SIEMENS

RUGGEDCOM ELAN v8.5

User Guide

07/2016

RC1269-EN-01

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Open Source

RUGGEDCOM ELAN contains Open Source Software. For license conditions, refer to the associated *License Conditions* document.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity .

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com .

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address	Telephone	E-mail
Siemens Canada Ltd Industry Sector 300 Applewood Crescent	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995	ruggedcom.info.i-ia@siemens.com **Web** www.siemens.com/ruggedcom

Concord, Ontario
Canada, L4K 5C7

Table of Contents

Preface

This guide describes the Maestro and RUGGEDCOM ELAN Web Interface (EWI) tools used for configuring and managing RUGGEDCOM ELAN servers. It contains instructions and guidelines on how to use the software, as well as some general theory.

It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.

Conventions

This User Guide uses the following conventions to present information clearly and effectively.

›› Alerts

The following types of alerts are used when necessary to highlight important information.

> **DANGER!**
> *DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.*

> **WARNING!**
> *WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.*

> **CAUTION!**
> *CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.*

> **IMPORTANT!**
> *IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.*

> **NOTE**
> *NOTE alerts provide additional information, such as facts, tips and details.*

›› CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
`command`	Commands are in bold.
`command` `parameter`	Parameters are in plain text.

Example	Description
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command { parameter3 | parameter4 }	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 { parameter3 | parameter4 }	All commands and parameters are presented in the order they must be entered.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM ROX II User Guide for RX1500 Series Devices*
- *RUGGEDCOM ROX II User Guide for RX1400*
- *RUGGEDCOM APE Developer Guide*

System Requirements

Browser Requirements

- Microsoft Internet Explorer 10.0 or higher
- Mozilla Firefox
- Google Chrome
- Iceweasel/IceCat (Linux Only)

Maestro Requirements

- Maestro v2.4.x
- Java SE 6, 32 or 64 bit

Accessing Documentation

The latest user documentation for RUGGEDCOM ELAN v8.5 is available upon request. To request or inquire about a user document, contact Siemens Customer Support.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens Sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

Online

Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx .

Mobile App

Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Introduction

Welcome to the RUGGEDCOM ELAN v8.5 User Guide. This document details how to configure and manage a RUGGEDCOM ELAN server via:

- **Maestro**, a Java-based tool for creating RUGGEDCOM ELAN server configurations
- The **RUGGEDCOM ELAN Web Interface (EWI)**, a web-based utility for managing and monitoring the RUGGEDCOM ELAN server

RUGGEDCOM ELAN is a family of applications for secure communication and data integration in any SCADA architecture, from the Substation to the Control Center. It facilitates the connection of enterprise information systems to any device, anywhere, at any time. RUGGEDCOM ELAN applications can be deployed in the substation, at the Control Center or elsewhere, to assist in accessing substation data.

CONTENTS

Section 1.1

Security Recommendations

To prevent unauthorized access to RUGGEDCOM ELAN, note the following security recommendations:

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before RUGGEDCOM ELAN is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different user names and systems, or after they expire.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.
- Restrict access to workstations running Maestro to only trusted personnel.
- Restrict access to the RUGGEDCOM ELAN configuration database to only trusted personnel. For more information, refer to Section 3.11, “Managing the RUGGEDCOM ELAN Configuration Database” .

Physical/Remote Access

- Restrict physical access to the RUGGEDCOM ELAN server to only trusted personnel. A person with malicious intent in possession of removable media (e.g. USB, external hard drive, etc.) could extract critical information, such as certificates, keys, etc., or reprogram the server.

- If a firewall is required, configure and start the firewall before connecting the server/device/workstation to a public network. Make sure the firewall is configured to accept connections from a specific domain.
- Configure a firewall to prevent Brute Force Attacks (BFAs) from third-parties attempting to obtain unauthorized access to the device. In the case of RUGGEDCOM ELAN running on RUGGEDCOM ROX II, enable the Brute Force Attack protection system. The ROX II firewall can also be utilized to restrict connections to trusted IP addresses, ports and services. For more information, refer to the *RUGGEDCOM ROX II User Guide* for RX1400 or RX1500 Series devices.
- Use the latest Web browser version compatible with RUGGEDCOM ELAN to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed.
- Replace all default SCADA communication certificates before deploying RUGGEDCOM ELAN. For more information, refer to Section 3.10.2, "Managing SCADA Communication Certificates" .
- Deactivate SSLv3 in all Web browsers used to access RUGGEDCOM ELAN and use the recommended TLSv1 protocol when connecting to RUGGEDCOM ELAN via HTTPS. SSLv3 is known to be vulnerable to the POODLE (Padding Oracle On Downgraded Legacy Encryption) security flaw. For more information, refer to the RUGGEDCOM ELAN Security Advisory SSB-583110 (PDF) [http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssb-583110.pdf].
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- Connect only to trusted IP addresses.
- Do not expose the Postgres TCP port or Jazz port (on the Jazz host) to the Internet.
- Limit access to the Jazz SDK to authorized personnel only.
- Disable access via SSH, unless when used within the security parameter and according to industry best practices. Access to the root account on the RUGGEDCOM ELAN base-system should be disabled.
- When connecting via SSH, wherever possible, configure the SSH client to:
  - Where possible, use Counter (CTR) operation mode based ciphers. CTR mode is considered more secure than the Cipher Block Chaining (CBC) operation mode.
  - Where possible, use SHA1 (256 bit) and SHA2 (512 bit) MAC algorithms. These are considered more secure than MD5 and 96 bit MAC algorithms.

Communication

- When transmitting data over the Internet, only use DNP 3.0 clients and servers secured with TLS v1.2 and certificated based authentication. All other protocols and their respctive client and server communications should be contained within the security perimeter or on a secure channel.
- All communications with Jazz and RUGGEDCOM REFLEX products should be contained within the security perimeter or on a secure channel.
- All communications with Maestro should be contained within the security perimeter.
- Make sure IP address allocations are managed by authenticated and privileged users only, and that all IP addresses within the network are unique.

Hardware/Software

- Make sure the latest firmware for the base system and RUGGEDCOM ELAN version are installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security website [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm] . Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.

- Only enable the services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- Management of the certificates and keys is the responsibility of the device owner. Before returning any hardware provided by Siemens for repair, replace the current certificates and keys with temporary *throwaway* certificates and keys that can be destroyed upon the device's return.
- Use redundant RUGGEDCOM ELAN setups whenever possible to increase availability of all services and to backup the configuration.
- Make sure robust Server Class hardware is used when installing RUGGEDCOM ELAN on custom hardware not provided by Siemens.

Policy

- Periodically audit all workstations that access the RUGGEDCOM ELAN server to make sure they comply with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with RUGGEDCOM ELAN for further security recommendations.

Section 1.2

Features and Benefits

The following describes the many features and benefits offered by RUGGEDCOM ELAN:

Primary Features

- Open, flexible access to all substation and distribution devices
- Protocol conversion and/or normalization of legacy and current protocols (e.g. DNP 3.0, etc.)
- Support for both SCADA and non-SCADA hosts (e.g. RUGGEDCOM REFLEX)
- Route SCADA traffic from any network application to any IED or RTU
- For SEL and GE UR relays, IED file management automatically uploads event records and files from downstream IEDs
- Integration with RUGGEDCOM multi-server platform appliances

High Availability

- Communication redundancy capabilities
- Multi-master, multi-protocol support for server-side communications
- Multi-device (up to 1000), multi-point (100,000+) support for each RUGGEDCOM ELAN server instance

Faster Deployment

- Easily configured with templates and bulk editing capabilities
- Installation on any hardware or virtual machine including RUGGEDCOM RX1400 and RUGGEDCOM RX1500 Series devices
- Can be installed from Substation to Control Center

Secure

- Support for TLS v1.2 and SSL secure communications
- Utilized by major wholesale electricity providers

Integration

- Concurrent standard and legacy protocol conversion
- Data concentration
- Accessible real time data and configuration information
- Automatic fault file retrieval
- RUGGEDCOM ELAN Jazz interface enables multi-protocol communication between RuggedApps and IEDs

Section 1.3

Available RUGGEDCOM ELAN Servers

RUGGEDCOM ELAN applications are run from a RUGGEDCOM ELAN server. Four types of servers are available:

›› Front End Processor (FEP)

The FEP server is deployed at the Control Center and is intended for high throughput, large scale protocol conversions. It offers the following features/benefits:

- Gathers system and subsystem data
- Serves data to Enterprise consumers (e.g. EMS, Historian)
- Protocol conversion and data concentration
- Enables or enhances redundancy using IP aliasing and listen clusters

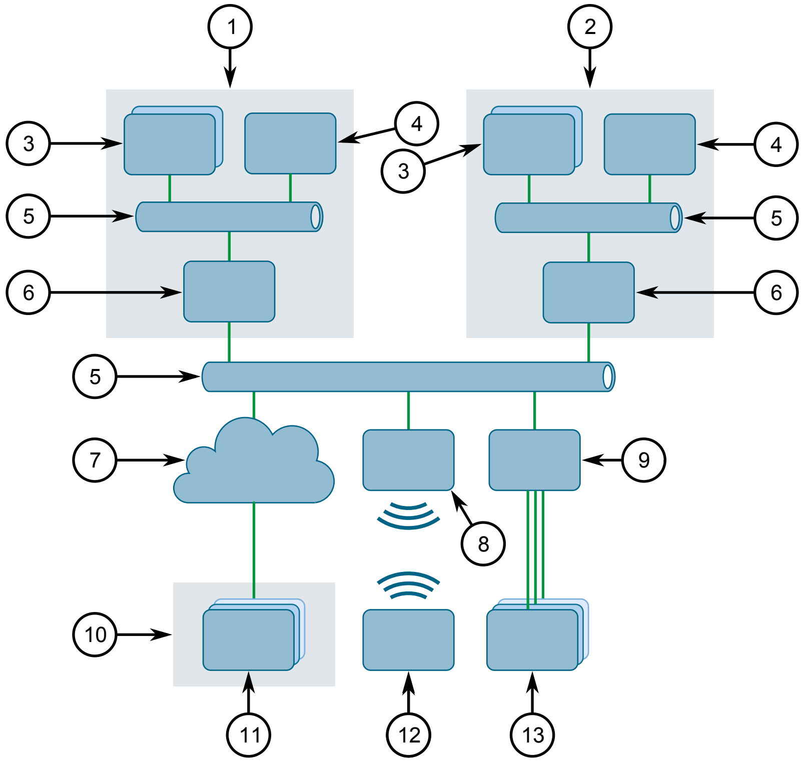


Figure 1: Example RUGGEDCOM ELAN FEP Server Application

1. Control Center (Primary) **2.** Control Center (Secondary) **3.** Energy Management System (EMS) **4.** Historian **5.** LAN **6.** RUGGEDCOM ELAN FEP Server **7.** Substation WAN **8.** Wireless **9.** Serial Server **10.** Substations **11.** IEDs **12.** Distribution Automation IEDs **13.** Serial IEDs

Universal Data Gateway (UDG) and Remote Intelligent Gateway (RIG)

The UDG server is a scaled-down version of the FEP server, and RIG is a secure communication version of UDG. UDG and RIG are deployed inside or outside the Substation and are designed for flexible, high performance protocol routing. UDG is primarily intended for protocol routing and/or translation. RIG is intended for secure DNP communications using TLS/SSL. Both offer the following features/benefits:

- Provides protocol conversion and data concentration for SCADA.
- Includes the RUGGEDCOM ELAN Protocol Router.
  - Device level configuration
  - Address masquerading
  - Listen clusters
- Integrates with RUGGEDCOM RX1400 and RUGGEDCOM RX1500 Series devices, eliminating the need for additional substation computers.
- Multi-host support allows multiple masters to communicate virtually with a given field device. The UDG/RIG server would typically be deployed in the Control Center for this feature.

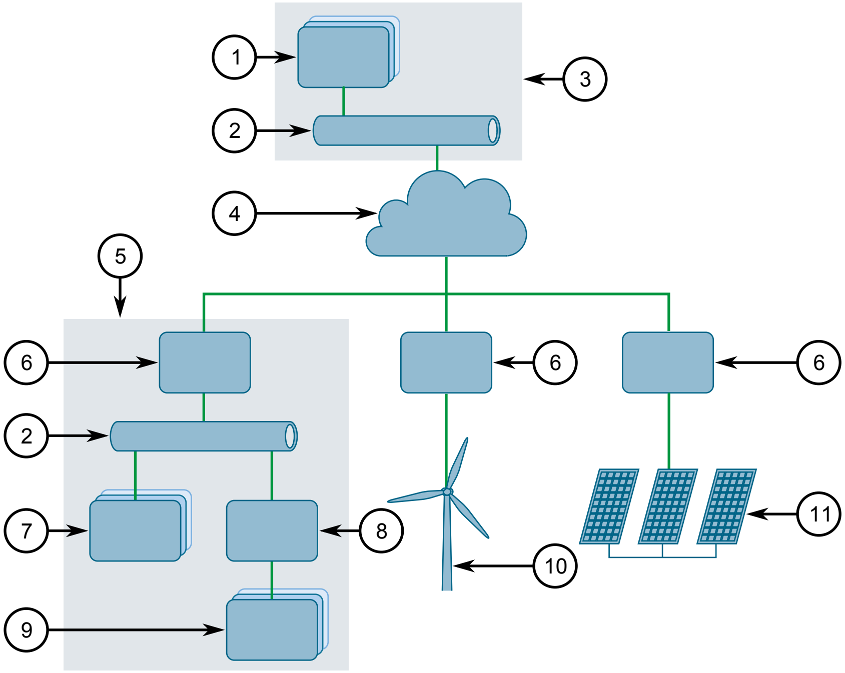


Figure 2: Example RUGGEDCOM ELAN UDG/RIG Server Application

1. Energy Management System (EMS) **2.** LAN **3.** Control Center **4.** System WAN **5.** Substation **6.** RUGGEDCOM ELAN UDG/RIG Server **7.** IEDs **8.** Serial Server **9.** Serial IEDs **10.** Wind Farm **11.** Solar Farm

›› Substation Communication Server (SCS)

The SCS server is similar to the UDG server, but with expanded functionality for complete substation data management. It is deployed at the Substation and typically used to collect substation data for Enterprise applications. It addresses the need for accessing IED data from a number of Control Center and Enterprise applications and remote users. It offers the following features/benefits:

- IED file management automatically uploads even records and files from downstream IEDs (non-operational data)
- May run on a RUGGEDCOM RX1400 device, RUGGEDCOM RX1500 Series device or a RUGGEDCOM APE module, eliminating the need for additional substation workstations

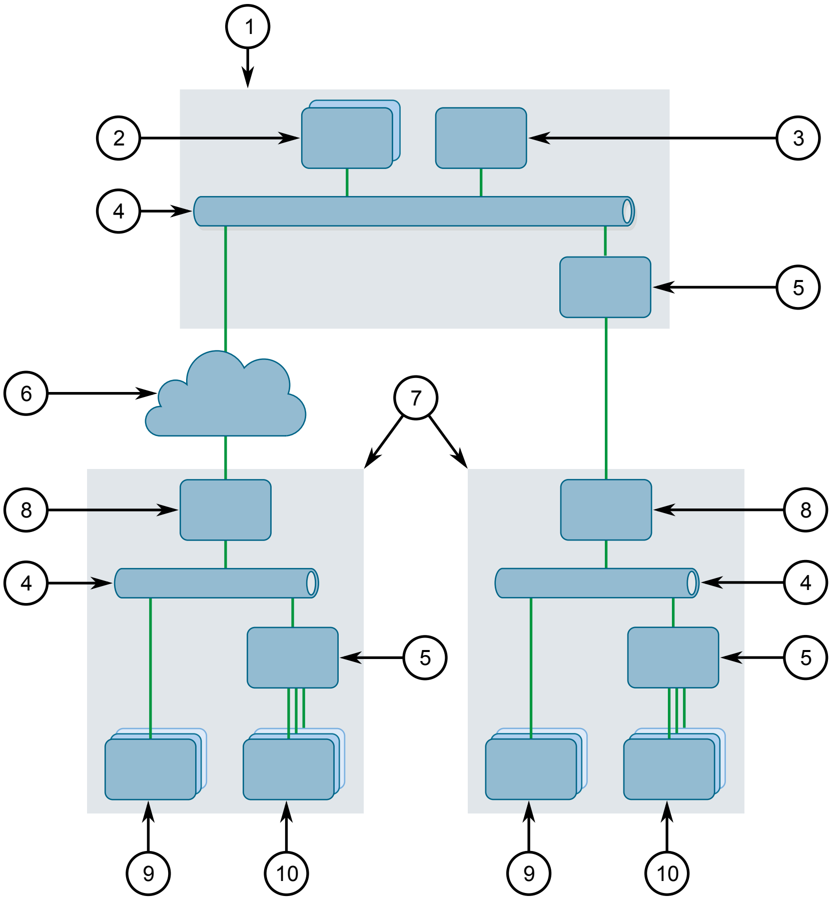


Figure 3: Example RUGGEDCOM ELAN SCS Server Application

1. Control Center **2.** Energy Management System (EMS) **3.** Non-Operational Data Repository **4.** LAN **5.** Serial Server **6.** Substation WAN **7.** Substations **8.** RUGGEDCOM ELAN SCS Server **9.** IEDs **10.** Serial IEDs

Section 1.4

ELAN Architecture and Operation

ELAN operates on the Debian 7.0 (Wheezy) Linux platform. It can be installed on a standalone server, virtual machine, a RUGGEDCOM RX1400 device, a RUGGEDCOM RX1500 Series device, or a RUGGEDCOM APE module.

> **NOTE**
> *For information about compatibility with other RUGGEDCOM products, contact a Siemens Sales representative.*

It includes the following components:

Data Communications

- Protocol Router for DNP and IEC 60870-5-104 Protocols

Data Processing

- PostgreSQL Database (Real-Time and Relational)
- Automatic File Manager

Visualization

- RUGGEDCOM ELAN Web Interface (EWI)
- RUGGEDCOM REFLEX (HMI)

- Real-Time SCADA Engine, Host Interfaces and Protocols
- IED/RTU Interfaces and Protocols (e.g. DNP 3.0, Modbus, IEC 60870-5-104, etc.)
- Maestro (Configuration Tool)

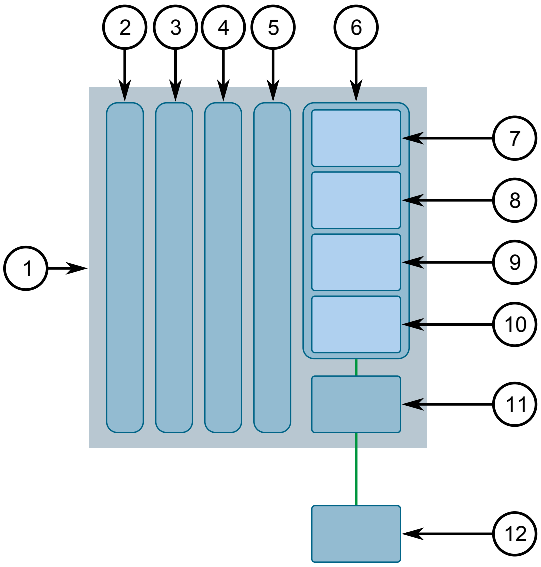


Figure 4: Application Architecture

1. Linux® (Debian) Operating System or RUGGEDCOM ROX II Operating System **2.** RUGGEDCOM ELAN Web Interface (EWI) **3.** Protocol Router **4.** IP Bridge (Optional) **5.** IP Aliasing (Optional) **6.** Telemetry Integration Environment (TIE) **7.** RUGGEDCOM REFLEX (HMI) **8.** Automatic File Manager **9.** Protocol Server (Host) **10.** Protocol Server (Client) **11.** PostgreSQL Database **12.** Maestro

CONTENTS

Section 1.4.1

Telemetry Integrated Environment (TIE)

The Telemetry Integrated Environment (TIE) is a real-time database engine that facilitates communication between hosts and remote devices that use incompatible protocols. It retrieves data autonomously from SCADA devices and makes it available to SCADA hosts, non-SCADA hosts, and other real-time acquisition systems.

While collecting and translating data from substation devices, TIE also features diagnostics, error reporting, communication statistics, and user maintenance access.

Section 1.4.2

Protocol Router

The Protocol Router routes SCADA messages between external clients/masters and external servers. It is concerned only with reading source and destination addresses in messages, as opposed to the actual payload.

Existing solutions for managing DNP communications in a networked environment add latency to communications, require extensive configuration effort to commission, and to re-configure as the network grows and changes. The Protocol Router, however, offers a seamless communications network.

›› Concurrent Access

The Protocol Router can manage access to a single IED from multiple hosts/clients and multiple servers (or VRTUs or slaves) simultaneously.

Because the Protocol Router is protocol-aware, sequence sensitive commands such as Select Before Operate (SBO) can be reliably executed without disruption from another host.

›› Address Masquerading

A number of address contention issues may arise when connecting legacy devices to complex networks with multiple or redundant hosts. Address masquerading allows the Routers to permit these devices to communicate with all required hosts, without contention.

›› Redundant Host Support (Listen Clusters)

Protocol routers allow a redundant host to listen (eavesdrop) to traffic to/from the primary host, so redundant hosts (Masters) can keep their database synchronized in case the primary Master fails.

›› Multi-Connection

Protocol servers configured as listen servers can support multiple connections.

›› Grouping IEDs/RTUs

A single protocol client interface could communicate with multiple remote devices. It allows multiple remote IEDs/ RTUs to communicate via a single protocol client connection in case the IED/RTU had multiple SCADA addresses.

›› Encryption

DNP communications may use SSL/TLS encrypted.

Section 1.4.3

Combining the Protocol Router with TIE

When DNP Masters need to communicate with non-DNP Remote IEDs and RTUs, TIE and the Protocol Router can provide the solution.

DNP 3.0 server devices configured via Maestro act as Virtual Remote Terminal Units (VRTUs) in TIE, which appear to the Protocol Router as regular IEDs or RTUs communicating using the DNP 3.0 protocol. Actual SCADA servers (e.g. IEDS or RTUs), internal interfaces/channels and address translations are hidden from view.

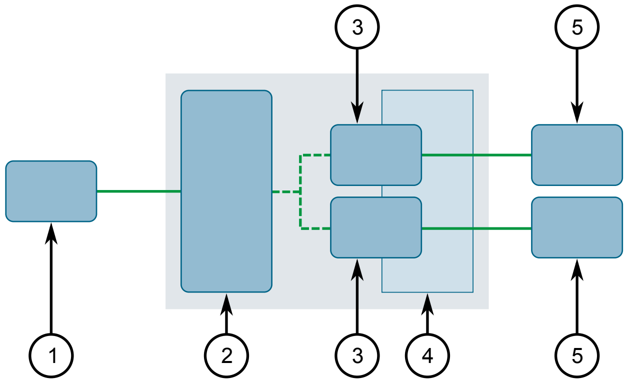


Figure 5: The Protocol Router Communicating with VRTUs

1. DNP 3.0 Master **2.** Protocol Router **3.** VRTU **4.** TIE **5.** IEDs/RTUs

Each VRTU can be configured as a data concentrator, programmed to communicate with one or many SCADA servers. A SCADA server may have its points mapped to multiple VRTUs, allowing multiple masters to independently send/receive data from the same SCADA server.

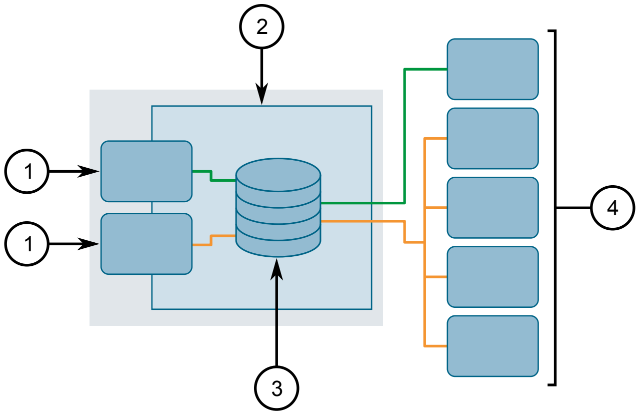


Figure 6: One-to-One and One-to-Many Communication

1. VRTU **2.** TIE **3.** TIE Database **4.** IEDs/RTUs

Section 1.4.4

Redundancy

RUGGEDCOM ELAN offers redundancy through IP aliasing and listen clusters.

IP aliasing allows two RUGGEDCOM ELAN servers to share the same Virtual IP (VIP) address. Should the primary RUGGEDCOM ELAN server fail, the previously inactive secondary RUGGEDCOM ELAN server seamlessly takes over.

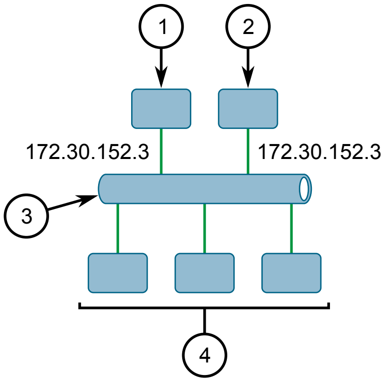


Figure 7: IP Aliasing

1. Active RUGGEDCOM ELAN Server **2.** Standby RUGGEDCOM ELAN Server **3.** LAN **4.** IEDs/RTUs

Protocol servers may be assigned to a listen cluster via the Protocol Router. Multiple clients (Masters) connected to different protocol servers are assigned the same listen cluster identifier. This allows clients belonging to the same cluster to receive the same messages from a VRTU.

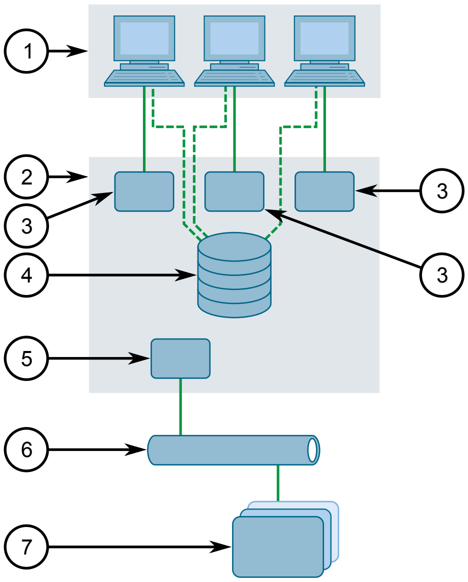


Figure 8: Listen Clusters

1. Clients (Masters) in Listen Cluster **2.** TIE **3.** Protocol Server **4.** TIE Database **5.** Protocol Client **6.** LAN **7.** IEDs/RTUs

Section 1.4.5

ELAN Listener (RUGGEDCOM APE Only)

RUGGEDCOM ELAN's ELAN Listener is a feature available only for the RUGGEDCOM APE module. It enables one or more client devices to listen to incoming TCP communications and copy specific packets to an RUGGEDCOM ELAN server with ELAN Listener enabled. Packets are converted to UDP messages upon capture and are chosen based on filters defined by the administrator.

ELAN Listener is designed for scenarios where specific SCADA data needs to be monitored by more than one control center. It allows users to mirror the data without significantly changing the existing network configuration. For more information, refer to Chapter 5, *Using ELAN Listener* .

IMPORTANT!
The ELAN Listener feature must be purchased separately and is not included in the standard RUGGEDCOM ELAN installation. For information about ordering ELAN Listener, contact a Siemens Sales representative.

Section 1.5

Best Practices

When installing/using a RUGGEDCOM ELAN server or Maestro, consider the following best practices:

- Backup Maestro's project database regularly and store it externally. For more information, refer to Section 4.5.5, “Exporting/Importing the Project Database” .
- Use only the recommended version of Java with Maestro.
- Use only the version of Maestro compatible with the running version of RUGGEDCOM ELAN. Undefined behavior could corrupt the database, otherwise.

Section 1.6

Default Usernames and Passwords

The following default passwords are pre-configured on the device for each access mode:

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, change the default passwords before commissioning the device.

NOTE
A default password does not exist for Maintenance mode.

Mode	Username	Password
Service	root	admin

2 Installing/Updating RUGGEDCOM ELAN

RUGGEDCOM ELAN can be run from a variety of platforms:

- third-party server or tower/desktop
- virtual machine
- RUGGEDCOM APE (Application Processing Engine) module
- RUGGEDCOM RX1400
- RUGGEDCOM RX1500 Series devices

In the case of RUGGEDCOM RX1400 and RUGGEDCOM RX1500 Series devices, RUGGEDCOM ELAN is installed as an application. Applications are special add-ons that extend the functionality of RUGGEDCOM ROX II.

> **IMPORTANT!**
> *The RUGGEDCOM ELAN application for RUGGEDCOM ROX II comes pre-installed and must be ordered in advance. It cannot be added to an existing RUGGEDCOM RX1500 Series device.*

For all other platforms, the following minimum hardware and software requirements must be met:

Platform	Scale	Operating System	CPU	Minimum Available RAM	Minimum Available Memory
Server	Large[a]	32- or 64-bit Linux Debian 7.0 (Wheezy)	4x Cores	512 MB	2 GB
Server with Virtual Machine		—	Multi Cores		
Virtual Machine		32- or 64-bit Linux Debian 7.0 (Wheezy)	4x Cores		
Tower/Desktop PC with Virtual Machine	Small/Medium[b]	32- or 64-bit Linux Debian 7.0 (Wheezy)	Multi Cores		
Virtual Machine		32- or 64-bit Linux Debian 7.0 (Wheezy)	4x Cores		
RUGGEDCOM APE		32--bit Linux Debian 7.0 (Wheezy)	—	—	—

[a] *Up to 1000 devices.*

[b] *Up to 100 devices.*

For assistance in choosing the proper platform, contact a Siemens Sales representative or Siemens Customer Support.

CONTENTS

- Section 2.3, “Installing Maestro”

Section 2.1

Installing a RUGGEDCOM ELAN Server

To install a RUGGEDCOM ELAN server, do the following:

›› RUGGEDCOM RX1400 Device

RUGGEDCOM ELAN is installed on RUGGEDCOM RX1400 devices as an application. For more information about installing applications, refer to the *RUGGEDCOM ROX II User Guide* for the device.

›› RUGGEDCOM RX1500 Device

The RUGGEDCOM ELAN application for RUGGEDCOM ROX II comes pre-installed and must be ordered in advance. It cannot be added to an existing RUGGEDCOM RX1500 Series device.

›› Server, Tower/Desktop, Virtual Machine or RUGGEDCOM APE

1. Make sure the platform has access to the Internet.
2. Log in to the server, tower/desktop, virtual machine or RUGGEDCOM APE as the root user.
3. Using vi, open the file `/etc/apt/sources.list` and add the following line:

   ```
   deb {uri} {distribution} {component}
   ```

   Where:

   - `{uri}` is the URL for the repository, typically in the form of `https://{server}/{repository_path}/`
   - `{distribution}` is the name of the RUGGEDCOM ELAN distribution
   - `{component}` is the name of the directory that contains the binary-{arch} directories, such as *main*
4. Save and close the file.
5. [Optional] Update all third-party packages by typing:

   ```
   apt-get update
   apt-get upgrade
   ```
6. Install the RUGGEDCOM ELAN server by typing:

   ```
   apt-get install elan-master
   ```
7. Verify the installation by typing:

   ```
   dpkg -l | grep elan
   ```

   This command lists the installed packages and their current states. For example:

   ```
   rc elan-addresslib  8.05.00 eLAN Address Libraries
   ii elan-afm   8.05.02 eLAN Automatic File Manager
   ir elan-master  8.05.00 eLAN Master Package
   ```

The first column indicates the status of the package, where *ii* indicates a successful installation, *rc* indicates a configuration error, and *ir* indicates the package is broken. Any packages that did not install properly need to be reinstalled. For more information, refer to Section 2.2, “Reinstalling a RUGGEDCOM ELAN Package” .

8. Add one or more database users. For more information, refer to Section 3.11.1, “Adding/Deleting a Database User” .
9. Update the EWI HTTPS and SCADA communication certificates. For more information, refer to Section 3.10, “Managing SSL Certificates” .
10. [Optional] Install feature keys to add features, such as TIE, Protocol Router, and SCADA protocols. For more information, refer to Section 3.9, “Managing ELAN Feature Keys” .

Section 2.2

Reinstalling a RUGGEDCOM ELAN Package

To reinstall a RUGGEDCOM ELAN package that failed to install properly, do the following:

1. Determine the name of the package by typing:

   ```
   dpkg -l | grep elan
   ```

   This command lists the installed packages and their current states. For example:

   ```
   rc elan-addresslib  8.05.00 eLAN Address Libraries
   ii elan-afm   8.05.02 eLAN Automatic File Manager
   ir elan-master  8.05.00 eLAN Master Package
   ```

   The second column indicates the name of the package.

2. Reinstall the package by typing:

   ```
   apt-get --reinstall install  name
   ```

   Where:

   - *name* is the name of the package

3. Verify the package installed correctly by repeating step Step 1 .

   The first column indicates the status of the package, where *ii* indicates a successful installation, *rc* indicates a configuration error, and *ir* indicates the package is broken.

Section 2.3

Installing Maestro

To install Maestro on a workstation running Windows, do the following:

> **NOTE**
> *Maestro v2.5.x is compatible with RUGGEDCOM ELAN 8.5.*

1. Make sure Java SE (Standard Edition) 6 is installed.
2. Obtain the Maestro software installation file from Siemens Customer Support.
3. Double-click the *.msi file. The installation wizard appears.

4. Follow the on-screen instructions to install Maestro.
5. Add a unique user to the PostgreSQL database. For more information, refer to Section 3.11.1, "Adding/Deleting a Database User" .

3 Using EWI

The RUGGEDCOM ELAN Web Interface (EWI) is the Web-based interface for the RUGGEDCOM ELAN server. It is used to view information about the server, SCADA data polled by TIE, connection information for the Protocol Router, redundancy information, and logs. It also includes tools for managing RUGGEDCOM ELAN feature keys, managing security certificates, and capturing support logs for Siemens Customer Support.

CONTENTS

Section 3.1

Logging In/Out

To log in or out of the RUGGEDCOM ELAN Web Interface (EWI), do the following:

›› Logging In

> **NOTE**
> *If the IP address for the RUGGEDCOM ELAN server is not known, log in to the CLI via SSH as the root user and issue the* **`ifconfig`** *command to display the IP address.*

1. Launch a Web browser and access the RUGGEDCOM ELAN server at its IP address.

   > **NOTE**
   > *If the RUGGEDCOM ELAN server is on a RUGGEDCOM device running RUGGEDCOM ROX II (e.g. RUGGEDCOM RX1400, RUGGEDCOM RX1500, etc.), access the server at* `https://{ip-address}/elan`*, where* ***{ip-address}*** *is the IP address of the RUGGEDCOM ELAN device.*

   The **Login** form appears.

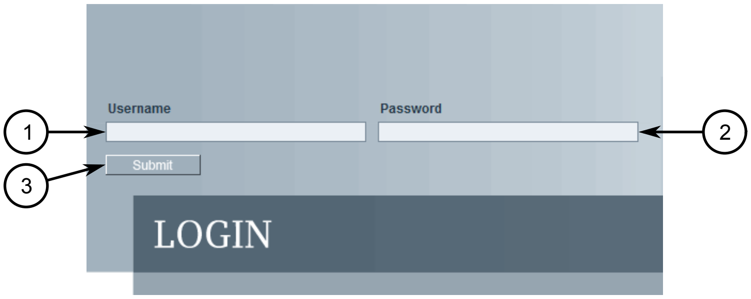


Figure 9: RUGGEDCOM ELAN Login Form

1. Username Box **2.** Password Box **3.** Submit Button

NOTE
RUGGEDCOM ELAN features two default user accounts: ***root*** *and* ***elanuser***. *Additional user accounts can be added. For information about adding user accounts, refer to Section 3.8.2, "Adding/Deleting a User" .*

2. In the **Username** field, type the user name.

NOTE
If a unique password has not been configured, use the factory default password. For more information, refer to Section 1.6, "Default Usernames and Passwords" .

3. In the **Password** field, type the password associated with the user name.
4. Click **Submit**. The **Overview** screen appears.

Logging Out

Log out of EWI by clicking the **Logout** link in top corner of the user interface.

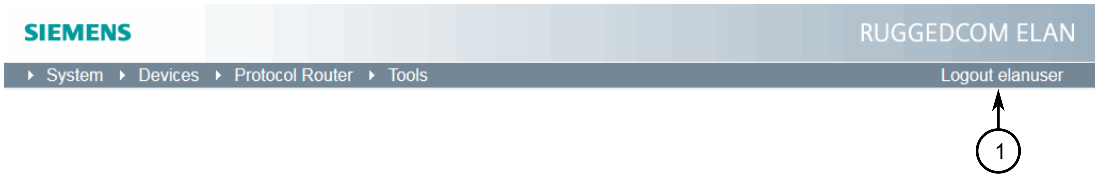


Figure 10: Logout Link

1. Logout Link

Section 3.2

Using the ELAN Web Interface

The RUGGEDCOM ELAN Web Interface (EWI) is the primary interface for each RUGGEDCOM ELAN server. It allows users to monitor server activities, troubleshoot issues, manage security certificates, and manage feature keys.

Use the menu bar to access the various screens available:

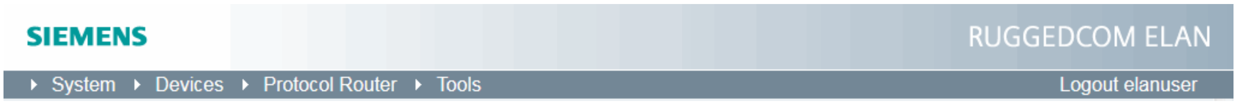


Figure 11: Menu Bar

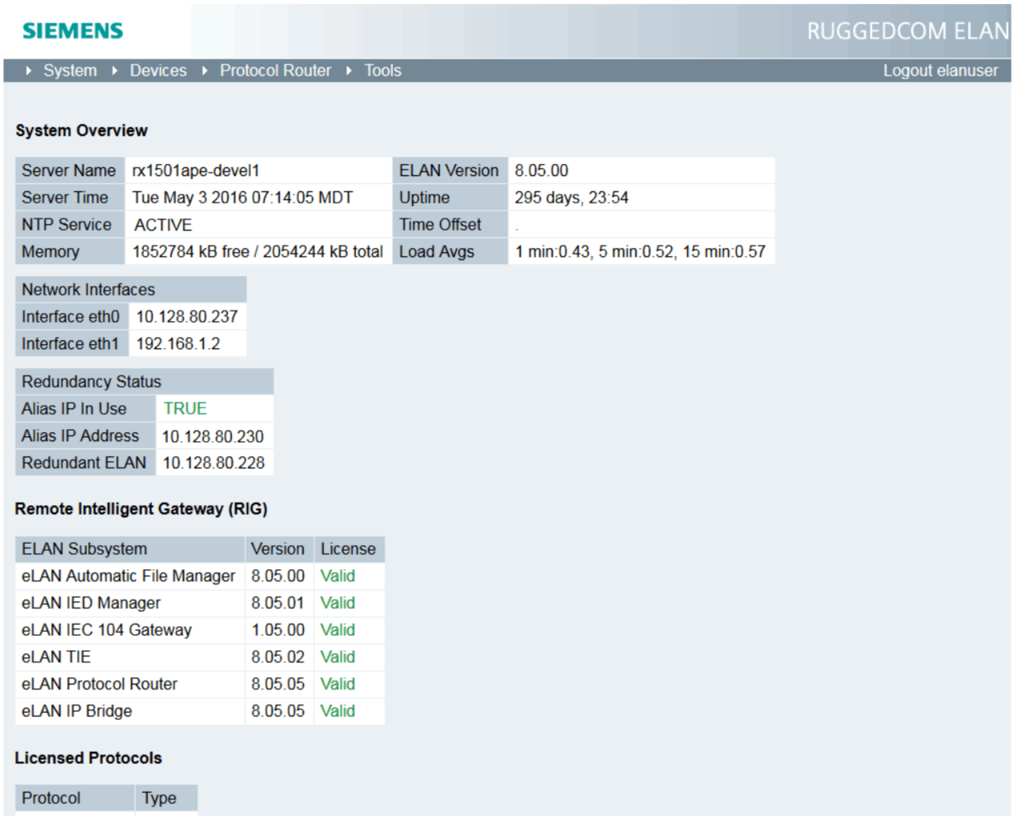
- **System** – Provides access to important system information, such as the status of the server, hardware monitoring, and system logs
- **Devices** – Provides details about client and server devices configured within RUGGEDCOM ELAN.
- **Protocol Router** – Provides details about routes, routing paths, and routing processes configured within RUGGEDCOM ELAN's Protocol Router.
- **Tools** – Provides details about internal data, feature keys, SSL certificates (non-ROX II systems only), licensing, and Siemens's software security disclaimer.

Section 3.3

Determining the Overall Status

To determine the overall status of the RUGGEDCOM ELAN server, visit the Overview screen in EWI by doing the following:

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **System** and then click **Overview**. The **Overview** screen appears.



System Overview

Server Name	rx1501ape-devel1	ELAN Version	8.05.00
Server Time	Tue May 3 2016 07:14:05 MDT	Uptime	295 days, 23:54
NTP Service	ACTIVE	Time Offset	-
Memory	1852784 kB free / 2054244 kB total	Load Avgs	1 min:0.43, 5 min:0.52, 15 min:0.57

Network Interfaces	
Interface eth0	10.128.80.237
Interface eth1	192.168.1.2

Redundancy Status	
Alias IP In Use	TRUE
Alias IP Address	10.128.80.230
Redundant ELAN	10.128.80.228

Remote Intelligent Gateway (RIG)

ELAN Subsystem	Version	License
eLAN Automatic File Manager	8.05.00	Valid
eLAN IED Manager	8.05.01	Valid
eLAN IEC 104 Gateway	1.05.00	Valid
eLAN TIE	8.05.02	Valid
eLAN Protocol Router	8.05.05	Valid
eLAN IP Bridge	8.05.05	Valid

Licensed Protocols

Protocol	Type

Figure 12: Overview Screen

The **Overview** screen provides a general overview of the server. Information is divided into three categories:

System Overview

The **System Overview** section details the following information about the RUGGEDCOM ELAN server (as applicable):

- **Server Name** – The user-defined name assigned to the server.
- **Server Time** – The current time.
- **NTP Service** – The current status of the Network Time Protocol (NTP) service.
- **Memory** – The total amount of memory available and the amount currently in use.
- **ELAN Version** – The version of ELAN installed on the server.
- **Uptime** – The amount of time the server has been consistently operational.
- **Time Offset** – The current time source and time delay in seconds (s).
- **Load Avgs** – The number of processes in the system run queue averaged over three periods of time: 1 minute, 5 minutes and 15 minutes.
- **Interface eth0** – The IP address of the server.
- **Interface ethX** – The Ethernet port(s) used by the server.
- **Alias IP In Use** – When *TRUE* an IP alias in use.

- **Alias IP Address** – The IP address used as an alias.
- **Redundant ELAN** – The IP address of the standby RUGGEDCOM ELAN server.

›› Front End Processor (FEP), Universal Data Gateway (UDG), Remote Intelligent Gateway (RIG) or Substation Communication Server (SCS)

While the title is dependent on the type of RUGGEDCOM ELAN installed, this section details the status of primary subsystems.

›› Licensed Protocols

Licensed Protocols lists the protocols by the RUGGEDCOM ELAN server.

Section 3.4

Accessing the CLI

To access the Command Line Interface (CLI), do one of the following:

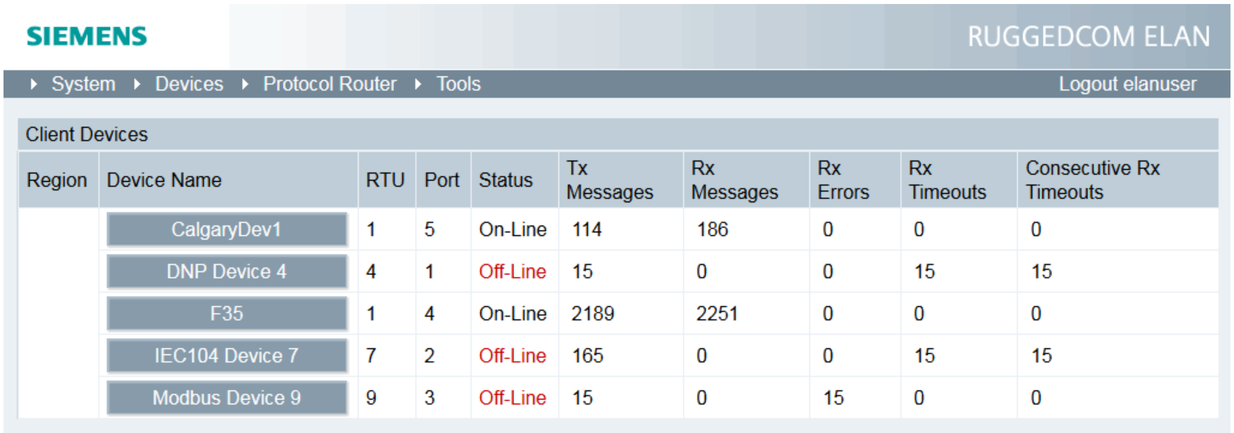
- For **servers** or **virtual machines**, use SSH
- For **RUGGEDCOM APE**, refer to the *RUGGEDCOM APE Developer Guide*
- For **RUGGEDCOM RX1400** or **RUGGEDCOM RX1500 series** devices, refer to the *RUGGEDCOM ROX II User Guide for the device*

Section 3.5

Viewing the Status of Devices

To view the status of client and server devices RUGGEDCOM ELAN communicates with, do the following:

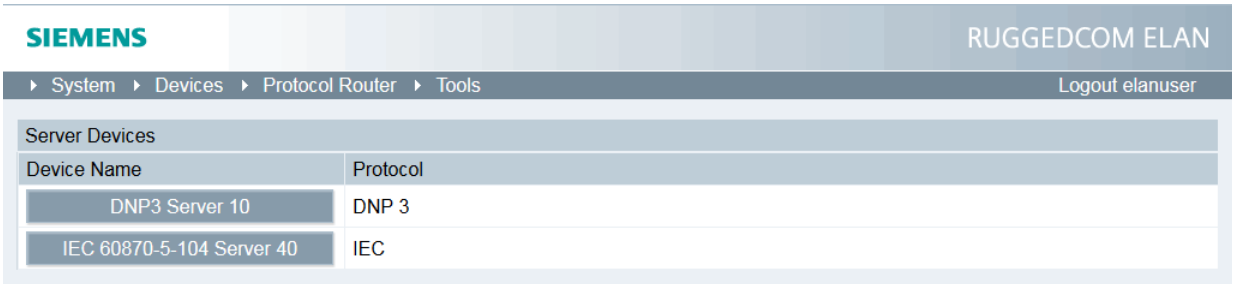
1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **Devices** and then click either **Client Devices** or **Server Devices**. A table listing the applicable devices is displayed.



Client Devices

Region	Device Name	RTU	Port	Status	Tx Messages	Rx Messages	Rx Errors	Rx Timeouts	Consecutive Rx Timeouts
	CalgaryDev1	1	5	On-Line	114	186	0	0	0
	DNP Device 4	4	1	Off-Line	15	0	0	15	15
	F35	1	4	On-Line	2189	2251	0	0	0
	IEC104 Device 7	7	2	Off-Line	165	0	0	15	15
	Modbus Device 9	9	3	Off-Line	15	0	15	0	0

Figure 13: Devices Screen – Client Devices

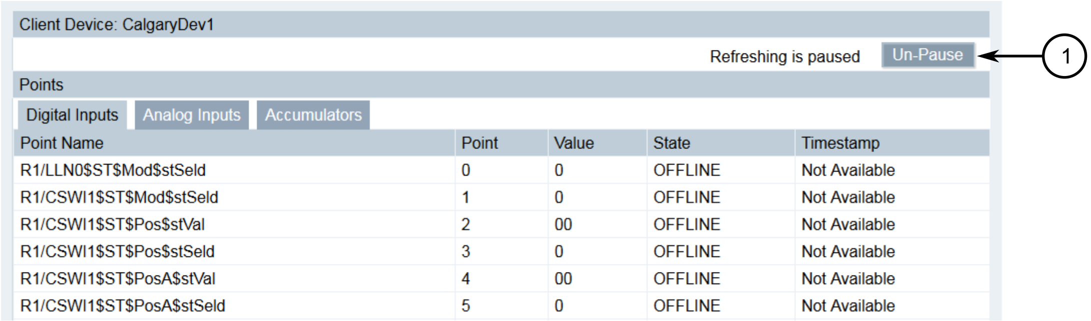


Server Devices

Device Name	Protocol
DNP3 Server 10	DNP 3
IEC 60870-5-104 Server 40	IEC

Figure 14: Devices Screen – Server Devices

3. [Optional] To view details information about a specific device, click the device name. A dialog box appears detailing the available inputs and accumulators on separate tabs.



Client Device: CalgaryDev1

Refreshing is paused

Points

Point Name	Point	Value	State	Timestamp
R1/LLN0$ST$Mod$stSeld	0	0	OFFLINE	Not Available
R1/CSWI1$ST$Mod$stSeld	1	0	OFFLINE	Not Available
R1/CSWI1$ST$Pos$stVal	2	00	OFFLINE	Not Available
R1/CSWI1$ST$Pos$stSeld	3	0	OFFLINE	Not Available
R1/CSWI1$ST$PosA$stVal	4	00	OFFLINE	Not Available
R1/CSWI1$ST$PosA$stSeld	5	0	OFFLINE	Not Available

Figure 15: Devices Dialog Box (Client Devices)

1. Un-Pause/Pause Button

IMPORTANT!
Degraded performance may be experienced if the auto-refresh features is enabled for a heavily loaded system. Only enable auto-refresh when needed.

4. [Optional] Click **Un-Pause** to have the dialog box refresh the data every 10 seconds.

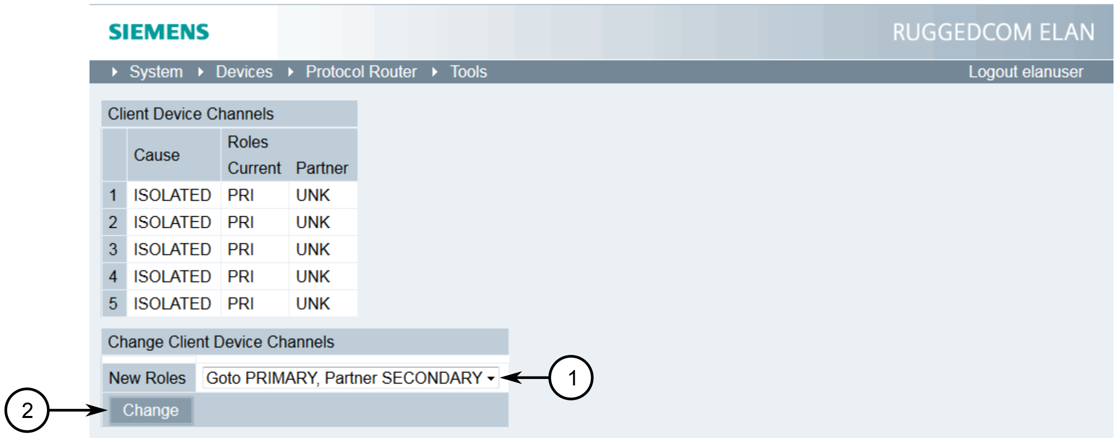
Section 3.6

Switching Secondary and Primary RUGGEDCOM ELAN Servers (FEP Only)

For RUGGEDCOM ELAN servers running as Front End Processors (FEPs), a redundant RUGGEDCOM ELAN server can be switched to be the primary server should the current primary server require maintenance.

To change the role of a RUGGEDCOM ELAN server in a server partnership, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, "Logging In/Out" .
2. On the menu bar, point to **Devices** and then click **Client Device Channels**. The **Client Device Channels** screen appears.



Client Device Channels

	Cause	Roles	
		Current	Partner
1	ISOLATED	PRI	UNK
2	ISOLATED	PRI	UNK
3	ISOLATED	PRI	UNK
4	ISOLATED	PRI	UNK
5	ISOLATED	PRI	UNK

Change Client Device Channels

New Roles: Goto PRIMARY, Partner SECONDARY

Change

Figure 16: Client Device Channels

1. New Roles List **2.** Change Button

3. Under **Change Client Device Channels**, click **New Roles** and select one of the following options:
   - `Goto PRIMARY, Partner SECONDARY` – Changes the current RUGGEDCOM ELAN server to the primary server.
   - `Goto SECONDARY, Partner PRIMARY` – Changes the current RUGGEDCOM ELAN server to the secondary server.
   - `Automatic Switching` – The role of the current RUGGEDCOM ELAN is based on the availability of its partner.
4. Click **Change**.

Section 3.7

Managing Logs in EWI

This section describes how to view and capture logs generated by EWI.

CONTENTS

Section 3.7.1

Viewing System Logs

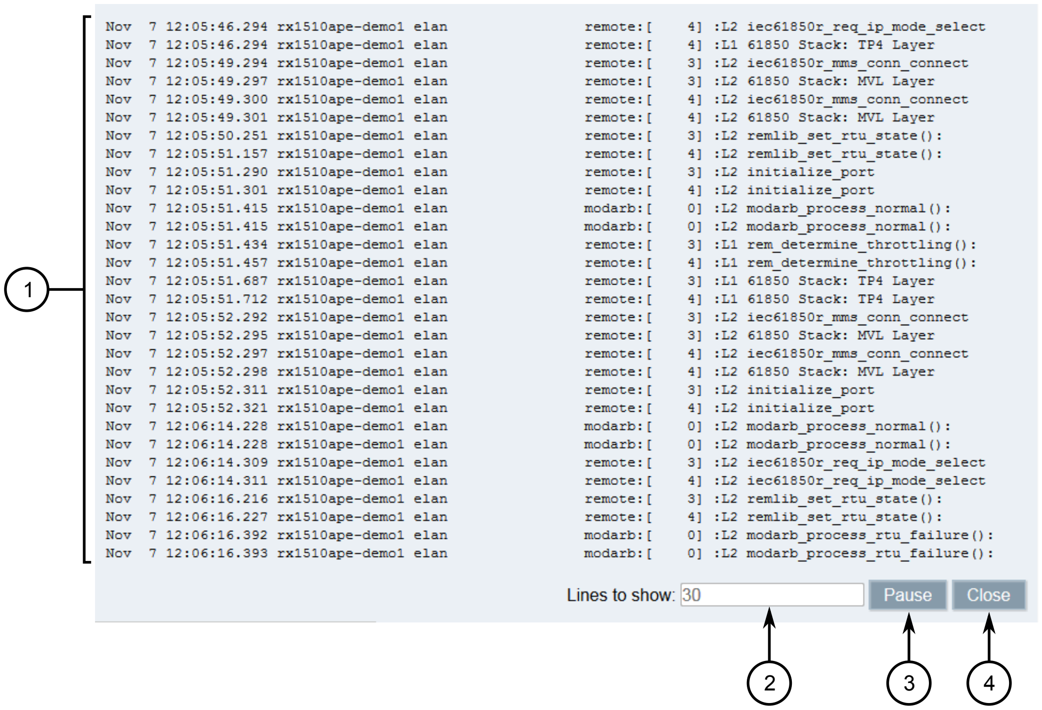
The following system logs are available via EWI:

- **Runtime Log** – A log of all RUGGEDCOM ELAN processes running during operation. This log is useful in identifying any runtime errors or warnings that occur during runtime.
- **Startup Log** – A log of all system events that occur during the startup and initialization of RUGGEDCOM ELAN. This log is useful for identifying errors in a configuration uploaded by Maestro.

›› Viewing the Runtime Log

To view the Runtime Log, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **System** and then click **Runtime Log**. The log is displayed in a new browser window.



```
Nov  7 12:05:46.294 rx1510ape-demo1 elan                remote:[    4] :L2 iec61850r_req_ip_mode_select
Nov  7 12:05:46.294 rx1510ape-demo1 elan                remote:[    4] :L1 61850 Stack: TP4 Layer
Nov  7 12:05:49.294 rx1510ape-demo1 elan                remote:[    3] :L2 iec61850r_mms_conn_connect
Nov  7 12:05:49.297 rx1510ape-demo1 elan                remote:[    3] :L2 61850 Stack: MVL Layer
Nov  7 12:05:49.300 rx1510ape-demo1 elan                remote:[    4] :L2 iec61850r_mms_conn_connect
Nov  7 12:05:49.301 rx1510ape-demo1 elan                remote:[    4] :L2 61850 Stack: MVL Layer
Nov  7 12:05:50.251 rx1510ape-demo1 elan                remote:[    3] :L2 remlib_set_rtu_state():
Nov  7 12:05:51.157 rx1510ape-demo1 elan                remote:[    4] :L2 remlib_set_rtu_state():
Nov  7 12:05:51.290 rx1510ape-demo1 elan                remote:[    3] :L2 initialize_port
Nov  7 12:05:51.301 rx1510ape-demo1 elan                remote:[    4] :L2 initialize_port
Nov  7 12:05:51.415 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_normal():
Nov  7 12:05:51.415 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_normal():
Nov  7 12:05:51.434 rx1510ape-demo1 elan                remote:[    3] :L1 rem_determine_throttling():
Nov  7 12:05:51.457 rx1510ape-demo1 elan                remote:[    4] :L1 rem_determine_throttling():
Nov  7 12:05:51.687 rx1510ape-demo1 elan                remote:[    3] :L1 61850 Stack: TP4 Layer
Nov  7 12:05:51.712 rx1510ape-demo1 elan                remote:[    4] :L1 61850 Stack: TP4 Layer
Nov  7 12:05:52.292 rx1510ape-demo1 elan                remote:[    3] :L2 iec61850r_mms_conn_connect
Nov  7 12:05:52.295 rx1510ape-demo1 elan                remote:[    3] :L2 61850 Stack: MVL Layer
Nov  7 12:05:52.297 rx1510ape-demo1 elan                remote:[    4] :L2 iec61850r_mms_conn_connect
Nov  7 12:05:52.298 rx1510ape-demo1 elan                remote:[    4] :L2 61850 Stack: MVL Layer
Nov  7 12:05:52.311 rx1510ape-demo1 elan                remote:[    3] :L2 initialize_port
Nov  7 12:05:52.321 rx1510ape-demo1 elan                remote:[    4] :L2 initialize_port
Nov  7 12:06:14.228 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_normal():
Nov  7 12:06:14.228 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_normal():
Nov  7 12:06:14.309 rx1510ape-demo1 elan                remote:[    3] :L2 iec61850r_req_ip_mode_select
Nov  7 12:06:14.311 rx1510ape-demo1 elan                remote:[    4] :L2 iec61850r_req_ip_mode_select
Nov  7 12:06:16.216 rx1510ape-demo1 elan                remote:[    3] :L2 remlib_set_rtu_state():
Nov  7 12:06:16.227 rx1510ape-demo1 elan                remote:[    4] :L2 remlib_set_rtu_state():
Nov  7 12:06:16.392 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_rtu_failure():
Nov  7 12:06:16.393 rx1510ape-demo1 elan                modarb:[    0] :L2 modarb_process_rtu_failure():
```

Lines to show: 30

Figure 17: Runtime Log (Example)

1. Log Information **2.** Lines to Show Box **3.** Pause/Start Button **4.** Close Button

By default, only the last 30 lines of the log are shown. To increase/decrease the number of lines shown, click **Pause**, enter a new number in the **Lines to show** box, and then click **Start**.

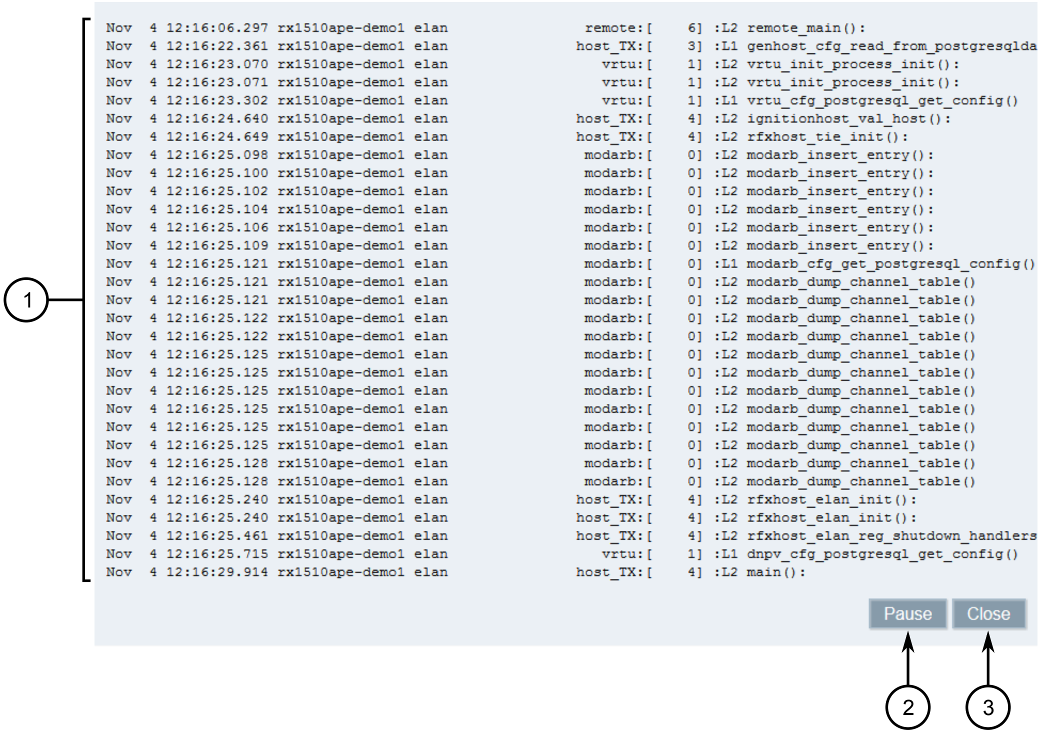
The log refreshes automatically every 5 seconds. To stop the log from refreshing, click **Pause**. To continue refreshing the log, click **Start**.

To close the log, click **Close**.

›› Viewing the Startup Log

To view the Startup Log, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **System** and then click **Startup Log**. The log is displayed in a new browser window.



```
Nov  4 12:16:06.297 rx1510ape-demo1 elan              remote:[    6] :L2 remote_main():
Nov  4 12:16:22.361 rx1510ape-demo1 elan             host_TX:[    3] :L1 genhost_cfg_read_from_postgresqlda
Nov  4 12:16:23.070 rx1510ape-demo1 elan                vrtu:[    1] :L2 vrtu_init_process_init():
Nov  4 12:16:23.071 rx1510ape-demo1 elan                vrtu:[    1] :L2 vrtu_init_process_init():
Nov  4 12:16:23.302 rx1510ape-demo1 elan                vrtu:[    1] :L1 vrtu_cfg_postgresql_get_config()
Nov  4 12:16:24.640 rx1510ape-demo1 elan             host_TX:[    4] :L2 ignitionhost_val_host():
Nov  4 12:16:24.649 rx1510ape-demo1 elan             host_TX:[    4] :L2 rfxhost_tie_init():
Nov  4 12:16:25.098 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.100 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.102 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.104 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.106 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.109 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_insert_entry():
Nov  4 12:16:25.121 rx1510ape-demo1 elan              modarb:[    0] :L1 modarb_cfg_get_postgresql_config()
Nov  4 12:16:25.121 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.121 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.122 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.122 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.125 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.128 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.128 rx1510ape-demo1 elan              modarb:[    0] :L2 modarb_dump_channel_table()
Nov  4 12:16:25.240 rx1510ape-demo1 elan             host_TX:[    4] :L2 rfxhost_elan_init():
Nov  4 12:16:25.240 rx1510ape-demo1 elan             host_TX:[    4] :L2 rfxhost_elan_init():
Nov  4 12:16:25.461 rx1510ape-demo1 elan             host_TX:[    4] :L2 rfxhost_elan_reg_shutdown_handlers
Nov  4 12:16:25.715 rx1510ape-demo1 elan                vrtu:[    1] :L1 dnpv_cfg_postgresql_get_config()
Nov  4 12:16:29.914 rx1510ape-demo1 elan             host_TX:[    4] :L2 main():
```

Figure 18: Startup Log (Example)

1. Log Information **2.** Pause/Start Button **3.** Close Button

The log refreshes automatically every 15 seconds. To stop the log from refreshing, click **Pause**. To continue refreshing the log, click **Start**.

To close the log, click **Close**.

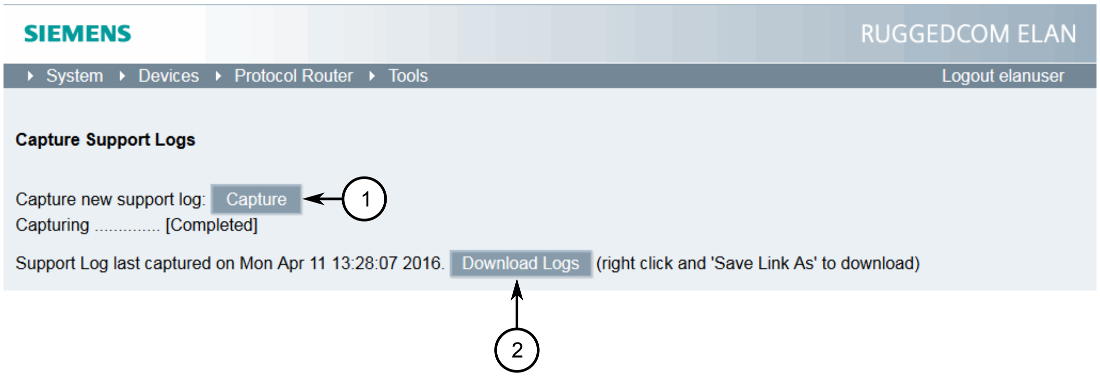
Section 3.7.2

Capturing Support Logs

Support logs may be requested by Siemens Customer Support to help troubleshoot technical issues.

To capture and/or download the latest support log, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, "Logging In/Out" .
2. On the menu bar, point to **System** and then click **Capture Support Logs**. The **Capture Support Logs** screen appears.



Capture Support Logs

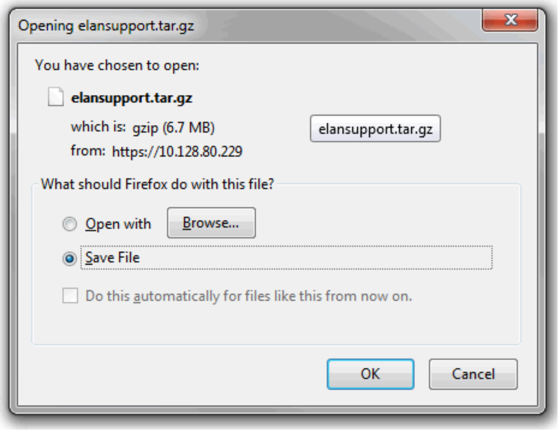
Capture new support log: Capture
Capturing .... [Completed]

Support Log last captured on Mon Apr 11 13:28:07 2016. Download Logs (right click and 'Save Link As' to download)

Figure 19: Capture Support Logs Screen

1. Capture Button **2.** Download Logs

3. Click **Capture** to start capturing the latest support log information. The **Download Logs** button disappears while new support logs are generated. The updated support logs are available when the **Download Logs** button appears.
4. Click **Download Logs**. A dialog box appears.



Opening elansupport.tar.gz

You have chosen to open:

elansupport.tar.gz

which is: gzip (6.7 MB)
from: https://10.128.80.229

elansupport.tar.gz

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

Figure 20: Dialog Box

NOTE
Support logs are provided in a tarball (.tar.gz) file.*

5. Save the file and then send it to Siemens Customer Support.

Section 3.8

Managing Users

Multiple user accounts can be created for accessing the RUGGEDCOM ELAN Web Interface (EWI). By default, all user accounts are authenticated locally. However, RUGGEDCOM ELAN also supports remote authentication using the Kerberos authentication protocol.

NOTE
Remote authentication using Kerberos is only available for non-ROX II systems (e.g. RUGGEDCOM APE, Debian server or virtual machine).

CONTENTS

Section 3.8.1

Configuring Remote Authentication

To remotely authenticate RUGGEDCOM ELAN users using the Kerberos authentication protocol, do the following:

1. Make sure `/etc/krb5.conf` is properly configured and present on the RUGGEDCOM ELAN server.
2. Add each user to `/etc/elan/web/users.allow`. For more information, refer to Section 3.8.2, “Adding/Deleting a User” .

Section 3.8.2

Adding/Deleting a User

To add/delete a user of the RUGGEDCOM ELAN server, do the following:

›› Adding a User

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.

   IMPORTANT!
   Do not create users with the name ***root****. This name is reserved by Linux.*

2. At the command prompt, add the new user by typing:

   ```
   adduser  username
   ```

3. When prompted, enter a strong password for the user. For recommendations, refer to Section 1.1, “Security Recommendations” .

   ```
   Enter new UNIX password:
   Retype new UNIX password:
   passwd: password updated successfully
   ```

4. When prompted, enter more information about the user or press **Enter** to access the default. For example:

```
Full Name []: elan ewi user
Room Number []:
Work Phone []: 555-5555
Home Phone []:
Other []: NOC access
```

5. When prompted, confirm the user's information by typing **`Y`**.
6. Using vi, open the file `/etc/elan/web/users.allow` and add the user name on a new line. For example:

```
# List of users that are allowed to login to ELAN Web interface
# configure each user on a separate line
# Lines start with # will be ignored.
elanuser2
~
~
```

7. Save and close the file.

›› Deleting a User

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
2. Using vi, open the file `/etc/elan/web/users.allow` and either remove the user from the list or place a **#** symbol in front. For example:

```
# List of users that are allowed to login to ELAN Web interface
# configure each user on a separate line
# Lines start with # will be ignored.
elanuser2
#elanuser3
~
~
```

> **IMPORTANT!**
> *Only delete users that were manually added.*

3. Save and close the file.
4. [Optional] Delete the user account fully by typing:

```
userdel  username
```

Section 3.8.3

Changing a User's Password

To change an existing user's password, do the following:

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
2. At the command prompt, type:

```
passwd  username
```

3. When prompted, enter the new password for the user.

```
Enter new UNIX password:
```

```
Retype new UNIX password:
passwd: password updated successfully
```

Section 3.9

Managing ELAN Feature Keys

RUGGEDCOM ELAN can be enhanced with additional features at any time by adding feature levels. Feature levels are encoded in feature keys that can be loaded on the RUGGEDCOM ELAN server. At the time of ordering, a base feature key is encoded into the electronic signature of the server. This feature key is independent of any additional, file-based feature keys that are purchased later on. File-based feature keys are stored in memory and can be transferred from server to server.

> **NOTE**
> *Some RUGGEDCOM ELAN features are only available through the purchase of feature levels. For more information about the available feature levels, refer to the product data sheet for the device available at www.siemens.com/ruggedcom or contact a Siemens Sales representative.*

When ordering feature levels, make sure to provide the serial number for the RUGGEDCOM ELAN server. An upgraded feature key file will be provided that is licensed to the server.

- For non-RUGGEDCOM ROX II systems, the serial number is listed as the **System Serial Number** under ***Tools » ELAN Feature Keys*** in EWI.
- For RUGGEDCOM RX1400 devices, the serial number is listed as the **System Serial Number** under **chassis** in RUGGEDCOM ROX II. For more information, refer to the *RUGGEDCOM ROX II User Guide* for the device.
- For RUGGEDCOM RX1500 Series devices, the serial number is listed under ***chassis » hardware » main*** in RUGGEDCOM ROX II. For more information, refer to the *RUGGEDCOM ROX II User Guide* for the device.

When uploading a new feature key, RUGGEDCOM ELAN evaluates the new file-based feature key and the embedded feature key and enables the most capable feature level described by the keys.

CONTENTS

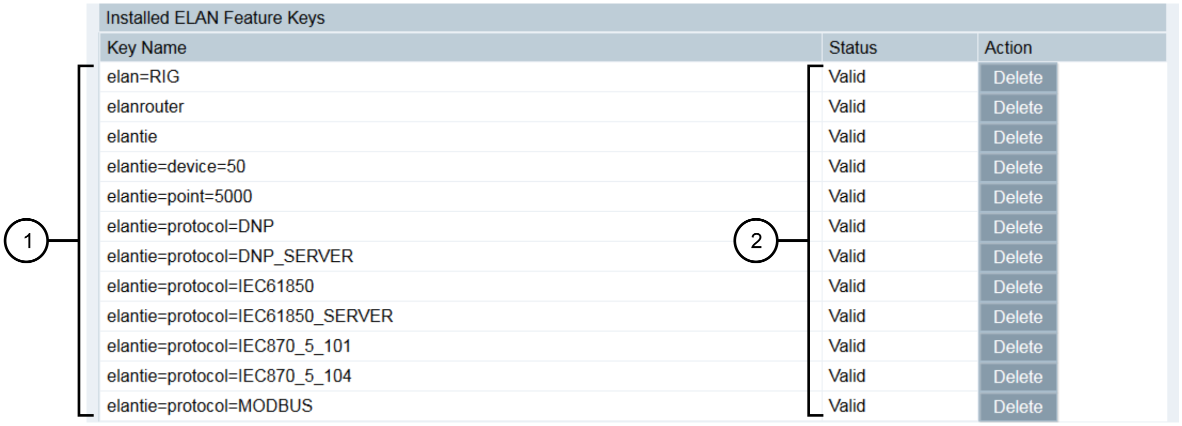
Section 3.9.1

Viewing Installed Feature Keys

To view the feature keys installed on the RUGGEDCOM ELAN server, do the following:

> **NOTE**
> *Only feature keys related to RUGGEDCOM ELAN are listed.*

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **Tools** and then click **ELAN Feature Keys**. The **ELAN Feature Keys** screen appears.



Installed ELAN Feature Keys

Key Name	Status	Action
elan=RIG	Valid	Delete
elanrouter	Valid	Delete
elantie	Valid	Delete
elantie=device=50	Valid	Delete
elantie=point=5000	Valid	Delete
elantie=protocol=DNP	Valid	Delete
elantie=protocol=DNP_SERVER	Valid	Delete
elantie=protocol=IEC61850	Valid	Delete
elantie=protocol=IEC61850_SERVER	Valid	Delete
elantie=protocol=IEC870_5_101	Valid	Delete
elantie=protocol=IEC870_5_104	Valid	Delete
elantie=protocol=MODBUS	Valid	Delete

Figure 21: ELAN Feature Keys Screen

1. Feature Keys **2.** Status

The **Status** column indicates which feature keys are valid.

Status	Description
Demo	The service will run for a fixed time length (2 hours) and then stop, after which manual intervention is required to start the server again.
Valid	The service is running normally.
Invalid	The service is running normally, but configuration downloads from Maestro are not permitted. An invalid feature key will prevent a new configuration from being downloaded if part of the configuration requires that server. If an invalid key is present, messages will be sent to the log file every 10 seconds.

Section 3.9.2

Uploading a Feature Key

To upload a feature key, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, "Logging In/Out" .
2. On the menu bar, point to **Tools** and then click **ELAN Feature Keys**. The **ELAN Feature Keys** screen appears.

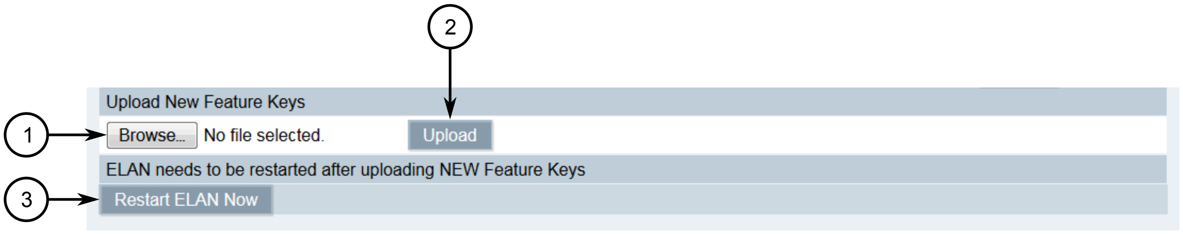


Figure 22: ELAN Feature Keys Screen

1. Browse Button **2.** Upload Button **3.** Restart ELAN Now Button

> **NOTE**
> *Feature keys may be individually packaged in separate files, with each containing a single key, or packaged together in a single tarball (*.tar.gz) file.*

3. Under **Upload New Feature Keys**, click **Browse** and locate the feature key.
4. Click **Upload**. The feature key is uploaded to the RUGGEDCOM ELAN server.

> **IMPORTANT!**
> *ELAN must be restarted after a new feature key is added.*

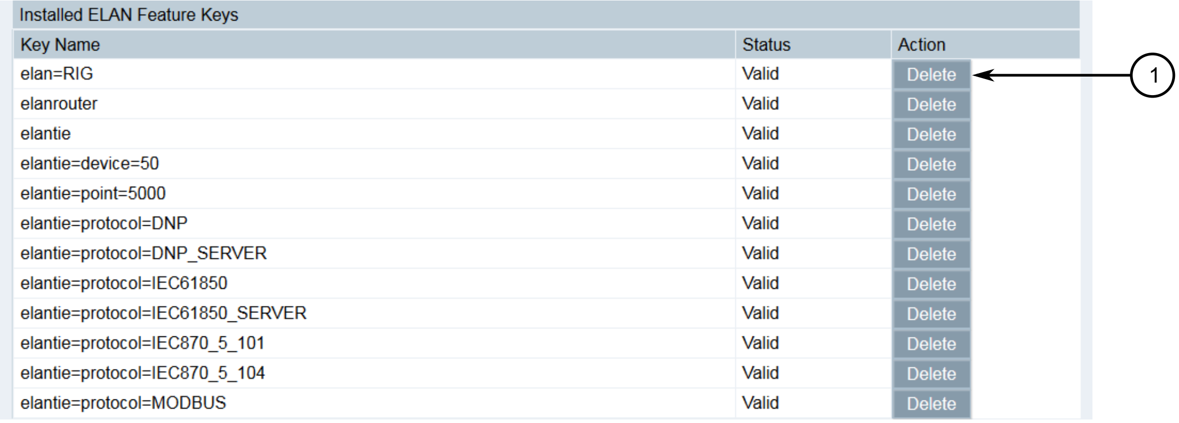
5. Click **Restart ELAN Now** or, if RUGGEDCOM ELAN is running on a RUGGEDCOM device, disable and then enable the RUGGEDCOM ELAN application. For more information about enabling/disabling the RUGGEDCOM ELAN application for RUGGEDCOM ROX II, refer to the *RUGGEDCOM ROX II User Guide* for the device.
6. Review the list of available feature keys to verify the new feature level is available. For more information, refer to Section 3.9.2, “Uploading a Feature Key” .

Section 3.9.3

Deleting a Feature Key

To delete a feature key from the RUGGEDCOM ELAN server, do the following:

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **Tools** and then click **ELAN Feature Keys**. The **ELAN Feature Keys** screen appears.



Installed ELAN Feature Keys

Key Name	Status	Action
elan=RIG	Valid	Delete
elanrouter	Valid	Delete
elantie	Valid	Delete
elantie=device=50	Valid	Delete
elantie=point=5000	Valid	Delete
elantie=protocol=DNP	Valid	Delete
elantie=protocol=DNP_SERVER	Valid	Delete
elantie=protocol=IEC61850	Valid	Delete
elantie=protocol=IEC61850_SERVER	Valid	Delete
elantie=protocol=IEC870_5_101	Valid	Delete
elantie=protocol=IEC870_5_104	Valid	Delete
elantie=protocol=MODBUS	Valid	Delete

Figure 23: ELAN Feature Keys Screen

1. Delete Button

3. Click **Delete** next to the desired feature key. A confirmation dialog box appears.
4. Click **Yes** to delete the feature key, or click **No** to abort.

Section 3.10

Managing SSL Certificates

RUGGEDCOM ELAN uses SSL (Secure Socket Layer) certificates to deliver the ELAN Web Interface (EWI) and for SCADA communications.

> **NOTE**
> *When RUGGEDCOM ELAN is installed as an application on a RUGGEDCOM ROX II device, SSL certificates are managed by RUGGEDCOM ROX II. For information about how to manage SSL certificates in RUGGEDCOM ROX II, refer to the RUGGEDCOM ROX II User Guide.*

CONTENTS

Section 3.10.1

Managing the EWI HTTPS Certificate

The ELAN Web Interface (EWI) uses an SSL certificate (on non-ROX II systems) to deliver encrypted Web pages through HTTPS.

When RUGGEDCOM ELAN is installed or upgraded, a self-signed SSL certificate is automatically generated. This certificate is unique to each instance of RUGGEDCOM ELAN.

To maintain a high level of security, the automatically generated certificate should be replaced before the system is deployed.

CONTENTS

Section 3.10.1.1

Uploading a Certificate with a USB

To upload a certificate directly using a USB flash drive, do the following:

1. Copy the new certificate to a USB flash drive.
2. Plug the drive into the RUGGEDCOM ELAN server. The drive should be mounted automatically.
3. Access the CLI for the RUGGEDCOM ELAN server.
4. Replace the current certificate with the new certificate by typing:

   ```
   cp /mnt/{certificate}  /etc/lighttpd/elan-webinterface.pem
   ```

   Where:

   - *{certificate}* is the path to the new certificate on the USB

5. Restart the Lighttpd Web server by typing:

   ```
   invoke-rc.d lighttpd restart
   ```

Section 3.10.1.2

Uploading a Certificate Remotely

To upload a certificate remotely from a host computer to the RUGGEDCOM ELAN server, do the following:

NOTE
The new certificate must be available on a host computer running Linux for this upload option.

IMPORTANT!
If the certificate has been deleted from the RUGGEDCOM ELAN server before a new certificate has been uploaded, file permissions and user rights must be set. For more information, refer to Step 6 .

1. Using Secure Copy (SCP), copy the new certificate from the host computer to the RUGGEDCOM ELAN server by typing:

   ```
   scp  source   destination
   ```

   Where:

   - *source* is the path to the new certificate on the host computer, including the name of the certificate. For example, */temp/certs/new_certificate.pem*.
   - *destination* is the path to a directory on the RUGGEDCOM ELAN server, including the name of the certificate. For example, *root@10.128.80.123:new_certificate.pem* or *root@10.128.80.123:/root/new_certificate.pem* accesses the RUGGEDCOM ELAN server as the root user and copies the new

certificate to the `/root` directory. Alternatively, *root@10.128.80.123:~/new_certificate.pem* accesses the RUGGEDCOM ELAN server as the root user and copies the new certificate to the user's home directory.

> **NOTE**
> *To retain the name of the certificate, enter the same name in the destination path or exclude it from the path entirely.*

For example:

```
scp /temp/certs/new_certificate.pem operator@10.128.80.123:elan-webinterface.pem
```

2. When prompted, enter the password associated with the user profile.
3. Log in remotely to the RUGGEDCOM ELAN server by typing:

   ```
   ssh -l  user   IP_address
   ```

   Where:

   - *user* is the user profile (e.g. root)
   - *IP_address* is the IP address for the RUGGEDCOM ELAN server
4. [Optional] Backup the current certificate by typing:

   ```
   cp /etc/lighttpd/elan-webinterface.pem /etc/lighttpd/elan-webinterface.pem.bak
   ```
5. Replace the current certificate with the new certificate by typing:

   ```
   cp  destination  /etc/lighttpd/elan-webinterface.pem
   ```

   Where:

   - *destination* is the path to the new certificate on the RUGGEDCOM ELAN server, including the name of the certificate
6. [Optional] If the original certificate was deleted before the new certificate was uploaded, set the file permissions and user rights by typing the following:

   ```
   chmod 740 /etc/lighttpd/elan-webinterface.pem
   chown www-data:www-data /etc/lighttpd/elan-webinterface.pem
   ```
7. Restart the Lighttpd Web server by typing:

   ```
   invoke-rc.d lighttpd restart
   ```

Section 3.10.2

Managing SCADA Communication Certificates

SSL certificates used for SCADA communication can be managed via the ELAN Web Interface (EWI) on non-ROX II systems.

CONTENTS

- Section 3.10.2.4, “Uploading a Certificate via EWI”

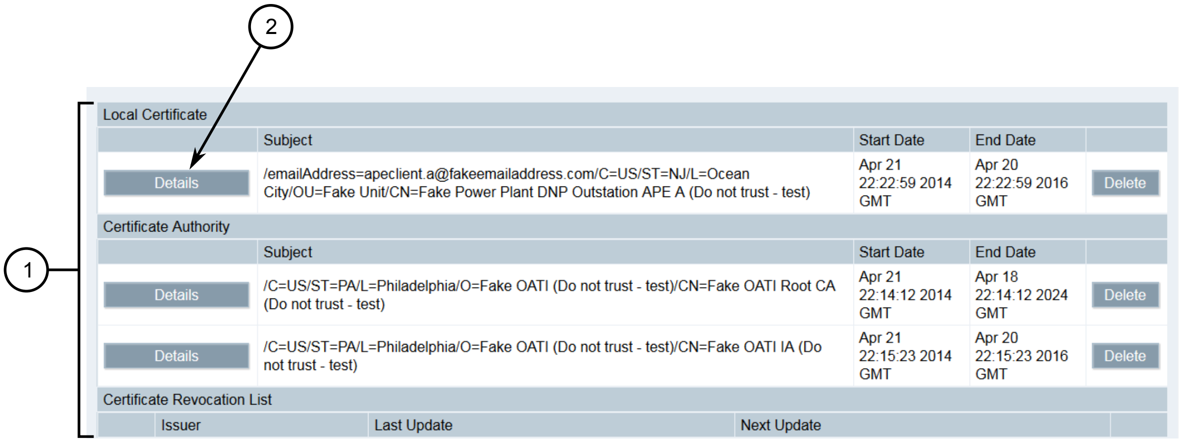
Section 3.10.2.1

Viewing Installed Certificates

To view the certificates installed on the RUGGEDCOM ELAN server, do the following:

> **NOTE**
> *Certificates cannot be viewed in EWI when accessed via ROX II. Certificates are viewed instead via the ROX II Web and CLI interfaces. For more information about viewing certificates via ROX II, refer to the ROX II User Guide for the device.*

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **Tools** and then click **Certificates**. The **Certificates** screen appears.



Local Certificate

	Subject	Start Date	End Date	
Details	/emailAddress=apeclient.a@fakeemailaddress.com/C=US/ST=NJ/L=Ocean City/OU=Fake Unit/CN=Fake Power Plant DNP Outstation APE A (Do not trust - test)	Apr 21 22:22:59 2014 GMT	Apr 20 22:22:59 2016 GMT	Delete

Certificate Authority

	Subject	Start Date	End Date	
Details	/C=US/ST=PA/L=Philadelphia/O=Fake OATI (Do not trust - test)/CN=Fake OATI Root CA (Do not trust - test)	Apr 21 22:14:12 2014 GMT	Apr 18 22:14:12 2024 GMT	Delete
Details	/C=US/ST=PA/L=Philadelphia/O=Fake OATI (Do not trust - test)/CN=Fake OATI IA (Do not trust - test)	Apr 21 22:15:23 2014 GMT	Apr 20 22:15:23 2016 GMT	Delete

Certificate Revocation List

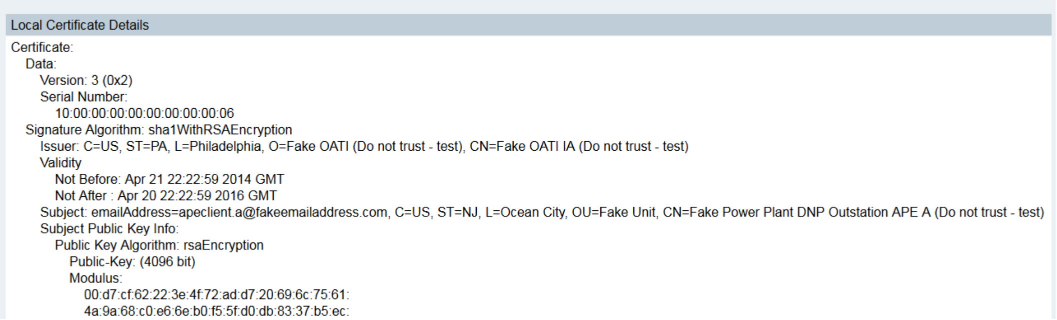
	Issuer	Last Update	Next Update	

Figure 24: Certificates Screen

1. Certificate Information **2.** Details Button

Certificates are organized by Local Certificate, Certificate Authority (CA) and Certificate Revocation Lists (CRLs).

3. [Optional] Click **Details** for the chosen certificate to view complete certificate. The **Local Certificate Details** dialog box appears detailing the issuer, public key, signature algorithms, and more.



```
Local Certificate Details
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         10:00:00:00:00:00:00:00:00:06
   Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=US, ST=PA, L=Philadelphia, O=Fake OATI (Do not trust - test), CN=Fake OATI IA (Do not trust - test)
      Validity
         Not Before: Apr 21 22:22:59 2014 GMT
         Not After : Apr 20 22:22:59 2016 GMT
      Subject: emailAddress=apeclient.a@fakeemailaddress.com, C=US, ST=NJ, L=Ocean City, OU=Fake Unit, CN=Fake Power Plant DNP Outstation APE A (Do not trust - test)
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
               00:d7:cf:62:22:3e:4f:72:ad:d7:20:69:6c:75:61:
               4a:9a:68:c0:e6:6e:b0:f5:5f:d0:db:83:37:b5:ec:
```

Figure 25: Local Certificate Details Dialog Box (Example)

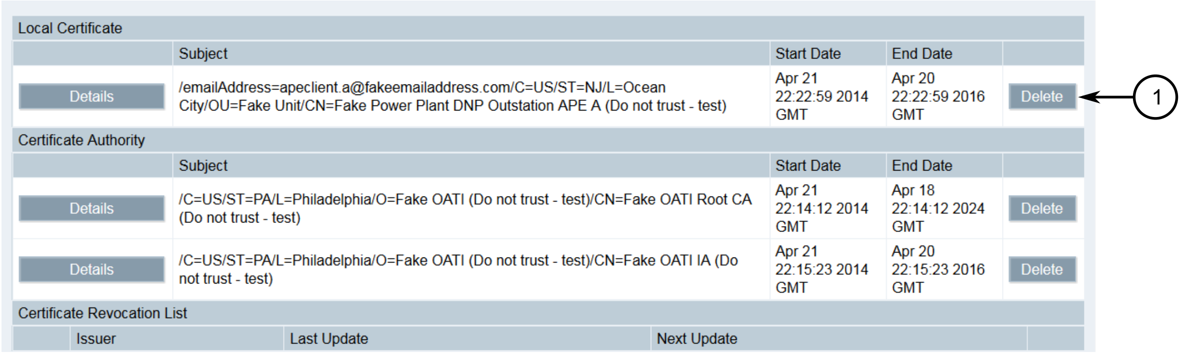
Section 3.10.2.2

Deleting a Certificate

To delete a certificate, do the following:

> **NOTE**
> *For information about how to delete a certificate via ROX II, refer to the ROX II User Guide for the device.*

1. Log in to EWI. For more information, refer to Section 3.1, “Logging In/Out” .
2. On the menu bar, point to **Tools** and then click **Certificates**. The **Certificates** screen appears.



Local Certificate

	Subject	Start Date	End Date	
Details	/emailAddress=apeclient.a@fakeemailaddress.com/C=US/ST=NJ/L=Ocean City/OU=Fake Unit/CN=Fake Power Plant DNP Outstation APE A (Do not trust - test)	Apr 21 22:22:59 2014 GMT	Apr 20 22:22:59 2016 GMT	Delete

Certificate Authority

	Subject	Start Date	End Date	
Details	/C=US/ST=PA/L=Philadelphia/O=Fake OATI (Do not trust - test)/CN=Fake OATI Root CA (Do not trust - test)	Apr 21 22:14:12 2014 GMT	Apr 18 22:14:12 2024 GMT	Delete
Details	/C=US/ST=PA/L=Philadelphia/O=Fake OATI (Do not trust - test)/CN=Fake OATI IA (Do not trust - test)	Apr 21 22:15:23 2014 GMT	Apr 20 22:15:23 2016 GMT	Delete

Certificate Revocation List

	Issuer	Last Update	Next Update	

Figure 26: Certificates Screen

1. Delete Button

3. Click **Delete** next to the desired certificate. A confirmation dialog box appears.
4. Click **Yes** to delete the certificate, or click **No** to abort.
5. Refresh the browser. The certificate disappears from the list.

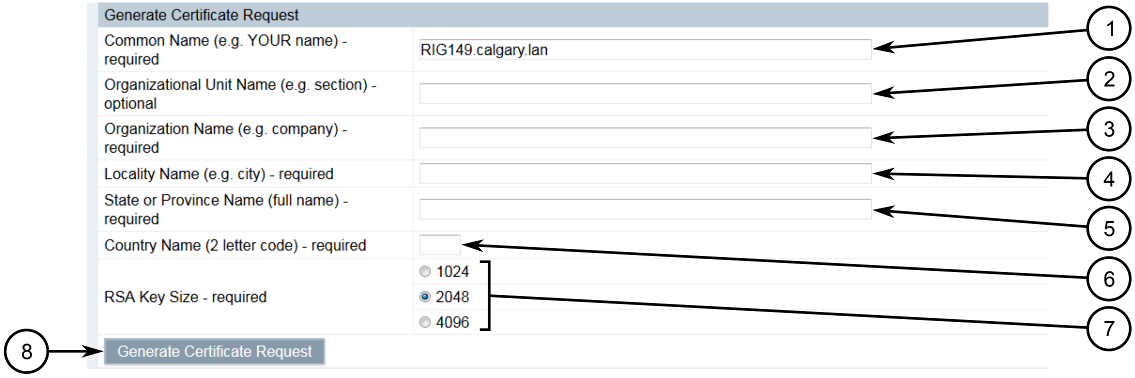
Section 3.10.2.3

Generating a Certificate Request

To generate a certificate request, do the following:

> **IMPORTANT!**
> *A new private key is created each time a certificate request is generated, replacing the previous private key. Therefore, do not generate multiple certificate requests at the same time. Always generate, sign and upload one certificate at a time. Uploading a new Local Certificate will replace the previous certificate.*

1. Log in to EWI. For more information, refer to Section 3.1, "Logging In/Out" .
2. On the menu bar, point to **Tools** and then click **Certificates**. The **Certificates** screen appears.



Generate Certificate Request

Common Name (e.g. YOUR name) - required	RIG149.calgary.lan
Organizational Unit Name (e.g. section) - optional	
Organization Name (e.g. company) - required	
Locality Name (e.g. city) - required	
State or Province Name (full name) - required	
Country Name (2 letter code) - required	
RSA Key Size - required	○ 1024 ● 2048 ○ 4096

Figure 27: Certificates Screen

1. Common Name Box **2.** Organizational Name Box **3.** Organization Name Box **4.** Locality Name Box **5.** State or Province Name Box **6.** Country Name Box **7.** RSA Key Size Options **8.** Generate Certificate Request Button

3. Under **Generate Certificate Request**, configure the following parameters as required:

Parameter	Description
Common Name	The name of the certificate owner.
Organizational Name	The name of the certificate owner's department or section within the organization. This information is optional.
Organization Name	The name of the company.
Locality Name	The name of the city where the company is located.
State or Province Name	The name of the state or province where the company is located.
Country Name	A two-letter code representing the country where the company is located.
RSA Key Size	**Synopsis:** { 1024, 2048, 4096 } **Default:** 2048 The required key size/length.

4. Click **Generate Certificate Request**.

Section 3.10.2.4

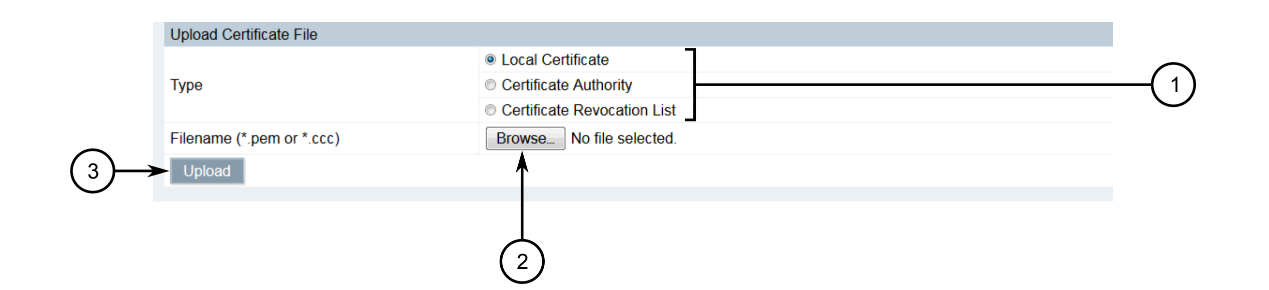
Uploading a Certificate via EWI

To upload a certificate using the RUGGEDCOM ELAN Web Interface (EWI), do the following:

> **IMPORTANT!**
> *Only CA-certified Local Certificates generated through a certificate request can be uploaded via EWI.*

1. Log in to EWI. For more information, refer to Section 3.1, "Logging In/Out" .
2. Generate a certificate request to create a Certificate Signing Request (CSR). The CSR will be signed by the Certificate Authority.

   For more information, refer to Section 3.10.2.3, "Generating a Certificate Request" .
3. On the menu bar, point to **Tools** and then click **Certificates**. The **Certificates** screen appears.



Upload Certificate File

Type: ● Local Certificate ○ Certificate Authority ○ Certificate Revocation List

Filename (*.pem or *.ccc): Browse... No file selected.

Upload

Figure 28: Certificates Screen

1. Type Options **2.** Browse Button **3.** Upload Button

4. Under **Upload Certificate File**, select the type of certificate that matches the certificate that will be uploaded. Options include:
   - `Local Certificate` – Select when uploading a Local Certificate. Local Certificates are signed by a Certificate Authority (CA) and generated by a Certificate Signing Request (CSR).
   - `Certificate Authority` – Select when uploading a CA Certificate. The specified Certificate Authority (CA) is appended to the list of CA's recognized by RUGGEDCOM ELAN. Local Certificates signed by any of the recognized CA's are automatically accepted.
   - `Certificate Revocation List` – Select when uploading a new Certificate Revocation List (CRL).
5. Click **Browse** and locate the certificate.
6. Click **Upload**. The certificate is uploaded to the RUGGEDCOM ELAN server.
7. If a CRL was uploaded, restart RUGGEDCOM ELAN.

Section 3.11

Managing the RUGGEDCOM ELAN Configuration Database

This section describes how to manage roles and access to the RUGGEDCOM ELAN configuration database.

CONTENTS

Section 3.11.1

Adding/Deleting a Database User

To add or delete a database user, do the following:

›› Adding a Database User

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
2. Access the database by typing:

   ```
   su - postgres
   ```

3. Create the new database user by typing:

   ```
   psql --command="CREATE USER username WITH SUPERUSER NOCREATEDB LOGIN PASSWORD 'password';"
   ```

   Where:

   - *username* is the name for the new user
   - *password* is the password for the new user

4. Grant the new user the same privileges as the *elansql* user by typing:

   ```
   psql --command="GRANT elansql TO username;"
   ```

   Where *username* is the name for the user.

5. [Optional] Grant the new user external access. For more information, refer to Section 3.11.3, “Configuring External Access” .
6. Return to the root prompt by typing:

   ```
   exit
   ```

›› Deleting a Database User

IMPORTANT!
*Do not delete the **elansql** or **postgres** users.*

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
2. Access the database by typing:

   ```
   su - postgres
   ```

3. Delete the database user by typing:

   ```
   dropuser --interactive  username
   ```

   Where `username` is the name of the user
4. Return to the root prompt by typing:

   ```
   exit
   ```

Section 3.11.2

Changing a Database User's Password

To change the password for an existing database user, do the following:

> **IMPORTANT!**
> *Do not change the default passwords for* ***elansql*** *or* ***postgres*** *users.*

1. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
2. Access the database by typing:

   ```
   su - postgres
   ```

3. Change the password for a select database user by typing:

   ```
   psql --command="ALTER ROLE username WITH PASSWORD 'password';"
   ```

   Where:

   - `username` is the name for the user
   - `password` is the new password for the user
4. Return to the root prompt by typing:

   ```
   exit
   ```

Section 3.11.3

Configuring External Access

External access to the database is granted by adding a client authentication rule to the end of the file `pg_hba.conf` and then reloading the updated file to the running PostgreSQL process.

To grant a specific user external access rights, do the following:

1. Open the file `/etc/postrgesql/9.1/main/pg_hba.conf` in an editor.

   > **IMPORTANT!**
   > *Do not modify the existing contents of the* `pg_hba.conf` *file.*

2. Add a client authentication rule to the end of the file.

   ```
   connection-type   database   user   address   authentication-method
   ```

   Where:

   - `connection-type` is the connection type. Options include:
     - `local` – For Unix-domain sockets.
     - `host` – For SSL or non-SSL encrypted TCP/IP connections.
     - `hostssl` – For SSL encrypted TCP/IP connections. Use this option only when the Postgres database is configured to use SSL, which is only applicable to non-RUGGEDCOM ROX II platforms.
     - `hostnossl` – For non-SSL encrypted TCP/IP connections.
   - `database` is the name of the database.
   - `user` is the name of the user.
   - `address` is the hostname or IP address for the users workstation.
   - `authentication-method` is the authentication method used to verify the connection. Options include:
     - `trust` – Always allow the connection.
     - `reject` – Always reject the connection.
     - `md5` – Require the user to supply an MD5 encrypted password.
     - `password` – Require the user to supply an unencrypted password.
     - `gss` – Authenticate using GSSAPI (Generic Security Services Application Program Interface).
     - `sspi` – Authenticate using SSPI (Security Support Provider Interface).
     - `krb5` – Authenticate using Kerberos v5. This is only available for TCP/IP connections.
     - `ident` – Using an ident server, compare the users operating system user name to the database user name. This is only available for TCP/IP connections.
     - `peer` – Compare the users operating system user name to the database user name. This is only available for local connections.
     - `ldap` – Authenticate using an LDAP server
     - `radius` – Authenticate using a RADIUS server
     - `cert` – Authenticate using SSL client certificates
     - `pam` – Authenticate using the Pluggable Authentication Modules (PAM) service

   Some examples:

   - This example grants the user *maestro* access via SSL from any external address to the *elan* database as long as the user supplies an MD5 encrypted password.

     NOTE
     The Postgres database must be configured to use SSL in this example.

     ```
     hostssl elan maestro 0.0.0.0 0.0.0.0 md5
     ```

   - This example grants the user *maestro* access from any external address (with or without encryption) to the *elan* database as long as the user supplies an MD5 encrypted password.

     ```
     host elan maestro 0.0.0.0 0.0.0.0 md5
     ```

- This example grants the user *maestro* access from any address on the 192.168.1.0/24 network (with or without encryption) to the *elan* database as long as the user supplies an MD5 encrypted password.

  ```
  host elan maestro 192.168.1.0/24 md5
  ```

- This example grants the user *maestro* access from any address on the same network (with or without encryption) to the *elan* database as long as the user supplies an MD5 encrypted password.

  ```
  host elan maestro samenet md5
  ```

3. Save and close the file.
4. Log in to the CLI for the RUGGEDCOM ELAN server as the *root* user via SSH.
5. Obtain the PID (Process Identifier) for the PostgreSQL process currently running by typing:

   ```
   pgrep -P 1 postgres
   ```

6. Reload the updated file to the running PostgreSQL process by typing:

   ```
   kill -SIGHUP  pid
   ```

   Where `pid` is the PID for the running PostgreSQL process obtained in Step 5 .
7. Return to the root prompt by typing:

   ```
   exit
   ```

4 Using Maestro

Maestro is the configuration tool in the RUGGEDCOM ELAN tool set. It allows users to independently configure one or more RUGGEDCOM ELAN servers – complete with devices, point mapping, gateways, etc. – and then download those configurations to the servers.

The typical process for configuring a RUGGEDCOM ELAN server is as follows:

1. Add a project.
2. Add and configure a RUGGEDCOM ELAN server.
3. Add and configure a device template for the desired protocol.
4. Add and further configure server and client devices based on the template created previously.
5. Configure at least one polling scheme (e.g. timed scan, poll scheme, or control follow-up scan) for each client device.
6. Map points between the server and client devices.
7. [Optional] Configure the protocol routes between server and client devices.
8. Download the configuration to the RUGGEDCOM ELAN server.

CONTENTS

Section 4.1

Launching Maestro

To launch Maestro, do one of the following:

- Double-click the Maestro shortcut icon on your desktop
- Click the **Start** button, click **All Programs**, click **RuggedCom** and then click **Maestro**

Once Maestro has initialized, the **Projects & ELAN Databases** screen appears.

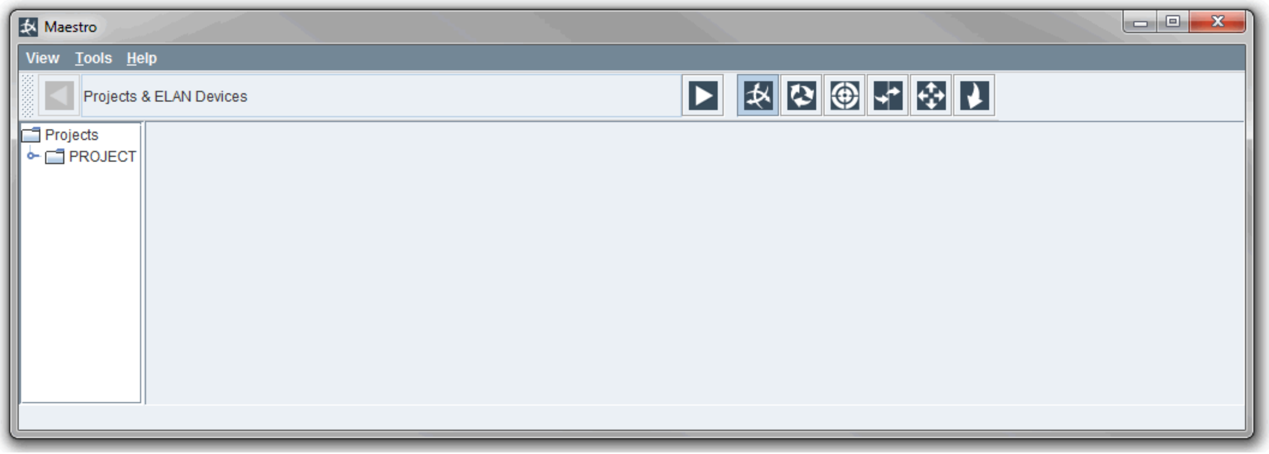
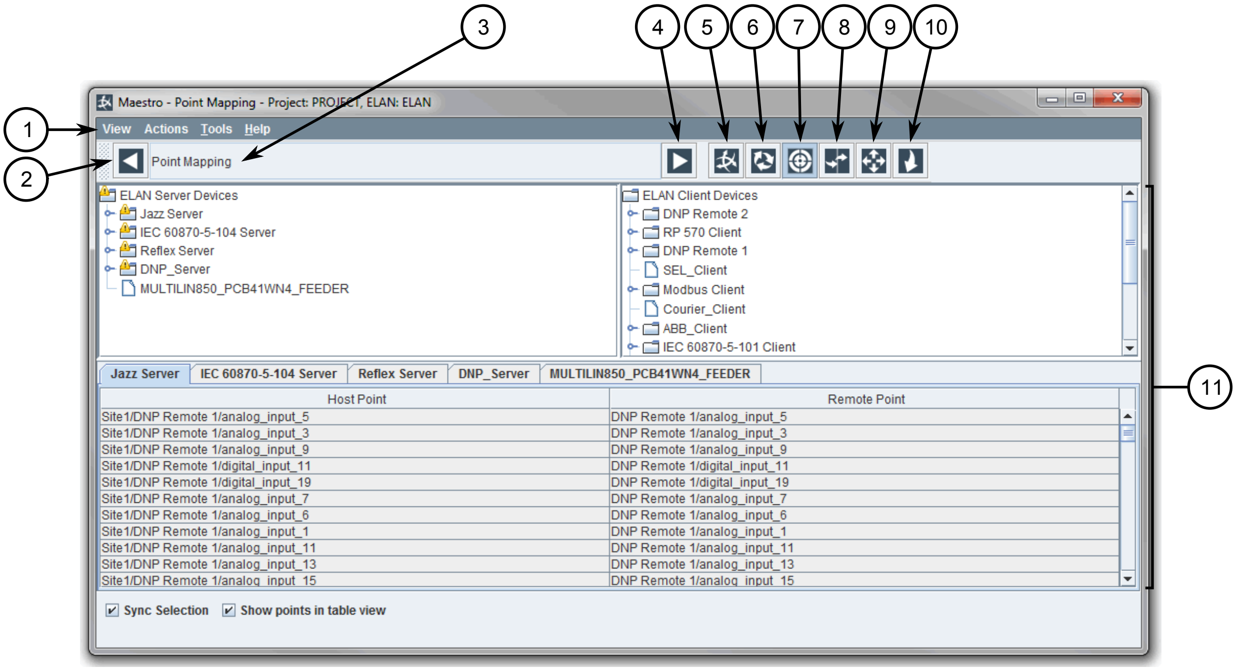


Figure 29: Maestro Start Screen – Projects & ELAN Devices

Section 4.2

Using the Maestro Interface

Maestro uses a Java-based graphical user interface (GUI) for navigating users through the various options for configuring a RUGGEDCOM ELAN server.



- ELAN Server Devices
  - Jazz Server
  - IEC 60870-5-104 Server
  - Reflex Server
  - DNP_Server
  - MULTILIN850_PCB41WN4_FEEDER

- ELAN Client Devices
  - DNP Remote 2
  - RP 570 Client
  - DNP Remote 1
  - SEL_Client
  - Modbus Client
  - Courier_Client
  - ABB_Client
  - IEC 60870-5-101 Client

Jazz Server | IEC 60870-5-104 Server | Reflex Server | DNP_Server | MULTILIN850_PCB41WN4_FEEDER

Host Point	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/digital_input_11	DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19	DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15

☑ Sync Selection ☑ Show points in table view

Figure 30: Main Elements of the Maestro User Interface

1. Menu Bar **2.** Previous Button **3.** Current Screen **4.** Next Button **5.** Projects & ELAN Devices Button **6.** Overview Button **7.** Point Mapping Button **8.** 101-104 Gateway Button **9.** Protocol Router Configuration Button **10.** Download Project Button **11.** Main Area

The menu bar includes the following menus:

- **View** – Includes options to enable or disable specific features, such as TIE, 101-014 Gateway, or the Protocol Router. Disabling a feature removes the associated screens and parameters from the user interface.
- **Actions** – This dynamic menu appears only for select features. It includes controls for common actions related to the feature being configured. In the case of the Protocol Router, for example, it lists the same controls that are available by right-clicking the main area and opening the shortcut menu.
- **Tools** – Provides access to various management and debug tools.
- **Help** – Includes links to extensive Help information, as well as licensing and version information.

Below the menu bar are tools for navigating the Maestro user interface. The **Previous** and **Current** buttons cycle through the available screens. The title for each screen is displayed between them.

Buttons are also available for directly opening the available screens.

Icon	Name	Description
	Projects & ELAN Devices	The **Project & ELAN Devices** screen includes features for managing projects, including RUGGEDCOM ELAN servers and device folders. For more information, refer to Section 4.5, “Managing Projects” , Section 4.6, “Managing RUGGEDCOM ELAN Servers” and/or Section 4.7, “Managing Device Folders” .
	Overview	The **Overview** screen provides an overview of the device templates, server devices, and client devices configured for the RUGGEDCOM ELAN server. For more information, refer to Section 4.8, “Managing Device Templates” , Section 4.9, “Managing Server Devices” , or Section 4.10, “Managing Client Devices” .
	Point Mapping	The **Point Mapping** screen includes features for mapping points between server and client devices. For more information, refer to Section 4.12, “Mapping Points” .

Icon	Name	Description
⇄	101-104 Gateway	The **101-104 Gateway** screen enables users to configure a gateway between IEC 60870-5-101 client devices and IEC 60870-5-104 server devices. For more information, refer to Section 4.13, "Managing the IEC 101-104 Gateway" .
✥	Protocol Router Configuration	The **Protocol Router Configuration** screen includes features for configuring the Protocol Router. For more information, refer to Section 4.14, "Managing Protocol Routes" .
⬇	Download Project	The **Download Project** screen enables users to download configurations to their associated RUGGEDCOM ELAN servers. For more information, refer to Section 4.15, "Downloading Configurations" .

Section 4.3

Sorting, Filtering and Renumbering Points

Each list of points can be sorted, filtered and returned to sequential order with ease.

›› Sorting Points

To sort the list of points in ascending or descending alphabetical order, click the heading for the desired column. The first click sorts the list in ascending order. Click again to sort the list in descending order.

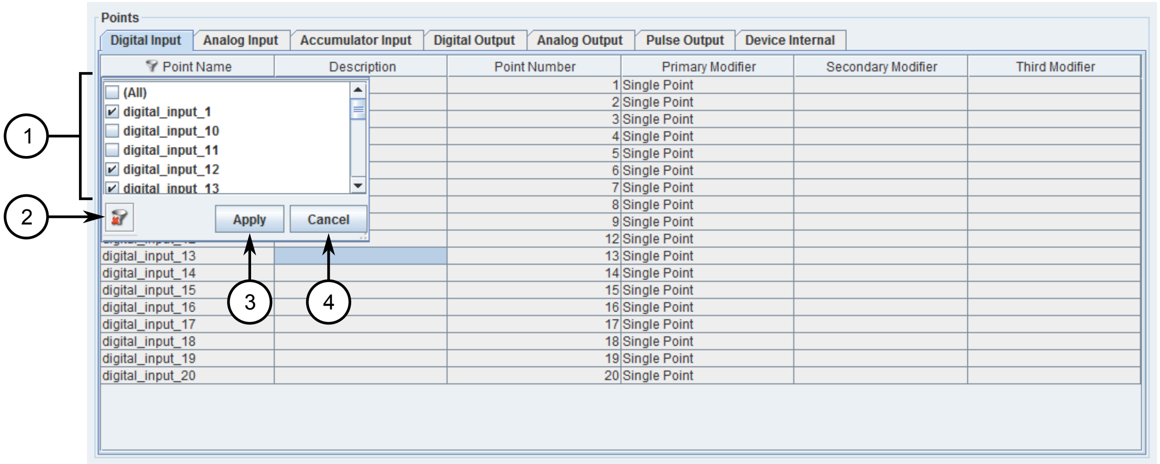
Points can also be moved manually up and down the list by dragging and dropping them in the desired order.

›› Filtering Points

Each column in the table can be filtered to display only select points. To filter the table, do the following:

NOTE
More than one column can be filtered at a time, allowing for more detailed searches.

1. Right-click any column heading and select/clear the desired check boxes. Only points that match the selected information appear in the table.



☐ (All)
☑ digital_input_1
☐ digital_input_10
☐ digital_input_11
☑ digital_input_12
☑ digital_input_13

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
		1	Single Point		
		2	Single Point		
		3	Single Point		
		4	Single Point		
		5	Single Point		
		6	Single Point		
		7	Single Point		
		8	Single Point		
		9	Single Point		
		12	Single Point		
digital_input_13		13	Single Point		
digital_input_14		14	Single Point		
digital_input_15		15	Single Point		
digital_input_16		16	Single Point		
digital_input_17		17	Single Point		
digital_input_18		18	Single Point		
digital_input_19		19	Single Point		
digital_input_20		20	Single Point		

Figure 31: Filtering Points

1. Filter Options **2.** Clear Filter Button **3.** Apply Button **4.** Cancel Button

2. Click **Apply** to apply the filtering or click **Cancel** to abort.

To clear filtering from a column, right-click any column heading and click the **Clear Filter** button.

›› Renumbering Points

To assign sequential numbers to a set of points in their current order, select two or more neighboring ports, then right-click and select **Renumber Points**. New point numbers based on each points order in the list are assigned.

NOTE
Renumbering points can result in duplicate point numbers and/or point names in the list. If this occurs, each row that contains a duplicate point number or name will be highlighted in red. This can be resolved by manually renaming the affected points or by selecting all points and renumbering them again.

Section 4.4

Managing Logs in Maestro

Maestro writes event information to the following logs:

- *hibernate.log* – Logs transaction information related to the OSM database.
- *maestro.log* – Logs information about runtime exceptions and startup information.

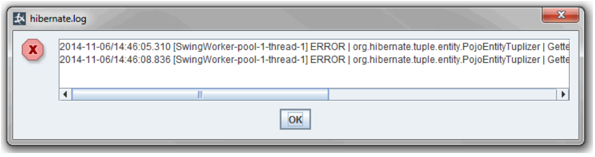
Both logs are for diagnostic purposes only. Users may be asked to forward these logs to Siemens Customer Support for troubleshooting assistance.

CONTENTS

Section 4.4.1

Viewing Logs

To view one of the available logs, under **Tools**, select **Debug Options** and then click either **hibernate.log** or **maestro.log**. The dialog box appears.



```
2014-11-06/14:46:05.310 [SwingWorker-pool-1-thread-1] ERROR | org.hibernate.tuple.entity.PojoEntityTuplizer | Gette
2014-11-06/14:46:08.836 [SwingWorker-pool-1-thread-1] ERROR | org.hibernate.tuple.entity.PojoEntityTuplizer | Gette
```

Figure 32: Hibernate Log (Example)

Section 4.4.2

Configuring Logs

To control the type of information logged by Maestro, do the following:

> **NOTE**
> *Changing the configuration of the logs should only be done as directed by Siemens Customer Support.*

- For the Hibernate log (hibernate.log), go to ***Tools*** » ***Debug Options*** » ***Hibernate*** , and select the level of information to be logged
- For the Maestro log (maestro.log), go to ***Tools*** » ***Debug Options*** » ***Application*** , and select the level of information to be logged

Options include: **DEBUG**, **INFO**, **WARN**, **ERROR** and **FATAL**.

Each option automatically selects all others below it. For example, selecting **ERROR** logs all error-level and fatal-level messages.

Section 4.5

Managing Projects

This section describes how to configure and manage projects in Maestro.

CONTENTS

- Section 4.5.5, “Exporting/Importing the Project Database”

Section 4.5.1

Opening/Closing a Project

To open or close a project in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the project and click either **Open** or **Close** depending on the project's current state. The project properties in the main pane are editable when the project is open and shaded when the project is closed.

Section 4.5.2

Adding/Deleting a Project

To add a project in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click on **Projects** and click **New Project**. A new project is added with the default name **PROJECT*n*** , where *n* is a sequential number.
3. Add one or more RUGGEDCOM ELAN servers. For more information, refer to Section 4.6.2, “Adding/Deleting a RUGGEDCOM ELAN Server” .
4. [Optional] Add one or more device folders. For more information, refer to Section 4.7.1, “Adding/Deleting a Device Folder” .

To delete a project in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the chosen project to open the shortcut menu and click **Delete**. A confirmation dialog box appears.
3. Click **OK**.

Section 4.5.3

Renaming a Project

To rename a project in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the project and click **Rename**. The project name becomes editable.
3. Type a new name for the project and press **Enter**.

Alternatively, a project can also be renamed by editing its properties.

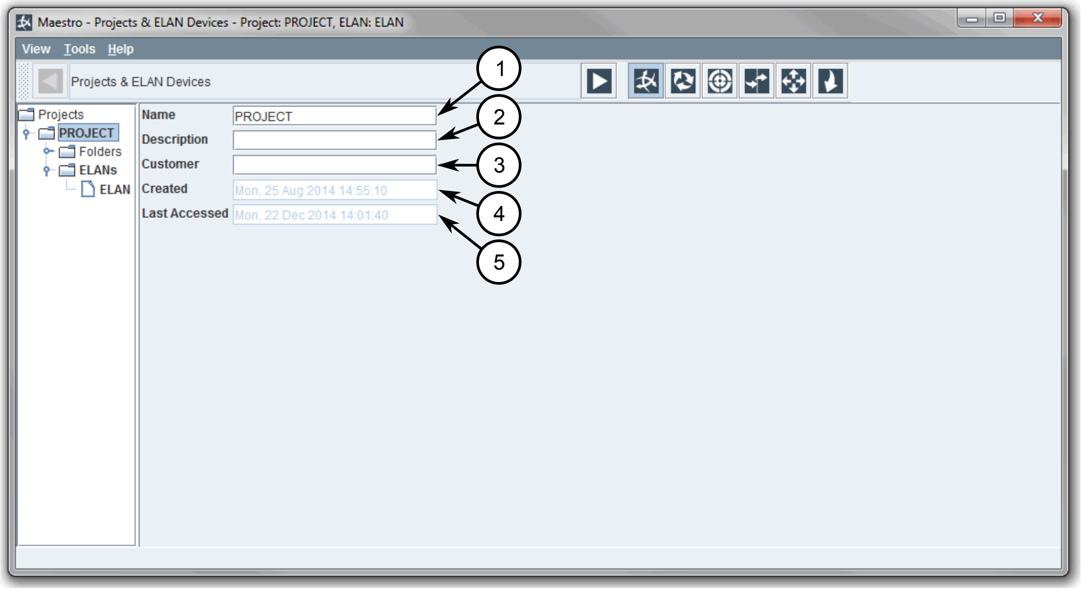
1. In the navigation pane, select the project. The project properties appear in the main pane.
2. Under **Name**, edit the name of the project.
3. Refresh the project name by clicking anywhere in the navigation pane.

Section 4.5.4

Configuring a Project

To configure a project in Maestro, do the following:

1. Open the project. For more information, refer to Section 4.5.1, "Opening/Closing a Project" .



Name: PROJECT
Description:
Customer:
Created: Mon, 25 Aug 2014 14:55:10
Last Accessed: Mon, 22 Dec 2014 14:01:40

Figure 33: Project Properties

1. Name Box **2.** Description Box **3.** Customer Box **4.** Created Box **5.** Last Accessed Box

2. Configure the following parameters as required:

Parameter	Description
Name	The name of the project.
Description	A description of the project.
Customer	The customer associated with the project.

Section 4.5.5

Exporting/Importing the Project Database

To export or import the project database, do the following:

Exporting the Database

1. On the **Tools** menu, click **Export Database**. A confirmation dialog box appears asking if the compressed file (*.zip) should be encrypted.
2. Click **Yes** to encrypt the file, or click **No** continue. The **Save** dialog box appears.

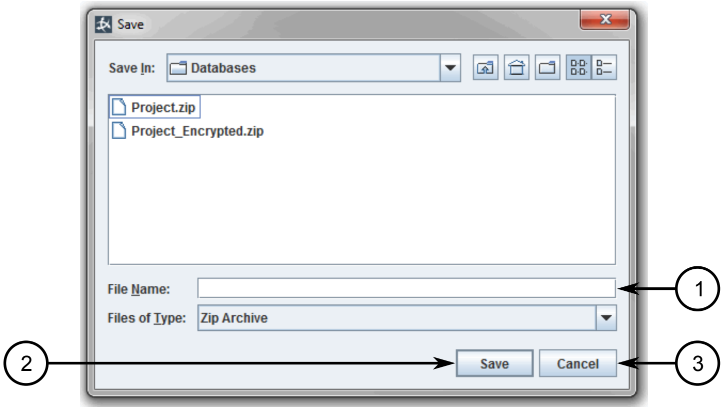


Figure 34: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

3. Navigate to and select the drive or folder where the file will be saved.
4. Under **File Name**, type a name for the file.
5. Click **Save** to save the file. If the file is to be encrypted, the **Enter Password** dialog box appears. Continue to Step 6 .

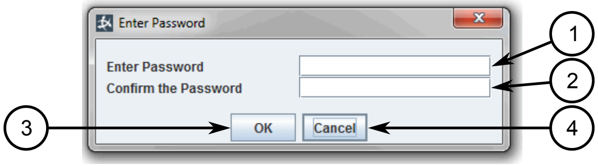


Figure 35: Enter Password Box

1. Enter Password Box **2.** Confirm the Password Button **3.** OK Button **4.** Cancel Button

6. Under **Enter Password** and **Confirm the Password**, enter the password, then click **OK**.

›› Importing a Database

1. On the **Tools** menu, click either **Import Database** or **Import Encrypted Database**. The **Open** dialog box appears.

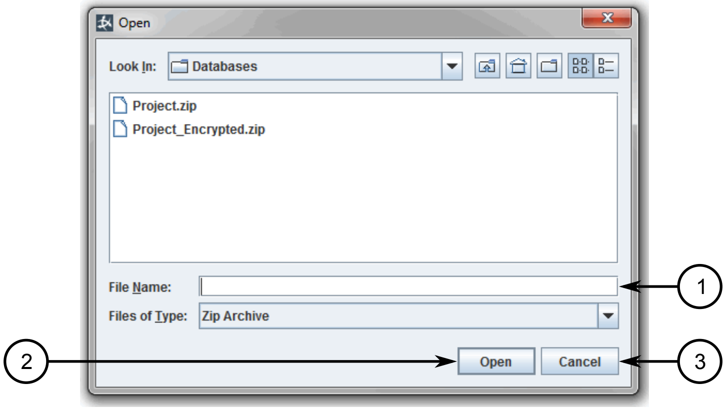


Figure 36: Open Dialog Box

1. File Name Box **2.** Open Button **3.** Cancel Button

2. Navigate to and select the desired compressed file (*.zip).
3. Click **Open** to import the file. If **Import Encrypted Database**, the **Enter Password** dialog box appears. Continue to Step 4 .

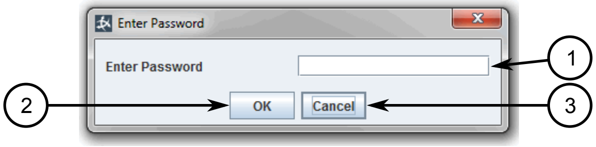


Figure 37: Enter Password Box

1. Enter Password Box **2.** OK Button **3.** Cancel Button

4. Under **Enter Password**, enter the password, then click **OK**.

Section 4.6

Managing RUGGEDCOM ELAN Servers

This section describes how to configure and manage RUGGEDCOM ELAN servers in Maestro.

CONTENTS

Section 4.6.1

Opening/Closing a RUGGEDCOM ELAN Server

To open or close a RUGGEDCOM ELAN server in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the RUGGEDCOM ELAN server and click either **Open** or **Close** depending on the server's current state. The project properties in the main pane are editable when the project is open and shaded when the project is closed.

Section 4.6.2

Adding/Deleting a RUGGEDCOM ELAN Server

To add a RUGGEDCOM ELAN server to a project in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click on either the project or **ELANs**, if present, and click **New ELAN**. An **ELANs** folder is created (if one did not exist previously) and a new RUGGEDCOM ELAN server is added.
3. Rename the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.3, “Renaming a RUGGEDCOM ELAN Server” .

To delete a RUGGEDCOM ELAN server from a project in Maestro, do the following:

- In the navigation pane, right-click on either a single RUGGEDCOM ELAN or **ELANs** and click **Delete**. Deleting **ELANs** will delete all RUGGEDCOM ELAN servers.

Section 4.6.3

Renaming a RUGGEDCOM ELAN Server

To rename a RUGGEDCOM ELAN server, do the following:

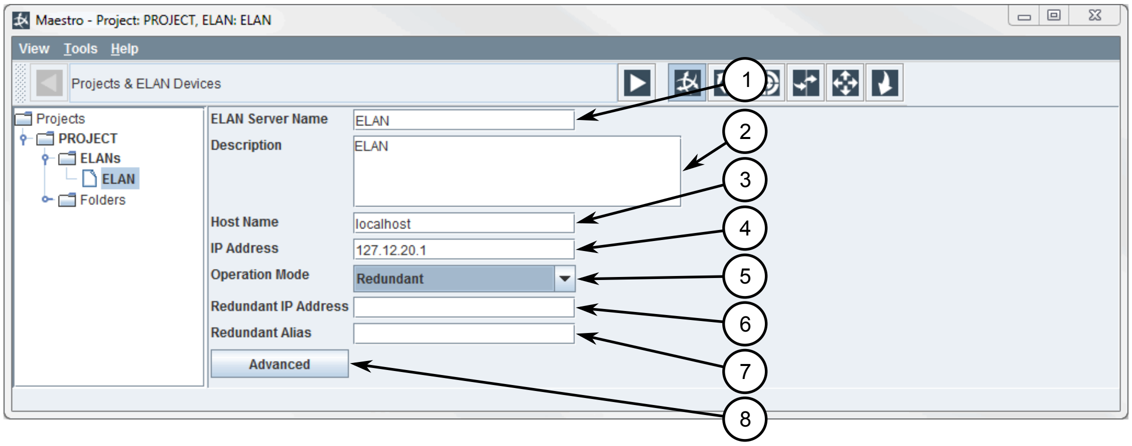
1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the RUGGEDCOM ELAN server and click **Rename**. The server name becomes editable.
3. Type a new name for the server and then press **Enter**.

Section 4.6.4

Configuring a RUGGEDCOM ELAN Server

To configure a RUGGEDCOM ELAN server in Maestro, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .



ELAN Server Name: ELAN
Description: ELAN
Host Name: localhost
IP Address: 127.12.20.1
Operation Mode: Redundant
Redundant IP Address:
Redundant Alias:

Figure 38: RUGGEDCOM ELAN server Properties

1. RUGGEDCOM ELAN server Name Box **2.** Description Box **3.** Host Name Box **4.** IP Address Box **5.** Operation Mode List **6.** Redundant IP Address Box **7.** Redundant Alias Box **8.** Advanced Button

2. In the main pane, edit the following parameters:

Parameter	Description
RUGGEDCOM ELAN server Name	The name of the RUGGEDCOM ELAN server.
Description	A description of the RUGGEDCOM ELAN server.
Host Name	The host name for the RUGGEDCOM ELAN server.
IP Address	The IP address for the RUGGEDCOM ELAN server and the Postgres database used by Maestro when downloading configuration files. Optionally, include the TCP port (e.g. *ipaddress:port*) used by the Postgres database if the default value of *5432* is not used. Available ports range from 1024 to 65535.
Operation Mode	**Synopsis:** { Default, Redundant, Listen } **Default:** Default Sets the mode in which the RUGGEDCOM ELAN server operates. Options include: • `Default` – The RUGGEDCOM ELAN server operates as a stand-alone server. • `Redundant` – The RUGGEDCOM ELAN server operates alongside a redundant server. • `Listen` – Sets all client devices to *Listen* mode, wherein they can be used to capture network traffic. For more information, refer to Chapter 5, *Using ELAN Listener* . **NOTE** *Listen mode is not supported by IEC 61850 client devices.*
Redundant IP Address	**Default State:** Disabled **Prerequisite:** *`Operation Mode`* is set to `Redundant` The IP address for the RUGGEDCOM ELAN server this server is paired with.

Parameter	Description
	The IP address for the redundant RUGGEDCOM ELAN server and the redundant Postgres database used by Maestro when downloading configuration files redundant server. Optionally, include the TCP port (e.g. *ipaddress:port*) used by the Postgres database if the default value of *5432* is not used. Available ports range from 1024 to 65535.
Redundant Alias	**Prerequisite:** *Operation Mode* is set to Redundant The floating IP address shared between the redundant pair.

3. [Optional] Configure advanced settings for the RUGGEDCOM ELAN server. For more information, refer to:
   - Section 4.6.5, "Configuring TIE Settings"
   - Section 4.6.7, "Managing Serial Interfaces"
   - Section 4.6.6, "Configuring RUGGEDCOM ELAN Ports"
   - Section 4.6.8, "Managing the Automatic File Manager (AFM)"

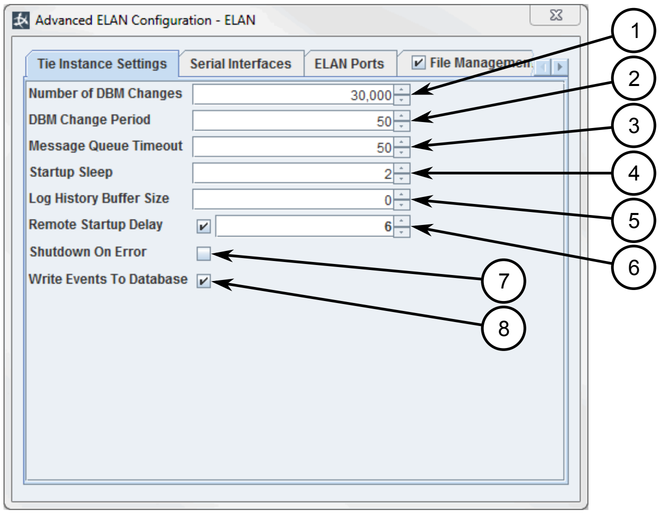
Section 4.6.5

Configuring TIE Settings

To configure the Telemetry Integration Environment (TIE) settings for a RUGGEDCOM ELAN server in Maestro, do the following:

> **CAUTION!**
> *Configuration hazard – risk of data loss, data corruption or reduced performance. Only advanced RUGGEDCOM ELAN users should be permitted to modify the settings for TIE.*

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, "Opening/Closing a RUGGEDCOM ELAN Server" .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. By default, the **TIE Instance Settings** tab is displayed.



Number of DBM Changes 30,000
DBM Change Period 50
Message Queue Timeout 50
Startup Sleep 2
Log History Buffer Size 0
Remote Startup Delay ☑ 6
Shutdown On Error □
Write Events To Database ☑

Figure 39: Advanced ELAN Configuration – TIE Instance Settings Tab

1. Number of DBM Changes Box **2.** DMB Change Period Box **3.** Message Queue Timeout Box **4.** Startup Sleep Box **5.** Log History Buffer Size Box **6.** Remote Startup Delay Check Box and Box **7.** Shutdown Error Check Box **8.** Write Events to Database Check Box

3. Configure the following parameters as required:

Parameter	Description
Number of DBM Changes	**Synopsis:** 10 to 100000 **Default:** 300000 The maximum number of events the generic host interface process will read from the Database Manager at a time.
DBM Change Period	**Synopsis:** 0 to 30000 ms **Default:** 50 ms The period in milliseconds at which to read events from the DBM.
Message Queue Timeout	**Synopsis:** 0 to 30000 ms **Default:** 50 ms The maximum amount of time in milliseconds to wait at the message queue for the receipts of a message.
Startup Sleep	**Synopsis:** 0 to 30 s **Default:** 2 s The time in seconds after the clients are started, before starting the server.
Log History Buffer Size	**Synopsis:** 0 to 65535 **Default:** 0 The number of log messages stored in the history buffer for the generic host interface process. These messages are printed out when a fatal error occurs.
Log History Buffer Size	**Synopsis:** 0 to 65535 **Default:** 0 The number of log messages stored in the history buffer for the generic host interface process. These messages are printed out when a fatal error occurs. A value of 0 disables the history buffer.

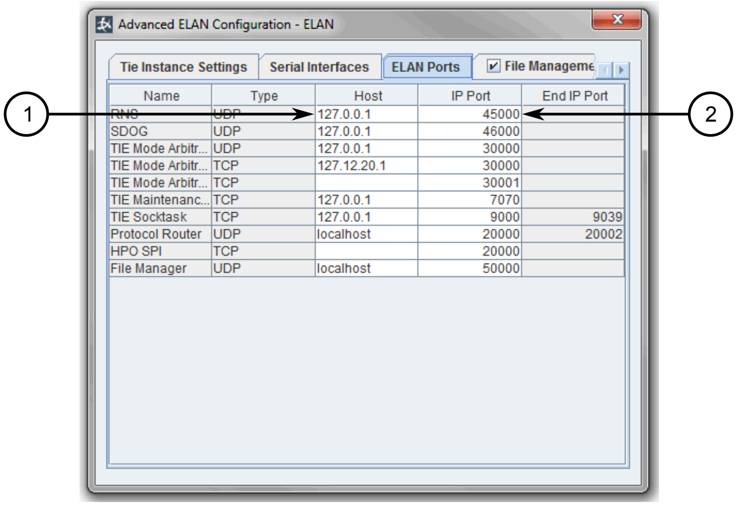
Parameter	Description
Remote Startup Delay	**Synopsis:** 0 to 90000 **Default Value:** 0 **Default State:** Disabled The time in milliseconds (ms) to elapse before launching the next remote process. This parameter specifies the number of milliseconds to elapse before launching the next remote process. If the current remote process completes its startup before the delay has elapsed, the delay timer will be reset and the next remote process will be launched. When disabled (cleared), each remote process must complete its startup before the next remote process will be started.
Shutdown on Error	**Default State:** Disabled When enabled, TIE is forced to shutdown when a fatal error occurs in the generic host interface process.
Write Events to Database	**Default State:** Disabled When enabled, all events are recorded in the RUGGEDCOM ELAN database.

Section 4.6.6

Configuring RUGGEDCOM ELAN Ports

To configure RUGGEDCOM ELAN ports, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **ELAN Ports** tab.



Name	Type	Host	IP Port	End IP Port
RNS	UDP	127.0.0.1	45000	
SDOG	UDP	127.0.0.1	46000	
TIE Mode Arbitr...	UDP	127.0.0.1	30000	
TIE Mode Arbitr...	TCP	127.12.20.1	30000	
TIE Mode Arbitr...	TCP		30001	
TIE Maintenanc...	TCP	127.0.0.1	7070	
TIE Socktask	TCP	127.0.0.1	9000	9039
Protocol Router	UDP	localhost	20000	20002
HPO SPI	TCP		20000	
File Manager	UDP	localhost	50000	

Figure 40: Advanced ELAN Configuration – ELAN Ports Tab

1. Host Box **2.** IP Port Box

The **ELAN Ports** tab displays the following information in a table format:

Column	Description
Name	The port name.
Type	The port type (TCP or UDP).
Host	The IP address or host name for the port.
IP Port	The TCP or UDP port number.
End IP Port	The end IP port for the range of TCP or UDP port numbers when an actual port range is represented by the row.

3. Under **Host**, type the host name or IP address for the desired port.
4. Under **IP Port**, type the TCP or UDP port number for the desired port.

Section 4.6.7

Managing Serial Interfaces

This section describes how to configure and manage serial interfaces in Maestro.

CONTENTS

Section 4.6.7.1

Adding/Deleting a Serial Interface

To add/delete a serial interface, do the following:

›› Adding a Serial Interface

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **Serial Interfaces** tab.

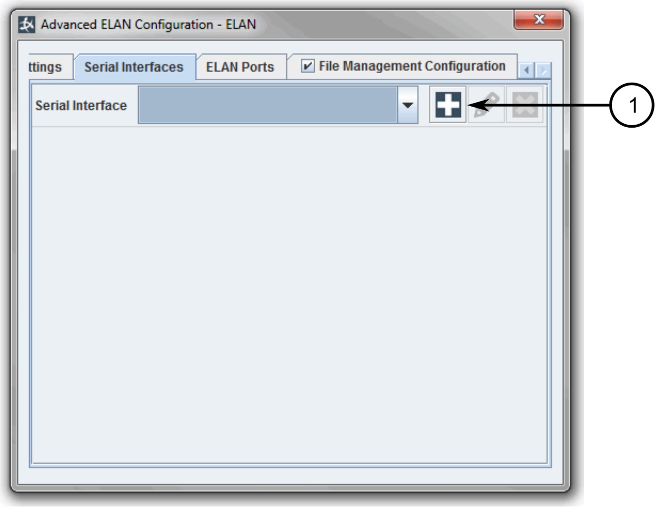

Advanced ELAN Configuration - ELAN
ttings
Serial Interfaces
ELAN Ports
File Management Configuration
Serial Interface
1

Figure 41: Advanced ELAN Configuration – Serial Interfaces Tab

1. Add Button

3. Click the **Add** button. The **New Object** dialog box appears.

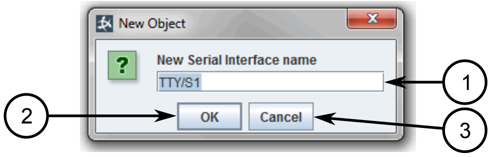


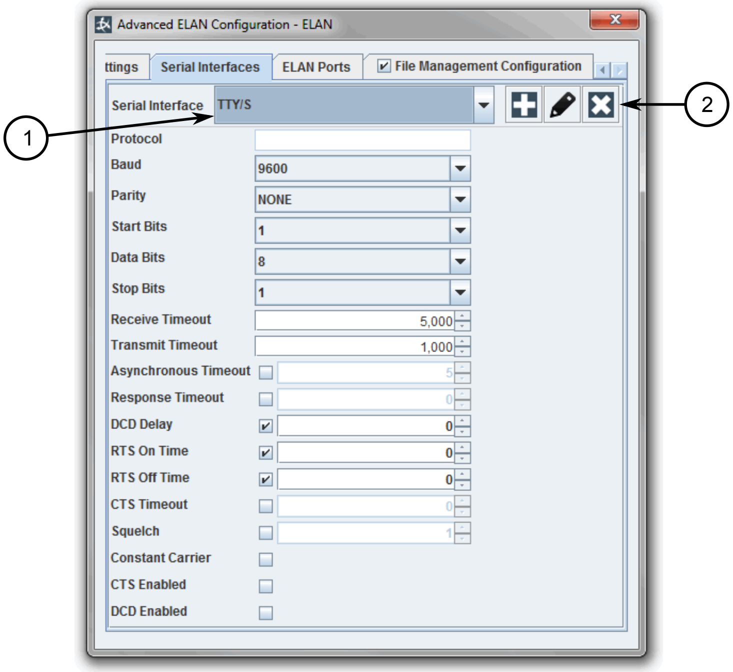
Figure 42: New Object Dialog Box

1. New Serial Interface Name Box **2.** OK Button **3.** Cancel Button

4. [Optional] Type a new name for the serial interface.
5. Click **OK** to add the serial interface, or click **Cancel** to abort.

Deleting a Serial Interface

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, "Opening/Closing a RUGGEDCOM ELAN Server" .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **Serial Interfaces** tab.


Advanced ELAN Configuration - ELAN
ttings
Serial Interfaces
ELAN Ports
☑ File Management Configuration
1
2

Serial Interface: TTY/S
Protocol:
Baud: 9600
Parity: NONE
Start Bits: 1
Data Bits: 8
Stop Bits: 1
Receive Timeout: 5,000
Transmit Timeout: 1,000
Asynchronous Timeout: □ 5
Response Timeout: □ 0
DCD Delay: ☑ 0
RTS On Time: ☑ 0
RTS Off Time: ☑ 0
CTS Timeout: □ 0
Squelch: □ 1
Constant Carrier: □
CTS Enabled: □
DCD Enabled: □

Figure 43: Advanced ELAN Configuration – Serial Interfaces Tab

1. Serial Interface List **2.** Delete Button

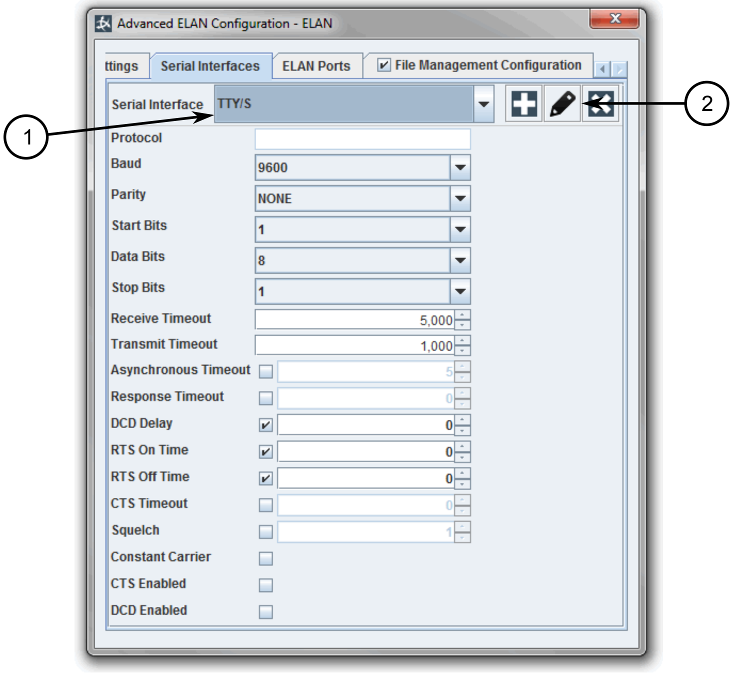
3. Select a serial interface from the **Serial Interface** list.
4. Click the **Delete** button. A confirmation dialog box appears.
5. Click **Yes** to delete the serial interface, or click **No** to abort.

Section 4.6.7.2

Renaming a Serial Interface

To rename a serial interface, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **Serial Interfaces** tab.


Advanced ELAN Configuration - ELAN
ttings
Serial Interfaces
ELAN Ports
☑ File Management Configuration
1
2

Serial Interface		TTY/S
Protocol		
Baud		9600
Parity		NONE
Start Bits		1
Data Bits		8
Stop Bits		1
Receive Timeout		5,000
Transmit Timeout		1,000
Asynchronous Timeout	□	5
Response Timeout	□	0
DCD Delay	☑	0
RTS On Time	☑	0
RTS Off Time	☑	0
CTS Timeout	□	0
Squelch	□	1
Constant Carrier	□	
CTS Enabled	□	
DCD Enabled	□	

Figure 44: Advanced ELAN Configuration – Serial Interfaces Tab

1. Serial Interface List **2.** Rename Button

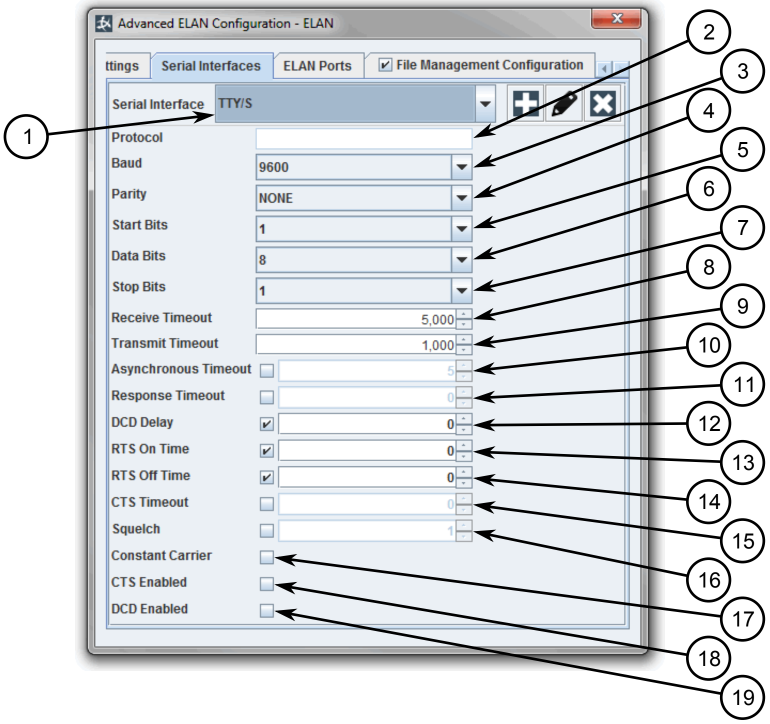
3. Select a serial interface from the **Serial Interface** list.
4. Click the **Rename** button and type a new name for the serial interface.

Section 4.6.7.3

Configuring a Serial Interface

To configure a serial interface for an RUGGEDCOM ELAN server, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **Serial Interfaces** tab.


Advanced ELAN Configuration - ELAN
ttings
Serial Interfaces
ELAN Ports
☑ File Management Configuration
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

Serial Interface: TTY/S

Protocol:

Baud: 9600

Parity: NONE

Start Bits: 1

Data Bits: 8

Stop Bits: 1

Receive Timeout: 5,000

Transmit Timeout: 1,000

Asynchronous Timeout: □ 5

Response Timeout: □ 0

DCD Delay: ☑ 0

RTS On Time: ☑ 0

RTS Off Time: ☑ 0

CTS Timeout: □ 0

Squelch: □ 1

Constant Carrier: □

CTS Enabled: □

DCD Enabled: □

Figure 45: Advanced ELAN Configuration – Serial Interfaces Tab

1. Serial Interface List **2.** Protocol Box **3.** Baud List **4.** Parity List **5.** Start Bits List **6.** Data Bits List **7.** Stop Bits List **8.** Receive Timeout Box **9.** Transmit Timeout Box **10.** Asynchronous Timeout Check Box and Box **11.** Response Timeout Check Box and Box **12.** DCD Delay Check Box and Box **13.** RTS On Time Check Box and Box **14.** RTS Off Time Check Box and Box **15.** CTS Timeout Check Box and Box **16.** Squelch Check Box and Box **17.** Constant Carrier Check Box **18.** CTS Enabled Check Box **19.** DCD Enabled Check Box

3. Select a serial interface from the **Serial Interface** list.
4. Configure the following parameters as required:

Parameter	Description
Baud	**Synopsis:** 3600, 4800, 7200, 9600, 19200, 38400, 57600, 115000 **Default:** 9600 The serial communications speed in bits-per-second (bps).
Parity	**Synopsis:** EVEN, ODD, NONE **Default:** NONE The parity to be used on the serial connection.
Start Bits	**Synopsis:** 0, 1, 2 **Default:** 1 The number of bits that precede each character.
Data Bits	**Synopsis:** 7, 8 **Default:** 8 The number of data bits contained in each character transmitted over the serial connection.

Parameter	Description
Stop Bits	**Synopsis:** 1, 2 **Default:** 1 The number of bits that follow each character.
Receive Timeout	**Synopsis:** 0 to 65535 **Default:** 5000 The maximum time in milliseconds (ms) to wait for an entire response message. If no message is received before the time period ends, the response will be considered to have failed.
Transmit Timeout	**Synopsis:** 0 to 65535 **Default:** 1000 The desired transmit timeout in milliseconds (ms). The time must be long enough to transmit the maximum length message sent to a client device at the given baud rate.
Asynchronous Timeout	**Synopsis:** 0 to 65535 **Default Value:** 20 **Default State:** Disabled The desired inter-message timeout in milliseconds (ms) used to detect the end of a message. The check box must be checked for this parameter to take effect.
Response Timeout	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Disabled The desired time in milliseconds (ms) to wait for a response message. Use for message types that require a response from the end device. The check box must be checked for this parameter to take effect.
DCD Delay	**Synopsis:** 0 to 65535 **Default Value:** 100 **Default State:** Enabled The desired time delay in milliseconds (ms) from the moment the serial device detects a Data Carrier Detect (DCD) control signal is received until the receiver hardware is enabled. The check box must be checked for this parameter to take effect.
RTS On Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to assert the Request to Send (RTS) control signal before transmitting a message. The check box must be checked for this parameter to take effect.
RTS Off Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to continue asserting the Request to Send (RTS) control signal after transmitting a message. The check box must be checked for this parameter to take effect.
CTS Timeout	**Synopsis:** 0 to 65535 **Default:** 100 The desired time in milliseconds (ms) to wait for a Clear to Send (CTS) control signal before aborting the transmission of a message. The check box must be checked for this parameter to take effect.
Squelch	**Synopsis:** 0 to 65535 **Default Value:** 100

Parameter	Description
	Default State: Disabled The desired time in milliseconds (ms) to wait after a Data Carrier Detect (DCD) control signal is received before enabling reception. The check box must be checked for this parameter to take effect.
Constant Carrier	**Default State:** Disabled When enabled (selected), the carrier is set to *constant*. Otherwise, the carrier is set to *switched*.
CTS Enabled	**Default State:** Disabled When enabled (selected), Clear to Send (CTS) control signals are enabled.
DCD Enabled	**Default State:** Disabled When enabled (selected), Data Carrier Detect (DCD) control signals are enabled.

Section 4.6.8

Managing the Automatic File Manager (AFM)

RUGGEDCOM ELAN's Automatic File Manager (AFM) works with either the IED Manager system or a DNP 3.0 Remote Interface system to collect reports from RTUs and IEDs and forward them to one or more targets for storage or processing. In addition to transferring reports, AFM can also be configured to send email notification to local or remote addresses, signaling it has sent a report to a specified target.

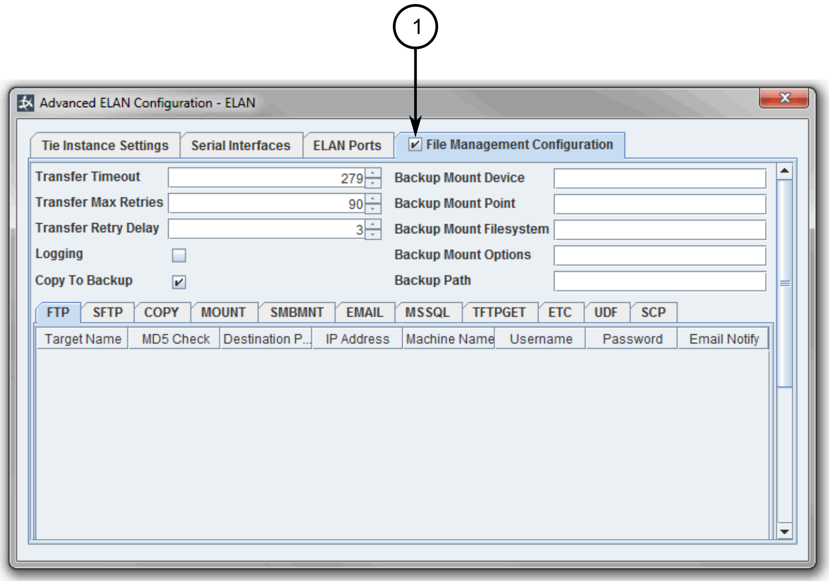
CONTENTS

Section 4.6.8.1

Enabling/Disabling the AFM

To enable or disable the AFM for a RUGGEDCOM ELAN server, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears.



Transfer Timeout 279
Transfer Max Retries 90
Transfer Retry Delay 3
Logging □
Copy To Backup ☑
Backup Mount Device
Backup Mount Point
Backup Mount Filesystem
Backup Mount Options
Backup Path

Target Name	MD5 Check	Destination P...	IP Address	Machine Name	Username	Password	Email Notify

Figure 46: Advanced ELAN Configuration – File Management Configuration Tab

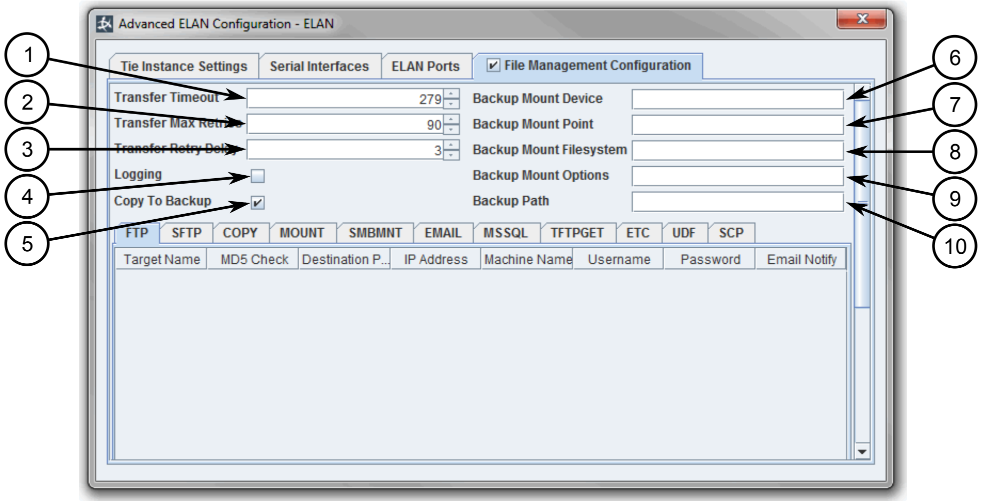
1. Enable/Disable Check Box

3. Enable or disable the AFM by doing the following:
    - To enable the AFM, click the check box on the **File Management Configuration** tab
    - To disable the AFM, clear the check box on the **File Management Configuration** tab

Section 4.6.8.2
Configuring the Automatic File Manager (AFM)

To configure the AFM for a RUGGEDCOM ELAN server, do the following:

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears. Click the **File Management Configuration** tab.



Transfer Timeout 279
Transfer Max Retries 90
Transfer Retry Delay 3
Logging □
Copy To Backup ☑
Backup Mount Device
Backup Mount Point
Backup Mount Filesystem
Backup Mount Options
Backup Path

Figure 47: Advanced ELAN Configuration – File Management Configuration Tab

1. Transfer Timeout Box **2.** Transfer Max Tries Box **3.** Transfer Retry Delay Box **4.** Logging Check Box **5.** Copy To Backup Box **6.** Backup Mount Device Box **7.** Backup Mount Point Box **8.** Backup Mount Filesystem Box **9.** Backup Mount Options Box **10.** Backup Path Box

3. Configure the following parameters as required:

Parameter	Description
Transfer Timeout	**Synopsis:** 1 to 10000 **Default:** 10 The time interval in seconds to wait for a response from the transfer target.
Transfer Max Tries	**Synopsis:** 0 to 100 **Default:** 3 The maximum number of times to retry sending a report.
Transfer Retry Delay	**Synopsis:** 0 to 10000 **Default:** 3 The time in seconds (s) to wait before resending a report.
Logging	**Default State:** Disabled When enabled (selected), all AFM transfers are logged to the file `afm_xfer.log`.
Copy To Backup	**Default State:** Disabled When enabled (selected), a copy of each sent report is saved.
Backup Mount Device	The drive or partition where reports will be copied for backup.
Backup Mount Point	The location on a drive or partition where copies of reports will be saved.
Backup Mount Filesystem	The file system to use for reports.
Backup Mount Options	The mount options for the backup mount point.

Parameter	Description
Backup Path	The path on a backup partition (BackupMountPoint) to a backup location.

4. Configure file management for one or more client devices:
   - For DNP client devices, refer to Section 4.10.7.6, “Configuring DNP File Management Settings”
   - For SEL client devices, refer to Section 4.10.13.4, “Configuring File Management Settings”

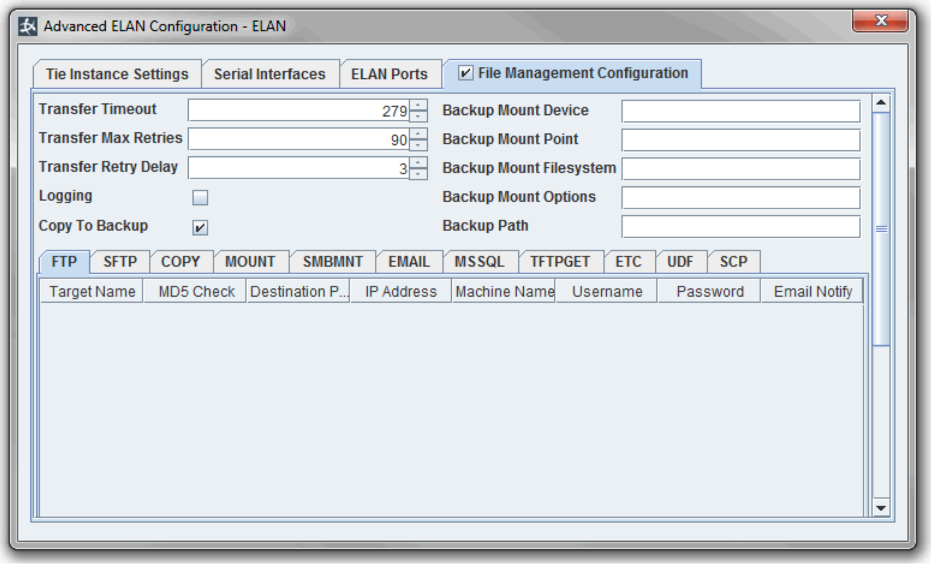
Section 4.6.8.3

Adding/Deleting AFM Targets

To add or delete an AFM target, do the following:

›› Adding an AFM Target

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears.



Transfer Timeout: 279
Transfer Max Retries: 90
Transfer Retry Delay: 3
Logging: □
Copy To Backup: ☑
Backup Mount Device:
Backup Mount Point:
Backup Mount Filesystem:
Backup Mount Options:
Backup Path:

Figure 48: Advanced ELAN Configuration – File Management Configuration Tab

3. Select the tab representing the desired report transfer protocol. Options include:
   - **FTP** – Use when transferring reports from a device with an FTP server enabled. The transfer will use the File Transfer Protocol to retrieve the report from the field device.
   - **SFTP (Secure FTP)** – Use when transferring reports from a device with an SFTP server enabled. The transfer will use the Secure File Transfer Protocol to retrieve the report from the field device. This is helpful in situations where a secure connection is desirable.
   - **Copy** – Use when transferring reports from one local directory to another. A simple file *copy* is made from one directory to another on the local RUGGEDCOM ELAN server.

- **Mount** – Use when a Unix Network Share is used for transferring reports. For example, a report may be retrieved from an RTU and then copied onto a Unix Network Shared directory on a corporate network. To access the Unix Network Share, it must be mounted as a local directory for accessing.
- **Samba** – Use when a Windows Network Share is used for transferring reports. For example, a report may be retrieved from an RTU and then copied onto a Windows Network Shared directory on a corporate network. To access the Windows Network Share, it must be mounted as a local directory for accessing. The report can then be copied to this mounted location.
- **Email** – Use to email reports to an email address. For example, after retrieving a report from the field device, it can then be e-mailed to a recipient using this method.
- **MSSQL** – Use to transfer a report to a Microsoft SQL Server.
- **TFTPGET** – Use when a field device has a Trivial File Transfer Protocol (TFTP) server enabled. A user will use this method to perform a `TFTP get` command to retrieve reports from the TFTP enabled field device.
- **ETC** – The proprietary RUGGEDCOM ELAN Transfer Client file transfer method.
- **UDF** – This is an advanced feature that allows a user to define their own file transfer method using Linux scripts.
- **SCP (Secure Copy)** – Use when transferring reports from one local directory to another with the Secure Copy command. A simple file *copy* is made securely from one directory to another, on the local RUGGEDCOM ELAN server or across the local network.

4. Right-click anywhere under the table to open the shortcut menuand click **New Target**. A new row is added to the table.
5. Configure the following common parameters as required:

Parameter	Description
Target Name	The name of the report target.
MD5 Check	**Default State:** Disabled When enabled, the original report is compared to the transferred report to verify the transfer.
Email Notify	**Default:** false When populated with a comma-separated (,) list of e-mail addresses, RUGGEDCOM ELAN sends an e-mail to each e-mail address whenever a report is sent to the target. Enter `false` to disable this feature.

6. Configure the following protocol-specific parameters as required:

›› FTP

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
IP Address	The IP address of the target PC or host.
Machine Name	The host name of the target PC or host. This is used in e-mail notifications.
Username	The user name to use for logging in to the target host or PC.

Parameter	Description
Password	The password associated with the user name used for logging in to the target host or PC.

SFTP

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
IP Address	The IP address of the target PC or host.
Machine Name	The host name of the target PC or host. This is used in e-mail notifications.

COPY

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.

MOUNT

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
Filesystem	**Synopsis:** { NFS, SMBFS } **Default:** NFS The type of file system to use on the target PC or host.
Options	Backup file options for the chosen file system.
Mount Device	The drive or partition where the target resides.
Mount Point	The path name for the mounted device.

SMBMNT

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
Username	The user name to use for logging in to the target host or PC.
Password	The password associated with the user name used for logging in to the target host or PC.
Options	Backup file options for the chosen file system.
Mount Point	The path name for the mounted device.

Parameter	Description
SMB Service	The SAMBA service where the target resides.

EMAIL

Parameter	Description
Email Address	The e-mail address where the report will be sent as an ASCII text file.

MSSQL

Parameter	Description
Username	The user name to use for logging in to the target host or PC.
Password	The password associated with the user name used for logging in to the target host or PC.
Server Name	The name of the server.
Database	The name of the database.
Event Type ID	The ID for the event type.
File Type ID	The ID for the file type.
Device Type ID	The ID for the device type.

TFTPGET

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
IP Address	The IP address of the target PC or host.
Machine Name	The host name of the target PC or host. This is used in e-mail notifications.
Device ID	The ID for the device associated with the transfer.

ETC

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
IP Address	The IP address of the target PC or host.
Port	The port used for the ETC application on the target PC or host.

UDF

Parameter	Description
Function	The user-defined function. Must be a valid Unix shell command.

SCP

Parameter	Description
Destination Path	The existing directory/path on the target where the report will be saved.
IP Address	The IP address of the target PC or host.
Machine Name	The host name of the target PC or host. This is used in e-mail notifications.
Username	The user name to use for logging in to the target host or PC.

Deleting an AFM Target

1. Open the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.1, “Opening/Closing a RUGGEDCOM ELAN Server” .
2. Click **Advanced**. The **Advanced ELAN Configuration** dialog box appears.
3. Select the tab representing the desired report transfer protocol.
4. Right-click the desired AFM target to open the shortcut menu and click **Delete Target**. A confirmation dialog box appears.
5. Click **Yes** to delete the target, or click **Cancel** to abort.

Section 4.7

Managing Device Folders

This section describes how to configure and manage device folders in Maestro.

CONTENTS

Section 4.7.1

Adding/Deleting a Device Folder

To add a device folder to a project or another folder in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.

2. In the navigation pane, right-click on either the project or **Folders**, if present, to open the shortcut menu and click **New Folder**. A **Folders** folder is created (if one did not exist previously) and a new folder titled **Folder** is added underneath.
3. Rename the folder. For more information, refer to Section 4.7.2, "Renaming a Device Folder" .

To delete a device folder or folders under a project in Maestro, do the following:

- In the navigation pane, right-click on either a single folder or **Folders** to open the shortcut menu and click **Delete**. Deleting **Folders** will delete all folders.

Section 4.7.2

Renaming a Device Folder

To rename a device folder in Maestro, do the following:

1. Select the **Projects & ELAN Devices** tab.
2. In the navigation pane, right-click the folder and click **Rename**. The folder name becomes editable.
3. Type a new name for the folder, such as a region name, and press **Enter**.

Section 4.8

Managing Device Templates

Device templates provide a common base for the creation of server and/or client devices. Points for server and client devices that are synchronized with a device template can also be managed through the template, creating a single point of control.

CONTENTS

- Section 4.8.16, “Managing Points for Templates”

Section 4.8.1

Viewing a List of Device Templates

Device templates are listed on the **Overview** screen in the left pane under **Device Templates**. Each is sorted by its associated protocol.

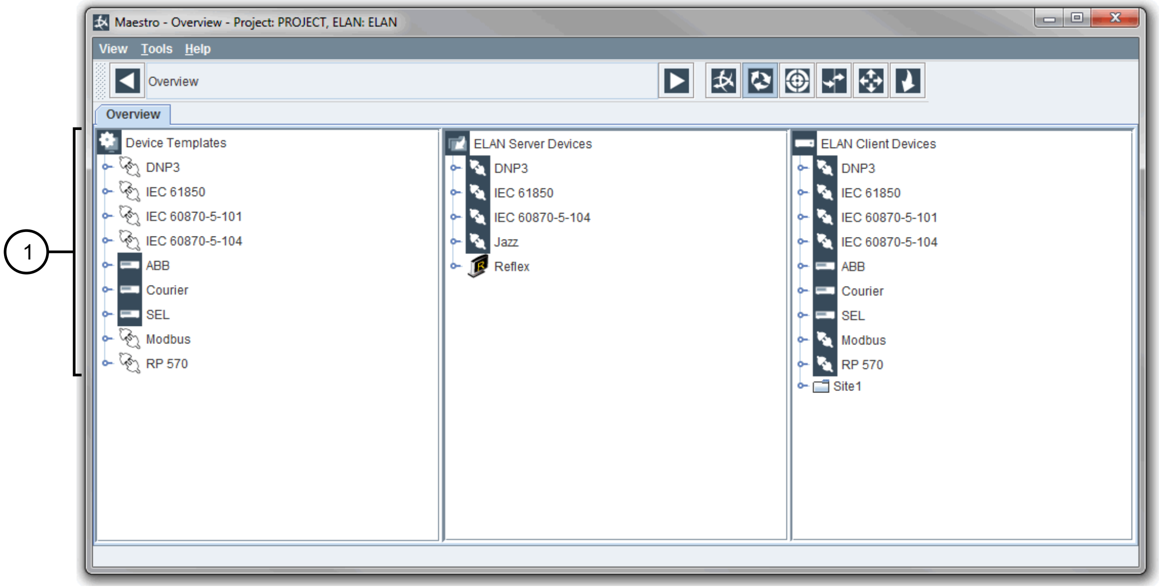


Figure 49: Overview Screen

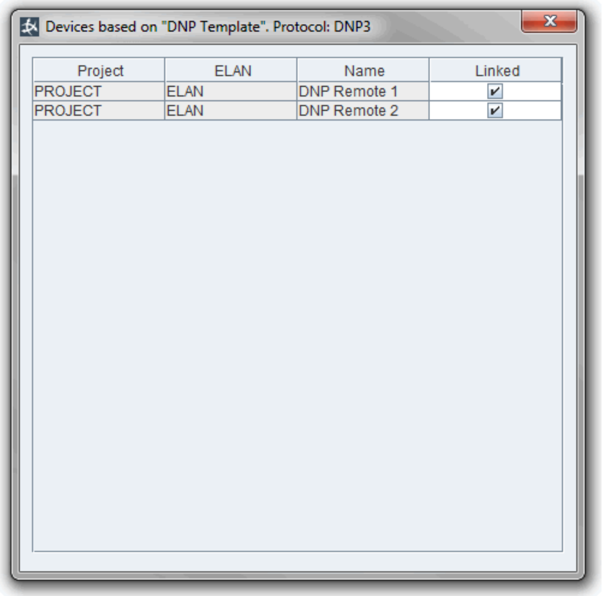
1. Device Templates

Section 4.8.2

Tracking Usage

To track where a template is used, do the following:

1. Navigate to the **Overview** screen.
2. Under **Device Templates**, right-click a device template and click **Usage**. A dialog box appears listing the devices that are based on the template. If no devices are based on the template, the dialog box is empty.



Devices based on "DNP Template". Protocol: DNP3

Project	ELAN	Name	Linked
PROJECT	ELAN	DNP Remote 1	☑
PROJECT	ELAN	DNP Remote 2	☑

Figure 50: Template Usage

Section 4.8.3

Controlling Template Links

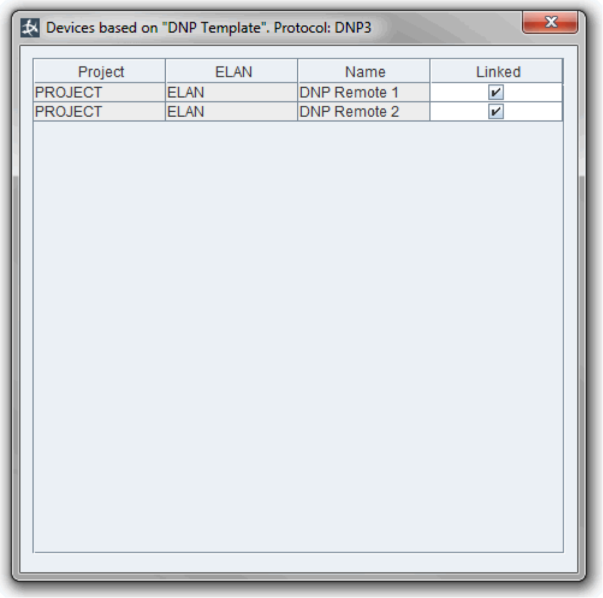
Server and client devices are by default linked to the device template they were created from. This allows users to update the points for multiple devices at once by editing only their shared device template. However, it may be desirable in some cases to break this relationship between a device and its template.

> **IMPORTANT!**
> *When associating a device with a template, all points are aligned with those defined in the device template.*

To break or restore the link between a device and its associated template, do the following:

›› Breaking/Restoring the Link From the Template

1. Navigate to the **Overview** screen.
2. [Optional] If necessary, determine which template the device is associated with by viewing the device's properties. For more information, refer to Section 4.10.1, “Adding/Deleting a Client Device” .
3. Under **Device Templates**, right-click the associated device template and click **Usage**. A dialog box appears listing the devices that are based on the template. If no devices are based on the template, the dialog box is empty.



Devices based on "DNP Template". Protocol: DNP3

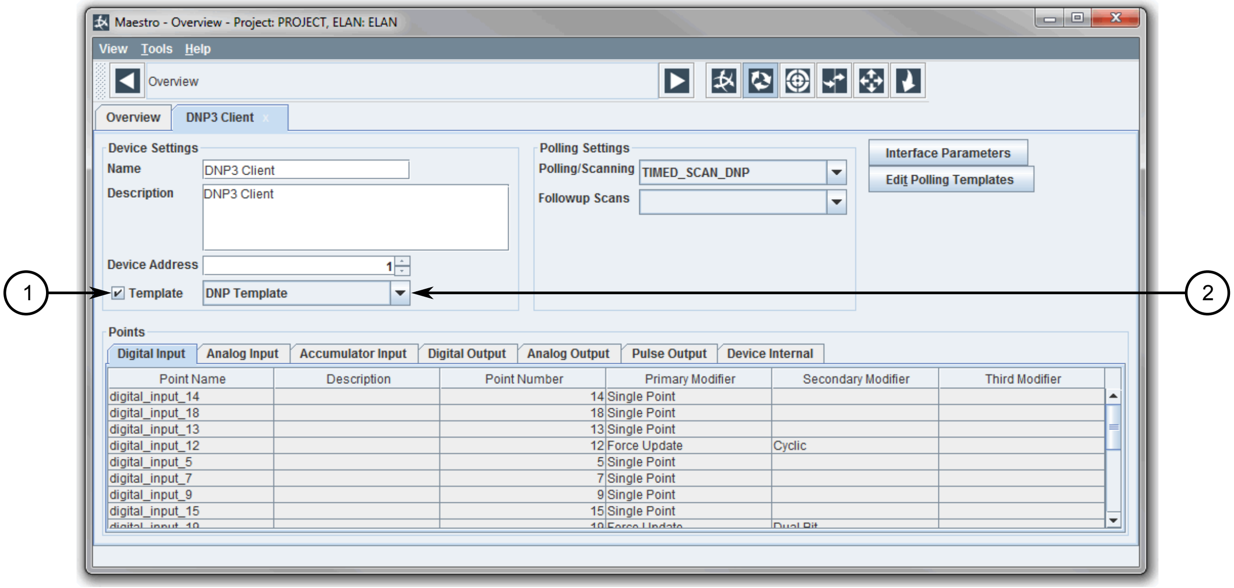
Project	ELAN	Name	Linked
PROJECT	ELAN	DNP Remote 1	☑
PROJECT	ELAN	DNP Remote 2	☑

Figure 51: Template Usage

4. Under **Linked**, either clear the check box for the device to break the link, or select (double-click) the check box to restore the link.
5. If the link has been restored, a confirmation dialog box appears. Click **Yes** to confirm or **No** to cancel.

›› Breaking/Restoring the Link From the Device

1. Navigate to the **Overview** screen.
2. Under **RUGGEDCOM ELAN server Devices** or **RUGGEDCOM ELAN Client Devices**, right-click a device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP3 Client

Description: DNP3 Client

Device Address: 1

☑ Template: DNP Template

Polling Settings

Polling/Scanning: TIMED_SCAN_DNP

Followup Scans:

Points

Digital Input | Analog Input | Accumulator Input | Digital Output | Analog Output | Pulse Output | Device Internal

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_14		14	Single Point		
digital_input_18		18	Single Point		
digital_input_13		13	Single Point		
digital_input_12		12	Force Update	Cyclic	
digital_input_5		5	Single Point		
digital_input_7		7	Single Point		
digital_input_9		9	Single Point		
digital_input_15		15	Single Point		
digital_input_10		10	Force Update	Dual Bit	

Figure 52: Device Properties

1. Template Check Box **2.** Template List

3. Clear the **Template** check box to break the link or select the check box and choose a template to link with the device.
4. If the link has been restored, a confirmation dialog box appears. Click **Yes** to confirm or **No** to cancel.

Section 4.8.4

Adding/Deleting a Device Template

To add or delete a device template, do the following:

NOTE
Device templates are not available for Jazz and RUGGEDCOM REFLEX server devices.

›› Adding a Device Template

1. Navigate to the **Overview** screen.
2. Add the device template using one of the following methods:
   - **Create a Blank Device Template**
     Under **Device Templates**, right-click one of the available protocols and click **New Template**. A new template is added under the protocol
   - **Create a Device Template From an Existing Server or Client Device**
     Under **RUGGEDCOM ELAN server Devices** or **RUGGEDCOM ELAN Client Devices**, right-click the device and click **Create Template**. A new template is added under **Device Templates** and the associated protocol.

3. [Optional] Rename the template. For more information, refer to Section 4.8.5, “Renaming a Device Template” .
4. Configure the device template.
   - For DNP device templates, refer to Section 4.8.7, “Configuring a DNP Template”
   - For IEC 60870-5-101 device templates, refer to Section 4.8.8, “Configuring an IEC 60870-5-101 Template”
   - For IEC 60870-5-104 device templates, refer to Section 4.8.9, “Configuring an IEC 60870-5-104 Template”
   - For ABB device templates, refer to Section 4.8.10, “Configuring an ABB Template”
   - For Courier device templates, refer to Section 4.8.11, “Configuring a Courier Template”
   - For SEL device templates, refer to Section 4.8.12, “Configuring an SEL Template”
   - For Modbus device templates, refer to Section 4.8.13, “Configuring a Modbus Template”
   - For RP 570 device templates, refer to Section 4.8.14, “Configuring an RP 570 Template”

›› Deleting a Device Template

1. Navigate to the **Overview** screen.

   > **IMPORTANT!**
   > *A template cannot be deleted if it is used by a server or client device.*

2. [Optional] Determine if the device template is used by any server or client devices. For more information, refer to Section 4.8.2, “Tracking Usage” .
3. [Optional] If the device template is in use, associate the server or client device(s) with another template. For more information, refer to Section 4.8.6, “Using a Device Template” .
4. Under **Device Templates**, right-click the device template and click **Delete**. A confirmation dialog box appears.
5. Click **Yes** to delete the template, or click **No** to abort.

Section 4.8.5

Renaming a Device Template

To rename a device template, do the following:

1. Navigate to the **Overview** screen.
2. Under **Device Templates**, right-click the device template and click **Rename**.
3. Type the new name for the device template.

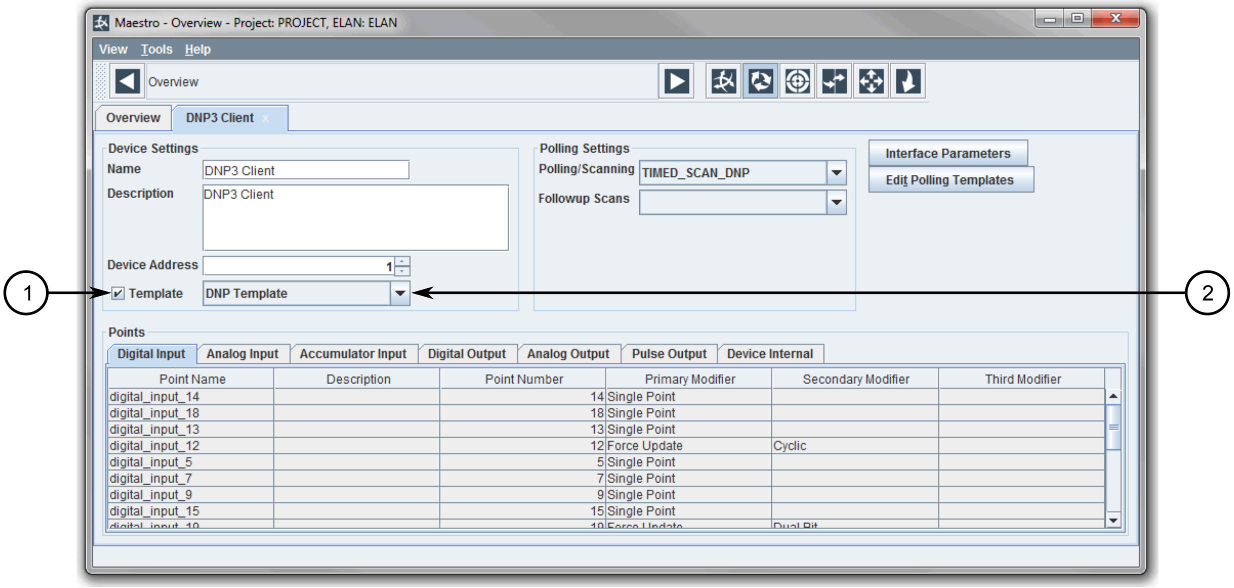
Section 4.8.6

Using a Device Template

To use a device template for a server or client device, do the following:

> **IMPORTANT!**
> *When associating a device with a template, all points are aligned with those defined in the device template.*

1. Navigate to the **Overview** screen.
2. Under **RUGGEDCOM ELAN server Devices** or **RUGGEDCOM ELAN Client Devices**, right-click a device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP3 Client

Description: DNP3 Client

Device Address: 1

☑ Template: DNP Template

Polling Settings

Polling/Scanning: TIMED_SCAN_DNP

Followup Scans:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_14		14	Single Point		
digital_input_18		18	Single Point		
digital_input_13		13	Single Point		
digital_input_12		12	Force Update	Cyclic	
digital_input_5		5	Single Point		
digital_input_7		7	Single Point		
digital_input_9		9	Single Point		
digital_input_15		15	Single Point		
digital_input_10		10	Force Update	Dual Bit	

Figure 53: Device Properties (Example)

1. Template Check Box   **2.** Template List

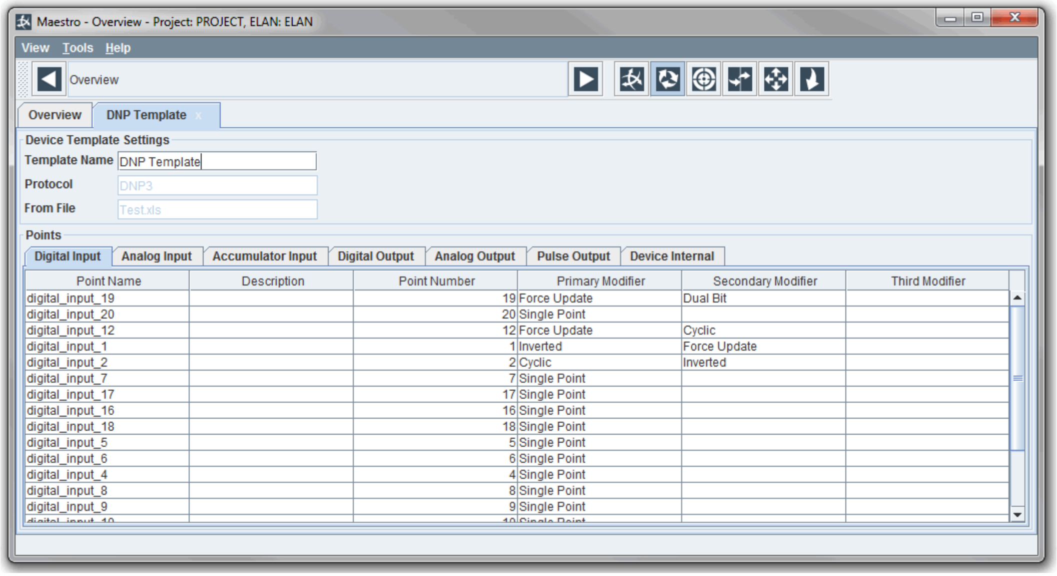
3. Under **Device Settings**, select a template from the **Template** list.
4. Select the **Template** check box.
5. A confirmation dialog box appears. Click **Yes** to confirm or **No** to cancel.

Section 4.8.7

Configuring a DNP Template

To configure a DNP template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP template and click **Properties**. The template's properties appear in a new tab.



Device Template Settings

Template Name: DNP Template

Protocol: DNP3

From File: Test.xls

Points

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_19		19	Force Update	Dual Bit	
digital_input_20		20	Single Point		
digital_input_12		12	Force Update	Cyclic	
digital_input_1		1	Inverted	Force Update	
digital_input_2		2	Cyclic	Inverted	
digital_input_7		7	Single Point		
digital_input_17		17	Single Point		
digital_input_16		16	Single Point		
digital_input_18		18	Single Point		
digital_input_5		5	Single Point		
digital_input_6		6	Single Point		
digital_input_4		4	Single Point		
digital_input_8		8	Single Point		
digital_input_9		9	Single Point		

Figure 54: DNP Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Single Point, Fleeting, Force Update, Cyclic, Inverted } The primary modifier. Options include: • `Single Point` – Use to identify a single status point. • `Fleeting` – Identifies a point that changes value temporarily, then changes back to its normal value. • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.
Secondary Modifier	**Synopsis:** { Cyclic, Inverted, Force Update, Dual Bit } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored.

Parameter	Description
	• `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device. • `Dual Bit` – Use to identify the first of two sequential single status points that are reported together as one point.
Third Modifier	**Synopsis:** { Cyclic, Inverted, Force Update, Dual Bit } The third modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device. • `Dual Bit` – Use to identify the first of two sequential single status points that are reported together as one point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Float, BCD, DAC, 16 Bit, Unipolar, 32 Bit } The primary modifier. Options include: • `Float` – Use to identify a point that is reported in IEEE floating point format. • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. • `16 Bit` – Use to identify a 16-Bit 2's complement point that is to be processed as a 16-Bit 2's complement value without any scaling applied. • `Unipolar` – Use to identify a 16-Bit or 32-Bit point that is always positive in value. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Secondary Modifier	**Synopsis:** { Cyclic, Force Update, Time Tagged, Negated, Scaled, 32 Bit } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Time Tagged` – Use to indicate the time tag will be stored.

Parameter	Description
	• `Negated` – Use to identify a point whose value has been negated (i.e. multiplied by -1) when it is stored in the database before being reported to the host. • `Scaled` – Use to restore an analog value to its raw value after it has been scaled at the remote device. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, 16 Bit or 32 Bit } The primary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `16 Bit or 32 Bit` – Use to identify a 16-Bit or 32-Bit binary accumulator input point.
Secondary Modifier	**Synopsis:** { Cyclic } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Close Trip Pair, Trip Close Pair, Single Point, Latch, Momentary } The primary modifier. Options include:

Parameter	Description
	• `Close Trip Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Trip Close Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. This indicates the control message sent to the RTU should include the latching option.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { 16 Bit } The primary modifier. Options include: • `16 Bit` – Use to identify a 16-Bit 2's complement analog output.
Units	A text field.

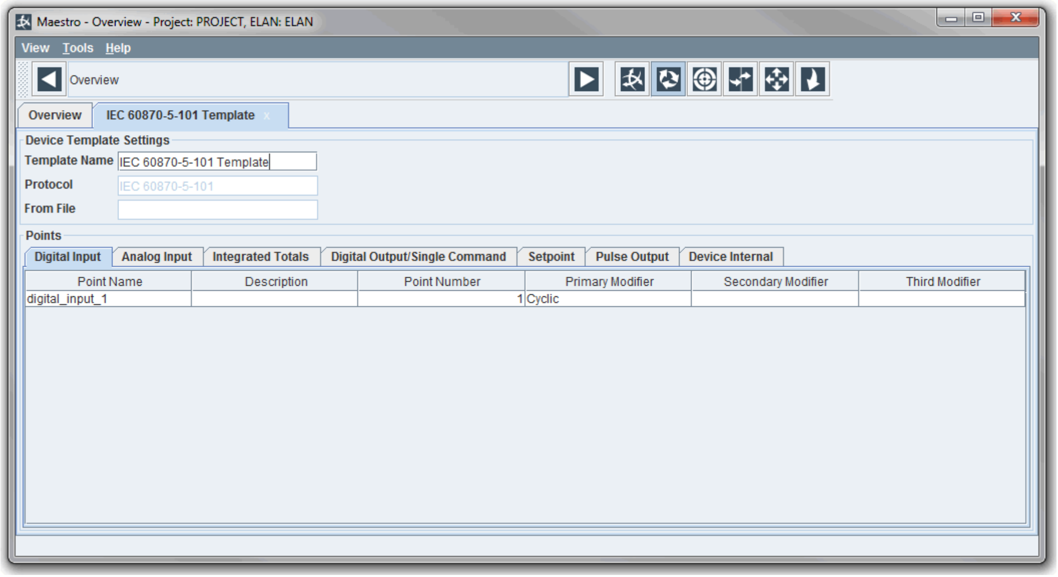
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.8

Configuring an IEC 60870-5-101 Template

To configure an IEC 60870-5-101 template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 template and click **Properties**. The template's properties appear in a new tab.



Maestro - Overview - Project: PROJECT, ELAN: ELAN

Device Template Settings

Template Name: IEC 60870-5-101 Template

Protocol: IEC 60870-5-101

From File:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Cyclic		

Figure 55: IEC 60870-5-101 Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant, Cyclic } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.

Parameter	Description
	• Cyclic – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The secondary modifier. Options include: • Fleeting – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • Single Point – Use to identify a single status point. • Bit Pair – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • Two Sequential Points – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • Redundant – Use to identify a point change of state and a time-tagged change of state are reported separately.
Third Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The third modifier. Options include: • Fleeting – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • Single Point – Use to identify a single status point. • Bit Pair – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • Two Sequential Points – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • Redundant – Use to identify a point change of state and a time-tagged change of state are reported separately.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, Force Update, BCD, DAC, 16 Bit } The primary modifier. Options include:

Parameter	Description
	• Force Update – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • BCD – Use to identify an analog input that is interpreted as a BCD value. • DAC – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • 16 Bit – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • Cyclic – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Cyclic, Force Update, BCD, DAC, 16 Bit } The secondary modifier. Options include: • Force Update – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • BCD – Use to identify an analog input that is interpreted as a BCD value. • DAC – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • 16 Bit – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • Cyclic – Use if cyclic reporting of a point is to be monitored.
Third Modifier	**Synopsis:** { Cyclic, Force Update, BCD, DAC, 16 Bit } The third modifier. Options include: • Force Update – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • BCD – Use to identify an analog input that is interpreted as a BCD value. • DAC – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • 16 Bit – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • Cyclic – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

›› Integrated Totals

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. integrated_totals_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, 32 Bit } The primary modifier. Options include: • Cyclic – Use if cyclic reporting of a point is to be monitored.

Parameter	Description
	• `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Secondary Modifier	**Synopsis:** { Cyclic } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Units	A text field.

Digital Output/Single Command

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_single_command_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Momentary, Single Point, Latch, Preconfig } The primary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).
Secondary Modifier	**Synopsis:** { Momentary, Single Point, Preconfig } The secondary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).

›› Setpoint

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. setpoint_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Units	A text field.

›› Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

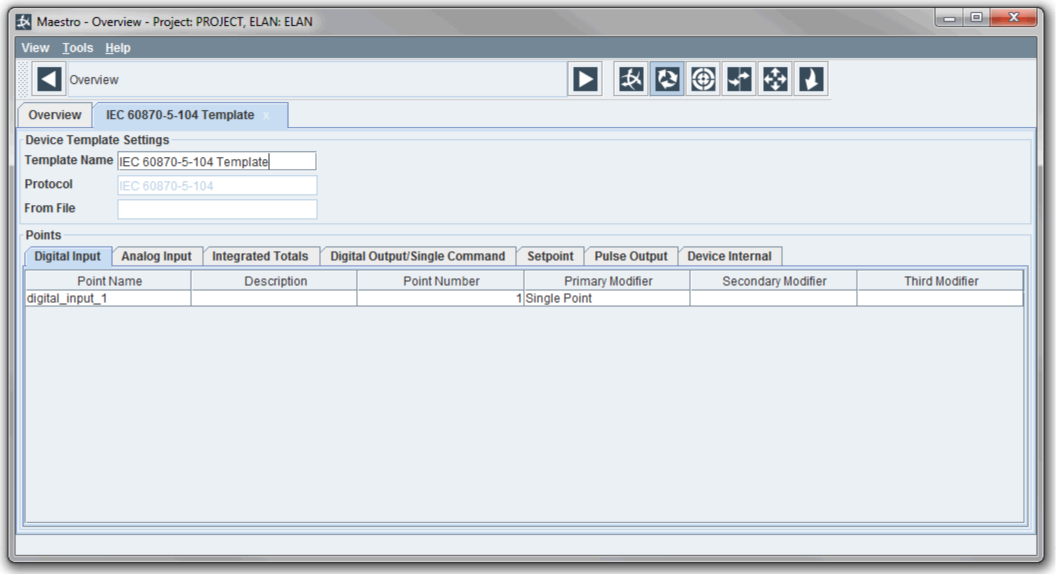
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.9

Configuring an IEC 60870-5-104 Template

To configure an IEC 60870-5-104 template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 template and click **Properties**. The template's properties appear in a new tab.



Device Template Settings

Template Name: IEC 60870-5-104 Template

Protocol: IEC 60870-5-104

From File:

Points

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Single Point		

Figure 56: IEC 60870-5-104 Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant, Cyclic } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.

Parameter	Description
	• `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The secondary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.
Third Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The third modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.

›› Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Force Update, BCD, DAC, 16 Bit, Cyclic } The primary modifier. Options include:

Parameter	Description
	• `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { BCD, DAC, 16 Bit, Cyclic } The secondary modifier. Options include: • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

Integrated Totals

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. integrated_totals_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, 32 Bit } The primary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Secondary Modifier	**Synopsis:** { Cyclic } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Units	A text field.

Digital Output/Single Command

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_single_command_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Momentary, Single Point, Latch, Preconfig } The primary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. This indicates the control message sent to the RTU should include the latching option. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).
Secondary Modifier	**Synopsis:** { Momentary, Single Point, Preconfig } The secondary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).

Setpoint

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. setpoint_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Units	A text field.

›› Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

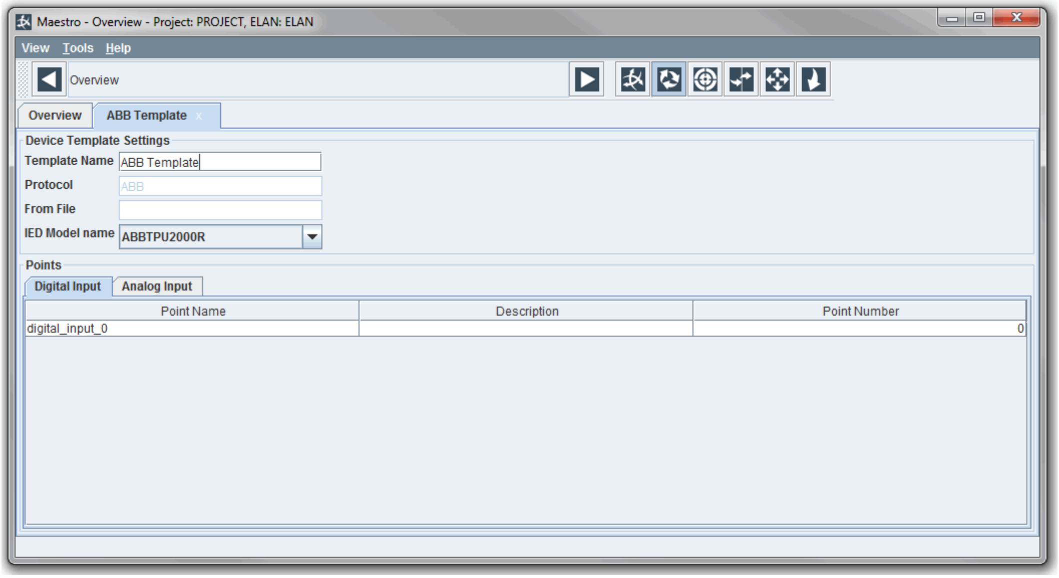
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.10

Configuring an ABB Template

To configure an ABB template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the ABB template and click **Properties**. The template's properties appear in a new tab.



Device Template Settings

Template Name: ABB Template

Protocol: ABB

From File:

IED Model name: ABBTPU2000R

Points

Point Name	Description	Point Number
digital_input_0		0

Figure 57: ABB Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

›› Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

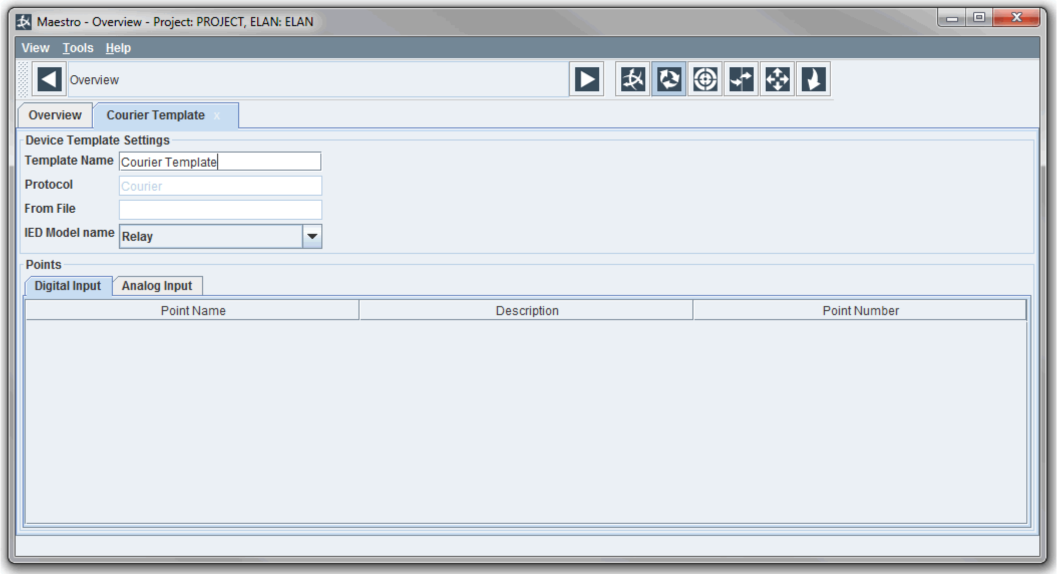
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.11

Configuring a Courier Template

To configure a Courier template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Courier template and click **Properties**. The template's properties appear in a new tab.



Template Name: Courier Template

Protocol: Courier

From File:

IED Model name: Relay

Figure 58: Courier Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.

Parameter	Description
Units	A text field.

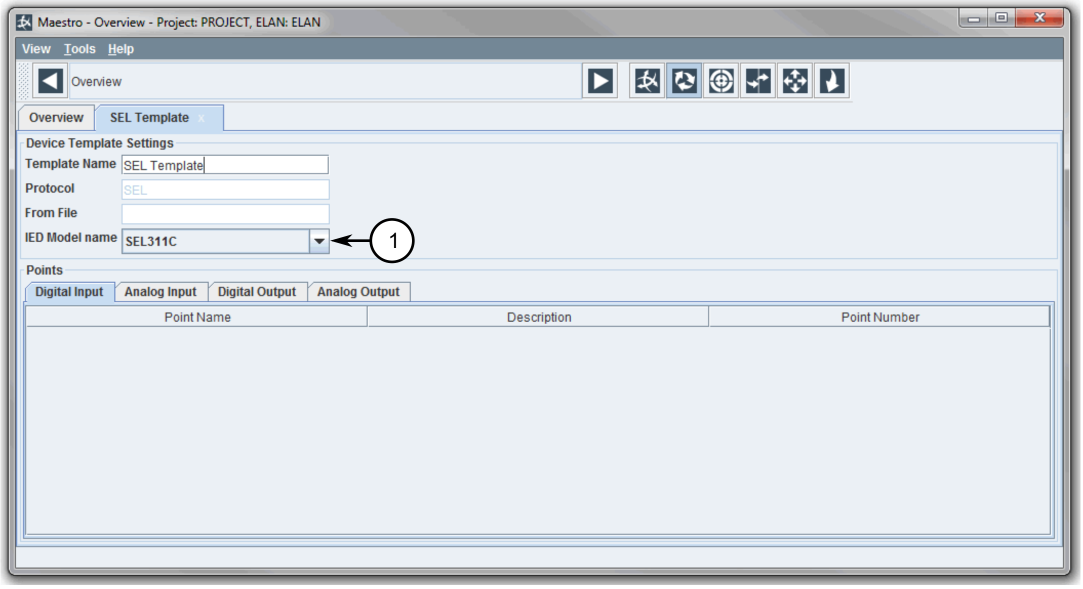
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.12

Configuring an SEL Template

To configure an SEL template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL template and click **Properties**. The template's properties appear in a new tab.



Template Name: SEL Template

Protocol: SEL

From File:

IED Model name: SEL311C

Point Name	Description	Point Number

Figure 59: SEL Template Properties

1. IED Model Name List

3. Under **IED Model Name**, select an SEL Relay type.
4. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .
5. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.

Parameter	Description
Point Number	The number assigned to the point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

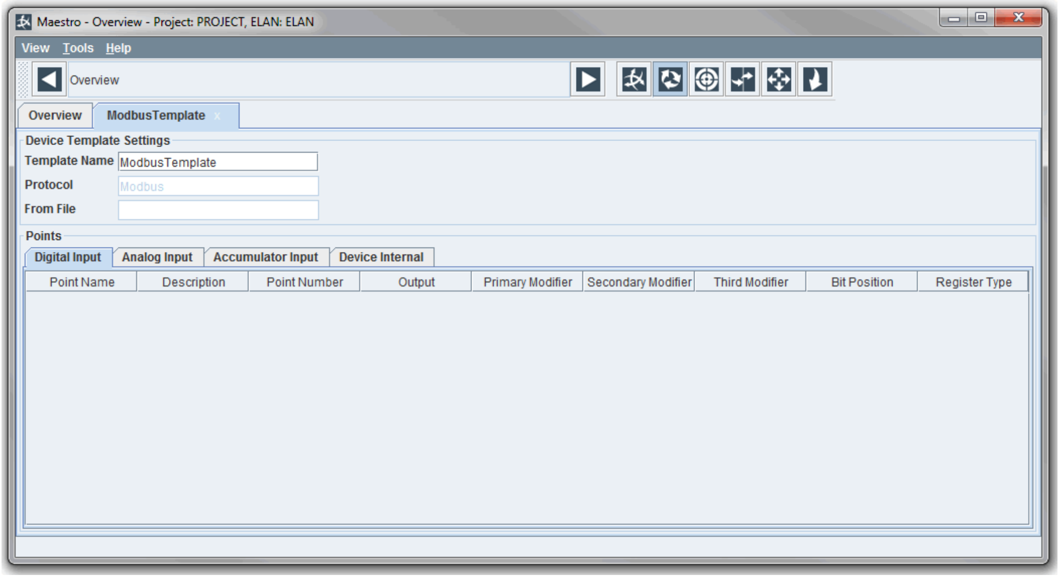
6. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.13

Configuring a Modbus Template

To configure a Modbus template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus template and click **Properties**. The template's properties appear in a new tab.



Maestro - Overview - Project: PROJECT, ELAN: ELAN

Template Name: ModbusTemplate

Protocol: Modbus

From File:

Figure 60: Modbus Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, "Adding/Deleting Points" .
4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Output	**Default State:** Disabled When enabled (selected), the output point is present for this input point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0).

Parameter	Description
	• `Single Point` – Use to identify a single status point. **NOTE** *Bit Pair points must reside with the returned data field boundaries. For bit-pair entries, only the first point is configured.* • `Bit Pair` – Use to combine two sequential single status points that are reported together as one point. The two state bits combined represent one of four possible states for the point. Bit pair points may be mixed with single status points within data field boundaries (one byte) reported by the RTU.
Secondary Modifier	**Synopsis:** { Force Update, Inverted } The secondary modifier. Options include: • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.
Third Modifier	**Synopsis:** { Force Update, Inverted } The third modifier. Options include: • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Output	**Default State:** Disabled When enabled (selected), the output point is present for this input point.
Primary Modifier	**Synopsis:** { 16 Bit, Float, 32 Bit } The primary modifier. Options include: • `16 Bit` – Use to identify a 16-Bit binary analog input or a 10-bit binary analog input point occupying a 16-bit data field with the six most significant bits set to zero. **NOTE** *Float and 32 Bit points require Maestro to process two points as a single entity. As such, if, when mapping server and client points, the user selects an analog input point (e.g. Point #1) and another analog input number exists with the next point number assigned (e.g. Point #2), Maestro*

Parameter	Description
	*automatically pairs the two points together. The point with the lowest number is considered the **Master Point**, while the other point is the **Secondary Point**.* *The **Secondary Point** is rendered non-editable (grayed-out) and assigned the same modifier as the **Master Point**.* *If the **Master Point** has an output point associated with it, an output point is automatically created for the **Secondary Point** if one does not already exist. However, if the **Master Point** does not have an output point associated with it, but the **Secondary Point** does, the output point for the **Secondary Point** is deleted to mirror the **Master Point**.* *Alternatively, if the user selects an analog input point for which there does not exist another analog input point with the next point number, Maestro silently creates the second analog input point. The second analog input will not be visible to the user and will be replaced if the user creates a new analog input point with the next point number.* *For more information about mapping Modbus analog points, and other types of points, refer to Section 4.12.1, "Mapping Server and Client Points" .* • `Float` – Use to identify analog inputs that are reported together as one point. A 32-bit floating point value is reported by two sequential registers, which are reported together as one point. An RTU may report a mix of floating points and non-floating points. Both registers containing a floating point value must be reported with the same RTU message. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Secondary Modifier	**Synopsis:** { Force Update, Scaled } The secondary modifier. Options include: • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Scaled` – Use to identify an analog point whose raw value should be stored in the database. The client process will calculate the raw value and store it in the database.
Register Type	**Synopsis:** { Holding, Input } The register type. Options include: • `Holding` – Use to identify Holding Registers • `Input` – Use to identify Input Registers
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Register Type	**Synopsis:** { Holding, Input } The register type. Options include: • `Holding` – Use to identify Holding Registers • `Input` – Use to identify Input Registers
Units	A text field.

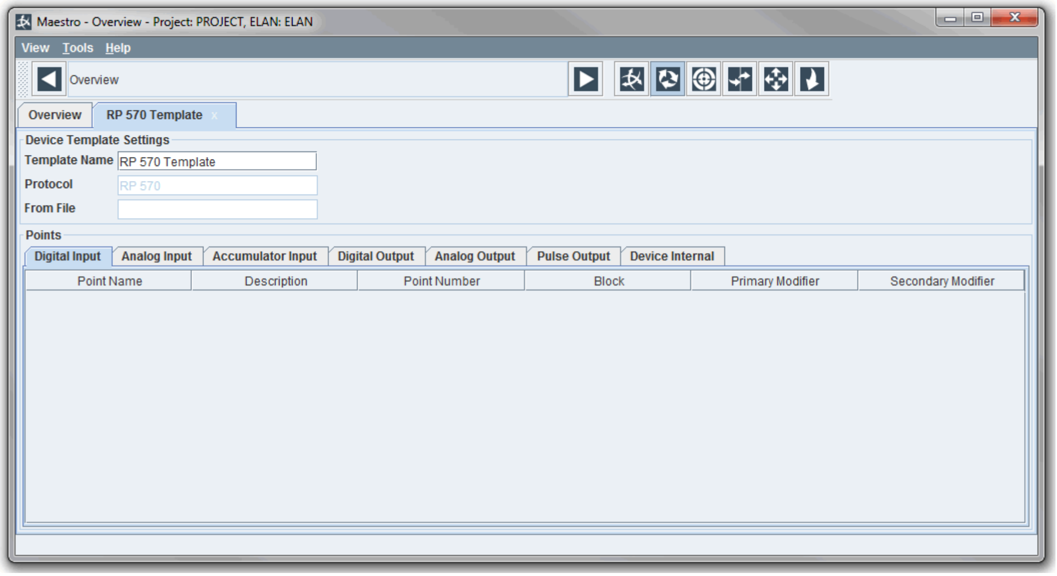
5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

Section 4.8.14

Configuring an RP 570 Template

To configure an RP 570 template, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RP 570 template and click **Properties**. The template's properties appear in a new tab.



Template Name: RP 570 Template
Protocol: RP 570
From File:

Point Name	Description	Point Number	Block	Primary Modifier	Secondary Modifier

Figure 61: RP 570 Template Properties

3. Add one or more points. For more information, refer to Section 4.8.16.2, “Adding/Deleting Points” .

4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Primary Modifier	**Synopsis:** { Two Sequential Points, Single Point } The primary modifier. Options include: • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as one point. The two state bits combined represent one of four possible states for the point. • `Single Point` – Use to identify a single status point.
Secondary Modifier	**Synopsis:** { Redundant } The primary modifier. Options include: • `Redundant` – Use to identify SOE points in protocols where a change of state of SOE points and a time tagged change of state are reported separately.

›› Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Primary Modifier	**Synopsis:** { Unipolar, 16 Bit } The primary modifier. Options include: • `Unipolar` – Use to identify a 12-bit analog input that is always positive in value. • `16 Bit` – Use to identify a 12-Bit 2's complement, 12-bit 2's complement with sign extended to 16-bit, and digital coded analog points.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Primary Modifier	**Synopsis:** { Close Trip Pair, Trip Close Pair, Single Point, Momentary } The primary modifier. Options include: • `Close Trip Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Trip Close Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests. • `Single Point` – Use when a single relay is used to trip (OFF) or close (ON) an external device. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host.
Secondary Modifier	**Synopsis:** { Inverted } The secondary modifier. Options include: • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Units	A text field.

Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Primary Modifier	**Synopsis:** { Single Point, Lower Raise Pair, Raise Lower Pair, Momentary } The primary modifier. Options include: • `Single Point` – Use when a single relay is used to raise or lower an external device. • `Lower Raise Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Raise Lower Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests.
Secondary Modifier	**Synopsis:** { Inverted } The secondary modifier. Options include: • `Inverted` – Inverts the action sent to the remote device.

5. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.8.15, “Enabling/Disabling Device Internal Points” .

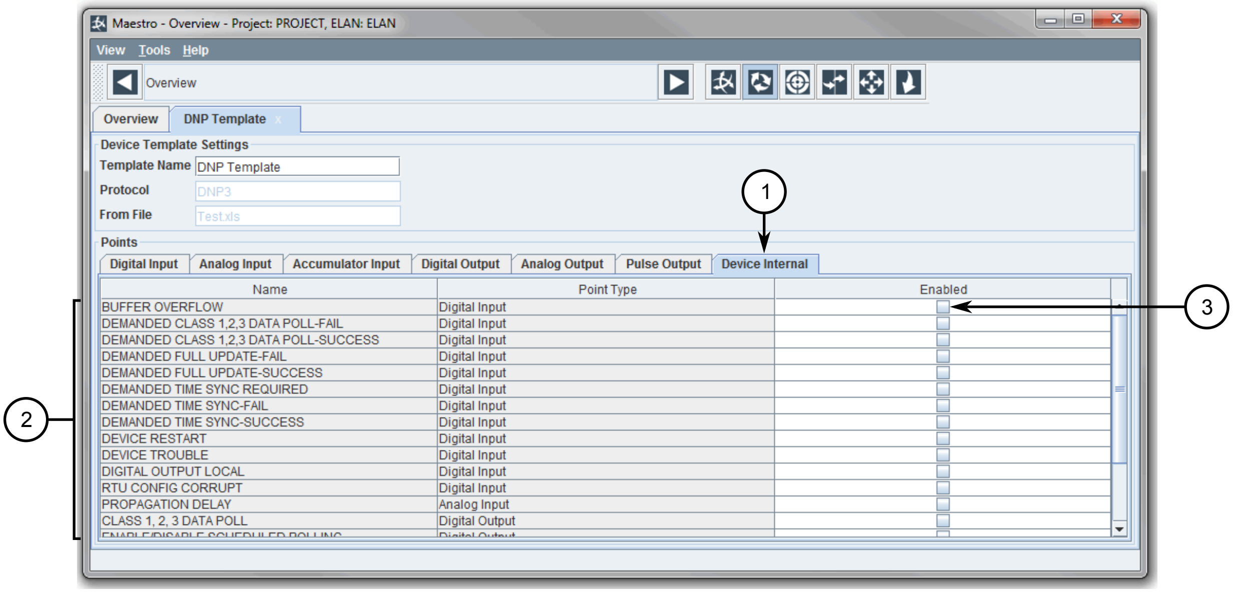
Section 4.8.15

Enabling/Disabling Device Internal Points

Device internal points are optional predefined points that indicate the status of a remote device. They are only available for remote client devices. For more information, refer to the remote client device's user documentation.

To enable/disable device internal points for a client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the template and click **Properties**. The device's properties appear in a new tab.
3. Under **Points**, select the **Device Internal** tab.



Template Name: DNP Template
Protocol: DNP3
From File: Test.xls

Name	Point Type	Enabled
BUFFER OVERFLOW	Digital Input	□
DEMANDED CLASS 1,2,3 DATA POLL-FAIL	Digital Input	□
DEMANDED CLASS 1,2,3 DATA POLL-SUCCESS	Digital Input	□
DEMANDED FULL UPDATE-FAIL	Digital Input	□
DEMANDED FULL UPDATE-SUCCESS	Digital Input	□
DEMANDED TIME SYNC REQUIRED	Digital Input	□
DEMANDED TIME SYNC-FAIL	Digital Input	□
DEMANDED TIME SYNC-SUCCESS	Digital Input	□
DEVICE RESTART	Digital Input	□
DEVICE TROUBLE	Digital Input	□
DIGITAL OUTPUT LOCAL	Digital Input	□
RTU CONFIG CORRUPT	Digital Input	□
PROPAGATION DELAY	Analog Input	□
CLASS 1, 2, 3 DATA POLL	Digital Output	□
ENABLE/DISABLE SCHEDULED POLLING	Digital Output	□

Figure 62: Device Internal Tab (Example)

1. Device Internal Tab **2.** Supported Device Internal Points **3.** Enable Check Box

4. For each device internal point, click the associated **Enable** check box to enable the point, or clear the **Enable** check box to disable it.

Section 4.8.16

Managing Points for Templates

This section describes how to manage points for templates in Maestro.

CONTENTS

- Section 4.8.16.2, “Adding/Deleting Points”

Section 4.8.16.1
Importing/Exporting Points

Points can be imported from or exported to a Microsoft® Excel spreadsheet to facilitate the quick configuration of device templates.

To import or export points, do the following:

›› Importing Points

1. Navigate to **Overview**, right-click the desired template and click **Import**. The **Open** dialog box appears.

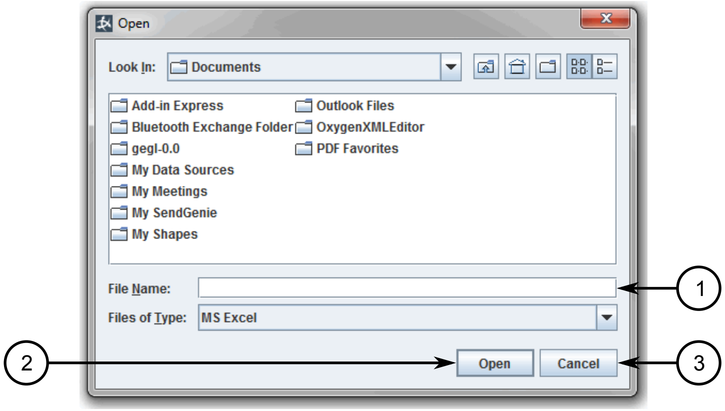


Figure 63: Open Dialog Box

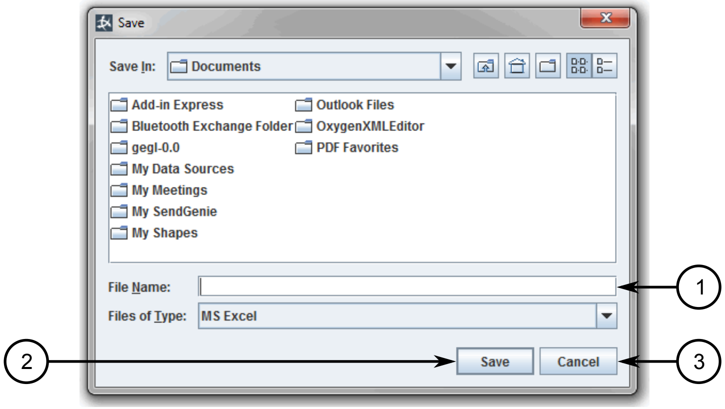
1. File Name Box **2.** Open Button **3.** Cancel Button

2. Navigate to and select the desired Excel spreadsheet.
3. Click **Open** to import the spreadsheet, or click **Cancel** to abort.

   If Maestro detects a problem with the points being imported, a dialog box appears detailing the errors. Remove or fix the affected points in the spreadsheet and then repeat this procedure.

›› Exporting Points

1. Navigate to **Overview**, right-click the desired template and click **Export**. The **Save** dialog box appears.



Save In: Documents

Files of Type: MS Excel

Figure 64: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

2. Navigate to and select the drive or folder where the Excel spreadsheet will be saved.
3. Under **File Name**, type a name for the spreadsheet.
4. Click **Save** to save the spreadsheet, or click **Cancel** to abort.

Section 4.8.16.2

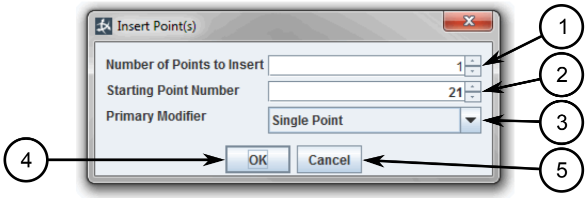
Adding/Deleting Points

New points can be imported from a Microsoft® Excel spreadsheet or they can be created from scratch.

To import/create points or delete points, do the following:

›› Adding Points

1. Navigate to the **Overview** screen.
2. Right-click the device template and click **Properties**. The template's properties appear in a new tab.
3. Under **Points**, select the desired tab. Each tab represents a point type.
4. Right-click anywhere on the table to open the shortcut menu and select **Insert Point(s)**. The **Insert Point(s)** dialog box appears.



Number of Points to Insert 1

Starting Point Number 21

Primary Modifier Single Point

Figure 65: Insert Point(s) Dialog Box

1. Number of Points to Insert Box **2.** Starting Point Number Box **3.** Primary Modifier **4.** OK Button **5.** Cancel Button

NOTE
An alternative method to consider for creating multiple points is to add and configure only one point, then export the points to a Microsoft® Excel spreadsheet where additional points can be added. The spreadsheet can be later imported. For more information about importing and exporting points for device templates, refer to Section 4.8.16.1, "Importing/Exporting Points" .

5. Configure the following parameters as required:

Parameter	Description
Number of Points to Insert	**Synopsis:** 1 to 65536 **Synopsis:** 1 The number of points to insert.
Starting Point Number	**Synopsis:** 1 to 65535 **Synopsis:** 1 The number assigned to the first label. All other points added will be assigned a sequential number. **NOTE** *If one or more point numbers are already in use, the row for each duplicate point in the list will be red. This can only be cleared by renaming the point.*
Primary Modifier	The primary modifier. Options are dependent on the protocol and point type. • For more information about **Primary Modifier** options for DNP templates, refer to Section 4.8.7, "Configuring a DNP Template" • For more information about **Primary Modifier** options for IEC 60870-5-101 templates, refer to Section 4.8.8, "Configuring an IEC 60870-5-101 Template" • For more information about **Primary Modifier** options for IEC 60870-5-104 templates, refer to Section 4.8.9, "Configuring an IEC 60870-5-104 Template" • For more information about **Primary Modifier** options for ABB templates, refer to Section 4.8.10, "Configuring an ABB Template" • For more information about **Primary Modifier** options for Courier templates, refer to Section 4.8.11, "Configuring a Courier Template" • For more information about **Primary Modifier** options for SEL templates, refer to Section 4.8.12, "Configuring an SEL Template" • For more information about **Primary Modifier** options for Modbus templates, refer to Section 4.8.13, "Configuring a Modbus Template" • For more information about **Primary Modifier** options for RP 570 templates, refer to Section 4.8.14, "Configuring an RP 570 Template"

6. Click **OK** to add the points, or click **Cancel** to abort.
7. [Optional] Further configure each point.
   - For more information about configuring points for a DNP template, refer to Section 4.8.7, "Configuring a DNP Template"
   - For more information about configuring points for an IEC 60870-5-101 template, refer to Section 4.8.8, "Configuring an IEC 60870-5-101 Template"

- For more information about configuring points for an IEC 60870-5-104 template, refer to Section 4.8.9, "Configuring an IEC 60870-5-104 Template"
- For more information about configuring points for an ABB template, refer to Section 4.8.10, "Configuring an ABB Template"
- For more information about configuring points for a Courier template, refer to Section 4.8.11, "Configuring a Courier Template"
- For more information about configuring points for an SEL template, refer to Section 4.8.12, "Configuring an SEL Template"
- For more information about configuring points for a Modbus template, refer to Section 4.8.13, "Configuring a Modbus Template"
- For more information about configuring points for an RP 570 template, refer to Section 4.8.14, "Configuring an RP 570 Template"

›› Deleting Points

1. Navigate to the **Overview** screen.
2. Right-click the device template and click **Properties**. The template's properties appear in a new tab.
3. Under **Points**, select the desired tab. Each tab represents a point type.
4. Select one or more points from the table.
5. Right-click the selected point(s) to open the shortcut menu and click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the point(s), or click **No** to abort.

Section 4.9

Managing Server Devices

A server device in Maestro is a Virtual Remote Terminal Unit (VRTU) or slave. It works on behalf of external clients (Masters) to autonomously poll one or more one or more SCADA devices (e.g. IEDs/RTUs) for telemetry/point data and issue commands.

CONTENTS

- Section 4.9.7, "Managing RUGGEDCOM REFLEX Server Devices"

Section 4.9.1

Adding/Deleting a Server Device

To add or delete a new server device, do the following:

> **NOTE**
> *Only one RUGGEDCOM REFLEX server can be created for a RUGGEDCOM ELAN server.*

> **NOTE**
> *For each DNP 3.0 and IEC 60870-5-104 server device added to the RUGGEDCOM ELAN server, a virtual device, associated client device and route is added to the Protocol Router configuration. For more information, refer to Section 4.14.8, "Managing Virtual Devices" .*

Adding a Server Device

1. Navigate to the **Overview** screen.
2. Add the server device by doing one of the following:

   > **NOTE**
   > *Device templates are not available for Jazz and RUGGEDCOM REFLEX server devices.*

   > **NOTE**
   > *If templates are not available or a new template is required, add a template. For more information, refer to Section 4.8.4, "Adding/Deleting a Device Template" .*

   - **Using a Template**
     Under ***Device Templates » {protocol}*** , right-click the desired template and click **New Server Device**.
   - **Without a Template**
     Under **RUGGEDCOM ELAN server Devices**, right-click the desired protocol and click **New Device**.
3. Configure the server device:
   - For DNP server devices, refer to Section 4.9.4, "Managing DNP Server Devices"
   - For IEC 60870-5-101 server devices, refer to Section 4.9.5, "Managing IEC 60870-5-104 Server Devices"
   - For Jazz server devices, refer to Section 4.9.6.1, "Configuring a Jazz Server"
   - For RUGGEDCOM REFLEX server devices, refer to Section 4.9.7, "Managing RUGGEDCOM REFLEX Server Devices"

Deleting a Server Device

1. Navigate to the **Overview** screen.
2. Under ***RUGGEDCOM ELAN server Devices » {protocol}*** , right-click the desired server device and click **Delete**. A confirmation message appears.
3. Click **Yes** to delete the server device, or click **No** to abort.

Section 4.9.2

Renaming a Server Device

To rename a server device, do the following:

1. Navigate to the **Overview** screen.
2. Under ***RUGGEDCOM ELAN server Devices*** » ***{protocol}*** , right-click the desired server device and click **Rename**.
3. Type the new name for the server device.

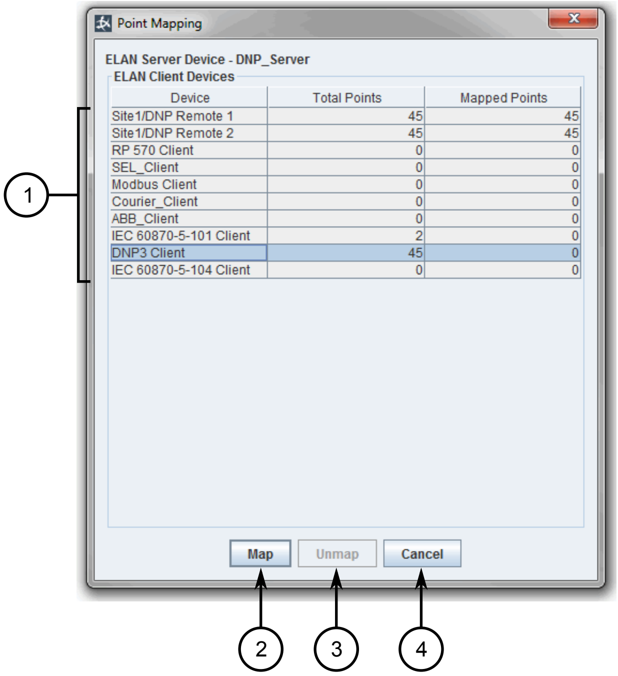
Section 4.9.3

Mapping/Unmapping Points for a Server

To map or unmap points for a server device, do the following:

> **NOTE**
> *During the automatic mapping of points for an IEC 61850 Server, Maestro will detect when it is mapping a Data attribute of the type* ***dbpos****, or* ***dual-bit position****. If the Data attribute is configured as a* ***dual-bit****, Maestro will automatically map the point as a digital output on the server side. However, if the Data attribute is configured as a* ***dual-bit split****, Maestro will automatically create two consecutive points on the server side and map the corresponding bits of the dual-bit position Data attribute.*
>
> *For information about mapping points manually between servers and clients, refer to Section 4.12.1, "Mapping Server and Client Points" .*

1. Navigate to the **Overview** screen.
2. Right-click the desired server device and click **Point Mapping**. The **Point Mapping** dialog box appears.



ELAN Server Device - DNP_Server

ELAN Client Devices

Device	Total Points	Mapped Points
Site1/DNP Remote 1	45	45
Site1/DNP Remote 2	45	45
RP 570 Client	0	0
SEL_Client	0	0
Modbus Client	0	0
Courier_Client	0	0
ABB_Client	0	0
IEC 60870-5-101 Client	2	0
DNP3 Client	45	0
IEC 60870-5-104 Client	0	0

Figure 66: Point Mapping Dialog Box (Example)

1. Available Devices **2.** Map Button **3.** Unmap Button **4.** Cancel Button

3. Select the desired device from the list. If the device was previously mapped, the **Map** button is enabled. Otherwise, the **Unmap** button is enabled.
4. Click either **Map** or **Unmap**. Mapping adds the points from the selected device to the server. Unmapping removes the points previously added from the selected device.

Section 4.9.4

Managing DNP Server Devices

This section describes how to configure and manage DNP server devices.

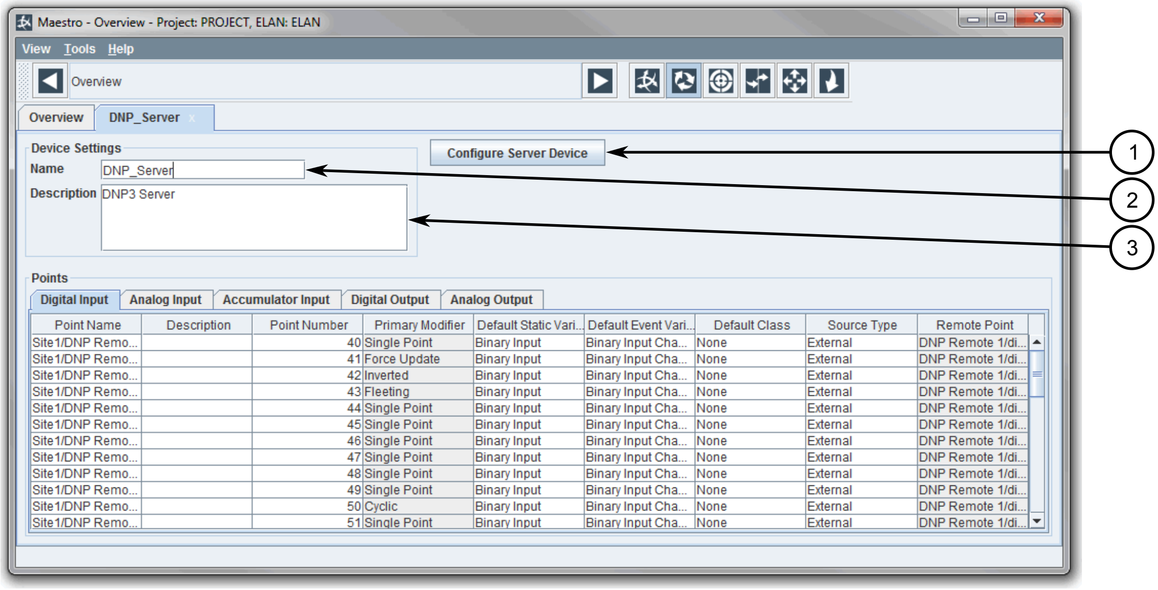
CONTENTS

- Section 4.9.4.8, “Exporting Server Points”

Section 4.9.4.1
Configuring DNP Server

To configure a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP server device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP_Server

Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 67: DNP Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the server device.
Description	A description of the server device.

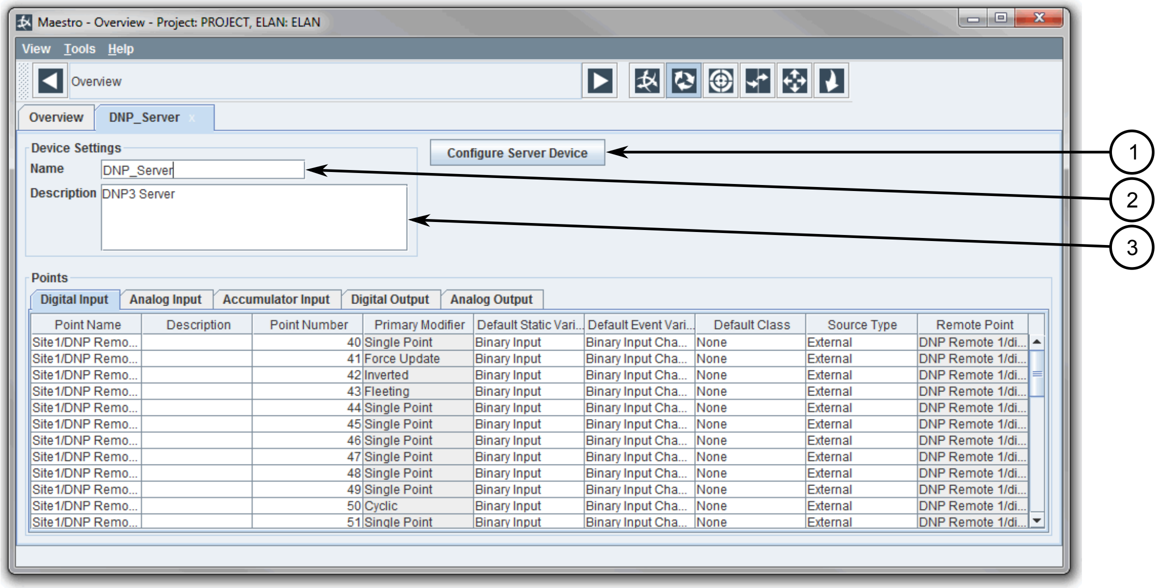
4. [Optional] Configure the advanced settings for the server. For more information, refer to Section 4.9.4.2, “Configuring Advanced Settings” .
5. [Optional] Configure the protocol settings for the server. For more information, refer to Section 4.9.4.3, “Configuring Protocol Settings” .
6. [Optional] Configure masters for the server. For more information, refer to Section 4.9.4.4, “Configuring Masters” .

Section 4.9.4.2

Configuring Advanced Settings

To configure advanced settings for a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Name: DNP_Server

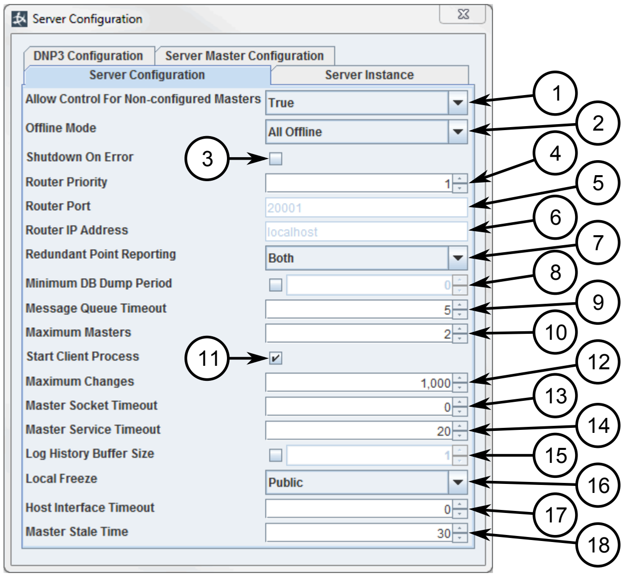
Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 68: DNP Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.



Allow Control For Non-configured Masters	True
Offline Mode	All Offline
Shutdown On Error	□
Router Priority	1
Router Port	20001
Router IP Address	localhost
Redundant Point Reporting	Both
Minimum DB Dump Period	□ 0
Message Queue Timeout	5
Maximum Masters	2
Start Client Process	☑
Maximum Changes	1,000
Master Socket Timeout	0
Master Service Timeout	20
Log History Buffer Size	□ 1
Local Freeze	Public
Host Interface Timeout	0
Master Stale Time	30

Figure 69: Server Configuration Tab

1. Allow Control For Non-configured Masters List **2.** Offline Mode List **3.** Shutdown On Error Check Box **4.** Router Priority Box **5.** Router Port **6.** Router IP Address **7.** Redundant Point Reporting List **8.** Minimum DB Dump Period Check Box and Box **9.** Message Queue Timeout Box **10.** Maximum Masters Box **11.** Start Client Process Check Box **12.** Maximum Changes Box **13.** Master Socket Timeout Box **14.** Master Service Timeout **15.** Log History Buffer Size Check Box and Box **16.** Local Freeze List **17.** Host Interface Timeout Box **18.** Master Stale Time Box

4. Configure the following parameters as required:

Parameter	Description
Allow Control for non-configured masters	**Synopsis:** { True, False, Freeze Only } **Default:** True Controls whether or not a master not explicitly defined the server's database is allowed to execute control operations on this remote device. Options include: • `True` – Any master is allowed to control this remote device • `False` – Masters not explicitly defined are not allowed to control this remote device. This is recommended for most new applications. • `Freeze Only` – Masters not explicitly defined are only allowed to execute the Immediate Freeze command.
Offline Mode	**Synopsis:** { Never, One Offline, All Offline } **Default State:** All Offline Controls how the server will respond when physical RTUs assocaite with the server fail. Options include: • `Never` – The server remains online. • `One Offline` – The server stops responding if one or more associated RTUs fail. • `All Offline` – The server stops responding if all associated RTUs fail.
Shutdown on error	**Default State:** Disabled

Parameter	Description
	When enabled (selected), RUGGEDCOM ELAN applications are forced to shut down when a fatal error occurs in the server process.
Router Priority	**Synopsis:** 1 to 100 **Default:** 1 This defines a numeric priority that affects which communication path is selected by the router when there is more than one way to reach a given device. The lower the number, the higher the priority.
Redundant Point Reporting	**Synopsis:** { Both, Both to External ELAN, COS Only, Redundant Only } **Default:** Both Determines how the RUGGEDCOM ELAN IEC 104 host will report redundant Sequence Of Event (SOE) points. Options include: • `Both` – Both redundant and Change Of State (COS) events are reported using their configured Default Event Variation. • `COS Only` – Only the COS event is reported using its configured Default Event Variation. The redundant event is suppressed. • `Redundant Only` – Only the redundant event is reported using its configured Default Event Variation. The COS event is suppressed. • `Both To External ELAN` – When a TIE IEC 104 remote process is communicating with the server process, both redundant and COS events are reported to the IEC 104 remote process. This upstream TIE will correctly interpret the redundant and COS events as long as: ▫ the corresponding points are configured as REDUNDANT in both system ▫ the server point is configured to report its Default Event Variation with time The redundant event is reported using its configured Default Event Variation. The COS event is reported without time.
Minimum DB Dump Period	**Synopsis:** 0 to 600000 **Default:** 0 **Default State:** Disabled The minimum rate in milliseconds (ms) at which to dump the local database to a file. The suggested value is 60,000 milliseconds (1 minute).
Message Queue Timeout	**Synopsis:** 0 to 30000 **Default:** 5 The maximum amount of time in milliseconds (ms) to wait at the message queue for the receipt of a message.
Maximum Masters	**Synopsis:** 1 to 100 **Default:** 2 The maximum number of masters permitted to communicate with this server at a time.
Start Client Process	**Default State:** Enabled When enabled (selected), the associated RUGGEDCOM ELAN client process is placed into Normal mode at start-up. If disabled (cleared), the associated RUGGEDCOM ELAN client process is placed into Standby mode at start-up.
Maximum Changes	**Synopsis:** 100 to 100000 **Default:** 1000

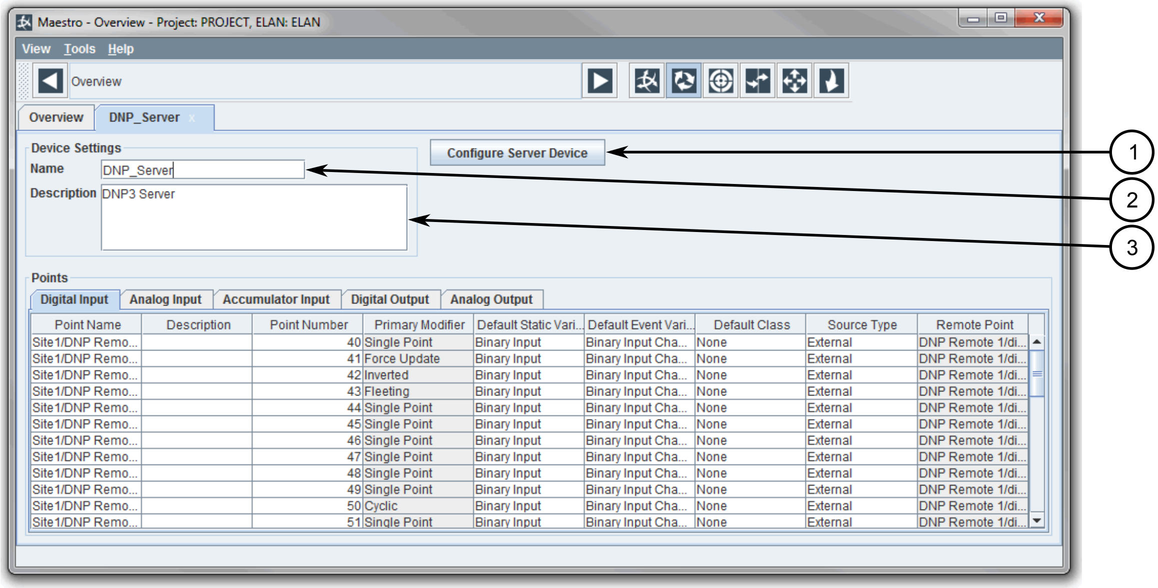
Parameter	Description
	The maximum number of events buffered per master. When the buffer is full, the oldest event is overwritten by the newest. **IMPORTANT!** *Since each server device buffers changes for each of its hosts, buffering a low number of events per master is recommended. Large numbers of events can have detrimental effects and should not be done unnecessarily.*
Master Socket Timeout	**Synopsis:** 0 to 30000 **Default:** 0 The maximum amount of time in milliseconds (ms) to wait at the master (RUGGEDCOM ELAN Router) socket for the receipt of a message from the master.
Master Service Timeout	**Synopsis:** 0 to 30000 **Default:** 20 The maximum amount of time in milliseconds (ms) to keep reading and processing messages received from the master (RUGGEDCOM ELANRouter) socket.
Log History Buffer Size	**Synopsis:** 0 to 65535 **Default:** 1 **Default State:** Disabled When enabled (selected), the specified number of log messages is stored in the history buffer for this server process. The messages are printed out when a fatal error occurs.
Local Freeze	**Synopsis:** { Disabled, Private, Public } **Default:** Disabled Controls how freeze requests are handled. Options include: • `Public` – IEC 104 freeze requests are processed within the server and not passed down to the associated remote process. The current running accumulator value will be written into the frozen accumulator value, and the new frozen accumulator value will be passed back up to any masters that are connected. • `Private` – IEC 104 freeze requests are processed within the server and not passed down to the associated remote process. The current running accumulator value will be written into a *master-specific* frozen accumulator value, and the new frozen accumulator value will be passed back up to *only* the master that initiated the freeze command. • `Disabled` – IEC 104 freeze requests are not processed by the server, but passed down to the remote processes and then on to the remote devices.
Host Interface Timeout	**Synopsis:** 0 to 30000 **Default:** 0 The maximum amount of time in milliseconds (ms) to wait at the message queue for the receipt of a message from the generic host interface process.
Master Stale Time	**Synopsis:** 5 to 3600 **Default:** 30 The amount of time in seconds (s) that must elapse since the last message was received from a non-permanent master before event buffers and all other information associated with that master are deleted.

Section 4.9.4.3

Configuring Protocol Settings

To configure a DNP server device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP_Server

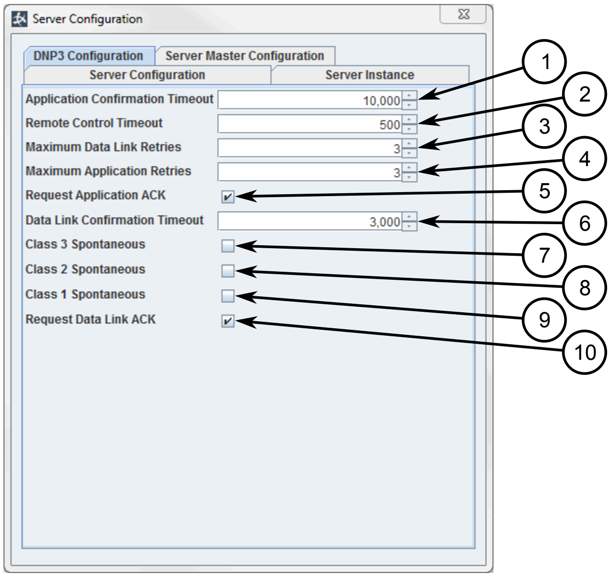
Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 70: DNP Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. On the **DNP3 Configuration** tab, configure the following parameters:



Server Configuration

DNP3 Configuration | Server Master Configuration

Server Configuration | Server Instance

Application Confirmation Timeout	10,000
Remote Control Timeout	500
Maximum Data Link Retries	3
Maximum Application Retries	3
Request Application ACK	☑
Data Link Confirmation Timeout	3,000
Class 3 Spontaneous	☐
Class 2 Spontaneous	☐
Class 1 Spontaneous	☐
Request Data Link ACK	☑

Figure 71: DNP3 Configuration Tab

1. Application Confirmation Timeout Box **2.** Remote Control Timeout Box **3.** Maximum Data Link Retries Box **4.** Maximum Application Retries Box **5.** Request Application ACK Check Box **6.** Data Link Confirmation Timeout Box **7.** Class 3 Spontaneous Check Box **8.** Class 2 Spontaneous Check Box **9.** Class 1 Spontaneous Check Box **10.** Request Data Link ACK Check Box

Parameter	Description
Remote Control Timeout	**Synopsis:** 1 to 100000 **Default:** 500 The maximum amount of time in milliseconds (ms) to wait for a response from a TIE remote process to a control type request.
Maximum Data Link Retries	**Synopsis:** 0 to 100 **Default:** 3 The maximum number of data link retries performed if a response was not received or was corrupted.
Maximum Application Retries	**Synopsis:** 0 to 100 **Default:** 3 The maximum number of application layer retries performed if a requested application layer confirmation was not received.
Request Application ACK	**Default State:** Enabled When enabled (selected), the DNP 3.0 host interface will always request application layer confirmations.
Data Link Confirmation Timeout	**Synopsis:** 0 to 100000 **Default:** 3000 The maximum time in milliseconds (ms) to wait for a data link confirmation.
Class 3 Spontaneous	**Default State:** Disabled When enabled, Class 3 data is spontaneously reported. Only use if `Unsolicited Response Mode` is set to `Unsolicited On Startup`.

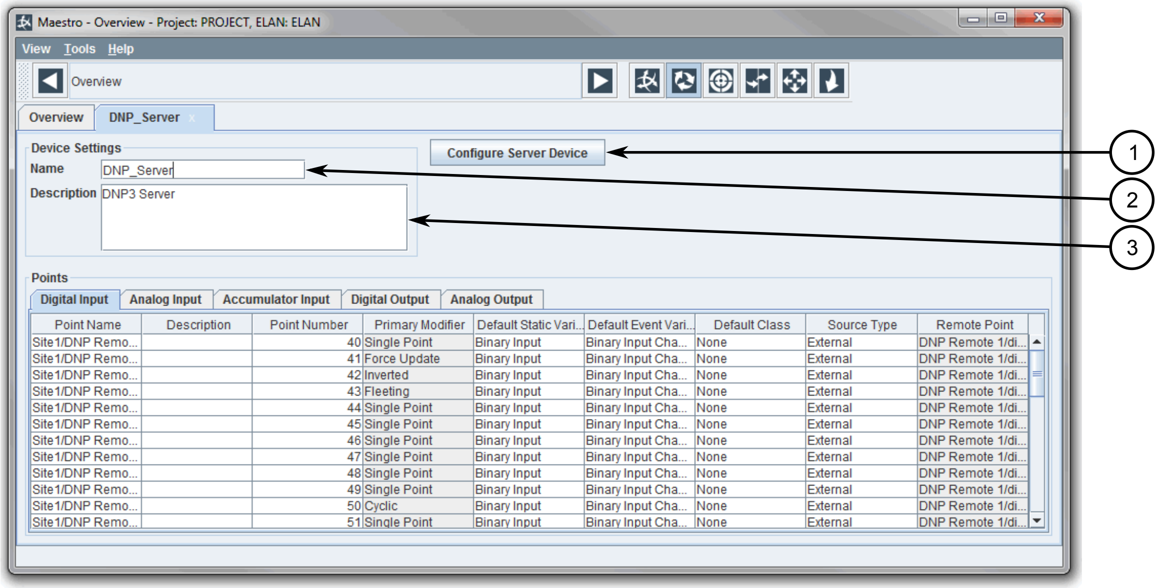
Parameter	Description
	NOTE *Applies only to permanent masters. The DNP server does not send unsolicited response messages to non-permanent Masters.*
Class 2 Spontaneous	**Default State:** Disabled When enabled, Class 2 data is spontaneously reported. Only use if `Unsolicited Response Mode` is set to `Unsolicited On Startup`. **NOTE** *Applies only to permanent masters. The DNP server does not send unsolicited response messages to non-permanent Masters.*
Class 1 Spontaneous	**Default State:** Disabled When enabled, Class 1 data is spontaneously reported. Only use if `Unsolicited Response Mode` is set to `Unsolicited On Startup`. **NOTE** *Applies only to permanent masters. The DNP server does not send unsolicited response messages to non-permanent Masters.*
Application Confirmation Timeout	**Synopsis:** 0 to 100000 **Default:** 10000 The maximum time in milliseconds (ms) to wait for an application layer confirmation.
Request Data Link ACK	**Default State:** Enabled When enabled, the DNP 3.0 host interface always requests data link layer confirmations.

Section 4.9.4.4

Configuring Masters

To configure one or more masters for a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP_Server

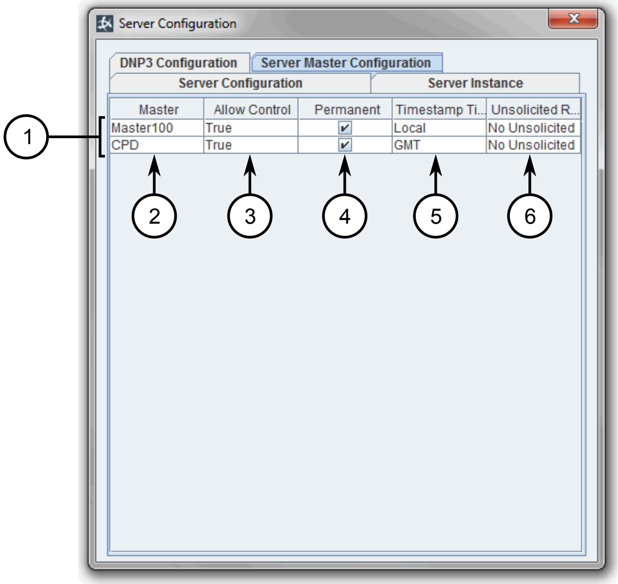
Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 72: DNP Server Device Tab

1. Name Box **2.** Description Box **3.** Configure Server Device Button

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. Click the **Server Master Configuration** tab and configure the following parameters as required:



Master	Allow Control	Permanent	Timestamp Ti...	Unsolicited R...
Master100	True	☑	Local	No Unsolicited
CPD	True	☑	GMT	No Unsolicited

Figure 73: Server Master Configuration

1. Masters **2.** Master List **3.** Allow Control List **4.** Permanent Check Box **5.** Timestamp Time Zone List **6.** Unsolicited Response Mode List

Parameter	Description
Master	**Synopsis:** { Master100, CPD } **Default:** Master100 The master that can interrogate and control this server.
Allow Control	**Synopsis:** { False, Freeze Only, True } **Default:** True Sets the level of control the master has over the server. Options include: • `False` – The master is not allowed to execute controls operations on this server. • `Freeze Only` – The master is only allowed to execute Immediate Freeze commands on this server. • `True` – The master is allowed to execute controls operations on this server.
Permanent	**Default State:** Enabled When enabled (selected), event buffers and other information associated with the master are retained permanently, regardless of whether or not messages are being received by the master. When disabled (cleared), event buffers and other information associated with the master are deleted after a period of time determined by the `Master Stale Time` parameter. For more information about this parameter, refer to Section 4.9.4.1, "Configuring DNP Server" . It is recommended to disable this parameter when the connection to a master is temporary, such as switched backup master/server connection, or a dial-up maintenance host connection. This prevents a master from being flooded with old events if it reconnects after an extended absence. This will also limit the number of duplicate events received by the master after switching to a backup connection.
Timestamp Time Zone	**Synopsis:** { GMT, Local } **Default:** Local The time zone to apply to time stamps reported to the master. Options include: • `GMT` – Time stamps are reported according to Greenwich Mean Time (GMT) • `Local` – Time stamps are reported according to the timezone where the ELAN system resides
Unsolicited Response Mode	**Synopsis:** { No Unsolicited, Unsolicited After Enabled, Unsolicited On Startup } **Synopsis:** No Unsolicited **NOTE** *Applies only when `Permanent` is set to `enabled`.* Enables or disables unsolicited message reporting. Options include: • `No Unsolicited` – Disables all unsolicited message reporting. Commands received from the master to enable unsolicited reporting will be rejected. • `Unsolicited After Enabled` – This option may be used if the master is capable of initiating the transmission of unsolicited messages. On startup, the TIE host Interface will not send any unsolicited messages. Following the receipt of a command from the master to enable unsolicited reporting, the

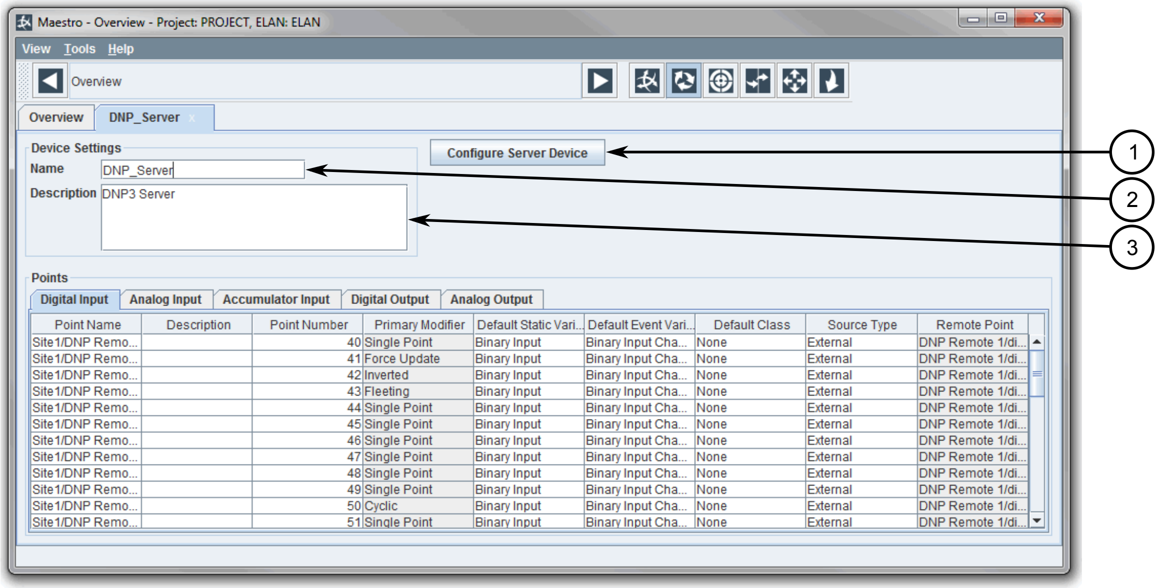
Parameter	Description
	TIE host Interface will start to transmit unsolicited messages. Unsolicited reporting will be limited to the objects enabled by the command received from the master. • `Unsolicited On Startup` – Enables unsolicited message reporting on startup (i.e. the TIE host Interface will not wait for the master to initiate unsolicited reporting). If this option is selected and the TIE host Interface protocol is DNP 3.0, the event classes to spontaneously report are defaulted by configuring the attributes Class 1 Spontaneous, Class 2 Spontaneous, and Class 3 Spontaneous of the Protocol Parameters element.

Section 4.9.4.5

Viewing the DNP Server Instance Settings

To view the server instance settings for a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Name: DNP_Server

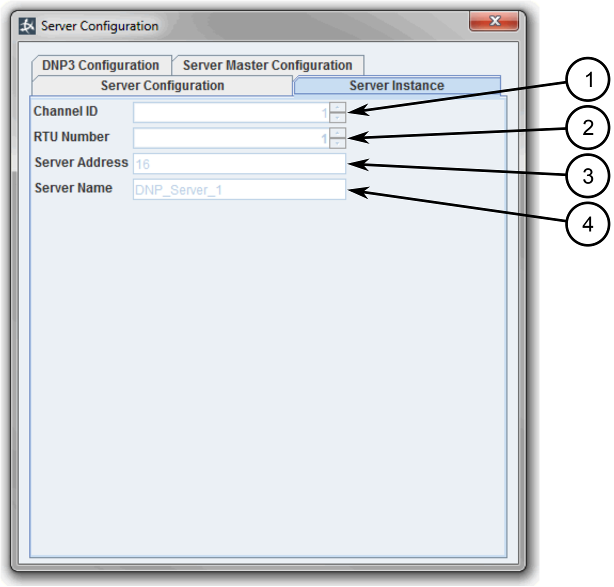
Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 74: DNP Server Device Tab

1. Name Box **2.** Description Box **3.** Configure Server Device Button

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. Click the **Server Instance** tab. This tab displays the following information:



Channel ID: 1

RTU Number: 1

Server Address: 16

Server Name: DNP_Server_1

Figure 75: Server Instance

1. Channel ID **2.** RTU Number **3.** Server Address **4.** Server Name

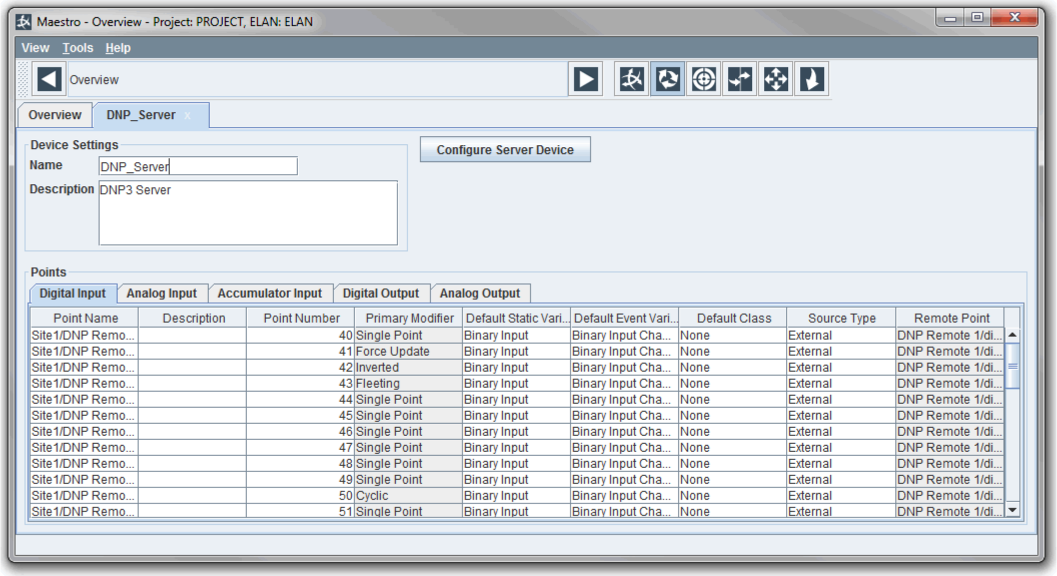
Parameter	Description
Channel ID	**Synopsis:** 1 to 192 **Default:** 1 The channel associated with this server.
RTU Number	**Synopsis:** 1 to 65532 **Default:** 1 The RTU number associated with this device. This is only used when no points are defined.
Server Address	**Synopsis:** 1 to 65532 The unique virtual address of this server assigned by Maestro. This address is the destination address used in internal request messages that originate from a DNP 3.0 master, forwarded by the inter-router to this server.
Server Name	The name of the server device.

Section 4.9.4.6

Configuring a Point

To configure/modify existing points for a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP server device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP_Server

Description: DNP3 Server

Points

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 76: DNP Server Properties

3. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Default Static Variation	**Synopsis:** { Binary Input, Binary Input with Status } The variation to use when reporting the static value of the point in response to a poll request for either Class 0 data or static data, variation 0.
Default Event Variation	**Synopsis:** { Binary Input Change without Time, Binary Input Change with Time, Binary Input Change with Relative Time } The variation to use when reporting event data for the point in response to a poll request for either event Class (1, 2 or 3) data or event data, variation 0.
Default Class	**Synopsis:** { None, Class 1, Class 2, Class 3 } Assigns events data for the point to one of the three event classes. Set to `None` to disable reporting.
Source Type	**Synopsis:** { External, Port All RTU Fail State, RTU Fail State } The source of the input data. Options include: • `External` – The source is external to the DNP server (i.e. coming from the TIE database)

Parameter	Description
	• Port All RTU Fail State – The DNP server creates an internal pseudo status point to indicate when all of the RTUs have failed (1 = Failed) • RTU Fail State – The DNP server creates an internal pseudo status point to indicate when the RTU has failed (1 = Failed)

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Default Static Variation	**Synopsis:** { 32-Bit Analog Input, 16-bit Analog Input, 32-Bit Analog Input without Flag, 16-Bit Analog Input without Flag } The variation to use when reporting the static value of the point in response to a poll request for either Class 0 data or static data, variation 0.
Default Event Variation	**Synopsis:** { Binary Input Change without Time, Binary Input Change with Time, Binary Input Change with Relative Time } The variation to use when reporting event data for the point in response to a poll request for either event Class (1, 2 or 3) data or event data, variation 0.
Default Class	**Synopsis:** { None, Class 1, Class 2, Class 3 } Assigns events data for the point to one of the three event classes. Set to None to disable reporting.
Source Type	**Synopsis:** { External, RTU Composite State } The source of the input data. Options include: • External – The source is external to the DNP server (i.e. coming from the TIE database) • RTU Composite State – The DNP server creates an internal pseudo-analog point to reflect the RTU detailed state

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Default Static Variation	**Synopsis:** { 32-Bit Frozen Counter, 16-Bit Frozen Counter, 32-Bit Frozen Counter without Flag, 16-Bit Frozen Counter without Flag } The variation to use when reporting the static value of the point in response to a poll request for either Class 0 data or static data, variation 0.

Parameter	Description
Default Event Variation	**Synopsis:** { 32-Bit Counter Change Event without Time, 16-Bit Counter Change Event without Time } The variation to use when reporting event data for the point in response to a poll request for either event Class (1, 2 or 3) data or event data, variation 0.
Default Class	**Synopsis:** { None, Class 1, Class 2, Class 3 } Assigns events data for the point to one of the three event classes. Set to `None` to disable reporting.
Running Static Variation	**Synopsis:** { 32-Bit Binary Counter, 16-Bit Binary Counter, 32-Bit Binary Counter without Flag, 16-Bit Binary Counter without Flag } The variation to use when reporting the static value of the point in response to a poll request for either Class 0 data or static data, variation 0.
Running Event Variation	**Synopsis:** { 32-Bit Counter Change Event without Time, 16-Bit Counter Change Event without Time, 32-Bit Counter Change Event with Time, 16-Bit Counter Change Event with Time } The variation to use when reporting event data for the point in response to a poll request for either event Class (1, 2 or 3) data or event data, variation 0.
Running Class	**Synopsis:** { None, Class 1, Class 2, Class 3 } Assigns events data for the point to one of the three event classes. Set to `None` to disable reporting.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Default Static Variation	**Synopsis:** { 32-Bit Analog Output Status, 16-Bit Analog Output Status } The variation to use when reporting the static value of the point in response to a poll request for either Class 0 data or static data, variation 0.
Default Class	**Synopsis:** { Disable for Class 0, Enable for Class 0 }

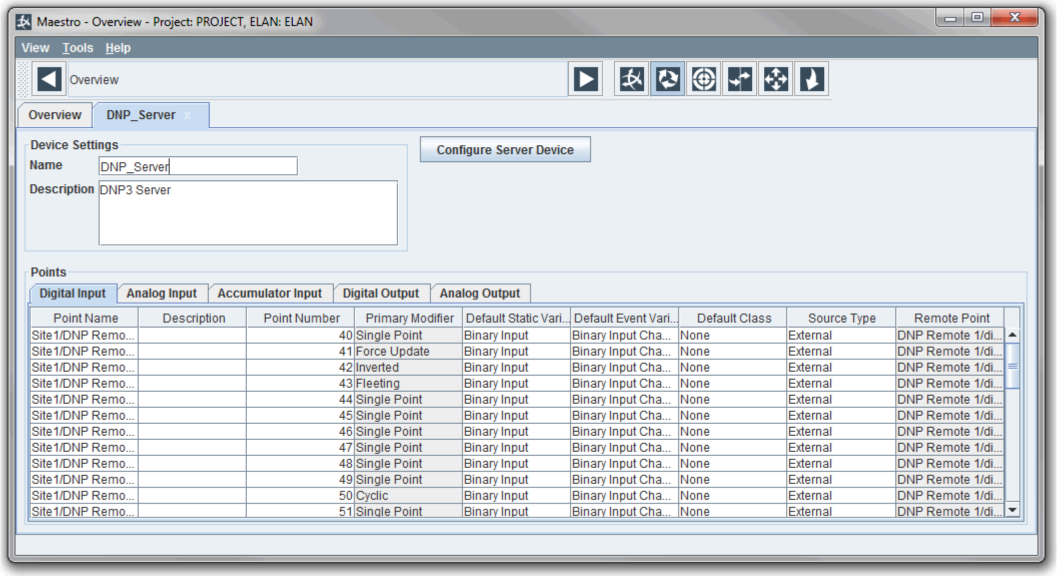
Parameter	Description
	Enables or disables reporting of the point in response to a poll request for Class 0 data.

Section 4.9.4.7

Deleting Points

To delete points mapped to a DNP server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: DNP_Server

Description: DNP3 Server

Point Name	Description	Point Number	Primary Modifier	Default Static Vari...	Default Event Vari...	Default Class	Source Type	Remote Point
Site1/DNP Remo...		40	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		41	Force Update	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		42	Inverted	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		43	Fleeting	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		44	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		45	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		46	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		47	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		48	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		49	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		50	Cyclic	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...
Site1/DNP Remo...		51	Single Point	Binary Input	Binary Input Cha...	None	External	DNP Remote 1/di...

Figure 77: DNP Server Device Tab

3. Under **Points**, select the desired tab.
4. Select one or more points from the table.
5. Right-click the selected points and click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the point(s), or click **No** to abort.

Section 4.9.4.8

Exporting Server Points

Points configured for a DNP server can be exported to a Microsoft® Excel spreadsheet and later imported into templates that support points.

To export the points to an Excel spreadsheet, do the following:

1. Navigate to **Overview**, right-click the desired server and click **Export**. The **Save** dialog box appears.

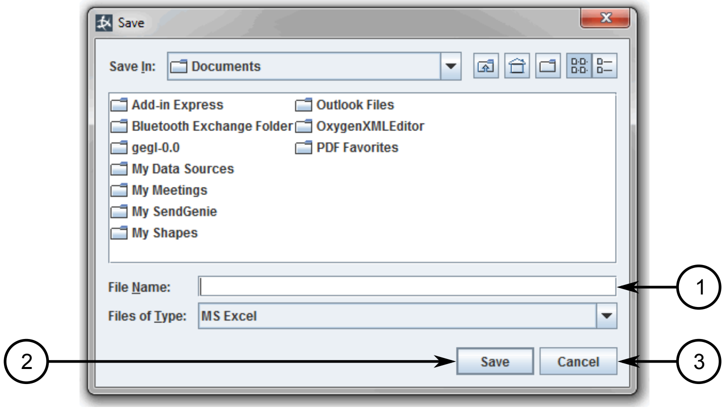


Figure 78: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

2. Navigate to and select the drive or folder where the Excel spreadsheet will be saved.
3. Under **File Name**, type a name for the spreadsheet.
4. Click **Save** to save the spreadsheet, or click **Cancel** to abort.

For information about how to import points into a template, refer to Section 4.8.16.1, “Importing/Exporting Points” .

Section 4.9.5

Managing IEC 60870-5-104 Server Devices

The following sections describe how to configure and manage IEC 60870-5-101 server devices:

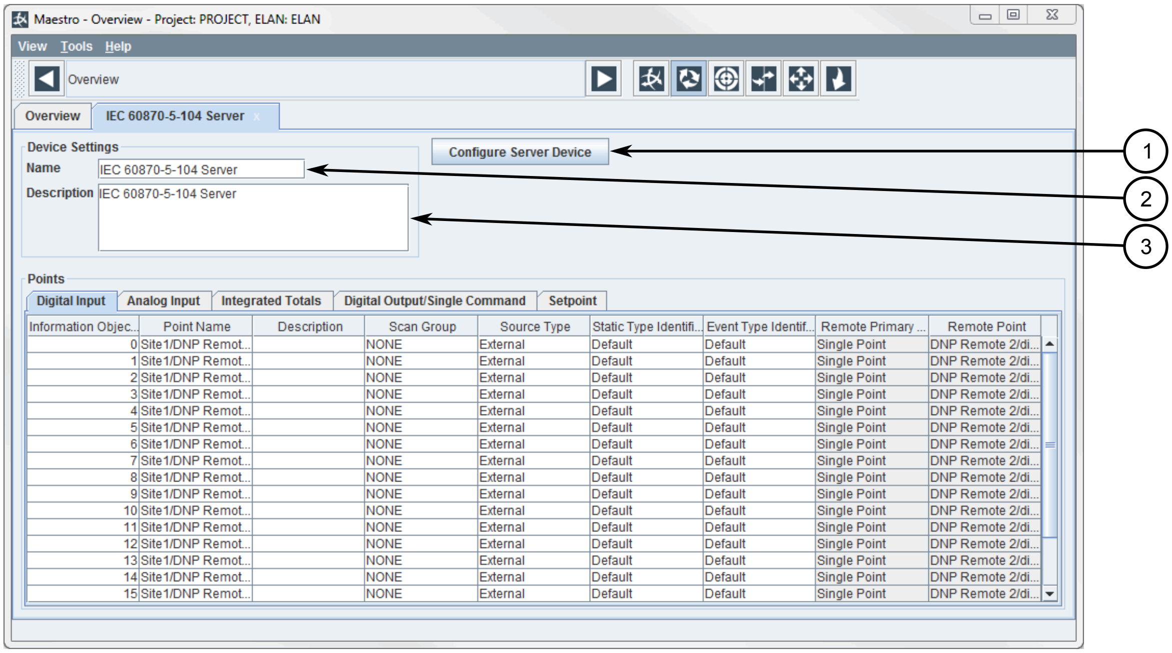
CONTENTS

Section 4.9.5.1

Configuring an IEC 60870-5-104 Server

To configure an IEC 60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: IEC 60870-5-104 Server

Description: IEC 60870-5-104 Server

Points

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 79: IEC 60870-5-104 Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the server device.
Description	A description of the server device.

4. [Optional] Configure the advanced settings for the server. For more information, refer to Section 4.9.5.2, “Configuring Advanced Settings” .
5. [Optional] Configure the protocol settings for the server. For more information, refer to Section 4.9.5.3, “Configuring Protocol Settings” .
6. [Optional] Configure masters for the server. For more information, refer to Section 4.9.5.4, “Configuring Masters” .

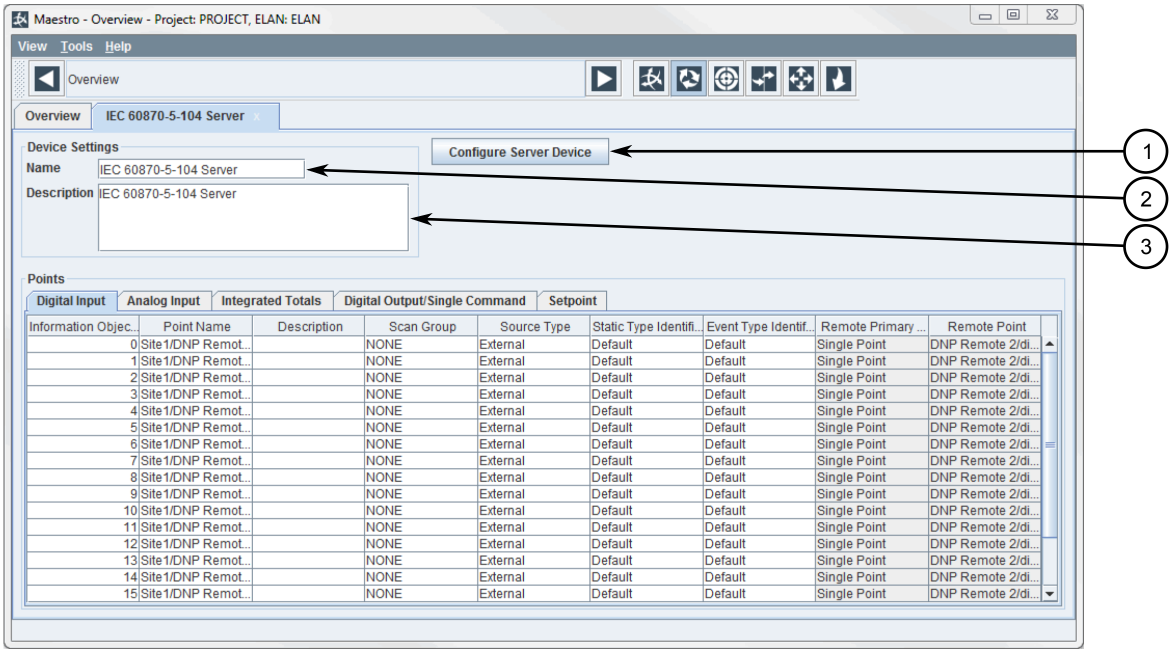
Section 4.9.5.2

Configuring Advanced Settings

To configure the advanced settings for an IEC 60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.

2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: IEC 60870-5-104 Server

Description: IEC 60870-5-104 Server

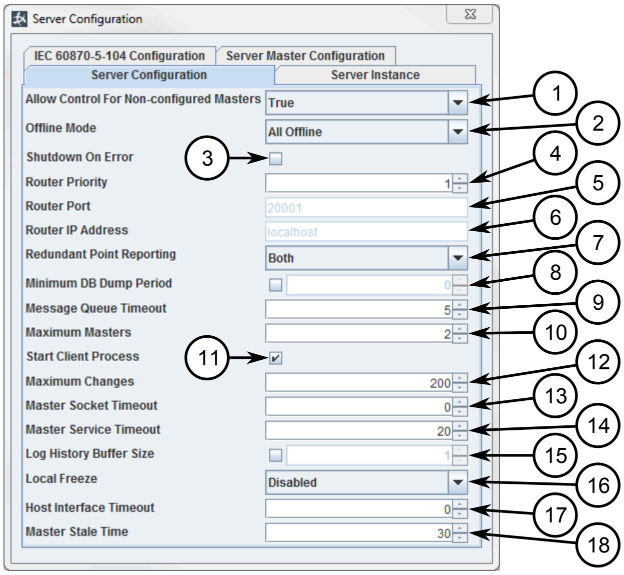
Points

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 80: IEC 60870-5-104 Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.



Allow Control For Non-configured Masters: True
Offline Mode: All Offline
Shutdown On Error: □
Router Priority: 1
Router Port: 20001
Router IP Address: localhost
Redundant Point Reporting: Both
Minimum DB Dump Period: □ 0
Message Queue Timeout: 5
Maximum Masters: 2
Start Client Process: ☑
Maximum Changes: 200
Master Socket Timeout: 0
Master Service Timeout: 20
Log History Buffer Size: □ 1
Local Freeze: Disabled
Host Interface Timeout: 0
Master Stale Time: 30

Figure 81: Server Configuration Tab

1. Allow Control For Non-configured Masters List **2.** Offline Mode List **3.** Shutdown On Error Check Box **4.** Router Priority Box **5.** Router Port **6.** Router IP Address **7.** Redundant Point Reporting List **8.** Minimum DB Dump Period Check Box and Box **9.** Message Queue Timeout Box **10.** Maximum Masters Box **11.** Start Client Process Check Box **12.** Maximum Changes Box **13.** Master Socket Timeout Box **14.** Master Service Timeout **15.** Log History Buffer Size Check Box and Box **16.** Local Freeze List **17.** Host Interface Timeout Box **18.** Master Stale Time Box

4. Configure the following parameters as required:

Parameter	Description
Allow Control for non-configured masters	**Synopsis:** { True, False, Freeze Only } **Default:** True Controls whether or not a master not explicitly defined the server's database is allowed to execute control operations on this remote device. Options include: • `True` – Any master is allowed to control this remote device • `False` – Masters not explicitly defined are not allowed to control this remote device. This is recommended for most new applications. • `Freeze Only` – Masters not explicitly defined are only allowed to execute the Immediate Freeze command.
Offline Mode	**Synopsis:** { Never, One Offline, All Offline } **Default State:** All Offline Controls how the server will respond when physical RTUs assocaite with the server fail. Options include: • `Never` – The server remains online. • `One Offline` – The server stops responding if one or more associated RTUs fail. • `All Offline` – The server stops responding if all associated RTUs fail.
Shutdown on error	**Default State:** Disabled

Parameter	Description
	When enabled (selected), RUGGEDCOM ELAN applications are forced to shut down when a fatal error occurs in the server process.
Router Priority	**Synopsis:** 1 to 100 **Default:** 1 Determines the preferred routing path for messages sent to a device (if more than one path is available). Lower numbers have higher priorities.
Redundant Point Reporting	**Synopsis:** { Both, Both to External ELAN, COS Only, Redundant Only } **Default:** Both Determines how the RUGGEDCOM ELAN IEC 104 host will report redundant Sequence Of Event (SOE) points. Options include: • `Both` – Both redundant and Change Of State (COS) events are reported using their configured Default Event Variation. • `COS Only` – Only the COS event is reported using its configured Default Event Variation. The redundant event is suppressed. • `Redundant Only` – Only the redundant event is reported using its configured Default Event Variation. The COS event is suppressed. • `Both To External ELAN` – When a TIE IEC 104 remote process is communicating with the server process, both redundant and COS events are reported to the IEC 104 remote process. This upstream TIE will correctly interpret the redundant and COS events as long as: ▫ the corresponding points are configured as REDUNDANT in both system ▫ the server point is configured to report its Default Event Variation with time The redundant event is reported using its configured Default Event Variation. The COS event is reported without time.
Minimum DB Dump Period	**Synopsis:** 0 to 600000 **Default:** 0 **Default State:** Disabled The minimum rate in milliseconds (ms) at which to dump the local database to a file. The suggested value is 60,000 milliseconds (1 minute).
Message Queue Timeout	**Synopsis:** 0 to 30000 **Default:** 5 The maximum amount of time in milliseconds (ms) to wait at the message queue for the receipt of a message.
Maximum Masters	**Synopsis:** 1 to 100 **Default:** 2 The maximum number of masters permitted to communicate with this server at a time.
Start Client Process	**Default State:** Enabled When enabled (selected), the associated RUGGEDCOM ELAN client process is placed into Normal mode at start-up. If disabled (cleared), the associated RUGGEDCOM ELAN client process is placed into Standby mode at start-up.
Maximum Changes	**Synopsis:** 100 to 100000 **Default:** 1000

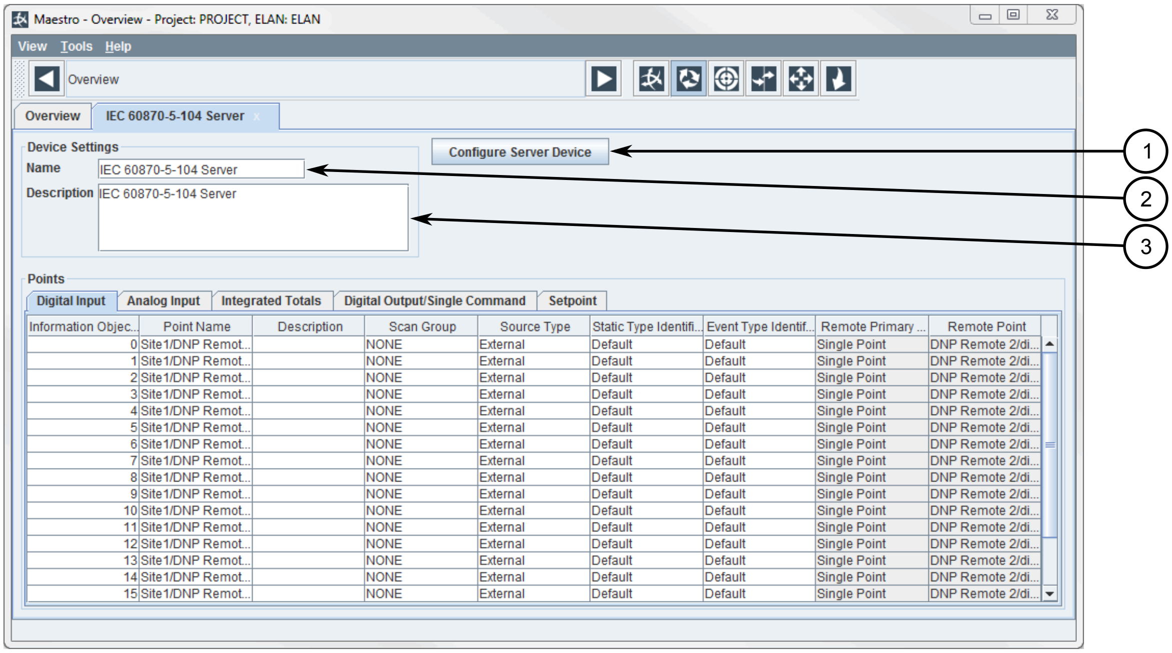
Parameter	Description
	The maximum number of events buffered per master. When the buffer is full, the oldest event is overwritten by the newest. **IMPORTANT!** *Since each server device buffers changes for each of its hosts, buffering a low number of events per master is recommended. Large numbers of events can have detrimental effects and should not be done unnecessarily.*
Master Socket Timeout	**Synopsis:** 0 to 30000 **Default:** 0 The maximum amount of time in milliseconds (ms) to wait at the master (RUGGEDCOM ELAN Router) socket for the receipt of a message from the master.
Master Service Timeout	**Synopsis:** 0 to 30000 **Default:** 20 The maximum amount of time in milliseconds (ms) to keep reading and processing messages received from the master (RUGGEDCOM ELAN Router) socket.
Log History Buffer Size	**Synopsis:** 0 to 65535 **Default:** 1 **Default State:** Disabled When enabled (selected), the specified number of log messages is stored in the history buffer for this server process. The messages are printed out when a fatal error occurs.
Local Freeze	**Synopsis:** { Disabled, Private, Public } **Default:** Disabled Controls how freeze requests are handled. Options include: • `Public` – IEC 104 freeze requests are processed within the server and not passed down to the associated remote process. The current running accumulator value will be written into the frozen accumulator value, and the new frozen accumulator value will be passed back up to any masters that are connected. • `Private` – IEC 104 freeze requests are processed within the server and not passed down to the associated remote process. The current running accumulator value will be written into a *master-specific* frozen accumulator value, and the new frozen accumulator value will be passed back up to *only* the master that initiated the freeze command. • `Disabled` – IEC 104 freeze requests are not processed by the server, but passed down to the remote processes and then on to the remote devices.
Host Interface Timeout	**Synopsis:** 0 to 30000 **Default:** 0 The maximum amount of time in milliseconds (ms) to wait at the message queue for the receipt of a message from the generic host interface process.
Master Stale Time	**Synopsis:** 5 to 3600 **Default:** 30 The amount of time in seconds (s) that must elapse since the last message was received from a non-permanent master before event buffers and all other information associated with that master are deleted.

Section 4.9.5.3

Configuring Protocol Settings

To configure an IEC 60870-5-104 server device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-104 Server

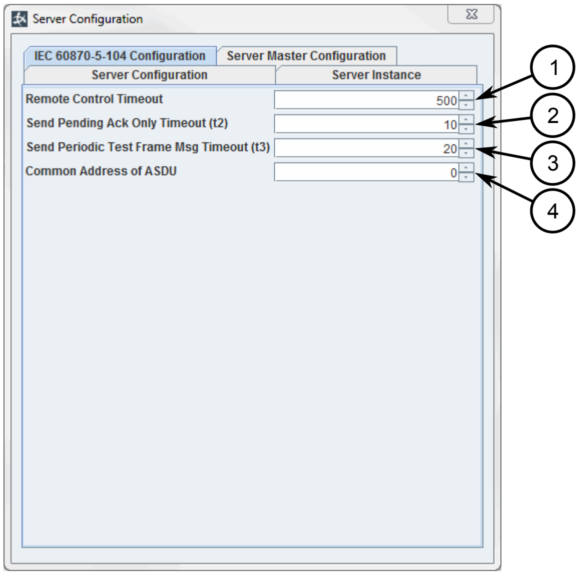
Description: IEC 60870-5-104 Server

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 82: IEC 60870-5-104 Server Device Tab

1. Configure Server Device Button **2.** Name Box **3.** Description Box

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. On the **IEC 60870-5-104 Configuration** tab, configure the following parameters:



Remote Control Timeout 500
Send Pending Ack Only Timeout (t2) 10
Send Periodic Test Frame Msg Timeout (t3) 20
Common Address of ASDU 0

Figure 83: IEC 60870-5-104 Configuration Tab

1. Remote Control Timeout Box **2.** Send Pending Ack Only Timeout (t_2) Box **3.** Send Periodic Test Frame Msg Timeout (t_3) Box **4.** Common Address of ASDU Box

Parameter	Description
Remote Control Timeout	**Synopsis:** 1 to 100000 **Default:** 500 The maximum amount of time in milliseconds (ms) to wait for a response from a TIE remote process to a control type request.
Send Pending Ack Only Timeout (t_2)	**Synopsis:** 1 to 300 **Default:** 10 The maximum time in seconds (s) for sending an acknowledge message in the case of no data message.
Send Periodic Test Frame Msg Timeout (t_3)	**Synopsis:** 1 to 300 **Default:** 20 The maximum time in seconds (s) for sending a test frame in the case of a long idle state.
Common Address for ASDU	**Synopsis:** 0 to 65535 **Default:** 0 The common address for the Application Service Data Unit (ASDU).

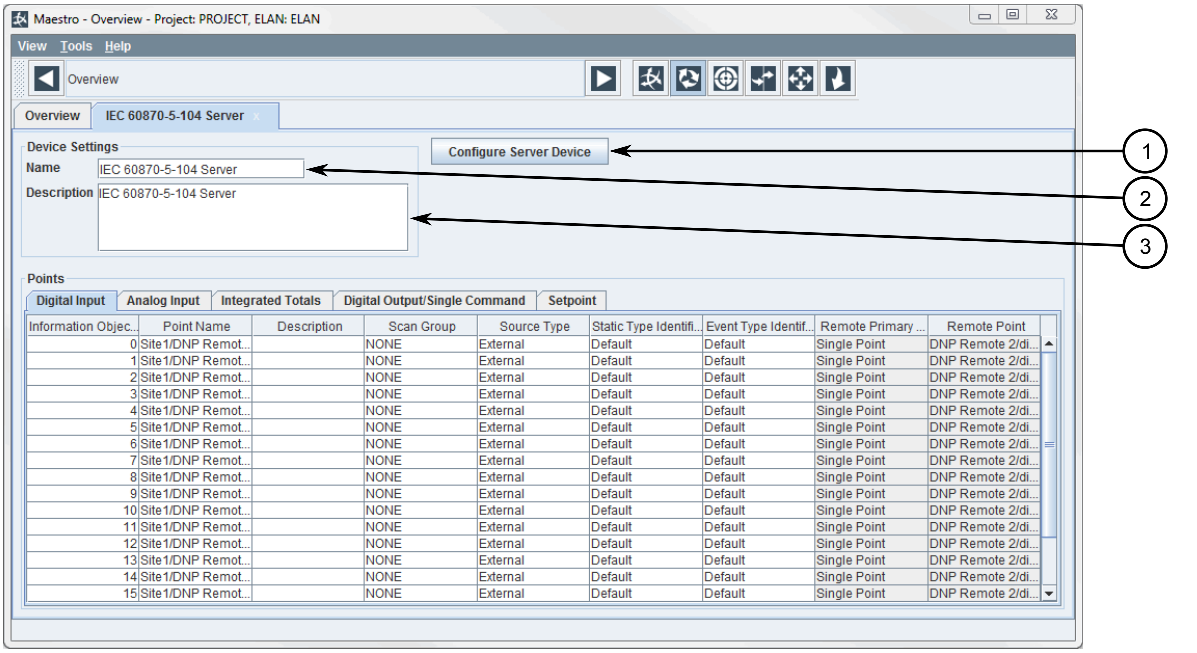
Section 4.9.5.4

Configuring Masters

To configure one or more masters for an IEC 60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.

2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-104 Server

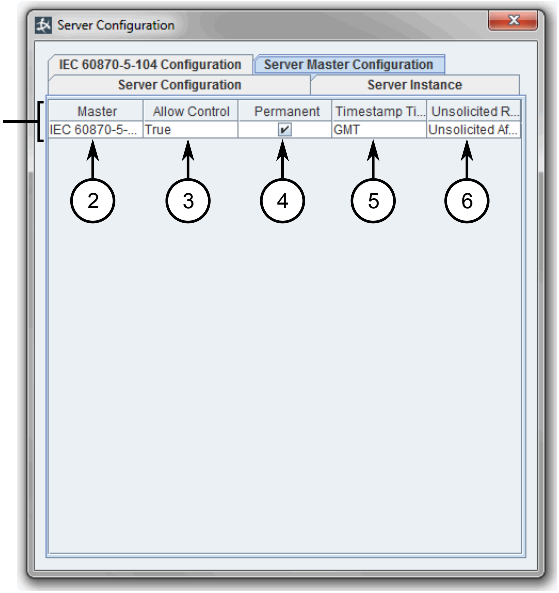
Description: IEC 60870-5-104 Server

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 84: IEC 60870-5-104 Server Device Tab

1. Name Box **2.** Description Box **3.** Configure Server Device Button

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. Click the **Server Master Configuration** tab and configure the following parameters as required:



Master	Allow Control	Permanent	Timestamp Ti...	Unsolicited R...
IEC 60870-5-...	True	☑	GMT	Unsolicited Af...

Figure 85: Server Master Configuration

1. Masters **2.** Master List **3.** Allow Control List **4.** Permanent Check Box **5.** Timestamp Time Zone List **6.** Unsolicited Response Mode List

Parameter	Description
Master	**Synopsis:** { Master100, CPD } **Default:** Master100 The master that can interrogate and control this server.
Allow Control	**Synopsis:** { False, Freeze Only, True } **Default:** True Sets the level of control the master has over the server. Options include: • `False` – The master is not allowed to execute controls operations on this server. • `Freeze Only` – The master is only allowed to execute Immediate Freeze commands on this server. • `True` – The master is allowed to execute controls operations on this server.
Permanent	**Default State:** Enabled When enabled (selected), event buffers and other information associated with the master are retained permanently, regardless of whether or not messages are being received by the master. When disabled (cleared), event buffers and other information associated with the master are deleted after a period of time determined by the `Master Stale Time` parameter. For more information about this parameter, refer to Section 4.9.4.1, "Configuring DNP Server" . It is recommended to disable this parameter when the connection to a master is temporary, such as switched backup master/server connection, or a dial-up maintenance host connection. This prevents a master from being flooded with old events if it reconnects after an extended absence. This will also limit the

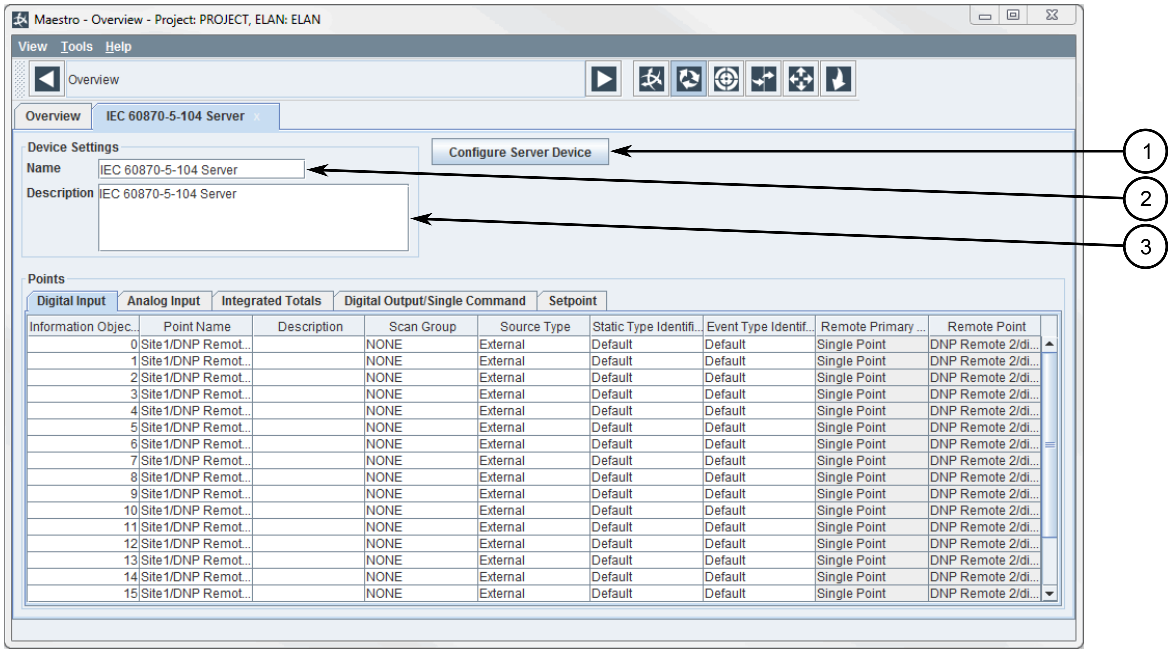
Parameter	Description
	number of duplicate events received by the master after switching to a backup connection.
Timestamp Time Zone	**Synopsis:** { GMT } **Default:** GMT The time zone to apply to time stamps reported to the master. Options include: • `GMT` – Time stamps are reported according to Greenwich Mean Time (GMT)
Unsolicited Response Mode	**Synopsis:** { No Unsolicited, Unsolicited After Enabled } **Synopsis:** Unsolicited After Enabled Enables or disables unsolicited message reporting. Options include: • `No Unsolicited` – Disables all unsolicited message reporting. Commands received from the master to enable unsolicited reporting will be rejected. • `Unsolicited After Enabled` – This option may be used if the master is capable of initiating the transmission of unsolicited messages. On startup, the TIE host Interface will not send any unsolicited messages. Following the receipt of a command from the master to enable unsolicited reporting, the TIE host Interface will start to transmit unsolicited messages. Unsolicited reporting will be limited to the objects enabled by the command received from the master.

Section 4.9.5.5

Viewing the IEC 60870-5-104 Server Instance Settings

To view the server instance settings for an IEC60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Maestro - Overview - Project: PROJECT, ELAN: ELAN

Device Settings

Name: IEC 60870-5-104 Server

Description: IEC 60870-5-104 Server

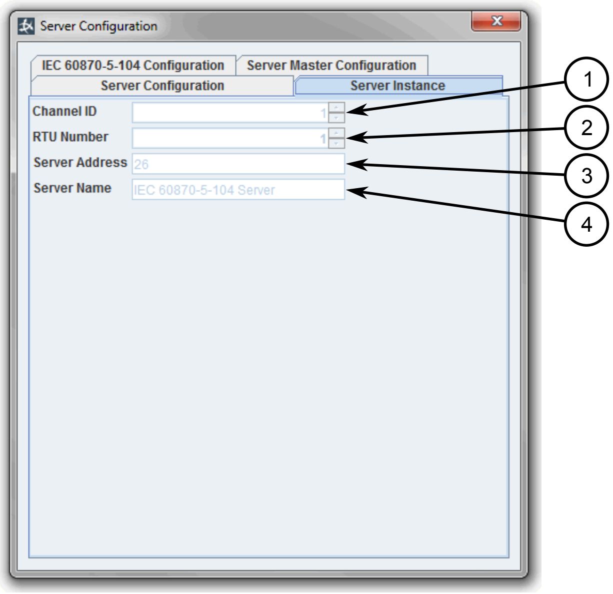
Points

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 86: IEC 60870-5-104 Server Device Tab

1. Name Box **2.** Description Box **3.** Configure Server Device Button

3. Click **Configure Server Device**. The **Server Configuration** dialog box appears.
4. Click the **Server Instance** tab. This tab displays the following information:



Server Configuration

Channel ID: 1

RTU Number: 1

Server Address: 26

Server Name: IEC 60870-5-104 Server

Figure 87: Server Instance

1. Channel ID **2.** RTU Number **3.** Server Address **4.** Server Name

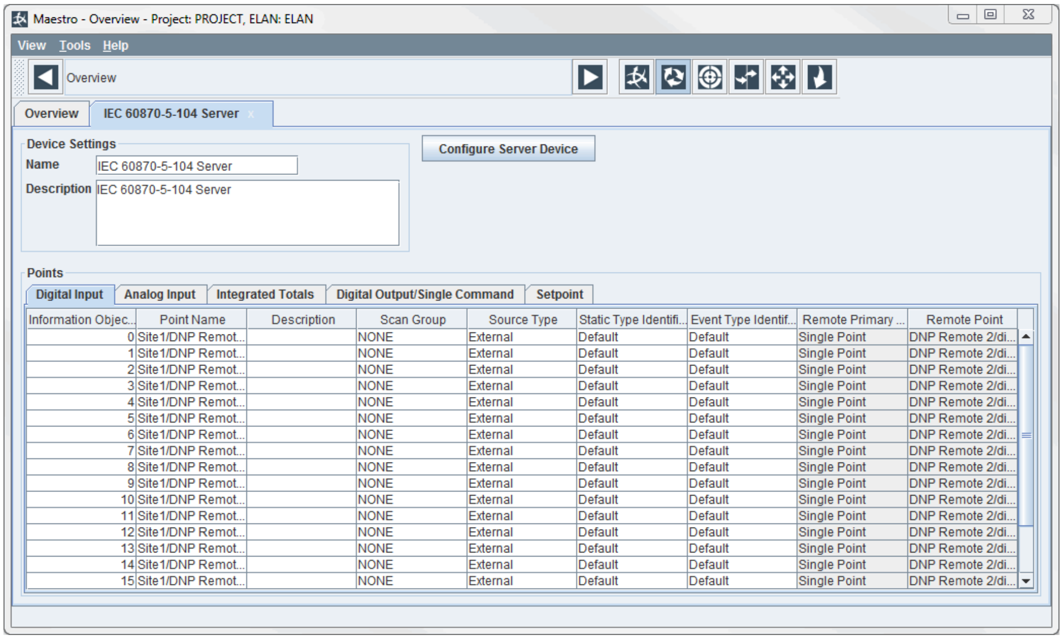
Parameter	Description
Channel ID	**Synopsis:** 1 to 192 **Default:** 1 The channel associated with this server.
RTU Number	**Synopsis:** 1 to 65532 **Default:** 1 The RTU number associated with this device. This is only used when no points are defined.
Server Address	**Synopsis:** 1 to 65532 The unique virtual address of this server assigned by Maestro. This address is the destination address used in internal request messages that originate from a DNP 3.0 master, forwarded by the inter-router to this server.
Server Name	The name of the server device.

Section 4.9.5.6

Configuring a Point

To configure/modify existing points for an IEC 60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the server device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: IEC 60870-5-104 Server

Description: IEC 60870-5-104 Server

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 88: IEC 60870-5-104 Server Properties

3. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Information Object Address	The point's object address.
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Scan Group	**Synopsis:** { None, Scan Group 1, Scan Group 2, Scan Group 3, Scan Group 4, Scan Group 5, Scan Group 6, Scan Group 7, Scan Group 8, Scan Group 9, Scan Group 10, Scan Group 11, Scan Group 12, Scan Group 13, Scan Group 14, Scan Group 15, Scan Group 16 } The scan group in which the point is to be processed.
Source Type	**Synopsis:** { External, Port All RTU Fail State, RTU Fail State } The source of the input data. Options include: • `External` – The source is external to the DNP server (i.e. coming from the TIE database) • `Port All RTU Fail State` – The DNP server creates an internal pseudo status point to indicate when all of the RTUs have failed (1 = Failed) • `RTU Fail State` – The DNP server creates an internal pseudo status point to indicate when the RTU has failed (1 = Failed)
Static Type Identifier	**Synopsis:** { Default, Single Point, Double Point } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected via polling. Options include: • `Default` – No type identifier is assigned. • `Single Point` – The type identifier is set to **1** (M_SP_NA_1). • `Double Point` – The type identifier is set to **3** (M_DP_NA_1).
Event Type Identifier	**Synopsis:** { Default, Single Point, Double Point, Single Point + time tag, Double Point + time tag } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected due to an event. Options include: • `Default` – No type identifier is assigned. • `Single Point` – The type identifier is set to **1** (M_SP_NA_1). • `Double Point` – The type identifier is set to **3** (M_DP_NA_1). • `Single Point + time tag` – The type identifier is set to **30** (M_SP_TB_1). • `Double Point + time tag` – The type identifier is set to **31** (M_DP_TB_1).

Analog Input

Parameter	Description
Information Object Address	The point's object address.

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Scan Group	**Synopsis:** { None, Scan Group 1, Scan Group 2, Scan Group 3, Scan Group 4, Scan Group 5, Scan Group 6, Scan Group 7, Scan Group 8, Scan Group 9, Scan Group 10, Scan Group 11, Scan Group 12, Scan Group 13, Scan Group 14, Scan Group 15, Scan Group 16 } The scan group in which the point is to be processed.
Source Type	**Synopsis:** { External } The source of the input data. Options include: • `External` – The source is external to the DNP server (i.e. coming from the TIE database)
Static Type Identifier	**Synopsis:** { Default, Normalized, Short Floating Point } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected via polling. Options include: • `Default` – No type identifier is assigned. • `Normalized` – The type identifier is set to **9** (M_ME_NA_1). • `Short Floating Point` – The type identifier is set to **13** (M_ME_NC_1).
Event Type Identifier	**Synopsis:** { Default, Normalized, Double Point, Normalized + time tag, Short Floating Point + time tag } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected due to an event. Options include: **IMPORTANT!** *Only select* `Normalized + time tag` *or* `Short Floating Point + time tag` *if data from the client point is also assigned a time tag. A configuration error will be generated otherwise.* • `Default` – No type identifier is assigned. • `Normalized` – The type identifier is set to **9** (M_ME_NA_1). • `Short Floating Point` – The type identifier is set to **13** (M_ME_NC_1). • `Normalized + time tag` – The type identifier is set to **34** (M_ME_TD_1). • `Short Floating Point + time tag` – The type identifier is set to **36** (M_ME_TF_1).

Integrated Totals

Parameter	Description
Information Object Address	The point's object address.
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. integrated_totals_1).

Parameter	Description
Description	A description of the point.
Scan Group	**Synopsis:** { None, Scan Group 1, Scan Group 2, Scan Group 3, Scan Group 4, Scan Group 5, Scan Group 6, Scan Group 7, Scan Group 8, Scan Group 9, Scan Group 10, Scan Group 11, Scan Group 12, Scan Group 13, Scan Group 14, Scan Group 15, Scan Group 16 } The scan group in which the point is to be processed.
Source Type	**Synopsis:** { External } The source of the input data. Options include: • `External` – The source is external to the DNP server (i.e. coming from the TIE database)
Static Type Identifier	**Synopsis:** { Default, Integrated Total } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected via polling. Options include: • `Default` – No type identifier is assigned. • `Integrated Total` – The type identifier is set to **15** (M_IT_NA_1).
Event Type Identifier	**Synopsis:** { Default, Normalized, Double Point, Normalized + time tag, Short Floating Point + time tag } **Default:** Default The type identifier applied to the header of any Application Service Data Unit (ASDU) collected due to an event. Options include: • `Default` – No type identifier is assigned. • `Integrated Total` – The type identifier is set to **15** (M_IT_NA_1). • `Integrated Total + time tag` – The type identifier is set to **37** (M_IT_TB_1).

Digital Output/Single Command

Parameter	Description
Information Object Address	The point's object address.
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_single_command_1).
Description	A description of the point.

Setpoint

Parameter	Description
Information Object Address	The point's object address.
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. setpoint_1).

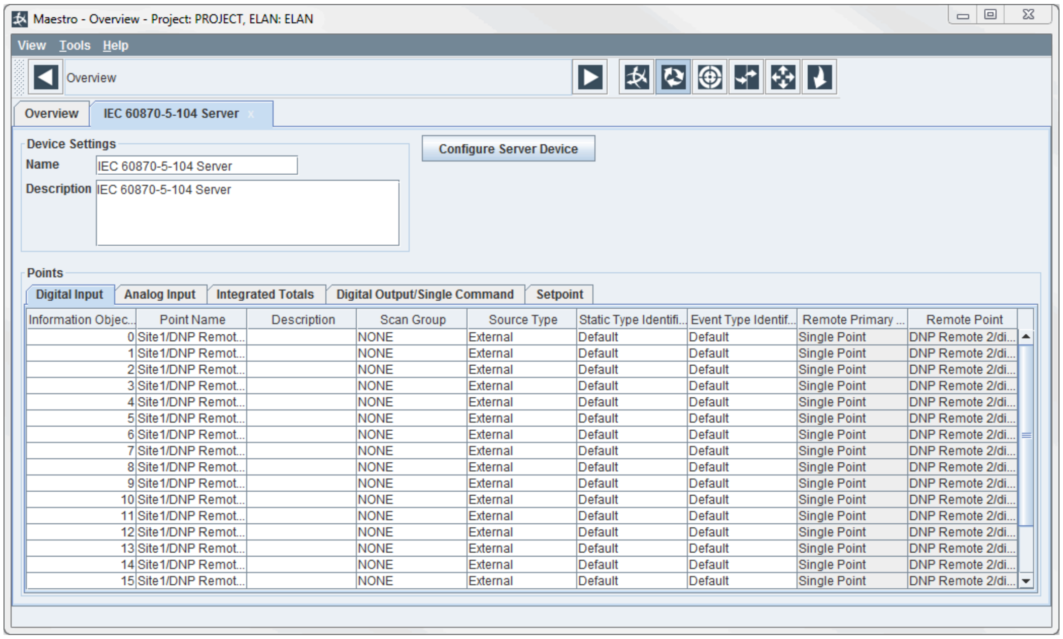
Parameter	Description
Description	A description of the point.

Section 4.9.5.7

Deleting Points

To delete points mapped to an IEC 60870-5-104 server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC60870-5-104 server and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-104 Server

Description: IEC 60870-5-104 Server

Information Objec...	Point Name	Description	Scan Group	Source Type	Static Type Identifi...	Event Type Identif...	Remote Primary ...	Remote Point
0	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
1	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
2	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
3	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
4	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
5	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
6	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
7	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
8	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
9	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
10	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
11	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
12	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
13	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
14	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...
15	Site1/DNP Remot...		NONE	External	Default	Default	Single Point	DNP Remote 2/di...

Figure 89: IEC 60870-5-104 Server Properties

3. Under **Points**, select the desired tab.
4. Select one or more points from the table.
5. Right-click the selected points and click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the point(s), or click **No** to abort.

Section 4.9.5.8

Exporting Server Points

Points configured for an IEC 60870-5-104 server can be exported to a Microsoft® Excel spreadsheet and later imported into templates that support points.

To export the points to an Excel spreadsheet, do the following:

1. Navigate to **Overview**, right-click the desired server and click **Export**. The **Save** dialog box appears.

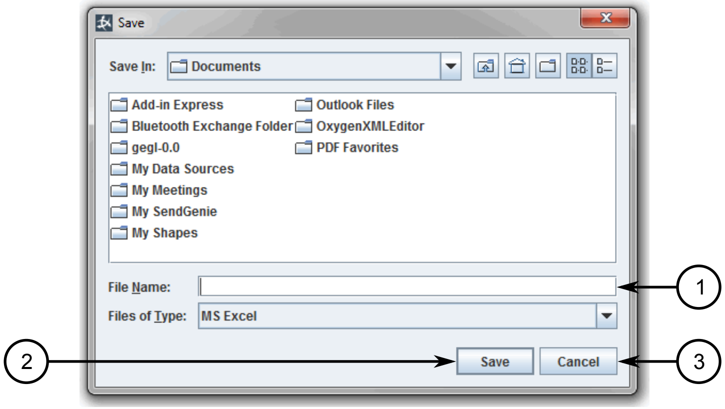


Figure 90: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

2. Navigate to and select the drive or folder where the Excel spreadsheet will be saved.
3. Under **File Name**, type a name for the spreadsheet.
4. Click **Save** to save the spreadsheet, or click **Cancel** to abort.

For information about how to import points into a template, refer to Section 4.8.16.1, “Importing/Exporting Points” .

Section 4.9.6

Managing Jazz Server Devices

This section describes how to configure and manage Jazz server devices.

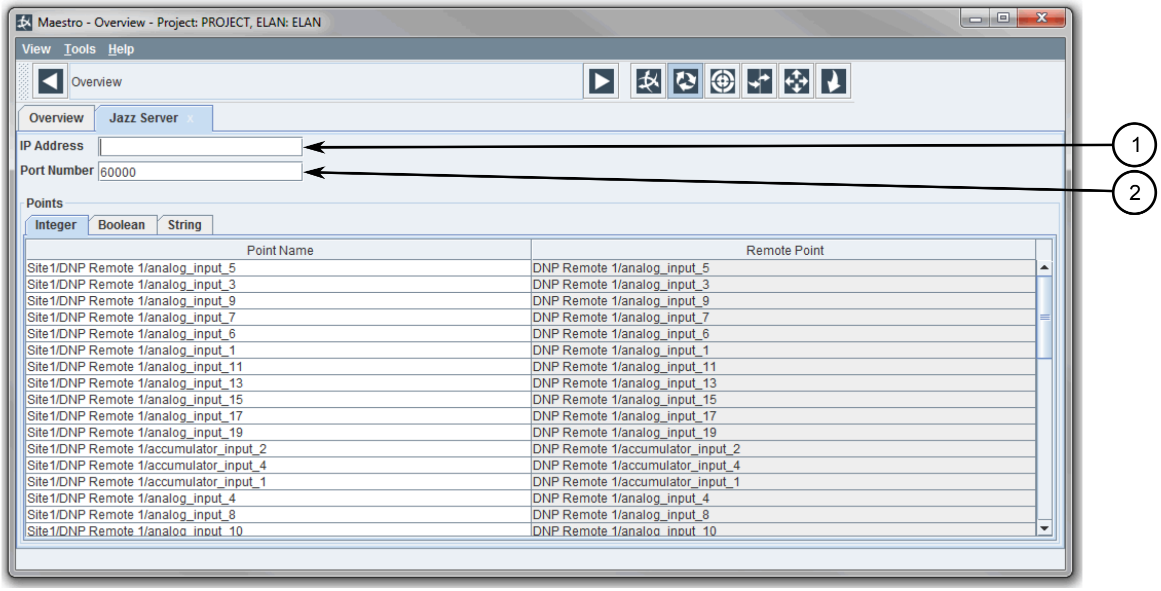
CONTENTS

Section 4.9.6.1

Configuring a Jazz Server

To configure a Jazz server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Jazz server device and click **Properties**. The device's properties appear in a new tab.



IP Address

Port Number 60000

Point Name	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15
Site1/DNP Remote 1/analog_input_17	DNP Remote 1/analog_input_17
Site1/DNP Remote 1/analog_input_19	DNP Remote 1/analog_input_19
Site1/DNP Remote 1/accumulator_input_2	DNP Remote 1/accumulator_input_2
Site1/DNP Remote 1/accumulator_input_4	DNP Remote 1/accumulator_input_4
Site1/DNP Remote 1/accumulator_input_1	DNP Remote 1/accumulator_input_1
Site1/DNP Remote 1/analog_input_4	DNP Remote 1/analog_input_4
Site1/DNP Remote 1/analog_input_8	DNP Remote 1/analog_input_8
Site1/DNP Remote 1/analog_input_10	DNP Remote 1/analog_input_10

Figure 91: Jazz Server Tab

1. IP Address Box **2.** Port Number Box

3. Configure the following parameters as required:

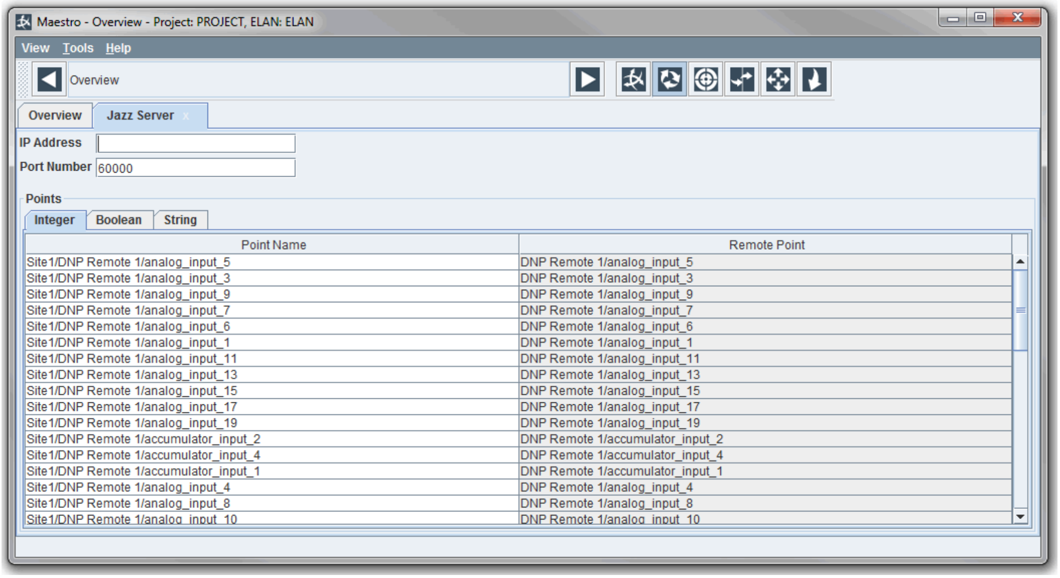
Parameter	Description
IP Address	The IP address for the Jazz server.
Port Number	**Synopsis:** 1 to 65335 **Default:** 60000 The port number for the Jazz server.

Section 4.9.6.2

Renaming a Point

To rename a point configured for a Jazz server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Jazz server and click **Properties**. The device's properties appear in a new tab.



IP Address

Port Number 60000

Point Name	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15
Site1/DNP Remote 1/analog_input_17	DNP Remote 1/analog_input_17
Site1/DNP Remote 1/analog_input_19	DNP Remote 1/analog_input_19
Site1/DNP Remote 1/accumulator_input_2	DNP Remote 1/accumulator_input_2
Site1/DNP Remote 1/accumulator_input_4	DNP Remote 1/accumulator_input_4
Site1/DNP Remote 1/accumulator_input_1	DNP Remote 1/accumulator_input_1
Site1/DNP Remote 1/analog_input_4	DNP Remote 1/analog_input_4
Site1/DNP Remote 1/analog_input_8	DNP Remote 1/analog_input_8
Site1/DNP Remote 1/analog_input_10	DNP Remote 1/analog_input_10

Figure 92: Jazz Server Tab

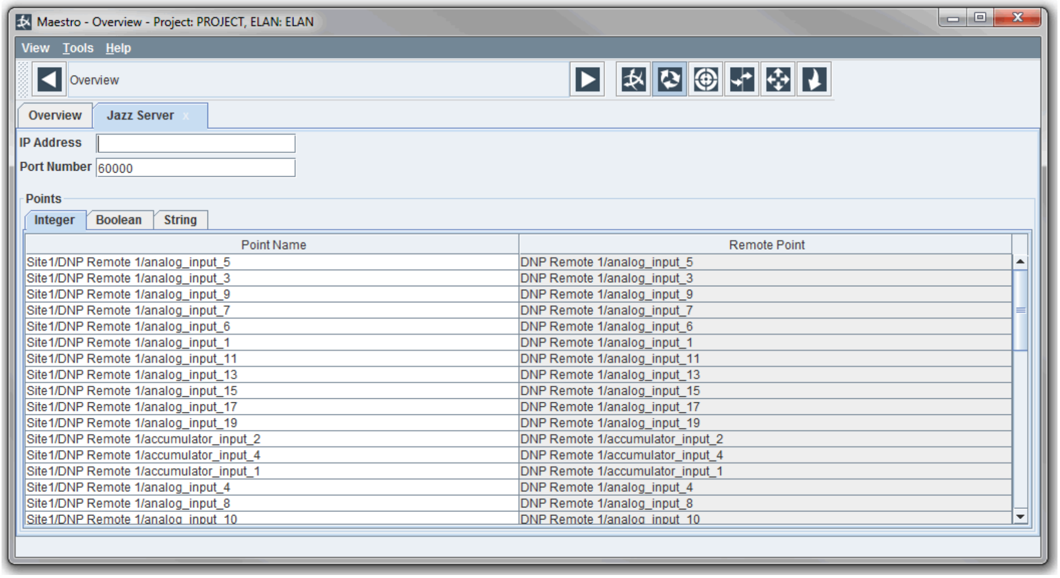
3. Under **Points**, select the desired tab.
4. Under **Point Name**, double-click the desired point and type a new name.

Section 4.9.6.3

Deleting Points

To delete points mapped to a Jazz server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Jazz server and click **Properties**. The device's properties appear in a new tab.



IP Address

Port Number 60000

Point Name	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15
Site1/DNP Remote 1/analog_input_17	DNP Remote 1/analog_input_17
Site1/DNP Remote 1/analog_input_19	DNP Remote 1/analog_input_19
Site1/DNP Remote 1/accumulator_input_2	DNP Remote 1/accumulator_input_2
Site1/DNP Remote 1/accumulator_input_4	DNP Remote 1/accumulator_input_4
Site1/DNP Remote 1/accumulator_input_1	DNP Remote 1/accumulator_input_1
Site1/DNP Remote 1/analog_input_4	DNP Remote 1/analog_input_4
Site1/DNP Remote 1/analog_input_8	DNP Remote 1/analog_input_8
Site1/DNP Remote 1/analog_input_10	DNP Remote 1/analog_input_10

Figure 93: Jazz Server Tab

3. Under **Points**, select the desired tab.
4. Select one or more points from the table.
5. Right-click the selected points and click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the point(s), or click **No** to abort.

Section 4.9.7

Managing RUGGEDCOM REFLEX Server Devices

This section describes how to configure and manage RUGGEDCOM REFLEX server devices via Maestro.

CONTENTS

Section 4.9.7.1

Adding/Deleting a Point

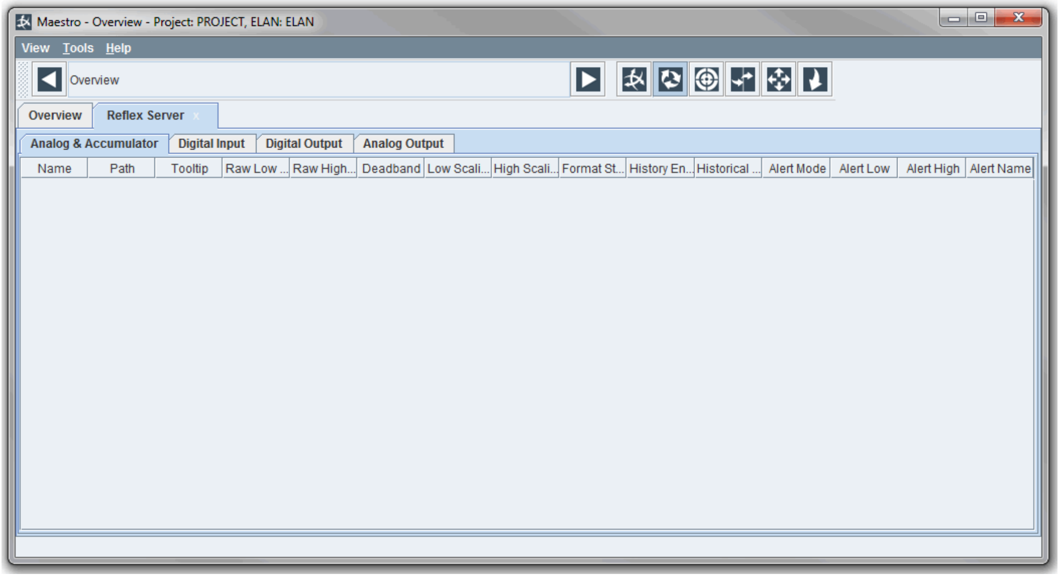
To manually add or delete a point for a RUGGEDCOM REFLEX server, do the following:

NOTE

Points from other server devices can also be mapped automatically to the RUGGEDCOM REFLEX server. For more information about this method, refer to Section 4.9.3, “Mapping/Unmapping Points for a Server” .

Adding a Point

1. Navigate to the **Overview** screen.
2. Right-click the RUGGEDCOM REFLEX server device and click **Properties**. The device's properties appear in a new tab.



Name	Path	Tooltip	Raw Low ...	Raw High...	Deadband	Low Scali...	High Scali...	Format St...	History En...	Historical ...	Alert Mode	Alert Low	Alert High	Alert Name

Figure 94: RUGGEDCOM REFLEX Server Properties

3. Select either the **Analog & Accumulator** or **Digital Input** tab.
4. Right-click anywhere on the table to open the shortcut menu and select **Create Point**. A new point is added.
5. Configuring the point. For more information, refer to Section 4.9.7.3, "Configuring a RUGGEDCOM REFLEX Server Point Folder" .

Deleting a Point

1. Navigate to the **Overview** screen.
2. Right-click the RUGGEDCOM REFLEX server device and click **Properties**. The device's properties appear in a new tab.
3. Select either the **Analog & Accumulator** or **Digital Input** tab.
4. Right-click the desired point and click **Delete**. A confirmation dialog box appears.
5. Click **Yes** to delete the point, or click **No** to abort.

Section 4.9.7.2

Adding/Deleting a Folder

To add or delete a folder for a RUGGEDCOM REFLEX server, do the following:

Adding a Folder

1. Navigate to the **Overview** screen.
2. Right-click the RUGGEDCOM REFLEX server device and click **Properties**. The device's properties appear in a new tab.

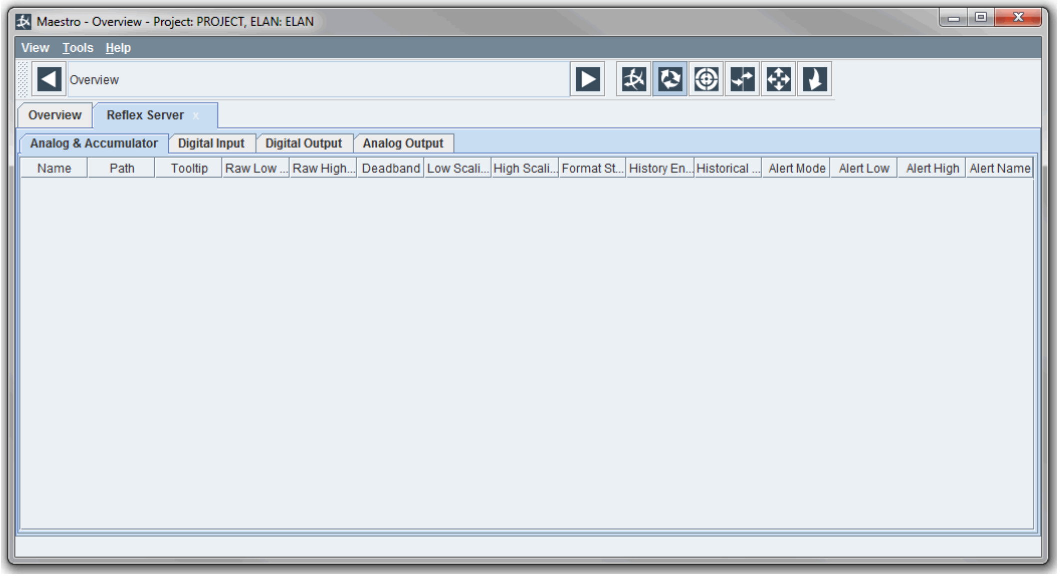


Figure 95: RUGGEDCOM REFLEX Server Properties

3. Select either the **Analog & Accumulator** or **Digital Input** tab.
4. Right-click anywhere on the table to open the shortcut menu and select **Create Folder**. A new folder is added.

Deleting a Folder

1. Navigate to the **Overview** screen.
2. Right-click the RUGGEDCOM REFLEX server device and click **Properties**. The device's properties appear in a new tab.
3. Select either the **Analog & Accumulator** or **Digital Input** tab.
4. Right-click the desired folder and click **Delete**. A confirmation dialog box appears.
5. Click **Yes** to delete the point, or click **No** to abort.

Section 4.9.7.3

Configuring a RUGGEDCOM REFLEX Server Point Folder

To configure a point or folder for a RUGGEDCOM REFLEX server, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RUGGEDCOM REFLEX server device and click **Properties**. The device's properties appear in a new tab.

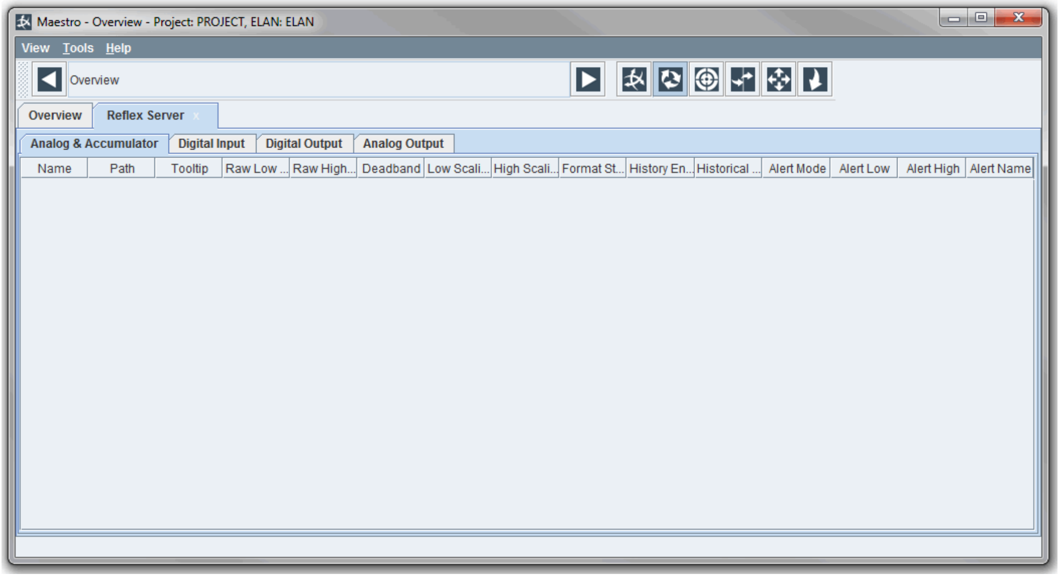


Figure 96: RUGGEDCOM REFLEX Server Properties

3. Select either the **Analog & Accumulator** or **Digital Input** tab and then configure the following parameters as required:

Parameter	Description
Name	The name of the tag as referenced in the system.
Path	The path folder structure of the tag.

Section 4.10

Managing Client Devices

A client device is a remote IED or RTU device the RUGGEDCOM ELAN server controls and/or receives telemetry/ point data from.

CONTENTS

- Section 4.10.9, “Managing IEC 60870-5-104 Client Devices”
- Section 4.10.10, “Managing IEC 61850 Client Devices”
- Section 4.10.11, “Managing ABB Client Devices”
- Section 4.10.12, “Managing Courier Client Devices”
- Section 4.10.13, “Managing SEL Client Devices”
- Section 4.10.14, “Managing Modbus Client Devices”
- Section 4.10.15, “Managing RP 570 Client Devices”

Section 4.10.1

Adding/Deleting a Client Device

To add or delete a client device, do the following:

Adding a Client Device

NOTE

For IEC 61850 client devices, the following procedure describes how to add a base device. For information about adding a fully configured IEC 61850 client device based on a CID file, refer to Section 4.10.10.2, “Adding an IEC 61850 Client from a CID File” .

1. Navigate to the **Overview** screen.
2. Under **Device Templates**, double-click the desired protocol to reveal the available device templates. If templates are not available or a new template is required, add a template. For more information, refer to Section 4.8.4, “Adding/Deleting a Device Template” .
3. Right-click the desired device template to use as a base for the new client device and then click **New Client Device**. A new client device is added under ***RUGGEDCOM ELAN Client Devices » {Protocol}*** .
4. [Optional] Group the client device with similar devices by either moving the device to an existing folder or creating a new folder. For more information, refer to Section 4.10.3, “Grouping Client Devices” .
5. Configure the new client device.
   - For more information about configuring DNP client devices, refer to Section 4.10.7.1, “Configuring DNP Client”
   - For more information about configuring IEC 60870-5-101 client devices, refer to Section 4.10.8.1, “Configuring IEC 60870-5-101 Client”
   - For more information about configuring IEC 60870-5-104 client devices, refer to Section 4.10.9.1, “Configuring IEC 60870-5-104 Client”
   - For more information about configuring IEC 61850 client devices, refer to Section 4.10.10.3, “Reloading an IEC 61850 Client Configuration”
   - For more information about configuring ABB client devices, refer to Section 4.10.11.1, “Configuring ABB Client”
   - For more information about configuring Courier client devices, refer to Section 4.10.12.1, “Configuring a Courier Client”
   - For more information about configuring SEL client devices, refer to Section 4.10.13.1, “Configuring an SEL Client”

- For more information about configuring Modbus client devices, refer to Section 4.10.14.1, “Configuring a Modbus Client”
- For more information about configuring RP 570 client devices, refer to Section 4.10.15.1, “Configuring a RP 570 Client”

›› Deleting a Client Device

1. Navigate to the **Overview** screen.
2. Under **RUGGEDCOM ELAN Client Devices**, right-click the client device to open the shortcut menu and then click **Delete**. A confirmation message appears.
3. Click **Yes** to delete the client device, or click **No** to abort.

Section 4.10.2

Renaming a Client Device

With the exception of IEC 61850 devices, client devices can be renamed for easy identification.

To rename a client device, do the following:

1. Navigate to the **Overview** screen.
2. Under ***RUGGEDCOM ELAN server Devices » {protocol}*** , right-click the device template and click **Rename**.
3. Type the new name for the client device.

Section 4.10.3

Grouping Client Devices

To help organize all of the possible client devices managed by RUGGEDCOM ELAN, client devices can be grouped together in folders. This can be used to reflect relationships between devices. For example, client devices that reside in the same location can be moved to a *Site X* folder.

›› Adding a Folder

To add a folder, do the following:

1. Navigate to the **Overview** screen.
2. Right-click **RUGGEDCOM ELAN Client Devices** and click **New Folder**. A new folder is added.
3. [Optional] Type a new name for the folder.

›› Adding Client Devices to a Folder

To add client devices to a folder, simply drag-and-drop each device over the folder name.

›› Deleting a Folder

To delete a folder, do the following:

1. Right-click the folder and click **Delete**. A confirmation dialog box appears.
2. Click **Yes** to delete the folder, or click **No** to abort.

›› Renaming a Folder

To rename an existing folder, right-click the folder, click **Rename** and type a new name.

Section 4.10.4

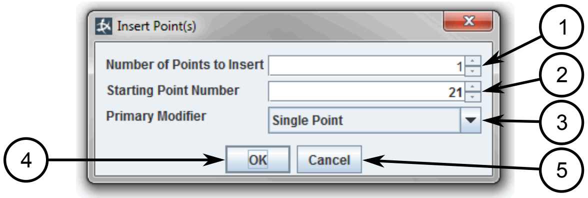
Adding/Deleting Points

With the exception of IEC 61850 devices, points can be manually added to or deleted from client devices.

To add or delete a point for a client device, do the following:

›› Adding a Point

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. If the device is linked to a template, break the link to be able to add points. For more information, refer to Section 4.8.3, "Controlling Template Links" .
4. Under **Points**, select the desired tab. Each tab represents a point type.
5. Right-click anywhere on the table to open the shortcut menu and select **Insert Point(s)**. The **Insert Point(s)** dialog box appears.



Insert Point(s)

Number of Points to Insert: 1

Starting Point Number: 21

Primary Modifier: Single Point

Figure 97: Insert Point(s) Dialog Box

1. Number of Points to Insert Box **2.** Starting Point Number Box **3.** Primary Modifier **4.** OK Button **5.** Cancel Button

6. Configure the following parameters as required:

Parameter	Description
Number of Points to Insert	**Synopsis:** 1 to 65536 **Synopsis:** 1 The number of points to insert.
Starting Point Number	**Synopsis:** 1 to 65536 **Synopsis:** 1 The number assigned to the first label. All other points added will be assigned a sequential number.

Parameter	Description
	NOTE *If one or more point numbers are already in use, the row for each duplicate point in the list will be red. This can only be cleared by renaming the point.*
Primary Modifier	The primary modifier. Options are dependent on the protocol and point type. • For more information about **Primary Modifier** options for DNP templates, refer to Section 4.10.7.1, "Configuring DNP Client" • For more information about **Primary Modifier** options for IEC 60870-5-101 templates, refer to Section 4.10.8.1, "Configuring IEC 60870-5-101 Client" • For more information about **Primary Modifier** options for IEC 60870-5-104 templates, refer to Section 4.10.9.1, "Configuring IEC 60870-5-104 Client" • For more information about **Primary Modifier** options for ABB templates, refer to Section 4.10.11.1, "Configuring ABB Client" • For more information about **Primary Modifier** options for Courier templates, refer to Section 4.10.12.1, "Configuring a Courier Client" • For more information about **Primary Modifier** options for SEL templates, refer to Section 4.10.13.1, "Configuring an SEL Client" • For more information about **Primary Modifier** options for Modbus templates, refer to Section 4.10.14.1, "Configuring a Modbus Client" • For more information about **Primary Modifier** options for RP 570 templates, refer to Section 4.10.15.1, "Configuring a RP 570 Client"

7. Click **OK** to add the points, or click **Cancel** to abort.
8. [Optional] Further configure each point.
   - For more information about configuring points for a DNP template, refer to Section 4.10.7.1, "Configuring DNP Client"
   - For more information about configuring points for an IEC 60870-5-101 template, refer to Section 4.10.8.1, "Configuring IEC 60870-5-101 Client"
   - For more information about configuring points for an IEC 60870-5-104 template, refer to Section 4.10.9.1, "Configuring IEC 60870-5-104 Client"
   - For more information about configuring points for an ABB template, refer to Section 4.10.11.1, "Configuring ABB Client"
   - For more information about configuring points for a Courier template, refer to Section 4.10.12.1, "Configuring a Courier Client"
   - For more information about configuring points for an SEL template, refer to Section 4.10.13.1, "Configuring an SEL Client"
   - For more information about configuring points for a Modbus template, refer to Section 4.10.14.1, "Configuring a Modbus Client"
   - For more information about configuring points for an RP 570 template, refer to Section 4.10.15.1, "Configuring a RP 570 Client"

Deleting a Point

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Under **Points**, select the desired tab. Each tab represents a point type.
4. Select one or more points from the table.
5. Right-click the selected point(s) to open the shortcut menu and click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the point(s), or click **No** to abort.

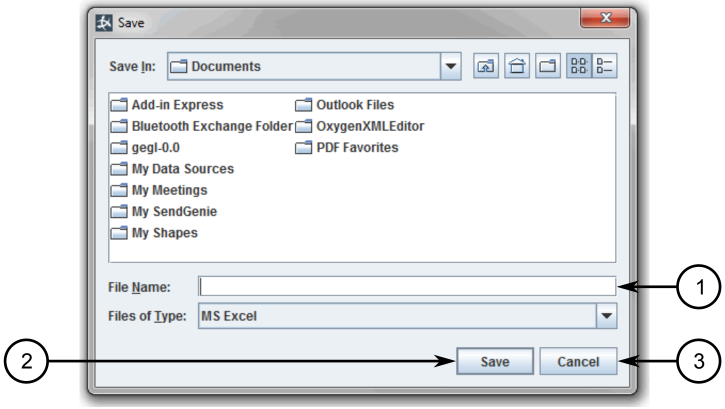
Section 4.10.5

Exporting Points

With the exception of IEC 61850 devices, points configured for a client device can be exported to a Microsoft® Excel spreadsheet and later imported into templates that support points.

To export the points to an Excel spreadsheet, do the following:

1. Navigate to **Overview**, right-click the desired client and click **Export**. The **Save** dialog box appears.



Save In: Documents

File Name:

Files of Type: MS Excel

Figure 98: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

2. Navigate to and select the drive or folder where the Excel spreadsheet will be saved.
3. Under **File Name**, type a name for the spreadsheet.
4. Click **Save** to save the spreadsheet, or click **Cancel** to abort.

For information about how to import points into a template, refer to Section 4.8.16.1, “Importing/Exporting Points” .

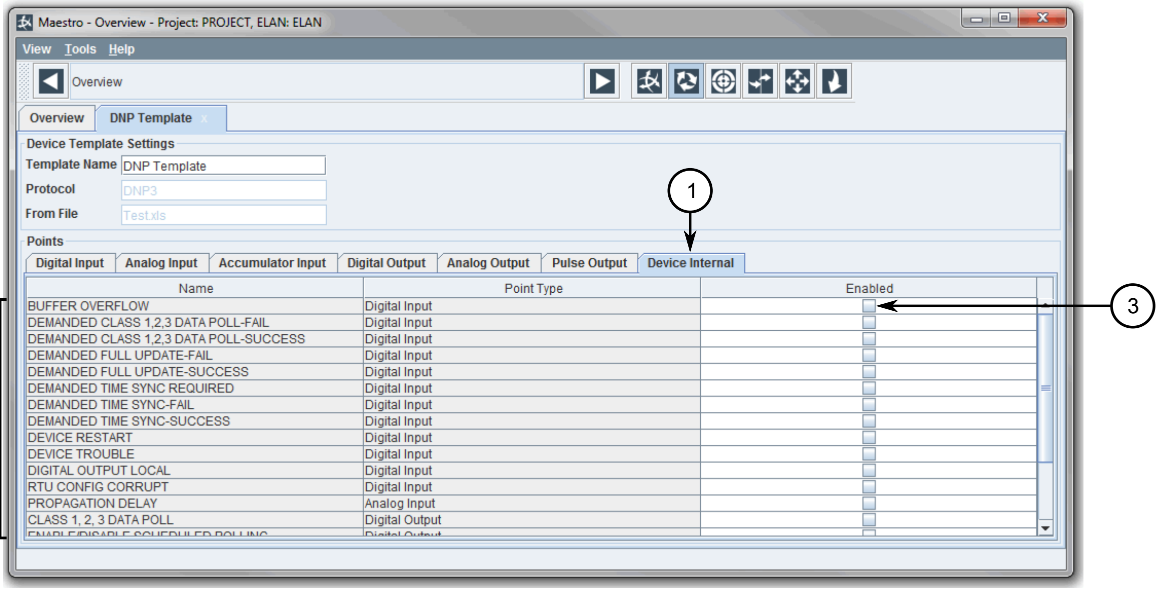
Section 4.10.6

Enabling/Disabling Device Internal Points

Device internal points are optional predefined points that indicate the status of a remote device. They are only available for remote client devices, with the exception of IEC 61850 devices. For more information, refer to the remote client device's user documentation.

To enable/disable device internal points for a client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Make sure the link between the device and its template is broken. Points cannot be modified if the device is linked to its template. For more information, refer to Section 4.8.3, "Controlling Template Links" .
4. Under **Points**, select the **Device Internal** tab.



Device Template Settings

Template Name: DNP Template

Protocol: DNP3

From File: Test.xls

Points

Name	Point Type	Enabled
BUFFER OVERFLOW	Digital Input	□
DEMANDED CLASS 1,2,3 DATA POLL-FAIL	Digital Input	□
DEMANDED CLASS 1,2,3 DATA POLL-SUCCESS	Digital Input	□
DEMANDED FULL UPDATE-FAIL	Digital Input	□
DEMANDED FULL UPDATE-SUCCESS	Digital Input	□
DEMANDED TIME SYNC REQUIRED	Digital Input	□
DEMANDED TIME SYNC-FAIL	Digital Input	□
DEMANDED TIME SYNC-SUCCESS	Digital Input	□
DEVICE RESTART	Digital Input	□
DEVICE TROUBLE	Digital Input	□
DIGITAL OUTPUT LOCAL	Digital Input	□
RTU CONFIG CORRUPT	Digital Input	□
PROPAGATION DELAY	Analog Input	□
CLASS 1, 2, 3 DATA POLL	Digital Output	□
ENABLE/DISABLE SCHEDULED POLLING	Digital Output	□

Figure 99: Device Internal Tab (Example)

1. Device Internal Tab **2.** Supported Device Internal Points **3.** Enable Check Box

5. For each device internal point, click the associated **Enable** check box to enable the point, or clear the **Enable** check box to disable it.

Section 4.10.7

Managing DNP Client Devices

This section describes how to configure and manage DNP client devices.

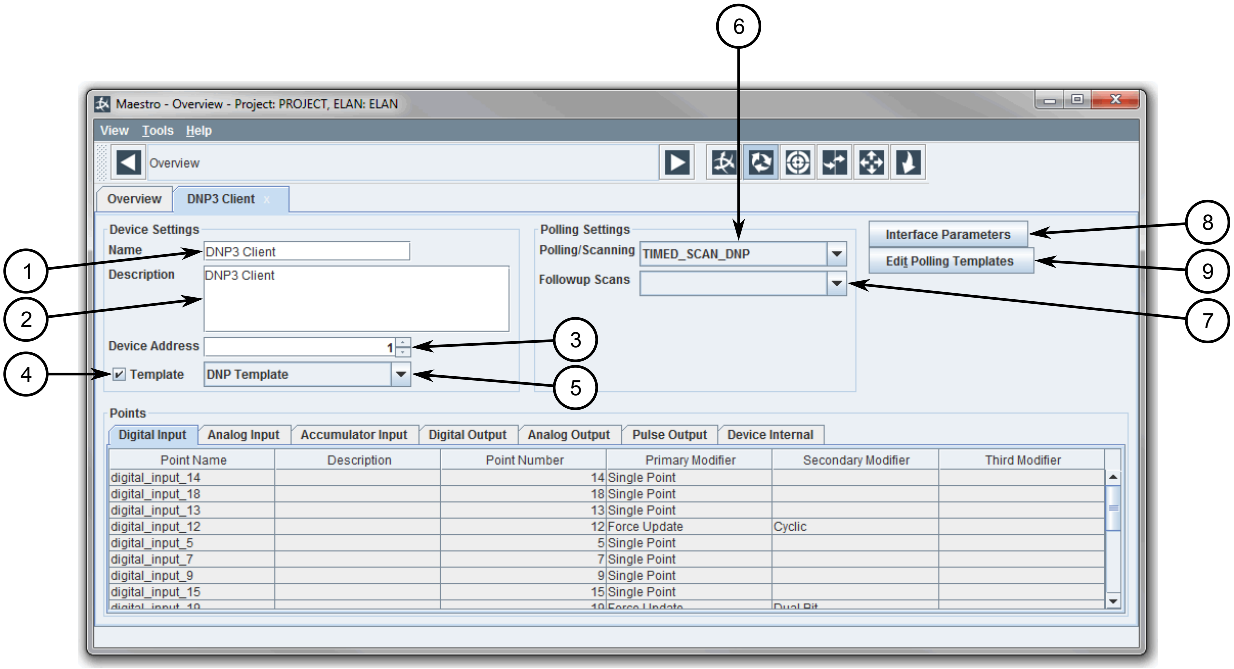
CONTENTS

- Section 4.10.7.2, “Configuring the Serial Communication Protocol”
- Section 4.10.7.3, “Configuring the TCP/UDP Communication Protocol”
- Section 4.10.7.4, “Configuring Basic RTU Settings”
- Section 4.10.7.5, “Configuring Protocol Settings”
- Section 4.10.7.6, “Configuring DNP File Management Settings”
- Section 4.10.7.7, “Configuring a Point”

Section 4.10.7.1
Configuring DNP Client

To configure a DNP client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.



Device Settings
Name: DNP3 Client
Description: DNP3 Client
Device Address: 1
☑ Template: DNP Template

Polling Settings
Polling/Scanning: TIMED_SCAN_DNP
Followup Scans:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_14		14	Single Point		
digital_input_18		18	Single Point		
digital_input_13		13	Single Point		
digital_input_12		12	Force Update	Cyclic	
digital_input_5		5	Single Point		
digital_input_7		7	Single Point		
digital_input_9		9	Single Point		
digital_input_15		15	Single Point		
digital_input_10		10	Force Update	Dual Bit	

Figure 100: DNP Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Polling/Scanning List **7.** Followup Scans List **8.** Interface Parameters Button **9.** Edit Polling Templates Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 65535

Parameter	Description
	The protocol address for the client device.

4. Under **Polling Settings**, configure the following parameters as required:

Parameter	Description
Polling/Scanning	The polling scheme group or timed scan group to use.
Followup Scans	The control follow-up group to use.

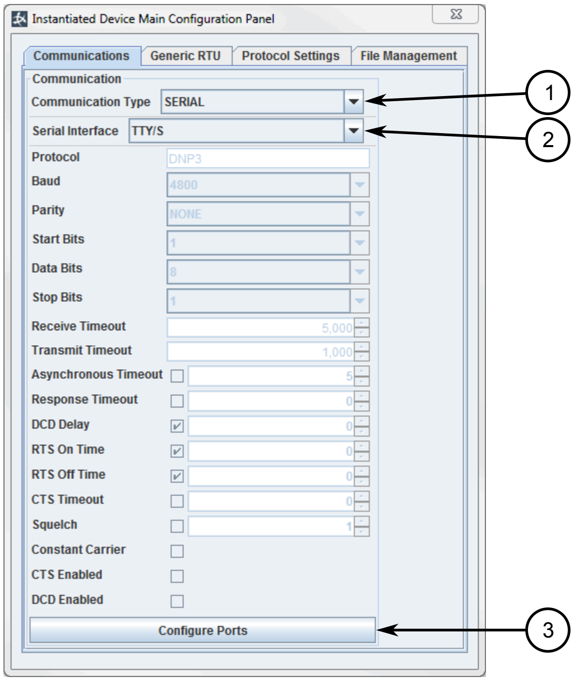
5. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
6. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
7. [Optional] Configure the communication protocol settings. For more information, refer to either Section 4.10.7.3, “Configuring the TCP/UDP Communication Protocol” or Section 4.10.7.2, “Configuring the Serial Communication Protocol”
8. [Optional] Configure the protocol settings. For more information, refer to Section 4.10.7.5, “Configuring Protocol Settings”
9. [Optional] Configure the file management settings. For more information, refer to Section 4.10.7.6, “Configuring DNP File Management Settings”
10. [Optional] Configure polling templates for the device. For more information, refer to Section 4.11, “Managing Polling Templates” .
11. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.10.6, “Enabling/Disabling Device Internal Points” .

Section 4.10.7.2

Configuring the Serial Communication Protocol

To configure the serial communication protocol for a DNP client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.

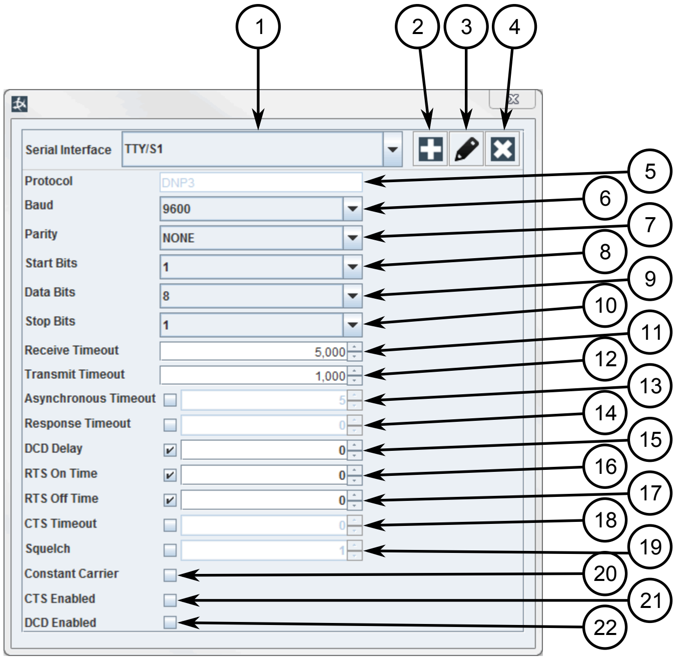


Communication Type: SERIAL
Serial Interface: TTY/S
Protocol: DNP3
Baud: 4800
Parity: NONE
Start Bits: 1
Data Bits: 8
Stop Bits: 1
Receive Timeout: 5,000
Transmit Timeout: 1,000
Asynchronous Timeout □ 5
Response Timeout □ 0
DCD Delay ☑ 0
RTS On Time ☑ 0
RTS Off Time ☑ 0
CTS Timeout □ 0
Squelch □ 1
Constant Carrier □
CTS Enabled □
DCD Enabled □

Figure 101: Instantiated Device Main Configuration Panel Dialog Box – Communications (Serial Protocol Selected)

1. Communication Type List **2.** Serial Interface List **3.** Serial Interface Settings

4. Under **Communication Type**, select `Serial`.
5. Under **Serial Interface**, select one of the available serial interfaces. The settings for the serial interface populate the fields below. If the settings need to be modified or if a new serial interface is required, proceed to the next step.
6. Click **Configure Ports**. A dialog box appears.



Serial Interface	TTY/S1
Protocol	DNP3
Baud	9600
Parity	NONE
Start Bits	1
Data Bits	8
Stop Bits	1
Receive Timeout	5,000
Transmit Timeout	1,000
Asynchronous Timeout	□ 5
Response Timeout	□ 0
DCD Delay	☑ 0
RTS On Time	☑ 0
RTS Off Time	☑ 0
CTS Timeout	□ 0
Squelch	□ 1
Constant Carrier	□
CTS Enabled	□
DCD Enabled	□

Figure 102: Dialog Box

1. Serial Interface List **2.** Create Serial Interface Button **3.** Rename Serial Interface Button **4.** Delete Serial Interface Button **5.** Protocol Box **6.** Baud List **7.** Parity List **8.** Start Bits List **9.** Data Bits List **10.** Stop Bits List **11.** Receive Timeout Box **12.** Transmit Timeout Box **13.** Asynchronous Timeout Check Box and Box **14.** Response Timeout Check Box and Box **15.** DCD Delay Check Box and Box **16.** RTS On Time Check Box and Box **17.** RTS Off Time Check Box and Box **18.** CTS Timeout Check Box and Box **19.** Squelch Check Box and Box **20.** Constant Carrier Check Box **21.** CTS Enabled Check Box **22.** DCD Enabled Check Box

7. Select a serial interface from the **Serial Interface** list to modify or click the **Create Serial Interface** button to create a new serial interface.
8. Configure the following parameters as required:

Parameter	Description
Baud	**Synopsis:** 3600, 4800, 7200, 9600, 19200, 38400, 57600, 115000 **Default:** 9600 The serial communications speed in bits-per-second (bps).
Parity	**Synopsis:** EVEN, ODD, NONE **Default:** NONE The parity to be used on the serial connection.
Start Bits	**Synopsis:** 0, 1, 2 **Default:** 1 The number of bits that precede each character.
Data Bits	**Synopsis:** 7, 8 **Default:** 8 The number of data bits contained in each character transmitted over the serial connection.

Parameter	Description
Stop Bits	**Synopsis:** 1, 2 **Default:** 1 The number of bits that follow each character.
Receive Timeout	**Synopsis:** 0 to 65535 **Default:** 5000 The maximum time in milliseconds (ms) to wait for an entire response message. If no message is received before the time period ends, the response will be considered to have failed.
Transmit Timeout	**Synopsis:** 0 to 65535 **Default:** 1000 The desired transmit timeout in milliseconds (ms). The time must be long enough to transmit the maximum length message sent to a client device at the given baud rate.
Asynchronous Timeout	**Synopsis:** 0 to 65535 **Default Value:** 20 **Default State:** Disabled The desired inter-message timeout in milliseconds (ms) used to detect the end of a message. The check box must be checked for this parameter to take effect.
Response Timeout	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Disabled The desired time in milliseconds (ms) to wait for a response message. Use for message types that require a response from the end device. The check box must be checked for this parameter to take effect.
DCD Delay	**Synopsis:** 0 to 65535 **Default Value:** 100 **Default State:** Enabled The desired time delay in milliseconds (ms) from the moment the serial device detects a Data Carrier Detect (DCD) control signal is received until the receiver hardware is enabled. The check box must be checked for this parameter to take effect.
RTS On Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to assert the Request to Send (RTS) control signal before transmitting a message. The check box must be checked for this parameter to take effect.
RTS Off Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to continue asserting the Request to Send (RTS) control signal after transmitting a message. The check box must be checked for this parameter to take effect.
CTS Timeout	**Synopsis:** 0 to 65535 **Default:** 100 The desired time in milliseconds (ms) to wait for a Clear to Send (CTS) control signal before aborting the transmission of a message. The check box must be checked for this parameter to take effect.
Squelch	**Synopsis:** 0 to 65535 **Default Value:** 100

Parameter	Description
	Default State: Disabled The desired time in milliseconds (ms) to wait after a Data Carrier Detect (DCD) control signal is received before enabling reception. The check box must be checked for this parameter to take effect.
Constant Carrier	**Default State:** Disabled When enabled (selected), the carrier is set to *constant*. Otherwise, the carrier is set to *switched*.
CTS Enabled	**Default State:** Disabled When enabled (selected), Clear to Send (CTS) control signals are enabled.
DCD Enabled	**Default State:** Disabled When enabled (selected), Data Carrier Detect (DCD) control signals are enabled.

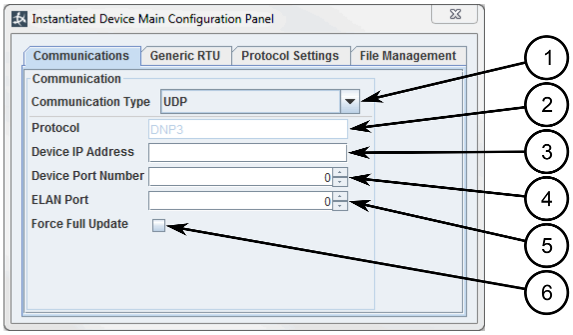
9. Close the dialog box.

Section 4.10.7.3

Configuring the TCP/UDP Communication Protocol

To configure the TCP or UDP communication protocol for a DNP client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.



Communication Type: UDP
Protocol: DNP3
Device IP Address:
Device Port Number: 0
ELAN Port: 0
Force Full Update: □

Figure 103: Instantiated Device Main Configuration Panel Dialog Box – Communications (UDP Protocol Selected)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box **5.** RUGGEDCOM ELAN Port Box **6.** Force Full Update Check Box

4. Under **Communication Type**, select either **TCP** or **UDP**.
5. Configure the following parameters:

Parameter	Description
Device IP Address	The IP address of the remote device or IED.

Parameter	Description
Device Port Number	**Synopsis:** 1 to 65535 **Default:** 0 The port for the remote device or IED. The suggested value for DNP client devices is 20000.
RUGGEDCOM ELAN Port	**Synopsis:** 0 to 65535 **Default:** 0 The port used by RUGGEDCOM ELAN to connect with the remote device or IED. A value of 0 represents a wild socket (any available port > 1024). Configure this parameter when a remote device or IED requires a connection on a specific port.
Force Full Update	Controls when data acquired as part of a full update is written to the TIE database. When checked/enabled, data is always written to the TIE database. When clear/disabled, data is only written to the TIE database if the value has changed.

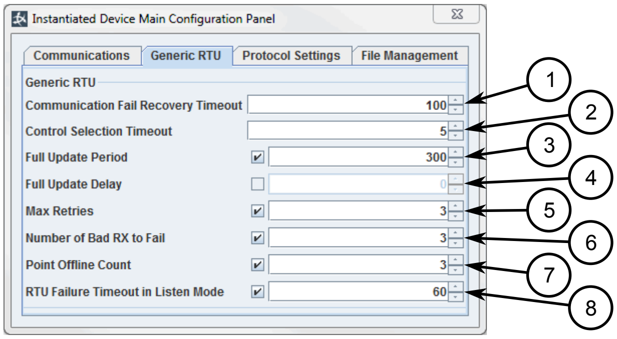
Section 4.10.7.4

Configuring Basic RTU Settings

To configure the basic Remote Terminal Unit (RTU) settings for a DNP client device, do the following:

> **NOTE**
> *For more advanced options, refer to Section 4.10.7.5, "Configuring Protocol Settings" .*

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Generic RTU** tab is displayed.



Generic RTU

Communication Fail Recovery Timeout: 100
Control Selection Timeout: 5
Full Update Period ☑ 300
Full Update Delay □ 0
Max Retries ☑ 3
Number of Bad RX to Fail ☑ 3
Point Offline Count ☑ 3
RTU Failure Timeout in Listen Mode ☑ 60

Figure 104: Instantiated Device Main Configuration Panel Dialog Box – Generic RTU

1. Communication Fail Recovery Timeout Box **2.** Control Selection Timeout Box **3.** Full Update Period Box **4.** Full Update Delay Box **5.** Max Retries Box **6.** Number of Bad RX to Fail Box **7.** Point Offline Count Box **8.** RTU Failure Timeout in Listen Mode Box

4. Configure the following parameters as required:

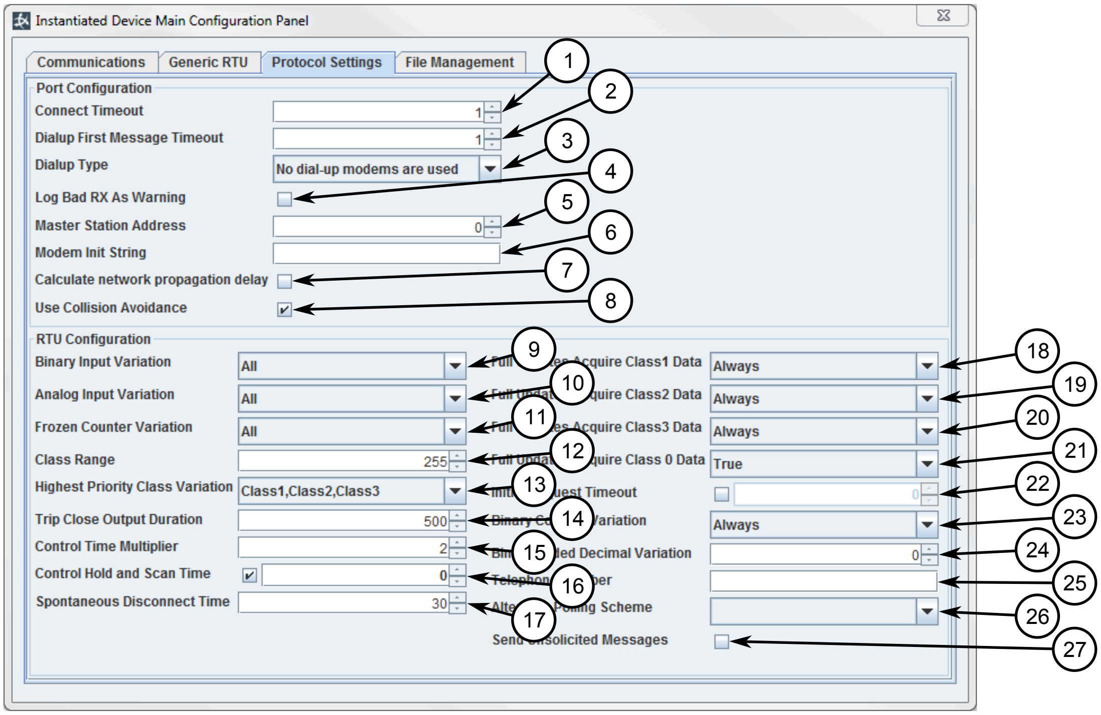
Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 100 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
Point Offline Count	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a scan – including retries – can consecutively fail to acquire the requested data before the unreported points are considered off-line (failed).
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.7.5

Configuring Protocol Settings

To configure protocol settings for DNP client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **Protocol Settings** tab.



Port Configuration

Connect Timeout 1

Dialup First Message Timeout 1

Dialup Type No dial-up modems are used

Log Bad RX As Warning □

Master Station Address 0

Modem Init String

Calculate network propagation delay □

Use Collision Avoidance ☑

RTU Configuration

Binary Input Variation All

Analog Input Variation All

Frozen Counter Variation All

Class Range 255

Highest Priority Class Variation Class1,Class2,Class3

Trip Close Output Duration 500

Control Time Multiplier 2

Control Hold and Scan Time ☑ 0

Spontaneous Disconnect Time 30

Full ...es Acquire Class1 Data Always

Full Updat... quire Class2 Data Always

Full ...es Acquire Class3 Data Always

Full Updat... quire Class 0 Data True

Initi... uest Timeout □ 0

Binary Co... Variation Always

Bin... ded Decimal Variation 0

Telephon... ber

Alte... Polling Scheme

Send ... solicited Messages □

Figure 105: Instantiated Device Main Configuration Panel Dialog Box – Protocol Settings

1. Connect Timeout Box **2.** Dialup First Message Timeout Box **3.** Dialup Type List **4.** Log Bad RX As Warning Check Box **5.** Master Station Address Box **6.** Modem Init String Box **7.** Calculate Network Propagation Delay Check Box **8.** User Collision Avoidance Check Box **9.** Binary Input Variation List **10.** Analog Input Variation List **11.** Frozen Counter Variation List **12.** Class Range Block **13.** Highest Priority Class Variation List **14.** Trip Close Output Duration Box **15.** Control Time Multiplier Box **16.** Control Hold and Scan Time Box **17.** Spontaneous Disconnect Time Box **18.** Full Updates Acquire Class1 Data List **19.** Full Updates Acquire Class2 Data List **20.** Full Updates Acquire Class3 Data List **21.** Full Updates Acquire Class 0 Data List **22.** Initial Request Timeout Box **23.** Binary Counter Variation Box **24.** Binary Coded Decimal Variation Box **25.** Telephone Number Box **26.** Alternate Polling Scheme List **27.** Send Unsolicited Messages Check Box

5. Under **Port Configuration**, configure the following parameters as required:

Parameter	Description
Connect Timeout	**Synopsis:** 1 to 120 **Default:** 1 The maximum time in seconds (s) to wait for a connection after dialing. Only applicable in dial-up mode.
Dialup First Message Timeout	**Synopsis:** 1 to 120 **Default:** 1

Parameter	Description
	The maximum time in seconds (s) to wait to receive the first message after a call has been answered. Only applicable in dial-up mode.
Dialup Type	**Synopsis:** No dial-up modems are used, Dial-up is performed by TIE DNP remote process itself **Default:** No dial-up modems are used The dial-up function in use.
Log Bad RX As Warning	When enabled (selected), bad messages received from an RTU, including the associated transmitted host WARNING message, are logged.
Master Station Address	**Synopsis:** 0 to 65534 **Default:** 0 The master station address associated with the TIE remote process on this port.
Modem Init String	The modem initialization string associated with this port.
Calculate Network Propagation Delay	When enabled (selected), the network propagation delay is calculated before time is synchronized on an RTU over the network. This is not applicable to serial ports, as the propagation delay is always calculated first.
Use Collision Avoidance	When enabled (selected), transmissions are delayed until an asserted Data Carrier Detect (DCD) signal is released. If a DCD has not been asserted, the transmission is sent immediately.

6. Under **RTU Configuration**, configure the following parameters as required:

Parameter	Description
Binary Input Variation	**Synopsis:** All, Binary Input, Binary Input with Flags **Default:** All The type of variation of the Binary Input object (object 1) to be used when requesting all binary point data as part of a full update.
Analog Input Variation	**Synopsis:** Disabled, All, 32 Bit with flag, 16 Bit with flag, 32 Bit, 16 Bit **Default:** All The type of variation of the Analog Input object (object 30) to be used when requesting all analog point data as part of a full update.
Frozen Counter Variation	**Synopsis:** Disabled, All, 32 Bit with flag, 16 Bit with flag, 32 Bit with flag delta, 16 Bit with flag delta, 32 Bit with flag and time, 32 Bit, 16 Bit **Default:** All The type of variation of the Frozen Counter object (object 21) to be used when reading all frozen counter after a DNP 3.0 *Immediate Freeze* or *Freeze and Clear* request.
Class Range	**Synopsis:** -1 to 255 **Default:** 255 The number of data objects requested with one DNP 3.0 *Read* request for Class 1, 2 or 3 data.
Highest Priority Class Variation	**Synopsis:** Class1,Class2,Class3, Class3,Class2,Class1 **Default:** Class1,Class2,Class3

Parameter	Description
	The type of variation of the Class object (object 60) that has the highest priority. Use to determine the order of polling an RTU for Class data when data for more than one class is available.
Trip Close Output Duration	**Synopsis:** 100 to 5000 **Default:** 500 The time in milliseconds (ms) to operate a Trip/Close relay if the *host select*, *execute*, or *direct execute* command does not specify an output duration.
Control Time Multiplier	**Synopsis:** 1 to 100 **Default:** 2 The multiplier to use against a non-zero value received from an internal *host select*, *execute*, or *direct execute* command for a Trip/Close relay. The result is time in milliseconds (ms) to operate a Trip/Close relay.
Control Hold and Scan Time	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Enabled The time in seconds (s) to scan the RTU for Class data after a control command (i.e. control operate, direct operate, accumulator freeze, accumulator freeze and reset) is issued before hanging up the dial-up connection initiated by the client process. In cases where the client process has initiated the dial-up connection to the RTU to clear the RTU's *Restart* bit, synchronize the RTU's time, request a full update, and/or acquire Class data previously indicated as being available, this parameter can also used to limit the time the client process can spend acting on IIN (Issuer Identification Number) bits set in a response message from the RTU. The client process will hang up once either the timer expires or the IIN bits are cleared in the last response message received from the RTU. The check box must be checked for this parameter to take effect.
Spontaneous Disconnect Time	**Synopsis:** 1 to 300 **Default:** 30 The time in seconds (s) before hanging up following a dial-up connection initiated by the RTU. During this time, the client device process may act on IIN (Issuer Identification Number) bits set in a message from the RTU. For example, the client may ask the RTU to clear its Restart bit, synchronize the RTU's time, and/or ask for required indicated class data. Even if the IIN bits are cleared in the last message received from the RTU (i.e. no restart is indicated, no time synchronization is needed, and no Class data is available), the client will not hang up until the Disconnect Time timer expires to allow the RTU to send more spontaneous messages.
Full Updates Acquire Class1 Data	**Synopsis:** Never, If Available, Always **Default:** Always Determines when full updates should acquire all Class 1 event data. Options include: • `Never` – Class 1 event data is never acquired • `If Available` – Class 1 event data is only acquired if it is available • `Always` – The full update always attempts to acquire Class 1 event data
Full Updates Acquire Class2 Data	**Synopsis:** Never, If Available, Always **Default:** Always Determines when full updates should acquire all Class 2 event data. Options include:

Parameter	Description
	• `Never` – Class 2 event data is never acquired • `If Available` – Class 2 event data is only acquired if it is available • `Always` – The full update always attempts to acquire Class 2 event data
Full Updates Acquire Class3 Data	**Synopsis:** Never, If Available, Always **Default:** Always Determines when full updates should acquire all Class 3 event data. Options include: • `Never` – Class 3 event data is never acquired • `If Available` – Class 3 event data is only acquired if it is available • `Always` – The full update always attempts to acquire Class 3 event data
Full Updates Acquire Class0 Data	**Synopsis:** False, True **Default:** True Determines when full updates should acquire all Class 0 data, specifically static data, as opposed to being limited to all Binary Inputs and (if configured) Analog Inputs, Floating Points Objects, BCD Objects and all Binary Counters. Options include: • `False` – Class 0 data is never acquired • `Truie` – The full update always attempts to acquire Class 0 data
Initial Request Timeout	**Synopsis:** 0 to 60000 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to wait for a response to an initial request. This parameter overrides the normal message response timeout settings in the case where DNP Reset Link requests are issued. The Reset Link request is issued on startup or when attempting to recover communications with the RTU. Configuring an extended timeout period for first message transactions may be useful for cases such as the use of SSL (Secure Socket Layer) communication for authentication and data decryption/encryption where the first message response may be delayed significantly while the SSL connection is established. Configuring a reduced timeout for first message transactions may be useful for cases where retrying failed RTUs results in delayed scanning due to long timeouts being required for normal communications. The check box must be checked for this parameter to take effect.
Binary Counter Variation	**Synopsis:** Disabled, Always, 32 Bit with Flag, 16 Bit with Flag, 32 Bit, 16 Bit **Default:** Always The type of variation of the Binary Counter Object (object 20) to be used when requesting all Binary Counter values as part of a full update.
Binary Coded Decimal Variation	**Synopsis:** 0 to 2 **Default:** 0 The type of variation of the BCD Object (object 101) to be used when reading all BCD values as part of a full update.
Telephone Number	The phone number to use for dial-up connections to an RTU. Add *ATDP* to the end of the number to indicate a Pulse dial operation, or *ATDT* to indicate a Tone dial operation. The complete dial string must be enclosed in single quotes (e.g. '{number}ATDP').

Parameter	Description
Alternate Polling Scheme	The alternate polling scheme number associated with this RTU. Leave blank to disable this option.

Section 4.10.7.6

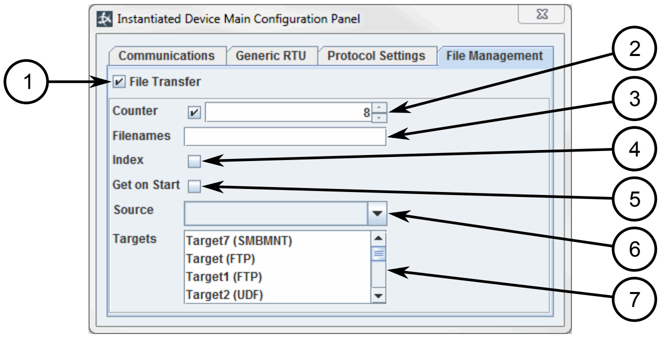
Configuring DNP File Management Settings

To configure file management settings for DNP client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.

> **NOTE**
> *The **File Management** tab is available only when RUGGEDCOM ELAN's Automatic File Management (AFM) is enabled. For more information about enabling AFM, refer to Section 4.6.8.1, “Enabling/Disabling the AFM” .*

4. Click the **File Management** tab.



☑ File Transfer

Counter ☑ 8

Filenames

Index □

Get on Start □

Source

Targets
Target7 (SMBMNT)
Target (FTP)
Target1 (FTP)
Target2 (UDF)

Figure 106: Instantiated Device Main Configuration Panel Dialog Box – File Management

1. File Transfer Check Box **2.** Counter Box **3.** Filenames Box **4.** Index Check Box **5.** Get On Start Check Box **6.** Source List **7.** Targets Box

5. Make sure the **File Transfer** check box is checked (enabled).
6. Configure the following parameters as required:

Parameter	Description
Counter	**Synopsis:** 0 to 65535 **Default Value:** 8 **Default State:** Enabled The specific counter to check for changes. Typical values for the UR F60 relay are 8 or 9. The check box must be checked for this parameter to take effect.
Filenames	The file names of one or more files to transfer (e.g. datalog.dat, faultreport.htm, etc.).
Index	**Default State:** Disabled

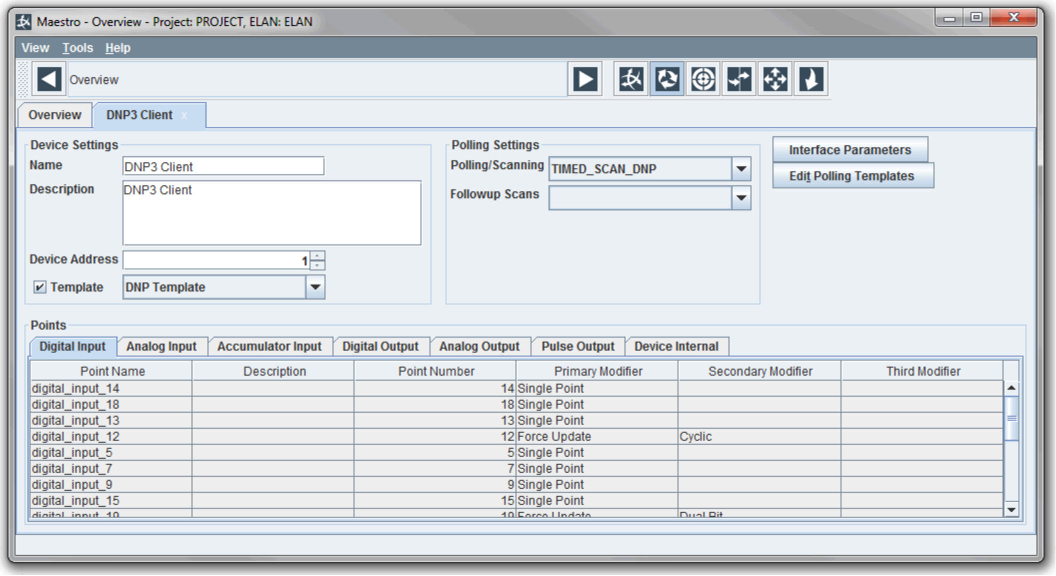
Parameter	Description
	When enabled (selected), filenames are indexed.
Get On Start	**Default State:** Disabled When enabled (selected), the target IED is polled at startup.
Source	The TFPTGET target from which the report will be retrieved. Targets are defined by the `Targets` parameter.
Targets	One or more defined TFTPGET targets where reports can be transferred to. The report will only be transferred to the select target(s)

Section 4.10.7.7

Configuring a Point

To configure/modify existing points for a DNP client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the DNP client device and click **Properties**. The device's properties appear in a new tab.



Name: DNP3 Client
Description: DNP3 Client
Device Address: 1
☑ Template: DNP Template
Polling/Scanning: TIMED_SCAN_DNP
Followup Scans:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_14		14	Single Point		
digital_input_18		18	Single Point		
digital_input_13		13	Single Point		
digital_input_12		12	Force Update	Cyclic	
digital_input_5		5	Single Point		
digital_input_7		7	Single Point		
digital_input_9		9	Single Point		
digital_input_15		15	Single Point		
digital_input_10		10	Force Update	Dual Bit	

Figure 107: DNP Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Single Point, Fleeting, Force Update, Cyclic, Inverted } The primary modifier. Options include: • `Single Point` – Use to identify a single status point. • `Fleeting` – Identifies a point that changes value temporarily, then changes back to its normal value. • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.
Secondary Modifier	**Synopsis:** { Cyclic, Inverted, Force Update, Dual Bit } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device. • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not.. • `Dual Bit` – Use to identify the first of two sequential single status points that are reported together as one point.
Third Modifier	**Synopsis:** { Cyclic, Inverted, Force Update, Dual Bit } The third modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device. • `Dual Bit` – Use to identify the first of two sequential single status points that are reported together as one point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).

Parameter	Description
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Float, BCD, DAC, 16 Bit, Unipolar, 32 Bit } The primary modifier. Options include: • `Float` – Use to identify a point that is reported in IEEE floating point format. • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. • `16 Bit` – Use to identify a 16-Bit 2's complement point that is to be processed as a 16-Bit 2's complement value without any scaling applied. • `Unipolar` – Use to identify a 16-Bit or 32-Bit point that is always positive in value. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Secondary Modifier	**Synopsis:** { Cyclic, Force Update, Time Tagged, Negated, Scaled, 32 Bit } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Time Tagged` – Use to indicate the time tag will be stored. • `Negated` – Use to identify a point whose value has been negated (i.e. multiplied by -1) when it is stored in the database before being reported to the host. • `Scaled` – Use to restore an analog value to its raw value after it has been scaled at the remote device. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Parameter	Description
Primary Modifier	**Synopsis:** { Cyclic, 16 Bit or 32 Bit } The primary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `16 Bit or 32 Bit` – Use to identify a 16-Bit or 32-Bit binary accumulator input point.
Secondary Modifier	**Synopsis:** { Cyclic } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digital_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Close Trip Pair, Trip Close Pair, Momentary, Single Point, Latch } The primary modifier. Options include: • `Close Trip Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Trip Close Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. This indicates the control message sent to the RTU should include the latching option.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.

Parameter	Description
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { 16 Bit } The primary modifier. Options include: • `16 Bit` – Use to identify a 16-Bit 2's complement analog output.
Units	A text field.

Section 4.10.8

Managing IEC 60870-5-101 Client Devices

This section describes how to manage IEC 60870-5-101 client devices.

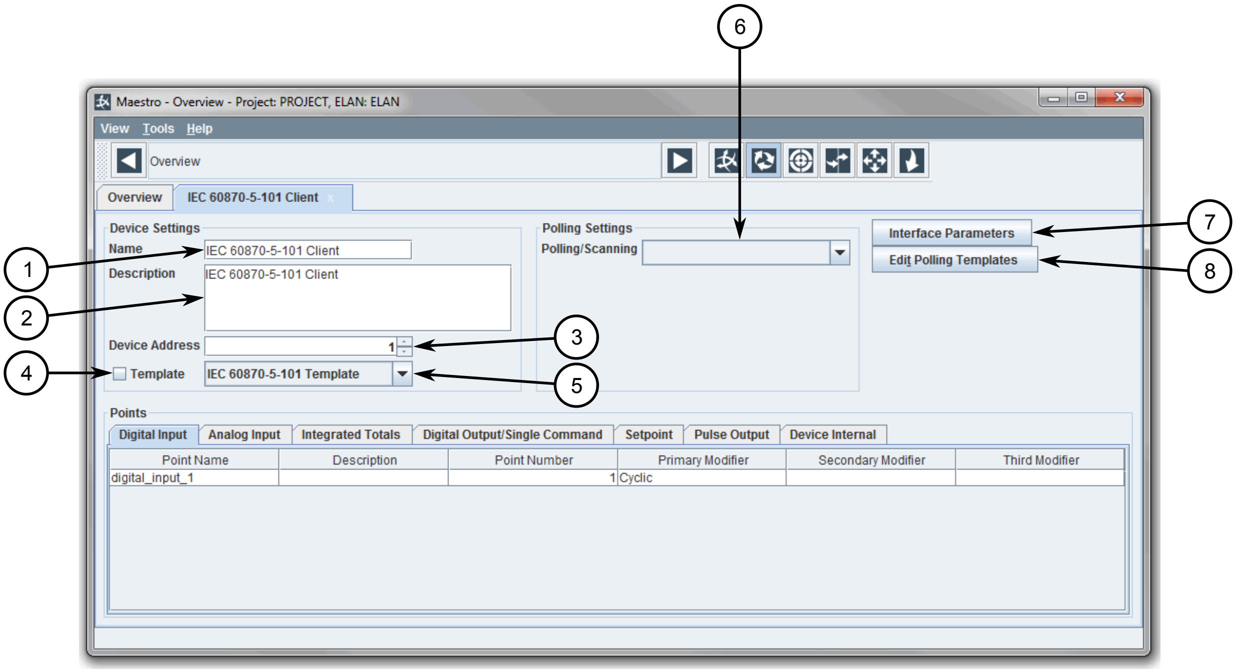
CONTENTS

Section 4.10.8.1

Configuring IEC 60870-5-101 Client

To configure an IEC 60870-5-101 client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 client device and click **Properties**. The device's properties appear in a new tab.



Overview | IEC 60870-5-101 Client

Device Settings

Name: IEC 60870-5-101 Client

Description: IEC 60870-5-101 Client

Device Address: 1

□ Template: IEC 60870-5-101 Template

Polling Settings

Polling/Scanning:

Points

Digital Input | Analog Input | Integrated Totals | Digital Output/Single Command | Setpoint | Pulse Output | Device Internal

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Cyclic		

Figure 108: IEC 60870-5-101 Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Polling/Scanning List **7.** Interface Parameters Button **8.** Edit Polling Templates Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 65535 The protocol address for the client device.

4. Under **Polling Settings**, configure the following parameters as required:

Parameter	Description
Polling/Scanning	The polling scheme group or timed scan group to use.

5. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
6. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
7. [Optional] Configure the communication protocol. For more information, refer to either Section 4.10.8.3, “Configuring the TCP/UDP Communication Protocol” or Section 4.10.8.3, “Configuring the TCP/UDP Communication Protocol” .
8. [Optional] Configure the protocol settings. For more information, refer to Section 4.10.8.5, “Configuring Protocol Settings”

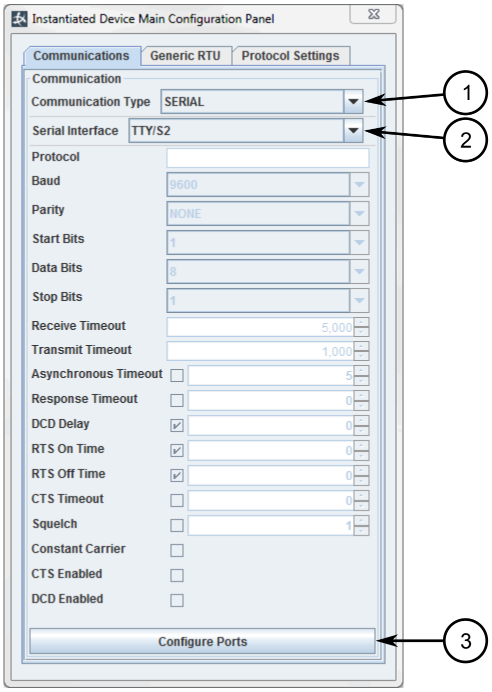
9. [Optional] Configure polling templates for the device. For more information, refer to Section 4.11, “Managing Polling Templates” .
10. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.10.6, “Enabling/Disabling Device Internal Points” .

Section 4.10.8.2

Configuring the Serial Communication Protocol

To configure the serial communication protocol for an IEC 60870-5-101 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.

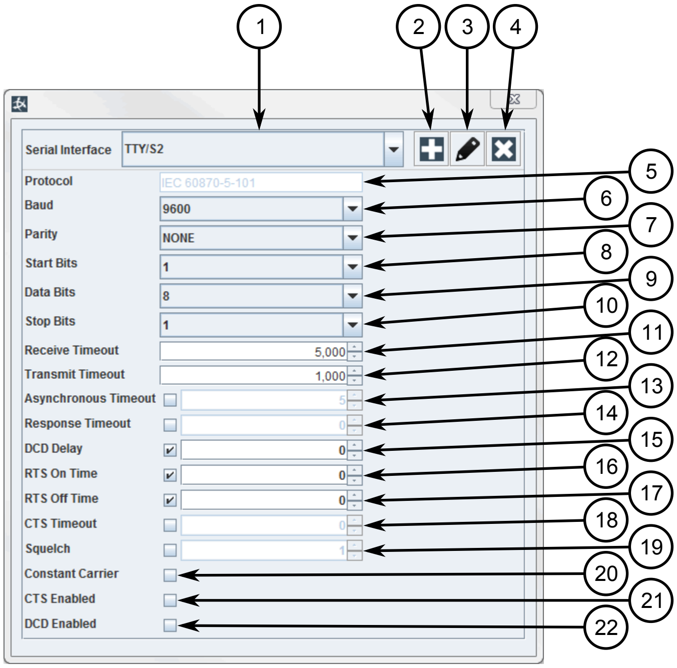


Communication Type: SERIAL
Serial Interface: TTY/S2
Protocol:
Baud: 9600
Parity: NONE
Start Bits: 1
Data Bits: 8
Stop Bits: 1
Receive Timeout: 5,000
Transmit Timeout: 1,000
Asynchronous Timeout: □ 5
Response Timeout: □ 0
DCD Delay: ☑ 0
RTS On Time: ☑ 0
RTS Off Time: ☑ 0
CTS Timeout: □ 0
Squelch: □ 1
Constant Carrier: □
CTS Enabled: □
DCD Enabled: □

Figure 109: Instantiated Device Main Configuration Panel Dialog Box – Communications (Serial Protocol Selected)

1. Communication Type List **2.** Serial Interface List **3.** Serial Interface Settings

4. Under **Communication Type**, select `Serial`.
5. Under **Serial Interface**, select one of the available serial interfaces. The settings for the serial interface populate the fields below. If the settings need to be modified or if a new serial interface is required, proceed to the next step.
6. Click **Configure Ports**. A dialog box appears.



Serial Interface TTY/S2

Protocol IEC 60870-5-101

Baud 9600

Parity NONE

Start Bits 1

Data Bits 8

Stop Bits 1

Receive Timeout 5,000

Transmit Timeout 1,000

Asynchronous Timeout □ 5

Response Timeout □ 0

DCD Delay ☑ 0

RTS On Time ☑ 0

RTS Off Time ☑ 0

CTS Timeout □ 0

Squelch □ 1

Constant Carrier □

CTS Enabled □

DCD Enabled □

Figure 110: Dialog Box

1. Serial Interface List **2.** Create Serial Interface Button **3.** Rename Serial Interface Button **4.** Delete Serial Interface Button **5.** Protocol Box **6.** Baud List **7.** Parity List **8.** Start Bits List **9.** Data Bits List **10.** Stop Bits List **11.** Receive Timeout Box **12.** Transmit Timeout Box **13.** Asynchronous Timeout Check Box and Box **14.** Response Timeout Check Box and Box **15.** DCD Delay Check Box and Box **16.** RTS On Time Check Box and Box **17.** RTS Off Time Check Box and Box **18.** CTS Timeout Check Box and Box **19.** Squelch Check Box and Box **20.** Constant Carrier Check Box **21.** CTS Enabled Check Box **22.** DCD Enabled Check Box

7. Select a serial interface from the **Serial Interface** list to modify or click the **Create Serial Interface** button to create a new serial interface.
8. Configure the following parameters as required:

Parameter	Description
Baud	**Synopsis:** 3600, 4800, 7200, 9600, 19200, 38400, 57600, 115000 **Default:** 9600 The serial communications speed in bits-per-second (bps).
Parity	**Synopsis:** EVEN, ODD, NONE **Default:** NONE The parity to be used on the serial connection.
Start Bits	**Synopsis:** 0, 1, 2 **Default:** 1 The number of bits that precede each character.
Data Bits	**Synopsis:** 7, 8 **Default:** 8 The number of data bits contained in each character transmitted over the serial connection.

Parameter	Description
Stop Bits	**Synopsis:** 1, 2 **Default:** 1 The number of bits that follow each character.
Receive Timeout	**Synopsis:** 0 to 65535 **Default:** 5000 The maximum time in milliseconds (ms) to wait for an entire response message. If no message is received before the time period ends, the response will be considered to have failed.
Transmit Timeout	**Synopsis:** 0 to 65535 **Default:** 1000 The desired transmit timeout in milliseconds (ms). The time must be long enough to transmit the maximum length message sent to a client device at the given baud rate.
Asynchronous Timeout	**Synopsis:** 0 to 65535 **Default Value:** 20 **Default State:** Disabled The desired inter-message timeout in milliseconds (ms) used to detect the end of a message. The check box must be checked for this parameter to take effect.
Response Timeout	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Disabled The desired time in milliseconds (ms) to wait for a response message. Use for message types that require a response from the end device. The check box must be checked for this parameter to take effect.
DCD Delay	**Synopsis:** 0 to 65535 **Default Value:** 100 **Default State:** Enabled The desired time delay in milliseconds (ms) from the moment the serial device detects a Data Carrier Detect (DCD) control signal is received until the receiver hardware is enabled. The check box must be checked for this parameter to take effect.
RTS On Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to assert the Request to Send (RTS) control signal before transmitting a message. The check box must be checked for this parameter to take effect.
RTS Off Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to continue asserting the Request to Send (RTS) control signal after transmitting a message. The check box must be checked for this parameter to take effect.
CTS Timeout	**Synopsis:** 0 to 65535 **Default:** 100 The desired time in milliseconds (ms) to wait for a Clear to Send (CTS) control signal before aborting the transmission of a message. The check box must be checked for this parameter to take effect.
Squelch	**Synopsis:** 0 to 65535 **Default Value:** 100

Parameter	Description
	Default State: Disabled The desired time in milliseconds (ms) to wait after a Data Carrier Detect (DCD) control signal is received before enabling reception. The check box must be checked for this parameter to take effect.
Constant Carrier	**Default State:** Disabled When enabled (selected), the carrier is set to *constant*. Otherwise, the carrier is set to *switched*.
CTS Enabled	**Default State:** Disabled When enabled (selected), Clear to Send (CTS) control signals are enabled.
DCD Enabled	**Default State:** Disabled When enabled (selected), Data Carrier Detect (DCD) control signals are enabled.

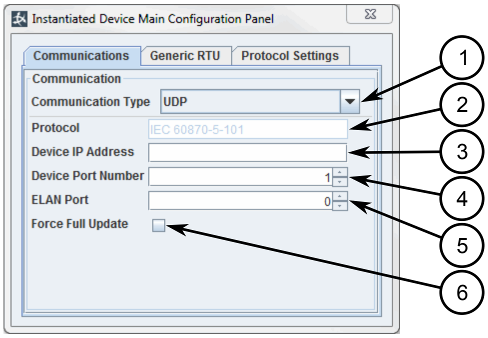
9. Close the dialog box.

Section 4.10.8.3

Configuring the TCP/UDP Communication Protocol

To configure the TCP or UDP communication protocol for a IEC 60870-5-101 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.



Communication Type UDP
Protocol IEC 60870-5-101
Device IP Address
Device Port Number 1
ELAN Port 0
Force Full Update □

Figure 111: Instantiated Device Main Configuration Panel Dialog Box – Communications (UDP Protocol Selected)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box **5.** RUGGEDCOM ELAN Port Box **6.** Force Full Update Check Box

4. Under **Communication Type**, select either **TCP** or **UDP**.
5. Configure the following parameters:

Parameter	Description
Device IP Address	The IP address of the remote device or IED.
Device Port Number	**Synopsis:** 1 to 65535 **Default:** 0 The port for the remote device or IED. The suggested value for IEC 60870-5-101 client devices is 20000.
RUGGEDCOM ELAN Port	**Synopsis:** 0 to 65535 **Default:** 0 The port used by RUGGEDCOM ELAN to connect with the remote device or IED. A value of 0 represents a wild socket (any available port > 1024). Configure this parameter when a remote device or IED requires a connection on a specific port.
Force Full Update	Controls when data acquired as part of a full update is written to the TIE database. When checked/enabled, data is always written to the TIE database. When clear/disabled, data is only written to the TIE database if the value has changed.

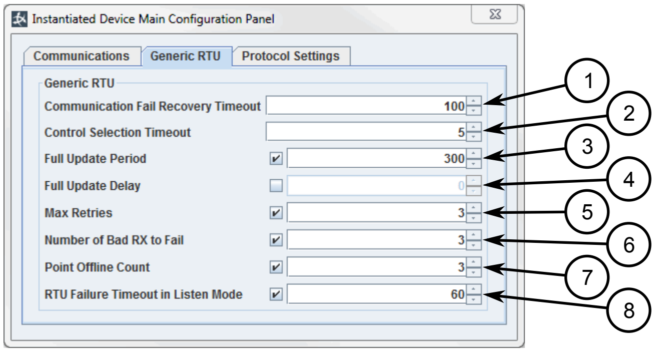
Section 4.10.8.4

Configuring Basic RTU Settings

To configure the basic Remote Terminal Unit (RTU) settings for an IEC 60870-5-101 client device, do the following:

> **NOTE**
> *For more advanced options, refer to Section 4.10.8.5, "Configuring Protocol Settings" .*

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Generic RTU** tab is displayed.



Generic RTU

Communication Fail Recovery Timeout 100

Control Selection Timeout 5

Full Update Period ☑ 300

Full Update Delay ☐ 0

Max Retries ☑ 3

Number of Bad RX to Fail ☑ 3

Point Offline Count ☑ 3

RTU Failure Timeout in Listen Mode ☑ 60

Figure 112: Instantiated Device Main Configuration Panel Dialog Box – Generic RTU

1. Communication Fail Recovery Timeout Box **2.** Control Selection Timeout Box **3.** Full Update Period Box **4.** Full Update Delay Box **5.** Max Retries Box **6.** Number of Bad RX to Fail Box **7.** Point Offline Count Box **8.** RTU Failure Timeout in Listen Mode Box

4. Configure the following parameters as required:

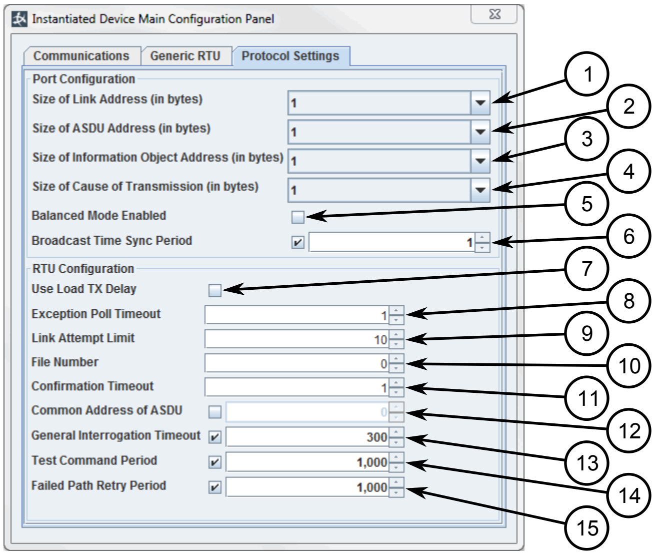
Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 100 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
Point Offline Count	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a scan – including retries – can consecutively fail to acquire the requested data before the unreported points are considered off-line (failed).
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.8.5

Configuring Protocol Settings

To configure protocol settings for IEC 60870-5-101 client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **Protocol Settings** tab.



Instantiated Device Main Configuration Panel

Communications | Generic RTU | Protocol Settings

Port Configuration

Size of Link Address (in bytes): 1

Size of ASDU Address (in bytes): 1

Size of Information Object Address (in bytes): 1

Size of Cause of Transmission (in bytes): 1

Balanced Mode Enabled ☐

Broadcast Time Sync Period ☑ 1

RTU Configuration

Use Load TX Delay ☐

Exception Poll Timeout: 1

Link Attempt Limit: 10

File Number: 0

Confirmation Timeout: 1

Common Address of ASDU ☐ 0

General Interrogation Timeout ☑ 300

Test Command Period ☑ 1,000

Failed Path Retry Period ☑ 1,000

Figure 113: Instantiated Device Main Configuration Panel Dialog Box – Protocol Settings

1. Size of Link Address (in bytes) List **2.** Size of ASDU Address (in bytes) List **3.** Size of Information Object Address (in bytes) List **4.** Size of Cause of Transmission (in bytes) List **5.** Balance Mode Enabled Check Box **6.** Broadcast Time Sync Period Box **7.** Use Load TX Delay Check Box **8.** Exception Poll Timeout Box **9.** Link Attempt Limit Box **10.** File Number Box **11.** Confirmation Timeout Box **12.** Common Address of ASDU Box **13.** General Interrogation Timeout Box **14.** Test Command Period Box **15.** Failed Path Retry Period Box

5. Under **Port Configuration**, configure the following parameters as required:

Parameter	Description
Size of Link Address (in bytes)	**Synopsis:** 0, 1, 2 **Default:** 1 The size of the link address. Link addresses are an optional address field in a Data Link frame. If no link address is sent by the RTU, set to 0.
Size of ASDU Address (in bytes)	**Synopsis:** 1, 2 **Default:** 1 The size in bytes of the Application Service Data Unit (ASDU) address. ASDU addresses is part of the Data Unit Identifier in an Application frame.
Size of Information Object Address (in bytes)	**Synopsis:** 1, 2, 3 **Default:** 1 The size in bytes of the Information Object Address (IOA). An IOA is part of each Information Object in an Application frame.
Size of of Cause of Transmission (in bytes)	**Synopsis:** 1, 2 **Default:** 1

Parameter	Description
	The size in bytes of the Cause of Transmission (COT). An COT is part of the Data Unit Identifier in an Application frame.
Balanced Mode Enabled	**Default State:** Disabled When enabled (selected), ELAN is placed in balanced mode, which prevents ELAN from polling an RTU for class data if the RTU is sending spontaneous messages.
Broadcast Time Sync Period	**Synopsis:** 1 to 9000 **Default Value:** 1 **Default State:** Enabled The time in seconds (s) between time synchronization broadcasts to all RTUs on the channel. The check box must be checked for this parameter to take effect. When disabled (cleared), no broadcasts are sent to the RTUs. Instead, each RTU will received individual time synchronization messages.

6. Under **RTU Configuration**, configure the following parameters as required:

Parameter	Description
Use Load TX Delay	When enabled (selected), a load transmission delay command is sent to the RTU between the acquisition of transmission delay and time synchronization commands.
Exception Poll Timeout	**Synopsis:** 0 to 60 **Default:** 1 The time in seconds (s) to poll for Class 1 data if the Automatic Call Distributor (ACD) flag is set.
Link Attempt Limit	**Synopsis:** 0 to 100 **Default:** 10 The number of attempts the remote process is allowed to establish a link with an RTU that is in restart mode before the RTU is considered failed.
File Number	**Synopsis:** 0 to 65535 **Default:** 0 The file number to be used as the file identifier in file transfer messages.
Confirmation Timeout	**Synopsis:** 0 to 10 **Default:** 1 The time in seconds (s) permitted to check for confirmation of an application-level command message.
Common Address of ASDU	**Synopsis:** 0 to 255 or 65535 **Default Value:** 1 **Default State:** Disabled The common address of the Application Service Data Unit (ASDU) used for point grouping by an ASDU address. The check box must be checked for this parameter to take effect. When disabled (cleared), the point group from point configuration is used. The value range is dependent on the size of the ASDU address set by the `Size of ASDU Address (in bytes)` parameter: • If the size is `1`, the range is 0 to 255 • If the size is `2`, the range is 0 to 65535

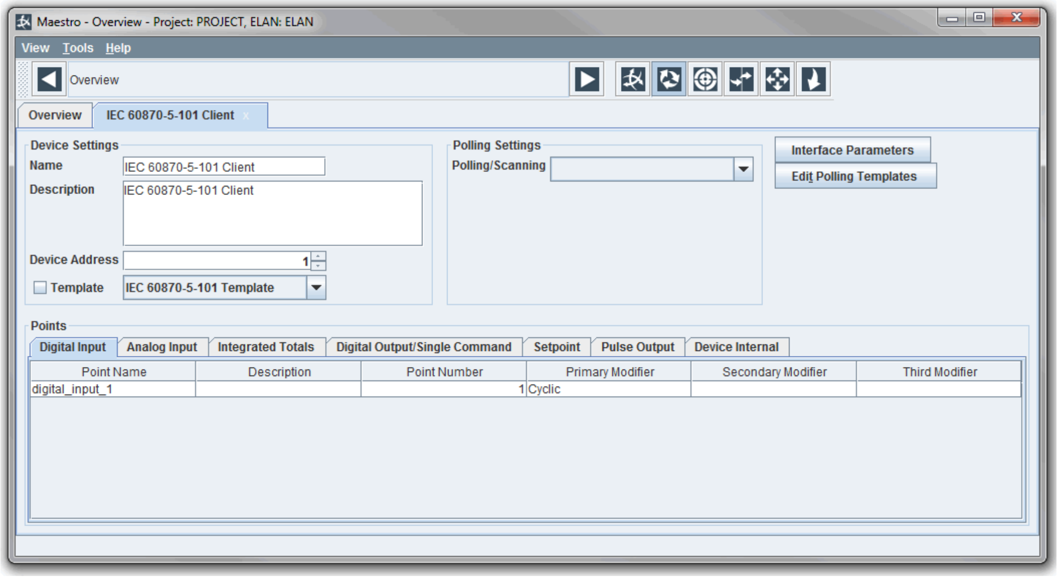
Parameter	Description
General Interrogation Timeout	**Synopsis:** 0 to 1000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait for an Activation Termination command to be received. If the command is not received before the time expires, a general interrogation (full update) is assumed to have completed. When disabled (cleared), the client process will wait infinitely for the command from the RTU.
Test Command Period	**Synopsis:** 0 to 90000 **Default Value:** 1000 **Default State:** Enabled The rate in seconds (s) at which to send a Test command to an RTU. When disabled (cleared), no Test command is sent.
Failed Path Retry Period	**Synopsis:** 0 to 90000 **Default Value:** 1000 **Default State:** Enabled The time in seconds (s) to wait before attempting to retry a failed higher-priority path to an RTU. When disabled (cleared), ELAN will not retry failed higher-priority paths.

Section 4.10.8.6

Configuring a Point

To configure/modify existing points for an IEC 60870-5-101 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-101 client device and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-101 Client

Description: IEC 60870-5-101 Client

Device Address: 1

□ Template: IEC 60870-5-101 Template

Polling/Scanning:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Cyclic		

Figure 114: IEC 60870-5-101 Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .

4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant, Cyclic } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point.

Parameter	Description
	• `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The secondary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.
Third Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The third modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. • `Bit Pair` – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • `Redundant` – Use to identify a point change of state and a time-tagged change of state are reported separately.

›› Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Force Update, BCD, DAC, 16 Bit, Cyclic }

Parameter	Description
	The primary modifier. Options include: • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Cyclic, Force Update, Time Tagged, Negated, Scaled, 32 Bit } The secondary modifier. Options include: • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

Integrated Totals

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. integrated_totals_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, 32 Bit } The primary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Secondary Modifier	**Synopsis:** { Cyclic } The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Units	A text field.

Digital Output/Single Command

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_single_command_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Momentary, Single Point, Latch, Preconfig } The primary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. This indicates the control message sent to the RTU should include the latching option. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).
Secondary Modifier	**Synopsis:** { Momentary, Single Point, Preconfig } The secondary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).

Setpoint

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. setpoint_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Units	A text field.

Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Section 4.10.9

Managing IEC 60870-5-104 Client Devices

This section describes how to manage IEC 60870-5-104 client devices.

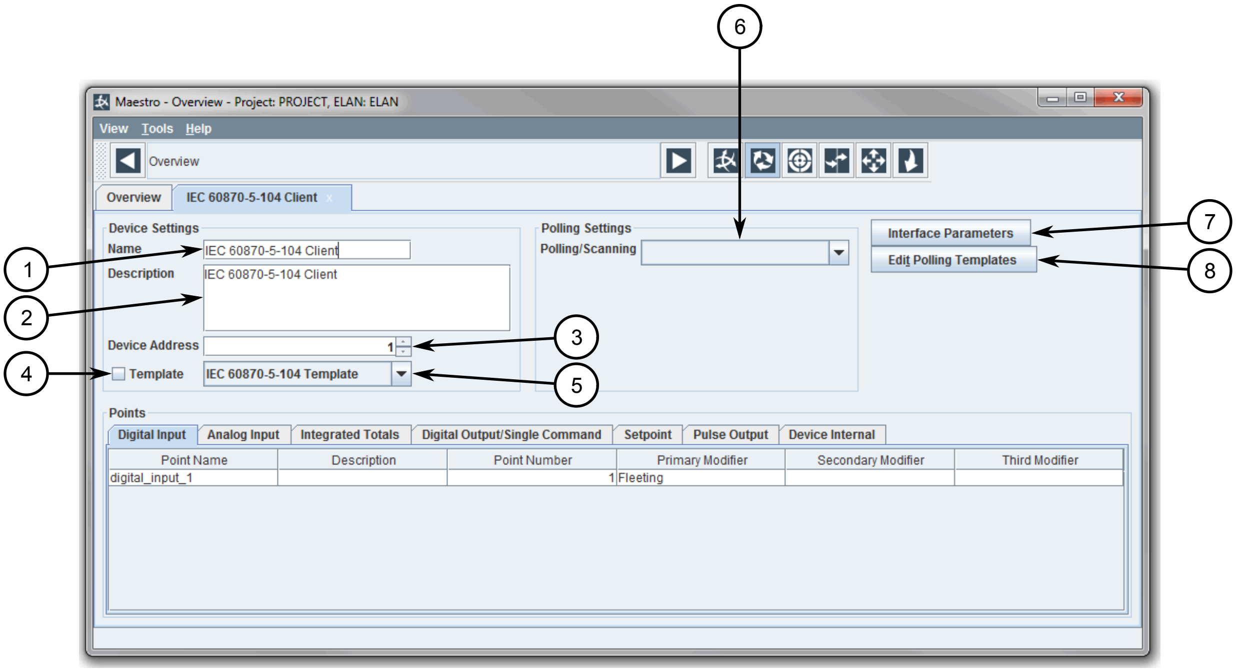
CONTENTS

Section 4.10.9.1

Configuring IEC 60870-5-104 Client

To configure an IEC 60870-5-104 client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 client device and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-104 Client

Description: IEC 60870-5-104 Client

Device Address: 1

□ Template: IEC 60870-5-104 Template

Polling/Scanning:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Fleeting		

Figure 115: IEC 60870-5-104 Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Polling/Scanning List **7.** Interface Parameters Button **8.** Edit Polling Templates Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 65535 The protocol address for the client device.

4. Under **Polling Settings**, configure the following parameters as required:

Parameter	Description
Polling/Scanning	The polling scheme group or timed scan group to use.

5. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
6. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
7. [Optional] Configure the communication protocol. For more information, refer to either Section 4.10.9.3, “Configuring the TCP/UDP Communication Protocol” or Section 4.10.9.3, “Configuring the TCP/UDP Communication Protocol” .
8. [Optional] Configure the protocol settings. For more information, refer to Section 4.10.9.5, “Configuring Protocol Settings”

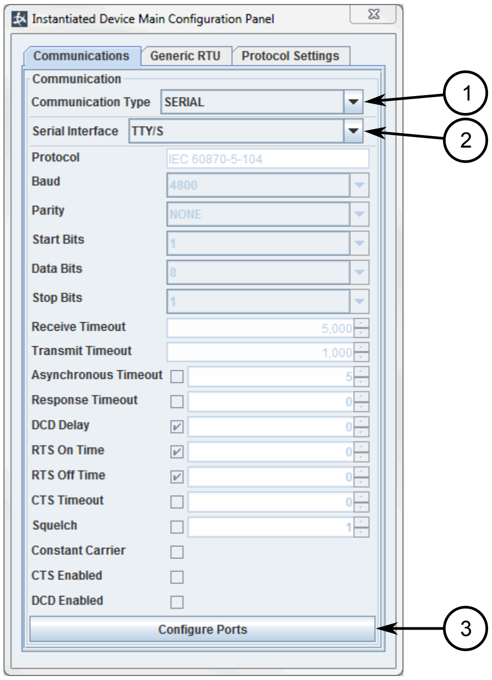
9. [Optional] Configure polling templates for the device. For more information, refer to Section 4.11, “Managing Polling Templates” .
10. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.10.6, “Enabling/Disabling Device Internal Points” .

Section 4.10.9.2

Configuring the Serial Communication Protocol

To configure the serial communication protocol for an IEC 60870-5-104 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.

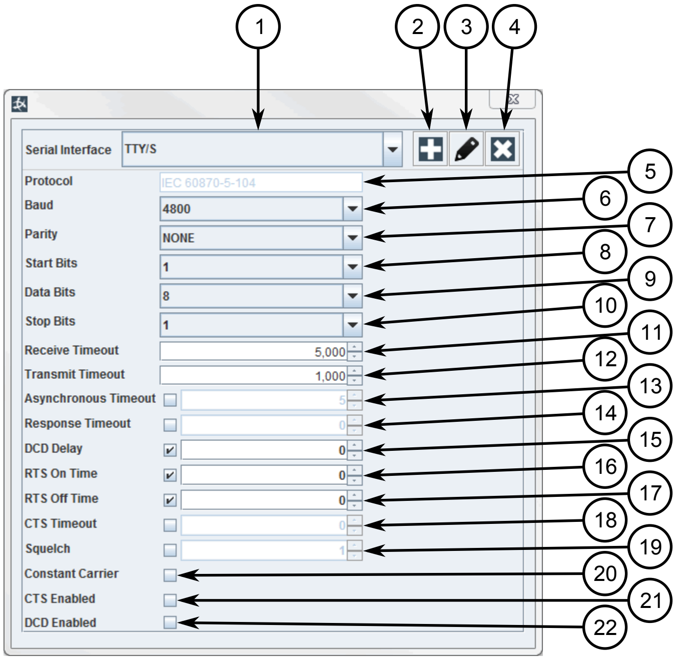


Communication Type: SERIAL
Serial Interface: TTY/S
Protocol: IEC 60870-5-104
Baud: 4800
Parity: NONE
Start Bits: 1
Data Bits: 8
Stop Bits: 1
Receive Timeout: 5,000
Transmit Timeout: 1,000
Asynchronous Timeout: □ 5
Response Timeout: □ 0
DCD Delay: ☑ 0
RTS On Time: ☑ 0
RTS Off Time: ☑ 0
CTS Timeout: □ 0
Squelch: □ 1
Constant Carrier: □
CTS Enabled: □
DCD Enabled: □

Figure 116: Instantiated Device Main Configuration Panel Dialog Box – Communications (Serial Protocol Selected)

1. Communication Type List **2.** Serial Interface List **3.** Serial Interface Settings

4. Under **Communication Type**, select `Serial`.
5. Under **Serial Interface**, select one of the available serial interfaces. The settings for the serial interface populate the fields below. If the settings need to be modified or if a new serial interface is required, proceed to the next step.
6. Click **Configure Ports**. A dialog box appears.



Serial Interface TTY/S

Protocol IEC 60870-5-104
Baud 4800
Parity NONE
Start Bits 1
Data Bits 8
Stop Bits 1
Receive Timeout 5,000
Transmit Timeout 1,000
Asynchronous Timeout □ 5
Response Timeout □ 0
DCD Delay ☑ 0
RTS On Time ☑ 0
RTS Off Time ☑ 0
CTS Timeout □ 0
Squelch □ 1
Constant Carrier □
CTS Enabled □
DCD Enabled □

Figure 117: Dialog Box

1. Serial Interface List **2.** Create Serial Interface Button **3.** Rename Serial Interface Button **4.** Delete Serial Interface Button **5.** Protocol Box **6.** Baud List **7.** Parity List **8.** Start Bits List **9.** Data Bits List **10.** Stop Bits List **11.** Receive Timeout Box **12.** Transmit Timeout Box **13.** Asynchronous Timeout Check Box and Box **14.** Response Timeout Check Box and Box **15.** DCD Delay Check Box and Box **16.** RTS On Time Check Box and Box **17.** RTS Off Time Check Box and Box **18.** CTS Timeout Check Box and Box **19.** Squelch Check Box and Box **20.** Constant Carrier Check Box **21.** CTS Enabled Check Box **22.** DCD Enabled Check Box

7. Select a serial interface from the **Serial Interface** list to modify or click the **Create Serial Interface** button to create a new serial interface.
8. Configure the following parameters as required:

Parameter	Description
Baud	**Synopsis:** 3600, 4800, 7200, 9600, 19200, 38400, 57600, 115000 **Default:** 9600 The serial communications speed in bits-per-second (bps).
Parity	**Synopsis:** EVEN, ODD, NONE **Default:** NONE The parity to be used on the serial connection.
Start Bits	**Synopsis:** 0, 1, 2 **Default:** 1 The number of bits that precede each character.
Data Bits	**Synopsis:** 7, 8 **Default:** 8 The number of data bits contained in each character transmitted over the serial connection.

Parameter	Description
Stop Bits	**Synopsis:** 1, 2 **Default:** 1 The number of bits that follow each character.
Receive Timeout	**Synopsis:** 0 to 65535 **Default:** 5000 The maximum time in milliseconds (ms) to wait for an entire response message. If no message is received before the time period ends, the response will be considered to have failed.
Transmit Timeout	**Synopsis:** 0 to 65535 **Default:** 1000 The desired transmit timeout in milliseconds (ms). The time must be long enough to transmit the maximum length message sent to a client device at the given baud rate.
Asynchronous Timeout	**Synopsis:** 0 to 65535 **Default Value:** 20 **Default State:** Disabled The desired inter-message timeout in milliseconds (ms) used to detect the end of a message. The check box must be checked for this parameter to take effect.
Response Timeout	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Disabled The desired time in milliseconds (ms) to wait for a response message. Use for message types that require a response from the end device. The check box must be checked for this parameter to take effect.
DCD Delay	**Synopsis:** 0 to 65535 **Default Value:** 100 **Default State:** Enabled The desired time delay in milliseconds (ms) from the moment the serial device detects a Data Carrier Detect (DCD) control signal is received until the receiver hardware is enabled. The check box must be checked for this parameter to take effect.
RTS On Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to assert the Request to Send (RTS) control signal before transmitting a message. The check box must be checked for this parameter to take effect.
RTS Off Time	**Synopsis:** 0 to 65535 **Default Value:** 0 **Default State:** Enabled The desired time in milliseconds (ms) to continue asserting the Request to Send (RTS) control signal after transmitting a message. The check box must be checked for this parameter to take effect.
CTS Timeout	**Synopsis:** 0 to 65535 **Default:** 100 The desired time in milliseconds (ms) to wait for a Clear to Send (CTS) control signal before aborting the transmission of a message. The check box must be checked for this parameter to take effect.
Squelch	**Synopsis:** 0 to 65535 **Default Value:** 100

Parameter	Description
	Default State: Disabled The desired time in milliseconds (ms) to wait after a Data Carrier Detect (DCD) control signal is received before enabling reception. The check box must be checked for this parameter to take effect.
Constant Carrier	**Default State:** Disabled When enabled (selected), the carrier is set to *constant*. Otherwise, the carrier is set to *switched*.
CTS Enabled	**Default State:** Disabled When enabled (selected), Clear to Send (CTS) control signals are enabled.
DCD Enabled	**Default State:** Disabled When enabled (selected), Data Carrier Detect (DCD) control signals are enabled.

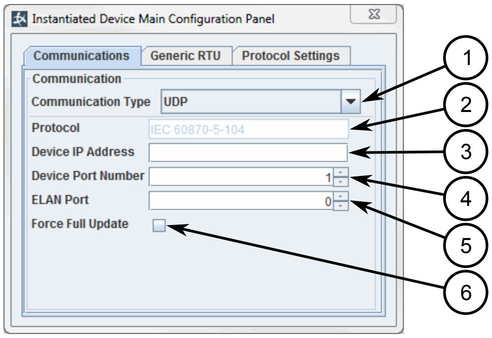
9. Close the dialog box.

Section 4.10.9.3

Configuring the TCP/UDP Communication Protocol

To configure the TCP or UDP communication protocol for a IEC 60870-5-104 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communications** tab is displayed.



Instantiated Device Main Configuration Panel

Communication

Communication Type: UDP

Protocol: IEC 60870-5-104

Device IP Address:

Device Port Number: 1

ELAN Port: 0

Force Full Update: □

Figure 118: Instantiated Device Main Configuration Panel Dialog Box – Communications (UDP Protocol Selected)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box **5.** RUGGEDCOM ELAN Port Box **6.** Force Full Update Check Box

4. Under **Communication Type**, select either **TCP** or **UDP**.
5. Configure the following parameters:

Parameter	Description
Device IP Address	The IP address of the remote device or IED.
Device Port Number	**Synopsis:** 1 to 65535 **Default:** 0 The port for the remote device or IED. The suggested value for IEC 60870-5-104 client devices is 20000.
RUGGEDCOM ELAN Port	**Synopsis:** 0 to 65535 **Default:** 0 The port used by RUGGEDCOM ELAN to connect with the remote device or IED. A value of 0 represents a wild socket (any available port > 1024). Configure this parameter when a remote device or IED requires a connection on a specific port.
Force Full Update	Controls when data acquired as part of a full update is written to the TIE database. When checked/enabled, data is always written to the TIE database. When clear/disabled, data is only written to the TIE database if the value has changed.

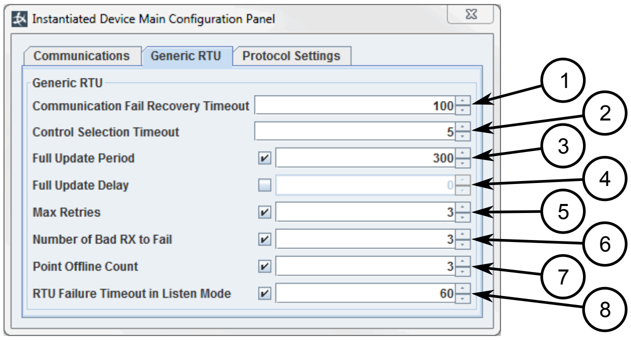
Section 4.10.9.4

Configuring Basic RTU Settings

To configure the basic Remote Terminal Unit (RTU) settings for an IEC 60870-5-104 client device, do the following:

> **NOTE**
>
> *For more advanced options, refer to Section 4.10.9.5, “Configuring Protocol Settings” .*

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Generic RTU** tab is displayed.



Generic RTU

Communication Fail Recovery Timeout 100

Control Selection Timeout 5

Full Update Period ☑ 300

Full Update Delay □ 0

Max Retries ☑ 3

Number of Bad RX to Fail ☑ 3

Point Offline Count ☑ 3

RTU Failure Timeout in Listen Mode ☑ 60

Figure 119: Instantiated Device Main Configuration Panel Dialog Box – Generic RTU

1. Communication Fail Recovery Timeout Box **2.** Control Selection Timeout Box **3.** Full Update Period Box **4.** Full Update Delay Box **5.** Max Retries Box **6.** Number of Bad RX to Fail Box **7.** Point Offline Count Box **8.** RTU Failure Timeout in Listen Mode Box

4. Configure the following parameters as required:

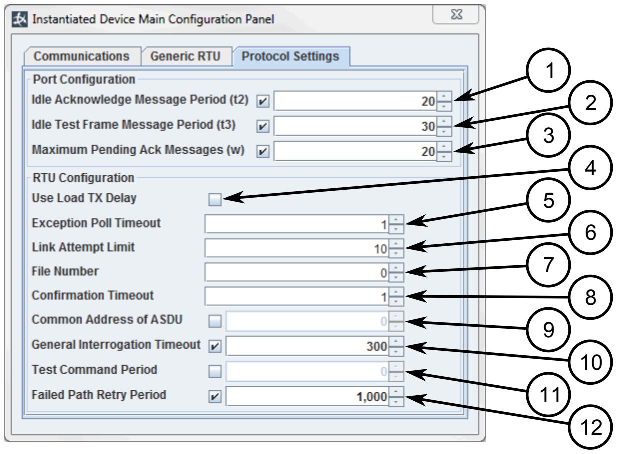
Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 100 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
Point Offline Count	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a scan – including retries – can consecutively fail to acquire the requested data before the unreported points are considered off-line (failed).
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.9.5

Configuring Protocol Settings

To configure protocol settings for IEC 60870-5-104 client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **Protocol Settings** tab.



Port Configuration

Idle Acknowledge Message Period (t2) ☑ 20

Idle Test Frame Message Period (t3) ☑ 30

Maximum Pending Ack Messages (w) ☑ 20

RTU Configuration

Use Load TX Delay □

Exception Poll Timeout 1

Link Attempt Limit 10

File Number 0

Confirmation Timeout 1

Common Address of ASDU □ 0

General Interrogation Timeout ☑ 300

Test Command Period □ 0

Failed Path Retry Period ☑ 1,000

Figure 120: Instantiated Device Main Configuration Panel Dialog Box – Protocol Settings

1. Idle Acknowledge Message Period (t2) Box **2.** Idle Test Frame Message Period (t3) Box **3.** Maximum Pending Ack Messages (w) Box **4.** Use Load TX Delay Check Box **5.** Exception Poll Timeout Box **6.** Link Attempt Limit Box **7.** File Number Box **8.** Confirmation Timeout Box **9.** Common Address of ASDU Box **10.** General Interrogation Timeout Box **11.** Test Command Period Box **12.** Failed Path Retry Period Box

5. Under **Port Configuration**, configure the following parameters as required:

Parameter	Description
Idle Acknowledge Message Period (t2)	**Synopsis:** 1 to 300 **Default:** 30 **Default State:** Enabled The number of seconds (s) after which any pending acknowledge message will be sent. When disabled (cleared), an acknowledgment will be sent immediately for each I format message received.
Idle Test Frame Message Period (t3)	**Synopsis:** 1 to 300 **Default:** 30 **Default State:** Enabled The number of seconds (s) after which to send test frames in case of a long idle state. When disabled (cleared), test frames are sent immediately after each data message.
Maximum Pending Ack Messages (w)	**Synopsis:** 1 to 100 **Default:** 20 **Default State:** Enabled The maximum number of received format messages for which an acknowledge message will be sent. When disabled (cleared), there is no limit on the number of acknowledge messages that can be sent.

6. Under **RTU Configuration**, configure the following parameters as required:

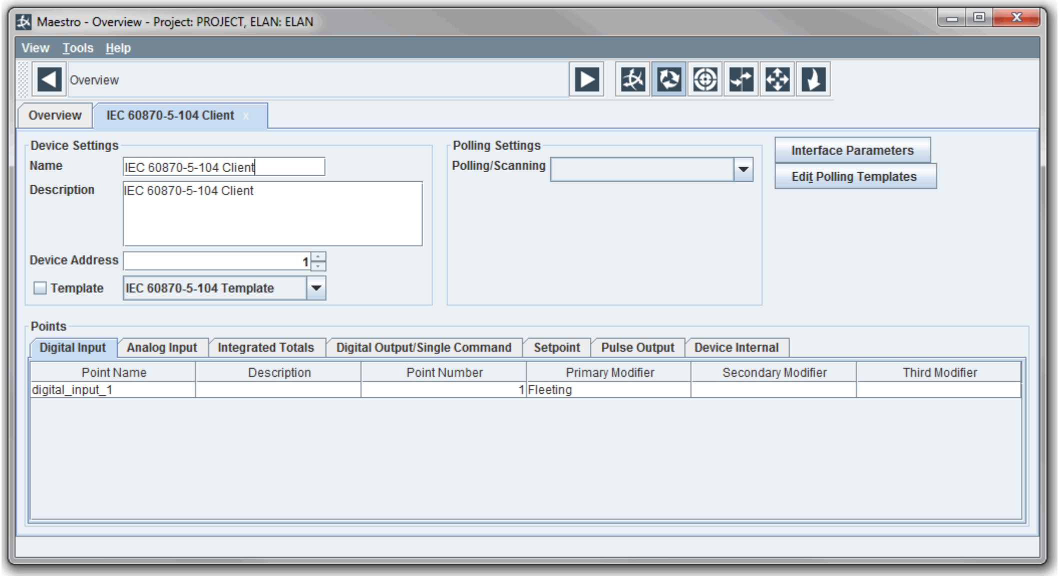
Parameter	Description
Use Load TX Delay	When enabled (selected), a load transmission delay command is sent to the RTU between the acquisition of transmission delay and time synchronization commands.
Exception Poll Timeout	**Synopsis:** 0 to 60 **Default:** 1 The time in seconds (s) to poll for Class 1 data if the Automatic Call Distributor (ACD) flag is set.
Link Attempt Limit	**Synopsis:** 0 to 100 **Default:** 10 The number of attempts the remote process is allowed to establish a link with an RTU that is in restart mode before the RTU is considered failed.
File Number	**Synopsis:** 0 to 65535 **Default:** 0 The file number to be used as the file identifier in file transfer messages.
Confirmation Timeout	**Synopsis:** 0 to 10 **Default:** 1 The time in seconds (s) permitted to check for confirmation of an application-level command message.
Common Address of ASDU	**Synopsis:** 0 to 65535 **Default Value:** 1 **Default State:** Disabled The common address of the Application Service Data Unit (ASDU) used for point grouping by an ASDU address. The check box must be checked for this parameter to take effect. When disabled (cleared), the point group from point configuration is used.
General Interrogation Timeout	**Synopsis:** 0 to 1000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait for an Activation Termination command to be received. If the command is not received before the time expires, a general interrogation (full update) is assumed to have completed. When disabled (cleared), the client process will wait infinitely for the command from the RTU.
Test Command Period	**Synopsis:** 0 to 90000 **Default Value:** 1000 **Default State:** Enabled The rate in seconds (s) at which to send a Test command to an RTU. When disabled (cleared), no Test command is sent.
Failed Path Retry Period	**Synopsis:** 0 to 90000 **Default Value:** 1000 **Default State:** Enabled The time in seconds (s) to wait before attempting to retry a failed higher-priority path to an RTU. When disabled (cleared), ELAN will not retry failed higher-priority paths.

Section 4.10.9.6

Configuring a Point

To configure/modify existing points for an IEC 60870-5-104 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 60870-5-104 client device and click **Properties**. The device's properties appear in a new tab.



Name: IEC 60870-5-104 Client

Description: IEC 60870-5-104 Client

Device Address: 1

☐ Template: IEC 60870-5-104 Template

Polling/Scanning:

Point Name	Description	Point Number	Primary Modifier	Secondary Modifier	Third Modifier
digital_input_1		1	Fleeting		

Figure 121: IEC 60870-5-104 Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant, Cyclic } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point.

Parameter	Description
	• Bit Pair – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • Two Sequential Points – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • Redundant – Use to identify a point change of state and a time-tagged change of state are reported separately. • Cyclic – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The secondary modifier. Options include: • Fleeting – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • Single Point – Use to identify a single status point. • Bit Pair – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • Two Sequential Points – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • Redundant – Use to identify a point change of state and a time-tagged change of state are reported separately.
Third Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair, Two Sequential Points, Redundant } The third modifier. Options include: • Fleeting – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • Single Point – Use to identify a single status point. • Bit Pair – Use to combine two sequential single status points that are reported individually by the RTU as single-point information objects. The two state bits combined represent one of four possible states for the point. Only the first of the two points is configured. • Two Sequential Points – Use to identify two sequential single status points, which are reported together as a double-point information object by the RTU. The two state bits combined represent one of four possible states for the point. • Redundant – Use to identify a point change of state and a time-tagged change of state are reported separately.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Force Update, BCD, DAC, 16 Bit, Cyclic } The primary modifier. Options include: • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Secondary Modifier	**Synopsis:** { Cyclic, Force Update, Time Tagged, Negated, Scaled, 32 Bit } The secondary modifier. Options include: • `BCD` – Use to identify an analog input that is interpreted as a BCD value. • `DAC` – Use to identify a point that stores a converted digital value. A maximum of 31 DAC points can be configured for each RTU. • `16 Bit` – Use to identify a 16-Bit normalized (-1 to 1-2-15) analog point. • `Cyclic` – Use if cyclic reporting of a point is to be monitored.
Units	A text field.

Integrated Totals

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. integrated_totals_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Cyclic, 32 Bit } The primary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Secondary Modifier	**Synopsis:** { Cyclic }

Parameter	Description
	The secondary modifier. Options include: • `Cyclic` – Use if cyclic reporting of a point is to be monitored. • `32 Bit` – Use to identify a 32-Bit 2's complement accumulator point.
Units	A text field.

Digital Output/Single Command

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_single_command_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Primary Modifier	**Synopsis:** { Momentary, Single Point, Latch, Preconfig } The primary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Latch` – Use for controls that latch into the *on* or *off* state. This indicates the control message sent to the RTU should include the latching option. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).
Secondary Modifier	**Synopsis:** { Momentary, Single Point, Preconfig } The secondary modifier. Options include: • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Single Point` – Use when a single relay is used to cause the Trip or Close of an external device. • `Preconfig` – Use to indicate the qualifier in the control message sent to the RTU should be set to *no additional information* (e.g. the time duration is pre-configured at the RTU).

Setpoint

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. setpoint_1).
Description	A description of the point.

Parameter	Description
Point Number	The number assigned to the point.
Units	A text field.

›› Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Section 4.10.10

Managing IEC 61850 Client Devices

> **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. Configured IED Description (CID) files should be protected from malicious users or malware. Make sure CID files are stored in a secure location and only authorized personnel are granted access.*

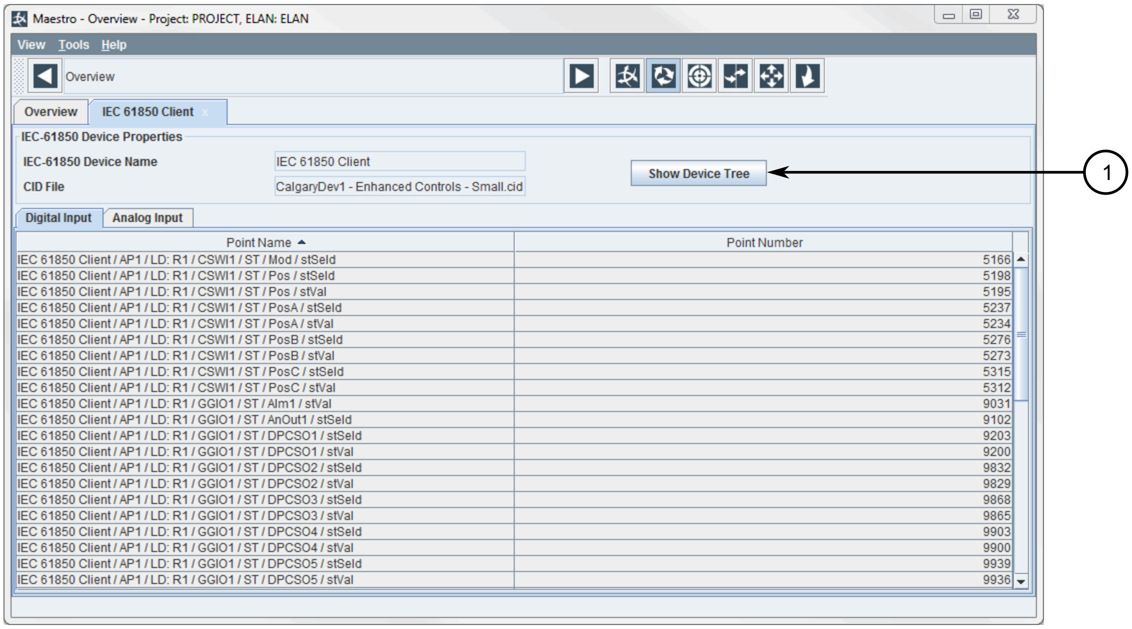
CONTENTS

Section 4.10.10.1

Viewing the Device Tree

To view the devices connected to the IEC 61850 client device in a tree format, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the IEC 61850 client device and click **Properties**. The device's properties appear in a new tab.



IEC-61850 Device Properties

IEC-61850 Device Name: IEC 61850 Client

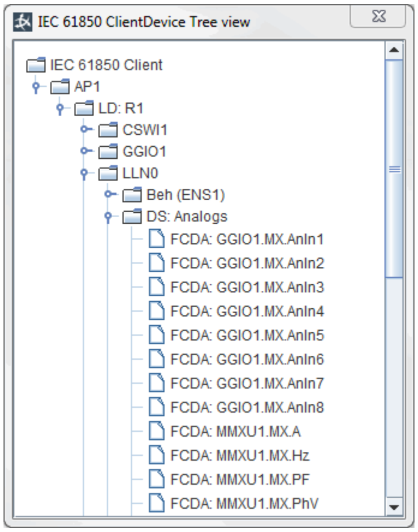
CID File: CalgaryDev1 - Enhanced Controls - Small.cid

Point Name ▲	Point Number
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Mod / stSeld	5166
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Pos / stSeld	5198
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Pos / stVal	5195
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosA / stSeld	5237
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosA / stVal	5234
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosB / stSeld	5276
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosB / stVal	5273
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosC / stSeld	5315
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosC / stVal	5312
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Alm1 / stVal	9031
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / AnOut1 / stSeld	9102
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO1 / stSeld	9203
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO1 / stVal	9200
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO2 / stSeld	9832
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO2 / stVal	9829
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO3 / stSeld	9868
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO3 / stVal	9865
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO4 / stSeld	9903
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO4 / stVal	9900
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO5 / stSeld	9939
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO5 / stVal	9936

Figure 122: IEC 61850 Client Properties

1. Show Device Tree Button

3. Click **Show Device Tree**. The **Device Tree View** dialog box appears.



- IEC 61850 Client
  - AP1
    - LD: R1
      - CSWI1
      - GGIO1
      - LLN0
        - Beh (ENS1)
        - DS: Analogs
          - FCDA: GGIO1.MX.AnIn1
          - FCDA: GGIO1.MX.AnIn2
          - FCDA: GGIO1.MX.AnIn3
          - FCDA: GGIO1.MX.AnIn4
          - FCDA: GGIO1.MX.AnIn5
          - FCDA: GGIO1.MX.AnIn6
          - FCDA: GGIO1.MX.AnIn7
          - FCDA: GGIO1.MX.AnIn8
          - FCDA: MMXU1.MX.A
          - FCDA: MMXU1.MX.Hz
          - FCDA: MMXU1.MX.PF
          - FCDA: MMXU1.MX.PhV

Figure 123: Device Tree View Dialog Box

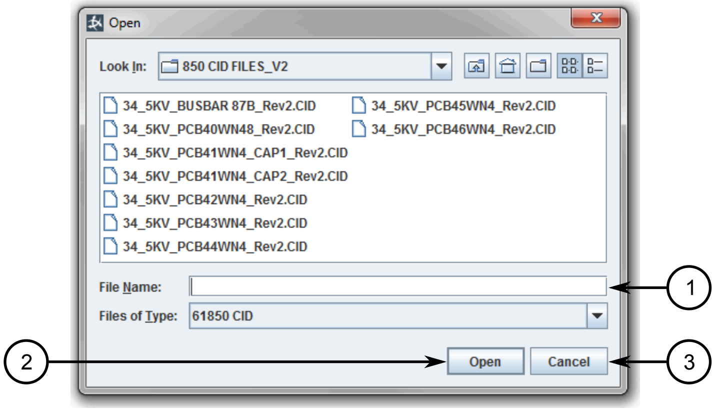
Section 4.10.10.2

Adding an IEC 61850 Client from a CID File

To add an IEC 61850 client from a Configured IED Description (CID) file, do the following:

> **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. Configured IED Description (CID) files should be reviewed before use to identify potentially unauthorized modifications made by a malicious user or malware.*

1. Navigate to the **Overview** screen.
2. Right-click the **RUGGEDCOM ELAN Client Devices** to open the shortcut menu and click **New 61850 device from CID**. The **Open** dialog box appears.



Look In: 850 CID FILES_V2

34_5KV_BUSBAR 87B_Rev2.CID
34_5KV_PCB40WN48_Rev2.CID
34_5KV_PCB41WN4_CAP1_Rev2.CID
34_5KV_PCB41WN4_CAP2_Rev2.CID
34_5KV_PCB42WN4_Rev2.CID
34_5KV_PCB43WN4_Rev2.CID
34_5KV_PCB44WN4_Rev2.CID
34_5KV_PCB45WN4_Rev2.CID
34_5KV_PCB46WN4_Rev2.CID

File Name:
Files of Type: 61850 CID

Figure 124: Open Dialog Box

1. File Name Box **2.** Open Button **3.** Cancel Button

3. Navigate to and select the desired CID file.
4. Click **Open** to import the CID file, or click **Cancel** to abort.

Section 4.10.10.3

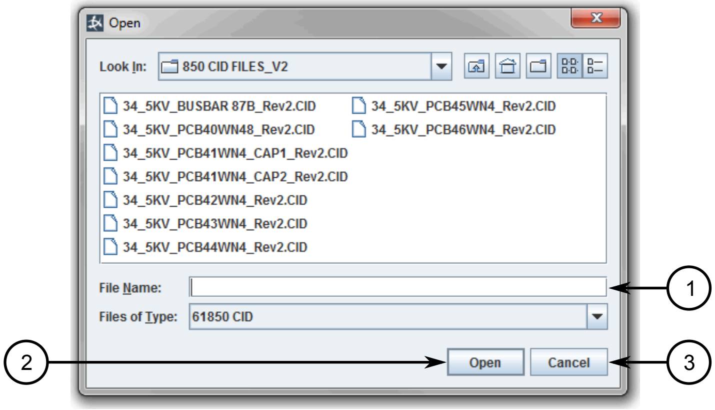
Reloading an IEC 61850 Client Configuration

To reload the configuration for an existing IEC 61850 client device from the CID file used to create it, do the following:

> **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. Configured IED Description (CID) files should be reviewed before use to identify potentially unauthorized modifications made by a malicious user or malware.*

> **NOTE**
> *Only the CID file used to create the initial IEC 61850 client device can be reload. Reloading any other CID file generate an error. The original CID file can, however, be modified to update the device's configuration.*

1. Navigate to the **Overview** screen.
2. Under **RUGGEDCOM ELAN client Devices**, expand the **IEC 61850** group.
3. Right-click the IEC 61850 client to open the shortcut menu and click **Reload IED configuration from CID file**. The **Open** dialog box appears.



Look In: 850 CID FILES_V2

34_5KV_BUSBAR 87B_Rev2.CID
34_5KV_PCB40WN48_Rev2.CID
34_5KV_PCB41WN4_CAP1_Rev2.CID
34_5KV_PCB41WN4_CAP2_Rev2.CID
34_5KV_PCB42WN4_Rev2.CID
34_5KV_PCB43WN4_Rev2.CID
34_5KV_PCB44WN4_Rev2.CID
34_5KV_PCB45WN4_Rev2.CID
34_5KV_PCB46WN4_Rev2.CID

File Name:

Files of Type: 61850 CID

Figure 125: Open Dialog Box

1. File Name Box **2.** Open Button **3.** Cancel Button

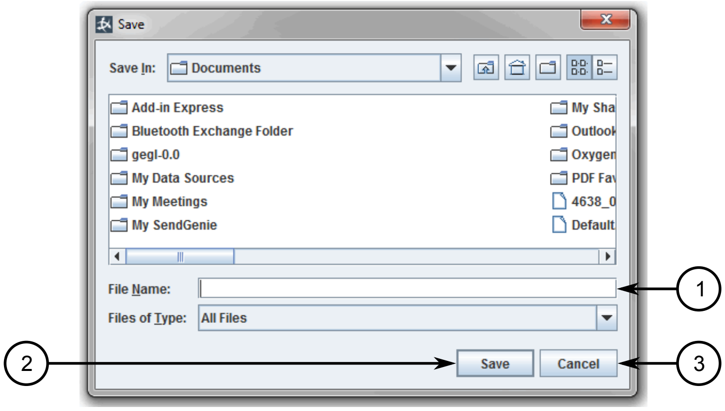
4. Navigate to and select the desired CID file.
5. Click **Open** to import the CID file, or click **Cancel** to abort.

Section 4.10.10.4

Saving an IEC 61850 Client to an SCL File

To save an IEC 61850 client to a Substation Configuration Language (SCL) file, do the following:

1. Navigate to the **Overview** screen.
2. Under **RUGGEDCOM ELAN client Devices**, expand the **IEC 61850** group.
3. Right-click the IEC 61850 client to open the shortcut menu and click **Save IED to SCL-file**. The **Save** dialog box appears.



Save In: Documents

Files of Type: All Files

Figure 126: Save Dialog Box

1. File Name Box **2.** Save Button **3.** Cancel Button

4. Navigate to and select the drive or folder where the SCL file will be saved.
5. Under **File Name**, type a name for the file.
6. Click **Save** to save the file, or click **Cancel** to abort.

Section 4.10.10.5

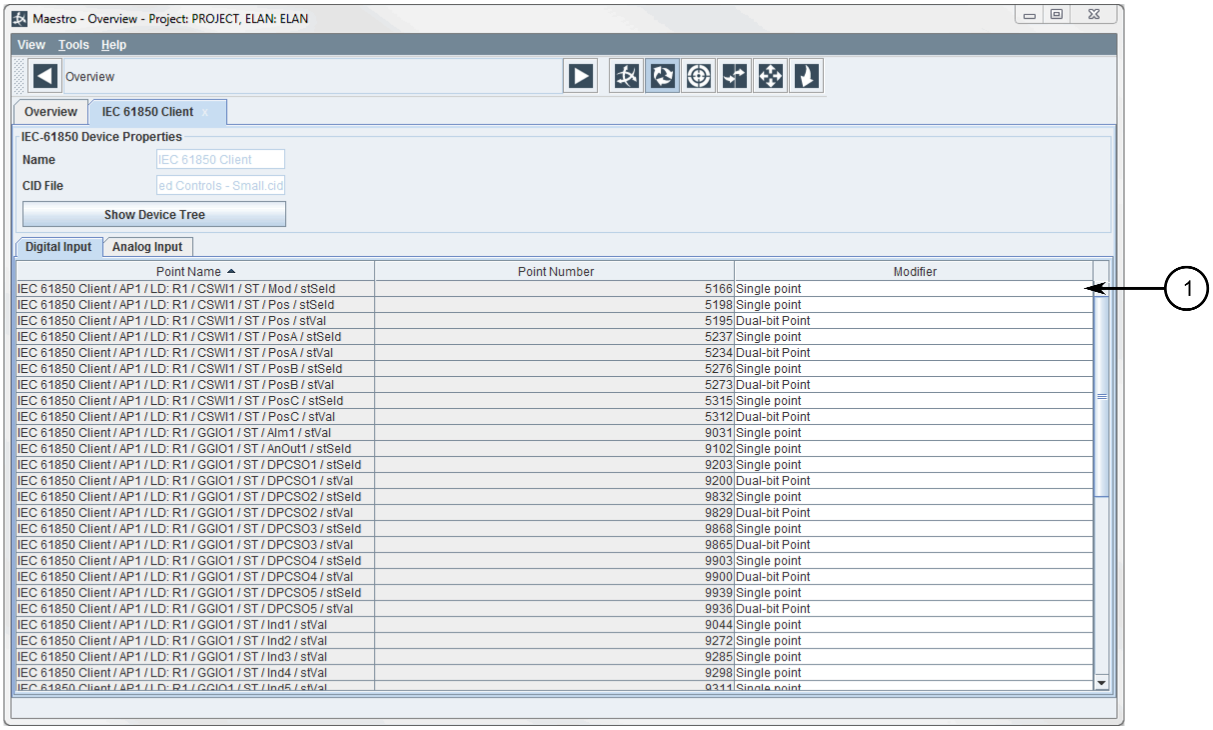
Configuring a Point

To configure/modify existing points for an IEC 61850 client device, do the following:

Digital Input Points

IMPORTANT!
Only dual-bit (dbpos) digital input points that are not mapped can be modified.

1. Navigate to the **Overview** screen.
2. Right-click the IEC 61850 client device and click **Properties**. The device's properties appear in a new tab.



Name: IEC 61850 Client

CID File: ed Controls - Small.cid

Point Name ▲	Point Number	Modifier
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Mod / stSeld	5166	Single point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Pos / stSeld	5198	Single point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / Pos / stVal	5195	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosA / stSeld	5237	Single point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosA / stVal	5234	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosB / stSeld	5276	Single point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosB / stVal	5273	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosC / stSeld	5315	Single point
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / ST / PosC / stVal	5312	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Alm1 / stVal	9031	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / AnOut1 / stSeld	9102	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO1 / stSeld	9203	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO1 / stVal	9200	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO2 / stSeld	9832	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO2 / stVal	9829	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO3 / stSeld	9868	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO3 / stVal	9865	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO4 / stSeld	9903	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO4 / stVal	9900	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO5 / stSeld	9939	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / DPCSO5 / stVal	9936	Dual-bit Point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Ind1 / stVal	9044	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Ind2 / stVal	9272	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Ind3 / stVal	9285	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Ind4 / stVal	9298	Single point
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / ST / Ind5 / stVal	9311	Single point

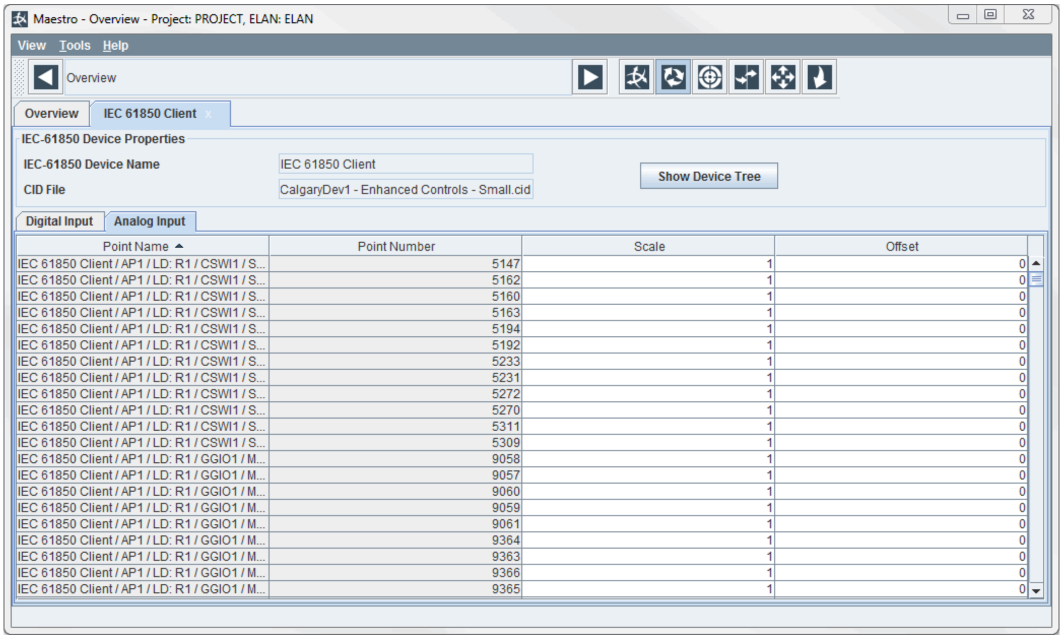
Figure 127: IEC 61850 Client Properties – Digital Input

1. Modifier List

3. Select the **Digital Input** tab and configure the **Modifier** list for the desired digital inputs. Options include:
   - `Single Point` – A single status point (as reported by the IED) that can be mapped to a single status point on the RUGGEDCOM ELAN server.
   - `Dual-bit Point` – Two sequential status points that are reported together as one point. The two state bits combined represent one of four possible states for the point. The single status point can be mapped to a single status point on the RUGGEDCOM ELAN server.
   - `Dual-bit Point Split` – Two sequential status points that are reported together as two points. Each status point represents bit 0 and bit 1 respectively, and can be mapped independently to a single point on the RUGGEDCOM ELAN server.

›› Analog Input Points

1. Navigate to the **Overview** screen.
2. Right-click the IEC 61850 client device and click **Properties**. The device's properties appear in a new tab.



IEC-61850 Device Properties

IEC-61850 Device Name: IEC 61850 Client

CID File: CalgaryDev1 - Enhanced Controls - Small.cid

Point Name ▲	Point Number	Scale	Offset
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5147	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5162	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5160	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5163	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5194	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5192	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5233	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5231	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5272	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5270	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5311	1	0
IEC 61850 Client / AP1 / LD: R1 / CSWI1 / S...	5309	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9058	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9057	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9060	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9059	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9061	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9364	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9363	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9366	1	0
IEC 61850 Client / AP1 / LD: R1 / GGIO1 / M...	9365	1	0

Figure 128: IEC 61850 Client Properties – Analog Input

3. Select the **Analog Input** tab and configure the following parameters as required:

Parameter	Description
Scale	**Default:** 1 Any positive or negative floating point value. Must not equal zero.
Offset	**Default:** 0 Any positive or negative floating point value.

Section 4.10.11

Managing ABB Client Devices

This section describes how to configure and manage ABB client devices.

CONTENTS

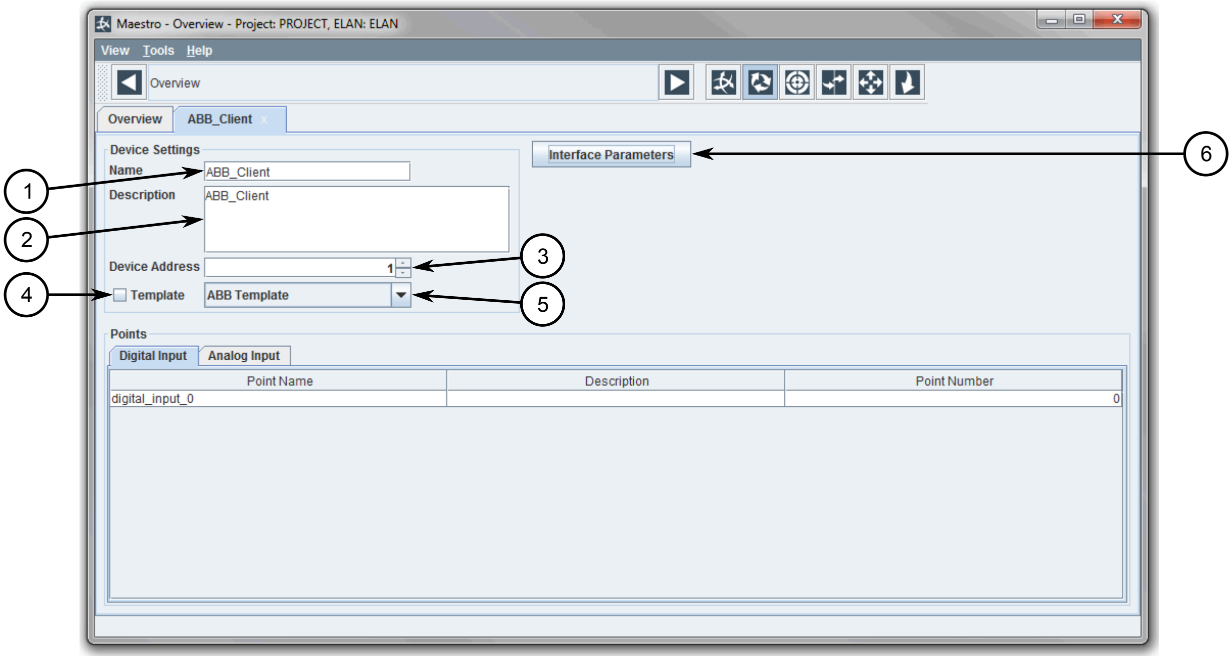
- Section 4.10.11.4, “Configuring a Point”

Section 4.10.11.1

Configuring ABB Client

To configure an ABB client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the ABB client device and click **Properties**. The device's properties appear in a new tab.



Name: ABB_Client

Description: ABB_Client

Device Address: 1

□ Template: ABB Template

Point Name	Description	Point Number
digital_input_0		0

Figure 129: ABB Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Interface Parameters Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 255 The protocol address for the client device.

4. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
5. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .

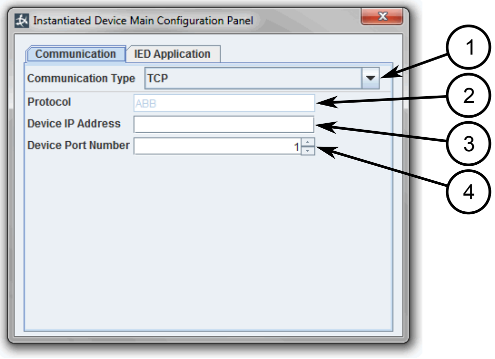
6. [Optional] Configure the communication settings. For more information, refer to Section 4.10.11.2, "Configuring Communication Settings"
7. [Optional] Configure the IED application settings. For more information, refer to Section 4.10.11.3, "Configuring IED Application Settings"

Section 4.10.11.2

Configuring Communication Settings

To configure communication settings for an ABB client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the ABB client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communication** tab is displayed.



Communication Type: TCP
Protocol: ABB
Device IP Address:
Device Port Number: 1

Figure 130: Instantiated Device Main Configuration Panel Dialog Box – Communication (Example)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box

4. Configure the following parameters as required:

Parameter	Description
Communication Type	**Synopsis:** TCP **Default:** TCP The interface used to communicate with the terminal server.
Device IP Address	The IP address of the terminal server connected to the IED.
Device Port Number	**Synopsis:** 1 to 65535 The port for the terminal server connected to the IED.

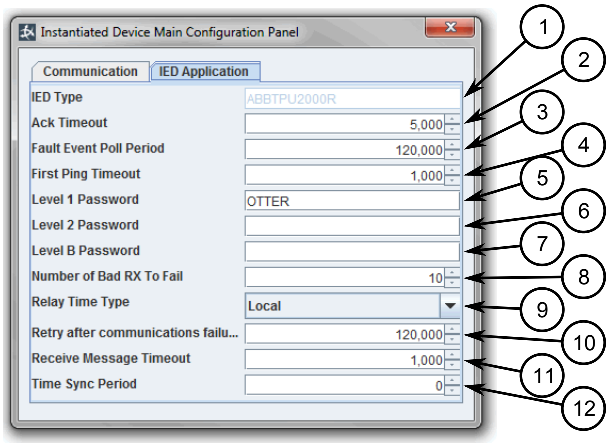
Section 4.10.11.3

Configuring IED Application Settings

To configure IED application settings for an ABB client device, do the following:

1. Navigate to the **Overview** screen.

2. Right-click the ABB client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **IED Application** tab.



Instantiated Device Main Configuration Panel

IED Type	ABBTPU2000R
Ack Timeout	5,000
Fault Event Poll Period	120,000
First Ping Timeout	1,000
Level 1 Password	OTTER
Level 2 Password	
Level B Password	
Number of Bad RX To Fail	10
Relay Time Type	Local
Retry after communications failu...	120,000
Receive Message Timeout	1,000
Time Sync Period	0

Figure 131: Instantiated Device Main Configuration Panel Dialog Box – IED Application

1. IED Type Box **2.** Ack Timeout Box **3.** Fault Event Poll Period Box **4.** First Ping Timeout Box **5.** Level 1 Password Box **6.** Level 2 Password Box **7.** Level B Password Box **8.** Number of Bad RX to Fail Box **9.** Relay Time Type List **10.** Retry After Communications Failure Box **11.** Receive Message Timeout Box **12.** Time Sync Period Box

5. Configure the following parameters as required:

Parameter	Description
Ack Timeout	**Synopsis:** 1 to 100000 **Default:** 5000 The time in milliseconds (ms) to wait for acknowledgment from a protocol drive.
Fault Event Poll Period	**Synopsis:** 6000 to 86400000 **Default:** 120000 The time in milliseconds (ms) between each fault-event poll.
First Ping Timeout	**Synopsis:** 0 to 90000 **Default:** 1000 The time in milliseconds (ms) to wait for an SEL Relay response to carriage-return.
Level 1 Password	**Default:** OTTER The password for level 1 access.
Level 2 Password	The password for level 2 access.
Level B Password	The password for level B (Breaker-level) access.
Number of Bad RX To Fail	**Synopsis:** 0 to 32 **Default:** 10 The number of allowed *no response* or *bad response* messages before the IED is considered failed.
Relay Time Type	**Synopsis:** UTC, UTC-Fallback, Local-Standard, Local **Default:** Local

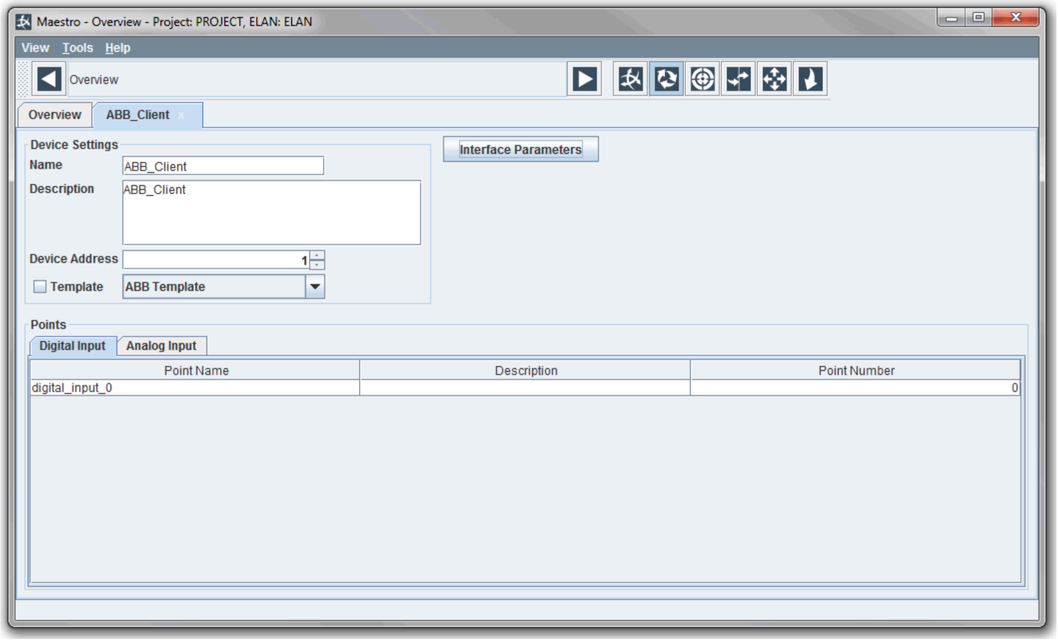
Parameter	Description
	The time standard to which a relay's time is set. When set to `Local`, the Relay is assumed to be able to handle STD/DST transitions and configured to transition to/from DST on the same dates and times as the host.
Retry After Communications Failure	**Synopsis:** 0 to 1000000 **Default:** 120000 The time in milliseconds (ms) to wait after a communication failure before retrying.
Receive Message Timeout	**Synopsis:** 0 to 86400 **Default:** 1000 The time in milliseconds (ms) between each reading of the serial port.
Time Sync Period	**Synopsis:** 0 to 1440 **Default:** 0 The time in minutes (m) between time synchronization attempts. Set to `0` to disable.

Section 4.10.11.4

Configuring a Point

To configure/modify existing points for an ABB client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the ABB client device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: ABB_Client

Description: ABB_Client

Device Address: 1

☐ Template: ABB Template

Points

Point Name	Description	Point Number
digital_input_0		0

Figure 132: ABB Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, "Controlling Template Links" .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Section 4.10.12

Managing Courier Client Devices

This section describes how to configure and manage Courier client devices via Maestro.

CONTENTS

- Section 4.10.12.4, “Configuring a Point”

Section 4.10.12.1

Configuring a Courier Client

To configure a Courier client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Courier client device and click **Properties**. The device's properties appear in a new tab.

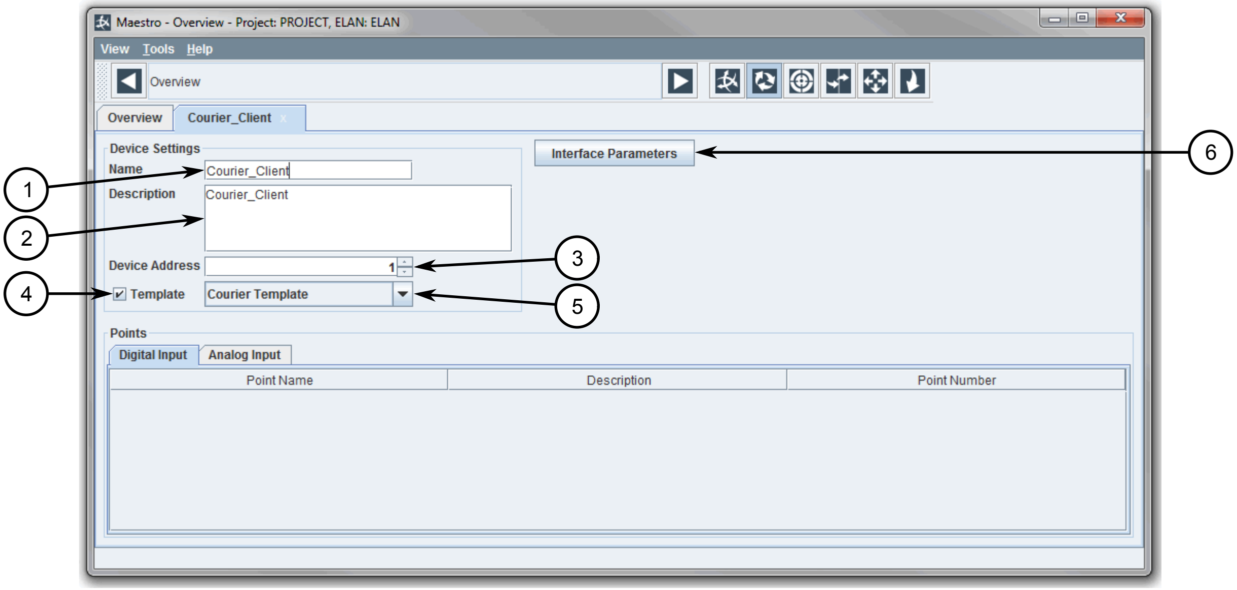


Figure 133: Courier Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Interface Parameters Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 255 The protocol address for the client device.

4. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
5. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
6. [Optional] Configure the communication settings. For more information, refer to Section 4.10.12.2, “Configuring Communication Settings”

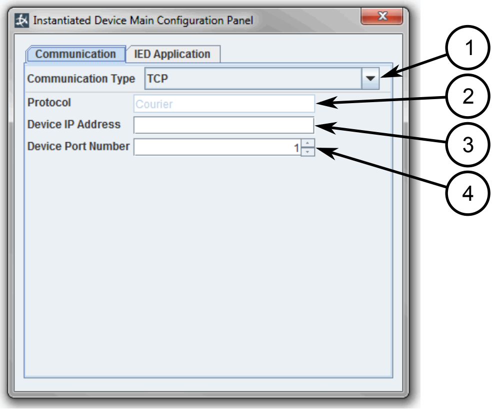
7. [Optional] Configure the IED application settings. For more information, refer to Section 4.10.12.3, “Configuring IED Application Settings”

Section 4.10.12.2

Configuring Communication Settings

To configure communication settings for a Courier client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Courier client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communication** tab is displayed.



Communication Type TCP
Protocol Courier
Device IP Address
Device Port Number 1

Figure 134: Instantiated Device Main Configuration Panel Dialog Box – Communication (Example)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box

4. Configure the following parameters as required:

Parameter	Description
Communication Type	**Synopsis:** TCP **Default:** TCP The interface used to communicate with the terminal server.
Device IP Address	The IP address of the terminal server connected to the IED.
Device Port Number	**Synopsis:** 1 to 65535 The port for the terminal server connected to the IED.

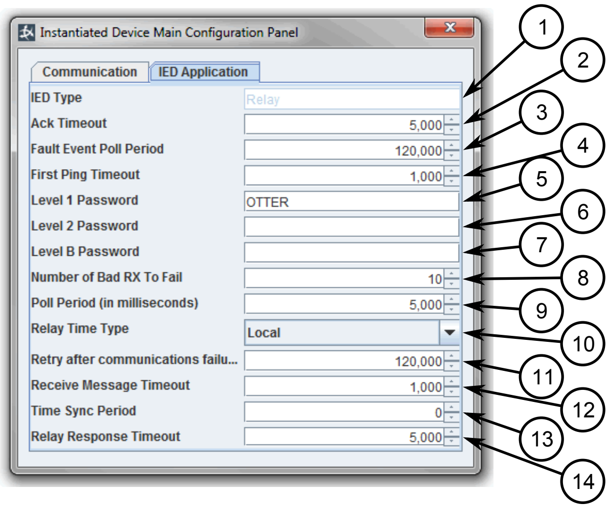
Section 4.10.12.3

Configuring IED Application Settings

To configure IED application settings for a Courier client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Courier client device and click **Properties**. The device's properties appear in a new tab.

3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **IED Application** tab.



IED Type	Relay
Ack Timeout	5,000
Fault Event Poll Period	120,000
First Ping Timeout	1,000
Level 1 Password	OTTER
Level 2 Password	
Level B Password	
Number of Bad RX To Fail	10
Poll Period (in milliseconds)	5,000
Relay Time Type	Local
Retry after communications failu...	120,000
Receive Message Timeout	1,000
Time Sync Period	0
Relay Response Timeout	5,000

Figure 135: Instantiated Device Main Configuration Panel Dialog Box – IED Application

1. IED Type Box **2.** Ack Timeout Box **3.** Fault Event Poll Period Box **4.** First Ping Timeout Box **5.** Level 1 Password Box **6.** Level 2 Password Box **7.** Level B Password Box **8.** Number of Bad RX To Fail Box **9.** Poll Period (in millseconds) Box **10.** Relay Time Type List **11.** Retry After Communications Failure Box **12.** Receive Message Timeout Box **13.** Time Sync Period Box **14.** Relay Response Timeout Box

5. Configure the following parameters as required:

Parameter	Description
Ack Timeout	**Synopsis:** 1 to 100000 **Default:** 5000 The time in milliseconds (ms) to wait for acknowledgment from a protocol drive.
Fault Event Poll Period	**Synopsis:** 6000 to 86400000 **Default:** 120000 The time in milliseconds (ms) between each fault-event poll.
First Ping Timeout	**Synopsis:** 0 to 90000 **Default:** 1000 The time in milliseconds (ms) to wait for an SEL Relay response to carriage-return.
Level 1 Password	**Default:** OTTER The password for level 1 access.
Level 2 Password	The password for level 2 access.
Level B Password	The password for level B (Breaker-level) access.
Number of Bad RX To Fail	**Synopsis:** 0 to 32 **Default:** 10 The number of allowed *no response* or *bad response* messages before the IED is considered failed.
Poll Period (in milliseconds)	**Synopsis:** 0 to 86400000

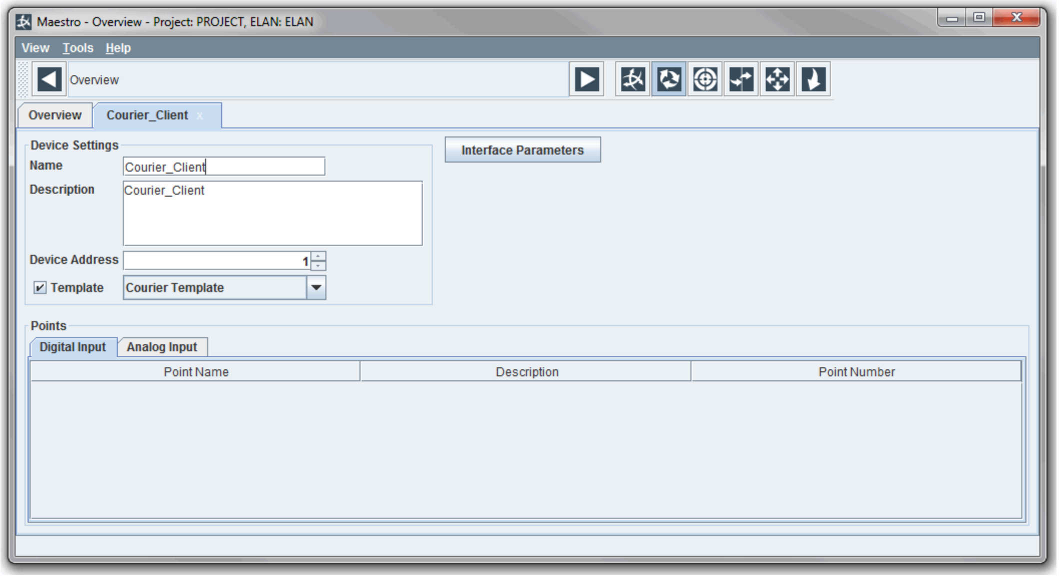
Parameter	Description
	Default: 5000 The time in milliseconds (ms) between each poll.
Relay Time Type	**Synopsis:** UTC, UTC-Fallback, Local-Standard, Local **Default:** Local The time standard to which a relay's time is set. When set to `Local`, the Relay is assumed to be able to handle STD/DST transitions and configured to transition to/from DST on the same dates and times as the host.
Retry After Communications Failure	**Synopsis:** 0 to 1000000 **Default:** 120000 The time in milliseconds (ms) to wait after a communication failure before retrying.
Receive Message Timeout	**Synopsis:** 0 to 86400 **Default:** 1000 The time in milliseconds (ms) between each reading of the serial port.
Time Sync Period	**Synopsis:** 0 to 1440 **Default:** 0 The time in minutes (m) between time synchronization attempts. Set to `0` to disable.
Relay Response Timeout	**Synopsis:** 0 to 86400 **Default:** 5000 The time in milliseconds (ms) to wait for a response from a relay before considering it failed.

Section 4.10.12.4

Configuring a Point

To configure/modify existing points for a Courier client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Courier client device and click **Properties**. The device's properties appear in a new tab.



Maestro - Overview - Project: PROJECT, ELAN: ELAN

Device Settings

Name: Courier_Client

Description: Courier_Client

Device Address: 1

☑ Template: Courier Template

Points

Point Name	Description	Point Number

Figure 136: Courier Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.

Parameter	Description
Units	A text field.

Section 4.10.13

Managing SEL Client Devices

This section describes how to configure and manage SEL client devices.

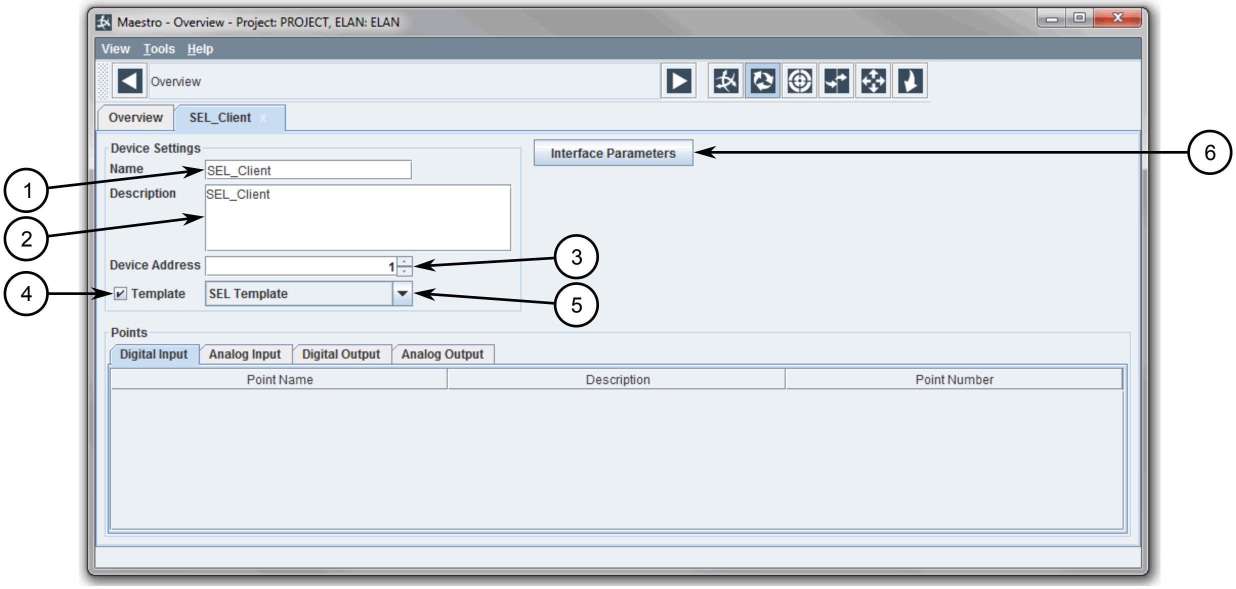
CONTENTS

Section 4.10.13.1

Configuring an SEL Client

To configure an SEL client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL client device and click **Properties**. The device's properties appear in a new tab.



Name: SEL_Client
Description: SEL_Client
Device Address: 1
☑ Template: SEL Template

Figure 137: SEL Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Interface Parameters Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 65535 The protocol address for the client device.

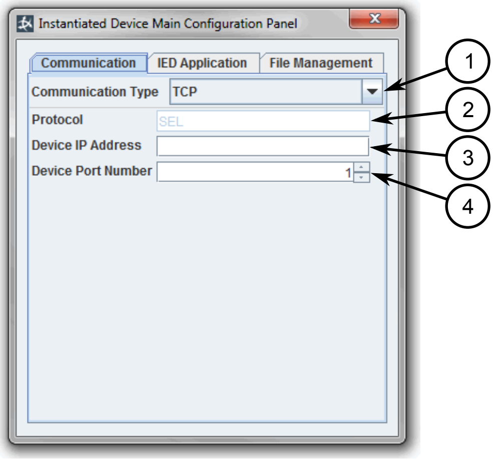
4. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
5. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
6. [Optional] Configure the communication settings. For more information, refer to Section 4.10.13.2, “Configuring Communication Settings”
7. [Optional] Configure the IED application settings. For more information, refer to Section 4.10.13.3, “Configuring IED Application Settings”
8. [Optional] Configure the file management settings. For more information, refer to Section 4.10.13.4, “Configuring File Management Settings”

Section 4.10.13.2

Configuring Communication Settings

To configure communication settings for an SEL client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Communication** tab is displayed.



Instantiated Device Main Configuration Panel

Communication | IED Application | File Management

Communication Type: TCP
Protocol: SEL
Device IP Address:
Device Port Number: 1

Figure 138: Instantiated Device Main Configuration Panel Dialog Box – Communication (Example)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box

4. Configure the following parameters as required:

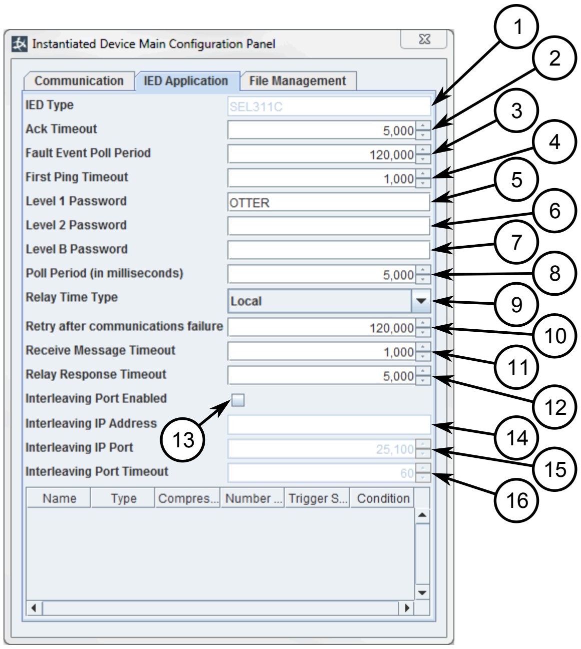
Parameter	Description
Communication Type	**Synopsis:** TCP **Default:** TCP The interface used to communicate with the terminal server.
Device IP Address	The IP address of the terminal server connected to the IED.
Device Port Number	**Synopsis:** 1 to 65535 The port for the terminal server connected to the IED.

Section 4.10.13.3

Configuring IED Application Settings

To configure IED application settings for an SEL client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **IED Application** tab.



IED Type: SEL311C
Ack Timeout: 5,000
Fault Event Poll Period: 120,000
First Ping Timeout: 1,000
Level 1 Password: OTTER
Level 2 Password:
Level B Password:
Poll Period (in milliseconds): 5,000
Relay Time Type: Local
Retry after communications failure: 120,000
Receive Message Timeout: 1,000
Relay Response Timeout: 5,000
Interleaving Port Enabled: □
Interleaving IP Address:
Interleaving IP Port: 25,100
Interleaving Port Timeout: 60

Figure 139: Instantiated Device Main Configuration Panel Dialog Box – IED Application

1. IED Type Box **2.** Ack Timeout Box **3.** Fault Event Poll Period Box **4.** First Ping Timeout Box **5.** Level 1 Password Box **6.** Level 2 Password Box **7.** Level B Password Box **8.** Poll Period (in milliseconds) Box **9.** Relay Time Type List **10.** Retry After Communications Failure Box **11.** Receive Message Timeout Box **12.** Relay Response Timeout Box **13.** Interleaving Port Enabled Check Box **14.** Interleaving IP Address Box **15.** Interleaving IP Port Box **16.** Interleaving Port Timeout Box

5. Configure the following parameters as required:

> **NOTE**
>
> *If passwords are configured for the IED application, RUGGEDCOM ELAN will attempt to log in to the SEL IED using the highest level password available. The password hierarchy is as follows:*
>
> - *Level 2*
> - *Level B*
> - *Level 1*

Parameter	Description
Ack Timeout	**Synopsis:** 1 to 100000 **Default:** 5000 The time in milliseconds (ms) to wait for acknowledgment from a protocol drive.
Fault Event Poll Period	**Synopsis:** 6000 to 86400000 **Default:** 120000 The time in milliseconds (ms) between each fault-event poll.
First Ping Timeout	**Synopsis:** 0 to 90000 **Default:** 1000 The time in milliseconds (ms) to wait for an SEL Relay response to carriage-return.

Parameter	Description
Level 1 Password	**Default:** OTTER The password for level 1 access.
Level 2 Password	The password for level 2 access.
Level B Password	The password for level B (Breaker-level) access.
Poll Period (in milliseconds)	**Synopsis:** 0 to 86400000 **Default:** 5000 The time in milliseconds (ms) between each poll.
Relay Time Type	**Synopsis:** UTC, UTC-Fallback, Local-Standard, Local **Default:** Local The time standard to which a relay's time is set. When set to `Local`, the Relay is assumed to be able to handle STD/DST transitions and configured to transition to/from DST on the same dates and times as the host.
Retry After Communications Failure	**Synopsis:** 0 to 1000000 **Default:** 120000 The time in milliseconds (ms) to wait after a communication failure before retrying.
Receive Message Timeout	**Synopsis:** 0 to 86400 **Default:** 1000 The time in milliseconds (ms) between each reading of the serial port.
Relay Response Timeout	**Synopsis:** 0 to 86400 **Default:** 5000 The time in milliseconds (ms) to wait for a response from a relay before considering it failed.

6. If communication between third-party applications and SEL client devices is required, select **Interleaving Port Enabled** and configure the following parameters:

> ⚠ **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. Only enable interleaving when communications between third-party applications and SEL client devices is within the security perimeter.*

Parameter	Description
Interleaving IP Address	**Default:** 0.0.0.0 The IP address of the TCP server on which the RUGGEDCOM ELAN server will listen for connections from third-party applications.
Interleaving IP Port	**Default:** 25100 The IP port of the TCP server on which the RUGGEDCOM ELAN server will listen for connections from third-party applications.
Interleaving Port Timeout	**Default:** 10 seconds The time in seconds (s) the third-party application must be idle before the RUGGEDCOM ELAN server closes the connection.

Section 4.10.13.4
Configuring File Management Settings

To configure file management settings for SEL client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **File Management** tab.

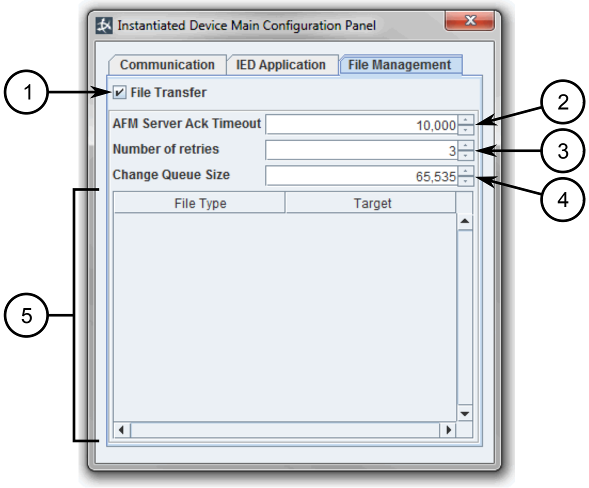


Figure 140: Instantiated Device Main Configuration Panel Dialog Box – File Management

1. File Transfer Check Box **2.** AFM Server Ack Timeout Box **3.** Number of Retries Box **4.** Change Queue Size Box **5.** Targets

5. Make sure the **File Transfer** check box is checked (enabled).
6. Configure the following parameters as required:

Parameter	Description
AFM Server Ack Timeout	**Synopsis:** 0 to 1000000 **Default:** 10000 The time in milliseconds (ms) to wait for an ACK message from the AFM server.
Number of Retries	**Synopsis:** 0 to 100 **Default:** 3 The maximum number of attempts to communicate with the AFM server before it is considered failed.
Change Queue Size	**Synopsis:** 0 to 65535 **Default:** 65535 The number of points in the change queue to be reported to the AFM server.

7. Configure one or more target destinations where reports can be sent. For more information, refer to Section 4.10.13.5, “Adding/Deleting AFM Targets” .

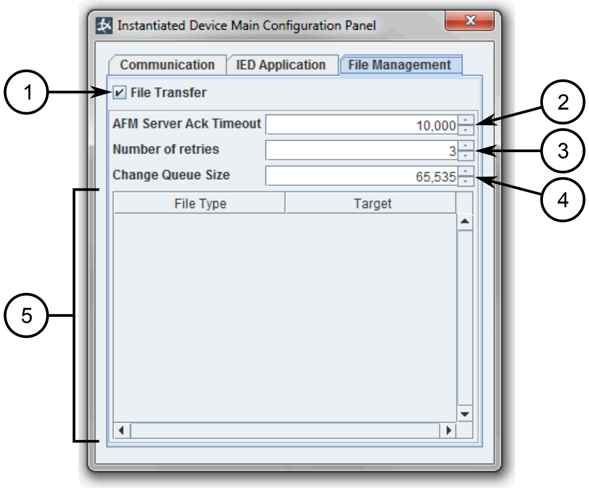
Section 4.10.13.5

Adding/Deleting AFM Targets

To add/delete SEL file targets, do the following:

›› Adding an SEL File Target

1. Make sure the Automatic File Manager (AFM) is configured for the RUGGEDCOM ELAN server. For more information, refer to Section 4.6.8, “Managing the Automatic File Manager (AFM)” .
2. Navigate to the **Overview** screen.
3. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
4. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
5. Click the **File Management** tab.



☑ File Transfer

AFM Server Ack Timeout 10,000

Number of retries 3

Change Queue Size 65,535

Figure 141: Instantiated Device Main Configuration Panel Dialog Box – File Management

1. File Transfer Check Box **2.** AFM Server Ack Timeout Box **3.** Number of Retries Box **4.** Change Queue Size Box **5.** Targets

6. Right-click anywhere in the targets area and click **New**. A new Event Report is added to the targets table.
7. Double-click the associated cell in the **Target** column and select a file management server.

›› Deleting an SEL File Target

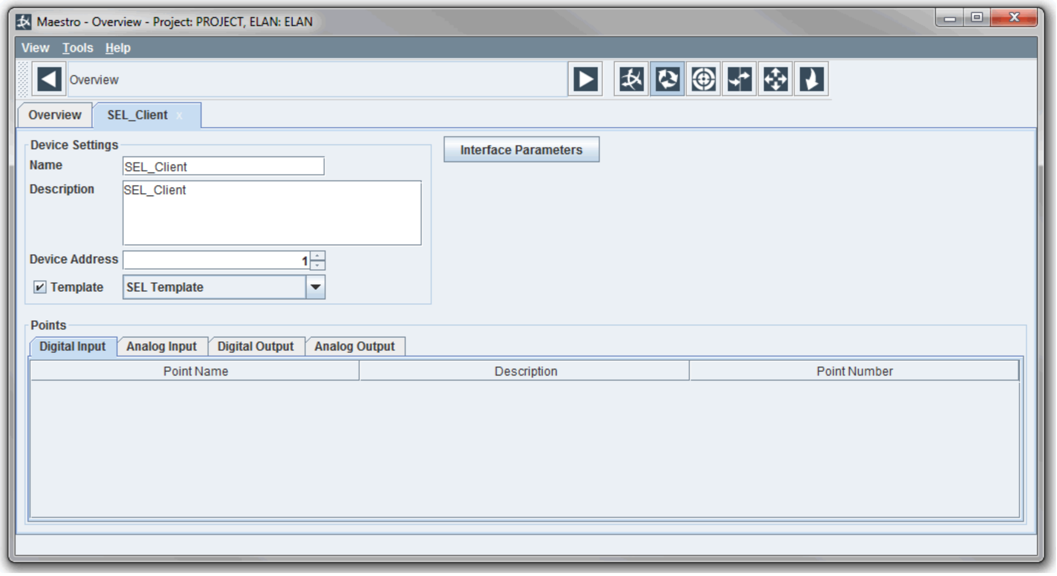
1. Right-click an Event Report row and click **Delete**. A confirmation dialog box appears.
2. Click **Yes** to delete the target, or click **No** to abort.

Section 4.10.13.6

Configuring a Point

To configure/modify existing points for a SEL client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the SEL client device and click **Properties**. The device's properties appear in a new tab.



Device Settings

Name: SEL_Client

Description: SEL_Client

Device Address: 1

☑ Template: SEL Template

Point Name	Description	Point Number

Figure 142: SEL Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

›› Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

›› Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.

Parameter	Description
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Scale	**Default:** 1 Any positive or negative floating point value.
Offset	**Default:** 0 Any positive or negative floating point value.
Units	A text field.

Section 4.10.14

Managing Modbus Client Devices

This section describes how to configure and manage Modbus client devices via Maestro.

CONTENTS

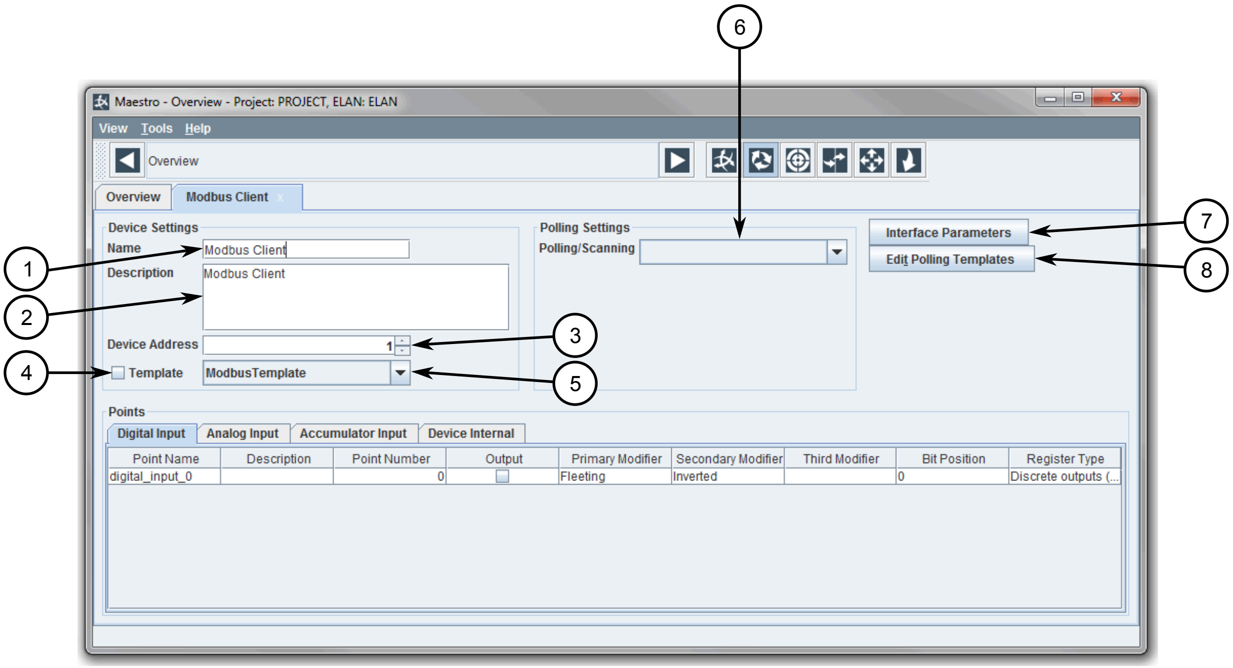
- Section 4.10.14.5, “Configuring a Point”

Section 4.10.14.1

Configuring a Modbus Client

To configure a Modbus client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus client device and click **Properties**. The device's properties appear in a new tab.



Name: Modbus Client

Description: Modbus Client

Device Address: 1

□ Template: ModbusTemplate

Polling/Scanning:

Point Name	Description	Point Number	Output	Primary Modifier	Secondary Modifier	Third Modifier	Bit Position	Register Type
digital_input_0		0	□	Fleeting	Inverted		0	Discrete outputs (...

Figure 143: Modbus Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Polling/Scanning List **7.** Interface Parameters Button **8.** Edit Polling Templates Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 247 The protocol address for the client device.

4. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
5. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .

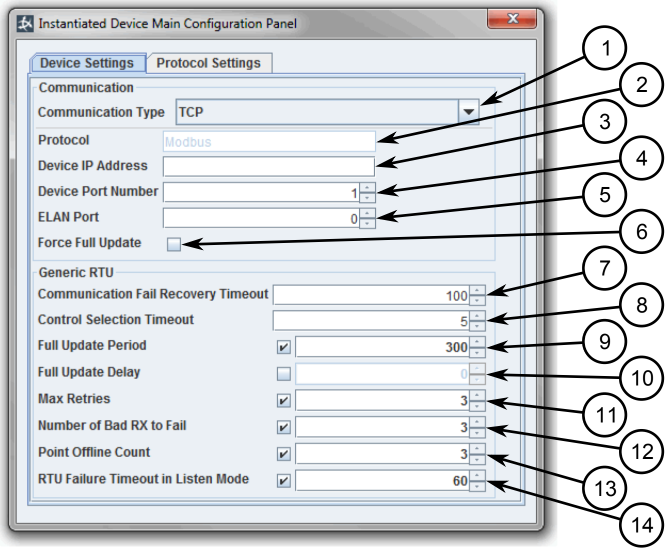
6. [Optional] Configure the device settings. For more information, refer to Section 4.10.14.2, “Configuring TCP/UDP Device Settings”
7. [Optional] Configure the protocol settings. For more information, refer to Section 4.10.14.4, “Configuring Protocol Settings”
8. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.10.6, “Enabling/Disabling Device Internal Points” .

Section 4.10.14.2

Configuring TCP/UDP Device Settings

To configure device settings for a Modbus client device using the TCP/UDP communication protocol, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Device Settings** tab is displayed.



Communication Type: TCP
Protocol: Modbus
Device IP Address:
Device Port Number: 1
ELAN Port: 0
Force Full Update: □
Communication Fail Recovery Timeout: 100
Control Selection Timeout: 5
Full Update Period: ☑ 300
Full Update Delay: □ 0
Max Retries: ☑ 3
Number of Bad RX to Fail: ☑ 3
Point Offline Count: ☑ 3
RTU Failure Timeout in Listen Mode: ☑ 60

Figure 144: Instantiated Device Main Configuration Panel Dialog Box – Device Settings (Example)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box **5.** RUGGEDCOM ELAN Port Box **6.** Force Full Update Check Box **7.** Communication Fail Recovery Timeout Box **8.** Control Selection Timeout Box **9.** Full Update Period Box **10.** Full Update Delay Box **11.** Max Retries Box **12.** Number of Bad RX to Fail Box **13.** Point Offline Count Box **14.** RTU Failure Timeout in Listen Mode Box

4. Under **Communication Type**, select either **TCP** or **UDP**, then configure the following parameters:

Parameter	Description
Device IP Address	The IP address of the remote device or IED.
Device Port Number	**Synopsis:** 1 to 65535 **Default:** 1

Parameter	Description
	The port for the remote device or IED.
RUGGEDCOM ELAN Port	**Synopsis:** 0 to 65535 **Default:** 0 The port used by RUGGEDCOM ELAN to connect with the remote device or IED. A value of 0 represents a wild socket (any available port > 1024). Configure this parameter when a remote device or IED requires a connection on a specific port.
Force Full Update	Controls when data acquired as part of a full update is written to the TIE database. When checked/enabled, data is always written to the TIE database. When clear/disabled, data is only written to the TIE database if the value has changed.

5. Under **Generic RTU**, configure the following parameters as required:

Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 100 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
Point Offline Count	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled

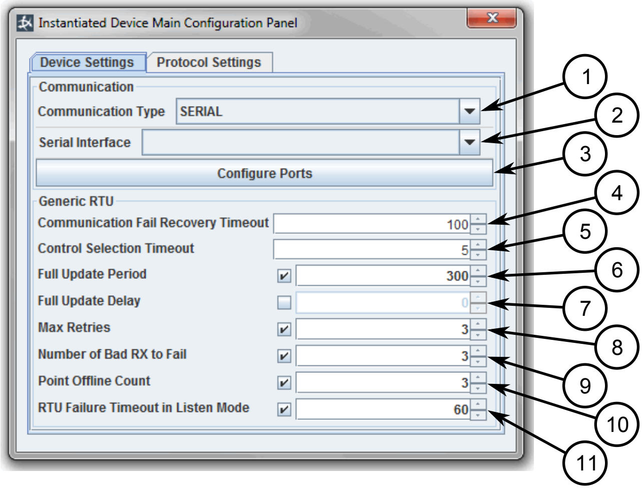
Parameter	Description
	The number of times a scan – including retries – can consecutively fail to acquire the requested data before the unreported points are considered off-line (failed).
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.14.3

Configuring Serial Device Settings

To configure device settings for a Modbus client device using serial communication, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Device Settings** tab is displayed.



Instantiated Device Main Configuration Panel

Communication Type: SERIAL

Serial Interface:

Communication Fail Recovery Timeout: 100

Control Selection Timeout: 5

Full Update Period: ☑ 300

Full Update Delay: ☐ 0

Max Retries: ☑ 3

Number of Bad RX to Fail: ☑ 3

Point Offline Count: ☑ 3

RTU Failure Timeout in Listen Mode: ☑ 60

Figure 145: Instantiated Device Main Configuration Panel Dialog Box – Device Settings (Example)

1. Communication Type List **2.** Serial Interface List **3.** Configure Ports Button **4.** Communication Fail Recovery Timeout Box **5.** Control Selection Timeout Box **6.** Full Update Period Box **7.** Full Update Delay Box **8.** Max Retries Box **9.** Number of Bad RX to Fail Box **10.** Point Offline Count Box **11.** RTU Failure Timeout in Listen Mode Box

4. Under **Communication Type**, select **Serial**.
5. Under **Serial Interface**, select a serial interface. If the serial interfaces do not meet the requirements, do one of the following:
   - Modify an existing serial interface by clicking **Configure Ports**. A dialog box appears. For more information about configuration options, refer to Step 3 in Section 4.6.7.3, “Configuring a Serial Interface” .
   - Create a new serial interface. For more information, refer to Section 4.6.7.1, “Adding/Deleting a Serial Interface” .

6. Under **Generic RTU**, configure the following parameters as required:

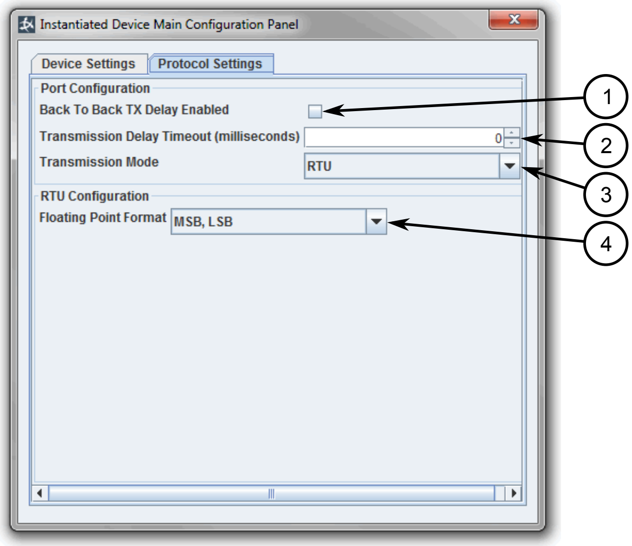
Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 100 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
Point Offline Count	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a scan – including retries – can consecutively fail to acquire the requested data before the unreported points are considered off-line (failed).
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.14.4

Configuring Protocol Settings

To configure protocol settings for a Modbus client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **Protocol Settings** tab.



Port Configuration

Back To Back TX Delay Enabled □

Transmission Delay Timeout (milliseconds) 0

Transmission Mode RTU

RTU Configuration

Floating Point Format MSB, LSB

Figure 146: Instantiated Device Main Configuration Panel Dialog Box – Protocol Settings

1. Back To Back TX Delay Enabled Check Box **2.** Transmission Delay Timeout (milliseconds) Box **3.** Transmission Mode List **4.** Floating Point Format List

5. Under **Port Configuration**, configure the following parameters as required:

Parameter	Description
Back To Back TX Delay Enabled	**Default State:** Disabled When enabled (selected), the time delay specified by the `Transmission Delay Timeout` parameter is used under the following conditions to pause before a message is transmitted. • If the previous message transmission involved the same RTU • If the previous and/or current message is a broadcast message When disabled (cleared), the time delay specified by the `Transmission Delay Timeout` parameter is used to apply a pause before all transmissions, regardless of the RTUs involved.
Transmission Delay Timeout (milliseconds)	**Synopsis:** 0 to 999 **Default:** 0 The time in milliseconds (ms) to pause before a message is transmitted to an RTU.
Transmission Mode	**Synopsis:** RTU, ASCII, TCP/IP **Default:** RTU The transmission mode associated with the client device.

6. Under **RTU Configuration**, configure the following parameters as required:

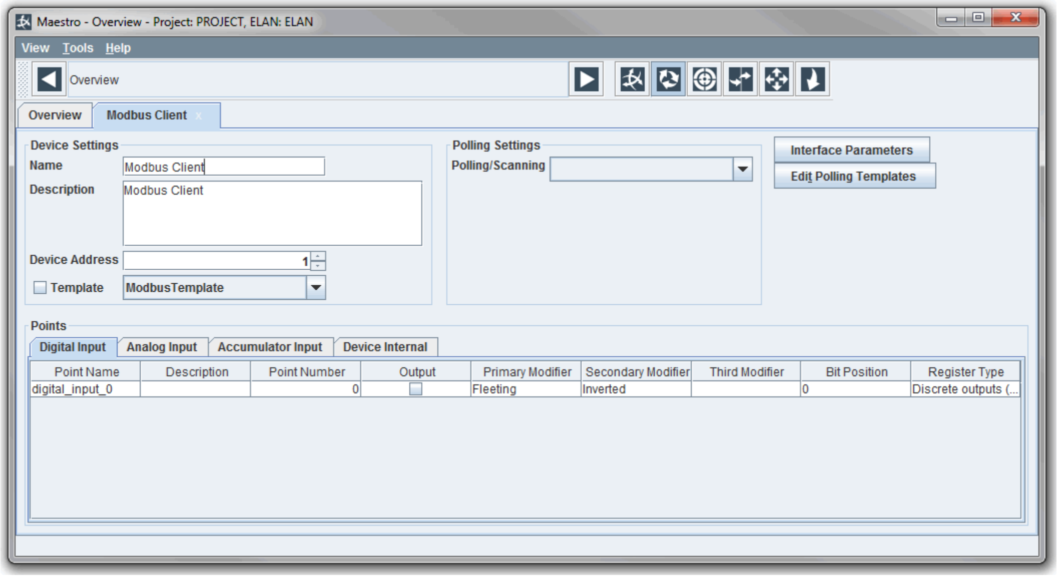
Parameter	Description
Floating Point Format	**Synopsis:** "MSB, LSB", "LSB, MSB" **Default:** MSB, LSB Determines how a 32-bit floating point is arranged over two 16-bit values.

Section 4.10.14.5

Configuring a Point

To configure/modify existing points for a Modbus client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the Modbus client device and click **Properties**. The device's properties appear in a new tab.



Name: Modbus Client
Description: Modbus Client
Device Address: 1
☐ Template: ModbusTemplate
Polling/Scanning:

Point Name	Description	Point Number	Output	Primary Modifier	Secondary Modifier	Third Modifier	Bit Position	Register Type
digital_input_0		0	☐	Fleeting	Inverted		0	Discrete outputs (...

Figure 147: Modbus Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, "Controlling Template Links" .
4. Under **Points**, select the desired tab and configure the following parameters as required:

» Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.

Parameter	Description
Output	**Default State:** Disabled When enabled (selected), the output point is present for this input point.
Primary Modifier	**Synopsis:** { Fleeting, Single Point, Bit Pair } The primary modifier. Options include: • `Fleeting` – Identifies a point that reports only when it enters a specific state (e.g. alarm), but not the change to the alternate state. Whenever the state to be reported is entered, the TIE sets the memory bit of the corresponding point to 1 (the status value of the point is always 0). • `Single Point` – Use to identify a single status point. **NOTE** *Bit Pair points must reside with the returned data field boundaries. For bit-pair entries, only the first point is configured.* • `Bit Pair` – Use to combine two sequential single status points that are reported together as one point. The two state bits combined represent one of four possible states for the point. Bit pair points may be mixed with single status points within data field boundaries (one byte) reported by the RTU.
Secondary Modifier	**Synopsis:** { Force Update, Inverted } The secondary modifier. Options include: • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.
Third Modifier	**Synopsis:** { Force Update, Inverted } The third modifier. Options include: • `Force Update` – Used to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Output	**Default State:** Disabled When enabled (selected), the output point is present for this input point.
Primary Modifier	**Synopsis:** { 16 Bit, Float, 32 Bit }

Parameter	Description
	The primary modifier. Options include: • `16 Bit` – Use to identify a 16-Bit binary analog input or a 10-bit binary analog input point occupying a 16-bit data field with the six most significant bits set to zero. **NOTE** _Float and 32 Bit points require Maestro to process two points as a single entity. As such, if, when mapping server and client points, the user selects an analog input point (e.g. Point #1) and another analog input number exists with the next point number assigned (e.g. Point #2), Maestro automatically pairs the two points together. The point with the lowest number is considered the **Master Point**, while the other point is the **Secondary Point**._ _The **Secondary Point** is rendered non-editable (grayed-out) and assigned the same modifier as the **Master Point**._ _If the **Master Point** has an output point associated with it, an output point is automatically created for the **Secondary Point** if one does not already exist. However, if the **Master Point** does not have an output point associated with it, but the **Secondary Point** does, the output point for the **Secondary Point** is deleted to mirror the **Master Point**._ _Alternatively, if the user selects an analog input point for which there does not exist another analog input point with the next point number, Maestro silently creates the second analog input point. The second analog input will not be visible to the user and will be replaced if the user creates a new analog input point with the next point number._ _For more information about mapping Modbus analog points, and other types of points, refer to Section 4.12.1, "Mapping Server and Client Points" ._ • `Float` – Use to identify analog inputs that are reported together as one point. A 32-bit floating point value is reported by two sequential registers, which are reported together as one point. An RTU may report a mix of floating points and non-floating points. Both registers containing a floating point value must be reported with the same RTU message. • `32 Bit` – Use to identify a 32-Bit 2's complement point that is to be processed as a 32-Bit 2's complement value without any scaling applied.
Secondary Modifier	**Synopsis:** { Force Update, Scaled } The secondary modifier. Options include: • `Force Update` – Use to identify a status point that is to be reported whenever the point's state is acquired, whether it has changed or not. • `Scaled` – Use to identify an analog point whose raw value should be stored in the database. The client process will calculate the raw value and store it in the database.
Register Type	**Synopsis:** { Holding, Input } The register type. Options include:

Parameter	Description
	• `Holding` – Use to identify Holding Registers • `Input` – Use to identify Input Registers
Scale	**Default:** 1 Any positive or negative floating point value.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Register Type	**Synopsis:** { Holding, Input } The register type. Options include: • `Holding` – Use to identify Holding Registers • `Input` – Use to identify Input Registers
Units	A text field.

Section 4.10.15

Managing RP 570 Client Devices

This section describes how to configure and manage RP 570 client devices.

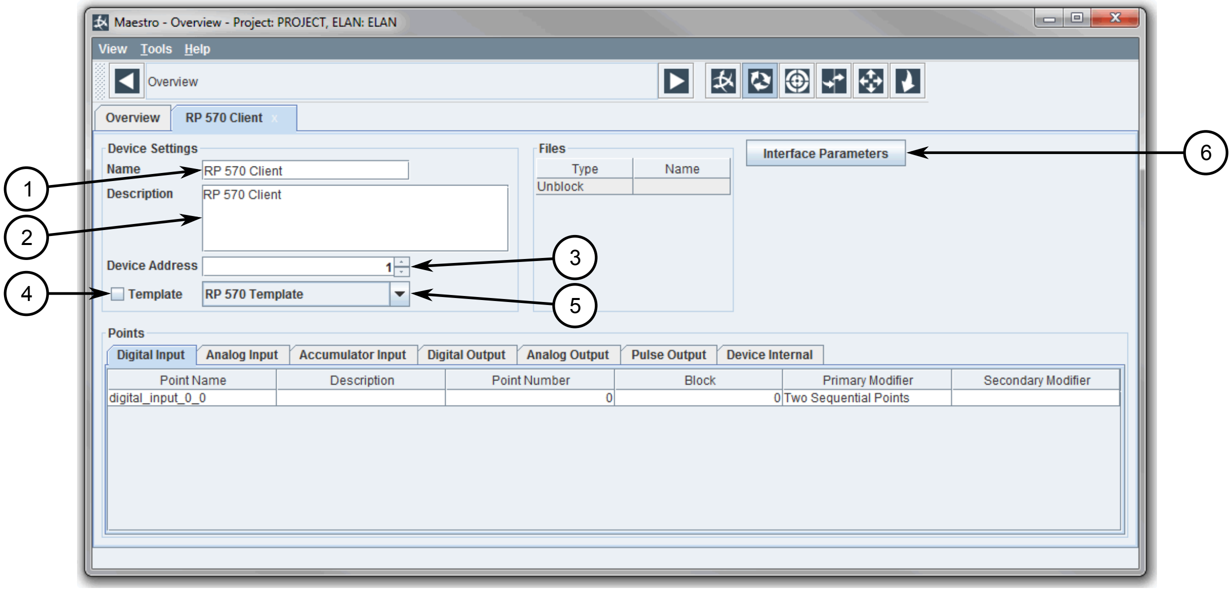
CONTENTS

Section 4.10.15.1

Configuring a RP 570 Client

To configure a RP 570 client, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RP 570 client device and click **Properties**. The device's properties appear in a new tab.



Name: RP 570 Client

Description: RP 570 Client

Device Address: 1

□ Template: RP 570 Template

Type	Name
Unblock	

Point Name	Description	Point Number	Block	Primary Modifier	Secondary Modifier
digital_input_0_0		0	0	Two Sequential Points	

Figure 148: RP 570 Client Properties

1. Name Box **2.** Description Box **3.** Device Address Box **4.** Template Check Box **5.** Template List **6.** Interface Parameters Button

3. Under **Device Settings**, configure the following parameters as required:

Parameter	Description
Name	The name of the client device.
Description	A brief description of the client device.
Device Address	**Synopsis:** 1 to 255 The protocol address for the client device.

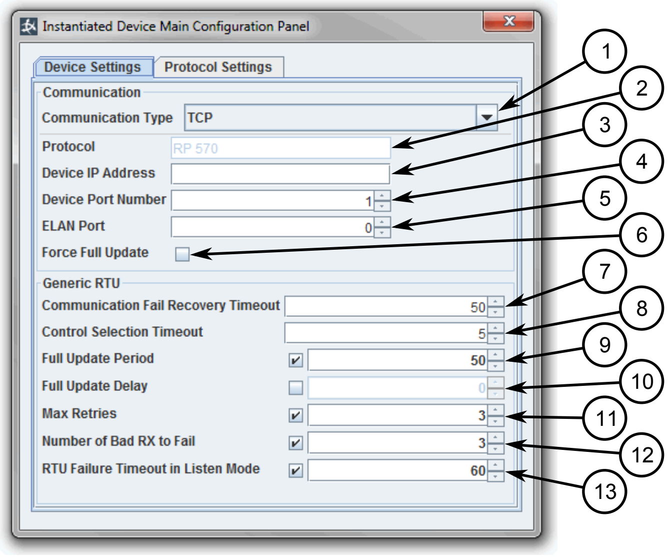
4. If points were not inherited from a device template or the points require modification, modify, add, or remove points as required. For more information, refer to Section 4.10.4, “Adding/Deleting Points” .
5. [Optional] Control whether or not the client device is based on a device template. For more information, refer to Section 4.8.6, “Using a Device Template” .
6. [Optional] Configure the device settings. For more information, refer to Section 4.10.15.2, “Configuring Device Settings”
7. [Optional] Configure the protocol settings. For more information, refer to Section 4.10.15.3, “Configuring Protocol Settings”
8. [Optional] Enable or disable the device internal points. For more information, refer to Section 4.10.6, “Enabling/Disabling Device Internal Points” .

Section 4.10.15.2

Configuring Device Settings

To configure device settings for RP 570 client devices, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RP 570 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears. By default, the **Device Settings** tab is displayed.



Instantiated Device Main Configuration Panel

Device Settings | Protocol Settings

Communication

Communication Type: TCP
Protocol: RP 570
Device IP Address:
Device Port Number: 1
ELAN Port: 0
Force Full Update: □

Generic RTU

Communication Fail Recovery Timeout: 50
Control Selection Timeout: 5
Full Update Period: ☑ 50
Full Update Delay: □ 0
Max Retries: ☑ 3
Number of Bad RX to Fail: ☑ 3
RTU Failure Timeout in Listen Mode: ☑ 60

Figure 149: Instantiated Device Main Configuration Panel Dialog Box – Device Settings (Example)

1. Communication Type List **2.** Protocol Box **3.** Device IP Address Box **4.** Device Port Number Box **5.** RUGGEDCOM ELAN Port Box **6.** Force Full Update Check Box **7.** Communication Fail Recovery Timeout Box **8.** Control Selection Timeout Box **9.** Full Update Period Box **10.** Full Update Delay Box **11.** Max Retries Box **12.** Number of Bad RX to Fail Box **13.** RTU Failure Timeout in Listen Mode Box

4. Under **Communication**, configure the following parameters as required:

Parameter	Description
Communication Type	**Synopsis:** Serial, UDP, TCP **Default:** TCP The interface used to communicate with the remote device.
Device IP Address	The IP address of the remote device or IED.
Device Port Number	**Synopsis:** 1 to 65535 **Default:** 1 The port for the remote device or IED.
ELAN Port	**Synopsis:** 0 to 65535 **Default:** 0 The port used by RUGGEDCOM ELAN to connect with the remote device or IED. A value of 0 represents a wild socket (any available port > 1024). Configure this parameter when a remote device or IED requires a connection on a specific port.

Parameter	Description
Force Full Update	Controls when data acquired as part of a full update is written to the TIE database. When checked/enabled, data is always written to the TIE database. When clear/disabled, data is only written to the TIE database if the value has changed.

5. Under **Generic RTU**, configure the following parameters as required:

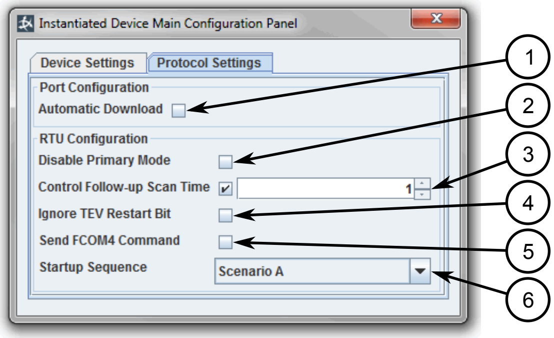
Parameter	Description
Communication Fail Recovery Timeout	**Synopsis:** 0 to 90000 **Default:** 50 The time in seconds (s) to wait after a communication failure before attempting to communication with the RTU.
Control Selection Timeout	**Synopsis:** 0 to 30 **Default:** 5 The time in seconds (s) to wait for an Operate request after sending a Select request. If the expected Operate request is not received within the time limit, the Select request is canceled.
Full Update Period	**Synopsis:** 1 to 30000 **Default Value:** 300 **Default State:** Enabled The time in seconds (s) to wait before polling the RTU for a full update. The check box must be checked for this parameter to take effect.
Full Update Delay	**Synopsis:** 0 to 300 **Default Value:** 0 **Default State:** Disabled The time in seconds (s) to delay the initial Full Update request after communication has been established with the RTU. The check box must be checked for this parameter to take effect.
Max Retries	**Synopsis:** 1 to 10 **Default Value:** 3 **Default State:** Enabled The number of times a message is retransmitted if a response is not received from the RTU or if the response was corrupted. The check box must be checked for this parameter to take effect.
Number of Bad RX to Fail	**Synopsis:** 1 to 32 **Default Value:** 3 **Default State:** Enabled The number of consecutive corrupted or missing responses from the RTU before the device is considered failed. The check box must be checked for this parameter to take effect.
RTU Failure Timeout in Listen Mode	**Synopsis:** 1 to 200 **Default Value:** 60 **Default State:** Enabled The time in seconds (s) after an RTU is declared off-line (failed) when operating in Listen Mode.

Section 4.10.15.3

Configuring Protocol Settings

To configure protocol settings for an RP 570 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RP 570 client device and click **Properties**. The device's properties appear in a new tab.
3. Click **Interface Parameters**. The **Instantiated Device Main Configuration Panel** dialog box appears.
4. Click the **Protocol Settings** tab.



Instantiated Device Main Configuration Panel

Port Configuration

Automatic Download □

RTU Configuration

Disable Primary Mode □

Control Follow-up Scan Time ☑ 1

Ignore TEV Restart Bit □

Send FCOM4 Command □

Startup Sequence: Scenario A

Figure 150: Instantiated Device Main Configuration Panel Dialog Box – Protocol Settings

1. Automatic Download Check Box **2.** Disable Primary Mode Check Box **3.** Control Follow-Up Scan Time Box **4.** Ignore TEV Restart Bit Check Box **5.** Send FCOM4 Command Check Box **6.** Startup Sequence List

5. Under **Port Configuration**, configure the following parameters as required:

Parameter	Description
Automatic Download	**Default State:** Disabled When enabled (selected), the TIE remote interface will automatically download the configuration file to an RTU when the RTU indicates a download is required. When disabled (cleared), the TIE remote interface will not automatically download the configuration file when requested by an RTU. It will instead notify the host of the required configuration, after which the download can be initiated manually.

6. Under **RTU Configuration**, configure the following parameters as required:

Parameter	Description
Disable Primary Mode	**Default State:** Disabled When disabled (cleared), the TIE remote interface will send an RP 570 message FCOM Number 23 as part of a communication initialization to place an RTU into primary mode. When enabled (selected), the message is not sent and RTUs are not placed in primary mode.
Control Follow-Up Scan Time	**Synopsis:** 1 to 300 **Default Value:** 1 **Default State:** Enabled

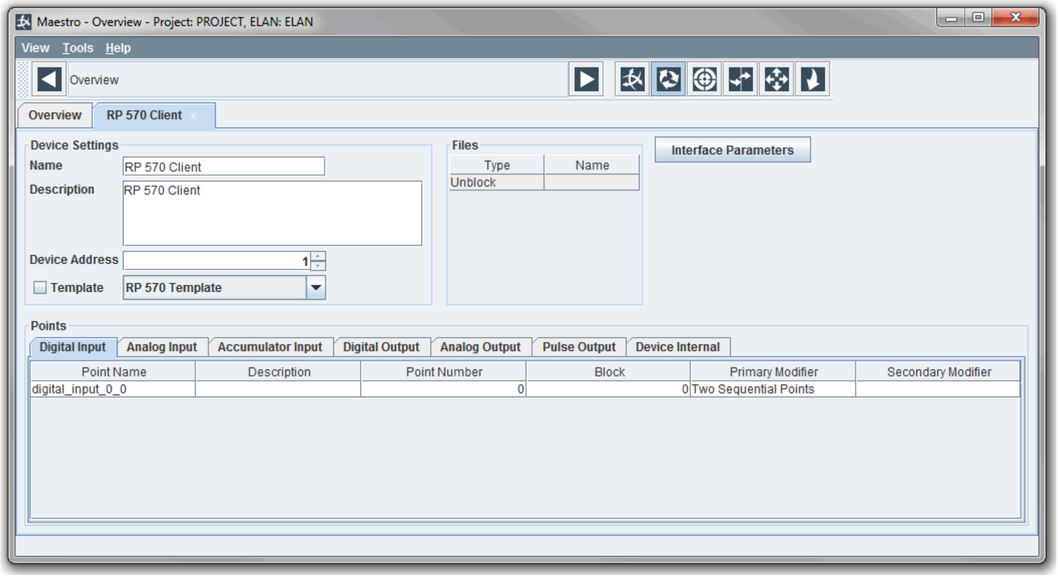
Parameter	Description
	The time in seconds (s) an RTU is scanned until a control (e.g. digital, raise/lower or set-point) is issued using the RB command. The check box must be checked for this parameter to take effect.
Ignore TEV Restart Bit	**Default State:** Disabled When disabled (cleared), the TEV restart bit is ignored. This may be required if an RTU continuously resets this bit.
Send FCOM4 Command	**Default State:** Disabled When enabled (selected), RUGGEDCOM ELAN sends an FCOM4 command to an RTU following the receipt of an EXR response to an FCOM2 command.
Startup Sequence	**Synopsis:** Scenario A, Scenario B, Scenario C **Default:** Scenario A The RTU startup sequence. Options include: Scenario A (00), Scenario B (01) and Scenario C (10).

Section 4.10.15.4

Configuring a Point

To configure/modify existing points for an RP 570 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the RP 570 client device and click **Properties**. The device's properties appear in a new tab.



Name: RP 570 Client
Description: RP 570 Client
Device Address: 1
☐ Template: RP 570 Template

Type	Name
Unblock	

Point Name	Description	Point Number	Block	Primary Modifier	Secondary Modifier
digital_input_0_0		0	0	Two Sequential Points	

Figure 151: RP 570 Client Properties

3. If the device is linked to a template, break the link to be able to configure/modify points. For more information, refer to Section 4.8.3, “Controlling Template Links” .
4. Under **Points**, select the desired tab and configure the following parameters as required:

Digital Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_input_1).
Description	A description of the point.
Point Number	The number assigned to the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Primary Modifier	**Synopsis:** { Two Sequential Points, Single Point } The primary modifier. Options include: • `Two Sequential Points` – Use to identify two sequential single status points, which are reported together as one point. The two state bits combined represent one of four possible states for the point. • `Single Point` – Use to identify a single status point.
Secondary Modifier	**Synopsis:** { Redundant } The primary modifier. Options include: • `Redundant` – Use to identify SOE points in protocols where a change of state of SOE points and a time tagged change of state are reported separately.

Analog Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_input_1).
Description	A description of the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Primary Modifier	**Synopsis:** { Unipolar, 16 Bit } The primary modifier. Options include: • `Unipolar` – Use to identify a 12-bit analog input that is always positive in value. • `16 Bit` – Use to identify a 12-Bit 2's complement, 12-bit 2's complement with sign extended to 16-bit, and digital coded analog points.
Units	A text field.

Accumulator Input

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. accumulator_input_1).
Description	A description of the point.
Block	**Synopsis:** 0 to 255 **Default:** 0 The block number assigned to the point.
Units	A text field.

Digital Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. digtial_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Primary Modifier	**Synopsis:** { Close Trip Pair, Momentary, Trip Close Pair, Single Point } The primary modifier. Options include: • `Close Trip Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Trip Close Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests. • `Single Point` – Use when a single relay is used to trip (OFF) or close (ON) an external device.
Secondary Modifier	**Synopsis:** { Inverted } The secondary modifier. Options include: • `Inverted` – Identifies a status point whose value is inverted when it is stored in the database before being reported through a server device.

Analog Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. analog_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Units	A text field.

Pulse Output

Parameter	Description
Point Name	The name of the point. Initially, each point is assigned a name in the format of *{point-type}_{point-number}* (e.g. pulse_output_1).
Description	A description of the point.
Object	**Synopsis:** 0 to 255 **Default:** 0 The object number assigned to the point.
Primary Modifier	**Synopsis:** { Single Point, Lower Raise Pair, Raise Lower Pair, Momentary } The primary modifier. Options include: • `Single Point` – Use when a single relay is used to raise or lower an external device. • `Lower Raise Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Close requests, while the second point, which is not displayed, receives the Trip requests. • `Momentary` – Use to send a momentary request to a Digital Output point from SCADA hosts. The same control request will be sent to the remove device, regardless of the value requested (either a Trip or Close) from the host. • `Raise Lower Pair` – Use to pair two consecutive remote Digital Output points and represent them as a single Digital Output point to SCADA hosts. The first displayed point will receive the Trip requests, while the second point, which is not displayed, receives the Close requests.
Secondary Modifier	**Synopsis:** { Inverted } The secondary modifier. Options include: • `Inverted` – Inverts the action sent to the remote device.

Section 4.11

Managing Polling Templates

This section describes how to configure and manage polling templates in Maestro.

CONTENTS

Section 4.11.1

Managing Timed Scans for DNP Devices

This section describes how to configure and manage timed scans for DNP client devices in Maestro.

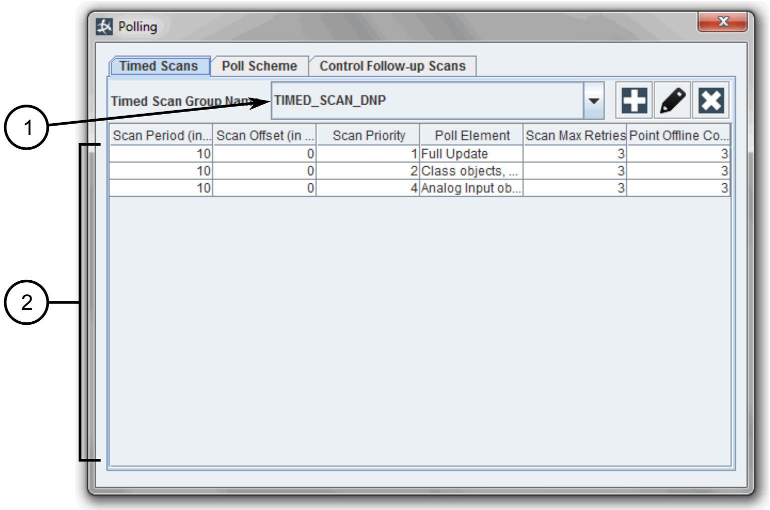
CONTENTS

Section 4.11.1.1

Viewing a List of Timed Scans

To view timed scans defined for a DNP client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 152: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

4. Select a group from the **Timed Scan Group Name** list. The elements associated with the group appear in the table.

   If a group does not exist, add one. For more information, refer to Section 4.11.1.2, “Adding/Deleting a Timed Scan Group” .

   If an element does not exist, add one. For more information, refer to Section 4.11.1.3, “Adding/Deleting a Timed Scan Element” .

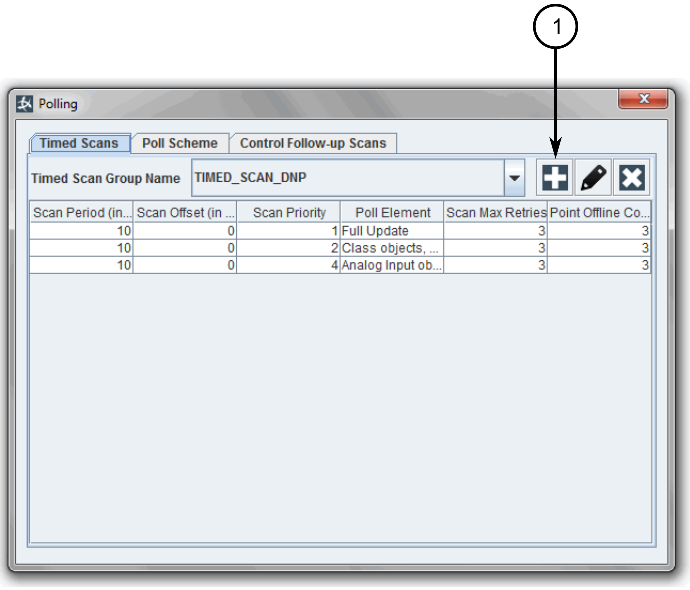
Section 4.11.1.2

Adding/Deleting a Timed Scan Group

To add/delete a timed scan group for a DNP client device, do the following:

›› Adding a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



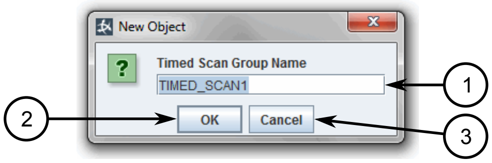
Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 153: Polling Dialog Box – Timed Scans

1. Add Button

4. Click the **Add** button. The **New Object** dialog box appears.



Timed Scan Group Name: TIMED_SCAN1

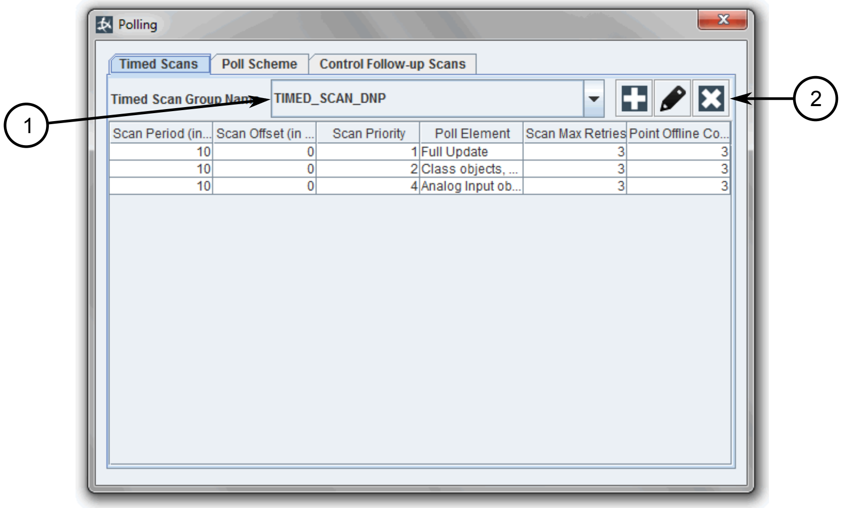
Figure 154: New Object Dialog Box

1. Timed Scan Group Name Box **2.** OK Button **3.** Cancel Button

5. [Optional] Type a new name for the group.
6. Click **OK** to add the group, or click **Cancel** to abort.

›› Deleting a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 155: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Delete Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Delete** button. A confirmation dialog box appears.
6. Click **Yes** to delete the group, or click **No** to abort.

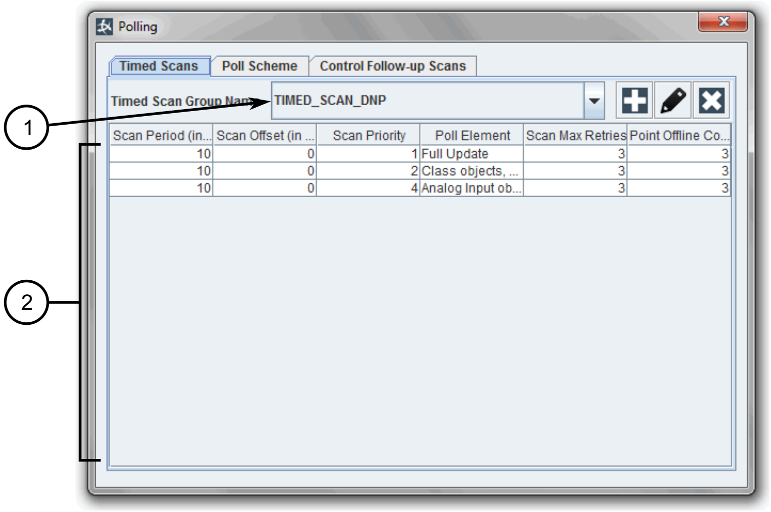
Section 4.11.1.3

Adding/Deleting a Timed Scan Element

To add/delete a timed scan element to a timed scan group for a DNP client device, do the following:

›› Adding a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 156: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

4. Select a group from the **Timed Scan Group Name** list.
5. Right-click anywhere in the elements area to open the shortcut menu and click **New**. A new poll element is added to the table.
6. Configure the following parameters as required:

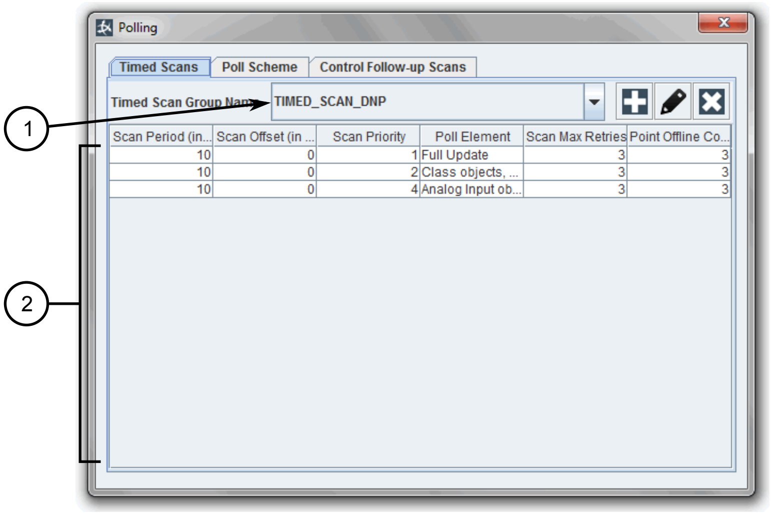
Parameter	Description
Scan Period (in seconds)	**Synopsis:** 1 to 3600 **Default:** 10 The maximum duration in seconds (s) to scan an RTU for specific data.
Scan Offset (in seconds)	**Synopsis:** 0 to 3600 **Default:** 11 The time in seconds (s), applied on TIE startup, to wait before unblocking an RTU after reestablishing the connection.
Scan Priority	**Synopsis:** 0 to 64 **Default:** 1 The priority of the scan, where zero (0) is the highest priority.
Poll Element	The poll element to use. Options include: • `Analog Input Objects, variation 0 (All variations)` – Polls the RTU for all Analog Input Objects (object 30, variation 0) • `Analog Input Objects, variation 1 (32-bit)` – Polls the RTU for 32-bit Analog Input Objects (object 30, variation 1) • `Analog Input Objects, variation 2 (16-bit)` – Polls the RTU for 16-bit Analog Input Objects (object 30, variation 2) • `Analog Input Objects, variation 3 (32-bit without flags)` – Polls the RTU for 32-bit Analog Input Objects without flags objects (object 30, variation 3)

Parameter	Description
	• `Analog Input Objects, variation 4 (16-bit without flags)` – Polls the RTU for 16-bit Analog Input Objects without flags objects (object 30, variation 4) • `Floating Point Objects, variation 1 (Short)` – Polls the RTU for Short Floating Point Objects (object 100, variation 1) • `BCD Objects, variation 0 (All variations)` – Polls the RTU for Binary Coded Decimal Objects (object 101, variation 0) • `BCD Objects, variation 1 (Small-Packed BCD Objects)` – Polls the RTU for Small-Packed Binary Coded Decimal Objects (object 101, variation 1) • `BCD Objects, variation 2 (Medium Packed BCD Objects)` – Polls the RTU for Medium-Packed Binary Coded Decimal Objects (object 101, variation 2) • `Class Objects, variation 2 (Class 1)` – Polls the RTU for Class 1 Objects (object 60, variation 2) • `Class Objects, variation 3 (Class 2)` – Polls the RTU for Class 2 Objects (object 60, variation 3) • `Class Objects, variation 4 (Class 3)` – Polls the RTU for Class 3 Objects (object 60, variation 4) • `Running Binary Counter Object, variation 0 (All variations)` – Polls the RTU for all *Running* Binary Counter Objects (object 20, variation 0) • `Running Binary Counter Object, variation 1 (32-bit)` – Polls the RTU for *Running* 32-bit Binary Counter Objects (object 20, variation 1) • `Running Binary Counter Object, variation 2 (16-bit)` – Polls the RTU for *Running* 16-bit Binary Counter Objects (object 20, variation 2) • `Running Binary Counter Object, variation 5 (32-bit without flag)` – Polls the RTU for *Running* 32-bit Binary Counter without flag Objects (object 20, variation 5) • `Running Binary Counter Object, variation 6 (16-bit without flag)` – Polls the RTU for *Running* 16-bit Binary Counter without flag Objects (object 20, variation 6) • `Full Update` – Polls the RTU for full update • `Time Synchronization` – Periodically synchronizes a DNP RTU's time
Scan Max Retries	**Synopsis:** 0 to 10 **Default:** 3 The maximum number of times the scan can be retransmitted if a response is not received or corrupted.
Point Offline Count	**Synopsis:** -1, 1 to 10 **Default:** 3 The number of times the scan can fail consecutively before the unreported points are considered off-line. Use -1 to disable this feature.

›› Deleting a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.

3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 157: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Elements

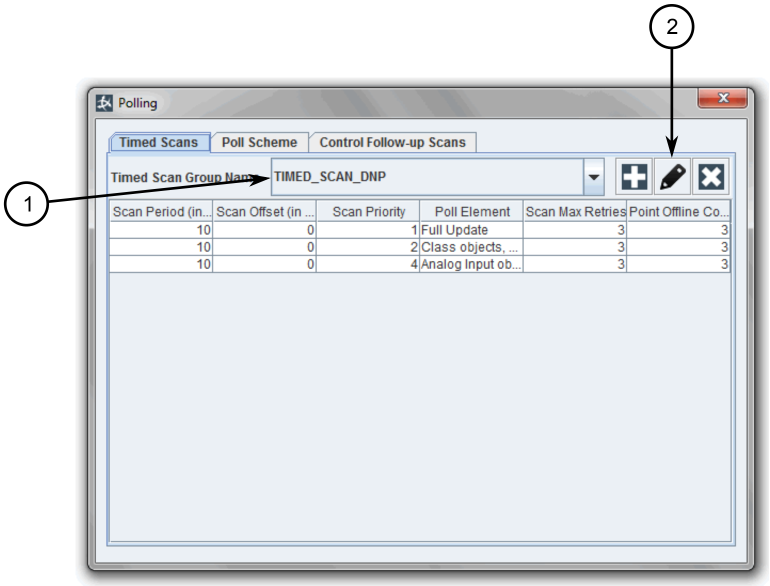
4. Select a group from the **Timed Scan Group Name** list.
5. Right-click the desired element to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the element, or click **No** to abort.

Section 4.11.1.4

Renaming a Timed Scan Group

To rename a timed scan group, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN_DNP

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	0	1	Full Update	3	3
10	0	2	Class objects, ...	3	3
10	0	4	Analog Input ob...	3	3

Figure 158: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Rename Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Rename** button and type a new name for the group.

Section 4.11.2

Managing Timed Scans for Modbus Devices

This section describes how to configure and manage timed scans for Modbus client devices in Maestro.

CONTENTS

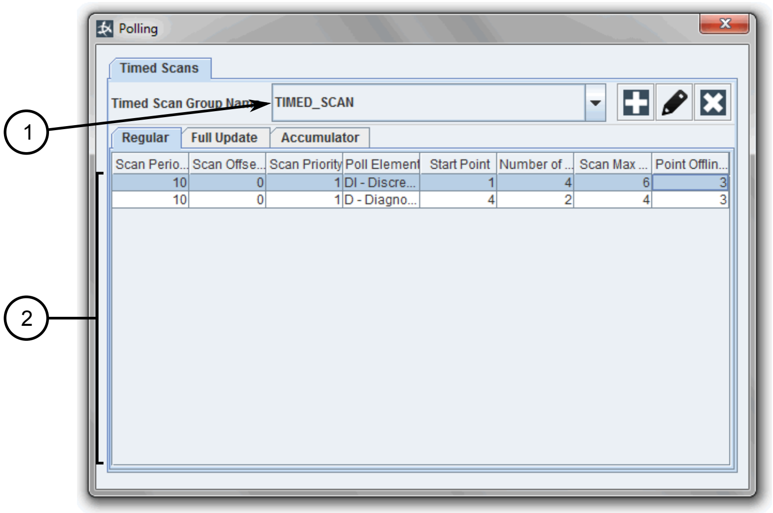
Section 4.11.2.1

Viewing a List of Timed Scans

To view timed scans defined for a Modbus client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.

3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN

Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 159: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

4. Select a group from the **Timed Scan Group Name** list. The elements associated with the group appear in the table.

   If a group does not exist, add one. For more information, refer to Section 4.11.2.2, "Adding/Deleting a Timed Scan Group" .

   If an element does not exist, add one. For more information, refer to Section 4.11.2.3, "Adding/Deleting a Timed Scan Element" .

5. Click the desired tab. Each tab represents a type of timed scan:

   - `Regular` – Scans that are executed at the configured frequency
   - `Full Update` – Scans that are executed during a full update
   - `Accumulator` – Scans that are executed following an Accumulator Freeze command

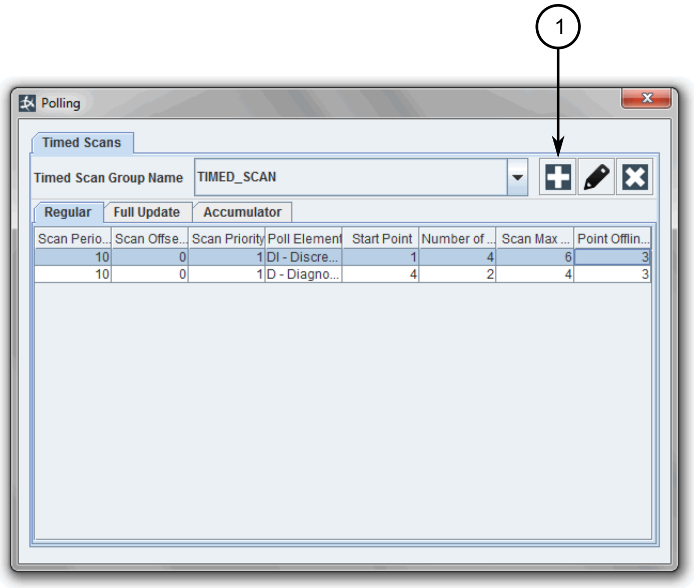
Section 4.11.2.2

Adding/Deleting a Timed Scan Group

To add/delete a timed scan group for a Modbus client device, do the following:

›› Adding a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



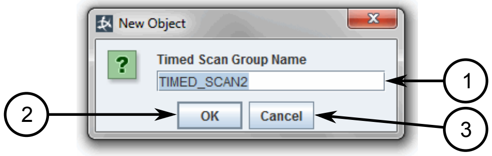
Timed Scan Group Name: TIMED_SCAN

Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 160: Polling Dialog Box – Timed Scans

1. Add Button

4. Click the **Add** button. The **New Object** dialog box appears.



Timed Scan Group Name: TIMED_SCAN2

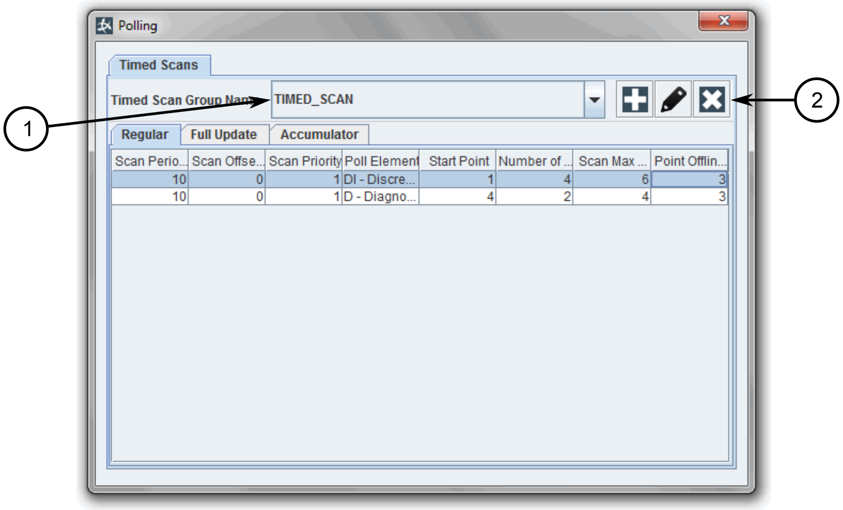
Figure 161: New Object Dialog Box

1. Timed Scan Group Name Box **2.** OK Button **3.** Cancel Button

5. [Optional] Type a new name for the group.
6. Click **OK** to add the group, or click **Cancel** to abort.

›› Deleting a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 162: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Delete Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Delete** button. A confirmation dialog box appears.
6. Click **Yes** to delete the group, or click **No** to abort.

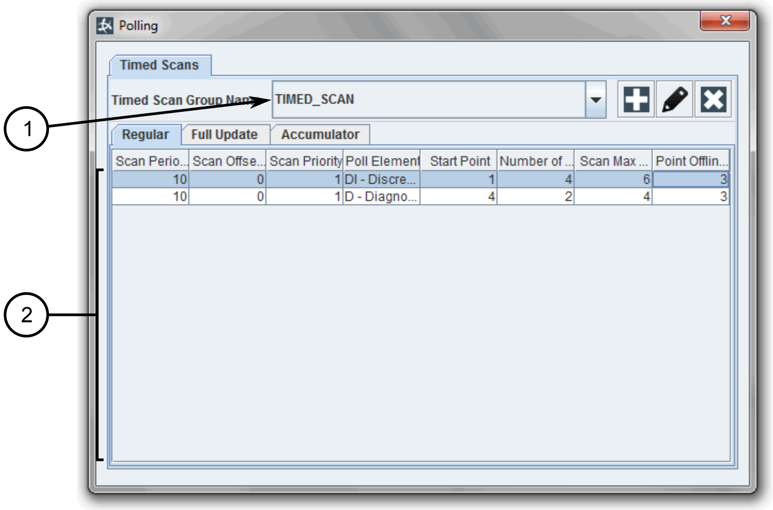
Section 4.11.2.3

Adding/Deleting a Timed Scan Element

To add/delete a timed scan element to a timed scan group for a Modbus client device, do the following:

›› Adding a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Nam TIMED_SCAN

Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 163: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

4. Select a group from the **Timed Scan Group Name** list.
5. Click the desired tab. Each tab represents a type of timed scan:
   - `Regular` – Scans that are executed at the configured frequency
   - `Full Update` – Scans that are executed during a full update
   - `Accumulator` – Scans that are executed following an Accumulator Freeze command
6. Right-click anywhere in the elements area to open the shortcut menu and click **New**. A new poll element is added to the table.
7. Configure the following parameters as required:
   - **Regular Timed Scans**

Parameter	Description
Scan Period (in seconds)	**Synopsis:** 1 to 3600 **Default:** 10 The maximum duration in seconds (s) to scan an RTU for specific data.
Scan Offset (in seconds)	**Synopsis:** 0 to 3600 **Default:** 11 The time in seconds (s), applied on TIE startup, to wait before unblocking an RTU after reestablishing the connection.
Scan Priority	**Synopsis:** 0 to 64 **Default:** 1 The priority of the scan, where zero (0) is the highest priority.
Poll Element	The poll element to use. Options include: ▫ `D - Diagnostic Register Poll` – Polls the RTU for diagnostic register data (Modbus Diagnostics/Return Diagnostic Register)

Parameter	Description
	▫ `DI - Discrete Input Poll` – Polls the RTU for discrete input data (Modbus Read Input Status) ▫ `DO - Discrete Output Poll` – Polls the RTU for discrete output data (Modbus Read Input Status) ▫ `E - Exception Status Poll` – Polls the RTU for its exception status (Modbus Read Exception Status) ▫ `Full Update` – Polls the RTU for full update ▫ `HR - Holding Register Poll` – Polls the RTU for holding register data (Modbus Read Holding Registers) ▫ `IR - Input Register Poll` – Polls the RTU for input register data (Modbus Read Input Registers)
Scan Max Retries	**Synopsis:** 0 to 10 **Default:** 3 The maximum number of times the scan can be retransmitted if a response is not received or corrupted.
Point Offline Count	**Synopsis:** -1, 1 to 10 **Default:** 3 The number of times the scan can fail consecutively before the unreported points are considered off-line. **NOTE** *If scans for event Class data (Class 1, 2 or 3) fail, no points will be considered off-line regardless of the configured point off-line count value, as the points contained in a response cannot be predicted.*

- **Full Update Timed Scans**

Parameter	Description
Poll Element	**Synopsis:** **Default:** The poll element to use. Options include: ▫ `D - Diagnostic Register Poll` – Polls the RTU for diagnostic register data (Modbus Diagnostics/Return Diagnostic Register) ▫ `DI - Discrete Input Poll` – Polls the RTU for discrete input data (Modbus Read Input Status) ▫ `DO - Discrete Output Poll` – Polls the RTU for discrete output data (Modbus Read Input Status) ▫ `E - Exception Status Poll` – Polls the RTU for its exception status (Modbus Read Exception Status) ▫ `HR - Holding Register Poll` – Polls the RTU for holding register data (Modbus Read Holding Registers) ▫ `IR - Input Register Poll` – Polls the RTU for input register data (Modbus Read Input Registers)
Start Point	**Synopsis:** 0 to 65535 **Default:** 0 **NOTE** *This parameter is ignored when **Poll Element** is set to* `Exception Status Poll` *or* `Diagnostic Register Poll`.

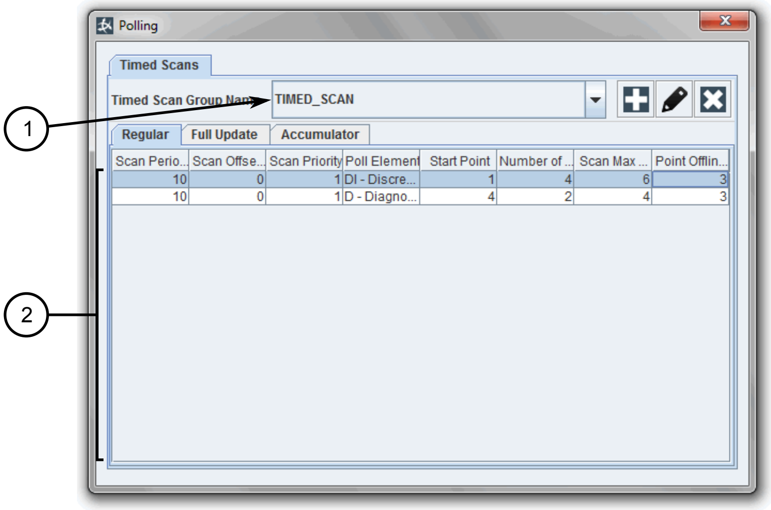
Parameter	Description
	The starting register associated with the poll element. The value must be less than or equal to the `Number of Points` parameter.
Number of Points	**Synopsis:** 0 to 65535 **Default:** 0 **NOTE** *This parameter is ignored when **Poll Element** is set to* `Exception Status Poll` *or* `Diagnostic Register Poll`. The number of registers associated with the poll element.

- **Accumulator Timed Scans**

Parameter	Description
Poll Element	**Synopsis:** **Default:** The poll element to use. Options include: ▫ `HR - Holding Register Poll` – Polls the RTU for holding register data (Modbus Read Holding Registers) ▫ `IR - Input Register Poll` – Polls the RTU for input register data (Modbus Read Input Registers)
Start Point	**Synopsis:** 0 to 65535 **Default:** 0 The starting register associated with the poll element. The value must be less than or equal to the `Number of Points` parameter.
Number of Points	**Synopsis:** 0 to 65535 **Default:** 0 The number of registers associated with the poll element.

›› Deleting a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 164: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Elements

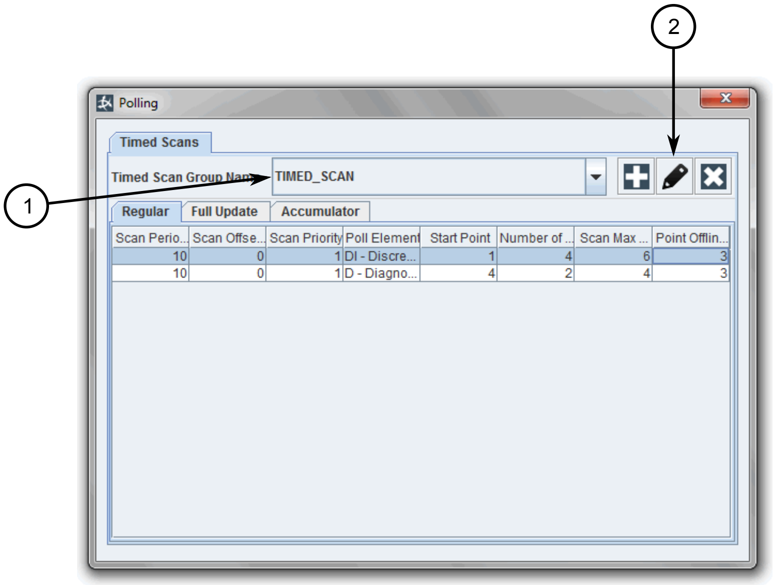
4. Select a group from the **Timed Scan Group Name** list.
5. Right-click the desired element to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the element, or click **No** to abort.

Section 4.11.2.4

Renaming a Timed Scan Group

To rename a timed scan group, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Scan Perio...	Scan Offse...	Scan Priority	Poll Element	Start Point	Number of ...	Scan Max ...	Point Offlin...
10	0	1	DI - Discre...	1	4	6	3
10	0	1	D - Diagno...	4	2	4	3

Figure 165: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Rename Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Rename** button and type a new name for the group.

Section 4.11.3

Managing Timed Scans for IEC 60870-5-101 Devices

This section describes how to configure and manage timed scans for IEC 60870-5-10 client devices in Maestro.

CONTENTS

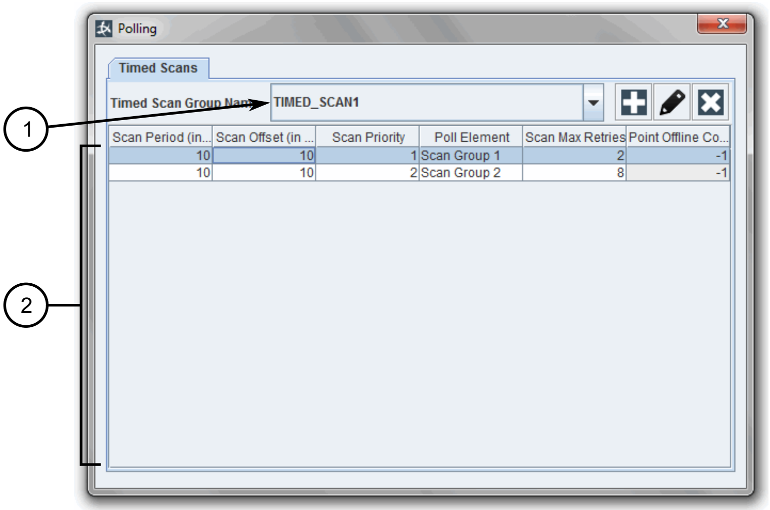
Section 4.11.3.1

Viewing a List of Timed Scans

To view timed scans defined for an IEC 60870-5-101 client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.

3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN1

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 166: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

4. Select a group from the **Timed Scan Group Name** list. The elements associated with the group appear in the table.

   If a group does not exist, add one. For more information, refer to Section 4.11.3.2, “Adding/Deleting a Timed Scan Group” .

   If an element does not exist, add one. For more information, refer to Section 4.11.3.3, “Adding/Deleting a Timed Scan Element” .

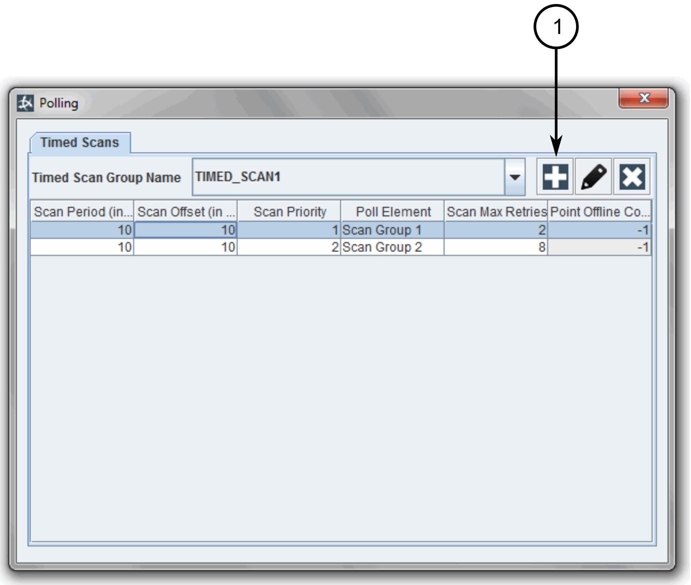
Section 4.11.3.2

Adding/Deleting a Timed Scan Group

To add/delete a timed scan group for an IEC 60870-5-101 client device, do the following:

›› Adding a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



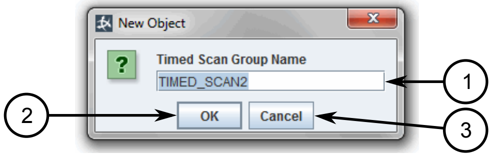
Timed Scan Group Name: TIMED_SCAN1

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 167: Polling Dialog Box – Timed Scans

1. Add Button

4. Click the **Add** button. The **New Object** dialog box appears.



Timed Scan Group Name: TIMED_SCAN2

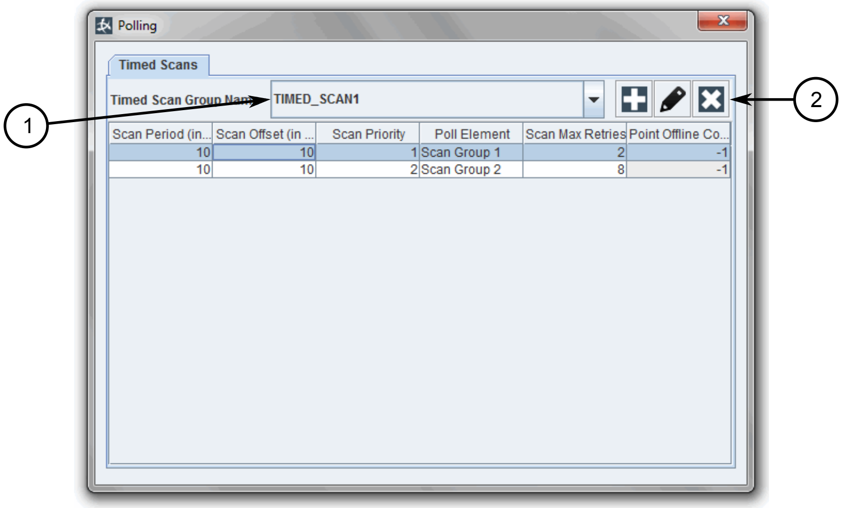
Figure 168: New Object Dialog Box

1. Timed Scan Group Name Box **2.** OK Button **3.** Cancel Button

5. [Optional] Type a new name for the group.
6. Click **OK** to add the group, or click **Cancel** to abort.

›› Deleting a Timed Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Name: TIMED_SCAN1

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 169: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Delete Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Delete** button. A confirmation dialog box appears.
6. Click **Yes** to delete the group, or click **No** to abort.

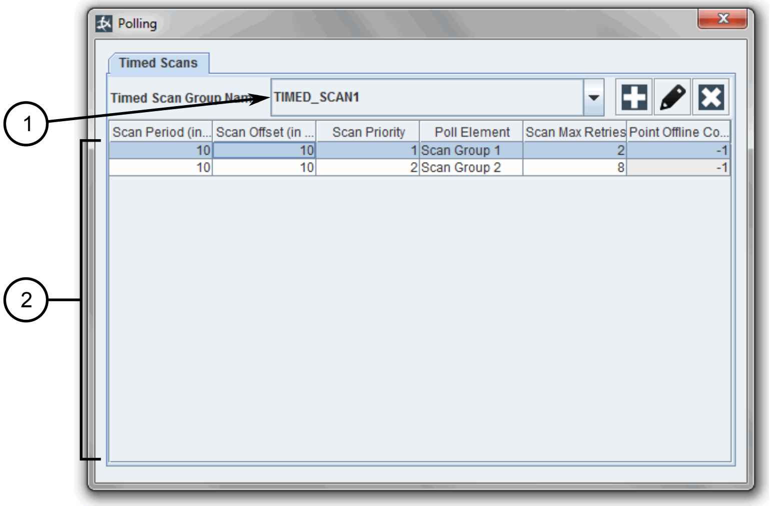
Section 4.11.3.3

Adding/Deleting a Timed Scan Element

To add/delete a timed scan element to a timed scan group for an IEC 60870-5-10 client device, do the following:

›› Adding a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Nam TIMED_SCAN1

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 170: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Poll Elements List

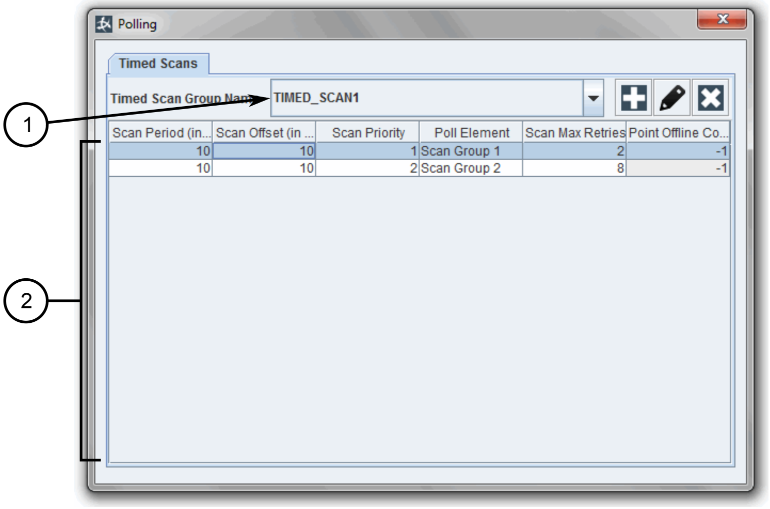
4. Select a group from the **Timed Scan Group Name** list.
5. Right-click anywhere in the elements area to open the shortcut menu and click **New**. A new poll element is added to the table.
6. Configure the following parameters as required:

Parameter	Description
Scan Period (in seconds)	**Synopsis:** 1 to 3600 **Default:** 10 The maximum duration in seconds (s) to scan an RTU for specific data.
Scan Offset (in seconds)	**Synopsis:** 0 to 3600 **Default:** 11 The time in seconds (s), applied on TIE startup, to wait before unblocking an RTU after reestablishing the connection.
Scan Priority	**Synopsis:** 0 to 64 **Default:** 1 The priority of the scan, where zero (0) is the highest priority.
Poll Element	**Synopsis:** Full Update, Scan Group 1, Scan Group 2, Scan Group 3, Scan Group 4, Scan Group 5, Scan Group 6, Scan Group 7, Scan Group 8, Scan Group 9, Scan Group 10, Scan Group 11, Scan Group 12, Scan Group 13, Scan Group 14, Scan Group 15, Scan Group 16, Time Synchronization The poll element to use.
Scan Max Retries	**Synopsis:** 0 to 10 **Default:** 3 The maximum number of times the scan can be retransmitted if a response is not received or corrupted.
Point Offline Count	**Synopsis:** -1, 1 to 10 **Default:** 3

Parameter	Description
	The number of times the scan can fail consecutively before the unreported points are considered off-line. **NOTE** *If scans for event Class data (Class 1, 2 or 3) fail, no points will be considered off-line regardless of the configured point off-line count value, as the points contained in a response cannot be predicted.*

Deleting a Timed Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Timed Scan Group Nam TIMED_SCAN1

Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 171: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Elements

4. Select a group from the **Timed Scan Group Name** list.
5. Right-click the desired element to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
6. Click **Yes** to delete the element, or click **No** to abort.

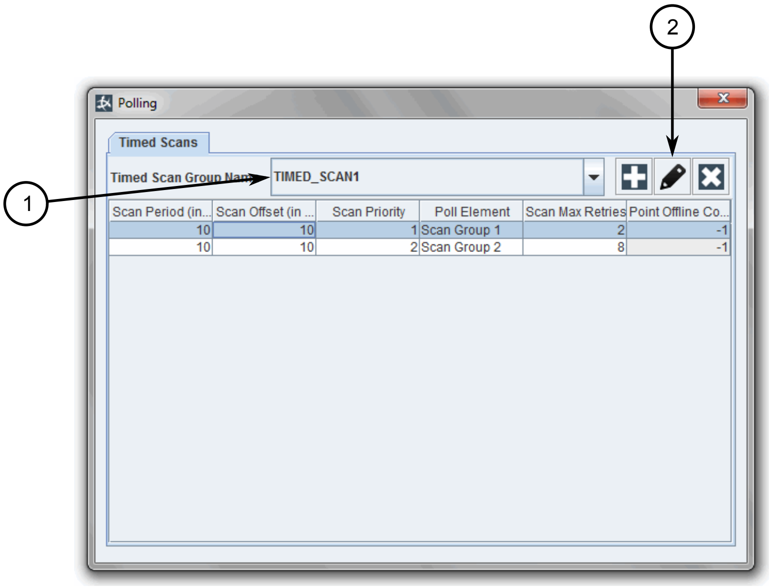
Section 4.11.3.4

Renaming a Timed Scan Group

To rename a timed scan group, do the following:

1. Navigate to the **Overview** screen.

2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears. The **Timed Scans** tab appears by default.



Scan Period (in...	Scan Offset (in ...	Scan Priority	Poll Element	Scan Max Retries	Point Offline Co...
10	10	1	Scan Group 1	2	-1
10	10	2	Scan Group 2	8	-1

Figure 172: Polling Dialog Box – Timed Scans

1. Timed Scan Group Name List **2.** Rename Button

4. Select a group from the **Timed Scan Group Name** list.
5. Click the **Rename** button and type a new name for the group.

Section 4.11.4

Managing Polling Schemes for DNP Devices

This section describes how to configure and manage polling schemes for DNP client devices in Maestro.

CONTENTS

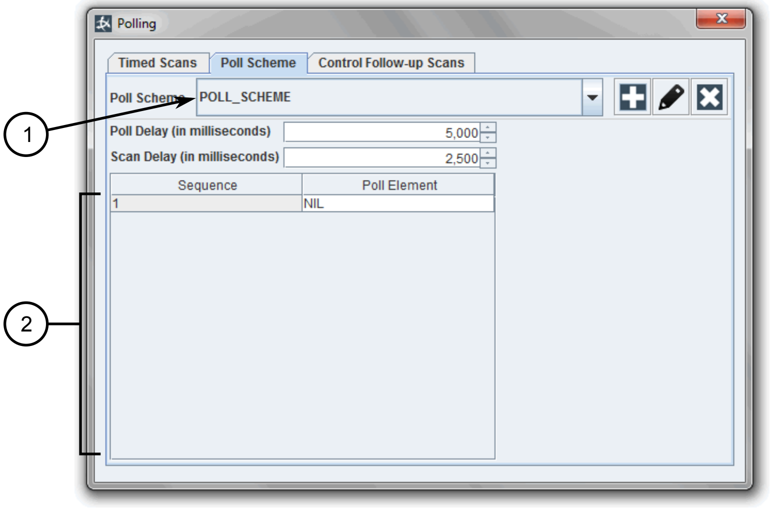
Section 4.11.4.1

Viewing a List of Polling Schemes

To view polling schemes defined for a DNP client device, do the following:

1. Navigate to the **Overview** screen.

2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.



Poll Scheme: POLL_SCHEME

Poll Delay (in milliseconds): 5,000

Scan Delay (in milliseconds): 2,500

Sequence	Poll Element
1	NIL

Figure 173: Polling Dialog Box – Poll Scheme

1. Poll Scheme List **2.** Elements

5. Select a group from the **Poll Scheme** list. The elements associated with the group appear in the table.

   If a group does not exist, add one. For more information, refer to Section 4.11.4.2, "Adding/Deleting a Polling Scheme Group" .

   If an element does not exist, add one. For more information, refer to Section 4.11.4.3, "Adding/Deleting a Polling Scheme Element" .

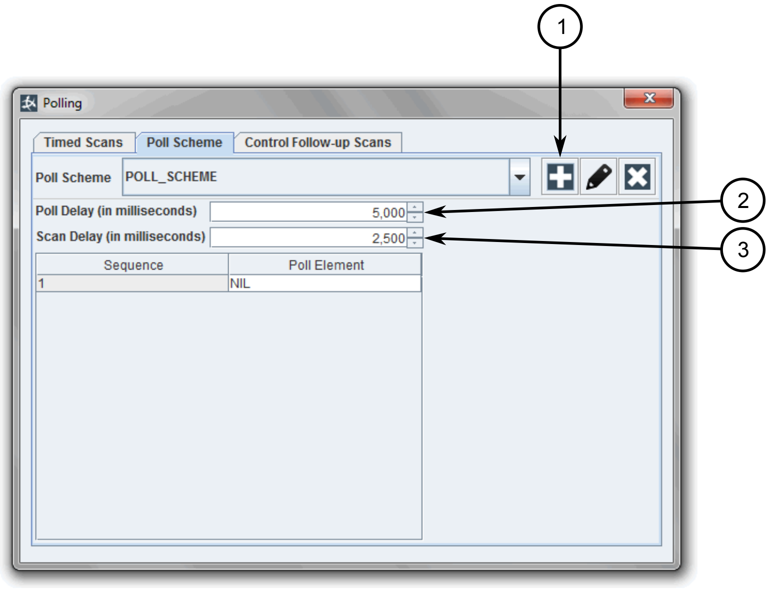
Section 4.11.4.2

Adding/Deleting a Polling Scheme Group

To add/delete a polling scheme group for a DNP client device, do the following:

›› Adding a Polling Scheme Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.



Poll Scheme POLL_SCHEME

Poll Delay (in milliseconds) 5,000

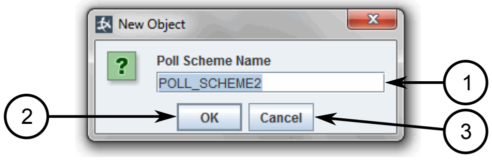
Scan Delay (in milliseconds) 2,500

Sequence	Poll Element
1	NIL

Figure 174: Polling Dialog Box – Poll Scheme

1. Add Button **2.** Poll Delay (In Milliseconds) Box **3.** Scan Delay (In Milliseconds) Box

5. Click the **Add** button. The **New Object** dialog box appears.



Poll Scheme Name POLL_SCHEME2

Figure 175: New Object Dialog Box

1. Poll Scheme Name Box **2.** OK Button **3.** Cancel Button

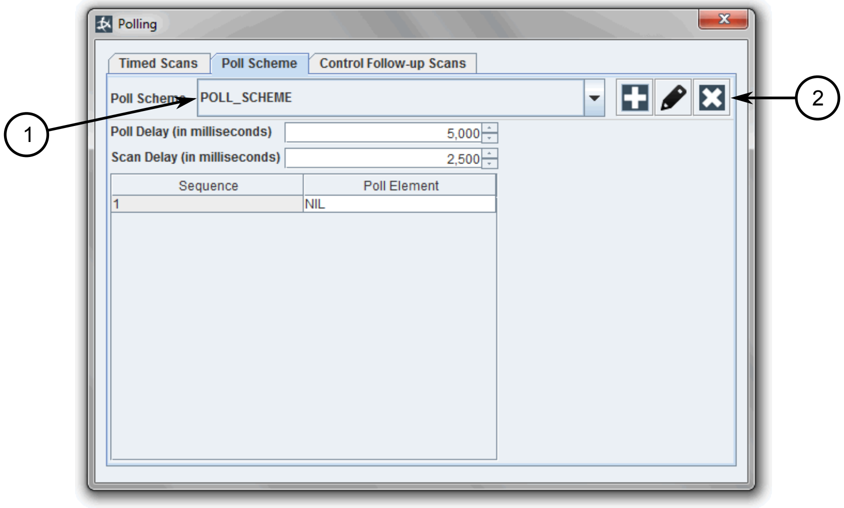
6. [Optional] Type a new name for the group.
7. Configure the following parameters as required:

Parameter	Description
Poll Delay (in milliseconds)	**Synopsis:** 1 to 86400000 **Default:** 5000 The time in milliseconds (ms) between the execution of each poll.
Scan Delay (in milliseconds)	**Synopsis:** 1 to 86400000 **Default:** 2500 The time in milliseconds (ms) to wait following the execution of the last poll in the polling scheme and the start of the next cycle.

8. Click **OK** to add the group, or click **Cancel** to abort.

Deleting a Polling Scheme Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.



Poll Scheme: POLL_SCHEME
Poll Delay (in milliseconds): 5,000
Scan Delay (in milliseconds): 2,500

Sequence	Poll Element
1	NIL

Figure 176: Polling Dialog Box – Poll Scheme

1. Poll Scheme List **2.** Delete Button

5. Select a group from the **Poll Scheme** list.
6. Click the **Delete** button. A confirmation dialog box appears.
7. Click **Yes** to delete the group, or click **No** to abort.

Section 4.11.4.3

Adding/Deleting a Polling Scheme Element

To add/delete a polling scheme element to a poll scheme group for a DNP client device, do the following:

Adding a Polling Scheme Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.

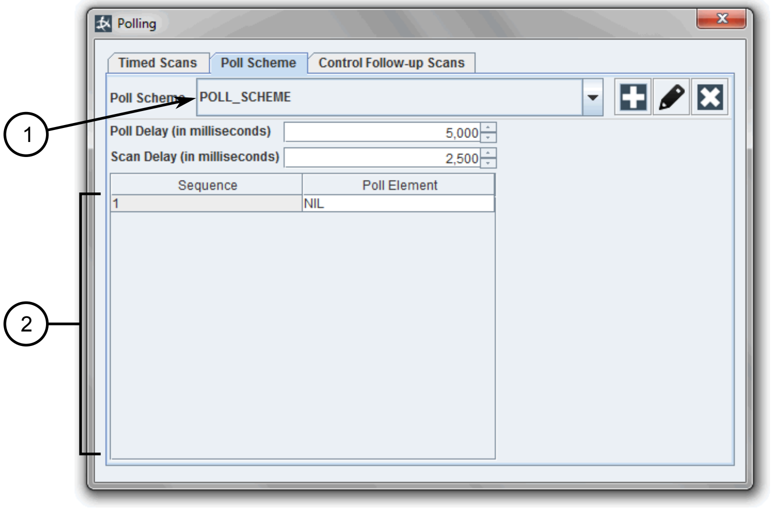


Figure 177: Polling Dialog Box – Poll Scheme

1. Poll Scheme List **2.** Elements

5. Select a group from the **Poll Scheme** list.

> **IMPORTANT!**
> *A new poll scheme element cannot be added if the last element in the sequence is **NIL**.*

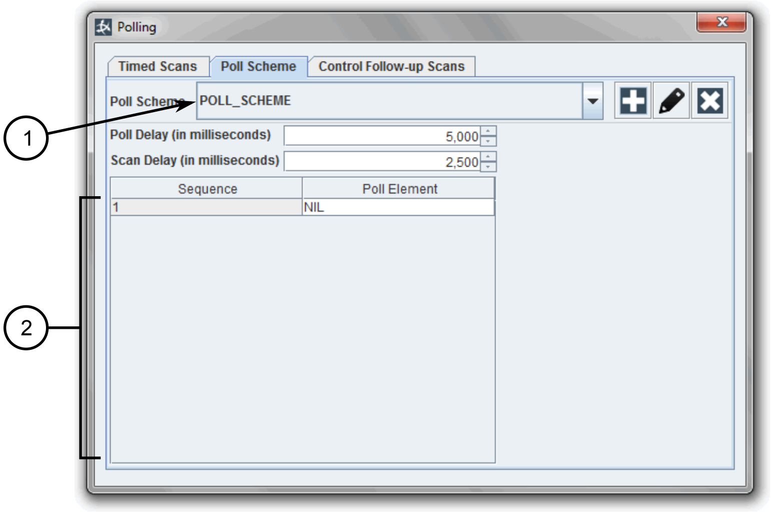
6. Right-click anywhere in the elements area to open the shortcut menu and click **New Poll Scheme Element**. A new poll element is added to the table.
7. Configure the following parameters as required:

Parameter	Description
Poll Element	The poll element to use. Options include: • `Analog Input Objects, variation 0 (All variations)` – Polls the RTU for all Analog Input Objects (object 30, variation 0) • `Analog Input Objects, variation 1 (32-bit)` – Polls the RTU for 32-bit Analog Input Objects (object 30, variation 1) • `Analog Input Objects, variation 2 (16-bit)` – Polls the RTU for 16-bit Analog Input Objects (object 30, variation 2) • `Analog Input Objects, variation 3 (32-bit without flags)` – Polls the RTU for 32-bit Analog Input Objects without flags objects (object 30, variation 3) • `Analog Input Objects, variation 4 (16-bit without flags)` – Polls the RTU for 16-bit Analog Input Objects without flags objects (object 30, variation 4) • `Floating Point Objects, variation 1 (Short)` – Polls the RTU for Short Floating Point Objects (object 100, variation 1) • `BCD Objects, variation 0 (All variations)` – Polls the RTU for Binary Coded Decimal Objects (object 101, variation 0)

Parameter	Description
	• `BCD Objects, variation 1 (Small-Packed BCD Objects)` – Polls the RTU for Small-Packed Binary Coded Decimal Objects (object 101, variation 1) • `BCD Objects, variation 2 (Medium Packed BCD Objects)` – Polls the RTU for Medium-Packed Binary Coded Decimal Objects (object 101, variation 2) • `Class Objects, variation 2 (Class 1)` – Polls the RTU for Class 1 Objects (object 60, variation 2) • `Class Objects, variation 3 (Class 2)` – Polls the RTU for Class 2 Objects (object 60, variation 3) • `Class Objects, variation 4 (Class 3)` – Polls the RTU for Class 3 Objects (object 60, variation 4) • `Running Binary Counter Object, variation 0 (All variations)` – Polls the RTU for all *Running* Binary Counter Objects (object 20, variation 0) • `Running Binary Counter Object, variation 1 (32-bit)` – Polls the RTU for *Running* 32-bit Binary Counter Objects (object 20, variation 1) • `Running Binary Counter Object, variation 2 (16-bit)` – Polls the RTU for *Running* 16-bit Binary Counter Objects (object 20, variation 2) • `Running Binary Counter Object, variation 5 (32-bit without flag)` – Polls the RTU for *Running* 32-bit Binary Counter without flag Objects (object 20, variation 5) • `Running Binary Counter Object, variation 6 (16-bit without flag)` – Polls the RTU for *Running* 16-bit Binary Counter without flag Objects (object 20, variation 6) • `NIL` – Do nothing (allows an RTU to be polled less often than other RTUs)

›› Deleting a Polling Scheme Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.



Poll Scheme POLL_SCHEME

Poll Delay (in milliseconds) 5,000

Scan Delay (in milliseconds) 2,500

Sequence	Poll Element
1	NIL

Figure 178: Polling Dialog Box – Poll Scheme

1. Poll Scheme List **2.** Elements

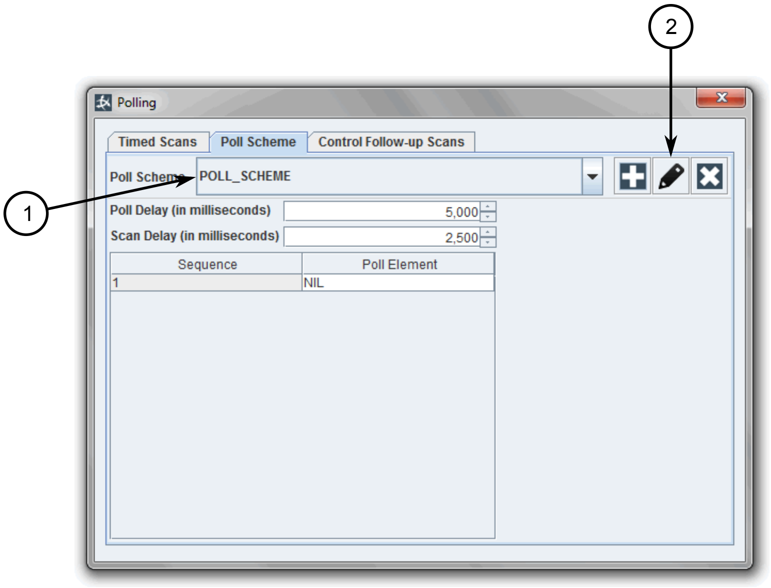
5. Select a group from the **Poll Scheme** list.
6. Right-click the desired element to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
7. Click **Yes** to delete the element, or click **No** to abort.

Section 4.11.4.4

Renaming a Polling Scheme Group

To rename a poll scheme group, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Poll Scheme** tab.



Poll Scheme: POLL_SCHEME

Poll Delay (in milliseconds): 5,000

Scan Delay (in milliseconds): 2,500

Figure 179: Polling Dialog Box – Poll Scheme

1. Poll Scheme List **2.** Rename Button

5. Select a group from the **Poll Scheme** list.
6. Click the **Rename** button and type a new name for the group.

Section 4.11.5

Managing Control Follow Up Scans

Control follow up scans define which data to poll after a control is issued for an RTU.

CONTENTS

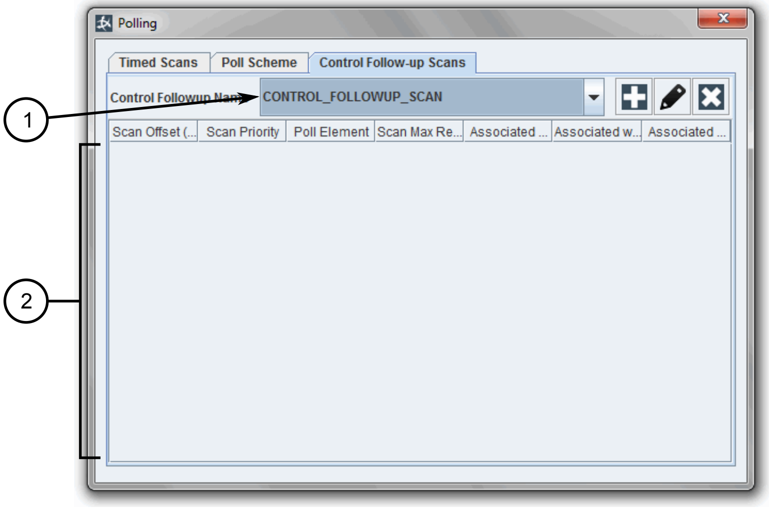
Section 4.11.5.1

Viewing a List of Control Follow Up Scans

To view control follow up scans defined for a DNP client device, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.

3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.



Control Followup Nam CONTROL_FOLLOWUP_SCAN

Figure 180: Polling Dialog Box – Control Follow-Up Scans

1. Control Followup Name List **2.** Elements

5. Select a group from the **Control Followup Name** list. The elements associated with the group appear in the table.

   If a group does not exist, add one. For more information, refer to Section 4.11.5.2, "Adding/Deleting a Control Follow-Up Scan Group" .

   If an element does not exist, add one. For more information, refer to Section 4.11.5.3, "Adding/Deleting a Control Follow Up Element" .

Section 4.11.5.2

Adding/Deleting a Control Follow-Up Scan Group

To add/delete a control follow-up scan group for a DNP client device, do the following:

›› Adding a Control Follow-Up Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.

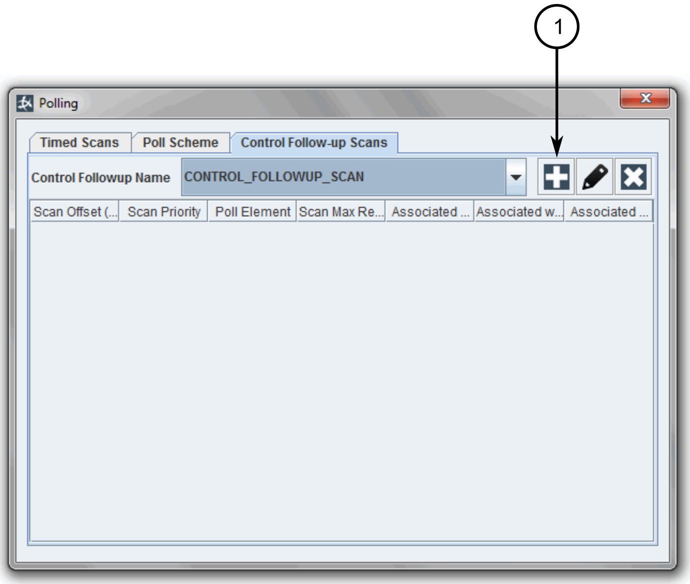


Figure 181: Polling Dialog Box – Control Follow-Up Scans

1. Add Button

5. Click the **Add** button. The **New Object** dialog box appears.

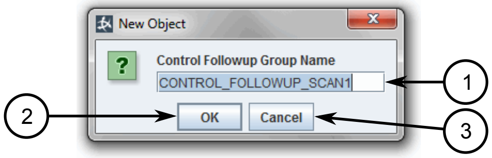


Figure 182: New Object Dialog Box

1. Control Followup Group Name Box **2.** OK Button **3.** Cancel Button

6. [Optional] Type a new name for the group.
7. Click **OK** to add the group, or click **Cancel** to abort.

›› Deleting a Control Follow-Up Scan Group

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.

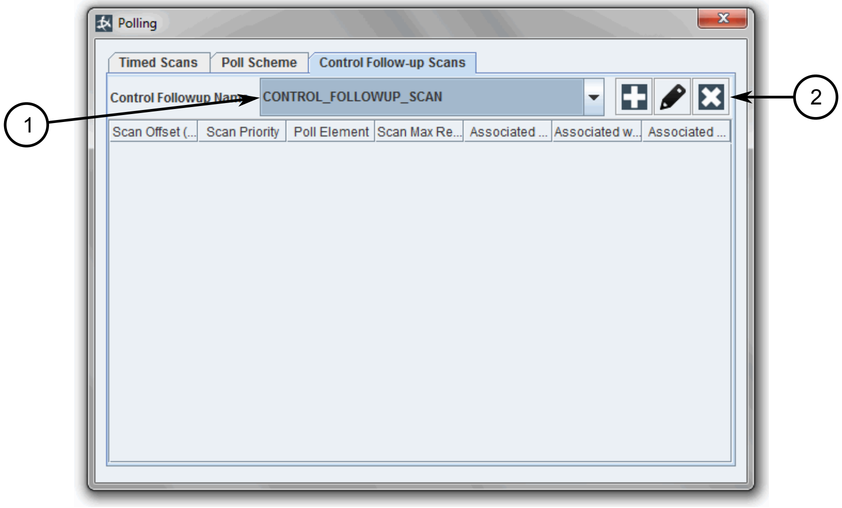


Figure 183: Polling Dialog Box – Control Follow-Up Scans

1. Control Followup Name List **2.** Delete Button

5. Select a group from the **Control Followup Name** list.
6. Click the **Delete** button. A confirmation dialog box appears.
7. Click **Yes** to delete the group, or click **No** to abort.

Section 4.11.5.3

Adding/Deleting a Control Follow Up Element

To add/delete a control follow-up scan element to a control follow-up scan group for a DNP client device, do the following:

›› Adding a Control Follow-Up Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.

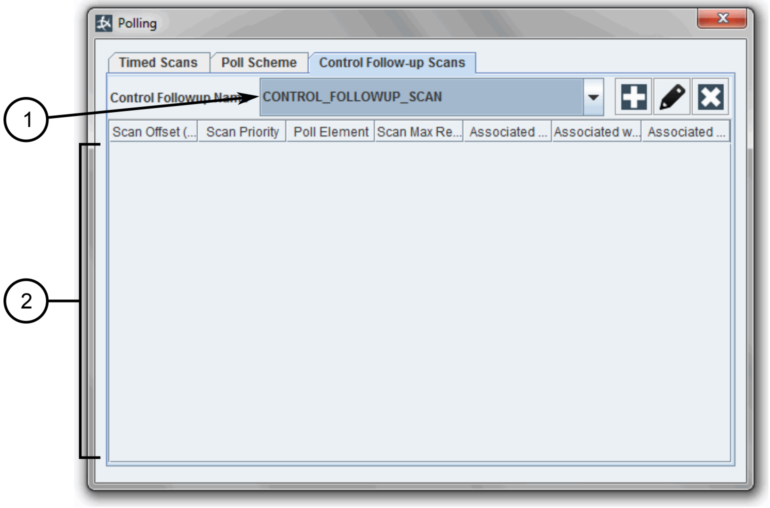


Figure 184: Polling Dialog Box – Control Follow-Up Scans

1. Control Followup Name **2.** Elements

5. Select a group from the **Control Followup Name** list.
6. Right-click anywhere in the elements area to open the shortcut menu and click **New**. A new poll element is added to the table.
7. Configure the following parameters as required:

Parameter	Description
Scan Offset (in seconds)	**Synopsis:** 0 to 3600 **Default:** 11 The time in seconds (s) to wait after a control command is issued before the TIE remote interface can execute the scan.
Scan Priority	**Synopsis:** 0 to 64 **Default:** 1 The priority of the scan, where zero (0) is the highest priority.
Poll Element	The poll element to use. Options include: • `Analog Input Objects, variation 0 (All variations)` – Polls the RTU for all Analog Input Objects (object 30, variation 0) • `Analog Input Objects, variation 1 (32-bit)` – Polls the RTU for 32-bit Analog Input Objects (object 30, variation 1) • `Analog Input Objects, variation 2 (16-bit)` – Polls the RTU for 16-bit Analog Input Objects (object 30, variation 2) • `Analog Input Objects, variation 3 (32-bit without flags)` – Polls the RTU for 32-bit Analog Input Objects without flags objects (object 30, variation 3) • `Analog Input Objects, variation 4 (16-bit without flags)` – Polls the RTU for 16-bit Analog Input Objects without flags objects (object 30, variation 4)

Parameter	Description
	• `Floating Point Objects, variation 1 (Short)` – Polls the RTU for Short Floating Point Objects (object 100, variation 1) • `BCD Objects, variation 0 (All variations)` – Polls the RTU for Binary Coded Decimal Objects (object 101, variation 0) • `BCD Objects, variation 1 (Small-Packed BCD Objects)` – Polls the RTU for Small-Packed Binary Coded Decimal Objects (object 101, variation 1) • `BCD Objects, variation 2 (Medium Packed BCD Objects)` – Polls the RTU for Medium-Packed Binary Coded Decimal Objects (object 101, variation 2) • `Class Objects, variation 2 (Class 1)` – Polls the RTU for Class 1 Objects (object 60, variation 2) • `Class Objects, variation 3 (Class 2)` – Polls the RTU for Class 2 Objects (object 60, variation 3) • `Class Objects, variation 4 (Class 3)` – Polls the RTU for Class 3 Objects (object 60, variation 4) • `Running Binary Counter Object, variation 0 (All variations)` – Polls the RTU for all *Running* Binary Counter Objects (object 20, variation 0) • `Running Binary Counter Object, variation 1 (32-bit)` – Polls the RTU for *Running* 32-bit Binary Counter Objects (object 20, variation 1) • `Running Binary Counter Object, variation 2 (16-bit)` – Polls the RTU for *Running* 16-bit Binary Counter Objects (object 20, variation 2) • `Running Binary Counter Object, variation 5 (32-bit without flag)` – Polls the RTU for *Running* 32-bit Binary Counter without flag Objects (object 20, variation 5) • `Running Binary Counter Object, variation 6 (16-bit without flag)` – Polls the RTU for *Running* 16-bit Binary Counter without flag Objects (object 20, variation 6) • `Full Update` – Polls the RTU for full update • `Time Synchronization` – Periodically synchronizes a DNP RTU's time
Scan Max Retries	**Synopsis:** 0 to 10 **Default:** 3 The maximum number of times the scan can be retransmitted if a response is not received or corrupted.
Associated with Digital Control	**Default State:** Disabled When enabled (selected), the scan is sent after Digital Control.
Associated with Analog Control	**Default State:** Disabled When enabled (selected), the scan is sent after Analog Control.
Associated with Pulse Control	**Default State:** Disabled When enabled (selected), the scan is sent after Pulse Control.

›› Deleting a Control Follow-Up Scan Element

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.

3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.

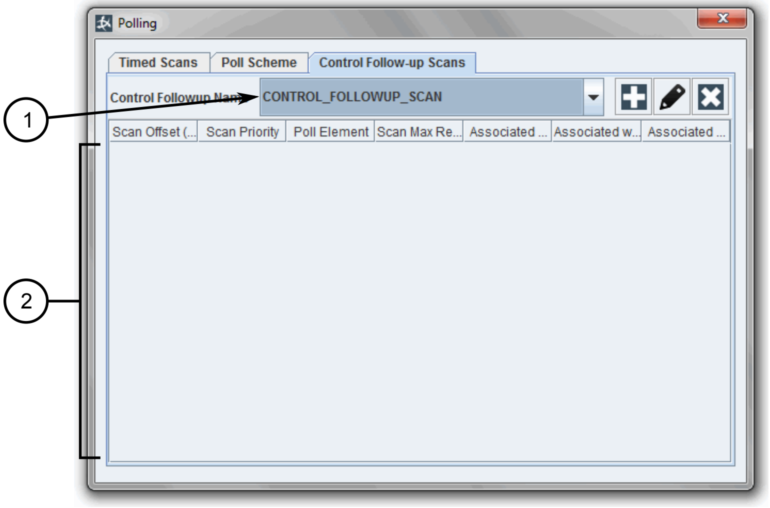


Figure 185: Polling Dialog Box – Control Follow-Up Scans

1. Control Followup Name **2.** Elements

5. Select a group from the **Control Followup Name** list.
6. Right-click the desired element to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
7. Click **Yes** to delete the element, or click **No** to abort.

Section 4.11.5.4

Renaming a Control Follow Up Scan Group

To rename a control follow up scan group, do the following:

1. Navigate to the **Overview** screen.
2. Right-click the client device to open the shortcut menu and click **Properties**. The device's properties appear in a new tab.
3. Click **Edit Polling Templates**. The **Polling** dialog box appears.
4. Click the **Control Follow-Up Scans** tab.

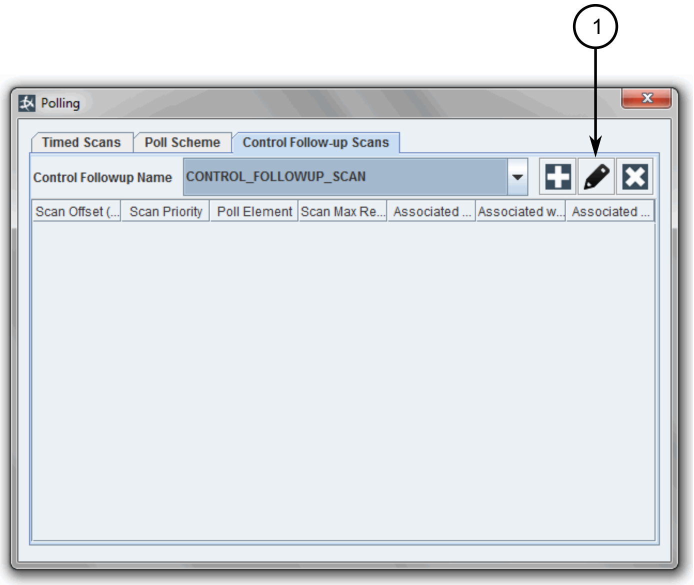


Figure 186: Polling Dialog Box – Control Follow-Up Scans

1. Control Followup Name List **2.** Rename Button

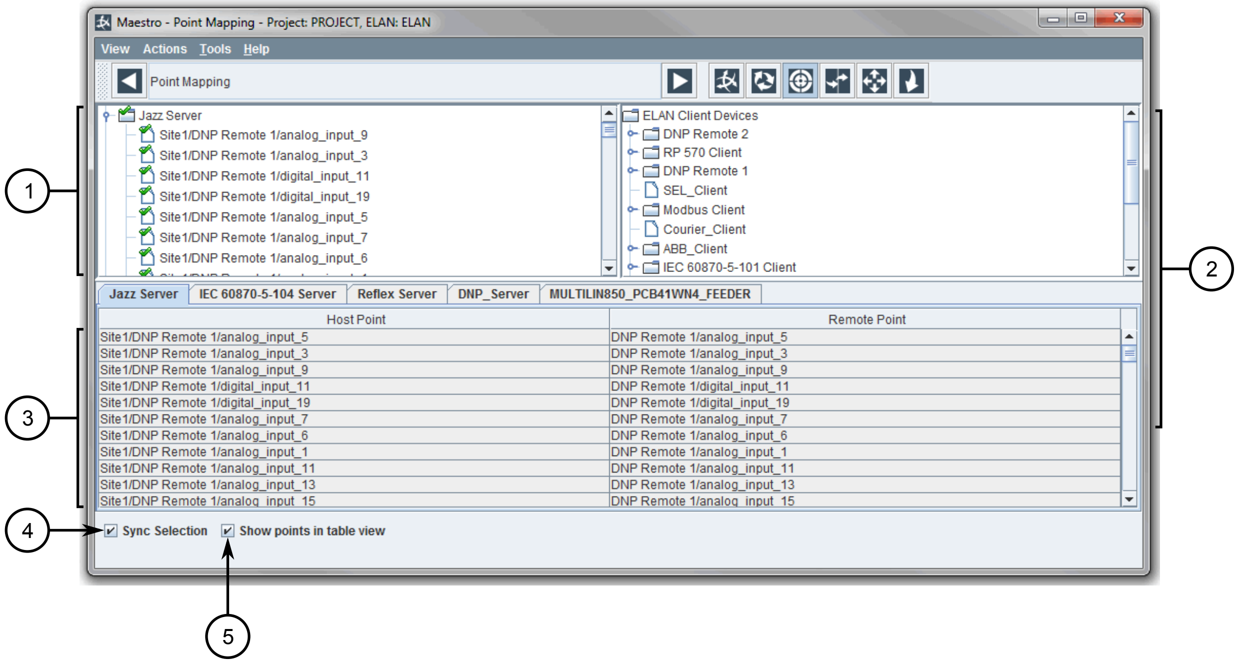
5. Select a group from the **Control Followup Name** list.
6. Click the **Rename** button and type a new name for the group.

Section 4.12

Mapping Points

The **Point Mapping** screen allows users to manage mappings between points for server and client devices. The screen is divided into three sections:

- **Server Devices** – The top left pane lists the server devices and their associated points.
- **Client Devices** – The top right pane lists the client devices and their associated points.
- **Mapped Points** – The bottom pane lists the server and client points that have been mapped together.


Maestro - Point Mapping - Project: PROJECT, ELAN: ELAN
View
Actions
Tools
Help
Point Mapping
Jazz Server
Site1/DNP Remote 1/analog_input_9
Site1/DNP Remote 1/analog_input_3
Site1/DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6
ELAN Client Devices
DNP Remote 2
RP 570 Client
DNP Remote 1
SEL_Client
Modbus Client
Courier_Client
ABB_Client
IEC 60870-5-101 Client
Jazz Server
IEC 60870-5-104 Server
Reflex Server
DNP_Server
MULTILIN850_PCB41WN4_FEEDER
1
2
3
4
5

Host Point	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/digital_input_11	DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19	DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15

☑ Sync Selection ☑ Show points in table view

Figure 187: Point Mapping Screen

1. Server Devices and Points **2.** Client Devices and Points **3.** Mapped Points **4.** Sync Selection Check Box **5.** Show Points in Table View Check Box

Devices and points displayed in the top panes each have a special icon to indicate their current status.

✓	The point mapping is correct.
STOP	The point mapping is incorrect.
⚠	A point is defined, but it is not mapped to a corresponding point for a client device.

NOTE
*If devices and/or points are missing from the **Points Mapping** screen, add them. For more information, refer to either Section 4.9, “Managing Server Devices” or Section 4.10, “Managing Client Devices” .*

CONTENTS

Section 4.12.1

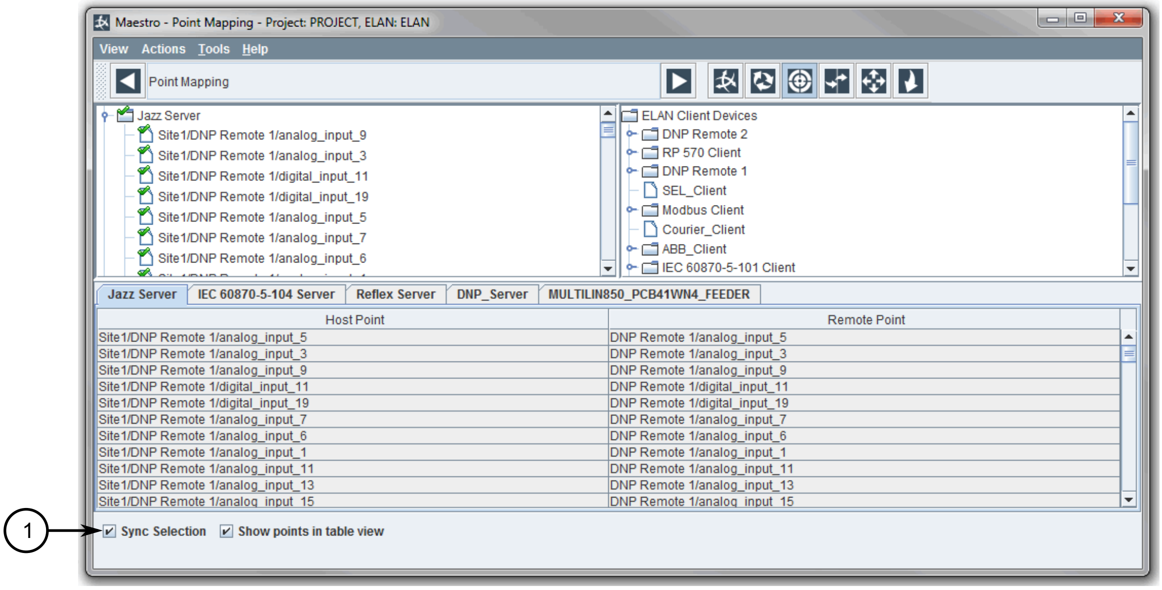
Mapping Server and Client Points

To map server and client points together, do either of the following:

> **NOTE**
> *A server point can only be mapped to a single client point.*

Traditional Method

1. Navigate to the **Point Mapping** screen.
2. Clear the **Sync Selection** check box.


Maestro - Point Mapping - Project: PROJECT, ELAN: ELAN
View
Actions
Tools
Help
Point Mapping
Jazz Server
Site1/DNP Remote 1/analog_input_9
Site1/DNP Remote 1/analog_input_3
Site1/DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6
ELAN Client Devices
DNP Remote 2
RP 570 Client
DNP Remote 1
SEL_Client
Modbus Client
Courier_Client
ABB_Client
IEC 60870-5-101 Client
Jazz Server
IEC 60870-5-104 Server
Reflex Server
DNP_Server
MULTILIN850_PCB41WN4_FEEDER
1

Host Point	Remote Point
Site1/DNP Remote 1/analog_input_5	DNP Remote 1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/digital_input_11	DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19	DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15

☑ Sync Selection ☑ Show points in table view

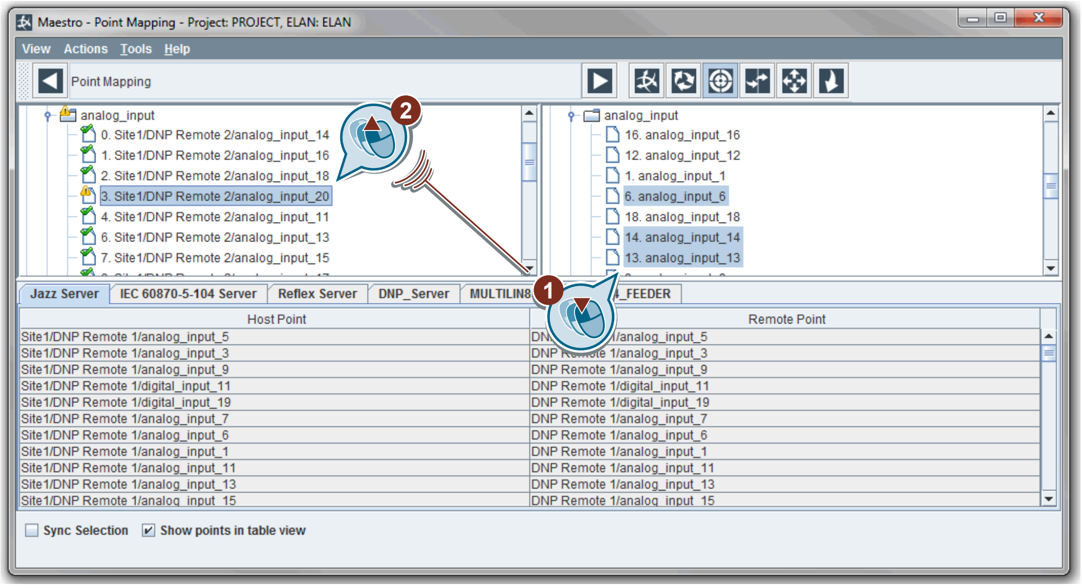
Figure 188: Point Mapping Screen

1. Sync Selection Check Box

3. Select a single point for a client device.
4. Select one or more points for a server device.
5. Right-click any of the selected points to open the shortcut menu and click **Create Mapping**. The point for the client point is mapped to the selected point(s) for the server device.
6. For IEC 61850 servers and clients only, if Maestro detects one of the selected points has a Data attribute with a type identifier of *dbpos*, or *dual-bit position*, a confirmation dialog box appears. Click either **Yes** or **No**.
   - **Yes** – Two consecutive points are created on the server side and mapped to the corresponding bits of the dual-bit position Data attribute
   - **No** – The point is mapped as a digital output on the server side

Drag and Drop Method

1. Navigate to the **Point Mapping** screen.



analog_input
- 0. Site1/DNP Remote 2/analog_input_14
- 1. Site1/DNP Remote 2/analog_input_16
- 2. Site1/DNP Remote 2/analog_input_18
- 3. Site1/DNP Remote 2/analog_input_20
- 4. Site1/DNP Remote 2/analog_input_11
- 6. Site1/DNP Remote 2/analog_input_13
- 7. Site1/DNP Remote 2/analog_input_15

analog_input
- 16. analog_input_16
- 12. analog_input_12
- 1. analog_input_1
- 6. analog_input_6
- 18. analog_input_18
- 14. analog_input_14
- 13. analog_input_13

Host Point	Remote Point
Site1/DNP Remote 1/analog_input_5	DN[illegible]1/analog_input_5
Site1/DNP Remote 1/analog_input_3	DNP Remote 1/analog_input_3
Site1/DNP Remote 1/analog_input_9	DNP Remote 1/analog_input_9
Site1/DNP Remote 1/digital_input_11	DNP Remote 1/digital_input_11
Site1/DNP Remote 1/digital_input_19	DNP Remote 1/digital_input_19
Site1/DNP Remote 1/analog_input_7	DNP Remote 1/analog_input_7
Site1/DNP Remote 1/analog_input_6	DNP Remote 1/analog_input_6
Site1/DNP Remote 1/analog_input_1	DNP Remote 1/analog_input_1
Site1/DNP Remote 1/analog_input_11	DNP Remote 1/analog_input_11
Site1/DNP Remote 1/analog_input_13	DNP Remote 1/analog_input_13
Site1/DNP Remote 1/analog_input_15	DNP Remote 1/analog_input_15

☐ Sync Selection ☑ Show points in table view

Figure 189: Point Mapping Screen

2. Expand the devices in the server and client device panes to reveal the points that will be mapped.
3. Select one or more points for the server device and drag them over the point for the client device. The unmapped point for the client device is now mapped to the point(s) for the server device.
4. If Maestro detects one of the selected points has a type identifier of *Double Point*, a confirmation dialog box appears. Click either **Yes** or **No**.
   - **Yes** – Two consecutive points are created on the server side and mapped to the corresponding bits of the dual-bit position Data attribute
   - **No** – The point is mapped as a digital output on the server side

Section 4.12.2

Deleting an Existing Mapping

To delete the mapping between two points, do the following:

1. Navigate to the **Point Mapping** screen.
2. Right-click a mapped point for a server device to open the shortcut menu and click **Remote TIE Mapping**. A confirmation dialog box appears.
3. Click **OK** to remove the mapping, or click **Cancel** to abort.
4. [Optional] Delete the unmapped point. For more information, refer to Section 4.12.3, “Deleting Unmapped Points” .

Section 4.12.3

Deleting Unmapped Points

To delete a point for a server device that is not mapped to a point for a client device, do the following:

›› Deleting a Single Unmapped Point or Selectively Deleting Multiple Unmapped Points

1. Navigate to the **Point Mapping** screen.
2. Expand the server point that contains the unmapped point(s).
3. Right-click one or more unmapped points to open the shortcut menu and click **Delete Unmapped Point**. The point(s) is removed from the list.

›› Deleting All Unmapped Points From One or More Server Devices

1. Navigate to the **Point Mapping** screen.
2. Right-click one or more server devices that contain unmapped points to open the shortcut menu and click **Delete Unmapped Point**. All unmapped points associated to the selected server device(s) are removed from the list.

Section 4.12.4

Pairing/Unpairing Control Points (IEC 61850 Client Devices Only)

Control points for an IEC 61850 client device can be paired together to act as a *trip/close pair*, where one point acts as the *trip* point and the other the *close* point.

- *Trip* points send a value of *0* by default to the end device when issued a **`trip`** command, and forward all **`close`** commands to the *close* point
- *Close* points send a value of *1* by default to the end device

> **NOTE**
> *Custom values can be switched if needed.*

CONTENTS

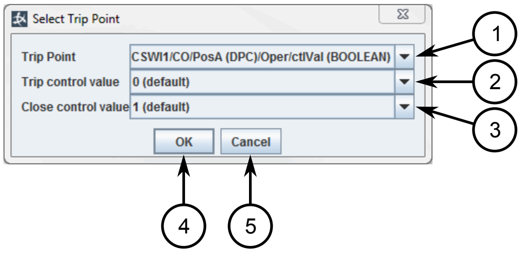
Section 4.12.4.1

Pairing Points

To pair two control points, do the following:

> **IMPORTANT!**
> *Control points can only be paired together if they belong to the same IEC 61850 client device and are not paired with any other control points.*

1. Make sure an IEC 61850 client device is configured. For more information, refer to Section 4.10.10, “Managing IEC 61850 Client Devices” .
2. Navigate to the **Point Mapping** screen.
3. In the right column under **ELAN Client Devices**, locate and expand the IEC 61850 client device until the desired control points (*ctVal*) are found.
4. Hold **Ctrl** and select both control points.
5. Right-click one of the points to open the shortcut menu and click **Create Trip/Close Pair**. The **Select Trip Point** dialog box appears.



Select Trip Point

Trip Point: CSWI1/CO/PosA (DPC)/Oper/ctlVal (BOOLEAN)
Trip control value: 0 (default)
Close control value: 1 (default)

Figure 190: Select Trip Point Dialog Box

1. Trip Point List **2.** Trip Control Value List **3.** Close Control Value List **4.** OK Button **5.** Cancel Button

6. Configure the following parameters as required:

Parameter	Description
Trip Point	The control point assigned to be the *trip* point.
Trip Control Value	**Synopsis:** 0, 1 **Default:** 0 The value at which the device trips.
Close Control Value	**Synopsis:** 0, 1 **Default:** 1 The value at which the device closes.

7. Click **OK**. The control points are now prefixed with ** (e.g. ** ctVal)

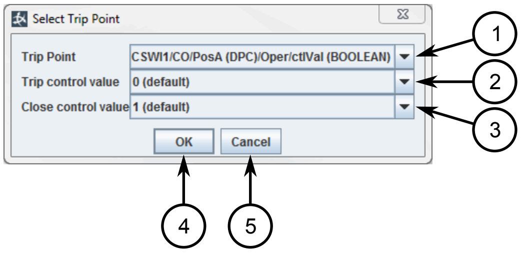
Section 4.12.4.2

Modifying an Existing Trip/Close Pair

To change which point is the *trip* point and which is the *close*, do the following:

1. Navigate to the **Point Mapping** screen.
2. In the right column under **ELAN Client Devices**, locate and expand the IEC 61850 client device until one of the desired control points (*ctVal*) is found.
3. Right-click one of the control points in the *trip/close* pair and then click **Configure Trip/Close Pairing**.

4. Right-click one of the points to open the shortcut menu and click **Configure Trip/Close Pairing**. The **Select Trip Point** dialog box appears.



Trip Point: CSWI1/CO/PosA (DPC)/Oper/ctlVal (BOOLEAN)
Trip control value: 0 (default)
Close control value: 1 (default)

Figure 191: Select Trip Point Dialog Box

1. Trip Point List **2.** Trip Control Value List **3.** Close Control Value List **4.** OK Button **5.** Cancel Button

5. Configure the following parameters as required:

Parameter	Description
Trip Point	The control point assigned to be the *trip* point.
Trip Control Value	**Synopsis:** 0, 1 **Default:** 0 The value at which the device trips.
Close Control Value	**Synopsis:** 0, 1 **Default:** 1 The value at which the device closes.

6. Click **OK**. The control points are now prefixed with ** (e.g. ** ctVal)

Section 4.12.4.3

Unpairing Points

To unpair a set of control points, do the following:

1. Navigate to the **Point Mapping** screen.
2. In the right column under **ELAN Client Devices**, locate and expand the IEC 61850 client device until the desired trip/close pair is found.
3. Hold **Ctrl** and select both control points.
4. Right-click one of the points to open the shortcut menu and click **Remove Trip/Close Pairing**. A confirmation dialog box appears.
5. Click **OK**.

Section 4.13

Managing the IEC 101-104 Gateway

This section describes how to configure and manage a gateway between IEC 60870-5-101 client devices and IEC 60870-5-104 server devices.

CONTENTS

Section 4.13.1

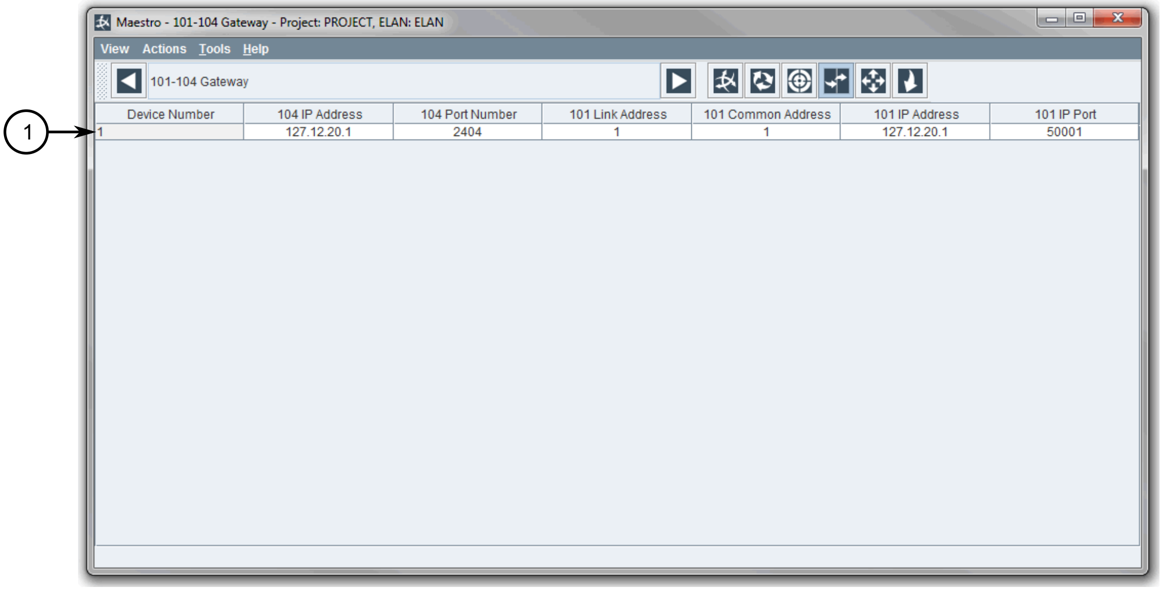
Adding/Deleting the IEC 101-104 Gateway

To add or delete the IEC 101-104 gateway, do the following:

IMPORTANT!
Only one gateway can be configured at a time.

›› Adding a Gateway

1. Navigate to the **101-104 Gateway** screen.
2. Right-click anywhere under the table heading row to open the shortcut menu and click **Insert Gateway Row**. A new row is added detailing the new gateway.



Device Number	104 IP Address	104 Port Number	101 Link Address	101 Common Address	101 IP Address	101 IP Port
1	127.12.20.1	2404	1	1	127.12.20.1	50001

Figure 192: 101-104 Gateway Screen

1. Gateway

3. Configure the gateway. For more information, refer to Section 4.13.2, “Configuring the IEC 101-104 Gateway” .

Deleting a Gateway

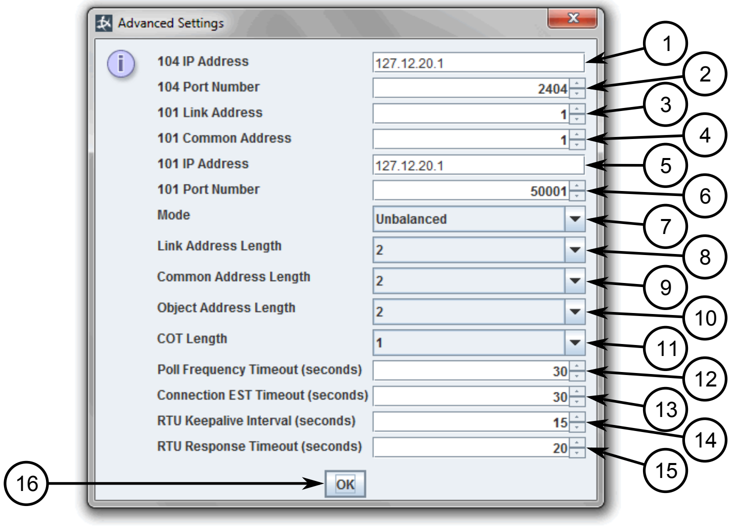
1. Navigate to the **101-104 Gateway** screen.
2. Right-click the gateway and click **Delete Gateway Row**. A confirmation message appears.
3. Click **OK** to confirm, or click **Cancel** to abort.

Section 4.13.2

Configuring the IEC 101-104 Gateway

To configure the IEC 101-104 gateway, do the following:

1. Navigate to the **101-104 Gateway** screen.
2. Right-click the desired gateway and click **Properties**. The **Advanced Settings** dialog box appears.



Advanced Settings

104 IP Address: 127.12.20.1
104 Port Number: 2404
101 Link Address: 1
101 Common Address: 1
101 IP Address: 127.12.20.1
101 Port Number: 50001
Mode: Unbalanced
Link Address Length: 2
Common Address Length: 2
Object Address Length: 2
COT Length: 1
Poll Frequency Timeout (seconds): 30
Connection EST Timeout (seconds): 30
RTU Keepalive Interval (seconds): 15
RTU Response Timeout (seconds): 20

Figure 193: Advanced Settings Dialog Box

1. 104 IP Address Box **2.** 104 Port Number Box **3.** 101 Link Address Box **4.** 101 Common Address Box **5.** 101 IP Address Box **6.** 101 Port Number Box **7.** Mode Box **8.** Link Address Length Box **9.** Common Address Length Box **10.** Object Address Length Box **11.** COT Length Box **12.** Poll Frequency Timeout Box **13.** Connector EST Timeout Box **14.** RTU Keepalive Interval Box **15.** RTU Response Timeout Box **16.** OK Button

3. Configure the following parameters as required:

Parameter	Description
104 IP Address	The gateway's IPv4 address. Configure the IEC 104 server side of the IEC 101-104 gateway to listen to this address.
104 Port Number	**Synopsis:** 1 to 65535 **Default:** 2404

Parameter	Description
	The TCP/IP port number. Configure the IEC 104 server side of the IEC 101-104 gateway to listen to this port.
101 Link Address	**Synopsis:** 1 to 65535 **Default:** 1 The IEC 101 RTU's link address.
101 Common Address	**Synopsis:** 1 to 65535 **Default:** 1 The IEC 101 RTU's common ASDU (Application Service Data Unit) address.
101 IP Address	The IP address for the gateway's IEC 101 terminal server used for access IEC 101 devices.
101 Port Number	**Synopsis:** 1 to 65535 **Default:** 50001 The TCP/IP port number for the terminal server to use when connecting an IEC 101 RTU.
Mode	**Synopsis:** Balanced, Unbalanced **Default:** Unbalanced The IEC 101 RTU's mode. Options include: • `Balanced` – Prevents ELAN from polling the RTU for class data if the RTU is sending spontaneous messages • `Unbalanced` – Allows ELAN to poll the RTU for class data, even if the RTU is sending spontaneous messages
Link Address Length	**Synopsis:** 0, 1, 2 **Default:** 2 The length in bytes of the IEC 101 RTU's link address.
Common Address Length	**Synopsis:** 1, 2 **Default:** 2 The length in bytes of the IEC 101 RTU's common address.
Object Address Length	**Synopsis:** 1, 2, 3 **Default:** 2 The length in bytes of the IEC 101 RTU's information object address.
COT Length	**Synopsis:** 1, 2, 3 **Default:** 1 The length in bytes of the IEC 101 RTU's Cause of Transmission (COT) address.
Poll Frequency Timeout (seconds)	**Synopsis:** 0 to 300 **Default:** 30 The IEC 101 Class 2 poll frequency in seconds (s)
Connection EST Timeout (seconds)	The time in seconds (s) to wait before trying again to establish a connection with the IEC 101 RTU.
RTU Keepalive Interval (seconds)	The interval in seconds (s) at which to send keepalive messages to the IEC 101 RTU.
RTU Response Timeout (seconds)	The time in seconds (s) to wait for a response from the IEC 101 RTU after sending a keepalive message.

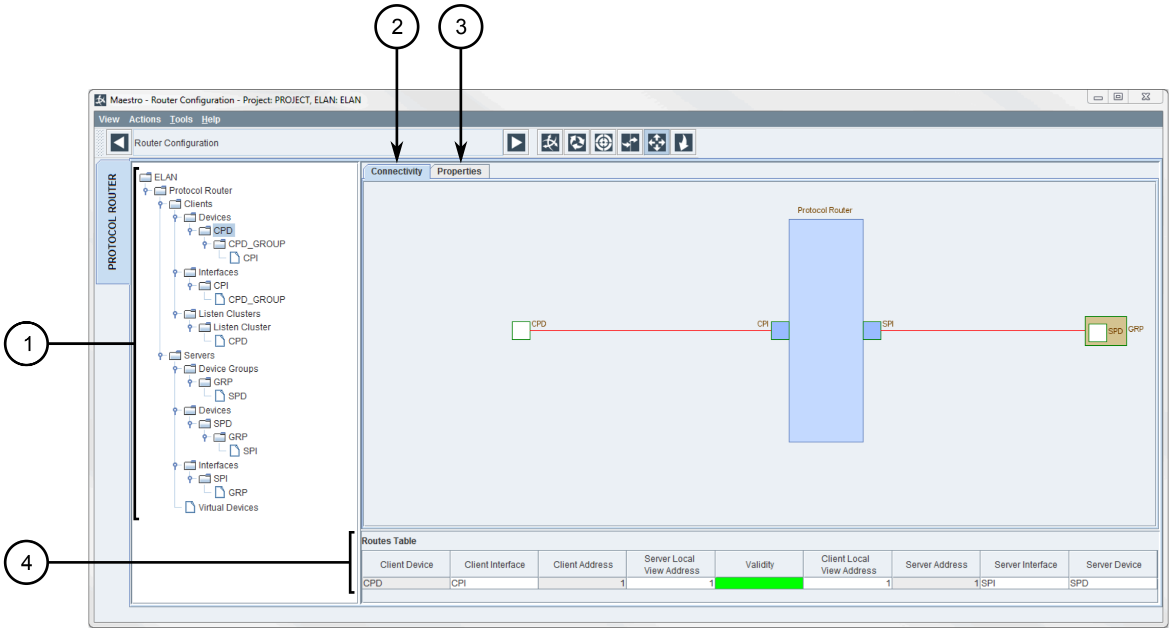
4. Click **OK**.

Section 4.14

Managing Protocol Routes

To help manage SCADA communications over complex network hierarchies, a Protocol Router can be configured for each RUGGEDCOM ELAN server. The Protocol Router manages SCADA protocol packets across communication networks, effectively acting as a transparent network cloud for a user's application. This greatly reduces communication costs by eliminating expensive leased lines and replacing them with low-cost IP communications.

Protocol routes are controlled via the **Router Configuration** screen.



Routes Table

Client Device	Client Interface	Client Address	Server Local View Address	Validity	Client Local View Address	Server Address	Server Interface	Server Device
CPD	CPI	1	1	🟩	1	1	SPI	SPD

Figure 194: Router Configuration Screen

1. Configuration Tree **2.** Connectivity Tab **3.** Properties Tab **4.** Routes Table

›› Configuration Tree

The Configuration Tree view details all devices and interfaces associated with the Protocol Router. Users can right-click on individual items in the tree to perform add, delete, rename or configure items.

›› Connectivity Tab

The **Connectivity** tab provides a visual representation of the Protocol Router configuration. The main box represents the Protocol Router, while boxes on the right represent server devices and their interfaces, and boxes on the left represent client devices and their interfaces.

›› Properties

The **Properties** tab displays the parameters associated with the selected item (if applicable) in the Configuration Tree view.

Routes Table

The **Routes Table** lists the connections to and from the Protocol Router. A protocol route is defined as a client device, a server device, and the interface that connects them.

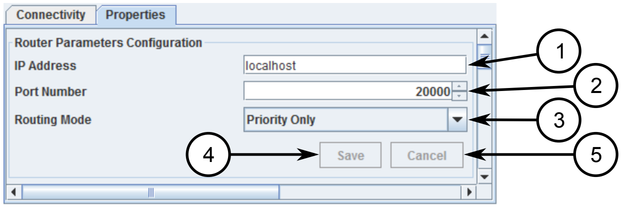
CONTENTS

Section 4.14.1

Configuring the Protocol Router

To configure the protocol router, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, select **Protocol Router** and then click the **Properties** tab.



Router Parameters Configuration
IP Address: localhost
Port Number: 20000
Routing Mode: Priority Only

Figure 195: Protocol Router Properties

1. IP Address Box **2.** Port Number Box **3.** Routing Mode List **4.** Save Button **5.** Cancel Button

3. Configure the following parameters as required:

Parameter	Description
IP Address	The local interface for the protocol router to use for inter-process communications. Set to `localhost` or `127.0.0.1`.
Port Number	**Synopsis:** 0 to 65535 **Default:** 0 The port used by the protocol router. Set to 20000.
Routing Mode	**Synopsis:** { Local Only, Local Only Then Priority, Priority Only } **Default:** Priority Only

Parameter	Description
	The method used by the protocol router for routing messages between router objects. Options include: • `Local Only` – Messages are routed only within the router instances. No messages are routed to external routers. • `Local Only Then Priority` – Messages are routed within the router instances and then based on priority to external routers. Messages may be routed to an external router only if there is no local route. The priority of local routes takes precedence over external routes regardless of their priorities. • `Priority Only` – Messages are routed based on priority. Messages may be routed to an external router if it has a higher priority.

4. Add and configure interfaces for client and server devices. For more information, refer to Section 4.14.4.1, “Adding an Interface” .
5. Add and configure client and server devices. For more information, refer to Section 4.14.5.1, “Adding a Client Device” and Section 4.14.5.2, “Adding a Server Device” .
6. Connect the interfaces to the devices. For more information, refer to Section 4.14.4.2, “Connecting an Interface” .
7. [Optional] Add listen clusters and assign them to client devices. For more information, refer to Section 4.14.7.1, “Adding a Listen Cluster” and Section 4.14.7.2, “Assigning/Removing a Listen Cluster” .
8. Add and configure routes. For more information, refer to Section 4.14.9.1, “Adding/Configuring a Route” .

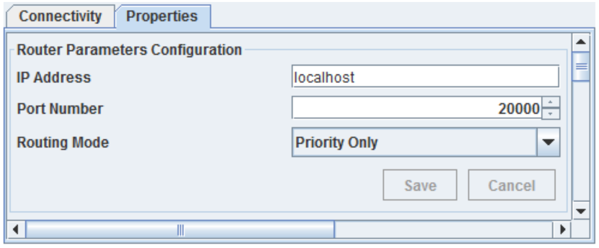
Section 4.14.2

Adding/Deleting the Protocol Router

To add or delete the Protocol Router, do the following:

›› Adding the Protocol Router

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right click **ELAN** to open the shortcut menu and then click **New Protocol Router**. The Protocol Router structure is added to the tree view and the Protocol Router core image appears on the **Connectivity** tab.



Router Parameters Configuration

IP Address: localhost

Port Number: 20000

Routing Mode: Priority Only

Figure 196: Protocol Router Properties

3. Configure the Protocol Router. For more information, refer to Section 4.14.1, “Configuring the Protocol Router” .

Deleting the Protocol Router

NOTE
The Protocol Router cannot be deleted if a route is attached to an internal device. To break the dependency, either delete the associated server device or remove the internal device from the master configuration for the server device. For more information, refer to:

- *Section 4.9.1, "Adding/Deleting a Server Device"*
- *Section 4.9.4.4, "Configuring Masters" (DNP Server Devices)*
- *Section 4.9.5.4, "Configuring Masters" (IEC 6807-5-104 Server Devices)*

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the **Protocol Router** to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
3. Click **OK** to delete the Protocol Router, or click **Cancel** to abort.

Section 4.14.3

Renaming Items in the Router Configuration

To rename a device, a device group, an interface or a listen cluster in the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired item and then click **Rename**. The label becomes an editable box.
3. Type the new name for the item and then press **Enter**.

Section 4.14.4

Managing Interfaces

Interfaces are used by the Protocol Router to communicate with client and server devices.

CONTENTS

Section 4.14.4.1

Adding an Interface

To add an interface for client or server devices, do the following:

1. Navigate to the **Router Configuration** screen.

> **NOTE**
> *Creating an interface from a device group automatically connects the interface with the devices in the group. Otherwise, the interface can be created separately and connected to devices manually.*

2. In the tree view, right click **Interfaces** under **Clients** or **Servers**, or the desired device group to open the shortcut menu and then click **Create Interface**. The **Properties** tab automatically displays the parameters associated with the interface.
3. Configure the following parameters:

Parameter	**Description**
Interface Name	The name of the interface.
Protocol Type	**Synopsis:** DNP3 The protocol type associated with the interface.
Connection Type	**Synopsis:** { TCP, UDP, SSL, TLS, Serial } or TCP **Default:** TCP The type of communication connection used by the interface. When the interface is associated with the IEC 60870-5-104 protocol type, only `TCP` is available. **NOTE** *The serial protocol is not available.*

4. Based on the connection type selected, configure the following parameters as required:

›› TCP

Parameter	**Description**
Initiation Mode	**Synopsis:** { Automatic, Demand Permanent, Demand Transient } **Default:** Automatic Defines when a connection with the client device will be established. Options include: • `Automatic` – A communications path is established at startup (even if there is no connection request) and remains active at all times. • `Demand Permanent` – A communications path is established only when a connection is requested by will remain active at all times. • `Demand Transient` – A communications path is established only when a connection is requested and will be closed when a connection is terminated.
Demand Transient Timeout	**Synopsis:** 1 to 86400 **Default:** 100 The time in seconds (s) that must elapse without traffic before the connection is dropped. **NOTE** *The **Initiation Mode** parameter must be set to `Demand Transient` for this parameter to take effect.*

Parameter	Description
IP Address	The local or remote IP address on which the interface will listen for incoming connections from hosts or remote devices associated with the interface. The value can be a DNS name or IPv4 address. This parameter is mandatory when **Connection Mode** is set to `Wait`.
IP Port	The local or remote IP port on which the interface will listen for incoming communications from hosts or remote devices associated with the interface.
Response Timeout	**Synopsis:** 1 to 3600 **Default:** 60 The time in seconds (s) to wait for a response from the a device after sending a message before trying to send the message again.
Retries	**Synopsis:** 1 to 100 **Default:** 10 The maximum number of attempts allowed to send a message to a device that does not respond.
Reconnect Interval	**Synopsis:** 0 to 86400 **Default:** 0 The time in seconds (s) the interface, acting as a client device, will wait after an unsuccessful connection attempt with a remote device before retrying the connection.
Redundant IP Address	The IP address of the secondary RUGGEDCOM ELAN server.

›› UDP

Parameter	Description
UDP Mode	**Synopsis:** { Compliant, ExplicitReplyToSource } **Default:** ExplicitReplyToSource Controls which port UDP response messages are sent to. Options include: • `Compliant` – Messages are always sent to port 20000 (in both directions) • `ExceptReplytoSource` – Messages are sent to the *source* port, which can be any number between 1024 and 65535.
Local IP Address	The local DNS name or IP address the interface will use to listen for incoming connections from client or server protocol devices associated with the interface.
Local IP Port	**Synopsis:** 1 to 65535 **Default:** 20005 The local IP port the interface will use to listen for incoming connections from client or server protocol devices associated with the interface.
Redundant IP Address	The IP address of the secondary RUGGEDCOM ELAN server.
Response Timeout	**Synopsis:** 1 to 3600 **Default:** 60 The time in seconds (s) to wait for a response from the a device after sending a message before trying to send the message again.
Retries	**Synopsis:** 1 to 100

Parameter	Description
	Default: 10 The maximum number of attempts allowed to send a message to a device that does not respond.

TLS/SSL

Parameter	Description
Connection Mode	**Synopsis:** { Wait, Initiate } **Default:** Initiate Defines how the connection with the client device will be initiated. Options include: • `Wait` – RUGGEDCOM ELAN waits for a connection to be made by the client device. • `Initiate` – RUGGEDCOM ELAN initiates a connection with the client device on startup.
Demand Transient Timeout	**Synopsis:** 1 to 86400 **Default:** 100 The time in seconds (s) that must elapse without traffic before the connection is dropped. **NOTE** *The **Initiation Mode** parameter must be set to* `Demand Transient` *for this parameter to take effect.*
IP Address	The local or remote IP address on which the interface will listen for incoming connections from hosts or remote devices associated with the interface. The value can be a DNS name or IPv4 address. This parameter is mandatory when **Connection Mode** is set to `Wait`.
IP Port	The local or remote IP port on which the interface will listen for incoming communications from hosts or remote devices associated with the interface.
Response Timeout	**Synopsis:** 1 to 3600 **Default:** 60 The time in seconds (s) to wait for a response from the a device after sending a message before trying to send the message again.
Retries	**Synopsis:** 1 to 100 **Default:** 10 The maximum number of attempts allowed to send a message to a device that does not respond.
Reconnect Interval	**Synopsis:** 0 to 86400 **Default:** 0 The time in seconds (s) the interface, acting as a client device, will wait after an unsuccessful connection attempt with a remote device before retrying the connection.
Redundant IP Address	The IP address of the secondary RUGGEDCOM ELAN server.
Renegotiation Time	**Synopsis:** 1 to 86400 **Default:** 3600 **Default State:** Enabled

Parameter	Description
	The maximum time in seconds (s) a connection a remote device can be open before it must be renegotiated. Clear the check box to disable this feature.
Renegotiation Size	**Synopsis:** 1 to 2147483647 **Default:** 1 **Default State:** Enabled The maximum number of bytes that can be received before a renegotiation occurs. Clear the check box to disable this feature.
Renegotiation Response Timeout	**Synopsis:** 1 to 86400 **Default:** 1 **Default State:** Enabled The time in seconds (s) to wait for a response from remote device after attempting to renegotiate the connection. Clear the check box to disable this feature.
Session Resume Timeout	**Synopsis:** 1 to 86400 **Default:** 1 **Default State:** Enabled The maximum time in seconds (s) a session can be in place before it may resume. Clear the check box to disable this feature.
Session Resume Size	**Synopsis:** 1 to 86400 **Default:** 1 **Default State:** Enabled The maximum number of bytes received before a session may resume. Clear the check box to disable this feature.
Certificate Size Limit	**Synopsis:** 1 to 2147483647 **Default:** 1 **Default State:** Enabled The maximum size of a certificate in bytes. Clear the check box to disable this feature.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Use strong ciphers whenever possible, such as RSA, DSA, and ECDSA. Other ciphers, such as AES, DES and RC4 are considered weak and could unnecessarily expose the system to attacks.

5. If the connection type is set to `TLS` or `SSL`, under **Ciphers**, select the ciphers to use.
   - Click **All** to select all available ciphers
   - Click **256 Bit** to select only the 256-bit ciphers
   - Double-click individual ciphers to create a custom list
6. Click **Save**.
7. If the interface was created independent of a device group, connect the interface to a client device. For more information, refer to Section 4.14.4.2, “Connecting an Interface” .

Section 4.14.4.2
Connecting an Interface

To connect an interface to a client or server device group, do the following:

> **NOTE**
> *Once a device group is connected to an interface, the protocol type for the device group is fixed. The type can only be changed once the device group and interface are disconnected.*

›› Connecting a Device Group to an Interface

1. Navigate to the **Router Configuration** screen.
2. In the tree view, under **Clients** or **Servers**, right-click the desired device group to open the shortcut menu and then click **Connect to Interface**. The **Connect to Interface** dialog box appears.

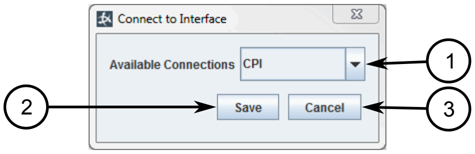


Figure 197: Connect to Interface Dialog Box

1. Available Connections List **2.** Save Button **3.** Cancel Button

3. Under **Available Connections**, select the desired interface.
4. Click **Save**. The interface name appears under the device group and the device group appears under the interface.

›› Connecting an Interface to a Device Group

1. Navigate to the **Router Configuration** screen.
2. In the tree view, under ***Clients » Interfaces*** or ***Servers » Interfaces*** , right-click the desired interface to open the shortcut menu and then click **Connect to Device**. The **Connect to Device** dialog box appears.

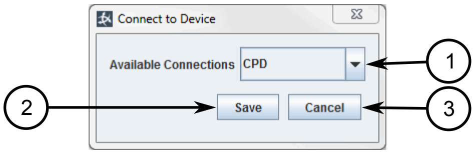


Figure 198: Connect to Device Dialog Box

1. Available Connections List **2.** Save Button **3.** Cancel Button

3. Under **Available Connections**, select the desired device group.
4. Click **Save**. The interface name appears under the device group and the device group appears under the interface.

Section 4.14.4.3

Disconnecting an Interface

To disconnect an interface from a client or server device group, do the following:

›› Disconnecting a Device Group from an Interface

1. Navigate to the **Router Configuration** screen.
2. In the tree view, under ***Clients » Devices » { Device } » { Group }*** or ***Servers » Devices » { Device } » { Group }***, right-click the interface to open the shortcut menu and then click **Disconnect from Device Group**. The interface is immediately disconnected.

›› Disconnecting an Interface from a Device Group

1. Navigate to the **Router Configuration** screen.
2. In the tree view, under ***Clients » Interfaces » { Group }*** or ***Servers » Interfaces » { Group }***, right-click the device group to open the shortcut menu and then click **Disconnect from Interface**. The interface is immediately disconnected.

Section 4.14.4.4

Deleting an Interface

To delete an interface from the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired interface under either ***Clients » Interfaces*** or ***Servers » Interfaces*** to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the interface, or click **Cancel** to abort.

Section 4.14.5

Managing Devices

Each device defined under the Protocol Router is a software representation of a physical device (either a client/host or server/remote) that communicates with RUGGEDCOM ELAN through the Protocol Router. Devices are either client devices or server devices:

- Client devices manage the communications interface with a Master or Host Device. A complete configuration consists of two sub-components: client device and client interface.
- Server devices manage the communications interface with a remote device, such as an IED or RTU. A complete configuration consists of three sub-components: server device, server interface and server device group.

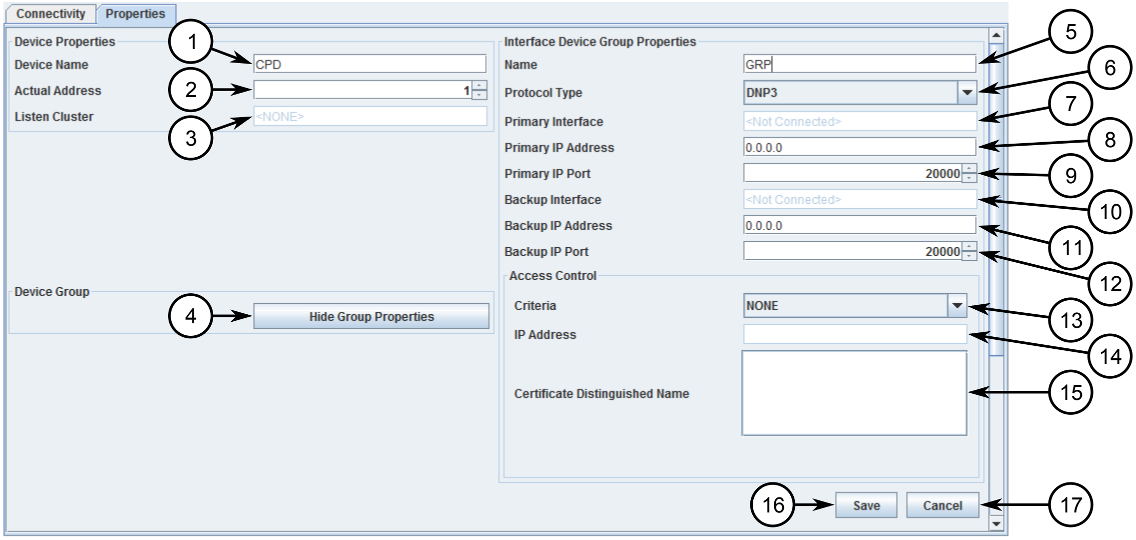
CONTENTS

- Section 4.14.5.3, “Deleting a Device”

Section 4.14.5.1
Adding a Client Device

To add a client device to the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click **Devices** under **Clients** to open the shortcut menu and then click **Create New Device**. The **Properties** tab automatically displays the parameters associated with the device.



Device Name CPD
Actual Address 1
Listen Cluster <NONE>
Name GRP
Protocol Type DNP3
Primary Interface <Not Connected>
Primary IP Address 0.0.0.0
Primary IP Port 20000
Backup Interface <Not Connected>
Backup IP Address 0.0.0.0
Backup IP Port 20000
Criteria NONE
IP Address
Certificate Distinguished Name

Figure 199: New Client Device Parameters

1. Device Name Box **2.** Actual Address List **3.** Listen Cluster Box **4.** Hide Group Properties Button **5.** Name Box **6.** Protocol Type List **7.** Primary Interface Box **8.** Primary IP Address Box **9.** Primary IP Port **10.** Backup Interface **11.** Backup IP Address **12.** Backup IP Port **13.** Criteria List **14.** IP Address Box **15.** Certificate Distinguished Name **16.** Save Button **17.** Cancel Button

3. Under **Device Properties**, configure the following parameters:

Parameter	Description
Device Name	The unique name of the device element.
Actual Address	**Synopsis:** 1 to 65535 **Default:** 1 The actual protocol address to use when communicating with the device element. This will always be the device element's actual protocol address, even if the device has a different virtual address for address mapping.

4. Under **Interface Device Group Properties**, define the associated device group by configuring the following parameters:

Parameter	Description
Name	The name of the device group.
Protocol Type	**Synopsis:** { DNP3, IEC 60870-5-104 } The communication protocol used by the device group. **NOTE** *The serial protocol is not available.*
Primary IP Address	The primary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Primary IP Port	The primary port the Protocol Router will use when communicating with devices in the device group.
Backup IP Address	The secondary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Backup IP Port	The secondary port the Protocol Router will use when communicating with devices in the device group.

5. Under **Access Control**, configure the following parameters:

Parameter	Description
Criteria	**Synopsis:** IP ADDRESS or { HOST ADDRESS, IP ADDRESS, IP AND HOST, NONE, DISTINGUISHED NAME } **Default:** NONE The selection criteria to use for address mapping. Options include: **NOTE** *Only `IP ADDRESS` is applicable to IEC 60870-5-104 interfaces.* • `HOST ADDRESS` – The host address is used for address mapping. • `IP ADDRESS` – The IP address of the host is used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `IP AND HOST` – The IP address of the host and host's address are used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `NONE` – Access to the device is not controlled. • `DISTINGUISHED NAME` – Access is determined based on the distinguished name of the subject. Define the distinguished name under **Certificate Distinguished Name** when this option is selected.
IP Address	The IP address used when the **Criteria** is set to `IP ADDRESS`.
Certificate Distinguished Name	The unique identifying name of the certificate used when the **Criteria** is set to `DISTINGUISHED NAME`.

6. Click **Save**.

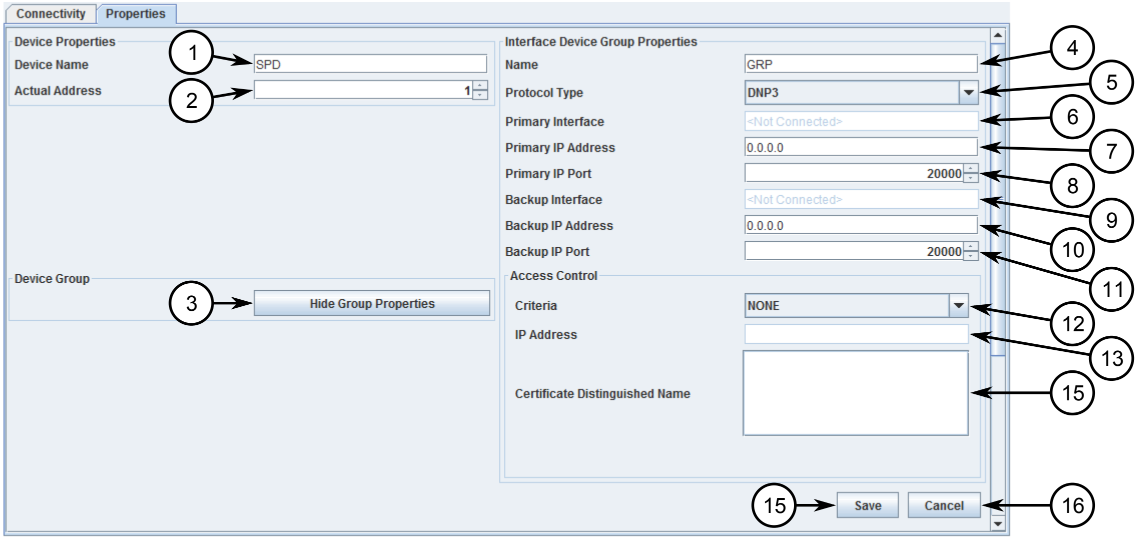
7. Connect the device to an interface. For more information, refer to Section 4.14.4.2, “Connecting an Interface” .

Section 4.14.5.2

Adding a Server Device

To add a server device to the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click **Devices** under **Servers** to open the shortcut menu and then click **Create New Device**. The **Properties** tab automatically displays the parameters associated with the device.



Device Name: SPD
Actual Address: 1
Name: GRP
Protocol Type: DNP3
Primary Interface: <Not Connected>
Primary IP Address: 0.0.0.0
Primary IP Port: 20000
Backup Interface: <Not Connected>
Backup IP Address: 0.0.0.0
Backup IP Port: 20000
Criteria: NONE
IP Address:
Certificate Distinguished Name:

Figure 200: New Server Device Parameters

1. Device Name Box **2.** Actual Address List **3.** New Device Group Option **4.** Select a Device Group Option **5.** Select a Device Group List **6.** Hide Group Properties Button **7.** Name Box **8.** Protocol Type List **9.** Primary Interface Box **10.** Primary IP Address Box **11.** Primary IP Port **12.** Backup Interface **13.** Backup IP Address **14.** Backup IP Port **15.** Criteria List **16.** IP Address Box **17.** Certificate Distinguished Name **18.** Save Button **19.** Cancel Button

3. Under **Device Properties**, configure the following parameters:

Parameter	Description
Device Name	The unique name of the device element.
Actual Address	**Synopsis:** 1 to 65535 **Default:** 1 The actual protocol address to use when communicating with the device element. This will always be the device element's actual protocol address, even if the device has a different virtual address for address mapping.

4. Under **Device Group**, either
   - Select **New Device Group** and proceed to the next step
   - Select **Select a Device Group**, select a device group from the list, and then proceed to Step 7
5. Under **Interface Device Group Properties**, configure the following parameters:

Parameter	Description
Name	The name of the device group.
Protocol Type	**Synopsis:** DNP3 The communication protocol used by the device.
Primary IP Address	The primary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Primary IP Port	The primary port the Protocol Router will use when communicating with devices.
Backup IP Address	The secondary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Backup IP Port	The secondary port the Protocol Router will use when communicating with devices.

6. Under **Access Control**, configure the following parameters:

Parameter	Description
Criteria	**Synopsis:** { HOST ADDRESS, IP ADDRESS, IP AND HOST, NONE, DISTINGUISHED NAME } **Default:** NONE The selection criteria to use for address mapping. Options include: • `HOST ADDRESS` – The host address is used for address mapping. • `IP ADDRESS` – The IP address of the host is used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `IP AND HOST` – The IP address of the host and host's address are used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `NONE` – Access to the device is not controlled. • `DISTINGUISHED NAME` – Access is determined based on the distinguished name of the subject. Define the distinguished name under **Certificate Distinguished Name** when this option is selected.
IP Address	The IP address used when the **Criteria** is set to `IP ADDRESS`.
Certificate Distinguished Name	The unique identifying name of the certificate used when the **Criteria** is set to `DISTINGUISHED NAME`.

7. Click **Save**.

NOTE
A new device group is created whenever a new device is added. This group can be removed once the device is moved to one of the other available device groups.

8. [Optional] If required, ungroup the new device from the device group RUGGEDCOM ELAN created automatically and add it to an existing device group. For more information, refer to Section 4.14.6.3, "Grouping/Ungrouping Server Devices" .

9. Connect the device to an interface. For more information, refer to Section 4.14.4.2, "Connecting an Interface" .

Section 4.14.5.3

Deleting a Device

To delete a client or server device from the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired device under either **Clients** or **Servers** to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the device, or click **Cancel** to abort.

Section 4.14.6

Managing Device Groups

Device groups are logical collections of devices that use the same connection parameters to communicate with the Protocol Router. A device can only belong to one device group at any given time.

When configuring server devices on the Protocol Router, users can manually group devices that use the same connection parameters into device groups. This allows users to set the parameters for the group, rather than for individual devices.

For client devices, Maestro enforces a one-to-one constraint, such that each device group can only contain one device. The parameters for modifying client-side device groups are accessible through the client devices.

CONTENTS

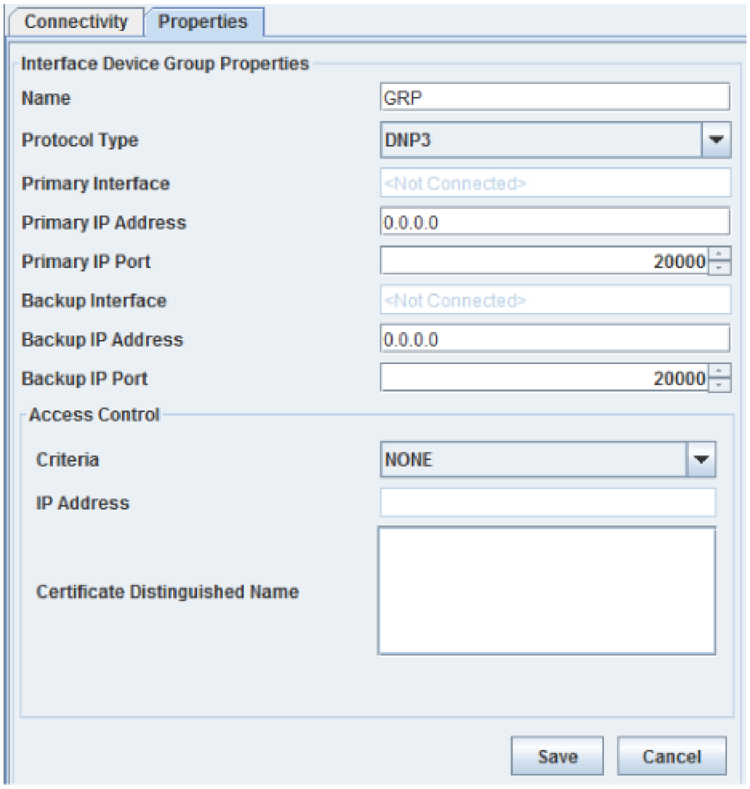
Section 4.14.6.1

Adding a Device Group

To add a device group, do the following:

NOTE
Device groups can only be added for server devices. Device groups for client devices are added automatically when a client device is created and are unique to each device.

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click **Device Groups** under **Servers** to open the shortcut menu and then click **Create New Device Group**. The **Properties** tab automatically displays the parameters associated with the device group.



Interface Device Group Properties

Name	GRP
Protocol Type	DNP3
Primary Interface	<Not Connected>
Primary IP Address	0.0.0.0
Primary IP Port	20000
Backup Interface	<Not Connected>
Backup IP Address	0.0.0.0
Backup IP Port	20000

Access Control

Criteria	NONE
IP Address	
Certificate Distinguished Name	

Figure 201: New Device Group Parameters

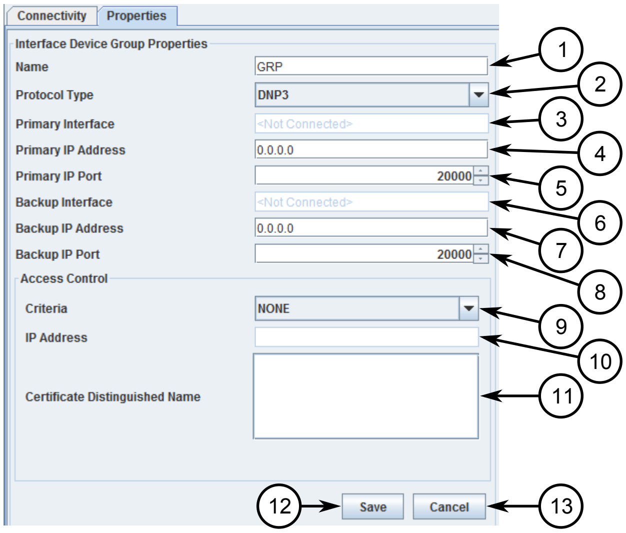
3. Configure the device group. For more information, refer to Section 4.14.6.2, “Configuring a Device Group” .

Section 4.14.6.2

Configuring a Device Group

To configure a device group, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, under ***Clients*** » ***Devices*** » ***{ Client }*** or ***Servers*** » ***Device Groups*** , select the desired device group. The **Properties** tab automatically displays the parameters associated with the device group.



Interface Device Group Properties

Name: GRP

Protocol Type: DNP3

Primary Interface: <Not Connected>

Primary IP Address: 0.0.0.0

Primary IP Port: 20000

Backup Interface: <Not Connected>

Backup IP Address: 0.0.0.0

Backup IP Port: 20000

Access Control

Criteria: NONE

IP Address:

Certificate Distinguished Name:

Figure 202: Device Group Parameters

1. Name Box **2.** Protocol Type List **3.** Primary Interface Box **4.** Primary IP Address Box **5.** Primary IP Port **6.** Backup Interface **7.** Backup IP Address **8.** Backup IP Port **9.** Criteria List **10.** IP Address Box **11.** Certificate Distinguished Name **12.** Save Button **13.** Cancel Button

3. Configure the following parameters as required:

Parameter	Description
Name	The name of the device group.
Protocol Type	**Synopsis:** DNP3 The communication protocol used by the device.
Primary IP Address	The primary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Primary IP Port	The primary port the Protocol Router will use when communicating with devices.
Backup IP Address	The secondary IP address the Protocol Router will use to communicate with devices that are downstream from the device group.
Backup IP Port	The secondary port the Protocol Router will use when communicating with devices.

4. Under **Access Control**, configure the following parameters:

Parameter	Description
Criteria	**Synopsis:** { HOST ADDRESS, IP ADDRESS, IP AND HOST, NONE, DISTINGUISHED NAME } **Default:** NONE The selection criteria to use for address mapping. Options include: • `HOST ADDRESS` – The host address is used for address mapping.

Parameter	Description
	• `IP ADDRESS` – The IP address of the host is used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `IP AND HOST` – The IP address of the host and host's address are used for address mapping. Define the IP Address under **IP Address** when this option is selected. • `NONE` – Access to the device is not controlled. • `DISTINGUISHED NAME` – Access is determined based on the distinguished name of the subject. Define the distinguished name under **Certificate Distinguished Name** when this option is selected.
IP Address	The IP address used when the **Criteria** is set to `IP ADDRESS`.
Certificate Distinguished Name	The unique identifying name of the certificate used when the **Criteria** is set to `DISTINGUISHED NAME`.

5. Click **Save**.
6. For server device groups only, connect the device group to an interface. For more information, refer to Section 4.14.4.2, “Connecting an Interface” .

Section 4.14.6.3

Grouping/Ungrouping Server Devices

To add (group) or remove (ungroup) server devices to a device group, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired device group under either ***Servers » Device Groups*** or ***Servers » Devices » { Device }*** to open the shortcut menu and then click **Manage Device Groups**. A dialog box appears.

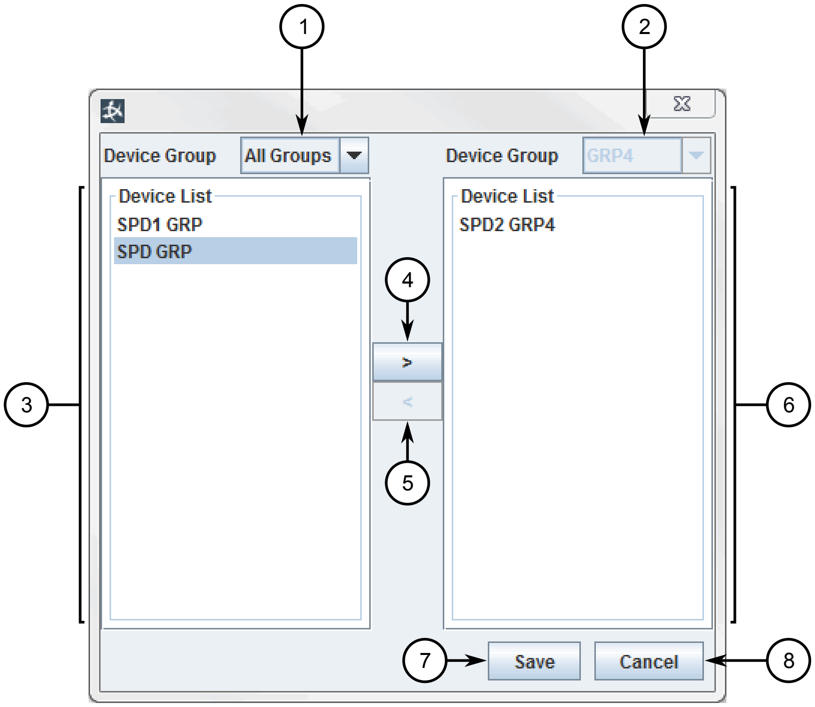


Figure 203: Manage Device Groups Dialog Box

1. Source Device Group **2.** Target Device Group **3.** Available Server Devices **4.** Server Devices in Target Device Group **5.** Add Button **6.** Remove Button **7.** Save Button **8.** Cancel Button

3. Add or remove a server device by selecting the desired device and using the **>** (add/group) or **<** (remove/ ungroup) buttons to move them in or out of the target device group.
4. Click **Save**.

Section 4.14.6.4

Deleting a Device Group

To delete a server device group from the Protocol Router configuration, do the following:

NOTE
Device groups for client devices can only be deleted by deleting the associated client device.

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired device group under either ***Servers » Device Groups*** to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the device group, or click **Cancel** to abort.

Section 4.14.7

Managing Listen Clusters

Listen clusters are groups of DNP clients that can listen to the received messages destined for any other client in the group.

Typically, at any given time, only one client in a listen cluster will be actively sending messages to remote end devices. The other DNP clients in the cluster will be able to listen to the the DNP response messages to keep track of end device information locally. The other DNP clients are not required to actively send messages to the end devices. This facilitates easy switching from one controlling DNP client to another.

CONTENTS

Section 4.14.7.1

Adding a Listen Cluster

To add a listen cluster to the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click **Listen Clusters** under **Clients** to open the shortcut menu and then click **Create Listen Cluster**. The new listen cluster appears under **Listen Clusters**.
3. Assign the listen cluster to a client device group. For more information, refer to Section 4.14.7.2, “Assigning/Removing a Listen Cluster” .

Section 4.14.7.2

Assigning/Removing a Listen Cluster

To assign a listen cluster to a client device group or remove a listen cluster from a client device group, do the following:

›› Assigning a Listen Cluster

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired device under ***Clients » Devices*** to open the shortcut menu, select **Assign Listen Cluster**, and then click the desired listen cluster. The client device is automatically listed under the listen cluster in ***Clients » Listen Clusters*** .

›› Removing a Listen Cluster

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the client device under ***Clients » Listen Clusters » Cluster*** or ***Clients » Devices*** to open the shortcut menu and then click **Remove Listen Cluster**. The listen cluster is automatically disassociated from the client device.

Section 4.14.7.3

Deleting a Device

To delete a listen cluster from the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click the desired listen cluster under either ***Clients » Listen Clusters*** to open the shortcut menu and then click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the listen cluster, or click **Cancel** to abort.

Section 4.14.8

Managing Virtual Devices

Virtual devices represent DNP 3.0 and IEC 60870-5-104 server devices created for the RUGGEDCOM ELAN server. These devices require the Protocol Router to facilitate their communication with other servers that use a different protocol. For instance, if a DNP 3.0 server needs to receive telemetry data from an IEC 60870-5-104 server, both servers must be created and then a route must be configured between them using the Protocol Router.

CONTENTS

Section 4.14.8.1

Adding a Virtual Device

RUGGEDCOM ELAN automatically generates a virtual device and associated client device for each DNP 3.0 or IEC 60870-5-104 server device added under the **Overview** screen. It also generates the required route between the virtual device and client device.

For information about adding a DNP 3.0 or IEC 60870-5-104 server device, refer to Section 4.9.1, “Adding/Deleting a Server Device” .

For information about configuring the route between virtual devices and their associated client devices, refer to Section 4.14.9.1, “Adding/Configuring a Route” .

Section 4.14.8.2

Deleting a Virtual Device

Virtual devices and their associated client devices can only be deleted from the **Overview** screen. For more information, refer to Section 4.9.1, “Adding/Deleting a Server Device” .

Section 4.14.9

Managing Routes

Routes define the communication route (or path) between client and server devices through the Protocol Router.

CONTENTS

Section 4.14.9.1

Adding/Configuring a Route

To add and/or a configure a route to the Protocol Router configuration, do the following:

›› Adding a Route

1. Navigate to the **Router Configuration** screen.
2. In the tree view, right-click **Protocol Router** to open the shortcut menu and then click **Add a Route**. A new route is added under **Route Tables**.
3. Configure the route.
4. For virtual server devices only, configure the Server Master for the new route. For more information, refer to Section 4.9.4.4, “Configuring Masters” .

›› Configuring a Route

1. Navigate to the **Router Configuration** screen.
2. Under the **Routes Table**, locate the desired route and configure the following parameters:

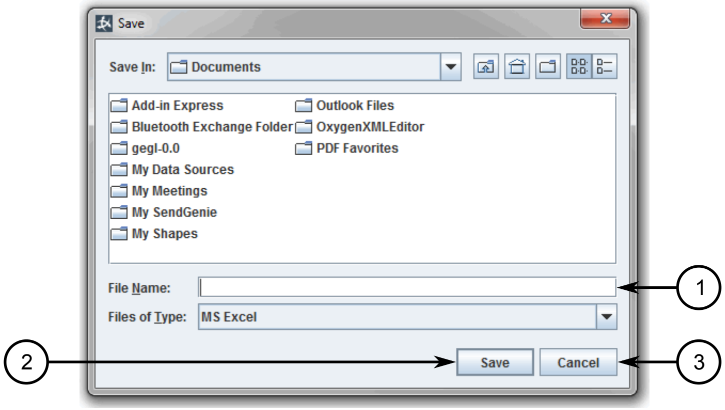
Parameter	Description
Client Device	The name of the associated client device.
Client Interface	The interface used by the associated client device.
Client Address	The actual protocol address of the associated client device.
Server Local View Address	The address used by the client device to connect with the server device.
Client Local View Address	The address used by the server device to connect with the client device.
Server Address	The actual protocol address of the associated server device.
Server Interface	The interface used by the associated server device.
Server Device	The name of the associated server device.

Section 4.14.9.2

Exporting Routes

To export all routes to a Microsoft® Excel spreadsheet, do the following:

1. Navigate to the **Router Configuration** screen.
2. Under **Action**, click **Export Routes**. The **Save** dialog box appears.



Save In: Documents

Files of Type: MS Excel

Figure 204: Save Dialog Box

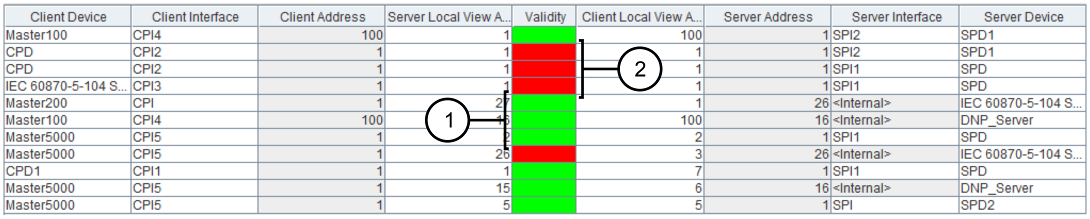
1. File Name Box **2.** Save Button **3.** Cancel Button

3. Navigate to and select the drive or folder where the Excel spreadsheet will be saved.
4. Under **File Name**, type a name for the spreadsheet.
5. Click **Save** to save the spreadsheet, or click **Cancel** to abort.

Section 4.14.9.3

Resolving Invalid Protocol Routes

Invalid protocol routes are identified in the **Routes Table** under the **Validity** column. Cells in this column are green if the route is valid, or red if the route is invalid.



Client Device	Client Interface	Client Address	Server Local View A...	Validity	Client Local View A...	Server Address	Server Interface	Server Device
Master100	CPI4	100	1	🟩	100	1	SPI2	SPD1
CPD	CPI2	1	1	🟥	1	1	SPI2	SPD1
CPD	CPI2	1	1	🟥	1	1	SPI1	SPD
IEC 60870-5-104 S...	CPI3	1	1	🟥	1	1	SPI1	SPD
Master200	CPI	1	27	🟩	1	26	<Internal>	IEC 60870-5-104 S...
Master100	CPI4	100	16	🟩	100	16	<Internal>	DNP_Server
Master5000	CPI5	1	2	🟩	2	1	SPI1	SPD
Master5000	CPI5	1	26	🟥	3	26	<Internal>	IEC 60870-5-104 S...
CPD1	CPI1	1	1	🟩	7	1	SPI1	SPD
Master5000	CPI5	1	15	🟩	6	16	<Internal>	DNP_Server
Master5000	CPI5	1	5	🟩	5	1	SPI	SPD2

Figure 205: Routes Tab

1. Valid Routes **2.** Invalid Routes

A protocol route is considered invalid if:

- It is the same as another protocol route. Duplicates are not permitted.

- It has the same server local view address and client local view address combination as another protocol route (DNP only)
- The device is connected to one or more client or server devices (IEC 60870-5-104 only)

Section 4.14.9.4

Deleting a Route

To delete a route from the Protocol Router configuration, do the following:

1. Navigate to the **Router Configuration** screen.
2. Under the **Routes Table**, right-click the desired route and then click **Delete**. A confirmation dialog box appears.
3. Click **Yes** to delete the device, or click **Cancel** to abort.

Section 4.15

Downloading Configurations

Once all server and/or client devices have been configured, the complete project can be downloaded to one or more of the target RUGGEDCOM ELAN servers. The required components in each RUGGEDCOM ELAN server is then restarted by Maestro to use the new configuration.

To download a configuration, do the following:

1. Navigate to the **Download Project** screen. Here, each RUGGEDCOM ELAN server defined by the project is listed.

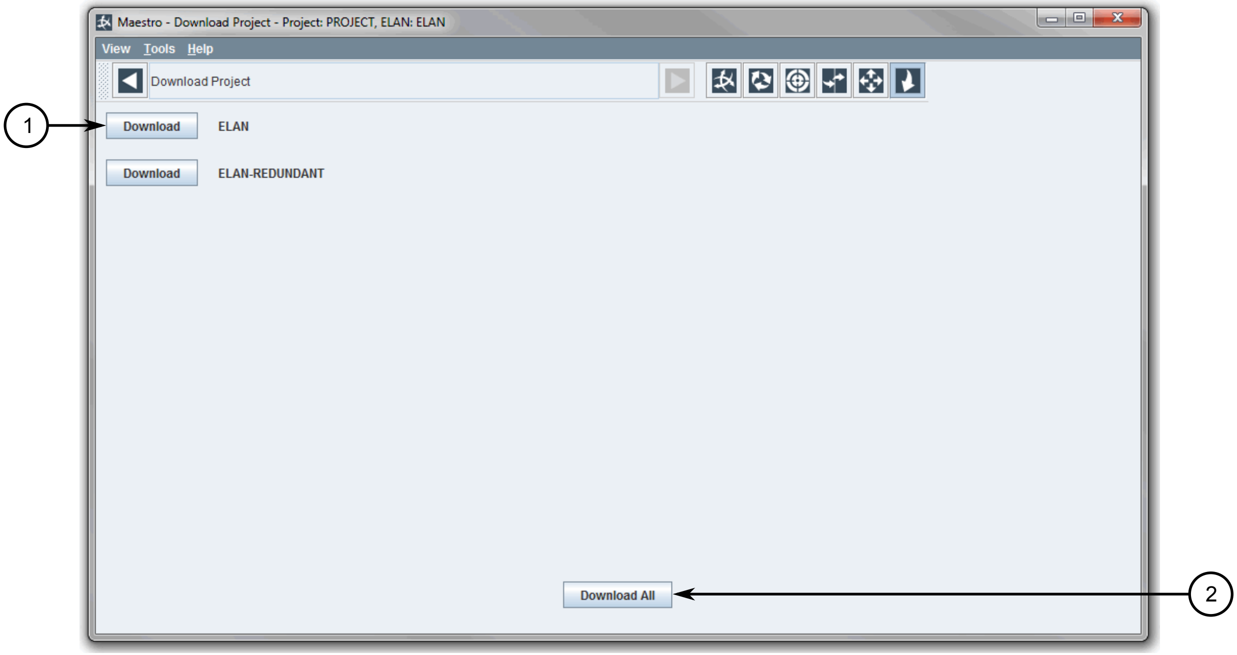


Figure 206: Download Project Screen

1. Download Button **2.** RUGGEDCOM ELAN server **3.** Download All Button

2. Download the configuration to a single RUGGEDCOM ELAN server by clicking the **Download** button next to it, or download the configuration to each RUGGEDCOM ELAN server by clicking the **Download All** button. If the RUGGEDCOM ELAN server is configured to authenticate specific users, the **ELAN Credentials** dialog box appears requesting the login credentials for the target RUGGEDCOM ELAN server. The title of the dialog box indicates the target RUGGEDCOM ELAN server by name and IP address.

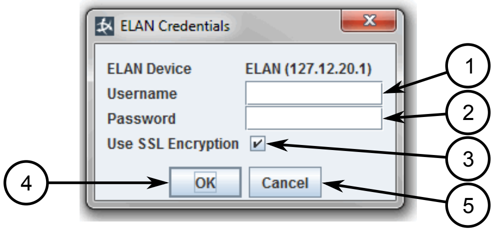


Figure 207: ELAN Credentials

1. Username Box **2.** Password Box **3.** Use SSL Encryption Check Box (non-RUGGEDCOM ROX II Platforms Only) **4.** OK Button **5.** Cancel Button

If authentication is not required, proceed to Step 8 .

3. In the **Username** box, type the user name for the RUGGEDCOM ELAN server.
4. In the **Password** box, type the password for the RUGGEDCOM ELAN server.

NOTE
*The **Use SSL Encryption** parameter is only available on non-RUGGEDCOM ROX II platforms.*

5. [Optional] Select **Use SSL Encryption** to encrypt the connection with the RUGGEDCOM ELAN server(s). When enabled (selected), a confirmation dialog box appears for each download target detailing the certificate information for the RUGGEDCOM ELAN server.

6. Click **OK**.

7. If **Use SSL Encryption** was selected, a confirmation dialog box appears detailing the following information about the SSL certificate:

    - The encryption algorithm used by the server
    - The start date of the security certificate
    - The end date of the security certificate
    - The certificate issuer
    - The certificate subject
    - The certificate signature

    Confirm the certificate information and then click **Yes** to proceed with the download.

8. If the configuration is being downloaded to more than one RUGGEDCOM ELAN server, repeat Step 3 to Step 6 for each remaining server as required.

5 Using ELAN Listener

RUGGEDCOM ELAN features ELAN Listener for RUGGEDCOM APE modules that monitors TCP communications received on a network interface and forwards specific packets to a UDP peer.

> **IMPORTANT!**
> *The ELAN Listener feature must be purchased separately and is not included in the standard RUGGEDCOM ELAN installation. For information about ordering ELAN Listener, contact a Siemens Sales representative.*

This tool is designed for users who want to duplicate data packets being sent by a SCADA server (slave) to a SCADA client (master), and forward the packets to a separate SCADA client without significantly changing the existing network configuration.

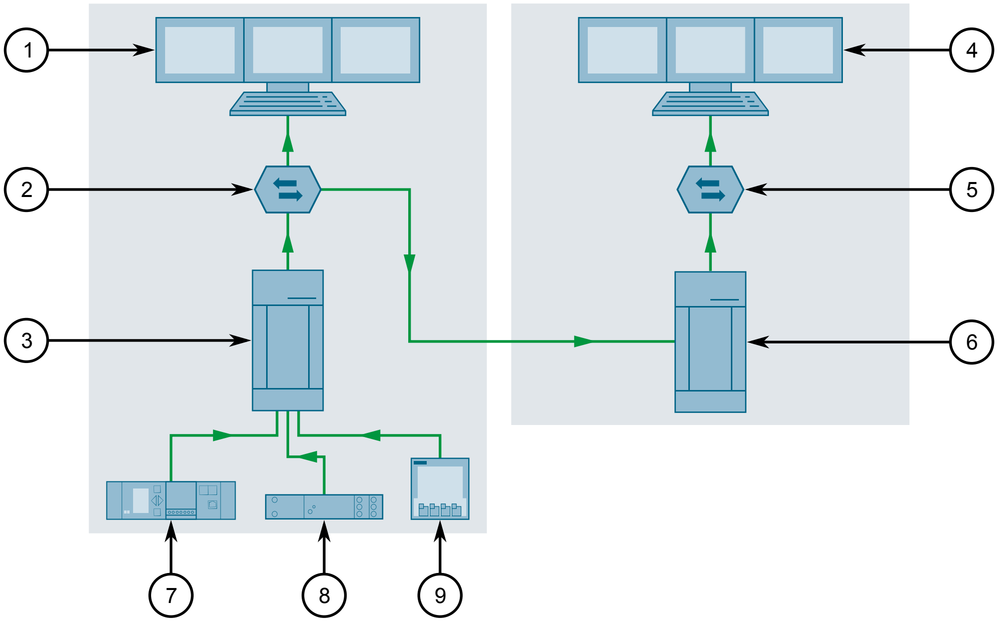


Figure 208: ELAN Listener

1. Primary SCADA Client **2.** Network Device (Switch with Port Mirroring or Hub) **3.** SCADA Server (Slave) **4.** Secondary SCADA Client in Listen Mode **5.** Network Device (Switch or Hub) **6.** RUGGEDCOM ELAN Server with ELAN Listener Enabled **7.** Relay **8.** RTU **9.** Transformer Monitor

To use ELAN Listener, the user must:

1. Connect a network device (switch or hub) that lies in the communication path between the SCADA client and server to the RUGGEDCOM ELAN port on a RUGGEDCOM ELAN server.
2. Configure the network device to forward incoming TCP communications to the port connected to the RUGGEDCOM ELAN server, typically using port mirroring.
3. Enable and configure ELAN Listener on the RUGGEDCOM ELAN server.
4. [Optional] Configure the secondary SCADA client to be in Listen mode.

5. Run ELAN Listener.

IMPORTANT!
ELAN Listener can only be run and configured by users with administrator access.

NOTE
ELAN Listener is not supported by IEC 61850 client devices.

CONTENTS

Section 5.1

Configuring Listen Mode

RUGGEDCOM ELAN's ELAN Listener requires all client devices to be in *Listen* mode.

Listen mode is enabled for all client devices when the operating mode for the RUGGEDCOM ELAN server is set to `Listen`. This is controlled via Maestro in the server configuration. For more information, refer to Section 4.6.4, “Configuring a RUGGEDCOM ELAN Server” .

Section 5.2

Running ELAN Listener From the Command Line

RUGGEDCOM ELAN's ELAN Listener can be run as a utility from the command line using the **`elistener`** command. The following are the various commands available.

NOTE
*Logs and errors generated when ELAN Listener is run from the command line are sent to **stdout** and **stderr** respectively.*

›› Running ELAN Listener As a Service

Use the `-d` option to run ELAN Listener as a service.

IMPORTANT!
*This option is not recommended, as it detaches eListerner from the terminal and thus provides no feedback to the user. The recommended method is to use the **`services`** command. For more information, refer to Section 5.3, “Starting/Stopping the ELAN Listener Service” .*

```
elistener  -d
```

Displaying Help Text

Use the `-h` option to display the Help text for the **`elistener`** command.

```
elistener  -h
```

Listing Available Network Interfaces

Use the `-l` option to list the network interfaces available on the system from which ELAN Listener can capture packets. Use the interface name as an argument using the `-e` option.

```
elistener  -l
```

Increasing the Verbosity Level of Logs

Use the `-v` option to increase the level of detail submitted to the syslog. This command can be specified multiple times. Each occurrence increases the verbosity level by one up to a maximum of five.

```
elistener  -v
```

Running ELAN Listener

Run ELAN Listener as a utility by typing:

```
elistener -v... -e interface  -f filter  -i client-ip-address  -p client-port  -u listen-ip-address
```

Where:

- *`interface`* is the network interface from which packets are to be captured. The default interface is *eth0*.
- *`filter`* is the filter syntax that determines which packets will be forwarded. The syntax typically consists of an ID (name or number0 followed by one or more qualifiers. For more information, refer to the manpage for *`pcap-filter`*.
- *`client-ip-address`* is the IP address of the client to which captured packets will be forwarded to as UDP messages.
- *`client-port`* is the number of the client's port to which captured packets will be forwarded.
- *`listen-ip-address`* is the IP address used for opening a UDP socket. Options include `localhost` (default) and `0.0.0.0`.

Stopping ELAN Listener

Stop ELAN Listener by pressing **Ctrl-C**.

Section 5.3

Starting/Stopping the ELAN Listener Service

RUGGEDCOM ELAN's ELAN Listener can be run in the background as a service. The service will run until stopped by the user.

IMPORTANT!
When ELAN Listener is run as a service, RUGGEDCOM ELAN refers to `/etc/default/elistener` *for configuration details.*

NOTE
Logs and errors generated when ELAN Listener is run as a service are sent to `/var/log/daemon.log`*.*

To start or stop the ELAN Listener service, do the following:

1. Log in to the RUGGEDCOM ELAN server as the *root* user via SSH.
2. Make sure ELAN Listener is properly configured. For more information, refer to Section 5.4, "Configuring ELAN Listener" .
3. At the command, prompt type the following and then press **Enter**:

```
service elistener [ start | stop ]
```

Section 5.4

Configuring ELAN Listener

When ELAN Listener is run as a service, RUGGEDCOM ELAN refers to `/etc/default/elistener` for configuration details.

IMPORTANT!
The ELAN Listener service must be disabled before any changes are made to the configuration.

To update the configuration for ELAN Listener, do the following:

1. Stop the ELAN Listener service. For more information, refer to Section 5.3, "Starting/Stopping the ELAN Listener Service" .
2. Open `/etc/default/elistener` in a text editor and update the configuration as described below.
3. Save and close the file.
4. Start the ELAN Listener service.

Enabling/Disabling ELAN Listener

Enable or disable ELAN Listener by editing the following line in `/etc/default/elistener`:

```
ENABLED={ 0 | 1}
```

A value of `0` disables ELAN Listener, while a value of `1` enables ELAN Listener.

Setting the Network Interface

Specify the network interface from which packets are captured by editing the following:

```
DEVICE={interface}
```

A list of network interfaces available to the RUGGEDCOM ELAN server can be determined from the command line. For more information, refer to Section 5.2, “Running ELAN Listener From the Command Line” .

›› Filtering Packets

Define which packets are copied by ELAN Listener by editing the following:

```
FILTER="{filter}"
```

Use the following filter to copy packets traveling from a SCADA server to a SCADA client:

```
FILTER="ip src host {server-ip} and src port {server-port} and dst host {client-ip}"
```

Use the following filter to copy packets traveling from both the SCADA server and the SCADA client:

```
FILTER="(ip src host {server-ip} and src port {server-port} and dst host {client-ip}) or (ip src host {client-ip} and dst port {server-port} and dst host {server-ip})"
```

›› Specifying the IP Address for the Secondary UDP Client

ELAN Listener forwards all packets that match its search criteria to a secondary UDP client. Specify the IP address for the UDP client by editing the following:

```
CLIENT_IP="{ip-address}"
CLIENT_PORT="{port}"
```

> ⚠ **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. ELAN Listener forwards all packets to the specified UDP client. Make sure the UDP client is trusted and on a secure network.*

›› Specifying the Listen Address

Specify the IP address or host name used by ELAN Listener to listen for packets by editing the following:

```
LISTEN_IP="{address}"
```

Options include:

- `localhost` – Use when the destination of the packets is the same system (e.g. 127.0.0.1)
- `0.0.0.0` – Use when the destination of the packets is a different system on the network

›› Increasing the Verbosity Level of Logs

Increase the level of detail submitted to `/var/log/daemon.log` by editing the following:

```
VERBOSITY="{level}"
```

Set the value to `-v` to set the value to level 1. Add `-v` again to increase the verbosity to level 2, and so on. For example, the following sets the verbosity to level 5, the highest level available:

```
VERBOSITY="-v-v-v-v-v"
```

6 Troubleshooting

This chapter describes troubleshooting steps to resolve potential problems that may be encountered when using RUGGEDCOM ELAN. If a specific problem is not addressed or further assistance is required, contact Siemens Customer Support.

Problem	Solution
Unable to Log into EWI	Make sure the user name and password are correct. If the user name is incorrect, use a different user name or add the user name to EWI. For more information about adding users, refer to Section 3.8.2, "Adding/Deleting a User" .
RUGGEDCOM ELAN Does Not Start	Problems with starting the RUGGEDCOM ELAN are typically associated a configuration error (e.g. IP address collision, port out of range, etc.) or a missing feature key. To identify the source, do the following: • Log into EWI and review the status of the RUGGEDCOM ELAN server. For more information, refer to Section 3.3, "Determining the Overall Status" . If none of the devices have started, an error occurred during startup. A TIE error will also be displayed if there was an internal error. • Review the system logs for related errors. For more information, refer to Section 3.7.1, "Viewing System Logs" . • If needed, capture the support logs and forward them to Siemens Custom Support for assistance.
Communication Failure with IED/RTU Device	A communication failure with an IED or RTU device is typically caused by one of the following problems: • The IP address is either invalid or not defined. For more information about configuring the IP address for an IED/RTU device, refer to either Section 4.9, "Managing Server Devices" or Section 4.10, "Managing Client Devices" . • Network issues. • The communication definition in Maestro is invalid. • Polling is not configured for the IED or RTU device. For more information about configuring polling, refer to Section 4.11, "Managing Polling Templates" .
Communication Failure with a RUGGEDCOM ELAN Server	A communication failure with a RUGGEDCOM ELAN server is typically caused by one of the following: • Physical connection with the RUGGEDCOM ELAN server • Protocol licensing • A configuration error with a virtual device (or VRTU)
Redundant RUGGEDCOM ELAN Servers Not Communicating	If redundant RUGGEDCOM ELAN servers are not communicating with one another, there may be networking issues or issues with the servers themselves. For the latter, do the following: 1. Make sure both RUGGEDCOM ELAN servers are running. 2. Make sure both RUGGEDCOM ELAN servers are configured to be a redundant pair. For more information, refer to Section 4.6.4, "Configuring a RUGGEDCOM ELAN Server" . 3. Make sure the redundant pair is accessible via the network.
Unable to Download a Configuration to a RUGGEDCOM ELAN Server	Issues with downloading configurations to RUGGEDCOM ELAN Server from Maestro are often related to the following: • External access the RUGGEDCOM ELAN configuration database is not configured or not configured properly. For more information, refer to Section 3.11.3, "Configuring External Access" . • The supplied user name and/or password is incorrect. • Invalid feature keys. For more information about feature keys, refer to Section 3.9, "Managing ELAN Feature Keys" .

Problem	Solution
	• The IP address and/or port for the RUGGEDCOM ELAN is incorrect. For more information about configuring the IP address and port for a RUGGEDCOM ELAN server, refer to Section 4.6.4, “Configuring a RUGGEDCOM ELAN Server” . • A version mismatch between Maestro and RUGGEDCOM ELAN. For more information about which version of Maestro is compatible with RUGGEDCOM ELAN v8.5, refer to the section called “System Requirements” .
Maestro Fails to Start or Displays an Exception (e.g. JDBC Error)	When Maestro exhibits difficulties starting, it may be related to a corrupted database. The RUGGEDCOM ELAN configuration database can become corrupted when a database operation fails to complete properly. If possible, attempt to load a previous version of the database. Otherwise, contact Siemens Customer Support.
Maestro Throws a Null Pointer or Generic Exception	Null point and generic exceptions are thrown when an unknown behavior is encountered. If Maestro throws an exception during operation, immediately restart the application. All configuration changes made previously by the user will have been saved automatically. To help Siemens improve RUGGEDCOM ELAN, send the latest support and Maestro logs to Siemens Customer Support. For more information, refer to Section 3.7, “Managing Logs in EWI” and Section 4.4, “Managing Logs in Maestro” .