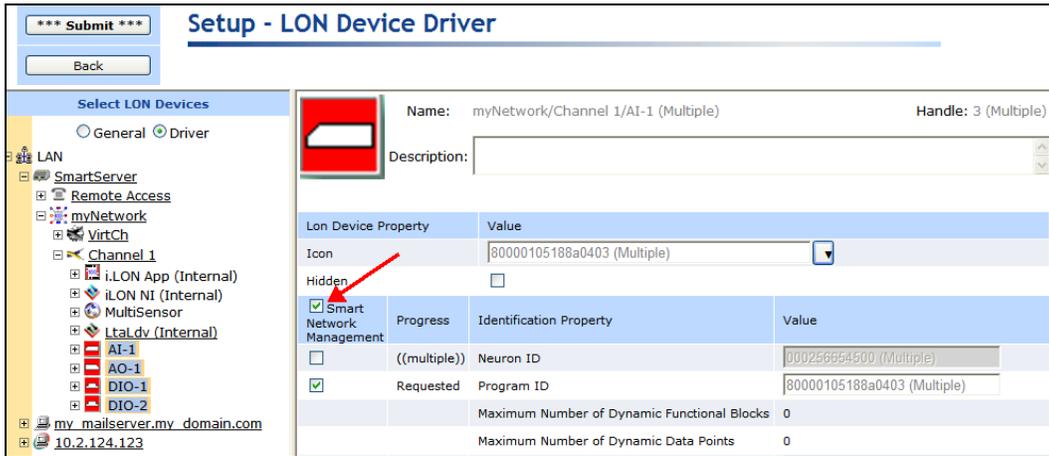
Once you have selected the devices to be installed, you use smart network management on the **Setup - LON Device Driver** Web page to install them. With this option, the SmartServer asynchronously sets the following device properties to the states it determines to be desired:

- program ID.
- commission status (commissioned or decommissioned).
- application state (online or offline).
- application image.
- device template (external interface).
- default configuration property values.

Enabling Smart Network Management

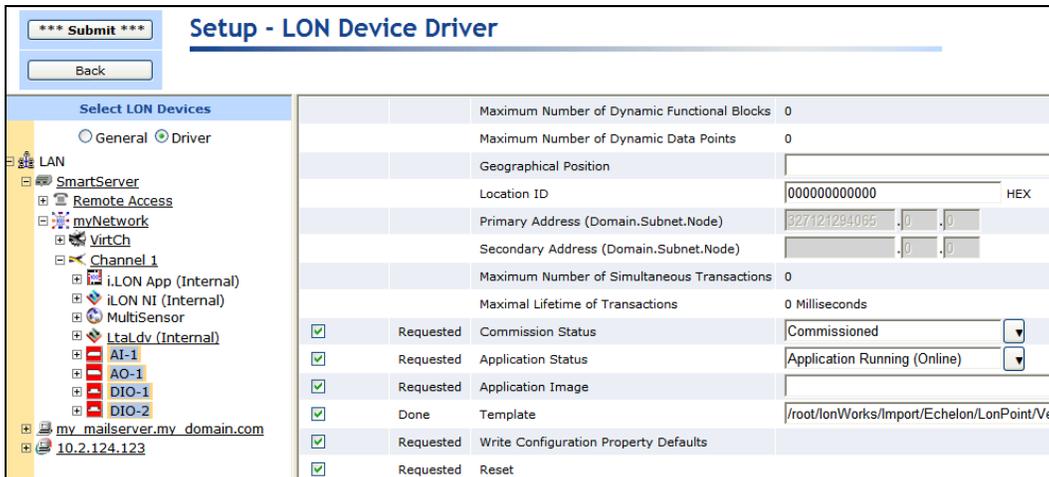
You can enable smart network management for all the device properties by selecting **Smart Network Management** in the **Smart Network Management** column header. Download the device application if you are installing devices that must be loaded with an application image files. The application image

to be downloaded to the devices must be in the **/LonWorks/import** folder on the SmartServer flash disk for the SmartServer to install the devices successfully.



You can also enable smart network management on individual device properties by selecting the check box located to the left of the property under the **Smart Network Management** column and clicking **Submit**. If you are installing pre-loaded devices, select the **Smart Network Management** check boxes for the following properties: **Commission Status**, **State**, **Template**, **Write Configuration Property Defaults**, and **Reset**. Verify that all other check boxes are cleared. This ensures that the SmartServer does not update the application image currently on the devices.

Once smart network management is enabled for a device property, the SmartServer attempts to perform the corresponding network management command. The current statuses of the network management commands appear in the **Progress** column.



Installing Devices

After enabling smart network management for all the applicable device properties, click **Submit**. The SmartServer then does the following for each device you are installing:

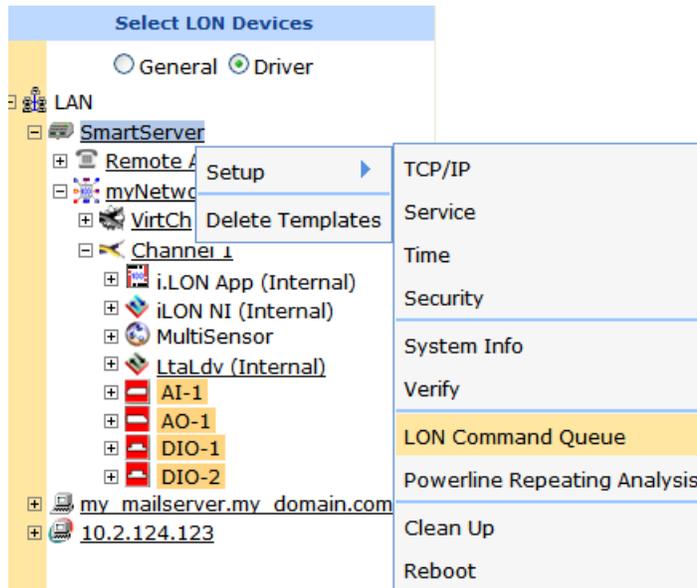
1. Fetches the program ID of the device (if the **Smart Network Management** check box is selected for the **Program ID** property).
2. Downloads the application image file to the device (if the **Smart Network Management** check box is selected for the **Application Image** property). The SmartServer downloads the application image file in the **/LonWorks/import** folder that has a program ID matching that of the device application.

3. Loads and instantiates the device interface (if the **Smart Network Management** check box is selected for the **Template** property).
 - a. The SmartServer first attempts to load the device template (.XML file) in the **/config/template/lonworks** folder on the flash disk that has a matching program ID.
 - b. If the SmartServer cannot find a matching device template, the SmartServer loads the device interface (XIF) file in the **/LonWorks/import** directory that has a matching program ID.
 - c. The SmartServer creates all the functional blocks and data points defined by the device interface.
4. Re-commissions the device. Commissioning downloads network configuration data and application configuration data to the device.
5. Writes default configuration property values to the device.
6. Resets the device, which starts the device application.
7. Sets the device application online.

Checking Device Status

You can use the **LON Command Queue** Web page to check the status of the management commands you have submitted for one or more devices. To use this Web page, follow these steps:

1. Right-click the SmartServer icon, point to **Setup**, and then click **LON Command Queue** on the shortcut menu. Alternatively, you can open the **Setup** menu and then click **LON Command Queue**.



2. The **LON Command Queue** Web page opens.

Name	Position	Unique ID	Command	Status	Last Update
myNetwork/Channel 1/MultiSensor		0700000095fe	ChangeApplicationStatus	STATUS_DONE	2009-09-17 11:02:15
myNetwork/Channel 1/MultiSensor		0700000095fe	ChangeCommissionStatus	STATUS_DONE	2009-09-17 11:00:53
myNetwork/Channel 1/iLON NI		03000028cd04	ChangeApplicationStatus	STATUS_DONE	2009-09-14 16:57:56
myNetwork/Channel 1/iLON NI		03000028cd04	ChangeCommissionStatus	STATUS_DONE	2009-09-14 16:57:53
myNetwork/Channel 1/AI-1		000256654500	UpdateCpDefaults	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/AI-1		000256654500	ImageDownload	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/AI-1		000256654500	ChangeApplicationStatus	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/AI-1		000256654500	ChangeCommissionStatus	STATUS_PENDING	2009-09-18 17:48:05
myNetwork/Channel 1/AI-1		000256654500	FetchProgId	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/AI-1		000256654500	Reset	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/AI-1		000256654500	GetTemplate	STATUS_DONE	2009-09-18 17:12:27

- The management commands submitted for all devices and their statuses appear in a table. By default, the names of the first 20 devices listed in the tree in the left frame are listed in descending alphabetical order and the commands executed on them are listed in descending chronological order (most recent to earliest). You can sort the management commands by clicking the column headers.

To view multiple additional devices, click a device in the tree, and then either hold down CTRL and click all other additional devices to be viewed, or hold down SHIFT and select another device to view the entire range of additional devices.

To view the status of a specific device, click one of the blue-highlighted devices in the tree to clear the pre-selected devices and then click the device to be viewed. To view the statuses for a set of specific devices, click one of the blue-highlighted devices in the tree to clear the pre-selected devices, click a device in the tree, and then either hold down CTRL and click all other devices to be viewed, or hold down SHIFT and select another device to view the entire range of devices.

- You can right-click the header, a table entry, or an empty space in the application frame and select one of the following options in the shortcut menu:

Name	Position	Unique ID	Command	Status	Last Update
myNetwork/Channel 1/MultiSensor		0700000095fe	ChangeApplicationStatus	STATUS_DONE	2009-09-17 11:02:15
myNetwork/Channel 1/MultiSensor			ChangeCommissionStatus	STATUS_DONE	2009-09-17 11:00:53
myNetwork/Channel 1/iLON NI			ChangeApplicationStatus	STATUS_DONE	2009-09-14 16:57:56
myNetwork/Channel 1/iLON NI			ChangeCommissionStatus	STATUS_DONE	2009-09-14 16:57:53
myNetwork/Channel 1/DIO-2		00a145791500	UpdateCpDefaults	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/DIO-2		00a145791500	ImageDownload	STATUS_PENDING	2009-09-18 17:48:44
myNetwork/Channel 1/DIO-2		00a145791500	ChangeApplicationStatus	STATUS_DONE	2009-09-18 17:48:29
myNetwork/Channel 1/DIO-2		00a145791500	ChangeCommissionStatus	STATUS_DONE	2009-09-18 17:48:29
myNetwork/Channel 1/DIO-2		00a145791500	FetchProgId	STATUS_DONE	2009-09-18 17:48:29
myNetwork/Channel 1/DIO-2		00a145791500	Reset	STATUS_REQUEST	2009-09-18 17:47:44
myNetwork/Channel 1/DIO-2		00a145791500	FetchNeuronId	STATUS_DONE	2009-09-18 17:37:03
myNetwork/Channel 1/DIO-2		00a145791500	GetTemplate	STATUS_DONE	2009-09-18 17:16:51
myNetwork/Channel 1/DIO-2		00a145784600	UpdateCpDefaults	STATUS_REQUEST	2009-09-18 17:47:44

Clear Table

Clears all entries in the **LON Command Queue** table. The table will automatically re-list pending commands (**STATUS_REQUEST**) and update their statuses after the commands successfully complete or fail.

Configure Device

Opens the **Setup – LON Device Driver** Web page for the selected device.

Cancel Command

Cancels the selected command and deletes it from the table. You can select multiple commands by clicking one, holding down CTRL, and clicking the

other commands to cancel. You can also use this option to delete inactive commands from the table.

Installing Routers

To commission a router in a LONWORKS network, follow these steps:

1. Click **Driver**.
2. Click the router shape in the SmartServer tree or OpenLNS tree representing the near side of the router (the side closest to the OpenLNS network interface)
3. The **Setup – LON Router Driver** Web page opens.

Lon Device Property	Value		
Icon	Router		
Hidden	<input type="checkbox"/>		
<input type="checkbox"/> Smart Network Management	Progress		
<input type="checkbox"/>	Identification Property		
<input type="checkbox"/>	Neuron ID	000000000000	Use Ser
<input type="checkbox"/>	Program ID	8000010101000000	
	Maximum Number of Dynamic Functional Blocks	0	
	Maximum Number of Dynamic Data Points	0	
	Geographical Position		

4. Acquire the Neuron ID of the near side of the router, or manually enter the Neuron ID in the **Neuron ID** box. You can acquire the Neuron ID automatically using device discovery or manually by pressing the service pin on the router.
 - To automatically acquire the Neuron ID of the near side of the router, verify that the router is uncommissioned, select the **Neuron ID** check box, and then click **Submit**. The SmartServer automatically acquires the Neuron ID using device discovery, and the Neuron ID appears in the **Neuron ID** box.
 - To manually acquire the Neuron ID of the near side of the router, follow these steps:
 - a. In the Neuron ID property on the **Setup – LON Router Driver** Web page, select **Use Service Pin**.
 - b. The **LON Device Identification** dialog opens.

Property	Value
Incoming Service Pin Messages	
Show Messages with Identical Program ID only	<input type="checkbox"/>
Neuron ID or LUID	000000000000
Program ID	8000010101000000

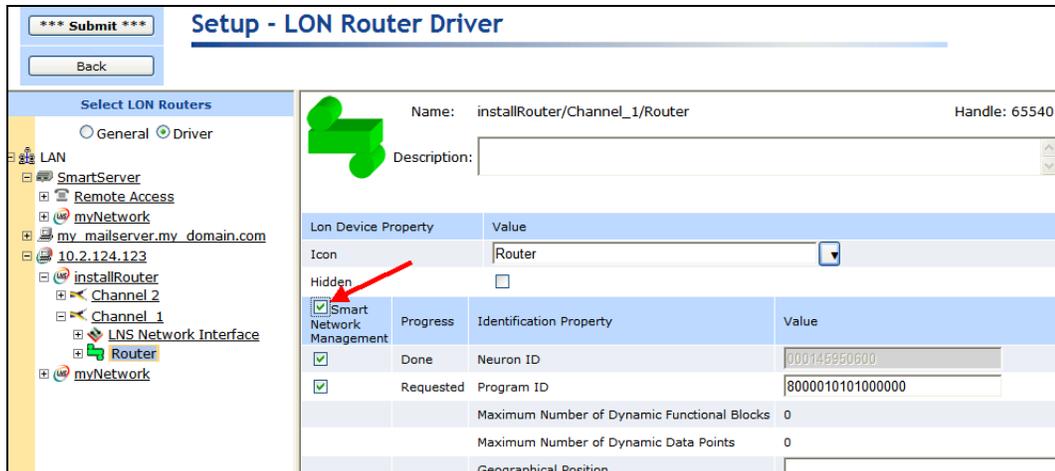
OK Cancel

- c. Press the service pin on the near side of the router. The Neuron ID and Program ID appear in the **Incoming Service Pin Messages** box.

Property	Value
Incoming Service Pin Messages	000145950600 8000010101010421 (Router)
Show Messages with Identical Program ID only	<input type="checkbox"/>
Neuron ID or LUID	000145950600
Program ID	8000010101010421

OK Cancel

- d. Click **OK** to return to the **Setup – LON Router Driver** Web page.
- e. Click **Submit**.
- To manually enter the Neuron ID, enter the 12-digit hex Neuron ID in the **Neuron ID** property and then click **Submit**.
5. Select the **Smart Network Management** check box at the top of the Web page and then click **Submit**. This automatically commissions the router and starts the router application.



Alternatively, you can scroll down to the **Commission Status** property, and either select the individual Smart Network Management property check box to the left or select **Commissioned** from the list to the right. In the **Application Status** property, select the individual Smart Network Management property check box to the left or select **Application Online (Running)** from the list to the right. Click **Submit**.

Detaching the OpenLNS Server from the Network

If the SmartServer is synchronized to an OpenLNS network database, but it will no longer have access to the OpenLNS Server after the network has been installed, change the network management service to **LNS Manual**. This will prevent the SmartServer from displaying repeated “Cannot Connect to OpenLNS Server” error messages. See *Configuring a LonWorks Network* earlier in this chapter for how to set the network management service on the SmartServer.

Maintaining LONWORKS Networks

You can perform routine maintenance to update, repair, and optimize an installed network. You can use the SmartServer to maintain the network, its components, and the network design (if you are using the SmartServer as a network design tool). For example, if a device or router fails, you can replace it on the physical network and then logically replace it on the SmartServer preserving the device’s configuration and all of its connections.

This section describes the following network maintenance tasks you can perform with the SmartServer:

- Load device applications
- Replace devices
- Decommission devices
- Test devices (set devices offline, query devices, and wink devices)

Loading Device Applications

You can use the SmartServer to load an application image into a Neuron-hosted device that has writable application memory (EEPROM or flash). A new application may be needed to change or improve the device’s capabilities or to repair a damaged device application. You can load devices one at a time, or you can perform a batch load.

To load a device application, first obtain from the device manufacturer the binary application image file (**.apb** extension) of the new application. The system image in the application image file must have the same firmware version as the Smart Transceiver or Neuron Chip on the device. If the device interface has changed, you must also obtain a new device interface (XIF) file for the device.

The SmartServer will use the application image file that has program ID matching that of the device from the **/LonWorks/import** folder on the SmartServer flash disk and then download it to the device. The device to be loaded must be online for the upgrade operation to succeed.

To load a device application, follow these steps:

1. Copy the APB file of the new application and the XIF file of the new device interface (if required) to the **/LonWorks/import** folder on the SmartServer flash disk.
2. Click **Driver**.
3. Select one or more devices from the tree to be upgraded.
 - To select one device, click that device.
 - To select multiple devices and perform a batch load, click one device and then either hold down CTRL and click all other devices to be loaded or hold down SHIFT and select another device to load the entire range of devices. The **Setup - LON Device Driver** Web page opens.
4. Select the APB file to be downloaded to the device, following these steps:
 - a. In the **Application Image** property, click the button to the right.

*** Submit ***

Back

Select LON Devices

General Driver

LAN

- SmartServer-Local
- Remote-Access
- Building
 - LON
 - AI-1
 - DIO-2
 - DIO-1
 - LON App (Internal)
 - AO-1
 - VirtCh
 - 192.168.1.84

Name: Building/LON/AO-1

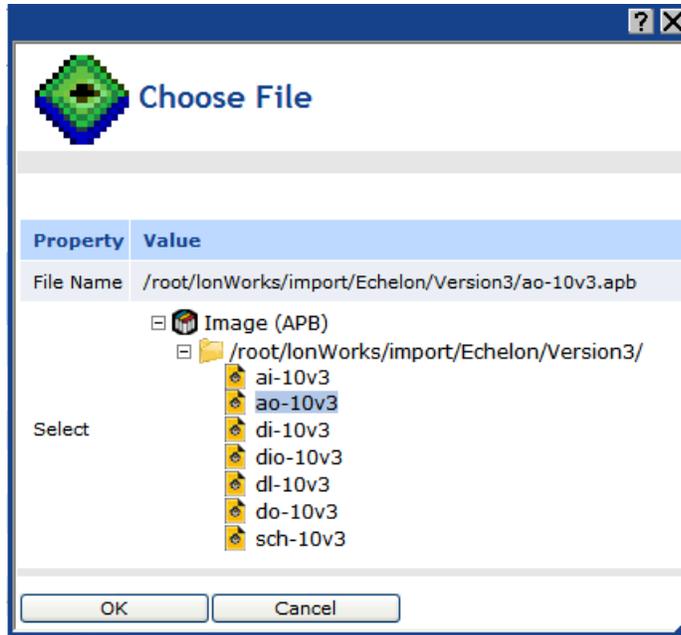
Description:

Lon Device Property		Value
Icon		80000105198a0403
Hidden		<input type="checkbox"/>
Smart Network Management	Progress	Identification Property
<input checked="" type="checkbox"/>	Done	Neuron ID
<input checked="" type="checkbox"/>	Done	Program ID
		Maximum Number of Dynamic Functional Blocks
		Maximum Number of Dynamic Data Points
		Geographical Position
		Location ID
		Primary Address (Domain.Subnet.Node)
		Secondary Address (Domain.Subnet.Node)
		Maximum Number of Simultaneous Transactions
		Maximal Lifetime of Transactions
<input checked="" type="checkbox"/>	Done	Commission Status
<input checked="" type="checkbox"/>	Done	Application Status
<input checked="" type="checkbox"/>	Done	Application Image
<input checked="" type="checkbox"/>	Done	Template

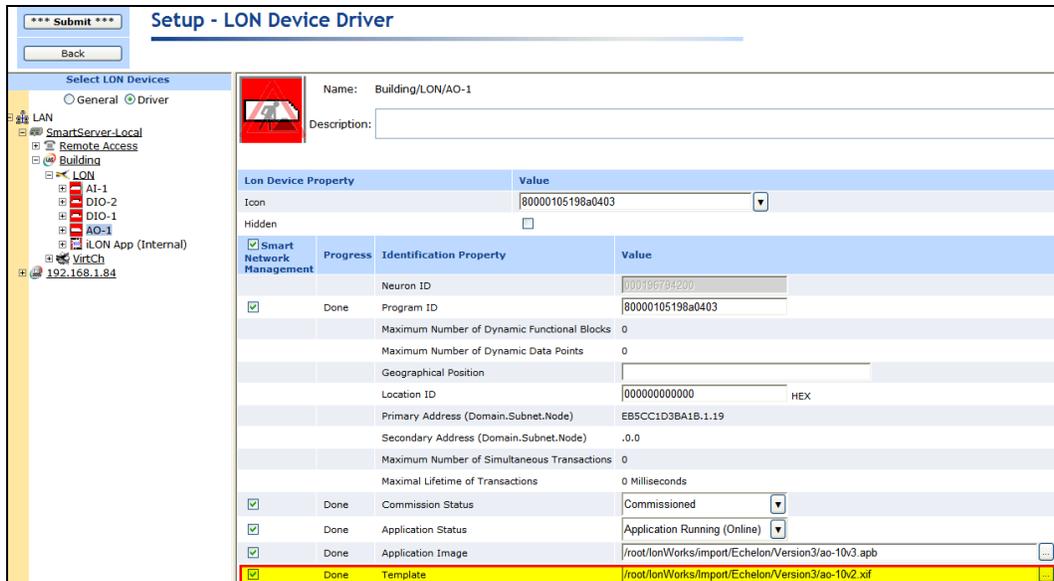
- b. The **Choose File** dialog opens.



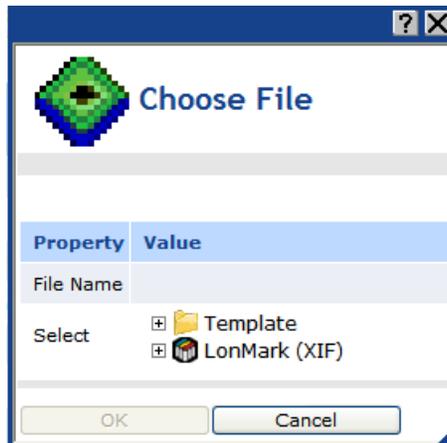
- c. Expand the LonMark **Image (APB)** entry to show the **/lonworks/import** folder. Expand the **lonworks/import** folder to show the application image files in it.



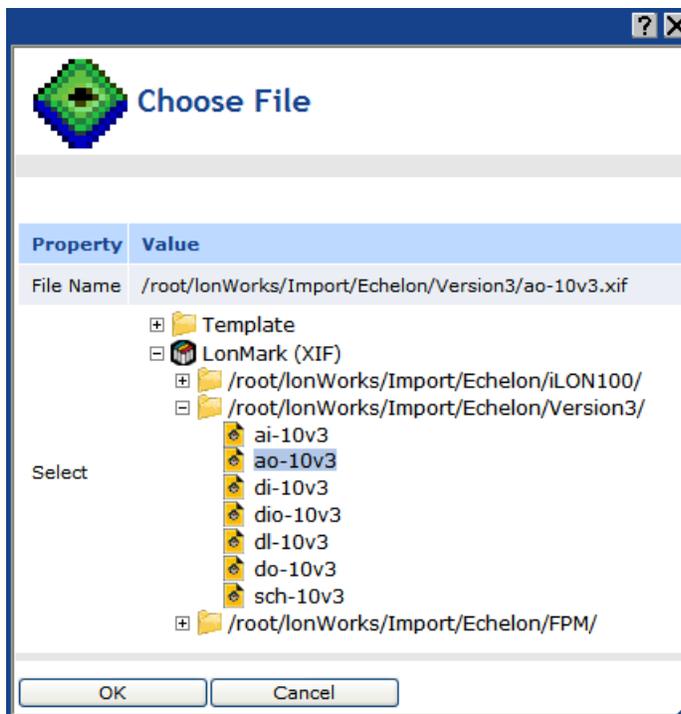
- d. Click the application image file to be downloaded to the devices.
 - e. Click **OK** to return to the **Setup - LON Device Driver** Web page.
5. If the device interface has changed, load a new XIF file for the device onto the SmartServer. To do this follow, these steps:
- a. In the **Template** property, click the button to the right.



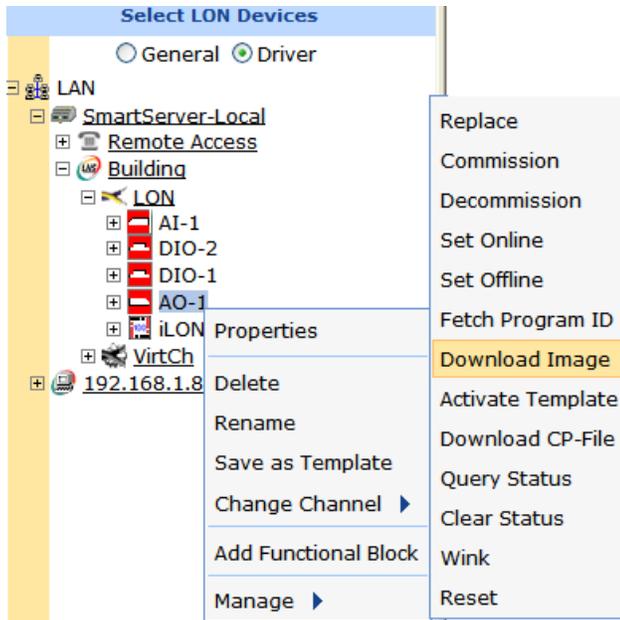
- b. The **Choose File** dialog opens.



- c. Expand either the **LonMark (XIF)** or **Template** folder depending on whether you are using a XIF or XML file for the device interface. If the device being loaded is located in the OpenLNS tree, the **Template** folder is not available.
- d. Expand the subfolders containing the XIF file to be loaded onto the SmartServer and then click the XIF file.



- e. Click **OK** to return to the **Setup - LON Device Driver** Web page.
6. Click **Submit**.
7. Download the application image to the selected devices. To do this, right-click one of the selected devices in the SmartServer tree or OpenLNS tree, point to **Manage**, and then click **Download Image** in the shortcut menu. Alternatively, you can clear and then select the **Smart Network Management** check box to the left of the **Application Image** property in the **Setup -LON Device Driver** Web page and then click **Submit**.



8. Activate the XIF files for the devices (if necessary). To do this, right-click one of the selected devices in the SmartServer tree or OpenLNS tree, point to **Manage**, and then click **Activate Template** in the shortcut menu. Alternatively, you can clear and then select the **Smart Network Management** check box to the left of the **Template** property in the **Setup -LON Device Driver** Web page and then click **Submit**.
9. To check the status of the device upgrade, open the **LON Command Queue** Web page. To do this, right-click the SmartServer entry, point to **Setup**, and then click **LON Command Queue** on the shortcut menu. Alternatively, you can open the **Setup** menu and then click **LON Command Queue**. See *Checking Device Status* earlier in this chapter for more information on using the **LON Command Queue** Web page.

Replacing Devices

You can use the SmartServer to automatically or manually replace a device if the device fails or a newer version of the device becomes available. Before you replace a device, verify that the replacement device has the same program ID as the original device.

If the original device still functions and if physically possible, leave the old device connected to the network until the device replacement has been completed. This allows the SmartServer to decommission the old device so that you can easily reuse it in a new network. This step is not required if the device has failed.

The following sections describe how to automatically and manually replace a device.

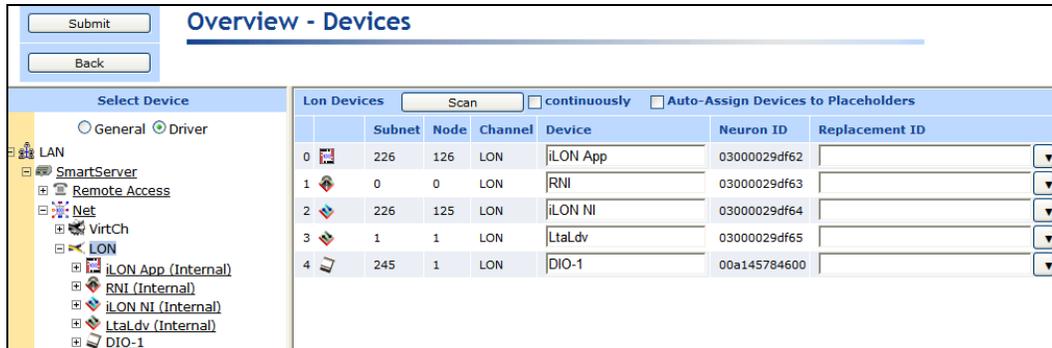
Automatically Replacing Devices

You can attach a replacement device to the network, acquire its Neuron ID automatically using device discovery, and then assign the replacement device to the original device in the SmartServer or OpenLNS database. The SmartServer will then automatically exchange the configurations of the replacement and original devices, preserving the configuration of all the data points and configuration properties of the original device, and then commission the replacement device. You can automatically replace devices from the SmartServer tree or OpenLNS tree in the SmartServer Web interface, and you can use it for OpenLNS managed and standalone networks.

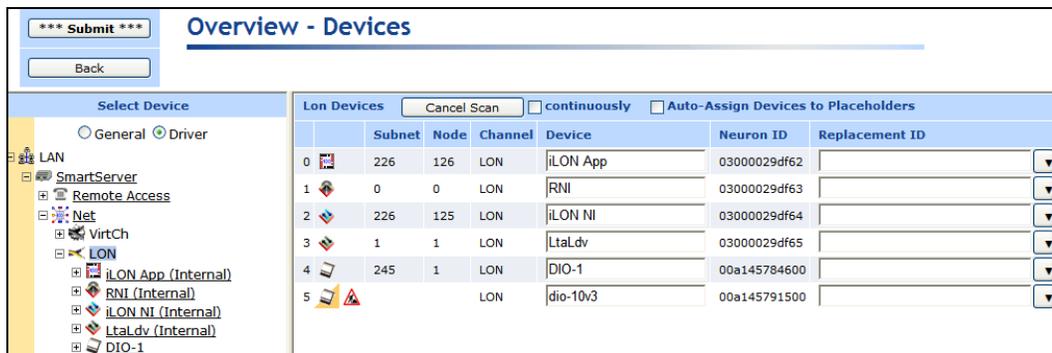
To automatically replace a device, follow these steps:

1. Attach the replacement device to the network by applying power to the device and attaching its network connection as documented by the device manufacturer.

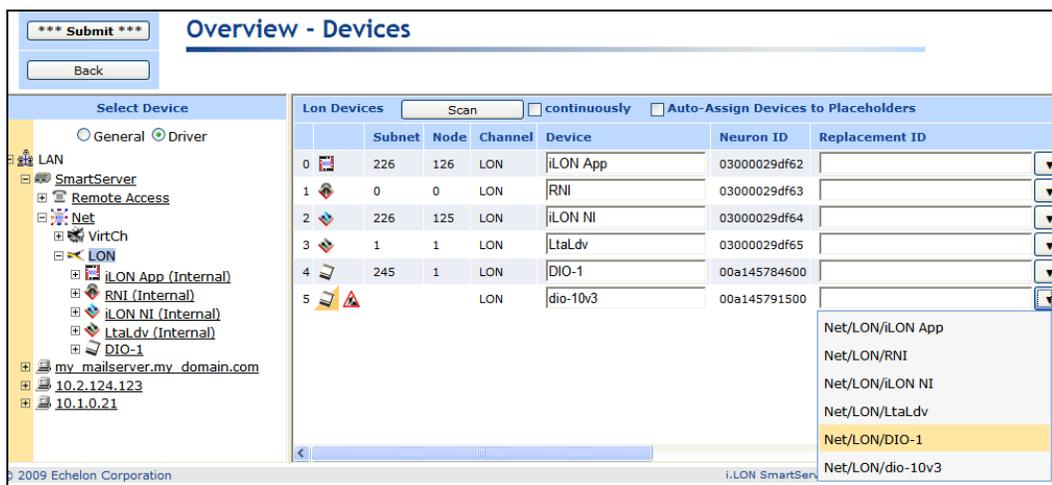
2. Click the **Driver** option at the top of the navigation pane on the left side of the SmartServer Web interface.
3. Open the **Overview – Devices** Web page. To do this right-click a network or channel, point to **Overview**, and then click **Devices**. This example replaces the **DIO-1** device.



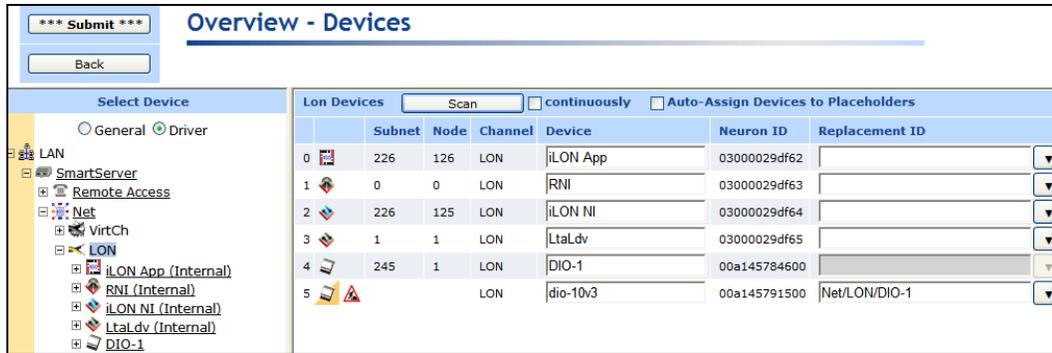
4. Click **Scan** to discover the replacement device.
5. When the replacement device is discovered (**dio-10v3** in this example), its Neuron ID appears in the **Neuron ID** box, and the under construction triangle appears to the right of the generic device icon.



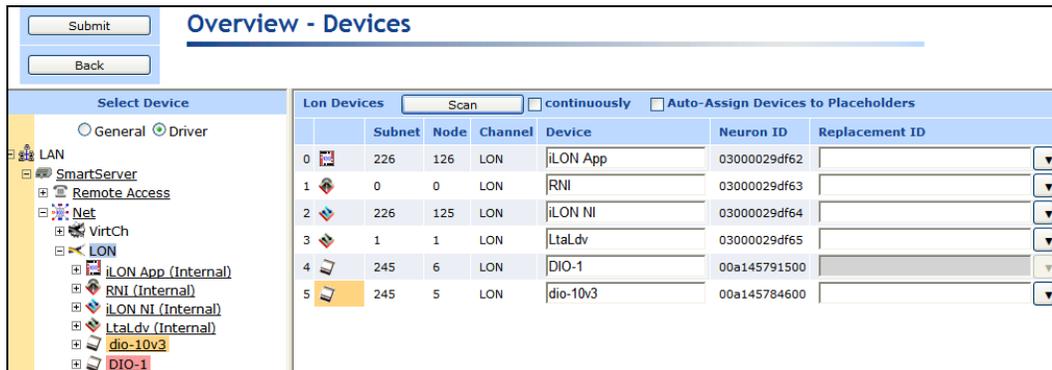
6. In the **Replacement ID** box of the replacement device, select the name of the original device to be replaced.



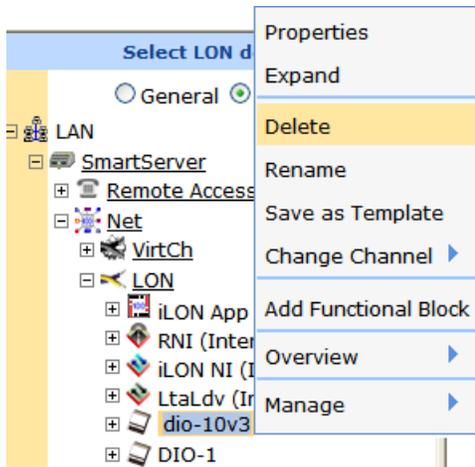
7. The **Replacement ID** of the replacement device is updated with the name of the original device, and the **Replacement ID** of the original device becomes unavailable.



8. Click **Submit**.
9. The SmartServer swaps the configuration of the replacement and original devices, and decommissions the original device (if available). You can observe that the replacement device has assumed the name of the original device (**DIO-1** in this example), and the original device has taken the name of the replacement device, which is based on the XIF file (**dio-10v3** in this example). In addition, the replacement device in the SmartServer tree is marked offline (red) in the SmartServer tree because it is applicationless, and the original device is marked uncommissioned (orange).



10. The replacement device is automatically downloaded, commissioned, set online, updated with the configuration and driver properties of the data points and configuration properties of the original device, and then reset, which starts the device application. You can use the **Lon Command Queue** Web page to check the status of the network management commands sent to the replacement device. To do this, right-click the SmartServer entry, point to **Setup**, and then click **LON Command Queue** on the shortcut menu. Alternatively, you can open the **Setup** menu and then click **LON Command Queue**.
11. You can delete the original device from the SmartServer. To do this, right-click the original device (**dio-10v3** in this example), and click **Delete** on the shortcut menu.

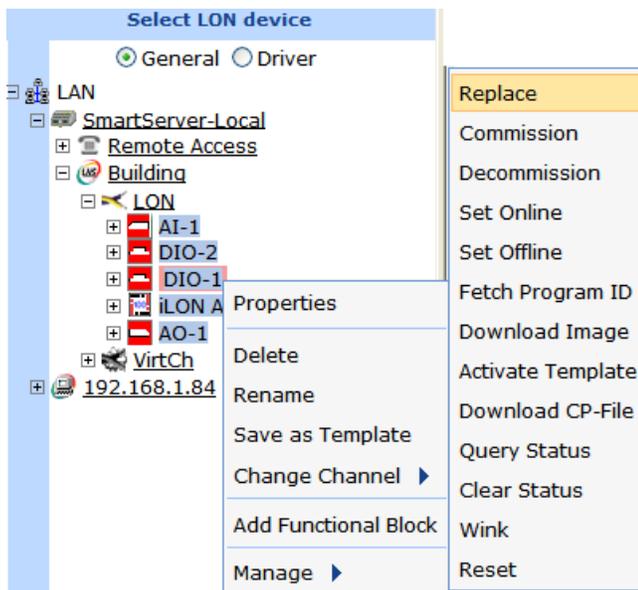


12. You can detach the original device from the network.

Manually Replacing Devices

To manually replace a device with the SmartServer, follow these steps:

1. Attach the replacement device to the network by applying power to the device and attaching its network connection as documented by the device manufacturer
2. Right-click the original device, point to **Manage**, and then click **Replace** on the shortcut menu.



3. The **Replace LON Device** dialog opens.

Property	Value
Incoming Service Pin Messages	
Show Messages with Identical Program ID only	<input checked="" type="checkbox"/>
Neuron ID or LUID	
Program ID	80000105288a0403

4. You can acquire the Neuron ID of the replacement device using a service pin or you can manually enter it.
 - If you are using the service pin method, press the service pin of the device. The Neuron ID and program ID of the device are both entered into the **Incoming Service Pin Messages** box and they are input into the **Neuron ID or LUID** and **Program ID** boxes, respectively.
 - If you are using the manual entry method, enter the 12-digit hex string of the device in the **Neuron ID or LUID** box.
5. Click **OK** to return to the **Setup - LON Device Driver** Web page.
6. Click **Submit**. The SmartServer downloads the application and the configuration data of the original device to the replacement device, decommissions the replacement device, and then commissions the replacement device.
7. To check the status of the device replacement, open the **LON Command Queue** Web page. To do this, right-click the SmartServer icon, point to **Setup**, and then click **LON Command Queue** on the shortcut menu. Alternatively, you can open the **Setup** menu and then click **LON Command Queue**. See *Checking Device Status* earlier in this chapter for more information on using the **LON Command Queue** Web page.

Decommissioning Devices

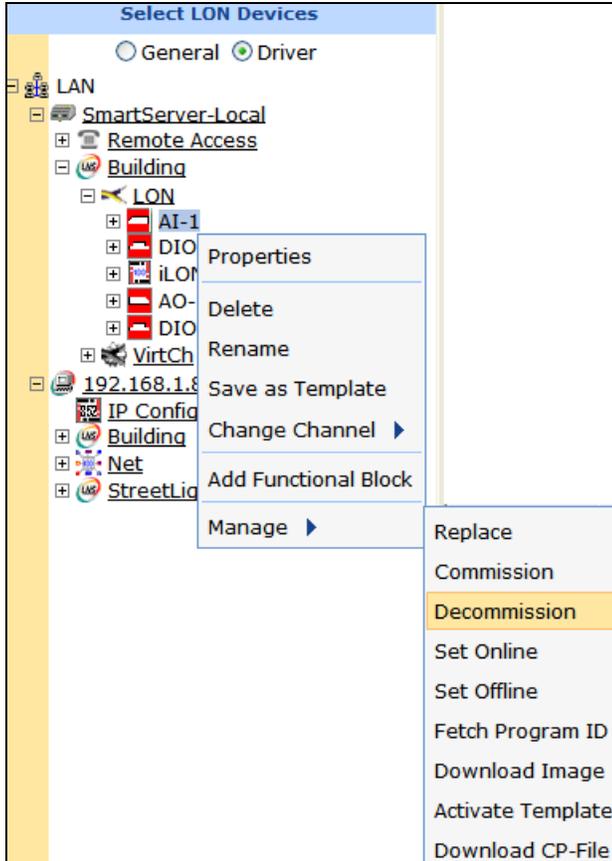
You can use the SmartServer to decommission a device if you are no longer using it or you are moving it to a new network. In addition, you can temporarily decommission a device to optimize, troubleshoot, or repair your network. Decommissioning logically removes the device from the network. When you decommission a device, its Neuron ID is preserved so you can subsequently recommission the device without having to re-acquire its Neuron ID. In addition, the configuration properties of the device are preserved in the SmartServer's internal database (the **/config/network** folder on the SmartServer flash disk) or the OpenLNS network database. You can then later recommission the same or different devices without having to load configuration property files to the device.

To decommission a device, follow these steps:

1. Click **Driver**.
2. Select one or more devices from the tree to be decommissioned. To select one device, click that device. To select multiple devices and perform a batch upgrade, click one device and then either

hold down CTRL and click all other devices to be decommissioned or hold down SHIFT and select another device to decommission the entire range of devices. The **Setup - LON Device Driver** Web page opens.

3. Right-click a selected device, point to **Manage**, and click **Decommission**.



Alternatively, you can change the **Commission Status** property to **Uncommissioned** in the **Setup - LON Device Driver** Web page, which appears when you select devices in step 2.

4. The SmartServer places the device in the soft-offline state (the device has an application loaded on it and the device is configured, but the device application is offline) and then unconfigures the devices. The offline device is highlighted red if it is located in the SmartServer tree; offline devices in the OpenLNS tree are not marked red.
5. To recommission an unconfigured device and place it back online, select one or more devices to recommission, right-click a selected device, point to **Manage**, and then click **Commission** on the shortcut menu. You then select the devices again, right-click a selected device, point to **Manage**, and then click **Set Online** on the shortcut menu.

Alternatively, you can select the **Smart Network Management** check boxes for the **Commission Status** and **Application Status** properties in the **Setup - LON Device Driver** Web page, and then click **Submit**. You can also change the **Commission Status** property to **Commissioned** and change the **Application Status** property to **Application Running (Online)**, and then click **Submit**.

Note: Changing the domain ID of the SmartServer causes all the devices on the network to be recommissioned automatically and reconfigured to the new domain ID.

Testing Devices

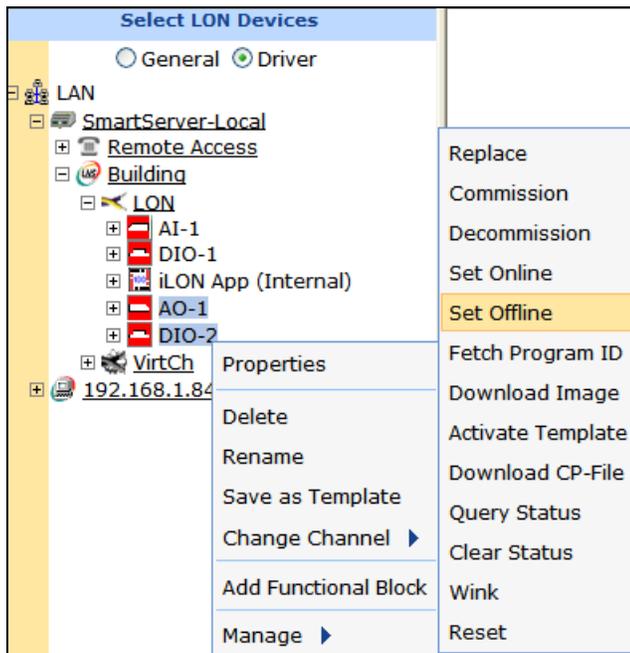
You can use the SmartServer to place devices offline, query the status of a device, and to wink a device. You can place a device offline to test the behavior of other devices on the network. You can query the status of a device to ensure that it is operating and it is configured correctly. Querying a device opens a dialog that lists network traffic statistics that you can use to evaluate the performance of the device. Winking a device enables you to identify the device on the network and verify that it is communicating properly.

Setting Devices Offline

You can set a device to the offline state in order to stop running its application. This may be useful for testing the behavior of other devices on the network. An offline device still receives data point updates; however, it does not process them. Instead, the offline device transmits the default values for its data points. In addition, an offline device can still process commission, decommission, set online, query status, clear status, wink and reset commands. Offline devices are highlighted red in the SmartServer tree.

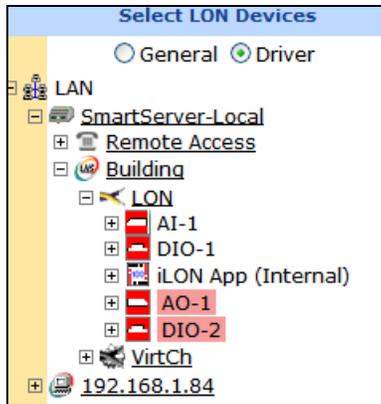
To set a device offline, follow these steps:

1. Click **Driver** mode.
2. Select one or more devices to place offline. To select one device, click that device. To select multiple devices, click one device and then either hold down CTRL and click all other devices to be installed or hold down SHIFT and select another device to place the entire range of devices offline. The **Setup - LON Device Driver** Web page opens.
3. Right-click a selected device, point to **Manage**, and click **Set Offline**.

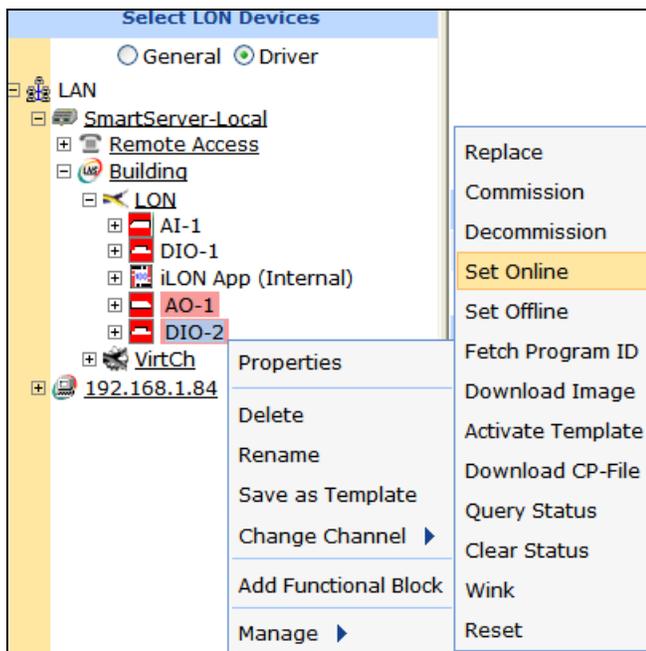


Alternatively, you can change the **Application Status** property to **Application Stopped (Offline)** in the **Setup - LON Device Driver** Web page, which appears when you select devices in step 2.

4. The SmartServer places the device in the soft offline state (the device has an application loaded on it and the device is configured, but the device application is offline). The offline device is highlighted red if it is located in the SmartServer tree; offline devices in the OpenLNS tree are not marked red.



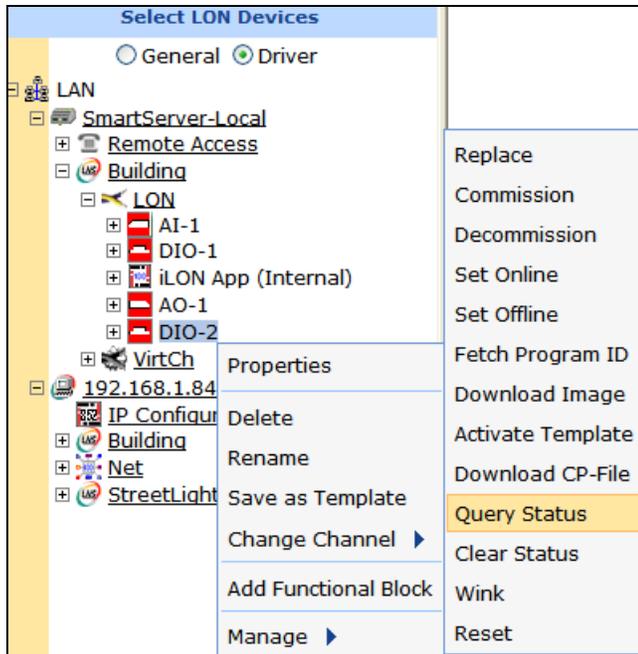
- To place a device back online, select one or more devices to set online, right-click a selected device, point to **Manage**, and then click **Set Online**. Alternatively, you can select the **Smart Network Management** check box for the **Application Status** property in the **Setup - LON Device Driver** Web page and then click **Submit**, or you can change the **Application Status** property to **Application Running (Online)** and then click **Submit**.



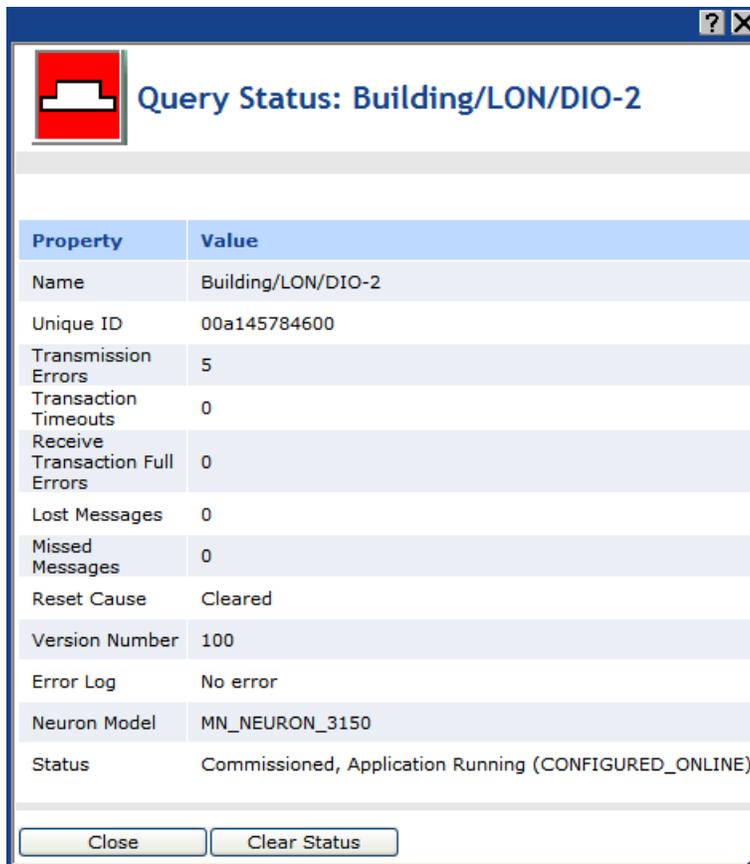
Querying Devices

You can query a device to evaluate its performance and diagnose any problems. You can query devices under normal and peak conditions to see the affect of network load. To query a device, follow these steps:

- Right-click the device, point to **Manage**, and then click **Query Status**.



2. The **Query Status** dialog opens.



3. This dialog lists the following network statistics. Non-zero values indicate that the device was unable to receive and/or respond to a message. Small values are expected; rapidly increasing values may indicate a problem. If the device is consistently reporting failures and new errors are being logged, the device may have a configuration problem or the network may be overloaded.

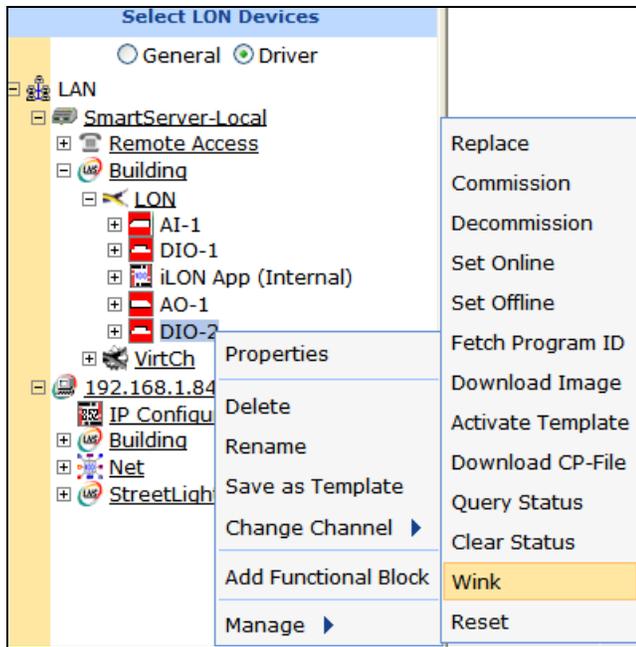
<i>Name</i>	The name of the device in the following format: <network>/<channel>/<device>
<i>Unique ID</i>	Displays the Neuron ID of the device as a 12-digit hex string. The Neuron ID is a unique 48-bit number burnt into the device's Neuron chip.
<i>Transmission Errors</i>	Transmission errors typically indicate cyclical redundancy check (CRC) errors. CRC errors are commonly caused by electromagnetic interference (EMI) on the channel.
<i>Transaction Timeouts</i>	Transaction timeouts occur when an acknowledged message times out after the last retry without the receiving device sending a confirmation that the message was delivered.
<i>Receive Transaction Full Errors</i>	Transaction full errors occur when the device's transaction database, which is used to detect duplicate message packets, overflows. This may indicate excessive network traffic or transaction timers that are set too high.
<i>Lost Messages</i>	Lost messages occur when a device's application buffer overflows. This may indicate excessive network traffic or a busy device application. If the incoming message is too large for the application buffer, an error is logged but the lost message count is not incremented.
<i>Missed Messages</i>	Missed messages occur when a device's network buffer overflows or network buffers are not large enough to accept all packets on the channel, whether or not addressed to this device.
<i>Reset Cause</i>	Displays an error code that indicates the cause for the device's most recent reset.
<i>Version Number</i>	Specifies the firmware version used by the device hardware
<i>Error Log</i>	Indicates whether errors have been logged for the device.
<i>Neuron Model</i>	Displays the model number of the device's Neuron Chip or Smart Transceiver, if any
<i>Status</i>	Indicates the status of the device (configured or unconfigured) and the device application (online or offline).

4. Click **Close** to exit this dialog.
5. Optionally, you can clear the log in the **Query Status** dialog. To do this, click **Clear Status** in the **Query Status** dialog, or click **Close** to return to the SmartServer Web interface, right-click the device, point to **Manage**, and then click **Clear Status**.

Winking Devices

Winking a device enables you to identify the device on the network and verify that it is communicating properly. A device that supports the Wink command generates an application-dependent audio or visual feedback such as a beep or a flashing service LED when winked. To wink a device, follow these steps:

1. Select one or more devices to wink. To select one device, click that device. To select multiple devices, click one device and then either hold down CTRL and click all other devices to be winked or hold down SHIFT and select another device to wink the entire range of devices.
2. Right-click one of the selected devices, point to **Manage**, and then click **Wink**.



3. Click **Submit**.

Alarming

This chapter describes the Alarm Generator and Alarm Notifier applications on the SmartServer that you can use to monitor and control the alarming of devices. It describes how to use Alarm Generators to trigger alarms based on monitored conditions, and it describes how to use Alarm Notifiers to send e-mail notifications and data point updates when an alarm condition occurs. It explains how to use the **Alarm Notifier: Summary** Web page on the SmartServer to view, acknowledge, and clear active alarms and how to use the **Alarm Notifier: History** Web page to view a log of active and cleared alarms.

Alarming Overview

The SmartServer contains Alarm Generator and Alarm Notifier applications that you can use to monitor and control the alarming of devices. The SmartServer also has an **Alarm Notifier: Summary** Web page that you can use to view, acknowledge, and clear active alarms and an **Alarm Notifier: History** Web page that you can use to view a log of active and cleared alarms reported by the Alarm Notifiers. In addition, you can use an Alarm Monitor application to view alarm conditions on your computer without connecting to the SmartServer Web page.

- The **Alarm Generator** application can monitor up to 40 data points and trigger alarms by setting the status of an input data point when a specified alarm conditions occur. You can add more than 40 Alarm Generators if you activate the v40 interface, which features a dynamic device interface, on your SmartServer. The Alarm Generator can optionally update **SNVT_alarm** or **SNVT_alarm_2** output data points, which can be connected to an Alarm Notifier or to another LONWORKS alarming device.
- The **Alarm Notifier** application can monitor the status of selected data points, as well as conditions sent via the **SNVT_alarm** and **SNVT_alarm_2** output data points. When an alarm occurs, the Alarm Notifier can handle the alarm condition by updating one or more data points, sending an e-mail notification, and saving the alarm to a log file. A single Alarm Notifier can be configured to monitor multiple data points.
- The **Alarm Notifier: Summary** Web page lists all active alarms. It includes an option to acknowledge an alarm so that the Alarm Notifier stops reporting the alarm condition, and an option for clearing the alarm once the alarm condition has been fixed.
- The **Alarm Notifier: History** Web page lists all the active and cleared alarms reported by selected Alarm Notifiers for a given period of time. It lets you filter alarms based on the functional block, data point, or time of alarm.

Using the Alarm Generator Application

The Alarm Generator application triggers alarms based on data point values. When you create an Alarm Generator, you specify an input point and a compare point. The compare point can be another data point or a constant value. When the input point or compare point are updated, the Alarm Generator compares the values of both using a binary or analog function, whichever you select.

With the binary function, the Alarm Generator evaluates whether the input point is less than, less than or equal, greater than, greater than or equal, equal, or not equal to the compare point based on the logical function you select. If the result of the comparison is true, the Alarm Generator triggers an alarm and updates the status of the input point to an alarm condition (**AL_ALM_CONDITION**). For example, if you select **Greater Than** and the value of the input point is greater than the compare point value, the Alarm Generator will trigger an alarm when either point is updated.

With the analog function, the Alarm Generator evaluates how far the input point is above or below the compare point. If the difference exceeds one of four offset limits that you define, the Alarm Generator triggers an alarm and updates the status of the input point to an alarm condition when either point is updated. After an alarm has been generated based on an offset limit, the value of the input point must return to the hysteresis level that you define for that offset limit before the alarm clears and another alarm can be generated based on the offset limit. This means that the Alarm Generator will not trigger additional alarms in between the time that the input point reaches an alarm condition and returns to a normal condition.

The binary and analog comparison functions both have a throttle that you can specify to prevent the Alarm Generator from triggering multiple alarms each time the input point reaches an alarm condition.

The Alarm Generator also has **SNVT_alarm** and **SNVT_alarm_2** output data points. The status of these output data points are updated to an alarm condition each time the Alarm Generator state changes

from passive to active or active to passive. You can connect these **SNVT_alarm** and **SNVT_alarm_2** output data points to an Alarm Notifier or to another LONWORKS alarming device.

You can create up to 40 Alarm Generators per SmartServer if you are using the default SmartServer v12 static interface. You can add more than 40 Alarm Generators if you activate the v40 dynamic interface, which features a dynamic device interface, on your SmartServer. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

To create an alarm generator, do the following:

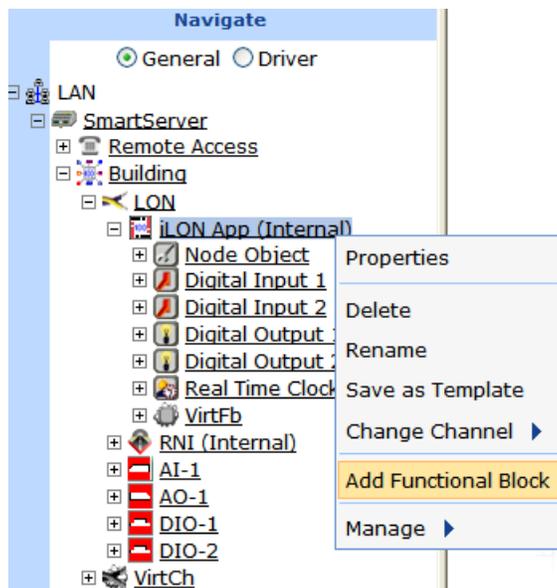
1. Open an Alarm Generator application.
2. Select an input data point.
3. Select or set a compare data point.
4. Select and configure a comparison function (binary or analog).
5. Optionally select **SNVT_alarm** and/or **SNVT_alarm_2** output data points.

Opening an Alarm Generator Application

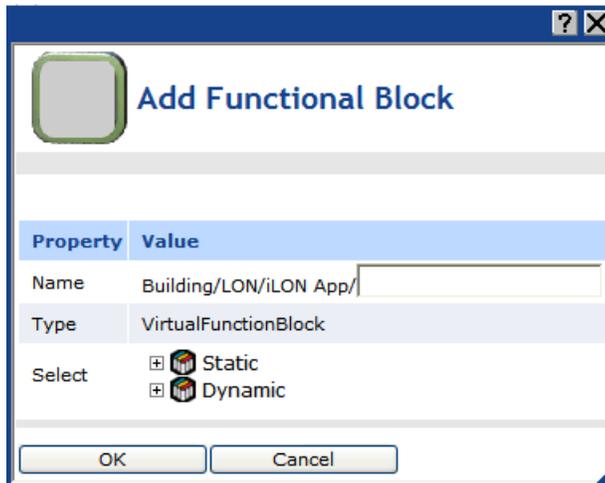
To open an Alarm Generator application, you must first create an Alarm Generator functional block. After you create the Alarm Generator functional block, the functional block appears on the SmartServer tree below the **i.LON App (Internal)** device, and you can click the functional block to open the Alarm Generator application.

To create an Alarm Generator functional block and open the application, follow these steps:

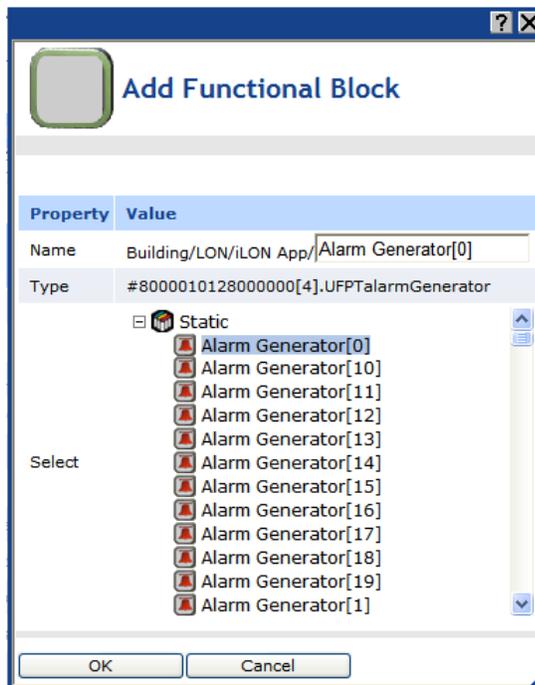
1. Click **General** above the navigation pane in the SmartServer Web interface.
2. Expand the network entry in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



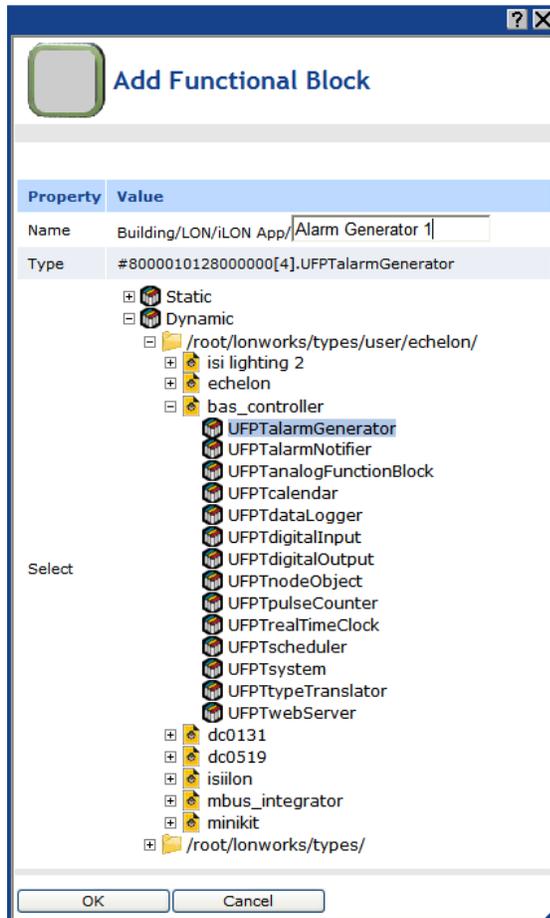
4. The **Add Functional Block** dialog opens.



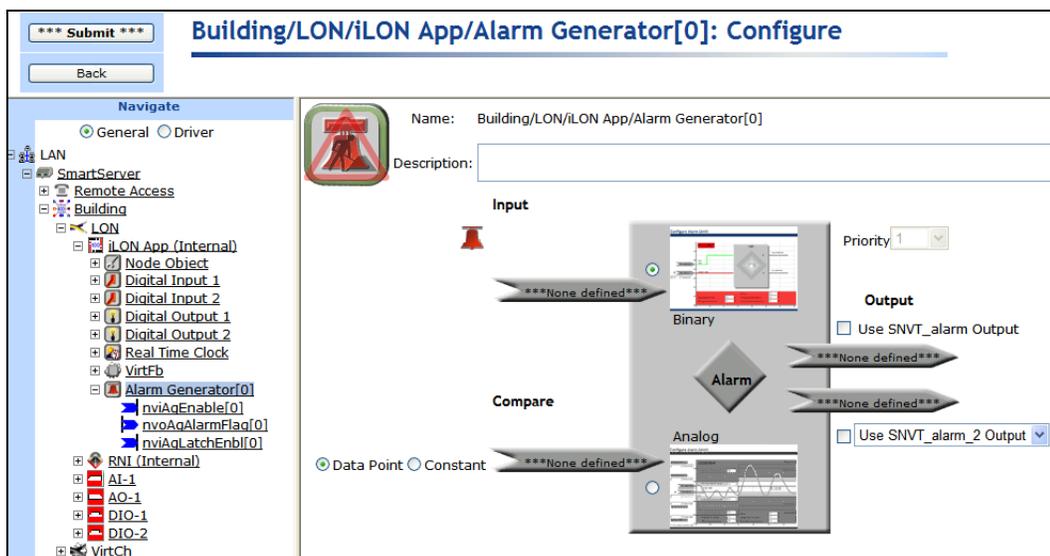
5. Select the Alarm Generator functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40interface.
 - If the SmartServer is using the default static v12 interface, expand the **Static** entry, select the **Alarm Generator** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Alarm Generator functional block from either the **Static** or the **Dynamic** folder. To select the Alarm Generator functional block from the **Dynamic** folder, expand the **Dynamic** entry, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile template (UFPT) for the alarm generator, enter a name for the functional block such as “Alarm Generator 1”, and then click **OK**.



6. A functional block representing the Alarm Generator application and all of its static data points are added to the bottom of the **i.LON App (Internal)** device tree, and the **Alarm Generator: Configure** Web opens in the application frame to the right. The construction symbol overlaid onto the Alarm Generator application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



7. Click **Submit**.

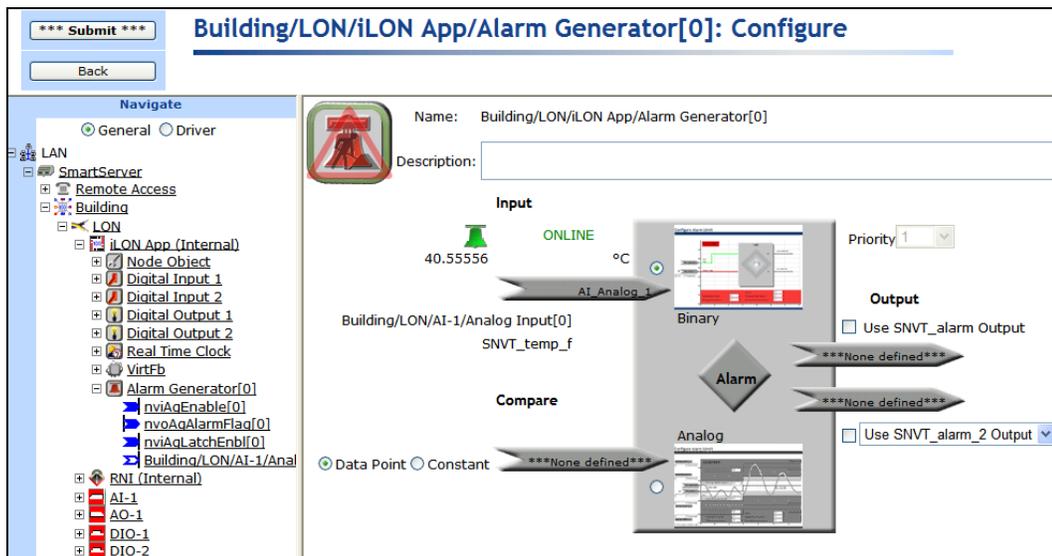
To open the Alarm Generator application from an existing Alarm Generator functional block, follow these steps:

1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Alarm Generator application.
2. Click the Alarm Generator functional block representing the Alarm Generator to be opened. The **Alarm Generator: Configure** Web page opens in the application frame to the right.

Selecting a Data Point

You can specify the input point to be monitored by the Alarm Generator application. To select an input point, follow these steps:

1. Click the data point icon () below **Input**.
2. Select the data point to be monitored by the Alarm Generator from the SmartServer tree. To monitor a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).
3. The current value, state, and unit string of the selected input point are displayed above the input point icon. The **Input** icon displays the programmatic name of the data point. The network variable type and location of the selected input point are listed below the **Input** icon. In addition, a reference to the selected input point () is added to the bottom of the Alarm Generator functional block tree, and a reference to the Alarm Generator functional block is added directly below the selected data point ().



The screenshot shows the configuration interface for the Alarm Generator. On the left, a navigation tree lists various components under 'Building/LON/iLON App', with 'Alarm Generator[0]' selected. The main configuration area is titled 'Building/LON/iLON App/Alarm Generator[0]: Configure'. It includes a 'Name' field with the value 'Building/LON/iLON App/Alarm Generator[0]' and a 'Description' field. Below this, there are three main sections: 'Input', 'Compare', and 'Output'. The 'Input' section shows a value of 40.55556, a state of 'ONLINE', and a unit of '°C'. The 'Compare' section shows a value of '***None defined***'. The 'Output' section shows two options: 'Use SNVT_alarm Output' and 'Use SNVT_alarm_2 Output'. The 'Alarm' icon is visible in the center of the configuration area.

4. Click **Submit**.

Selecting a Compare Point

You can specify the compare point that the Alarm Generator will evaluate against the selected input point. You can select a data point to be used as the compare point or you can enter a constant value.

Selecting a Data Point

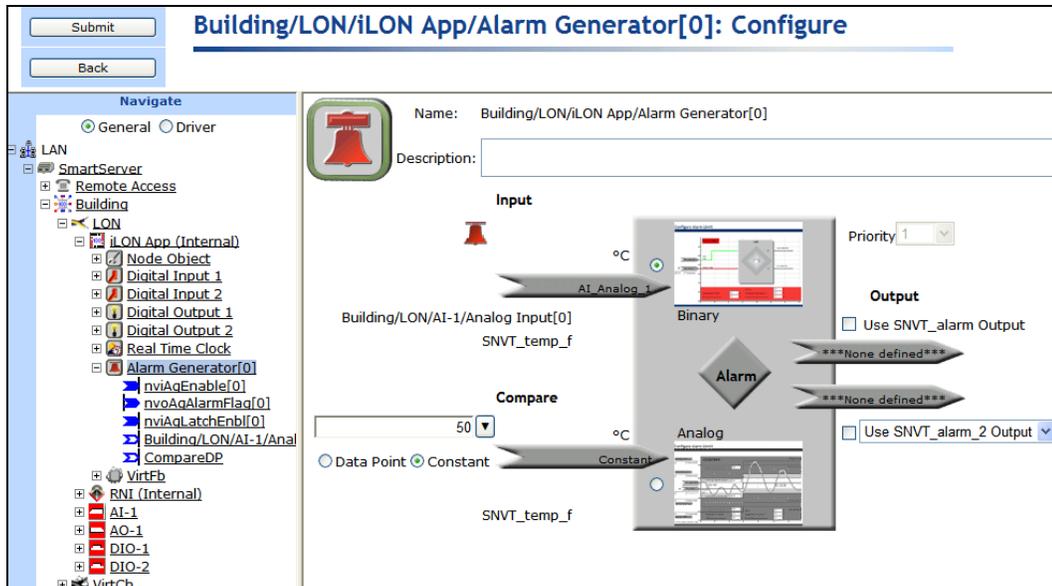
To select a data point to be used as the compare point, follow these steps:

1. Click the data point icon () below **Compare**.
2. Select the data point to be used by the Alarm Generator as the compare point from the SmartServer tree. The compare data point must be of the same scalar or structured network variable type as the input point. For example, if the input point is a **SNVT_temp** type, the compare data point must also be a **SNVT_temp** type. To use a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4, *Using the Web Interface*, for more information on adding data points to a SmartServer application).
3. The **Compare** icon displays the programmatic name of the data point, and the network variable type and location of the selected input point are listed below the Compare Point icon.
4. Click **Submit**. A reference to the selected compare point is added to the Alarm Generator functional block tree.

Entering a Constant Value

To enter a constant value to be used as the compare point, follow these steps:

1. Click **Constant**. A box appears above the **Data Point** and **Constant** buttons, and the format and network variable type of the input point appear above and below the compare point icon, respectively.
2. Enter a value in the box to be used as the compare point. If the input point has presets defined for it, you can alternatively click the arrow to the right of the box and select a preset. The Alarm Generator will use the value corresponding to the preset as the compare point. See Chapter 5, *Using the SmartServer as a Network Management Tool*, for more information on using presets.



3. Click **Submit**. A reference to the “**CompareDP**” data point is added to the bottom of the Alarm Generator functional block tree. This data point is a constant that has the same format, unit string, and presets as the input point. Its default value is enabled and corresponds with the value entered in step 2.

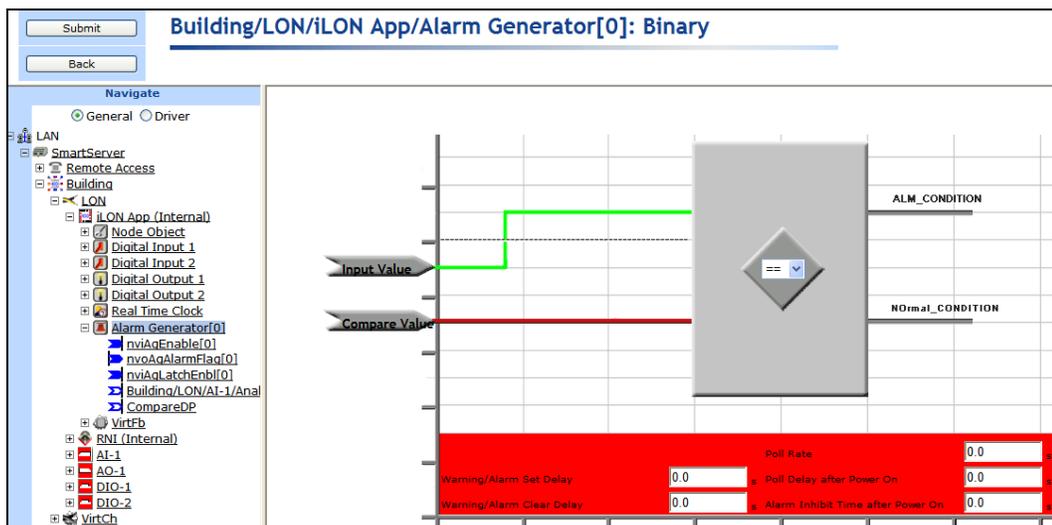
Selecting and Configuring a Comparison Function

You can select whether the Alarm Generator uses a binary or analog function to evaluate the value of the input point against that of the compare point. After you select the comparison function to be used, you configure the function. For the binary function, this means selecting the logical function to be used to compare the points; for the analog function, this means defining offsets and hysteresis levels.

Using a Binary Comparison Function

To use a binary function for comparing the input point to the compare point, follow these steps:

1. In the **Alarm** box, click **Binary** and then click the **Binary** icon. The **Alarm Generator: Binary** Web page opens.



- Select one of the following binary comparison functions: equals ($==$), is not equal to (\neq), greater than ($>$), greater than or equal to (\geq), less than ($<$), and less than or equal to (\leq). When the selected comparison function is evaluated to be true, the Alarm Generator triggers an alarm and updates the status of the input point to **AL_ALM_CONDITION**. For example, if you select the equals comparison function ($==$), the Alarm Generator triggers an alarm when it determines that the value of the input point is equal to the value of the compare point.

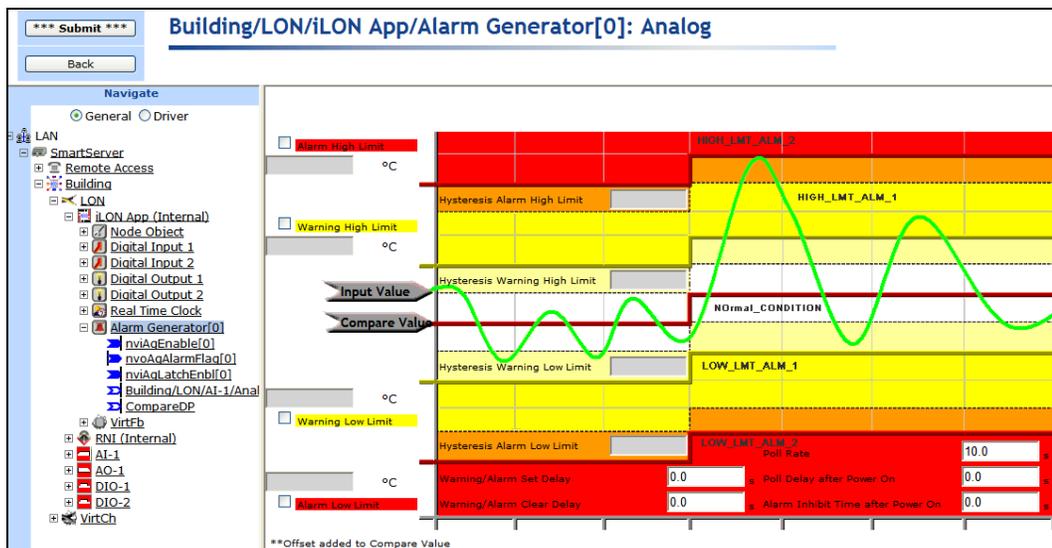
- Configure the following alarm properties:

<i>Warning/Alarm Set Delay</i>	Enter the period of time (in seconds) that the alarm condition must exist to generate an alarm.
<i>Warning/Alarm Clear Delay</i>	Enter the period of time (in seconds) that the normal condition must exist to clear an alarm.
<i>Poll Rate</i>	Enter how frequently (in seconds) the Alarm Generator polls the SmartServer's internal data server for the values of the selected input point and the compare point (if a data point). You must enter a non-zero value; otherwise polling is disabled.
<i>Poll Delay After Power On</i>	Enter the period of time (in seconds) that the Alarm Generator waits after it has been reset before polling the input point and the compare point (if a data point).
<i>Alarm Inhibit Time After Power On</i>	Enter the period of time (in seconds) that the Alarm Generator waits after it has been reset before triggering alarms.

Using an Analog Comparison Function

To use an analog function for comparing the input point to the compare point, follow these steps:

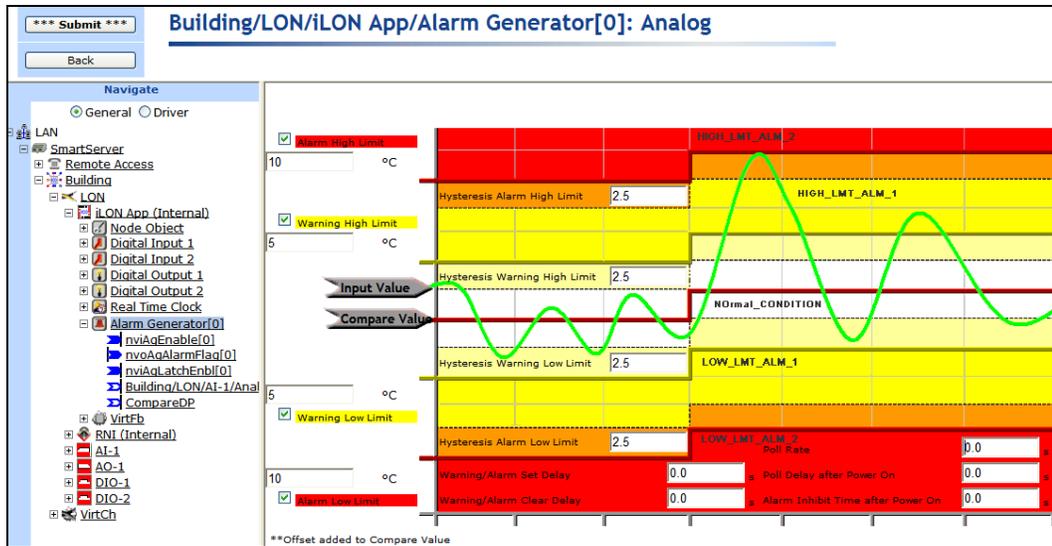
- In the **Alarm** box, click **Analog**, and then click the **Analog** icon. The **Configure: Analog** Web page opens.



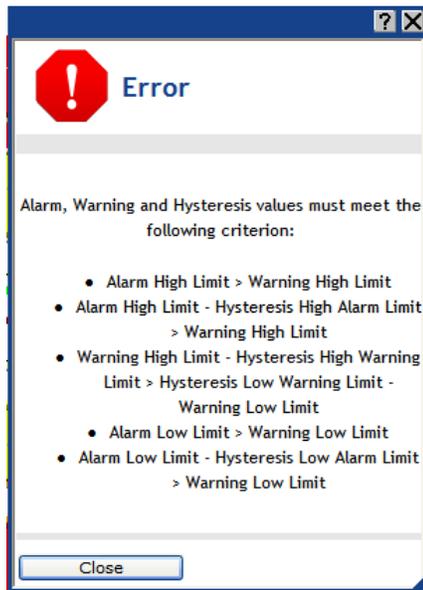
- Enable and set offset limits used to trigger the following alarms:

<i>Alarm High Limit</i>	<p>When the Input Value exceeds the Compare Value by this amount or more, the Alarm Generator triggers a HIGH_LMT_ALM_2 alarm condition. This value minus the Hysteresis Alarm High Limit must be greater than the Warning High Limit.</p> <p>(Alarm High Limit - Hysteresis Alarm High Limit > Warning High Limit)</p>
<i>Warning High Limit</i>	<p>When the Input Value exceeds the Compare Value by this amount or more, the Alarm Generator triggers a HIGH_LMT_ALM_1 condition. This value must be less than the Alarm High Limit minus the Hysteresis Alarm High Limit, and this value minus the Hysteresis Warning High Limit must be greater than the Hysteresis Warning Low Limit minus the Alarm Low Limit.</p> <p>((Warning High Limit < Alarm High Limit - Hysteresis Alarm High Limit) & (Warning High Limit - Hysteresis High Warning Limit > Hysteresis Warning Low Limit - Warning Low Limit))</p>
<i>Warning Low Limit</i>	<p>When the Input Value is below the Compare Value by this amount or more, the Alarm Generator triggers a LOW_LMT_ALM_1 alarm condition.</p> <p>The Hysteresis Alarm Low Limit minus this value must be less than Warning High Limit minus the Hysteresis Alarm High Limit, and this value must be less than the Alarm Low Limit minus the Hysteresis Alarm Low Limit.</p> <p>((Hysteresis Warning Low Limit - Warning Low Limit < Warning High Limit - Hysteresis Warning High Limit) & (Warning Low Limit < Alarm Low Limit - Hysteresis Warning Alarm Limit)).</p>
<i>Alarm Low Limit</i>	<p>When the Input Value is below the Compare Value by this amount or more, the Alarm Generator triggers, a LOW_LMT_ALM_2 condition.</p> <p>This value must be greater than the Warning Low Limit plus the Hysteresis Alarm Low Limit.</p> <p>(Alarm Low Limit - Hysteresis Low Alarm Limit > Warning Low Limit)</p>

3. Set hysteresis levels to be associated with the offset limits defined in step 2. When a hysteresis level is set for an offset limit, the input value must return to the hysteresis level before the alarm clears and another alarm can be generated based on that limit. This means that the Alarm Generator will not trigger additional alarms in between the time that the input point reaches an alarm condition and returns to a normal condition.



If the alarm, warning, and hysteresis values you enter do not meet the listed requirements, the incorrect fields are highlighted red and the following error dialog opens:



Click **Close** and then correct the highlighted fields so they meet the listed criteria.

The following table demonstrates the alarms triggered and the state of an input point as its value goes above the high warning and alarm limits and then returns to the hysteresis level for the high warning limit.

Data Point Value	Alarm Condition	Alarm Triggered ?	Alarm State
Value of input point is normal.	AL_NO_CONDITION	No	Normal condition.
Value of input point goes above the Warning High Limit.	AL_HIGH_LMT_ALM1	Yes	Updated to the high warning condition.

Value of input point goes above the Alarm High Limit.	AL_HIGH_LMT_ALM2	Yes	Updated to the more severe high alarm condition.
Value of input point changes, but remains above the Alarm High Limit.	AL_HIGH_LMT_ALM2	No	Remains at the high alarm condition, as the data point has not reached the specified hysteresis level for that condition.
Value of input point goes below the hysteresis level defined for the Alarm High Limit.	AL_HIGH_LMT_ALM1	No	Returned to the high warning condition.
Value of input point goes below the hysteresis level defined for the Warning High Limit.	AL_NO_CONDITION	No	Returned to normal condition

4. Configure the following alarm properties:

<i>Warning/Alarm Set Delay</i>	Enter the period of time (in seconds) that the alarm condition must exist to generate an alarm.
<i>Warning/Alarm Clear Delay</i>	Enter the period of time (in seconds) that the normal condition must exist to clear an alarm.
<i>Poll Rate</i>	Enter how frequently (in seconds) the Alarm Generator polls the SmartServer's internal data server for the values of the selected input point and the compare point (if a data point). You must enter a non-zero value; otherwise polling is disabled.
<i>Poll Delay After Power On</i>	Enter the period of time (in seconds) that the Alarm Generator waits after it has been reset before polling the input point and the compare point (if a data point).
<i>Alarm Inhibit Time After Power On</i>	Enter the period of time (in seconds) that the Alarm Generator waits after it has been reset before triggering alarms.

5. Click **Submit**.

Selecting SNVT_alarm Output Data Points

After you have selected an input point, a compare point, and a comparison function, you can select **SNVT_alarm** and/or **SNVT_alarm_2** output data points to be updated to an alarm condition when an alarm is generated. This means that you can check the status of an input point, or one of the **SNVT_alarm** or **SNVT_alarm_2** output data points to determine whether an alarm has been generated. You can also create an Alarm Notifier to send an alarm notification each time the input point or either of the **SNVT_alarm** and **SNVT_alarm_2** output data points is updated to an alarm condition as described in the next section, *Using the Alarm Notifier*.

To select the **SNVT_alarm** and/or **SNVT_alarm_2** output data points to be updated to an alarm condition, follow these steps:

1. Select the **Use SNVT_alarm Output** and/or the **Use SNVT_alarm_2 Output** check box.
2. Click the data point icon () directly below the **Use SNVT_alarm Output** check box to select a **SNVT_alarm** data point. Click the data point icon directly above the **Use SNVT_alarm_2 Output** check box to select a **SNVT_alarm_2** data point, and then select whether you are using a **SNVT_alarm_2** or a **UNVT_alarm_2** data point from the list.

3. Select a **SNVT_alarm** or **SNVT_alarm_2** data point from the SmartServer tree (based on whichever icon has its text highlighted blue) to be updated to an alarm condition when an alarm occurs. If you want to use a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4, *Using the Web Interface*, for more information on adding data points to a SmartServer application).

NOTE: If you add an Alarm Generator functional block with OpenLNS CT, a **SNVT_alarm** output data point is automatically created for use with the Alarm Generator. See the *OpenLNS Commissioning Tool User's Guide* for more information on adding functional blocks.

4. You can set the priority level of the alarm in the **Priority** box. Select a value from 0 to 11, with 0 being the highest priority and 11 being the lowest. This value will be sent in the priority field of the **SNVT_alarm** and/or **SNVT_alarm_2** output data point when an alarm is generated.
5. Click **Submit**.
6. References to the selected **SNVT_alarm** and **SNVT_alarm_2** output data points are added to the bottom of the Alarm Generator functional block tree.

The screenshot shows the configuration page for the 'Building/LON/iLON App/Alarm Generator[0]' block. The interface includes a 'Submit' and 'Back' button at the top left. A 'Navigate' sidebar on the left shows a tree structure with 'Building/LON/iLON App/Alarm Generator[0]' highlighted. The main configuration area features a red bell icon, a 'Name' field, and a 'Description' field. The 'Input' section shows a red bell icon with the value '60' and a temperature unit '°C', connected to 'AI_Analog_1'. The 'Compare' section has a dropdown set to 'TOO HOT' and a 'Constant' radio button selected, with 'SNVT_temp_f' as the data point. The 'Output' section has two checkboxes: 'Use SNVT_alarm Output' (checked) and 'Use SNVT_alarm_2 Output' (checked). A central 'Alarm' block icon is also visible.

Using the Alarm Notifier Application

The Alarm Notifier communicates alarms generated by application devices, including the SmartServer. When a device transmits a **SNVT_alarm** or **SNVT_alarm_2** output data point on the network or a data point goes offline, the Alarm Notifier can send e-mail messages, update data points, and log alarm conditions.

The Alarm Notifier reads the status of selected data points each time they are updated to determine if their statuses have been changed to an alarm condition. If a data point is in an alarm condition, the Alarm Notifier can send an e-mail message describing the alarm. If an e-mail profile is specified for the Alarm Notifier, the e-mail message is sent to the addresses specified for that profile each time an alarm notification occurs. This is useful if different groups need to receive notifications for specific alarm conditions that may occur on your network. When a data point is in an alarm condition, the Alarm Notifier can also update selected data points to specified values.

When the Alarm Notification sends an alarm notification, it creates and updates an Alarm Summary log file that records all active alarms. By default, the file is located in the **//AlarmLog** folder on the SmartServer flash disk and is named `sumlog0`. In addition, the Alarm Notifier creates an Alarm History log file that records all alarm notifications. By default, this file is located in the **//AlarmLog** folder on the SmartServer flash disk and is named `histlog<x>`, where *x* is the index number assigned to the file when it was created. You can have the SmartServer automatically transfer the alarm log files (binary or CSV format) to a remote server and extract the selected data to a .CSV or XML file.

Although the SmartServer does not limit how much alarm data can be logged, you must maintain at least 1,024 KB of free space on the SmartServer flash disk. To view the amount of free disk space on the SmartServer right-click the SmartServer point to **Setup**, and then click **System Info** on the shortcut menu. The **Setup – System Info** Web page opens. In the **General Statistics** section, check the **Free disk space / Total disk space** property.

You can create up to 40 Alarm Notifiers per SmartServer if you are using the default static v12 interface. You can add more than 40 Alarm Notifiers if you activate the dynamic v40 interface, which features a dynamic external interface, on your SmartServer. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 XIF on the SmartServer.

To create an Alarm Generator, follow these steps:

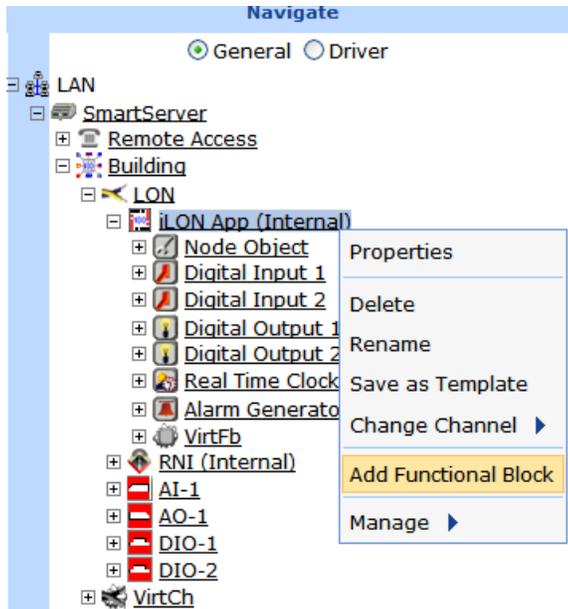
1. Open an Alarm Notifier application.
2. Select and configure input points.
3. Configure alarm conditions.
4. Configure e-mail and data point destinations.
5. Configure the alarm summary and history log files stored on the SmartServer.

Opening an Alarm Notifier Application

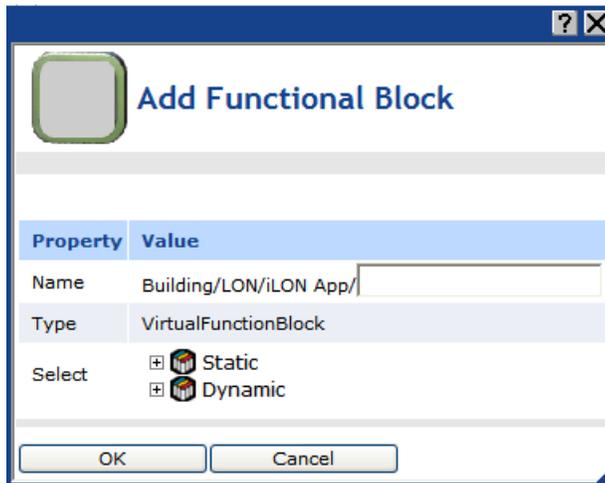
To open an Alarm Notifier application, you must first create an Alarm Notifier functional block. After you create the Alarm Notifier functional block, the functional block appears on the SmartServer tree below the **i.LON App (Internal)** device, and you can click the functional block to open the Alarm Notifier application.

To create an Alarm Notifier functional block and open the application, follow these steps:

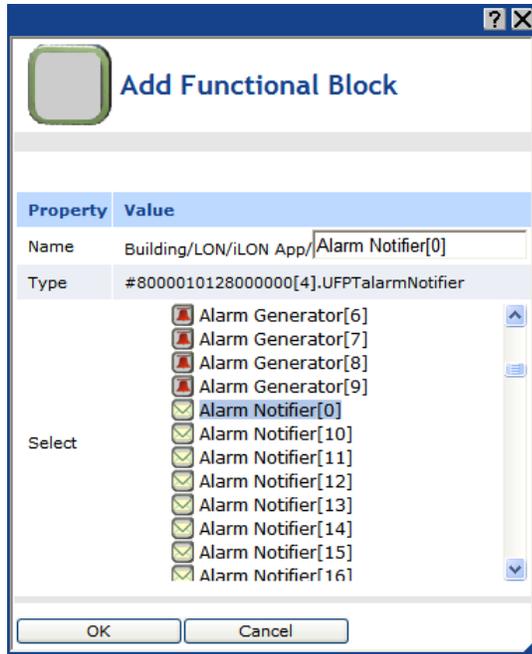
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



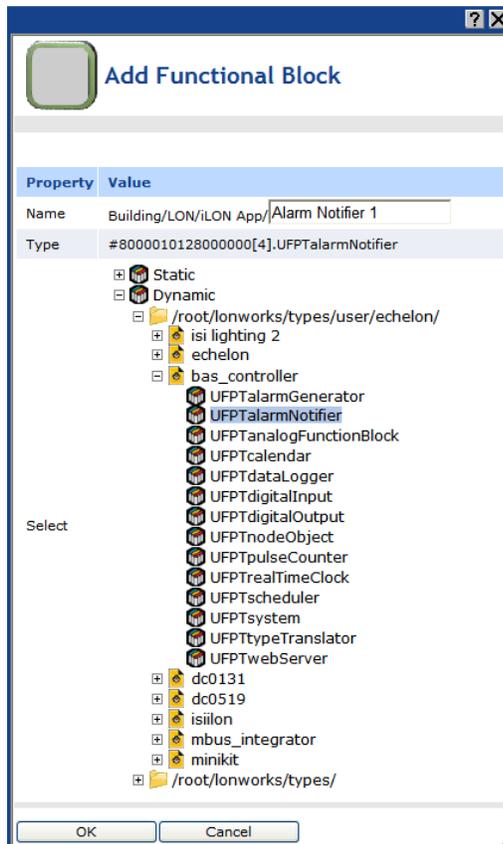
4. The **Add Functional Block** dialog opens.



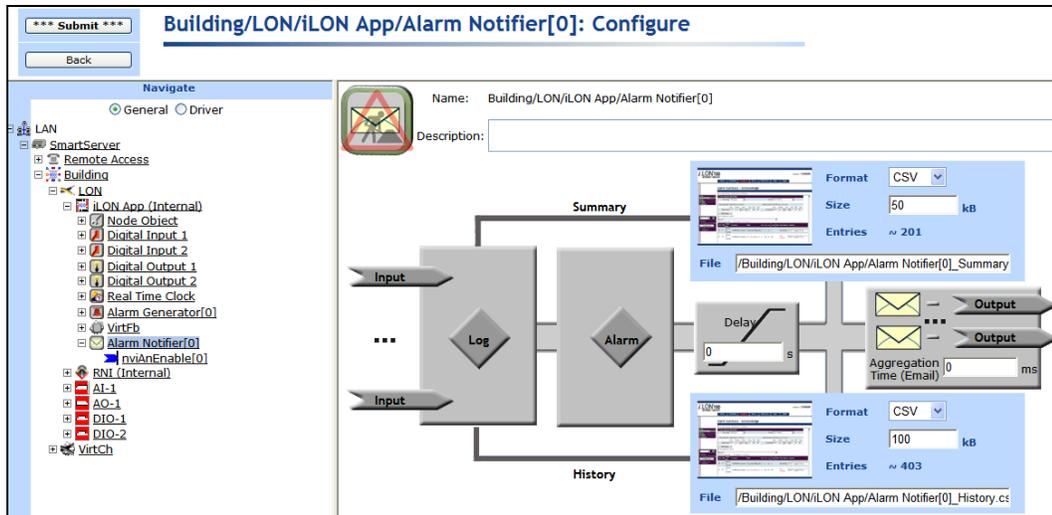
5. Select the Alarm Notifier functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface file or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Alarm Notifier** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Alarm Notifier functional block from either the **Static** or the **Dynamic** folder. To select the Alarm Notifier functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the alarm Notifier, enter a name for the functional block such as “Alarm Notifier 1”, and then click **OK**.



- A functional block representing the Alarm Notifier application and all of its static data points are added to the bottom of the **i.LON App (Internal)** device tree, and the **Alarm Notifier: Configure** Web page opens in the application frame to the right. The construction symbol overlaid onto the Alarm Notifier application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



- Click **Submit**.

To open the Alarm Notifier application from an existing Alarm Notifier functional block, follow these steps:

- Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Alarm Notifier application.
- Click the Alarm Notifier functional block representing the Alarm Notifier to be opened. The **Alarm Notifier: Configure** Web page opens in the application frame to the right.

Selecting and Configuring Input Points

You can select and configure the input points to be monitored by the Alarm Notifier application. To select an input point, follow these steps:

- Click one of the **Input** icons (), or click anywhere in the **Log** box (). The **Alarm Notifier: Data Points** Web page opens.
- Select the data points to be monitored by the Alarm Notifier from the SmartServer tree. The Alarm Notifier will check the status of the selected input points when they are updated, and send an alarm notification if their statuses have been changed to an alarm condition. References to the selected input points () are added to the bottom of the Alarm Notifier functional block tree, and references to the Alarm Notifier functional block are added directly below the selected data points ().

If you want to monitor a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).

Building/LON/iLON App/Alarm Notifier[0]: Data Points			
<input type="checkbox"/> Show Advanced			
	Data Point	Priority	Alarm Group
0	Building/LON/AI-1/Analog Input[0]/AI_Analog_1	0	0

3. Configure the following properties of the selected input points:

Data Point Displays the name of the data point being monitored using the following format: <network>/<channel>/<device>/<functional block>/<data point>. This is also the location of the data point in the SmartServer tree.

Priority Enter the priority of the alarm associated with this input point. This value may range from 0 to 255 (highest to lowest priority).

This property has no effect on the alarm function, but it can be included in e-mails to provide the recipient with more information, and it can be used as a sort field when viewing alarm logs in Excel.

Alarm Group Enter an alarm group number to be assigned to the input point. This value can be from 1 to 127. A value of 0 indicates the alarm has not been assigned to a group.

This property has no effect on the alarm function, but it can be included in e-mails to provide the recipient with more information, and it can be used as a sort field when viewing alarm logs in Excel.

4. Select the **Show Advanced** check box to configure the following advanced properties:

Building/LON/iLON App/Alarm Notifier[0]: Data Points									
<input checked="" type="checkbox"/> Show Advanced									
	Data Point	Priority	Alarm Group	Disabled	Clear Required	Acknowledgement Required	Store Only Most Recent	Alarm Summary	Alarm History
0	Building/LON/AI-1/Analog Input [0]/AI_Analog_1 Description:	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Disabled Disables alarm notifications for the input point. No alarm notifications will be sent for the input point. This check box is cleared by default.

Clear Required Requires the input point to be manually cleared to end the alarm condition. You can clear alarms in the **Alarm Notifier: Summary** Web page, as described later in this chapter. This may be useful for keeping an alarm active, even when the alarm condition has returned to normal. This option is cleared by default.

Acknowledgement Required Requires the input point to be manually acknowledged to end the alarm condition. You can acknowledge alarms in the **Alarm Notifier: Summary** Web page, as described later in this chapter. This may be useful for keeping an alarm active, even when the alarm condition has returned to normal. This option is selected by default.

Store Only Most Recent Stores in the Alarm Summary log only the most recent alarm received on the input point. All alarms are stored in the Alarm History log, regardless of whether this check box is selected. This option is selected by default.

Alarm Summary Writes the alarms received on the input point to the Alarm Summary log file and lists the alarms in the **Alarm Notifier: Summary** Web page. This option is selected by default.

Alarm History Writes the alarms received on the input point to the Alarm History log file and lists the alarms in the **Alarm Notifier: History** Web page. This option is selected by default.

5. Click **Submit**.

Configuring Alarm Conditions

You can select which alarm conditions received by the selected input points cause the Alarm Notifier to send an alarm notification. To configure the alarm conditions of the selected input points, follow these steps:

1. Click anywhere in the Alarm box () . The **Alarm Notifier: Alarm Conditions** Web page opens.

Building/LON/iLON App/Alarm Notifier[0]: Alarm Conditions

Alarm	Alarm	Description	Level
0 AL_HEADER	0 AL_OFFLINE	Offline	255
1 AL_FOOTER	1 AL_HIGH_LMT_ALM_1	High Warning	250
2 AL_DEBUG	2 AL_LOW_LMT_ALM_1	Low Warning	250
3 AL_INFO	3 AL_HIGH_LMT_ALM_2	High Alarm	240
4 AL_SYSTEM_INFO	4 AL_LOW_LMT_ALM_2	Low Alarm	240
5 AL_VALUE_INVALID	5 AL_ALM_CONDITION	Alarm	240
6 AL_CONSTANT			
7 AL_UNKNOWN			
8 AL_NUL			
9 AL_TOT_SVC_ALM_1			
10 AL_TOT_SVC_ALM_2			
11 AL_TOT_SVC_ALM_3			
12 AL_LOW_LMT_CLR_1			
13 AL_LOW_LMT_CLR_2			
14 AL_HIGH_LMT_CLR_1			
15 AL_HIGH_LMT_CLR_2			
16 AL_FIR_ALM			
17 AL_FIR_PRE_ALM			
18 AL_FIR_TRBL			
19 AL_FIR_SUPV			
20 AL_FIR_TEST_ALM			
21 AL_FIR_TEST_PRE_ALM			
22 AL_FIR_ENVCOMP_MAX			

No Alarm	Description	Level
0 AL_NO_CONDITION	Online	255

The left pane lists all of the alarm conditions that an input point can receive. The right pane contains separate lists for the alarm conditions defined as active (top) and passive (bottom). You can click a column heading to sort a list by that heading.

- An active alarm indicates a data point that is in an alarm condition. An active alarm is represented by a red alarm bell. By default, the following five alarms are registered as active alarm conditions: **AL OFFLINE**, **AL_HIGH_LMT_ALM_1**, **AL_LOW_LMT_ALM_1**, **AL_HIGH_LMT_ALM_2**, **AL_LOW_LMT_ALM_2**, and **AL_ALM_CONDITION**.
- A passive alarm indicates a data point that is in its normal condition or has returned to its normal condition after being in an alarm condition. A passive alarm is represented by a green alarm bell. By default, there is one alarm condition registered as a passive alarm condition: **AL_NO_CONDITION**.

The following table lists and describes the alarm conditions that you can set as active and passive. These alarm conditions are defined in the **SNVT_AL.H** header file in the **LonWorks\NeuronC\Include** folder on your computer.

Default Alarm Type	Alarm Condition	Description
Active	AL_OFFLINE	The device is offline
	AL_HIGH_LMT_ALM_1	Alarm high limit alarm 1
	AL_LOW_LMT_ALM_1	Alarm low limit alarm 1
	AL_HIGH_LMT_ALM_2	Alarm high limit alarm 2
	AL_LOW_LMT_ALM_2	Alarm low limit alarm 2
	AL_ALM_CONDITION	Unspecified alarm condition
Passive	AL_NO_CONDITION	No alarm condition present
None	AL_HEADER	Update sequence header
	AL_FOOTER	Update sequence footer
	AL_DEBUG	Debug information (not an alarm)
	AL_INFO	Information update (not an alarm)
	AL_SYSTEM_INFO	System information (not an alarm)
	AL_VALUE_INVALID	Valid alarm, but invalid data point value
	AL_CONSTANT	The value is a constant value (not an alarm)
	AL_NUL	Invalid data point value
	AL_TOT_SVC_ALM_1	Total/service interval alarm 1
	AL_TOT_SVC_ALM_2	Total/service interval alarm 2
	AL_TOT_SVC_ALM_3	Total/service interval alarm 3
	AL_LOW_LMT_CLR_1	Alarm low limit alarm clear 1
	AL_LOW_LMT_CLR_2	Alarm low limit alarm clear 2
	AL_HIGH_LMT_CLR_1	Alarm high limit alarm clear 1
	AL_HIGH_LMT_CLR_2	Alarm high limit alarm clear 2
	AL_FIR_ALM	Fire Alarm Condition
	AL_FIR_PRE_ALM	Pre-alarm condition
	AL_FIR_TRBL	Trouble (fault) condition with an object
	AL_FIR_SUPV	Supervisory condition with an object (for example, sprinkler pressure)
	AL_FIR_TEST_ALM	Alarm condition with an object in Test Mode
	AL_FIR_TEST_PRE_ALM	Pre-Alarm condition with an object in Test Mode
	AL_FIR_ENVCOMP_MAX	Maximum environmental compensation level reached
	AL_FIR_MONITOR_COND	Abnormal condition with an input object
	AL_FIR_MAINT_ALERT	Maintenance Alert
	AL_FATAL_ERROR	Fatal application error
	AL_ERROR	Other error condition
	AL_WARNING	Other warning condition

2. Move alarm conditions in and out of each list with the << and >> buttons. You can move one or more alarm conditions at a time. To move one alarm condition, click that alarm condition and then click the desired direction. To move multiple alarm conditions at one time, click one alarm

condition and then either hold down CTRL and click all the other alarm conditions to be moved or hold down SHIFT and select another alarm condition to move the entire range of alarm conditions.

- Optionally, you can click the **Description** property header to enter a description that will be stored in the Alarm Summary and Alarm History logs when the alarm condition occurs.
- Optionally, you can click the **Level** property header to set the priority to be assigned to the alarm condition. You can later configure the Alarm Notifier in the **Configure - Alarm Notifier - Destinations** Web page to respond to different alarm conditions based on the priority level they have been assigned.
- Click **Submit**.



- In the **Delay** box (), you can enter the minimum period of time (between 0 to 65,536 seconds) that an alarm condition must exist for the alarm to be considered to be active. Setting a delay can be useful. Using a temperature control system with backup heating and cooling systems for example, you could set a 5-minute delay so that the backup systems could attempt to resolve an alarm condition before the alarm is considered active and the Alarm Notifier sends an e-mail notification.
- Click **Submit**.

Configuring E-mail and Data Point Destinations

You can specify the e-mail recipients and customize the e-mail message for the e-mail notification sent when an alarm condition is received by one of the selected input points. You can also select the data points to be updated and set their values when an alarm condition is received.



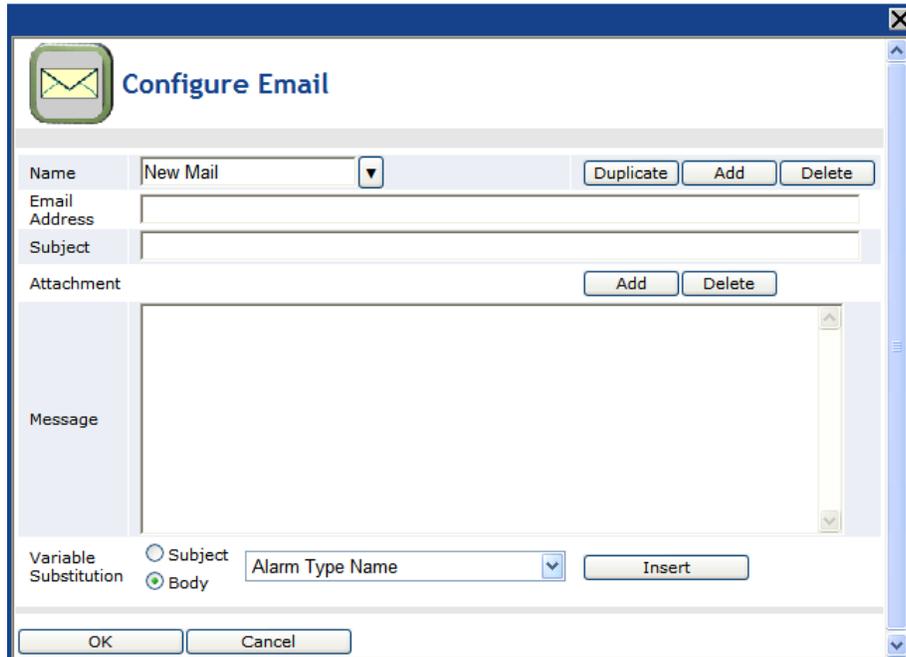
- In the **Aggregation Time (e-mail)** box (), you can enter the period of time (between 0 to 65,536 ms) that the Alarm Notifier waits between generating and sending an e-mail notification in order to merge multiple e-mail notifications to the same address into a single e-mail message. Setting an e-mail aggregation period can reduce e-mail traffic. For example, if you have a number of alarms in a system that trigger when the temperature reaches a certain point, setting an e-mail aggregation time of a minute (60,000 ms) causes a single e-mail message to be sent in the case of a system-wide temperature fluctuation, rather than multiple e-mail messages. The e-mail aggregation period resets each time a new alarm occurs.
- Click **Submit**.
- Click any of the e-mail or data point icons above the **Aggregation Time (e-mail)** box. The **Alarm Notifier: Destination** Web page opens.

Building/LON/iLON App/Alarm Notifier[0]: Destination				
<input type="checkbox"/> Show Advanced				
	Mail to	Output	Value	
0		-	-	-
		-	-	-

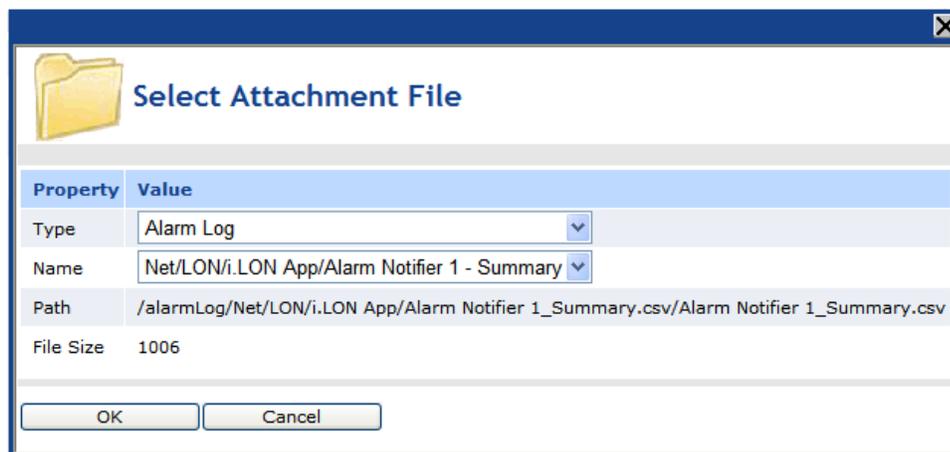
Each row in the table represents an e-mail message and data point update (collectively referred to as a *destination*) to be sent by the Alarm Notifier when an alarm notification event occurs. Each destination is divided into two rows: the top row, which is marked with a red alarm bell, is for active alarms; the bottom row, which is marked with a green alarm bell, is for passive alarms. This setup enables active and passive alarms to be addressed separately.

To add a destination, right-click anywhere in an existing destination and click **Add Destination** in the shortcut menu. To delete a destination, right-click anywhere in the destination to be deleted and click **Delete Destination** in the shortcut menu. To make a destination the default, right-click anywhere in the destination to be used as the default and click **Set to Default** in the shortcut menu

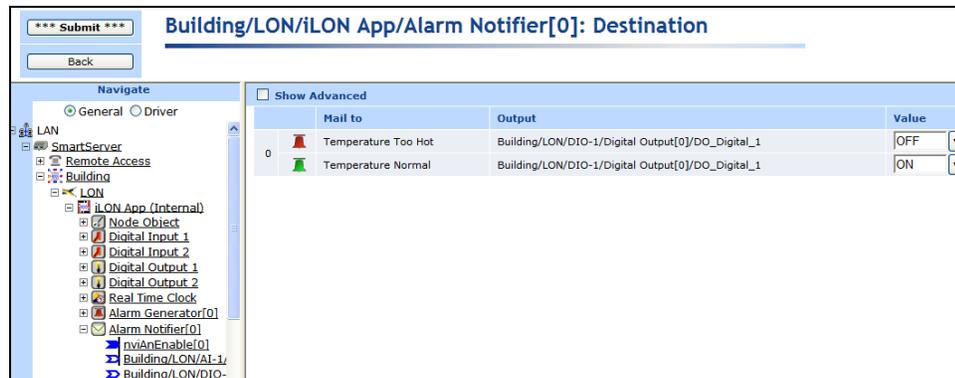
4. For each destination, configure the e-mail message to be sent when active and passive alarm conditions occur. To do this, follow these steps:
 - a. Click anywhere in the **Mail To** column. The **Configure E-mail** dialog opens.



- b. Enter the e-mail profile **Name**, **E-mail address**, **Subject**, and the **Message**. You can select a user profile from **Name** list to use the same e-mail for multiple alarm destinations. The **Name** list includes all the e-mail profiles that have previously been added to the Alarm Notifier. You can click **Duplicate** to copy an existing profile and then add or remove e-mail addresses from the **E-mail address** property. Click **Add** to create a new e-mail profile; click **Delete** to remove the selected e-mail profile.
 - c. Click **Add** to open the **Select Attachment** dialog in which you select an alarm log, data log, event log or other user-defined file to be inserted in the e-mail. After selecting a file, click **OK**.



- d. You can optionally select a **Variable Substitution** to be placed in the subject or body of the e-mail message and then click **Insert**. The variable substitution provides specific data pertaining to the alarm notification event such as the value of the data point that triggered the alarm. The on-line help includes a detailed list and descriptions of the variable substitutions you can use.
 - e. Click **OK** to return to the **Alarm Notifier: Destination** Web page.
5. For each destination, configure the data point update to be sent when active and passive alarm conditions occur. To do this, follow these steps:
 - a. Click the **Output** column and then click a data point in the SmartServer tree to be updated when the destination is used. To update a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4, *Using the Web Interface*, for more information on adding data points to a SmartServer application).
 - b. Click the **Value** column and then enter the value to which the selected data point is updated or select a preset (if one or more are defined for the data point). When an alarm condition is received, the data point is set to the active alarm value. When the alarm is cleared, the data point is set to the passive value. The selected data point will be updated when the e-mail for the destination has been sent (or as soon as the alarm occurs if no e-mail profile has been specified). To update a data point without having to wait for the e-mail notification to be sent, enter the e-mail message and data point update in separate destinations.



6. Select the **Show Advanced** check box to configure the following advanced properties:



Enable

Select a **SNVT_switch** data point from the SmartServer tree to be used to enable and disable the destination. After you select a data point, the destination is used when the data point is set to the ON value, and it is not used when the data point is set to the OFF value.

- Level Range** Set the active and passive alarm level ranges that will cause the destination to be used. You assigned each alarm condition an alarm level in the **Configure: Alarm Conditions** Web page. These properties determine for which alarm levels the destination is used.
- Set not ACK after** Determines the period of time (in minutes) the Alarm Notifier waits for an alarm to be cleared before using the destination.

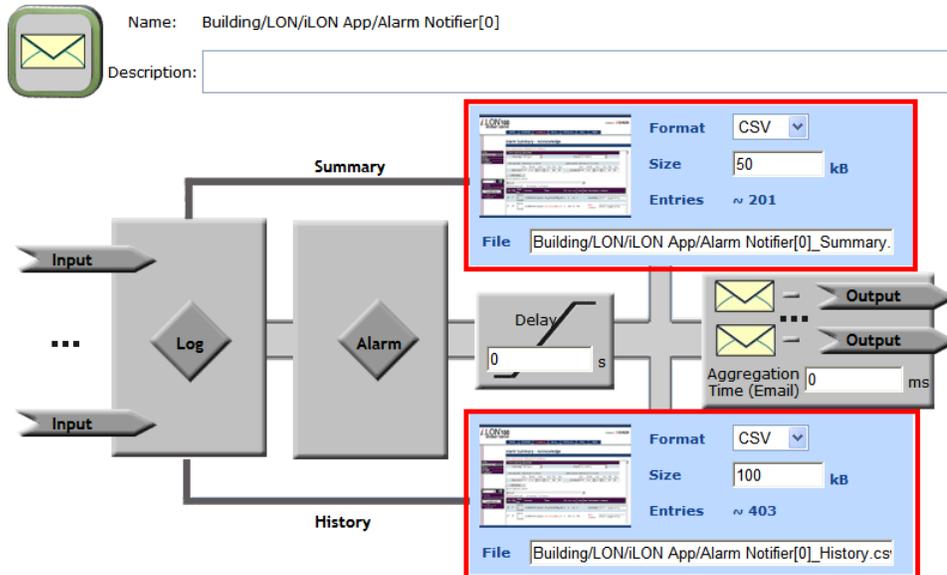
7. Click **Submit**.

Configuring the Alarm Summary and History Log Files

The SmartServer stores alarm summary and alarm history log files on its flash disk. The alarm summary log file lists all active alarms received by the Alarm Notifiers. The alarm history log file lists all the alarm notification events that have been generated by the Alarm Notifier.

You can use the alarm summary and alarm history icons on the top and bottom of the right side of the **Alarm Notifier: Configure** Web page to configure the alarm summary and alarm history log files. You can select in which format the log files are stored (CSV or binary); set the maximum file size, which sets the maximum number of entries that can be stored in the log file; and specify where the log files are stored on the flash disk.

Note: The SmartServer does not limit how much alarm data can be logged; however, you must maintain at least 1,024 KB of free space on the SmartServer server flash disk.



You can click the alarm summary and alarm summary icons to open the **Alarm Notifier: Summary** and **Alarm Notifier: History** Web pages, respectively. For more information on how to use these Web pages to acknowledge and clear the alarms reported by the Alarm Notifier, see the next section, *Automatically Transferring Alarm Logs*.

You can have the SmartServer automatically transfer alarm log files (binary or CSV format) to a remote server and extract the selected data to a .csv or XML file. For more information on how to do this, see *Automatically Transferring Data Logs* in Chapter 8.

Automatically Transferring Alarm Logs

You can have the SmartServer automatically transfer alarm log files (binary or CSV format) to a remote server and extract the selected data to a CSV or XML file. For more information on how to do this, see *Automatically Transferring Data Logs* in Chapter 8.

Viewing the Alarm Summary and Alarm History Logs

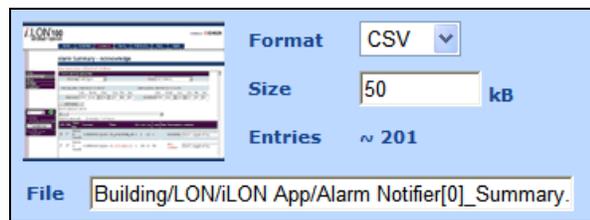
You can use the **Alarm Notifier: Summary** and **Alarm Notifier: History** Web pages on the SmartServer to monitor, view, acknowledge, and clear alarms. The **Alarm Notifier: Summary** Web page lets you view all active alarms, and acknowledge and clear alarms. The **Alarm Notifier: History** Web page lets you view a log of active and cleared alarms.

Using the Alarm Notifier: Summary Web Page

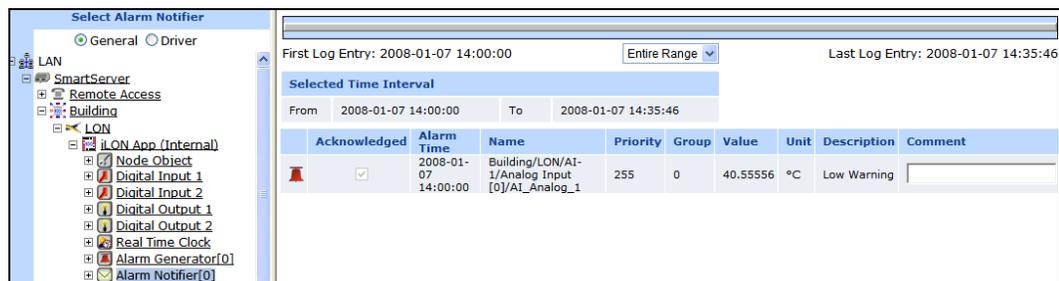
You can use the **Alarm Notifier: Summary** Web page to list all active alarms and to acknowledge and clear active alarms. For example, a building supervisor may acknowledge alarms once a maintenance company has been notified of a system problem, and the maintenance company will clear the alarm once they fix the problem. Once an active alarm is cleared, it is removed from the list.

To use the **Alarm Notifier: Summary** Web page, follow these steps:

1. Open the **Alarm Notifier: Summary** Web page. You can do this in two ways:
 - Click **View** and then click **Alarm Summary**. By default, the **Alarm Notifier: Summary** Web page will list the active alarms recorded by all the Alarm Notifiers on the SmartServer.
 - Click **General** and then click an Alarm Notifier functional block to open the **Alarm Notifier: Configure** Web page. Click the alarm summary icon on the top, right side of the Web page. By default, the **Alarm Notifier: Summary** Web page will list only the active alarms recorded by the selected Alarm Notifier.



2. The **Alarm Notifier: Summary** Web page opens.



3. You can change whether this Web page lists the events recorded by one or more Alarm Notifiers on the SmartServer.
 - To view the alarms recorded by one specific Alarm Notifier, click that Alarm Notifier in the SmartServer tree (if you opened the **Alarm Notifier: Summary** Web from the main SmartServer Web page, you initially need to click the Alarm Notifier to be viewed twice).

- To view the alarms recorded by multiple Alarm Notifiers on the SmartServer, hold down CTRL and click the Alarm Notifiers to be viewed in the SmartServer tree, or hold down SHIFT and click an Alarm Notifier to view all the Alarm Notifiers within the selected range.
4. By default, the data points are listed by the **Alarm Time** property in descending order. You can sort the alarms by clicking a property header. This Web page displays the following properties for each alarm:

<i>Alarm Time</i>	Displays the date and time of when the alarm occurred.
<i>Name</i>	Displays the name of the data point that triggered the alarm using the following format: <code><network>/<channel>/<device>/<functional block>/<data point></code> . This is also the location of the data point in the SmartServer tree.
<i>Priority</i>	Displays the alarm priority assigned to the data point in the Alarm Notifier: Data Points Web page.
<i>Group</i>	Displays the alarm group assigned to the data point in the Alarm Notifier: Data Points Web page.
<i>Value</i>	Displays the data point value that triggered the alarm. <ul style="list-style-type: none"> • If this alarm was triggered by a SNVT_alarm type data point, this will be the value of the data point that caused the SNVT_alarm or update to be sent. • If this alarm was triggered by a SNVT_alarm_2 data point, this value will be the location of the alarm (for example, the location property for an Alarm Generator). • If the data point is set to a preset value, the preset name will be displayed instead of the actual value.
<i>Unit</i>	The unit string of the data point value that triggered the alarm condition. If this alarm was triggered by a SNVT_alarm or SNVT_alarm_2 type data point, this field will be blank.
<i>Description</i>	The alarm type or other description of the alarm entered in the Alarm Notifier: Alarm Conditions Web page.

5. Use the slide bar at the top to display the alarms reported during a specific time interval. You can specify the length of the interval using the drop-down list directly below the slider. By default, the **Entire Range** of when alarms were first and lastly reported is displayed.
6. Select **Acknowledgement** to have the **Alarm Notifier** stop reporting the alarm condition for a data point that has triggered an alarm. A check box will be available if **Acknowledgement Required** in the **Alarm Notifier: Data Points** Web page for the data point is selected.
7. Select **CLR** to clear the alarm from a data point. A check box will be available if **Clear Required** in the **Alarm Notifier: Data Points** Web page for the data point is selected.
8. Optionally, you can enter a comment, such as a description of how the alarm was resolved or further maintenance work required, in the **Comment** box. The comment will be added to the alarm summary log file.

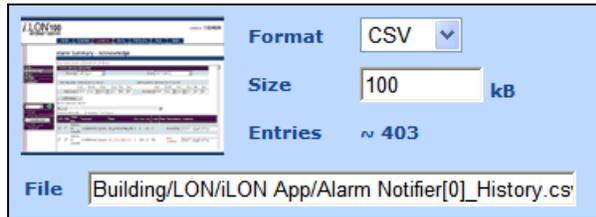
Tip: If you need to print this page, use the landscape format.

Using the Alarm Notifier: History Web Page

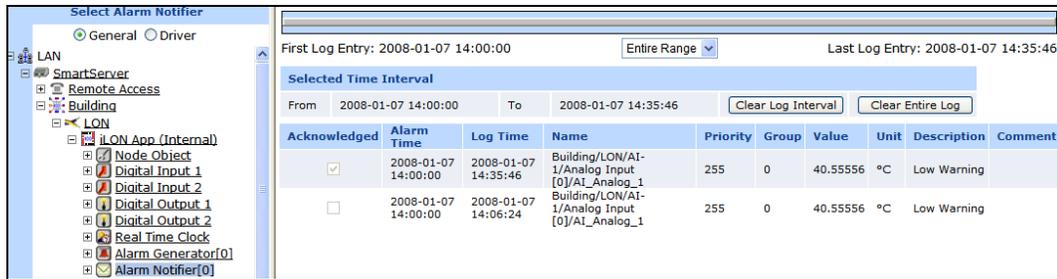
The **Alarm Notifier: History** Web page lists all active and cleared alarms reported by all the Alarm Notifiers on the SmartServer. To use this Web page, follow these steps:

1. Open the **Alarm Notifier: History** Web page. You can do this in two ways:

- Click **View** and then click **Alarm History**. By default, the **Alarm Notifier: History** Web page will list the active and cleared alarms recorded by all the Alarm Notifiers on the SmartServer.
- Click **General** and then click an Alarm Notifier functional block to open the **Alarm Notifier: Configure** Web page. Click the alarm history icon on the bottom, right side of the Web page. By default, the **Alarm Notifier: History** Web page will list only the active and cleared alarms recorded by the selected Alarm Notifier.



2. The **Alarm Notifier: History** Web page opens.



3. You can change whether this Web page lists the active and cleared alarms recorded by one or more Alarm Notifiers on the SmartServer.
 - To view the active and cleared alarms recorded by one specific Alarm Notifier, click that Alarm Notifier in the SmartServer tree (if you opened the **Alarm Notifier: History** Web from the main SmartServer Web page, you initially need to click the Alarm Notifier to be viewed twice).
 - To view the active and cleared alarms recorded by multiple Alarm Notifiers on the SmartServer, hold down CTRL and click the Alarm Notifiers to be viewed in the SmartServer tree, or hold down SHIFT and click an Alarm Notifier to view all the Alarm Notifiers within the selected range.
4. By default, the data points are listed by the **Alarm Time** property in descending order. You can sort the alarms by clicking a property header. You can click **Clear Log Interval** to delete the alarms currently displayed; you can click **Clear Entire Log** to delete all the alarms in the log. The **Alarm Notifier: History** Web page displays the following properties for each alarm:

- Acknowledged* Indicates whether the alarm has been acknowledged. A check box will be available if **Acknowledgement Required** in the **Alarm Notifier: Data Points** Web page for the data point is selected.
- Cleared* Indicates whether the alarm has been cleared. A check box will be available if **Clear Required** in the **Alarm Notifier: Data Points** Web page for the data point is selected.
- Alarm Time* Displays the date and time of when the alarm occurred.
- Log Time* Displays the date and time of when the alarm was recorded by the Alarm Notifier.
- Name* Displays the name of the data point that triggered the alarm using the following format: <network>/<channel>/<device>/<functional block>/<data

	<i>point</i> >. This is also the location of the data point in the SmartServer tree.
<i>Priority</i>	Displays the alarm priority assigned to the data point in the Alarm Notifier: Data Points Web page.
<i>Group</i>	Displays the alarm group assigned to the data point in the Alarm Notifier: Data Points Web page.
<i>Value</i>	Displays the data point value that triggered the alarm. <ul style="list-style-type: none"> • If this alarm was triggered by a SNVT_alarm type data point, this will be the value of the data point that caused the SNVT_alarm or update to be sent. • If this alarm was triggered by a SNVT_alarm_2 data point, this value will be the location of the alarm (for example, the location property for an Alarm Generator). • If the data point is set to a preset value, the preset name will be displayed instead of the actual value.
<i>Unit</i>	The unit string of the data point value that triggered the alarm condition. If this alarm was triggered by a SNVT_alarm or SNVT_alarm_2 type data point, this field will be blank.
<i>Description</i>	The alarm type or other description of the alarm entered in the Alarm Notifier: Alarm Conditions Web page.

5. Use the slide bar at the top to display the alarms reported during a specific time interval. You can specify the length of the interval using the drop-down list directly below the slider. By default, the **Entire Range** of when alarms were first and lastly reported is displayed.
6. Optionally, you can enter a comment, such as a description of how the alarm was resolved or further maintenance work required, in the **Comment** box. The comment will be added to the Alarm History log file. By default, the alarm description is displayed in this box.

Tip: If you need to print this page, use the landscape format.

Scheduling

This chapter describes how to use the Event Scheduler on the SmartServer to schedule daily, weekly, and monthly updates to the data points on your network. It describes how to overlap events and how to start or stop events based on the calculated sundown and sunrise.

Scheduling Overview

The SmartServer contains an Event Scheduler application that you can use to update data points at specific times. Each Event Scheduler includes a day-based daily schedule and a date-based exception schedule.

The daily schedule occurs every week on a specified day. You can assign a single daily schedule to multiple days of the week. For example, you can define two daily schedules: one for weekdays and another for weekends, or you can even define seven daily schedules (one for each day of the week) to create a weekly schedule.

The exception schedule may occur on holidays, inventory, or on any user-specified date or range of dates when the system being controlled requires specific events or needs to be shut down. You use the exception schedule to enable alternate daily schedules to become active on a range of user-specified dates such as “January 12th to February 2nd” or on recurring dates such as “Every other Monday” or “the third Monday of every month.” You can also use the exception schedule to schedule events to occur at sunrise and sundown or a specified period of time before or after.

The daily and exception schedules both consist of a series of events. An event is a data point update that occurs at specific time. An event includes a time and a value, typically a preset, to which the selected data points are updated (for example, 09:00: OPEN). You can use presets to enable one or more data points to be updated at a time. For example, you can use the OPEN event to set the temperature for an HVAC system and turn on the lights, as long as the data points for those systems have been added to the Event Scheduler.

All Event Schedulers are connected to the Event Calendar and the Real-Time Clock on the SmartServer. The Event Calendar contains exceptions that are applied globally to the Event Schedulers on the SmartServer. The Real-Time Clock maintains the current date and time on the SmartServer and it includes an astronomical position sensor that determines the position of the sun based on the time and location of the SmartServer. You can use this information to schedule events based on the sunrise and sundown times calculated by the astronomical position sensor.

Each Event Scheduler can update multiple data points. For example, you can create several Event Schedulers for a single building: one to control heating, one to control lighting, and so on. This flexibility allows you to set schedules that meet the requirements of a wide range of different applications.

You can create up to 40 Event Schedulers per SmartServer if you are using the default SmartServer v12 static interface. You can add more than 40 Event Schedulers if you activate the v40 dynamic interface, which features a dynamic external interface, on your SmartServer. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

Creating an Event Scheduler

To create an Event Scheduler, follow these steps:

1. Plan your schedule. For example, “On weekday mornings at 6:00 AM the heating system will be started and the thermostat set to 65°. At 8:00 AM, the thermostat will be set to 70°.” See the next section, *Planning Your Schedule*, for more information.
2. Configure the SmartServer’s real-time clock if you plan on creating sunrise and sundown events.
3. Open an Event Scheduler application.
4. Select the data points to be updated by the Event Scheduler.
5. Create the daily schedules by editing the daily schedules (selecting which days use a daily schedule) and creating events.

6. Create the exception schedules by setting the range of dates for which the exception schedules are used by creating one-time exceptions, exceptions, and recurring exceptions, and creating events. You can also create exception schedules in the Event Calendar and apply them to all the Event Schedulers on the SmartServer.

Planning Your Schedule

Before using the Event Scheduler, plan your schedule to determine the schedules and events that need to be created. The following example demonstrates a simple schedule for scheduling HVAC and lighting controls in a retail store. In this example one preset is used to update data points in both the HVAC and lighting controls.

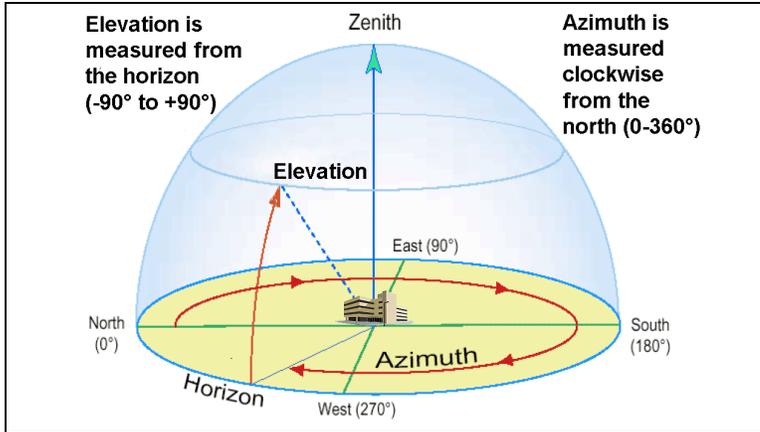
- On weekdays, the heat is set to 60°F at 7:00 AM (WARMUP); the heat is set to 70°F and the lighting turned on at 9:00 AM (OPEN); the heat and the lighting are turned off at 6:00 PM (CLOSE).
- On weekends, the heating and lighting remain off.
- For inventory (the last Sunday of each month), the heat is set to 65°F and the lighting turned on at 9:00 AM (OPEN_INVENTORY), and the heat and the lighting are turned off at 6:00 PM (CLOSED). In this case, you need to create a recurring exception.
- Every year you will have a winter vacation. In 2013–2014, the vacation is from December 22nd to January 1st, but you may change the dates every year.

Configuring the Real-Time Clock

You can use the real-time clock on the SmartServer to schedule events to start or stop based on the calculated sundown or sunrise, or a configured amount of time before or after the sundown or sunrise. The real-time clock includes an astronomical position sensor that calculates the position of the sun based on the time-of-day stored on the SmartServer and the location (geographic coordinates) of the SmartServer, which you specify. Based on the calculated position of the sun, the real-time clock can determine the sunrise and sundown times and pass this information to the Event Scheduler.

More specifically, the astronomical position sensor application in the SmartServer calculates the elevation and azimuth of the sun relative to the location of the SmartServer and then stores the results in its `nvoElevation` and `nvoAzimuth` **SNVT_angle_deg** data points. The elevation is returned as a value between -90 and 90, where a positive value indicates that the sun is up and a negative value indicates that the sun is down. The azimuth is returned as a value between 0 and 360, where 0 indicates that the sun is directly to the north, 90 indicates that the sun is to the East, 180 indicates that the sun is to the South and 270 indicates the sun is to the West.

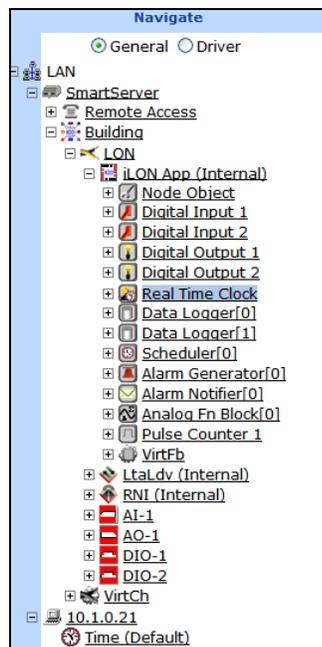
The following figure demonstrates how the elevation and azimuth are mapped to the sun's location. In this figure, the elevation of the sun is calculated to be approximately 60° and the azimuth is measured to be approximately 290°, which means that the sun is up in the mid-afternoon and is located northwest of the SmartServer. The calculated elevation and azimuth are stored in the `nvoElevation` and `nvoAzimuth` data points.



Based on the latitude, longitude and the actual date, the real-time clock on the SmartServer calculates the sunrise and sundown times and stores the results in nvoSunRise and nvoSunSet **SNVT_time_stamp** data points. The information in these data points is then passed to the Event Scheduler.

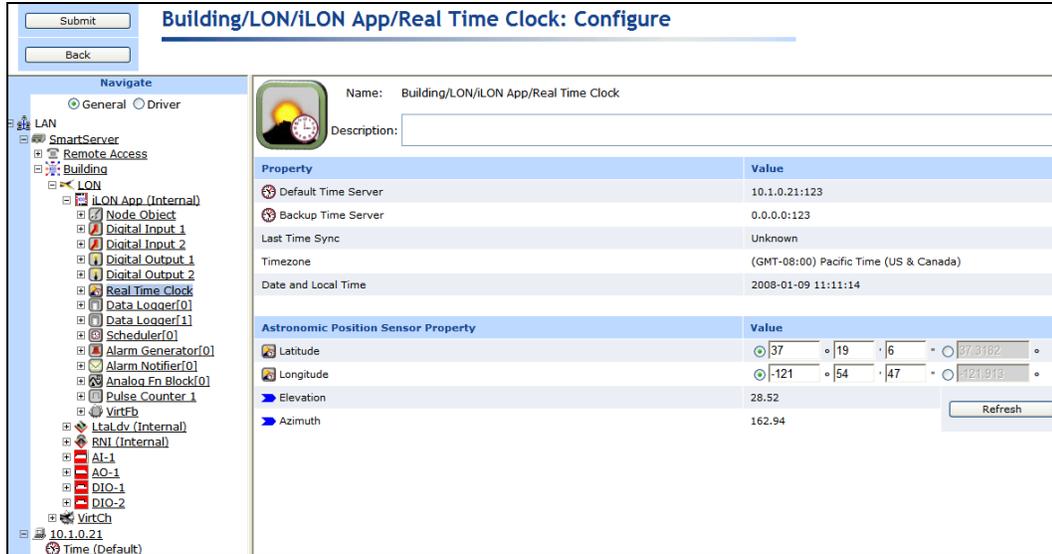
To configure the real-time clock in the Event Scheduler, follow these steps:

1. Add a time (SNTP) server to the LAN on which the SmartServer resides, or manually set the time on the SmartServer.
 - To add a time server to the LAN, follow the instructions in *Adding a Time (SNTP) Server to the LAN* in Chapter 3, *Configuring and Managing the SmartServer*.
 - To set the time on the SmartServer manually, follow the instructions in *Configuring Time Properties* in Chapter 3, *Configuring and Managing the SmartServer*.
2. Open the Real-Time Clock application on the SmartServer. You can do this two ways:
 - Click **General**; expand the network icon in the SmartServer tree, expand the **LON** channel, expand the **i.LON App (Internal)** device; and then click the **Real-Time Clock** functional block.



- Create or open an Event Scheduler application following the steps described in *Creating Event Schedulers* later in this chapter, and then click the **Real-Time Clock / Astronomic Position Sensor** icon in the **Scheduler: Configure Web** page.

3. The **Real Time Clock: Configure Web** page opens.



4. Configure the following properties for the real-time clock and astronomical position sensor on the SmartServer :

Name Displays the network path of the real-time clock functional block in the following format: `<network>/<channel>/<device>/<functional block>`. This field is read-only.

Description Enter an optional description of the real-time clock. This description has no effect on network operation, but you can use it to provide additional documentation for as-built reports.

Time Property

Default Time Server Displays the IP address of the designated default SNTP time server used by the real-time clock. You can click the IP address to access the **Setup – TimeService** Web page of the SNTP time server. From this Web page, you can change the properties of the SNTP time server, including clearing its default designation.

See *Adding a Time (SNTP) Server to the LAN* in Chapter 3 for how to configure the properties of an SNTP time server.

Backup Time Server Displays the IP address of the backup SNTP time server used by the real-time clock. You can click the IP address to access the **Setup – TimeService** Web page of the SNTP time server. From this Web page, you can change the properties of the SNTP time server, including selecting it as the default time server.

See *Adding a Time (SNTP) Server to the LAN* in Chapter 3 for how to configure the properties of an SNTP time server.

Last Time Sync Displays the last time in which the SmartServer synchronized its clock with the default SNTP time server. The amount of time varies between 1 to 15 minutes, depending on the difference in time between the SmartServer’s clock and the SNTP time server. As the difference approaches 75 ms or less, the interval will keep increasing until it reaches

the maximum of 15 minutes.

Time Zone Displays the time zone in which the SmartServer is located. You can click the displayed time zone to access the **Setup – Time** Web page. From this Web page, you can select a different time zone.

Date and Local Time Displays the time and date currently stored in the real time clock. You can click the displayed time to access the **Setup – Time** Web page. From this Web page, you can enter a different time to be stored in the real-time clock.

Astronomical Position Sensor Property

Latitude Enter the north-south location of the SmartServer relative to the equator. Select the first radio button to enter the latitude in sexagesimal notation (degrees, minutes, and seconds); select the second radio button to enter the latitude as a decimal fraction.

If the SmartServer is located south of the equator, enter a negative value between 0 and –90. If it is located north of the equator, enter a positive value between 0 and 90.

Longitude Enter the east-west location of the SmartServer relative to the Prime Meridian. Select the first radio button to enter the longitude in sexagesimal notation (degrees, minutes, and seconds); select the second radio button to enter the longitude as a decimal fraction.

If the SmartServer is located west of the Prime Meridian, enter a negative value between 0 and –180. If it is located east of the Prime Meridian, enter a positive value between 0 and 180.

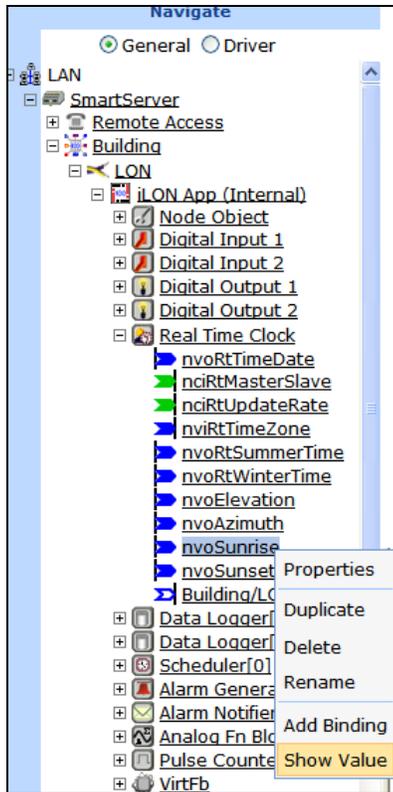
Elevation Displays the altitude of the sun calculated by the SmartServer. The elevation is the angle between the sun and the horizon of the SmartServer. The displayed elevation is based on the time and SmartServer position stored in the real-time clock and astronomical position sensor, respectively. This field is read-only.

Click **Refresh** to obtain the current elevation of the sun. This is useful if you change the time or location of the SmartServer.

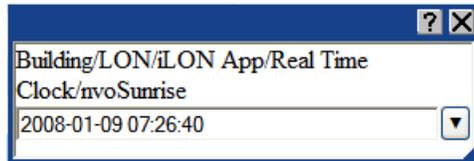
Azimuth Displays the azimuth of the sun calculated by the SmartServer. The azimuth is the angle of the sun around the horizon (measured from the north point towards the east). The displayed azimuth is based on the time and SmartServer position stored in the real-time clock and astronomical position sensor, respectively. This field is read-only.

Click **Refresh** to obtain the current azimuth of the sun. This is useful if you change the time or location of the SmartServer.

5. Click **Submit**. The elevation and azimuth are stored in the `nvoElevation` and `nvoAzimuth` **SNVT_angle_deg** data points. Based on these data points, the SmartServer calculates the sunrise and sundown and stores the results in `nvoSunRise` and `nvoSunSet` **SNVT_time_stamp** data points. You can then schedule events to start or end at the sunrise and sundown or a configured time before or after. This is useful for a variety of applications such as street lighting, outdoor lighting, sun blind, and sun shade controls.
6. You can also view the calculated sunrise and sundown times. To do this, expand the **Real-Time Clock** functional block, right-click the `nvoSunrise` or `nvoSunset` data point, and then click **Show Value** on the shortcut menu.



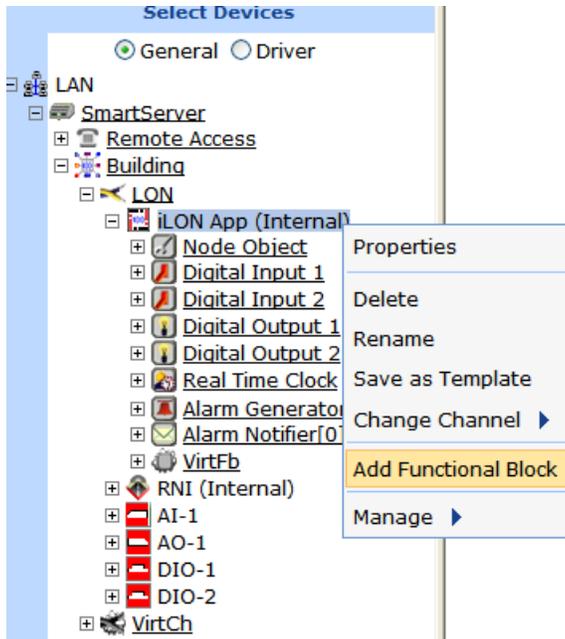
7. A dialog opens and displays the current sunrise or sundown time stored in the data point in the following format: YYYY-MM-DD hh:mm:ss.



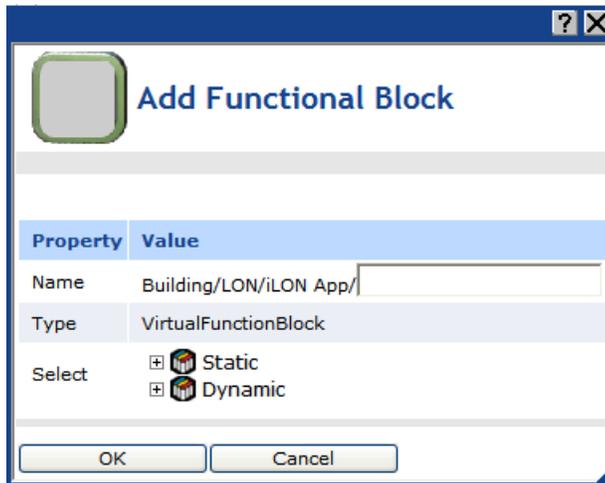
Opening an Event Scheduler Application

To open an Event Scheduler application, you must first create a Scheduler functional block. After you create the Scheduler functional block, the functional block appears on the SmartServer tree below the **i.LON App (Internal)** device, and you can click the functional block to open the Event Scheduler application. To create a Scheduler functional block and open the application, follow these steps:

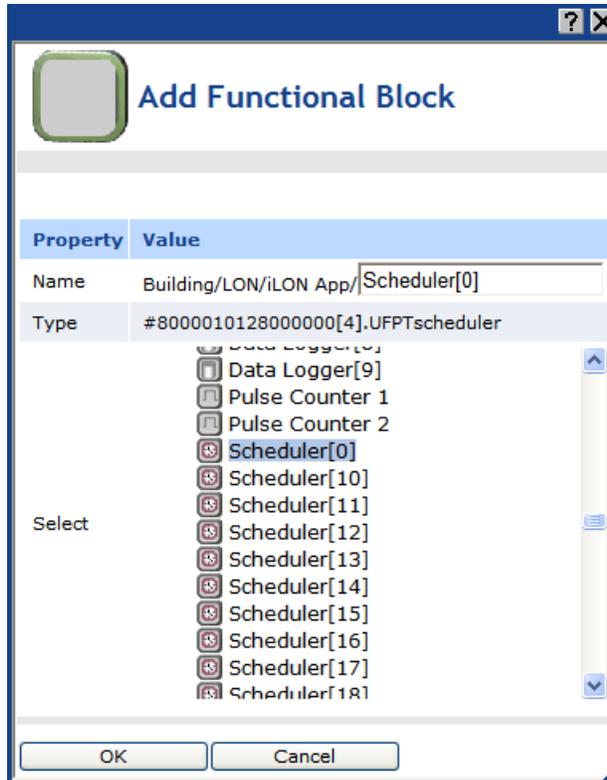
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



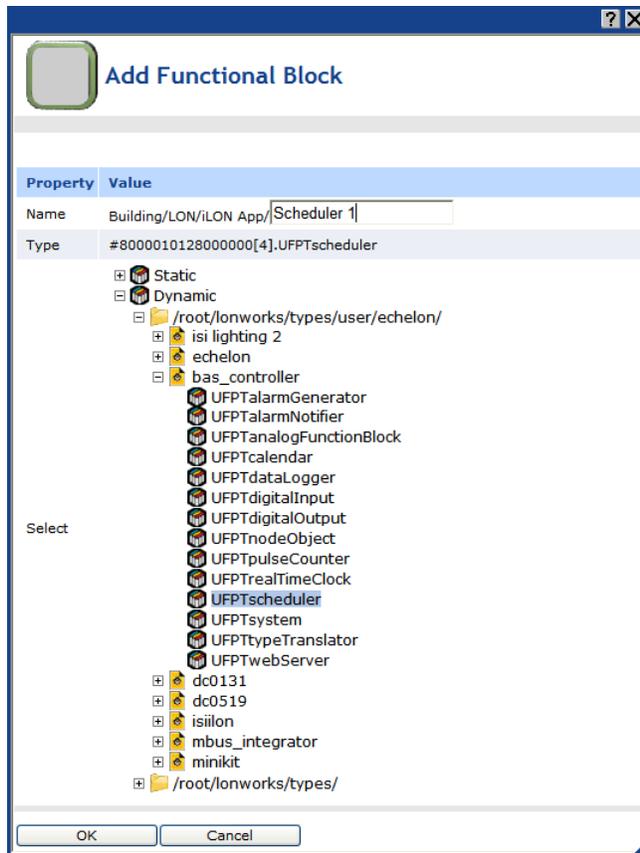
4. The **Add Functional Block** dialog opens.



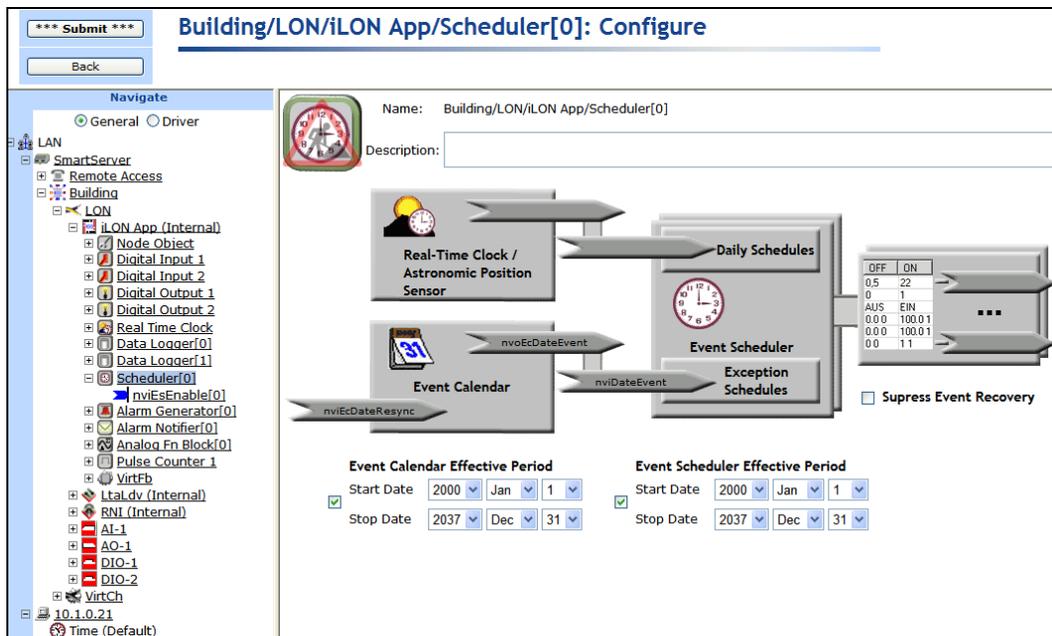
5. Select the Scheduler functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Scheduler** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Scheduler functional block from either the **Static** or the **Dynamic** folder. To select the Scheduler functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the Scheduler, enter a name for the functional block such as “Scheduler 1”, and then click **OK**.



- A functional block representing the Scheduler application and all of its static data points are added to the bottom of the **iLON App (Internal)** device tree, and the **Scheduler: Configure** Web opens in the application frame to the right. The construction symbol overlaid onto the Scheduler application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



7. Optionally, under **Event Calendar Effective Period** and **Event Scheduler Effective Period**, you can configure the period of time for which the Event Calendar and Event Scheduler are active, respectively. By default, both are active for a 37-year period starting on January 1, 2000 and ending December 31, 2037. To configure a different effective period, specify the **Start Date** and **Stop Date**. If you clear the check box, the default 37-year effective period is used.
8. By default, the **Suppress Event Recovery** check box is cleared. This means that the Scheduler executes the next scheduled event when the SmartServer has been rebooted, the system time has been changed, or a data point's priority has been reset at the end of a one-time exception. This enables the SmartServer to maintain the current value stored in the data point if the data point has been overridden by another application.

You can select the **Suppress Event Recovery** check box so that when the SmartServer has been rebooted, the system time has been changed, or a data point's priority has been reset at the end of a one-time exception, the Scheduler will attempt to restore the values and priorities of the selected input points by searching for the most recent past event and executing it. Ultimately, the Scheduler exclusively determines the value of each selected input point (as long as it has the highest priority assigned to the data point).

9. Click **Submit**.

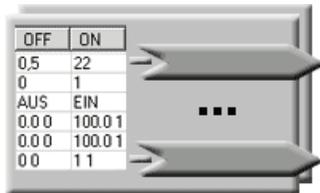
To open the Scheduler application from an existing Scheduler functional block, follow these steps:

1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Scheduler application.
2. Click the Scheduler functional block representing the Scheduler to be opened. The **Scheduler: Configure** Web page opens in the application frame to the right.

Selecting Data Points

You can select and configure the input points to be updated by the Event Scheduler application. To select a data point, follow these steps:

1. Click the data point box on the right side of the **Scheduler: Configure** Web page.



2. The **Scheduler: Data Points** Web page opens. Click the data points to be updated by the Event Scheduler from the SmartServer tree. The selected data points are added to the Web page; any presets defined for the selected data points are displayed to the right. In addition, references to the selected data points () are added to the bottom of the Scheduler functional block tree, and references to the Scheduler functional block are added directly below the selected data points ().

Building/LON/iLON App/Scheduler[0]: Data Points						
	Data Point	Unit	Stagger Delay	CLOSED	WARMUP	OPEN
0	Building/LON/AI-1/Analog Input[0]/AI_Analog_1	°F	0.0 s	0	60	70
1	Building/LON/DIO-1/Digital Output[0]/DO_Digital_1	% of full level	0.0 s	0.0 0		100.0 1

To update a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree

to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).

3. View or configure the following properties of the selected data points:

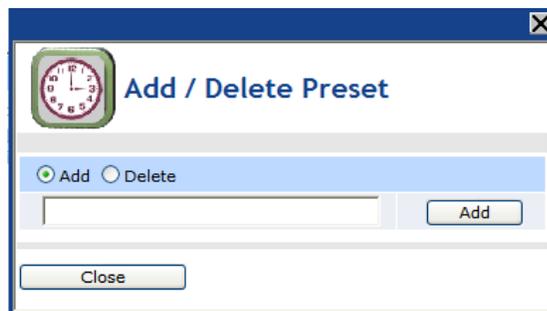
- Data Point** Displays the name of the data point to be updated using the following format: `<network>/<channel>/<device>/<functional block>/<data point>`. This is also the location of the data point in the SmartServer tree.
- Unit** Displays the unit string describing the data point to be updated. A **SNVT_temp_f#US** data point, for example, has “degrees F” describing the data point. A **SNVT_switch** data point has “% of full level” and “state code” unit strings describing its state and value fields. This field is read-only. You can edit the unit string of a data point in the **Configure - Data Point Web** page, which you can access by clicking the data point in **General** mode.
- Stagger Delay** Displays the period of time (in seconds) that the Event Scheduler will wait before updating the specified data point at each schedule interval. This enables you to ramp up or wind down a system. For example, consider a schedule that controls the power for 100 stores in a mall, and the schedule indicates that power should be turned on at 8:00AM. However, turning on power for 100 stores at once could cause a power surge. To avoid this, you could use varying **Stagger Delays** for the different points to bring power up for 1 or 2 stores at a time.

You can create a default **Stagger Delay** and apply that value to all the currently added data points by filling in the **Default Stagger Delay** box, and then clicking **Set All to Default**. The delay will be cascaded for each data point. For example, if you set the default stagger delay to 2 seconds, the delay between the first and second updates would be two seconds (so the delay shown for the first data point would be 0 seconds, and the delay shown for the second data point would be 2 seconds). The delay for the third data point to be updated would be 4 seconds, and then a 6 second delay for the fourth data point, and so on. This way, a different data point would be updated every two seconds.

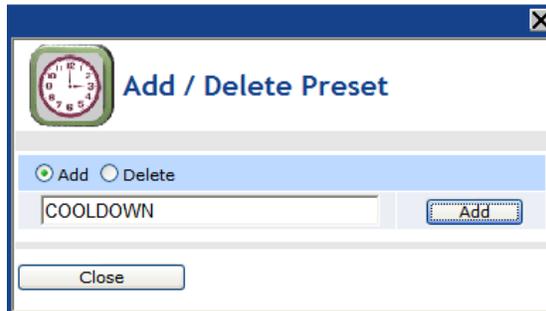
4. Optionally, you can add new presets to the data point and delete existing presets. To do this, follow these steps:
 - a. Right-click the data point and select **Add/Delete Preset** on the shortcut menu.

	Data Point	Unit	Stagger Delay	CLOSED	WARMUP	OPEN
0	Net/LON/Thermostat_AI/Analog Fn Block 1/Heat	°F	0.0 s	0	60	70
1	Net/LON/Lamp_DO/Digital Output 1/Light On_Off	Remove marked Data Point(s)		0.0	0	100.0
		Add / Delete Preset				

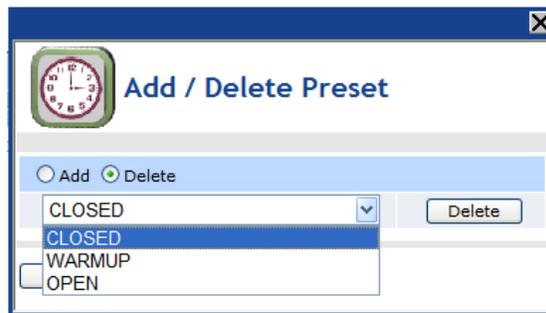
- b. The **Add/Delete Preset** dialog opens.



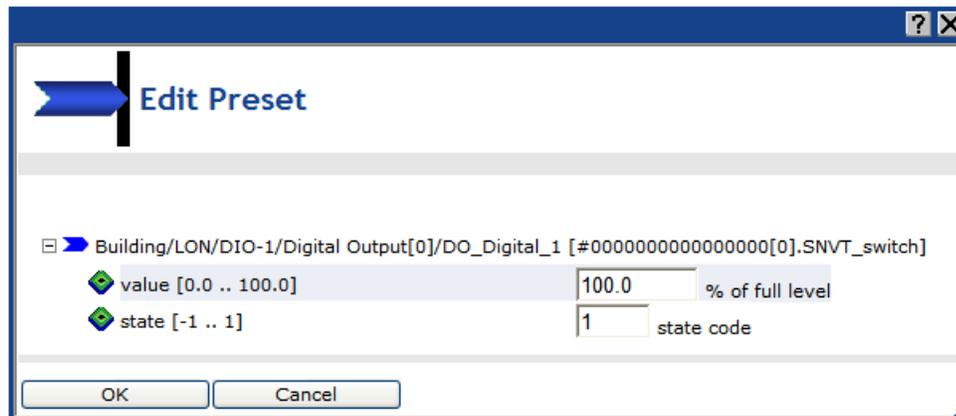
- To create a new preset, click the **Add** radio button at the top, enter the name of the new preset in the field, and then click the **Add** button on the right side next to the field in which you entered the name of the preset. The new preset appears without a value in the **Scheduler: Data Points** Web page.



- To delete an existing preset, click the **Delete** radio button at the top, select the preset from the list of presets, and then click the **Delete** button on the right side next to the list of presets. The preset is removed from the **Scheduler: Data Points** Web page.



- c. Click **Close**.
5. Optionally, you can edit the values of existing presets. To do this, follow these steps:
 - a. Click the preset to be edited. The **Edit Presets** dialog opens.



- b. Enter the value (or values if you are editing the preset of a structured data point) for the preset.
- c. Click **OK**.
6. Click **Submit**.
7. Click **Back** to return to the **Scheduler: Configure** Web page.

Creating Daily Schedules

You can set the daily schedules for the Event Scheduler by defining for which days a schedule is applicable and creating events. After you define the daily schedules and create events, you can copy and delete schedules.

Defining Schedules

By default, the Event Scheduler has two daily schedules: **Weekday** (Monday–Friday) and **Weekend** (Saturday–Sunday). You can create separate schedules for individual days and modify for which days the schedules are applicable. To define the scope of the schedules, follow these steps:

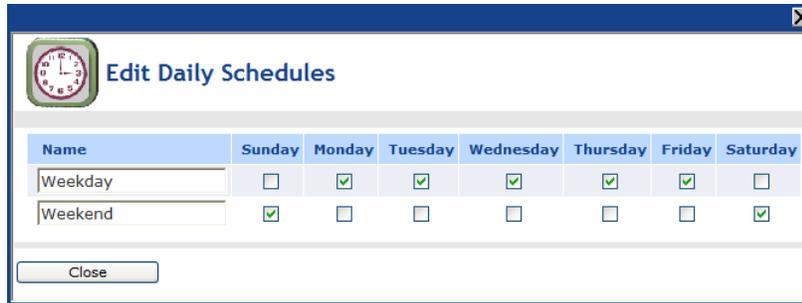
1. Click the **Daily Schedules** icon in the **Scheduler: Configure** Web page.



2. The **Scheduler: Daily Schedules** Web page opens. By default, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, and **Friday** are selected, which means that all five weekdays use the same weekday schedule. The check boxes for **Saturday** and **Sunday** are cleared, which means that both weekend days use the same weekend schedule by default.

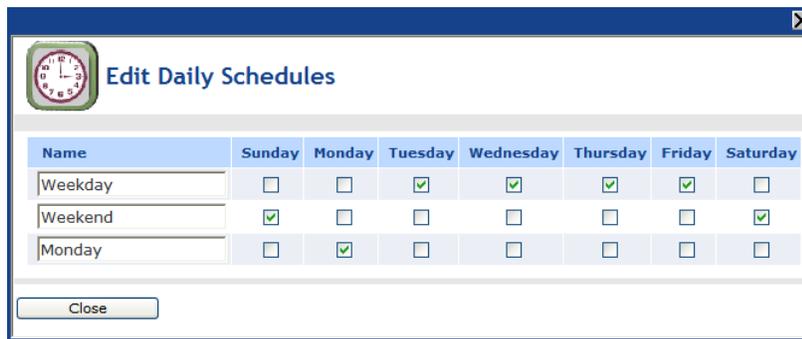
Building/LON/iLON App/Scheduler[0]: Daily Schedules							
Time	<input type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							

3. Optionally, you can create separate schedules for individual days. You can do this in two ways:
 - In the current **Scheduler: Daily Schedules** Web page, click the check box for the day that is to use a separate schedule. The check boxes for all the other days are cleared, which means that the selected day now uses its own daily schedule. For example, you can click the Monday check box to create a separate schedule for Monday. When you click the Monday check box, it is selected and the check boxes for Tuesday–Friday are cleared. To create a separate daily schedule for Saturday or Sunday, you click the check box for the weekend day twice. The first click adds the weekend day to the Monday–Friday daily schedule, and the second click then creates a separate daily schedule for that day.
 - Right-click anywhere in the daily schedules and click **Edit Daily Schedules** on the shortcut menu. The **Edit Daily Schedules** dialog opens.

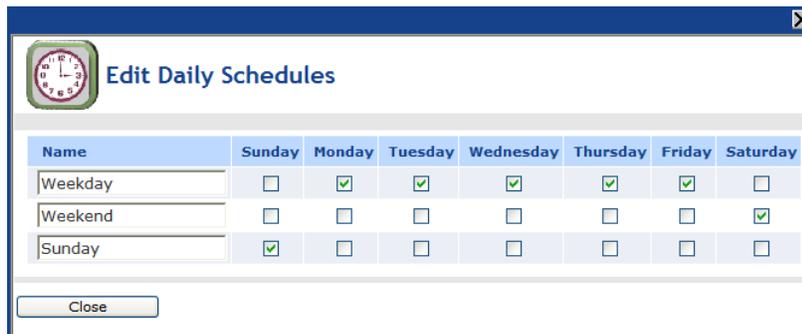


This dialog functions similarly to the **Scheduler: Daily Schedules** Web page, except that it also lets you view the current daily schedules as you group days into different schedules. It lists two schedules: **Weekday** and **Weekend**. The Monday–Friday check boxes are selected in the daily schedule, and the Saturday–Sunday check boxes are selected in the weekend schedule. This means that the five weekdays use the same daily schedule, and the weekend days use a separate weekend schedule.

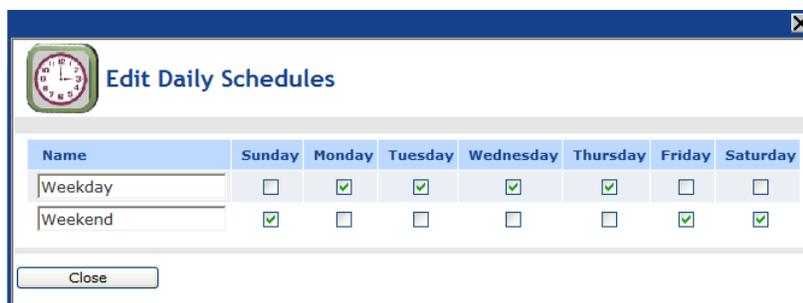
To create a separate schedule for a day, clear its check box. A new daily schedule with that day’s name is added to the list of daily schedules. For example, you can clear the Monday check box to add a new schedule named **Monday** to the list of daily schedules and remove Monday from the default **Weekday** schedule.



This is the same procedure you use to create a separate daily schedule for Saturday or Sunday. You clear the check box for that weekend day. For example, you can clear the Sunday check box to add a new schedule named **Sunday** to the list of daily schedules and remove Sunday from the default **Weekend** schedule.



You can also add a day to an existing daily schedule. For example, you could select the Friday check box in the weekend schedule. This would remove Friday from the **Weekday** schedule, and add it to the **Weekend** schedule.



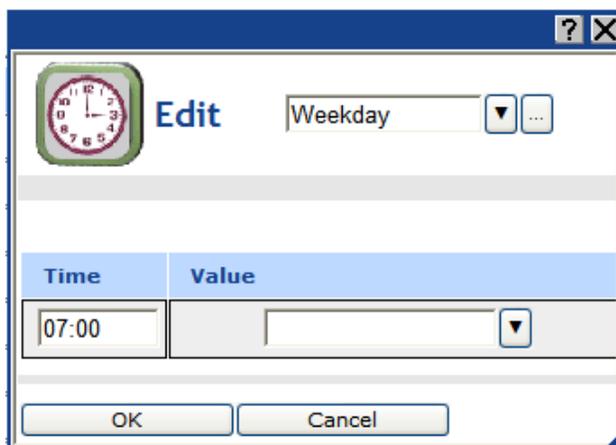
You can also re-name any of the daily schedules. When you are done editing and re-naming the daily schedules, click **Close** to return to the **Scheduler: Daily Schedules** Web page.

4. Click **Submit**.

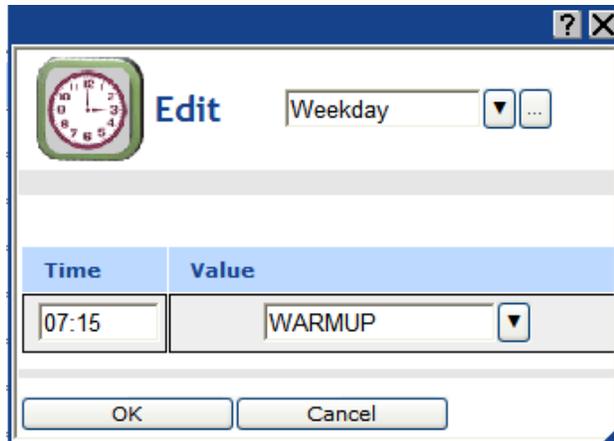
Creating Events in the Daily Schedule

You can add and edit events from the **Scheduler: Daily Schedules** Web page. To do this, follow these steps:

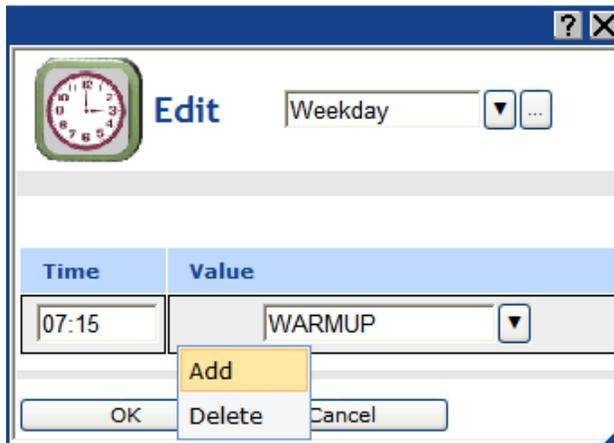
1. Click the box corresponding to the day and time for which an event is to be created. For example, to schedule an event at 7:00 on Monday, click the box that is in the **7:00** row and under the **Monday** column. The **Edit** dialog opens.



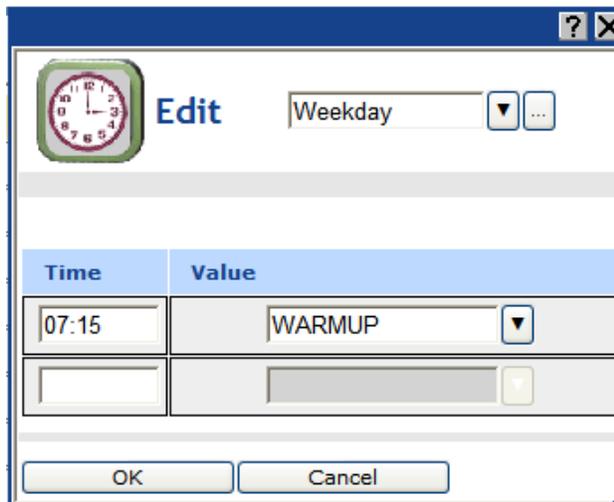
2. By default, the daily schedule in which the selected day is a member is displayed at the top of the dialog (for example, **Weekday**, **Weekend**, or some other user-defined daily schedule). You can select a different daily schedule from the list to add events to that daily schedule. In addition, you can click the box to the right of the daily schedule list to open the **Edit Daily Schedules** dialog and configure the scope of the daily schedules. See the previous section, *Defining Schedules*, for more information on configuring the daily schedules.
3. In the **Time** box, enter the exact time the event is to occur if it is different than the default time, which is on the hour of the selected time. For example, to create an event that occurs at 7:15 A.M. instead of the default 7:00 A.M, enter **07:15**. Note that you can create up to one event per minute.
4. In the **Value** box, do one of the following:
 - Select the preset to be used to update the values of all the data points added to the Scheduler that have that preset defined for them. Alternatively, you can enter a new preset and then go back to the **Scheduler: Data Points** Web page and define the value (or values) for the preset.
 - Enter a valid value to be written to all the data points. To enter a value, all the data points added to the Scheduler must have the same network variable type (for example, **SNVT_switch**).



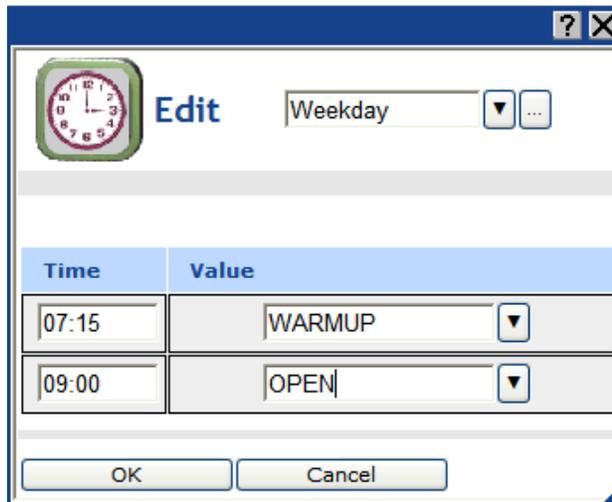
5. To create additional events in the daily schedule, follow these steps:
 - a. Right-click anywhere in the **Time** or **Value** boxes, and then click **Add** in the shortcut menu.



- b. A new row for the event is added to the **Edit** dialog.



- c. Follow steps 3–4 to specify the **Time** and **Value** of the new event.



6. Click **OK** to save your events and return to the **Scheduler: Daily Schedules** Web page. Click **Cancel** to delete all changes and return to the **Scheduler: Daily Schedules** Web page.
7. The **Scheduler: Daily Schedules** Web page is updated to reflect the events you created, which are listed under each day of the selected daily schedule. For example, if you created events for Monday, and Monday is in the default Monday–Friday **Weekday** schedule, the events you created will also be listed under the Tuesday, Wednesday, Thursday, and Friday schedules. If you scheduled multiple events within an hour, an arrow appears to the right of the time under the **Time** column. You can click the arrow to show all the events under that time.

Building/LON/iLON App/Scheduler[0]: Daily Schedules							
Time	<input type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00		07:15 WARMUP	07:15 WARMUP	07:15 WARMUP	07:15 WARMUP	07:15 WARMUP	
8:00							
9:00		09:00 OPEN	09:00 OPEN	09:00 OPEN	09:00 OPEN	09:00 OPEN	
10:00							
11:00							

Note: To edit an event, click the event in the **Scheduler: Daily Schedules** Web page, change the time or value, and then click **OK**. To delete an event, click the event in the **Scheduler: Daily Schedules** Web page, right-click the event, click **Delete** on the shortcut menu, and then click **OK**.

8. Repeat steps 1–6 to create events for other Daily Schedules in the Scheduler.
9. Click **Submit**.
10. Click **Back** to return to the **Scheduler: Configure** Web page.

Copying and Deleting Schedules

After you create a daily schedule for one day, you can copy it to another day. This is ideal for creating a new daily schedule that requires some or all of the events defined in an existing schedule. For example, if a building shuts down early on Friday, you can create a schedule for Monday-Thursday, copy it to Friday, and then edit a CLOSED event, for example, so that it occurs earlier.

To copy a schedule, follow these steps:

1. Right-click the day with the schedule to be copied and then click **Copy Schedule** on the shortcut menu.
2. Right-click the day to which the schedule is to be copied and then click **Paste Schedule** on the shortcut menu.
3. Click **Submit**.

To delete a daily schedule, right-click the day with the schedule to be deleted and then click **Delete Schedule** on the shortcut menu. The events for the selected day and any other days using the same daily schedule are removed.

Creating the Exception Schedule

You can create an Exception Schedule for a Scheduler. An Exception Schedule is an alternate Daily Schedule that is used on one date over a specific interval (a one-time exception), over a range of dates (an exception), or over a range of dates in a specific pattern (a recurring exception). You can create exceptions in the Event Scheduler to apply the exceptions to the current Event Scheduler or to all the Event Schedulers on the SmartServer.

You can create three types of exceptions:

- **One-time exceptions.** One-time exceptions occur over a user-defined interval on a single calendar date. You can use one-time exceptions to schedule special events, such as building maintenance, for a period of time on a given date.
- **Exceptions.** Exceptions occur on a range of user-specified dates. One example of when an exception could be used is a building shutdown over a long holiday. Another use of an exception would be holidays such as Chinese New Year where the dates vary each year based on the lunar calendar. You can also use the exception schedule to schedule events to occur at sunrise and sundown or a specified period of time before or after.
- **Recurring exceptions.** Recurring exceptions occur in a certain pattern over a range of user-specified dates. One example of when a recurring exception could be used is inventory for a retail store. Inventory typically occurs once a month on a specific day such as the last Sunday of the month. Another example is holidays such as Thanksgiving, which occurs on the fourth Thursday of November, or New Year's Day, which occurs January 1st.

After you create two or more of these exceptions, you can create an exception group and add exceptions to it. The exceptions will then implement the schedule you create for the exception group. You can also edit and delete the exceptions and exception groups.

After you create exceptions and exception groups, you can add events to their schedules just as you were creating a daily schedule.

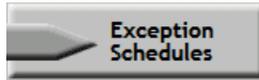
Note: You can also create exceptions and apply them to all the Event Schedulers on the SmartServer using the Event Calendar. See *Using the Event Calendar* in this chapter for how to do this.

Creating One-Time Exceptions

You can create a one-time exception to apply an alternate schedule to specific interval on a single calendar date such as 05:00 to 08:00 on May 20, 2007, or 15:00 to 20:00 on December 21, 2008. You can create a one-time exception in the Event Scheduler to apply it to the current Event Scheduler or to all the Event Schedulers on the SmartServer.

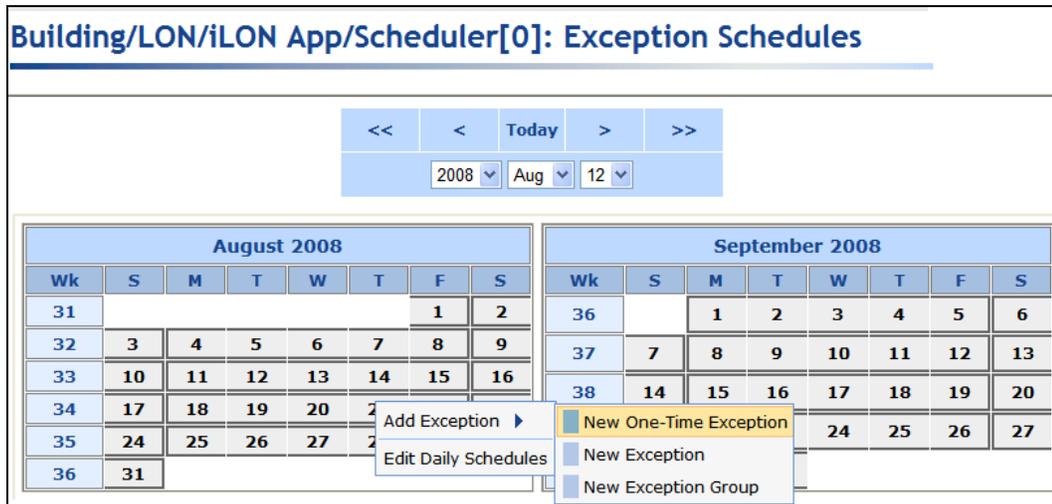
To create a one-time exception in the Event Scheduler, follow these steps:

1. Click the Exception Schedules icon in the **Scheduler: Configure** Web page.

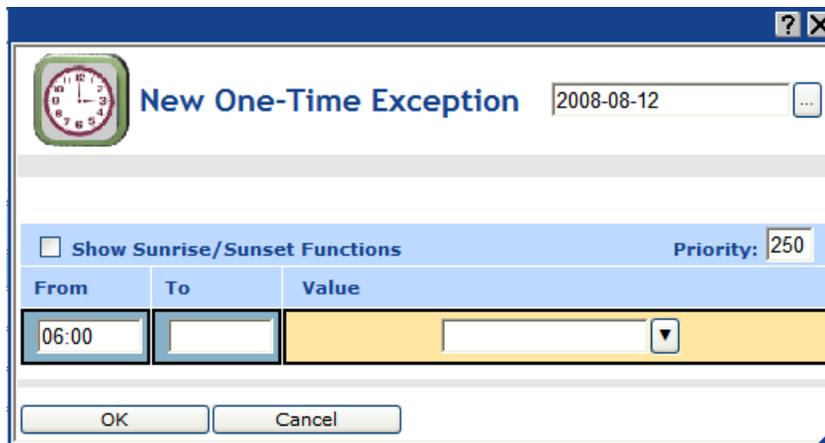


The **Scheduler: Exception Schedules** Web page opens.

2. To create a one-time exception, right-click the date on which the one-time exception schedule is to be used, point to **Add Exception**, and then click **New One-Time Exception** on the shortcut menu.



3. The **New One-Time Exception** dialog opens.



4. By default, the name of the one-time exception is the date on which it is being created. You can enter a different, descriptive name in the box at the top of the dialog. Additionally, you can click the box to the right of the one-time exception name to open the **Edit Exception** dialog and change the scope, dates, and recursions of the exception. See *Creating Exception Dates in the Exception Schedule* later in this chapter for more information on the properties in this dialog.
5. Optionally, you can click the **Show Sunrise/Sunset Functions** check box to create events based on sundown and sunrise times. In the **Function** box, you can select the Sunrise (☀) or Sundown (🌇) icon if you are creating an event based on the calculated sundown or sunrise time. The calculated sunrise or sundown time appears in the **Time** box, which becomes read-only, and an **Offset** box is added to the right of the **Time** box. In the **Offset** box, you can enter the time before or after sunrise or sundown that the event is to occur.

If you are creating an event based on a specific time of day, select the **Clock** icon (🕒), which is selected by default. This hides the **Offset** box and enables you to enter a time in the **Time** box.

See *Creating Sunrise and Sunset Events* later in this chapter for creating schedules based on sunrise and sunset times.

6. Specify the start and end time of the one-time exception following these steps:
 - a. In the **Time** box under the **From** property, enter the exact time the event is to start.
 - b. In the **Time** box under the **To** property, enter the exact time the event is to end.
 - c. In the **Value** box, do one of the following:
 - Select the preset to be used to update the values of all the data points added to the Scheduler that have that preset defined for them. Alternatively, you can enter a new preset and then go back to the Scheduler: Data Points Web page and define the value (or values) for the preset.
 - Enter a valid value to be written to all the data points. To enter a value, all the data points added to the Scheduler must have the same network variable type (for example, **SNVT_switch**).
 - d. In the **Priority** box, enter a priority for the event between 0 to 255 (highest to lowest priority). The default priority for an event in an exception schedule is five more than the priorities of events in the daily schedule. For example, if you created an event with a priority of 255 in the daily schedules, the events in the exception schedule will have a priority of 250. This priority essentially locks out events with lower priorities so that they cannot update the data points written to by this event. When the event ends, lower priority events can update the data points.

From	To	Value
18:00	20:00	OPEN

- e. To create additional events in the one-time exception, right-click anywhere in the **Time** or **Value** boxes, and then click **Add** in the shortcut menu. A new row for the event is added to the dialog. Follow steps a–c to specify the **Time** and **Value** of the new event in the one-time exception.
 - f. Click **OK** to save your events and return to the **Scheduler: Exception Schedules** Web page. Click **Cancel** to delete all changes and return to the **Scheduler: Exception Schedules** Web page.
7. The date on which the one-time exception is to occur is highlighted teal (or dark blue) in the calendar.

Building/LON/iLON App/Scheduler[0]: Exception Schedules

<<
<
Today
>
>>

2008
Aug
12

August 2008								September 2008							
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S
31						1	2	36		1	2	3	4	5	6
32	3	4	5	6	7	8	9	37	7	8	9	10	11	12	13
33	10	11	12	13	14	15	16	38	14	15	16	17	18	19	20
34	17	18	19	20	21	22	23	39	21	22	23	24	25	26	27
35	24	25	26	27	28	29	30	40	28	29	30				
36	31														

8. Click **Submit**.
9. To edit the one-time exception, click the teal-highlighted date in the calendar. The **Edit:** *<exception name>* dialog opens. This dialog lists the events that are scheduled to occur on the selected date.

The intervals specified by the events in the one-time exception are highlighted teal, and the events in the daily schedule are highlighted grey. When events in the one-time exception end, their priority is reset to 255 and the schedule reverts to the regular daily schedule. This means that the highest priority event in the applicable daily and exception schedules that was supposed to occur prior to the event in the one-time exception is executed. If there are no such events, the next highest-priority event will execute at its regularly scheduled time.



Edit: 2008-08-12

Time	Schedule	Event Time	Value	Priority
00:00				
01:00				
02:00				
03:00				
04:00				
05:00				
06:00				
07:00	Weekday	07:15	WARMUP	255
08:00				
09:00	Weekday	09:00	OPEN	255
10:00				
11:00				
12:00				
13:00				
14:00				
15:00				
16:00				
17:00				
18:00	2008-08-12	18:00	OPEN	250
19:00				
20:00	2008-08-12	20:00		255
	Weekday	20:00	CLOSE	255
21:00				
22:00				

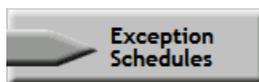
Creating Exceptions in the Event Scheduler

You can create an exception or recurring exception in the Event Scheduler. An exception is an alternate daily schedule that is used over a range of dates. A recurring exception is an alternate daily schedule that is used over a range of dates in a specific pattern (such as every third Sunday). To create an exception or recurring exception, you set the dates of the exception and then create the events in the exception.

Creating Exception Dates in the Exception Schedule

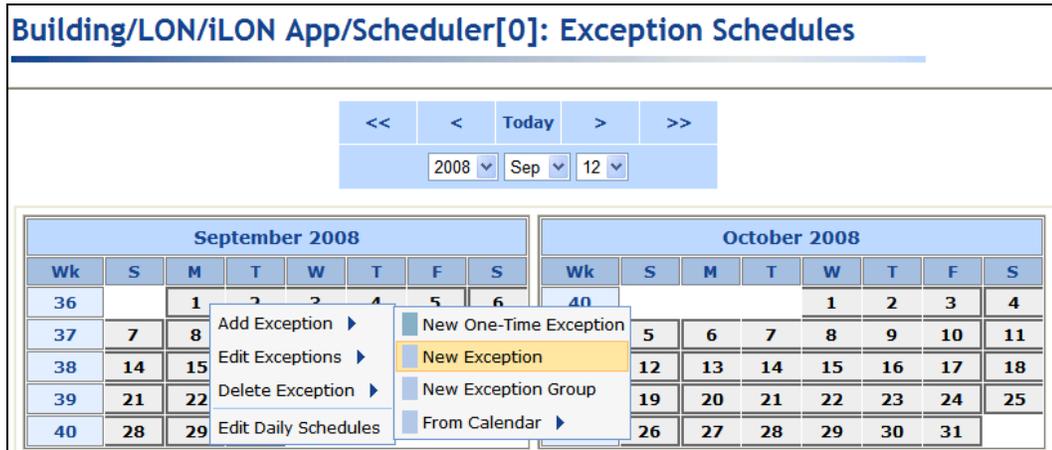
To create an exception in the Event Scheduler and specify the range of dates and recursions for the exception, follow these steps:

1. Click the Exception Schedules icon in the **Scheduler: Configure** Web page.



The **Scheduler: Exception Schedules** Web page opens.

- Right-click the start date on which the exception schedule is to begin, point to **Add Exception**, and then click **New Exception** on the shortcut menu.

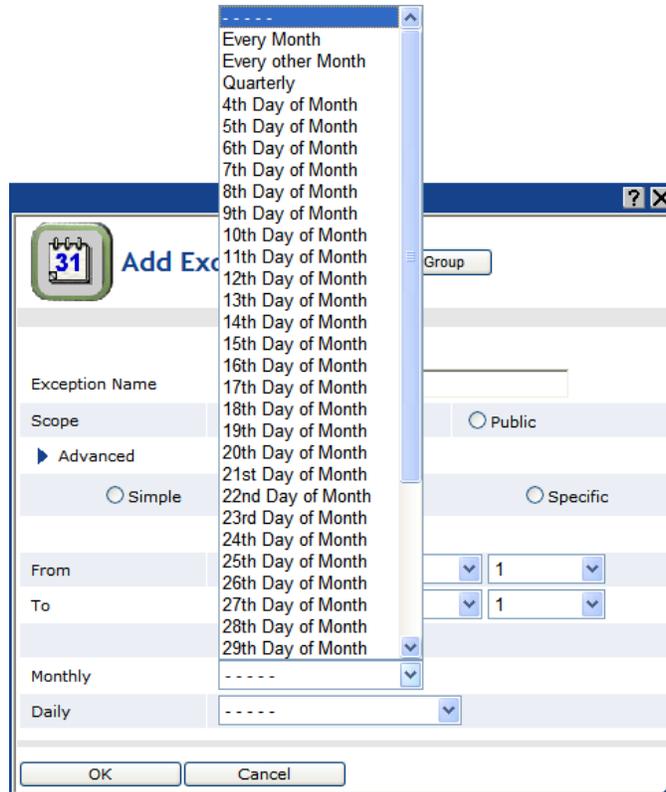


- The **Add Exception** dialog opens.

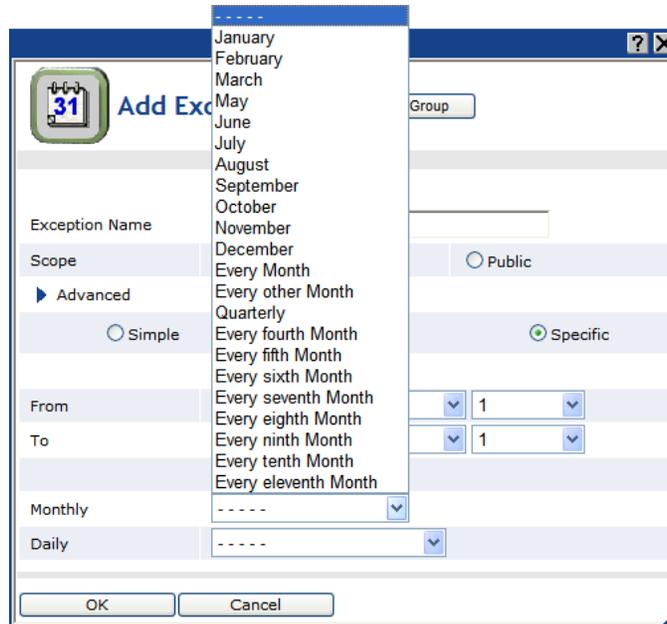


- In the **Exception Name** property, enter a descriptive name for the exception. The default name is the selected start date in the following format: *<year>-<month>-<date>*.
- In the **Scope** property, select whether the exception is **Private** (can only be applied to the current Scheduler) or **Public** (can be applied to all Schedulers). The default scope is **Private**.
- To create an exception group (a set of exceptions that use the same schedule), click the blue arrow in the **Advanced** property (located directly below the **Scope** property) to show options for adding, deleting, and editing additional exceptions included under the current exception.
 - Click **Add** to create an exception group and add new exceptions to the group. All new exceptions you add to the group will use the same Exception Schedule, but you can specify a different range of dates and recursions for the new exception. For example, you could create a new exception for Thanksgiving that uses the same range of dates as the current exception, but uses a different set of recursions. With an exception group, all the changes you make to the schedule of one exception are globally applied to the schedules of all the exceptions within the group. For example, if you create an ON event in the schedule for the Thanksgiving exception, that ON event is automatically added to the schedule of all other exceptions in the exception group.
 - Once you click **Add**, specify the range of dates for the exception in the **From** and **To** boxes and click **Standard** or **Specific** if you want the exception to be a recurring exception.

- c. You can click the arrows to scroll through the exceptions in the Exception Group and edit their dates and recursions. Click **Delete** to remove an exception from the Exception Group.
 - d. Select the **Delete when Expired** check box to have the exception removed from the Exception Group once the last date in the range of dates specified for the exception has ended.
7. To create a recurring exception, click the **Standard** or **Specific** options to expand the dialog to show the Recurrence property.
- Clicking **Standard** lets you apply the exception to every month, every other month, every third month, and so on up to every eleventh month. It also lets you apply the exception to specific days such as every Monday, every Tuesday, and so on; every weekday or every weekend day; and every other day, every third day, and so on up to every sixth day.

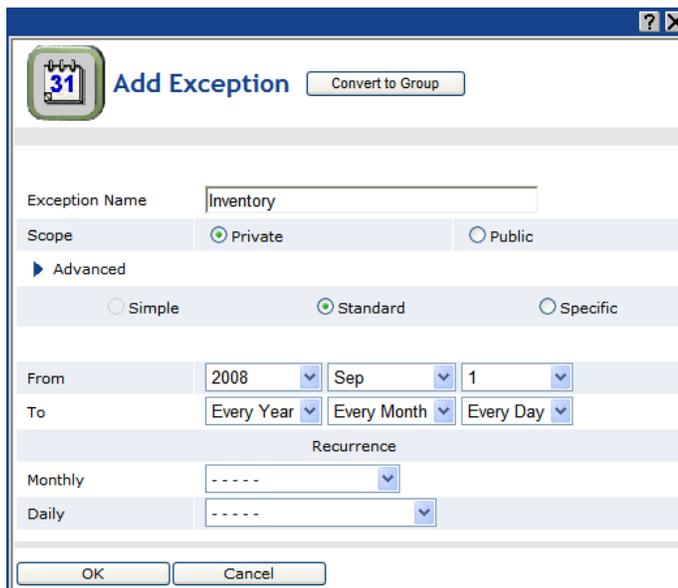


- Clicking **Specific** lets you apply the exception to specific months such as January, February, and so on up to December in addition to the monthly options offered by clicking **Standard**. It also lets you apply the exception to specific dates such as the 1st to 30th day of the month; specific dates starting from the end of the month such as last day of the month, 2nd last day of the month, and so on up to the 30th last day of the month; and specific recurring days such as every first, second, third, fourth, fifth, or last Sunday, Monday, and so on up to Saturday. This is in addition to the daily options offered by clicking **Standard**.



- Specify the range of dates for which the exception schedule is used. Specify the start and end dates in the **From** and **To** properties, respectively.

Tip: You can create an exception that occurs every day from the specified start time to the specified stop time instead of specifying actual start and end years, months, and dates. In the **To** and **From** properties, select **Every Year**, **Every Month**, or **Every Day** in the year, month, or day boxes based on when this recurring exception is to begin and end. This is useful for creating complex recurring exceptions in which the recurring exception specified in this property is combined with the recursion defined in the **Recurrence** property. It takes longer for the Event Calendar to calculate and display exceptions when complex recurring exceptions are used.



- Under **Recurrence**, select the monthly and daily recursions from the **Monthly** and **Daily** lists. The default monthly recursion is every month. This means that if you do not specify a monthly recursion, the events will occur every month within the specified range. The default daily recursion is every day. This means that if you do not specify a daily recursion, the events will occur every day within the specified range.

10. Optionally, you can click **Convert to Group** at the top of the dialog to open the **New Exception Group** dialog. You can use this dialog to create a new exception group (a set of individual exceptions that share the same schedule) that includes this exception and one or more other existing exceptions. See *Creating Exception Groups* for more information on exception groups and using this dialog to create them.
11. Click **OK** to add the exception and return to the **Scheduler: Exception Schedules** Web page (click **Cancel** to discard all changes and return to the **Scheduler: Exception Schedules** Web page). The range of dates on which the exception is to occur is highlighted light blue in the calendar and outlined with a color differentiating it from the other exceptions in the calendar.

Building/LON/iLON App/Scheduler[0]: Exception Schedules

<< < Today > >>
 2008 Sep 13

September 2008								October 2008							
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S
36		1	2	3	4	5	6	40				1	2	3	4
37	7	8	9	10	11	12	13	41	5	6	7	8	9	10	11
38	14	15	16	17	18	19	20	42	12	13	14	15	16	17	18
39	21	22	23	24	25	26	27	43	19	20	21	22	23	24	25
40	28	29	30					44	26	27	28	29	30	31	

12. Click **Submit**.

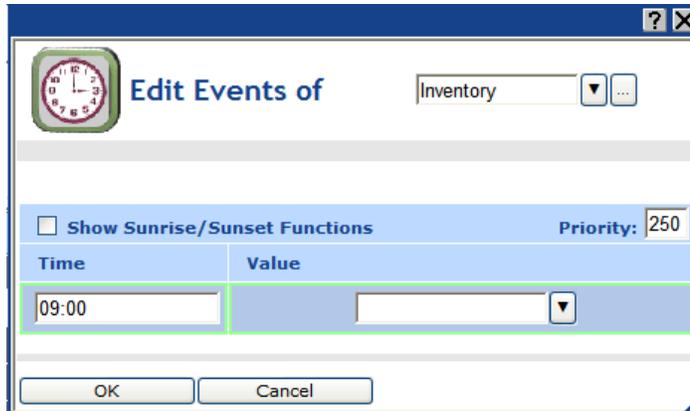
Creating Exception Events in the Exception Schedule

To create events for an exception schedule, follow these steps:

1. Click one of the light blue-highlighted dates in the exception to specify the events for the exception. The **Edit: <exception date>** dialog opens.
2. This dialog lists the events scheduled in an exception. It is updated in real-time as you add, edit, and delete events.



3. Click anywhere in the row under the **Schedule**, **Event Time**, **Value**, or **Priority** columns at the time the event is to occur. The **Edit Events Of** dialog opens. Alternatively, you can right-click a time under the **Time** column or right-click the column to the right and click **Add Event** on the shortcut menu to open the **Edit Events Of** dialog.

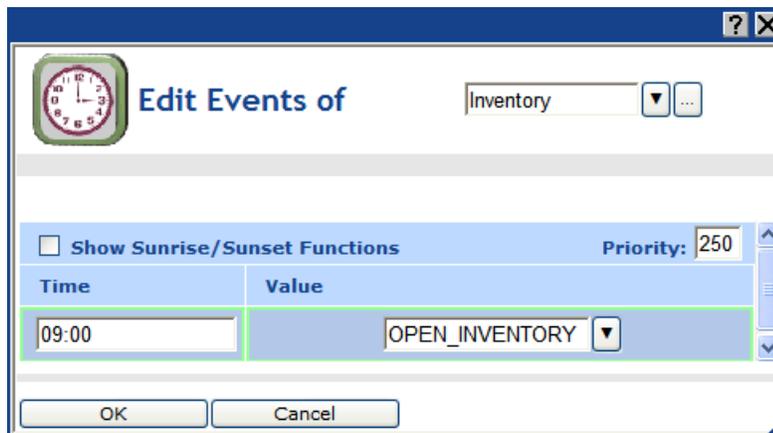


4. By default, the exception schedule in which you are creating events is displayed in the list box at the top of the dialog. You can select the applicable daily schedule and other applicable exception schedules from the list. Additionally, you can click the box to the right of the exception name to open the **Edit Exception** dialog and change the scope, dates, and recursions of the exception. See *Creating Exception Dates in the Exception Schedule* later in this chapter for more information on the properties in this dialog.
5. Optionally, you can click the **Show Sunrise/Sunset Functions** check box to create events based on sundown and sunrise times. In the **Function** box, you can select the Sunrise (☀️) or Sundown (🌑) icon if you are creating an event based on the calculated sundown or sunrise time. The calculated sunrise or sundown time appears in the **Time** box, which becomes read-only, and an **Offset** box is added to the right of the **Time** box. In the **Offset** box, you can enter the time before or after sunrise or sundown that the event is to occur.

If you are creating an event based on a specific time of day, select the **Clock** icon (🕒), which is selected by default. This hides the **Offset** box and enables you to enter a time in the **Time** box.

See *Creating Sunrise and Sunset Events* later in this chapter for creating schedules based on sunrise and sunset times

6. Create the schedule for the exception following these steps:
 - a. In the **Time** box, enter the time the event is to occur if it is different than the default time, which is on the hour of the selected time. For example, to create an event that occurs at 10:15 A.M. instead of the default 10:00 A.M, enter **10:15**.
 - b. In the **Value** box, do one of the following:
 - Select the preset to be used to update the values of all the data points added to the Scheduler that have that preset defined for them. Alternatively, you can enter a new preset and then go back to the Scheduler: Data Points Web page and define the value (or values) for the preset.
 - Enter a valid value to be written to all the data points. To enter a value, all the data points added to the Scheduler must have the same network variable type (for example, **SNVT_switch**).
 - c. In the **Priority** box, enter a priority for the event between 0 to 255 (highest to lowest priority). The default priority for an event in an exception schedule is five more than the priorities of events in the daily schedule. For example, if you created an event with a priority of 255 in the daily schedules, the events in the exception schedule will have a priority of 250. This priority essentially locks out events with lower priorities so that they cannot update the data points written to by this event. Once the Scheduler executes the event, the data points can only be updated by an event that has an equal or higher priority.



- d. To create additional events in the exception, right-click anywhere in the **Time** or **Value** boxes, and then click **Add** in the shortcut menu. A new row for the event is added to the dialog. Follow steps a–b to specify the **Time** and **Value** of the new event in the exception. You can create up to one event per minute.

The screenshot shows a dialog box titled "Edit Events of" with a clock icon on the left and a dropdown menu set to "Inventory" on the right. Below the title bar, there is a checkbox labeled "Show Sunrise/Sunset Functions" and a "Priority:" field with the value "250". A table with two columns, "Time" and "Value", contains two rows: the first row has "09:00" in the "Time" column and "OPEN_INVENTORY" in the "Value" column; the second row has "18:00" in the "Time" column and "CLOSE" in the "Value" column. At the bottom of the dialog are "OK" and "Cancel" buttons.

Time	Value
09:00	OPEN_INVENTORY
18:00	CLOSE

- e. Click **OK** to save your events and return to the **Edit: <exception date>** dialog. Click **Cancel** to delete all changes and return to the **Edit: <exception date>** dialog.
7. The **Edit: <exception date>** dialog is updated to reflect the events you created.

The screenshot shows a dialog box titled "Edit: 2008-09-28" with a clock icon on the left. It displays a table with a time column on the left and four columns for event details. The first row shows an event at 09:00 for "Inventory" with the value "OPEN_INVENTORY" and a priority of "250". The second row shows an event at 18:00 for "Inventory" with the value "CLOSE" and a priority of "250". Other time slots from 10:00 to 21:00 are empty. At the bottom are "OK" and "Cancel" buttons.

Time	Inventory	Value	Priority
09:00	Inventory	OPEN_INVENTORY	250
10:00			
11:00			
12:00			
13:00			
14:00			
15:00			
16:00			
17:00			
18:00	Inventory	CLOSE	250
19:00			
20:00			
21:00			

8. Click **OK** to save your changes to the **Edit: <exception date>** dialog and return to the **Scheduler: Exception Schedules** Web page. Click **Cancel** to delete all changes and return to the **Scheduler: Exception Schedules** Web page.
9. Click **Submit**.
10. Click **Back** to return to the **Scheduler: Configure** Web page.

Creating Exception Groups

You can create an exception group and add exceptions to it. This creates a new exception with its own schedule that is followed by all exceptions within the group. Exception groups enable you to configure at one time a set of common individual exceptions that share the same schedule.

The changes you make to the exception group are applied globally to all the exceptions within that group. For example, if you change the priority of an exception group, all events in the schedules of the exceptions within the group are updated with the new priority value. Also, if you add, delete, or modify the event schedule of an exception that is a member of an exception group, the event schedules for all the exceptions within the group are updated accordingly. For example, if you have a “Holiday” exception group that includes Memorial Day, the Fourth of July, Labor Day, and Thanksgiving exceptions, and you change the time of a CLOSED event in the Memorial Day event schedule, that CLOSED event is automatically updated to the same time in the Fourth of July, Labor Day, and Thanksgiving event schedule.

Note: When you add an exception to an exception group, the exception’s existing schedule is cleared and updated with the schedule of the exception group. Therefore, create an exception group before creating the event schedule of an exception that is to be added to the group.

To create an exception group, follow these steps:

1. Right-click an exception date or an empty space in the calendar, point to **Add Exceptions**, and then click **New Exception Group** on the shortcut menu.

The screenshot shows a calendar application window titled "Building/LON/iLON App/Scheduler[0]: Exception Schedules". The calendar displays four months: July 2008, August 2008, September 2008, and October 2008. A context menu is open over the date 27 in July 2008. The menu options are:

- Add Exception ▶
- Edit Exceptions ▶
- Delete Exception ▶
- Edit Daily Schedules
- New One-Time Exception
- New Exception
- New Exception Group**
- From Calendar ▶

2. The **New Exception Group** dialog opens. All the exceptions in the exception schedule are listed in order of creation.



3. Select the check boxes for two or more of the exceptions to be added to the new Exception Group (an exception group must contain at least two exceptions). The **Exception Group** and **Priority** boxes become available. Each exception can only belong to one exception group. To remove an exception from a group, clear its check box.
4. In the **Exception Group** box, enter a descriptive name for the exception group. The default name is **New Exception Group**.



5. In the **Priority** box, enter the priority to be assigned to the events in the exception group's schedule. Enter a value between 0 to 255 (highest to lowest priority). The default priority is five more than the priorities of the events in the exceptions being added to the group. This means that lower priority events in the applicable daily and exception schedules are locked out and cannot update the data points until the exception ends.

- Optionally, you can click **Edit** for any of the listed exceptions to open the **Edit Exception** dialog and change the name, scope, dates, and recursions of the exception and any other of the exception instances created under it. See *Creating Exception Dates in the Exception Schedule* in the previous section for more information.
- Click **OK** to save your exception group and return to the **Scheduler: Exception Schedules** Web page. Click **Cancel** to delete all changes and return to the **Scheduler: Exception Schedules** Web page.
- In the **Scheduler: Exception Schedules** Web page, the dates for the exceptions in the exception group are now outlined in the same color and the name of the exception group appears in all the shortcut menus in place of the names of the individual exceptions in the group. You can edit and delete the exception group just as you would any exception. See the next section, *Editing and Deleting Exceptions in the Event Scheduler*, for more information.
- Click one of the light blue-highlighted dates of the exception group in the calendar to create the exception group's schedule. The **Edit: <exception date >** dialog opens.
- Create the recurring exception schedule for the range of dates following the steps described in *Creating Exception Events in the Exception Schedule* in the previous section.

Editing and Deleting Exceptions in the Event Scheduler

After you create a one-time exception, exception, recurring exception, or exception group in the Event Scheduler, you can edit or delete it.

Editing Exceptions

To edit a one-time exception, exception, or recurring exception, follow these steps:

- Right-click the exception date or one of the dates in a range of exception dates, point to **Edit Exceptions**, and then either click the name of the exception to be edited on the shortcut menu or point to **All** and then click the name of the exception to be edited from the list on the shortcut menu of all the exception schedules in the Event Scheduler.

You can also right-click anywhere in the exception schedule, point to **Edit Exceptions**, point to **All**, and then click the name of the exception to be edited from the list on the shortcut menu of all the exception schedules in the Event Scheduler.

The screenshot displays the 'Exception Schedules' interface. At the top, there are navigation buttons: '<<', '<', 'Today', '>', and '>>'. Below these are dropdown menus for the year (2008), month (Aug), and day (13). The main area contains two calendar grids. The left grid is for August 2008, and the right grid is for September 2008. Both grids have columns for 'Wk', 'S', 'M', 'T', 'W', 'T', 'F', and 'S'. In the August grid, the date 31 is highlighted in light blue. A context menu is open over this date, with the following options: 'Add Exception', 'Edit Exceptions', 'Delete Exception', and 'Edit Daily Schedules'. The 'Edit Exceptions' option is highlighted in yellow. A sub-menu is open for 'Edit Exceptions', showing 'Inventory' and 'All' options.

- The **Edit Exceptions** dialog opens.



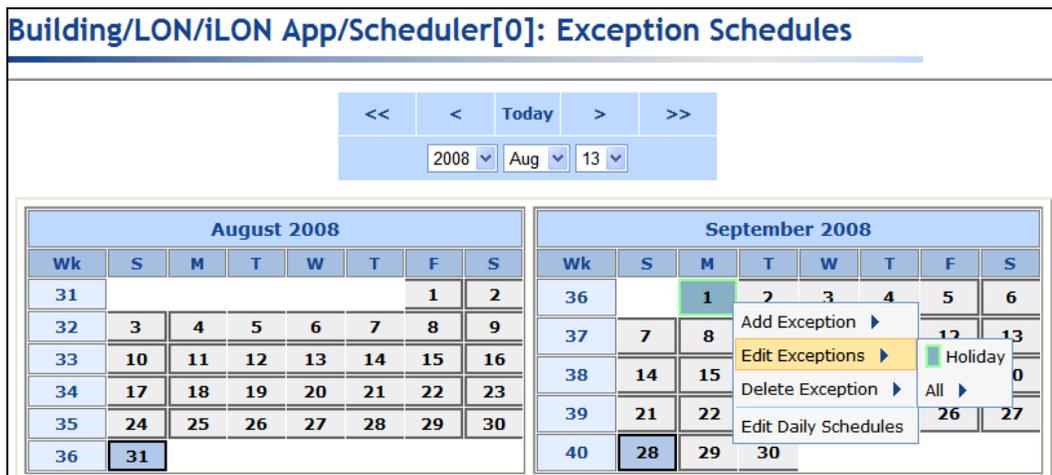
3. Edit the name, scope, dates, and recursions of the exception and any other instances created under this exception. See *Creating Exception Dates in the Exception Schedule* earlier in this chapter for more information on the properties in this dialog.
4. Click **Close** to return to the **Scheduler: Exception Schedules** Web page.
5. Click **Submit**.

Editing Exception Groups

To edit an exception group, follow these steps:

1. Right-click one of the exception dates of the exception group, point to **Edit Exceptions**, and then either click the name of the exception group to be edited on the shortcut menu or point to **All** and then click the name of the exception group to be edited from the list on the shortcut menu of all the exceptions in the Event Scheduler.

You can also right-click anywhere in the exception schedule, point to **Edit Exceptions**, point to **All**, and then click the name of the exception group to be edited from the list on the shortcut menu of all the exceptions in the Event Scheduler.



2. The **Edit Exception Group** dialog opens. All the exceptions in the Event Scheduler are listed and the check boxes for the exceptions that are currently in the exception group are selected.



3. You can rename the exception group, change the priorities of the events in the exception group, add and remove exceptions to and from the exception group, and edit the individual exceptions.
 - To add an exception to the exception group, select its check box. The selected exception will adopt the exception group's schedule.
 - To remove an exception from the exception group, clear its check box. The schedule of the cleared exception is reset to the default exception schedule.
 - To edit an exception, click **Edit**. The **Edit Exception** dialog opens. You can modify the name, scope, dates, and recursions of the exception and any other instances created under it. When you finish editing the exception, click **Close**.
4. Click **Close** to return to the **Scheduler: Exception Schedules** Web page.
5. Click **Submit**

Deleting Exceptions and Exception Groups

To delete an exception or exception group, follow these steps:

1. Right-click the exception date or one of the dates in a range of exception dates, point to **Delete Exceptions**, and then either click the name of the exception to be deleted on the shortcut menu or point to **All** and then click the name of the exception to be deleted from the list on the shortcut menu of all the exceptions in the Event Scheduler.

You can also right-click anywhere in the exception schedule, point to **Edit Exceptions**, point to **All**, and then click the name of the exception to be deleted from the list on the shortcut menu of all the exceptions in the Event Scheduler.

Building/LON/iLON App/Scheduler[0]: Exception Schedules

<< < Today > >>
 2008 Aug 13

August 2008								September 2008							
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S
31						1	2	36		1	2	3	4	5	6
32	3	4	5	6	7	8	9	37	7	8				12	13
33	10	11	12	13	14	15	16	38	14	15				19	20
34	17	18	19	20	21	22	23	39	21	22				26	27
35	24	25	26	27	28	29	30	40	28	29	30				
36	31														

2. Click **Submit**.

How the Scheduler Works with Daylight Savings Time

When daylight savings time starts, events scheduled in the switch hour are executed at the start of the next hour. For example, if you have the following schedule in North America before DST:

1:59	ON
2:30	OFF
3:01	ON

It is executed as follows when DST starts (time switches from 02:00 to 03:00). Observe that the 2:30 OFF events occurs at 03:00.

1:59	ON
3:00	OFF
3:01	ON

When daylight savings time ends, events scheduled in the switch hour are executed only once, instead of twice. For example, the following schedule in North America is executed as written when standard time starts (time switches from 02:00 to 01:00). Observe that the events in 01:00 hour are only executed once, even though that the hour occurs twice on that day.

12:59	STATE_3
1:15	STATE_1
1:45	STATE_2
2:01	STATE_3

Creating Sunrise and Sundown Events

You can create events in the exception schedule to occur at sunrise or sundown or a configured period of time before or after. This is useful for controlling systems where the device behavior is determined by the level of light (lux) such as street lighting, outdoor lighting, sun blinds, and sun shades. The sunrise and sundown times are calculated by the astronomical position sensor application on the SmartServer and then transmitted to the Event Scheduler. See the *Configuring the Real-Time Clock* section earlier in this chapter for more detailed information on how the astronomical position sensor functions.

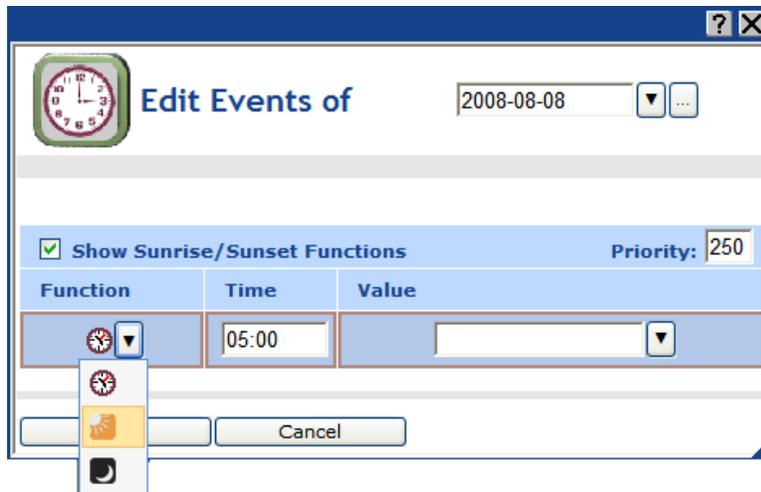
Note: Sunrise is the time at which the first part of the sun appears above the horizon in the east. At this time, there is complete light. Sunrise should not be confused with dawn, which is the point at which the sky begins to lighten, some time before the sun itself appears. Sundown is the time at which the sun disappears below the horizon in the west. At this time, there is still light, but it begins to gradually decrease until dusk, which is the point at which darkness falls.

To create events based on the sunrise or sundown, follow these steps:

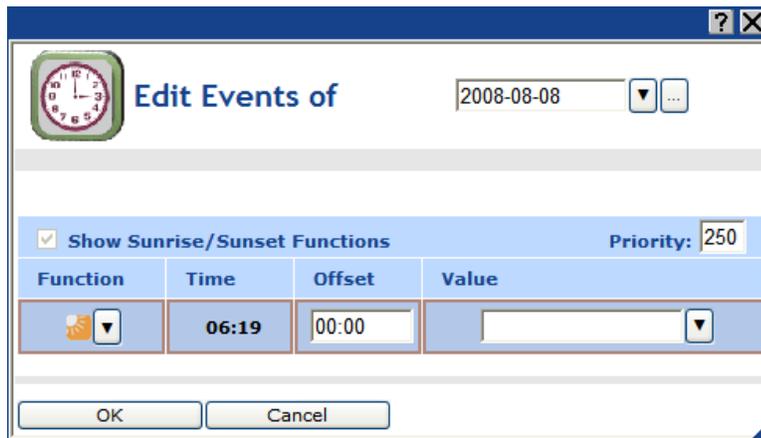
1. Add a time (SNTP) server to the LAN on which the SmartServer resides, or manually set the time on the SmartServer using the **Setup – Time** Web page.
 - To add a time server to the LAN, follow the instructions in *Adding a Time (SNTP) Server to the LAN* in Chapter 3, *Configuring and Managing the SmartServer*.
 - To set the time on the SmartServer manually using the **Setup – Time** Web page, follow the instructions in *Configuring Time Properties* in Chapter 3, *Configuring and Managing the SmartServer*.
2. Enter the location (geographic coordinates) of your SmartServer in the **Real-Time Clock: Configure** Web page following the steps described in the *Configuring the Real-Time Clock* section earlier in this chapter.
3. Click the Exception Schedules icon in the **Scheduler: Configure** Web page. The **Scheduler: Exception Schedules** Web page opens.
4. Right-click anywhere in the exception schedule, point to **Add Exception**, and then click **New One-Time Exception** or **New Exception** on the shortcut menu. If you are creating a one-time exception, skip to step 6. If you are creating an exception, proceed to step 5.
 - Create the sundown/sunrise events in a one-time exception to overlap events in the daily schedule and in other exception schedules with these sundown/sunrise events.
 - Create the sundown/sunrise events in an exception to replace the daily schedule with the exception schedule.

See *Demonstrating Sunrise and Sundown Events* for scenarios where you want to create sundown/sunrise events in a one-time exception and in an exception.

5. If you clicked **New Exception** in step 4, the **New Exception** dialog opens. Follow these steps:
 - d. Enter the name, scope, dates, and recursions for the exception; click **Close** to return to the **Scheduler: Exception Schedules** Web page; and then click **Submit**. See *Creating Exception Dates in the Exception Schedule* for more information on how to create an exception and set the range of dates and recursions for it in this dialog.
 - e. Click one of the blue-highlighted dates in the calendar to create the exception schedule for the range of dates specified in step a. The **Edit: <exception date >** dialog opens.
 - f. Click anywhere in the row under the **Schedule, Event Time, Value, or Priority** columns at the time the event is to occur. The **Edit Events Of** dialog opens. Alternatively, you can right-click a time under the **Time** column or right-click the column to the right and click **Add Event** on the shortcut menu to open the **Edit Events Of** dialog.
6. Create the sunrise and sundown events following these steps:
 - g. Select **Show Sunrise/Sunset Functions**. A **Function** box appears to the right of the **Exception** box.



- h. In the **Function** box, select Sunrise (☀️) or Sundown (🌑). The calculated sunrise or sundown time appears in the **Time** box, which becomes read-only, and an **Offset** box is added to the right of the **Time** box.



- i. If the event is to occur sometime before or after sunrise or sundown, enter that period of time in the **Offset** box. To schedule an event to occur before sunrise or sundown, enter a negative value; to schedule an event to occur after these times, enter a positive value. For example, to configure an ON_100 event to occur 30 minutes after sundown, enter **00:30**. To configure a DIMMING event to occur 15 minutes before sunrise, enter **-00:15**.



- j. In the **Value** box, do one of the following:
 - Select the preset to be used to update the values of all the data points added to the Scheduler that have that preset defined for them. Alternatively, you can enter a new preset and then go back to the Scheduler: Data Points Web page and define the value (or values) for the preset.
 - Enter a valid value to be written to all the data points. To enter a value, all the data points added to the Scheduler must have the same network variable type (for example, **SNVT_switch**).
 - k. In the **Priority** box, enter a priority for the event between 0 to 255 (highest to lowest priority). The default priority for an event in an exception schedule is five more than the priorities of events in the daily schedule. For example, if you created an event with a priority of 255 in the daily schedules, the events in the exception schedule will have a priority of 250. This priority locks out events with lower priorities so that they cannot update the data points written to by this event until the exception ends. If you are creating the sunrise/sundown events in a one-time exception, lower-priority events can update the data points as soon as the sunrise/sundown event ends.
7. Click **OK** to save your sunrise/sundown events. Click **Cancel** to delete all changes. If you are creating an exception, click **OK** to save your changes to the **Edit: <exception date>** dialog and return to the **Scheduler: Exception Schedules** Web page. Click **Cancel** to delete all changes and return to the **Scheduler: Exception Schedules** Web page.
 8. Click **Submit**.

Demonstrating Sunrise and Sundown Events

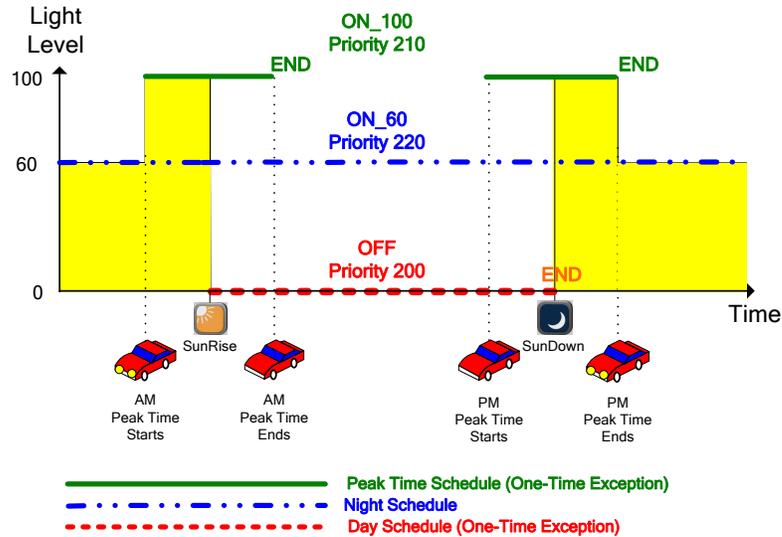
The following section demonstrates how to create overlapping one-time exceptions and exception schedules that use sunrise and sundown events to control the lighting in a public parking garage.

Every event in the Event Scheduler has a priority (0 to 255) that determines which data point updates are executed. After a Scheduler executes an event and updates a data point, only equal or higher priority events can update that data point. The priority therefore functions as a lock that prevents lower priority events from updating a data point after it has been written to by an earlier event.

For example, Scheduler 1 executes an OFF event in an exception with a priority of 200 that updates a **SNVT_switch** data point to 0.0 0. Sometime thereafter, Scheduler 2 attempts to execute an ON_60 event in an exception with a priority of 210 that updates the same **SNVT_switch** data point to 60.0 0. In this case, the data point remains OFF because the ON_60 event (210 priority) has a lower priority than the OFF event (200 priority). For the ON_60 event to update the data point in the previous example, its priority must be between 0 and 200 (if both events have the same priority, the second event updates the data point).

Alternatively, you can create the OFF event in a one-time exception in Scheduler 1. This would enable the lower priority ON_60 event to update the **SNVT_switch** data point. When the OFF events ends, its priority is reset to 255, which releases its lock on the **SNVT_switch** data point. The highest-priority event that was scheduled to occur prior to the OFF event then executes. If there are no such events, the next highest-priority event will execute at its scheduled time. Creating events in a one-time exception therefore enables lower priority events to write updated values to the data points. This lets you to overlap events in daily and exception schedules, and ultimately allows you to create an Event Scheduler that provides a single solution for a number of different scenarios.

The following graphic illustrates how to overlap one-time exceptions and exception schedules that use sunrise and sundown events.



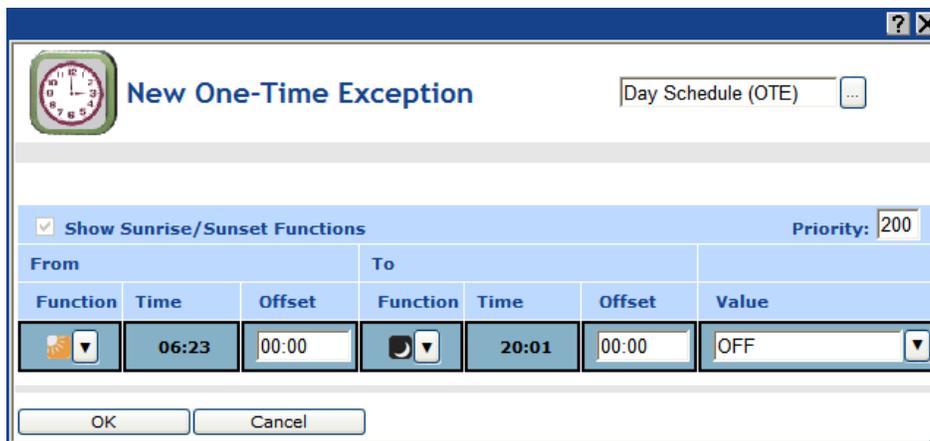
In this example, three recurring exceptions are used in a single Event Scheduler to turn off, turn on, brighten, and dim a luminaire through its **SNVT_switch** data point: the Day Schedule (OTE) turns off the luminaire every day, the Peak Time Schedule (OTE) turns on the luminaire and sets its brightness to 100% every weekday, and the Night Schedule dims the luminaire to 60% every day.

Note: In this example, additional user-defined presets have been created for the **SNVT_switch** data point on the luminaire. These presets include ON_60 and ON_100, which set the **SNVT_switch** data point to 60.0.1 (60% brightness and on) and 100.0 1 (100% brightness and on), respectively. These presets are used in addition to the pre-defined OFF preset, which sets the **SNVT_switch** data point to 0.0.0 (0% brightness and off). See the *Selecting Data Points* section earlier in this chapter for more information on creating presets for data points that have been added to the Event Scheduler.

Creating the Day Schedule (One-Time Exception)

The example Day Schedule (OTE) turns off the luminaire at sunrise. Designing the Day Schedule (OTE) entails creating a one-time exception that recurs every day with a single event:

1. An OFF event with a 200 priority that is scheduled to start at sunrise and end at sundown. At sunrise, this event sets the luminaire's **SNVT_switch** data point to 0.0 0, turning the luminaire off. The OFF event executes because its priority (200) is higher than that of the current ON_60 event (220) or ON_100 event (210). At sundown, the OFF event ends, which resets its priority to 255 and releases its lock on the luminaire's **SNVT_switch** data point. The highest-priority event occurring prior to the OFF event (if any) is executed. If there are no such events, the next highest-priority event will execute at its scheduled time.

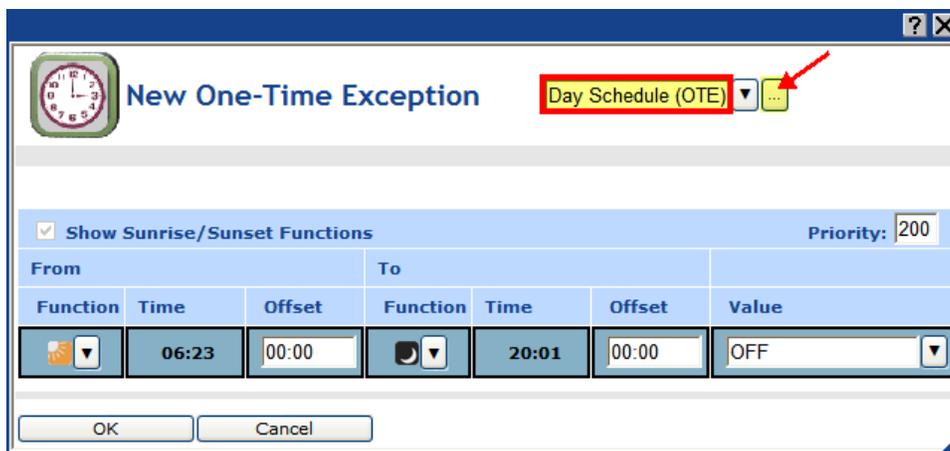


Tip: To create a recurring one-time exception, follow these steps:

1. Create a new one-time exception from the **Scheduler: Exception Schedules** Web page.



2. In the **New One-Time Exception** dialog, enter a descriptive name for the exception in the box at the top of the dialog and then click the box to the right of the one-time exception name to open the **Edit Exception** dialog.



3. In the **Edit Exception** dialog, confirm the start date of the exception, set the end date, click the **Standard** or **Specific** option, and then set the desired recurrence. For this example, click the **Standard** option, and then select **Every Year**, **Every Month**, and **Every Day** for the year, month, and day in the **To** property because this exception recurs every day.



The following graphic demonstrates the exception schedule with the events of the Day Schedule (OTE). This exception schedule will be updated as the Night Schedule and Peak-Time Schedule (OTE) exceptions are created.

Time	Schedule	Event Time	Value	Priority
00:00				
01:00				
02:00				
03:00				
04:00				
05:00				
06:00	Day Schedule (OTE)	06:23	OFF	200
07:00				
08:00				
09:00				
10:00				
11:00				
12:00				
13:00				
14:00				
15:00				
16:00				
17:00	Day Schedule (OTE)	17:02		255
	Weekday	17:02		255
18:00				
19:00				
20:00				
21:00				
22:00				

Creating the Peak Time Schedule (One-Time Exception)

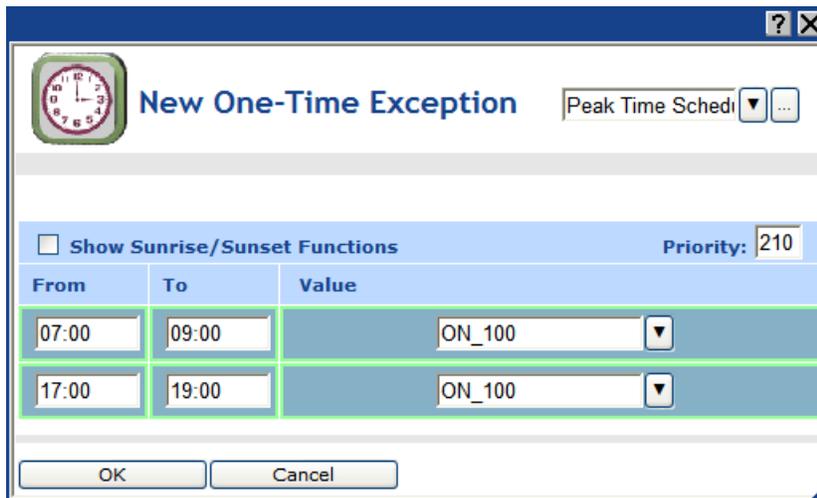
The Peak Time Schedule (OTE) turns on the luminaire and sets the brightness at 100%. Designing the Peak Time Schedule (OTE) entails creating a one-time exception that recurs every weekday with the following events:

1. An ON_100 event with a 210 priority that is scheduled to start at the beginning of the morning peak time (07:00 in this example) and end at the conclusion of the morning peak time (09:00 in this example). If or when this event actually occurs depends on the calculated sunrise time.
 - If the start of the morning peak time occurs before sunrise, the ON_100 event is executed and brightens the lights from 60% to 100%. This is because the priority of the ON_100 event in the Peak Time Schedule (210) is higher than that of the current ON_60 event in the Night Schedule (220).
 - If the start of the morning peak time occurs after sunrise, the ON_100 event is not executed. This is because the ON_100 event in the Peak Time Schedule has a lower priority (210) than

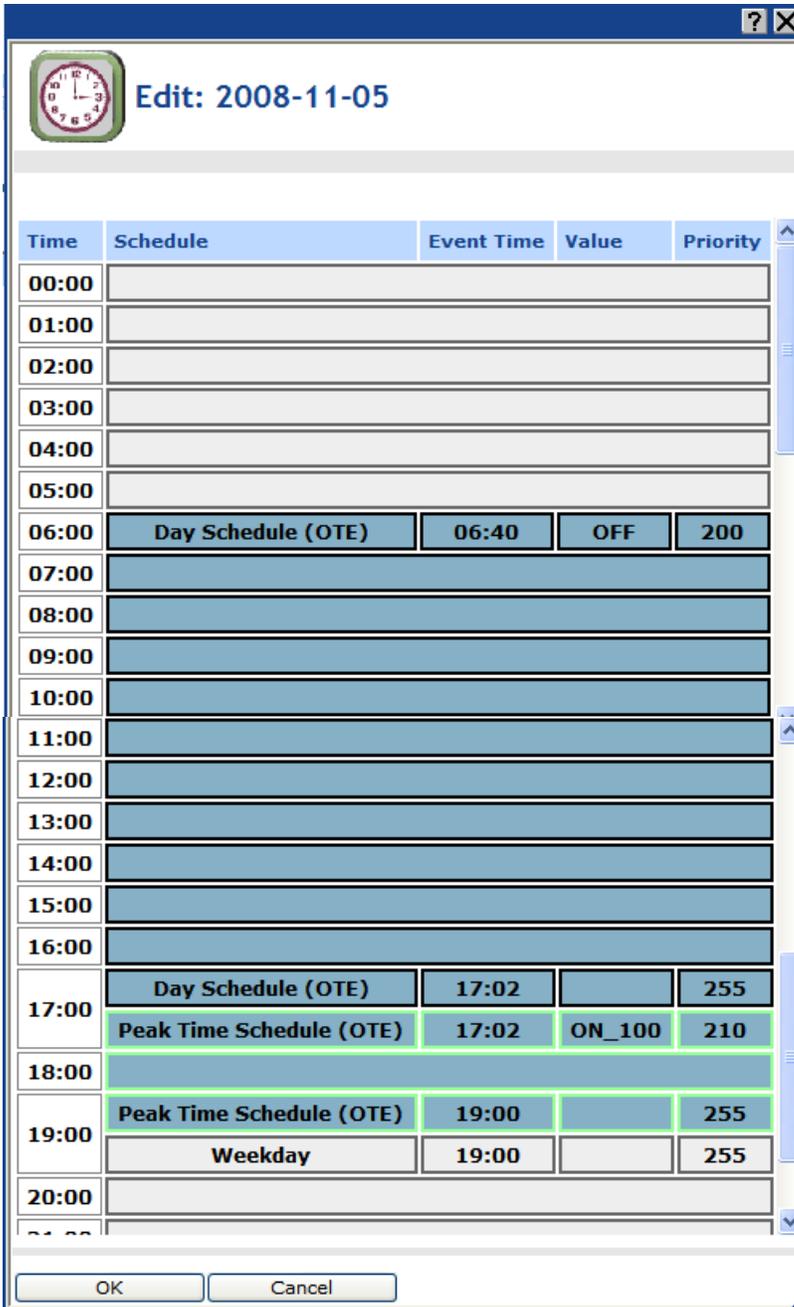
that of the OFF event in the Day Schedule (200), which occurs at sunrise. Essentially, starting at sunrise, the Day Schedule locks out events that have priorities lower than 200. It maintains the lock until the OFF event ends at sundown.

At the end of the morning peak time, the ON_100 event ends, which resets its priority to 255 and releases its lock on the luminaire's **SNVT_switch** data point. This is only relevant if sunrise occurs after the end of the morning peak time. In this case, the resetting of the data point priority enables the ON_60 event in the Night Schedule to dim the lights back to 60% and keep them at that level until sunrise.

2. An ON_100 event with a 210 priority that is scheduled to start at the beginning of the evening peak time (17:00 in this example) and end at the conclusion of the evening peak time (19:00 in this example). If or when this event actually occurs depends on the calculated sundown time.
 - If the start of the evening peak time occurs before sundown, the ON_100 event is not executed until sundown. This is because the ON_100 event in the Peak Time Schedule has a lower priority (210) than that of the OFF event in the Day Schedule (200), which does not end until sundown. Once the OFF event in the Day Schedule ends at sundown, the ON_100 event is executed and the lights are turned on and fully illuminated to 100%. The ON_100 event is executed instead of the ongoing ON_60 event in the Night Schedule because its priority (210) is higher than that of the ON_60 event (220).
 - If the start of the evening peak time occurs after sundown, the ON_100 event is executed and brightens the lights from 60% to 100%. This is because the priority of the ON_100 event in the Peak Time Schedule (210) is higher than that of the current ON_60 event in the Night Schedule (220). The ON_60 event in the Night Schedule was executed at sundown, when the OFF event in the Day Schedule ended.
 - If the end of the evening peak time occurs before sundown, the ON_100 event is never executed. This is because the ON_100 event in the Peak Time Schedule has a lower priority (210) than that of the ongoing OFF event in the Day Schedule (200) and is locked out until the OFF event ends, which it is not scheduled to do until sundown. When the OFF event in the Day Schedule does end at sundown, the ON_100 event has already expired; therefore, the only active event, the ON_60 event in the Night Schedule, executes.



The following graphic demonstrates the exception schedule with the events of the Day Schedule (OTE), and the Peak-Time Schedule (OTE).



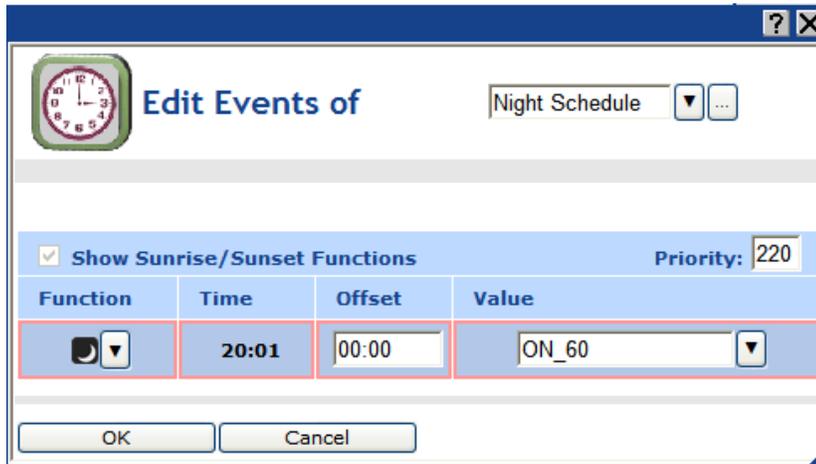
Note: To account for weekday holidays in this example, create an exception group that includes all such holidays. The exception group requires a priority of 205 (a priority that is higher than that of the Peak Time Schedule, but lower than that of the Day Schedule) so that it can prevent the Peak Time Schedule from brightening the lights to 100% at the normal peak time times, yet allow the Day Schedule to turn off the lights. The schedule used by the exception group is a copy of the Peak Time Schedule—but has ON_60 events in the place of the ON_100 events in the Peak Time Schedule.

Creating the Night Schedule

The Night Schedule turns on the luminaire and sets it to 60%, and it dims the luminaire from 100% to 60%. To create a Night Schedule, create an exception schedule with a single event as follows:

1. Create an ON_60 event that is scheduled at sundown with a 220 priority. The time at which this event actually executes depends on when the end of the evening peak time occurs. This is because

the priority of the ON_60 event in the Night Schedule (220) is lower than that of the ON_100 event in the Peak Time Schedule (210). The Night Schedule is therefore locked out until the ON_100 event in the Peak Time Schedule ends at the conclusion of the evening peak time.



- Once the ON_100 event in the Peak Time Schedule ends at the conclusion of the evening peak time, the Night schedule executes its ON_60 event, setting the luminaire to 60%. The luminaire remains at 60% until the morning peak time starts or sunrise, whichever comes first.
- If the start of the morning peak time comes before sunrise, the Peak Time Schedule executes its higher-priority ON_100 event at the start of peak time and fully illuminates the luminaire to 100%. If the end of the morning peak time occurs before sunrise, the Night Schedule dims the luminaire back to 60% once the Peak Time Schedule ends at the conclusion of the morning peak time. The luminaire stays at 60% until the Day Schedule executes its higher-priority OFF event at sunrise and turns the luminaire off.
- If sunrise comes before the start of the morning peak time, the Day Schedule executes its higher-priority OFF event at sunrise and turns the luminaire off.

The following graphic demonstrates the exception schedule with the events of the Day Schedule, Peak-Time Schedule, and Night Schedule.


Edit: 2008-11-05

Time	Schedule	Event Time	Value	Priority
00:00				
01:00				
02:00				
03:00				
04:00				
05:00				
06:00	Day Schedule (OTE)	06:40	OFF	200
07:00				
08:00				
09:00				
10:00				
11:00				
12:00				
13:00				
14:00				
15:00				
16:00				
17:00	Day Schedule (OTE)	17:02		255
	Peak Time Schedule (OTE)	17:02	ON_100	210
18:00				
19:00	Peak Time Schedule (OTE)	19:00		255
	Night Schedule	19:00	ON_60	220
20:00				
21:00				

Using the Event Calendar

The Event Calendar lists and displays all the exceptions created in all the Event Scheduler on the SmartServer. You can use the Event Calendar to create one-time exceptions, exceptions, and recurring exceptions and apply them to all the Event Schedulers on the SmartServer and you can use the Event Calendar to edit and delete existing exceptions.

Note: After you create exceptions in the Event Calendar, click the **Exception Schedules** icon in the **Scheduler: Configure Web** page to create the schedules for the exceptions.

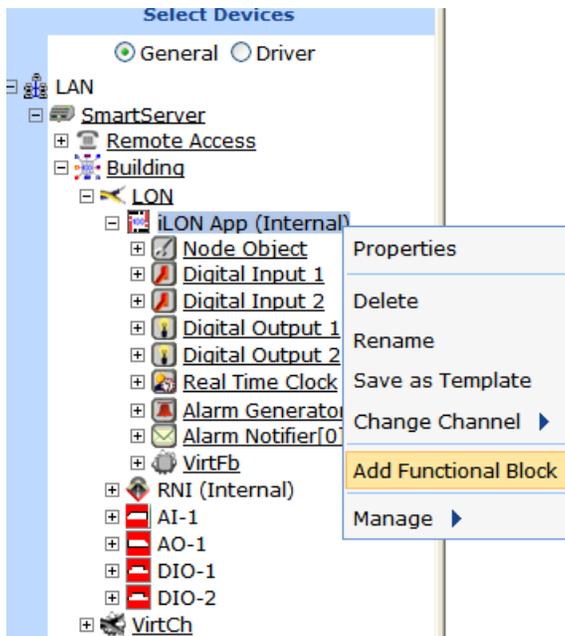
Opening the Event Calendar

The Event Calendar lists and displays all the exceptions created in all the Event Scheduler on the SmartServer. You can open the Event Calendar from the SmartServer tree or from within an Event Scheduler. To open the Event Calendar from within an Event Scheduler, click the **Event Calendar** icon in the **Scheduler: Configure Web** page.

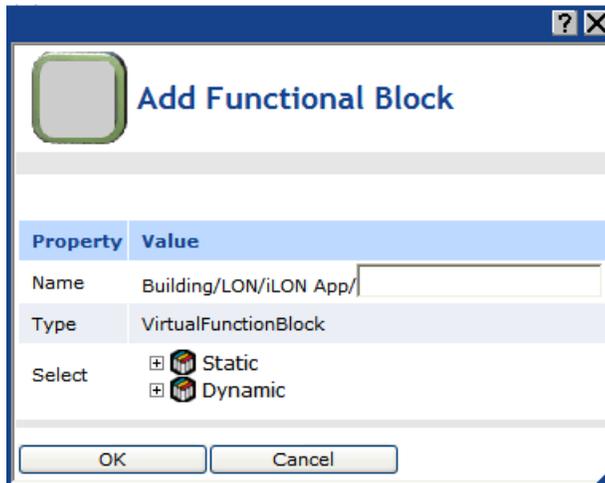


To open the Event Calendar from the SmartServer tree, follow these steps:

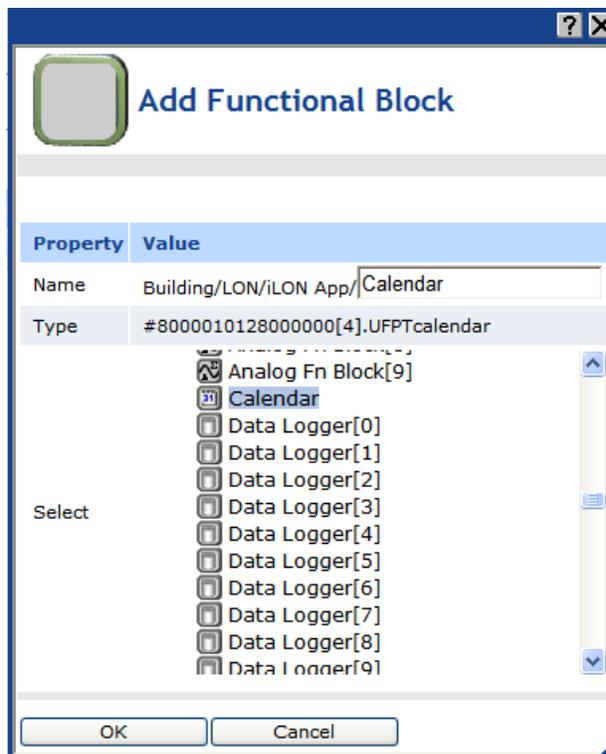
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



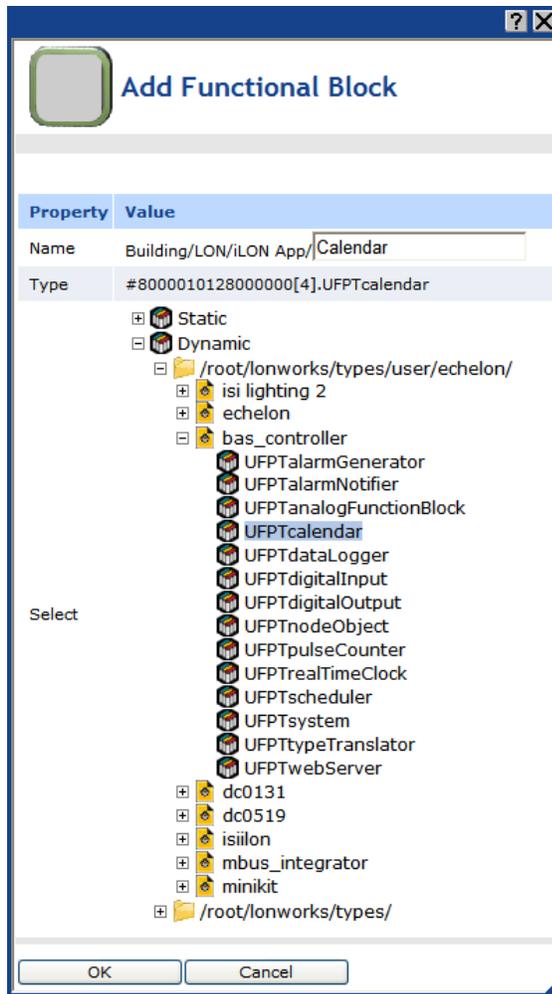
4. The **Add Functional Block** dialog opens.



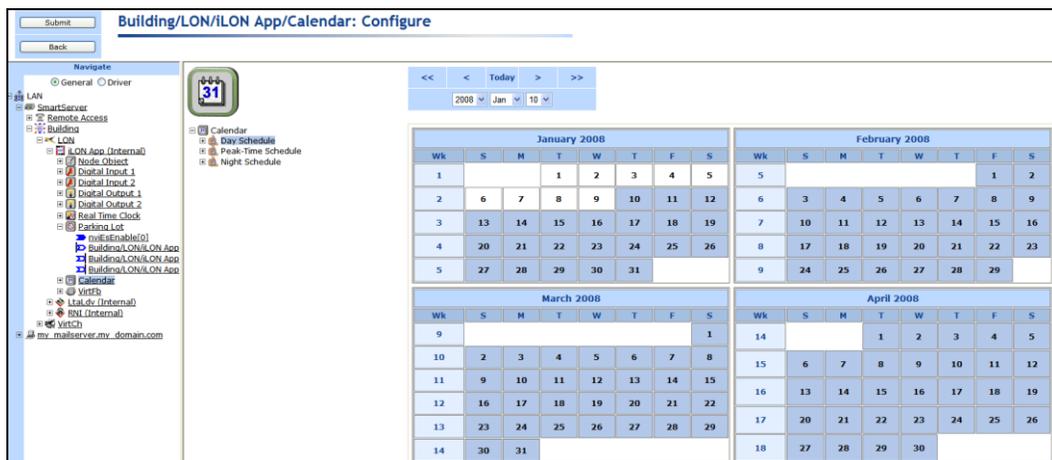
5. Select the Event Calendar functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the default static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Event Calendar** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Scheduler functional block from either the **Static** or the **Dynamic** folder. To select the Scheduler functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the Event Calendar, enter a name for the functional block such as “Calendar”, and then click **OK**.



6. A functional block representing the Event Calendar and all of its static data points are added to the bottom of the **iLON App (Internal)** device tree, and the **Event Calendar: Configure** Web opens in the application frame to the right. The construction symbol overlaid onto the Scheduler application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



7. Click **Submit**.

To open the Event Calendar application from an existing Calendar functional block, follow these steps:

1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Calendar application.
2. Click the Calendar functional block. The **Calendar: Configure** Web page opens in the application frame to the right.

Viewing Exceptions in the Event Calendar

The left side of the Event Calendar lists the names of all the exceptions in the Schedulers on your SmartServer. The scope of the exception is indicated by the icon to the left of the exception name. If the exception is public, the following icon appears next to the exception (🌐); if the exception is private, the following icon appears next to the exception (🔒). You can view the dates of the exception by clicking the exception. The dates in the exception are then highlighted in the calendar on the right side.

Building/LON/iLON App/Calendar: Configure

Calendar navigation: << < Today > >> 2008 Jan 10

Left sidebar:

- Calendar
- Day Schedule
- Peak-Time Schedule
- Night Schedule

January 2008							February 2008								
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S
1			1	2	3	4	5	5						1	2
2	6	7	8	9	10	11	12	6	3	4	5	6	7	8	9
3	13	14	15	16	17	18	19	7	10	11	12	13	14	15	16
4	20	21	22	23	24	25	26	8	17	18	19	20	21	22	23
5	27	28	29	30	31			9	24	25	26	27	28	29	

For exceptions created in an Event Scheduler, you can expand them to show the Event Scheduler in which they were created. You can then click the Event Scheduler shown to open the corresponding Scheduler application.

Building/LON/iLON App/Calendar: Configure

Calendar navigation: << < Today > >> 2008 Jan 10

Left sidebar:

- Calendar
- Day Schedule
 - Building/LON/iLON App/Parking Lot
- Peak-Time Schedule
- Night Schedule
 - Building/LON/iLON App/Parking Lot

January 2008							February 2008								
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S
1			1	2	3	4	5	5						1	2
2	6	7	8	9	10	11	12	6	3	4	5	6	7	8	9
3	13	14	15	16	17	18	19	7	10	11	12	13	14	15	16
4	20	21	22	23	24	25	26	8	17	18	19	20	21	22	23
5	27	28	29	30	31			9	24	25	26	27	28	29	

Creating Exceptions in the Event Calendar

You can create an exception or recurring exception in the Event Calendar to apply an alternate schedule to a specific range of dates to all the Event Schedulers on the SmartServer. To create an exception in the Event Calendar, follow these steps:

1. Click the date in the calendar that will be the start date for the exception schedule. Alternatively, you can right-click the start date in the calendar, and then click **Add Exception** on the shortcut menu.
2. The **New Exception** dialog opens.



3. Enter the name, scope, dates, and recursions for the exception; click **Close** to return to the **Calendar: Configure** Web page; and then click **Submit**. See *Creating Exception Dates in the Exception Schedule* earlier in this chapter for more information on how to create an exception and set the range of dates and recursions for it in this dialog.
4. Click **OK** to add the exception and return to the **Calendar: Configure** Web page (click **Cancel** to discard all changes and return to the **Calendar: Configure** Web page). The exception is added under the Calendar icon and the range of dates specified in the **New Exception** dialog are highlighted blue in the Event Calendar.
5. You can create the schedule for the exception in an Event Scheduler. To do this, follow these steps:
 - a. Open the Scheduler in which the exception is to be used.
 - b. In the **Scheduler: Configure** Web page, click the Exception Schedules icon. The **Scheduler: Exception Schedules** Web page opens.
 - c. Right-click anywhere in the exception schedule, point to **Add Exceptions**, point to **From Calendar**, and then click the exception created in the Calendar.

Building/LON/iLON App/Scheduler[0]: Exception Schedules

The screenshot shows the 'Exception Schedules' interface. At the top, there are navigation buttons for '<<', '<', 'Today', '>', and '>>'. Below these are dropdown menus for the year (2008), month (Aug), and day (14). The main area contains two calendar grids: 'August 2008' and 'September 2008'. The 'August 2008' calendar has a context menu open over the date 31. The menu options are: 'Add Exception', 'Edit Exceptions', 'Delete Exception', and 'Edit Daily Schedules'. A sub-menu is also open, showing options: 'New One-Time Exception', 'New Exception', 'New Exception Group', and 'From Calendar'. The 'From Calendar' option is highlighted in yellow. To the right, a list of exceptions is visible, including 'Inventory', 'LaborDay', 'MemorialDay', 'Thanksgiving', 'FourthofJuly', and 'Calendar Exception'.

- d. The **Edit Exceptions** dialog opens. Optionally, you can edit the name, scope, dates, and recursions of the exception. See *Creating Exception Dates in the Exception Schedule* earlier in this chapter for more information on configuring the properties in this dialog.
- e. Click **OK** to save any changes to the exception and return to the **Scheduler: Exception Schedules** Web page.
- f. Click **Submit**.
- g. Click one of the light blue-highlighted dates in the exception to specify the events for the exception. The **Edit: <exception date>** dialog opens.
- h. Add events to the exception. See *Creating Exception Events in the Exception Schedule* earlier in this chapter for more information on how to do this.

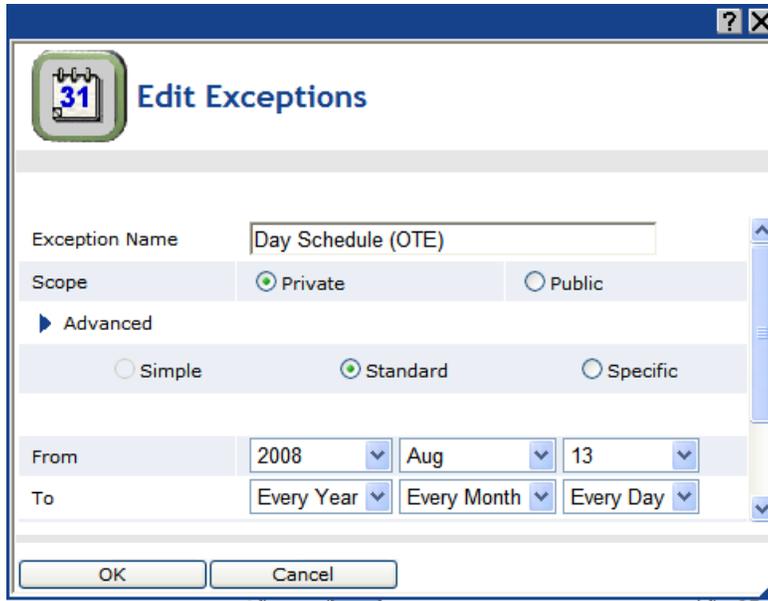
Editing Exceptions in the Event Calendar

After you create a one-time exception, exception, or recurring exception in an Event Scheduler or the Event Calendar, you can edit it. To edit an exception in the Event Calendar, follow these steps:

1. Right-click the exception to be edited under the Calendar icon and then click **Edit** '<Exception Name>' on the shortcut menu.

The screenshot shows the 'Calendar: Configure' interface. At the top, there are navigation buttons for '<<', '<', 'Today', '>', and '>>'. Below these are dropdown menus for the year (2008), month (Jan), and day (10). The main area contains two calendar grids: 'January 2008' and 'February 2008'. The 'January 2008' calendar has a context menu open over the date 31. The menu options are: 'Edit Day Schedule' and 'Delete Day Schedule'. On the left, there is a tree view showing a 'Calendar' icon and a list of items: 'Day Schedule', 'Peak-Time Schedule', and 'Night Schedule'. The 'Day Schedule' item is selected and highlighted.

2. The **Edit Exceptions** dialog opens.

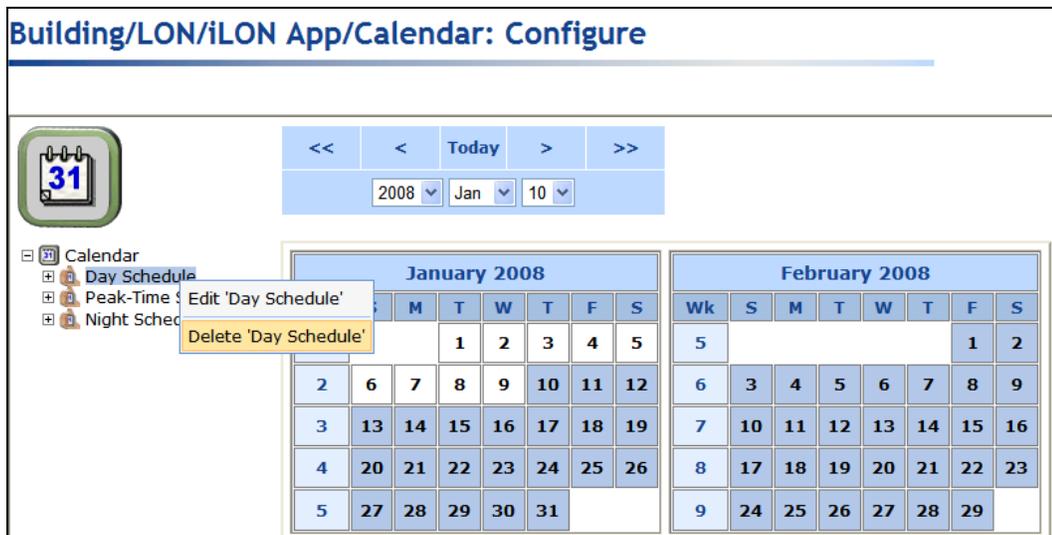


3. Edit the name, scope, dates, and recursions of the exception and any other instances created under this exception. See *Creating Exception Dates in the Exception Schedule* earlier in this chapter for more information on configuring the properties in this dialog.
4. Click **OK** to save changes to the exception and return to the **Calendar: Configure** Web page. Click **Cancel** to discard all changes and return to the **Calendar: Configure** Web page.
5. Click **Submit**.

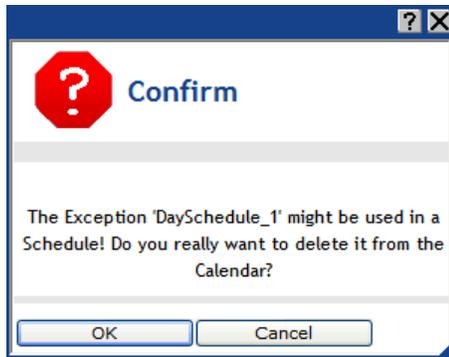
Deleting Exceptions in the Event Calendar

You can use the Event Calendar to delete a one-time exception, exception, or recurring exception in an Event Scheduler or the Event Calendar. To delete an exception from the Event Calendar, follow these steps:

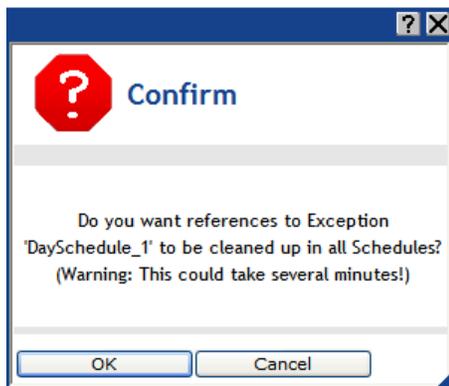
1. Right-click the exception to be edited under the Calendar icon and then click **Delete** <'Exception Name'> on the shortcut menu.



2. A message appears reminding you that a Scheduler might be using the exception to be deleted from the Event Calendar.



3. Click **OK** to delete the exception from the Scheduler.
4. A message appears asking you whether references to the exception to be deleted should be cleaned up in all Schedulers on the SmartServer.



5. Click **OK** to cleanup references to the exception. Click **Cancel** to keep references to the exception in the Event Calendar.
6. Click **Submit**.

Data Logging

This chapter describes how to use the Data Logger on the SmartServer to record data point updates. It describes how to create historical and circular data loggers. It describes how to automatically transfer data log files to a remote server and extract them to a CSV or XML file. It explains how to view data logs using the **Data Logger: View** Web page, and how to monitor and control data points using the **View – Data Points** Web page.

Data Logging Overview

The SmartServer contains a Data Logger application that you can use to record data point values and store them to a log file. To use a data logger, you select the type of log file to store the data point values (historical or cyclical), select the data points to be tracked, and then select the method used to record data point values (polling and/or event-driven updates). You can also have the data logger trigger an alarm when the log file is becoming full. You can view log entries using the **Data Logger: View** Web page. You can also view, chart, and update data points using the **View – Data Points** Web page.

You store data point values in a historical or circular log. A historical log stops recording data point updates when the log file is full. A circular log file removes the records for older updates when new updates occur and the log file is full. You can save the historical and circular logs to an ASCII text (.csv) or binary (.bin) file. In addition, you can save a historical log as a compressed ASCII text (.csv.gz) file. Saving a historical log to a .csv.gz file reduces the size of the log to approximately half of that of the .csv file. To view a log in a compressed ASCII text file, you just extract the .csv file from the .csv.gz file. By default, the log file is stored in the `/data/Net/LON/i.LON App (Internal)` folder, and it is named **Data Logger [x]**, where *x* is the index number of the Data Logger functional block. You can remove data from a log file by specifying a percentage of the log file to be cleared, sending an update to the clear point on the data logger (**nviDIClear[x]** data point, where *x* is the index number of the data logger).

For each data point you are tracking, you can select whether the data logger uses polling and/or event-driven updates to record its value. With event-driven updates, the data point is only recorded when its value is updated. You can filter event-driven updates by specifying a minimum period of time that must elapse between log entries and the minimum change in value required between log entries to record the data point. With polling, the data point value is recorded at a specified rate, regardless of any event-driven filters that you may have set.

You can also have the data logger trigger an alarm when the log file is becoming full. To do this, you specify a limit for the log file that, when reached, causes the data logger to trigger an alarm. You can have an Alarm Notifier monitor the alarm data point and send a notification when the data point receives an alarm condition. This is particularly useful if you are using a historical log file because it becomes disabled once it is full.

You can have the SmartServer automatically transfer data log files (binary or CSV format) to a remote server and extract the selected data to a CSV or XML file. You can view and chart log entries using the **Data Logger: View** Web page. You can access the data in a log by manually opening the log file or by using a SOAP function. You can also monitor, chart, and control data point using the **View – Data Points** Web page.

You can create up to 10 Data Loggers per SmartServer if you are using the default SmartServer v12 static interface. You can add more than 10 Data Loggers if you activate the v40 dynamic interface, which features a dynamic external interface, on your SmartServer. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

Creating a Data Logger

To create a Data Logger, do the following:

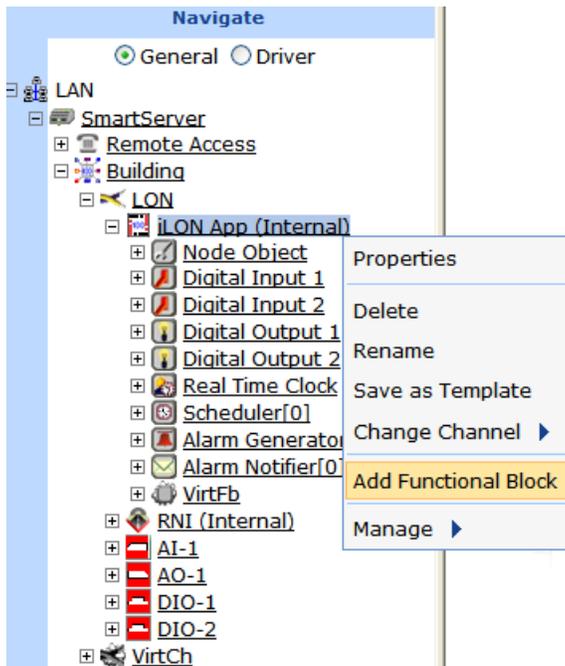
1. Open a Data Logger application.
2. Select and configure a log file.
3. Select and configure the data points to be logged.
4. Set the alarm limit.

Opening a Data Logger Application

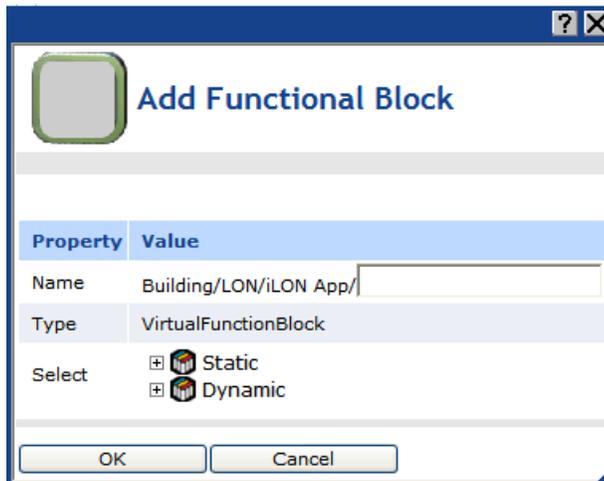
To open a Data Logger application, first create a Data Logger functional block. After you create the Data Logger functional block, the functional block appears on the SmartServer tree below the **i.LON App (Internal)** device, and you can click the functional block to open the Data Logger application.

To create a Data Logger functional block and open the application, follow these steps:

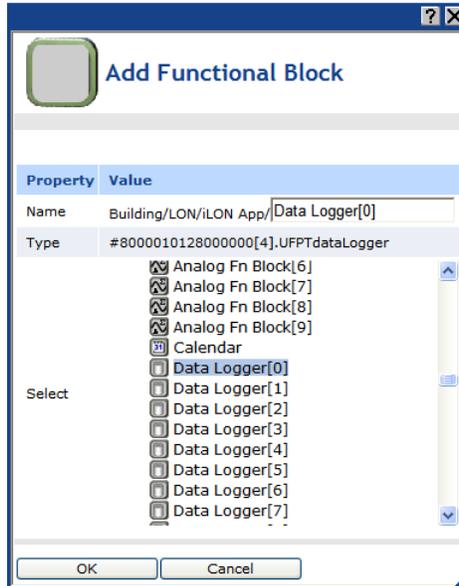
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



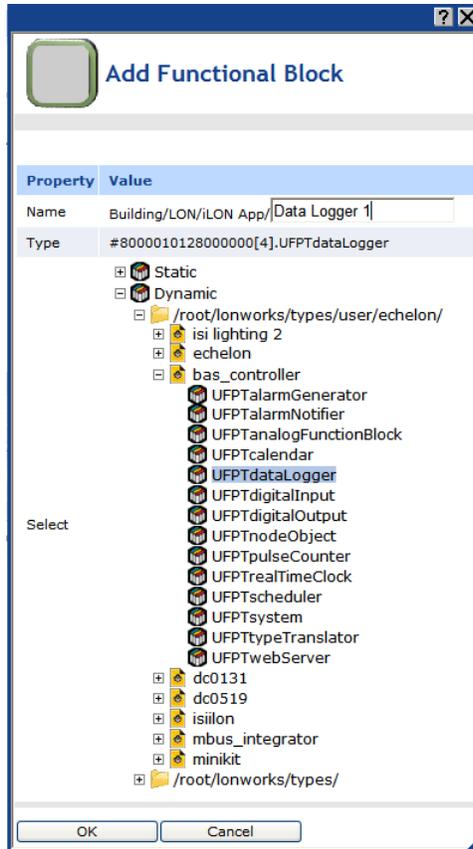
4. The **Add Functional Block** dialog opens.



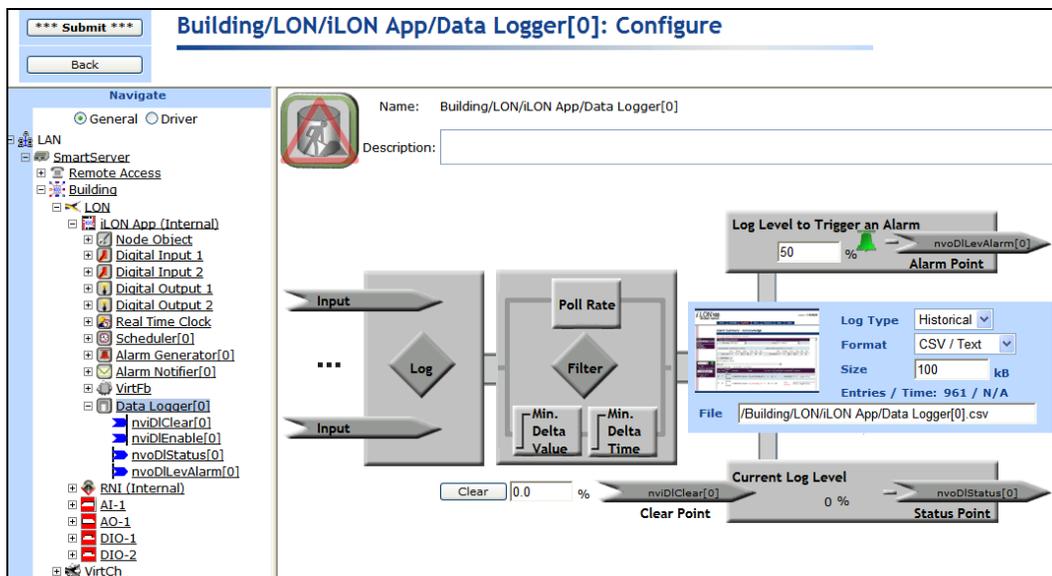
5. Select the Data Logger functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Data Logger** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Data Logger functional block from either the **Static** or the **Dynamic** folder. To select the Data Logger functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the Data Logger, enter a name for the functional block such as “Data Logger 1”, and then click **OK**.



6. A functional block representing the Data Logger application and all of its static data points are added to the bottom of the **i.LON App (Internal)** device tree, and the **Data Logger: Configure** Web page opens in the application frame to the right. The construction symbol overlaid onto the Data Logger application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



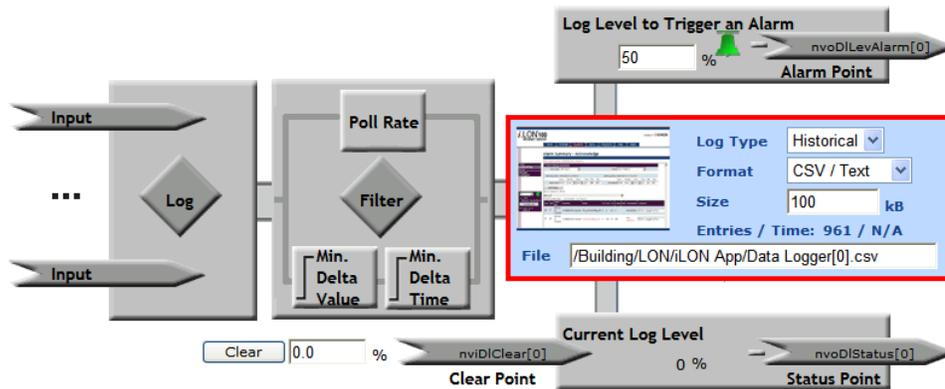
7. Click **Submit**.

To open the Data Logger application from an existing Data Logger functional block, follow these steps:

1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Data Logger application.
2. Click the Data Logger functional block representing the Data Logger to be opened. The **Data Logger: Configure** Web page opens in the application frame to the right.

Selecting and Configuring a Log File

In the log file box in the **Data Logger: Configure** Web page, you can select the type of log file used to record data point values; select the format of the log file; enter the maximum file size; and enter the location to which the log files are stored on the SmartServer flash disk.



To select and configure a log file, follow these steps:

1. In the **Log Type** list, select whether to store data point values in a **Historical** or **Circular** log.
 - A **Historical** log stops recording data point updates when the log file is full. This is the default log type.
 - A **Circular** log file removes the records for older updates when new updates occur and the log file is full.
2. In the **Format** list, select the format of the log file.
 - Select **CSV/ text** to save the log file as an ASCII text file (.csv extension). Each entry in a log using this format consumes approximately 0.2 KB. A CSV (comma separated value) file is a text file that can be read by any application that can read text files. You can view a CSV file by importing into a spreadsheet application such as Microsoft Excel. This is the default file format.
 - Select **CSV - zipped** to save the log file as a compressed ASCII text file (.csv.gz extension). This format is only available for historical log files. Each entry in a log using this format consumes approximately 0.008 KB. A compressed CSV file conserves space on the SmartServer flash disk. You can view a compressed CSV file by extracting it from the .csv.gz file and then importing it into a spreadsheet application such as Microsoft Excel.

Removing a data point from a compressed data log or deleting a specific interval within a compressed data log will decompress the log file. If the SmartServer does not have enough memory to store a decompressed log file in RAM, it will not allow the action that would cause the log file to be decompressed, and it will report an error in the system logger. Always ensure that there is enough free space in the SmartServer RAM to decompress the log file when removing data points or portions of a compressed data log. The estimated required RAM to decompress a log file is as follows:

- **CSV/text.** Approximately 2 times the size of the log file.
- **CSV - zipped.** Approximately 10–20 times the size of the log file.
- **Binary.** Approximately 20–30 times the size of the log file.

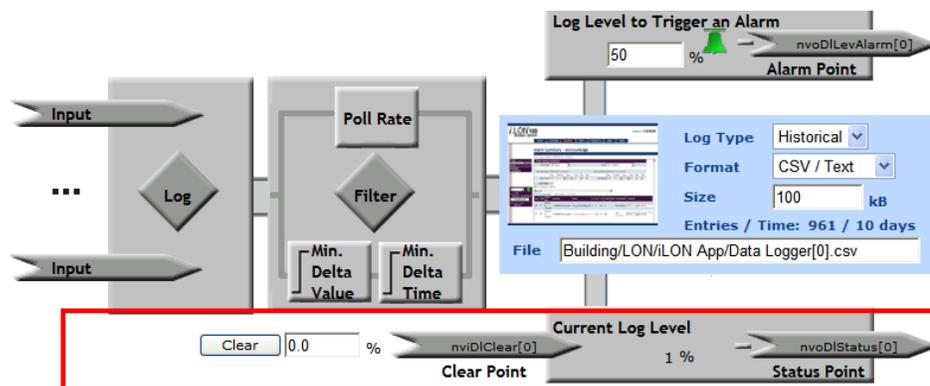
Log files must be no larger than 1 MB.

- Select **Binary** to save the log file as a binary data file (.bin extension). Each entry in a log using this format consumes approximately 0.032 KB. You can only view a binary file with the **Data Logger: View** Web page.
3. In the **Size** box, enter the maximum size of the log file. The file size determines the number of entries the log file can store. The default maximum file size is **100 KB**. When you enter a size, the maximum number of entries that the log can store is displayed directly underneath the box.

Although the SmartServer does not limit how much data can be logged, you must maintain at least 1,024 KB of free space on the SmartServer server flash disk. To view the amount of free disk space on the SmartServer right-click the SmartServer, point to **Setup**, and then click **System Info** on the shortcut menu. The **Setup – System Info** Web page opens. In the **General Statistics** section, check the **Free disk space / Total disk space** property.

4. In the **File** box, enter the full path to which the log file is stored on the SmartServer flash disk. By default, the log file is stored in the **/data/Net/LON/i.LON App** folder, and it is named Data Logger [x], where x is the index number of the data logger.
5. Click **Submit**.

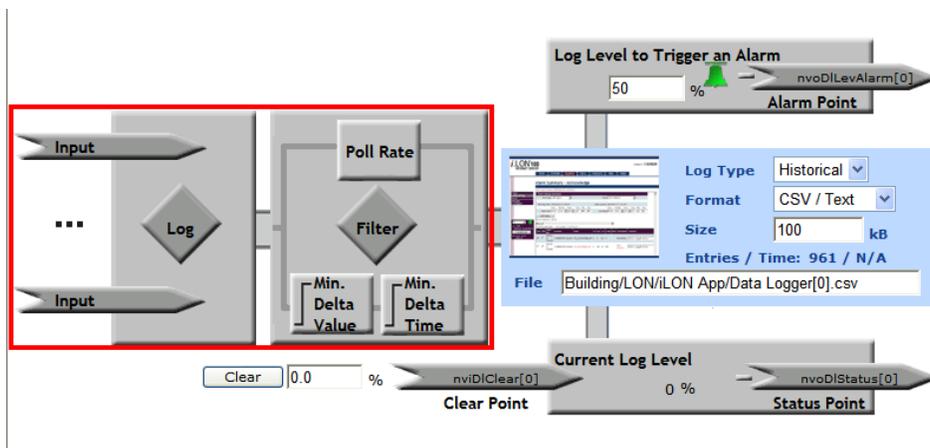
Note: You can remove data from a log file using the **Data Logger: Configure** Web page. To do this, enter a percentage of the log file to be cleared in the box directly below the data point **Filter** box and then click **Clear**. This updates the clear data point on the data logger (**nviDIClear[x]**, where x is the index number of the data logger) and removes the specified percentage of data from the log file. For example, if your data log is only 30% full, entering 60.0 will clear your entire log. If your data log is 90% full, entering 60.0 will leave the log 30% full. Entering 100.0 and then clicking **Submit** erases all logged data. You cannot clear a data log while the logging is disabled.



Selecting and Configuring Data Points

You can specify the data points to be recorded by the Data Logger application. After you select the data points, you can specify whether the data logger uses polling and/or event-driven updates to record their values.

1. In the **Data Logger: Configure** Web page, click anywhere in the **Log** or **Filter** boxes.



2. The **Data Logger: Data Points** Web page opens. Select the data points to be recorded by the Data Logger from the SmartServer tree. References to the selected data points (🔗) are added to the bottom of the Data Logger functional block tree, and references to the Data Logger functional block are added directly below the selected data points (🔗).

To record a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).

Show Advanced			
Data Point	Poll Rate	Unit	
0 Building/LON/AI-1/Analog Input[0]/AI_Analog_1	15min	°C	
1 Building/LON/DIO-1/Digital Output[0]/DO_Digital_1	15min	% of full level	

3. View the following properties of the selected data points:

- Data Point** Displays the name of the data point being recorded using the following format: `<network>/<channel>/<device>/<functional block>/<data point>`. This is also the location of the data point in the SmartServer tree.
- Poll Rate** Displays the rate at which the data logger records the value of the selected data point. The default rate is **15** minutes. If the poll rate is set to 0, the data point will only be logged when its value changes.
- Unit** Displays the unit string describing the data point to be updated. A **SNVT_temp_f** data point, for example, has “degrees F” describing the data point. A **SNVT_switch** data point has “% of full level” and “state code” unit strings describing its state and value fields. This field is read-only. You can edit the unit string of a data point in the **Configure - Data Points** Web

page, which you can access by clicking the data point in **General** mode.

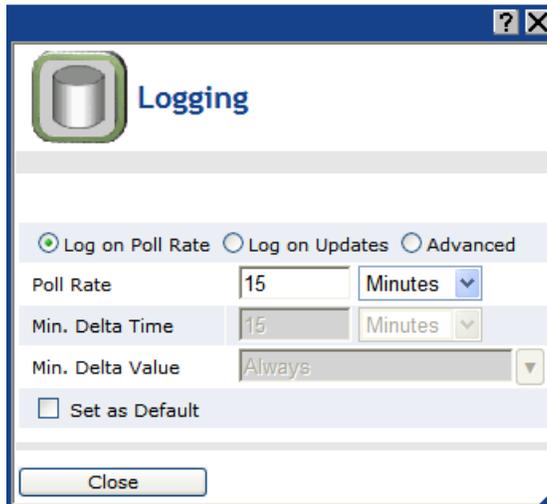
4. Select the **Show Advanced** check box to view the following properties used to configure the frequency in which data is logged.

Building/LON/iLON App/Data Logger[0]: Data Points					
<input checked="" type="checkbox"/> Show Advanced					
	Data Point	Poll Rate	Min. Delta Time	Min. Delta Value	Unit
0	Building/LON/AI-1/Analog Input[0]/AI_Analog_1	15min	15min	Always	°C
1	Building/LON/DIO-1/Digital Output[0]/DO_Digital_1	15min	15min	Always	% of full level

Minimum Delta Time Displays the minimum period of time that must elapse between log entries. The default value is **15** minutes. This means that the data logger will record the data point's value every 15 minutes.

Minimum Delta Value Displays the minimum change in value required between log entries to record the data point. If this property is set to 0, the data logger records the data point every time its value changes, regardless of the amount of change.

5. To configure how the data logger records the values of the selected data points, click the **Poll Rate** or **Min. Delta Time** box for any data point. The **Logging** dialog opens.



6. Select whether the data logger uses polling and/or event-driven updates to record the values of the selected data points.
 - Select **Log on Poll Rate** to have the Data Logger record the values of the data points at a specified rate. In the **Poll Rate** property, enter a value and then select a measurement of time (seconds, minutes, hours). The default poll rate is **15 minutes**.
 - Select **Log on Updates** to have the Data Logger record the values of the data points when they change.
 - In the **Min. Delta Time** property, enter the minimum period of time that must elapse between log entries. Enter a value and then select a measurement of time (seconds, minutes, hours). The default minimum delta time is 15 minutes, which means that the data logger will record the data point's value every 15 minutes, regardless of how frequently the value changes between intervals.
 - In the **Min. Delta Value** property, select the minimum change in value required between log entries to record the data point. The default minimum delta value is **Always**, which means that the data logger always receives data point updates, regardless of whether the

value changes. You can set this property to **On Change** so that the data point is logged only when its value or state changes.

- Select **Advanced** to use a combination of the polling rate and event-driven update values to filter the data point updates. Select the **Set as Default** check box to use the configured properties as the default values for new data points added to the current Data Logger.

7. Click **Close**.

8. Click **Submit**. The Data Logger begins recording data point updates. You can view the log file at any time with the SmartServer Web pages or with a spreadsheet, as described in the *Viewing Data Logs* section later in this chapter.

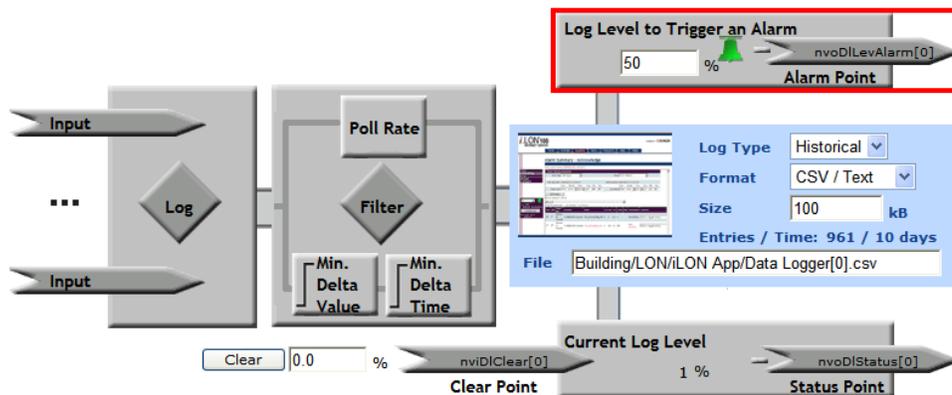
Note: You can remove one or more data points from a Data Logger. To remove one data point, right-click the data point and click **Remove Marked Data Point(s)** on the shortcut menu and then click **Submit**. To remove multiple data points, click one data point and then either hold down CTRL and click all other data points to be deleted or hold down SHIFT and select another data point to delete the entire range of data points, right-click one data point, click **Remove Marked Data Point(s)** on the shortcut menu, and then click **Submit**.

Setting Alarm Limits

You can enable the data logger to trigger an alarm when the log file is becoming full and have an Alarm Notifier send a notification. This is particularly useful if you are using a historical log file because it becomes disabled once it is full.

To specify an alarm limit and configure an Alarm Notifier to send a notification when the limit is reached, follow these steps:

1. In the **Log Level to Trigger an Alarm** box on the **Configure - Data Points** Web page, enter the percentage of the log file that when reached, triggers an alarm. The default log level is **50%**, which means that once the log is half full, the Data Logger updates the status of its alarm point (**nvoDILevAlarm [x]**, where x is the index number of the data logger) to **AL_ALM_CONDITION**.



2. Click **Submit**. When the alarm limit is reached, the alarm bell icon becomes red.
3. Open an Alarm Notifier application, following the steps described in the *Opening an Alarm Notifier Application* section in Chapter 6, *Alarming*.
4. Click one of the **Input Point** icons (), or click anywhere in the **Log** box (). The **Alarm Notifier: Data Points** Web page opens.
5. Click the **nvoDILevAlarm** data point under the Data Logger functional block tree as a data point to be monitored by the Alarm Notifier. The **nvoDILevAlarm** data point is added to the Web page.

6. Click **Submit**.
7. Configure the Alarm Notifier to send a notification each time the **nvoDILevAlarm** data point receives an alarm condition following the *Configuring E-mail and Data Point Destinations* section in Chapter 6, *Alarming*. Enter the full path of the log file as an attachment in an e-mail destination. This enables the log file to be sent to the specified recipients as soon as it becomes full.

Automatically Transferring Alarm and Data Logs

You can use the SmartServer to automatically transfer alarm and data logs (binary or CSV format) to a computer running the LNS Proxy Web service included with EES 2.2 and extract selected data to a CSV or XML file. To do this, you create a Web connection between the SmartServer and LNS Proxy Web service (in LNS mode) or between the SmartServer and a Web Connection target that is set to the IP address of the LNS Proxy Web service (in Standalone mode), and add then attach the desired data log file to the Web connection.

Each time the source data point in the Web connection is updated, the data log file is downloaded to the **LonWorks\iLON\EnterpriseServices\repository\ees-lnsproxy\ReceivedFiles** folder on your EES 2.2 computer. You can manually update the source data point using the **Show Value** dialog, the **Data Points: View** Web page, a custom SmartServer Web page, or other method. You can also program updates to the source data point using the SmartServer's built-in applications (for example, the Scheduler or Type Translator), a custom app, or a SOAP application.

To automatically transfer alarm and data logs, follow these steps:

1. Verify that EES 2.2 and OpenLNS Server has been installed on your OpenLNS Server computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
2. Verify that the device resource files for the subject data points are installed on your EES 2.2 computer. You can install the standard version 14 LONMARK resource files on your EES 2.2 computer by installing the Echelon NodeBuilder Resource Editor from the SmartServer 2.2 DVD (see *Installing Echelon NodeBuilder Resource Editor* in Chapter 2 for how to do this). You can manually copy any user-defined resource files to the **LonWorks\types\user\<company>** folder on your EES 2.2 computer.
3. Create a Web connection between the SmartServer and the LNS Proxy Web service running on your EES 2.2 computer.
4. Add a Data Logger or add an Alarm Generator and Alarm Notifier to your SmartServer and configure it. See Chapter 6 of for more information on configuring Alarm Generators and Alarm Notifiers, and see *Creating a Data Logger* earlier in this chapter for configuring data loggers.
Note: To speed up log transfer, set the format of the alarm or data log file to the binary format, and the data log extractor will automatically convert it to a CSV file on your computer.
5. Attach an alarm or data log file to the Web connection.
6. Configure a method for triggering updates to the source data point in the Web connection to which the data log file is attached.
7. View the extracted data log files.

The following sections describe how to perform steps 3 and 5–7.

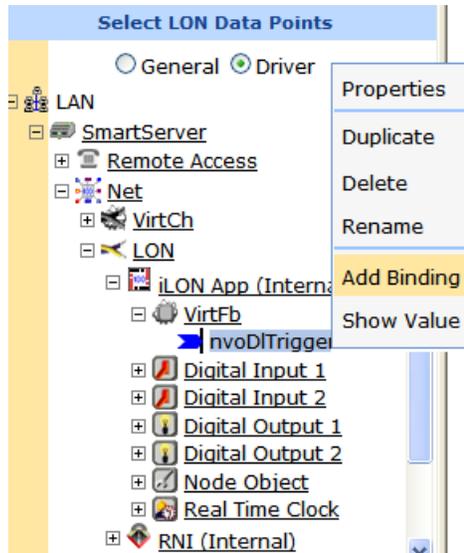
Creating a Web Connection for Logger Extraction

The following sections describe how to create a Web connection to be used for the data log extractor feature on a SmartServer running in LNS mode or standalone mode.

Creating the Web Connection in LNS Mode

To create a Web connection with the SmartServer running in LNS mode, follow these steps:

1. Add an OpenLNS Server to the LAN in the SmartServer Web interface following *Adding an OpenLNS Server to the LAN* in Chapter 3.
2. From the navigation pane in the left frame of the SmartServer Web interface, right-click a source data point in the SmartServer tree and then click **Add Connection** in the shortcut menu. This example adds a **SNVT_switch** dynamic data point to the SmartServer i.LON App device's Virtual Functional Block (**Net/LON/iLON App/VirtFB/nvoDITrigger**).

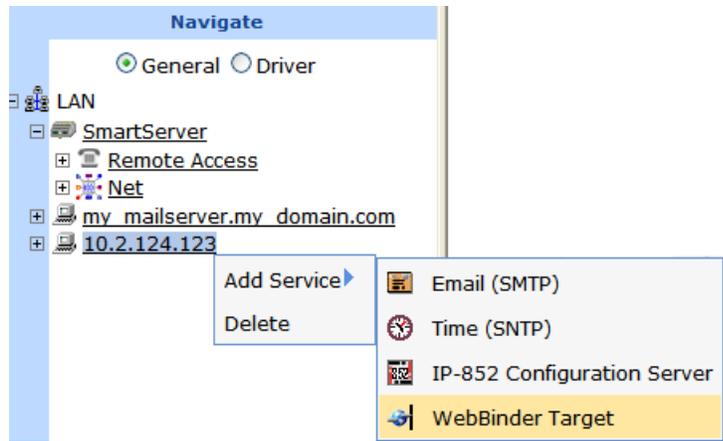


3. The **Configure – Web Connection** Web page opens and the hostnames of the local SmartServer and the OpenLNS Server or Web Connection Target Server you added to the LAN appear in the application frame to the right. The host devices in the right frame are collectively referred to as *Web-Connection Destinations*.
4. From the Web-Connection Destinations tree on the right frame, expand the LNS Server icon, expand a network, channel, device and functional block, and then click a data point. A reference to the target data point (➤) is added underneath the source data point in the SmartServer tree in the navigation pane.

Creating the Web Connection in Standalone Mode

To create a Web connection with the SmartServer running in standalone mode, follow these steps:

1. Add a Web Connection Target Server to the LAN in the SmartServer Web interface. To do this, follow these steps:
 - a. Right-click the **LAN** entry at top of navigation pane, point to **Add Host**, click **Server**.
 - b. Click the **Host** option, and then enter IP address of your computer, which must be running the LNS Proxy Web service and OpenLNS Server.
 - c. Right-click the server icon, point to **Add Service**, then and click **Web Connection Target** on the shortcut menu.



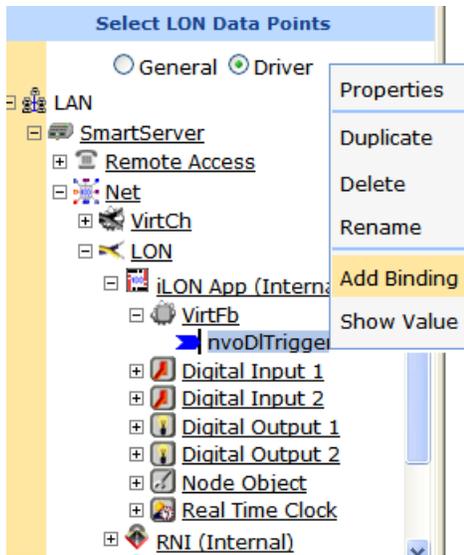
- d. The **Setup – Web Service** Web page opens.
- e. Enter the following properties:
 - In the **SOAP Path** box, enter **/LnsProxy/LnsProxyService** (this is the SOAP path to the Echelon Enterprise Service running on your computer).
 - In the **HTTP Port** box, enter the port on your computer used for accessing the Echelon Enterprise Service (**80** by default).
 - In the **SOAP User Name** box, enter the user name for logging into the Echelon Enterprise Service. The default user name is **ilon**.
 - In the **SOAP Password** box, click **Change Password**, enter and re-enter the password for logging into the Echelon Enterprise Service, and then click **OK**. The default password is **ilon**.

Note: If you changed the default user name and password for logging into EES 2.2, you can use the EES 2.2 tray icon in the notification area to check the current user name and password. See Chapter 3 of the *Echelon Enterprise Services 2.2 User's Guide* for more information on viewing and changing the Echelon Enterprise Service user name and password.

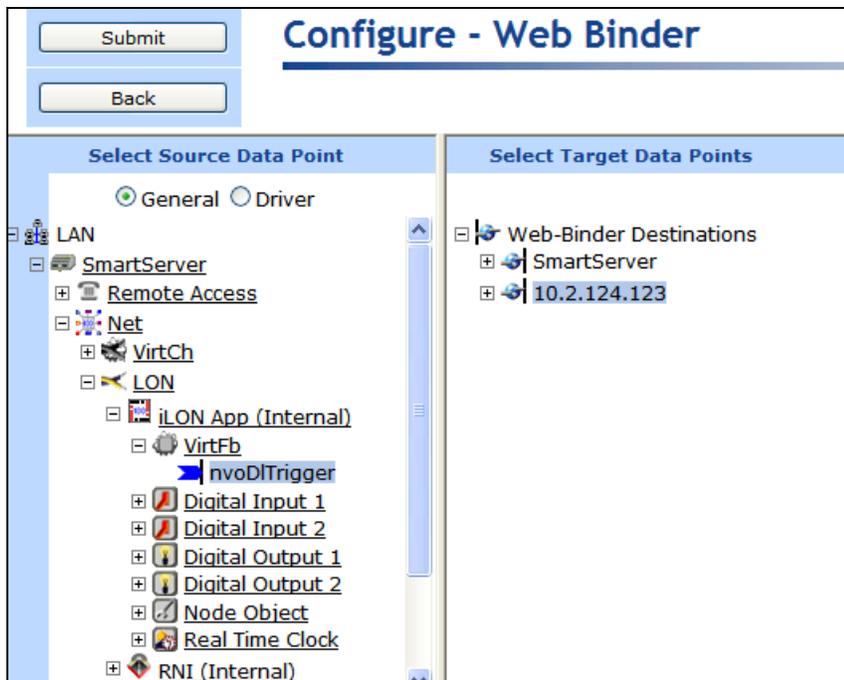
- f. Click **Submit**.



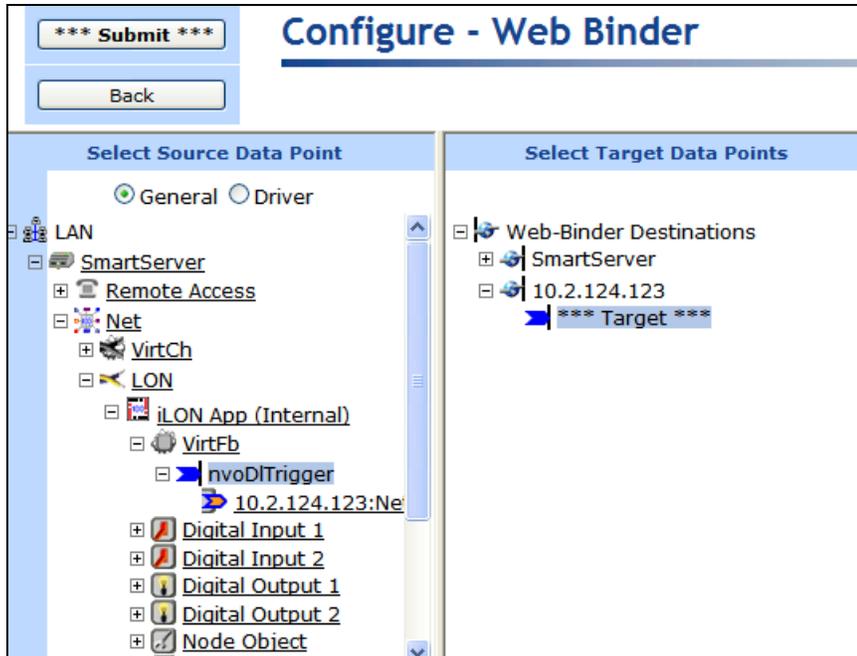
- 2. From the navigation pane, right-click a source data point in the SmartServer tree and then click **Add Connection** in the shortcut menu. This example adds a **SNVT_switch** dynamic data point to the SmartServer i.LON App device's Virtual Functional Block (**Net/LON/iLON App/VirtFB/nvoDITrigger**).



3. The **Configure – Web Connection** Web page opens and the hostnames of the local SmartServer and the Web Connection Target Server you added to the LAN in step 2 appear in the application frame to the right. The host devices in the right pane are collectively referred to as *Web Connection Destinations*.



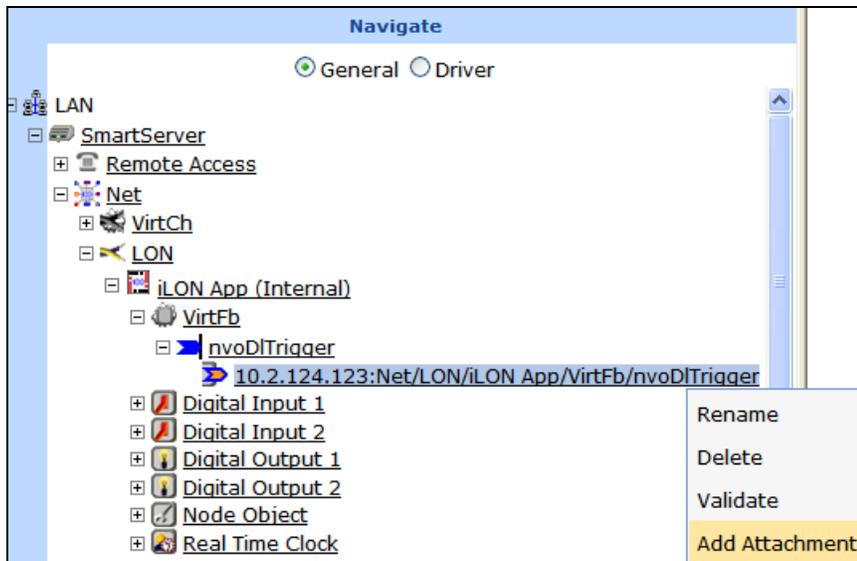
4. From the Web-Connection Destinations tree on the right pane, expand the Web Connection Target Server and then click ***** Target *****. A reference to the target data point (📌) is added underneath the source data point in the SmartServer tree.



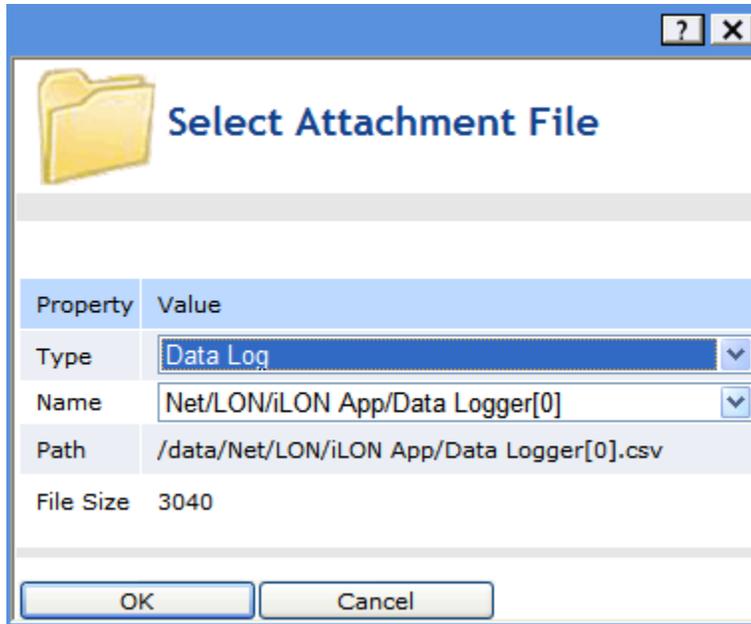
Attaching a Log File

To attach an alarm or data log file to the Web connection, follow these steps:

1. Under the source data point icon in the SmartServer tree, right click the reference to the target data point in the Web connection, and then click **Add Attachment** on the shortcut menu.



2. The **Select Attachment File** dialog opens.
3. In the **Type** box select **Alarm Log** or **Data Log**.
4. In the **Name** box, select the name of the log file to be attached. The names displayed are the locations of the logs on the SmartServer tree in the following format:
`<network>/<channel>/<device>/<functional block>`. The **Path** and **File Size** properties display the location of the selected log file on the root directory of the SmartServer flash disk and its size in bytes.



5. Click **OK**. An attachment icon (📎) is added to the target data point icon.
6. Click **Submit**.

Triggering Log Transfer

Each time the source data point in the Web connection used for the log transfer is updated, the SmartServer downloads the specified data log file attachment to your OpenLNS Server computer running EES 2.2.

You can manually update the source data point with the SmartServer using the **Show Value** dialog, the **Data Points: View** Web page, a custom SmartServer Web page, or other method. Using the **Show Value** dialog or the **Data Points: View** Web page is useful for testing the data log extractor in a development environment. In a deployment environment, you can provide a custom SmartServer Web page for users to manually extract a data log file.

To integrate log transfer with your own applications, you can use one of the SmartServer's built-in applications such as an Alarm Generator, Scheduler, or Type Translator to update the data point at a certain time or when a certain condition exists. You can also use a custom app or a SOAP application to programmatically trigger the data point update. The following sections provide examples of how to use the Scheduler and Type Translator built-in applications on the SmartServer to update the source data point programmatically.

Example 1: Scheduling a Log transfer

You can use the SmartServer's built-in Scheduler application to update the source data point in the Web connection used for the log transfer. In this example, the Scheduler updates the source data point at 07:00 every day. To do this, do the following:

1. Identify a data point in the SmartServer tree to be used as the trigger for the log transfer. This example adds a **SNVT_switch** dynamic data point to the SmartServer i.LON App device's Virtual Functional Block (**Net/LON/iLON App/VirtFB/nvoDITrigger**).
2. Create a Web connection, configure a data logger, and attach a data log file as described in the previous sections.
3. Create a Scheduler. See Chapter 7, *Scheduling* for more information.

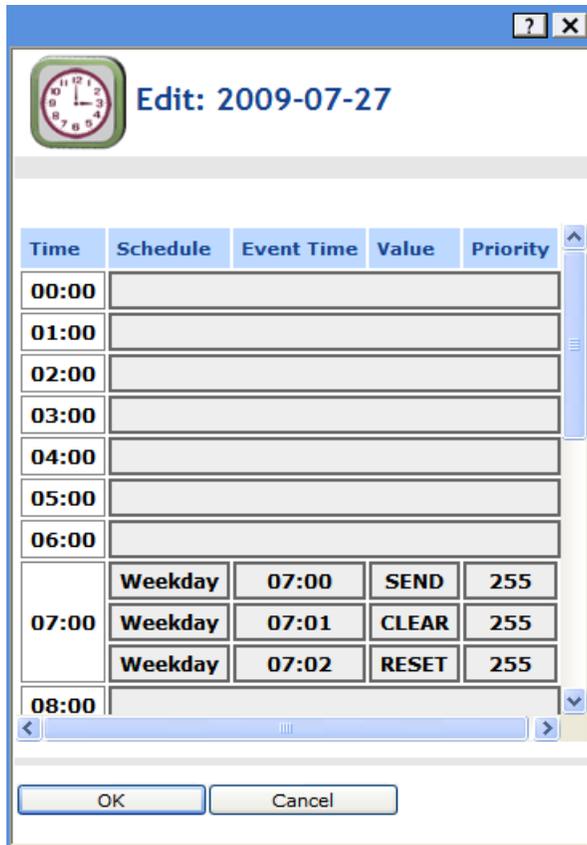
- Add your specified trigger source data point and the **nviDIClear** data point on the specified data logger to the Scheduler.
- Add the following presets, and then assign them to the data points with the listed values:

Preset	Data Point	Value
SEND	nvoDITrigger	100.0 1
CLEAR	nviDIClear	100.0 1
RESET		0.0 0

Data Point	Unit	Stagger Delay	SEND	CLEAR	RESET
0 Net/LON/iLON App/VirtFb/nvoDITrigger	value, state	0.0 s	100.0 1		
1 Net/LON/iLON App/Data Logger[0]/nviDIClear[0]		0.0 s		100.0 1	0.0 0

- Create a daily schedule that has the following three events:

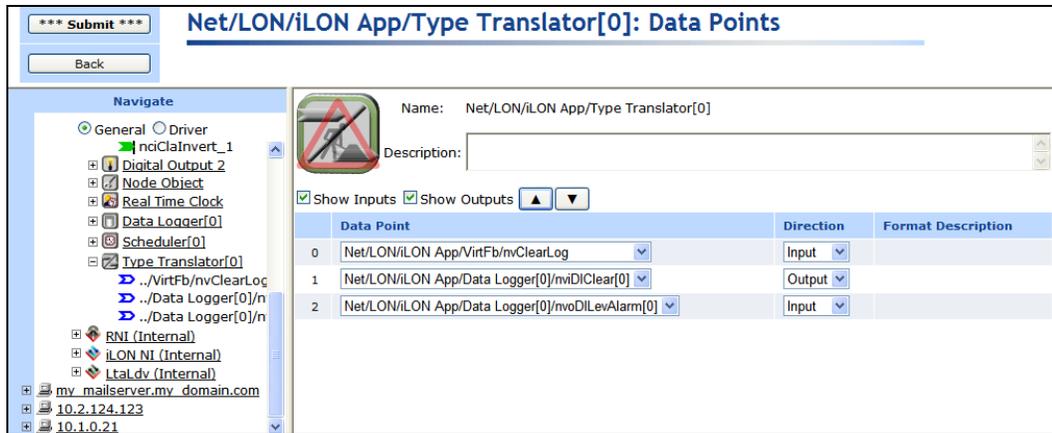
Event Time	Preset	Description
7:00	SEND	Sends the data log file.
7:01	CLEAR	Clears the data log file.
7:02	RESET	Resets the clear data point.



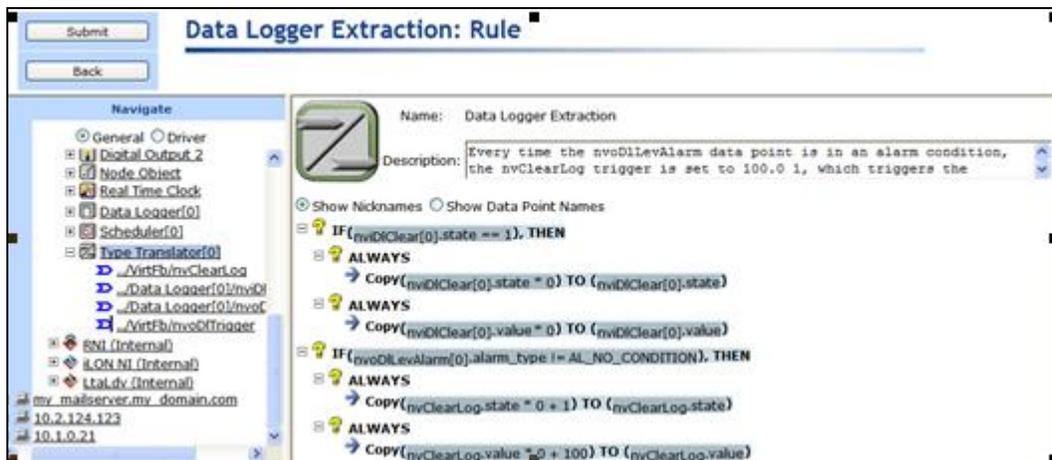
Example 2: Using Case Logic for Log transfer

You can use the SmartServer's built-in Type Translator application to update the source data point in the Web connection used for the log transfer. In this example, case logic is used to update the source data point and send the data log file when the data logger becomes full. To do this, you do the following:

1. Identify a data point in the SmartServer tree to be used as the trigger for the log transfer. This example adds a **SNVT_switch** dynamic data point to the SmartServer i.LON App device's Virtual Functional Block (**Net/LON/iLON App/VirtFB/nvClearLog**).
2. Create a Web connection for data logger extraction, configure a data logger, and attach a data log file as described in the previous sections.
3. Create a Type Translator. See Chapter 11, *Using Type Translators*, for more information.
4. Add your specified trigger source data point and the **nviDIClear** and **nvoDILevAlarm** data points on the specified data logger to the Type Translator.



5. Create a Web connection between the **nvClearLog** and **nviDClear** data points.
6. Create a new type translator rule with the following case logic: every time the **nvoDILevAlarm** data point is in an alarm condition, set the **nvClearLog** trigger to 100.0 1, which triggers the download of the data log file. When the **nvClearLog** data point is set to 100.0 1, update the **nviDClear** data point with this value via the Web connection created in step 5 and the data log is cleared completely. This then triggers the rule for resetting the **nviDClear** data point to 0.0 0.



7. In the **Type Translator: Configure** Web page, specify a delay of at least 5 seconds.

Viewing Extracted Data Log Files

Each time the source data point in the Web connection used for the log transfer is updated, the data log file attached to the Web connection is downloaded to the **LonWorks\iLON\EnterpriseServices\repository\ees-Insproxy\ReceivedFiles** folder on your computer.

For example, if the data log file attached to the Web connection is “data/Net/LON/iLON App/Data Logger[0].bin”, your SmartServer’s logical ID is “0300002910062”, and the source data point has been updated three times the **ReceivedFiles** folder will have the following hierarchy:

```
+-- ReceivedFiles
  +- 0300002910062
    +- data
      +- Net
        +- LON
```

```

+- iLON App
  +- Data Logger[0].csv.bak.1
    Data Logger[0].csv.bak.2
    Data Logger[0].csv
  
```

Note: You can view the logical ID of your SmartServer from the **Setup – Local SmartServer** Web page on the SmartServer. To access this Web page, right-click the SmartServer icon, point to **Setup**, and then click **Service** on the shortcut menu. Alternatively, you can click **Setup** and then click **Service**.

By default, the logical ID is set to the Neuron ID of the SmartServer’s i.LON App device. You can change the logical ID to any value containing one or more 2 digit hex pairs (00–FF). For example, 00, 00FF, and 00FF00 are legal logical IDs.

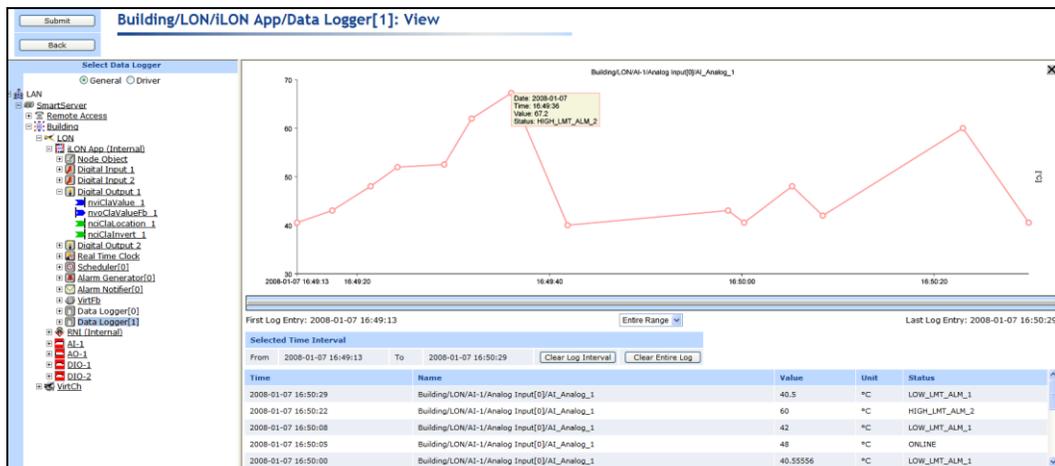
Viewing Data Logs

You can view the data point updates recorded by the data loggers on your SmartServer using the SmartServer Web pages, and you can view the data logs stored on the SmartServer flash disk by manually transferring them to your computer and using a spreadsheet application such as Microsoft Excel. This section describes how to use the SmartServer Web pages and spreadsheet applications to view the data point updates and data logs.

Viewing Data Logs with the SmartServer Web Pages

You can use the **Data Logger: View** Web page to view the data point updates recorded by the data loggers on your SmartServer. To use the **Data Logger: View** Web page, follow these steps:

- Open the **Data Logger: View** Web page. You can do this in two ways:
 - Click **View** and then click **Data Logger**. By default, the **Data Logger: View** Web page will list the data point updates recorded by the first data logger listed under the **i.LON App (Internal)** device in the SmartServer tree. To view the data recorded by a different Data Logger, click that Data Logger in the SmartServer tree
 - Click **General** and then click a Data Logger functional block in the tree to open the **Data Logger: Configure** Web page. Click the data logger image in the middle of the right side of the Web page. By default, the **Data Logger: View** Web page will list only the data point updates recorded by the selected Data Logger.
- The **Data Logger: View** Web page opens.



The **Data Logger: View** Web page includes a trend graph and a log that chart and list the data point updates that have been recorded by the data logger.

3. The trend graph charts all the data point updates recorded by the selected Data Logger. For multiple data points to be scaled accurately on the trend graph at the same time, they must have the same **Unit String** property. You can add a unit string to a data point or edit the one defined for it in the **Configure - Data Points** Web page on the SmartServer. In addition, if the selected points have structured data types, the same fields must be selected.

You can move the mouse pointer over one of the plotted data point updates to show a ToolTip. The ToolTip lists the date and time of the update and the value and state of the data point at the time the update was recorded.

4. The log lists the first to last data point updates recorded by the selected data logger in descending chronological order. You can sort the data point updates by clicking a property header. This Web page displays the following properties for each data point update recorded in a data logger:

<i>Selected Time Interval</i>	Displays the user-specified interval, which determines the data points currently shown on the Web page. The default interval is the time from the first to last data point recorded by the data loggers on your SmartServer. <ul style="list-style-type: none">• Click Clear Log Interval to clear the currently selected range of data points from the Web page. Note that the Web page only shows the first 60 entries in the range, but the entire range will be deleted.• Click Clear Entire Log to clear all the selected data points from the Web page.
<i>Time</i>	Displays the date and time when the data point update occurred.
<i>Name</i>	Displays the name of the data point that was updated using the following format: <code><network>/<channel>/<device>/<functional block>/<data point></code> . This is also the location of the data point in the SmartServer tree.
<i>Value</i>	Displays the value of the data point at the time of the update. If the data point is set to a preset value, the preset name will be displayed instead of the actual value.
<i>Unit</i>	Displays the unit string of the data point.
<i>Status</i>	Displays the status of the data point at the time of the update.

In some cases, there may be more log entries within the selected range than can be displayed on the screen at once. In this case, a warning message will be displayed, and you can use the slide bar to browse the log entries.

5. You can use the slide bar at the top to browse the first to last updates recorded for the selected data point. Move the slider bar to the left to display older sets of values, or move it to the right to display the more recent values. If there are too many values within the selected range to be displayed, a warning message appears informing you that only a subset of the data points is being displayed.
6. You can specify the time interval for which recorded data point updates are listed in the log and displayed in the trend graph using the drop-down list directly below the slider. The default is **Entire Range**, which means that the log lists the first to last data point updates recorded in the data loggers on the SmartServer and the trend graph plots the first to last updates recorded for a selected data point.

For example, select **1 hour** to have the log list the data point updates that have been recorded in the last 1 hour. You can still browse the updates beyond the specified time interval using the slider.

Tip: If you need to print this page, use the landscape format.

Manually Transferring Data Logs

You can manually copy the data logs stored on the SmartServer flash disk to your computer via FTP and then view the data log file using a spreadsheet application such as Microsoft Excel. To do this, follow these steps:

1. Verify that you have the correct user name and password to access the SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - b. In the **General** property, check the **FTP/Telnet User Name** and **FTP/Telnet Password** properties.
 - c. In the **Service** property, verify that **Enable FTP** is selected.
2. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example).
3. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
4. Browse to the **/data/<network>/<channel>/<SmartServer App device>** folder. This folder contains the log files for each Data Logger on your SmartServer. The log files are named **Data Logger [x].<file extension>**, where *x* is the index number of the Data Logger functional block and *file extension* is the file format you selected (**.csv**, **.bin**, or **.csv.gz**).
5. You can copy the data log file to your computer and then open it with a specific spreadsheet application. You can also double-click the log file, click **Open**, and then enter your FTP/Telnet user name and password. The log file opens in the default spreadsheet application for your computer. If the log is saved as a compressed ASCII text file (**.csv.gz** extension), you need to first extract the **.csv** file from the **.csv.gz** file using WinZip or Gnu Zip.

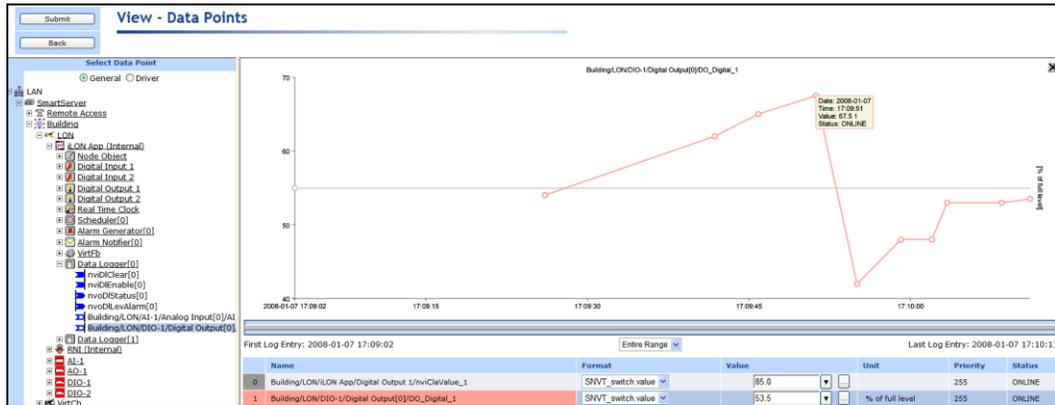
Viewing Data Points

You can monitor, chart, and control data points using the **View - Data Points** Web page. This Web page includes a log that displays the current values and states of the selected data points, a trend graph that charts the data point values over a specified interval, and fields for writing values to the data points.

To use the **View - Data Points** Web page, follow these steps:

1. Click **View** and then click **Data Points**. The **View - Data Points** Web page opens. This Web page includes a log and a trend graph that list and chart the values of selected data points respectively.
2. Select the data points to monitor and control from either the local SmartServer, a remote SmartServer, or an OpenLNS network database in the navigation pane.
 - To select data points from a remote SmartServer in the tree, you must first add a remote SmartServer to the LAN.
 - To select data points from an OpenLNS network database, you must first install the Echelon Enterprise Services 2.2 from the SmartServer 2.2 DVD (see *Installing Echelon i.LON Enterprise Services* in Chapter 2 for more information); install OpenLNS Server from the SmartServer 2.2 DVD if you installed Echelon Enterprise Services 2.2 (see *Installing Echelon OpenLNS Server* in Chapter 2 for more information); and then add an OpenLNS Server to the LAN that contains the OpenLNS network database (see *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information). The selected data points are listed in the log and plotted on the trend graph.

Note: Alternatively, you can reverse steps 1 and 2 to view a data point in the **View - Data Points** Web page. This means that you can click the data point, click **View**, and then click **Data Points**.



- The trend graph charts all the selected data points. For multiple data points to be scaled accurately on the trend graph at the same time, they must have the same **Unit String** property. You can add a unit string to a data point or edit the one defined for it in the **Configure - Data Points** Web page on the SmartServer. In addition, if the selected points have structured data types, the same fields must be selected.

You can move the mouse pointer over one of the plotted data point updates to show a ToolTip. The ToolTip lists the date and time of the update and the value and state of the data point at the time the update was recorded.

- By default, the log lists the data points in the order they were selected. You can sort the data points by clicking a property header. This Web page displays the following properties for the selected data points:

Name Displays the name of the data point using the following format: `<network>/<channel>/<device>/<functional block>/<data point>`. This is also the location of the data point in the SmartServer tree.

IP Address Displays the IP address of the SmartServer or OpenLNS Server on which the data point resides. This property appears if you select a data point from a remote SmartServer or an OpenLNS Server.

Format Displays the SNVT, UNVT, or built-in data type used by the data point, and it specifies the format (for example, SI metric or US customary) used if the type has multiple formats such as **SNVT_temp_p**.

If the data point has structured type (i.e. a structure or union with multiple fields), you can select which field to monitor and control from the list. For example, if you select a **SNVT_switch** data point, you can select the value or the state of the data point.

Value Displays the current value of the data point. To update the data point, enter a valid value in this box and then click **Submit**, press ENTER, or press TAB.

If presets are defined for the data point, you can select a preset from the list and the data point will be updated with the value defined by the preset. You can edit the values defined by the selected preset by clicking the button to the right and opening the **Edit Value** dialog.

- If a Manual Override icon () appears to the left of the data point, the data point is in manual override mode (another application has been assigned a priority for updating this data point). You can enter a value

for the data point and override the other application.

- If a Locked icon () appears to the left of the data point, a “Priority too low to set value” error has occurred. You need to click the button to the right and enter a higher priority in the **Edit Value** dialog for the **View – Data Points** Web page to write to the data point.
- If an unplugged icon () appears above the data point, the data point is offline.
- If a yellow alarm bell icon () or a red alarm bell icon () appears to the left of the data point, the data point is an alarm condition.
- If a warning symbol appears () to the left of the data point, the data point has a configuration error.

Unit

Displays the unit string of a scalar data point or the unit string of the selected field of a structured data point. This field is read-only.

For example, the unit string for an **SNVT_temp_f#US** data point, which is scalar, is “degrees F”. A **SNVT_switch** data point, which is a structured, has “% of full level” and “state code” unit strings describing its state and value fields. The unit string displayed for a structured data point depends on the field selected in the **Format** list.

Multiple data point values will only be scaled properly in the trend graph if they have the same unit string. You can edit the unit string of a data point in the **Configure – Data Point** Web page, which you can access by clicking **General** and then clicking the data point in the navigation pane.

Priority

Displays the priority the **View - Data Points** Web page has for writing updated values to the data point. This value may range from 0 to 255 (highest to lowest priority). By default, this property displays the priority currently assigned to the data point. This is the priority used by the last object or application that updated the data point. For example, if a Scheduler with a priority of 220 updated the data point last, the data point’s priority is 220.

You can assign the **View - Data Points** Web page a priority for writing updated values to a data point by clicking the button to the right in the **Values** box, which opens the **Edit Value** dialog. In the **Priority** box to the right of the data point name, enter the priority for the **View - Data Points** Web page to use in order to write to the data point and then click **OK**.

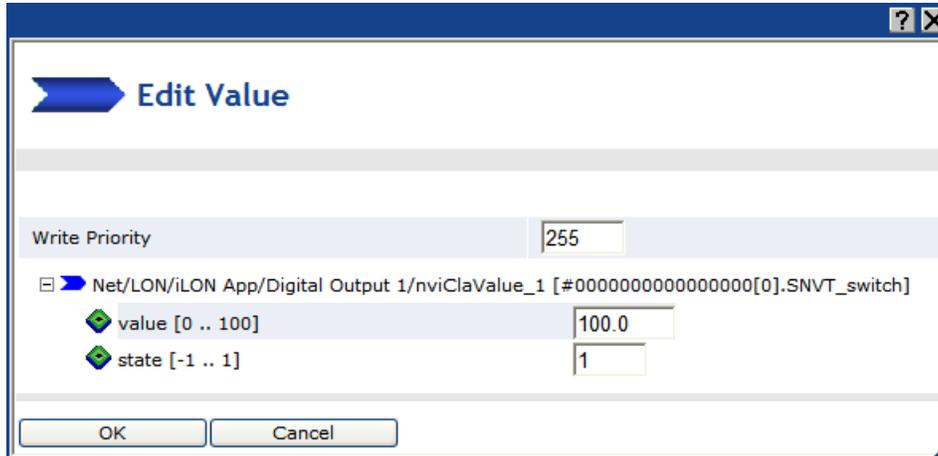
The priority you specify must be equal to or higher than the priority used by the last application that updated the data point. Similarly, if you update the data point with this Web page, the next application must specify a priority equal to or higher than the one you specified in order to write to the data point. If you set a priority that is less than priority used by the last application that updated the data point, an error message opens stating that the priority level you set it to low and that you can click the green hand icon in the **View - Data Points** Web page to reset the data point priority.

You can reset the priority of a data point by clicking the green hand manual override icon () in the **View - Data Points** Web page. This sets the data point's priority to 255 and notifies all other objects and applications in which the subject data point is registered. The next highest priority application or object will then assume the priority for writing values to the data point. For example, if a Scheduler is currently active and has the highest priority for writing to the data point at 220, the data point priority is set to 220.

Status

Displays the current status of the data point.

5. You can click the button to the right of the **Values** property to open the **Edit Value** dialog. You can use this dialog to assign the **View - Data Points** Web page a different priority for writing updated values to a data point, and to enter a different value for the data point or for the fields of a structured data point.



- a. In the **Write Priority** box, you can assign the priority the **View - Data Points** Web page has for writing updated values to the data point. The priority you specify must be equal to or higher than the priority used by the last application that updated the data point. Similarly, if you update the data point with the **View - Data Points** Web page, the next application must specify a priority equal to or higher than the one you specified in order to write to the data point. If you set a priority that is less than priority used by the last application that updated the data point, a “Priority too low to set value” error occurs and a red hand locked icon () appears to the left of the data point. You need to enter a higher priority in this dialog for the **View - Data Points** Web page to be able to write to the data point.
 - b. In the **Value** box, enter a valid value to be written to the data point. If you selected a structured data point (for example, a **SNVT_switch** data point), you can enter values for one or more of the fields in the data point. If you selected an enumerated data point (for example, a **SNVT_lev_disc** data point), select one of the enumerated values from the list.
 - c. Click **OK** to return to the **View – Data Points** Web page.
6. You can point to one of the listed data points in the log or click its line on the trend graph to highlight the updates recorded for that data point on the trend graph. You can then move the mouse pointer over one of the plotted data point updates to show a ToolTip. The ToolTip lists the date and time of the update and the value and state of the data point at the time the update was recorded.
 7. You can use the slide bar at the top to browse the first to last updates recorded for the selected data point. Move the slider bar to the left to display older sets of values, or move it to the right to display the more recent values. If there are too many values within the selected range to be displayed, a warning message appears informing you that only a subset of the data points is being displayed.
 8. You can specify the time interval for which recorded data point updates are listed in the log and displayed in the trend graph using the drop-down list directly below the slider. The default is **Entire Range**, which means that the log lists the first to last data point updates recorded in the data loggers on the SmartServer and the trend graph plots the first to last updates recorded for a selected data point.

For example, you can select **1 hour** to have the log list the data point updates that have occurred in the last 1 hour. You can then click a data point, and the trend graph by default will plot the updates that have been recorded for the data point over the last hour. You can still browse the updates beyond the specified time interval using the slider.

9. To clear a data point from the log and graph, right-click the data point and then click **Remove** on the shortcut menu.

Tip: If you need to print this page, use the landscape format.

Connecting Legacy Devices Using SmartServer Inputs and Outputs

This chapter describes how to use the inputs and outputs on the SmartServer to connect legacy devices to it. It describes how to use the pulse counter inputs on the SmartServer to connect electric, gas, and water meters. It explains how to use the digital inputs and output on the SmartServer to connect legacy digital input and output devices such as switches, push buttons, drive contractors, and alarm bells.

Connecting Legacy Devices Overview

The SmartServer includes two pulse meter inputs for connecting electric, gas, and water meters; two digital inputs for connecting legacy digital input devices such as switches and push buttons; and two dry-contact relay outputs for connecting legacy digital output devices such as drive contactors and alarm bells. A legacy device is a device that does not have a LONWORKS interface and thus cannot be attached to a LONWORKS network directly.

- You can connect a meter that measures energy or measures the flow of a gas or liquid to the pulse meter inputs on the SmartServer. You can then use the Pulse Counter application on the SmartServer to count the pulses generated by the meter and store the pulse count and pulse rate.
- You can connect a switch or sensor device to the digital inputs on the SmartServer. You can then use the Digital Input application on the SmartServer to monitor the device state and store it in **SNVT_switch** and **SNVT_setting** output data points.
- You can connect a digital output device such as a drive contactor or alarm bell to the digital outputs on the SmartServer. You can then use the Digital Output application on the SmartServer to get the current device state and store it in a **SNVT_switch** output data point.

The following sections describe how to connect legacy pulse meter, digital output, and digital input devices to the SmartServer and use the corresponding applications on the SmartServer Web pages.

Connecting Pulse Meters

The SmartServer includes two pulse meter inputs. Each pulse meter input registers pulses when the circuit between its positive and negative connections is closed (the voltage is 0) for 30ms or longer. You can connect the pulse meter inputs on the SmartServer to legacy devices that have a pulse output. The pulse output device is typically a meter that measures energy or measures the flow of a gas or liquid, and generates a pulse for a pre-defined unit such as kilowatt-hours, liters, or gallons.

After you connect a pulse meter to the SmartServer you can use the Pulse Counter application on the SmartServer to count the pulses generated by the pulse meter, calculate a pulse rate, and store the pulse counts and pulse rates in electrical or flow rate output data points (Wh, kWh, volts, liters, or gallons). You can then use an Alarm Notifier or Data Logger to monitor these output data points, or you can use a Type Translator to translate the output data points to a compatible type for use in another SmartServer application.

Note: The Pulse Counter is the first application to start after the SmartServer is rebooted to minimize the number of pulse counts lost during software initialization.

To connect a pulse meter to the SmartServer and use the Pulse Counter application, you do the following:

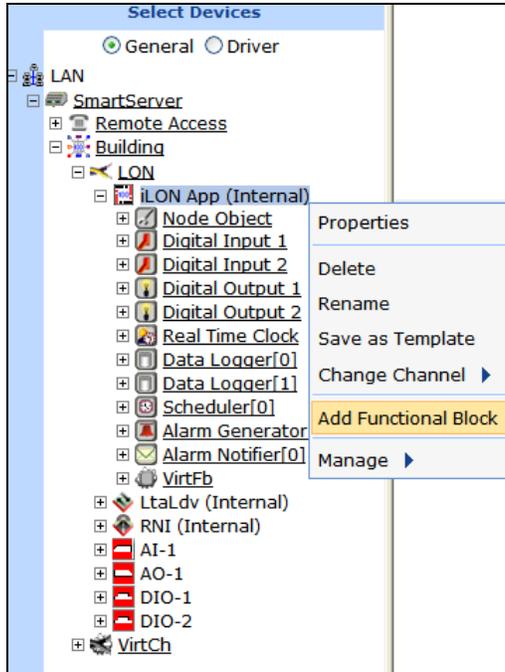
1. Connect the pulse meter device to one of the pulse meter inputs on the SmartServer. See the SmartServer *Hardware Guide* for instructions on how to do this.
2. Open the Pulse Counter application on the SmartServer.
3. Configure the Pulse Counter application.

Opening the Pulse Counter Application

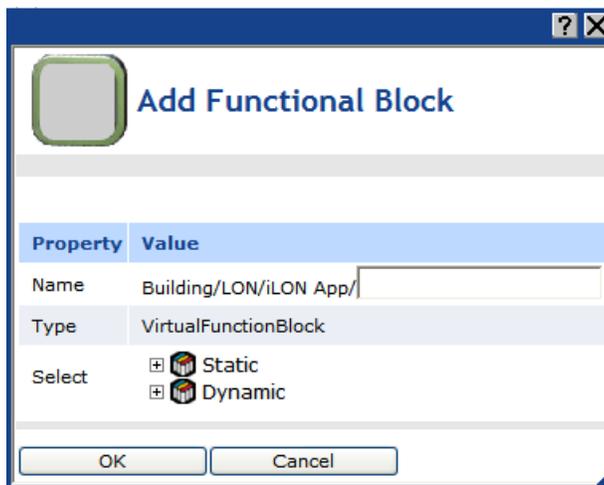
To open a Pulse Counter application, you must first create a Pulse Counter functional block. After you create the Data Logger functional block, the functional block appears on the SmartServer tree below the **i.LON App (Internal)** device, and you can click the functional block to open the Pulse Counter application.

To create a Pulse Counter functional block and open the application, follow these steps:

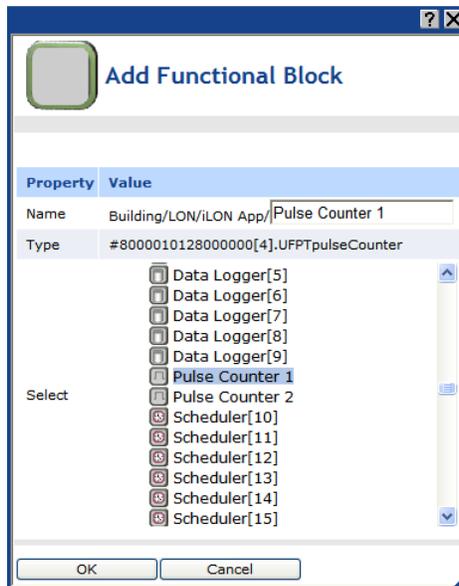
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **iLON App (Internal)** device.
3. Right-click the **iLON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



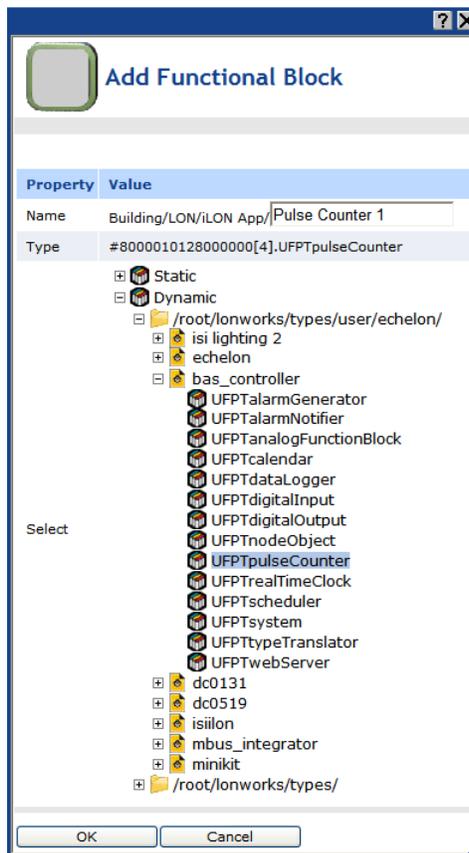
4. The **Add Functional Block** dialog opens.



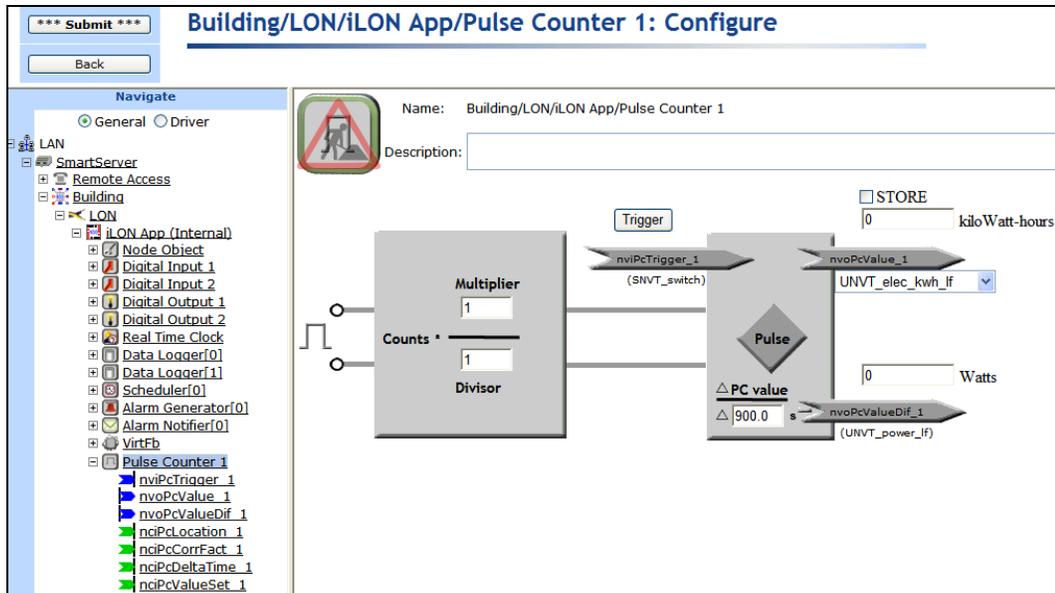
5. Select the Pulse Counter functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the default static v12 interface, expand the **Static** icon, select the **Pulse Counter** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Pulse Counter functional block from either the **Static** or the **Dynamic** folder. To select the Pulse Counter functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile template (UFPT) for the Pulse Counter, enter a name for the functional block such as “Pulse Counter 1”, and then click **OK**.



- A functional block representing the Pulse Counter application and all of its static data points are added to the bottom of the **i.LON App (Internal)** device tree, and the **Pulse Counter: Configure** Web opens in the application frame to the right. Note that construction symbol overlaid onto the Pulse Counter application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



- Click **Submit**.

To open the Pulse Counter application from an existing Pulse Counter functional block, follow these steps:

- Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Pulse Counter application.
- Click the Pulse Counter functional block representing the Pulse Counter to be opened. The **Pulse Counter: Configure** Web page opens in the application frame to the right.

Configuring the Pulse Counter Application

You can configure the Pulse Counter application on the SmartServer following these steps:

- To convert the units per pulse, enter multiplier and divisor factors in the **Multiplier** and **Divisor** boxes. For example, if a power meter sends 1 pulse every 10 kilowatt hours (kWh), you can convert the data to kWh and by entering **10** in the **Multiplier** box and **1** in the **Divisor** box.

For example, if a power meter sends 1 pulse every 10 kilowatt hours (kWh) and the building has a scale factor of 0.5 kWh /pulse, you can convert the data to kWh by entering **1** in the **Multiplier** box and **2** in the **Divisor** box.

- To reset the sample interval used to calculate the pulse rate, click **Trigger**. The SmartServer stores the accumulated pulse count and the pulse rate in the **nvoPcValue** and **nvoPCValueDif** data points, respectively, and starts a new sample interval. This also resynchronizes the pulse counter.

The values stored in the **nvoPcValue** and **nvoPCValueDif** data points are sent when the time interval specified in step 3 expires or the value of the **nviPcTrigger** data point changes from off to on.

3. To set the sample interval, enter the time (in seconds) in the box below the **Pulse** icon and the **PC value** text. The default sample interval is 15 minutes (**900.0s**). This value also determines how frequently the output data point values are updated.
4. To specify a starting value for the **nvoPcValue** or **nvoPCValueDif** data points, select the **STORE** check box, enter the starting value in the box above the corresponding output data point. The starting value you specify overwrites the pulse count or pulse rate previously calculated by the SmartServer. When the **STORE** check box is selected, the data point value is not updated as a result of polling.
5. To change the unit of measure used for the **nvoPcValue** and **nvoPCValueDif** data points, select the corresponding data point type in the list below the **nvoPcValue** data point. You can select units of measure such as Wh and kWh in load and load factor formats, and volts and gallons in US customary and SI unit formats. The default unit of measure is kWh load factor (**UNVT_elec_kwh_lf**).

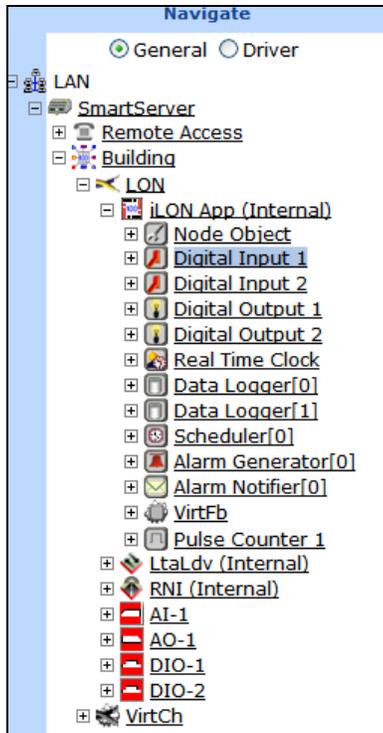
If you have specified an OpenLNS Server and an OpenLNS network database in the **Setup – LON Network Driver** Web page, the SmartServer transmits the change in data point type to the specified OpenLNS network database automatically. See *Adding an OpenLNS Server to the LAN* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on adding an OpenLNS Server to the LAN. See Chapter 5, *Using the SmartServer as a Network Management Tool*, for more information on configuring the LONWORKS network driver properties.

6. You can monitor the **nvoPcValue** and **nvoPCValueDif** output data points using an Alarm Notifier or Data Logger. For more information on using these applications, see Chapter 7, *Alarming* and Chapter 8, *Data Logging*. You can also translate the output data points to a compatible type for use in another SmartServer application using a Type Translator. For more information on using the Type Translator application, see Chapter 11, *Using Type Translators*.

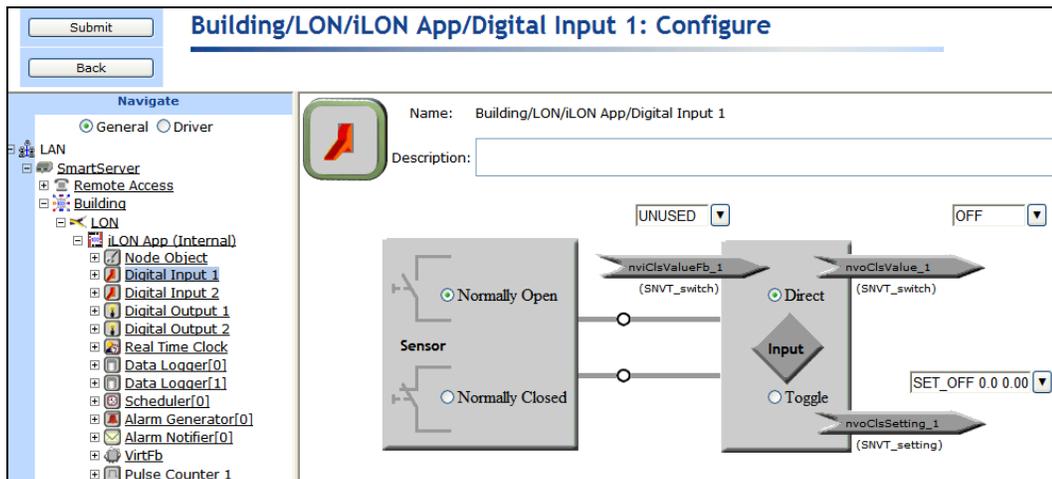
Connecting Digital Input Devices

The SmartServer includes two optically isolated, polarity sensitive digital inputs that you can use to monitor switch and sensor devices such as switches and push buttons and send the data to other devices. To connect a digital input device to the SmartServer and use the Digital Input application, follow these steps:

1. Connect the digital input device to one of the digital inputs on the SmartServer. See the SmartServer *Hardware Guide* for instructions on how to do this.
2. Open the Digital Input application on the SmartServer. To do this, click **General**; expand the network icon in the SmartServer tree, expand the **LON** channel, expand the **i.LON App (Internal)** device; and then click **Digital Input** functional block corresponding to the input connection on the SmartServer to which the device is attached.



3. The **Digital Input: Configure** Web page opens.



4. The Digital Input application contains the following three data points:

- **nviClsValueFB (SNVT_switch)**. Used to synchronize a group of switches.
- **nvoClsValue (SNVT_switch)**. Sends the value and state of the digital input (ON or OFF) to a device that accepts a **SNVT_switch** input. The value and state are derived from the raw values received from the device.
- **nvoClsSetting (SNVT_setting)**. Sends the setting, scene setting level, and rotation angle of the digital input device (SET_ON 0.0 0.00 or SET_OFF 0.0 0.00) to devices such as occupancy sensors and constant light controllers that accept a **SNVT_setting** input.

5. Select whether the digital input device uses a **Normally Open** or **Normally Closed** sensor. This determines how the signal received from the digital input device is processed before being sent to the **nvoClsValue** and **nvoClsSetting** output data points.

- Select **Normally Open** if the sensor normally does not conduct electricity when it is open. When this option is selected, an OFF value is sent when the sensor is open and an ON value is sent when it is closed. This means that signal received from the digital input device is sent directly to the **nvoClsValue** and **nvoClsSetting** output data points.
 - Select **Normally Closed** if the sensor normally conducts electricity when it is open. When this option is selected, an ON value is sent when the sensor is open and an OFF value is sent when it is closed. This means that signal received from the digital input device is inverted before being sent to the **nvoClsValue** and **nvoClsSetting** output data points.
6. Select how the state of the hardware input is translated to the **nvoClsValue** and **nvoClsSetting** output data points.
 - Select **Direct** to have the **nvoClsValue** and **nvoClsSetting** output data points reflect the current state of the hardware input (ON or OFF). This option is typically selected for switch devices connected to the SmartServer. This is the default.
 - Select **Toggle** to have the **nvoClsValue** and **nvoClsSetting** output data points switch from OFF to ON or ON to OFF when the hardware input changes. This option is typically selected for push button devices connected to the SmartServer.
 7. Optionally, you can set manual override values for each of the three data points in their respective input boxes. If you set an override value, the SmartServer uses this value and ignores any updates to it regardless of the current state of the hardware input.

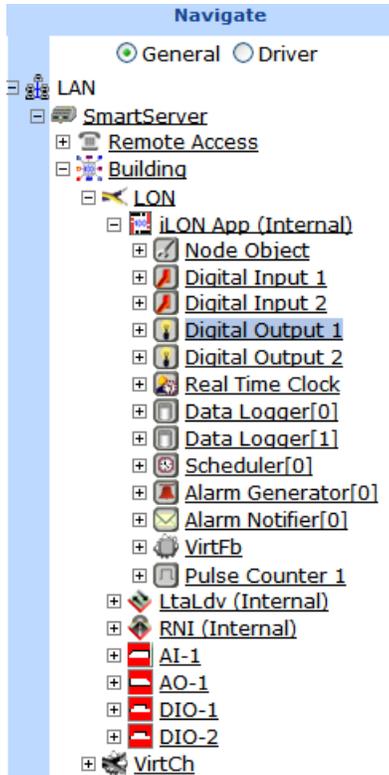
To set an override value, you can select one of the pre-defined presets for the data point or enter a properly formatted value. A manual override icon () indicates that the data point is in manual override mode.

The Digital Input application uses a priority of 100 to write values to the data point. This means that another application must have a priority of 100 or higher to write to the data point. You can release the lock the Digital Input application has on a data point, by clicking the Manual Override icon. This temporarily resets the Digital Input application's priority to 255 (the default value), and it causes the SmartServer to notify all other applications in which the subject data point is registered. The next highest priority application will then assume the priority for writing values to the data point.

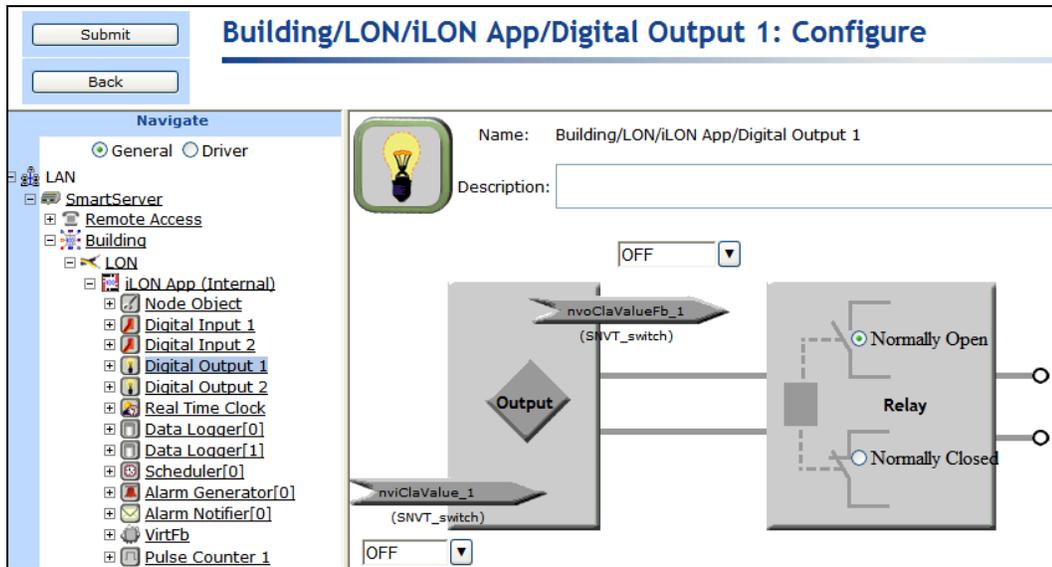
Connecting Digital Output Devices

The SmartServer includes two dry-contact relay outputs that you can use to control digital output devices such as drive contactors or alarm bells. To connect a digital output device to the SmartServer and use the Digital Output application, follow these steps:

1. Connect the digital output device to one of the dry-contact relay outputs on the SmartServer. See the SmartServer *Hardware Guide* for instructions on how to do this.
2. Open the Digital Output application on the SmartServer. To do this, click **General**; expand the network icon in the SmartServer tree, expand the **LON** channel, expand the **i.LON App (Internal)** device; and then click **Digital Input** functional block corresponding to the input connection on the SmartServer to which the device is attached.



3. The **Configure – Digital Output** Web page opens.



4. The Digital Output functional block contains the following two data points:
 - **nviClaValue (SNVT_switch)**. Drives the relay of the digital output hardware.
 - **nvoClaValueFB (SNVT_switch)**. Indicates the last value sent to the **nviClsValue** data point. It is used to synchronize a group of digital output devices.
5. Select how the state of the **nviClaValue** input data point is translated to the dry contact relay outputs.

- Select **Normally Open** to send the current state of the **nviClValue** input data point directly to the relay outputs. When this option is selected, the SmartServer opens the relay when an OFF value is received and closes it when an ON value is received. This is the default.
 - Select **Normally Closed** to invert the state of the **nviClValue** input data point before sending it to the relay outputs. When this option is selected, the SmartServer opens the relay when an ON value is received and closes it when an OFF value is received.
6. Optionally, you can set manual override values for each of the two data points in their respective input boxes. If you set an override value, the SmartServer uses this value and ignores any updates to it.

To set an override value, you can select one of the pre-defined presets for the data point or enter a properly formatted value. A manual override icon () indicates that the data point is in manual override mode.

The Digital Output application uses a priority of 100 to write values to the data point. This means that another application must have a priority of 100 or higher to write to the data point. You can release the lock the Digital Output application has on a data point, by clicking the Manual Override icon. This temporarily resets the Digital Output application's priority to 255 (the default value), and it causes the SmartServer to notify all other applications in which the subject data point is registered. The next highest priority application will then assume the priority for writing values to the data point.

Using Analog Functional Blocks

This chapter describes how to use the Analog Functional Block application to perform mathematical and logical operations on a set of input points and store the result in an output point, which can be used to control one or more actuator devices.

Analog Functional Block Overview

The SmartServer includes an Analog Functional Block that you can use to perform mathematical or logical operations on a set of input points and store the result in a specified output point. The Analog Functional Block will then perform the specified operation each time any of the input points are updated or at a specific interval.

You can select any scalar data point (data point with a single field) or the field of structured data point as an input point. After you select the input points, you specify whether the Analog Functional Block performs a mathematical or logical function on the input points. You can select a mathematical operation to determine the minimum, maximum, average, or sum of two or more input points. The calculated data point value is then written to the output point you specify (provided that it does not exceed or go below the maximum and minimum values you specify). For example, consider a case in which three **SNVT_temp_f** input points with values of 68, 72.5, and 78 are selected and a mathematical function is selected and set to **Average**. The value sent to the output point is 72.83 (the sum of the data points [218.5] divided by the number of input points [3]), provided that it does not exceed or go below the specified maximum or minimum values.

You can use select a logical operation to compare the value of one or more input points to that of a compare point, which can be another data point or a constant value. The Analog Functional Block evaluates whether one, all, or a percentage of the input points are equal, not equal, less than, less than or equal, greater than, or greater than or equal to the compare point based on the logical and output functions you select. The result of the logical operation (TRUE or FALSE) is to the output point you specify. For example, consider a case in which five input points are selected, a logical function is selected and set to Greater Than, and three of the data points are actually greater than the compare point:

- If the output function is set to **And**, which means all the selected data points must be greater than the compare point to return a TRUE value, the result of the logical function is FALSE.
- If the output function is set to **Or**, which means that only one of the selected data points needs to be greater than the compare point to return a TRUE value, the result of the logical function is TRUE.
- If the output function is set to **Majority** and the specified percentage is **50%**, which means that at least half of the selected data points needs to be greater than the compare point to return a TRUE value, the result of the logical function is TRUE as 60% of the data points are greater than the compare point.

After you select and configure a mathematical or logical operation, you select an output point. If the Analog Functional Block is performing a mathematical operation, you can select a scalar data point with the same type as the selected input points as the output point. If the Analog Functional Block is performing a logical operation, you must select a **SNVT_switch** data point as the output point. You can use the result stored in the output point to control one or more actuator devices.

You can create up to 20 Analog Functional Blocks per SmartServer if you are using the default SmartServer v12 static interface. You can add more than 20 Analog Functional Blocks if you activate the v40 dynamic interface, which features a dynamic external interface, on your SmartServer. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

Creating an Analog Functional Block

To create an analog functional block, do the following:

1. Open an Analog Functional Block application.
2. Select input points, which can include scalar data points or the individual fields of structured data points. If you are performing a mathematical operation select two or more input points; if you are performing a logical operation select one or more input points and a compare point.

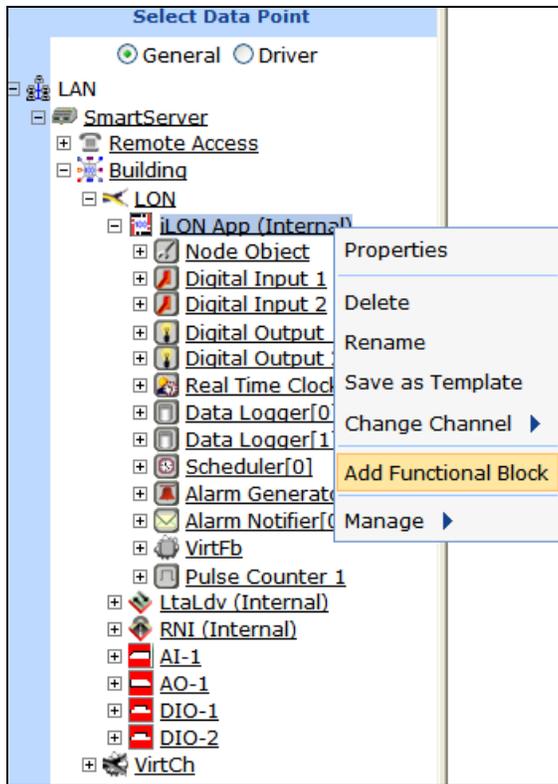
3. Select and configure a mathematical or logical operation.
4. Select a scalar or **SNVT_switch** output point and specify override behavior.

Opening an Analog Functional Block Application

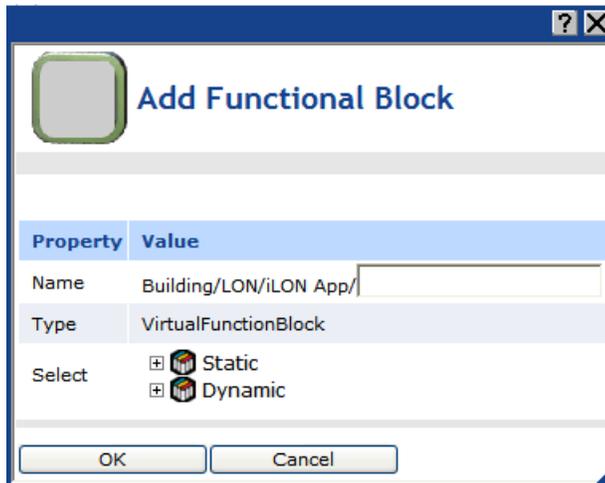
To open an Analog Functional Block application, you must first create an analog functional block. After you create the analog functional block, it appears on the SmartServer tree below the **i.LON App (internal)** device, and you can click the functional block to open the Analog Functional Block application.

To create an Analog Functional Block and open the application, follow these steps:

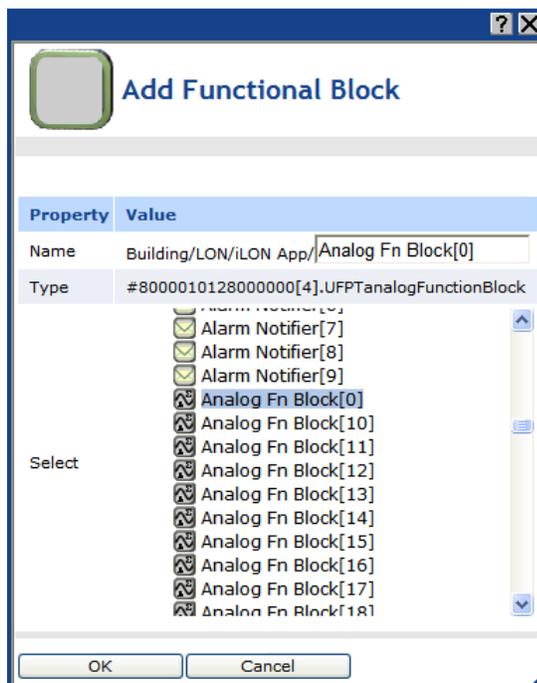
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



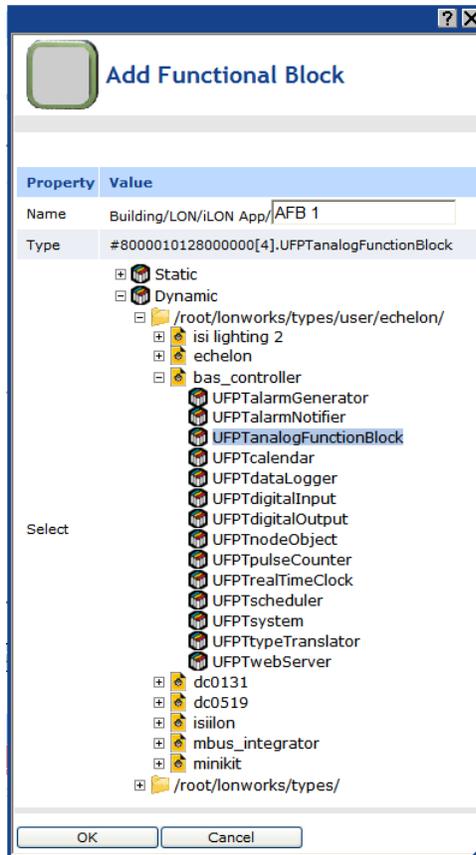
4. The **Add Functional Block** dialog opens.



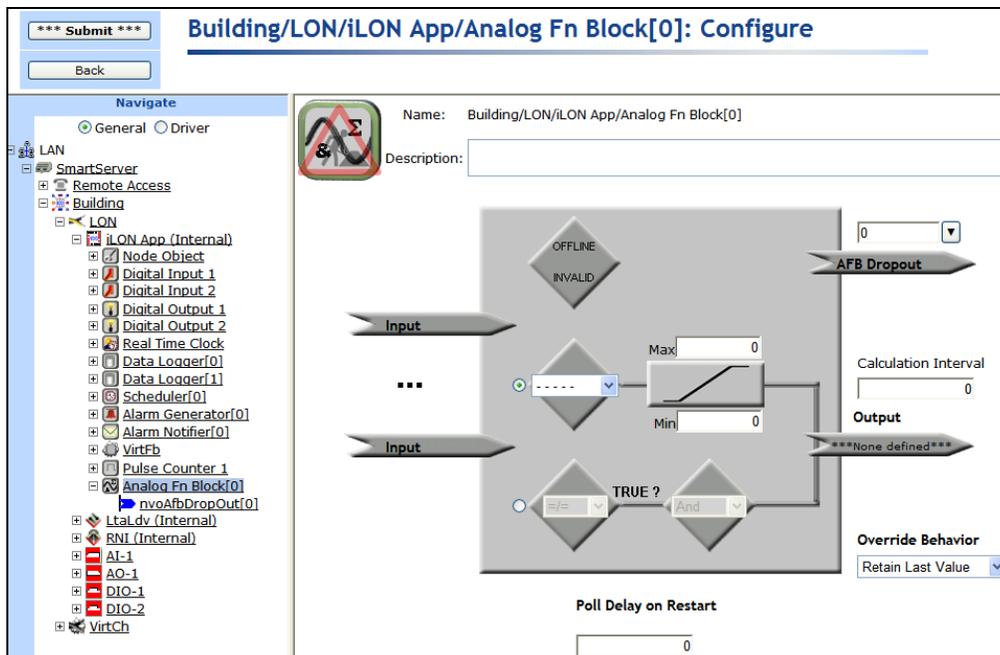
5. Select the Analog Functional Block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Analog Functional Block** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Analog Functional Block from either the **Static** or the **Dynamic** folder. To select the Analog Functional Block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the Analog Functional Block, enter a name for the functional block such as “AFB 1”, and then click **OK**.



6. A functional block representing the Analog Functional Block application and all of its static data points are added to the bottom of the **iLON App (Internal)** device tree, and the **Analog Functional Block: Configure** Web page opens in the application frame to the right. The construction symbol overlaid onto the Analog Functional Block application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



7. Click **Submit**.

To open the Analog Functional Block application from an existing Analog Functional Block, follow these steps:

1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Analog Functional Block application.
2. Click the Analog Functional Block representing the Analog Functional Block to be opened. The **Analog Functional Block: Configure** Web page opens in the application frame to the right.

Selecting Input Points

You can select any scalar data point (data point with a single field) or the field of structured data point as an input point. If you are performing a mathematical operation select two or more input points; if you are performing a logical operation select one or more input points and a compare point.

1. Click one of the **Input Points** icons (). The **Analog Functional Block: Data Points** Web page opens.
2. Select the data points on which the Analog Functional Block is to operate from the SmartServer tree. References to the selected input points () are added to the bottom of the Analog Functional Block tree, and references to the Analog Functional Block are added directly below the selected input points ().

To select a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).

Building/LON/iLON App/Analog Fn Block[0]: Data Points			
<input type="checkbox"/> Show Advanced			
	Data Point	Format	Poll Rate
0	Building/LON/DIO-1/Digital Encoder[0]/DE_D1_1	#0000000000000000[0].SNVT_switch	15min
1	Building/LON/DIO-2/Digital Encoder[0]/DE_D1_1	#0000000000000000[0].SNVT_switch	15min

3. View the following properties of the selected data points:

Data Point Displays the name of the data point being recorded using the following format: <network>/<channel>/<device>/<functional block>/<data point>. This is also the location of the data point in the SmartServer tree.

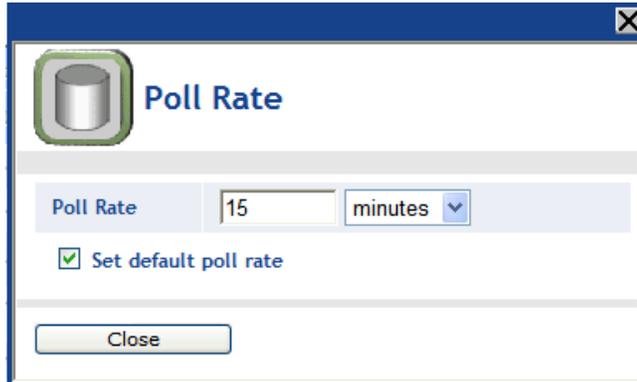
Format Displays the SNVT, UNVT, or built-in data type used by the data point, and it specifies the format (for example, SI metric or US customary) used if the type has multiple formats such as **SNVT_temp_f**. This field is read-only.

4. Select the **Show Advanced** check box to view the following properties and configure the rate at which the data points are updated.

Building/LON/iLON App/Analog Fn Block[0]: Data Points					
<input checked="" type="checkbox"/> Show Advanced					
	Data Point	Format	Field Name	Unit	Poll Rate
0	Building/LON/DIO-1/Digital Encoder[0]/DE_D1_1	#0000000000000000[0].SNVT_switch	SNVT_switch		15min
1	Building/LON/DIO-2/Digital Encoder[0]/DE_D1_1	#0000000000000000[0].SNVT_switch	SNVT_switch		15min

<i>Field Name</i>	If the selected input point is a structured data point (has multiple fields) , select the field to be used in the selected function. For example, if the selected input point has a SNVT_switch data type, you can use the value or state fields of the data point in the function.
<i>Unit</i>	Displays the unit string describing the data point to be updated. A SNVT_temp_f#US data point, for example, has “degrees F” describing the data point. A SNVT_switch data point has “% of full level” and “state code” unit strings describing its state and value fields. This field is read-only. You can edit the unit string of a data point in the Configure - Data Points Web page, which you can access by clicking the data point in General mode.
<i>Poll Rate</i>	Displays the rate at which the Analog Functional Block polls the SmartServer’s internal data server for updated data point values. The default rate is 15 minutes. If the poll rate is set to 0, the data point will only be updated when its value changes.

- To configure the rate at which the Analog Functional Block polls the value of the selected data points in the application, click the **Poll Rate** box for the data point. The **Poll Rate** dialog opens.



- In the **Poll Rate** box, enter a value and then select a measurement of time (seconds, minutes, or hours). The default poll rate is **15 minutes**. To apply the specified poll rate to only the selected data point, clear the **Set Default Poll Rate** check box. Click **Close** to return to the **Analog Functional Block: Data Points** Web page.
- Click **Submit**.
- Click **Back** to return to the **Analog Functional Block: Configure** Web page.
- In the **Poll Delay On Restart** box, specify the amount of time (in seconds) that the Analog Functional Block waits after a reset before polling the values of the input data points. The default value is **0**, which means that the Analog Functional Block will resume polling the data points at the poll rates specified in the **Analog Functional Block: Data Points** Web page.
- Click **Submit**.

Selecting and Configuring a Mathematical or Logical Operation

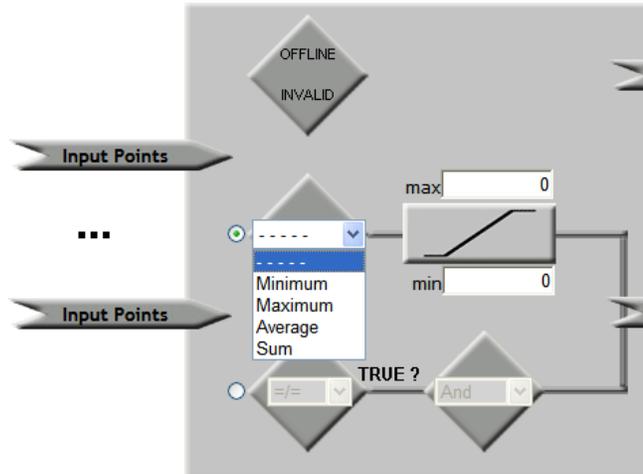
You specify whether the Analog Functional Block performs a mathematical or logical function on the selected input points. You can select a mathematical operation to determine the minimum, maximum, average, or sum of two or more input points. You can use select a logical operation to compare the value of one or more input points to that of a compare point, which can be another data point or a constant value.

Selecting and Configuring a Mathematical Operation

You can select a mathematical operation to determine the minimum, maximum, average, or sum of two or more input points and then specify the minimum and maximum values that can be passed to the output data point.

To select and configure a mathematical operation, follow these steps:

1. Click the middle icon, which is selected by default.



2. Select one of the following mathematical functions from the list to determine the value to be sent to the output point:
 - Select **Minimum** to send the value of the input point with the lowest value.
 - Select **Maximum** to send the value of the input point with the highest value.
 - Select **Average** to send the average value of the input points (sum divided by number of input points). If you select this option, you can set the **Depth** property to calculate a straight average from the previous averages. For example, if you set the **Depth** property to 2, the average equals the sum of the last two calculated averages divided by two. This means that if the last calculated average was 20, and the previous calculated average was 30, the average value sent to the output point is 25.
 - Select **Sum** to send the total sum of the input point values.
3. In the **Max** and **Min** boxes, specify the maximum and minimum values that can be sent to the output point. If the calculated value exceeds the maximum or goes below the minimum, the maximum or minimum value is sent to the output point instead of the calculated value.
4. Click **Submit**. After you select an output point, the Analog Functional Block will perform the specified mathematical function each time any of the input points are updated and store the result in the specified output data point.

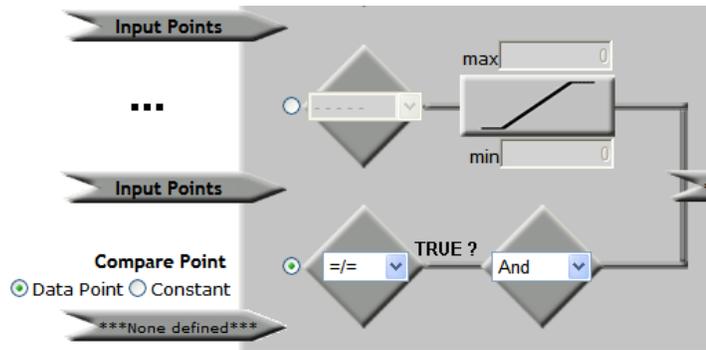
Selecting and Configuring a Logical Operation

You can use select a logical operation to compare the value of one or more input points to that of a compare point, which can be another data point or a constant value. The Analog Functional Block evaluates whether one, all, or a percentage of the input points are equal, not equal, less than, less than or equal, greater than, or greater than or equal to the compare point based on the logical and output functions you select. The result of the logical operation, TRUE or FALSE, is sent to the specified output point.

To select and configure a mathematical operation, follow these steps:

1. Click the bottom icon.

2. A **Compare Point** property appears on the Web page.

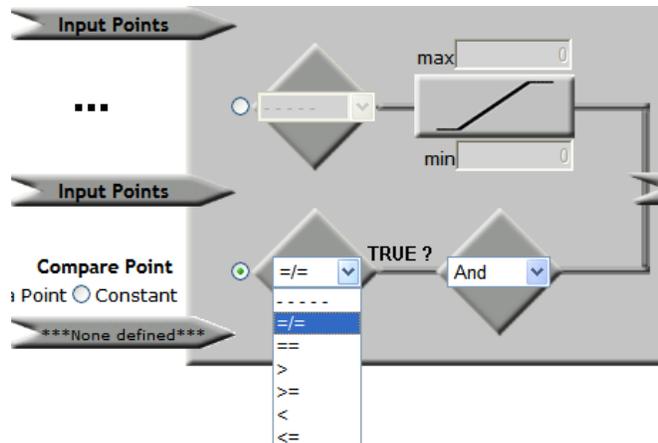


3. Select whether the compare point is another data point or a constant value.

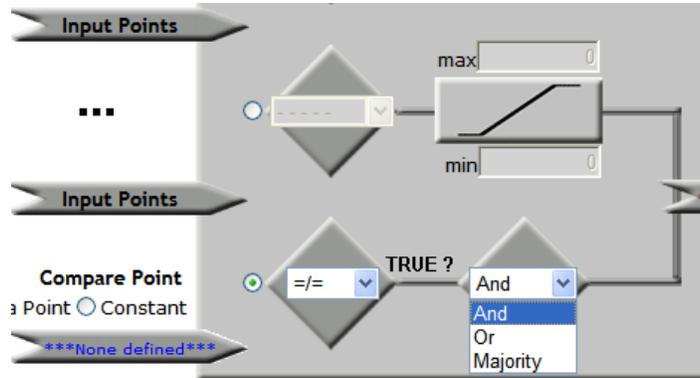
- Click **Data Point** to select a data point as the compare point. Click the **None Defined** icon (*****None defined*****), which turns the text in the icon blue, and then click the data point in SmartServer tree to be used as the compare point. The value of the selected data point will be compared to the values of the selected input points.
- Click **Constant** to enter a specific value in the box that appears to be compared to the values of the selected input points.

4. Select one of the following logical functions from the list to determine whether a TRUE or FALSE value is to be sent to the output point:

- \neq . Returns TRUE if the value of the input data point does not equal the value of the compare data point.
- $=$. Returns TRUE if the value of the input data point equals the value of the compare data point.
- $>$. Returns TRUE if the value of the input data point is greater than the value of the compare data point.
- \geq . Returns TRUE if the value of the input data point is greater than or equal to the value of the compare data point.
- $<$. Returns TRUE if the value of the input data point is less than the value of the compare data point.
- \leq . Returns TRUE if the value of the input data point is less than or equal to the value of the compare data point.



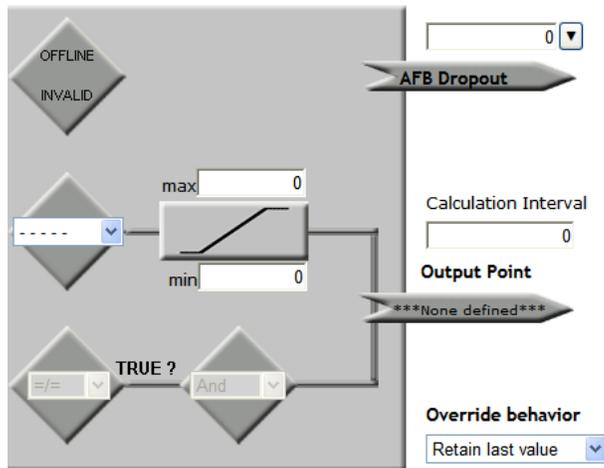
5. From the **True?** list, select whether one, all, or a minimum percentage of the input points need to evaluate to TRUE in order for the logical function to send a TRUE value to the output point.
 - Select **And** to require that all the selected data points evaluate to TRUE in order for the logical function to return a TRUE value.
 - Select **Or** to require that only one of the selected data points evaluates to TRUE in order for the logical function to return a TRUE value
 - Select **Majority** to specify a minimum percentage of data points that must evaluate to TRUE in order for the logical function to return a TRUE value. If you select this option, enter a percentage in the box that appears below the output function box.



6. Click **Submit**. After you select an output point, the Analog Functional Block will perform the specified logical function each time any of the input points are updated and store the result in the specified output data point.

Selecting an Output Point

After you select and configure a mathematical or logical operation, you select an output point. The output point may be any scalar data point or a **SNVT_switch** data point. You can then configure how the output point is updated and overridden.

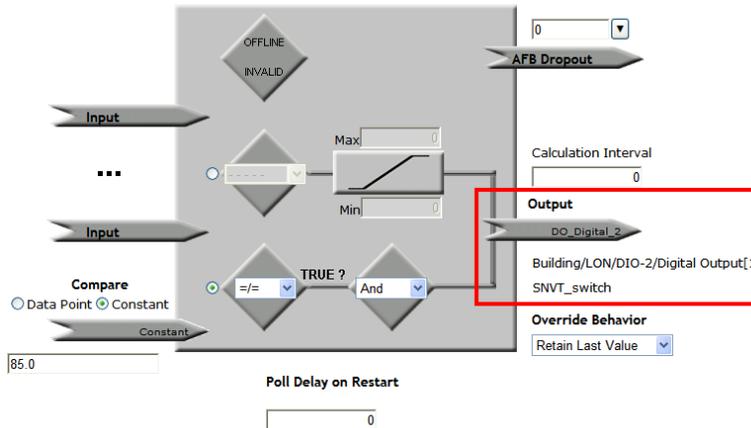


To select an output point, follow these steps:

1. Click the **None Defined** icon below the **Output Point** text on the right side of the application. The text in the icon is highlighted blue.



2. Click a scalar data point with the same data type as the selected input points or select a **SNVT_switch** data point in the SmartServer tree to be used as the output point.
 - If the Analog Functional Block is performing a mathematical operation, you can select a scalar data point with the same type as the selected input points.
 - If the Analog Functional Block is performing a logical operation, you must select a **SNVT_switch** data point as the output point.
3. The programmatic name of the selected data point appears on the output point icon and the programmatic name and type of the data point are listed directly below the icon.



4. Click **Submit**. The Analog Functional Block will perform the specified mathematical or logical function each time any of the input points are updated and store the result in the specified output data point.
 - If the Analog Functional Block is performing a mathematical function, the calculated value is stored in the selected scalar output point.
 - If the Analog Functional Block is performing a logical function, and the function returns TRUE, the **SNVT_switch** output point is set to 100.0 1. If the function returns FALSE, the **SNVT_switch** output point is set to 0.0 0.
5. In the **Calculation Interval** box on the right side of the application, you can specify the amount of time (in seconds) that must elapse between updates to the output point. Setting an interval may be useful to ensure that the output data point is only updated when all the input point updates have been received. The default value is 0, which means that the Analog Functional Block updates the output point each time an input point is updated.

Calculation Interval

6. In the **Override Behavior** box on the right side of the application, you can specify the behavior of the output data point when the analog functional block is placed in override mode.
 - Select **Retain Last Value** for the output data point to retain the last value assigned to it by the Analog Functional Block. This is the default.
 - Select **Use Specified Value** and then enter a value in the **Value** box that appears below to be assigned to the data point.
 - Select **Use Default Value** to assign the output data point its default value, as defined for its type in the resource files. You can change the default value for a data in the **Configure - Data Points** Web page, which you can access by clicking the data point in **General** mode.

Output

DO_Digital_2

Building/LON/DIO-2/Digital Output[1]
SNVT_switch

Override Behavior

Retain Last Value

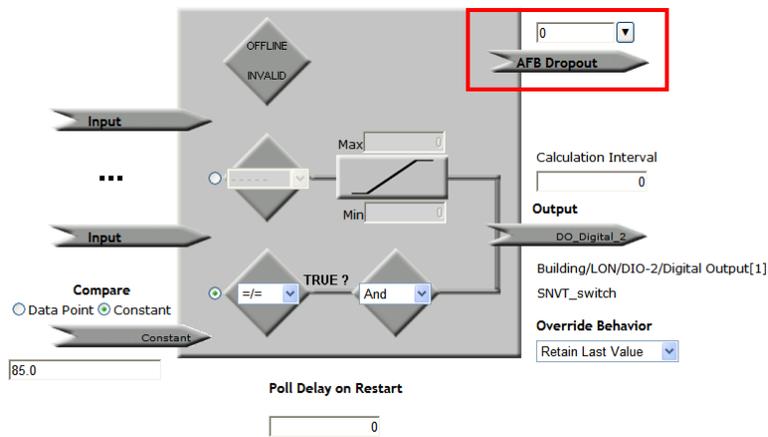
Retain Last Value

Use Specified Value

Use Default Value

7. Click **Submit**. You can use the result stored in the output point to control one or more actuator devices.

Note: The **AFB Dropout** box indicates the number of input points with an OFFLINE or INVALID status.



Using Type Translators

This chapter describes how to use the Type Translator on the SmartServer to connect devices with different data types. It describes how to create and use scalar-based translations to directly convert an input data point with one type to an output data point with another type. It explains how to create and use rule-based translations that merge multiple input points to create one output point, split one input point to create multiple output points, and split a structured data point into its individual fields.

Type Translator Overview

The SmartServer includes a Type Translator that can convert data points of one type to another type. This enables you to connect LONWORKS devices with incompatible external interfaces and integrate data generated by BACnet, Modbus, and M-Bus devices into a LONWORKS network.

With the type translator, you can use scalar-based or rule-based translations to connect devices with different data types. A scalar-based translation lets you directly convert an input point of one type to an output point of another type (the data points must be both be of an integral or floating-point type). For example, you can use a scalar-based translation in an HVAC system to convert a **SNVT_temp** input data point generated by a thermostat to a **SNVT_temp_p** output data point used by a chiller. In this case, both data points have an integral data type (a long).

A rule-based translation lets you convert, split, and merge input data points using case logic to generate the desired output. This is useful for translating structured data points as their individual fields can be isolated. For example, you can use a rule-based translation to have a scene controller turn on, illuminate, and turn off a lamp and set the position of a sunblind. In this case, the function and scene_number fields of the scene controller's **SNVT_scene** data point determine the settings of the value and state fields of the lamp's **SNVT_switch** data point and the function, setting, and rotation fields of the sunblind's **SNVT_setting** data point.

To create a type translator, you select the input and output points to be converted, and then you either select a pre-defined translation that is applicable to the selected data points or create a custom translation.

The SmartServer comes with 15 pre-defined translations. This includes one pre-defined scalar-based translation that directly converts an input point to an output point, which you can use for all your scalar-based translations that do not require scaling, and 14 pre-defined rule-based translations. The rule-based translations including ones for LONWORKS devices that convert a **SNVT_switch** data point to a **SNVT_setting** data point and vice versa, convert 16 **SNVT_switch** data points to one **SNVT_switch.state** data point and vice versa, split a **SNVT_setting** data point into its individual fields and conversely merge the fields to create a **SNVT_setting** data point, and so on. In addition, the pre-defined rules include ones for converting M-Bus data points.

If none of the pre-defined rule-based translations are compatible with your specific application, you can create your own custom scalar-based or rule-based translation. Creating a custom scalar-based translation entails simply defining the scaling to be performed on the value of the input point before it is converted to the output point. Creating a custom rule-based translation entails defining one or more cases and a rule for each case that executes when the case is true. You can specify whether a case is always true or if it is only true when an expression is true. The expression can be an if-then statement or a nested if-then statement. The rule specifies the value to be copied from the input point to the output point.

After you select the input and output points, and select or create a type translation, you specify the period of time the Type Translator waits after an input data point has been updated before performing a translation.

You can create up to 40 Type Translators per SmartServer if you are using the default SmartServer v12 static interface. You can add more than 40 Type Translators if you activate the v40 dynamic interface on your SmartServer, which features a dynamic external interface. See *Activating the SmartServer V40 XIF* in Chapter 3, *Configuring and Managing the SmartServer*, for more information on loading the V40 interface on the SmartServer.

Creating a Type Translator

To create a type translator, do the following:

1. Open a Type Translator application.
2. Select the input points and output points to be translated.

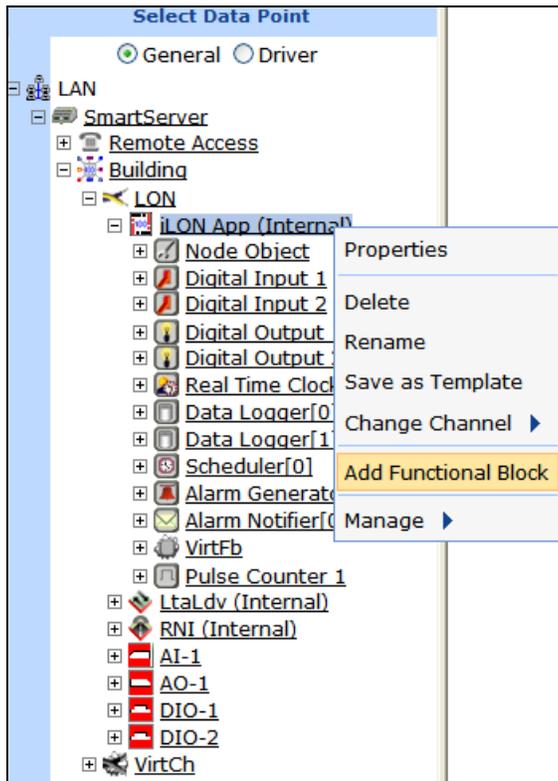
3. Select a pre-defined type translation that is compatible with the selected input and output points, or create a custom rule-based translation.
4. Specify a delay.

Tip: If you plan on using a pre-defined type translation, you can reverse the order of steps 2 and 3. One advantage of doing this is that the Type Translator will guide you on the types of data points to be selected for that translation. If you need to create a custom type translation, perform the steps in the order listed.

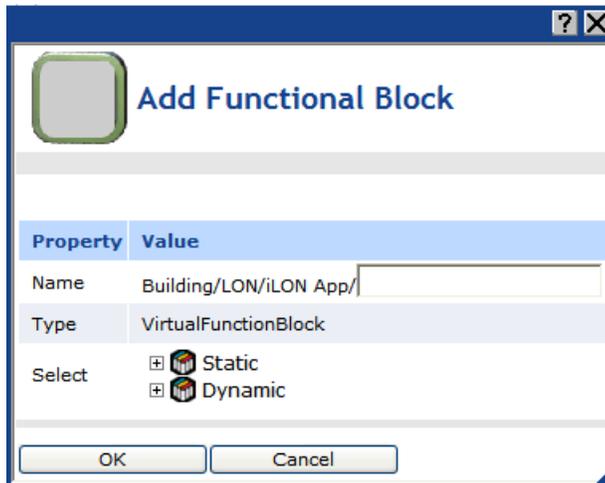
Opening a Type Translator

To create a Type Translator functional block and open the Type Translator application, follow these steps:

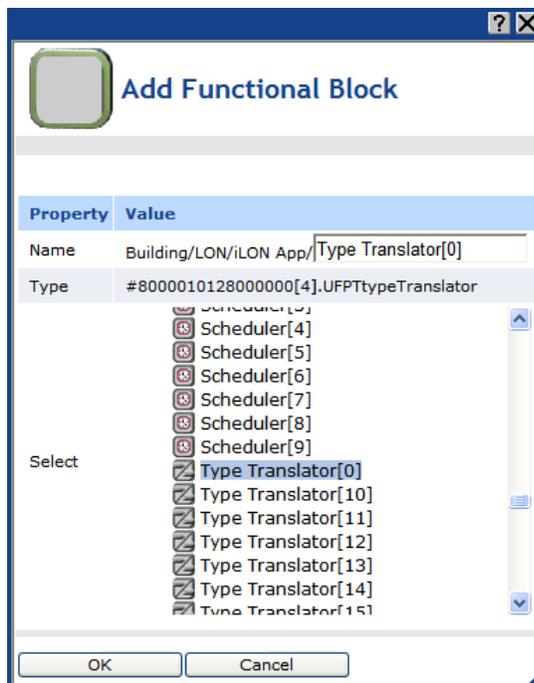
1. Click **General** above the navigation pane in the left frame of the SmartServer Web interface.
2. Expand the network icon in the SmartServer tree, and then expand the **LON** channel to show the **i.LON App (Internal)** device.
3. Right-click the **i.LON App (Internal)** device and then select **Add Functional Block** in the shortcut menu.



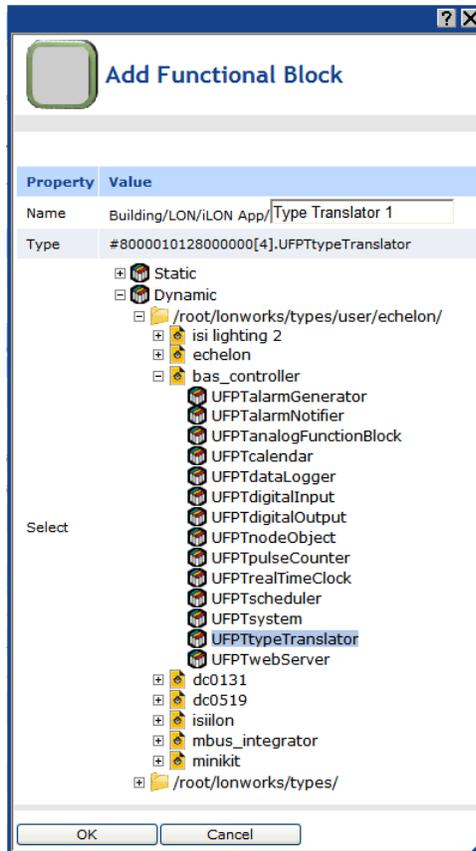
4. The **Add Functional Block** dialog opens.



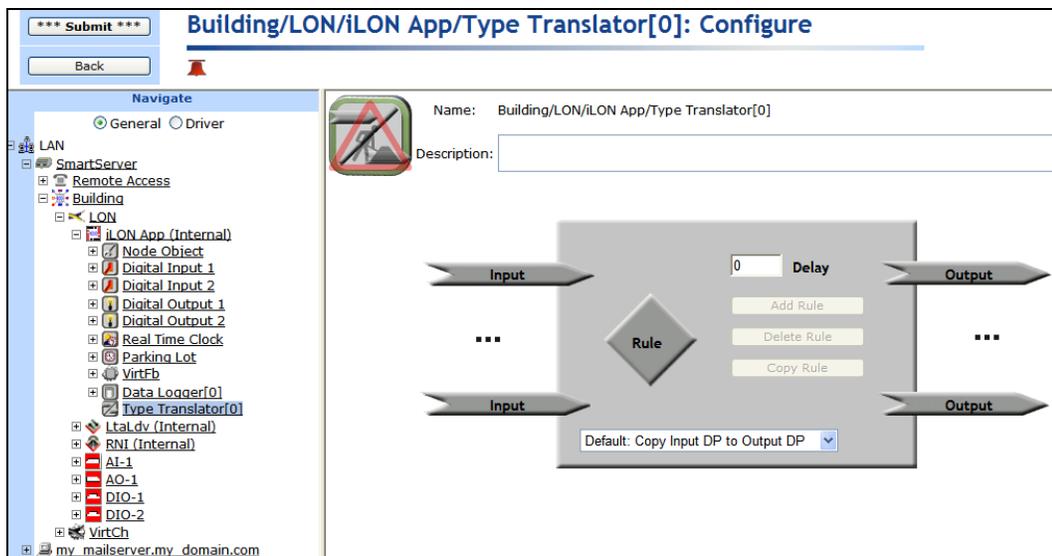
5. Select the Type Translator functional block from the **Static** or **Dynamic** LonMark folder. The folder available in the dialog depends on whether the SmartServer is using the static v12 interface or the dynamic v40 interface.
 - If the SmartServer is using the static v12 interface (the default), expand the **Static** icon, select the **Type Translator** functional block, optionally enter a different name than the default programmatic functional block name, and then click **OK**.



- If you have activated the dynamic v40 interface on the SmartServer and you are managing the network in Standalone mode, you can select the Type Translator functional block from either the **Static** or the **Dynamic** folder. To select the Type Translator functional block from the **Dynamic** folder, expand the **Dynamic** icon, expand the **/lonworks/types** folder, expand the **bas_controller** folder, select the user-defined functional profile for the Type Translator functional block, enter a name for the functional block such as “Type Translator 1”, and then click **OK**.



6. A functional block representing the Type Translator functional block application and all of its static data points are added to the bottom of the **iLON App (Internal)** device tree, and the **Type Translator: Configure** Web page opens in the application frame to the right. The construction symbol overlaid onto the Type Translator functional block application icon in the upper-left hand corner of the Web page indicates that the application has not been configured yet.



7. Click **Submit**.

To open the Type Translator functional block application from an existing Type Translator functional block, follow these steps:

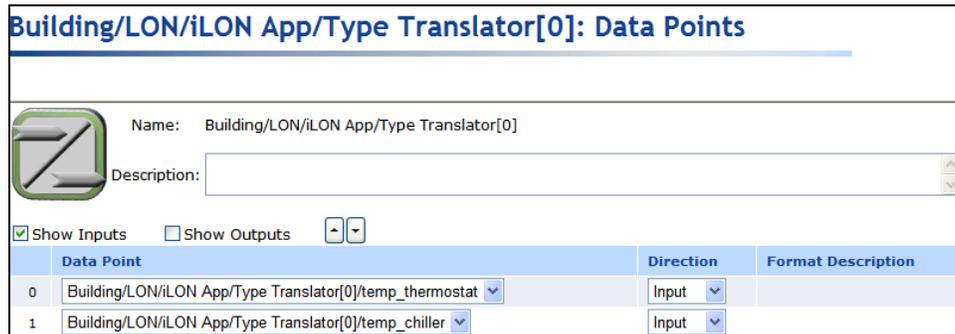
1. Click **General** if the SmartServer is not already operating in **General** mode. If the SmartServer is in **Driver** mode when you click the functional block, the **Setup - LON Functional Block Driver** Web page opens instead of the Type Translator functional block application.
2. Click the Type Translator functional block representing the Type Translator functional block to be opened. The **Type Translator: Configure** Web page opens in the application frame to the right.

Selecting Input and Output Points

You can select the input and output points to be used in the translation. To select a data point, follow these steps:

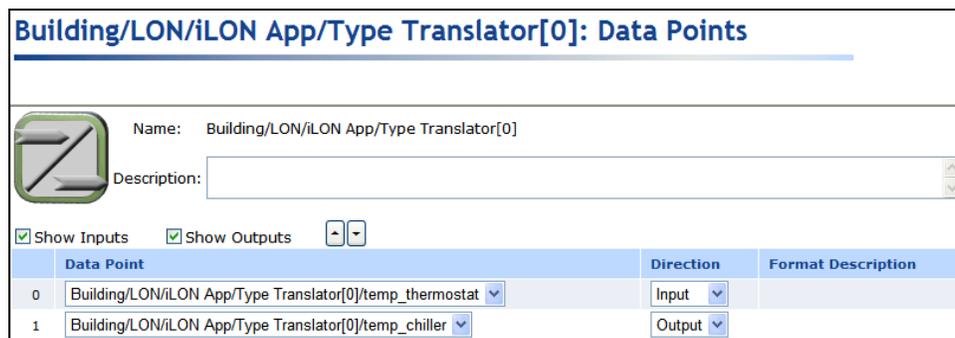
1. Click the **Input** data point icon () on the left side of the **Type Translator: Configure** Web page.
2. The **Type Translator: Data Points** Web page opens. Click the data points to be used by the Type Translator from the SmartServer tree. References to the selected data points () are added to the bottom of the Type Translator functional block tree, and references to the Type Translator functional block are added directly below the selected data points (). By default, only input data points will be shown. To show the output data points, select the **Show Outputs** check box.

To select a data point of an external device that is being managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application, you must first copy the data point from the OpenLNS tree to the SmartServer tree (see *Adding Data Points to SmartServer Applications* in Chapter 4 for more information).



	Data Point	Direction	Format Description
0	Building/LON/iLON App/Type Translator[0]/temp_thermostat	Input	
1	Building/LON/iLON App/Type Translator[0]/temp_chiller	Input	

3. Under the **Direction** column, select whether the data point is an input or output point. When you select **Output**, the data point is added to the list of output points. You can access the list of output points by clicking the **Output** data point icon () on the right side of the **Type Translator: Configure** Web page.



	Data Point	Direction	Format Description
0	Building/LON/iLON App/Type Translator[0]/temp_thermostat	Input	
1	Building/LON/iLON App/Type Translator[0]/temp_chiller	Output	

Note: If you have selected a pre-defined type translation prior to selecting the data points in the translation, an additional **Nickname** column appears in this Web page. The nickname is a

user-defined name that is associated with a given data point format description (for example, **SNVT_switch** or **SNVT_temp**). Nicknames are used in a type translation rule to reference the selected input and output points. Once you have created and used a nickname do not modify it because doing so breaks all other existing Type Translators that use the same translation. By default, a data point's nickname is the data point portion of its full network name. For example, a data point with a name of “Net/LON/iLON App/VirtFb/nvoLevDisc” has a default nickname of “nvoLevDisc”.

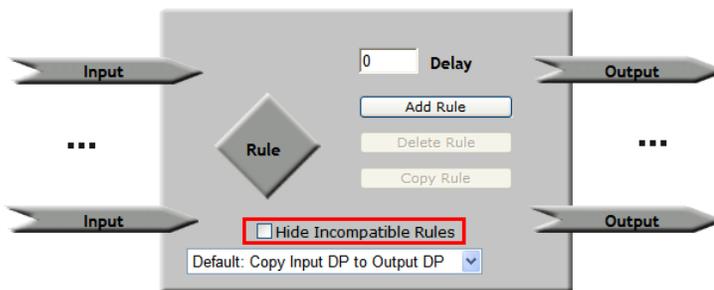
4. Click **Submit**.
5. Click **Back** to return to the **Type Translator: Configure** Web page.

Note: If you are using a scalar-based translation, the input and output points must be both be of an integral or floating-point type.

Selecting or Creating a Type Translation

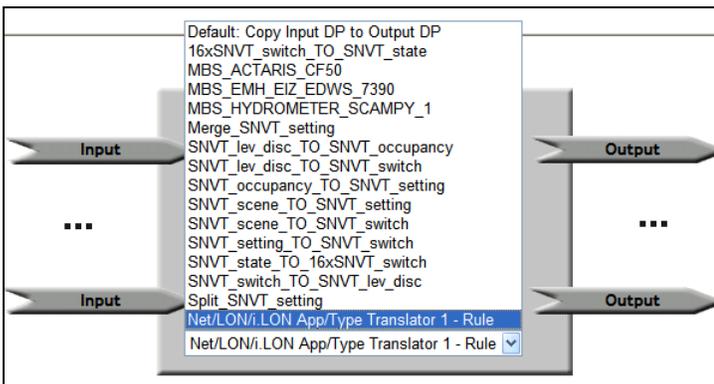
You can select a pre-defined type translation, or you can create a custom type translation. Once you create a custom type translation, you can select it and re-use it for other translations.

If you select a type translation that is not compatible with the selected input and output points, a “rule is incompatible” warning appears just above the tree/application frame. You can hide incompatible type translations by selecting the **Hide Incompatible Rules** check box directly below the **Rules** icon.



Selecting a Pre-Defined Type Translation

The Type Translator includes 15 pre-defined Type Translator rules that you select from the list below the **Rule** icon. You can select a pre-defined rule provided that it is compatible with the selected input and output points. Once you create a custom rule-based translation, it is added to the list of defined translations that you can select.



The default translation, **Copy Input DP to Output DP**, is a scalar-based translation that directly converts the value of the input point directly to the output point without any scaling. Of the other 14 pre-defined translations, which are all rule-based translations, 11 are for converting LONWORKS data points and 3 are for converting M-Bus data points. The following subsections describe each of the 11 pre-defined rule-based translations that you can use to convert LONWORKS data points. See

Integrating M-Bus Devices with a Type Translator in this chapter for more information on the three pre-defined type translations used to convert M-Bus data points.

16xSNVT_switch_TO_SNVT_state

This rule-based translation converts up to 16 **SNVT_switch** input data points into a single **SNVT_state** output data point. The value of the state field of each **SNVT_switch** data point is assigned a field in the **SNVT_state** output data point.

You can select up to 16 input **SNVT_switch** data points and a single output **SNVT_state** data point. The value of the state field of the input **SNVT_switch** data points referenced by these elements will be read and stored in the **SNVT_state** output data point in the order they appear in the Inputs list. For example, the value of the state field of the first input **SNVT_switch** data point in the Inputs list would be stored in the 0 bit of the output **SNVT_state** data point. If fewer than 16 data points are added to the Inputs list, the extra bits in the **SNVT_state** output data point will be assigned a value of 0.

Merge SNVT Setting

This rule-based translation merges a **setting_t** enumeration, a **SNVT_lev_cont** input data point, and a **SNVT_angle_deg** input data point to produce a **SNVT_setting** output data point.

SNVT_lev_desc_TO_SNVT_occupancy

This rule-based translation converts a **SNVT_lev_disc** input data point to a **SNVT_occupancy** output data point. You add a **SNVT_lev_disc** data point to the list of input points and a **SNVT_occupancy** data point to the list of output points. Each time a type translation is made, the **SNVT_occupancy** output data point is assigned a value based on the current enumeration stored in the **SNVT_lev_desc** input data point, as described in the following table:

SNVT_lev_desc (input point)	SNVT_occupancy (output point)
ST_NUL	OC_NUL
ST_OFF	OC_UNOCCUPIED
ST_ON	OC_OCCUPIED
ST_HIGH	OC_BYPASS
ST_LOW or ST_MED	OC_STANDBY

SNVT_lev_desc_TO_SNVT_switch

This rule-based translation converts a **SNVT_lev_disc** input point to a **SNVT_switch** data point. You add a **SNVT_lev_disc** data point to the list of input points and a **SNVT_switch** data point to the to the list of output points. Each time a type translation is made, the **SNVT_switch** output data point is assigned a value and state based on the current enumeration stored in the **SNVT_lev_desc** input data point, as described in the following table:

SNVT_lev_desc (input point)	SNVT_switch (output point)
ST_NUL	OFF
ST_OFF	value: 0.0 state: 0 (OFF)
ST_ON	value: 100.0 state: 1 (ON)
ST_HIGH	value: 75.0 state: 1 (ON)
ST_MED	value: 50.0 state: 1 (ON)

SNVT_scene (input point)	SNVT_switch (output point)
function: SC_NUL scene_number: 0	No update made to output data point
function: SC_NUL scene_number: >0	value: 0.0 state: 0 (OFF)
function: SC_RECALL scene_number: 1	value: 25.0 state: 1 (ON)
function: SC_RECALL scene_number: 2	value: 50.0 state: 1 (ON)
function: SC_RECALL scene_number: 3	value: 75.0 state: 1 (ON)
function: SC_RECALL scene_number: >3	value: 100.0 state: 1 (ON)
function: SC_RECALL scene_number: 255	value: 0.0 state: 0 (OFF)

SNVT_setting_TO_SNVT_switch

This rule-based translation converts a **SNVT_setting** input data point to a **SNVT_switch** output data point. You add a **SNVT_setting** data point to the list of input points and a **SNVT_switch** data point to the list of output points. Each time a type translation is made, the value and state fields of the **SNVT_switch** output data point are assigned values based on the current values stored in the function and setting fields of the **SNVT_setting** input data point, as described in the following table:

SNVT_scene (input point)	SNVT_switch (output point)
function: SET_STATE setting: <=100.0	value: 0.0 state: 0 (OFF)
function: SET_STATE setting: >100.0	value: <=setting> state: 0 (OFF)
function: SET_NUL setting: any	value: 0.0 state: 0 (OFF)

SNVT_state_TO_16xswitch

This rule-based translation converts a **SNVT_state** input data point to up to multiple **SNVT_switch** output data points. You add a **SNVT_state** data point to the list of input points and up to 16 **SNVT_switch** data point to the list of output points. Each time a type translation is made, the value and state fields for each **SNVT_switch** output data point are assigned values matching the value stored in the corresponding bit of the **SNVT_state** input data point.

For example, if the value stored in the 0 bit of the **SNVT_state** input data point is 1, the first **SNVT_switch** output data point will be assigned a value of 100.0 1. If the value stored in the 1 bit of the **SNVT_state** input data point is 0, the second **SNVT_switch** output data point will be assigned a value of 0.0 0.

SNVT_switch_TO_SNVT_lev_desc

This rule-based translation converts a **SNVT_switch** input point to a **SNVT_lev_desc** output data point. You add a **SNVT_switch** data point to the list of input points and a **SNVT_lev_desc** data point to the list of output points. Each time a type translation is made, the **SNVT_lev_desc** output data point is assigned an enumeration based on the current value and state stored in the **SNVT_switch** input data point, as described in the following table:

SNVT_switch (input point)	SNVT_lev_desc (output point)
value: any	ST_NUL

state: 0	
value: 0.0	ST_OFF
state: 1	
value: 0.1–25.0	ST_LOW
state: 1	
value: 25.0–50.0	ST_MED
state: 1	
value: 50.0–75.0	ST_HIGH
state: 1	
value: 75.0–100.0	ST_ON
state: 1	
value: >100.0	ST_NUL
state: 1	

Split SNVT Setting

This rule-based translation splits the **SNVT_setting** input data point to produce three output data points corresponding to each of its fields: function (a **setting_t** enumeration), setting (**SNVT_lev_cont**), and rotation (**SNVT_angle_deg**).

Creating a Custom Type Translation

If none of the pre-defined translations are compatible with your specific application, you can create your own custom scalar-based or rule-based translation. To create a custom scalar-based translation, define the scaling to be performed on the value of the input point before it is converted to the output point.

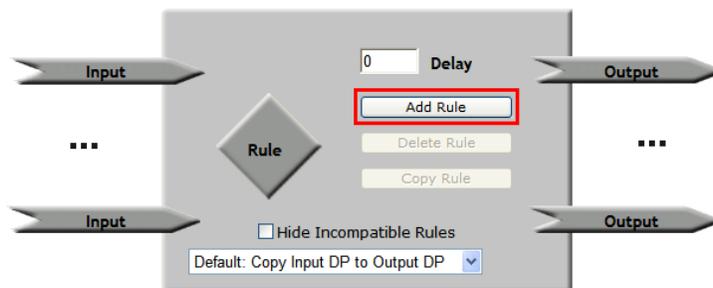
To create a custom rule-based translation, define one or more cases and a rule for each case that executes when the case is true. You can specify whether a case is always true or if it is only true when an expression is true. The expression can be an if-then statement or a nested if-then statement. The rule specifies the value to be copied to the output points. Once you create a custom type translator rule, you can select it from the list of defined rules and use it for other translations.

Creating a Custom Scalar-Based Translation

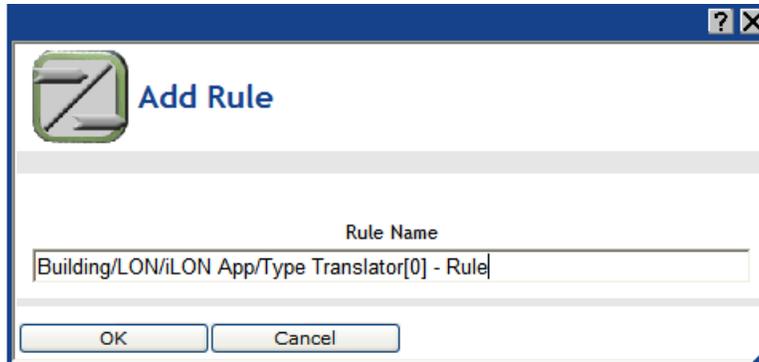
You can create a custom scalar-based translation with the Type Translator. This is useful if you need to perform some scaling on the value of the input point before it is translated to the output point. If you do not need to scale the input point, you can use the pre-defined **Copy Input DP to Output DP** translation.

To create a custom scalar-based translation, follow these steps:

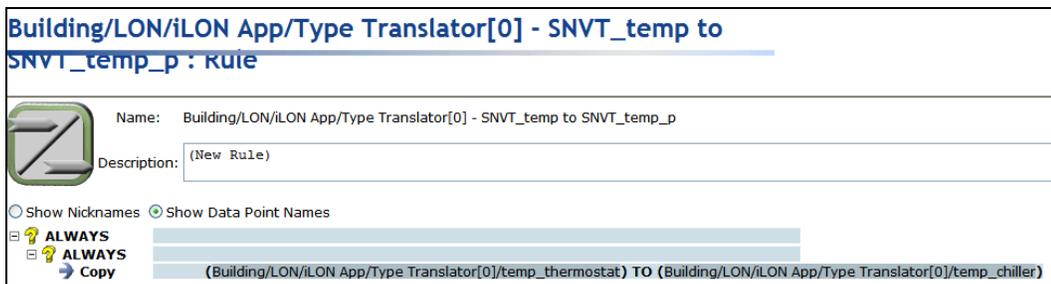
1. On the **Rule** box, click **Add Rule**.



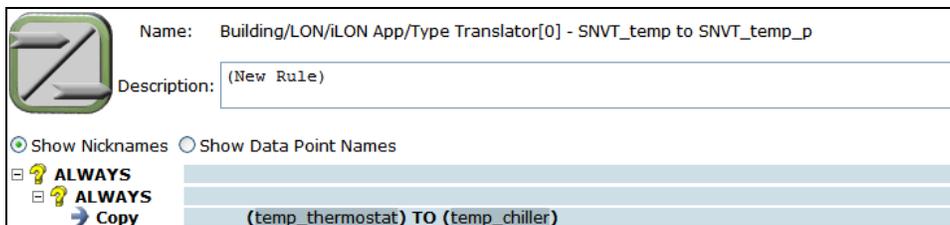
2. The **Add Rule** dialog opens.



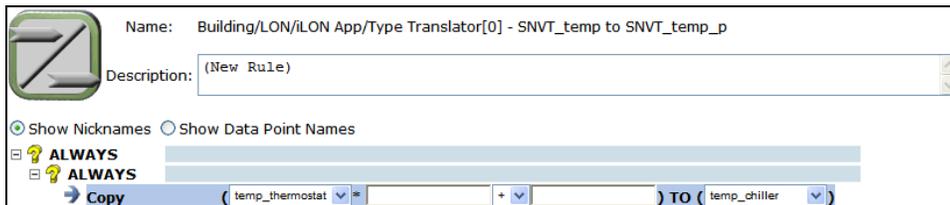
3. Enter a descriptive name for the new Type Translator rule, or accept the default rule name, which is *<functional block name> - Rule*, and then click **OK**.
4. The **Type Translator: Rule** Web page opens



5. Optionally, enter a description of the type translation.
6. By default, **Show Data Point Names** is selected, which means that the names of the selected data points are displayed by location in the following format: *network/channel/device/functional block/data point*. Click **Show Nicknames** to display the programmatic names of the selected data points, which are much shorter. For example, selecting **Show Nicknames** abbreviates a data point with the name *Net/LON/Lamp 1/Digital Ouput/DO_Digital_1* to just *DO_Digital_1*. The graphics in this section use the **Show Nicknames** option.



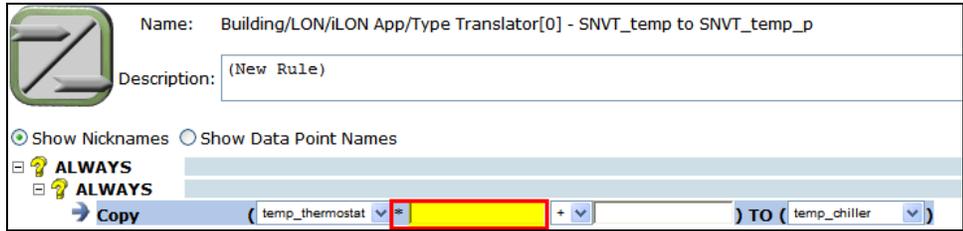
7. Click anywhere in the **COPY** rule to scale the input point and/or add an offset.



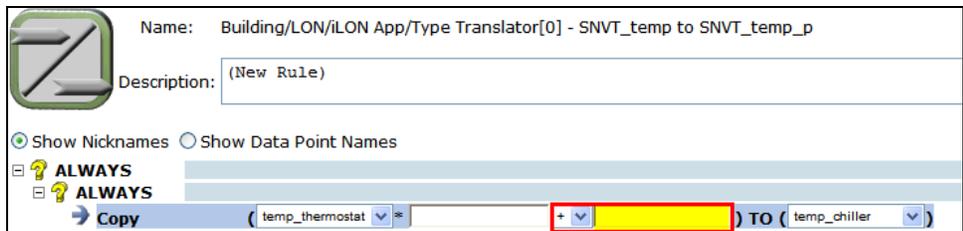
- a. If you added more than one input point, you can change the default input point by clicking it and then selecting an input point from the list.
- b. If the input point is a structured data point, a list box is added to the right of the input data point. Select whether to evaluate a field within the structure or the entire structure. By

default, the entire structure is evaluated. You can explicitly set the rule to evaluate the entire structure by selecting * from the list. This is required if you first select a field and then decide to evaluate the entire structure.

- c. To scale the value of the input point, enter a multiplier (a whole or decimal number) in the multiplier box. The default multiplier is 1. If you are copying an enumerated value to the output point, this box is unavailable.



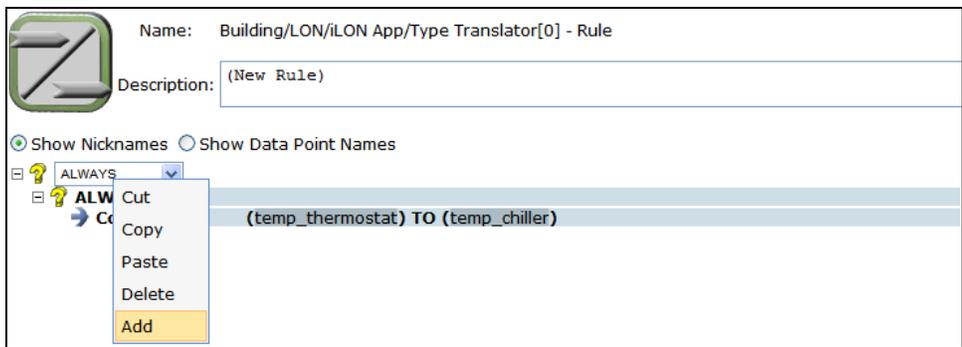
- d. To add or subtract an offset to the value of the input point, select the desired operator and then enter the value of the offset in the constant box. The default constant is 0. If you are copying to an enumerated output point, select the string value (for example, HVAC_HEAT) of an enumerated data point or field in this box. You cannot copy an index to an enumerated output point. If you are copying to an enumerated field within a structured data point, you must first select the enumerated field from the output point box (to the right of the TO operator) as described in step f.



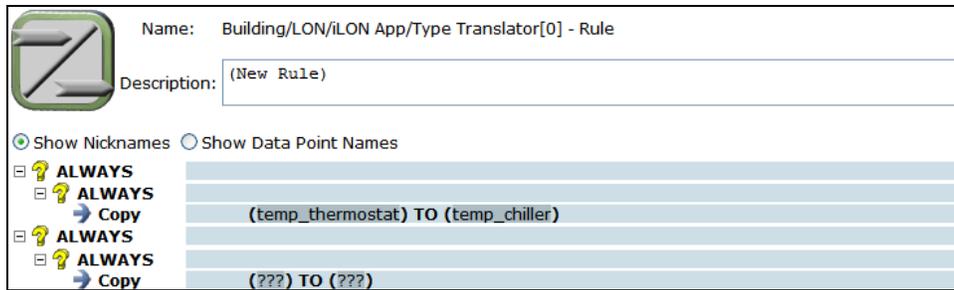
- e. If you added more than one output point, you can change the default output point by clicking it and then selecting an output point from the list.
- f. If the output point is a structured data point, a list box is added to the right of the output data point. Select whether to evaluate a field within the structure or the entire structure. By default, the entire structure is evaluated.

8. Click **Submit**.

- 9. To add another case to the type translation, right-click either of the **ALWAYS** cases or the **COPY** rule and then click **Add** on the shortcut menu.



10. A new case is added to the translation. Click **Submit**.



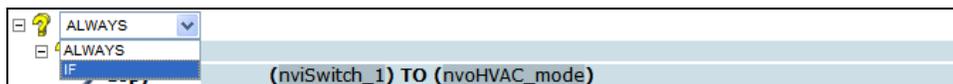
- Repeat steps 7–8 for each case to be created in the current type translation. Each case in the translation will be executed.

Creating a Custom Rule-Based Translation

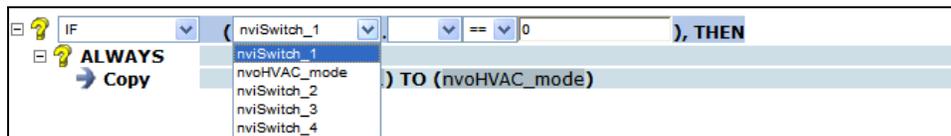
To create a custom rule-based translation, you define one or more cases and a rule for each case that executes when the case evaluates to TRUE. Each case is declared in an if-then statement or a nested if-then statement. The rule specifies the value to be copied to the output points.

To create a custom rule-based translation, follow these steps:

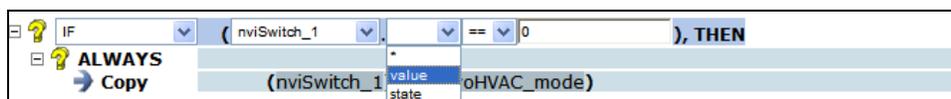
- Create a custom rule-based translation by adding a new translation or selecting a pre-defined translation and customizing it to fit your application.
 - To add a new translation, on the Rule box, click Add Rule.
 - To create a custom translation by editing a pre-defined one, select the pre-defined translation from the list below the Rule icon and then click Copy Rule. Alternatively, you can select a pre-defined translation, click the Rule icon, and then begin editing the rule. The dialog in which you create a new Type Translation appears. Proceed to step 2.
- Follow steps 2–6 in the previous section, *Creating a Custom Scalar-Based Translation*.
- Click the top-level **ALWAYS** case, select **IF** from the list, and then click **Submit**.



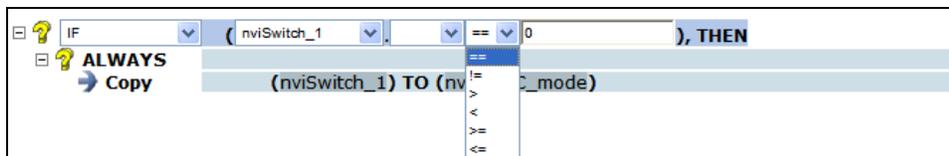
- The **IF-THEN** statement can then be edited.
 - If you added more than one input point, you can change the default input point by clicking it and then selecting an input point from the list.



- If the input point is a structured data point, you can select a field within the data point to be evaluated. By default, the entire structure is evaluated. You can explicitly set the rule to evaluate the entire structure by selecting * from the list. This is required if you first select a field and then decide to evaluate the entire structure.

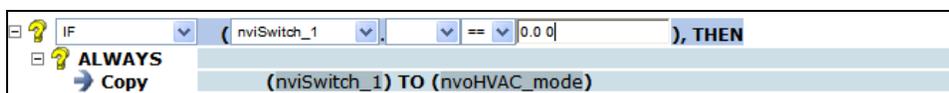


- Select one of the following comparison functions: equal to (default), not equal to, greater than, less than, greater than or equal to, or less than or equal to. If you are evaluating a structured data point as a whole, you can only select the equal (=) or not equal to (!=) comparison functions.

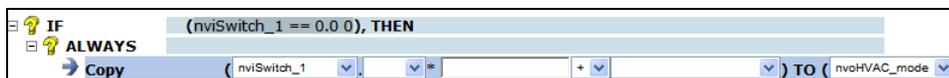


- d. Enter a comparison value. The default comparison value is 0. The comparison value can be one of the following:
- An integral or floating-point value if evaluating a scalar data point or a field within a structured data point that has a scalar type.
 - A space-separated structured value (for example, 100.0 1) if evaluating a structured data point as a whole.
 - An enumeration string (for example, HVAC_HEAT) if evaluating an enumerated data point or a field within a structured data point that has an enumerated type.

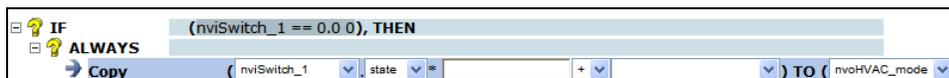
Note: You cannot use a preset as the comparison value.



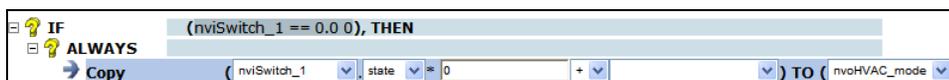
- e. To create another condition that must evaluate to TRUE for the case to be executed (create a nested IF-THEN statement), click the bottom level ALWAYS case and repeat steps 3–4. Otherwise, skip to step f.
- f. Expand the bottom-level ALWAYS or IF-THEN statement to show the CASE rule.
- g. Click **Submit**.
5. Click anywhere in the **COPY** rule to edit the rule.



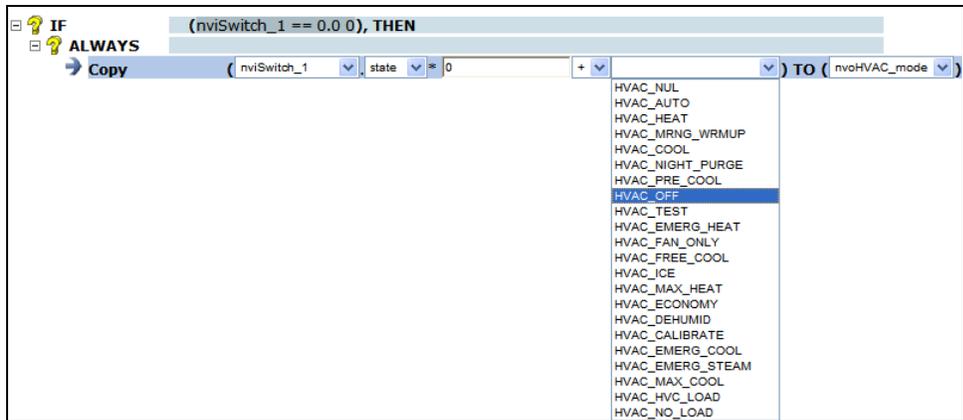
- a. Select an input point (to the left of the TO operator) from the list. If you created a nested IF-THEN statement (two IF statements), the input point in the **Copy** rule is the same input point you selected in the nested (second) IF statement, and it cannot be changed.
- b. If you selected a structured data point in the ALWAYS statement, select whether to copy a field or the entire structure to the output point. By default, the entire structure is selected.



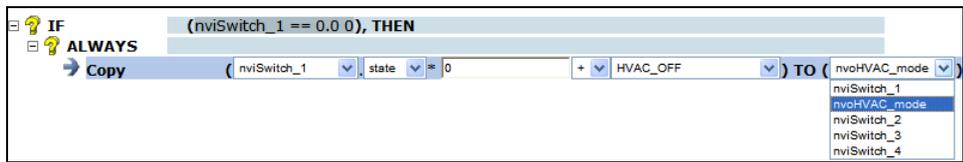
- c. Enter a multiplier (a whole or decimal number) in the multiplier box to scale the value of the input point. The default multiplier is 1. If you are copying an enumerated value to the output point, this box is unavailable.



- d. Add or subtract a constant to the value of the input point. To do this, select the desired operator and then enter the value of the constant in the constant box. The default constant is 1. If you are copying to an enumerated output point, select the string value (for example, HVAC_HEAT) of an enumerated data point or field in this box. You cannot copy an index to an enumerated output point. If you are copying to an enumerated field within a structured data point, you must first select the enumerated field from the output point box (to the right of the **TO** operator) as described in step f.



e. Select an output point (to the right of the **TO** operator) from the list.

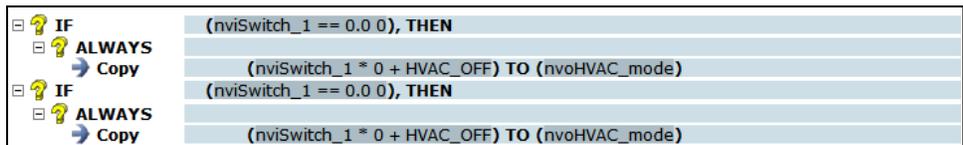
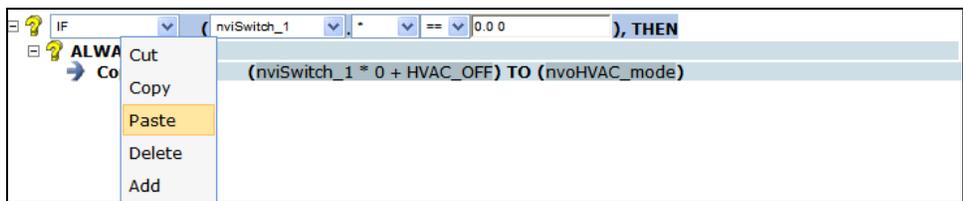
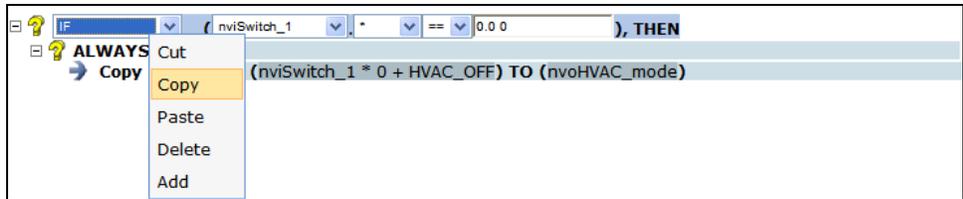


f. If the output point is a structured data point, select a field from the list to be written to by the input point.

g. Click **Submit**.

6. You can create a new case to the current translation or add another **IF-THEN** statement to the current case by adding a case or statement or copying an existing one. You can copy an existing method to create more complex rule-based translations. The method you choose depends on whether you want to re-use the previous case or **IF-THEN** statement.

- To create a new case in the current translation by re-using a previous case, right-click the top-level **IF-THEN** statement, click **Copy** on the shortcut menu, right-click the top-level **IF-THEN** statement again, and then click **Paste** on the shortcut menu. You can use this method to copy and re-use any case.



- To create a new case in the current translation without re-using a previous one, right-click the top-level **IF-THEN** statement and then click **Add** on the shortcut menu.

- To add a new **IF-THEN** statement to the current case by re-using a previous **IF-THEN** statement, right-click the bottom-level **IF-THEN** statement in the case, click **Copy** on the shortcut menu, right-click the **IF-THEN** statement again, and then click **Paste** on the shortcut menu. You can use this method to copy and re-use any **IF-THEN** statement.
 - To add a new **IF-THEN** statement to the current case without re-using a previous one, right-click the bottom-level **IF-THEN** statement and then click **Add** on the shortcut menu.
7. Repeat steps 3–6 to modify the cases and rules you add to the current translation. Each case in the translation will be evaluated even after a case evaluates to TRUE.

IF	(nviSwitch_1 == 0.0 0), THEN
ALWAYS	
Copy	(nviSwitch_1 * 0 + HVAC_OFF) TO (nvoHVAC_mode)
IF	(nviSwitch_1 == 100.0 1), THEN
ALWAYS	
Copy	(nviSwitch_1.state * 0 + HVAC_HEAT) TO (nvoHVAC_mode)

The following example demonstrates a custom rule-based translation that takes the data of a scene controller and turns on and illuminates or turns off a lamp, and completely opens a sunblind.

IF	(scene_controller.function == SC_RECALL), THEN
IF	(scene_controller.scene_number == 255), THEN
Copy	(scene_controller.scene_number * 0) TO (switch.state)
IF	(scene_controller.scene_number < 255), THEN
Copy	(scene_controller.scene_number * 0 + 1) TO (switch.state)
IF	(scene_controller.scene_number <= 4), THEN
Copy	(scene_controller.scene_number * 25) TO (switch.value)
IF	(scene_controller.scene_number <= 4), THEN
Copy	(scene_controller.scene_number * 0 + SET_UP) TO (sunblind.function)
IF	(scene_controller.scene_number <= 4), THEN
Copy	(scene_controller.scene_number * 25) TO (sunblind.setting)
IF	(scene_controller.scene_number <= 4), THEN
Copy	(scene_controller.scene_number * 0) TO (sunblind.rotation)
IF	(scene_controller.scene_number >= 5), THEN
Copy	(scene_controller.scene_number * 0 + SET_NULL) TO (sunblind.function)
IF	(scene_controller.scene_number >= 5), THEN
Copy	(scene_controller.scene_number * 0 + 100) TO (sunblind.setting)
IF	(scene_controller.scene_number >= 5), THEN
Copy	(scene_controller.scene_number * 0) TO (sunblind.rotation)
IF	(scene_controller.function == SC_NULL), THEN
IF	(scene_controller.scene_number > 0), THEN
Copy	(scene_controller.scene_number * 0) TO (switch.state)
IF	(scene_controller.scene_number > 0), THEN
Copy	(scene_controller.scene_number * 0) TO (switch.value)
ALWAYS	
Copy	(scene_controller.scene_number * 0 + SET_NULL) TO (sunblind.function)

Notes:

- You can delete or more cases or statements from a translation. To delete one case or statement, right-click the case or statement, click **Delete** on the shortcut menu, and then click **Submit**. To remove multiple cases or statements, click one case or statement and then either hold down CTRL and click all other cases or statements to be deleted or hold down SHIFT and select another case or statement to delete the entire range of cases or statements, right-click one case or statement, click **Delete** on the shortcut menu, and then click **Submit**.

Integrating M-Bus Devices With a Type Translator

You can use a type translation to integrate the data generated by an M-Bus device into a LONWORKS network. This entails doing the following:

1. Installing an M-Bus device and adding it to the SmartServer network **Net** tree.
2. Viewing the M-Bus data point properties.
3. Evaluating the M-Bus device specifications.
4. Selecting or creating an M-Bus type translation.

Tip: If you would like more information about the specific device used in this tutorial, you can download the data sheet of the Scampy water meter from the Hydrometer GmbH web site at www.hydrometer.de.

Installing an M-Bus Device

You can install an M-Bus device on the SmartServer and add it to the SmartServer network **Net** tree. To do this, you do the following:

1. Connect the M-Bus device to the RS-232 or RS-485 ports on the SmartServer following the steps described in the SmartServer *Hardware Guide*.
2. Add a new M-Bus channel to the SmartServer network **Net** icon, as described in Chapter 5, *Using the SmartServer as a Network Management Tool*.
3. Add a new M-Bus device to the M-Bus channel you created in step 2, as described in Chapter 5, *Using the SmartServer as a Network Management Tool*.

Viewing M-Bus Data Point Properties

After you have installed an M-Bus device and added it to the SmartServer, you can examine the properties of the data points of the M-Bus device. To do this, you do the following:

1. Expand the M-Bus device created in the previous section, *Installing an M-Bus Device*.
2. Expand the Virtual Functional Block **VirtFB** icon under the M-Bus device to show all the data points of the M-Bus device.
3. Click **General**.
4. Click an M-Bus data point. The **Configure - Data Point** Web page for the M-Bus data point opens.
5. View the **Format Description** and **Unit String** properties to ascertain the type of data to be translated. For example, consider an M-Bus data point that has the following **Format Description: UCPT_MBS8**. This means that this data point is an array with 8 elements. The **Unit String** property provides the type of data stored in each element of the array. For example, the first element of this data point is a measurement of volume in **m³** format, the second element is a time stamp, and so on.

The formats used for the M-Bus data point are described in the M-BUS_Integrator resource file set which is installed with the SmartServer software. These files may be viewed with the LonMark Resource Editor, which is also included with the SmartServer software

Note: The format description and unit string will not be set if the SmartServer cannot communicate with the M-Bus device.

Evaluating Device Specification

Although the format description and unit string can be easily read from the device, many M-Bus devices have complex data structures. As a result, you may need to read the device specification to determine how each piece of data should be interpreted. To do this, follow these steps:

1. In the section of the specification describing the M-Bus protocol (such a section is typically included in the specification for an M-Bus device), locate the description of the data being returned by the device on the REQ_UD2 M-BUS command. This command could also be called the *standard telegram* or the *response RSP_UP*.
2. Map the entries in the **Unit String** property one by one to the values in the vendor specification.

Using the **UCPT_MBS8** data point described in the previous section, for example, the device specification shows a structure with the following elements:

- **value[0] m³**: This value reflects the current meter reading (total amount of water).

- **value[1] Datetime:** The current date and time stored in the M-Bus device.
- **value[2] m³:** The meter reading at the last reference day. *Reference days* are configured by the installation tool for the device and define a fixed date or recurring pattern when data will be recorded.
- **value[3] Date:** The last reference day.
- **value[4] Date:** The next reference day.
- **value[5] l/h:** The current flow of water.
- **value[6] m³:** The meter reading at the end of the month.
- **value[7] Date:** The date of last months reading.

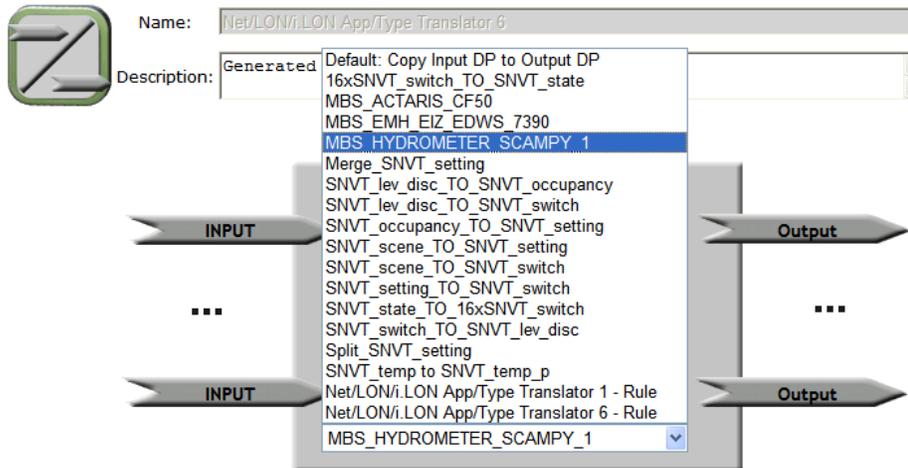
Creating an M-Bus Type Translation

After you have read the data specification for the M-Bus device and determined how to interpret the various elements in the M-Bus data point, you can use a type translation to extract each element and convert it to a LONWORKS data point.

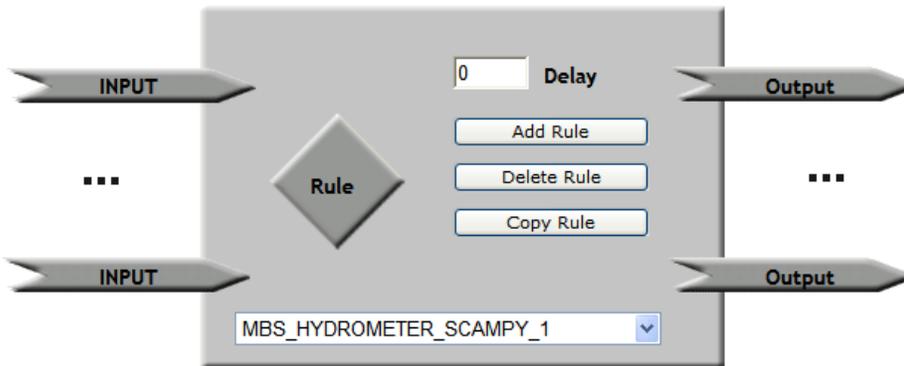
The Type Translator includes three pre-defined rule-based type translations for converting water, power, and thermal measurements generated by M-Bus devices. The names of these translations consist of the manufacturer and model number of actual devices for which they were designed.

- **MBS_HYDROMETER_SCAMPY_1.** Converts the current meter reading (the [0] element) and the current water flow (the [5] element) of the UCPT_MBS8 input data point of an M-Bus water meter to **SNVT_vol_f** and **SNVT_flow_f** output data points.
- **MBS_EMH_EIZ_EDWS_7390.** Converts the total watts per hour (the [2] element) and total watts (the [3] element) of an UCPT_MBS7 input data point of an M-Bus power meter to **SNVT_elec_kwh_1** and **SNVT_power_f** output data points.
- **MBS_ACTARIS_CF50.** Converts the total energy (the [0] element), current energy (the [2] element), flow temperature (the [4] element), return temperature (the [5] element), and temperature differential (the [6] element) of an UCPT_MBS9 input data point of an M-Bus thermal meter to **SNVT_elec_kwh_1**, **SNVT_power_f**, **SNVT_temp_f**, **SNVT_temp_f**, and **SNVT_temp_diff_p** output data points.

You can either use one of these pre-defined M-Bus type translations or create your own custom M-Bus type translation using one of these as a starting point. To use one of these three pre-defined rules, select one from the list below the **Rule** icon.



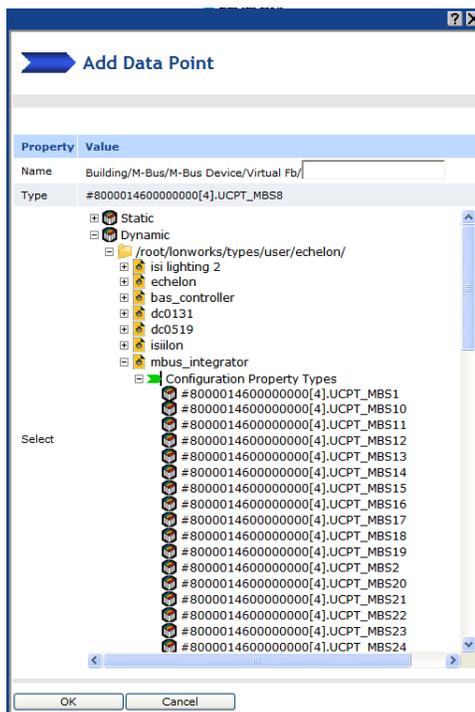
To create a custom M-Bus type translation based on one of the pre-defined translations, select the source translation from the list, click **Copy Rule**, enter a name for the custom M-Bus type translation, and then modify the M-Bus type translation to fit your application.



In this example, the **MBS_HYDROMETER_SCAMPY_1** is used. This translation converts an M-Bus **UCPT_MBS8** input data point to **SNVT_vol_f** and **SNVT_flow_f** output data points. You add an M-Bus **UCPT_MBS8** data point to the list of input points and **SNVT_vol_f** and **SNVT_flow_f** data points to the list of output points.

If the input data point for the M-Bus device does not use the **UCPT_MBUS8** format, you can dynamically add a data point with the correct type to match your device. To do this, follow these steps:

1. Right click the **VirtFB** functional block icon and click **Add Data Point** on the shortcut menu. The **Add Data Point** dialog opens.
2. Expand the **Dynamic** folder, expand the **/lonworks/types/user/echelon** folder, expand the **mbus_integrator** folder, expand the **Configuration Property Types** folder, select the **UCPT_MBUS8** data point, and then click **OK**.



3. Click **Submit**.

You can add more input and output points to the translation in order to convert other data elements in the M-Bus device to LONWORKS data points. Add the M-Bus and LONWORKS data point to their respective input and output lists, add an **ALWAYS** case that maps a data field from the M-Bus device to the appropriate LONWORKS data type. For example, you can convert the last month value property (the [6] element) of the MBS_HYDROMETER_SCAMPY_1 device to a **SNVT_vol_f** data point.

Note: The M-Bus driver represents all scalar values as double precision floating-point numbers (8 bytes). The use of 4 byte floating-point types such as **SNVT_vol_f** may exhibit a loss of precision when values become very large. You can use the **Pulse Counter** output data point **nvoPcValue**, which is 8 bytes, as a template to create output data points with double precision floating point types. The **bas_controller** resource file set on the SmartServer includes double precision floating point types that you can use such as **UNVT_double_float**, **UNVT_elec_kwh_lf**, and **UNVT_power_lf**.

Deleting a Type Translation

You can delete a pre-defined or custom type translation from a Type Translator. Deleting a type translation not only removes it from the current Type Translator application, but it removes it from all other existing Type Translators on your SmartServer and any new Type Translators that you may create.

To delete a type translation, select the type translation to be deleted from the list below the **Rule** icon, click **Delete Rule**, click **OK** to confirm the deletion of the selected type translation, and then click **Submit**.

Specifying a Delay

You can specify the period of time that the Type Translator waits after an input data point has been updated before performing a translation. This is useful if the translation has multiple inputs. Setting a delay in this case ensures that translations occur only after most or all of the input points have been updated. To specify a delay, enter the period of time (in seconds) in the **Delay** box for the type translator to wait after input point updates.

The type translations will reflect any additional data point updates that occur during the delay interval. This means that if an input data point is updated a second time before the delay interval expires, the delay will not be reset, and the second update will be the one translated.

Using the SmartServer with OpenLNS CT

This chapter describes how to install the SmartServer with OpenLNS CT, maintain synchronization between the SmartServer and a OpenLNS CT drawing, and launch the SmartServer's built-in applications from a OpenLNS CT drawing. It describes how to link the network variables of external devices in a OpenLNS CT drawing (formerly referred to as "NVEs") to the SmartServer's built-in applications and custom SmartServer Web pages after synchronizing the SmartServer to an OpenLNS network database.

Introduction

You can install the SmartServer using OpenLNS CT and then synchronize the SmartServer to an OpenLNS network database. You can then maintain synchronization between the SmartServer and a OpenLNS CT drawing. You can also launch the SmartServer's built-in applications from a OpenLNS CT drawing using the SmartServer Configuration Utility.

After you synchronize the SmartServer to an OpenLNS network database, you can link the network variables of external devices in a OpenLNS CT drawing (formerly referred to as "NVEs") to the SmartServer's built-in applications and your custom SmartServer Web pages. You can do this in two ways: (1) use OpenLNS CT to bind the network variables on the external devices to the network variables on the SmartServer App device's functional blocks, or (2) use the SmartServer Web interface to directly add the network variables of the external devices in the OpenLNS CT drawing to the SmartServer's internal database, and then poll the external data points.

Note that you do not use the SmartServer Configuration Utility to create data points of external devices on the SmartServer, or to configure the SmartServer's built-in applications as you did with the i.LON 100 e3 Server. You can directly use the SmartServer Web interface to accomplish these tasks.

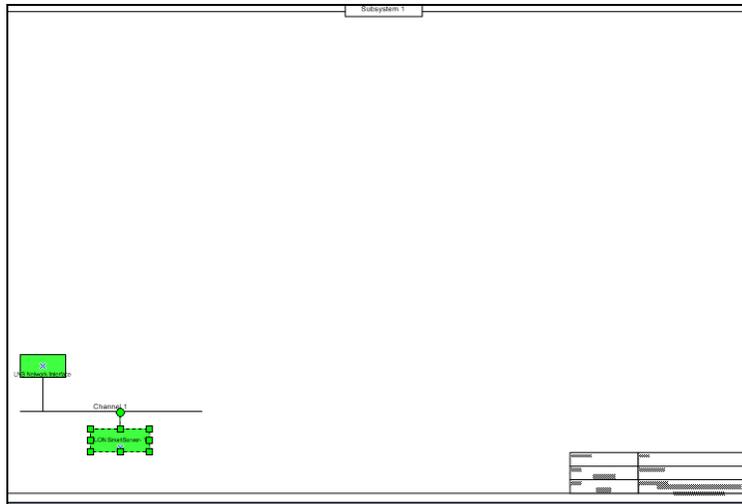
Installing the SmartServer with OpenLNS CT

You can install the SmartServer with OpenLNS CT, synchronize the SmartServer to an OpenLNS network database, and then update your OpenLNS CT drawing. To do this, follow these steps:

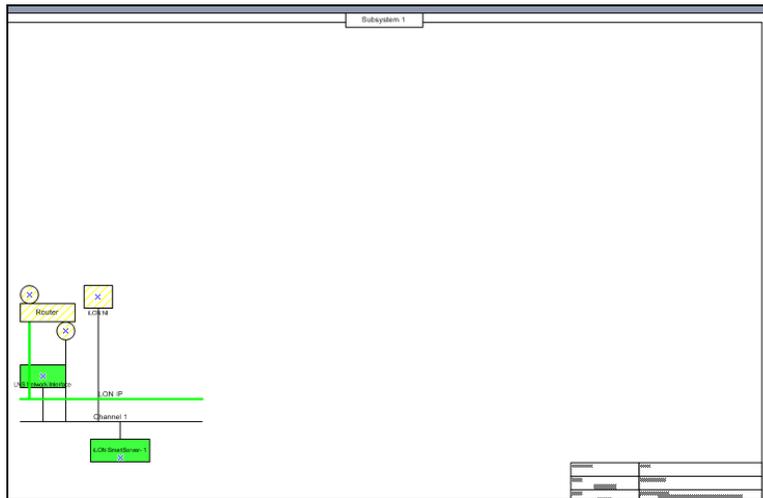
1. Create a new OpenLNS CT network design or open an existing design as described in the in the *OpenLNS Commissioning Tool User's Guide*.
2. Drag an i.LON device shape corresponding to your hardware model (FT [free topology twisted-pair] or PL [power line]) from the **SmartServer Static Shapes** stencil to the OpenLNS CT drawing.

Note: The SmartServer Shapes stencil is installed with the SmartServer software. It contains OpenLNS CT shapes for the SmartServer device and functional blocks. If the SmartServer Shapes stencil does not appear in the Shapes window, you can open it following these steps.

- a. Open the **File** menu, point to **Shapes**, and then click **Open Stencil**. The **Open Stencil** dialog opens.
 - b. Browse to the LonWorks\LonMaker\Visio folder on your computer.
 - c. Select the **iLON100.vss** stencil.
3. The New Device Wizard opens, unless you enabled automatic channel selection and dropped a custom device master shape near a channel shape.
 4. Define and commission the device as described in the *OpenLNS Commissioning Tool User's Guide*.



5. Synchronize the SmartServer to an OpenLNS network database following the steps described in *Automatically Synchronizing the SmartServer to an OpenLNS network database* in Chapter 5.
6. Open your OpenLNS CT drawing. If IP-852 routing is licensed and activated on your SmartServer, a router shape representing the SmartServer's IP-852 router and the LON IP channel to which it is connected has been added to your drawing. In addition, an iLON NI device shape representing the SmartServer's local network interface that is used to poll the data points of external devices and test and wink the devices has been added to the channel to which the SmartServer is attached.



Note: If you did not commission the SmartServer with OpenLNS CT before synchronizing the SmartServer to the OpenLNS network database, your OpenLNS CT drawing will have two uncommissioned SmartServer device shapes: iLON App on a **LON** channel that cannot communicate with the OpenLNS network interface, and iLON SmartServer- 1 on a different channel. In this case, use OpenLNS CT to move any functional block shapes on the iLON SmartServer-1 device shape to the iLON App device shape; delete the iLON SmartServer-1 device shape; move the iLON App, IP-852 router, and iLON NI shapes to a channel that can communicate with OpenLNS network interface; commission the iLON App, IP-852 router, and iLON NI device shapes; and then delete the **LON** channel.

7. If IP-852 routing is licensed and activated on your SmartServer, you can commission the SmartServer's IP-852 router. To do this, right-click the router shape, click **Commission** in the shortcut menu, and step through the New Router Wizard (the router shape already includes the

router's Neuron IDs so you don't have to press the SmartServer's service pin to commission the router).

You can move the router and LON IP channel shapes to simplify your drawing, or you can delete these shapes (doing so hides the corresponding objects in the SmartServer tree).

8. Commission the i.LON NI device. To do this, right-click the **i.LON NI** device shape, click **Commission** in the shortcut menu, and then click **Finish** in the Commission Device Wizard. The **i.LON NI** device shape represents the SmartServer's local network interface that is used to poll the data points of external devices, and test and wink the devices.

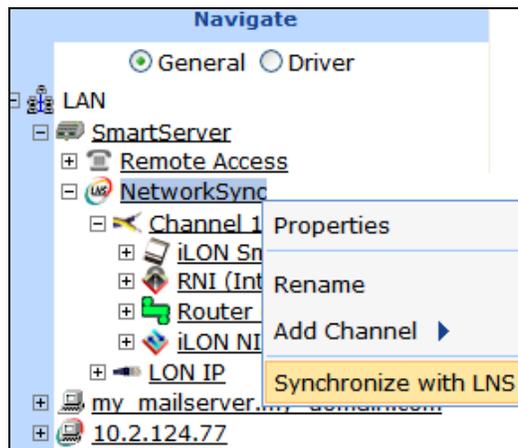
Note: Do not delete the i.LON NI device shape. If you delete the i.LON NI device shape, it is deleted from the OpenLNS network database and it cannot be re-added to the OpenLNS CT drawing.

Synchronizing the SmartServer with a OpenLNS CT drawing

After synchronizing the SmartServer with an OpenLNS network database, you still periodically need to manually synchronize the SmartServer and the OpenLNS CT drawing to the OpenLNS network database—this is even true if you are running the SmartServer in **LNS Auto** mode. This ensures that your OpenLNS CT drawing and the SmartServer tree are consistent. For more information on changes to a OpenLNS CT drawing requiring you to manually synchronize the SmartServer to an OpenLNS network database, see *Changes Requiring Manual SmartServer Synchronization*.

To manually synchronize the SmartServer and a OpenLNS CT drawing to the OpenLNS network database, follow these steps:

1. Right-click the network icon in the target SmartServer tree, and then click **Synchronize with LNS** in the shortcut menu.



Alternatively, you can click **Driver**, click the network icon in the SmartServer tree to open the **Setup – LON Network Driver** Web page, and then click the **Synchronize** button in the **OpenLNS Network** property.

2. The **SmartServer Resync** dialog opens.



3. Set the following synchronization options:

Synchronize All Internal SmartServer Items

Synchronizes all internal items in the SmartServer's internal database, including hidden items, with the OpenLNS network database.

Internal items include the following:

- LONWORKS channels.
- The SmartServer's internal App device and its child functional blocks and data points.
- The SmartServer's internal IP-852 router.
- Custom app devices and their child functional blocks and data points.

Selecting this option also transmits changes made to the LON driver properties of the internal items in the SmartServer tree to the OpenLNS network database, and it updates the SmartServer's internal database with changes made to the LON driver properties of the internal items with OpenLNS CT, OpenLNS tree, or other OpenLNS application.

This option is cleared by default, which means that the SmartServer sends only changes made to the internal items in the SmartServer tree to the OpenLNS network database. In addition, the SmartServer's internal database is updated only with the following changes made to internal items with OpenLNS CT:

- Renaming of devices or functional blocks.
- Addition of functional blocks to the SmartServer's internal App device that have stencils with no dynamic network variables on them.
- Deletion of the SmartServer App device's functional blocks.
- Addition or deletion of dynamic network variables

on the SmartServer's internal App device while it is uncommissioned.

Note: Selecting this option may significantly increase the time required for the manual synchronization as all hidden internal items are synced.

Synchronize All External Items

Synchronizes all external items in the SmartServer's internal database with the OpenLNS network database.

External items include the following:

- LONWORKS channels.
- External devices and their child functional blocks and data points.
- Routers.

Selecting this option also transmits any changes made to the LON driver properties of the external items in the SmartServer tree to the OpenLNS network database, and it updates the SmartServer's internal database with any changes made to the LON driver properties of the external items with OpenLNS CT, OpenLNS tree, or other OpenLNS application.

This option is cleared by default, which means that the SmartServer sends only changes made to the external items in the SmartServer tree to the OpenLNS network database. In addition, the SmartServer's internal database is updated only with any changes made to the names of external devices or functional blocks with OpenLNS CT.

4. Click **Start**.
5. The **Items to be Synced** property lists the number of objects in the SmartServer tree to be updated. This number counts down as the synchronization operation progresses. When the synchronization operation has been completed, this number is 0, and you can then click **Close** to close the dialog. During the synchronization, this dialog displays any errors that occur.

You can shrink and move the **SmartServer Resync** dialog so that you can continue to use the SmartServer Web interface during the synchronization. You can cancel the synchronization operation anytime by clicking **Close** and the clicking **Yes** in the confirmation dialog.

Note: You can view a log of the current synchronization in the SmartServer's console application. To view the sync log, enter the `trace 2` command. For more information on the SmartServer console application, see Appendix B, *Using the SmartServer Console Application*.

6. When the synchronization operation on the SmartServer has been completed, you can synchronize your OpenLNS CT drawing to the OpenLNS network database as described in the *OpenLNS Commissioning Tool User's Guide*. This updates your OpenLNS CT drawing with changes made to the OpenLNS network database by the SmartServer.

Changes Requiring Manual SmartServer Synchronization

You need to regularly synchronize the SmartServer to the OpenLNS network database to account for changes made by OpenLNS CT that are not propagated automatically over the LonTalk channel. These changes include the following:

- Modifying the LON driver properties of objects such as description, timing parameters of channels, commission status and application status of external devices, and format descriptions of

external data points. To update the SmartServer's internal database with changes made to objects' LON driver properties, you must select the appropriate **Synchronize All** check box in the **SmartServer Resync** dialog. See the previous section, *Synchronizing the SmartServer with a OpenLNS CT drawing*, for more information on these options.

- Renaming devices or functional blocks. If you re-name a network variable with OpenLNS CT, the change is automatically propagated to the SmartServer.
- Adding functional blocks that have stencils with no dynamic network variables on them. This includes the following functional blocks on the SmartServer's internal App device:
 - Calendar
 - Data Logger
 - Digital Input
 - Digital Output
 - Node Object
 - Scheduler
 - Type translator
 - Web Server

Note: You can add these functional blocks to the SmartServer tree by opening their corresponding Web pages with the SmartServer Configuration Utility in OpenLNS CT (see Using OpenLNS CT to Open SmartServer Applications for more information), or by adding dynamic network variables to them.

This means that the addition of the SmartServer's Alarm Generator, Alarm Notifier, Analog Functional Block, and Real-Time Clock functional blocks with OpenLNS CT is automatically propagated to the SmartServer (the stencils for these functional blocks have red network variables that signify the NVs as dynamic).

For example, you can add one of these functional blocks to your OpenLNS CT drawing and it will appear in the SmartServer tree after the functional block has been instantiated (this takes approximately 15 seconds after you add the functional block shape to your OpenLNS CT drawing). The functional block initially will be highlighted yellow in the SmartServer tree, indicating that it is not synced with the OpenLNS network database. If the SmartServer is operating in **LNS Auto** mode, the functional block will automatically be synchronized after approximately 20 seconds and it will no longer be highlighted yellow in the SmartServer tree.

- Deleting the SmartServer App device's functional blocks in the OpenLNS CT drawing. Deleting a functional block on the SmartServer's App device hides the corresponding functional block in the SmartServer tree after synchronization. A hidden SmartServer App device functional block will still run its application.

You can use the SmartServer tree to delete a SmartServer App device functional block and permanently remove its XML configuration from the SmartServer's internal database. To do this, right-click the functional block in the SmartServer tree, click **Delete** on the shortcut menu, and then click **Submit**.

- Adding or deleting dynamic network variables in the OpenLNS CT drawing while the SmartServer's internal App device is uncommissioned. The addition or deletion of dynamic network variables is propagated once the device is commissioned.

This also means that the addition or deletion of dynamic network variables to a functional block on the SmartServer's internal App device with OpenLNS CT is automatically propagated to the SmartServer (provided that the SmartServer's App device has been commissioned).

If a dynamic network variable is added to one of the functional blocks that have no dynamic network variables on them with OpenLNS CT, the functional block and its dynamic data point will appear in the SmartServer tree. For example, you can add a Data Logger functional block to your OpenLNS CT drawing. This does not cause any change to the SmartServer tree because the Data Logger functional block does not have any dynamic network variables on it. But if you add a

dynamic network variable to the Data Logger functional block, the Data Logger and the dynamic data point will be added to the SmartServer tree.

Changes Requiring OpenLNS CT Synchronization

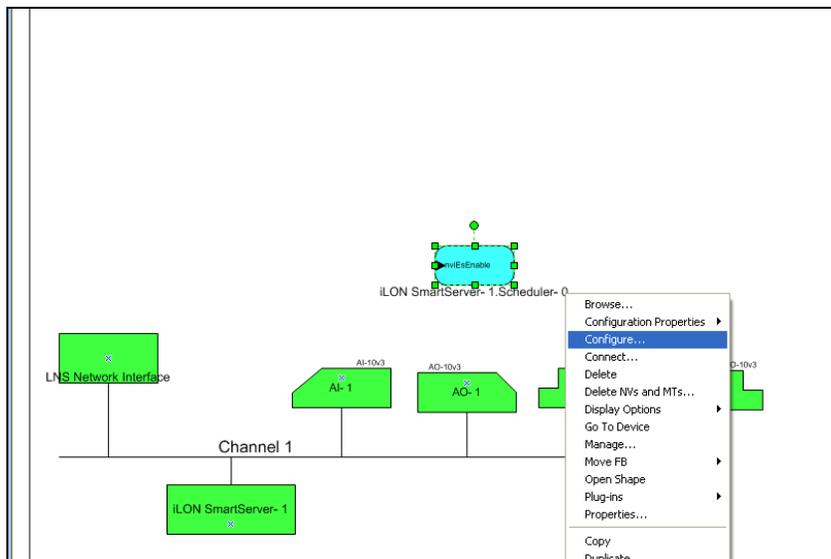
You can synchronize OpenLNS CT to the OpenLNS network database to update it with all network configuration changes made in the SmartServer tree. You may need to periodically synchronize OpenLNS CT to the OpenLNS network database because changes made in the SmartServer tree are not propagated automatically to OpenLNS CT.

Opening SmartServer Applications with OpenLNS CT

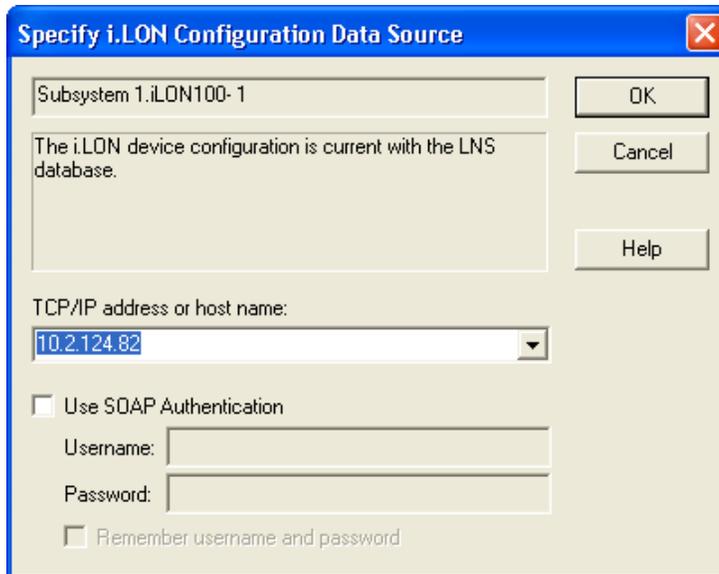
You can create an instance of a SmartServer application's functional block and open the application using the SmartServer Configuration Utility in OpenLNS CT. Using this method to open a SmartServer application is comparable to launching a Web plug-in. You right-click the functional block shape in the OpenLNS CT drawing representing the SmartServer application to be configured, and then click **Configure** on the shortcut menu. You cannot use OpenLNS CT to open a SmartServer application when the network is being managed with the SmartServer running in Standalone mode.

To create an instance of an application's functional block and launch the Web plug-in using OpenLNS CT, follow these steps:

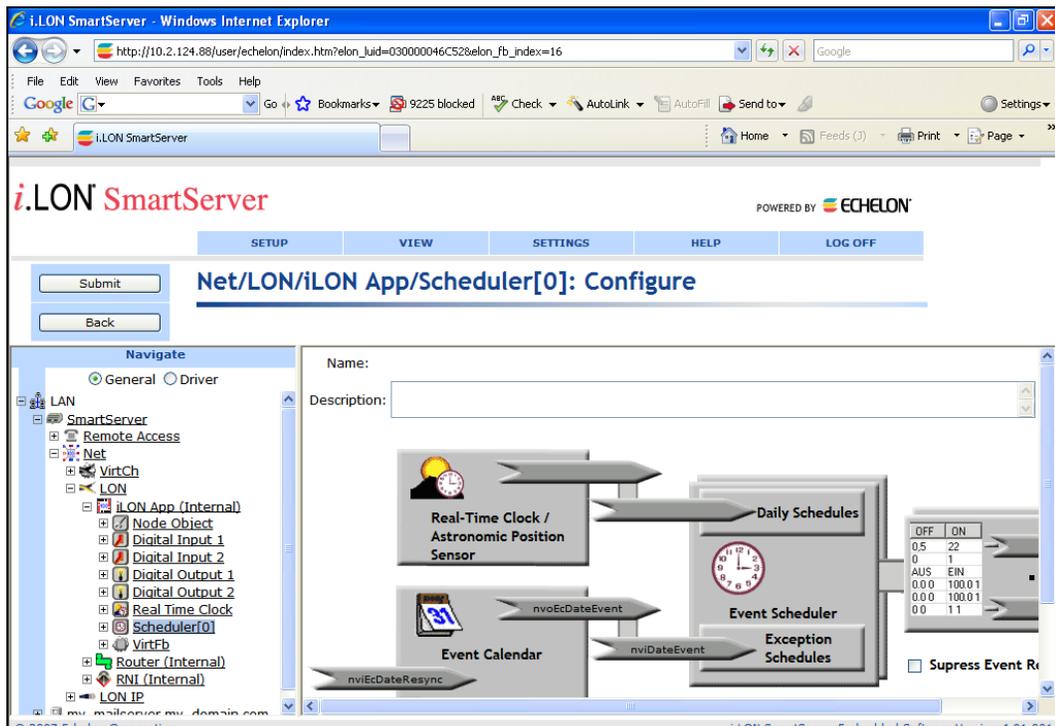
1. Verify that the SmartServer is operating in LNS mode (**LNS Auto** or **LNS Manual**). To do this, click **Driver** at the top of the navigation pane on the left side of the SmartServer Web interface, click the network in the SmartServer tree to open the **Setup – LON Network Driver** Web page, and check that **Network Management Service** property is set to **LNS Auto** or **LNS Manual**.
2. Drag the functional block shape representing the SmartServer application to be configured from the **SmartServer Static Shapes** stencil to the OpenLNS CT drawing.
3. Right-click the functional block shape representing the SmartServer application, and then click **Configure** on the shortcut menu.



4. The **Specify iLON Configuration Data Source** dialog opens.



5. Enter the IP address or hostname of the SmartServer in the **TCP/IP Address or host name** box. If you have configured the SmartServer to use a port other than 80, you must specify the port with the IP address. For example, to specify port 8080 if your SmartServer has an IP address of 172.25.130.18, you would enter 172.25.130.18:8080.
6. Select **Use SOAP Authentication** and enter the **Username** and **Password** for your SmartServer to enable authentication for SOAP messages sent to and from your SmartServer. The **Username** and **Password** both default to *ilon*.
7. Click **OK**. The SmartServer Web interface opens in a new browser, a functional block icon representing the application is added to the SmartServer's App device in the navigation pane, and the selected SmartServer application opens in the application frame to the right. The same browser will be used each time you open a SmartServer application using OpenLNS CT.



8. Click **Submit** when you have finished configuring the SmartServer application.

Connecting the SmartServer to External Devices

You can use the SmartServer's built-in applications and your custom Web pages to monitor and control the external devices on a LONWORKS network. External devices are physical application devices that are connected to the SmartServer. External devices are either stored in an OpenLNS database and managed with OpenLNS CT or other OpenLNS application with the SmartServer running in LNS mode (**LNS Auto** or **LNS Manual**), or they are stored exclusively on the internal database of the SmartServer (the XML files in the **/config/network** folder on the SmartServer flash disk) and managed with the SmartServer operating in **Standalone** mode.

For a SmartServer application or a custom Web page to monitor and control an external device, you must provide it a data point representing data produced or consumed by the external device. If you are using OpenLNS CT with the SmartServer, you can provide two types of data points:

- Data points on the SmartServer's internal automated systems device (i.LON App, iLON SmartServer- 1, or other user-defined name) that are bound with LONWORKS connections to network variables on the external devices.

In this case, you use OpenLNS CT to bind the network variables on the external devices to dynamic network variables on the SmartServer's functional blocks. This creates an event-driven update connection between the external device and the SmartServer. You then use the SmartServer Web interface to add the dynamic network variables on the SmartServer functional blocks to their respective applications (configuration Web pages).

This method enables you to maintain a OpenLNS CT drawing that provides a graphical representation of your network's data flow. It is ideal for small networks in which you only need to create a minimum number of LONWORKS connections. For larger networks, you can save time by copying the network variables on the external devices to the SmartServer and polling them.

- A data point that is a copy of the network variable on the external device that is polled by the SmartServer's internal data server.

In this case, you can use SmartServer Web interface to copy the network variables of the external devices from OpenLNS to the SmartServer's internal database. You then add the copied data points to the desired SmartServer applications or to your custom Web pages.

This method does not provide a graphical representation of your network's data flow, but it allows you to use a single tool to add the network variables to the SmartServer's application quickly. Because this method involves the SmartServer periodically polling the network variables of the external devices, it is also useful for monitoring network variable values that change rapidly. However, frequent polling of network variables values that change rarely may generate unnecessary network traffic and impact network performance. set appropriate poll rates for the network variables.

The following sections describe how to add data points to the SmartServer's applications and your custom Web pages using bound monitoring and polling.

Binding External Network Variables

You can use LONWORKS connections in OpenLNS CT to bind the network variables on external devices to dynamic network variables on the SmartServer's internal automated systems device.

If you are connecting a SmartServer functional block that only has static network variables in its stencil (the Data Logger, Scheduler, Type Translator, Virtual Functional Block, and Web Server functional blocks), add a dynamic network variable to the functional block that has the same SNVT or UNVT as the network variable on the external device.

If you are connecting a SmartServer functional block that includes dynamic network variables in its stencil (the Alarm Generator, Alarm Notifier, Analog Functional Block, and Real-Time Clock

functional blocks), verify that the dynamic network variables in the functional block have the same SNVTs or UNVTs as the network variables on the external device. If the SNVTs or UNVTs are different, change them so they are compatible.

The following sections describe how to connect network variables in the SmartServer's functional blocks to network variables on external devices:

- The first section describes how to connect SmartServer functional blocks that only have static network variables in their stencils. It demonstrates how to do this using the SmartServer's Scheduler and Data Logger functional blocks.
- The second section describes how to connect SmartServer functional blocks that have dynamic network variables in their stencils. It demonstrates how to do this using the SmartServer's Alarm Generator and Alarm Notifier functional blocks.

Binding SmartServer FBs (with only Static NVs in Stencils)

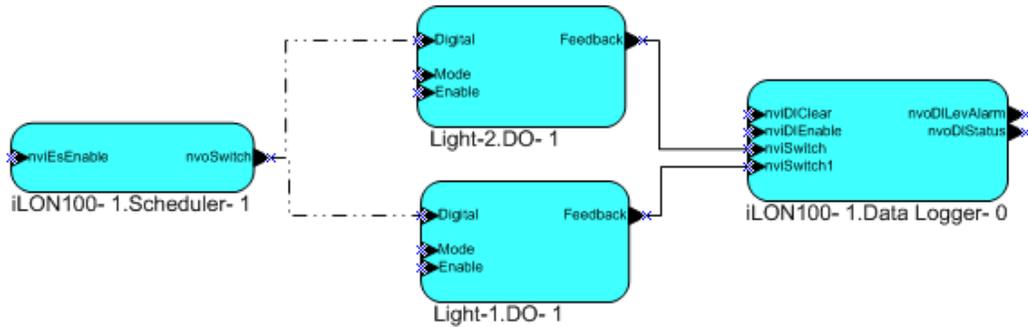
You can use OpenLNS CT to connect the network variables of external devices to the following SmartServer functional blocks that only have static network variables in their stencils: the Data Logger, Scheduler, Type Translator, Virtual Functional Block, and Web Server functional blocks.

To do this, add dynamic network variables to a SmartServer functional block that has the same SNVT or UNVT as the source or target network variable on the external device. Then create a LONWORKS connection between the dynamic network variables on the SmartServer functional block to the source or target network variables on the external device. Finally, add the dynamic network variables as input points in the functional blocks' corresponding configuration Web pages in the SmartServer Web interface.

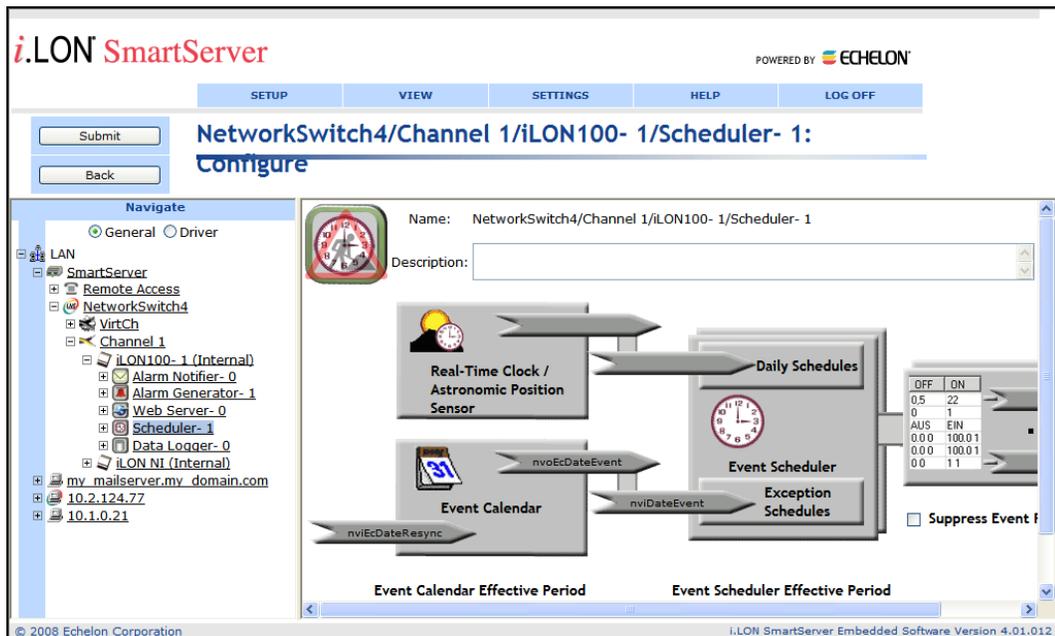
Consider a scenario in which you want to connect a SmartServer Scheduler, a lighting system, and a SmartServer Data Logger so that the lights are turned on and off at a given time and the state and lux of the lights are logged.

To create the solution for this scenario, you could follow these steps:

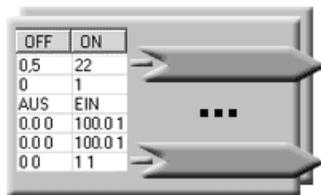
1. In OpenLNS CT, drag the functional blocks for the external devices to the OpenLNS CT drawing, and drag the SmartServer's Scheduler and Data Logger functional blocks from the **SmartServer Static Shapes** stencil to the drawing.
2. Because the input network variables on the lights have **SNVT_switch** types, drag an **nvoSwitch** output network variable shape from the **LonMaker NV Shapes** stencil onto the Scheduler functional block.
3. **Note:** When you add a dynamic network variable to a SmartServer functional block, the change to the OpenLNS network database is automatically propagated to the SmartServer over the LONWORKS channel. As a result, the functional block and the dynamic network variable are automatically added to the navigation pane. You do not need to manually synchronize the SmartServer to the OpenLNS network database in order to display these objects in the navigation pane.
4. Connect the **nvoSwitch** output network variable on the Scheduler functional block to the **SNVT_switch** input network variables on the lights' functional blocks.
5. Because the feedback output network variables on the lights have **SNVT_switch** types, drag an **nviSwitch** input network variable shape from the **LonMaker NV Shapes** stencil onto the Data Logger functional block and create two **nviSwitch** input network variables.
6. Connect the feedback output network variables on the lights' functional blocks to the **nviSwitch** input network variables on the Data Logger functional block.



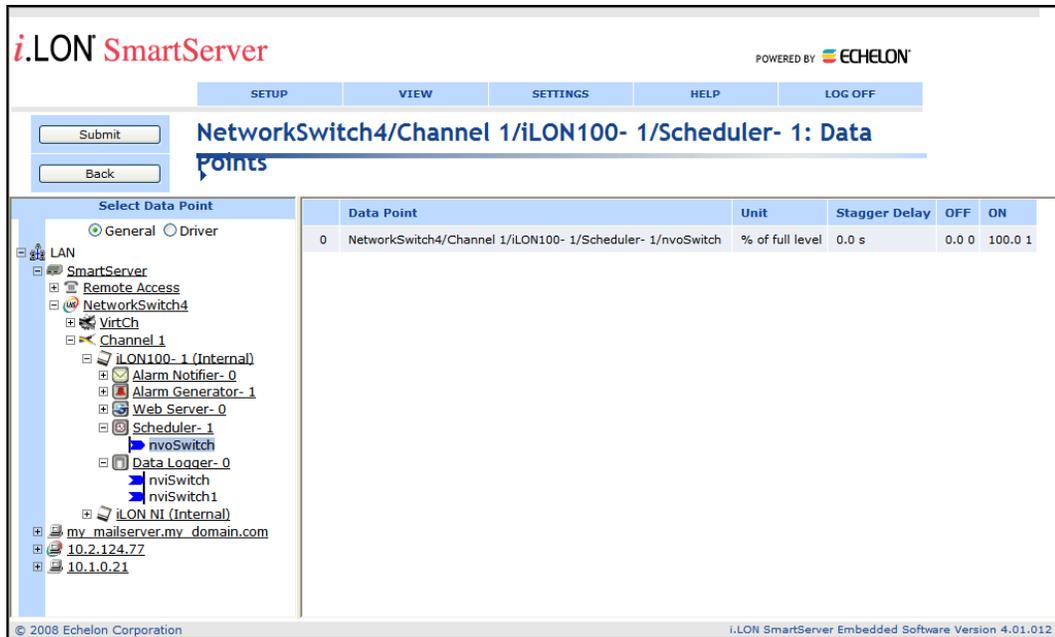
- Open the Scheduler Configuration Web page on the SmartServer following the steps described in the previous section, *Opening SmartServer Applications with OpenLNS CT*. The **Scheduler: Configure** Web page opens.



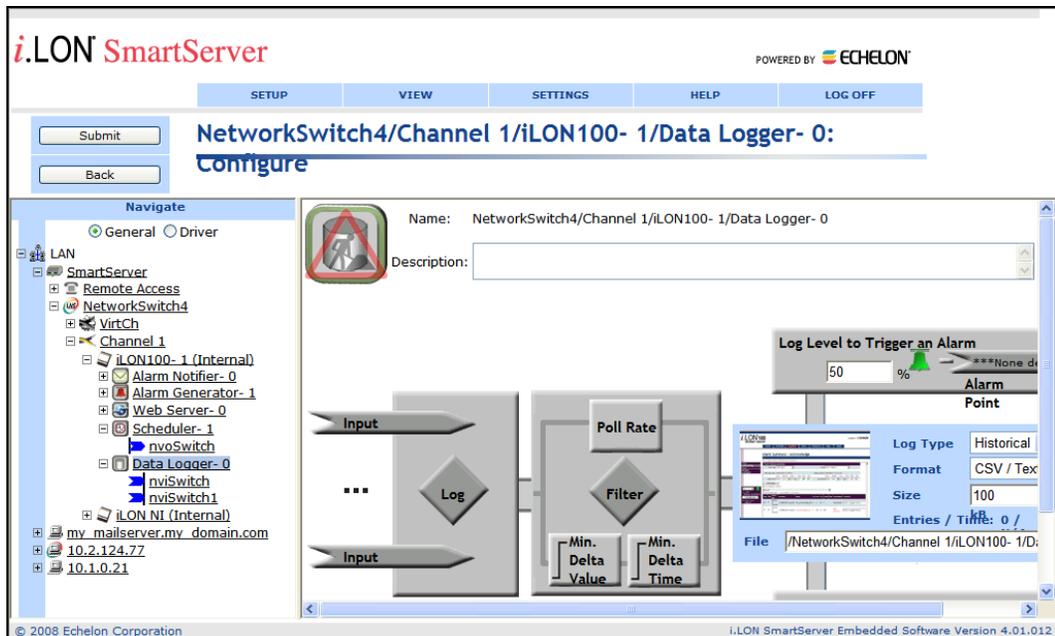
- In the navigation pane, expand the blue-highlighted Scheduler functional block to show the dynamic network variable (**nvoSwitch**) you added to the Scheduler functional block with OpenLNS CT in step 2.
- Click the data point box on the right side of the **Scheduler: Configure** Web page to open the **Scheduler: Data Points** Web page.

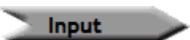


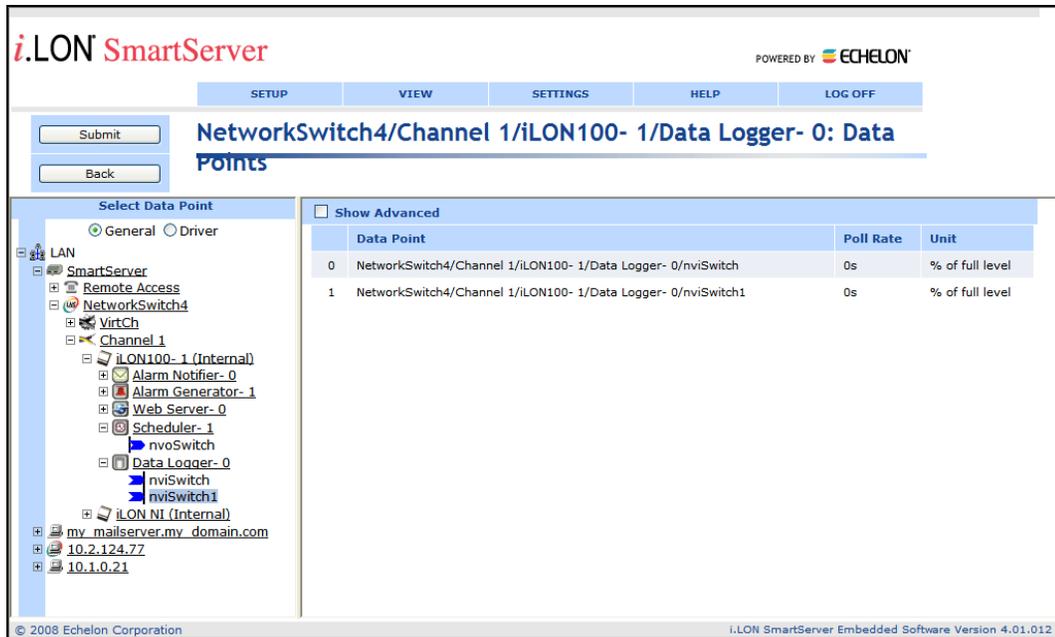
- Add the **nvoSwitch** data point to the Scheduler application. To do this, click the **nvoSwitch** data point in the navigation pane to the left. Optionally, you can add or modify the data point's presets (see Chapter 7 of the *SmartServer User's Guide* for more information for how to do this).



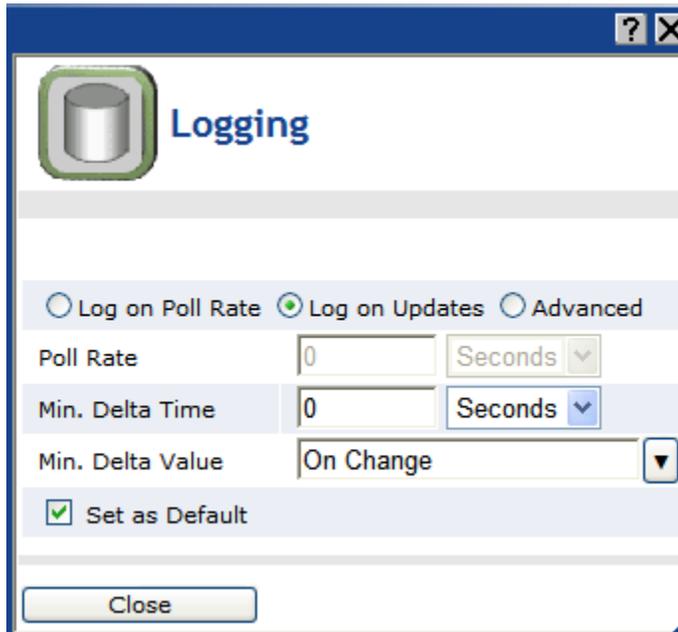
11. Click **Submit**, and then click **Back** to return to the **Scheduler: Configure** Web page. Finish configuring the Scheduler application following Chapter 7, *Scheduling*.
12. In the navigation pane, click the Data Logger functional block. The **Data Logger: Configure** Web page opens. Expand the Data Logger functional block to show the dynamic network variables (**nviSwitch** and **nviSwitch1**) that you added to the Data Logger functional block with OpenLNS CT in step 4.



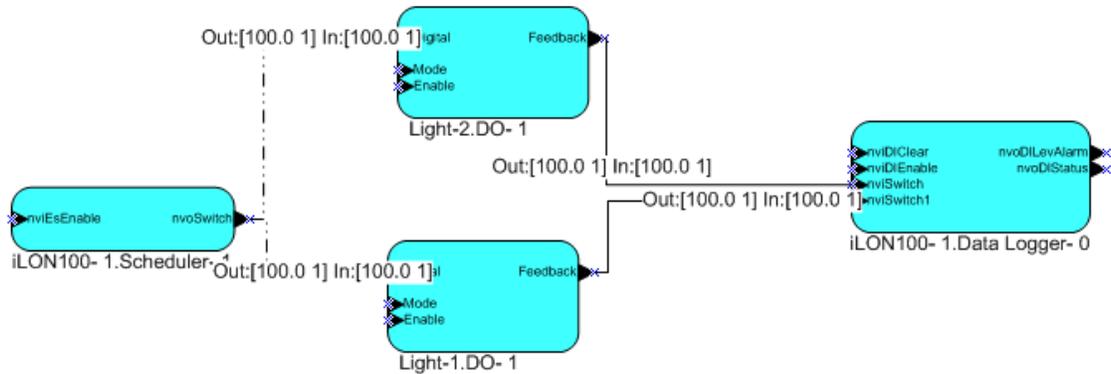
13. Click one of the **Input** icons (), or click anywhere in the **Log** box (). The **Data Logger: Data Points** Web page opens in the application frame to the right.
14. Click the **nviSwitch** and **nviSwitch1** data points in the navigation pane to add them to the Data Logger application.



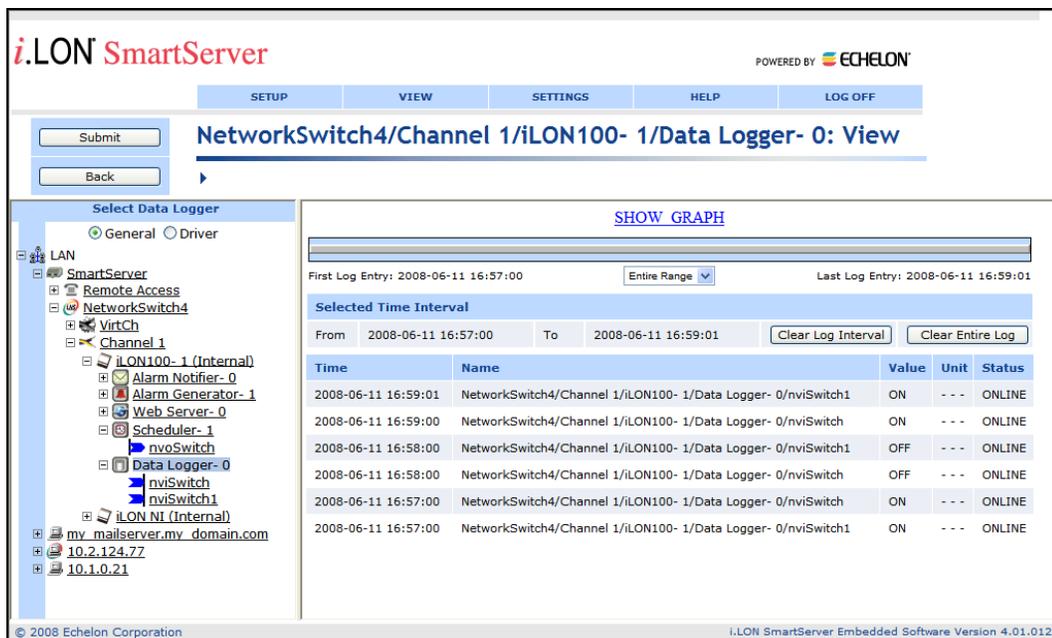
- Click the **Poll Rate** box for either data point to open the **Logging** dialog. Select the **Log on Updates** option, select **On Change** in the **Min. Delta Value** box, and then select **Set as Default**. This means that entries will be added to the Data Logger whenever the **nviSwitch** or **nviSwitch1** values change.



- Click **Close**, click **Submit**, and then click **Back** to return to the **Data Logger: Configure Web** page. Finish configuring the Data Logger application following Chapter 8, *Data Logging*.
- In your OpenLNS CT drawing, verify that the **SNVT_switch** input network variables on the lights' functional blocks have been updated after the Scheduler executed its events on the **nvoSwitch** output network variable.



18. In the SmartServer Web interface, click **View** and then click **Data Logger** to verify that the Data Logger recorded updates to the **nviSwitch** and **nviSwitch1** data points when the Scheduler changed their values.



Binding SmartServer FBs with Dynamic NVs in Stencils

The SmartServer’s internal automated systems device (i.LON App, iLON SmartServer- 1, or other user-defined name) includes four functional blocks/applications that have dynamic network variables in their stencils: the Alarm Generator, Alarm Notifier, Analog Functional Block, and Real-Time Clock functional blocks.

You can bind the dynamic network variables in these functional blocks to compatible network variables on other devices with LONWORKS connections in OpenLNS CT or other OpenLNS application. You can then select the dynamic network variables as input, output, and compare data points in the functional blocks’ corresponding configuration Web pages in the SmartServer Web interface.

Consider a scenario in which you want to connect a thermostat, a SmartServer Alarm Generator, a SmartServer Alarm Notifier, and an AC unit so that an alarm is triggered when the temperature is x degrees below a given setpoint, an e-mail notification is sent by the Alarm Notifier, and the AC unit is turned off.

To create the solution for this scenario, you could follow these steps:

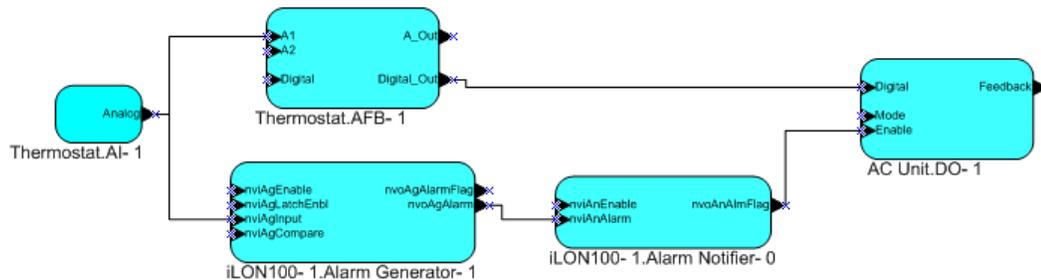
1. In OpenLNS CT, drag the functional blocks for the external devices to the OpenLNS CT drawing, and drag the SmartServer's Alarm Generator and Alarm Notifier functional blocks from the **SmartServer Static Shapes** stencil to the drawing.
2. Connect the output network variable on the thermostat to the **nviAgInput** input network variable on the Alarm Generator functional block. The **nviAgInput** input network variable contains the value to be evaluated by the Alarm Generator.

Connect another compatible output network variable to the **nviAgCompare** input network variable on the Alarm Generator functional block, or use a Data Point shape or the OpenLNS CT Browser to set the value of the **nviAgCompare** network variable. The **nviAgCompare** input network variable represents the value to that will be evaluated against the **nviAgInput** network variable. You can also specify a constant value to be compared against the **nviAgInput** network variable using the Alarm Generator configuration Web page in the SmartServer Web interface.

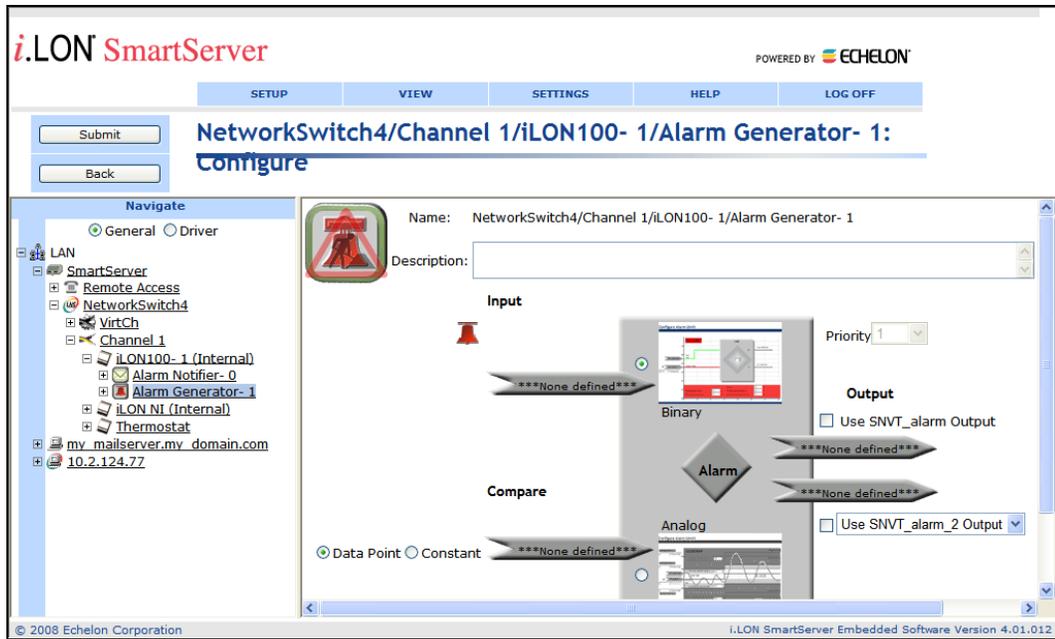
By default, the referenced network variables on the on the Alarm Generator are of a **SNVT_temp_f** type. If this type is not compatible with the output network variables on the devices to which they are bound, you can change the type. To do this, right-click the network variable on the Alarm Generator functional block and then click **Properties** in the shortcut menu. In the **Type Name** property, click the button to the right to open up the **Select Network Variable Type** dialog and then change the network variable type.

You can repeat this process for changing the types of other dynamic network variables on the SmartServer's Alarm Generator, Alarm Notifier, Analog Functional Block, and the Real-Time Clock functional blocks so that they are compatible with the network variables on other devices.

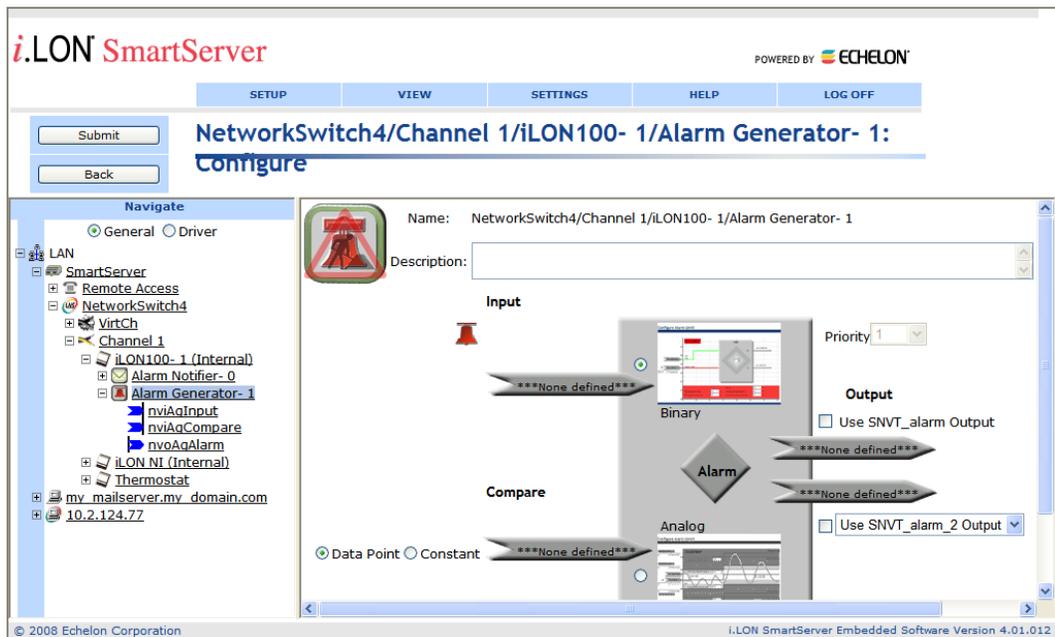
3. Connect the **nvoAgAlarm** output network variable on the Alarm Generator functional block to the **nviAnAlarm** input network variables on the Alarm Notifier functional block. Both of these network variables are of a **SNVT_alarm** type.
4. Connect the **nvoAnAlmFlag** output network variable on the Alarm Notifier functional block to the input network variable on the AC unit that enables and disables the device (for example, an **nviEnable** network variable). The **nvoAnAlmFlag** output network variable is of a **SNVT_switch** type.



5. Open the Alarm Generator Configuration Web page on the SmartServer following the steps described in the previous section, *Opening SmartServer Applications with OpenLNS CT*. The **Alarm Generator: Configure** Web page opens.



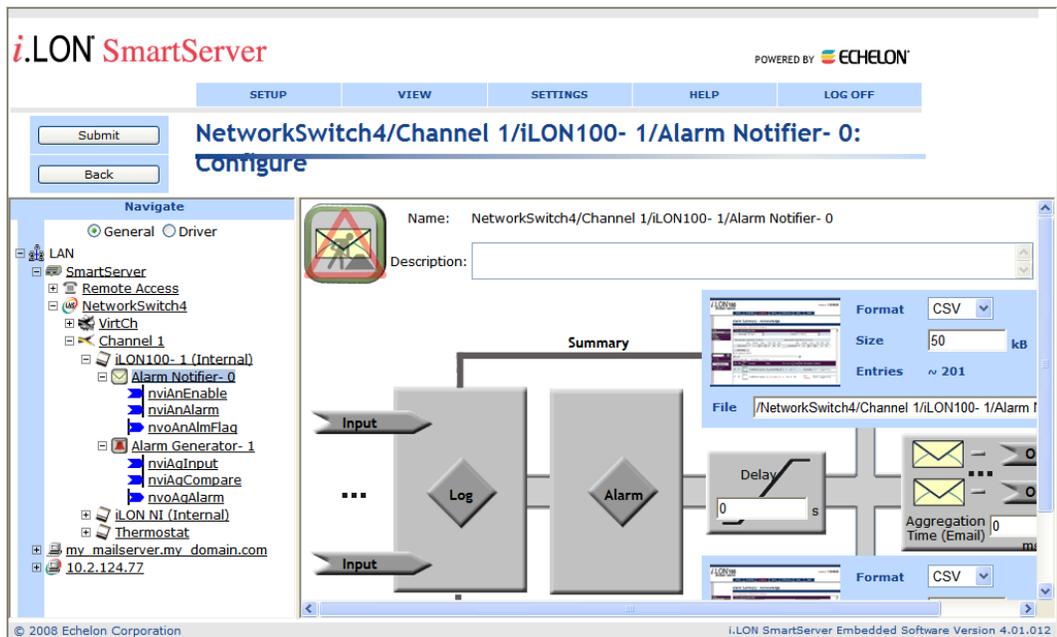
6. In the navigation pane, expand the blue-highlighted Alarm Generator functional block to show its data points. The data points shown correspond to the dynamic network variables in the functional block's LonMaker stencil.



7. Select the input, compare, and output data points to be used by the Alarm Generator following these steps:
 - a. Click the data point icon (***None defined***) below **Input** in the application frame to the right and then click the **nviAgInput** data point in the navigation pane to the left.
 - b. Click the data point icon (***None defined***) below **Compare** in the application frame and then click the **nviCompare** data point in the navigation pane.
 - c. Click the data point icon (***None defined***) directly below the **Use SNVT_alarm Output** check box in the application frame to select a SNVT_alarm data point, or click the data point

icon directly above the **Use SNVT_alarm_2 Output** check box to select a **SNVT_alarm_2** data point and then select whether you are using a **SNVT_alarm_2** or a **UNVT_alarm_2** data point from the list. Click the **nvoAgAlarm** data point in the navigation pane.

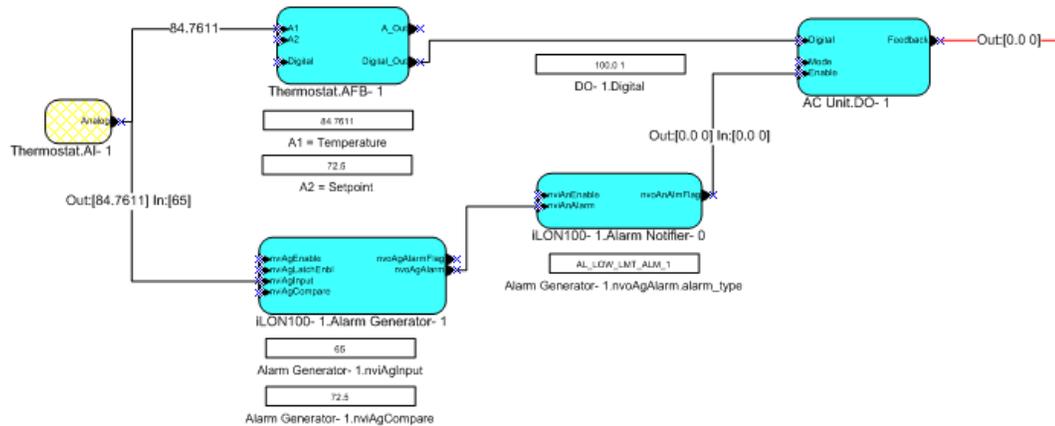
- d. Click **Submit**.
8. Select whether the Alarm Generator uses a binary or analog function to evaluate the value of the input point against that of the compare point. After you select the comparison function to be used, configure the function. For the binary function, this means selecting the logical function to be used to compare the points; for the analog function, this means defining offsets and hysteresis levels. See Chapter 6 of the *SmartServer User's Guide* for more information on how to do this.
9. In the navigation pane, click the Alarm Notifier functional block. The **Alarm Notifier: Configure** Web page opens. Expand the Alarm Notifier functional block to show its data points.



10. Click the Alarm Notifier functional block in the SmartServer to open the **Alarm Notifier: Configuration** Web page.
11. Select the input and output data points to be used by the Alarm Notifier following these steps:
 - a. Click one of the **Input** icons (), or click anywhere in the **Log** box (). The **Alarm Notifier: Data Points** Web page opens in the application pane.
 - b. Click the **nviAnAlarm** data point in the navigation pane, click **Submit**, and then click **Back** to return to the **Alarm Notifier: Configuration** Web page.
 - c. Click any of the e-mail or data point icons above the **Aggregation Time (e-mail)** box in the application frame to the right. The **Alarm Notifier: Destination** Web page opens.
 - d. Under the **Output** column, click the Active Alarm Condition row (), click the **nvoAnAlmFlag** data point in the navigation pane to the left, and then select the OFF preset in the **Value** column. The data point is set to 0.0 0 when an active alarm condition is received. By default, active alarm conditions include **AL OFFLINE**, **AL_HIGH_LMT_ALM_1**, **AL_LOW_LMT_ALM_1**, **AL_HIGH_LMT_ALM_2**, **AL_LOW_LMT_ALM_2**, and **AL_ALM_CONDITION**.
 - e. Repeat step d, except click the click the Passive Alarm Condition row () under the **Output** column and select the ON preset in the Value column. The nvoAnAlmFlag data point is

updated to 100.0 1 when the data point returns to its passive (normal) condition (**AL_NO_CONDITION** by default).

- f. Click **Submit** and then click **Back** to return to the **Alarm Notifier: Configuration** Web page.
12. In your OpenLNS CT drawing, use a Data Point shape or the OpenLNS CT Browser to set the **nviAgInput** on the Alarm Generator functional block to a value that triggers an active alarm condition. Observe that the AC Unit is disabled when its enable input data point receives the 0.0 0 value from the Alarm Notifier for the active alarm condition.



13. Return the **nviAgInput** to its previous value. The AC Unit is re-enabled when its enable input data point receives the 100.0 1 value from the Alarm Notifier for the passive alarm condition.

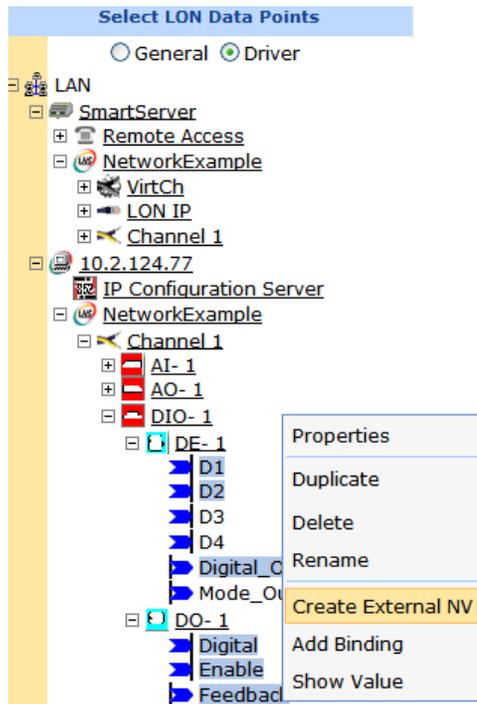
Polling External Network Variables

You can use the SmartServer Web interface to copy the network variables of external devices managed with OpenLNS CT, OpenLNS tree, or another OpenLNS application (formerly referred to as NVEs) to the SmartServer. The SmartServer's internal data server will then poll the external data point at the rate specified in the data point's **Setup – LON Data Point Driver** Web page. You can then add the data points to the SmartServer's built-in applications and to your custom SmartServer Web pages.

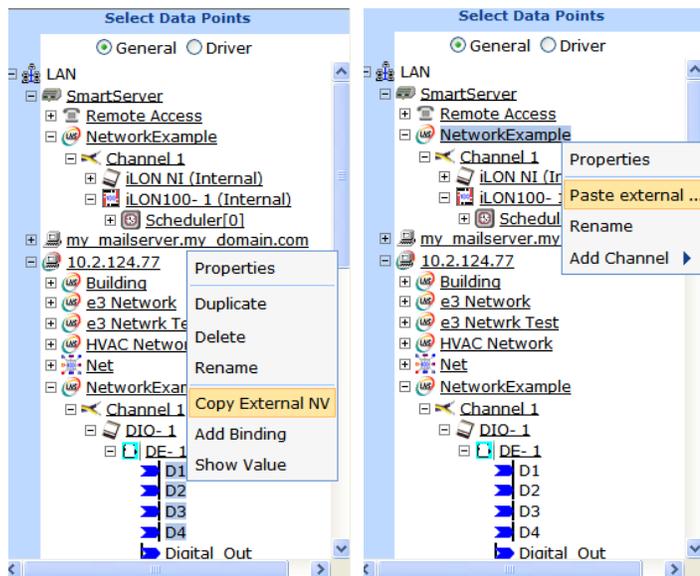
To copy network variables from OpenLNS CT to the SmartServer and set their poll rates, follow these steps:

1. Verify that you have installed the Echelon iLON Enterprise Services from the SmartServer 2.2 DVD. See *Installing Echelon iLON Enterprise Services* in Chapter 2 for more information on how to do this.
2. Verify that you have added an OpenLNS Server to the LAN that contains the OpenLNS network database in which the network variable or configuration property is stored. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for more information on how to do this.
3. Verify that you have synchronized the target SmartServer with the OpenLNS network database containing the external network variables or configuration property you are copying. See *Synchronizing the SmartServer to an OpenLNS network database* in Chapter 5 for more information on how to do this.
4. Expand the LNS Server icon, and then, if prompted, enter the **User Name** and **Password** for logging in to the OpenLNS Server via the Echelon Enterprise Services 2.2. You initially specified the user name and password in the Echelon Enterprise Services 2.2 installer. If you forgot the user name and password, you can right-click the Echelon Enterprise Services 2.2 tray icon in the notification area of your computer, and then click **Options** on the shortcut menu..
5. In the OpenLNS tree, expand the OpenLNS network database, channel, device, and functional block containing the network variable to be copied to the local SmartServer, right-click the network variable, and then select **Create External NV** on the shortcut menu. To copy multiple

network variables, click one, and then either hold down CTRL and click all others to be copied or hold down SHIFT and select another to select the entire range, right-click one of the selected network variables, and then click **Create External NV** on the shortcut menu.



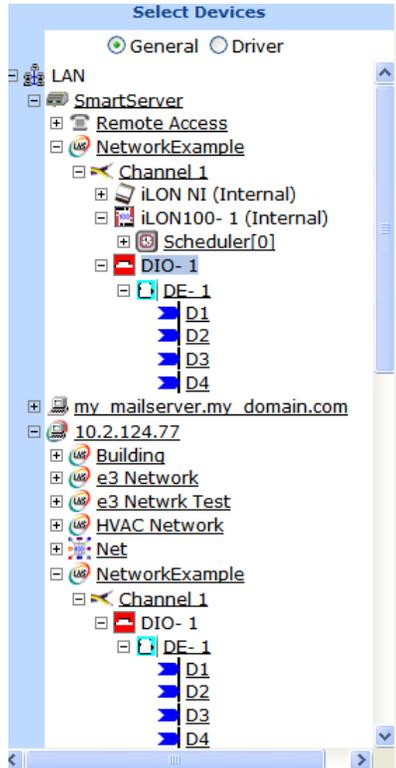
Note: If you have one or more remote SmartServers on the LAN, the **Create External NV** option is not available in the shortcut menu of the network variable in the OpenLNS tree. Instead, right-click the network variable in the OpenLNS tree, select **Copy External NV** on the shortcut menu, right-click any object in the network tree of the target SmartServer, and then click **Paste External** on the shortcut menu.



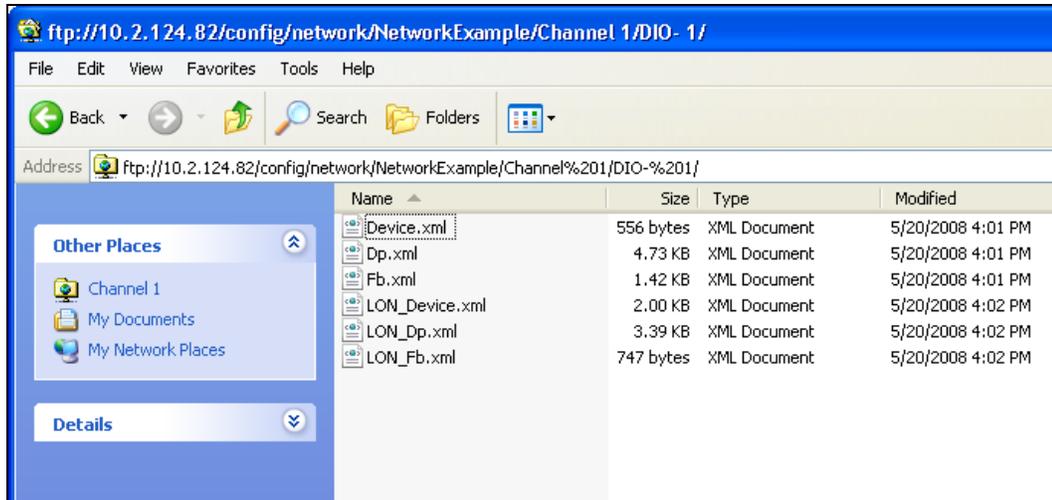
Tip: If you need to copy a large number of external data points to the SmartServer, you can copy one or more external devices in the OpenLNS tree that have the same program ID and then use a device template to paste specific data points in the device interface to the SmartServer tree. This feature provides the functionality of the i.LON 100 PointFactory Plug-in, which is compatible

with the e2 and e3 releases of the i.LON 100 software. For more information on using device templates to copy external data points to the SmartServer, see *Creating External Data Points from Device Templates* in Chapter 4, *Using the SmartServer Web Interface*.

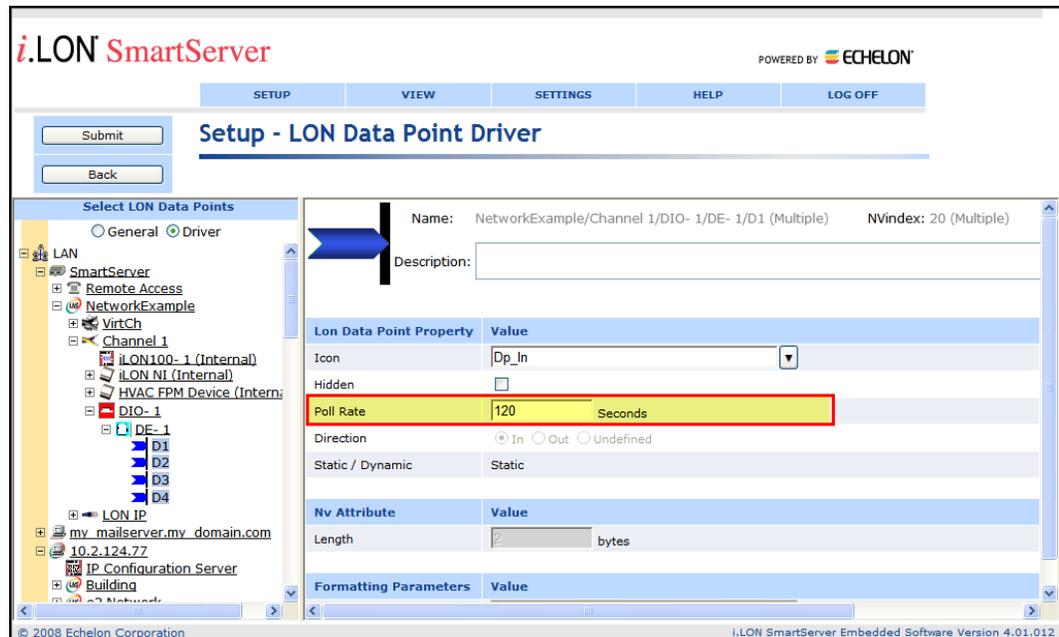
6. The data points and their parent channels, devices, and functional blocks are added to the network tree of the target SmartServer. The parent objects are only added if they do not already exist in the internal database of the target SmartServer.



7. Copying data points from the OpenLNS tree to the SmartServer tree also creates or updates the data points and their parent objects in the SmartServer's internal database. Specifically, new or updated XML files representing the general and LONWORKS properties of the copied data points and their parent objects are saved to the `/config/network/<Network>/<Channel>/<Device>` folder on the SmartServer's flash disk. This means that you can now directly make changes to these objects in the SmartServer tree, and they will be propagated to the OpenLNS network database (the changes are propagated automatically if you are using **LNS Auto** mode, or they are propagated when you manually synchronize the SmartServer to the OpenLNS network database).



8. Click **Submit**.
9. Set how frequently the SmartServer's internal data server polls the external data points. To do this, follow these steps:
 - a. Click the **Driver** option above the navigation pane on the left side of the SmartServer Web interface.
 - b. In the navigation tree of the target SmartServer, select one or more external data points. The **Setup – LON Data Point Driver** Web page opens.
 - c. In the **Poll Rate** box, set the poll rate (in seconds). The default poll rate for external network variables copied from the OpenLNS tree to the SmartServer tree is **120** seconds. The recommended minimum poll rate is 30 seconds; the maximum poll rate is 1 second.



Note: The actual poll rate for a data point is determined by calculating the greatest common divisor of all the poll rates set for the data point in the applications to which it has been added.

For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 7 seconds, the SmartServer's internal data server will poll the data point every 1 second.

Therefore, set poll rates in the SmartServer's applications that are the same for a given data point, or poll rates that are at least multiples of each other. For example, if a Data Logger polls a data point every 5 seconds, and an Alarm Generator polls the same data point every 10 seconds, the SmartServer's internal data server will poll the data point every 5 seconds.

10. Click **Submit**.
11. You can now add the data points of the external devices to the SmartServer's built-in applications and to your custom SmartServer Web pages. For more information on adding data points to the SmartServer's built-in applications, see *Adding Data Points to SmartServer Applications* in Chapter 4, *Using the SmartServer Web Interface*. For more information on adding data points to your custom SmartServer Web pages, see Chapter 12, *Creating Custom SmartServer Web Pages*.

Troubleshooting SmartServer-OpenLNS CT Synchronization

This section describes some of the problems that you could encounter when synchronizing the SmartServer with OpenLNS CT.

The SmartServer Web page doesn't show changes after a resynchronization or the Web page application icon still has a construction red triangle on it.

Refresh the SmartServer Web page. Sometimes the Web page will take some time to update. The construction red triangle could also mean you haven't finished configuring the functional block (for example, you haven't assigned the Alarm Generator a compare data point).

I don't see the information that I expect in the OpenLNS CT drawing or SmartServer.

The OpenLNS network database and the SmartServer are out of sync, the OpenLNS CT drawing is out of sync with the OpenLNS network database, or functional blocks in the OpenLNS CT drawing are on top of each other.

To update the SmartServer, manually synchronize the SmartServer to the OpenLNS network database, refresh the SmartServer web pages, delete all temporary internet files stored, and then close and re-open your Web browser.

If you are missing functional blocks in the OpenLNS CT drawing, check if you have any functional blocks in the upper left-hand corner of the OpenLNS CT drawing. Sometimes OpenLNS CT will overlay functional blocks in the upper-left hand corner. You can move these functional blocks to see if there are functional blocks underneath. You can then synchronize the OpenLNS CT drawing to the OpenLNS network database.

I get an "Attempt to assign a neuron ID that is already in use by another device. (Subsystem: LNS, #102" error) when I try to commission the SmartServer.

This means that there are two SmartServer shapes in the OpenLNS CT drawing (i.LON App on a LON channel that cannot communicate with the OpenLNS network interface, and iLON SmartServer- 1 on a different channel). This probably occurred because you did not commission the SmartServer with OpenLNS CT before synchronizing the SmartServer to the OpenLNS network database. In this case, use OpenLNS CT to delete the iLON SmartServer-1 device shape; move the i.LON App, IP-852 router, and iLON NI shapes to a channel that can communicate with OpenLNS network Interface; commission the i.LON App, IP-852 router, and iLON NI device shapes; and then delete the LON channel.

I try to add a new Functional Block (for example, Alarm Generator) but the FB shows up and then disappears.

You probably tried to use a functional block index that was already added in either the OpenLNS CT drawing or through the SmartServer. If you are using LNS Auto mode, you will see the functional

block appear and then disappear after the SmartServer automatically performs a synchronization. You need to use a different functional block index when you add the functional block.

I added a SmartServer functional block through the SmartServer Web page (LNS Auto mode), but it didn't show up in my OpenLNS CT drawing.

This probably means that the OpenLNS CT drawing is out of sync with the OpenLNS database. Synchronize the OpenLNS CT drawing to the OpenLNS network database

I added a SmartServer functional block in the OpenLNS CT drawing but it doesn't show up in the SmartServer tree after synchronizing the SmartServer to the OpenLNS network database.

All SmartServer functional blocks are either shown in the SmartServer tree under the SmartServer's internal App device or are hidden (and have the items hidden flag set). You can show all hidden functional blocks by clicking **Settings** and then selecting the **Functional Blocks** checkbox in the **Display Hidden** property in the **Global Settings** dialog, or you can right click the SmartServer's internal App device and add the functional block using the same name the functional block has in the OpenLNS network database. Re-adding the functional block doesn't actually add a new functional block, it just clears the functional block's hidden flag.

Appendix A

Troubleshooting the SmartServer

This appendix describes how to diagnose and resolve common problems that may occur when using the SmartServer.

Troubleshooting

I can access my SmartServer Web pages but some content seems to be missing.

The SmartServer has been tested with Microsoft Internet Explorer 8 and 9, Mozilla Firefox 18, Google Chrome 24, and Apple Safari 6.0. Some pages may not display correctly on other browsers.

My network variables based on UNVTs show up and then disappear

Most likely the resource files that you are using are in the wrong folder on the SmartServer flash disk. If you saved the resource files in the `/lonWorks/types` folder they may not show up. Save the resource files in a company-specific directory in the `/lonWorks/types` folder (e.g., `/lonWorks/types/User/YourCompany`).

The SmartServer exhibits problems due to a low-memory condition. This could be indicated by one or more of the following: “out-of-memory” messages, slow network access, application performance problems, or even an unexpected reboot. What is wrong?

Reduce the number of Alarm Notifiers and/or the size limit of the alarm Summary Logs (which are kept in RAM).

Reduce the number of Web clients that are simultaneously accessing the SmartServer.

If you are making calls to the SOAP interface on the SmartServer refer to the *SmartServer 2.2 Programmer's Reference* for specific recommendations on limiting SOAP messages.

I can't make my SmartServer send an e-mail message. What am I doing wrong?

E-mails are sent as a result of alarm conditions. Verify that the alarm condition actually triggers and that the e-mail should be sent.

After changing the type of a data point using the LonMaker browser, the data point starts showing incorrect data.

The OpenLNS Server may be using old format data. Close and restart all OpenLNS applications.

My Service LED is blinking, what does this mean?

The Service LED blinks when the SmartServer is not commissioned. When the SmartServer is added to a network and commissioned, the Service LED will turn off.

When updating the SmartServer, I get an error that the update completed successfully, but the device has not been updated successfully yet. What is wrong?

This error occurs when you attempt to update the SmartServer while monitoring many of its network variables with a very short poll time. Try turning off monitoring or increasing the poll time.

I can't open the network using a non-SmartServer network interface. What is wrong?

If you were using the SmartServer as an RNI and then switched to another network interface, you need to disable RNI on the SmartServer in order to open the network. This can be done using the console application or the Setup - Security Web page.

I can't open the network using the SmartServer as an RNI. What is wrong?

Can you access the SmartServer via HTTP (*i.e.* the SmartServer Web pages)? If not, then you may not be in TCP/IP communication with the SmartServer. Check the connection. If using static IP addresses, make sure that your computer is on the same subnet as the SmartServer. If using DHCP, consult your network administrator.

If you can see the SmartServer Web pages, but still cannot open the network via RNI, check the following:

Ensure that RNI is enabled on the SmartServer with the Setup - Security Web page or with the console application.

Ensure that you have created an RNI entry for the SmartServer with the LONWORKS Interfaces application that has the correct IP address/hostname, port and MD5 Authentication Key.

The SmartServer gets a duplicate IP address assigned from a DHCP server, and either boots using its default IP address (*i.e.* 192.168.1.222), or boots using the duplicate IP address.

If the SmartServer boots using its default IP address when it has obtained an address via DHCP, it is probably because the DHCP server assigned an address already in use by another computer on the network. This may happen if the other computer is disconnected from the network long enough for its DHCP lease to expire, yet continues using that address after reconnecting to the network. Make sure all other computers on the network using DHCP have valid leases. If the SmartServer detects this condition, it will boot using its default IP address (typically 192.168.1.222), and will continue attempting to contact a DHCP server. Once it can contact a DHCP server, the SmartServer will reboot to obtain a new IP address.

The SmartServer may not initially detect the above condition, in which case it will boot using the duplicate IP address. At some point the SmartServer may discover that the address is a duplicate, but will continue using it. Make sure all computers on the network using DHCP have valid leases. Reboot the SmartServer to obtain another address, if necessary, or use a statically configured address.

Appendix B

Using the SmartServer Console Application

This appendix describes how to use the SmartServer's console application.

Using the Console Application

You can use the console application to configure and troubleshoot the SmartServer. To access the console application, connect one end of a RS-232 null modem cable to the console port on the SmartServer, and then connect the other end to one of the COM ports on your computer. You can then use a terminal emulation program such as PuTTY on your computer to access the SmartServer's console application and configure the SmartServer. The default communication properties for the SmartServer are **9600-8-None-1-None**. For more information on the console port on the SmartServer hardware, see the SmartServer *Hardware Guide*.

Notes:

- Use the SmartServer's built-in Web pages to configure the SmartServer whenever possible.

Console Command List

Once you have accessed the SmartServer console application, you can issue commands. You must reboot the SmartServer using the SmartServer Web pages or the console application to implement any changes made with commands in the console application.

- To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.
- To reboot your SmartServer using the SmartServer console application, enter the `reboot` command.

The following table lists the commands you can use with the SmartServer console application.

Command	Description
activateapp <i>index/name</i>	The SmartServer uses a multitasking operating system that can simultaneously run multiple processes. This command allows you to selectively activate or deactivate processes.
archive <i>name</i>	Create a compressed tar archive of a directory or file on the SmartServer and store its contents in a Gnu Zip file. The directory remains unchanged by this command. For example, if you ran the command archive data , the SmartServer would create a file called data.tar.csv.gz that contains the entire data directory. The directory or file to be archived must be located in the current working directory. This command is CPU intensive and may cause a delayed response to requests (for example SOAP requests) that are sent while the SmartServer is processing the command. The contents of this file can be extracted with the extract command.
authkey <i>type key</i>	Sets the 16-byte MD5 authentication keys for RNI and the IP-852 router.
bootlog	Enables or disables the bootlog on the root directory of the SmartServer flash disk. If you disable the bootlog, the two most recent bootlogs (<code>bootlog.txt</code> and <code>bootlogprev.txt</code>) are preserved on the SmartServer flash disk and then new bootlogs are no longer recorded.
cd [<i>directory</i>]	Changes to the specified directory. If no argument is provided, displays current directory.

Command	Description
compress <i>name</i>	<p>Compresses a text file, specified by its file name, into Gnu Zip format (.csv.gz file extension). A new file is created by this command, and the original file remains uncompressed.</p> <p>The file to be compressed must be located in the current working directory.</p> <p>If you ran the command Compress exceptionlog1.txt, then a compressed version of the exceptionlog1.txt file named exceptionlog1.txt.csv.gz would be created.</p> <p>This command is CPU intensive and may cause a delayed response to requests (for example SOAP requests) that are sent while the SmartServer is processing the command.</p>
confirmation <i>on/off</i>	Sets confirmation on and off
csaddr <i>address</i>	Sets the IP address of the IP-852 Configuration Server on the IP-852 channel to which the SmartServer is attached.
csport <i>port</i>	Sets the port used by the IP-852 Configuration Server to receive messages from the SmartServer.
copy <i>file1 file2</i>	Copies <i>file1</i> to <i>file2</i> .
createapp <i>name</i>	Creates an application instance, specified by name, and returns the index assigned to the application. The application is automatically activated upon creation. Generally, you will not need to use this command.
cenelec <i>on/off</i>	Power line model only. Puts the SmartServer in CENELEC mode (for communicating on European C-band power line networks). If you change this value, close all applications to which the SmartServer is connected as an RNI, reboot the SmartServer and re-establish an RNI connection.
date <i>dd/mm/yyyy</i>	Sets or displays the date if the SmartServer is not synched to an SNTP server.
deactivateapp <i>index/name</i>	Deactivates an application instance, specified by index or name. See listapp for supported names. This command does not delete the instance of the application; it deactivates the application. Primarily used for troubleshooting.
decompress <i>file</i>	<p>Decompresses a file created in Gnu Zip format (.csv.gz file extension) into a normal text file. A new file is created by this command, and the original file remains uncompressed.</p> <p>The directory or file to be decompressed must be located in the current working directory.</p> <p>If you ran the command Compress exceptionlog1.txt.csv.gz, then a decompressed version of the exceptionlog1.txt.csv.gz file named exceptionlog1.txt would be created.</p> <p>This command is CPU intensive and may cause a delayed response to requests (for example SOAP requests) that are sent while the SmartServer is processing the command.</p>
delete <i>file</i>	Deletes <i>file</i> .

Command	Description
deviceid <i>hexID</i>	Sets or displays the Neuron ID of the SmartServer's application device [i.LON App (Internal) in the SmartServer tree].
diag <i>Module subcommand [params]</i>	Performs diagnostic commands on the SmartServer. The <i>module</i> argument may be set to one of the following: <ul style="list-style-type: none"> • task • system • ftp • network • routes • dhcp • flashdiskwearmonitor
dir [<i>directory</i>]	Lists directory contents. If no directory is specified, lists the contents of the current directory.
disable <i>service</i>	Disables a service. Available services are: <p>eFtp – FTP access.</p> <p>Web – HTTP access.</p> <p>Dial-in – Dial-in access.</p> <p>IPv4DnsServerViaDhcp – Obtaining DNS server from DHCP on IPv4 networks.</p> <p>IPv4DnsDomainViaDhcp – Obtaining DNS suffix via DHCP on IPv4 networks.</p> <p>IPv6ManualAddress – Manually setting the IPv6 network address and gateway address with the IPv6address, IPv6prefixlength and IPv6gateway commands.</p> <p>IPv6stack – Disables the IPv6 interface on the SmartServer.</p> <p>secureaccess – Disables security access mode temporarily, until the next time the SmartServer is rebooted. You can also re-enable security access mode with the enable command after running this command.</p> <p>secureaccess always – Disables security access mode persistently, even through reboots of the SmartServer. You can re-enable security access mode with the enable command after running this command.</p>
dnsdomain <i>domain</i>	Sets the DNS domain name. This command is valid only when DHCP is turned off, or Obtaining DNS Suffix From DHCP is disabled while DHCP is enabled (see the enable and disable commands for more information).
dnsprimary <i>address</i>	Sets the IP address of the primary DNS server. This command is valid only when DHCP is turned off, or Obtaining DNS Suffix Via DHCP feature is disabled while DHCP is enabled (see the enable and disable commands for more information). This command accepts both IPv4 and IPv6 addresses.
dnssecondary <i>address</i>	Sets the IP address of the secondary DNS server. This will only be used if the primary DNS server cannot be contacted. This command accepts both IPv4 and IPv6 addresses.

Command	Description
dump ip852config	Copies the IP-852 configuration to the <code>//ltconfig/xmldump/LTIP_config.xml</code> file.
enable <i>service</i>	<p>Enables a service. Available services are:</p> <ul style="list-style-type: none"> • Ftp – FTP access. • Web – HTTP access. • Dial-in – Dial-in access. • ipv4DnsServerViaDhcp – Obtaining DNS Server from DHCP when using IPv4. • ipv4DnsDomainViaDhcp – Obtaining DNS suffix via DHCP when using IPv4. • ipv6dhcp dnsdomain – Obtaining DNS suffix via DHCP when using IPv6. • ipv6dhcp dnsserver – Obtaining DNS Server from DHCP when using IPv6. • ipv6ManualAddress – Manually setting the IPv6 network address and gateway address with the <code>IPv6address</code>, <code>IPv6prefixlength</code> and <code>IPv6gateway</code> commands. • ipv6stack – Enables the IPv6 interface on the SmartServer. • SecureAccess – Enables security access mode temporarily, until the next time the SmartServer is rebooted. You can also disable security access mode with the disable command after running this command. • SecureAccess always – Enables security access mode persistently. This is the default setting. You can disable security access mode with the disable command.
ethernetspeed <i>mode</i>	<p>Sets the Ethernet speed (10 or 100 MB per second) and mode (full-duplex or half-duplex) of the SmartServer to one of the following values:</p> <ul style="list-style-type: none"> • auto (auto-negotiation). The SmartServer employs auto negotiation to determine the Ethernet speed and mode to use based upon the device with which it is communicating. This is the default. • 100f (100 MB full-duplex). Data streams in both directions simultaneously at 100 MB/s. • 100h (100 MB half-duplex). Data streams in one direction at a time at 100 MB/s. • 10f (10 MB full-duplex). Data streams in both directions simultaneously at 10 MB/s. • 10h (10 MB half-duplex). Data streams in one direction at a time at 10 MB/s.
eventlog <i>on/off</i>	Turns the console event log on and off. The event log is kept in <code>eventlog.txt</code> in the root directory of the SmartServer.

Command	Description
extract <i>name</i>	<p>Extracts the contents of a directory or file created with the compress command. The directory or file to be extracted must have the extension .tar.csv.gz, and must be located in the current working directory. The archive will be extracted into the current directory.</p> <p>This command is CPU intensive and may cause a delayed response to requests (for example SOAP requests) that are sent while the SmartServer is processing the command.</p>
factorydefaults [<i>keepipaddrs</i>]	<p>Resets the SmartServer to its factory default settings. Files added by the user outside of the //software directory (<i>i.e.</i> Web pages) are not affected. If you specify the <i>keepipaddrs</i> parameter, the basic IPv4 or IPv6 addresses are preserved.</p> <p>Run this command from the SmartServer bootrom console. See the <i>Interrupting the Boot Process</i> section later in this appendix for more information.</p>
ftppassword <i>password</i>	Sets the FTP password to <i>password</i> (you cannot use anonymous FTP). The default password is <i>ilon</i> .
ftpport <i>port</i>	Sets the port the used by the SmartServer for FTP communication. The default port is 21 .
ftpuser <i>name</i>	Sets the FTP username to <i>name</i> . The default user name is <i>ilon</i> .
format	<p>Formats the SmartServer's flash disk. This command deletes all files, including the SmartServer's system image file. After using this command, you must upload a new software image to the SmartServer. If you have licensed the IP-852 router, you must also restore the license file.</p> <p>Run this command from the SmartServer bootrom console. Be sure to first back up any files that you may wish to save. See the <i>Interrupting the Boot Process</i> later in this appendix for more information.</p>
help	Displays a listing of the typically used commands. Help all displays a complete command list.
history [<i>size</i>]	If you do not specify the <i>size</i> parameter, this command displays a history of console commands issued since the last reboot. You can specify a size from 10 to 100 to determine how far back the command history is kept.
hostname <i>name</i>	<p>Modifies the hostname. For example, hostname ilon100.</p> <p>Name characters are limited to letters, digits, and embedded hyphens (-). The first character must be a letter and the last character must be a letter or digit.</p>
install <i>idx/name</i> [<i>dmn</i>] <i>sn</i> <i>nd</i>	Installs a LONWORKS domain/subnet/icon address for the application specified by <i>idx</i> . This command is provided for backward compatibility to add a SmartServer to a pre-installed network.
ipv4address <i>address</i>	Modifies the IPv4 network address assigned to the SmartServer. For example, ipv4address 101.253.100. This command is valid only when DHCP is turned off.

Command	Description
ipv4dhcp <i>on/off</i>	Turns IPv4 DHCP on and off. If DHCP is on, the SmartServer DHCP client gets its IP address, gateway, subnet mask, primary DNS server (if used), and DNS domain from a DHCP server.
ipv4gateway <i>address</i>	Modifies the IPv4 gateway address the SmartServer is using. Enter 0.0.0.0 to specify no gateway. For example, <code>ipv4gateway 10.1.10.1</code> . This command is valid only if DHCP is turned off.
ipv6address <i>address</i>	<p>Modifies the IPv6 network address assigned to the SmartServer. The IP address you enter must conform to the IPv6 addressing standards. For example, <code>ipv6address fefe::fefe:dddd</code>.</p> <p>See Table 2.2 for more information on IPv6 network addresses. You must enable the IPv6 interface on the SmartServer and then enable manual entry of the IPv6 configuration, before using this command. You can perform both tasks with the <code>enable</code> command.</p>
ipv6prefixlength <i>length</i>	<p>Modifies the prefix length for the IPv6 network address the SmartServer is using. This must be a decimal integer between 0 and 128. For example, <code>ipv6prefixlength 64</code>.</p> <p>You must enable the IPv6 interface on the SmartServer and then enable manual entry of the IPv6 configuration, before using this command. You can perform both tasks with the <code>enable</code> command.</p>
ipv6gateway <i>address</i>	<p>Modifies the network address of the IPv6 gateway the SmartServer is using. The IP address you enter must conform to the IPv6 addressing standards. For example, <code>ipv6gateway fefe::fefe:dddd</code>.</p> <p>You must enable the IPv6 interface on the SmartServer and then enable manual entry of the IPv6 configuration, before using this command. You can perform both tasks with the <code>enable</code> command.</p>

Command	Description
ip852chanmode <i>mode</i>	<p>Displays the IP-852 channel mode or sets it to one of the following values:</p> <ul style="list-style-type: none"> • 1 - Backward Compatible (required for the i.LON 1000 and LNS 3). You must enable this option if your channel will contain any i.LON 1000's or LNS 3 LONWORKS/IP interfaces. This causes the SmartServer to operate using a protocol that is compatible with these devices, but is not strictly EIA-852 compliant. In backward compatible mode, you can use a maximum of 40 devices. You can only have one device located behind each NAT firewall, and you cannot have duplicate IP addresses or duplicate port assignments. • 2 - Standard EIA-852. Select this option when using a standard LONWORKS IP-852 channel. When using this mode, you can only have one device located behind each NAT firewall. You can use up to 256 devices per channel in this mode. The IP address (including the port assignment) must be unique. This is the default. • 3 - Extended Firewall Support. This option is recommended whenever your IP-852 channel crosses an IP firewall, whether or not the firewall is using Network Address Translation (NAT). Depending on the particular firewall and its configuration, this option may be required. In addition, this will allow you to place more than one IP-852 device behind an NAT firewall, and to create multiple OpenLNS LONWORKS/IP interfaces in the same channel using the same IP address (but with different ports). Without this option, only one device may reside behind a NAT firewall, and all devices on the channel must have unique IP addresses. This option extends the EIA-852 protocol in a way that is not strictly compliant with that standard, though it should still be compatible with other EIA-852 devices. You can use up to 256 devices per channel in this mode.
ip852port <i>portnumber</i>	Sets the local IP port for the IP-852 router.
linkstats [<i>all clear</i>]	<p>Reports or clears the following LonTalk link statistics:</p> <ul style="list-style-type: none"> • Trans pkts. Number of packets transmitted. • Recvd pkts. Number of packets received • Trans errs. Number of transmission errors. • RecvPrPkts. Number of packets received from a retry. • Collisions. Number of packet collisions. • MissedPkts. Number of missed packets.
listapp	Lists the current application instances.
logout	Terminates a Telnet session
ltipport	Reserved.
mkdir <i>directory</i>	Makes a directory.
nataddress <i>address</i>	Sets the external NAT address to be used when the SmartServer is used as an IP-852 router and is installed behind a NAT firewall.
ping <i>hostaddr</i>	Tests communications to another IP host. This command accepts both IPv4 and IPv6 network addresses.

Command	Description
reboot	Reboots the SmartServer. If the SmartServer is currently being used as an RNI, the networks for which it is acting as an interface must be closed and re-opened.
removeapp <i>index/name</i>	Deletes an existing application instance, specified by index or name. The user does generally not use this command.
rename <i>file1 file2</i>	Renames <i>file1</i> to <i>file2</i> .
sendhttp	Sends a SOAP/HTTP messages to the SmartServer's Web server.
servicepin <i>index</i>	Sends a service pin message for the application specified by <i>index</i> . See listapp for supported indexes.
show [<i>all/hwInfo</i>]	This displays configuration information about the SmartServer including the IPv4 and IPv6 network addresses assigned to the SmartServer the MAC address, the hostname, and the subnet mask. Show all displays all parameters. Show hwinfo displays hardware properties.
shutdown	Closes all applications on the SmartServer. A reboot is required to restore operation of all modules.
sntpaddress <i>address</i>	Modifies the address of the SNTP server. If you have a backup SNTP server, you can enter sntpaddress <i>address1 address2</i> to specify the backup server's address. This command accepts both IPv4 and IPv6 addresses.
sntpinterval <i>value</i>	Sets the SNTP update interval in seconds. Set the value to 0 for automatic (adaptive), or to -1 to disable SNTP updates.
sntplog <i>on/off</i>	Enables or disables SNTP logging. The SNTP log file is named sntp.log and is located in the root directory of the SmartServer. The time logged in the SNTP log file is in universal coordinated time (UTC). The maximum size of the SNTP log file is 50 Kbytes. When the file exceeds 50 Kbytes, logging is automatically disabled. Use this command to diagnose time synchronization problems.
staticroute <i>add/delete/show</i>	Use these commands to add, delete or show manual static IP routing entries. This command accepts both IPv4 and IPv6 addresses.
subnetmask <i>address</i>	Modifies the subnet mask. For example, subnetmask 255.255.255.0. This command is valid only when DHCP is turned off.
telnet <i>port</i>	Sets the port the used by the SmartServer for Telnet communication. The default port is 23 .
time <i>hh:mm:ss</i>	Sets the time if the SmartServer is not synched to an SNTP server.
timezone <i>zone</i>	Sets the time zone with the following format: <i>nameOfZone;timeInMinutesFromUTC:dstUsed:daylightStart:daylightEnd</i> where <i>dstUsed</i> is 0 or 1, and daylight savings start/end times are in the form <i>rank.day.month.hour</i> . For example, 1.1.4.2 is the first Sunday in April at 02:00. Rank is a number from 1 to 5 with 5 meaning the last instance in the month. Days are numbered 1 to 7 starting with Sunday. Months are numbered 1 to 12, starting with January.

Command	Description
trace <i>level</i> [<i>stamp</i>]	Sets the tracing level: 0 = None; 1 = Urgent tracing only (default); 2 = Verbose tracing (for debugging only, not recommended). Set the optional <i>stamp</i> parameter to True to enable time stamping.
type <i>file</i>	Types the contents of <i>file</i> .
unconfigapp <i>index/name</i>	Unconfigures the specified application (removes the LonTalk addresses).
update <i>bootrom</i> [<i>file</i>]	Updates the bootrom of the SmartServer. By default, this command will look for the bootrom.upd file in the /root directory of the SmartServer. Run this command from the SmartServer bootrom console. See the following section, <i>Interrupting the Boot Process</i>, for more information.
web <i>port</i>	Sets the port the used by the SmartServer for HTTP communication. The default port is 80 .

Interrupting the Boot Process

The SmartServer undergoes an extensive boot process upon power-up, and when reset by the reset button on the SmartServer hardware or a `reboot` command issued in the console application. During the boot process, the SmartServer's disk structure is automatically checked to ensure that any structural errors on the disk are repaired, and a message is displayed on the screen if any corrections are made to the disk. Additional information about the corrections is written to the event log file. The boot process then loads the SmartServer's system image. Successful completion is indicated when the SmartServer displays its normal command-line prompt.

If the SmartServer repeatedly fails to boot up, you are unable to FTP files to it, or you suspect the image is corrupted, you may interrupt the boot process and troubleshoot the SmartServer. To interrupt and bypass the boot process, press the exclamation point (!) key after the "Press the '!' key to stop auto-boot..." message appears on the console, but before the SmartServer begins loading files. If the auto-boot is interrupted, the boot image is then loaded from ROM, and the SmartServer enters the bootrom state.

The Bootrom State

When the boot process is interrupted or fails (for example if the iLonSystem image is corrupt or not available, perhaps due to a power cycle during image download), the SmartServer loads its system image from ROM and starts a console application similar to that run by the normal iLonSystem image. This state, called the *bootrom state*, is indicated by a command-line prompt prefixed with `[Bootrom]`. If caused by a boot failure, you may need to reload or upgrade the SmartServer software to restore proper operation.

While in the bootrom state, only a subset of the normal console commands are available. The SmartServer provides the minimal functionality required to troubleshoot and recover its system image. The FTP server runs, and the console application provides commands needed to recover the image. However, application commands such as `listapp` and `createapp` are not available and certain attributes are not displayed.

Updating the Bootrom

Echelon may provide updates to the SmartServer bootrom. You can update the bootrom with the console application. The bootrom file that ships with the SmartServer (**bootrom.upd**) is installed in the **LonWorks\iLon100\images\iLon100 4.00** folder on your computer when you install the SmartServer software. Bootrom updates are installed in the **LonWorks\iLon100\images\BootROM 4.xx** folder on your computer, where *xx* represents the sub-version number.

To update the bootrom, follow these steps:

1. Reboot the SmartServer using the console application. When the console reads “Press the `^!` key to stop auto-boot”, press `^!`. The SmartServer will reboot to the bootrom state, halting all applications.
2. Upload via FTP the updated **bootrom.upd** file to the root directory of your SmartServer.
3. Enter the `update bootrom` command in the console application. If the bootrom file name is different than the default (**bootrom.upd**), specify the actual file name as an additional parameter.
4. After the bootrom update has been completed, reboot your SmartServer.

Note: Do not interrupt the bootrom update process. Doing so will render the SmartServer unable to boot. If this happens, you will need to ship your SmartServer back to Echelon to be repaired.

Appendix C

Securing the SmartServer

This appendix describes how to secure folders and files in the SmartServer. This information is provided for example purposes only and is not guaranteed to work in every environment.

Securing the SmartServer Overview

You can secure a folder or individual files in the SmartServer using the **i.LON Web Server Security and Parameters** program. This program is included with the SmartServer software. With the **i.LON Web Server Security and Parameters** program, you can add a *security realm* to a **WebParams.dat** file. A realm defines which folder or file (URL) can be accessed by which users (group) and from which IP addresses (location). For more information on basic authentication, see the following Web site: www.faqs.org/rfcs/rfc2617.HTML.

The SmartServer parses the **WebParams.dat** file upon startup to establish Web page restrictions. The **WebParams.dat** file is stored as plain text with no encryption or password protection. This means that SmartServer's security is protected from inspection by FTP security (user name and password) only. You must use proper user names and passwords for FTP access to prevent the **WebParams.dat** file from being viewed, as described in *Configuring Security Properties* in Chapter 3, *Configuring and Managing the SmartServer*. In addition, you should secure the computer that you are using to create the **WebParams.dat** file.

This appendix does the following:

1. Describes how to update the SmartServer's default security settings using the **i.LON Web Server Security and Parameters** program.
2. Lists the key folders and files in the SmartServer and explains how they should be secured.
3. Provides the formats of the realms that you can add to the **WebParams.dat** file for securing folders and files.
4. Demonstrates how to secure SmartServer Web pages based on the number of user groups, the level of security (minimal to complete password protection), and the types of pages being accessed (system or custom).

Note: You may need to add a realm for any file in a shared folder that needs to be secured. Securing User Accounts

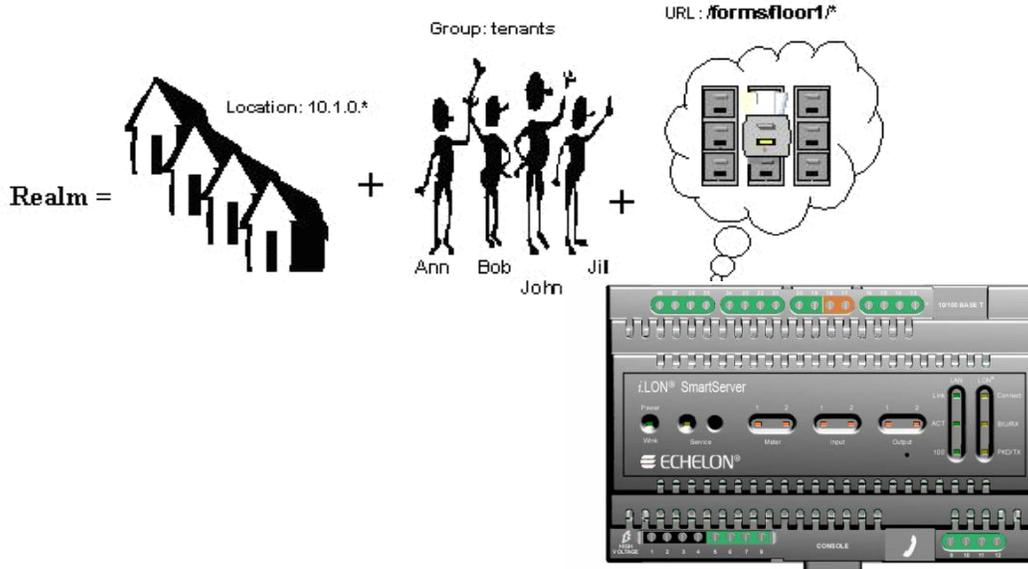
Updating SmartServer Security Settings

The SmartServer's factory default **WebParams.dat** file allows access to all files under the **root/Webfolder** on the SmartServer flash disk from any location by any user. To update the SmartServer's security settings, follow these steps:

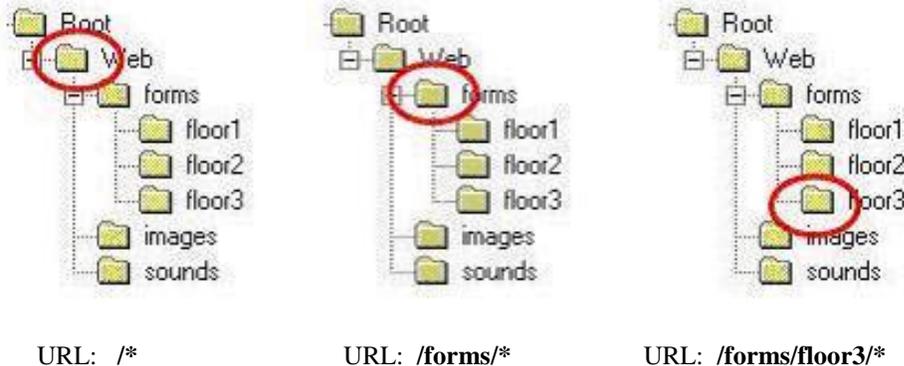
1. Download via FTP the existing **WebParams.dat** file from the root directory on the SmartServer flash disk to your computer.
2. Start the i.LON Web Server Parameter utility. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer Software**, and then select **SmartServer Web Server Security and Parameters**.
3. Open the **WebParams.dat** file. To do this, click **File**, click **Open**, and then browse to and select the **WebParams.dat** file that you saved to your computer in step 1.
4. Update the **WebParams.dat** file. See the next section in this appendix, *Setting Access Restrictions*, for how to do this.
5. Save the updated **WebParams.dat** file. To do this, click **File** and then click **Save**.
6. Upload via FTP the updated **WebParams.dat** file to the root directory on the SmartServer flash disk.
7. Reboot the SmartServer to implement the new security settings.

Setting Access Restrictions

Security realms are used to define the SmartServer's security access restrictions. A *realm* consists of a URL (folder in SmartServer), group (users group name), and location (IP address range from where the URL may be accessed).



URLs are defined with the assumption that you are starting from the root directory of the Web site, and not the SmartServer. For example, to restrict access to <http://building10/forms/floor3/> the URL must be defined as `"/forms/floor3/*"`. The wildcard is required in order to place this setting across the entire directory. To restrict access to the whole site you need to use the URL `"/*"`. The following figure shows examples of URLs (note that the leading `"/` is required syntax).



}
Users and Groups

Individuals who can access the SmartServer with a user name and password are called users. Users are organized into groups. Each group must contain one or more users, and all users in a given group will have identical access. A group can contain a maximum of 16 users. This limit is not enforced by the Web Server Parameter utility. If you add more than 16 users to a group, the SmartServer will ignore all users after the 16th. If each user must have different access rights, you must define a group for each user.

In order to create a group, you must first define a list of users and passwords. For example:

Ann : boxcar
Bob : trumpet
John : foxtrot
Jill : mustang
superuser : sfs43fs6f

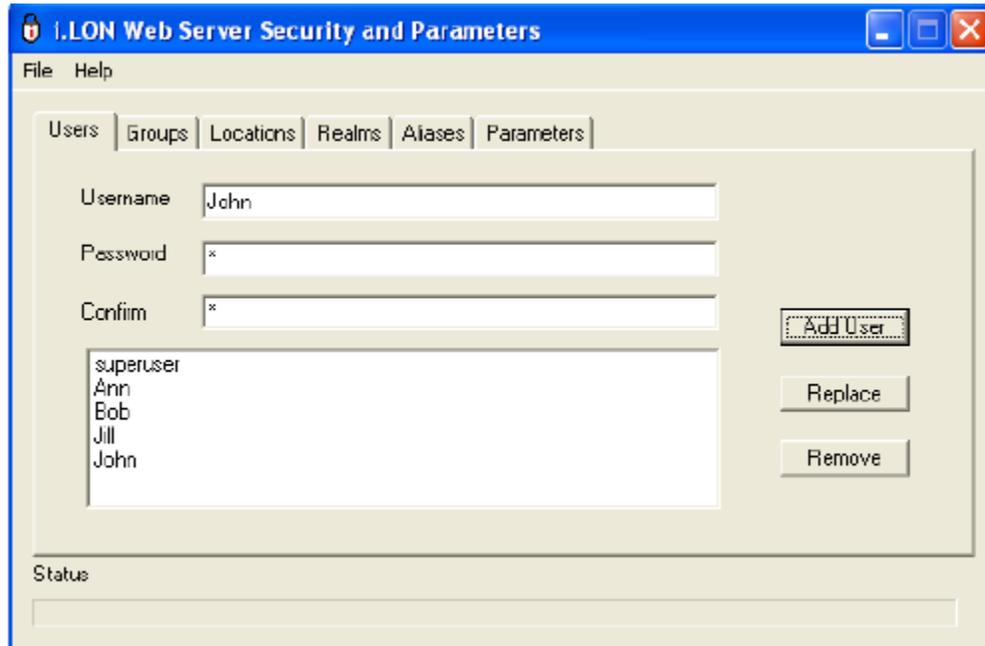
Users should be grouped together based on the Web folders on the SmartServer that they are going to access. For example, if Ann, Bob, Jill and John live in the same building, you could group them by floor. Ann, Bob, and Jill have apartments on the second floor, Bob also happens to have a workshop on the first floor. Finally, John has an apartment on the third floor. The property management company maintains the Web site. Their Web master has the access name **superuser**. The following table shows which users are to have access to which folders:

	floor 1	floor2	floor3
Ann		X	
Bob	X	X	
Jill		X	
John			X
Superuser	X	X	X

The SmartServer security mechanism allows each user to be a member of one group only. As a result, you need to create four groups: one for access to floor 1 and floor 2 for Bob, one for access to floor 2 for Ann and Jill, one for access to floor 3 for John, and for access to all floors for superuser.

To set up the users and groups described above, follow these steps:

1. In the **Users** tab, enter a user name in the **Username** box, enter the password to be used by the user in the **Password** and **Confirm Password** boxes, and then click **Add User**.



2. Click the **Groups** tab to create the necessary groups. To create a group, enter a group name in the **Group Name** box and then click **Add Group**.

3. Add users to specific groups. To do this, click the group under the **Groups** column to which users are to be added, click a user, and then click **Add User**. Repeat this step for each user to be added to the group.



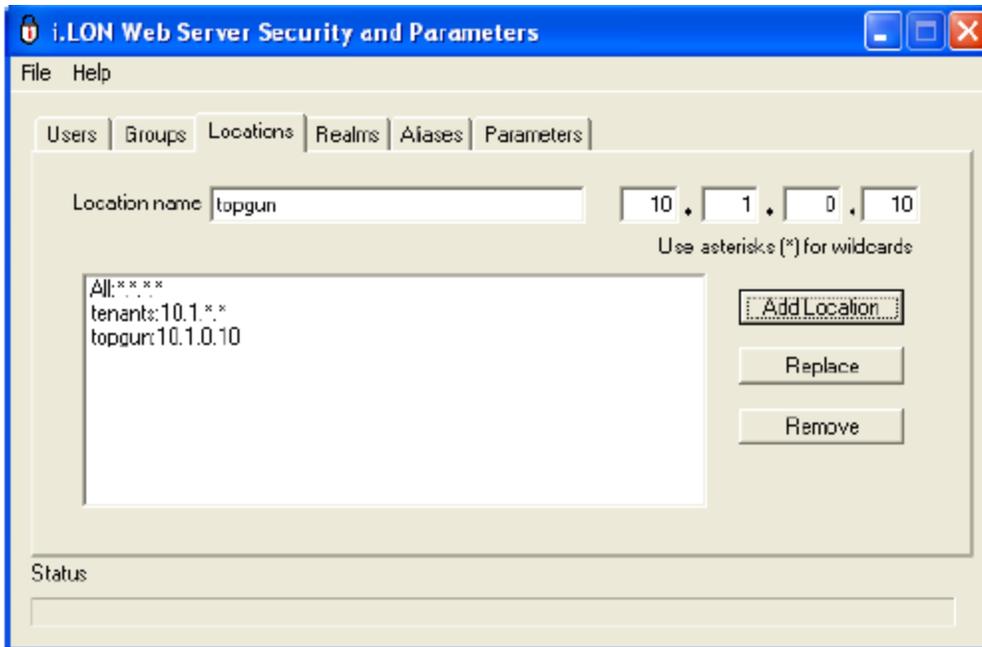
Note: If you create 16 or more groups of users, you may need to change some of the parameters as described in the *Parameters* section later in this appendix.

Locations

Locations are defined as ranges of IP addresses from which a particular group of users can access a particular folder. “*” is used as a wildcard. To create a location, follow these steps:

The following table lists some example location settings.

Location Name	IP Address Range	Comments
All	*.*.*.*	Any IP address
Tenants	10.1.0.*	Any host with IP in the range 10.1.0.1 – 10.1.0.254 Note: 10.1.0.0 is a network address and 10.1.0.255 is a broadcast address; therefore, they are not included
Topgun	10.1.0.10	IP address of the host used by superuser (property manager) to update Web pages



Note: If you declare a location “A” that happens to be a subset of another location “B,” it is assumed that “A” is not included in the access rights of users in location “B.” For example:

```
topgun: 10.1.0.10
tenants: 10.1.*.*
all: *.*.*.*
```

This declaration means that tenants is the whole range 10.1.*.* with the exception of 10.1.0.10. Similarly, all excludes 10.1.*.*.

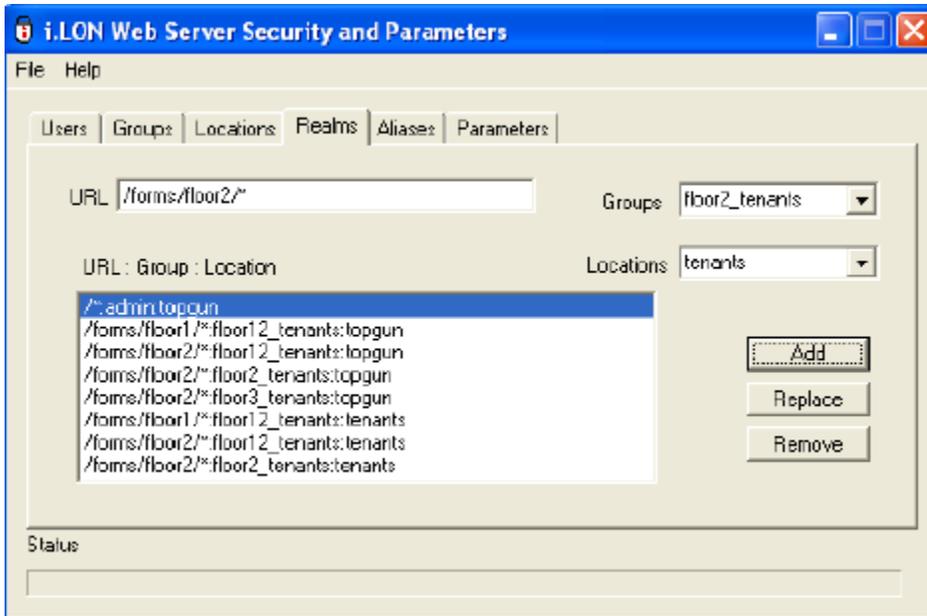
Realms

Realms define the folders the various groups and locations are allowed to access. Each realm is defined using the format URL:GROUP:LOCATION, where users from the specified GROUP and LOCATION are given access to the specified URL. To create a realm follow these steps:

1. In the **URL** box, Enter the path of the folder on the SmartServer flash disk containing the Web pages to be protected. This path is relative to the root/Web folder on the SmartServer flash disk.
2. Select the group to have access to the URL specified in step 1 from the **Group** list and then click **Add Group**.
3. Select the location that must be used to access the URL specified in step 1 from the **Location** list and then click **Add Location**.

For example, consider a SmartServer Web site that allows users to monitor occupancy information, temperature, and light level on the floor on which they live within a three-story building. Floors 1, 2, and 3 have corresponding Web pages stored in folders under **/forms: /forms/floor1, /forms/floor2, and /forms/floor3**. There are five users that can access this site: superuser, Ann, Bob, Jill, and John. They belong to the following groups: tenants_floor12, tenants_floor2, tenants_floor3, and admin as described above.

Tenants are allowed to access Web pages of their floor only, but can login from any local host. Local hosts may have any IP address in the network 10.1.0.0 / 254 (for example, 10.1.0.1–10.1.0.254). There is one “superuser” that designs Web pages, and has unlimited access to the Web site. For security purposes, “superuser” accesses the site from one host only using IP address 10.1.0.10. The Web site should be restricted to all other users.



Aliases

Aliases allow redirecting URLs to other URLs in the web server directory structure. You can use aliases to create cross-references, or to define realms for Web page security. The syntax for an alias is: URL:Path. The following example redirects a request made with the URL element **/forms/DIRA/Nvpage.HTML** and converts it to **/secureforms/Nvpage.htm** redirects all URLs ending in a slash to the index.htm file in the same path. By default, the ***/*/index.htm** alias is defined implicitly (i.e. it will not appear in the URL : Path field). This alias redirects all URLs ending in a slash to the index.htm file in the same path. The following example redirects a request made with the URL element **/forms/DIRA/Nvpage.HTML** and converts it to **/secureforms/Nvpage.html**
/forms/DIRA/*:/secureforms/*

Tip: Use the asterisk (*) as a wildcard in both the URL string and alias string. It must occur only once in the URL string and once in the alias string.

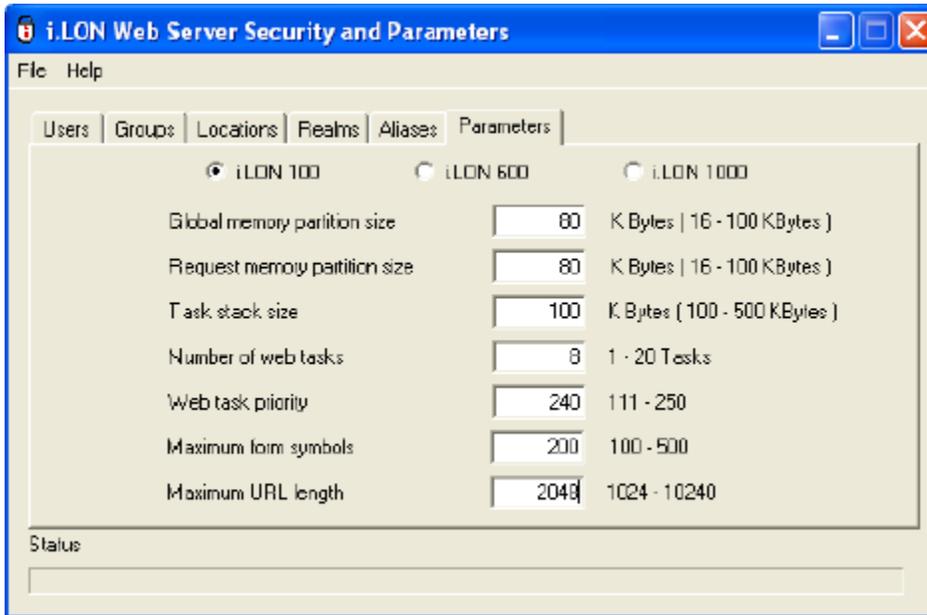
To create an alias:

1. Click the **Aliases** tab.
2. In **URL**, enter the URL that identifies the path to the Web pages for which you wish to define an alias.
3. In **Path**, enter the path to which you wish to redirect.
4. Click **Add**.
5. Your new alias definition appears in the window.

Parameters

You can set the Web server parameters for memory partitions and task management using the **Parameters** tab. These parameters govern the behavior of the Web server. Typically, you will not change any of the values in the **Parameters** tab; however, if you create 16 or more groups of users and you have trouble accessing the SmartServer, click the **Parameters** tab and then make the following changes to the listed properties:

Global memory partition size	80 KB
Request memory partition size	80 KB
Maximum form symbols	200
Maximum URL length	2,048



Sample WebParams.dat file

The following **WebParams.dat** file was generated according to the scenario described previously.

```
iLonSecurity 1.2
GlobalMemoryBytes:16384
RequestMemoryBytes:16384
TaskStackBytes:10240
NumTasks:1
TaskPriority:240
MaxSymbols:100
(Users)
admin:superuser:sfs43fs6t
floor12_tenants:Bob:trumpet
floor2_tenants:Ann:boxcar
floor2_tenants:Jill:mustang
floor3_tenants:John:foxtrot
(Locations)
all:*.***.*
tenants:10.1.*.*
topgun:10.1.0.10
(Realms)
/*:admin:topgun
/forms/floor1/*:floor12_tenants:topgun
/forms/floor2/*:floor12_tenants:topgun
/forms/floor2/*:floor2_tenants:topgun
/forms/floor3/*:floor3_tenants:topgun
/forms/floor1/*:floor12_tenants:tenants
/forms/floor2/*:floor12_tenants:tenants
/forms/floor2/*:floor2_tenants:tenants
/forms/floor3/*:floor3_tenants:tenants
```

Securing Folders and Files

You can secure a folder or individual files in the SmartServer. This section does the following:

1. Lists the key folders in the SmartServer, explains how they should be secured, and provides the formats of the realms that you can add to the **WebParams.dat** file to secure them.
2. Provides the formats of the realms that you can add to the **WebParams.dat** file to secure individual files.

Securing Folders

/user

The **/user** folder includes the directories that hold custom Web pages, factory *i.LON Vision* Web pages and framesets, and web pages that do not contain web tags. If you have a single user group (for example, “all”), you can secure the entire **/user** folder by creating a realm with the following format:
`/user/*:all:everywhere`

/user/Echelon

The **/user/Echelon** folder contains the factory *i.LON Vision* Web pages and framesets. Some of the HTML files in this folder are also used for custom framesets.

- If you password protect the entire **/user/Echelon** folder, you must add a realm for each HTML file used in your custom framesets and web pages.
- If you have multiple user groups, do not secure the entire **/user/Echelon** folder. This is because all custom framesets use specific HTML files in this folder. Instead, you can secure the **/user/Echelon/Menu.html** file and then secure all custom Web page folders using the following format:

```
/user/Echelon/Menu.html:all:everywhere
```

See *Securing Files* for more information about the **/user/Echelon/Menu.html** file.

/user/<customWebPages>

The **/user/<customWebPages>** folder contains the user-created folders that hold the user *i.LON Vision* framesets. If you secure the entire **/user/Echelon** folder, you will have to add a realm entry for any factory HTML files, such as **ViewEventScheduler.html**, that are used by the custom Web pages or framesets.

To secure a custom Web page folder, create a realm using the following format:

```
</dir path>/*:<group>:<location>
```

The following example displays a realm created for a custom Web page folder:

```
/user/user1/*:all:everywhere
```

/WSDL

The **/WSDL** folder contains WSDL files, which are used by SOAP clients accessing the SmartServer. If you secure the WSDL files, all SOAP clients need a user name and password to access the SmartServer.

Securing the **/WSDL** folder, affects the following Web pages and applications:

- All Web pages, including those that have functions using SOAP calls. This folder does not contain Web Tags or *i.LON Vision* objects.
- Client programs, such as .NET applications, that use SOAP to access the SmartServer.
- Web connections.

If you secure this folder, add a new realm with the URL of the folder for each user group. For SOAP applications, create a new user group for SOAP applications such as “soapuser”. The following **WebParams.dat** file demonstrates the recommended settings for securing the **/WSDL** folder.

```
(Users)
  all:ilon:ilon
  soapuser:soap:soap
  supervisor:super:super
  supervisor:super1:super
  enduser:Tom:cat
  enduser:Steve:dog
  enduser2:Jack:mouse
  enduser2:Dave:rat
(Locations)
  everywhere:*. *.*.*.*
(Realms)
  /WSDL/*:soapuser:everywhere
  /WSDL/*:all:everywhere
  /WSDL/*:supervisor:everywhere
  /WSDL/*:enduser:everywhere
  /WSDL/*:enduser2:everywhere
```

Securing Files

You can protect a file in the SmartServer by creating a realm using the following format:

```
/<dir path>/<file name>:<group>:<location>
```

Note: For *.gz files in the **/user/Echelon** folder, do not include the .gz extension in the file name. The .gz extension is used for compressed files. For example, to secure the **View Event Scheduler.html.gz** file, create a realm using the following format:

```
/user/Echelon/ViewEventScheduler.html:all:everywhere
```

/user/Echelon/Menu.html file

You can automatically secure all the files in the **user/Echelon** folder by securing the **/user/Echelon/Menu.html** file. The protected files can still be accessed by your custom Web pages.

If you secure only the **/user/Echelon/Menu.html** file in the **/Echelon** folder, Web page security will still function when you access other files in the **/Echelon** folder through a factory or custom frameset.

Note: If you directly access a file in the **user/Echelon** folder using its URL, the web page may appear briefly before the **Login-in** dialog is displayed. The information momentarily displayed on the Web page (the port numbers for the Web server and Telnet) is statically added to the HTML page and is not dynamically retrieved from the SmartServer; therefore, no security risk exists.

To prevent Web pages from being displayed prior to the **Login-in** dialog, you have to secure all the files in the **user/Echelon** folder; therefore, secure only the **/user/Echelon/Menu.html** file.

Examples for Securing a SmartServer

This section demonstrates how to secure SmartServer Web pages based on the number of user groups, the level of security (minimal to complete password protection), and the types of pages being accessed (system or custom). Example **WebParams.dat** files based on the scenario are then provided.

The example **WebParams.dat** files are based on a Web site consisting of the SmartServer home page, which is not secured, and the system frameset (access through a button on the SmartServer home page). A **menu.htm** file is used for the system frameset. These examples are for i.LON Vision Web pages only.

Tip: Examples 2 and 7 illustrate the most common scenarios for single and multiple user groups,

respectively. The **WebParams.dat** files included in these examples provide the recommended solutions for these scenarios.

Example 1

Users: Single user group (or multiple user groups with only the system web pages secured).

Security Level: Minimal password protection.

Types of Pages Accessed: Factory Web pages only (no custom web pages).

WebParams.dat file:

```
(Users)
all:ilon:ilon
(Locations)
everywhere:*. *.*.*
(Realms)
/user/Echelon/Menu.html:all:everywhere
(Aliases)
```

Note: This is the **factory default** setting. It provides Login security to all factory Web pages.

Example 2 (recommended for single user group)

Users: Single user group.

Security Level: Complete password protection.

Types of Pages Accessed: Factory and custom Web pages.

WebParams.dat file:

```
(Users)
all:ilon:ilon
(Locations)
everywhere:*. *.*.*
(Realms)
/WSDL/*:all:everywhere
/user/*:all:everywhere
(Aliases)
```

Note: If you are using SOAP applications or the Web Binding feature, provide a user name and password for these features to work and create a separate user group and realm for SOAP users. The **WebParams.dat** file would then appear as follows:

```
(Users)
all:ilon:ilon
soapuser:ilon1:ilon
(Locations)
everywhere:*. *.*.*
(Realms)
/WSDL/*:all:everywhere
/WSDL/*:soapuser:everywhere
/user/*:all:everywhere
(Aliases)
```

Example 3

Users: Two user groups (“all” and “enduser”).

Security Level: Factory system Web pages secured only.

Types of Pages Accessed: Factory Web pages though the frameset (not accessed directly). SOAP applications and Web connections can access the SmartServer without password protection. See example 4 for how to implement full password protection for this scenario.

WebParams.dat file:

```

(Users)
all:ilon:ilon
enduser:Tom:user
enduser:Steve:user
(Locations)
everywhere:*. *.*.*
(Realms)
/user/tools/*:all:everywhere
/user/Echelon/Menu.html:all:everywhere
(Aliases)

```

Example 4

Users: Two user groups (“all” and “enduser”).

Security Level: Complete password protection.

Types of Pages Accessed: “all” user group can access all Web pages; “enduser” group can only access custom Web pages.

WebParams.dat file:

```

(Users)
all:ilon:ilon
soapuser:soap:soap
enduser:Tom:user
enduser:Steve:user
(Locations)
everywhere:*. *.*.*
(Realms)
/WSDL/*:all:everywhere
/WSDL/*:soapuser:everywhere
/WSDL/*:enduser:everywhere
/user/tools/*:all:everywhere
/user/Echelon/Menu.html:all:everywhere
/user/user1/*:all:everywhere
/user/user1/*:enduser:everywhere
(Aliases)

```

Example 5

Users: Two user groups (“all” and “enduser”).

Security Level: All Web pages secured, but some system Web pages can be accessed by “enduser” group.

Types of Pages Accessed: “all” user group can access all Web pages; “enduser” group can access custom Web pages and some system Web pages (such as Event Scheduler).

WebParams.dat file:

```

(Users)
all:ilon:ilon
soapuser:soap:soap
enduser:Tom:user
enduser:Steve:user
(Locations)
everywhere:*. *.*.*
(Realms)
/WSDL/*:all:everywhere
/WSDL/*:soapuser:everywhere
/WSDL/*:enduser:everywhere
/user/tools/*:all:everywhere
/user/Echelon/Menu.html:all:everywhere
/user/Echelon/ViewEventScheduler.html:all:everywhere

```

```

/user/Echelon/ViewEventScheduler.html: enduser:everywhere
/user/user1/*:all:everywhere
/user/user1/*:enduser:everywhere
(Aliases)

```

Example 6

Users: Three user groups (“all”, “enduser”, and “enduser2”).

Security Level: User groups have varying access to Web pages in a single custom frameset.

Types of Pages Accessed: “all” user group can access all Web pages; “enduser” group can access custom Web pages except **room2.htm**; and “enduser2” group can access custom Web pages except **room1.htm**.

You can secure the SmartServer in two ways in this scenario:

- Store all files in a custom Web folder. In this custom Web folder, store common files in one subdirectory, and store files to be accessed by specific user groups in separate subdirectories.
- Store all common files in a custom Web folder, and create separate subdirectories in the **/user** folder for each set of files to be accessed by specific user groups. This is the recommended solution.

The partial **WebParams.dat** for the second solution is provided. The **/user1** folder contains the frameset and common custom web page files. The **/enduserDir/** and **/enduser2Dir** folders contain the files accessible by individual user groups.

```

(Users)
all:ilon:ilon
soapuser:soap:soap
supervisor:super:super
supervisor:super1:super
enduser:Tom:user
enduser:Steve:user
enduser2:Ed:money
enduser2:Tyler:monk
(Locations)
everywhere:*. *.*.*.*
(Realms)
/WSDL/*:all:everywhere
/WSDL/*:soapuser:everywhere
/WSDL/*:supervisor:everywhere
/WSDL/*:enduser:everywhere
/WSDL/*:enduser2:everywhere
/user/tools/*:all:everywhere
/user/Echelon/Menu.html:all:everywhere
/user/user1/*:all:everywhere
/user/user1/*:nduser:everywhere
/user/user1/*:enduser2:everywhere
/user/enduserDir/*:all:everywhere
/user/enduserDir/*:supervisor:everywhere
/user/enduserDir/*:enduser:everywhere
/user/enduser2Dir/*:all:everywhere
/user/enduser2Dir/*:supervisor:everywhere
/user/enduser2Dir/*:enduser2:everywhere
(Aliases)

```

Example 7 (recommended for multiple user groups)

Users: Five user groups (“all”, “supervisor”, “enduser”, “enduser2”, and “soapuser”).

Security Level: User groups have varying access to Web pages.

Types of Pages Accessed: “all” user group can access all Web pages and framesets; “supervisor” group can access all custom Web pages and some system Web pages; and “enduser” and “enduser2” groups can access most custom web pages. The “soapuser” group is used by non-Web page applications such as Web binding and client SOAP applications (for example, VC# programs). Figures 1 and 2 illustrate the Web page and directory layouts, respectively, in this scenario. The “soapuser” user group is not shown in the figures.

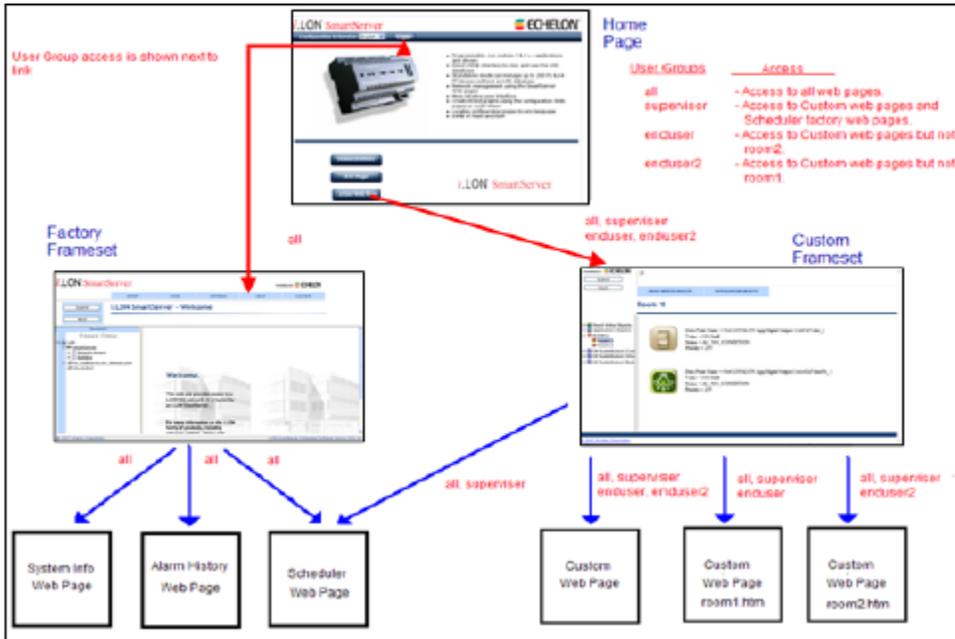


Figure 1—Web Page Layout



Figure 2—Directory Layout

WebParams.dat file:

```
iLonSecurity 1.3 100
GlobalMemoryBytes:16384
RequestMemoryBytes:16384
```

```

TaskStackBytes:204800
NumTasks:5
TaskPriority:240
MaxSymbols:100
MaxUrlSize:1024
(Users)
all:ilon:ilon
soapuser:soap:soap
supervisor:super:super
supervisor:super1:super1
enduser:Tom:user
enduser:Steve:user
enduser2:Jack:user
enduser2:John:user
(Locations)
everywhere:*. *.*.*
(Realms)
/WSDL/*:soapuser:everywhere
/WSDL/*:all:everywhere
/WSDL/*:supervisor:everywhere
/WSDL/*:enduser:everywhere
/WSDL/*:enduser2:everywhere
/user/Tools/*:all:everywhere
/user/Echelon/Menu.html:all:everywhere
/user/user1/*:all:everywhere
/user/user1/*:supervisor:everywhere
/user/user1/*:enduser:everywhere
/user/user1/*:enduser2:everywhere
/user/enduserDir/*:all:everywhere
/user/enduserDir/*:supervisor:everywhere
/user/enduserDir/*:enduser:everywhere
/user/enduser2Dir/*:all:everywhere
/user/enduser2Dir/*:supervisor:everywhere
/user/enduser2Dir/*:enduser2:everywhere
(Aliases)

```

Figures 3–9 show how to use the **iLON Web Server Security and Parameters** program to create the above **WebParams.dat** file used for this scenario.



Figure 3—Setup for “all” user group

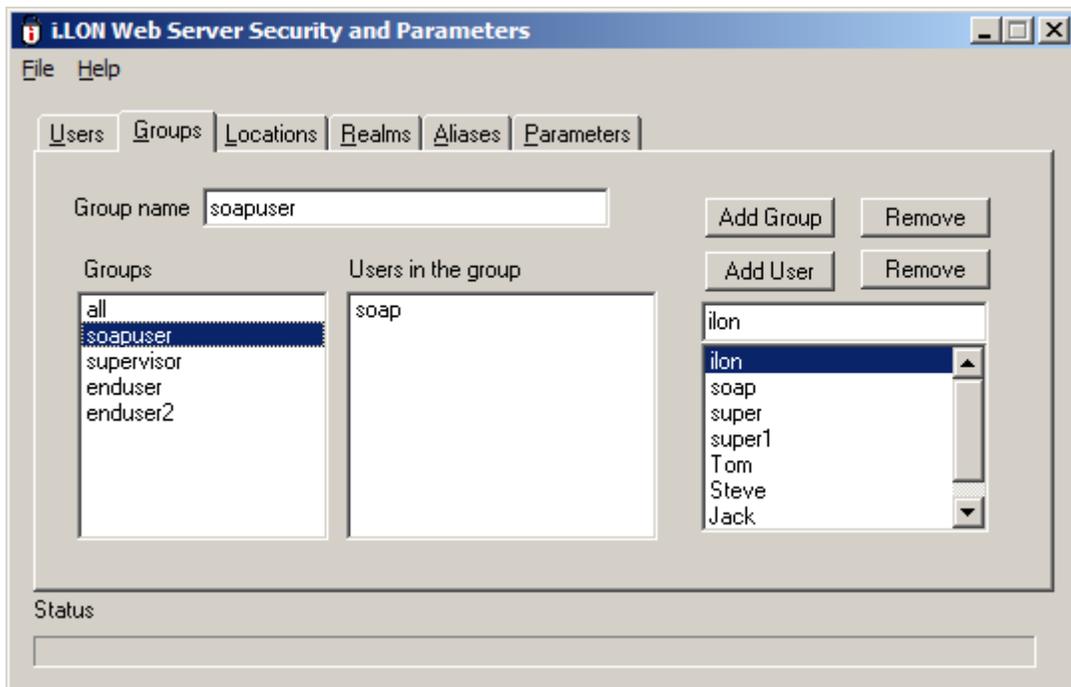


Figure 4— Setup for “soapuser” user group

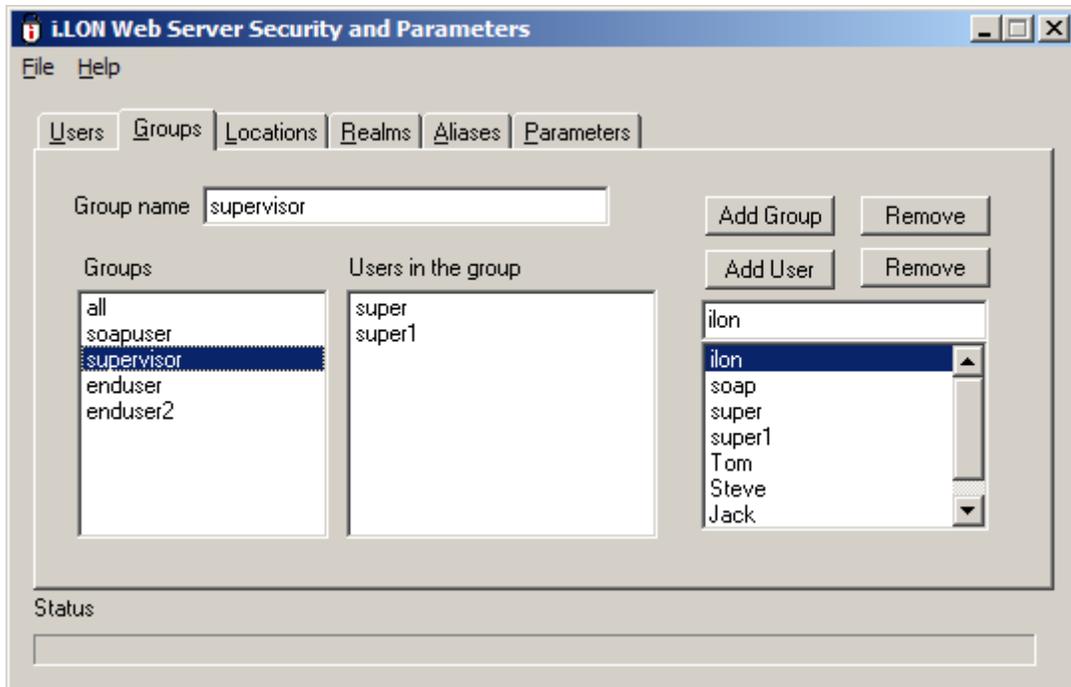


Figure 5—Setup for “supervisor” user group

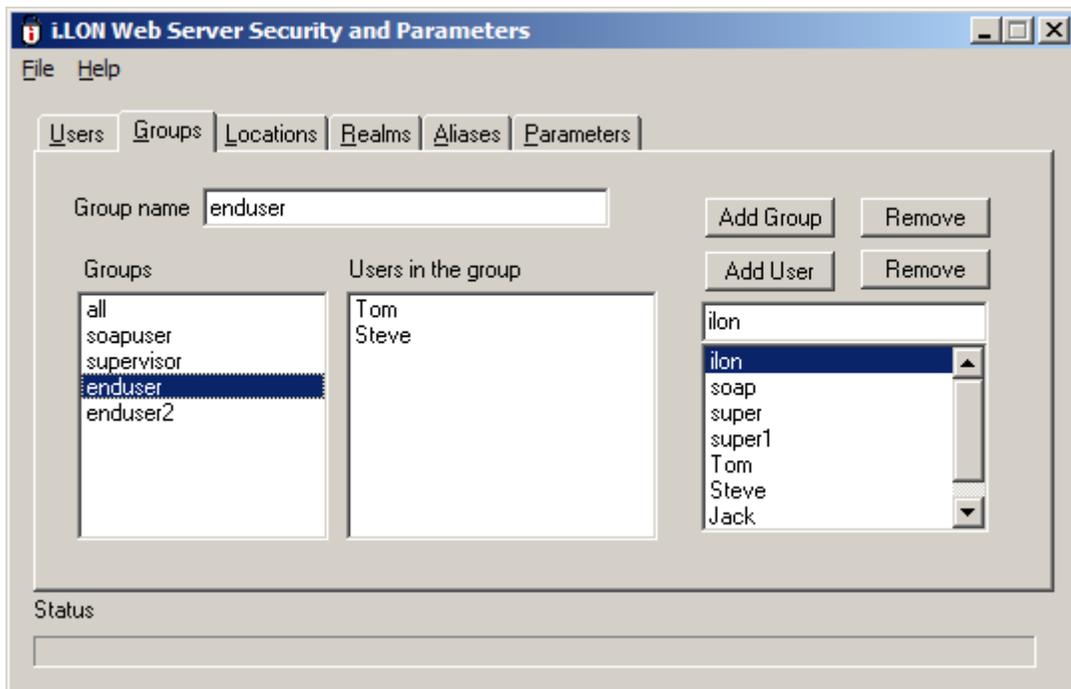


Figure 6— Setup for “enduser” user group

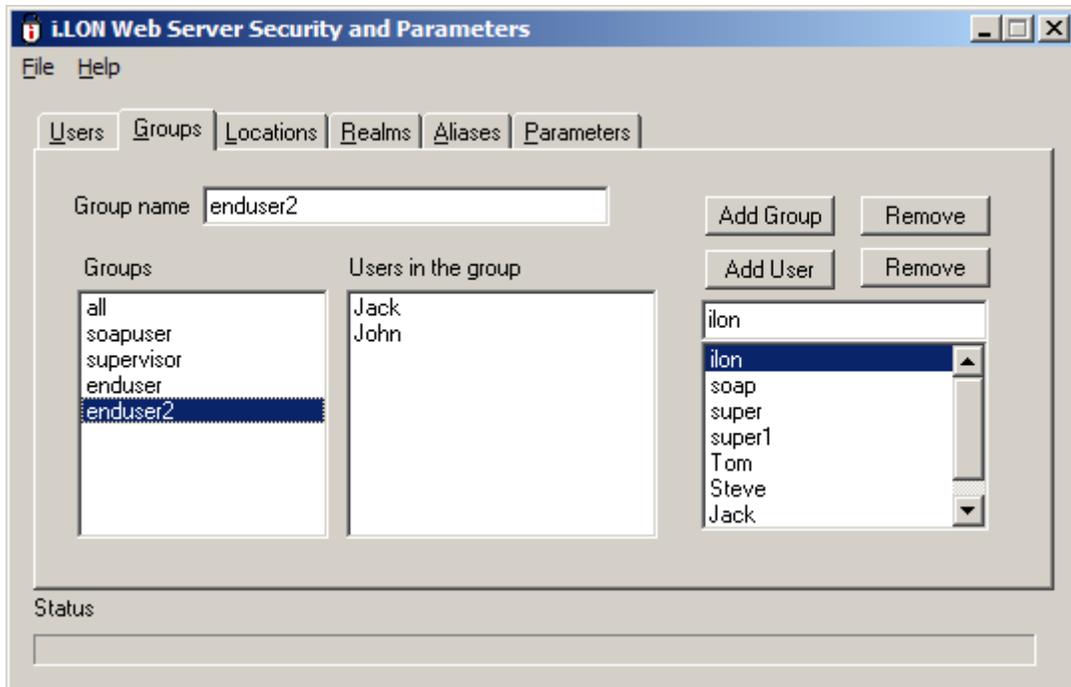


Figure 7— Setup for “enduser2” user group

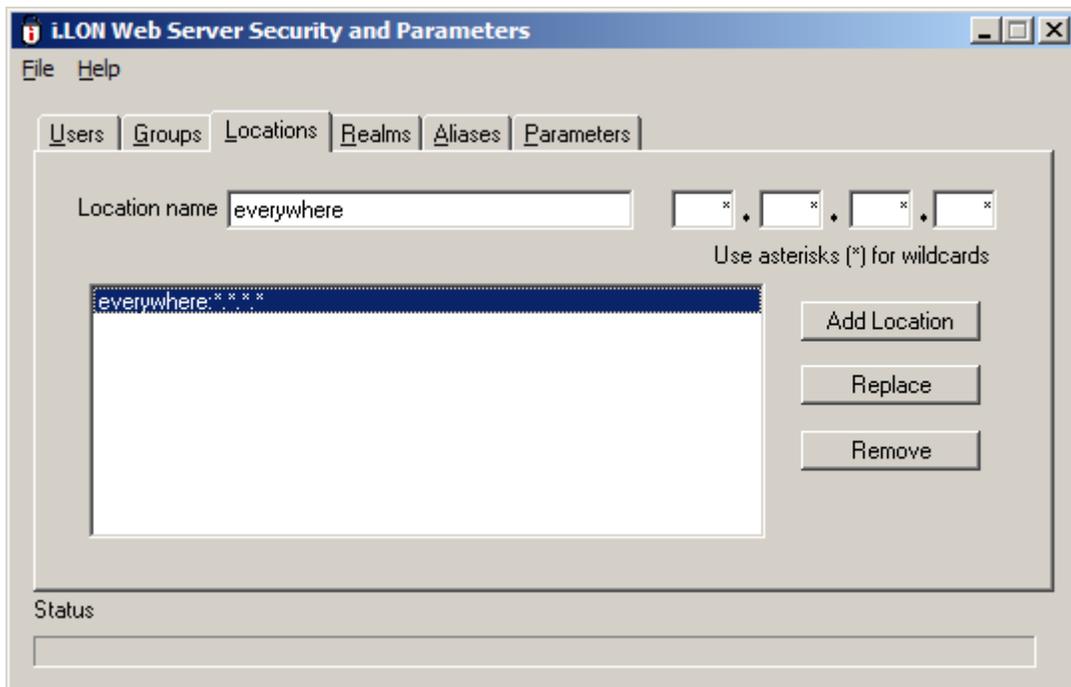


Figure 8—Setup for “everywhere” location

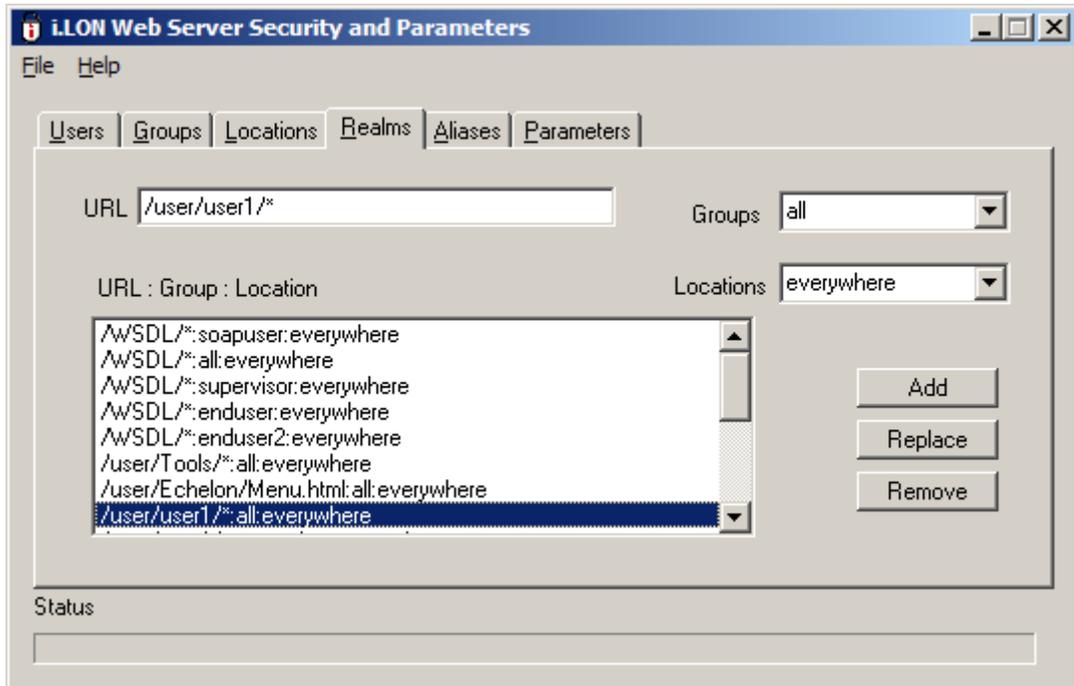


Figure 9a—Setup for realms

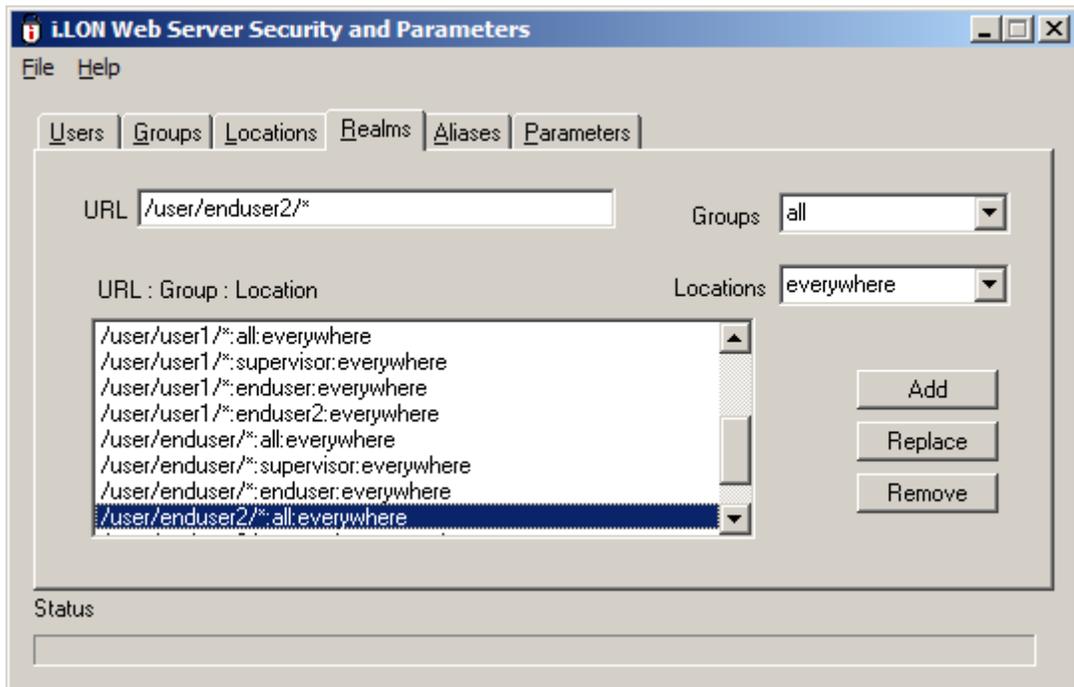


Figure 9b— Setup for realms

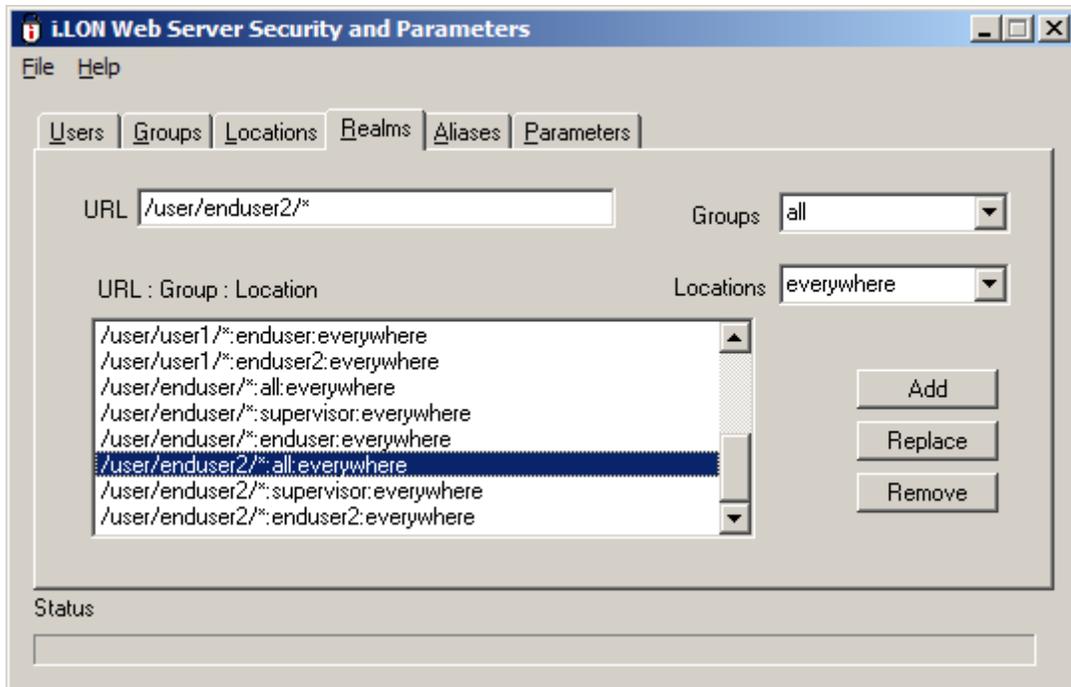


Figure 9c— Setup for realms

Appendix D

Manually Managing and Deploying SmartServers

This appendix describes how to manually upgrade, backup/restore, and deploy SmartServers via FTP instead of using the i.LON AdminServer.

Introduction

You can manually upgrade, backup/restore, and deploy SmartServers via FTP instead of using the i.LON AdminServer. You may need to manually manage your SmartServer if you have previously downgraded it to the i.LON 100 e3 version, as the i.LON AdminServer can only be used on SmartServers running the Release 4.0 firmware or newer. The following sections describe how to manually perform the following tasks:

1. Backup the SmartServer firmware.
2. Upgrade the SmartServer firmware.
3. Restore the SmartServer firmware.
4. Copying device templates to a SmartServer.
5. Deploy a pre-configured SmartServer in a single network.
6. Deploy pre-configured SmartServers in multiple networks.
7. Deploy a network configuration on multiple SmartServers.

Manually Backing Up the SmartServer Firmware

You can manually back up the SmartServer firmware via FTP. Regularly back up your SmartServer to protect your network configuration and your custom SmartServer Web pages. To create a backup of your SmartServer, follow these steps:

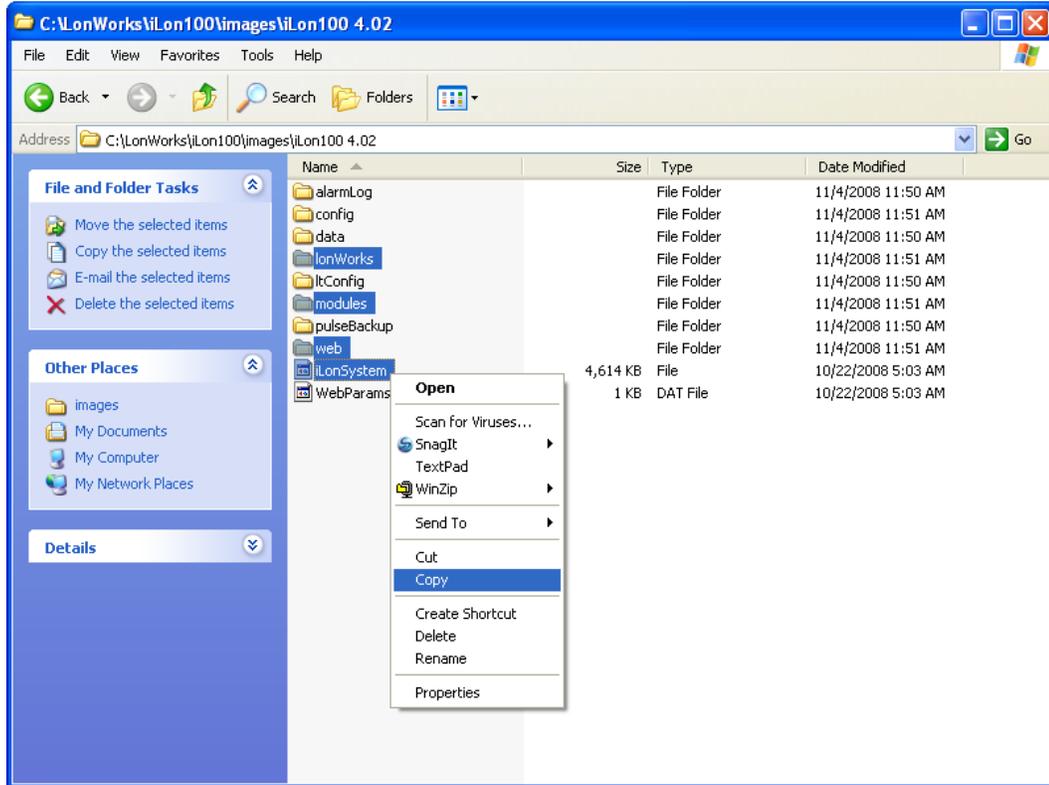
1. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the local SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click Security. The **Setup – Security** Web page opens.
 - b. In the **General** property, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - c. In the **Service** property, verify that the **Enable FTP** check box is selected.
2. In the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example).
3. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
4. Copy all the folders in the root directory to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions.

Manually Upgrading the SmartServer Firmware

You can manually upgrade the firmware on your SmartServer via FTP as service packs are made available for the SmartServer. To upgrade the firmware on your SmartServer to the latest version, follow these steps (you can use these steps to upgrade SmartServers running the Release 4, 4.01, or 4.02 firmware to the Release 4.06 firmware):

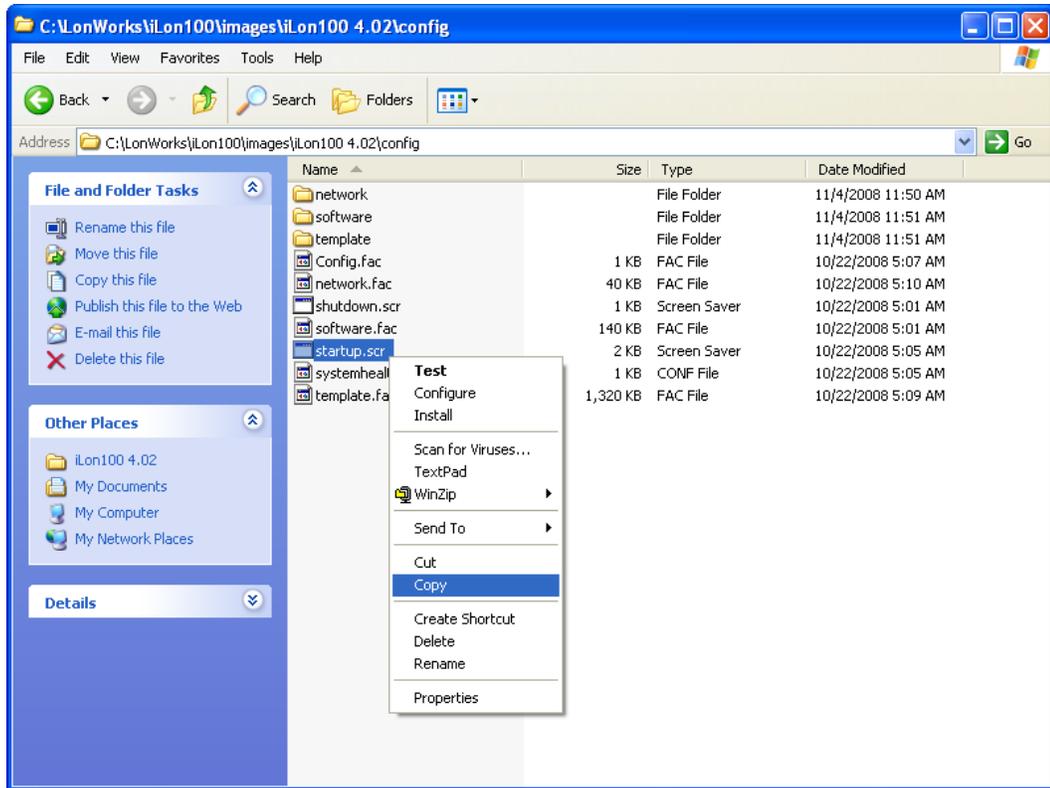
1. Back up the SmartServer firmware via FTP following the steps described in the previous section, *Manually Backing Up the SmartServer Firmware*.
2. Verify that you have installed the latest SmartServer firmware to the LonWorks\iLon100\images folder on your computer. See *Installing Echelon SmartServer 2.2 Software* in Chapter 2 for more information.
3. Open the SmartServer images folder. To do this, click **Start**, point to **Programs**, point to **Echelon SmartServer Software**, and the select **SmartServer Images Folder**. Alternatively, you can browse to the file path of the SmartServer image folder, which is **LonWorks\iLon100\images\iLon100 4.<xx>** by default, where *xx* represents the current SmartServer image.

- Copy the following folders and files in the **LonWorks\iLon100\images\iLon100 4.<xx>** folder on your computer to the root directory of the SmartServer flash disk: **lonWorks**, **modules**, **web**, and **iLonSystem**.



Note: Do not copy the **config** folder or the **WebParams.dat** file in the **LonWorks\iLon100\images\iLon100 4.<xx>** directory to your SmartServer. This prevents the following:

- Deletion of network configuration data if you did not change the name of the network from the default **Net**.
 - Duplication of network configuration data if you are running the SmartServer in Standalone mode.
 - Overwriting the **/config/systemhealth.conf** file, which determines how the SmartServer's system health is monitored.
 - Overwriting the **/config/software/lspa.xml** file, which contains the current LonScanner Protocol Analyzer settings that you may have specified in the **Setup – Security** Web page.
 - Overwriting any pre-defined type translator rule XML files in the **/config/software/translatorRules** folder that you may have modified
 - Overwriting any pre-defined template XML files in the **/config/template** folder that you may have modified.
 - Overwriting any Web page restrictions you may have created with the **i.LON Web Server Security and Parameters** program.
- Copy the **startup.scr** file in the **LonWorks\iLon100\images\iLon100 4.<xx>\config** folder on your computer to the **/config** directory of the SmartServer flash disk.



6. Copy the following files from the backup to the SmartServer flask disk, if necessary:
 - **web/index.htm** (if you modified the SmartServer home page or added a link to your custom SmartServer Web pages to it; see *Chapter 12* for more information).
 - **web/images/[app/ || tree/]<image>.gif** (if you wrote over any of the SmartServer’s built-in images, which is not supported).
7. Reboot your SmartServer using the SmartServer Web pages or the SmartServer console application.
 - To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.
 - To reboot your SmartServer using the SmartServer console application, enter the **reboot** command. For more information on using the SmartServer console application, see *Appendix B*.

Manually Restoring the SmartServer Firmware

You can manually restore the configuration of a SmartServer from a backup following these steps:

1. Verify that you have the correct user name and password to access your SmartServer via FTP and that FTP access is enabled on your SmartServer. To do this, follow these steps:
 - a. Right-click the local SmartServer icon, point to **Setup**, and then click **Security** on the shortcut menu. Alternatively, you can click **Setup** and then click **Security**. The **Setup – Security** Web page opens.
 - b. In the **General** box, verify that the **FTP/Telnet User Name** and **FTP/Telnet Password** properties are correct.
 - c. In the **Service** box, verify that the **Enable FTP** check box is selected.

2. Format the SmartServer flash disk using the bootrom console. To do this, follow these steps:
 - a. Enter the **reboot** command in the SmartServer console application.
 - b. When the console reads “**Press the ‘!’ key to stop auto-boot**”, press ‘!’. The SmartServer will enter the bootrom state, halting all applications.
 - c. Enter the **format** command in the bootrom application.
- See Appendix B, *Using the SmartServer Console Application*, for more information on using the bootrom and console applications.
3. After the SmartServer has rebooted, enter the FTP URL of your SmartServer (ftp://192.168.1.222, for example) in the browser of an FTP client such as Core FPT, WS FTP Pro, and Cute FTP.
 4. Enter the FTP/Telnet user name and password for accessing your SmartServer via FTP.
 5. Copy all the folders in the SmartServer backup directory to the root directory of the SmartServer flash disk.
 6. Enter the **reboot** command in the SmartServer console application.

Note: You can follow these steps to create a new SmartServer that has the same configuration as the backup of an existing SmartServer.

Manually Copying Device Templates to a SmartServer

After you create a device template on a SmartServer, you can manually copy it to one or more other SmartServers. You can then create new devices from the template or use the template to change the interface of existing devices.

To manually copy a device template from one SmartServer to another, follow these steps:

1. Use FTP to access the **/config/template** directory on the source SmartServer flash disk.
2. Click the folder (and any subfolders) containing the template to be copied. By default, the **/config/template** directory contains folders for LONWORKS and Modbus templates.
3. Copy the template (.XML file) to the local drive of your computer, a USB drive, a floppy disk, another removable media, or a shared network drive with read/write permissions (you cannot copy a file from one SmartServer and directly paste it into another). If you copy it to your local drive, you can save it to **C:/LonWorks/iLon100/images/iLon100 4.00/config/template/<driver>** directory. This is useful for copying a set of templates to a SmartServer.
4. Use FTP to access the **/config/template/<driver>** directory on the flash disk of the target SmartServers.
5. Copy the template from the location where it was saved in step 3 to the **/config/template/<driver>** directory on the target SmartServer flash disk.
6. Create new devices from the template as described in *Creating Devices from Templates* in Chapter 4.

Manually Deploying a Pre-Configured SmartServer in a Single Network

You can pre-configure the SmartServer in your office and then manually deploy the pre-configured SmartServer in a single network, using the same OpenLNS network database if you are running the SmartServer in LNS mode. To deploy a pre-configured SmartServer in a single network, follow these steps:

1. If you are using OpenLNS network management service (**LNS Auto** or **LNS Manual**) on the SmartServer, commission the SmartServer and synchronize it to an OpenLNS network database

- following steps 2–3. If you are using **Standalone** network management on the SmartServer, skip to step 4.
2. Commission the SmartServer with OpenLNS CT, OpenLNS tree, or another OpenLNS application. For more information on installing the SmartServer, see *Installing the SmartServer with OpenLNS CT* in Chapter 12.
 3. Synchronize the target SmartServer to the OpenLNS network database in which the target SmartServer was installed in step 2. To do this, follow these steps:
 - a. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
 - b. Add the OpenLNS Server containing the OpenLNS network database in which the target SmartServer was installed in step 8. See *Adding an OpenLNS Server to the LAN* in Chapter 3 for how to do this.
 - c. Click **Driver**, and then click the **Net** network icon. The **Setup – LON Network Driver** Web Page opens.
 - d. In the **Network Management Service** property, click **LNS Auto** or **LNS Manual**.
 - Select **LNS Auto** to have the SmartServer automatically synchronize with the selected OpenLNS network database via the LNS Proxy Web service (you can also manually initiate synchronization by pressing the **Synchronize** button in the **OpenLNS Network** property). In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service. Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default). This is the default.
 - Select **LNS Manual** to have the SmartServer manually synchronize with the selected OpenLNS network database via the LNS Proxy Web service. In this mode, you can synchronize the SmartServer with the selected OpenLNS network database by pressing the **Synchronize** button in the **OpenLNS Network** property. This mode does not require the SmartServer to access to the LNS Proxy Web service port on the OpenLNS Server computer. Select this mode if a firewall is blocking the SmartServer's access to the LNS Proxy Web service port on the OpenLNS Server computer (port 80 by default)..
 - e. In the **LNS Server** property, select the IP address of the OpenLNS Server you added to the LAN in step b.
 - f. Enter the **User Name** and **Password** for logging into the OpenLNS Server via the LNS Proxy Web service.
 - g. The **LNS Network** dialog opens. In the **LNS Network** dialog, select the OpenLNS network database in which the target SmartServer was installed in step 8.
 - h. The **Use OpenLNS Network Interface** option is selected and the network interface used for communication between the OpenLNS Server and the network is listed automatically. Accept these defaults if the OpenLNS Server is attached to the physical network and you want the SmartServer to communicate with the devices on the network through the selected network interface.
 - i. If the **Use OpenLNS Network Interface** option is selected, the **Network Management Mode** property is set to **OnNet** automatically. This means that network changes are propagated to the network immediately. Click **OffNet** to store network changes in the selected OpenLNS network database and propagate them to the network when you place the SmartServer **OnNet**.
 - j. Click **Submit**. The network icon is changed to an LNS Server icon and its name is changed from "Net" to the name of the network you specified in step g. If you selected LNS Auto in step d, the SmartServer automatically begins synchronizing its internal database (the

/config/network folder on the SmartServer flash disk) to the OpenLNS network database. If icons in the network tree are highlighted yellow, it means that the SmartServer's internal database is not yet synchronized with the selected OpenLNS network database.

- k. When synchronization is done, the icons in the network tree should no longer highlighted yellow. If any icons are highlighted yellow or you selected **LNS Manual** in step d, manually synchronize the SmartServer to the OpenLNS network database. To do this, click the **Synchronize** button in the **OpenLNS Network** property.
4. Configure the SmartServer's built-in applications, FPM applications, and custom SmartServer Web pages.
5. If you are using OpenLNS network management service, decommission the SmartServer.
6. Physically install the SmartServer in the field.
7. If you are using OpenLNS network management service, recommission the SmartServer using OpenLNS CT, OpenLNS tree, or another OpenLNS application.
8. If you are using OpenLNS network management service, manually resynchronize the SmartServer to the OpenLNS network database. To do this, right-click the network icon in the SmartServer tree, and then click **Synchronize with LNS** in the shortcut menu. In the **SmartServer Resync** dialog, click **Start**.

Manually Deploying Pre-Configured SmartServers in Multiple Networks

You can pre-configure the SmartServer's built-in applications on a single source SmartServer and manually copy the SmartServer's internal App device to multiple target SmartServers. A common use-case scenario is the configuration of multiple SmartServers at one site. For example, on one source SmartServer, you can configure one or more schedulers, data loggers, type translators, or other applications on the SmartServer's internal App device, back up the SmartServer's internal App device on your computer, copy the SmartServer App device backup to other target SmartServers that have been set to the factory default settings, and then reboot the target SmartServers. The built-in applications on the on the target SmartServers will have the same configuration (data points, presets, and so on) as those on the source SmartServer. If you are using OpenLNS network management service, you can then commission the target SmartServers and synchronize them to their respective OpenLNS network databases.

To deploy pre-configured SmartServers in different networks, follow these steps:

1. Configure the built-in applications on a single source SmartServer.
2. Copy the **/config/network/<Network>/<Channel>/<SmartServer App Device>** folder on the source SmartServer flash disk to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions.
3. Restore the target SmartServer to its factory default settings with the **Setup – Cleanup** Web page or the console application.
 - To restore your SmartServer to its factory default settings using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Clean Up** on the shortcut menu. The **Setup – Cleanup** dialog opens. Click **Cleanup** to reset the SmartServer.
 - To restore your SmartServer to its factory default settings using the console application, enter the **factorydefaults** command, or enter the **factorydefaults keepipaddr** command to reset the SmartServer but keep its basic IPv4 and IPv6 IP addresses. For more information on using the SmartServer console application, see *Appendix B*.
4. Copy the **config/network/<Network>/<Channel>/<SmartServer App Device>** folder to the **/config/network/<Network>/<Channel>** folder on the flash disk of the target SmartServer.

5. Reboot the target SmartServer using the SmartServer Web pages or the SmartServer console application.
 - To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.
 - To reboot your SmartServer using the SmartServer console application, enter the **reboot** command. For more information on using the SmartServer console application, see *Appendix B*.
6. You can open the Web interface of the target SmartServer and expand the SmartServer's App device in the navigation pane on the left side. The functional blocks and data points in the SmartServer App device match those of the source. You can click of the functional blocks under the SmartServer App device (e.g, Data Logger, Scheduler) to see that it has the same configuration as the source.
7. Physically install the SmartServer in the field.
8. If you are using OpenLNS network management (**LNS Auto** or **LNS Manual**) on the target SmartServer, commission the SmartServer and synchronize it to an OpenLNS network database following steps 9–10. If you are using **Standalone** network management on the target SmartServer, you can skip these steps.
9. Commission the SmartServer with OpenLNS CT, OpenLNS tree, or another OpenLNS application. For more information on installing the SmartServer, see *Installing the SmartServer with OpenLNS CT* in Chapter 12.
10. Synchronize the target SmartServer to the OpenLNS network database in which the target SmartServer was installed in step 9. To do this, follow these steps:
 - a. Install the Echelon Enterprise Services 2.2 from the SmartServer 2.2 DVD as described in *Installing Echelon i.LON Enterprise Services* in Chapter 2. If you install Echelon Enterprise Services 2.2 on your computer, you must install OpenLNS Server from the SmartServer 2.2 DVD as described in *Installing Echelon OpenLNS Server* in Chapter 2.
 - b. Add the OpenLNS Server containing the OpenLNS network database in which the target SmartServer was installed in step 9. See *Adding an OpenLNS Server to the LAN* earlier in this chapter for how to do this.
 - c. Click **Driver**, and then click the **Net** network icon. The **Setup – LON Network Driver** Web Page opens.
 - d. In the **Network Management Service** property, click **LNS Auto** or **LNS Manual**.
 - Select **LNS Auto** to have the SmartServer automatically synchronize with the selected OpenLNS network database via the LNS Proxy Web service (you can also manually initiate synchronization by pressing the **Synchronize** button in the **OpenLNS Network** property). In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service. Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default). This is the default.
 - Select **LNS Manual** to have the SmartServer manually synchronize with the selected OpenLNS network database via the LNS Proxy Web service. In this mode, you can synchronize the SmartServer with the selected OpenLNS network database by pressing the **Synchronize** button in the **OpenLNS Network** property. This mode does not require the SmartServer to access to the LNS Proxy Web service port on the OpenLNS Server computer. Select this mode if a firewall is blocking the SmartServer's access to the LNS Proxy Web service port on the OpenLNS Server computer (port 80 by default).

- e. In the **LNS Server** property, select the IP address of the OpenLNS Server you added to the LAN in step b.
 - f. Enter the **User Name** and **Password** for logging into the OpenLNS Server via the LNS Proxy Web service.
 - g. The **LNS Network** dialog opens. In the **LNS Network** dialog, select the OpenLNS network database in which the target SmartServer was installed in step 9.
 - h. The **Use OpenLNS Network Interface** option is selected and the network interface used for communication between the OpenLNS Server and the network is listed automatically. Accept these defaults if the OpenLNS Server is attached to the physical network and you want the SmartServer to communicate with the devices on the network through the selected network interface.
 - i. If **Use OpenLNS Network Interface** is selected, the **Network Management Mode** option is set to **OnNet** automatically. This means that network changes are propagated to the network immediately. Click **OffNet** to store network changes in the selected OpenLNS network database and propagate them to the network when you place the SmartServer **OnNet**.
 - j. Click **Submit**. The network icon is changed to an LNS Server icon and its name is changed from “Net” to the name of the network you specified in step g. If you selected **LNS Auto** in step d, the SmartServer automatically begins synchronizing its internal database (the /config/network folder on the SmartServer flash disk) to the OpenLNS network database. If icons in the network tree are highlighted yellow, it means that the SmartServer’s internal database is not yet synchronized with the selected OpenLNS network database.
 - k. When synchronization is done, the icons in the network tree will no longer be highlighted yellow. If any icons are highlighted yellow or you selected **LNS Manual** in step d, manually synchronize the SmartServer to the OpenLNS network database. To do this, click the **Synchronize** button in the **OpenLNS Network** property.
11. Repeat steps 3–10 to copy the SmartServer App device configuration to additional target SmartServers.

Manually Deploying a Network Configuration on Multiple SmartServers

You can configure a network on a single source SmartServer and then manually deploy that network configuration on multiple target SmartServers. Specifically, you can add or copy external devices and their data points to the source SmartServer, configure the source SmartServer’s built-in applications, configure your custom apps on the source SmartServer, and create custom Web pages for monitoring and controlling the external data points and the internal data points on the source SmartServer.

After configuring the source SmartServer, you can make a backup and then copy the backup to one or more target SmartServers that have been set to the factory default settings. After copying the backup to a target SmartServer, reboot the target SmartServer, commission the target SmartServer and synchronize it to an OpenLNS network database (if you are using OpenLNS network management services [**LNS Auto** or **LNS Manual**]), and then logically replace the external devices in the target SmartServer’s internal network database.

To deploy a network configuration on multiple SmartServers, follow these steps:

1. Copy all the folders in the root directory of the source SmartServer flash disk except for the **alarmLog** and **data** folders to the local drive of your computer, a USB drive, another removable media, or a shared network drive with read/write permissions.
2. In the **config** folder of the source SmartServer backup, delete the following folders and files:
 - **license** folder (to preserve programmability and IP-852 routing licenses on target SmartServers).

- **config.sys** file (to preserve TCP/IP configurations on target SmartServers).
 - **software/dci** file (if the source SmartServer was in standalone mode when the backup was made; this avoids the duplication of network configuration data).
3. Restore the target SmartServer to its factory default settings with the **Setup – Cleanup** Web page or the console application.
 - To restore your SmartServer to its factory default settings using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Clean Up** on the shortcut menu. The **Setup – Cleanup** dialog opens. Click **Cleanup** to reset the SmartServer.
 - To restore your SmartServer to its factory default settings using the console application, enter the **factorydefaults** command, or enter the **factorydefaults keepipaddrs** command to reset the SmartServer but keep its basic IPv4 and IPv6 IP addresses. For more information on using the SmartServer console application, see *Appendix B*.
 4. Copy the modified backup of the source SmartServer to the flash disk of the target SmartServer.
 5. In the **config/network** folder on the target SmartServer, delete the **Net** folder.
 6. Reboot your SmartServer using the SmartServer Web pages or the SmartServer console application.
 - To reboot your SmartServer using the SmartServer Web pages, right-click the local SmartServer, point to **Setup**, and then click **Reboot** on the shortcut menu. The **Setup – Reboot** dialog opens. Click **Reboot** to start the reboot.
 - To reboot your SmartServer using the SmartServer console application, enter the `reboot` command. For more information on using the SmartServer console application, see *Appendix B*.
 7. If you are using OpenLNS network management (**LNS Auto** or **LNS Manual**) on the target SmartServer, commission the SmartServer and synchronize it to an OpenLNS network database following steps 8–9. If you are using **Standalone** network management on the target SmartServer, skip to step 10.
 8. Commission the SmartServer with OpenLNS CT, OpenLNS tree, or another OpenLNS application. For more information on installing the SmartServer, see *Installing the SmartServer with OpenLNS CT* in Chapter 12.
 9. Synchronize the target SmartServer to the OpenLNS network database in which the target SmartServer was installed in step 8. To do this, follow these steps:
 - a. Verify that EES 2.2 and OpenLNS Server have been installed on your computer. See Chapter 1 of the *Echelon Enterprise Services 2.2 User's Guide* for how to perform these installations.
 - b. Add the OpenLNS Server containing the OpenLNS network database in which the target SmartServer was installed in step 8. See *Adding an OpenLNS Server to the LAN* earlier in this chapter for how to do this.
 - c. Click **Driver**, and then click the **Net** network icon. The **Setup – LON Network Driver** Web Page opens.
 - d. In the **Network Management Service** property, click **LNS Auto** or **LNS Manual**.
 - Select **LNS Auto** to have the SmartServer automatically synchronize with the selected OpenLNS network database via the LNS Proxy Web service (you can also manually initiate synchronization by pressing the **Synchronize** button in the **OpenLNS Network** property). In this mode, the SmartServer independently initiates communication with the LNS Proxy Web service. Select this mode if a firewall is not blocking the SmartServer's access to the port on the OpenLNS Server computer selected for the LNS Proxy Web service (port 80 by default). This is the default.

- Select **LNS Manual** to have the SmartServer manually synchronize with the selected OpenLNS network database via the LNS Proxy Web service. In this mode, you can synchronize the SmartServer with the selected OpenLNS network database by pressing the **Synchronize** button in the **OpenLNS Network** property. This mode does not require the SmartServer to access to the LNS Proxy Web service port on the OpenLNS Server computer. Select this mode if a firewall is blocking the SmartServer's access to the LNS Proxy Web service port on the OpenLNS Server computer (port 80 by default)..
- e. In the **LNS Server** property, select the IP address of the OpenLNS Server you added to the LAN in step b.
 - f. Enter the **User Name** and **Password** for logging into the OpenLNS Server via the LNS Proxy Web service.
 - g. The **LNS Network** dialog opens. In the **LNS Network** dialog, select the OpenLNS network database in which the target SmartServer was installed in step 8.
 - h. The **Use OpenLNS Network Interface** option is selected and the network interface used for communication between the OpenLNS Server and the network is listed automatically. Accept these defaults if the OpenLNS Server is attached to the physical network and you want the SmartServer to communicate with the devices on the network through the selected network interface.
 - i. If the **Use OpenLNS Network Interface** option is selected, the **Network Management Mode** property is set to **OnNet** automatically. This means that network changes are propagated to the network immediately. Click **OffNet** to store network changes in the selected OpenLNS network database and propagate them to the network when you place the SmartServer **OnNet**.
 - j. Click **Submit**. The network icon is changed to an LNS Server icon and its name is changed from "Net" to the name of the network you specified in step g. If you selected LNS Auto in step d, the SmartServer automatically begins synchronizing its internal database (the **/config/network** folder on the SmartServer flash disk) to the OpenLNS network database. If icons in the network tree are highlighted yellow, it means that the SmartServer's internal database is not yet synchronized with the selected OpenLNS network database.
 - k. When synchronization is done, the icons in the network tree should no longer be highlighted yellow. If any icons are highlighted yellow or you selected **LNS Manual** in step d, you need to manually synchronize the SmartServer to the OpenLNS network database. To do this, click the **Synchronize** button in the **OpenLNS Network** property.
10. Use the SmartServer Web interface to logically replace the external devices in the network tree of the target SmartServer. See *Replacing Devices* in Chapter 5 for more information on how to do this.
 11. If you selected **LNS Manual** mode in step 8, manually synchronize the SmartServer to the OpenLNS network database to update the OpenLNS network database with the Neuron IDs of the external devices on the network.
 12. If you copied SmartServer custom Web pages to the target SmartServer, open all pages containing i.LON Vision objects and update the selected data points monitored and controlled by the objects.

Tip: If the i.LON Vision objects in your custom Web pages on the source SmartServer use alias names, you can skip step 12.

The data points on the SmartServer's internal App and Virtual devices [**iLON App (Internal)** and **iLON System (Internal)**] have default alias names, with NVL_ and iLON System prefixes, respectively.

You can define an alias name for an external data point in its **Configure - Data Point** Web page, which you can access by clicking **General** and then clicking the external data point in the network branch of the SmartServer tree.

13. Repeat steps 3–12 to copy the network configuration to additional target SmartServers.

Appendix E

Software License Agreements

When installing the SmartServer 2.2 and i.LON LNS Server software, you must agree to the terms of the software license agreements detailed in this appendix.

SmartServer 2.2 Software

NOTICE

This is a legal agreement between you (“You” “Your”) and Echelon Corporation (“Echelon”). YOU MUST READ AND AGREE TO THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT BEFORE ANY SOFTWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE “ACCEPT” BUTTON OF THIS SOFTWARE LICENSE AGREEMENT, OR DOWNLOADING SOFTWARE, OR INSTALLING SOFTWARE, OR USING SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND NOT DOWNLOAD OR INSTALL OR USE ANY SOFTWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE SOFTWARE AND YOU MAY RETURN IT TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND (IF APPLICABLE).

SmartServer 2.2 Software License Agreement

Echelon grants You a non-exclusive, non-transferable license to use the Licensed Software and accompanying documentation and any updates or upgrades thereto provided by Echelon according to the terms set forth below. As used herein:

- "Licensed Software" means the i.LON Utilities, i.LON System Image, and the Programming Tools.
- "i.LON Utilities" means the i.LON Server computer software utilities listed in the utilities.txt file, and associated media, printed materials, and online or electronic documentation, including without limitation any and all executable files, add-ons, stencils, templates, i.LON Vision 2.2 shapes, SmartShapes® symbols, SOAP APIs, filters, tutorials, help files, Web pages and other files, that accompany such software or are in the accompanying documentation.
- "i.LON Server" means Echelon's i.LON e3 plus Internet Server, SmartServer, or SmartServer 2.2 product, or any successor product sold by Echelon.
- "i.LON System Image" means the firmware preloaded on an i.LON Server or listed in the system.txt file, and associated media, printed materials, and online or electronic documentation, including without limitation any and all executable files, tutorials, help files, Web pages and other files, that accompany such software or are in the accompanying documentation.
- "LNS Proxy" means the driver that allows access to the OpenLNS Server, synchronization between the i.LON Server and the OpenLNS database, and copying of external data points from the OpenLNS database to the i.LON Server. The LNS Proxy includes Web applications files, the Spring 2.5.6 Framework, Spring-WS 1.5.7 and JAXB2 2.1 SOAP frameworks library files, and the LnsNative.dll and LnsNativeUtil.dll files which access an OpenLNS Server.

- “OpenLNS Server” means the Echelon OpenLNS Server product, or the executable files generated by running the Echelon LNS Redistributable Maker (version 3.0 or higher) product identified for use by OpenLNS Servers.
- "ISO/IEC 14908-1" means the ISO/IEC 14908-1 Control Network Protocol. Echelon’s implementation of this protocol is known as the LonTalk[®] protocol.
- "IP-852 Channel" means a collection of devices that communicate using the ISO/IEC 14908-4 protocol.
- “IP-852 Device” means a device that attaches to an IP-852 Channel.
- "Control" means to write network variable values as defined by the ISO/IEC 14908-1 Protocol using the i.LON Utilities or SOAP protocol.
- "Configure" means to provide a valid ISO/IEC 14908-1 domain, subnet, and node address, as well as valid group, network variable selector, and message tag values, and device state information as defined by the ISO/IEC 14908-1 Protocol to the i.LON Server, to set configuration properties on an i.LON Server using the i.LON Utilities or SOAP protocol, and to create custom Web pages for an i.LON Server using the i.LON Utilities.
- "Monitor" means to read, process, and view network variable values, application message contents, and device state information as defined by the ISO/IEC 14908-1 Protocol using the i.LON Utilities or SOAP protocol.
- “Programming Tools” means the demonstration or full version of the Echelon SmartServer Programming Tools as provided on the DVD or DVD image containing the Licensed Software which includes the (i) GNU Compiler; (ii) Header Files; and (iii) Libraries, all from the Wind River Platform for Industrial Devices 3.2 and any subsequent versions thereof.
- “SOAP API” means the programmatic interface used to access an i.LON Server or an LNS Proxy using the SOAP protocol.

If the Licensed Software is being provided to You as an update or upgrade to software which You have previously licensed, then You agree to destroy all copies of the prior release of this software within thirty (30) days after installing the Licensed Software; provided, however, that You may retain one (1) copy of the prior release for backup, archival and support purposes.

LICENSE

You may:

- (a) use the i.LON Utilities internally to Monitor, Control, and Configure i.LON Servers and to create IP-852 Channels, each with a minimum of one (1) i.LON Server and up to 255 additional IP-852 Devices;
- (b) copy the i.LON Utilities as reasonably necessary for such permitted internal use and for backup or archival purposes consistent with Your archive procedures, provided that You reproduce, unaltered, all proprietary notices on or in such copies;
- (c) use the Programming Tools solely within the Echelon freely programmable modules (“FPM”) framework to create and install custom apps on one or more i.LON Servers;

- (d) use the Programming Tools solely with an i.LON Server;
- (e) use the LNS Proxy and LNS Proxy SOAP API solely to access an OpenLNS Server from an i.LON Server or a client application.
- (f) make one (1) copy of the i.LON System Image for the purpose of loading it into an i.LON Server in order to replace or update the i.LON System Image on the i.LON Server and one (1) copy for backup or archival purposes consistent with Your archive procedures, provided that You reproduce, unaltered, all proprietary notices on or in such copies; and
- (g) transfer Your rights under this Agreement to an end user of the Licensed Software; provided that (i) You require the transferee to execute both copies of the Software License Transfer Agreement included with the Licensed Software, and (ii) You retain one (1) signed original thereof and furnish Echelon with a copy of same upon request. This right of transfer is exercisable on a one-time-only basis, and Your transferee shall have no right whatsoever to further transfer any rights to the Licensed Software.

You may not:

- (a) use the Licensed Software for purposes other than the purposes set forth above;
- (b) copy the Licensed Software, or any part thereof, except as expressly permitted above, or copy the accompanying documentation;
- (c) modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Licensed Software, including without limitation any such mechanism used to restrict or control the functionality of the Licensed Software, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the software from the Licensed Software (except to the extent that such activities may not be prohibited under applicable law), or
- (d) distribute, rent, transfer or grant any rights in the Licensed Software or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Echelon.

This license is not a sale. The Licensed Software may contain or be derived from materials provided to Echelon under license from a third party supplier. Title and copyrights to the Licensed Software, accompanying documentation and any copy made by You remain with Echelon or its suppliers. Unauthorized copying of the Licensed Software or the accompanying documentation, or failure to comply with the above restrictions, will result in automatic termination of this license and will make available to Echelon and its suppliers other legal remedies. You agree to indemnify, to the fullest extent permitted by law, Echelon and its suppliers (“Indemnitees”), for any third party infringement claims that may arise as a result of Your use of any Licensed Software in violation of the license granted in this provision.

You may make appropriate and truthful reference to Echelon and Echelon products and technology in Your company and product literature; provided that You properly

attribute Echelon's trademarks. No license is granted, express or implied, under any Echelon trademarks, trade names or service marks.

OPEN SOURCE AND THIRD PARTY SOFTWARE

(a) Open Source Software. The Licensed Software may include, or may be distributed on the same media or in the same download with, software that is subject to open source licensing terms ("Open Source Software") which terms are available at www.echelon.com. Open Source Software shall remain subject to such terms. The Open Source Software is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ALL SUCH WARRANTIES ARE HEREBY DISCLAIMED. NEITHER ECHELON NOR THE AUTHORS OF THE OPEN SOURCE SOFTWARE SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), 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 OR DISTRIBUTION OF THE OPEN SOURCE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Copyrights to the Open Source Software are held by the copyright holders indicated in the copyright notices in the corresponding source files. If the Open Source Software license also requires source code to be made available, such source code is available at www.echelon.com. Without limiting the foregoing, the Licensed Software may be distributed on the same media or in the same download with certain software that is subject to a General Public License (GPL) ("GPL Software"), and such GPL Software is licensed to You free of charge.

(b) Wind River Software. The Licensed Software may contain software licensed from Wind River Systems, Inc. ("Wind River"). The license terms applicable to software licensed to Echelon by Wind River are incorporated herein.

TERMINATION

This license will continue until terminated. Unauthorized copying of the Licensed Software or failure to comply with the above restrictions will result in automatic termination of this Agreement and will make available to Echelon other legal remedies. This license will also automatically terminate if You go into liquidation, suffer or make any winding up petition, make an arrangement with Your creditors, or suffer or file any similar action in any jurisdiction in consequence of debt. Upon termination of this license for any reason You will destroy all copies of the Licensed Software. Any use of the Licensed Software after termination is unlawful.

TRADEMARKS

You may make appropriate and truthful reference to Echelon, Echelon products and technology in Your company and product literature; provided that You properly attribute Echelon's trademarks and do not use the name of Echelon or any Echelon trademark in Your name or product name. No license is granted, express or implied, under any Echelon trademarks, trade names, trade dress or service marks.

LIMITED WARRANTY AND DISCLAIMER

Echelon warrants that, for a period of ninety (90) days from the date of delivery or transmission to You, the Licensed Software under normal use will perform substantially in accordance with the Licensed Software specifications contained in the documentation accompanying the Licensed Software. Echelon's entire liability and Your exclusive remedy under this warranty will be, at Echelon's option, to use reasonable commercial efforts to attempt to correct or work around errors, to replace the Licensed Software with functionally equivalent Licensed Software, or to terminate this Agreement. EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTIES, ECHELON AND ITS SUPPLIERS MAKE AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND ECHELON AND ITS SUPPLIERS SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT AND THEIR EQUIVALENTS. Echelon does not warrant that the operation of the Licensed Software will be uninterrupted or error free or that the Licensed Software will meet Your specific requirements.

SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE AND JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY

IN NO EVENT WILL ECHELON OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA, LOST PROFITS, COST OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES OR OTHER SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING FROM THE USE OF THE LICENSED SOFTWARE OR ACCOMPANYING DOCUMENTATION, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE). THIS LIMITATION WILL APPLY EVEN IF ECHELON OR AN AUTHORIZED DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN. IN NO EVENT SHALL ECHELON'S OR ITS SUPPLIERS' LIABILITY EXCEED THE AMOUNTS PAID FOR THE LICENSED SOFTWARE. ALL LIABILITY UNDER THIS AGREEMENT IS

CUMULATIVE AND NOT PER INCIDENT AND BENEFIT ECHELON'S THIRD PARTY SUPPLIERS. YOU ACKNOWLEDGE THAT THE AMOUNTS PAID BY YOU FOR THE LICENSED SOFTWARE REFLECT THIS REASONABLE ALLOCATION OF RISK.

SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

SAFE OPERATION

YOU ASSUME RESPONSIBILITY FOR, AND HEREBY AGREE TO USE YOUR BEST EFFORTS IN, ROUTING, MONITORING, CONTROLLING LONWORKS DEVICES TO PROVIDE FOR SAFE OPERATION THEREOF, INCLUDING, BUT NOT LIMITED TO, COMPLIANCE OR QUALIFICATION WITH RESPECT TO ALL SAFETY LAWS, REGULATIONS AND AGENCY APPROVALS, AS APPLICABLE. THE SMART TRANSCEIVER, NEURON CHIP, ISO/IEC 14908-1 PROTOCOL, NEURON CHIP FIRMWARE, i.LON SERVER, AND THE LICENSED SOFTWARE ARE NOT DESIGNED OR INTENDED FOR USE AS COMPONENTS IN EQUIPMENT INTENDED FOR SURGICAL IMPLANT INTO THE BODY, OR OTHER APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH THE FAILURE OF THE SMART TRANSCEIVER, NEURON CHIP, LONTALK PROTOCOL, NEURON CHIP FIRMWARE, i.LON SERVER, OR THE LICENSED SOFTWARE COULD CREATE A SITUATION IN WHICH PERSONAL INJURY OR DEATH MAY OCCUR, AND YOU SHALL HAVE NO RIGHTS HEREUNDER FOR ANY SUCH APPLICATIONS.

COMPLIANCE WITH EXPORT CONTROL LAWS

You agree to comply with all applicable export and re-export control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the United States Department of Commerce. Specifically, You covenant that You shall not—directly or indirectly—sell, export, re-export, transfer, divert, or otherwise dispose of any software, source code, or technology (including products derived from or based on such technology) received from Echelon under this Agreement to any country (or national thereof) subject to antiterrorism controls or U.S. embargo, or to any other person, entity, or destination prohibited by the laws or regulations of the United States, without obtaining prior authorization from the competent government authorities as required by those laws and regulations. You agree to indemnify, to the fullest extent permitted by law, Echelon from and against any fines or penalties that may arise as a result of Your breach of this provision. This export control clause shall survive termination or cancellation of this Agreement.

LANGUAGE

The parties hereto confirm that it is their wish that this Agreement, as well as other documents relating hereto, have been and shall be written in the English language only.

Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise.

GENERAL

This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods; rather, this Agreement shall be governed by the laws of the State of California, including its Uniform Commercial Code, without reference to conflicts of laws principles. This Agreement is the entire agreement between us and supersedes any other communications or advertising with respect to the Licensed Software and accompanying documentation. If any provision of this Agreement is held invalid or unenforceable, such provision shall be revised to the extent necessary to cure the invalidity or unenforceability, and the remainder of the Agreement shall continue in full force and effect. If You are acquiring the Licensed Software on behalf of any part of the U.S. Government, the following provisions apply. The Licensed Software and accompanying documentation were developed at private expense and are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Licensed Software and/or the accompanying documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be "technical data/commercial items" pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b). You agree not to export the Licensed Software in violation of the laws and regulations of the United States or any other nation. Echelon's direct and indirect licensors of software incorporated into the Licensed Software are third party beneficiaries of this Agreement and this Agreement is made expressly for the benefit of, and is enforceable by, Echelon and such licensors.

Echelon, LON, LonTalk, LonMaker, LonWorks, i.LON, and Neuron are registered trademarks of Echelon Corporation in the U.S. and other countries. SmartShapes is a U.S. registered trademark of Microsoft Corporation.

