SIEMENS

RUGGEDCOM EXPLORER v1.5

User Guide

Preface

Introduction 1

User Interface 2

Theory Of Operation 3

RCEXPLORER.ini Configuration File A

10/2015
RC1071-EN-03

Disclaimer Of Liability

Siemens has verified the contents of this manual 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

ROX™, Rugged Operating System On Linux™, CrossBow™ and ELAN™ are trademarks of Siemens Canada Ltd. ROS® is a registered trademark 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 EXPLORER 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

Siemens Canada Ltd.
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone

Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail

ruggedcom.info.i-ia@siemens.com

Web

www.siemens.com/ruggedcom

Table of Contents

Preface v
Alerts v
Accessing Documentation v
Training vi
Customer Support vi

Chapter 1
Introduction 1
1.1 Features 1
1.2 Use Cases 1
1.3 System Requirements 2
1.4 Installation Notes 2
1.5 Compatibility/Operating Requirements 3

Chapter 2
User Interface 5
2.1 Initialization 5
2.2 Main Window 5
2.2.1 Main Window Display 6
2.2.1.1 Device Display Table 6
2.2.1.2 Color-Coded Indicators 7
2.2.1.3 Operations on Table Entries 7
2.2.1.4 Main Window Display Columns 8
2.2.2 Main Window Buttons 9
2.2.3 Main Window Menu Bar 10
2.3 Device Discovery 13
2.3.1 Auto Discovery 14
2.3.1.1 Auto Discovery Access Configuration 14
2.3.2 Manual Discovery 15
2.3.2.1 IP Address Range Discovery/Validation 16
2.3.3 Rescanning Discovered Devices 17
2.4 Device Configuration 17
2.4.1 Single Device Configuration 17
2.4.2 Group Device Configuration 18
2.5 Device Control 20

2.5.1 Download 20
2.5.2 Upload 21
2.5.2.1 Upload Process Sequence 23
2.5.3 Maintenance 24
2.5.4 Progress Indication 25
2.6 Device Export 27
2.7 Device Import 27
2.7.1 Importing Devices 28
2.7.2 Adding Devices Individually 29
2.7.3 Adding Multiple Devices 29

Chapter 3
Theory Of Operation 31
3.1 Device Discovery Methods 31
3.1.1 Automatic (RCDP-based) Device Discovery 31
3.1.2 Manual (TCP/IP-based) Device Discovery 31
3.1.3 RCDP Versus TCP/IP Discovery Comparison 32
3.2 Security Considerations 32
3.3 Duplicate Instance Detection 33

Appendix A
RCEXPLORER.ini Configuration File 35
A.1 Auto Configuration Parameters 35
A.2 Logging Parameters 35
A.3 General Parameters 35

Preface

This guide describes the RUGGEDCOM EXPLORER software utility for the discovery, initial configuration and general maintenance of ROS and RUGGEDCOM server networking products.

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.

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.

Accessing Documentation

The latest Hardware Installation Guides and Software User Guides for most RUGGEDCOM products are available online at www.siemens.com/ruggedcom.

For any questions about the documentation or for assistance finding a specific document, contact a Siemens sales representative.

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.

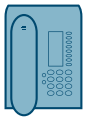
For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

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:

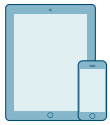
Online

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

RUGGEDCOM EXPLORER is a lightweight, standalone tool providing limited management capabilities of ROS devices. It allows a technician to discover, identify and configure all ROS-based devices. The tool will only allow for the configuration of a small number of parameters to be discussed in detail later in this document.

Using the RUGGEDCOM proprietary Layer 2 RUGGEDCOM Discovery Protocol (RCDP), RUGGEDCOM EXPLORER is able to discover and configure ROS-based devices irrespective of their IP network configuration, including devices having no IP configuration at all.

RUGGEDCOM EXPLORER's Automatic Discovery mode requires RCDP support to be present in devices to be discovered. This requires that devices be running ROS version 3.7 or newer. RCDP is enabled on ROS-based devices by default when they are shipped from the factory.

Section 1.1
Features

- Automatic discovery of new, unconfigured RUGGEDCOM devices running ROS version 3.7.0 or greater using RCDP over Ethernet.
- Manual discovery of RUGGEDCOM devices running ROS versions prior to 3.7.0 using TCP/IP.
- Basic configuration of IP addressing and system identification parameters.
- Bulk firmware updating of multiple ROS-based devices.
- Summary display of discovered devices, their status and some basic parameters.
- Easy identification of devices via control of panel LEDs.
- Easy manual importation of devices from a device list.

Section 1.2
Use Cases

Some common uses of RUGGEDCOM EXPLORER are:

- *Commissioning of new devices:* Using RCDP, RUGGEDCOM EXPLORER allows a network of ROS devices to be commissioned in place in the network with no prior configuration necessary. It is capable of discovering and configuring ROS devices that have been taken directly from the factory and connected to the network.
- *Bulk configuration or reconfiguration:* RUGGEDCOM EXPLORER can be used to modify the network and identification configuration parameters of one or multiple ROS devices, either one at a time, or using a template-based auto-incrementing tool.
- *Asset reporting:* RUGGEDCOM EXPLORER can generate a report of ROS-based network device assets on a network segment. If RCDP is supported on all devices, RUGGEDCOM EXPLORER need not have any prior knowledge of IP addressing used by ROS devices.

- *Network debugging:* RUGGEDCOM EXPLORER can be used to report the occurrence of duplicate IP addresses, or of inconsistencies in IP address allocation among ROS devices. Note that RCDP support is required in order to detect certain IP addressing misconfigurations.
- *Bulk firmware upgrade:* RUGGEDCOM EXPLORER can be used to upgrade the firmware of one or multiple devices at once.
- *System backup:* The configuration, firmware, log, and other ancillary files of one or multiple devices can be retrieved and archived in a single step.
- *Diagnostic data retrieval:* Diagnostic data (system logs and alarms) from one or multiple devices can be retrieved and archived in a single step.

Section 1.3
System Requirements

RUGGEDCOM EXPLORER is a Java-based application with a graphical user interface that that must be installed and run with administrative privileges on a computer running Microsoft Windows. It has been tested against and verified to operate correctly under Microsoft Windows XP Service Pack 3, Windows 7, Windows 8 (32 and 64 bit) and Windows 10 (64 bit).

RUGGEDCOM EXPLORER must be installed and run on a computer with an Ethernet network card. The network card must be configured to use TCP/IP and have a valid IPv4 address.

An Internet connection is not required to install and run RUGGEDCOM EXPLORER but a Web browser is required to make use of the integrated online Help (accessed via Help links within the software).

IMPORTANT!
Use RUGGEDCOM EXPLORER in a secured environment with controlled and monitored network access and local machine access. This is because RUGGEDCOM EXPLORER is prone to Denial of service attacks when flooded with maliciously crafted RCDP packets for the duration of the attack. In such a case, you would not be able to configure new ROS devices.

Section 1.4
Installation Notes

The installation program contains the RUGGEDCOM EXPLORER application, integrated online Help, PDF documentation, and all supporting software libraries required by the application. The RUGGEDCOM EXPLORER installation program unpacks all files into a user-selectable directory.

NOTE
*The online Help is displayed in a Web browser running with full administrator privileges. During installation, you have the option to disable the online Help. Select **No** when asked if you want to install the user guide, and this will disable the online Help.*

NOTE
As part of the RUGGEDCOM EXPLORER software installation, WinPcap (the Windows Packet Capture Library), is also installed. If WinPcap is already installed, its installation routine will ask whether to continue or to cancel the WinPcap installation. Selecting "Cancel" at this point cancels the reinstallation of WinPcap, and not the installation of RUGGEDCOM EXPLORER.

Section 1.5

Compatibility/Operating Requirements

RUGGEDCOM EXPLORER is available in two different versions:

- The *Non-Controlled* version of RUGGEDCOM EXPLORER contains support for the RSH and TFTP protocols for remote command and file transfer. The main window banner of the *Non-Controlled* version is marked "NC".
- The *Controlled* version additionally contains support for the SSH and SFTP protocols.

NOTE
ROS has a three-digit version numbering system of the form X.Y.Z, where:

- *X represents the major revision number.*
- *Y represents the minor revision number.*
- *Z represents the patch level.*

RUGGEDCOM EXPLORER, and the different discovery methods it supports, have different ROS version requirements from devices that it is to discover and manage:

- The Controlled and Non-controlled versions require ROS v3.5.3 or newer.
- The Automatic Discovery mode requires RCDP support, which is present in ROS v3.7.0 and newer.

In addition, it is assumed that no VLANs (tagged or untagged) have been configured in the devices to be discovered and managed by RUGGEDCOM EXPLORER. In other words, ROS devices must have default VLAN settings.

2 User Interface

Section 2.1
Initialization

When RUGGEDCOM EXPLORER is run for the first time on a computer system that has more than one network interface, it will prompt the user to select a network interface to use:

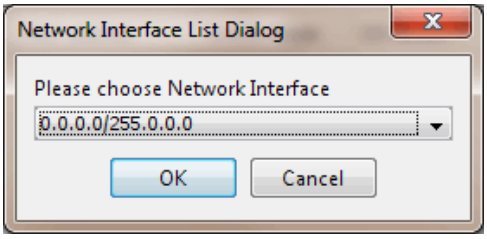


Figure 1: Network Interface List Dialog Box

If the computer system has only one network interface, this dialog box will not be displayed.

Section 2.2
Main Window

The RUGGEDCOM EXPLORER main window is displayed upon program initialization. RUGGEDCOM EXPLORER configuration and control, device discovery, upload, download and configuration, are all accessed via buttons and menu items located in the main window. Devices discovered by RUGGEDCOM EXPLORER are displayed in real time in the table that occupies most of the main window.

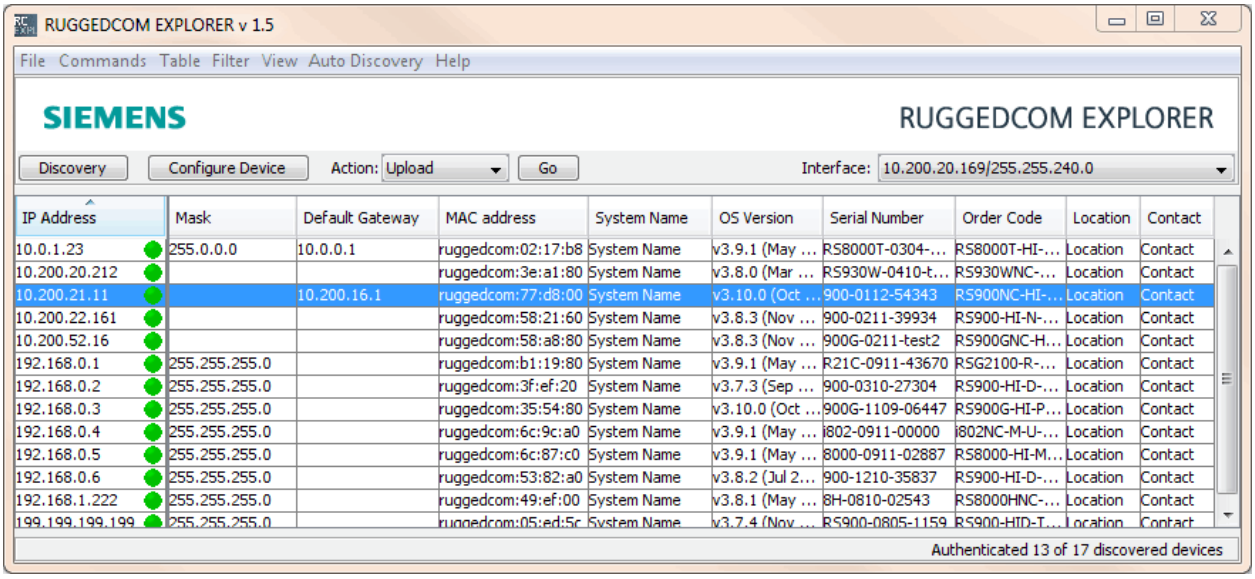


Figure 2: Main Window

Section 2.2.1

Main Window Display

The main RUGGEDCOM EXPLORER window consists chiefly of a list of discovered RUGGEDCOM devices that is updated in real time. As devices are discovered, they are displayed in the list and sorted by IP address. Each row in the table contains information about the corresponding device.

Section 2.2.1.1

Device Display Table

The display is separated into two panes:

- The *Status Pane*, on the left, includes only a column for IP Address and a the section called “Status Lamp Icon”. The size of this column is static and does not allow resizing.
- The *Information Pane*, to the right, includes all the remaining information columns (see the list below).

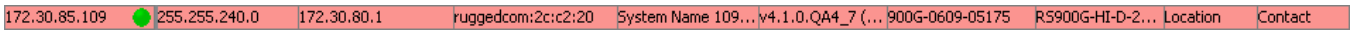
The Information Pane is customizable in several ways:

- Each column may be moved in relation to the others by clicking on the column title and dragging it left or right across the pane.
- The entire display may be sorted on the basis of any one of the columns (including the IP Address column). Clicking on a column title will sort the whole list in increasing order of the items in that column. Clicking again will sort in decreasing order.
- Each column may be resized by clicking and dragging the rightmost edge of a column title.
- Selected columns may be hidden altogether by disabling them in the the section called “View Menu”. Note that the "MAC Address" column cannot be hidden since it is the only piece of data that is guaranteed to be unique among devices.

Section 2.2.1.2
Color-Coded Indicators

Row Color

The row containing the data for a given device is displayed in a different background color depending on its status:

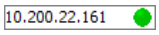
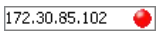
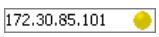
-  An IP address field displayed in a flashing yellow background indicates that the device has accepted the "Flash LEDs" command. This state persists until a "Stop flashing LEDs" command is issued or until it reaches its internal timeout (by default 5 minutes). This state is displayed at the same time as one of the others described below.
- 

  Entries displayed in a red background have duplicate IP addresses. When the device's IP address has been reconfigured, its background will revert to plain white.
- 

  Entries displayed in a blue background have been selected for further manipulation. Device selection is made by clicking on an entry, holding down the Shift key and selecting a range of entries, holding down the Ctrl key and clicking on additional entries, in the standard Windows interface style. Details of what can be done with selected devices will be discussed in detail throughout this guide.

Status Lamp Icon

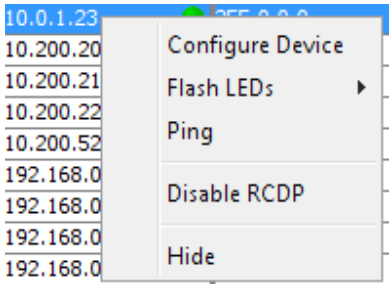
The Status Pane contains a lamp icon to the right of the IP address of the device, indicating the status of the device. Moving the mouse to pause over this icon will cause a "tool-tip" window to be displayed with additional status information. The status icon is displayed in one of three colors depending on the status of the device:

-  An IP address field displayed with a green lamp icon indicates that RUGGEDCOM EXPLORER has successfully established communication with the device.
-  An IP address field displayed with a red lamp icon indicates that RUGGEDCOM EXPLORER has not been able to establish communication with the device.
-  An IP address field displayed with a yellow lamp icon indicates that RUGGEDCOM EXPLORER has detected some error condition on the device, for example, that a file transfer has failed.

Section 2.2.1.3
Operations on Table Entries

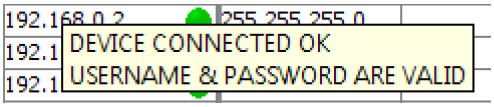
Device entries in the Device Display Table support several operations and shortcuts:

- *Clicking* on a device entry selects it for further operations using the Section 2.2.3, “Main Window Menu Bar” or the Section 2.2.2, “Main Window Buttons”.
- *Double-clicking* on a device entry brings up the Section 2.4.1, “Single Device Configuration” dialog box.
- *Right-clicking* on a device entry brings up a pop-up menu:



This pop-up menu contains the following: a link to the Section 2.4.1, “Single Device Configuration” dialog box; the ability to start or stop flashing LEDs on the device; a single "ping" test to verify that the device is reachable via IP; and the ability to to disable RCDP.

- *Hovering* over an IP address field displays a tool-tip message containing a brief summary of the corresponding device's status, for example:



Section 2.2.1.4
Main Window Display Columns

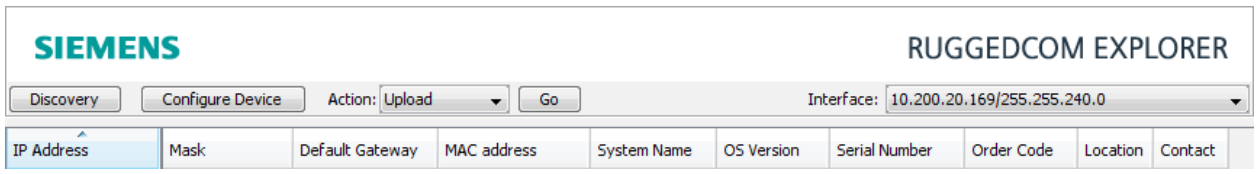


Figure 3: Main Window Display Columns

RUGGEDCOM EXPLORER's main window displays columns of information captured from a device when the device is first discovered.

Parameter	Description
IP Address	The IP address of the discovered device. RUGGEDCOM EXPLORER can discover devices with duplicate IP addresses when they are discovered using the Auto Discovery method. Devices with duplicate IP addresses will be highlighted in red to visually differentiate them from unique IP addresses. This is the only fixed column on the main window, meaning that it cannot be moved from its location. The information in this column can be modified by RUGGEDCOM EXPLORER.
Mask	The IP address mask of the discovered device. The information in this column can be modified by RUGGEDCOM EXPLORER.
Default Gateway	The default IP gateway of the discovered device. The information in this column can be modified by RUGGEDCOM EXPLORER and may be blank.

Parameter	Description
MAC Address	The MAC address of the discovered device. This is a fixed value and therefore this column is not modifiable by RUGGEDCOM EXPLORER.
System Name	The configured system name of the discovered device. This column could contain the default value of the device ("System Name") or any string that has been configured. The information in this column can be modified by RUGGEDCOM EXPLORER.
OS Version	This column will display the current running version of ROS on the discovered device. The information in this column cannot be modified by RUGGEDCOM EXPLORER.
Serial Number	The unique serial number assigned to this device by Siemens at the factory. The information in this column cannot be modified by RUGGEDCOM EXPLORER.
Order Code	The order code of this device as set by Siemens at the factory. The information in this column cannot be modified by RUGGEDCOM EXPLORER.
Location	The configured location string of the discovered device. This column could contain the default value of the device ("Location") or any string that has been configured. The information in this column can be modified by RUGGEDCOM EXPLORER.
Contact	The configured contact information of the discovered device. This column could contain the default value of the device ("Contact") or any string that has been configured. The information in this column can be modified by RUGGEDCOM EXPLORER.

Section 2.2.2
Main Window Buttons

Figure 4: Main Window Buttons

Several buttons and controls are located in a row above the main display window. These provide rapid and convenient access to the most commonly required functions of RUGGEDCOM EXPLORER.

Parameter	Description
Discovery	Clicking *Discovery* on the main window launches the Automatic and Manual device discovery processes. Please refer to Section 2.3, "Device Discovery" for more detail.
Configure Device / Group	This button is sensitive to context: • Configure Device is displayed when no discovered devices are selected. • Configure Device is displayed when a single discovered device is selected. Clicking this button displays the Section 2.4.1, "Single Device Configuration" dialog box

Parameter	Description
	• Configure Group is displayed when multiple discovered devices are selected. Clicking this button displays the Section 2.4.2, “Group Device Configuration” dialog box.
Action	The *Action* section on the main window gives options for the file transfer and maintenance features of RUGGEDCOM EXPLORER. The pull-down menu has three options: • Upload - Upload files from RUGGEDCOM EXPLORER to one or more ROS devices. • Download - Download files from one or more ROS devices to RUGGEDCOM EXPLORER. • Maintenance - Gives the following three options: ▪ Clear logs ▪ Reset device ▪ Load factory defaults
Interface	The *Interface* list on the main window is used to select the network interface to be used by RUGGEDCOM EXPLORER for network discovery and all device access except SSH. The interface selection may be changed at any time without the need to restart RUGGEDCOM EXPLORER.

Section 2.2.3
Main Window Menu Bar

File Menu

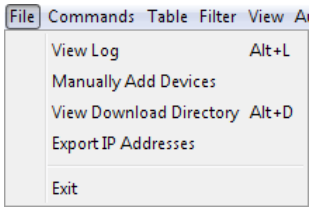


Figure 5: File Menu

Parameter	Description
View Log	Open RUGGEDCOM EXPLORER's log file in a text editor.
Manually Add Devices	Import devices into RUGGEDCOM EXPLORER. (For more information, see Section 2.7, “Device Import”.)
View Download Directory	Open the download directory, into which RUGGEDCOM EXPLORER writes files downloaded from discovered devices.
Export IP Addresses	Export a device list from RUGGEDCOM EXPLORER. (For more information, see Section 2.6, “Device Export”.)
Exit	Terminate RUGGEDCOM EXPLORER.

Commands Menu

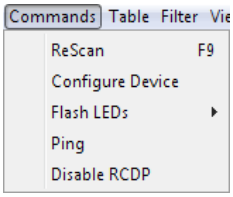


Figure 6: Commands Menu

As with the buttons on the main window, some items in the *Commands* menu are relevant only when a device is selected in the list. When more than one device is selected in the list, some menu items change name and function. These special cases are noted below.

Parameter	Description
Rescan	Rescan all discovered devices and update the parameters displayed in the main window.
Configure Device/Group	This menu item is displayed as *Configure Device* if only one device is highlighted in the main window, and opens the Section 2.4.1, "Single Device Configuration" dialog box. If more than one device is highlighted in the main window, the menu item is displayed as *Configure Group*, and opens the Section 2.4.2, "Group Device Configuration" dialog box.
Flash LEDs	The Flash LEDs menu selection will start and stop a visual identifier on the selected devices. This visual identification is in the form of LEDs flashing on the selected devices. This option is not available for devices discovered using the manual discovery mechanism.
Ping	Ping a single device to see if it is reachable. This menu item is only displayed if only one device is highlighted in the main window. Note that ping is unreliable in certain IP addressing situations, but if Automatic Discovery was used to discover the device, it is still accessible using RUGGEDCOM EXPLORER.
Disable RCDP	Disable RCDP on the switch.

Table Menu

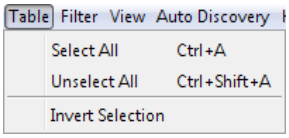


Figure 7: Table Menu

Parameter	Description
Select All	Select (highlight) all devices displayed in the main window.
Unselect All	Unselect (remove the highlights) from all selected devices.
Invert Selection	Invert selection will select all currently unselected devices and unselect all currently selected devices as seen on the main window.

Filter Menu

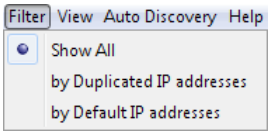


Figure 8: Filter Menu

The *Filter* menu controls the display of discovered devices in the main window. Only one of the three following filters is selected at once.

Parameter	Description
Show All	Display all discovered devices.
by Duplicated IP addresses	Display only devices with duplicate IP address settings.
by Default IP addresses	Display only devices with the default IP address set. Note that ROS devices ship with a default IP address of 192.168.0.1.

View Menu

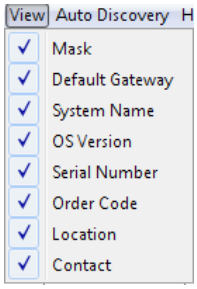


Figure 9: View Menu

The settings in the *View* menu select the fields that are displayed for each discovered device in the main window. Clicking on an item in the view menu toggles its state. A check mark beside the item indicates that a column for the corresponding field will be displayed in the main window.

- Mask
- Default Gateway
- System Name
- OS Version
- Serial Number
- Order Code
- Location
- Contact

Auto Discovery Menu

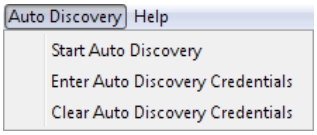


Figure 10: Auto Discovery Menu

RUGGEDCOM EXPLORER is capable of automatically discovering devices using the RUGGEDCOM Discovery Protocol (RCDP), an Ethernet-based protocol that allows RUGGEDCOM EXPLORER to discover and manage devices irrespective of their IP network configuration. At the time of writing, only ROS-based devices running ROS version 3.7.0 or greater have support for RCDP.

Parameter	Description
Start Auto Discovery	Starts the automatic discovery.
Enter Auto Discovery Credentials	Allows a user to enter user name and password credentials to validate RUGGEDCOM EXPLORER on the target devices. As many credentials can be entered as required. The user names and passwords entered are kept secure in RUGGEDCOM EXPLORER and not retained by the application after RUGGEDCOM EXPLORER is shut down. Credentials can be entered at any time, even after discovery is run, to display devices found by RUGGEDCOM EXPLORER.
Clear Auto Discovery Credentials	Clicking on this menu entry will clear all the credentials known by RUGGEDCOM EXPLORER.

Help Menu

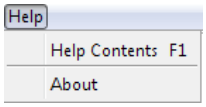


Figure 11: Help Menu

Parameter	Description
Help Contents	Display the HTML format of this User Guide.
About	Display brief information about RUGGEDCOM EXPLORER.

NOTE
*Selecting **No** for the option to install the user guide during installation disables the online Help. If the online Help is disabled, nothing will happen when you select **Help Contents**.*

Section 2.3
Device Discovery

RUGGEDCOM EXPLORER supports two device discovery mechanisms:

- *Automatic Discovery* uses the RUGGEDCOM Discovery Protocol (RCDP) to discover devices running version 3.7.0 of ROS or newer.
- *Manual Discovery* uses TCP/IP to find devices running ROS versions older than 3.7.0. The manual discovery process is optional and is enabled by specifying an IP address range to scan for devices.

Section 2.3.1
Auto Discovery

The Auto Discovery mechanism is started directly from the the section called “Auto Discovery Menu” or in parallel with a Section 2.3.2, “Manual Discovery”. It relies only on having an Ethernet connection to the ROS-based devices to be discovered. Devices may have nothing more than factory settings, and require no TCP/IP configuration.

Section 2.3.1.1
Auto Discovery Access Configuration

RUGGEDCOM EXPLORER attempts to authenticate itself with every device that it discovers in order to access device parameters. It uses default authentication parameters to access ROS-based devices whose authentication parameters have not been changed from factory defaults.

In order to be able to access devices whose authentication parameters have been configured away from factory defaults, RUGGEDCOM EXPLORER must be provided with authentication credentials for those devices. Multiple sets of user name / password credentials may be configured in RUGGEDCOM EXPLORER for use during the Auto Discovery process. Several sets of authentication credentials may be added to RUGGEDCOM EXPLORER using the *Auto Discovery Access* dialog box, accessible by selecting *Enter Auto Discovery Credentials* from the the section called “Auto Discovery Menu”.

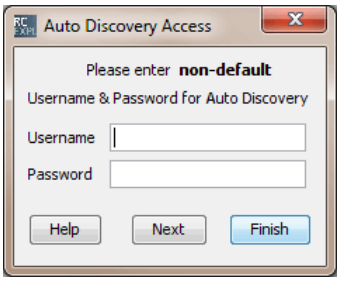


Figure 12: Auto Discovery Access Dialog Box

Parameter	Description
Username	A user name to add to RUGGEDCOM EXPLORER's database to be used during Auto Discovery.
Password	A password to add to RUGGEDCOM EXPLORER's database to be used during Auto Discovery.
Next	Clicking *Next* adds the user name and password currently in the dialog and clears the dialog box's contents to be ready to accept another set of credentials.

Parameter	Description
Finish	Clicking *Finish* adds the user name and password currently in the dialog and exits the dialog box.

All authentication credentials added to RUGGEDCOM EXPLORER using this dialog box may be deleted at once by selecting *Clear Auto Discovery Credentials* from the the section called “Auto Discovery Menu”.

Section 2.3.2
Manual Discovery

Both the Automatic and Manual device discovery processes are initiated using the *Manual Device Discovery* dialog box, which is accessible from the Section 2.2.2, “Main Window Buttons”. The Automatic Discovery mechanism is run as a part of every discovery process, and has no configurable parameters. The Manual Discovery process must be configured (via the specification of an IP range using this dialog box) in order to enable it to run.

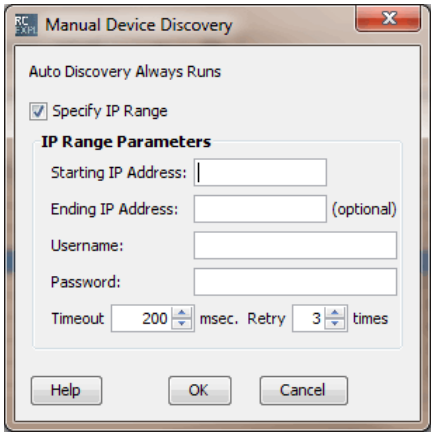


Figure 13: Device Discovery Dialog Box

Parameter	Description
Specify IP Range	Checking the box will enable Manual Discovery. If this box is not checked, then only the Auto Discovery will run.
Starting IP Address	Starting IP address for the ping sweep.
Ending IP Address	Ending IP address for the ping sweep. If this field is left empty, then only one device will be pinged (the Starting IP Address).
Username	The user name that RUGGEDCOM EXPLORER will use when validating itself on discovered devices.
Password	The password that RUGGEDCOM EXPLORER will use when validating itself on discovered devices.
Timeout	The ping timeout value used by Manual Discovery.
Retry	The number of ping retries before RUGGEDCOM EXPLORER determines that no device exists at a given IP address.
OK	Clicking OK will start the discovery process. Devices discovered via RCDP will be entered directly into the Section 2.2.1.1, “Device

Parameter	Description
	Display Table". Note that if a given device is discovered via TCP/IP and also via RCDP, then RCDP will take precedence and will be used for subsequent access to the device.
Cancel	Exit the dialog box and do not perform a discovery process.

NOTE

Since ROS allows ten failed password attempts before disallowing logins, please do not perform multiple manual device discovery runs on the same IP range in order to accommodate different sets of authentication credentials.

If possible, try to group the IP ranges to discover by common authentication credentials. In the extreme, in which every device had different credentials, it would be necessary to perform a manual discovery for each device, in an IP range restricted to each device.

NOTE

Discovering devices in IP address ranges that are not on the locally connected network requires that a default gateway be correctly configured on the PC running RUGGEDCOM EXPLORER.

Section 2.3.2.1

IP Address Range Discovery/Validation

If a manual device discovery is configured to run (by specifying *IP Range Parameters* in the Figure 13), the *IP Address Range Discovery/Validation* dialog box will report its progress.

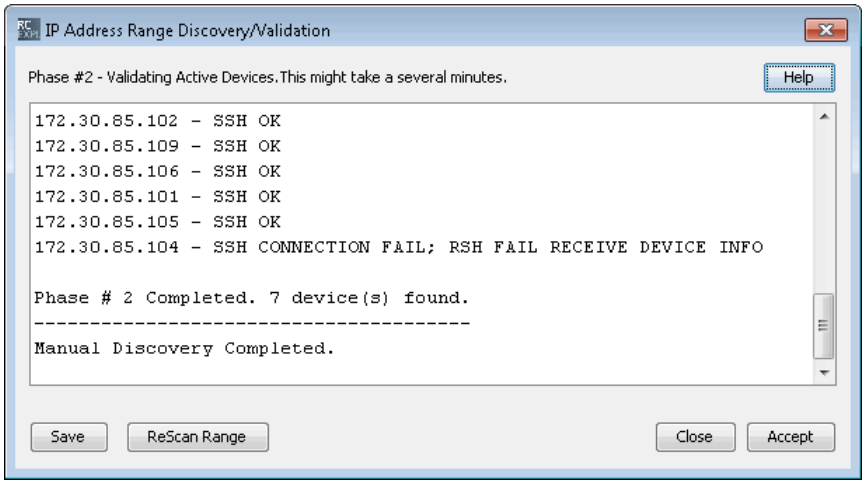


Figure 14: IP Address Range Discovery/Validation

The manual discovery process is carried out in two phases:

- During Phase 1, RUGGEDCOM EXPLORER determines which devices in the selected IP address range respond to IP "ping" requests.
- During Phase 2, RUGGEDCOM EXPLORER probes those devices it discovered during phase 1 to verify that it can access them.

Section 2.3.3
Rescanning Discovered Devices

RUGGEDCOM EXPLORER can be made to update its information about the devices it has already discovered by selecting *Rescan* from the the section called “Commands Menu”. If a device was discovered using RCDP (Auto Discovery), it will be rescanned using RCDP. If it was discovered using TCP/IP (Manual Discovery), it will be rescanned using TCP/IP.

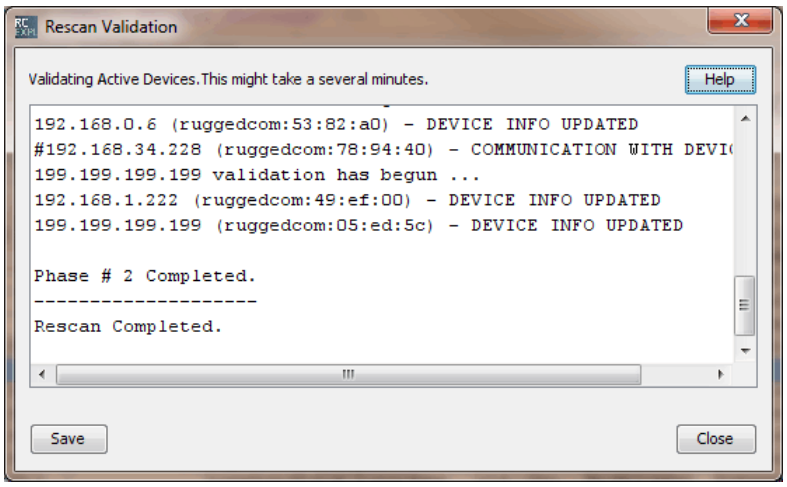


Figure 15: Rescan Validation

Section 2.4
Device Configuration

Depending on whether one or multiple discovered devices are selected in the main window Section 2.2.1.1, “Device Display Table”, either the *Configure Device* or the *Configure Group* button will be displayed, respectively. A different dialog box is presented in each case, as detailed in the next two sections.

Section 2.4.1
Single Device Configuration

RUGGEDCOM EXPLORER allows a user to modify certain configuration parameters on a device. The single device dialog box below shows the parameters available for configuration.

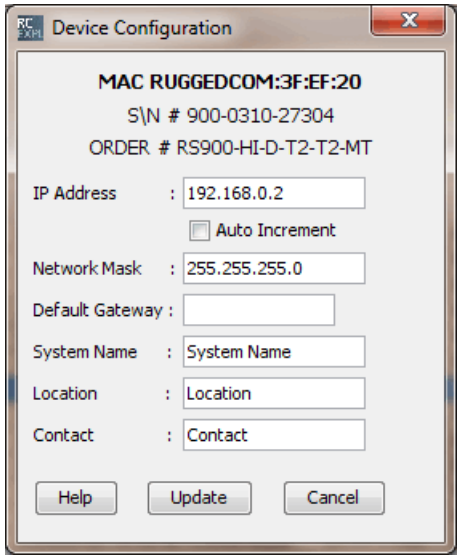


Figure 16: Device Configuration Dialog Box

Parameter	Description
IP Address	The IP address to be configured.
Auto Increment	If this box is checked, the IP address will be automatically incremented next time this dialog box is opened.
Network Mask	The network mask to be configured.
Default Gateway	The default gateway to be configured.
System Name	The system name to be configured
Location	The location to be configured.
Contact	The contact information to be configured.
Update	Clicking Update will commit the requested configuration changes to the selected device.
Cancel	Clicking Cancel will exit this dialog, discarding any specified configuration changes.

NOTE
Attempting to configure an IP address that is already in use elsewhere in the network will cause RUGGEDCOM EXPLORER to report an error.

Section 2.4.2
Group Device Configuration

RUGGEDCOM EXPLORER allows a user to select multiple devices in the user interface for group configuration. When multiple devices are selected and Group Configuration is chosen, the dialog box seen below is displayed. Group configuration enables the automated configuration of the selected devices.

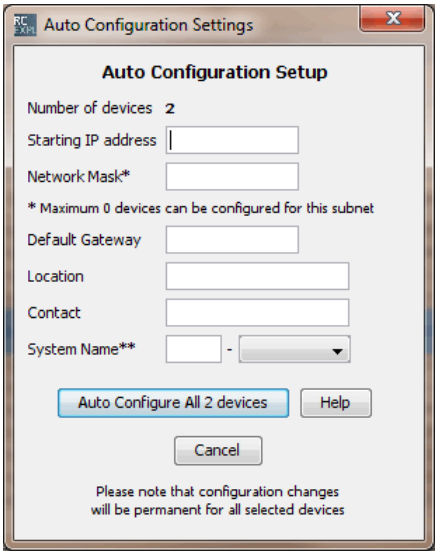


Figure 17: Group Configuration Dialog Box

Parameter	Description
Number of Devices	This field displays the number of devices that were selected in the main window for configuration.
Starting IP address	The selected devices will be assigned consecutive addresses starting with this IP address. IP addresses in the sequence that are detected to already be in use are simply skipped over and not used.
Network Mask	The specified mask will be applied to all selected devices.
Default Gateway	The specified default gateway will be applied to all selected devices.
Location	The specified location will be applied to all selected devices.
Contact	The specified contact information will be applied to all selected devices.
System Name	This field is used as a template to assign a different system name to each discovered device. The first field is a static prefix to every device name and the second field is selected from a pull-down for the variable, template-based portion of the system name. Two templates are available: • $ip - the IP address of the device. • $sequence - a sequence number, automatically incremented for each device. A sample system name based on the specified prefix and template is displayed below the *System Name* field.
Auto Configure All Devices	Clicking on this button will start the auto-configuration process.
Cancel	Clicking Cancel will exit this dialog, discarding any specified configuration changes.

Section 2.5
Device Control

RUGGEDCOM EXPLORER is capable of performing a selected set of operations on devices it has discovered. One or more devices may be selected by highlighting them in the Main Window Section 2.2.1.1, “Device Display Table”. The following operations, described in subsequent sections, are performed on all highlighted devices:

- file downloads
- file uploads
- system management commands

Section 2.5.1
Download

The File Download dialog box presents a choice of files that may be downloaded from selected ROS-based devices, along with the option to create an archive file of all downloaded files.

RUGGEDCOM EXPLORER downloads files from multiple selected devices concurrently.

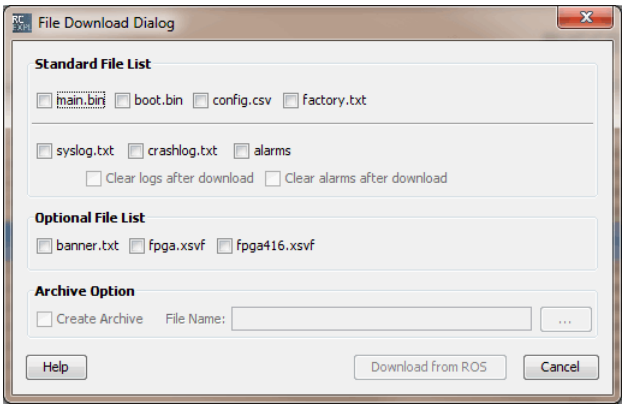


Figure 18: File Download Dialog Box

Files To Download

The files that may be downloaded from a ROS device are:

- `main.bin` - the main ROS firmware image file
- `boot.bin` - the ROS bootloader firmware (very infrequently updated)
- `config.csv` - the ROS system configuration file
- `syslog.txt` - log of system events
- `crashlog.txt` - log of debilitating system events
- `alarms` - list of active alarms
- `banner.txt` - the optional ROS login banner text file
- `banner.txt` - the optional ROS login banner text file
- `fpga.xsvf` - FPGA programming image file

- `fpga416.xsvf` - Second FPGA programming image file specific to the RS416

The following files may optionally be erased from the device after having been downloaded. Note that selecting "Clear logs after download" forces the download of both "syslog.txt" and "crashlog.txt" since these may not be deleted individually.

- syslog.txt
- crashlog.txt
- alarms

Downloaded Files

Downloaded files are placed in subdirectories of the download directory (by default, this is the "downloads" subdirectory of the RUGGEDCOM EXPLORER installation directory).

Text files (configuration, logs, etc.) downloaded from a particular device are placed in subdirectories whose name contains the device's IP address. Every downloaded text file will be saved with an extended file name including a date stamp and a numeric identifier to guarantee that each downloaded file is unique. For example, the system log (syslog.txt) from a device might be saved with the following file name:

```
Syslog-20090101-000101.txt
```

Binary files are saved in the root of the download directory. Duplicate files are not downloaded; that is, if multiple devices have the same firmware version, the firmware file will only be downloaded once. Binary files will be saved with extended file names including the firmware image name and version. For example, the ROS main firmware image (main.bin) from a device running ROS version 3.6.1 would be saved with the following file name:

```
ROS-CF52_Main_v3-6-1.bin
```

When the "Create Archive" option is selected, a unique archive file name is automatically generated and presented in the "File Name" field, for example:

```
downloads\archive-20090802-181011.zip
```

This file name can be overridden by editing the field. The complete set of downloaded files is archived to this file name.

Section 2.5.2

Upload

The File Upload dialog box presents a choice of files on ROS devices that may be uploaded for replacement.

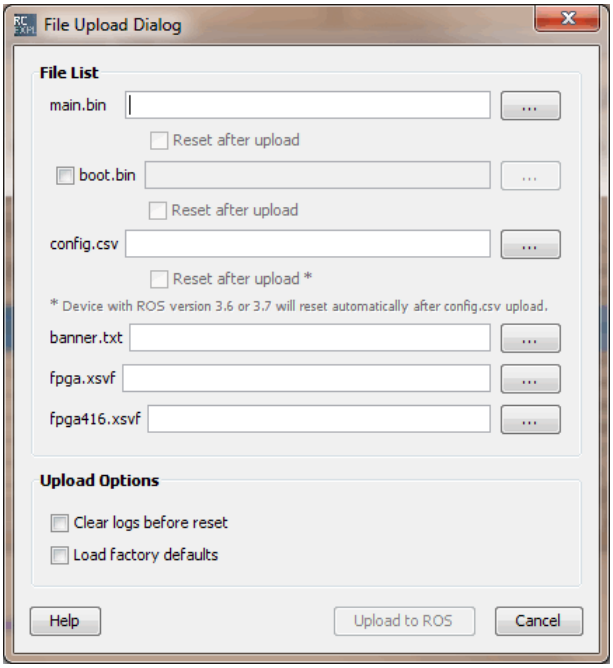


Figure 19: File Upload Dialog Box

The files that may be replaced via a file upload on a ROS device are:

- `main.bin` - the main ROS firmware image file
- `boot.bin` - the ROS bootloader firmware (very infrequently updated)
- `config.csv` - the ROS system configuration file
- `banner.txt` - the optional ROS login banner text file
- `fpga.xsvf` - FPGA programming image file
- `fpga416.xsvf` - Second FPGA programming image file specific to the RS416

RUGGEDCOM EXPLORER takes a conservative approach to uploading firmware and configuration files to many ROS-based devices at a time.

When a file upload operation is initiated on multiple devices with the reset option enabled, RUGGEDCOM EXPLORER begins by selecting a "pilot device" on which to test the complete operation before committing to performing the same operations on the whole list of selected devices. The pilot device is defined to be the selected device with the lowest numeric IP address.

If more than one file is chosen for upload at a time, they are be uploaded in the following sequence:

1. boot.bin
2. main.bin
3. config.csv
4. other files

Note that for some of these files, it will be necessary to reset the device prior to uploading the next file. RUGGEDCOM EXPLORER will automatically select the corresponding *Reset after upload* check box accordingly. The pilot / remainder sequence described above is used for `boot.bin` and `main.bin`. The `config.csv` file is uploaded sequentially, and never concurrently.

If an error occurs while uploading files to multiple ROS devices, RUGGEDCOM EXPLORER will exclude the affected device from the processing list but will continue to process the other devices in the list.

Two more options are available for the file upload process:

- Selecting *Clear logs before reset* erases the contents of `syslog.txt` and `crashlog.txt` on the ROS devices to which files are being uploaded before they are reset.
- Selecting *Load factory defaults after reset* causes factory default settings to be restored to the ROS devices to which files are being uploaded after they are reset.

NOTE
ROS devices running version 3.6 or 3.7 automatically reset upon receiving an upload of a new system configuration file, `config.csv`*.*

NOTE
When using the controlled version of RUGGEDCOM EXPLORER to upload a configuration file (`config.csv`*) from a ROS device running ROS v4.0 or older, the IP interface record should be removed from the configuration file. This is not required for newer versions of ROS.*

Section 2.5.2.1
Upload Process Sequence

Prior to updating system files on network infrastructure devices, it is important to note the sequence of firmware updates and device resets that will be performed. The sequence of updates and resets for the different files that can be uploaded to ROS devices is outlined in detail below:

- Upload `main.bin` with "Reset after upload" disabled:

  RUGGEDCOM EXPLORER uploads `main.bin` concurrently to all selected devices in one phase.

- Upload `main.bin` and/or `boot.bin` with "Reset after upload" enabled:

  In the case of multiple uploads (i.e. `main.bin` and `boot.bin`) to multiple devices, the sequence will be as follows:

  1. Upload `boot.bin` to the "pilot" device and reset it. RUGGEDCOM EXPLORER will abort the process if either the upload or the reset fails.
  2. Concurrently upload `boot.bin` to the other selected devices. Any device that fails to receive the upload is removed from the process list, but RUGGEDCOM EXPLORER will not abort the whole process.
  3. Sequentially reset and verify all remaining selected devices. RUGGEDCOM EXPLORER will abort the process if it encounters any errors in this part of the process.
  4. Repeat the steps above for `main.bin`.

- Upload `config.csv`:

  Sequentially upload `config.csv` to all selected devices, reset and verify each one in turn if "Reset after upload" is enabled. Note that devices running ROS 3.6 and 3.7 reboot unconditionally after receiving an upload of `config.csv`.

- Upload files other than `main.bin`, `boot.bin`, or `config.csv`:

  Concurrently upload the file to all selected devices.

Three examples of typical updates are summarized below:

- Uploading `boot.bin`, `main.bin`, `config.csv` and `banner.txt` with Reset after upload" enabled takes place in eight phases:

1. Upload `boot.bin` to pilot device, reset.
2. Upload `boot.bin` to remaining devices.
3. Reset all remaining devices in sequence.
4. Upload `main.bin` to pilot device, reset.
5. Upload `main.bin` to remaining devices.
6. Reset all remaining devices in sequence.
7. Upload `config.csv` sequentially to all devices, resetting each in turn.
8. Concurrently upload `banner.txt` to all devices.

- Uploading `main.bin` and `config.csv` with "Reset after upload" enabled takes place in four phases:
  1. Upload `main.bin` to pilot device, reset.
  2. Upload `main.bin` to remaining devices.
  3. Reset all remaining devices in sequence.
  4. Upload `config.csv` sequentially to all devices, resetting each in turn.
- Uploading `config.csv` and `banner.txt` with "Reset after upload" enabled takes place in two phases:
  1. Upload `config.csv` sequentially to all devices, resetting each in turn.
  2. Concurrently upload `banner.txt` to all devices.

NOTE
If a boot upgrade is required from Boot v2.15.0 or older, it is recommended to run the flashfiles defrag command from the CLI shell prior to the bootloader upgrade.

Section 2.5.3
Maintenance

RUGGEDCOM EXPLORER performs maintenance operations on multiple selected devices sequentially.

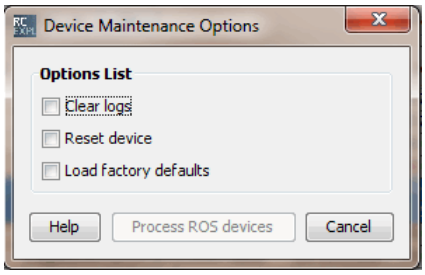


Figure 20: Device Maintenance Dialog Box

Parameter	Description
Clear logs	Delete all log files on the device.
Reset device	Perform a device reset.

Parameter	Description
Load factory defaults	Set all configurable device parameters to their factory default settings

Section 2.5.4
Progress Indication

After initiating a download, upload, or maintenance command for selected devices, a dialog box will be displayed indicating the progress relative to each device. Note that entries in green indicate devices that RUGGEDCOM EXPLORER is accessing the corresponding device using encrypted (SSH) communications and entries in blue indicate devices that it is accessing using unencrypted (RSH) communications.

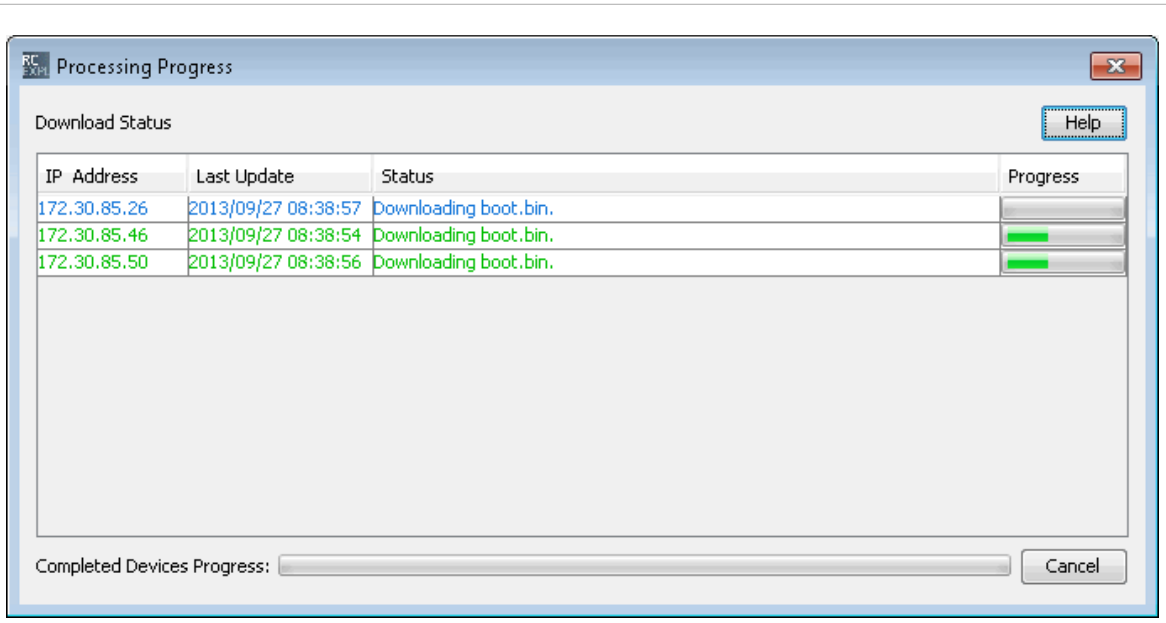


Figure 21: Progress Dialog Box (Processing in Progress)

Note the *Completed Devices Progress* bar, which indicates the proportion of devices for which RUGGEDCOM EXPLORER has completed processing. Moving the mouse over any given entry causes a tool-tip window to be displayed, indicating whether the device is being accessed using encryption.

Clicking the *Cancel* button aborts the multi-device process.

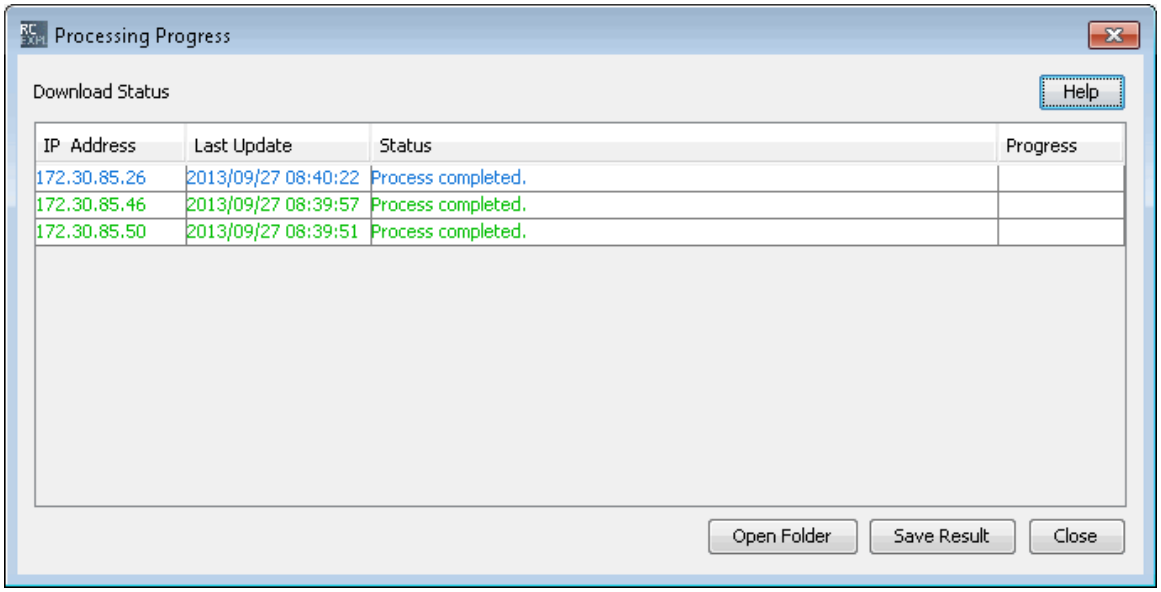


Figure 22: Progress Dialog Box (Processing Complete)

Clicking *Save Result* saves RUGGEDCOM EXPLORER log files for each processed device.

Open Folder opens a file browser in the file download directory.

NOTE

Uploading a Non-Controlled version of ROS prior to 3.8.0 to a device that is running the Controlled version will result in a lapse in (Controlled) RUGGEDCOM EXPLORER's communication with the device.

Attempting to upload a Controlled version of ROS 3.8.0 or newer to a Non-Controlled device will not succeed, and will be reported in the Process Dialog box as the error condition: "No pending version".

Attempting to upload a version of ROS firmware that is identical to that running on a device will not result in a firmware update, and will also be reported in the Process Dialog box as the error condition: "No pending version".

It is generally recommended to avoid mixing ROS versions in any of the foregoing ways.

Double-clicking on an entry in the *Processing Progress* dialog box brings up a window displaying the log for the corresponding device. The same information displayed here is also reflected in the `RCEXPLORER.log` file, although there it is interleaved with log data for all other devices.

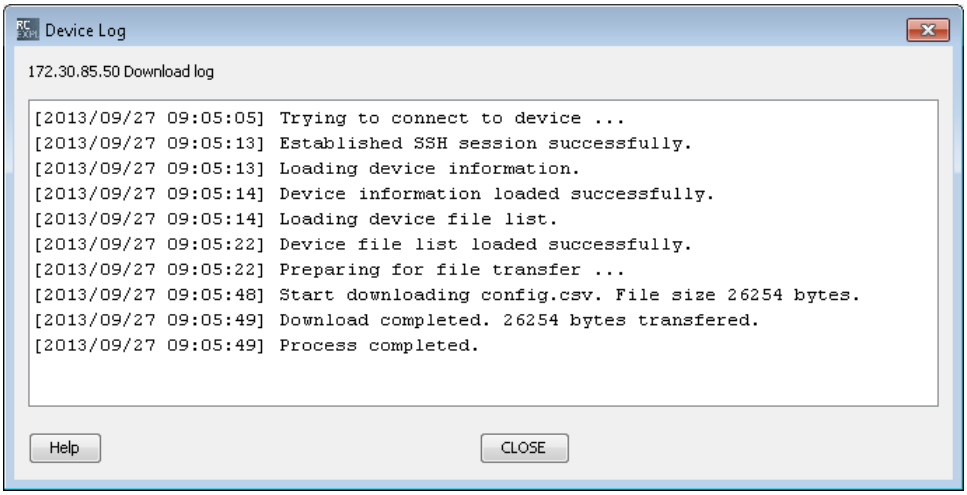


Figure 23: Device Log

Section 2.6

Device Export

A user can export a list of devices from RUGGEDCOM EXPLORER to a text file. This text file contains a list of IP addresses (one per line) which can then be edited by a user for later importation back into RUGGEDCOM EXPLORER (for more information on importing devices, see Section 2.7, “Device Import”). This eliminates the need to run a ping sweep. Users can use this function by selecting *Export IP Addresses* from the *File* menu and then saving the file to a local workstation.

Section 2.7

Device Import

Devices can be imported directly into RUGGEDCOM EXPLORER . A user can manually add device information or import a file with the device administrators’ user names and passwords, and a list of IP addresses. RUGGEDCOM EXPLORER will scan the file and add the listed devices. Device validation can be enabled if needed.

The validation process will:

- Ping the device to verify its existence
- Attempt to log on to the device to verify the user name and password
- Verify that the device is a member of the RUGGEDCOM family of devices
- Acquire information required to populate the user interface

After devices are added to RUGGEDCOM EXPLORER , you can use them in RUGGEDCOM EXPLORER as if they were discovered by any other mechanism.

NOTE
For security reasons, do not leave files with the list of IP addresses and administrator passwords where they can be discovered and used maliciously.

Section 2.7.1
Importing Devices

To import devices, do the following:

Procedure: Importing Devices

1. From the main window in RUGGEDCOM EXPLORER, click *File* on the toolbar. The *File* menu appears.

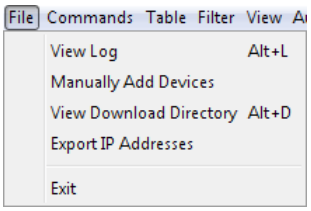


Figure 24: File Menu

2. Click *Manually Add Devices*. The *Manually Add Devices* dialog box appears.

Figure 25: Manually Add Devices Dialog Box

3. If required, click the *Validate connectivity* check box.
4. To add individual devices, go to Procedure 2.2, “Adding Devices Individually”

   OR

   To add devices in bulk, go to Procedure 2.3, “Adding Multiple Devices”.

Section 2.7.2
Adding Devices Individually

To add devices individually, do the following:

Procedure: Adding Devices Individually

1. Enter the required information in the *IP address*, *user name* and *password* fields.
2. If required, click *Next* to add another device. Repeat the previous step.
3. Click *Finish* to add the device(s) to RUGGEDCOM EXPLORER.

Section 2.7.3
Adding Multiple Devices

To add multiple devices, do the following:

Procedure: Adding Multiple Devices

1. Click *Load*. The *Select IP List File* dialog box appears.

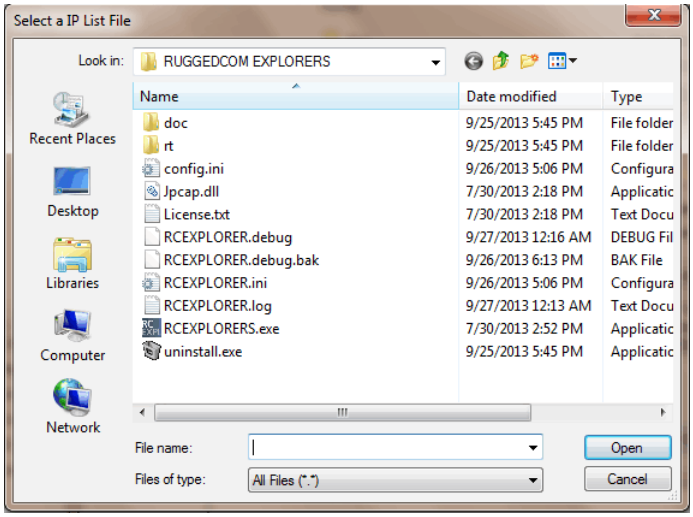


Figure 26: Select IP List File Dialog Box

2. Navigate to the location of your load file and select the file.
3. Click *Open*.

   The file can have only one of two formats as seen below:

NOTE
Only one format must be used for the entire file.

Table: File Formats

Format	Description	

Format 1	`Username admin`
	`Password  admin`
	`10.10.10.1`
	`10.10.10.2`
	`10.10.10.3`
	`10.10.10.4`
	`Password ruggedcom`
	`11.11.11.1`
	`11.11.11.2`
		Initially, you will need to enter a valid user name and password for the devices listed above. The second entry (which starts where it says Password ruggedcom) in this example does not require you to give a user name if the same user name can be used from the previous configuration.
		In this format, the first line of a group must start with the admin user name and password for the devices which immediately follow. The next several lines contain the list of IP addresses for this group. If you need to add additional credentials for a different group of IP addresses, follow the same procedure described above or only enter a password if the previous user name is the same.

Format 2	`10.10.10.1, admin, admin`
	`10.10.10.2, admin, admin`
	`10.10.10.3, admin, admin`
	`10.10.10.4, admin, admin`
	`11.11.11.1, admin, ruggedcom`
	`11.11.11.2, admin, ruggedcom`
		In this format, each line must contain an IP address, user name and administrator password for each device. This process can be repeated for each device that you want to manage in RUGGEDCOM EXPLORER.
		RUGGEDCOM EXPLORER begins adding (and if selected, validating) the devices in the list. The list of devices added to RUGGEDCOM EXPLORER will not appear until all devices in the list have been processed (including validation). This process can take a while, particularly if there are a large number of devices in the list. Each device can take about one minute to add if encrypted protocols are used and validation is selected. Validation can take longer if errors are encountered and retries are required. Any errors that are encountered are reported in the RUGGEDCOM EXPLORER user interface.

3 Theory Of Operation

This chapter provides information on how RUGGEDCOM EXPLORER operates from a network perspective.

Section 3.1
Device Discovery Methods

RUGGEDCOM EXPLORER uses two different methods to discover ROS devices for management:

- Automatic (RCDP-based)
- Manual (TCP/IP-based)

Section 3.1.1
Automatic (RCDP-based) Device Discovery

The Automated Discovery method is based on a proprietary Layer 2 Ethernet protocol called the RUGGEDCOM Discovery Protocol (RCDP). ROS version 3.7.0 devices running RCDP actively listen for RCDP discovery messages, sent as Ethernet multicasts, from RUGGEDCOM EXPLORER . A ROS device must acknowledge the reception of a discovery message from RUGGEDCOM EXPLORER to register itself with the management application and establish a session.

Upon completion of the session registration between RUGGEDCOM EXPLORER and ROS, RUGGEDCOM EXPLORER can begin management of the device. Since RCDP messages are based on Ethernet and its addressing mechanism, and do not make any use of IP, RUGGEDCOM EXPLORER can communicate with ROS devices that have not been assigned an IP address. As a result, RUGGEDCOM EXPLORER can be used to configure the IP address on ROS devices irrespective of their network configuration. Moreover, since RCDP is not dependent on IP, it can be used to discover and display devices that have conflicting IP addresses and allow a user to reconfigure these devices.

To discover new devices added to the network or devices that were not initially discovered, RUGGEDCOM EXPLORER periodically sends rediscovery messages. Only ROS devices that did not previously complete the registration process with RUGGEDCOM EXPLORER will respond to the rediscovery messages to control network traffic. The rediscovery process runs periodically after RUGGEDCOM EXPLORER sends the initial discovery message.

Section 3.1.2
Manual (TCP/IP-based) Device Discovery

The Manual Discovery method uses a ping sweep to discover ROS devices that have a valid IP address and do not support RCDP. The manual discovery process has 2 phases:

- Phase 1 requires a user to select the discovery dialog and enter a starting and ending IP address. Clicking the OK button causes RUGGEDCOM EXPLORER to start the pinging process which will sequentially go through the list of IP addresses and records IP addresses that respond.

- Phase 2 attempts to log on to the devices that responded to a ping with the provided user name and password to assess whether it is a ROS device or not. At the end of phase 2, a list of devices is available for management by RUGGEDCOM EXPLORER.

Section 3.1.3

RCDP Versus TCP/IP Discovery Comparison

The following table provides a brief comparison of the two discovery mechanisms used by RUGGEDCOM EXPLORER:

	RCDP	Ping Sweep
Discovery method	Ethernet messages	ICMP Ping messages
Rediscovery	Send periodically	Not supported
Display configuration parameters	Supported	Supported
Visual identification	Supported (based on device capabilities)	Not supported
Change configuration parameters	Supported	Supported
Determine support for encryption when discovered	No	Yes (for version that supports encryption only)

Section 3.2

Security Considerations

In order for RUGGEDCOM EXPLORER to authenticate itself to the devices it connects to, it must be given the user names and passwords for these devices.

NOTE
For security reasons, user name and password device credentials are not stored permanently by RUGGEDCOM EXPLORER.

Automatic Discovery requires a user to enter the credential pairs through the user interface using the Section 2.3.1.1, “Auto Discovery Access Configuration” menu. Manual Discovery asks for device credentials when the ping sweep is being configured. The device credentials for each discovery type are only used by that type meaning that the information is not shared. To manually discover devices with different credentials, the ping sweep must be re-run with a different user name and password. Doing this does not discard any previously discovered devices unless a user chooses to remove them. All user names and passwords entered via the user interface are discarded when RUGGEDCOM EXPLORER is shut down.

RCDP does not send user names and passwords in its messages so this information remains secure. The Non-Controlled version of RUGGEDCOM EXPLORER does send user names and passwords in clear text and would be readable by someone snooping on the line. The Controlled version of RUGGEDCOM EXPLORER does not expose any sensitive information.

RCDP will be disabled on all devices when a user closes RUGGEDCOM EXPLORER . If RUGGEDCOM EXPLORER is unable to disable RCDP on the device, ROS will automatically disable RCDP after approximately one hour of inactivity. Users need to re-enable RCDP in ROS if they would like devices to be auto-discovered by RUGGEDCOM EXPLORER again after RCDP is disabled.

A user can disable RCDP on specific devices by right-clicking on the device(s) on the screen and selecting *Disable RCDP* from the pop-up menu. A user can also disable RCDP by selecting *Disable RCDP* from the *Commands* menu. However, this can be done only to the devices discovered by RCDP. Since RCDP is a layer 2 protocol, disabling RCDP on a device in a remote subnet is not applicable.

NOTE
RCDP is enabled by default on ROS devices running version 3.7.0 or newer.

Section 3.3

Duplicate Instance Detection

While RUGGEDCOM EXPLORER runs, it monitors the network for other nodes that may be attempting to perform RCDP-based discovery, since the presence of more than one active RCDP master on the network is disruptive to the correct operation of the Automatic Discovery mechanism and of subsequent command and control of RCDP-compliant devices.

If RUGGEDCOM EXPLORER detects another instance running on the network, it issues a warning similar to the following:

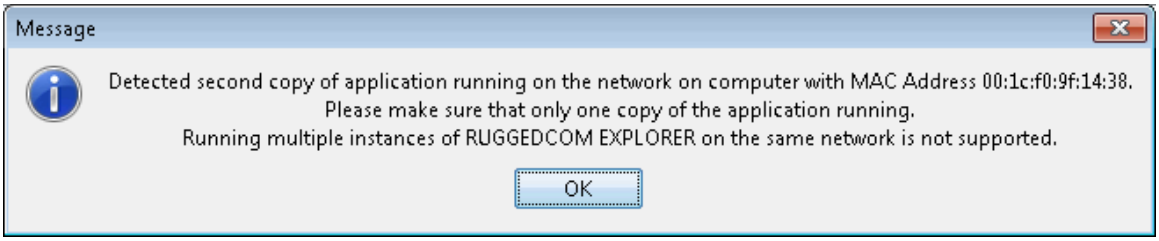


Figure 27: Detecting Another Instance Of RUGGEDCOM EXPLORER On The LAN

NOTE
In order to be able to detect other instances on the network, RUGGEDCOM EXPLORER places the network interface in promiscuous mode.

If RUGGEDCOM EXPLORER detects another instance running on the same computer, it issues a different warning:

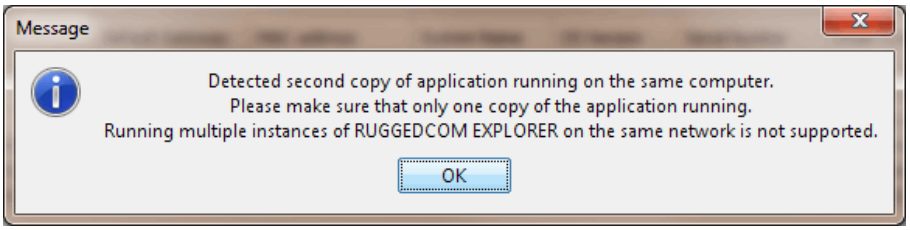


Figure 28: Detecting Another Instance Of RUGGEDCOM EXPLORER On The Same Computer

RCEXPLORER.ini Configuration File

The `RCEXPLORER.ini` file, located in the RUGGEDCOM EXPLORER installation directory, stores program defaults, parameters specified and discovered at run-time. It is also possible to edit the file using a regular ASCII text editor in order to explicitly configure certain aspects of RUGGEDCOM EXPLORER.

The file has a simple structure:

- `[section name]` - denotes the start of one of the configuration file sections.
- `;` - A line beginning with a semicolon is a comment.
- `variable = value` - A line of this form assigns a value to one of RUGGEDCOM EXPLORER's configurable variables.

In the following sections, the different sections of `RCEXPLORER.ini` are presented as they appear in the file. The configurable variables for each section are listed, preceded by comment fields describing the function of each one.

Auto Configuration Parameters

```
[auto_config]
; Last network mask used for Auto-Configuration process
net_mask =

; Last default gateway used for Auto-Configuration process
default_gw =

; Last starting IP address used for Auto-Configuration process
start_ip =
```

Logging Parameters

```
[log]
; Maximum size of the log file
file_max_size = 5000

; Destination directory for log file. If unspecified, this defaults
; to the directory in which the RUGGEDCOM EXPLORER executable resides
directory_name =
```

General Parameters

```
[general]
; Preferred communication protocol. Valid values are "ssh" (encrypted)
; or "rsh" (unencrypted)
```

```
pref_comm = ssh

; Default administrator password used by the Layer 2
; auto discovery protocol
admin_pwd = admin

; Last interface used by RUGGEDCOM EXPLORER . If this is empty,
; RUGGEDCOM EXPLORER  will present a drop-down list with all interfaces.
; upon start-up
management_ip =

; Show a disclaimer when running the Controlled version.
secure_ver_warning = true

; Destination directory for device file downloads.
; If unspecified, this defaults to the directory in which the
; RUGGEDCOM EXPLORER  executable resides.
downloads = downloads

; Whether to make use of SSH for encrypted communication with
; discovered devices. Note that this has no impact on the
; Non-Controlled version of RUGGEDCOM EXPLORER.
secure_mode = false

; Default administrator user name used by the Layer 2
; auto discovery protocol
admin_username = admin

; Upload configuration file continue or stop on error
upload_continue_on_error = true
```