

SEL-3610 Port Server, SEL-3620 Ethernet Security Gateway, and SEL-3622 Security Gateway

Instruction Manual

20241010

SEL SCHWEITZER ENGINEERING LABORATORIES



© 2009–2024 by Schweitzer Engineering Laboratories, Inc.

Content subject to change without notice. Unless otherwise agreed in writing, all SEL product sales are subject to SEL's terms and conditions located here: <https://selinc.com/company/termsandconditions/>.

PM3620-01

Table of Contents

List of Tables.....v

List of Figures.....vii

Prefacexvii

 Manual Overview xvii

 Safety Information xviii

 General Information xx

Section 1: Introduction and Specifications

Introduction.....	1.1
Product Overviews.....	1.1
Product Features	1.3
Product Applications.....	1.5
SEL-3610/SEL-3620 Connections and LED Indicators	1.9
SEL-3622 Connections and LED Indicators	1.15
Software System Requirements	1.19
General Safety and Care Information	1.20
SEL-3610 and SEL-3620 Specifications	1.21
SEL-3622 Specifications	1.24

Section 2: Installation

Introduction.....	2.1
Dimension Drawings	2.1
Installation of the SEL-3622.....	2.2
Connecting to the Device.....	2.3
Commissioning the Device	2.6
Navigating the User Interface	2.7
The Device Dashboard.....	2.9

Section 3: Managing Users

Introduction.....	3.1
User-Based Accounts.....	3.1
Adding a User	3.4
Editing a User and Resetting a Password	3.5
Removing a User	3.6
Enabling or Disabling a User.....	3.6
Changing a User Password	3.7
Local Groups.....	3.7
Centralized User Accounts With LDAP.....	3.8
Using RADIUS	3.15

Section 4: Job Done Examples

Introduction.....	4.1
Job Done Example 1: Central User Access	4.1
Job Done Example 2: Adding Ports to a Modbus Polling System	4.7
Job Done Example 3: Detect Physical Tampering	4.11
Job Done Example 4: Secure DNP3 Serial-to-Ethernet Conversion Over a Cellular Network	4.14
Job Done Example 5: Using IPsec to Secure Communication.....	4.21
Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant.....	4.26
Job Done Example 7: Using VLANs on the SEL-3620 With a Managed Ethernet Switch	4.29
Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control	4.33

Section 5: Settings and Commands

Introduction.....	5.1
Commissioning Page	5.2
System.....	5.4
Network	5.18
Serial Ports.....	5.33
Security	5.49
Reports	5.59

Section 6: SEL-3620 and SEL-3622 Security Services

Introduction.....	6.1
Firewall	6.1
Network Address Translation	6.6
IPsec Connections.....	6.10
MACsec Connections	6.16

Section 7: Proxy Services and Password Management

Terms and Definitions	7.1
Navigating This Section.....	7.1
Introduction.....	7.2
Theory of Operation.....	7.5
General Information About SEL-3620 Password Management, IED Proxy, and QuickSet User	
Authentication Capabilities	7.6
Initial Configuration	7.8
Configuring Group Access Permissions for Proxy Services	7.14
Using the SEL-3620 Proxy Services	7.26
Implementing Password Management.....	7.50
Management of Ethernet-Connected IEDs	7.74
Management of SEL Communications Processors.....	7.87
Management of GE Devices	7.112
Using TEAM With the SEL-3620 Proxy	7.128
Technical Support.....	7.140

Section 8: Testing and Troubleshooting

Introduction.....	8.1
Testing Philosophy	8.1
LED Indicators.....	8.2
Diagnostics Page.....	8.4
Troubleshooting	8.5
Technical Support.....	8.8

Appendix A: Firmware and Manual Versions

Firmware	A.1
Manual	A.20

Appendix B: Firmware Upgrade Instructions

Introduction.....	B.1
Firmware Files	B.1
Upgrading Firmware From Earlier Revisions	B.1
Special Firmware Upgrade Process	B.3
Downgrading Firmware to an Earlier Revision	B.4
Firmware File Loading Procedure	B.4
Reverting to Previous Firmware	B.6
Technical Support.....	B.6

Appendix C: Best Practices for Emergency Readiness

Replacing a Damaged SEL-3620.....	C.1
Emergency Access When LDAP Is Unavailable.....	C.3

Appendix D: Open Network Ports**Appendix E: User-Based Accounts**

Introduction.....	E.1
Benefits of User-Based Accounts	E.1
Administration of User-Based Accounts	E.2
SEL Use Banner.....	E.2
Logging in With SEL User-Based Accounts	E.2
Passphrases	E.3

Appendix F: Syslog

Introduction.....	F.1
Remote Syslog Servers	F.3
Open Source Syslog Servers.....	F.3
Event Logs	F.3

Appendix G: Networking Fundamentals

Introduction.....	G.1
OSI Model.....	G.1

Appendix H: Classless Inter-Domain Routing**Appendix I: Virtual Local Area Networks****Appendix J: Internet Protocol Security**

Introduction.....	J.1
Security Provided.....	J.1
Protected Paths.....	J.2
Two Protection Protocols.....	J.2
Two Modes of Use.....	J.3
Transport Mode.....	J.3
Tunnel Mode.....	J.3
Internet Key Exchange.....	J.3
Security Associations.....	J.4

Appendix K: X.509

Introduction.....	K.1
Public-Key Cryptography	K.1
X.509 Certificates	K.2
Digital Signatures	K.3
Public-Key Infrastructure	K.3
Web of Trust	K.4
Simple Public-Key Infrastructure	K.4
Online Certificate Status Protocol (OCSP).....	K.5
Sample X.509 Certificate.....	K.5

Appendix L: Lightweight Directory Access Protocol

SEL LDAP Client Implementation.....	L.1
Certificate Chain	L.1
LDAP Settings Form	L.2

Appendix M: SEL RADIUS Dictionary**Appendix N: Web Server Security With Transport Layer Security**

Introduction.....	N.1
HTTP Session Cookies	N.1
TLS	N.1

Appendix O: Media Access Control Security (MACsec)

Overview	O.1
IEEE 802.1AE MACsec Protocol	O.2
IEEE 802.1X-2010 Clause 9: MKA Protocol	O.4
MACsec Architecture	O.6
SEL Innovations	O.6

Appendix P: Cybersecurity Features

Version Information	P.1
Ports and Services	P.1
Centralized User-Based Access to Protected IEDs	P.2
Cryptographic Message Protection	P.2
Alerts and Logging	P.3
Backup and Restore	P.4
Decommissioning	P.4
Malware Protection Features	P.4
Revision Management	P.4
Contact SEL	P.5

Glossary

List of Tables

Table 1.1	Serial DB-9 Port Pinout.....	1.10
Table 1.2	Isolated Port Pinout	1.11
Table 1.3	Ethernet Port Option.....	1.12
Table 1.4	Power Supply Options	1.12
Table 1.5	I/O Pin Designations.....	1.13
Table 1.6	Conditions for SEL-3610/SEL-3620 Alarm Contacts.....	1.13
Table 1.7	Syslog Message Description.....	1.14
Table 1.8	Jumper Pin Designations	1.14
Table 1.9	Serial DB-9 Port Pinout.....	1.16
Table 1.10	Ethernet Port Option.....	1.17
Table 1.11	I/O Pin Designations.....	1.17
Table 1.12	Conditions for SEL-3622 Alarm Contacts	1.18
Table 1.13	Syslog Message Description.....	1.18
Table 1.14	Jumper Location	1.19
Table 2.1	Network Interface Icon Colors	2.11
Table 2.2	Serial Port Icon Colors	2.11
Table 2.3	System Statistics	2.12
Table 3.1	Administrative Accounts Features/Roles	3.3
Table 3.2	Description of RADIUS Settings	3.17
Table 4.1	Job Done Syslog Settings	4.2
Table 4.2	Job Done LDAP Settings.....	4.2
Table 4.3	Job Done Example 5 Settings	4.22
Table 4.4	Commissioning Methods.....	4.34
Table 4.5	Additional MACsec Devices and Firmware Versions.....	4.34
Table 5.1	Commissioning Settings	5.3
Table 5.2	IRIG-B Output Quality Settings	5.7
Table 5.3	NTP Server Settings	5.8
Table 5.4	NTP Output Stratum Setting.....	5.8
Table 5.5	Web Server Settings	5.14
Table 5.6	Service Port Settings.....	5.14
Table 5.7	Service Port Commands	5.14
Table 5.8	Input Contact Settings	5.16
Table 5.9	Light Sensor Settings.....	5.17
Table 5.10	Motion Sensor Settings.....	5.18
Table 5.11	Global Network Settings	5.19
Table 5.12	TCP Keepalive Settings.....	5.19
Table 5.13	Network Interface Icon Colors	5.19
Table 5.14	Network Interface Capabilities	5.20
Table 5.15	Ethernet Interface Settings.....	5.20
Table 5.16	Network Address Form Settings.....	5.21
Table 5.17	Bridge Interface Form Settings.....	5.22
Table 5.18	Static Route Symbols.....	5.24
Table 5.19	Static Route Settings.....	5.24
Table 5.20	Syslog Destination Settings	5.27
Table 5.21	Syslog General Settings	5.29
Table 5.22	SNMP v1/v2c Parameters.....	5.30
Table 5.23	SNMP v3 Parameters.....	5.31
Table 5.24	Supported MIBs.....	5.31
Table 5.25	Serial Interface Settings	5.34
Table 5.26	Serial Port Icon Colors	5.34
Table 5.27	Serial Interface Settings	5.35
Table 5.28	One-Way Bit-Time Delays	5.36
Table 5.29	Maximum Number of Supported Bit-Based Serial Ports	5.37

Table 5.30	Add Serial Form Settings	5.40
Table 5.31	Add Serial Master Port Form Settings.....	5.41
Table 5.32	Add Ethernet Listen Local Form Settings	5.42
Table 5.33	Add Ethernet Listen Local Master Port Form Settings	5.44
Table 5.34	Add Ethernet Connect Remote Form Settings	5.45
Table 5.35	Device Capability Matrix	5.45
Table 5.36	Master Port Commands	5.47
Table 5.37	Ethernet Diagnostics Explanation	5.48
Table 5.38	Serial Diagnostics Explanation.....	5.49
Table 5.39	X.509 Generation Settings.....	5.52
Table 5.40	Allowed Client Settings.....	5.56
Table 5.41	Key Exchange Algorithm	5.57
Table 6.1	Firewall Symbols	6.2
Table 6.2	General Rule Settings	6.2
Table 6.3	Firewall Rule Settings	6.3
Table 6.4	Ports Automatically Opened by Firewall	6.4
Table 6.5	Global NAT Settings	6.8
Table 6.6	Port Forwarding Rule Settings	6.9
Table 6.7	IPsec Settings.....	6.12
Table 6.8	IPsec Using Passphrase Settings.....	6.12
Table 6.9	IPsec Using X.509 Certificates Settings.....	6.13
Table 6.10	Lemnos IKEv2 Profile	6.13
Table 6.11	Lemnos IKEv1 Profile	6.13
Table 6.12	Cisco Profile	6.14
Table 6.13	SEL - Secure (2022) Profile	6.14
Table 6.14	IPsec Symbols.....	6.15
Table 6.15	MACsec Settings	6.17
Table 6.16	SEL-3622 Test Results	6.21
Table 6.17	SEL-3620 Test Results	6.21
Table 7.1	SEL-3620 Password Management Capabilities	7.7
Table 7.2	SEL-3620 IED Proxy Capabilities	7.7
Table 7.3	SELF Controller Menu Options	7.68
Table 7.4	GE Product Support for Proxy and Password Management.....	7.113
Table 8.1	System LED Indicators.....	8.3
Table 8.2	Subsystem LED Indicators	8.3
Table 8.3	System LED Indicators.....	8.4
Table 8.4	Subsystem LED Indicators	8.4
Table 8.5	Troubleshooting Procedure.....	8.6
Table B.1	SEL-3610 Firmware	B.2
Table B.2	SEL-3620 Firmware	B.2
Table B.3	SEL-3622 Firmware	B.2
Table B.4	Firmware Downgrades and Reversions	B.4
Table F.1	Syslog Message Severities.....	F.1
Table F.2	Syslog Message Facilities.....	F.1
Table F.3	Syslog Messages.....	F.4
Table G.1	Sample IP Address.....	G.4
Table H.1	CIDR to Dotted-Decimal Mapping	H.2
Table N.1	TLSv1.2 Cipher List	N.2
Table N.2	TLSv1.3 Cipher List	N.2

List of Figures

Figure 1.1	SEL-3610 Port Server.....	1.2
Figure 1.2	SEL-3620 Ethernet Security Gateway.....	1.2
Figure 1.3	SEL-3622 Security Gateway	1.3
Figure 1.4	Serial Port Expansion	1.5
Figure 1.5	Serial Over Ethernet	1.5
Figure 1.6	Port Mirroring.....	1.6
Figure 1.7	User-Based Access to IEDs	1.7
Figure 1.8	Active Traffic Filtering.....	1.7
Figure 1.9	Encrypted and Authenticated Ethernet Communications.....	1.8
Figure 1.10	Password Management	1.8
Figure 1.11	SEL-3622 Communication Encryption	1.9
Figure 1.12	Front-Panel Diagrams.....	1.9
Figure 1.13	Rear-Panel Diagrams	1.10
Figure 1.14	EIA-485 Typical Two-Wire Connection	1.11
Figure 1.15	EIA-485 Typical Four-Wire Connection.....	1.11
Figure 1.16	Rear Connector Diagram	1.13
Figure 1.17	Connecting a Sensor to the Discrete Input	1.14
Figure 1.18	Jumper Locations.....	1.14
Figure 1.19	SEL-3622 Front-Panel Diagram.....	1.15
Figure 1.20	SEL-3622 Rear-Panel Diagrams	1.16
Figure 1.21	Rear Connector Diagram	1.17
Figure 1.22	Connecting a Sensor to the Discrete Input on the SEL-3622	1.18
Figure 1.23	JMP1 Location.....	1.19
Figure 2.1	SEL-3610/SEL-3620 Dimension Drawing.....	2.1
Figure 2.2	SEL-3622 Dimension Drawing	2.2
Figure 2.3	SEL-3622 Light Sensor Location	2.2
Figure 2.4	Ethernet Commissioning Network	2.3
Figure 2.5	USB Commissioning Network	2.3
Figure 2.6	Open Terminal With Run Command.....	2.4
Figure 2.7	Windows IP Configuration	2.4
Figure 2.8	Open Network Connections With Run Command	2.4
Figure 2.9	Open Connection Properties	2.5
Figure 2.10	Local Area Connection Properties.....	2.5
Figure 2.11	Internet Protocol (TCP/IP) Properties	2.5
Figure 2.12	Device Commissioning Page	2.6
Figure 2.13	Device Commissioning Form	2.7
Figure 2.14	Device Status Dashboard.....	2.8
Figure 2.15	User Accounts.....	2.8
Figure 2.16	Add User.....	2.9
Figure 2.17	Device Dashboard.....	2.10
Figure 2.18	Network Interfaces.....	2.11
Figure 2.19	Serial Ports.....	2.11
Figure 2.20	System Statistics	2.12
Figure 2.21	SEL-3610/SEL-3620 LED Indicators	2.13
Figure 2.22	SEL-3622 LED Indicators	2.13
Figure 2.23	Connection Status	2.13
Figure 2.24	Version Information	2.13
Figure 2.25	Resource Usage	2.14
Figure 2.26	Logs by Severity	2.14
Figure 3.1	User Accounts.....	3.2
Figure 3.2	Add User Form	3.4

Figure 3.3	Update User Form	3.5
Figure 3.4	Confirm Deletion	3.6
Figure 3.5	Change Password.....	3.7
Figure 3.6	Add Local Group Form	3.8
Figure 3.7	Local Group List.....	3.8
Figure 3.8	LDAP Login Process	3.9
Figure 3.9	Host Settings.....	3.9
Figure 3.10	Add Host.....	3.10
Figure 3.11	LDAP Settings	3.11
Figure 3.12	Edit LDAP Settings	3.12
Figure 3.13	Add LDAP Server	3.13
Figure 3.14	Edit Attribute Mapping.....	3.14
Figure 3.15	Group Mappings	3.14
Figure 3.16	RADIUS Settings	3.17
Figure 3.17	Adding a RADIUS Server on the Hosts Page	3.18
Figure 3.18	Selecting a RADIUS Server by Hostname	3.18
Figure 3.19	Selecting the RADIUS Authentication Type.....	3.18
Figure 4.1	Centralization Network.....	4.2
Figure 4.2	Add Trusted Network	4.3
Figure 4.3	Update Network Interface.....	4.3
Figure 4.4	Syslog Configuration Page	4.4
Figure 4.5	Add Syslog Destination	4.4
Figure 4.6	Import X.509 Certificate	4.5
Figure 4.7	Add Host.....	4.5
Figure 4.8	Modify LDAP Settings	4.6
Figure 4.9	Add LDAP Server	4.6
Figure 4.10	Add Group Mapping.....	4.7
Figure 4.11	Port Expansion Communication Paths	4.8
Figure 4.12	Add New Profile	4.8
Figure 4.13	Assign Serial Interface Settings.....	4.9
Figure 4.14	Add Ethernet Local Driver	4.10
Figure 4.15	Add Modbus Serial Driver	4.10
Figure 4.16	Configured Port Mappings	4.10
Figure 4.17	Modbus Settings	4.11
Figure 4.18	Recloser Cabinet Installation.....	4.12
Figure 4.19	Syslog Configuration Page	4.13
Figure 4.20	Add Syslog Destination	4.13
Figure 4.21	Job Done 4 Architecture	4.14
Figure 4.22	MTU Size Discovery on Windows.....	4.16
Figure 4.23	PREDLY Setting on SEL Relay	4.16
Figure 4.24	Configuring the SEL-3622 Interface for Cellular Connectivity	4.17
Figure 4.25	Configuring the SEL-3622 Default Gateway for the DHCP Gateway	4.17
Figure 4.26	SEL-3622 With the Cellular Default Gateway	4.17
Figure 4.27	IPsec Settings.....	4.18
Figure 4.28	IPsec Connection Status	4.18
Figure 4.29	Port Profile DNP Port Settings	4.19
Figure 4.30	Serial Port Enabled and Updated.....	4.19
Figure 4.31	Serial Port	4.20
Figure 4.32	Ethernet Listen Local Settings.....	4.20
Figure 4.33	DNP Serial-to-Ethernet Port Mapping	4.21
Figure 4.34	Configure Centralized Alerts	4.21
Figure 4.35	Diagram of Two Substation Networks	4.22
Figure 4.36	Add Untrusted Network.....	4.23
Figure 4.37	Add Protected Network	4.23
Figure 4.38	Add IPsec Connection to Substation B.....	4.24
Figure 4.39	Add Untrusted Network at Substation B	4.25

Figure 4.40	Add Protected Network at Substation B	4.25
Figure 4.41	Add IPsec Connection to Substation A	4.26
Figure 4.42	SSH to TELNET Port Map.....	4.27
Figure 4.43	Setting the Port Number	4.28
Figure 4.44	Setting Connection Parameters.....	4.28
Figure 4.45	Using the SEL-5020 Terminal Window	4.29
Figure 4.46	Using the SEL-3620 With a Managed Ethernet Switch	4.30
Figure 4.47	Adding the VLAN 751 Subinterface	4.31
Figure 4.48	Completed SEL-3620 Interface	4.31
Figure 4.49	Adding the Firewall Rule	4.32
Figure 4.50	Completed VLAN Configuration on the SEL-2730M	4.33
Figure 4.51	Example SEL-651RA and SEL-3622 MACsec Connection	4.34
Figure 4.52	Adding a New MACsec Connection	4.35
Figure 4.53	Commissioning Options	4.35
Figure 4.54	Select Commissioning Window Start Date/Time.....	4.36
Figure 4.55	MACsec Connection Added	4.36
Figure 4.56	Key Server MAC Address	4.36
Figure 4.57	MACsec Commissioning Status and Alias.....	4.37
Figure 4.58	Embedded Client Commissioning Status	4.37
Figure 4.59	Reset SEL-651RA MACsec Connection.....	4.37
Figure 4.60	MACsec Commissioning Attempt.....	4.37
Figure 4.61	Confirm Commissioning With SEL-3622	4.38
Figure 4.62	MACsec Commissioning Successful.....	4.38
Figure 4.63	Commissioned Automatic MACsec Connection With SEL-3622	4.38
Figure 4.64	MCS C Command Response	4.39
Figure 4.65	SEL-651RA Port 5 Settings.....	4.39
Figure 4.66	MCS A Command	4.40
Figure 4.67	Successful MCS A Command With SLR Command Response.....	4.40
Figure 4.68	Successful SEL-3622 MACsec Connection Commissioning.....	4.41
Figure 4.69	Manual Key Commissioning Option	4.41
Figure 4.70	Generating a New MACsec Manual Key	4.42
Figure 4.71	Manual MACsec Commissioning	4.42
Figure 4.72	Command Line Manual MACsec Commissioning	4.43
Figure 4.73	MACsec Command Line Commissioning Successful.....	4.43
Figure 4.74	MACsec Manual Commissioning SEL-3622 Pairing Successful	4.43
Figure 4.75	Front Panel MACsec Commissioning Failed	4.44
Figure 4.76	MACsec Automatic Command Line Commissioning Failed.....	4.44
Figure 4.77	MACsec SLR Command With Failure.....	4.45
Figure 4.78	MACsec Commissioning Failed.....	4.45
Figure 4.79	Successful SLR Command Response.....	4.46
Figure 5.1	Security Exception.....	5.2
Figure 5.2	Commissioning Page	5.3
Figure 5.3	System Settings.....	5.4
Figure 5.4	Time Synchronization With NTP and/or IRIG-B.....	5.5
Figure 5.5	Date/Time Configuration Page	5.6
Figure 5.6	Manual Time Input	5.6
Figure 5.7	Time Synchronization Settings.....	5.7
Figure 5.8	NTP Stratum Levels	5.8
Figure 5.9	NTP Synchronization Settings.....	5.9
Figure 5.10	File Management Window	5.10
Figure 5.11	Firmware Version Window	5.10
Figure 5.12	Connection Directory Window.....	5.10
Figure 5.13	System Settings.....	5.11
Figure 5.14	Single File Backup Window.....	5.12
Figure 5.15	Management Interface	5.13
Figure 5.16	Input Contact Settings and Recent Events.....	5.16

Figure 5.17	Light Sensor.....	5.16
Figure 5.18	Motion Sensor Settings and Recent Events	5.17
Figure 5.19	Network Settings	5.18
Figure 5.20	Network Interfaces.....	5.19
Figure 5.21	Add Network Address Form.....	5.21
Figure 5.22	Add Bridge Interface Form.....	5.22
Figure 5.23	Configured Addresses.....	5.22
Figure 5.24	Disable Unused Ports.....	5.23
Figure 5.25	Static Routes	5.23
Figure 5.26	Static Route Form	5.24
Figure 5.27	Address and Port Group	5.25
Figure 5.28	Syslog	5.26
Figure 5.29	Add Syslog Destination	5.27
Figure 5.30	Updated Syslog Destination Table	5.28
Figure 5.31	Syslog General Settings.....	5.28
Figure 5.32	SNMP Setting Page	5.29
Figure 5.33	Adding an SNMP v1/v2c Profile.....	5.30
Figure 5.34	Adding an SNMP v3 Profile.....	5.30
Figure 5.35	Adding a Trap Server	5.31
Figure 5.36	Serial Ports Page	5.33
Figure 5.37	Serial Interface Settings Form	5.34
Figure 5.38	Push-to-Talk RTS vs. Data Pin Behavior	5.36
Figure 5.39	Master Port for Engineering Access	5.38
Figure 5.40	Easy Connection Filtering	5.38
Figure 5.41	Archiving, Supervision, and Data Redundancy.....	5.39
Figure 5.42	Add Group Form	5.39
Figure 5.43	Add Device Form	5.39
Figure 5.44	Add Serial Form	5.40
Figure 5.45	Add Serial Master Port Form.....	5.41
Figure 5.46	Add Ethernet Listen Local Form	5.42
Figure 5.47	Add Ethernet Listen Local Master Port Form	5.43
Figure 5.48	Add Ethernet Connect Remote Form	5.44
Figure 5.49	Example Port Mapping	5.45
Figure 5.50	Terminal Access to Master Port	5.46
Figure 5.51	Device List and Connect.....	5.47
Figure 5.52	Modbus Conversion Configuration	5.48
Figure 5.53	Ethernet Device Diagnostics	5.48
Figure 5.54	Serial Device Diagnostics.....	5.49
Figure 5.55	Security Settings	5.50
Figure 5.56	Installed X.509 Certificates	5.50
Figure 5.57	Import X.509 Certificate Form	5.51
Figure 5.58	X.509 Certificate Generation Form	5.52
Figure 5.59	View X.509 Certificate	5.53
Figure 5.60	Export X.509 Certificate	5.53
Figure 5.61	Confirm Deletion	5.53
Figure 5.62	Allowed Client Services	5.54
Figure 5.63	Allowed Clients	5.55
Figure 5.64	Add Client.....	5.55
Figure 5.65	Device SSH Host Key	5.58
Figure 5.66	Reports Settings	5.59
Figure 5.67	System Logs	5.60
Figure 5.68	System Log Filters.....	5.61
Figure 6.1	Firewall Rules.....	6.2
Figure 6.2	Default NAT Webpage	6.6
Figure 6.3	Outbound NAT Example.....	6.6
Figure 6.4	Port Forwarding Example.....	6.7

Figure 6.5	Edit Global NAT Settings Dialog Box	6.7
Figure 6.6	Add Port Forwarding Rule Dialog Box	6.8
Figure 6.7	Configured Port Forward Entries	6.9
Figure 6.8	Port Forward, Enabled, Disabled, and System Disabled States	6.9
Figure 6.9	IPsec Connections.....	6.11
Figure 6.10	Add IPsec Using Passphrase Form.....	6.11
Figure 6.11	MACsec Connections	6.16
Figure 6.12	Initial MACsec Form (Fewer Options)	6.17
Figure 6.13	MACsec Form (More Options)	6.17
Figure 6.14	MACsec Connections Commissioning.....	6.18
Figure 6.15	Commissioned MACsec Connections	6.19
Figure 6.16	Updating an Existing MACsec Connection.....	6.20
Figure 6.17	Embedded Client Removed From Existing MACsec Connection	6.20
Figure 6.18	Test Configurations	6.21
Figure 7.1	User Accessing a Global Shared IED Account	7.3
Figure 7.2	Accessing an IED with the SEL-3620 Proxy	7.4
Figure 7.3	Users and Groups.....	7.5
Figure 7.4	Groups Are Mapped to IED Permissions	7.5
Figure 7.5	SEL-3620 Proxy Login Scenario.....	7.6
Figure 7.6	Initial Configuration Network Diagram	7.8
Figure 7.7	SEL-3620 Users Page With QuickSet Account	7.9
Figure 7.8	Adding a Device Template	7.9
Figure 7.9	Select the Is Managed Check Box in the SEL-3620 Template	7.9
Figure 7.10	SEL-3620 Template Connection Tab	7.10
Figure 7.11	Adding SEL-787 Beneath the SEL-3620 Template	7.10
Figure 7.12	SEL-787 Global Device ID	7.11
Figure 7.13	SEL-787 Connection Tab Parameters	7.12
Figure 7.14	Successful Upload of the Connection Directory From QuickSet.....	7.12
Figure 7.15	Invalid Certificate Message	7.13
Figure 7.16	Failed: 400 Message	7.13
Figure 7.17	Failed: 10058 Message	7.13
Figure 7.18	Initial Configuration Network Diagram	7.15
Figure 7.19	Local Users and Groups on the SEL-3620 and Device Manager.....	7.16
Figure 7.20	Creating the Local Users	7.17
Figure 7.21	Local User Groups on the SEL-3620	7.17
Figure 7.22	Three Local QuickSet Users.....	7.18
Figure 7.23	Allow Log in to ACCELERATOR Database Check Box.....	7.18
Figure 7.24	QuickSet Local Groups and Users.....	7.18
Figure 7.25	Centralized User Access to the SEL-3620 Proxy Services	7.19
Figure 7.26	LDAP Users and Groups	7.20
Figure 7.27	QuickSet Configure LDAP	7.21
Figure 7.28	Parsing the LDAP Groups to Find the Supervisors Group.....	7.21
Figure 7.29	Supervisor Users Within the Centralized Supervisors Group	7.22
Figure 7.30	LDAP User Groups	7.22
Figure 7.31	RADIUS Authorizations in Device Manager.....	7.23
Figure 7.32	Associate LDAP Groups With IED Permissions	7.24
Figure 7.33	Associate Local/RADIUS Groups With IED Permissions.....	7.24
Figure 7.34	Selecting Groups in the IED Permissions Tab	7.25
Figure 7.35	IED Permissions Tab Settings	7.26
Figure 7.36	Uploading the Connection Directory to the SEL-3620	7.26
Figure 7.37	Initial Configuration Network Diagram	7.27
Figure 7.38	Adding a New Group.....	7.28
Figure 7.39	Ethernet Listen Local Driver	7.28
Figure 7.40	Engineering Access SMP	7.28
Figure 7.41	Local Access to the SEL-3620 Proxy	7.29
Figure 7.42	LDAP Access to the SEL-3620 Proxy	7.30

Figure 7.43	RADIUS Access to the SEL-3620 Proxy	7.31
Figure 7.44	Tera Term Connection to SMP	7.31
Figure 7.45	WHO Command From the SMP	7.32
Figure 7.46	SEL IED Interface on the SMP	7.32
Figure 7.47	SEL IED Access Levels	7.33
Figure 7.48	SEL-3620 SMP Blocks the PAS Command.....	7.33
Figure 7.49	Binary Mode Control.....	7.34
Figure 7.50	Allow Ctrl Characters on QuickSet Terminal	7.35
Figure 7.51	QuickSet Communications Options	7.36
Figure 7.52	SEL-3620 Connection Settings	7.36
Figure 7.53	Connecting to the SEL-787	7.37
Figure 7.54	Successful Proxy Services Connection Through QuickSet	7.37
Figure 7.55	Commands and Devices Report	7.38
Figure 7.56	Commands and Devices Report Generation.....	7.38
Figure 7.57	Direct Terminal Connection to SEL IED	7.40
Figure 7.58	Terminal Connection to SEL IED (Proxied)	7.40
Figure 7.59	“Scrambled” Connection Directory IED	7.41
Figure 7.60	User Manager With Groups and Permissions.....	7.42
Figure 7.61	No Available Devices	7.42
Figure 7.62	Connection Directory Permissions Tab	7.43
Figure 7.63	Unable to Connect to a Serial Connection Directory Device	7.43
Figure 7.64	SEL-3620 SMP Reports “Device failed to gain access to level”	7.43
Figure 7.65	Setting MAXACC on the Port	7.44
Figure 7.66	SEL-3620 SMP Reports ‘Device responded with: ‘Invalid Password’’	7.44
Figure 7.67	SEL-3620 SMP “Traceback”.....	7.44
Figure 7.68	Unsupported Access Script on IED	7.45
Figure 7.69	SEL-3620 SMP Interfering With BAC	7.45
Figure 7.70	SMP Unexpected Response String	7.46
Figure 7.71	SMP Port Busy Response	7.46
Figure 7.72	SMP Connects at Elevated Access Level	7.47
Figure 7.73	Simple IED “QUIT” Terminate Script	7.47
Figure 7.74	QuickSet Options Menu	7.48
Figure 7.75	Advanced Communication Options Window	7.48
Figure 7.76	SSH Authentication Timeout.....	7.49
Figure 7.77	QuickSet Terminal.....	7.50
Figure 7.78	Password Management Network Diagram	7.51
Figure 7.79	Password Management Cycle With New IED.....	7.52
Figure 7.80	Normal Password Management Cycle	7.53
Figure 7.81	Revert Password Cycle	7.53
Figure 7.82	Device Checkout Cycle	7.53
Figure 7.83	Set Password and Generate Password Scripts	7.55
Figure 7.84	Default Managed Device Passwords Report	7.56
Figure 7.85	Managed Device List.....	7.57
Figure 7.86	Manual Password Management	7.58
Figure 7.87	Automated Password Management Box.....	7.59
Figure 7.88	Password Management Device Selection.....	7.59
Figure 7.89	Managed Device Passwords Report With Proposed Passwords.....	7.59
Figure 7.90	Managed Device Passwords Report With New Complex Passwords	7.60
Figure 7.91	SEL-3620 Default Passwords Warning Banner	7.61
Figure 7.92	Managed Device Password Editing Window	7.62
Figure 7.93	Edit Persistence Form	7.64
Figure 7.94	Persistence Report	7.65
Figure 7.95	Password Change Scheduler Options	7.66
Figure 7.96	Next Scheduled Password Change Box.....	7.66
Figure 7.97	Managed Device Passwords Report With Next Change Date	7.66
Figure 7.98	Check Out Allowed	7.67

Figure 7.99	Device Check Out.....	7.68
Figure 7.100	SELF Controller	7.69
Figure 7.101	Generating and Downloading Reports From SELF Controller	7.69
Figure 7.102	Generating and Applying Passwords.....	7.70
Figure 7.103	Empty Set Password Script.....	7.70
Figure 7.104	SMP Busy Error.....	7.72
Figure 7.105	Failed Access Level C Password Change.....	7.73
Figure 7.106	Password Management Over Ethernet Network Diagram.....	7.75
Figure 7.107	SEL-3620 SMP and FTP Proxy Ports	7.76
Figure 7.108	Ethernet-Connected IED Connection Tab	7.77
Figure 7.109	Selecting Groups on the IED Permissions Tab	7.78
Figure 7.110	Uploading the Connection Directory to the SEL-3620	7.78
Figure 7.111	SMP With FTP Proxy Port	7.78
Figure 7.112	Windows Command Line Terminal	7.79
Figure 7.113	FTP Login Prompt	7.79
Figure 7.114	FTP LS Command	7.80
Figure 7.115	FTP Proxy GET Command	7.80
Figure 7.116	Connecting to the SEL-787	7.81
Figure 7.117	Successful Proxy Services Connection Through QuickSet	7.81
Figure 7.118	QuickSet FTP File Transfer.....	7.81
Figure 7.119	Commands and Devices Report (FTP).....	7.82
Figure 7.120	Active FTP Session Command.....	7.82
Figure 7.121	Duplicate Proxy Port (FTP) Value	7.83
Figure 7.122	SEL-3620 Diagnostics Dump	7.84
Figure 7.123	FTP Proxy 421 Error	7.84
Figure 7.124	FTP Proxy 530 Error	7.85
Figure 7.125	FTP Active Mode	7.86
Figure 7.126	FTP Passive Mode	7.87
Figure 7.127	Communications Processor Password Management Network Diagram	7.88
Figure 7.128	SEL-3620 Communications Processor and Child Password Change Process	7.90
Figure 7.129	SEL-2032 Master Port Settings	7.92
Figure 7.130	SEL-2032 Device Tab	7.94
Figure 7.131	SEL-2032 Connection Tab	7.95
Figure 7.132	Selecting Groups on the IED Permissions Tab	7.95
Figure 7.133	Tiered SEL-2032 and SEL-451-5.....	7.96
Figure 7.134	SEL-451 Tiered Connection Tab.....	7.97
Figure 7.135	Selecting Groups on the IED Permissions Tab	7.97
Figure 7.136	SEL-2032, SEL-351, SEL-451 Tiered Scenario	7.98
Figure 7.137	Uploading the Connection Directory to the SEL-3620	7.98
Figure 7.138	SMP With a Communications Processor Tiered Scenario	7.98
Figure 7.139	SEL-5827 Settings for SEL-5020 Integration	7.99
Figure 7.140	SEL-5827 Login Information Window	7.100
Figure 7.141	SEL-5827 Terminal Interface for a Communications Processor.....	7.100
Figure 7.142	SEL-5827 Connection Directory Entry	7.101
Figure 7.143	SEL-5020 Configuration Options.....	7.101
Figure 7.144	SEL-5020 Terminal Through the SEL-5827 Virtual Port	7.102
Figure 7.145	Communications Processor Password Change Logs.....	7.103
Figure 7.146	Escape Character	7.105
Figure 7.147	Communications Processor STA Command	7.106
Figure 7.148	SEL-2032 PAS P Command.....	7.106
Figure 7.149	QuickSet “Unable to access port 0” Message.....	7.107
Figure 7.150	SEL-2700-Series Ethernet Card “Service is not available” Message.....	7.108
Figure 7.151	Custom Password Change Script for SEL Communications Processor IEDs.....	7.111
Figure 7.152	GE Password Management Network Diagram.....	7.112
Figure 7.153	GE T60 Global Device ID	7.114
Figure 7.154	Serial GE T60 Connection Tab Parameters.....	7.115

Figure 7.155	Ethernet GE T60 Connection Tab Parameters.....	7.116
Figure 7.156	Selecting Groups on the IED Permissions Tab	7.116
Figure 7.157	Uploading the Connection Directory to the SEL-3620	7.117
Figure 7.158	SEL-5827 Settings for Serial GE IED	7.117
Figure 7.159	SEL-5827 Login Information Window	7.118
Figure 7.160	SEL-5827 Terminal Interface	7.118
Figure 7.161	GE EnerVista UR Setup Window	7.119
Figure 7.162	Device Setup Window	7.119
Figure 7.163	GE EnerVista Installation Status Window	7.120
Figure 7.164	SEL-5827 Settings for Ethernet GE IED.....	7.121
Figure 7.165	SEL-5827 Login Information Window	7.121
Figure 7.166	SEL-5827 Terminal Interface	7.122
Figure 7.167	GE EnerVista UR Setup Window	7.122
Figure 7.168	GE Device Setup Window.....	7.123
Figure 7.169	GE EnerVista Installation Status Window	7.123
Figure 7.170	Change All Passwords Now Box.....	7.124
Figure 7.171	Managed Device Passwords Report With GE Proposed Passwords	7.124
Figure 7.172	Password Change Syslogs for GE IED.....	7.124
Figure 7.173	Managed Device Passwords Report With New Complex Passwords for GE IED.....	7.125
Figure 7.174	SEL-5827 Enable Break Option	7.125
Figure 7.175	Add a New SSH Device to the QuickSet Device Manager.....	7.126
Figure 7.176	Example Password Generation Script for Admin User	7.127
Figure 7.177	Example Access Script	7.127
Figure 7.178	Example Terminate Script	7.127
Figure 7.179	Configure an SSH Connection in the QuickSet Device Manager	7.127
Figure 7.180	SEL-3620 TEAM Software Network Diagram.....	7.128
Figure 7.181	Exporting a QuickSet Connection Directory	7.129
Figure 7.182	Connection Directory Export Select Data Window.....	7.130
Figure 7.183	Import an Existing DMX File.....	7.130
Figure 7.184	New Imported Connection Directory	7.131
Figure 7.185	Device Manager Passwords	7.132
Figure 7.186	TEAM Username and Password.....	7.132
Figure 7.187	SEL-3620 In Service Check Box.....	7.133
Figure 7.188	Select a Non-Listening Network Connection	7.133
Figure 7.189	3620 Log Collector Job	7.134
Figure 7.190	3620 Configure Job	7.134
Figure 7.191	3620 Job Start Date.....	7.135
Figure 7.192	SEL-3620 Reports Folder	7.136
Figure 7.193	SEL-3620 TEAM Configuration.....	7.137
Figure 7.194	SEL-787 Team Tab Inherited Communication Channel	7.137
Figure 7.195	SEL Default Event Collection Job.....	7.138
Figure 7.196	SEL-787 Reports Folder	7.138
Figure 7.197	TEAM Logging Directory	7.139
Figure 8.1	Successful Ping Host	8.5
Figure B.1	File Management Window	B.5
Figure B.2	Select Firmware File.....	B.5
Figure B.3	Firmware Versions	B.6
Figure C.1	Define Passwords	C.2
Figure C.2	Editing Passwords for Device Accounts	C.3
Figure F.1	Central Syslog Server	F.3
Figure G.1	OSI Model	G.2
Figure G.2	Ethernet Segment.....	G.3
Figure G.3	Ethernet Frame	G.3
Figure G.4	Layer 3 IP Network	G.4
Figure G.5	TCP Three-Way Handshake	G.5
Figure H.1	Classful Route Advertisements	H.1

Figure H.2	CIDR Route Advertisements	H.2
Figure I.1	Network Illustration Not Utilizing VLANs.....	I.1
Figure I.2	Network Illustration Utilizing VLANs.....	I.2
Figure K.1	Asymmetric Keys	K.1
Figure K.2	Confidentiality With Asymmetric Keys	K.2
Figure K.3	Authentication With Asymmetric Keys	K.2
Figure K.4	Digital Signatures	K.3
Figure K.5	Web of Trust.....	K.4
Figure L.1	LDAP Transaction	L.1
Figure O.1	MACsec Protocol Attributes	O.2
Figure O.2	Ethernet II Frame	O.3
Figure O.3	MACsec-Enabled Ethernet II Frame	O.3
Figure O.4	MACsec on Point-to-Point ICS LAN	O.4
Figure O.5	Secure Communication Using MACsec	O.5
Figure O.6	Point-to-Point Architecture.....	O.6
Figure O.7	MKA Verification.....	O.7
Figure O.8	Automatic MKA CAK Rotation.....	O.8

This page intentionally left blank

Preface

Manual Overview

This instruction manual covers the SEL-3610 Port Server, the SEL-3620 Ethernet Security Gateway, and the SEL-3622 Security Gateway, a small form-factor version of the SEL-3620. Although the SEL-3622 is functionally similar to the SEL-3620, some features are different because of the small size of the SEL-3622. Mentions of the SEL-3620 apply also to the SEL-3622, except where noted. This instruction manual describes the functionality and use of the SEL-3610 Port Server and the SEL-3620 Ethernet Security Gateway, as well as the use of the SEL-3622 Security Gateway for space- and power-constrained applications.

An overview of the manual's layout and the topics that are addressed follows.

Section 1: Introduction and Specifications. Introduces device applications, connectivity, and use requirements. This section also lists specifications.

Section 2: Installation. Provides device dimension drawings and instructions for initialization.

Section 3: Managing Users. Explains how users are managed on the devices.

Section 4: Job Done Examples. Provides four Job Done examples. These examples provide step-by-step configuration of the SEL-3610 and SEL-3620 for application in various SCADA and engineering access environments.

Section 5: Settings and Commands. Lists and describes all of the settings that are shared between the SEL-3610 and SEL-3620.

Section 6: SEL-3620 and SEL-3622 Security Services. Lists and describes the Security features of the SEL-3620 including IPsec, Firewall, and Proxy Services.

Section 7: Proxy Services and Password Management. Describes Proxy Services and Password Management for SEL-3620 and SEL-3622 Security Gateways.

Section 8: Testing and Troubleshooting. Describes specific services, settings, and commands.

Appendix A: Firmware and Manual Versions. Lists firmware and manual revisions.

Appendix B: Firmware Upgrade Instructions. Provides instructions to update device firmware.

Appendix C: Best Practices for Emergency Readiness. Provides recommended practices for continued IED access through the SEL-3620/SEL-3622 in the event of system failures.

Appendix D: Open Network Ports. Provides information intended to help security auditors verify that the network hosts and open ports on a control network are what is expected.

Appendix E: User-Based Accounts. Provides an introduction to user-based accounts and the benefits associated with using user-based accounts.

- Appendix F: Syslog. Provides an introduction to the Syslog Protocol and its uses in SEL products.
- Appendix G: Networking Fundamentals. Provides an introduction to the Open Systems Interconnect model.
- Appendix H: Classless Inter-Domain Routing. Explains Classless Inter-Domain Routing (CIDR) and CIDR notation.
- Appendix I: Virtual Local Area Networks. Describes what VLANs are, what they were designed for, and how they should be used in control system environments.
- Appendix J: Internet Protocol Security. Describes how the SEL-3620 employs IPsec and the strengths and shortcomings of IPsec.
- Appendix K: X.509. Explains X.509 certificates structure and use.
- Appendix L: Lightweight Directory Access Protocol. Describes Lightweight Directory Access Protocol (LDAP) and its use in SEL products.
- Appendix M: SEL RADIUS Dictionary. Contains the descriptions of the attributes that are supported by the SEL-3620.
- Appendix N: Web Server Security With Transport Layer Security. Describes how Transport Layer Security (TLS) protects web server communications.
- Appendix O: Media Access Control Security (MACsec). Provides an overview and description of the Media Access Control Security (MACsec) protocol and its implementation in SEL devices.
- Appendix P: Cybersecurity Features. Describes the mechanisms within the SEL-3620 for managing electronic access.

Safety Information

To ensure proper safety and operation, the equipment ratings, installation instructions, and operating instructions must be checked before commissioning or maintenance of the equipment. The integrity of any protective conductor connection must be checked before carrying out any other actions. It is the responsibility of the user to ensure that the equipment is installed, operated, and used for its intended function in the manner specified in this manual. If misused, any safety protection provided by the equipment may be impaired.

This manual uses three kinds of hazard statements, defined as follows.



DANGER
Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.



WARNING
Indicates a potentially hazardous situation that, if not avoided, **could** result in death or serious injury.



CAUTION
Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury or equipment damage.

Safety Symbols

The following symbols are often marked on SEL products.

	CAUTION Refer to accompanying documents.	ATTENTION Se reporter à la documentation.
	Earth (ground)	Terre
	Protective earth (ground)	Terre de protection
	Direct current	Courant continu
	Alternating current	Courant alternatif
	Both direct and alternating current	Courant continu et alternatif
	Instruction manual	Manuel d'instructions

Safety Marks

The following statements apply to this device.

General Safety Marks

CAUTION There is danger of explosion if the battery is incorrectly replaced. Replace only with Rayovac no. BR2335 or equivalent recommended by manufacturer. See Owner's Manual for safety instructions. The battery used in this device may present a fire or chemical burn hazard if mistreated. Do not recharge, disassemble, heat above 100°C or incinerate. Dispose of used batteries according to the manufacturer's instructions. Keep battery out of reach of children.	ATTENTION Une pile remplacée incorrectement pose des risques d'explosion. Remplacez seulement avec un Rayovac no BR2335 ou un produit équivalent recommandé par le fabricant. Voir le guide d'utilisateur pour les instructions de sécurité. La pile utilisée dans cet appareil peut présenter un risque d'incendie ou de brûlure chimique si vous en faites mauvais usage. Ne pas recharger, démonter, chauffer à plus de 100°C ou incinérer. Éliminez les vieilles piles suivant les instructions du fabricant. Gardez la pile hors de la portée des enfants.
For use in Pollution Degree 2 environment.	Pour l'utilisation dans un environnement de Degré de Pollution 2.
Ambient air temperature shall not exceed 40°C (104°F).	La température de l'air ambiant ne doit pas dépasser 40°C (104°F).
Terminal Ratings Tightening Torque Terminal Blocks: 0.8 Nm (7 in-lb)	Spécifications des bornes Couple de serrage Borniers: 0.8 Nm (7 livres-pouce)

Other Safety Marks (Sheet 1 of 2)

DANGER Disconnect or de-energize all external connections before opening this device. Contact with hazardous voltages and currents inside this device can cause electrical shock resulting in injury or death.	DANGER Débrancher tous les raccordements externes avant d'ouvrir cet appareil. Tout contact avec des tensions ou courants internes à l'appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	AVERTISSEMENT L'utilisation de cet appareil suivant des procédures différentes de celles indiquées dans ce manuel peut désarmer les dispositifs de protection d'opérateur normalement actifs sur cet équipement.
WARNING Halting the system requires physical access to the device in order to restart it.	AVERTISSEMENT Arrêter le système requiert un accès direct à l'équipement pour être capable de le redémarrer.

Other Safety Marks (Sheet 2 of 2)

⚠️WARNING The Halt System function should only be used in emergencies. If this feature is used, the only way to restore the unit to service is to physically cycle the power applied. This requires physical access to the unit.	⚠️AVERTISSEMENT La fonction Arrêt du Système (Halt System) ne devrait être utilisée qu'en cas d'urgence. Si cette caractéristique est utilisée, la seule façon de remettre l'unité en état de marche est de débrancher puis rebrancher l'alimentation. Ceci requiert un accès direct à l'unité.
⚠️WARNING Have only qualified personnel service this equipment. If you are not qualified to service this equipment, you can injure yourself or others, or cause equipment damage.	⚠️AVERTISSEMENT Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n'êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d'autres personnes ou endommager l'équipement.
⚠️CAUTION Equipment components are sensitive to electrostatic discharge (ESD). Undetectable permanent damage can result if you do not use proper ESD procedures. Ground yourself, your work surface, and this equipment before removing any cover from this equipment. If your facility is not equipped to work with these components, contact SEL about returning this device and related SEL equipment for service.	⚠️ATTENTION Les composants de cet équipement sont sensibles aux décharges électrostatiques (DES). Des dommages permanents non-détectables peuvent résulter de l'absence de précautions contre les DES. Raccordez-vous correctement à la terre, ainsi que la surface de travail et l'appareil avant d'en retirer un panneau. Si vous n'êtes pas équipés pour travailler avec ce type de composants, contacter SEL afin de retourner l'appareil pour un service en usine.
⚠️CAUTION If you enable a new Web Client and your current computer is not in the Allowed Web Clients list, you will be locked out of the web interface.	⚠️ATTENTION Si vous autorisez un nouveau Client de Toile et que votre ordinateur n'est pas sur la liste de Clients de Toile Autorisés, l'accès à l'interface de toile vous sera verrouillé.
⚠️CAUTION To avoid losing system logs during a factory-default reset, configure the SEL-3620 to forward Syslog messages.	⚠️ATTENTION Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-3620 pour envoyer les messages de l'enregistreur du système ("Syslog").

General Information

Typographic Conventions

There are three ways to communicate with the SEL-3610/SEL-3620/SEL-3622:

- Using a command line interface on a PC terminal emulation window
- Using the front-panel menus and pushbuttons
- Using ACCELERATOR QuickSet Software

The instructions in this manual indicate these options with specific font and formatting attributes. The following table lists these conventions:

Example	Description
STATUS	Commands, command options, and command variables typed at a command line interface on a PC.
n SUM n	Variables determined based on an application (in bold if part of a command).
<Enter>	Single keystroke on a PC keyboard.
<Ctrl+D>	Multiple/combination keystroke on a PC keyboard.
Start > Settings	PC software dialog boxes and menu selections. The > character indicates submenus.
ENABLE	Relay front- or rear-panel labels and pushbuttons.
MAIN > METER	Relay front-panel LCD menus and relay responses visible on the PC screen. The > character indicates submenus.

Trademarks

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission.

SEL trademarks appearing in this manual are shown in the following table.

ACSELERATOR Architect®	ACSELERATOR QuickSet®
ACSELERATOR Report Server®	

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-3610 and the SEL-3620. These examples are for demonstration purposes only; the firmware identification information or settings values included in these examples may not necessarily match those in the current version of your devices.

Copyrighted Software

The software included in this product may contain copyrighted software licensed under terms that give you the opportunity to receive source code. You may obtain the applicable source code from SEL by sending a request to:

Legal Department
GPL Compliance
Schweitzer Engineering Laboratories, Inc.
One Schweitzer Drive
Pullman, WA 99163

Please include your return address, product number, and firmware revision.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

This page intentionally left blank

S E C T I O N 1

Introduction and Specifications

Introduction

The SEL-3610 Port Server and the SEL-3620 Ethernet Security Gateway are two closely related products in form and function. The two devices are built upon the same platform and many similarities exist between the two products. This manual describes and illustrates the use of both products. Typically, the SEL-3620 will be located as the access point into a control system LAN while the SEL-3610 will be located within the control system LAN.

The SEL-3622 Security Gateway is a small form-factor version of the SEL-3620, built on a smaller and lower-power platform, intended for application in small enclosures such as pole cabinets.

This section includes the following information about these products.

- *Product Overviews* on page 1.1
- *Product Features* on page 1.3
- *Product Applications* on page 1.5
- *SEL-3610/SEL-3620 Connections and LED Indicators* on page 1.9
- *Software System Requirements* on page 1.19
- *General Safety and Care Information* on page 1.20
- *SEL-3610 and SEL-3620 Specifications* on page 1.21
- *SEL-3622 Specifications* on page 1.24

Product Overviews

SEL-3610 Port Server Overview

The SEL-3610 is a cryptographic port server that is capable of mapping 17 EIA-232, EIA-422, or EIA-485 serial connections to Ethernet connections through any combination of serial-to-Ethernet, serial-to-serial, and Ethernet-to-serial conversions. These mappings establish virtual bonds between one or more logical Ethernet ports and one or more physical serial ports. The SEL-3610 provides five options for sending serial data over Ethernet links: SSH, Telnet, Raw TCP, Modbus TCP, and UDP encapsulation. The port server converts serial DNP3 to Ethernet DNP3 by using the Raw TCP or UDP encapsulation options. The port server also converts serial Modbus to Ethernet Modbus by using the Modbus protocol option. The SEL-3610 filters communications based on which connections are allowed to listen and those that are allowed to transmit. The SEL-3610 is primarily used as a serial port expansion for an existing communications processor or hardened computer.



Figure 1.1 SEL-3610 Port Server

SEL-3620 Ethernet Security Gateway Overview

The SEL-3620 Ethernet Security Gateway is an access control device that provides single sign-on functionality to protected IEDs, cryptographic message protection across untrusted Ethernet or serial communications links, and a stateful deny-by-default firewall. The SEL-3620 routes information between Ethernet networks and maps communications between any combination of logical Ethernet ports and its 17 physical serial ports. The SEL-3620 is extremely flexible with the ability to supply transparent connections and cryptographically authenticated connections for protected SCADA communications and Engineering Access.

As the access point, the SEL-3620 has many features designed to allow authorized communications while denying unauthorized access. The SEL-3620 exe-GUARD feature ensures system integrity by using a secure kernel to prevent unauthorized access or modification of system data and monitors critical system services to detect unexpected activity caused by unauthorized modifications to the device program. The SEL-3620 provides all the same port server functionality described in the SEL-3610 summary with the addition of being able to configure Ethernet-to-Ethernet protocol conversions, such as Telnet to SSH or TCP to UDP.



Figure 1.2 SEL-3620 Ethernet Security Gateway

SEL-3622 Security Gateway Overview

The SEL-3622 Security Gateway delivers the functionality of the SEL-3620 Ethernet Security Gateway in a small package while consuming less power. The SEL-3622 protects IED access with the same access control, single sign-on, cryptographic message protection, and firewall features provided by the SEL-3620. Redesigned for applications serving just a few IEDs in remote locations, the SEL-3622 routes information between Ethernet networks and maps communications between any combination of logical Ethernet ports and its four physical serial ports. Physical access can be a bigger concern in the environments for which the SEL-3622 is intended. To mitigate these concerns, the SEL-3622 contains physical sensors and an input contact to detect physical tampering.



Figure 1.3 SEL-3622 Security Gateway

Product Features

SEL-3620 and SEL-3622 Features

The following features are unique to the SEL-3620 and the SEL-3622:

- **Single Sign-On Engineering Access.** Obtain user authenticated engineering access to managed devices by entering your unique username and password only once.
- **Password Management.** Schedule and perform regular password changes of managed devices.
- **Stateful Firewall.** Prevent malicious traffic from entering or exiting your private networks.
- **Secure VPN Ethernet Communication.** Provide confidential communication and maintain integrity between devices through the use of IPsec VPNs.
- **Secure Layer 2 Ethernet Communication.** Maintain integrity and provide optional confidentiality for communication between devices via the use of Media Access Control Security (MACsec).
- **Routing and NAT.** Perform static routing and network address translation (NAT) with outbound NAT and port forwarding.
- **Script Engine.** Run scripts to perform regular activities on managed devices.
- **Online Certificate Status Protocol (OCSP).** Verify X.509 certificates have not been revoked.
- **Ethernet to Ethernet port mappings.**
- **Multiple outbound TCP or UDP Ethernet destinations from one serial source.**

SEL-3622 Features

The following features are unique to the SEL-3622.

- **Small Size.** The small size of the SEL-3622 makes it usable even in small enclosures.
- **Low Power.** Low power consumption allows the SEL-3622 to be powered from a battery.
- **Physical Tamper Detection.** Detect physical tampering with the built-in accelerometer, light sensor, and input contact.

Common Features

The following features are common to the SEL-3600 family of devices.

- **Ethernet Bridging.** Ethernet bridging allows you to create a reliable Ethernet ring topology.
- **Secure Architecture and Malware Protection.** Maximize reliability with integrated exe-GUARD whitelist antivirus and other malware protections, eliminating costly patch management and signature updates. Prevent unauthorized executables from running on the SEL-3600 platform with the built-in exe-GUARD whitelist protection suite.
- **RADIUS Support.** Authenticate logins by using Remote Authentication Dial-In User Service (RADIUS) servers for strong centralized access control and user accountability.
- **SNMP Monitoring.** Monitor system health and integrity by using SNMP.
- **Serial-to-Ethernet Communications.** Establish persistent serial connections over an Ethernet infrastructure by using SSH, Telnet, Raw TCP, or UDP encapsulation.
- **Modbus TCP/Serial Conversions.** Communicate with serial and Ethernet Modbus products.
- **Serial Mappings.** Create highly granular SCADA and protection network configurations with a variety of serial-to-serial, serial-to-Ethernet, and point-to-multipoint mappings.
- **Master Port.** Configure one or more serial or Ethernet ports as master ports for authenticated access to protected devices.
- **X.509 Certificates.** Cryptographically authenticate connection requests.
- **Centralized User-Based Access.** Provide strong, centralized access control and user accountability with Lightweight Directory Access Protocol.
- **Time Synchronization.** Maintain synchronous logs among your devices, and source time synchronization to downstream devices.
- **Syslog.** Log events with Syslog for consistency, compatibility, and centralized collection and analysis.
- **Interoperability.** Communicate securely with devices from multiple vendors.
- **5V Pin 1 Power on Serial Ports.** Directly power 5 V devices from the serial ports. (SEL-3610/SEL-3620 only. On the SEL-3622, the serial ports are unpowered.)
- **802.1Q VLAN Tagging.** Segregate traffic to improve network organization, manageability, and performance.
- **Reliability.** SEL products are built for availability, hardened for harsh environments, and carry a ten-year warranty.
- **Analog Bit-Based Conversion.** Transform Conitel and other bit-based protocols to Ethernet and reduce reliance on expensive analog circuits.
- **Service Port.** Automate base-lining of the device settings with a basic command-line interface.
- **Front-Port USB.** Ethernet Out of Band Management Port for local access only. Dynamic Host Configuration Protocol (DHCP) server provides IP address for a connected device.
- **EIA-232 Character Pacing.** Add additional whole-character periods of idle time between each character.

Product Applications

SEL-3610 Applications

The SEL-3610 is ideally suited for serial port expansion applications through its serial tunneling over Ethernet and Modbus and DNP3 serial-to-Ethernet conversion features. The flexible port mapping of the SEL-3610 enables creating logical port mappings to eliminate future physical rewiring.

Serial Port Expansion

The SEL-3610 increases the number of serial devices that hardened control systems computers and communications processors can support. *Figure 1.4* shows the SEL-3610 providing serial port expansion for the SEL-3530 Real-Time Automation Controller (RTAC). Communications processors or computers will route Ethernet traffic destined for a serial device hooked to the SEL-3610 across the LAN. The SEL-3610 uses SSH for cryptographically protected data communications, Telnet, Raw TCP, or UDP encapsulation for unencrypted, serial encapsulated communications, and Modbus for conversions between the RTAC and the connected serial devices. DNP3 can also be used with the Raw TCP or UDP mapping mode.

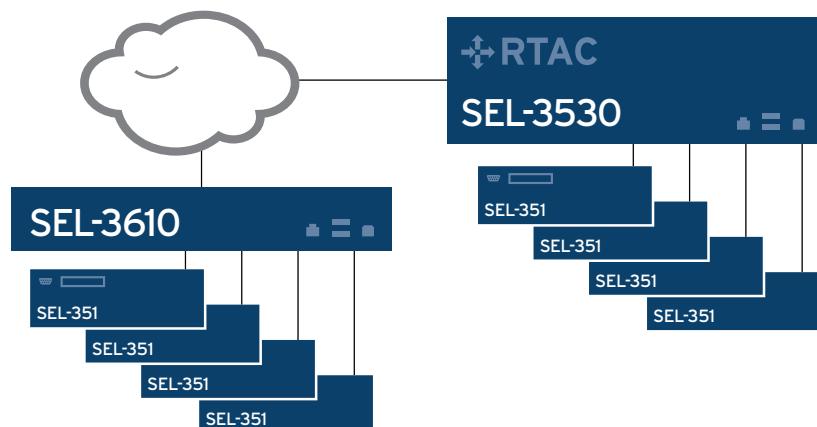


Figure 1.4 Serial Port Expansion

Point-to-Point Serial Over Ethernet Network

Figure 1.5 shows the SEL-3610 in a point-to-point application in which serial devices can communicate with each other across an Ethernet network. The SEL-3610 supports SSH for encrypted and authenticated communications.

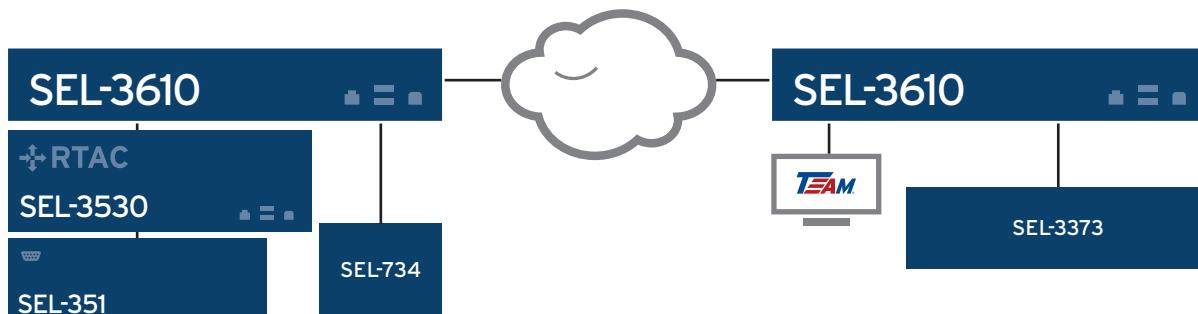


Figure 1.5 Serial Over Ethernet

Communications Diagnostics

The port switch functionality of the SEL-3610 enables the configuration and troubleshooting of a variety of Ethernet and serial communication scenarios without having to physically pull plugs or rewire cables. The port server can filter communications based on which connections listen or transmit. This can provide a mirroring function to listen in on control system communications. *Figure 1.6* illustrates the mirroring of a serial communication stream between the SEL-2411 Programmable Automation Controller and the SEL-3355 Automation Controller to an engineer's laptop over an Ethernet connection. The SEL-2411 and SEL-3355 do not listen for any response from the engineer's laptop, effectively making the laptop a read-only serial data sniffer.

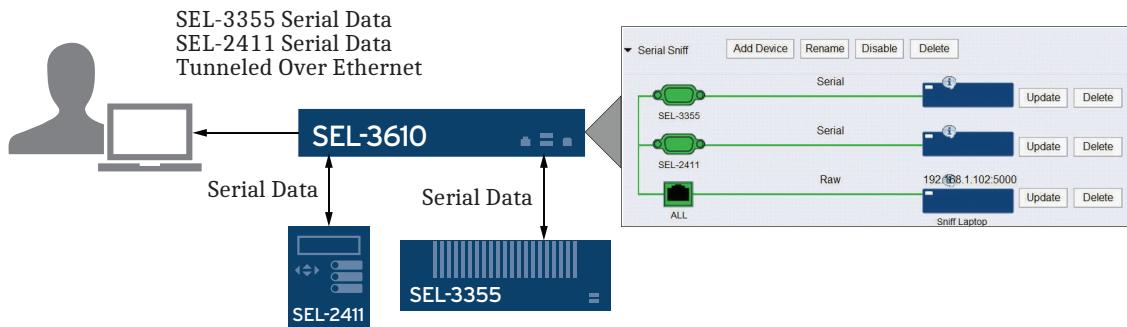


Figure 1.6 Port Mirroring

SEL-3620 Applications

The SEL-3620 is ideally suited for access control applications with its strong cryptographic, reporting, and automation capabilities. It is well suited to being placed at the security perimeter of your control system network. Specific applications the SEL-3620 has been designed for include user-based access to managed devices, routing, traffic filtering, protecting communications that traverse an untrusted physical network, and managing the passwords of managed devices.

The SEL-3622 is the choice for applications that demand the security and access controls of the SEL-3620 in tight quarters such as remote cabinets. In the applications below, the SEL-3622 is a drop-in replacement for the SEL-3620.

Secure User-Based Access to IEDs

The proxy services in the SEL-3620 provide user-based access to serial and Ethernet devices within the secured network. The SEL-3620 records and logs all user activity to provide an audit trail and user accountability.

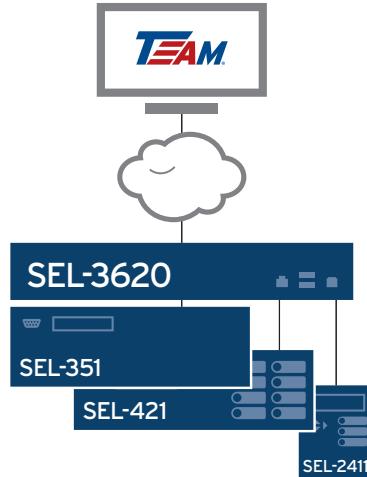


Figure 1.7 User-Based Access to IEDs

Routing

The SEL-3620 forwards communications among separate Ethernet networks. Any device that has access to the SEL-3620 can use it to forward Ethernet packets to a destination on a different network. This eliminates the need for a flat network and solves many of the security and management concerns with large flat networks. Additionally, the SEL-3620 also supports NAT, which allows for the masquerading of networks or hosts.

Ethernet Filtering

The SEL-3620 contains a stateful, deny-by-default firewall to prevent unauthorized incoming and outgoing communications. This ensures that all transmissions ingressing or egressing the trusted network are relevant to the protection and engineering functions of the site (see *Figure 1.8*). For additional network security and operator visibility, the SEL-3620 can provide granular control of logging for all established, rejected, dropped, or closed connections.



Figure 1.8 Active Traffic Filtering

Secure Communications Over Untrusted Networks

The SEL-3620 secures all communication by establishing IPsec VPN tunnels with other SEL-3620 gateways and IPsec-enabled devices.

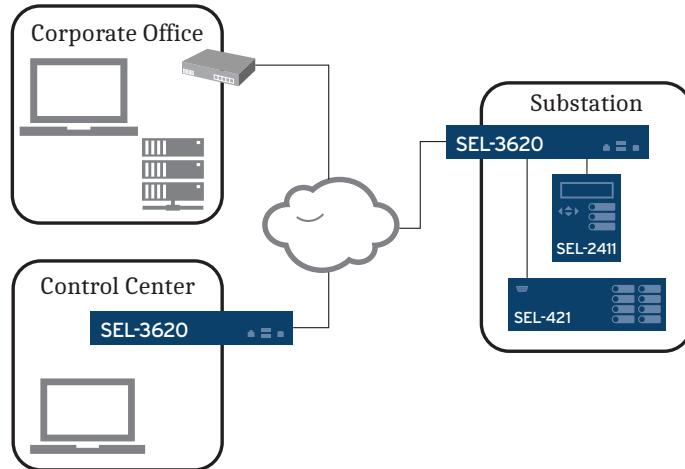


Figure 1.9 Encrypted and Authenticated Ethernet Communications

Password Management

The SEL-3620 is uniquely designed to manage the passwords of all your protected IEDs. The single sign-on capabilities of the proxy services require that the SEL-3620 is aware of the passwords of all protected devices behind it. The combination of the internal script engine and the password knowledge gives the SEL-3620 the ability to manage the passwords of your managed devices, enforce strong passwords, and provide audit reports of all password changes.

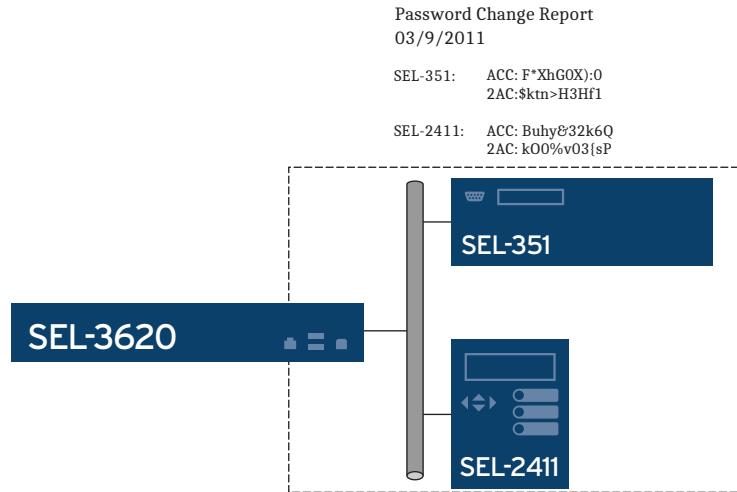


Figure 1.10 Password Management

SEL-3622 Applications

The SEL-3622 makes strong cryptographic, reporting, and automation capabilities available to protection device communications in smaller-scale environments such as pole cabinets where small size and low power requirements are essential.

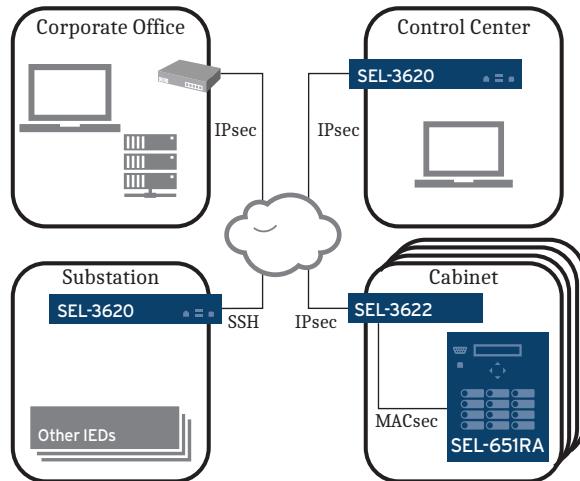


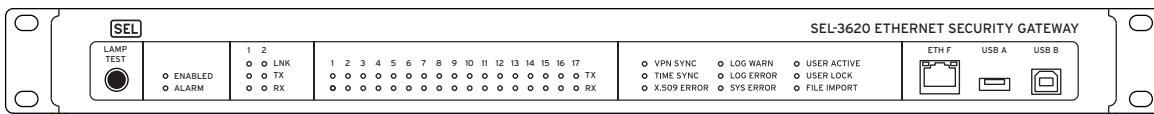
Figure 1.11 SEL-3622 Communication Encryption

SEL-3610/SEL-3620 Connections and LED Indicators

Front Panel

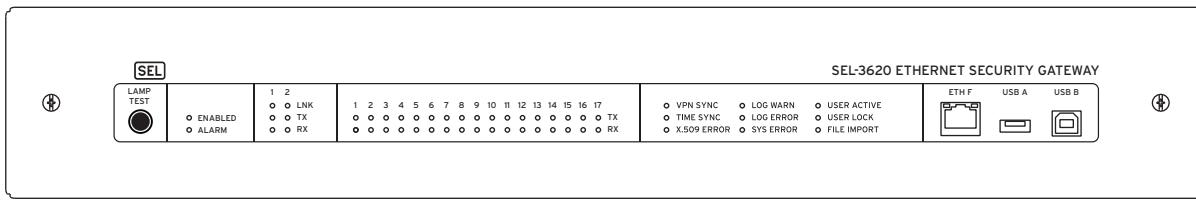
Figure 1.12 shows the front panel of the SEL-3620. The front panel of the SEL-3610 is identical in function. The front panel includes all of the activity and status LED indicators of the device. There are TX and RX indicators for each serial port and the rear Ethernet ports. Additionally, the rear Ethernet ports have link indicators. The front Ethernet port has link and activity indicators built into the port itself. There are 11 status indicators on the front panel. During normal operations, each of these indicators should be green. If certain services are disabled, some of these LEDs may not be illuminated. A red LED indicates a non-optimal condition has been found.

Rack Mount



i4468e

Panel Mount



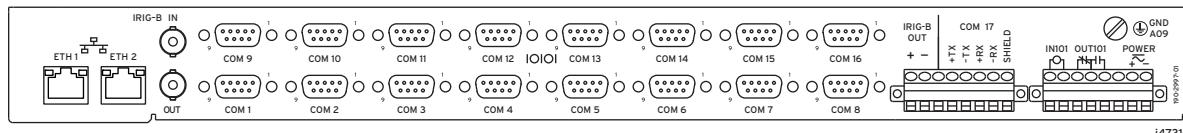
i4467f

Figure 1.12 Front-Panel Diagrams

Rear Panel

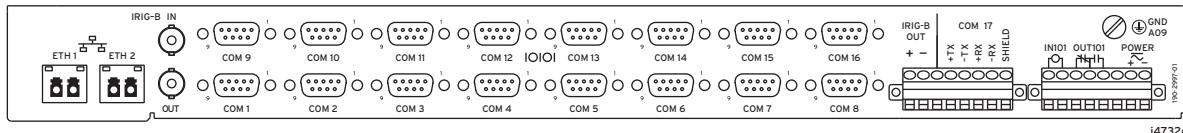
Figure 1.13 shows the rear panel of the device. The device has 16 DB-9 serial ports, one isolated 8-pin serial port, two Ethernet ports, two IRIG coaxial ports, the power connector, and the alarm contact on the back panel.

Copper Ethernet



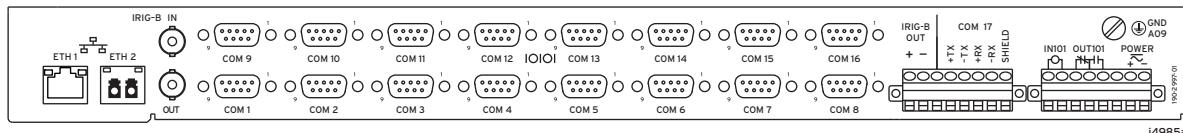
i4731c

Fiber Ethernet



i4732c

Mixed Ethernet



i4985a

Figure 1.13 Rear-Panel Diagrams

Serial Ports

There are 16 DB-9 serial ports on the rear panel of the device. These serial ports are all capable of EIA-232, EIA-422, and EIA-485 communications. There is one isolated 8-pin crimp-style connected port.

See *Table 1.1* for the pinout for the 16 DB-9 ports. See *Table 1.2* for the pinout of the isolated 8-position crimp-style connector port.

Table 1.1 Serial DB-9 Port Pinout

EIA-232	EIA-422/EIA-485 (4 Wire) ^a
Pin 1: N/C or +5 Vdc ^b	Pin 1: N/C or +5 Vdc ^b
Pin 2: RXD	Pin 2: -RXD ^a
Pin 3: TXD	Pin 3: -TXD ^a
Pin 4: +IRIG-B ^c	Pin 4: +IRIG-B
Pin 5: GND	Pin 5: GND
Pin 6: -IRIG-B ^d	Pin 6: -IRIG-B
Pin 7: RTS ^e	Pin 7: +TXD ^a
Pin 8: CTS	Pin 8: +RXD ^a
Pin 9: GND	Pin 9: GND

^a For 2-wire EIA-485 operation, jumper 2 to 3 and jumper 7 to 8.

^b Also DCD input on COM1 if +5 Vdc is disabled.

^c DTR jumper JMP2 option for COM1.

^d DSR jumper JMP1 option for COM1.

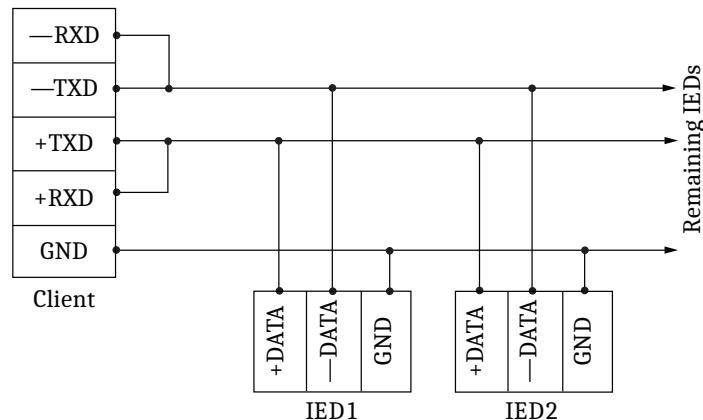
^e RTS line is normally always HIGH, unless Push-To-Talk mode is enabled.

Table 1.2 Isolated Port Pinout

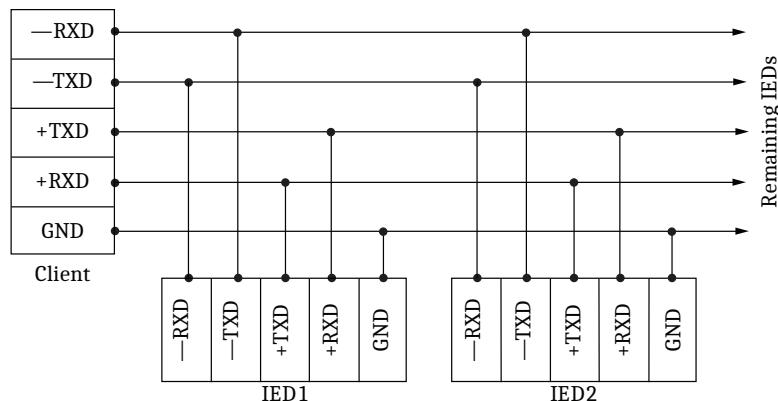
EIA-232	EIA-422/EIA-485 (4 Wire) ^a
Pin 1: +IRIG-B	Pin 1: +IRIG-B
Pin 2: -IRIG-B	Pin 2: -IRIG-B
Pin 3: N/C	Pin 3: N/C
Pin 4: RTS ^b	Pin 4: +TX ^a
Pin 5: TX	Pin 5: -TX ^a
Pin 6: CTS	Pin 6: +RX ^a
Pin 7: RX	Pin 7: -RX ^a
Pin 8: Shield ^c	Pin 8: Shield

^a For 2-wire EIA-485 operation, jumper 4 to 6 and jumper 5 to 7.^b RTS line is normally always HIGH, unless Push-To-Talk mode is enabled.^c Normally, this terminal is connected to the cable shield, which is also connected to the chassis ground on the distant end equipment.

Example EIA-485 Wiring Scenarios



Termination and bias resistors are not shown, but may be necessary for some networks.

Figure 1.14 EIA-485 Typical Two-Wire Connection

Termination and bias resistors are not shown, but may be necessary for some networks.

Figure 1.15 EIA-485 Typical Four-Wire Connection

Ethernet Ports

The device has three orderable options for Ethernet ports. The options are described in *Table 1.3*.

Table 1.3 Ethernet Port Option

Option 0	Three 10/100 Mbps RJ45 Ethernet ports. Two are located on the rear panel, and one is located on the front panel.
Option 1	Two 10/100 Mbps RJ45 Ethernet ports, one located on the front panel and one on the rear panel, and one 100 Mbps LC multimode fiber Ethernet port on the rear panel.
Option 2	One 10/100 Mbps RJ45 Ethernet port on the front panel, and two 100 Mbps LC multimode fiber Ethernet ports on the rear panel.
Option 3	Two 10/100 Mbps RJ45 Ethernet ports, one located on the front panel and one on the rear panel, and one 100 Mbps LC single-mode fiber Ethernet port on the rear panel.
Option 4	One 10/100 Mbps RJ45 Ethernet port on the front panel, and two 100 Mbps LC single-mode fiber Ethernet ports on the rear panel.

The rear RJ45 Ethernet ports are capable of auto-crossover, making a crossover cable between a computer and the device unnecessary. The front RJ45 Ethernet port is not capable of auto-crossover, so a hub or crossover cable may be required if your connected device does not perform auto-crossover.

IRIG Coaxial Ports

There are two coaxial ports on the rear panel of the device. These ports are labeled **IRIG-B IN** and **IRIG-B OUT**. The device can receive a modulated or demodulated IRIG-B signal. The device can output a demodulated IRIG-B signal.

Power Supply Connections

The device has three orderable power supply options described in *Table 1.4*.

Table 1.4 Power Supply Options

Option 1	125–250 Vdc or 110–230 Vac at 50/60 Hz
Option 2	48–125 Vdc or 110 Vac at 50/60 Hz
Option 3	24–48 Vdc

The **POWER** terminal on the rear panel must connect to a source within the rated range of the SEL-3620. The **POWER** terminals are isolated from the chassis ground. Use 1.5–2.5 mm² (16–14 AWG) wire to connect to the **POWER** terminals. See *Figure 1.16* and *Table 1.5* for more information about wiring the power input terminals.

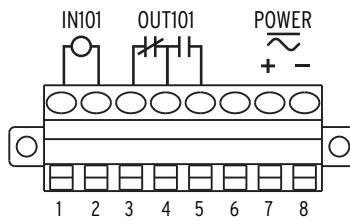


Figure 1.16 Rear Connector Diagram

Table 1.5 I/O Pin Designations

Pin	Designation
1	IN101
2	IN101
3	OUT101 NC
4	OUT101 Common
5	OUT101 NO
6	(not connected)
7	Power + (Hot)
8	Power - (Neutral)

Connect the ground terminal **GND (A09)** on the rear panel to a rack frame or switchgear ground for proper safety and performance. Use 2.5 mm² (14 AWG) wire less than 2 meters (6.6 feet) in length for the ground connection.

Alarm Output Connections

The device comes with an alarm contact to alert you to various system events. Under normal operations, the alarm contact will be closed. The alarm contact will pulse or latch in response to various system events. The device features a normally open (NO) and normally closed (NC) contact across Pins 3–5 (see *Table 1.5*).

NOTE: When the unit is turned off, the NC alarm contact will be closed, and the NO contact will be open.

Table 1.6 Conditions for SEL-3610/SEL-3620 Alarm Contacts

Condition	Alarm Contact Activity
All device subsystems are operational	NC alarm contact will be latched open, and NO alarm contact will be latched closed
Successful settings change	One-second alarm contact pulse
Successful user login	One-second alarm contact pulse
User account lockout	Three one-second alarm contact pulses
Hardware warning event	Five-second alarm contact pulse
Kernel audit failure	Five-second alarm contact pulse
Hardware failure	NC alarm contact will be latched closed, and NO alarm contact will be latched open

See *Digital Outputs* on page 1.23 for information about wiring the alarm contacts.

Discrete Input Connections (SEL-3610/SEL-3620 Only)

The two discrete input terminals can be used to sense a dc input voltage. For example, you can connect the terminals to a sensing voltage through a switch activated by a physical sensor (moisture, door opening, temperature, etc.—see

Figure 1.21). The sensing voltage for the SEL-3610 and SEL-3620 is 125 Vdc, polarity independent. If the terminals were so connected, Syslog messages would be produced every time the switch opened or closed.

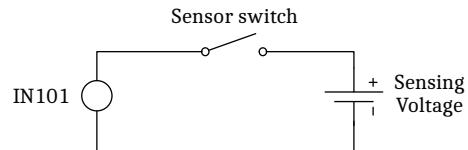


Figure 1.17 Connecting a Sensor to the Discrete Input

With the discrete input terminals connected as shown in *Figure 1.21*, Syslog messages are sent each time the switch opens or closes. *Table 1.7* describes the default Syslog messages. The Syslog messages are user-configurable.

Table 1.7 Syslog Message Description

Switch	Syslog Message
Closed	Input contact energized
Open	Input contact de-energized

Jumper Pins

Jumper pins are needed to enable modem usage on COM 1 of the device or to enable emergency access mode (see *Section 8: Testing and Troubleshooting*).

Table 1.8 Jumper Pin Designations

Jumper	Position
JMP1	1–2 routes DSR signal to COM 1 pin 6. 2–3 routes IRIG-B ground to COM 1 pin 6 (default).
JMP2	1–2 routes DTR signal to COM 1 pin 4. 2–3 routes IRIG-B+ to COM 1 pin 4 (default).
JMP3	OPEN (default).
JMP4	OPEN (default).
JMP6	OPEN (default). Block C enables emergency access.

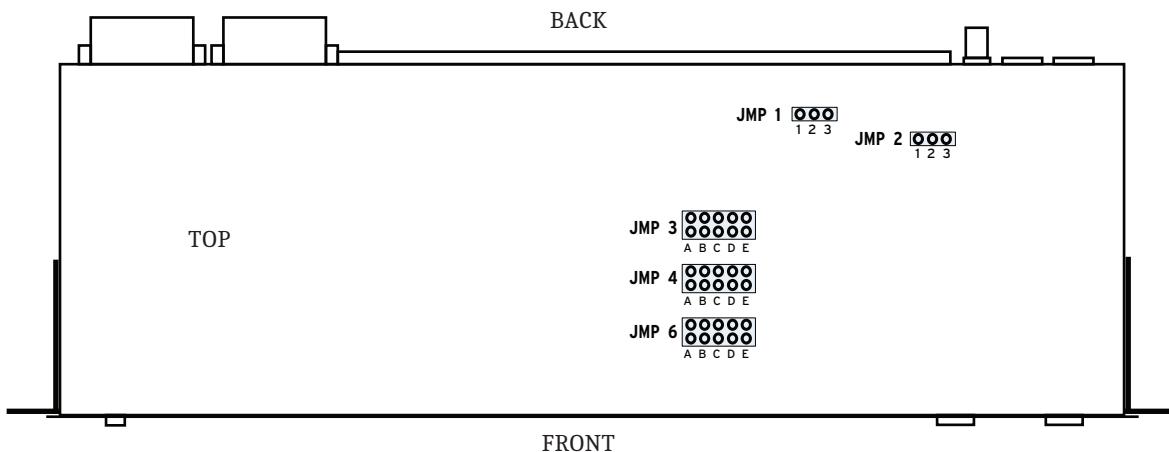


Figure 1.18 Jumper Locations

SEL-3622 Connections and LED Indicators

Front Panel

Figure 1.19 shows the front panel of the SEL-3622. The front panel includes all of the activity and status LED indicators of the device. There are RX and TX indicators for each serial port and the rear Ethernet ports. Additionally, the rear Ethernet ports have link indicators. The front Ethernet port has link and activity indicators built into the port itself. There are eight status indicators on the front panel. During normal operations, each of these indicators should be green. If certain services are disabled, some of these LEDs may not be illuminated. A red LED indicates that a non-optimal condition exists.

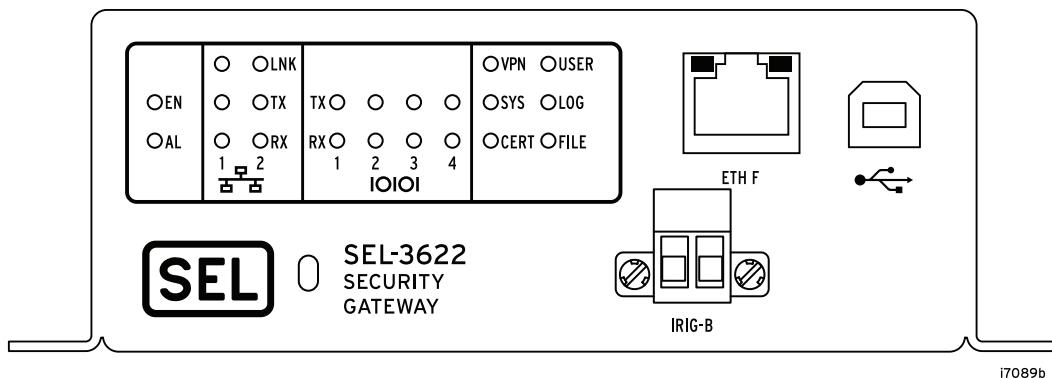


Figure 1.19 SEL-3622 Front-Panel Diagram

Rear Panel

Figure 1.20 shows the rear panel of the device. The device has four DB-9 serial ports, two Ethernet ports, the power connector, and the alarm contact on the back panel. Ordering options provide for two copper, one fiber and one copper, or two fiber Ethernet ports.

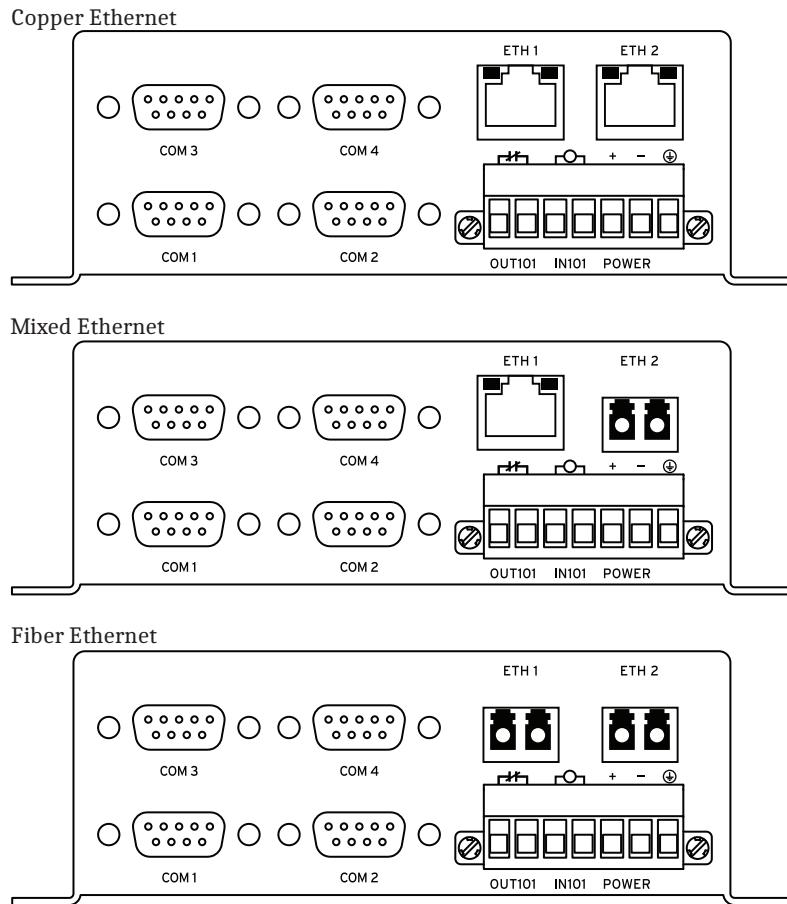


Figure 1.20 SEL-3622 Rear-Panel Diagrams

Serial Ports

NOTE: Do not use serial cables longer than 10 meters.

There are four DB-9 serial ports on the rear panel of the device. COM 1 and COM 2 are capable of EIA-232, EIA-422, and EIA-485 communications. COM 3 and COM 4 are EIA-232 only. See *Table 1.9* for the pinout for the four DB-9 serial ports. Note that the SEL-3622 does *not* support Pin 1 power.

Table 1.9 Serial DB-9 Port Pinout

EIA-232	EIA-422/EIA-485(4 Wire)	EIA-485 (2 Wire)
Pin 1: N/C	Pin 1: N/C	Pin 1: N/C
Pin 2: RXD	Pin 2: -RXD	Pin 2: N/C
Pin 3: TXD	Pin 3: -TXD	Pin 3: TXD
Pin 4: +IRIG-B	Pin 4: +IRIG-B	Pin 4: N/C
Pin 5: GND	Pin 5: GND	Pin 5: GND
Pin 6: -IRIG-B	Pin 6: -IRIG-B	Pin 6: N/C
Pin 7: RTS ^a	Pin 7: +TXD	Pin 7: N/C
Pin 8: CTS	Pin 8: +RXD	Pin 8: RXD
Pin 9: GND	Pin 9: GND	Pin 9: N/C

^a RTS line is normally always HIGH, unless Push-To-Talk mode is enabled.

Ethernet Ports

The device has five orderable options for Ethernet ports. The options are described in *Table 1.10*.

Table 1.10 Ethernet Port Option

Option 0	Two 10/100 Mbps RJ45 Ethernet ports on the rear panel.
Option 1	One 10/100 Mbps RJ45 Ethernet port and one 100 Mbps LC multimode fiber Ethernet port on the rear panel.
Option 2	Two 100 Mbps LC multimode fiber Ethernet ports on the rear panel.
Option 3	One 10/100 Mbps RJ45 Ethernet port and one 100 Mbps LC single-mode fiber Ethernet port on the rear panel.
Option 4	Two 100 Mbps LC single-mode fiber Ethernet ports on the rear panel.

All RJ45 Ethernet ports on the SEL-3622 are capable of auto-crossover, making a crossover cable between a computer and the device unnecessary.

Power Supply Connections

The device is designed to operate from a 12–24-volt or 24–48-volt dc power source. The **POWER** terminals are isolated from the chassis ground. Use 1.5–2.5 mm² (16–14 AWG) wire to connect to the **POWER** terminals. See *Figure 1.21* for more information about wiring the power input terminals.

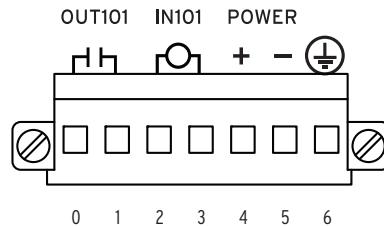


Figure 1.21 Rear Connector Diagram

Table 1.11 I/O Pin Designations

Pin	Description
0	Alarm Contact Output
1	Alarm Contact Output
2	Discrete Input
3	Discrete Input
4	DC Power +
5	DC Power -
6	Frame Ground

Connect the ground terminal labeled with the ground symbol on the rear panel to a rack frame or switchgear ground for proper safety and performance. Use 14 AWG (2.5 mm²) wire less than 2 m (6.6 feet) in length for the ground connection.

For both the alarm contact output and digital input, SEL recommends 20–14 AWG (0.5–2.0 mm²) wire of sufficient current capacity and voltage rating for the application.

Alarm Output Connections

The device comes with an alarm contact to alert you to various system events. Under normal operations the alarm contact will be open. The alarm contact will pulse or latch in response to various system events. By default, the device features a single NO alarm contact on Pins 0–1. Later versions of the hardware added the ability to select an NC alarm contact. If the 10th character of the MOT of the device is “X,” then the alarm contact is NO.

NOTE: When the unit is turned off, the alarm contact will be open.

Table 1.12 Conditions for SEL-3622 Alarm Contacts

Condition	Alarm Contact Activity
All device subsystems are operational	Alarm contact will be latched closed
Successful settings change	One-second alarm contact pulse
Successful user login	One-second alarm contact pulse
Physical system event	One-second alarm contact pulse
User account lockout	Three 1-second alarm contact pulses
Hardware warning event	Five-second alarm contact pulse
Kernel audit failure	Five-second alarm contact pulse
Hardware failure	Alarm contact to be latched open

See *Electromechanical Output* on page 1.26 for information about wiring the alarm contacts.

Discrete Input Connections (SEL-3622 Only)

The two discrete input terminals can be used to sense a dc input voltage. For example, you can connect the terminals to a sensing voltage through a switch activated by a physical sensor (moisture, door opening, temperature, etc.) (see *Figure 1.21*). The sensing voltage for the SEL-3622 is either 12 Vdc or 24 Vdc nominal (depending on the ordering option), polarity independent. If the terminals were so connected, Syslog messages would be produced every time the switch opened or closed.

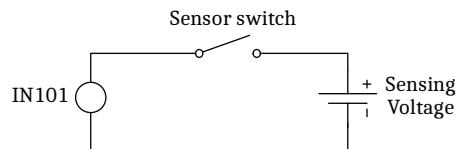


Figure 1.22 Connecting a Sensor to the Discrete Input on the SEL-3622

With the discrete input terminals connected as shown in *Figure 1.21*, Syslog messages are sent each time the switch opens or closes. *Table 1.13* describes the default Syslog messages. The Syslog messages are user-configurable.

Table 1.13 Syslog Message Description

Switch	Syslog Message
Closed	Input contact energized
Open	Input contact de-energized

Jumper Pins

Jumper pins are used to enable emergency access mode. See *Section 8: Testing and Troubleshooting* for more information.

Table 1.14 Jumper Location

Jumper	Position
JMP1	Block C enables emergency access

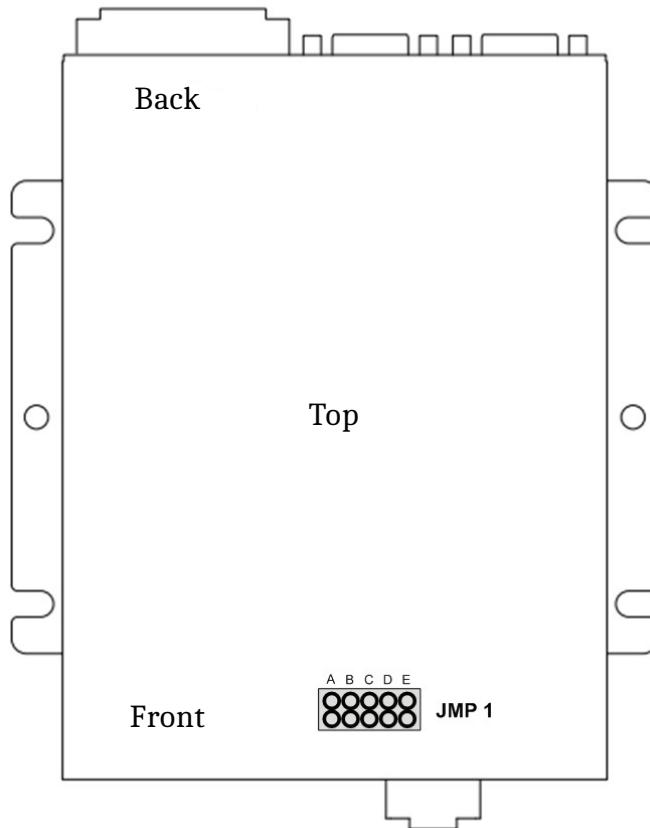


Figure 1.23 JMP1 Location

Software System Requirements

The device is primarily managed through the internal HTTPS server. This server requires a web browser capable of HTTPS communication.

The SEL-3620 Proxy Services require a connection directory that can be built with ACCELERATOR QuickSet SEL 5030 Software. This software is freely available from SEL.

General Safety and Care Information

General Safety Notes

The SEL-3610 and SEL-3620/SEL-3622 are designed for restricted access locations. Access should be limited to qualified service personnel.

The SEL-3610 and SEL-3620/SEL-3622 should not be installed or operated in a condition not specified in this manual.

Cleaning Instructions

The device should be de-energized (by removing the power connection to both the power and alarm connection) before cleaning.

The case can be wiped down with a damp cloth. Solvent-based cleaners should not be used on plastic parts or labels.

SEL-3610 and SEL-3620 Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

47 CFR 15B, Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

UL Listed to U.S. and Canadian safety standards (File E220228; NRAQ, NRAQ7)

CE Mark

UKCA Mark

RCM Mark

Networking

Web Management

Protection Protocols:	HTTPS, TLSv1.2, TLSv1.3
Authentication:	X.509 and Username/Password
Encryption Key Strength:	128-bit, 256-bit

Virtual Private Networks (SEL-3620 Only)

Maximum Throughput:	30 Mbps
Maximum Concurrent Sessions:	16
Protection Protocols:	IPsec
Key Exchange:	IKEv1, IKEv2
Authentication:	Passphrase, X.509, OCSP
Accelerated Encryption Algorithms:	AES
Nonaccelerated Encryption Algorithms:	3DES, Blowfish
Encryption Key Strength:	128-bit, 256-bit, 512-bit

Routing Functions (SEL-3620 Only)

Static Routing

Network Address Translation: Port Forwarding (DNAT) as many as 200 user-specified rules

Network Address Translation: Outbound NAT (SNAT)

Ethernet Protocols

Address Resolution Protocol (ARP)
Dynamic Host Configuration Protocol (DHCP) Client
Dynamic Host Configuration Protocol (DHCP) Server (USB-B Only)
Encapsulating Security Payload (ESP) (SEL-3620 only)
File Transfer Protocol (FTP) (SEL-3620 only)
Hypertext Transfer Protocol Secure (HTTPS)

Internet Control Message Protocol (ICMP)

Internet Key Exchange (IKEv1/v2) (SEL-3620 only)

Internet Protocol Security (IPsec) Protocol Suite (SEL-3620 only)

Internet Secure Association and Key Management Protocol (ISAKMP) (SEL-3620 only)

Lightweight Directory Access Protocol (LDAP) Client

MACsec Key Agreement (SEL-3620 Only)

Media Access Control Security (MACsec) (SEL-3620 Only)

Modbus TCP/IP

Network Time Protocol (NTP) Client/Server

Online Certificate Revocation Protocol (OCSP) (SEL-3620 only)

Remote Authentication Dial-In User Service (RADIUS)

Secure Shell version 2 (SSHv2) Client/Server

Simple Network Management Protocol (SNMP)

Spanning Tree Protocol (STP)

Syslog

Telnet

Transmission Control Protocol (TCP)

Transport Layer Security (TLS)

User Datagram Protocol (UDP)

VLAN

Maximum number of VLANs per physical interface (SEL-3610): 1

Maximum number of VLANs per physical interface (SEL-3620): 4

Security

User-Based Accounts

Maximum Local Accounts:	256
Password Length:	8–128 characters
Password Set:	All printable ASCII characters
User Roles:	Administrative and Technician

Syslog

Storage for 60,000 messages

Forwarding to 3 destinations

Firewall (SEL-3620 Only)

Implementation:	iptables
As many as 1000 user-specified rules supported	

Proxy Services (SEL-3620 Only)

Maximum number of simultaneous users: 10

Maximum number of managed devices: 150

Time to generate 1050 passwords: <20 minutes

MACsec (SEL-3620 Only)

Connectivity Associations:	One per physical Ethernet port
Encryption Key:	GCM-AES-128

General

Operating Temperature Range

-40° to +85°C (-40° to +185°F)
Note: Not applicable to UL applications.

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II
Relative Humidity:	5%–95%, non-condensing
Maximum Altitude:	2000 m

Dimensions

1U Rack Mount:	482.6 mm W x 43.7 mm H x 159 mm D (19" W x 1.72" H x 6.26" D)
1U Panel Mount:	502.9 mm W x 80 mm H x 159 mm D (19.8" W x 3.15" H x 6.26" D)

Weight

2.35 kg (5.2 lb)

Warranty

10 Years

Processing and Memory

Processor Speed:	533 MHz
Memory:	1024 MB DDR2 ECC SDRAM
Storage:	4 GB

System Speeds

Firmware Update Time (Varies):	10 min
Cold Boot-Up Time:	2 min

Time-Code Input

IRIG accuracy depends on external GPS source

Input Type:	IRIG-B000 or B002, Even or Odd parity
-------------	---------------------------------------

NTP accuracy depends on network conditions

Modulated IRIG-B (BNC)

On (1) State:	$V_{ih} \geq 3.3 \text{ V}_{pp}$
Off (0) State:	$V_{il} \leq 0.1 \text{ V}_{pp}$
Input Impedance:	2.5 kΩ
Accuracy:	500 μs

Demodulated IRIG-B (BNC)

On (1) State:	$V_{ih} \geq 2.2 \text{ V}$
Off (0) State:	$V_{ih} \leq 0.8 \text{ V}$
Input Impedance:	2.5 kΩ
Accuracy:	250 ns

Network Time Protocol (Ethernet)

Accuracy:	10 ms (varies)
-----------	----------------

Time-Code Output

IRIG accuracy depends on source accuracy
 NTP accuracy depends on network conditions

Demodulated IRIG-B000 Even Parity (BNC and Serial)

On (1) State:	$V_{oh} \geq 2.4 \text{ V}$
Off (0) State:	$V_{ol} \leq 0.8 \text{ V}$
Load:	50 Ω

Output Drive Levels

Demodulated IRIG-B:	TTL 120 mA, 3.5 Vdc, 25 Ω
Serial Port:	TTL 2.5 mA, 2.4 Vdc, 1 kΩ
Network Time Protocol (Ethernet)	

Accuracy: 250 μs (ideal on LAN)

Communications Ports

Ethernet Ports

Ports:	2 rear, 1 front
Data Rate:	10 or 100 Mbps
Front Connector:	RJ45 Female
Rear Connectors:	RJ45 Female or LC Fiber (single-mode or multimode, 100 Mbps only)
Standard:	IEEE 802.3

Fiber Optic

100BASE-FX Multimode Option (to 2 km)	
Maximum TX Power:	-14 dBm
Minimum TX Power:	-19 dBm
RX Sensitivity:	-30 dBm
System Gain:	11 dB
Source:	LED
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

100BASE-LX10 Single-Mode Option (to 15 km)

Maximum TX Power:	-8 dBm
Minimum TX Power:	-15 dBm
RX Sensitivity:	-25 dBm
System Gain:	10 dB
Source:	Laser
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

Serial Ports

Type:	EIA-232/EIA-422/EIA-485 (software selectable)
Data Rate:	1200 to 115200 bps
Connectors:	DB-9 Female (Ports 1–16), Isolated 8 pin (Port 17)
Power:	+5 Vdc power on Pin 1 (500 mA maximum cumulative for 16 ports)

USB Ports					
1 Host Port:	Type A (nonfunctional, for future use)	Cyclic Capacity (2.5 Cycles/Second):	Per IEC 60255-0-20: 1974: 24 V 0.75 A L/R = 40 ms 48 V 0.50 A L/R = 40 ms 125 V 0.30 A L/R = 40 ms 250 V 0.20 A L/R = 40 ms		
1 Device Port:	Type B Supports USB Networking with DHCP server for out-of-band management access (driver downloadable from selinc.com)	Mechanical Durability:	10 million no-load operations		
Power Supply					
Input Voltage					
Rated Supply Voltage:	125–250 Vdc; 110–240 Vac, 50/60 Hz 48–125 Vdc; 120 Vac, 50/60 Hz 24–48 Vdc	Operational Voltage (U_e):	250 Vac/Vdc		
Input Voltage Range:	85–300 Vdc or 85–264 Vac 38.4–137.5 Vdc or 88–132 Vac, 18–60 Vdc polarity dependent	Rated Insulation Voltage (U_i):	300 Vac/Vdc		
Power Consumption					
AC:	<40 VA	Utilization Category:	AC-15 (control of electromagnetic loads >72 VA)		
DC:	<30 Watts	Contact Rating Designation:	B300 (B = 5A, 300 = rated insulation voltage)		
Input Voltage Interruptions					
20 ms at 24 Vdc 20 ms at 48 Vdc 50 ms at 125 Vac/Vdc 100 ms at 250 Vac/Vdc	Rated Operational Current (I_e):	3 A at 120 Vac 1.5 A at 240 Vac			
Digital Inputs					
Contact Input					
125 Vdc:	Pickup: 105–150 Vdc Dropout: <75 Vdc	Conventional Enclosed Thermal Current (I_{the}) Rating:	5 A		
Digital Outputs					
DC Ratings					
Rated Operational Voltage (U_e):	24–250 Vdc	Operate Current:	>1 mA		
Rated Voltage Range:	19.2–275 Vdc	Rated Operational Voltage (U_e):	240 Vac		
Rated Insulation Voltage (U_i):	300 Vdc	Voltage Protection Across Open Contacts:	270 Vac, 40 J		
Continuous Carry:	6 A at 70°C 4 A at 85°C	Pickup/Dropout Time:	≤ 16 ms (coil energization to contact closure).		
Make:	30 A at 250 Vdc per IEEE C37.90	Electrical Durability Make VA Rating:	3600 VA, cos j = 0.3		
Thermal:	50 A for 1 s	Electrical Durability Break VA Rating:	360 VA, cos j = 0.3		
Contact Protection:	360 Vdc, 40 J MOV protection across open contacts	Mechanical Durability:	10,000 no-load operations		
Leakage Current in a 500 Ω load at Rated Voltage:	<0.02 mA	Rated Frequency:	50/60 ± 5 Hz		
Impedance of a Closed Output, in D.C.:	<1 Ω				
Bouncing Measured in Resistive Load of 10 kW at Rated Voltage:	<5 ms				
Operating Time (Coil Energization to Contact Closure, Resistive Load):	Pickup time ≤5 ms typical Dropout time of ≤5 ms typical				
Breaking Capacity (10,000 Operations):	Per IEC 60255-0-20: 1974: 24 V 0.75 A L/R = 40 ms 48 V 0.50 A L/R = 40 ms 125 V 0.30 A L/R = 40 ms 250 V 0.20 A L/R = 40 ms				
Type Tests					
Electromagnetic Compatibility (EMC)					
Emissions:	IEC 60255-25:2000 Canada ICES-001 (A) / NMB-001 (A)				
Electromagnetic Compatibility Immunity					
Conducted RF Immunity:	IEC 60255-22-6:2001 10 Vrms IEC 61000-4-6:2008 10 Vrms				
Digital Radio Telephone RF Immunity:	ENV 50204:1995 10 V/m at 900 MHz and 1.89 GHz				
Electrostatic Discharge Immunity:	IEC 60255-22-2:2008 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEC 61000-4-2:2008 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEEE C37.90.3-2001 2, 4, and 8 kV contact; 4, 8, and 15 kV air				
Fast Transient/Burst Immunity:	IEC 60255-22-4:2008 Class A: 4 kV at 5 kHz, 2 kV at 5 kHz on comm ports IEC 61000-4-4:2004 + CRGD:2006 4 kV at 5 kHz				

Magnetic Field Immunity:	IEC 61000-4-8:2001 1000 A/m for 3 s, 100 A/m for 1 min IEC 61000-4-9:2001 1000 A/m	Dry Heat:	IEC 60068-2-2:2007 16 hours at +85°C
Power Supply Immunity:	IEC 60255-11:2008 IEC 61000-4-11:2004 IEC 61000-4-29:2000	Vibration:	IEC 60255-21-1:1988 Class 1 Endurance, Class 2 Response IEC 60255-21-2:1988 Class 1 Shock Withstand, Bump Class 2 Shock Response IEC 60255-21-3:1993 Class 2 Quake Response
Radiated Radio Frequency Immunity:	IEC 60255-22-3:2007 10 V/m IEC 61000-4-3:2008 10 V/m IEEE C37.90.2-2004 35 V/m		
Surge Immunity:	IEC 60255-22-5:2008 1 kV Line-to-Line 2 kV Line-to-Earth IEC 61000-4-5:2005 1 kV Line-to-Line 2 kV Line-to-Earth	Safety	
Surge Withstand Capability:	IEC 60255-22-1:2007 2.5 kV peak common mode 1.0 kV peak differential mode IEEE C37.90.1-2002 2.5 kV oscillatory 4 kV fast transient waveform	Dielectric Strength:	IEC 60255-5:2000 2500 Vac on contact inputs and contact outputs, 1 min 3100 Vdc on power supply, 1 min IEEE C37.90-2005 2500 Vac on contact inputs and contact outputs, 1 min 3100 Vdc on power supply, 1 min
Environmental Tests		Impulse:	IEC 60255-5:2000, 0.5 Joule 5 kV IEEE C37.90-2005, 0.5 Joule 5 kV
Cold:	IEC 60068-2-1:2007 16 hours at -40°C	IP Code:	IEC 60529:2001 + CRGD:2003 IP20
Damp Heat, Cyclic:	IEC 60068-2-30:2005 25°C to 55°C, 6 cycles, 95% relative humidity		

SEL-3622 Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

47 CFR 15B, Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

UL Listed to U.S. and Canadian safety standards (File E220228; NRAQ, NRAQ7)

CE Mark

UKCA Mark

RCM Mark

Networking

Web Management

Protection Protocols:	HTTPS, TLSv1.2, TLSv1.3
Authentication:	X.509 and Username/Password
Encryption Key Strength:	128-bit, 256-bit, 512-bit

Virtual Private Networks

Maximum Throughput:	4 Mbps
Maximum Concurrent Sessions:	4
Protection Protocols:	IPsec
Key Exchange:	IKEv1, IKEv2
Authentication:	Passphrase, X.509, OCSP
Nonaccelerated Encryption Algorithms:	AES, 3DES, Blowfish
Encryption Key Strength:	128-bit, 256-bit

Routing Functions

Static Routing
Network Address Translation: Port Forwarding (DNAT) as many as 200 user-specified rules

Network Address Translation: Outbound NAT (SNAT)

Ethernet Protocols

Address Resolution Protocol (ARP)
Dynamic Host Configuration Protocol (DHCP) Client
Dynamic Host Configuration Protocol (DHCP) Server (USB-B Only)
Encapsulating Security Payload (ESP)
File Transfer Protocol (FTP)

Hypertext Transfer Protocol Secure (HTTPS)
 Internet Control Message Protocol (ICMP)
 Internet Key Exchange (IKEv1/v2)
 Internet Protocol Security (IPsec) Protocol Suite
 Internet Secure Association and Key Management Protocol (ISAKMP)
 Lightweight Directory Access Protocol (LDAP) Client
 MACsec Key Agreement (MKA)
 Media Access Control Security (MACsec)
 Modbus TCP/IP
 Network Time Protocol (NTP) Client/Server
 Online Certificate Revocation Protocol (OCSP)
 Remote Authentication Dial-In User Service (RADIUS)
 Secure Shell version 2 (SSHv2) Client/Server
 Simple Network Management Protocol (SNMP)
 Spanning Tree Protocol (STP)
 Syslog
 Telnet
 Transmission Control Protocol (TCP)
 Transport Layer Security (TLS)
 User Datagram Protocol (UDP)

VLAN

Maximum number of VLANs per physical interface: 4

Security**User-Based Accounts**

Maximum Local Accounts: 256
 Password Length: 8–128 characters
 Password Set: All printable ASCII characters
 User Roles: Administrative and Technician

Syslog

Storage for 60,000 messages
 Forwarding to 3 destinations

Firewall

Implementation: iptables
 As many as 1000 user-specified rules supported

Physical Tamper Sensors

Accelerometer, light sensor, discrete contact input

Proxy Services

Maximum number of simultaneous users: 5
 Maximum number of managed devices: 25
 Time to generate 175 passwords: <10 minutes

MACsec

Connectivity Associations: One per physical Ethernet port
 Encryption Key: GCM-AES-128

General**Operating Temperature Range**

–40° to +85°C (–40° to +185°F)
Note: Not applicable to UL applications.

Operating Environment

Pollution Degree:	2
Oversupply Category:	II
Relative Humidity:	5%–95%, non-condensing
Maximum Altitude:	2000 m
Insulation Class:	Class I equipment

Dimensions

Surface Mount: 140.7 mm W x 45.1 mm H x 176.1 D
 (5.54" W x 1.78" H x 6.93" D)

Weight

0.54 kg (1.2 lb)

Warranty

10 Years

Processing and Memory

Processor Speed:	333 MHz
Memory:	512 MB DDR2 SDRAM
Storage:	2 GB

System Speeds

Firmware Update Time (Varies):	15 min
Cold Boot-Up Time:	3.5 min

Time-Code Input

IRIG accuracy depends on external GPS source
 Input Type: IRIG-B000 or B002, Even or Odd parity

NTP accuracy depends on network conditions

Demodulated IRIG-B (Front-Panel Connector)

On (1) State:	$V_{ih} \geq 2.2$ V
Off (0) State:	$V_{il} < 0.8$ V
Input Impedance:	1.5 k Ω
Accuracy:	250 ns

Network Time Protocol (Ethernet)

Accuracy: 10 ms (varies)

Time-Code Output

IRIG accuracy depends on source accuracy
 NTP accuracy depends on network conditions
Demodulated IRIG-B000 Even Parity (Serial)
 On (1) State: $V_{oh} \geq 2.4$ V
 Off (0) State: $V_{ol} \leq 0.8$ V

Output Drive Levels		Input Voltage	
Serial Port:	TTL 24 mA 2.4 Vdc 120 Ω	Rated Supply Voltage:	12–24 Vdc 24–48 Vdc
Network Time Protocol (Ethernet)		Input Voltage Range	
Accuracy:	250 µs (ideal on LAN)	Input Voltage Range:	9.8–30 Vdc, polarity dependent 19.2–57.6 Vdc, polarity dependent
Communications Ports		Power Consumption	
Ethernet Ports		DC:	<5 W copper Ethernet; <7 W fiber
Ports:	2 rear 1 front	F1:	
Data Rate:	10 or 100 Mbps interface, 5 Mbps firewall throughput	Type:	Time lag T
Front Connector:	RJ45 Female	Current Rating:	3.15 A
Rear Connectors:	RJ45 Female or LC Fiber (single-mode or multimode, 100 Mbps only)	Voltage Rating:	250 Vac, 300 Vdc
Standard:	IEEE 802.3	IEC 60127-2/5:	H = 1500 A at 250 Vac, p.f. = 0.7–0.8
Fiber Optic		UL 248-14:	10 kA at 125 Vac, p.f. = 0.7–0.8 / 1500 A at 250 Vac, p.f. = 0.7–0.8 / 1500 A at 300 Vdc
100BASE-FX Multimode Option (to 2 km)		Input	
Maximum TX Power:	-14 dBm	Optoisolated Control Input	
Minimum TX Power:	-19 dBm	12 Vdc Option	
RX Sensitivity:	-30 dBm	ON:	9.6–18 Vdc
System Gain:	11 dB	OFF:	<7.2 Vdc
Source:	LED	Current Draw at Nominal DC Voltage:	2–6 mA, Nominal is 12 Vdc
Wavelength:	1300 nm	24 Vdc Option	
Connector Type:	LC (IEC 61754-20)	ON:	19.2–28.8 Vdc
100BASE-LX10 Single-Mode Option (to 15 km)		OFF:	<11 Vdc
Maximum TX Power:	-8 dBm	Current Draw at Nominal DC Voltage:	4–7 mA, Nominal is 24 Vdc
Minimum TX Power:	-15 dBm	Electromechanical Output	
RX Sensitivity:	-25 dBm	Ratings	
System Gain:	10 dB	Normally Open (NO):	10th MOT digit is X
Source:	Laser	Normally Closed (NC):	10th MOT digit is 1
Wavelength:	1300 nm	Mechanical Durability:	10 M no-load operations
Connector Type:	LC (IEC 61754-20)	DC Output Ratings	
Serial Ports		Voltage:	250 Vdc
Type:	2 EIA-232/EIA-485 (software selectable on Ports 1 and 2) 2 EIA-232 (Ports 3 and 4)	Rated Voltage Range*:	24–250 Vdc
Data Rate:	1200 to 115200 bps	Rated Insulation Voltage:	300 Vdc
Connectors:	DB-9 Female (Ports 1–4)	Utilization Category:	DC-13
Serial Protocols Supported:	Bit- and Byte-based	Pilot Duty Ratings [†] :	R300, 250 Vdc
USB Port		Make (Short Duration Contact Current)*:	30 A @ 250 Vdc
1 Device Port:	Type B Supports USB Networking with DHCP server for out-of-band management access (driver downloadable from selinc.com)	Continuous Carry*:	6 A @ 70°C; 4 A @ 85°C
Power Supply		Thermal*:	50 A for 1 s
Complies with IEC HiPot and Impulse standards, except when connected to substation battery. The auxiliary (power supply) circuit should be connected to a battery (or other external power supply meeting application requirements) that is not used for switching inductive loads.		Contact Protection:	360 Vdc, 40 J MOV protection across open contacts
		Operation Time (Coil Energization to Contact Closure, Resistive Load)*:	Pickup/Dropout Time ≤ 8 ms typical

Breaking Capacity (10,000 Operations)*:		
48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms

Cyclic Capacity (2.5 cycles/second)*:		
48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms

AC Output Ratings

Rated Operational Voltage:	240 Vac
Rated Voltage*:	110–240 Vac
Rated Insulation Voltage:	300 Vac
Utilization Category:	AC-15 (control of electromechanic loads > 72 VA)
Pilot Duty Ratings [†] :	B300, 240 Vac
Contact Protection:	270 Vac, 40 J
Continuous Carry*:	6 Arms @ 70°C; 4 Arms @ 85°C
Rated Frequency:	50/60 ±5 Hz
Operating Time (Coil Energization to Contact Closure)*:	Pickup/Dropout Time ≤ 8 ms

* Parameters verified by SEL per IEC 60255-1:2009 and IEEE C37.90-2005.

[†] Per UL 508.

Solid-State Output Contact (Units Manufactured Prior to April 2017)

Ratings

100 mA continuous
250 Vdc or 120 Vac Operational Voltage
Maximum On Resistance: 50 Ω
Minimum Off Resistance: 10 MΩ
Insulation: 2500 Vdc
Wiring Size: 14 AWG Max. 26 AWG Min. 0.4 mm Min. Insulation 105°C, 250 V Min.

Product Standards

Communications Equipment in Utility Substations:	IEC 61850-3:2013 IEEE 1613-2009 Severity Level: Class 1
Measuring Relays and Protection Equipment:	IEC 60255-26:2013* IEC 60255-27:2013

* Acceptance Criteria C applied to 0% dc voltage dips for 10 ms. The auxiliary (power supply) circuit is intended to be connected to a battery (or other external power supply meeting application requirements) that is not used for switching inductive loads and will provide the required hold-up time.

Type Tests

Environmental Tests

Enclosure Protection:	IEC 60529:2001 + CRGD:2003 Severity Level: IP30 (excluding the terminal blocks)
-----------------------	--

Vibration Resistance:	IEEE 1613-2009 IEC 60255-21-1:1988 Severity Level: Endurance Class 2 Response Class 2
Shock Resistance:	IEEE 1613-2009 IEC 60255-21-2:1988 Severity Level: Shock Withstand, Bump Class 1 Shock Response Class 2
Seismic:	IEC 60255-21-3:1993 Severity Level: Quake Response Class 2
Cold, Operational and Storage:	IEC 60068-2-1:2007 Severity Level: -40°C, 16 hours
Dry Heat, Operational and Storage:	IEC 60068-2-2:2007 Severity Level: 85°C, 16 hours
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25–55°C, 6 cycles, 95% relative humidity
Damp Heat, Steady State:	IEC 60068-2-78:2012 Severity Level: +40°C, 240 hours, 93% relative humidity

Dielectric Strength and Impulse Tests

The following IEC standards only apply if the device is not connected directly to the station battery.
Dielectric (HiPot): IEC 60255-27:2013 IEEE C37.90-2005 Class B, Section 8: Dielectric Tests Dielectric Strength Section Severity Level: 2500 Vac for one minute on contact inputs, contact outputs 1600 Vdc for one minute on power supply
Impulse: IEC 60255-27:2013 IEEE C37.90-2005 Class B Severity Level: 0.5 Joule, 2.5 kV

RFI and Interference Tests

EMC Immunity	
Electrostatic Discharge Immunity:	IEEE C37.90.3-2001 IEC 61000-4-2:2008 Severity Level: 2, 4, 6, 8 kV contact discharge; 2, 4, 8, 15 kV air discharge
Magnetic Field Immunity:	IEC 61000-4-8:2009 Severity Level: 1000 A/m for 3 s, 100 A/m for 1 min IEC 61000-4-9:2001 Severity Level: 1000 A/m
Power Supply Immunity:	IEC 61000-4-11:2004 IEC 61000-4-17:1999+A1:2001+ A2:2008 IEC 61000-4-29:2000
Radiated RF Immunity:	IEC 61000-4-3:2010 Severity Level: 10 V/m IEEE C37.90.2-2004 Severity Level: 35 V/m

Fast Transient, Burst Immunity:	IEC 61000-4-4:2012 Severity Level: 4 kV at 5.0 kHz 2 kV at 5.0 kHz for comm. ports
Surge Withstand Capability Immunity:	IEEE C37.90.1-2002 Severity Level: 2.5 kV oscillatory 4 kV fast transient IEC 61000-4-18:2006 + A1:2010 Severity Level: 2.5 kV common-mode 1.0 kV differential-mode 1 kV common-mode on comm. ports
Surge Immunity:	IEC 61000-4-5:2005 Severity Level: 1 kV line-to-line 2 kV line-to-earth 2 kV comm. ports
Conducted RF Immunity:	IEC 61000-4-6:2008 Severity Level: 10 Vrms
Digital Radio Telephone RF Immunity:	ENV 50204:1995 Severity Level: 10 V/m at 900 MHz and 1.89 GHz
EMC Emissions	
Radiated and Conducted Emissions:	CISPR 11:2009+A1:2010 CISPR 22:2008 ANSI C63.4-2014 Class A Canada ICES-001 (A) / NMB-001 (A)

S E C T I O N 2

Installation

Introduction

This section describes the installation and preparation for first-time use of the SEL-3610, the SEL-3620, and the SEL-3622. Except as otherwise noted, references to the SEL-3620 refer also to the SEL-3622.

This section includes the following information:

- *Dimension Drawings* on page 2.1
- *Connecting to the Device* on page 2.3
- *Commissioning the Device* on page 2.6
- *Navigating the User Interface* on page 2.7
- *The Device Dashboard* on page 2.9

Dimension Drawings

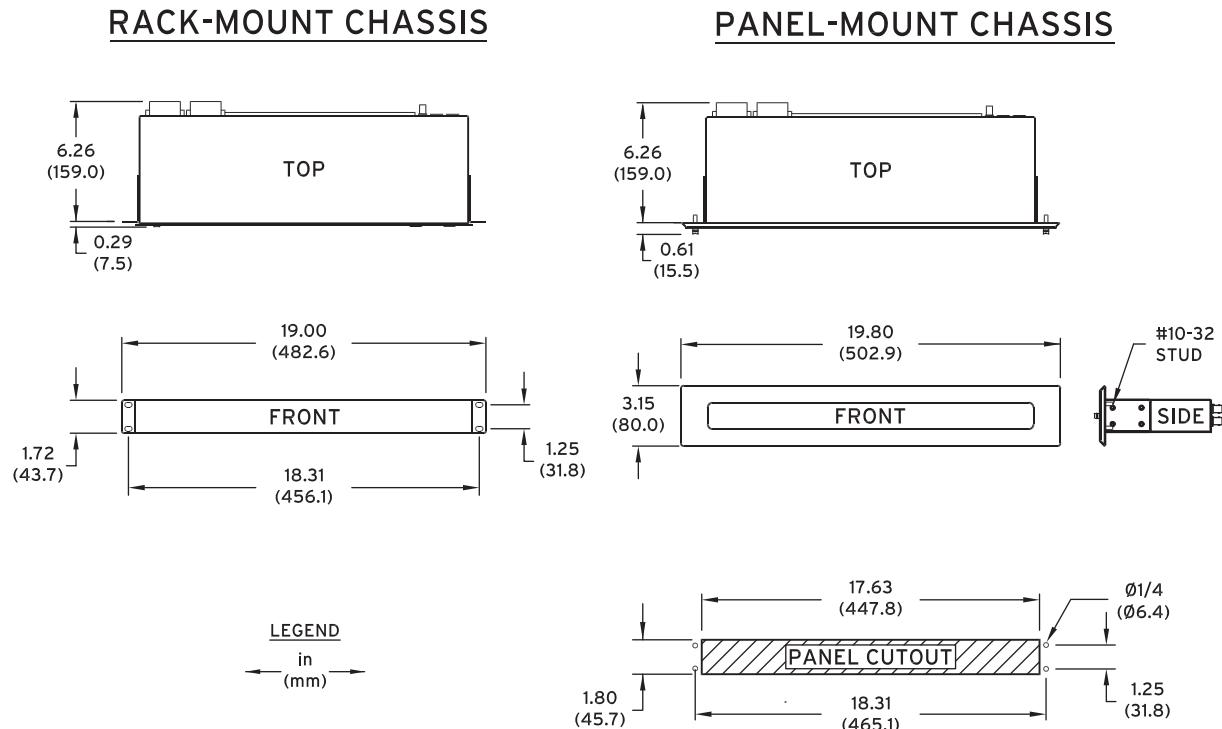


Figure 2.1 SEL-3610/SEL-3620 Dimension Drawing

i9201d

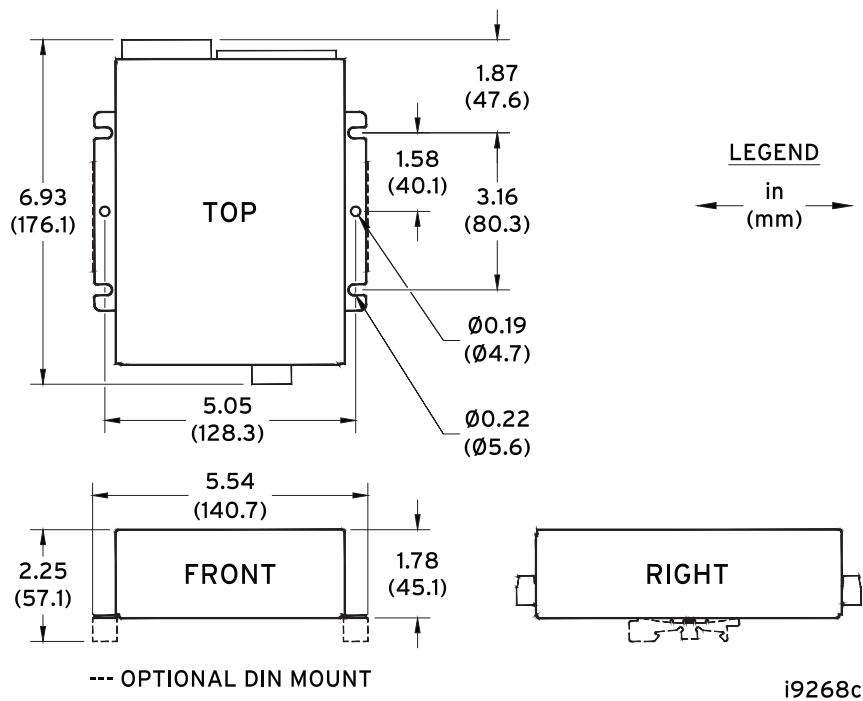


Figure 2.2 SEL-3622 Dimension Drawing

i9268c



Figure 2.3 SEL-3622 Light Sensor Location

Installation of the SEL-3622

The SEL-3622 has a light sensor to help detect physical tamper events, such as a recloser cabinet door opening. This sensor works best when it is oriented towards the opening/light source to be detected.

The light sensor aperture is located on the front panel of the SEL-3622 (circled in red in *Figure 2.3*).

Connecting to the Device

NOTE: As of firmware version R201, the device web server no longer supports connections via SSL. Ensure your web browser supports TLS 1.2 or higher.

The device includes an HTTPS web server, accessible by standard web browsers, for most of the available configuration and management functions. The device requires QuickSet to configure proxy services functionality (SEL-3620 and SEL-3622). SEL has tested the following web browsers to work with the device.

- Microsoft Internet Explorer 7 or later
- Mozilla Firefox 3.05 or later
- Google Chrome 36.0 or later

For the initial connection to a device, you will need to have the following:

- A computer with a wired Ethernet port or USB-A port
- An uncommissioned device
- One RJ45 Ethernet cable or USB-A to USB-B cable with SEL-3600 USB driver

The Physical Network

You can either use an Ethernet cable or a USB cable for the initial connection to a device. For an Ethernet connection, connect the device to your computer as shown in *Figure 2.4*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the front Ethernet port of the device. The default IP address on the device front port is 192.168.1.2 with a subnet mask of 255.255.255.0. Ensure that the IP address of your computer is in the same sub-network, e.g., 192.168.1.1.

NOTE: The front Ethernet ports of the SEL-3610 and SEL-3620 are not capable of auto-crossover. A hub, switch, or crossover cable may be necessary for your computer to communicate with it.

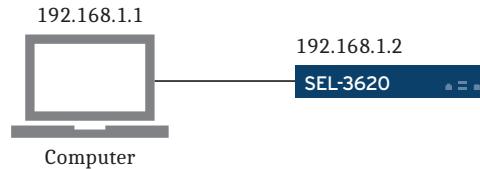


Figure 2.4 Ethernet Commissioning Network

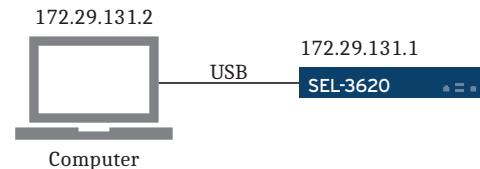


Figure 2.5 USB Commissioning Network

For a USB connection, connect the device as shown in *Figure 2.5*. Using a USB-A to USB-B cable, connect a USB port of your computer to the USB-B (front) port of the device. You will need to install the SEL-3600 USB driver if you have not already done so. The DHCP server on the USB-B port assigns the default IP address of 172.29.131.2 to the computer and 172.29.131.1 to the device.

Configuring Microsoft Windows Networking

Confirm that your computer is configured to communicate on the 192.168.1.0/24 subnet. For a description of the Classless Inter-Domain Routing (CIDR) notation, see *Appendix H: Classless Inter-Domain Routing*.

2.4 Installation Connecting to the Device

NOTE: Depending on your company's computer use policies and your user privileges, you may need the assistance of your IT department to configure networking on your workstation.

- Step 1. Start the Microsoft Windows Command Terminal. Use the Microsoft Windows Run function (from the Start menu) to run **cmd** (type **cmd** and select **OK**), as shown in *Figure 2.6*, to start the command terminal.

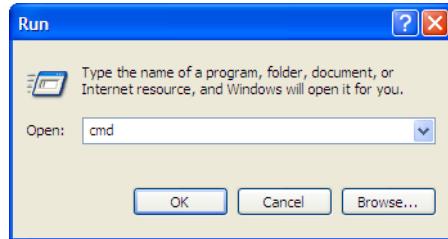


Figure 2.6 Open Terminal With Run Command

- Step 2. In the command terminal, type **ipconfig <Enter>** as shown in *Figure 2.7*. This will show you the IP address and subnet mask that your Ethernet connection is configured for. The IP address must match 192.168.1.1 and the subnet mask must match 255.255.255.0. If these values are correct, skip to *Commissioning the Device* on page 2.6.

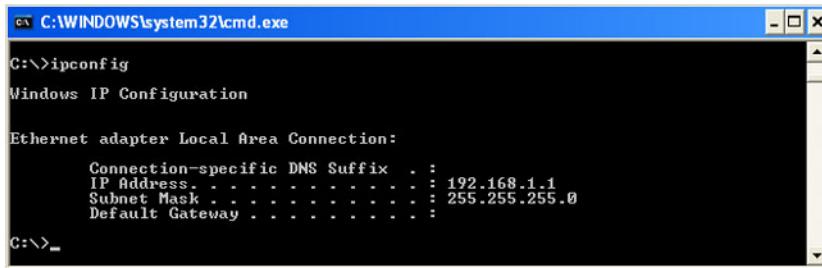


Figure 2.7 Windows IP Configuration

NOTE: Any IP address in the 192.168.1.0/24 subnet is acceptable, except for 192.168.1.2, which is taken by the device.

- Step 3. If you need to configure your computer to communicate on the 192.168.1.0/24 subnet, then open Microsoft Windows Network Connections. Do this by typing **ncpa.cpl** in the Windows Run dialog box, as shown in *Figure 2.8*. Selecting **OK** will open the Network Connections window, which contains a list of the network devices available on your computer.

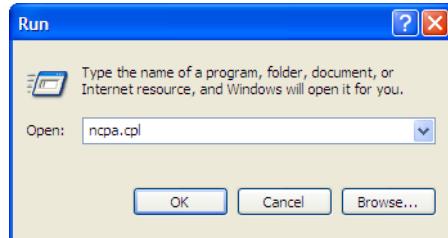


Figure 2.8 Open Network Connections With Run Command

- Step 4. Right-click on the connection you will be using to communicate with the device and select **Properties**. This connection may be labeled Local Area Connection.

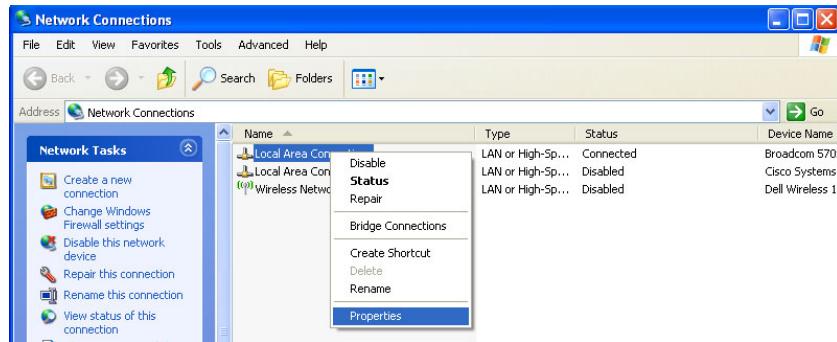


Figure 2.9 Open Connection Properties

Step 5. Select **Internet Protocol (TCP/IP)** from the list in the **This connection uses the following items** area (this entry is usually located last in the list). Select **Properties**.

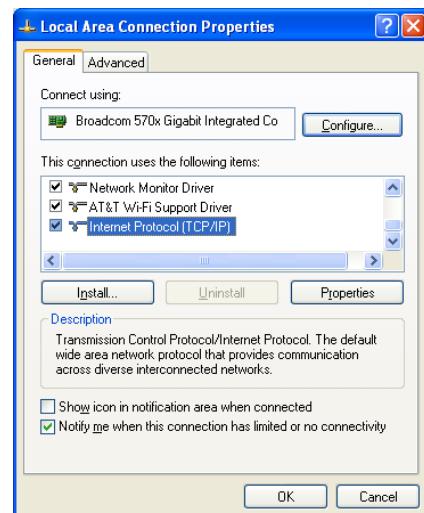


Figure 2.10 Local Area Connection Properties

Step 6. Select **Use the following IP address**. Enter **192.168.1.1** as the IP address and **255.255.255.0** as the subnet mask as shown in *Figure 2.11*. Select **OK**.

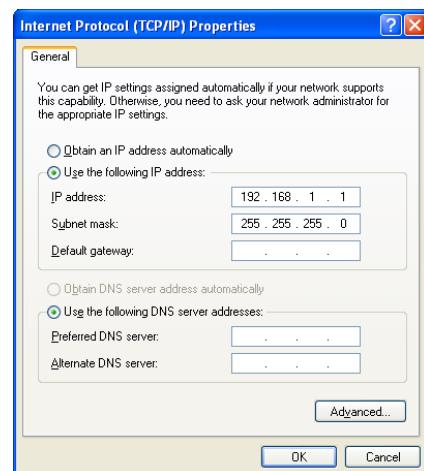


Figure 2.11 Internet Protocol (TCP/IP) Properties

- Step 7. Select **OK** in the **Local Area Connection Properties** dialog box.
The new settings will take effect once this is done.

Commissioning the Device

NOTE: You may receive a certificate error from your browser. The message depends on the browser you use. This error appears because the certificate the device is presenting to your browser does not match the IP address assigned to the device. You will need to create a certificate exception to access the device login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

NOTE: To increase security, SEL recommends creating a new certificate after commissioning your device. For information on creating an X.509 certificate, see Section 5: Settings and Commands.

The device has a default IP address of 192.168.1.2 assigned to the **ETH F** port. To connect to the device, open your preferred internet browser.

- Step 1. In your browser's address bar, enter **https://192.168.1.2**. This opens the device Commissioning Page.

With firmware R208 and higher, you can also connect locally with a USB Type B cable. The system has a DHCP server on the USB port that assigns an IP address of 172.29.131.1. The USB port is intended for short-term programming or commissioning purposes only, not for continuous use. Do not use USB cables longer than three meters.

Figure 2.12 Device Commissioning Page

NOTE: The device requires that complex passwords are used. Passwords must be at least 8 characters in length and require at least one character from each of the character sets listed below. Spaces are allowed.

Passwords can contain the following.

- Lowercase letters
- Uppercase letters
- Numbers
- Special characters (any printable character that is not alphanumeric)

- Step 2. Enter the account information for an administrative user. This includes the username and password.
- Step 3. (Optional) Enter the Network Configuration information. This information can be edited later within the device user interface. A description of these settings can be found in *Section 5: Settings and Commands*.

NOTE: Usernames are unique on the device. The same username cannot be used for multiple accounts. Once a username is taken, no other account may be created with that username unless the existing account is deleted. Usernames are case sensitive.

NOTE: If you change the protected IP address on the Commissioning Page, you will need to reconfigure your computer to communicate on the same subnet as the device.

COMMISSIONING PAGE

Admin User Account (required)	
Username:	<input type="text" value="unique_username"/>
Password:	<input type="password" value="*****"/>
Retype Password:	<input type="password" value="*****"/>
Network Configuration (required)	
Hostname:	<input type="text" value="SEL3620A"/>
Front Ethernet Port:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="2"/> / <input type="text" value="24"/>
Network Configuration (optional)	
Domain Name:	<input type="text"/>
Default Router:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
VLAN:	<input type="text"/>
<input type="button" value="Submit"/>	

Figure 2.13 Device Commissioning Form

Step 4. Select **Submit**.

Navigating the User Interface

NOTE: Your web browser must be configured to enable cookies. Enabling JavaScript is recommended, but not required.

The device has an HTTPS interface to enable easy device configuration. This HTTPS interface can be accessed by opening a web browser and navigating to the device management address. By default, this address is <https://192.168.1.2> for the front Ethernet port or <https://172.29.131.1> for the USB-B port.

When you log in to the device, you are presented with the Dashboard as shown in *Figure 2.14*. The Dashboard gives a quick overview of the status of the device. The features of the Dashboard are explained in greater detail later in this section. The SEL-3622 Dashboard page is similar, except that it shows fewer ports and LED indicators.

2.8 Installation

Navigating the User Interface



Figure 2.14 Device Status Dashboard

The far left frame of the device web interface is the navigation panel. Selecting any link on this panel will take you to the associated page that includes all of the settings and configurations for that part of the system. The navigation panel is always present on the web interface. Selecting the **Accounts** link in the navigation panel will open the User Accounts page, as shown in *Figure 2.15*.

USER ACCOUNTS					
Add User					
Username	First Name	Last Name	Admin	Account State	Creation Date Last Login Password Changed
admin			Yes	ENABLED	2015-12-18 18:23:37 2015-12-20 15:03:47 2015-12-18 18:23:37
alice	Alice	Avery	No	ENABLED	2015-12-20 15:07:07 Never 2015-12-20 15:07:07
bob	Bob	Brown	Yes	ENABLED	2015-12-20 15:07:20 Never 2015-12-20 15:07:20
joe	Joe	Johnson	No	ENABLED	2015-12-20 15:07:31 Never 2015-12-20 15:07:31

Figure 2.15 User Accounts

The User Accounts page shown in *Figure 2.15* shows the main panel of the web interface. The main panel will change depending on what part of the system you are looking at. Many pages provide a table in the main panel such as that seen in *Figure 2.15*.

The main panel is where all configuration information is displayed. In *Figure 2.15* we can see that this device has four users configured. We can also see the status of each user account and details about the users.

Actions can be performed from the main panel. Each page has different buttons to perform actions specific to that page. You will notice that the User Accounts page has an **Add User** button above the table. There are also action buttons specific to each user in the table. Selecting any of these buttons will cause the associated action to be performed.

Select **Add User** to display the user form on the right side of the page (see *Figure 2.16*). The right side of the page is where all configuration forms are shown.

Username	First Name	Last Name	Admin	Account State	Creation Date	Last Login	Password Changed	Options
admin			Yes	ENABLED	2013-11-26 08:23:20	2013-11-26 12:38:27		<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
					2013-11-26 08:23:20			
alice	Alice	Avery	No	ENABLED	2013-11-26 12:39:44	Never	2013-11-26 12:39:44	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
					2013-11-26 12:39:44			
bob	Bob	Brown	No	ENABLED	2013-11-26 12:40:03	Never	2013-11-26 12:40:03	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
					2013-11-26 12:40:03			
joe	Joe	Johnson	No	ENABLED	2013-11-26 12:40:57	Never	2013-11-26 12:40:57	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
					2013-11-26 12:40:57			

Add User

Username:

First Name: Last Name:

New Password: Retype New Password:

Title: Division:

Employee Identification:

Address:

City: State:

Country: Postal Code:

Work Phone: Mobile Phone:

Email:

Admin: Enabled:

*required

Figure 2.16 Add User

Detailed information about each of the webpages and their settings is provided in *Section 5: Settings and Commands*.

The Device Dashboard

The device dashboard is the page that is displayed when a user logs in to the device. The dashboard provides a quick overview of the state of the device. To access the dashboard from another device webpage, select **Dashboard** on the left navigation panel.



Figure 2.17 Device Dashboard

The device dashboard is divided into the following seven categories:

- Network Interfaces
- Serial Ports
- System Statistics
- LED Indicators
- Connection Status
- Version Information
- Resource Usage
- Logs By Severity

Network Interfaces

The Network Interfaces section of the dashboard contains icons representing each physical Ethernet network interface on the device. You may mouse over any of the network interface port icons to see the current alias and status information of the port. More information about network interface configuration can be found in *Section 5: Settings and Commands*.

**Figure 2.18 Network Interfaces**

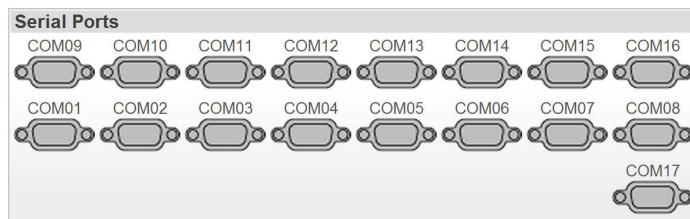
The network interface icons are color-coded to indicate the configuration state of that interface. The interface icon colors and their meanings can be found in *Table 2.1*.

Table 2.1 Network Interface Icon Colors

Interface	Status
(Green)	Enabled (configured)
(Blue)	Enabled (not configured)
(White)	Disabled (configured)
(Gray)	Disabled (not configured)

Serial Ports

The Serial Ports section of the dashboard contains icons representing each physical serial DB-9 interface on the device. You may mouse over any of the serial port icons to see the current alias and status information of the port. More information about serial port configuration can be found in *Section 5: Settings and Commands*.

**Figure 2.19 Serial Ports**

The serial ports are color-coded to indicate the configuration state of that interface. The interface icon colors and their meanings can be found in *Table 2.2*.

Table 2.2 Serial Port Icon Colors

Interface	Status
(Green)	Enabled (configured)
(Gray)	Disabled (not configured)

System Statistics

The System Statistics area (*Figure 2.20*) of the dashboard provides some basic statistics of the device operations. This information can quickly help determine the health of the device, and that it is being used properly.

System Statistics	
IPsec Connections:	0
MACsec Connections:	3
Web Users:	1
Uptime:	0y 0d 1h 57m 40s
Hours:	61489
Power Cycles:	437
<hr/>	
# of Firewall Rules:	0
<hr/>	
Syslog Statistics	
# Messages:	177
# Unacknowledged:	177
Oldest Unacknowledged:	0 days

Figure 2.20 System Statistics

Table 2.3 explains the meaning of each of these statistics.

Table 2.3 System Statistics

Statistic	Meaning
IPsec Connections (SEL-3620 and SEL-3622 only)	Number of configured IPsec VPN connections
MACsec Connections (SEL-3620 and SEL-3622 only)	Number of configured MACsec connections.
Web Users	Number of users currently connected to the web management interface.
Uptime	Length of time the device has been operating without a power cycle.
Hours	Total number of hours the device has been turned on since leaving the factory.
Power Cycles	Number of times the device has gone through the boot-up process since leaving the factory.
# of Firewall Rules (SEL-3620 and SEL-3622 only)	Number of configured firewall rules.
# Messages	Number of Syslog messages currently stored on the device.
# Unacknowledged	Number of Syslog messages that a user has not acknowledged.
Oldest Unacknowledged	Length of time the oldest unacknowledged Syslog message has been on the system.

LED Indicators

The LED indicators and their states are mirrors of the physical LED indicators found on the device front panel. Explanations for the indicators can be found in *Section 8: Testing and Troubleshooting*.

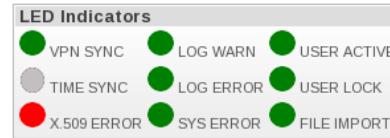


Figure 2.21 SEL-3610/SEL-3620 LED Indicators

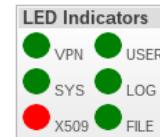


Figure 2.22 SEL-3622 LED Indicators

Ethernet Connections

The Ethernet Connections and IPsec Connections (IPsec and MACsec Connections only on the SEL-3620 and the SEL-3622) section of the dashboard provides statistics for the physical Ethernet network interfaces and configured IPsec connections of the device. Each Ethernet interface and configured IPsec connection are listed by name, with the current state (UP/DOWN), and amount of traffic passed in and out of the respective interface or connection.

Ethernet Connections			
Alias	State	In	Out
Eth F	NO-CARRIER	18229339 Bytes	0 Bytes
Eth 1	UP	74914837 Bytes	3502530 Bytes
Eth 2	UP	656373526 Bytes	3217441 Bytes
USB B	NO-CARRIER	412493 Bytes	1892485 Bytes

IPsec Connections			
Alias	State	In	Out

MACsec Connections			
Alias	State	In	Out
CA-1	DOWN	0 Bytes	0 Bytes

Figure 2.23 Connection Status

Version Information

This section of the dashboard provides Version Information, including serial number, firmware version, and the firmware identification string. This information can be useful when factory support or firmware upgrades are necessary.

Version Information	
Serial Number:	1130020553
Version:	R208
FID String:	SEL-3620-R208-V3-Z014006-D20210426
MOT String:	3620XHA2XXX0

Figure 2.24 Version Information

Resource Usage

Device Resource Usage provides a visual indication of CPU, RAM, and disk resource utilization. Any potential problems related to system resource utilization would be noticeable through this indicator on the dashboard.

NOTE: The resource utilization meters display a 10 second running average when the page loads. It is common to see CPU or RAM pegged at 100 percent for a short period of time after commissioning and when configuration changes are made.

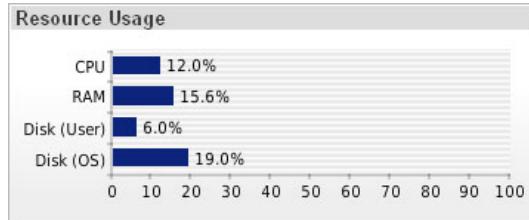


Figure 2.25 Resource Usage

Logs by Severity

The Logs by Severity pie chart provides a visual categorization of the system logs based on severity. From the dashboard, users can quickly view the quantity and severity of system logs. System logs are viewable by navigating to the Reports/ System Logs page. For more information on system logs and their severity levels, see *Section 5: Settings and Commands* and *Appendix F: Syslog*.

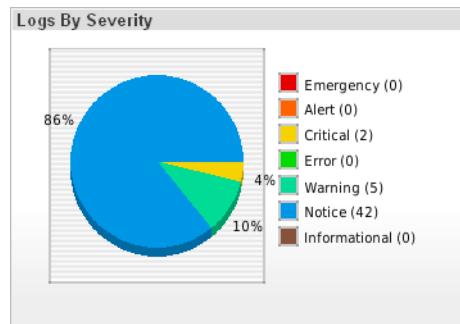


Figure 2.26 Logs by Severity

S E C T I O N 3

Managing Users

Introduction

This section describes the user account management features of the SEL-3610, SEL-3620, and the SEL-3622. Unless otherwise noted, references to the SEL-3620 refer also to the SEL-3622.

This section includes the following:

- *User-Based Accounts* on page 3.1
- *Adding a User* on page 3.4
- *Editing a User and Resetting a Password* on page 3.5
- *Removing a User* on page 3.6
- *Enabling or Disabling a User* on page 3.6
- *Changing a User Password* on page 3.7
- *Local Groups* on page 3.7
- *Centralized User Accounts With LDAP* on page 3.8
- *Using RADIUS* on page 3.15

User-Based Accounts

The device has user-based access control to provide for greater authentication, authorization, and accountability. Individuals responsible for configuring, monitoring, or maintaining the device will have their own unique user accounts. User-based access controls are organized to answer, “Who did what and when?”, and allow flexibility for detailed auditing. This structure also eases the burden of password management for the operators by only requiring each user to remember their own personal password. This eliminates the need for each operator to remember a new password every time an employee leaves or no longer needs access as required in a global account structure.

Operators with administrative privileges are authorized to create, delete, or modify accounts. Changes to accounts are logged and linked to the username of who altered it. Accounts include first name, last name, username, title, division, employee identification, address, phone numbers, and email. An administrator can disable each user account to help control temporary access or strengthen security when employees are on extended leave.

The device presents you with different views of the User Accounts page depending on your account type. An administrative user will see a list of all currently installed user accounts. This list is presented in alphabetical order of the Username (see *Figure 3.1*). The account list shows an account’s username, first name,

last name, privilege level, state, and dates associated with account creation, last login, and last password change. As many as 256 local user accounts can be configured on the device.

USER ACCOUNTS					
Add User					
Username	First Name	Last Name	Admin	Account State	Creation Date Last Login Password Changed
alice	Alice	Allen	No	ENABLED	2011-06-13 17:22:37 Never 2011-06-13 17:22:37
bob	Bob	Brown	No	DISABLED	2011-06-13 17:23:40 Never 2011-06-13 17:23:40
charlie	Charles	Clark	No	ENABLED	2011-06-13 17:24:17 Never 2011-06-13 17:24:17
sub1a_admin	Substation_#1A	Administrator	Yes	ENABLED	2011-06-13 17:25:09 2011-06-13 17:41:51 2011-06-13 17:25:09

Figure 3.1 User Accounts

There are five actions an administrator can perform on this page: update user, enable user, disable user, delete user, and add user. The update, enable, disable, and delete functions are performed with the buttons associated with each individual account. The add user function can be accessed with the **Add User** button above the account list.

The update function allows an administrator to change any or all settings associated with a particular account, including the password. The update function is required to reset a forgotten password.

The **Enable/Disable** button will change depending on if the account is currently enabled or disabled. Use this feature to disable the account of a user who temporarily does not need to access this device. This will prevent the device from being accessed by someone who does not need access. When they return, reenable their account to restore their access.

If a user will not ever again need access to this device, remove their account from the system with the **Delete** button. This will prevent any unauthorized access with that person's credentials.

During commissioning of the device, an administrative-level account was configured. The device allows two different roles to be assigned to users: administrative and nonadministrative. To view, add, edit, enable, disable, or delete users from the device, one must be logged in with administrative privileges.

All configuration changes to system users are logged.

Administrative Accounts

The device has support for two user roles: administrative and nonadministrative. A user with administrative privileges has all the privileges of a nonadministrative user with some additions. These additions include the ability to manage all user accounts, manage the date and time settings of the device, update the firmware on the device, and perform certain diagnostics commands. See *Table 3.1* for more information.

Table 3.1 Administrative Accounts Features/Roles

Feature/Role	Administrator	Technician
Modify Date/Time Settings	Yes	No
Modify Current Date/Time	Yes	No
Modify Device Usage Policy	Yes	No
Manage Firmware	Yes	No
Import/Export System Settings Files	Yes	No
Single File Backup/Restore	Yes	No
Upload a Connection Directory	Yes	Yes
Modify Physical Sensor Settings	Yes	No
Initiate Factory-Default Reset	Yes	No
Modify Local User Accounts	Yes	No
Change Local Account Password	Any	Own
Modify LDAP Settings	Yes	No
Modify RADIUS Settings	Yes	No
Modify Local Group Settings	Yes	No
Modify Network Settings	Yes	Yes
Modify Static Routes	Yes	Yes
Modify Firewall Rules	Yes	Yes
Modify NAT Functions	Yes	Yes
Modify Host/IP Mappings	Yes	No
Modify Syslog Settings	Yes	No
Modify SNMP Settings	Yes	Yes
Modify Serial Ports Settings	Yes	Yes
Modify Port Mappings	Yes	Yes
Modify X.509 Certificate Settings	Yes	Yes
Modify IPsec Settings	Yes	Yes
Modify MACsec Settings	Yes	Yes
Modify Allowed Client Settings	Yes	Yes
Modify SSH Host Keys	Yes	No
Perform IED Password Management	Yes	No
View Managed IED Passwords	Yes	No
Acknowledge System Logs	Yes	Yes
Reboot System	Yes	Yes
Update Diagnostics	Yes	Yes
Generate/View Proxy Reports	Yes	No
Halt System	Yes	No

Adding a User

The device supports as many as 256 unique local user accounts. Use the following steps to create a new user account.

- Step 1. Log in to the device with an account that has administrative privileges. The account that was created during the commissioning step is one such account.
- Step 2. Select **Accounts** from the left frame of the webpage. This link will open the device User Accounts page. From here, an administrative user can view, add, edit, enable, disable, or delete other users.
- Step 3. Select **Add User** to show the Add User Form (see *Figure 3.2*).
- Step 4. Enter the username and password of the new user along with your current password. You will need to enter the new user's password twice to confirm that it is correct. These are the required fields on this form.
- Step 5. Enter any optional information as desired.

NOTE: Usernames are unique on the device. The same username cannot be used for multiple accounts. Once a username is assigned, no other account may be created with that username unless the existing account is deleted. Usernames are case sensitive.

NOTE: The device requires that complex passwords are used. Passwords must be at least 8 characters in length and require at least one character from each of the character sets listed below. Spaces are allowed.

- Lowercase letters
- Uppercase letters
- Numbers
- Special characters (any printable character that is not alphanumeric)

It is recommended that a new user change their password on their first login to the system. This will ensure that they are the only person to know their password, and will protect them from other users accessing their account.

Passwords should never be shared or written down. The effectiveness of any password relies on only one person knowing that password.

NOTE: Boxes on the User Form that are marked by * are required. All other boxes are optional.

Figure 3.2 Add User Form

- Step 6. If the new user is to have administrative privileges, select the **Admin** check box. Otherwise leave the **Admin** check box empty.
- Step 7. Select **Submit**. This adds the new user to the device. If your current password was not entered correctly then the new user will not be added.

Editing a User and Resetting a Password

The device provides an administrative user with the ability to edit account information for existing accounts. This is to maintain records and contact information when employee information changes or mistakes are found. It also serves as a function to reset forgotten passwords. Use the following steps to edit account information or to reset an account's password.

- Step 1. Log in to the device with an account that has administrative privileges. The account that was created during the commissioning step is one such account.
- Step 2. Select **Accounts** from the left frame of the webpage. This link will open the device User Accounts page. From here, an administrative user can view, add, edit, enable, disable or delete other users.
- Step 3. Select the **Update** button associated with the account that you want to edit. This opens the Update User form (see *Figure 3.3*).

Figure 3.3 Update User Form

NOTE: If a user forgets their password, a user with administrative privileges must log in to the device and use the edit user feature to reset their password. The first time a user logs in after a password reset, it is recommended that they change their password. This will ensure that they are the only person to know their password, and will protect them from other users accessing their account.

- Step 4. If you want to change user information, edit the appropriate box in the upper section of the form.
- Step 5. Once all edits are completed, select **Update**. If you want to change the user's password, enter your current password followed by the new password into the lower section of the form and select **Change Password**. You will need to enter the new password a second time to confirm it was typed correctly. The password change attempt will fail if your current password verification fails or if the new password is not correctly confirmed.

Removing a User

In the case where an employee leaves the company, their account should be removed to prevent security breaches. The device allows for the easy removal of user accounts. Follow these steps to remove an account.

- Step 1. Log in to the device with an account that has administrative privileges. The account that was created during the commissioning step is one such account.
- Step 2. Select **Accounts** from the left frame of the webpage. This link opens the device User Accounts page. From here, an administrative user can view, add, edit, enable, disable, or delete other users.
- Step 3. Select the **Delete** button associated with the account that you want to remove. Enter your password when the prompt appears. Once you enter your password the Confirm Deletion page opens as shown in *Figure 3.4*.



Figure 3.4 Confirm Deletion

- Step 4. Verify that the user to be deleted is the correct user.
- Step 5. Once verified, select **Delete**. If this is not the correct user, select **Cancel** to go back to the User Accounts page.

Enabling or Disabling a User

In the case where an employee may take an extended leave of absence or a temporary change in duties, their account should be disabled to prevent unauthorized access to the device. This will maintain their account information while preventing unauthorized access to the system in their absence. Their account can be reactivated when they resume their normal duties. Use the following steps to enable or disable a user's account.

- Step 1. Log in to the device with an account that has administrative privileges. The account that was created during the commissioning step is one such account.
- Step 2. Select **Accounts** from the left frame of the webpage. This link opens the device User Accounts page. From here, an administrative user can view, add, edit, enable, disable, or delete other users.
- Step 3. Select the **Enable** button associated with the account to be enabled, or select the **Disable** button associated with the account to be disabled. If an account is currently enabled, only the **Disable** button will show. If an account is currently disabled, then only the **Enable** button will show.
Enter your password when the prompt appears to enable or disable a user.

Changing a User Password

Many organizations have policies requiring employees to change their system passwords at regular intervals. To aid with these policies, a user on the device can change their own password. Use the following steps to change your password.

Step 1. Log in to the device.

Step 2. Select **Accounts** from the left frame of the webpage. This link opens the device User Accounts page. From here, a nonadministrative user can change their password. Nonadministrative users will only be able to see their own user information and the Change Password form.

The screenshot shows a 'Change Password' form with a blue header. It contains three input fields: 'Your Current Password*' (with a red asterisk), 'New Password*' (with a red asterisk), and 'Retype New Password*' (with a red asterisk). Below the fields is a note 'required'. At the bottom is a 'Change Password' button.

Figure 3.5 Change Password

Step 3. Enter your current password, then enter the new password twice. Select **Submit** to change your password.

Local Groups

The SEL-3620 has a Local Groups page to sort users into groups whose members have the same privileges. These groups and privileges are relevant for the proxy services of the device, meaning these groups help categorize who can perform which activities on the SEL-3620 managed devices. The Local Group Names must exactly match the Local Group names that are configured in QuickSet.

Privileges on the SEL-3620 web interface are not determined by the Local Groups. They are determined via the Administrative Privileges check box associated with each individual user on the Accounts page.

To create a new group, access the Local Groups page by selecting the **Local Groups** link from the navigation panel. From the Local Groups page, select **Add Local Group** at the top of the page. This shows a form on the right side of the page for creating a new local group. Provide the new group with a name and select the local users that should be part of this group. The name must be the same as a group name configured in QuickSet.

The screenshot shows a modal window titled "Add Local Group". Inside, there is a text input field labeled "Alias*" with the value "Technicians". Below this is a list box titled "Local Users*:" containing four entries: "root", "alfred", "bruce", and "calvin". The checkbox next to "bruce" is checked. At the bottom right of the modal is a "Submit" button.

Figure 3.6 Add Local Group Form

In the list of local groups, select the arrow next to the name of each group to view or hide the members of that group. Select the **Update** button associated with a local group to add or remove group members or to change the group Alias. Select the **Delete** button associated with a local group to delete that local group. Select the **Delete** button associated with a member of the local group to quickly remove that user from the group.

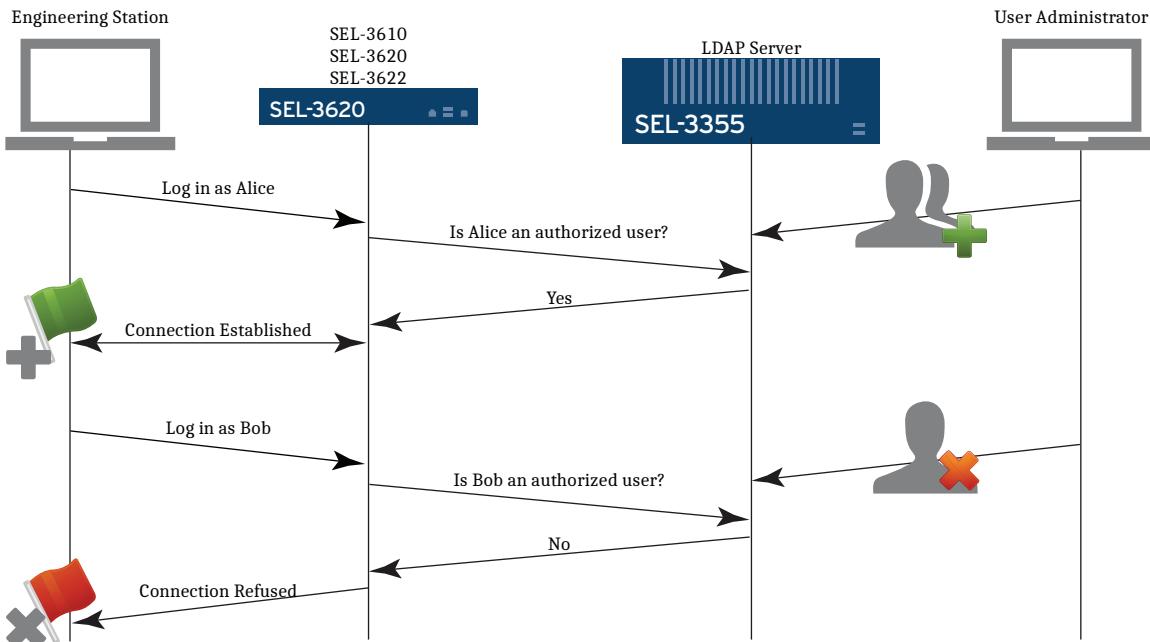
Local Groups		Options
	Alias	
▼	Technicians	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	bruce	<input type="button" value="Delete"/>
	calvin	<input type="button" value="Delete"/>
▶	Engineers	<input type="button" value="Update"/> <input type="button" value="Delete"/>

Figure 3.7 Local Group List

Centralized User Accounts With LDAP

Lightweight Directory Access Protocol (LDAP) is used by many IT departments to manage the users and devices on their corporate networks. LDAP is a powerful and flexible protocol that allows for fast information lookups from servers that are optimized for read access. The information stored on LDAP servers can be any type of record based information that is stored in a directory structure, such as user and device lists, phone books, and recipes.

LDAP is included in the device to provide a mechanism for centralized user management. With LDAP, users can be managed at a central server. When a user who does not have a local account requests access to the device, the device will poll the central directory to verify that they are authorized to access the unit, see *Figure 3.8*.

**Figure 3.8 LDAP Login Process**

To support this behavior, certain parameters must be configured in the device to allow it to communicate with your LDAP server. All of these parameters are configurable through the web interface of the device. To configure LDAP on your device, access the web interface of the device and log in by using an account with administrative privileges.

NOTE: As of firmware version R210, the SEL-3620 no longer supports TLSv1.1 authentication. Ensure that the CAS supports TLSv1.2 or TLSv1.3 authentication.

NOTE: This device is not compatible with LDAP deployments that permit commas in usernames.

The device has been tested to bind with the following LDAP servers in supported configurations:

- Active Directory Domain Services on Windows Server 2008 and Server 2012 Standard/Enterprise
- CentOS Directory Server 8.1 on CentOS 5.5-5.6

SEL cannot guarantee that the device will be compatible with all possible LDAP server architectures and implementations. Commissioning and configuration of an LDAP server typically requires advanced knowledge of certificate authority hierarchies and centralized user group configurations. It is important that an organization's LDAP server administrators be involved during the design and implementation process to ensure that the device will be compatible with your organization's specific trust management infrastructure.

Hosts

The device needs to know the name and IP address of your LDAP server to know how to contact it. Select **Hosts** from the navigation panel on your webpage to view and edit the **Hosts** settings, see *Figure 3.9*.

Hosts		
<input type="button" value="Add Host"/>		
Hostname	IP Address	Options
terrier.rdttest.local	10.203.42.253	<input type="button" value="Delete"/>

Figure 3.9 Host Settings

The Host Settings page provides a method to statically map IP addresses with external device hostnames such as your LDAP servers. To map an IP address to a hostname, select **Add Host**. This will show the Add Host form on the right side of the page, see *Figure 3.10*.

The screenshot shows a modal dialog titled "Add Host". It contains two input fields: "Hostname*" with the value "terrier.rdttest.local" and "IP Address*" with the value "10.203.42.253". Below the fields are two labels: "*required" and a "Submit" button.

Figure 3.10 Add Host

Populate the Add Host form with the correct hostname and IP address of an LDAP server. The device supports as many as 64 hosts. For your convenience, we have included a form for your LDAP administrators to complete in *Appendix L: Lightweight Directory Access Protocol*. Have your LDAP Administrators complete the form and map the information they provide into the Host Settings of the device.

LDAP Certificates

The LDAP client of the device uses STARTTLS with X.509 certificates for securing LDAP connections. This is to ensure that attackers are not spoofing the authentication server to gain unauthorized access. The device requires that all CA certificates of the certificate chain of the LDAP server are stored locally.

LDAP Settings

Now that your device knows who and where your LDAP servers are, we can configure the device to access those servers. Select the LDAP Settings link from the navigation panel on your webpage to view the LDAP parameters, see *Figure 3.11*.

LDAP SETTINGS

Modify LDAP Settings			
LDAP Enabled	User ID Attribute		
Yes	(sAMAccountName=(USERNAME))		
Group Member Attribute	Server Synchronization Interval		
memberOf	8		
Search Base	DC=rdtest,DC=local		
Bind DN	CN=ldap_bind,CN=Users,DC=rdtest,DC=local		
Add LDAP Server			
Priority	LDAP Server Hostname	Port	Options
1	terrier.rdstest.local	389	<input type="button" value="Update"/> <input type="button" value="Delete"/>
Modify Attribute Mappings			
Local Attribute	LDAP Attribute		
First Name	givenName		
Last Name	sn		
Email	email		
Work Phone	telephoneNumber		
Add Group Mapping			
Device Role	DN	Options	
Administrator	CN=Domain Admins,CN=Users,DC=rdtest,DC=local	<input type="button" value="Delete"/>	
Technician	CN=Domain Users,CN=Users,DC=rdtest,DC=local	<input type="button" value="Delete"/>	

Figure 3.11 LDAP Settings

Figure 3.11 shows the LDAP Settings page and all the options for communicating with your LDAP servers. To simplify configuration, we have included a form for your LDAP administrators to complete, which you can use to populate all the LDAP boxes. This form is located in *Appendix L: Lightweight Directory Access Protocol*.

To modify the LDAP settings select **Modify LDAP Settings** located at the top of the main page. This will show the Edit LDAP Settings form on the right side of the page, see *Figure 3.12*.

The screenshot shows a configuration interface titled "Modify LDAP Settings". It includes the following fields:

- LDAP Enabled
- Search Base:
- User ID Attr.:
- Group Member Attr.:
- Synchronization Interval: 1-24 Hours (Zero is every request)
- Bind DN:
- Submit button
- Bind DN Password Options section with Password and Confirm Password fields, and a Change Bind Password button.
- Note: "NOTE: When password is not set anonymous binding will be performed."

Figure 3.12 Edit LDAP Settings

The LDAP Search Base can be thought of as the root directory to begin your user search from. It is formed by listing all the components of the search base separated by commas going from the most specific component to the broadest component. In the figure above, the Search Base is configured as “DC=centralauth,DC=local.” In this search base, DC refers to domain component. The domain components are later combined with “.” to create the search domain. In this case the search domain is centralauth.local. This search base can be interpreted to mean “search the directory residing on an LDAP server in the centralauth.local domain.”

NOTE: The broader your search base, the more users/groups may be able to access the device. Be aware that broader search bases can take significantly more time to search than search bases that specify organizational units or groups.

NOTE: Bind DN strings with escaped characters, commas, and spaces are not allowed.

One other common LDAP component is CN. The component CN is short for “common name.” It is a name that refers to a specific object that may or may not be unique. Examples of CNs are groups and usernames.

The User ID and Group Member attributes are the LDAP labels that identify the usernames and groups of users of the system. If these are not correctly entered, the device will not be able to determine which LDAP boxes to search for usernames or privileges. The User ID should be configured similar to **(sAMAccountName={USERNAME})** or **(uid={USERNAME})**. In these examples, “sAMAccountName” or “uid” is the name of the attribute on the directory server that identifies the owner of a user account. The {USERNAME} portion of the User ID is the variable that holds the username of the person attempting to log in to the device. For example, if the User ID were configured as **(sAMAccountName={USERNAME})**, and a person with the username **jsmith** were to attempt to log in to the device, then the device would search the LDAP directory for an entry with an sAMAccountName attribute that contained a value of “jsmith.” This box is extendable, so you can search for entries matching multiple criteria. For example, the search box “**(&(sAMAccountName={USERNAME})(memberOf=cn=activeusers,dc=your,dc=domain))**” would only allow access to users with a valid username who are members of the **activeusers** group of your domain.

The synchronization interval setting exists to reduce the overhead associated with pulling account information from an LDAP server. The device locally caches the credentials and privileges of centralized users for the period of time configured. The synchronization interval is settable from 0 to 24 hours. If the synchronization interval is set to 0, then the device will resynchronize on every login. The synchronization interval exists to speed up the login process. The SEL-3620 will continue to verify the authenticity of users against the central directory even if their privilege information is locally cached.

The device supports both authenticated and anonymous binds to your LDAP servers. Authenticated binds use a service account to access the LDAP server. If the service account is revoked, or the password expires, the device will not be able to access the LDAP server, and centralized users will be unable to access the device. Anonymous binds forgo the use of service accounts. Find out from your LDAP administrators which method is preferred for your system.

If you use a service account for LDAP binds, you will need to supply the service account username in the Bind DN box, and you will need to supply the password in the Bind DN Password Options boxes. The password information must be separately set or changed by using the **Change Bind Password** button on the Modify LDAP Settings form.

Obtain the necessary configuration information from your LDAP administrators, and input the settings. For your convenience, we have included a form for your LDAP administrators to complete in *Appendix L: Lightweight Directory Access Protocol*. Have your LDAP administrators complete the form and map the information they provide into the LDAP settings of the device.

LDAP Server

To improve availability when the primary LDAP server may be inaccessible, the device supports accessing a secondary LDAP server. To add an LDAP server select **Add LDAP Server**. This will show the Add LDAP Server form on the right side of the page, see *Figure 3.13*.

Add LDAP Server	
Hostname*	terrier.rdttest.local
Port*	389
*required	
<input type="button" value="Submit"/>	

Figure 3.13 Add LDAP Server

LDAP servers are identified by their hostname and port numbers. Use **Port 389** unless a different port number is specified by your LDAP administrator. This information should be obtained from your LDAP Administrators by using the form found in *Appendix L: Lightweight Directory Access Protocol*.

The device allows for two LDAP servers to be configured for redundancy and increased reliability. LDAP servers are assigned a priority and will be queried in their order of priority until the user accessing the device is found, or the list has been exhausted.

Attribute Mappings

The device can pull user attributes from your LDAP server and store those attributes on the local machine. To map your LDAP attributes to device attributes, select **Modify Attribute Mappings**. This will show the Edit Attribute Mappings form on the right side of the page, see *Figure 3.14*.

First Name:	givenName
Last Name:	sn
Email:	mail
Work Phone:	telephoneNumber
Submit	

Figure 3.14 Edit Attribute Mapping

The box labels in the Edit Attribute Mappings form are the titles for the device attributes. To map LDAP attributes to these local attributes, enter the appropriate LDAP attributes into the text boxes. These settings are optional. This information should be obtained from your LDAP Administrators by using the form found in *Appendix L: Lightweight Directory Access Protocol*.

Group Mappings

The device has specific device roles that can be mapped to LDAP group memberships. Select **Add Group Mapping** to configure a new group mapping. This will expand a table that shows all the LDAP groups the device can access, based upon your search base, see *Figure 3.15*.

Device Role	DN	Options
Administrator	CN=Domain Admins,CN=Users,DC=rdtest,DC=local	<input type="button" value="Delete"/>
Technician	CN=Domain Users,CN=Users,DC=rdtest,DC=local	<input type="button" value="Delete"/>

Technician

- ▼ OU=SubA,OU=Control_Systems,DC=rdtest,DC=local
 - ▶ OU=Devices,OU=SubA,OU=Control_Systems,DC=rdtest,DC=local
 - ▶ OU=Groups,OU=SubA,OU=Control_Systems,DC=rdtest,DC=local
 - ▶ OU=Users,OU=SubA,OU=Control_Systems,DC=rdtest,DC=local
 - ▶ OU=SubB,OU=Control_Systems,DC=rdtest,DC=local
- ▶ OU=Corporate,DC=rdtest,DC=local
- ▶ OU=Domain Controllers,DC=rdtest,DC=local
- ▶ CN=ForeignSecurityPrincipals,DC=rdtest,DC=local
- ▶ OU=Global,DC=rdtest,DC=local

Figure 3.15 Group Mappings

To configure a group mapping, select the device user type from the dropdown list on the left, and navigate through the tree to the user or group that should be given the role's privileges. Select the user or group and select **Add** to create the mapping. Your server administrator may need to create new groups and assign members appropriate for these mappings. Work with your LDAP administrator to determine group mappings by using the form found in *Appendix L: Lightweight Directory Access Protocol*.

The device distills search results coming back from the LDAP server by using the following filter:

```
(!(objectClass=organizationalUnit)
(objectClass=container)
(objectClass=group))
```

(objectClass=groupOfNames)
(objectClass=groupOfUniqueNames)
(objectClass=posixGroup))

Note that if you have a group container without one of these object class attributes, it will not be shown in the group mappings window. In that case, you can still add the DN of the object manually.

Using RADIUS

About RADIUS

The name of the Remote Authentication Dial-In User Service (RADIUS) reflects its origins as a technology for handling login requests from modem banks used for dial-up access to computer systems. The RADIUS protocol is designed to be a simple, high-performance way to allow a computer system or device to delegate the job of user authentication. RADIUS allows a system that needs to authenticate a user to give the user's credentials to a central authority for processing and receive either an access grant or an access deny. The connection between the requester and the RADIUS server is protected by encryption built into the RADIUS protocol.

Some organizations already use RADIUS for user authentication, so providing centralized access control to SCADA devices by using RADIUS with the device is a natural choice. SEL has application guides that provide step-by-step instructions to help you configure the following RADIUS servers:

- FreeRADIUS 2.0+ (open source at <http://freeradius.org>)
- RSA Authentication Manager
- Cisco Secure ACS
- Cisco Secure ISE
- Microsoft Windows NPS

Prerequisites

Centralized User Accounts

To enforce distinct centrally managed privileges for RADIUS user authentication, user accounts must normally belong to security groups in your enterprise directory (e.g., Active Directory) that can be mapped to the different user roles supported by the device, or for different user roles for the SEL-3620 Authentication Proxy that are managed by QuickSet. The RADIUS server receives group membership information for an authenticating user and uses this information to determine the user's role when logging onto the device or into the Authentication Proxy. The user role for logging onto the device is returned to the client in the SEL-User-Role attribute. The user role for the Authentication Proxy is returned in the SEL-Proxy-Group attribute.

It is also possible to use the RADIUS server with accounts and privilege information in a local configuration file maintained on the RADIUS server, but this is not the usual practice for reasons of security and scalability.

User Roles for Login

Two levels of privilege for logging onto the device are supported: Administrator and Technician. An administrator has full administrative control privileges. Users with administrator privilege can read and write all settings and information on the device. A technician is granted limited control privileges. Users with technician privilege can read most settings and data, but can only write a limited subset of settings. In particular, a technician user cannot view or modify settings that affect user authentication (user accounts, LDAP, or RADIUS).

Configuring Your RADIUS Server

To use the device with your organization's RADIUS server, you need to configure the RADIUS server to include certain SEL Vendor Specific Attributes (VSAs) in the Access-Accept message returned when you successfully log in. These attributes are used to send information to the device about your role and proxy group. They are defined in the dictionary.sel file that you can download from the RADIUS configuration page on the device website. This file can also be found in *Appendix M: SEL RADIUS Dictionary*.

NOTE: As of firmware version R210, the SEL-3620 no longer supports TLSv1.1 authentication. Ensure that the CAS supports TLSv1.2 or TLSv1.3 authentication.

The RADIUS client implementation sends four RADIUS Attribute Value Pairs (AVP) when making an initial Access-Request to a remote RADIUS Server: User-Name (AVP Type 1), User-Password (AVP Type 2), Calling-Station-Id (AVP Type 31), and NAS-Identifier (AVP Type 32). The Calling-Station-Id attribute contains the IP address of the device connecting to the SEL-3620. This can be used for assigning permissions based upon the user's location. For example, the Calling-Station-Id attribute can be used to grant location-specific read or write permissions depending on whether the user is in the office or the substation. The NAS-Identifier attribute contains the fully qualified domain name (hostname and domain name) of the device (e.g., sel3620.central.home).

You will find more information about configuring particular RADIUS environments under the Publications tab on the device product page of the SEL website.

Configuring the Device as a RADIUS Client

Configuring the RADIUS client involves setting the network address information for one or two RADIUS servers, selecting a few options, choosing an authentication type, and setting the shared secret (i.e., password) used to encrypt the RADIUS protocol. *Figure 3.16* shows the RADIUS Settings page of the device.

You are required to set the primary server, authentication port, shared secret, and authentication type.

RADIUS SETTINGS

Enable RADIUS Authentication (Default is Off)
 Enable RADIUS Accounting (when RADIUS Authentication is On) (Default is On)

Primary Server Hostname/IP Address <input type="button" value="IP Address ▾"/> <small>Hosts can be added on the Hosts page</small>	IP Address <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Backup Server <input type="button" value="IP Address ▾"/> <small>Hosts can be added on the Hosts page</small>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Primary Server Authentication Port (UDP) <small>(Default is 1812)</small> <input type="text"/>	Accounting Port (UDP) <small>(Default is 1813)</small> <input type="text"/>
Backup Server <input type="text"/>	<input type="text"/>
All Servers RADIUS Shared Secret <input type="text"/>	Authentication Type <input type="button" value="PAP ▾"/>
All Servers Confirm Shared Secret <input type="text"/>	
All Servers Connection Timeout (in seconds) <input type="text" value="2"/>	
Advanced Options <hr/> <p> <input type="checkbox"/> Prevent Sending Unencrypted Username (Default is Off) <i>(Extensible Authentication Protocol (EAP) Only)</i> <input checked="" type="checkbox"/> Enable Interim RADIUS Accounting Updates (Syslog) (Default is On) <input checked="" type="checkbox"/> Verify Server Identity/Hostname (Default is On) </p>	
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> Download SEL RADIUS Dictionary <small>Download a file to your computer containing the SEL Vendor Specific Attribute (VSA) definitions for integration into the RADIUS server.</small> </div> <div style="border: 1px solid black; padding: 2px; background-color: #e0e0e0; display: inline-block;"> Download </div>	

Figure 3.16 RADIUS Settings**Table 3.2 Description of RADIUS Settings (Sheet 1 of 2)**

Setting Name	Description
Enable RADIUS Authentication	Configures the device to forward requests for authentication of users to your RADIUS server if the username is not found in the local accounts on the device.
Enable RADIUS Accounting	Configures the device to send information about the user's session to the RADIUS server for logging.
Primary Server	Network address for your RADIUS server, either as a hostname (in the hosts table), or as an IP address. Choose either IP Address, or select one of the Hosts listed. This server will receive all RADIUS requests unless it is offline (does not respond, timing out three times in a row).
Backup Server	A backup server switched to when the primary server is offline. The primary server will be tried again on the next request after five minutes have elapsed since it was found to be offline.
Authentication Port	UDP port number on the RADIUS server that listens for authentication requests. The default value is 1812.
Accounting Port	UDP port number on the RADIUS server that listens for accounting information messages. The default value is 1813.
RADIUS Shared Secret	A string of 1–128 characters that is set on both the RADIUS server and the SEL-3620 to provide cryptographic protection for the data in authentication requests and replies from the server. Normally, you will get this information from your RADIUS administrator. The RADIUS Shared Secret must be set to use RADIUS.
Authentication Type	Authentication Type describes how authentication data are encoded in the messages between the device and your RADIUS server. Normally, this value will be given to you by your RADIUS administrator. If yours is a new deployment, SEL recommends using one of the EAP values for better security. The default value is PAP. If you use an EAP protocol, you need to import onto the device the full CA certificate chain for the RADIUS server.

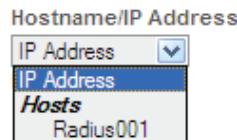
Table 3.2 Description of RADIUS Settings (Sheet 2 of 2)

Setting Name	Description
Connection Timeout	This value in seconds is set to exceed the longest time expected in which to receive a reply from the RADIUS server. The device switches to the backup RADIUS server after three times that the primary server does not reply to a request within the time-out interval. The default value is 2 seconds. The maximum value permitted is 10 seconds.
Prevent Sending Unencrypted Username	Select this box to hide usernames by using an anonymous username (anonymous) to send requests to the RADIUS server. When this is done, the actual username is sent in the encrypted portion of the message.
Enable Interim RADIUS Accounting Updates (Syslog)	Select this box if you want your RADIUS server to receive notifications.
Verify Server Identity/Hostname	Select this box if you want the device to verify that the subject name of the certificate of the RADIUS server matches the IP address or hostname that you use to connect to it.
Download SEL RADIUS Dictionary	The Download button, which is not actually a setting, lets you retrieve the RADIUS dictionary file from the device. This file defines the Schweitzer Engineering Labs (SEL) vendor-specific attributes that must be defined on your RADIUS server and that are used by your device to appropriately grant or restrict privileges for users.

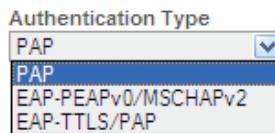
When a RADIUS server is defined using its hostname, the hostname and its IP address must be entered in the Hosts page by selecting **Network > Hosts** (see *Figure 3.17*).

**Figure 3.17 Adding a RADIUS Server on the Hosts Page**

Figure 3.18 shows how to select a RADIUS server through use of its hostname. In this example, the hostname Radius001 has been added to the Hosts page and is now available in the dropdown list for the Hostname/IP Address.

**Figure 3.18 Selecting a RADIUS Server by Hostname**

To configure your SEL-3620 or SEL-3622 to use your RADIUS server, you will need to configure the shared secret and the authentication type settings on your device to the same values used by your RADIUS server. Obtain these setting values from your RADIUS administrator. *Figure 3.19* shows the choices for Authentication Type.

**Figure 3.19 Selecting the RADIUS Authentication Type**

Your RADIUS server needs to know SEL-specific role and privilege attributes to be able to work with the SEL-3620 and SEL-3622. That information is found in the SEL RADIUS dictionary, which defines the vendor number for Schweitzer Engineering Labs (SEL), as well as identifiers for user attributes that are set using values from your Active Directory.

Pressing the **Download** button in the Download SEL RADIUS Dictionary area sends the SEL dictionary file to your browser as a file.

This page intentionally left blank

S E C T I O N 4

Job Done Examples

Introduction

This section contains Job Done examples for the SEL-3610, SEL-3620, and SEL-3622. Except as otherwise noted, references to the SEL-3620 refer also to the SEL-3622. All Job Done examples assume that the device has already been commissioned.

The following Job Done examples apply to all devices:

- *Job Done Example 1: Central User Access* on page 4.1
- *Job Done Example 2: Adding Ports to a Modbus Polling System* on page 4.7

The following Job Done example applies to the SEL-3622:

- *Job Done Example 3: Detect Physical Tampering* on page 4.11

The following Job Done examples apply to the SEL-3620 and the SEL-3622. The SEL-3620 and SEL-3622 are interchangeable in these examples:

- *Job Done Example 4: Secure DNP3 Serial-to-Ethernet Conversion Over a Cellular Network* on page 4.14
- *Job Done Example 5: Using IPSec to Secure Communication* on page 4.21
- *Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant* on page 4.26
- *Job Done Example 7: Using VLANs on the SEL-3620 With a Managed Ethernet Switch* on page 4.29
- *Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control* on page 4.33

Job Done Example 1: Central User Access

Manage Users and Collect Logs at a Central Location

As control systems become more complex and more individuals have access to sensitive systems, it is important to know who is performing what actions on the system to identify training opportunities and to hold individuals accountable for their actions. The device supports user-based accounts to make this possible. For ease of management, the devices support Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and Syslog for central management of users and collection of device logs.

Identifying the Problem

Your objective is to manage users for your whole system from one central LDAP server, and to collect event logs at a central Syslog collector. You already have the central servers configured and need to configure the device to communicate with those servers. The networking settings of the device have already been configured.

Figure 4.1 is a representation of the SEL-3610, the central server running both LDAP and Syslog services, and the communications path between the two devices.



Figure 4.1 Centralization Network

Defining the Solution

Two sets of configuration settings are necessary to complete this; the settings for LDAP and the settings for Syslog. *Table 4.1* defines the Syslog settings we will need. *Table 4.2* defines the LDAP settings we will need. The central server is already configured with its Syslog and LDAP settings. The server is running Microsoft Server 2008 with Active Directory.

Table 4.1 Job Done Syslog Settings

Setting Name	Setting Value
Alias	Syslog Collector
IP Address	172.24.49.8
Port	514
Minimum Threshold	Warning

The Syslog settings are all entered on the Syslog page of the device.

Table 4.2 Job Done LDAP Settings

Setting Name	Setting Value
Hostname	cc.app3620.selu.local
IP Address	172.24.49.8
Search Base	dc=app3620,dc=selu,dc=local
User ID Attribute	(sAMAccountName={USERNAME})
Group Member Attribute	memberOf
Bind DN	cn=ldap_bind,cn=Users,dc=app3620,dc=selu,dc=local
Bind DN Password	seluAPP-3620
Server Synchronization Interval	8
Port Number	389
Administrator Group	cn=administrators,cn=Groups,dc=app3620,dc=selu,dc=local
Technician Group	cn=technicians,cn=Groups,dc=app3620,dc=selu,dc=local

The public certificate of the private key used to sign the certificate of the LDAP server is also necessary. This certificate is required to authenticate and start LDAP encryption. The device requires encryption for LDAP communications.

The tasks that must be performed to complete this system are:

- *Configure Networking*
- *Add the Substation Syslog Server*
- *Add the X.509 Certificate Chain of the LDAP Server*
- *Add the Hostname and IP Address Mapping of the LDAP Server*
- *Configure the LDAP Settings*
- *Map LDAP Groups*

Configure Networking

NOTE: You may receive a certificate error from your browser. The message depends on the browser you use. This error appears because the certificate the device is presenting to your browser does not match the IP address assigned to your SEL device. You will need to create a certificate exception to access the SEL login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

If you are unable to connect to the SEL device, verify that your PC is configured to access the same subnet as the SEL device. Instructions for doing this can be found in Section 2: Installation.

- Step 1. Access your device with your preferred web browser by typing **https://192.168.1.2** into the address bar. This is the default IP address of the **ETH F** port. If a different IP address was assigned during commissioning, use that address instead. Enter your login credentials and select **Submit**.
- Step 2. Access the **Network Settings** page by selecting the **Network Settings** link from the navigation panel located on the left of the screen.
- Step 3. Select **Add Ethernet Address** on the top of the **Network Settings** page to show the **Add Network Address** form.
- Step 4. Complete the **Add Network Address** form as shown in *Figure 4.2*.

The screenshot shows the 'Add Network Address' dialog box. The 'Interface' dropdown is set to 'Eth 1'. The 'Enable DHCP' checkbox is unchecked. The 'Manual IP Address' field is set to 172.24.49.1. The 'VLAN' section has 'Native' selected. The 'Alias' field contains 'Trusted Net'. A note at the bottom says '*required'. At the bottom right is a 'Submit' button.

Figure 4.2 Add Trusted Network

- Step 5. Select the **Update** link underneath the Eth 1 Port icon as seen in *Figure 4.3* to show the Ethernet Interface Eth 1 Settings form.



Figure 4.3 Update Network Interface

- Step 6. Select the **Enabled** check box and select **Submit** to enable the interface.

4.4 Job Done Examples

Job Done Example 1: Central User Access

Add the Substation Syslog Server

- Step 1. Select the **Syslog** link from the navigation panel located on the left of the screen. This will open the **Syslog** configuration page.

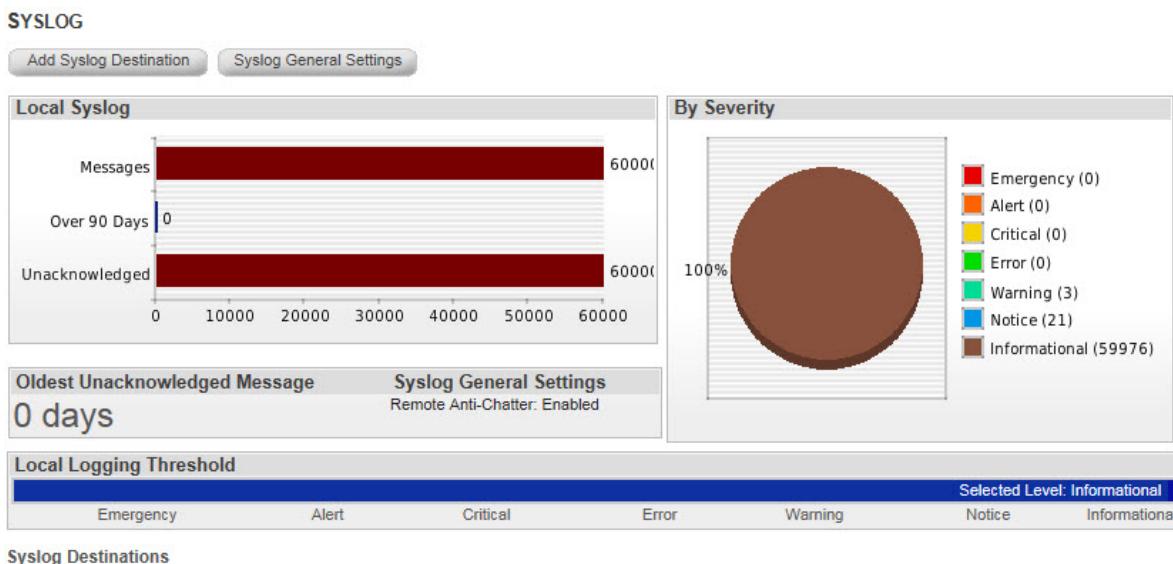


Figure 4.4 Syslog Configuration Page

NOTE: The Syslog server should be able to accept incoming messages without any additional configuration. If Syslog messages are not received, refer to your Syslog server documentation. See Appendix F: Syslog for the list of Syslog messages and the events that generate them.

- Step 2. Select **Add Syslog Destination** to show the **Syslog Destination** form on the right side of the page.
- Step 3. Complete the form as shown in *Figure 4.5* and select **Submit** to submit the changes. The proper settings can also be found in *Table 4.1*.

The 'Add Syslog Destination' form has fields for 'Destination', 'Alias*' (Syslog Collector), 'Description', 'IP Address*' (172.24.49.8), 'Port*' (514), 'Filters**', and a 'Submit' button. It includes checkboxes for 'Enable Advanced Filtering' and 'Minimum Severity Threshold Filter' (set to 'Notice'). Footnotes indicate '*required' and '**at least one filter required'.

Figure 4.5 Add Syslog Destination

Add the X.509 Certificate Chain of the LDAP Server

- Step 1. Obtain the public certificate of the root CA of the LDAP server from your LDAP administrator. This file must be in .pem format.
- Step 2. Navigate to the X.509 Certificates page by selecting the **X.509 Certificates** link from the navigation panel.

- Step 3. Select **Import** at the top of the page to show the Import X.509 Certificate form.
- Step 4. Select **Browse** and locate the public certificate of the root CA of the LDAP server.
- Step 5. Enter a descriptive name for the certificate in the **Name** box and select **Submit**. A password is not necessary for public certificates.

The dialog box has a title bar 'Import X.509 Certificate'. It contains fields for 'Certificate*' (with a 'Browse...' button), 'Name:' (containing 'CA'), and 'Password**' (with a note: '*required only if private certificate'). There is also a note '**required only if private certificate'. At the bottom is a 'Submit' button.

Figure 4.6 Import X.509 Certificate

Add the Hostname and IP Address Mapping of the LDAP Server

- Step 1. Select the **Add Hosts** button at the top of the page to show the Add Host form.
- Step 2. Populate the **Hostname** and **IP Address** boxes with the hostname and IP address of your LDAP server and select **Submit**.

The dialog box has a title bar 'Add Host'. It contains fields for 'Hostname*' (containing 'cc.app3620.selu.local') and 'IP Address*' (containing '172.24.49.8'). There is also a note '*required'. At the bottom is a 'Submit' button.

Figure 4.7 Add Host

Configure the LDAP Settings

- Step 1. Access the LDAP Settings page by selecting **LDAP Settings** from the navigation panel.
- Step 2. Select the **Modify LDAP Settings** button to show the Modify LDAP Settings form.
- Step 3. Enable LDAP and complete the form with the information found in *Table 4.2*. Be careful to not add any additional white space to the distinguished name strings.
- Step 4. Select the **Submit** button to save these settings.

Modify LDAP Settings

LDAP Enabled:

Search Base: dc=app3620,dc=selu,dc

User ID Attr.: sAMAccountName={US}

Group Member Attr.: memberOf

Synchronization Interval: 8
1-24 Hours (Zero is every request)

Bind DN: cn=ldap_bind,cn=Users,

Bind DN Password Options:

Password: (*****)

Confirm Password: (*****)

Submit

Figure 4.8 Modify LDAP Settings

- Step 5. Select the **Add LDAP Server** button to show the Add LDAP Server form.
- Step 6. Enter the **Hostname** and open **Port** of your LDAP server. The **Hostname** needs to match the hostname you entered on the Hosts page.
- Step 7. Select the **Submit** button to save these settings.

Add LDAP Server

Hostname*: cc.app3620.selu.local

Port*: 389

* required

Submit

Figure 4.9 Add LDAP Server

- Step 8. Modify the Attribute Mappings if desired. These settings are optional and will collect the relevant information about an accessing user if configured.

Map LDAP Groups

- Step 1. Select the **Add Group Mapping** button on the LDAP Settings page to map local user roles to central user groups. If a list appears at the bottom of the page with the structure of your directory server, then LDAP communications are working. If a red error message appears, then something is not configured correctly.
If a red error message appears, verify all your LDAP settings have been entered correctly, verify the X.509 certificates are valid, verify your system time is correct, and verify the SEL device has network connectivity to the LDAP server.
- Step 2. If you can see the directory structure, then browse through the directory by selecting the arrows to find the groups you want to map to user roles on the SEL device, or manually enter the distinguished name of the group in the text box.
- Step 3. Select the corresponding local **Device Role** from the dropdown list.

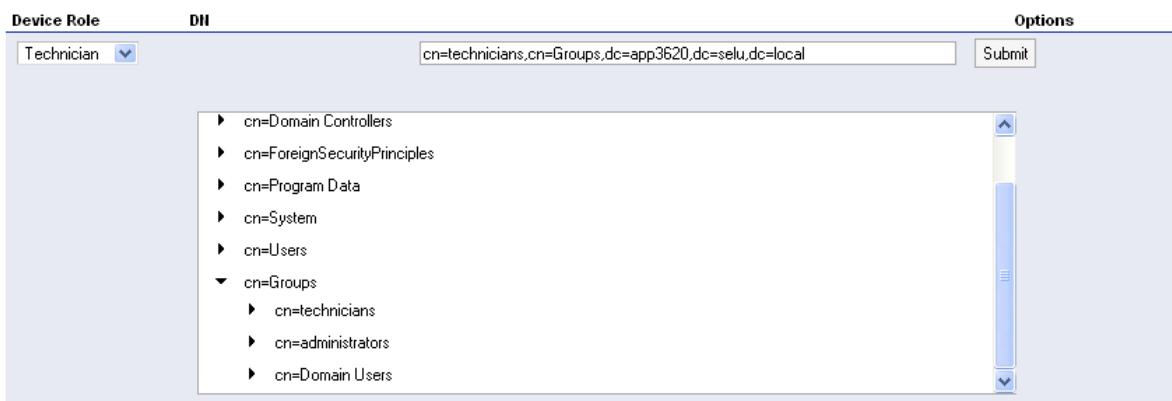


Figure 4.10 Add Group Mapping

Step 4. Select the **Submit** button to create this group mapping. You should now be able to log in to the SEL device with a member of that LDAP group.

Job Done Example 2: Adding Ports to a Modbus Polling System

Increase the Available Serial Ports in an Existing Modbus Polling Scheme

In this example, the SEL-3610 Port Server is installed to provide a communications processor with more serial ports. To do this, you will install the SEL-3610 and configure port mappings to route communications between the new serial devices and the existing communications processor. This example assumes networking on the SEL-3610 has been configured as in *Job Done Example 1: Central User Access*.

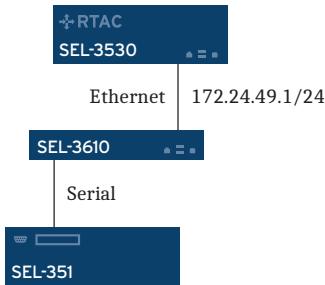
Identifying the Problem

Your objective is to add serial devices to a control system installation by using the Modbus protocol. The problem is that you do not have any available serial ports on your existing communications processor. You decide for the following reasons that the SEL-3610 is the most cost-effective method for solving this problem:

- The SEL-3610 has flexible port switching features.
- The SEL-3610 converts Modbus TCP to Modbus RTU.
- The SEL-3610 is designed to be easy to use.

Defining the Solution

Figure 4.11 is a representation of the communications and device paths that need to be added to the installation. The SEL-3530 needs two-way communications with the SEL-351. The SEL-3530 and the SEL-3610 communicate via Ethernet, while the SEL-3610 and the SEL-351 communicate via serial. The SEL-3530, acting as the Modbus master, has already been configured to talk to the SEL-351 via the SEL-3610.

**Figure 4.11 Port Expansion Communication Paths**

These steps must be performed on the SEL-3610 to configure this system.

- *Create a Serial Port Profile*
- *Enable and Configure the Necessary Serial Ports*
- *Create Serial Mappings*

Create a Serial Port Profile

- Step 1. Access your device with your preferred web browser by typing **<https://192.168.1.2>** into the address bar. This is the default IP address of the ETH F port. If a different IP address was assigned during commissioning, use that address instead. Enter your login credentials and select **Submit**.
- Step 2. Select **Port Profiles** from the navigation panel to access the Port Profiles page.
- Step 3. Select **Add New Profile** to show the New Profile form on the right side of the page.
- Step 4. Create a profile that will allow the SEL-3610 to communicate with the SEL-351. Be sure to set Max Frame Length to **255**.

NOTE: You may receive a certificate error from your browser. The message depends on the browser you use. This error appears because the certificate the device is presenting to your browser does not match the IP address assigned to your SEL device. You will need to create a certificate exception to access the SEL login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

If you are unable to connect to the SEL device, verify that your PC is configured to access the same subnet as the SEL device (see Section 2: Installation).

Name *	SEL-351
Baud Rate :	38400
Communication Interface :	232
<input checked="" type="checkbox"/> Allow Port Power	
<input type="checkbox"/> Bit Based Framing	
Byte Based Framing	
Data Bits :	8
Parity :	None
Stop Bits :	1
Flow Control :	Off
Max Frame Length *:	255
<input type="checkbox"/> Intercharacter Delay	
*required	
Update	

Figure 4.12 Add New Profile

- Step 5. Select the **Submit** button to save the new profile.

Enable and Configure the Necessary Serial Ports

- Step 1. Select **Port Settings** from the navigation panel to access the Port Settings page.
- Step 2. Select the **Update** button associated with serial Port1 to show the Serial Interface Settings form on the right side of the page.
- Step 3. Enable the port by selecting the **Enable** check box.
- Step 4. Select the newly created profile from the dropdown list to assign it to this port.
- Step 5. Provide the port with a descriptive alias.
- Step 6. Select the **Submit** button to save the new port configuration.

Serial Interface COM1 Settings

Enabled

Use Profile
SEL-351 ▾

Baud Rate : 38400
Intercharacter Delay : Disabled
Communication Interface : 232
Allow Port Power : Enabled
Data Bits : 8
Parity : None
Stop Bit : 1
Flow Control : Off
Max Frame Length : 255
Bit Based Framing : Disabled

Alias* :

*required

Submit

Figure 4.13 Assign Serial Interface Settings

Create Serial Mappings

- Step 1. Select the **Port Mappings** link from the navigation panel to access the Port Mappings page.
- Step 2. Select the **Add Group** button from the top of the page to show the Add Group form.
- Step 3. Give the new group an **Alias** of Modbus **Expansion** and select the **Submit** button to create the group.
- Step 4. Select the **Add Device** button associated with the new group to show the Add Device form.
- Step 5. Select **Ethernet Listen Local** from the dropdown list and select **Submit** to access the Add Ethernet Local Driver form.
- Step 6. This driver will be used to communicate with the communications processor. Complete the Add Ethernet Local Driver form as shown in *Figure 4.14. Port 502* is the usual port for Modbus/TCP.

Add Ethernet Local Driver

Group : Modbus Expansion

Alias *:
Eth

Network Interface :
MODBUS:172.24.49.1/24

Port *:
18000

Protocol **:
Modbus/TCP

* Required
** Listening ports selection is ignored if Master port is set or Protocol is Modbus

Submit

Figure 4.14 Add Ethernet Local Driver

Step 7. Select the **Add Device** button associated with your group to show the Add Device form.

Step 8. Select **Serial** from the dropdown list and select **Submit** to access the Add Serial Driver form.

Add Serial

Group : Modbus Expansion

Serial Port :
SEL-351:SEL-351

Protocol **:
Modbus

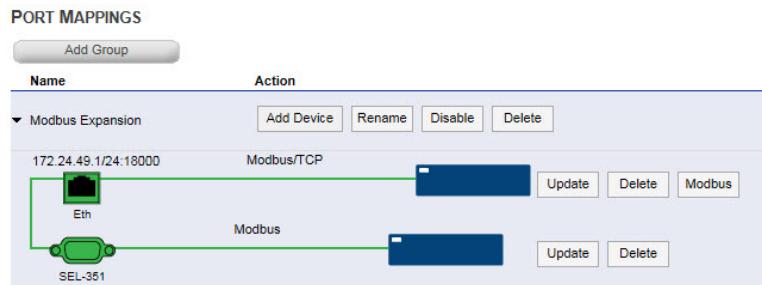
Modem

* Required
** Listening ports selection is ignored if Master port is set or Protocol is Modbus

Submit

Figure 4.15 Add Modbus Serial Driver

Step 9. Select one of your configured serial ports from the **Serial Port** dropdown list, and select **Modbus** from the **Protocol** dropdown list. Select **Submit** to create the new Serial Driver.

**Figure 4.16 Configured Port Mappings**

Step 10. Select the **Modbus** button associated with the Ethernet port of the group to show the Modbus Settings form.

Step 11. Associate the SEL-351 TCP unit ID with its **Serial** address. The Modbus/TCP unit ID is how the communications processor identifies the SEL-351 and the serial address is how the SEL-351 identifies itself. These values are usually the same. When finished, you should have a mapping as shown in *Figure 4.17*.

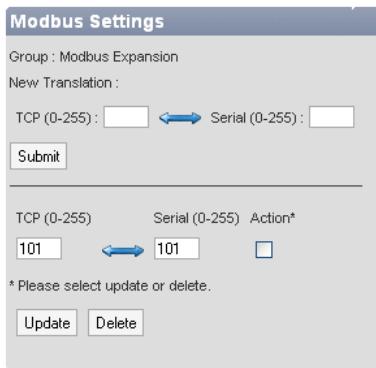


Figure 4.17 Modbus Settings

Your Modbus master can now communicate to the SEL-351 via an Ethernet connection to the SEL-3610.

Job Done Example 3: Detect Physical Tampering

Detect Physical Intrusions

In this example, the SEL-3622 is installed in a recloser control cabinet with an SEL-651R Advanced Recloser Control. The SEL-3622 is used to provide secure, reliable communications between the recloser controller and the upstream substation. The recloser control cabinet is physically accessible to vandals and attackers, so you want to use the physical sensors of the SEL-3622 to alert when someone has physically accessed the cabinet.

Identifying the Problem

Your objective is to secure a recloser control cabinet and the enclosed equipment from physical intrusion and tampering. Select the SEL-3622 to aid this process for the following reasons:

- The SEL-3622 contains an input contact to detect when the recloser cabinet door has been opened.
- The SEL-3622 contains a light sensor to detect when there is a change in light levels.
- The SEL-3622 has a built-in accelerometer to detect when someone is handling the system or trying to break into the cabinet.
- The SEL-3622 has multiple methods of alerting you to activity: Syslog, SNMP (Poll or Trap), and an alarm contact.

Defining the Solution

Figure 4.18 is a representation of the installation that needs to be secured. An SEL-651R acting as a recloser controller is installed in a cabinet with an SEL-3622 acting as the communications security gateway for the cabinet. In addition to using communications gateway capabilities, you will be using the physical sensors built into the SEL-3622 to detect physical access to the recloser cabinet. When a physical event is detected, the device will alert you via Syslog messages.



Figure 4.18 Recloser Cabinet Installation

The following steps must be performed to configure this solution.

- Enable and configure the physical sensors
- Send event messages to a Syslog collector

This solution assumes you have already configured the SEL-3622 to communicate on your system and that you have already configured a working Syslog collector at 172.24.49.8.

Enable and Configure the Physical Sensors

- Step 1. Access your SEL-3622 with your preferred web browser by typing <https://192.168.1.2> into the address bar. This is the default IP address of the ETH F port. If a different IP address has been assigned to the SEL-3622, use that address instead. Enter your login credentials and select **Submit**.
- Step 2. Select the **Physical Sensors** link from the navigation panel to access the physical sensors configuration page.
- Step 3. Enable the physical sensors by selecting the **Enabled** check box at the top of the page.
- Step 4. Your input contact is wired to the recloser cabinet door sensor, so rename the **Energization message** to “Recloser A door closed” and the **De-energization message** to “Recloser A door opened.”
- Step 5. Select the **High** sensitivity level for the **Light Sensor**. This device is installed in a dark cabinet, so there is little chance of a false positive even with the High sensitivity setting.
- Step 6. Select the **Impact and Tilt** sensitivity level for the **Motion Sensor**. This instructs the accelerometer to trigger events both when it detects a sharp spike in movement such as from an impact as well as when it detects a change in orientation of the device.
- Step 7. Select the **Submit** button at the bottom of the page to save the Physical Sensor configuration.

NOTE: Tilt Only may be a good choice if this recloser cabinet is installed in a high vibration environment.

You have now configured the physical sensors. You can use the same physical sensors page to view the last 10 events recorded by each sensor. For this information to be truly useful, you need to get the event data forwarded to a monitoring station in a near real-time manner. To do this, we use the Syslog Protocol.

Send Events to the Syslog Collector

- Step 1. Select the **Syslog** link from the navigation panel located on the left of the screen. This will open the Syslog configuration page.

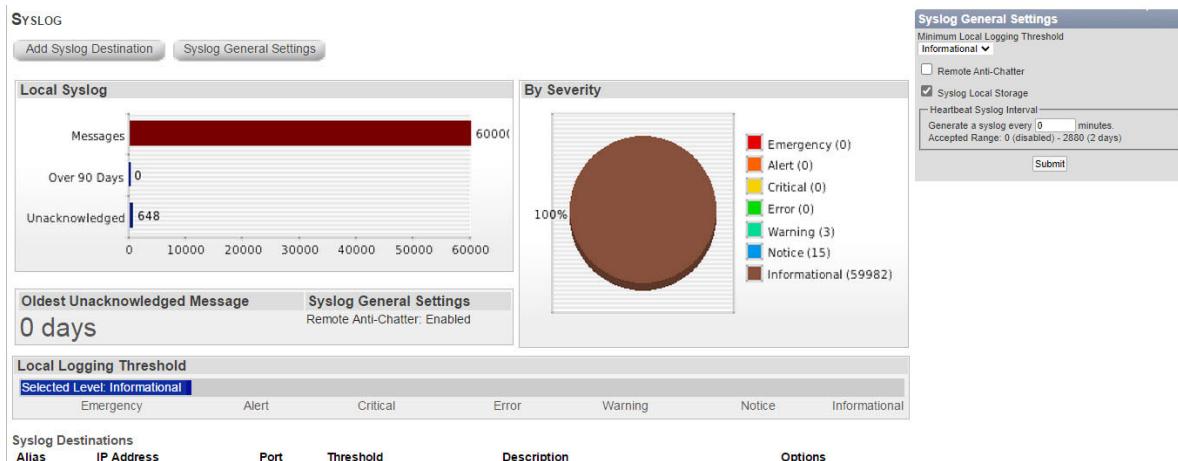


Figure 4.19 Syslog Configuration Page

- Step 2. Select **Add Syslog Destination** to show the **Syslog Destination** form on the right side of the page.
- Step 3. Complete the form as shown in *Figure 4.5* and select **Submit** to submit the changes. The proper settings can also be found in *Table 4.1*.
- Step 4. For bandwidth-constrained wide-area network links, select the **Remote Anti-Chatter** check box. This will prevent environmental events from consuming a large amount of bandwidth resulting from event messages.

The 'Add Syslog Destination' form has the following fields:

- Destination** section: Alias*: Syslog Collector, Description: (empty text area).
- IP Address***: 172.24.49.8
- Port***: 514
- Filters**** section: Enable Advanced Filtering (unchecked), Minimum Severity Threshold Filter: Notice.
- Buttons: Submit.

Figure 4.20 Add Syslog Destination

The physical sensors you configured will now detect door open/close events, light level increase/decrease events, and physical movement events while the Syslog service ensures you have near real-time notification of this activity.

Job Done Example 4: Secure DNP3 Serial-to-Ethernet Conversion Over a Cellular Network

Convert Serial DNP3 to Ethernet by Using UDP for Transport

The SEL-3622 Security Gateway is a low-power device that offers a number of security features specific to field cabinets like those that are used to host recloser controls. The IPsec feature on the SEL-3622 Security Gateway provides powerful data protection through confidentiality and data integrity mechanisms. The physical tamper alerting features add powerful physical–cyber awareness to remote field cabinets. The serial-to-Ethernet conversion capabilities of the SEL-3622 remove the need for additional hardware devices, and allow remote Front-End Processors (FEP) to connect seamlessly to the IED in the field.

Defining the Problem

Your objective is to connect your remote field distribution cabinets to your FEPs over a cellular wireless network. The problem is how to go about securing the cellular link and adding additional physical tamper awareness to the remote site. Furthermore, the SEL-651R recloser control currently in the cabinet has no Ethernet connectivity, so serial-to-Ethernet conversion must be configured.

Defining the Solution

You decide to use the SEL-3622 Security Gateway because it is a low-power device that offers a number of security features specific to field cabinets like those that are used to host recloser controls.

- The IPsec feature on the SEL-3622 Security Gateway provides powerful data protection through confidentiality and data integrity mechanisms.
- The SEL-3622 has specialized physical tamper alerting hardware that adds powerful physical–cyber awareness to remote field cabinets.
- The serial-to-Ethernet conversion capabilities in the SEL-3622 remove the need for additional hardware devices, and allow remote FEPs to connect seamlessly to the IED in the field.
- The SEL-3622 supports strong engineering access controls through use of the proxy services feature.

The architecture of the solution will roughly resemble *Figure 4.21*.

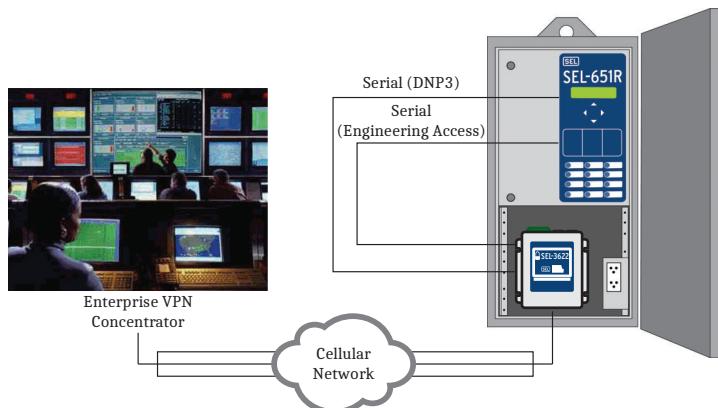


Figure 4.21 Job Done 4 Architecture

Cellular Network Considerations

Latency Considerations

Cellular networks typically have higher latency than wired communication links. Typical latencies on cellular links can range from 100–400 milliseconds or longer for Edge and 3G connections, and 50–150 milliseconds for LTE connections. While such latencies do not present a problem for the SEL-3622, be aware that time-out settings for your DNP3 connections may need to be adjusted. Anticipate an extra 3–10 milliseconds for IPsec when budgeting for latency.

Bandwidth Considerations

In relation to bandwidth, SEL recommends that the wireless communications link support at least 100 kbps speeds and above. This ensures the ability to perform maintenance duties on the unit remotely, including firmware upgrades and configuration changes over the webpage.

Ethernet Transport Protocol (UDP, TCP) Considerations

For serial-to-Ethernet transport, you can configure the SEL-3622 to use either TCP or UDP protocols. TCP is a stateful protocol that includes a three-way handshake mechanism when beginning connections, error correction, resending of lost packets, and acknowledgments built into the protocol. UDP is not a stateful protocol and is a “send and forget” protocol. While UDP protocol has less overhead than TCP, UDP cannot guarantee delivery of data. UDP is typically a better choice if your cellular service provider charges for data consumption, and if you are not concerned about dropping packets once in a while (i.e., 99.9% for delivery for UDP vs. 99.99% for TCP). UDP may also be a better choice if the protocol being converted to Ethernet would be negatively affected by the TCP feature of resending “old” data (i.e., 5 seconds old) in case of packet loss. This job done example uses UDP as the transport mechanism for serial DNP3 data.

Maximum Transmission Unit (MTU) Size Considerations

When using IPsec over cellular networks, be aware that you may need to set a lower maximum transmission unit (MTU) size on the SEL-3622 **Network Settings** page. In some cases, MTU sizes of 1430 bytes or lower are required. Be aware of this if you encounter problems with larger packet sizes being dropped. You can find the usable MTU size on your cellular network by configuring the modem in Bridge mode, connecting it to your PC, and using the Ping command on Microsoft Windows via “ping -f -l <packet size> <address>” (“ping -M -s <packet size> <address>” in Linux). Adjust the packet size and repeat the Ping command until you identify the packet size at which warnings about fragmentation occur. In *Figure 4.22*, the MTU size is of the link is 1514 bytes (1472 bytes + 42 byte ICMP header).

```
C:\Users\User\Desktop>ping -f -l 1472 google.com
Pinging google.com [209.118.208.55] with 1472 bytes of data:
Reply from 209.118.208.55: bytes=1472 time=102ms TTL=50
Reply from 209.118.208.55: bytes=1472 time=186ms TTL=50
Reply from 209.118.208.55: bytes=1472 time=142ms TTL=50

Ping statistics for 209.118.208.55:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 102ms, Maximum = 186ms, Average = 143ms
Control-C
^C
C:\Users\User\Desktop>ping -f -l 1473 google.com

Pinging google.com [209.118.208.55] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 209.118.208.55:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
    Control-C
    ^C
C:\Users\User\Desktop>_
```

Figure 4.22 MTU Size Discovery on Windows

Serial-to-Ethernet Conversion Considerations

When converting serial DNP3 to Ethernet, you must take cabling and SEL relay settings into consideration.

- When connecting an SEL-3600 device to a serial port on an SEL relay for DNP3 conversion, set the PREDLY setting on the DNP3-enabled SEL relay serial port to OFF. This will ensure the normally high RTS line on the SEL-3600 serial port will not block the relay from responding.
- SEL suggests using the SEL-C273A cable, or SEL-C272A cable when connecting SEL-3600 devices to serial ports on SEL relays.

```
=acc
Password: ? *****

FEEDER 1                               Date: 03/03/15      Time: 11:56:02.032
STATION A

Level 1

=>sho p 1

Port 1

EPORT    = Y
PROTO    = DNP
SPEED    = 19200      PARITY   = 0      STOP     = 2      DVARAI   = 4
DNPADR   = 0          REPADR  = 0      DNPMAP   = 1      DECPLA   = 1
ECLASSB  = 1          ECLASSC = 0      ECLASSA = 2      ANADBA   = 100
DECPLV   = 1          DECPML  = 1      ANADBA  = 100
ANABDM   = 100         TIMERQ  = I      STIMEO   = 1.0
ETIMEO   = 5           UNSOL   = N      MINDLY   = 0.05
PREDLY   = OFF         MINDIST = OFF      MAXDIST = OFF
RPEVTYP  = ALL
=>
```

Figure 4.23 PREDLY Setting on SEL Relay

Cellular Modem Considerations

The SEL-3622 has been successfully used with various Digi, Sierra Wireless, and other cellular modem models from other manufacturers. Note that when using IPsec, the cellular modem needs to be set in bridge or transparent mode, so that

Job Done Example 4: Secure DNP3 Serial-to-Ethernet Conversion Over a Cellular Network

the IP address normally assigned by the cellular provider is given to the SEL-3622 Ethernet interface instead. The SEL-3620/SEL-3622 IPsec function does not feature NAT-Traversal (NAT-T) at this point in time.

Configuring the SEL-3622 Cellular-Connected Interface

- Step 1. When configuring the SEL-3622 interface that will connect to the cellular modem, set the **Enable DHCP Client** option. A manual IP address is required, and is used in case DHCP connectivity is lost.

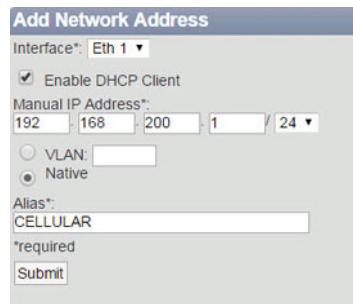


Figure 4.24 Configuring the SEL-3622 Interface for Cellular Connectivity

- Step 2. Be sure to set the cellular connection as the default gateway. To do this, go to global settings and select **CELLULAR (DHCP)** as the manual default gateway.

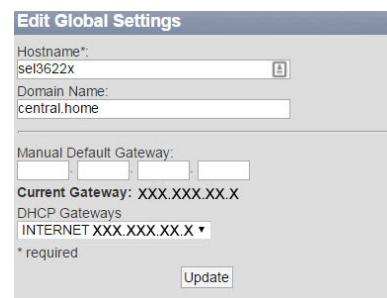


Figure 4.25 Configuring the SEL-3622 Default Gateway for the DHCP Gateway

- Step 3. The default gateway of the SEL-3622 unit will automatically switch to the DHCP gateway when it is received by the cellular modem, as shown in *Figure 4.26*, as seen from the **Network Settings** page.



Figure 4.26 SEL-3622 With the Cellular Default Gateway

Configuring IPsec

To configure IPsec on the SEL-3622 to a third-party firewall, follow these steps.

- Step 1. Navigate to IPsec Connections.
- Step 2. Select Add w/Passphrase.

Step 3. Enter the remote network where the SCADA FEP resides, the remote internet-connected third-party VPN gateway IP address, the local gateway (cellular connection), the local network to share with the remote VPN gateway, and the mutual passphrase (see *Figure 4.27*).

The screenshot shows a configuration dialog titled "Add IPsec using Passphrase". The "IPsec Profile" dropdown is set to "Lemnos - IKEv2". Under "Remote Network", the IP is set to 192.168.5.0 with a subnet mask of 24, and the alias is REMOTE_FEP_NET. Under "Remote Gateway", the IP is listed as [redacted] and the alias is REMOTE_VPN_GATEWAY. The "Local Gateway" is set to "CELLULAR" and the "Local Network" is "Default". In the "Passphrase" section, two password fields are shown, both containing "*****". A note at the bottom says "* required". At the bottom right is a "Submit" button.

Figure 4.27 IPsec Settings

Step 4. Next, you will need to configure your third-party VPN gateway to connect to the SEL-3622 via IPsec. Refer to *Table 6.10*, *Table 6.11*, or *Table 6.12* (depending on chosen IPsec profile) for configuration settings on the third-party VPN gateway. If all goes well, you should be able to navigate to the SEL-3622 dashboard and see that the IPsec interface is UP.

IPsec Connections			
Alias	State	In	Out
Default- REMOTE_FEP_NET	UP	1092 Bytes	1092 Bytes

Figure 4.28 IPsec Connection Status

Configuring DNP3 Serial-to-Ethernet Configuration

To configure DNP3 serial to UDP Ethernet conversion, follow these steps:

Step 1. Navigate to **Serial Ports > Port Profiles** and select **Add New Profile**. Ensure the profile matches the serial DNP3 port of the SEL relay to which you are connecting from the SEL-3622. In *Figure 4.29*, you may choose to use a different Max Frame Length setting. However, for UDP, having the Max Frame Length as high as possible (255) will package as much serial data as possible into a single UDP packet, and help prevent the splitting of DNP3 serial data into multiple UDP packets. The packaging of as much serial data into one UDP packet as possible will lower the chance of dropped polls because any dropped data packet may render the overall DNP3 poll response invalid.

New Profile

Name *: SEL Relay DNP Serial Port

Baud Rate : 19200

Communication Interface : 232

Allow Port Power

Bit Based Framing

Byte Based Framing

Data Bits : 8

Parity : None

Stop Bits : 1

Flow Control : Off

Max Frame Length *: 255

Intercharacter Delay

*required

Submit

Figure 4.29 Port Profile DNP Port Settings

- Step 2. Navigate to Port Settings and select **Update** on COM1.
- Step 3. Select the serial port profile just created, and select the **Enabled** check box.
- Step 4. Select **Submit**.

Serial Interface COM2 Settings

Enabled

Use Profile : SEL Relay DNP Serial Port

Baud Rate : 19200

Intercharacter Delay : Disabled

Communication Interface : 232

Allow Port Power : Disabled

Data Bits : 8

Parity : None

Stop Bit : 1

Flow Control : Off

Max Frame Length : 255

Bit Based Framing : Disabled

Alias* : COM02

*required

Submit

Figure 4.30 Serial Port Enabled and Updated

- Step 5. Navigate to **Port Mappings** and add a new Port Mapping group. When finished, select **Submit**.
- Step 6. On the new Port Mapping group, select **Add Device**.
- Step 7. Choose **Serial**, and choose the serial port you configured, then select **Submit**.

Add Serial

Group : DNP Conversion
Serial Port :
SEL-651R: SEL Relay DNP Serial Port
Protocol **:
Serial
 Master Port **

Listening Ports :

* Required
** Listening ports selection is ignored if Master port is set or Protocol is Modbus

Submit

Figure 4.31 Serial Port

- Step 8. Select **Add Device** again and select Ethernet Listen Local.
- Step 9. Give the driver an Alias and port.
- Step 10. For protocol, choose UDP, and for Network Interface choose the local network used in your IPsec configuration. You may choose to set UDP Response Destination Override if the remote Front-End Processor is using an unusual Network Address Translation (NAT) configuration.

Add Ethernet Local Driver

Group : DNP Conversion
Alias *:
UDP DNP Ethernet
Network Interface :
Default: 192.168.1.23/24
Port *:
20000
Protocol **:
UDP
UDP Response Destination
 Override

Listening Ports :

SEL-651R

* Required
** Listening ports selection is ignored if Master port is set or Protocol is Modbus

Submit

Figure 4.32 Ethernet Listen Local Settings

- Step 11. Once configured, your serial-to-Ethernet Port Mapping should look similar to *Figure 4.33*.

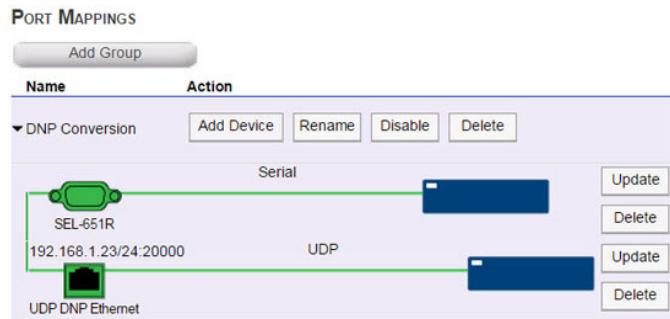


Figure 4.33 DNP Serial-to-Ethernet Port Mapping

Configuring Physical Awareness Alerts on the SEL-3622

Finally, we need to enable physical awareness alerts from the SEL-3622 to a remote logging server:

- Step 1. Navigate to **System > Physical Sensors**. Enable the physical sensor alerts by selecting the **Enabled** box under Global Settings. For this example, we enabled the Input Contact alerts, Light Sensor alerts on High sensitivity, and Motion Sensor alerts for both Impact and Tilt.
- Step 2. Next, we must enable an alerting output. For this example, we chose to use Syslog, though you may choose to use Syslog and/or SNMP traps. To enable Syslog, navigate to **Network > Syslog**, and select **Add Syslog Destination**, and then configure remote the Syslog destination (see *Figure 4.34*).

The form has fields for 'Alias*' (Central Syslog Server), 'IP Address*' (192.168.1.5100), 'Port*' (514), 'Minimum Threshold*' (Informational), and a 'Description' text area (Centralized Security Information Event Management System). There is also a note '*required' and a 'Submit' button.

Figure 4.34 Configure Centralized Alerts

Job Done Example 5: Using IPSec to Secure Communication

Communicate Securely Over Untrusted Networks

In this example, SEL-3620 Ethernet Security Gateways are installed as the access points to the Ethernet networks of two substations. You must ensure that all data moving between these substations are secured. To do this, you will configure and install two SEL-3620 gateways to communicate with each other through IPsec VPN tunnels. The SEL-3620 gateways will authenticate each other by using pre-

shared passphrases. This example assumes default configurations after the device has been commissioned. In this example, the SEL-3622 could be used in place of the SEL-3620.

Identifying the Problem

Your objective is to secure the data in transit between two substation networks. You decide for the following reasons that the SEL-3620 is the most cost-effective method for solving this problem.

- The SEL-3620 solution provides many proven technologies to protect your data, including IPsec and a stateful firewall.
- The SEL-3620 is hardened for substation use.
- The SEL-3620 is designed to be easy to use.

Defining the Solution

Figure 4.35 is a representation of two substation networks communicating through SEL-3620 gateways.

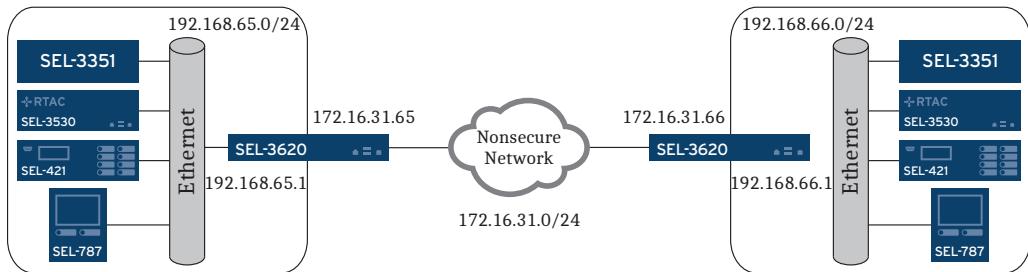


Figure 4.35 Diagram of Two Substation Networks

Table 4.3 defines the network settings we will apply to the SEL-3620 gateways to configure the system shown in *Figure 4.35*.

Table 4.3 Job Done Example 5 Settings

Setting	SEL-3620 at Substation A	SEL-3620 at Substation B
Trusted Interface	192.168.65.1	192.168.66.1
Trusted Network	192.168.65.0/24	192.168.66.0/24
Untrusted Interface	172.16.31.65	172.16.31.66
Untrusted Network	172.16.31.0/24	172.16.31.0/24
IPsec Profile	Lemnos–IKEv2	Lemnos–IKEv2
Passphrase	Asdf123\$	Asdf123\$

These steps must be performed on each SEL-3620 to configure this system.

- *Configure the Untrusted Interface of Substation A* on page 4.23 or *Configure the Untrusted Interface of Substation B* on page 4.24.
- *Configure the Trusted Interface of Substation A* on page 4.23 or *Configure the Trusted Interface of Substation B* on page 4.25.
- *Configure the IPsec Connection to Substation B From Substation A* on page 4.24 or *Configure the IPsec Connection to Substation A From Substation B* on page 4.25.

We will first perform these steps on the SEL-3620 that will be placed in Substation A. Then we will go through similar steps to configure the SEL-3620 that will be placed in Substation B.

Configure the Untrusted Interface of Substation A

- Step 1. Log in to the SEL-3620 that will be placed in Substation A. Access your SEL-3620 with your preferred web browser by typing **https://192.168.1.2** in the address bar. This is the default IP address. If a different IP address was assigned during commissioning of the SEL-3620, use that address instead. Enter your login credentials and select **Submit**.
- Step 2. Select the **Network Settings** link from the navigation panel to access the Network Settings page.
- Step 3. Select **Add Ethernet Address** on the top of the page to show the Add Network Address form.
- Step 4. Complete the Add Network Address form as shown in *Figure 4.36* and select **Submit**.

NOTE: You may receive a certificate error from your browser. The message depends on the browser you use. This error appears because the certificate the device is presenting to your browser does not match the IP address assigned to your SEL device. You will need to create a certificate exception to access the SEL login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

If you are unable to connect to the SEL device, verify that your PC is configured to access the same subnet as the SEL device. Instructions for doing this can be found in Section 2: Installation.

Figure 4.36 Add Untrusted Network

- Step 5. Select the **Update** link underneath the **Eth 1** icon to show the Ethernet Interface Eth 1 Settings form.
- Step 6. Enable the interface and select **Submit**.

Configure the Trusted Interface of Substation A

- Step 1. From the Network Settings page, select **Add Ethernet Address** on the top of the page to show the Add Network Address form.
- Step 2. Complete the Add Ethernet Address form as shown in *Figure 4.37* and select **Submit**.

Figure 4.37 Add Protected Network

- Step 3. Select the **Update** link underneath the **Eth 2** icon to show the Ethernet Interface Eth 2 Settings form.
- Step 4. Enable the interface and select **Submit**.

Configure the IPsec Connection to Substation B From Substation A

- Step 1. Select the **IPsec Connections** link from the navigation panel to access the IPsec Connections page.
- Step 2. Select **Add w/Passphrase** at the top of the page to show the Add IPsec using Passphrase form.
- Step 3. Complete the **Add IPsec using Passphrase** form with the settings shown in *Figure 4.38*.

The screenshot displays the 'Add IPsec using Passphrase' configuration dialog. At the top, the 'IPsec Profile' is set to 'Lemnos - IKEv2'. Under 'Remote Network', the IP address is 192.168.66.0 with a subnet mask of 24, and the alias is 'Substation B Network'. Under 'Remote Gateway', the IP address is 172.16.31.66, and the alias is 'Substation B Gateway'. The 'Local Gateway' is set to 'Untrusted Interface', and the 'Local Network' is set to 'Trusted Interface'. In the bottom section, the 'Passphrase' field contains 'Asdf123\$', and the 'Retype Passphrase' field also contains 'Asdf123\$'. A note indicates '* required'. A 'Submit' button is at the bottom right.

Figure 4.38 Add IPsec Connection to Substation B

- Step 4. Enter **Asdf123\$** as the **Passphrase** and verify it in the **Retype Passphrase** box.
- Step 5. Select **Submit** to save the IPsec configuration.

Configure the Untrusted Interface of Substation B

- Step 1. Log in to the SEL-3620 that will be placed in Substation B. Access your SEL-3620 with your preferred web browser by typing **https://192.168.1.2** in the address bar. This is the default IP address. If a different IP address was assigned during commissioning of the SEL-3620, use that address instead. Enter your login credentials and select **Submit**.
- Step 2. Select the **Network Settings** link from the navigation panel to access the Network Settings page.
- Step 3. Select **Add Ethernet Address** on the top of the page to show the Add Network Address form.

NOTE: You may receive a certificate error from your browser. The message depends on the browser you use. This error appears because the certificate the device is presenting to your browser does not match the IP address assigned to your SEL device. You will need to create a certificate exception to access the SEL login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

If you are unable to connect to the SEL device, verify that your PC is configured to access the same subnet as the SEL device. Instructions for doing this can be found in Section 2: Installation.

- Step 4. Complete the **Add Network Address** form as shown in *Figure 4.39* and select **Submit**.

Figure 4.39 Add Untrusted Network at Substation B

- Step 5. Select the **Update** link underneath the **Eth 1** icon to show the Ethernet Interface Eth 1 Settings form.
Step 6. Enable the interface and select **Submit**.

Configure the Trusted Interface of Substation B

- Step 1. From the Network Settings page, select **Add Ethernet Address** on the top of the page to show the Add Network Address form.
Step 2. Complete the **Add Network Address** form as shown in *Figure 4.40* and select **Submit**.

Figure 4.40 Add Protected Network at Substation B

- Step 3. Select the **Update** link underneath the **Eth 2** icon to show the Ethernet Interface Eth 1 Settings form.
Step 4. Enable the interface and select **Submit**.

Configure the IPsec Connection to Substation A From Substation B

- Step 1. Select the **IPsec Connections** link from the navigation panel to access the IPsec Connections page.
Step 2. Select **Add w/Passphrase** at the top of the page to show the Add IPsec using Passphrase form.
Step 3. Complete the **Add IPsec using Passphrase** form with the settings shown in *Figure 4.41*.

The screenshot displays the 'Add IPsec using Passphrase' configuration interface. Key settings include:

- IPsec Profile:** Lemnos - IKEv2
- Remote Network:** IP: 192.168.65.0/24, Alias: Substation A Network
- Remote Gateway:** IP: 172.16.31.65, Alias: Substation A Gateway
- Local Gateway:** Untrusted Interface
- Local Network:** Trusted Interface
- Passphrase:** Asdf123\$
- Retype Passphrase:** Asdf123\$

Figure 4.41 Add IPsec Connection to Substation A

Step 4. Enter **Asdf123\$** as the **Passphrase** and verify it in the **Retype Passphrase** box.

Step 5. Select **Submit** to save the IPsec configuration.

Verify the IPsec Connection

Verify that the newly configured IPsec connection works by connecting the untrusted ports (Eth 1) of both SEL-3620 gateways with an Ethernet cable. The **VPN SYNC** indicator LED of both units should be illuminated and green. If they are not illuminated, then log in to the SEL-3620 and enable IPsec on the IPsec Connections page. If they are not green, then verify the physical connection between the two units and the settings of each unit.

Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant

Use the SEL-5828 Virtual Port Service Software to Improve Security

SEL-5020 Settings Assistant Software is used to configure communications processors such as the SEL-2032 Communications Processor. The problem is that the connection between the SEL-5020 and the communications processor is unencrypted. You can use the SEL-3620 with the SEL-5828 Virtual Port Service software to provide a secure SSH communications channel that protects the data sent over this connection from interception or tampering on the network.

Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant

Your objective is to secure the connection between the SEL-5020 and a communications processor on a remote network. You choose the SEL-5828 solution for the SEL-3620 for the following reasons:

- The SEL-5828 can transform a serial connection into a secure SSH connection to the SEL-3610, SEL-3620, or SEL-3622.
- The SEL-5828 comes free with the SEL-3610, SEL-3620, or SEL-3622.
- The SEL-3620 can use port maps to perform SSH-to-Serial or SSH-to-Telnet conversion for the connection to the SEL-2032 Communications Processor.

The following steps use the SEL-5828 and an SEL-3620 to set up a secure communications path between an SEL-5020 and the communications processor.

- Step 1. Ensure that the PC running the SEL-5020 can reach the SEL-3620 over the Ethernet network, and that the SEL-2032 is on the local substation network that is protected by the SEL-3620.
- Step 2. Set up a Port Map on the SEL-3620 to map an incoming SSH connection to a Telnet connection to the SEL-2032.
 - a. Open the web interface of the SEL-3620, and navigate to **Security** and then to **Port Mappings**.
 - b. Select **Add Group** to create a new port map.
 - c. In the Alias box, give this group the name **SSH to TELNET**.
 - d. Add an Ethernet Listen Local device.
 - e. Set the Alias to **INCOMING SSH**.
 - f. Set the Network interface to **Listen on All**.
 - g. Set the Protocol to **SSH**.
 - h. Set the TCP Port to **22**.
 - i. Select **Submit**.
 - j. Add an Ethernet Connect Remote device.
 - k. Set the Alias to **2032 TELNET**.
 - l. Set the Remote IP Address to the IP address of your SEL-2032.
 - m. Set the Protocol to **TELNET**.
 - n. Set the TCP Port to **23**.
 - o. Select **Submit**.

The finished port map will look like this one:

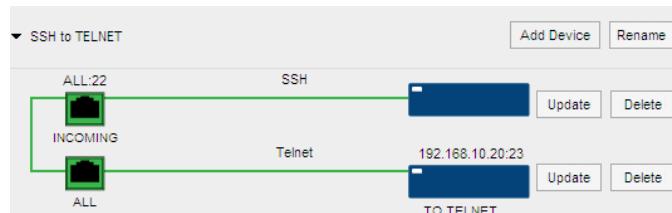


Figure 4.42 SSH to TELNET Port Map

Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant

Step 3. Start SEL-5828 and create a virtual serial port for an SSH connection to the SEL-3620.

(See *Getting Started With the SEL-5828 Virtual Port Service* on the SEL website for information about setting up this software on your computer.)

- a. Open the SEL-5828 configuration application (VirtualPortService.Manager.exe).
- b. Select **Port / Add** from the menu to open the **Settings** window.
- c. In the **General** tab, you can assign an optional name to the new port.
- d. In the **Port** tab (*Figure 4.43*) set the port type to **Serial** and choose an unused port number to be used for connections from the SEL-5020.

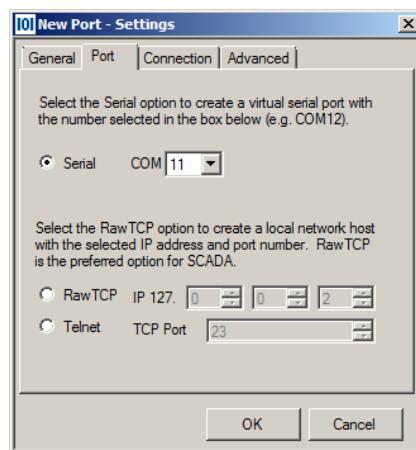


Figure 4.43 Setting the Port Number

- e. Go to the **Connection** tab, and set the connection parameter to match the INCOMING SSH port you configured on the SEL-3620 (*Figure 4.44*). Select **Use saved username and password for this connection** if you want to avoid being prompted for credentials when connecting using this port.

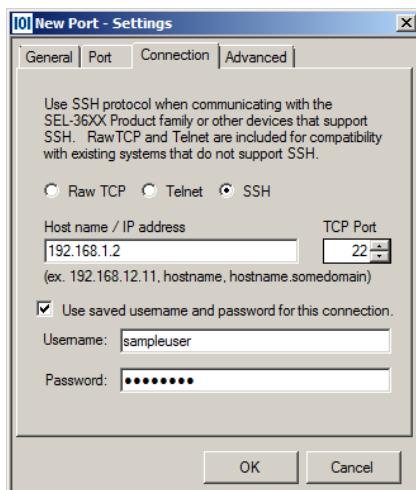


Figure 4.44 Setting Connection Parameters

Job Done Example 7: Using VLANs on the SEL-3620 With a Managed Ethernet Switch

- > Select protocol **SSH**
- > Host name / IP address = <IP address of your SEL-3620>
- > TCP Port = 22
- > Username and Password are credentials for a valid account on the SEL-3620

f. Select **OK**

- Step 4. Start the SEL-5020 and connect to the virtual serial port.
- a. Choose **Connection Directory** > **Add** from the SEL-5020 menu.
 - b. Give the connection a descriptive name.
 - c. Set **Connection Type** to **Serial**.
 - d. Select the highest baud rate.
 - e. For **Comm Port**, select **Direct to COM11**. Leave other settings as they are.
 - f. Choose **Communications** and then **Terminal** from the SEL-5020 menu.
 - g. In the Terminal window, select **Communications** and then **Open** from the menu.
 - h. Log in normally to the SEL-2032 as shown in *Figure 4.45*. The connection between the SEL-5020 and the SEL-3620 will be securely protected by SSH.

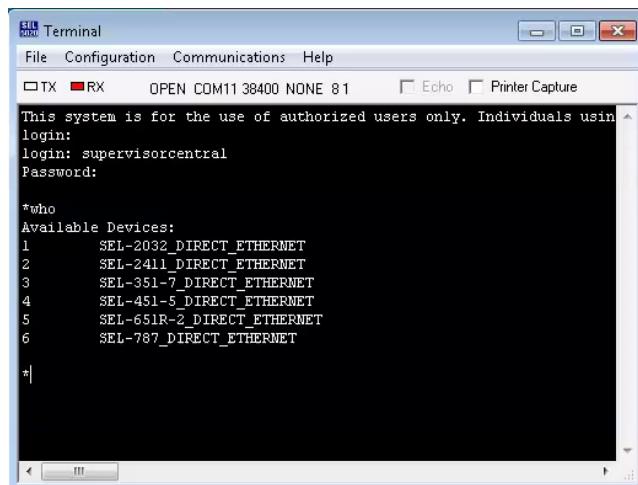


Figure 4.45 Using the SEL-5020 Terminal Window

Job Done Example 7: Using VLANs on the SEL-3620 With a Managed Ethernet Switch

NOTE: The SEL-3610 currently supports one VLAN interface or one “native” interface per physical network port.

The SEL-3620 and SEL-3622 support as many as four VLAN-tagged logical network interfaces, commonly referred to as subinterfaces, per physical network port. This allows the SEL-3620 or SEL-3622 to communicate directly with as many as 12 logical networks by using all three of its physical network ports. When communicating with host devices that do not natively support VLANs, the ability to use VLAN-tagged subinterfaces requires a managed switch.

The following scenario involves an SEL-3620 and an SEL-2730M Managed Ethernet Switch. See *Figure 4.46* for a diagram of the scenario.

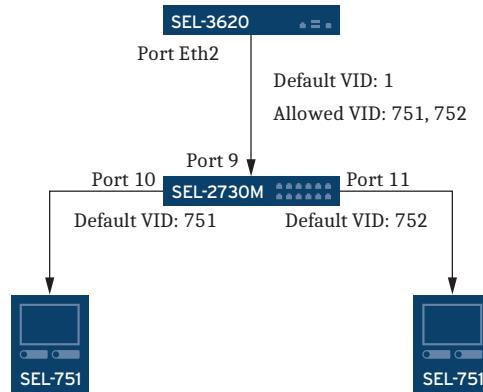


Figure 4.46 Using the SEL-3620 With a Managed Ethernet Switch

In this scenario, use SEL-751 Feeder Protection Relays, each on an isolated VLAN communicating on two separate logical networks and protected by the SEL-3620 firewall. Use the SEL-3620 to create two separate VLAN subinterfaces and the SEL-2730M to achieve the solution.

This scenario assumes the SEL-751 Relays are configured as follows:

SEL-751-01:

- IP address: 172.16.1.51/24
- Default Router: 172.16.1.1
- Connected to the SEL-2730M, Port 10

SEL-751-02:

- IP address: 172.16.2.51/24
- Default Router: 172.16.2.1
- Connected to the SEL-2730M, Port 11

This Job Done example explains how to configure the SEL-3620 and SEL-2730M as follows:

SEL-3620, Port Eth2:

- VLAN 751, IP address: 172.16.1.1/24
- VLAN 752, IP address: 172.16.2.1/24
- Connected to the SEL-2730M, Port 9
- Firewall configured to allow all traffic between the SEL-751 Relays

SEL-2730M:

- Port 9 (SEL-3620): Default VID (VLAN identification) 1; Allowed VIDs: 751, 752
- Port 10 (SEL-751-01): Default VID: 751
- Port 11 (SEL-751-02): Default VID: 752

Configuring the SEL-3620

From the SEL-3620 web management interface:

- Step 1. Navigate to the Network Settings page. Select **Update** under the port and ensure the Eth2 interface is enabled.
- Step 2. Select **Add Network Address**. Add the IP address and VLAN information, as shown in *Figure 4.47*.
- Step 3. When finished, select **Submit**.

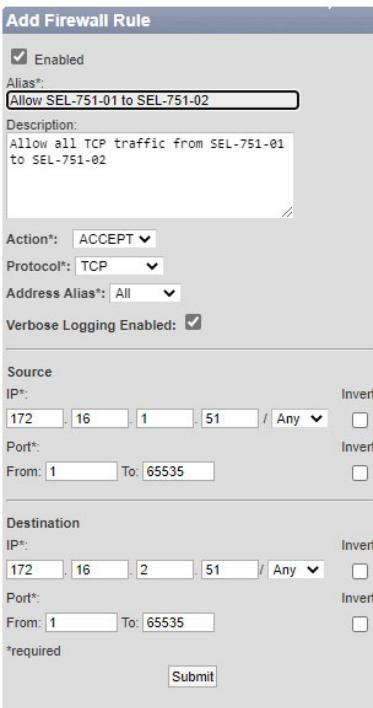
Figure 4.47 Adding the VLAN 751 Subinterface

- Step 4. Repeat Step 2 for VLAN 752 by changing the appropriate boxes based on *Figure 4.47*. The IP address for the VLAN 752 interface is 172.16.2.1 with a subnet mask of 24.
- Step 5. When you have finished, the SEL-3620 should have two VLAN interfaces on Port Eth2, as seen in *Figure 4.48*.

Address Alias	Interface Alias	IP Address	VLAN	MACsec	Web Server	Options
Default	Eth F	192.168.1.120/24		Yes	<input type="button" value="Update"/> <input type="button" value="Delete"/>	
USB	USB B	172.29.131.1/24		Yes		
LAN751	Eth 2	172.16.1.1/24	751		<input type="button" value="Update"/> <input type="button" value="Delete"/>	
LAN752	Eth 2	172.16.2.1/24	752		<input type="button" value="Update"/> <input type="button" value="Delete"/>	

Figure 4.48 Completed SEL-3620 Interface

- Step 6. Navigate to the SEL-3620 Firewall settings page. Select **Add Firewall Rule** at the top of the page.
- Step 7. Configure a firewall rule to allow traffic from SEL-751-01 to SEL-751-02, as shown in *Figure 4.49*. When finished, select **Submit**.

**Figure 4.49 Adding the Firewall Rule**

Step 8. Repeat *Step 7* for traffic from SEL-751-02 to SEL-751-01. The source and destination addresses should be switched.

When you have finished, the SEL-3620 is configured to allow traffic from each SEL-751 to the other.

Configuring the SEL-2730M

From the SEL-2730M web management interface:

- Step 1. Navigate to the Global Settings page and ensure the VLAN-aware check box is checked.
- Step 2. Navigate to the VLAN Settings page and select **Port View**.
- Step 3. For Port 9, enter **1** for the **Default VID**, and **751-752** for the **Allowed VIDs**.
- Step 4. For Port 10, enter **751** for the **Default VID**.
- Step 5. For Port 11, enter **752** for the **Default VID**.
- Step 6. When you have finished, select **Submit** on the bottom of the page. You should have the VLANs configured, as shown in *Figure 4.50*.

VLAN Settings		
VLAN View	Port View	
Ports	Default VID	Allowed VIDs
1	1	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	
8	1	
9	1	751-752
10	751	
11	752	

Figure 4.50 Completed VLAN Configuration on the SEL-2730M

So long as the VLANs, ports, firewall, and IP addresses are configured per this guide, you will have a working VLAN scenario with the SEL-3620.

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

Overview

Commission MACsec With an SEL-651RA Recloser Control

Commissioning a MACsec connection between two devices can be a daunting task for someone who has never completed this procedure before. SEL has enhanced MACsec with innovations that serve to make this process easier while maintaining security.

Defining the Problem

Remote recloser control cabinets are at higher risk because they normally have less physical security. This increases the need to employ logical security within the cabinet to protect communications and data. You decide that MACsec is the best method to provide this security and need to configure and commission the system.

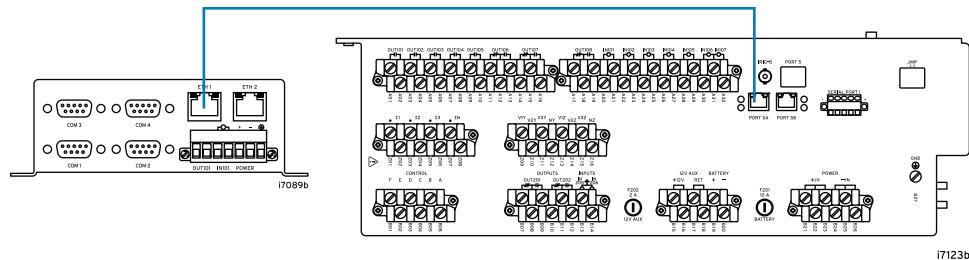
Defining the Solution

NOTE: The naming of each commissioning method refers to the steps accomplished on the SEL-651RA. Commissioning of the SEL-3622 is done exclusively through the SEL-3622 web interface.

SEL supports MACsec Key Agreement (MKA) verification to simplify the MACsec commissioning process. This example covers three commissioning methods for a MACsec connection between an SEL-651RA and an SEL-3622, allowing for different scenarios and field conditions.

Table 4.4 Commissioning Methods

Commissioning Mode	When to Use
Automatic Commissioning Front Panel	When you have physical access to the SEL-651RA front panel and are comfortable navigating its screens, this is the simplest method for field commissioning. Uses derived keys that are rotated immediately after initial adoption is complete.
Automatic Commissioning Command Line	If you prefer to use a terminal session on the SEL-651RA instead of navigating its front panel screens or are commissioning in a lab prior to deployment in the field. Uses derived keys that are rotated immediately after initial adoption is complete.
Manual Commissioning Command Line	Use this method if cable integrity cannot be physically verified. Commissioning is done through the SEL-651RA terminal session which is out of band of the Ethernet communications link.

**Figure 4.51 Example SEL-651RA and SEL-3622 MACsec Connection**

Considerations for the SEL-651RA and SEL-3622 Commissioning Methods

- SEL-651RA Firmware version R105 or later is required
- SEL-3622 Firmware version R211 or later is required
- The SEL-3622 supports only one point-to-point connection per Ethernet port as of firmware R211
- During commissioning there may be packet loss of about 15–40 seconds for systems configured with existing communications on that same interface

These commissioning methods may also be used for the following SEL devices and respective firmware versions:

Table 4.5 Additional MACsec Devices and Firmware Versions

Device	Firmware Version
SEL-3620	R211 or later
SEL-651R-2	R412 or later

For more device-specific MACsec information, please refer to the instruction manual relevant to your SEL device.

If your SEL-3622 has already been configured for MACsec, jump to *SEL-651RA Automatic Commissioning Front Panel Method* on page 4.37, *SEL-651RA Automatic Commissioning Command Line Method* on page 4.38, or *SEL-651RA Manual Commissioning Command Line Method* on page 4.41 as desired to configure the SEL-651RA to complete the commissioning process.

Set up MACsec Automatic Commissioning on the SEL-3622

- Step 1. Log in to the SEL-3622 web interface. Open the dashboard to verify that the Firmware ID String (FID) in the version information is at least R211 or later.

If the firmware version is earlier than R211, update the firmware to R211 or later prior to continuing with these steps (see *Appendix B: Firmware Upgrade Instructions* in the SEL-3610/SEL-3620/SEL-3622 Instruction Manual).

- Step 2. Navigate to the **MACsec Connections** view under the **Security** menu.
 Step 3. Select **New Connection**.

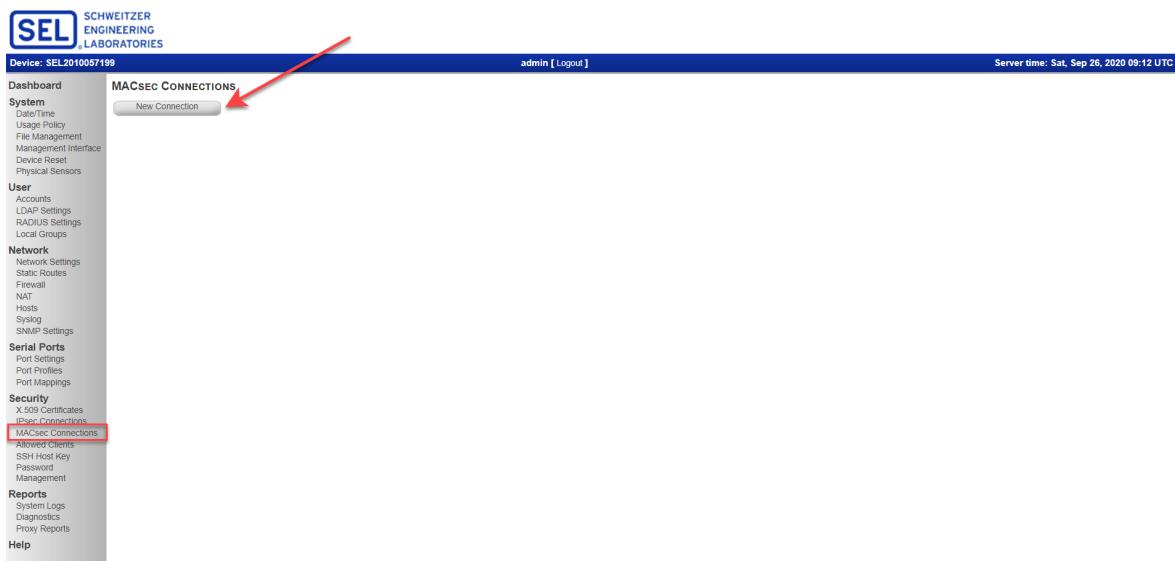


Figure 4.52 Adding a New MACsec Connection

- Step 4. Set the Commissioning Options in the dialog box that appears on the right side of the page.

- Select the interface to secure with MACsec. Note that:
 - > Only interfaces that are enabled can be selected.
 - > The use of an interface configured for VLANs, DHCP client, or as a member of a bridge is not currently supported.
 - > The selected interface is dedicated for MACsec traffic only.

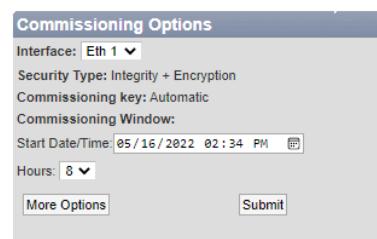


Figure 4.53 Commissioning Options

- Use the drop down menu to select a Commissioning Window start date and time. This can be selected via the date and time pop-up widget (shown in Figure 4.54).

NOTE: Some web browsers do not allow the date and time widget to pop up, requiring the user to type in the entry in the format defined by the SEL-3622, for example, 09/15/2021 03:29 PM for an SEL-3622 with a date/time format of MM/DD/YYYY hh:ss.

NOTE: The pairing window start date/time must be set to the current or a future time according to the time zone configured in the SEL-3622.

4.36 Job Done Examples

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

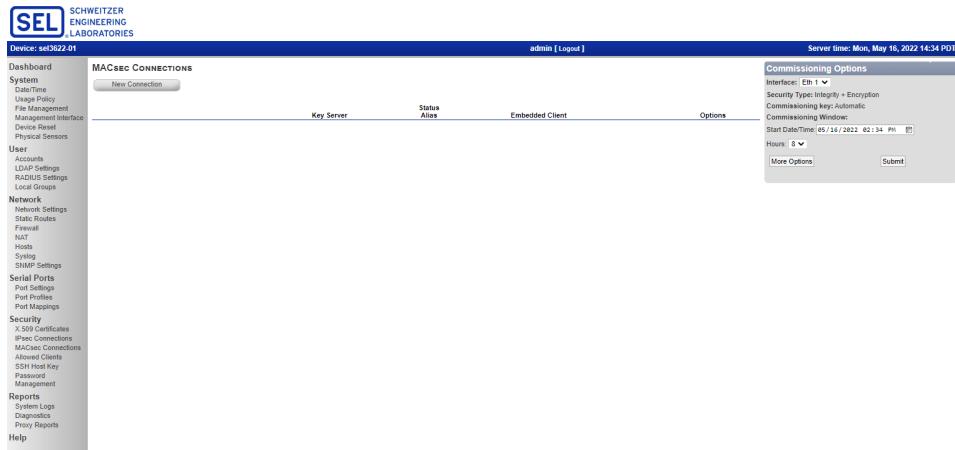


Figure 4.54 Select Commissioning Window Start Date/Time

- c. Select the duration of the commissioning window (Hours) by using the drop down menu.
- Step 5. Select **Submit** to save the settings. The More Options button is discussed further in *SEL-651RA Manual Commissioning Command Line Method* on page 4.41.



Figure 4.55 MACsec Connection Added

Note that the MACsec Connection information is updated after submitting the settings:

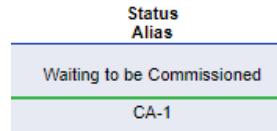
- Key Server displays the hardware MAC address of the local interface.



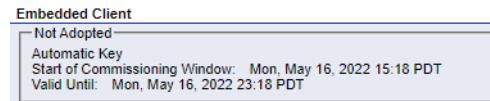
Figure 4.56 Key Server MAC Address

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

- Status displays Waiting to be Commissioned with the Alias name below it.

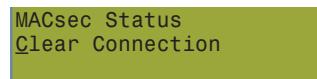
**Figure 4.57 MACsec Commissioning Status and Alias**

- Embedded Client indicates the Commissioning Adoption status in *Figure 4.58* (Not Adopted), key type (Automatic Key), Starting Commissioning Window (configured start time), and the commissioning Valid Until time.

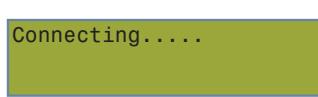
**Figure 4.58 Embedded Client Commissioning Status**

SEL-651RA Automatic Commissioning Front Panel Method

- Step 1. On the front panel of the SEL-651RA, navigate to **Status Submenu > Diag Status Menu >Diag Status Display** and scroll down to view the relay Firmware ID (FID). Verify that the FID is at least R105 or later.
- Step 2. If the firmware version is earlier than R105, update the firmware to R105 or later prior to continuing with these steps (see *Appendix B: Firmware Upgrade Instructions* in the SEL-651RA instruction manual).
- Step 3. If the SEL-651RA does not have an active MACsec connection, proceed to *Step 4*. Otherwise, navigate to the **Security Submenu > MACsec Submenu** and select the **Clear Connection** option on the front panel. To clear the MACsec connection, the user must enter in the 2AC access level password to confirm.

**Figure 4.59 Reset SEL-651RA MACsec Connection**

- Step 4. Navigate to the SEL-651RA front panel **Set>Show Menu > Port Submenu > Port 5 > Ethernet Port Settings** (Note: The user needs to enter the 2AC level password to change the following settings):
 - a. Configure **EPORTSEC** [default – N], change to **Y**.
 - b. Configure **MSECCKEY** [default-A for Auto], change to **A**.
 - c. Save settings changes.
- Step 5. The SEL-651RA front panel display shows the Connecting screen while it is attempting to commission a MACsec connection with the SEL-3622. The SEL-651RA shows this Connecting screen for up to a minute while searching for the SEL-3622.

**Figure 4.60 MACsec Commissioning Attempt**

NOTE: The SEL-651RA only shows the Connecting screen if the user has changed and saved the EPORTSEC setting from a N to a Y and if MSECCKEY is set to A for Automatic Commissioning Mode.

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

- Step 6. Once the SEL-651RA connects to the SEL-3622, the SEL-651RA displays the last 3 octets of the SEL-3622 MAC address on its front panel for the user to confirm the correct device is used in the MACsec Connectivity Association. The last 3 octets shown on the SEL-651RA front panel matches the 3 octets shown as the key server local interface of the SEL-3622 web interface. Press <Enter> to confirm.

```
Join CA? KS:...04:05:06
ESC=N; ENT=Y
```

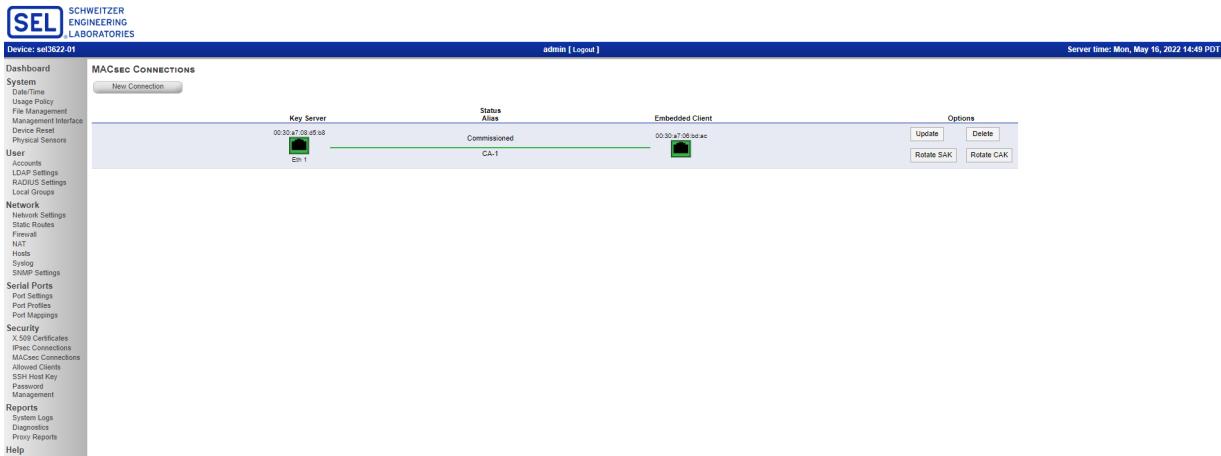
Figure 4.61 Confirm Commissioning With SEL-3622

- Step 7. When the MACsec Connection has been established, the SEL-651RA displays the MACsec commissioning success message as shown in *Figure 4.62*.

```
MACsec Commissioning
Successful
```

Figure 4.62 MACsec Commissioning Successful

- Step 8. Refresh the MACsec connections page on the SEL-3622 webpage and verify that the MACsec connection status is “Commissioned” (see *Figure 4.63*). Note that the MAC address shown under Embedded Client is the SEL-651RA MAC address.

**Figure 4.63 Commissioned Automatic MACsec Connection With SEL-3622**

You have now successfully commissioned the system by using the SEL-651RA Automatic Commissioning Front Panel Method.

SEL-651RA Automatic Commissioning Command Line Method

- Step 1. Refer to *Set up MACsec Automatic Commissioning on the SEL-3622* on page 4.35 to set up the SEL-3622 to commission MACsec with the Automatic Commissioning Key.
- Step 2. Log in to the **Command Line Interface (CLI)** of the SEL-651RA to verify that the FID in the version information is at least R105 or later.
- Step 3. If the firmware version is earlier than R105, update the firmware to R105 or later prior to continuing with these steps (see *Appendix B: Firmware Upgrade Instructions* in the SEL-651RA instruction manual).

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

Step 4. If the SEL-651RA does not have an active MACsec connection, proceed to *Step 5*. Otherwise, access the SEL-651RA from the command line and access the 2AC level. Type the **MCS C** command to clear the active MACsec connection.

```
=>>MCS C <Enter>
WARNING: This command will clear any existing MACsec Connectivity Association
and all associated keys. Traffic will no longer be secured.
Clear MACsec connection and clear all keys (Y/N)? Y <Enter>
Connectivity Association Cleared
=>>
```

Figure 4.64 MCS C Command Response

Step 5. From the 2AC level of the SEL-651RA command line, ensure that the Port 5 settings are set to **EPORTSEC = Y** and **MSECCKEY = A**.

If you need to update the settings on the SEL-651RA from the command line, enter the **SET P 5** command to access the Port 5 settings. Refer to *Figure 4.65* for an example command response.

```
=>>SET P 5 <Enter>
Port 5
Port Enable:
Enable Port(Y,N) EPORT := Y ? Y <Enter>

Ethernet Port Settings:
Enable Port Security(Y,N) EPORTSEC:= N ? Y <Enter>
MACsec Commissioning Key(A=Auto, M=Manual, S=Static) MSECCKEY:= A ? A <Enter>

Device IP Address(zzz.yyy.xxx.www)
IPADDR := 192.168.1.2
? END <Enter>

EPORT := Y EPORTSEC:= Y MSECCKEY:= A
IPADDR :=192.168.1.2
SUBNETM :=255.255.255.0
DEFRTR :=192.168.1.1
ETCPKA := Y
NETMODE := FAILOVER FTIME := 1.00 NETPORT := A
NET5ASPD:= AUTO NET5BSPD:= AUTO
ETELNET := Y MAXACC := C TPORT := 23
TCBAN :=TERMINAL SERVER
TIDLE := 30 AUTO := N FASTOP := Y
EFTPSEERV:= Y
FTPUSER :=FTPUSER
FTPCBAN :=FTP SERVER
FTPIDLE := 255
EHTTP := N
E61850 := Y EGSE := Y EMMSFS := Y
EDNP := 0
ESNTP := OFF

Save changes(Y/N)? Y <Enter>
Settings saved
=>>
```

Figure 4.65 SEL-651RA Port 5 Settings

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

NOTE: If the automatic initial commissioning process is activated (via settings change or front panel confirmation) the user must wait until the automatic process via the front panel has completed or failed. At the point of success or failure, the user can issue the **MCS A** command on the SEL-651RA.

- Step 6. From the command line of the SEL-651RA, type the **MCS A** command.
This opens the automatic commissioning window on the SEL-651RA.

=>>MCS A <Enter>

WARNING: This command should not be issued over the Ethernet link to be secured, unless the integrity of the cable can be verified. Failure to follow this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? Y <Enter>

Figure 4.66 MCS A Command

- Step 7. If the MACsec connection is successful, the command line interface of the SEL-651RA appears similar to *Figure 4.67*.

NOTE: Figure 4.67 also contains the SEL-651RA **SLR** command response after a successful MACsec Commissioning process. Note that for commissioning to succeed, a new CAK and SAK must be sent to the SEL-651RA (both CAK and SAK Rotation must be successful).

=>>MCS A <Enter>

WARNING: This command should not be issued over the Ethernet link to be secured, unless the integrity of the cable can be verified. Failure to follow this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? Y <Enter>

Listening for MACsec Key Agreement (MKA) Key Server Activity.

A Key Server (KS) was found at 00:30:a7:0c:92:70

Continue (Y/N)? Y <Enter>

Joining Connectivity Association.....

CAK Obtained Successfully from KS at 00:30:a7:08:d5:b8
SAK Obtained Successfully from KS at 00:30:a7:08:d5:b8
Secured Port 5

=>>SLR <Enter>

Serial Number: 1130390591

FEEDER 1	Date: 05/17/2022 Time: 00:01:31.219
STATION A	Time Source: internal

FID=SEL-651R-2-X700-V0-Z012003-D20220515 CID=CF9E

Date	Time	Tag	Severity	Facility	Message
05/17/2022	00:01:23.719	1	2	4	Commissioning Successful
05/17/2022	00:01:22.844	3	6	4	SAK Installation Successful
05/17/2022	00:01:22.844	1	2	4	MSOK=1,block non-secure comms
05/17/2022	00:01:22.843	0	2	4	MS_EANDI=1,encryption enabled
05/17/2022	00:01:21.790	3	5	4	Rx SAK from 00:30:a7:08:d5:b8
05/17/2022	00:01:17.640	3	6	4	CAK Installation Successful
05/17/2022	00:01:17.637	3	5	4	Rx CAK from 00:30:a7:08:d5:b8
05/17/2022	00:01:07.791	1	2	4	Commissioning in Progress
05/16/2022	23:56:22.862	1	2	4	SLR archive cleared

=>>

Figure 4.67 Successful MCS A Command With SLR Command Response

- Step 8. Refresh the SEL-3622 MACsec Connections page on the web interface to verify that the SEL-3622 has been added to a MACsec Connectivity Association with the SEL-651RA.

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

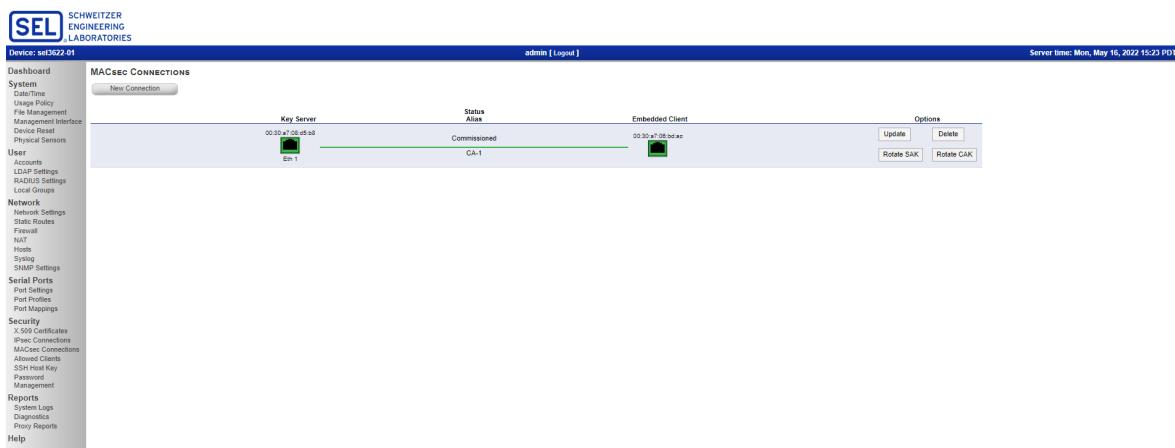


Figure 4.68 Successful SEL-3622 MACsec Connection Commissioning

You have now successfully commissioned the system by using the Automatic Commissioning Key and the Command Line of the SEL-651RA.

SEL-651RA Manual Commissioning Command Line Method

- Step 1. Perform *Step 1* through *Step 3* of *Set up MACsec Automatic Commissioning on the SEL-3622* on page 4.35. In *Step 4*, select the **More Options** button to expand the **Commissioning Options** selections. Select **Manual** for the **Commissioning Key**.
- Step 2. Select **Submit**. Once the webpage refreshes, the SEL-3622 randomly generates a manual key (128-bits). The key is shown in hexadecimal values with dashes to improve readability (see *Figure 4.70*).

Interface:	Eth 1
Alias:	CA-1
Security Type:	<input checked="" type="radio"/> Integrity + Encryption <input type="radio"/> Integrity Only
Commissioning key:	<input type="radio"/> Automatic <input checked="" type="radio"/> Manual
Commissioning Window:	Start Date/Time: 05/16/2022 03:37 PM Hours: 8
Maximum Key Lifetimes:	SAK Lifetime: 24 Hours CAK Lifetime: 168 Hours
<input type="button" value="Less Options"/> <input type="button" value="Submit"/>	

Figure 4.69 Manual Key Commissioning Option

4.42 Job Done Examples

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control



Figure 4.70 Generating a New MACsec Manual Key

NOTE: The randomly generated key needs to be entered into the SEL-651RA command line. The easiest way to proceed is to copy and paste the key directly from the SEL-3622 web interface to the SEL-651RA command line (see Step 6).

- Step 3. Once the random key has been generated, the SEL-3622 web interface displays the key under the Embedded Client section.

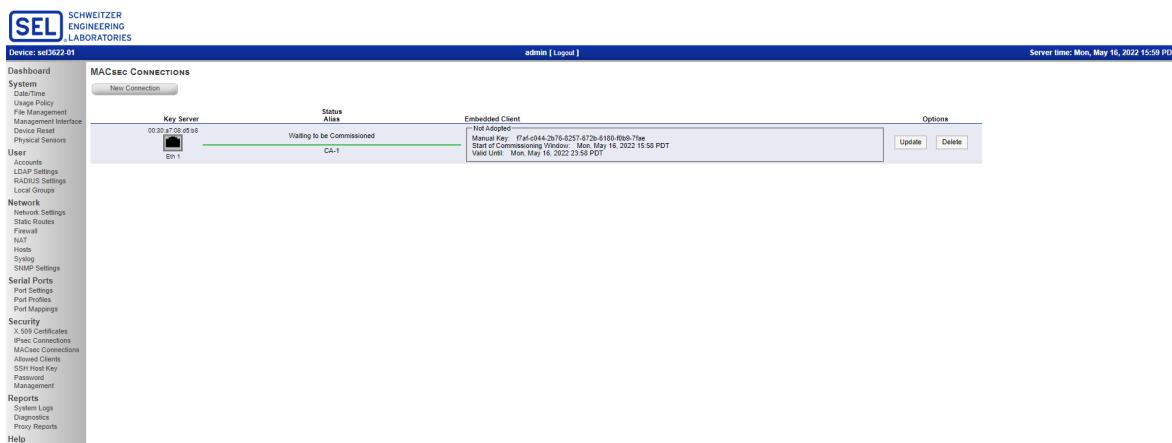


Figure 4.71 Manual MACsec Commissioning

IMPORTANT NOTE: If the SEL-3622 is power cycled during pairing, a new manual key is generated and displayed.

NOTE: If the user needs to update the settings on the SEL-651RA from the command line, enter the **SET P 5** command to access the Port 5 settings. Refer to Figure 4.65 for an example command response.

- Step 4. Inspect the Ethernet cable connecting the SEL-3622 to the SEL-651RA. If the cable cannot be physically inspected, ensure that these steps are done over a local serial or USB connection to eliminate undesired interception or manipulation of the messages. Note that the ultimate security of this connection depends on the integrity of this cable during commissioning.
- Step 5. From the command line of the SEL-651RA, ensure that the Port 5 settings are set to **EPORTSEC = Y** and **MSECCKEY = M**.
- Step 6. Copy the generated MACsec key from the SEL-3622 web interface.
- Step 7. Enter the **MCS M** command in the SEL-651RA terminal window to start the manual pairing method for the SEL-651RA.
 - Enter **<Y>** to agree with the warning prompt and continue with manual pairing.
 - Paste the **SEL-3622** MACsec key into the SEL-651RA terminal window when prompted.

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

```
=>>MCS M <Enter>

WARNING: This command should not be issued over the Ethernet link to be
secured, unless the integrity of the cable can be verified. Failure to follow
this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? Y <Enter>

Enter Connectivity Association Key (CAK), with or without dashes
? f7af-c044-2b76-8257-672b-6180-f0b9-7fae <Enter>

Listening for MACsec Key Agreement (MKA) Key Server Activity.

A Key Server (KS) was found at 00:30:a7:08:d5:b8

Continue (Y/N)? Y <Enter>
```

Figure 4.72 Command Line Manual MACsec Commissioning

The SEL-651RA displays the SEL-3622 Ethernet interface MAC address (see *Figure 4.72*).

Step 8. Enter **<Y>** to agree with the command response.

Step 9. When MACsec has been successfully commissioned, the SEL-651RA sends the following response (see *Figure 4.73*).

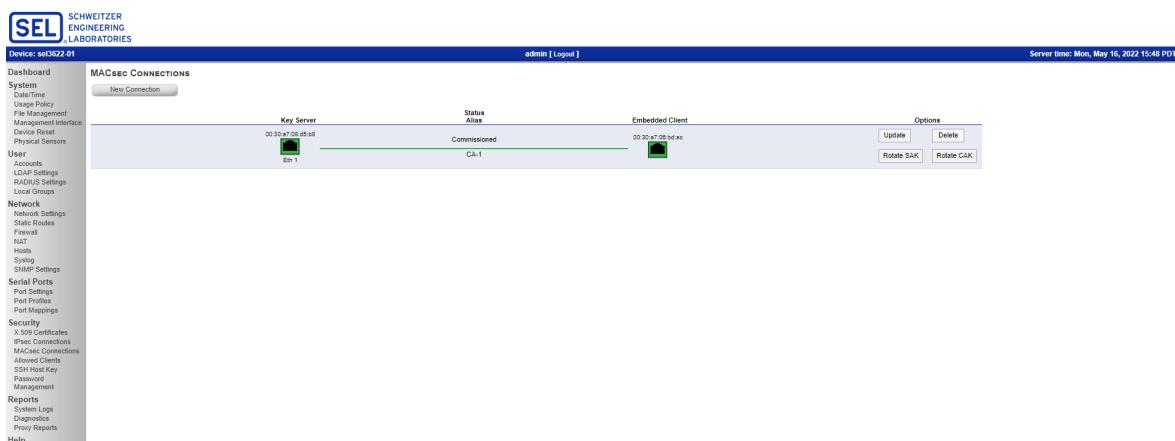
```
Joining Connectivity Association.....
CAK Obtained Successfully from KS at 00:30:a7:08:d5:b8
SAK Obtained Successfully from KS at 00:30:a7:08:d5:b8

Secured Port 5

=>>
```

Figure 4.73 MACsec Command Line Commissioning Successful

Step 10. Refresh the SEL-3622 web interface and verify that it is successfully paired to the SEL-651RA.

**Figure 4.74 MACsec Manual Commissioning SEL-3622 Pairing Successful**

You have now successfully commissioned the system by using the Manual Commissioning Command Line Method.

Troubleshooting MACsec Communications

If the SEL-651RA cannot establish a MACsec connection to the SEL-3622, the following sections can provide assistance in troubleshooting the connection. These SEL-651RA Relay Word bits can also provide initial insight as to the state of the device's MACsec connection:

- MSEN (MACsec is available for use) is asserted when the Port 5 setting EPORTSEC is enabled. This must be asserted in order to establish a MACsec connection.
- MSOK is asserted when MACsec is operational or a secure association has been established. Note that this bit can remain asserted even if the SEL-651RA is disconnected from the SEL-3622.

Troubleshooting Automatic Commissioning Front Panel Issues

Step 1. If the SEL-651RA cannot establish a MACsec connection to the SEL-3622, the front panel displays the message shown in *Figure 4.75*.

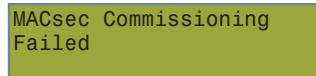


Figure 4.75 Front Panel MACsec Commissioning Failed

- Step 2. If MACsec commissioning fails, verify the physical integrity of the Ethernet cable between the SEL-3622 and the SEL-651RA.
- Step 3. At the 2AC level, navigate to the **SEL-651RA Front Panel Set/Show Menu > Port Submenu > Port 5 > Ethernet Port Settings** and verify that **EPORTSEC = Y** and **MSECCKEY = A**.
- Step 4. Connect to the SEL-3622 web interface and verify the following MACsec Commissioning options are correct:
 - a. Interface: Verify that the interface selected is the one connected to the SEL-651RA
 - b. Commissioning Key: Automatic
 - c. Commissioning Window: date/time and duration cover the current time period
- Step 5. Navigate to the SEL-3622 **Diagnostics** and **Syslog** pages to determine if the point where commissioning failed is identified. Refer to the SEL-651RA instruction manual for additional troubleshooting steps.
- Step 6. At the 2AC level, navigate to **SEL-651RA Front Panel Security > MACsec > Secure Port 5 > Open Commissioning Window**. This will re-open the commissioning window on the SEL-651R for the Automatic Commissioning Mode.

Troubleshooting Automatic Commissioning Command Line Issues

Step 1. In the event the SEL-651RA cannot pair, the following information is displayed on the command line:

```
>>>MCS A <Enter>

WARNING: This command should not be issued over the Ethernet link to be
secured, unless the integrity of the cable can be verified. Failure to follow
this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? Y <Enter>
Listening for MACsec Key Agreement (MKA) Key Server Activity.....
No Key Server (KS) was found
MACsec Commissioning Process Failed
```

Figure 4.76 MACsec Automatic Command Line Commissioning Failed

- Step 2. Enter the SEL-651RA **SLR** command to see more information on which step might have failed. Note that for commissioning to be successful, both CAK Rotation and SAK rotation must succeed.

```
=>>SLR <Enter>

Serial Number: 1130390591

FEEDER 1 Date: 05/17/2022 Time: 00:35:55.286
STATION A Time Source: internal

FID=SEL-651R-2-X700-V0-Z012003-D20220515 CID=CF9E

Date Time Tag Severity Facility Message
05/17/2022 00:35:49.198 1 2 4 Commissioning Failure
05/17/2022 00:35:29.153 1 2 4 Commissioning in Progress
05/17/2022 00:35:22.907 1 2 4 SLR archive cleared
```

Figure 4.77 MACsec SLR Command With Failure

- Step 3. Verify the physical integrity of the Ethernet cable between the SEL-3622 and the SEL-651RA.
- Step 4. Connect to the SEL-3622 web interface and verify the following MACsec Commissioning options are correct:
- Interface: Verify that the interface selected is the one connected to the SEL-651RA
 - Commissioning Key: Automatic
 - Commissioning Window: date/time and duration cover the current time period
- Step 5. Ensure that the Port 5 settings are set to **EPORTSEC = Y** and **MSECCKEY = A**.
- Step 6. Navigate to the SEL-3622 **Diagnostics** and **Syslog** pages to determine if the point where commissioning failed is identified. Refer to the SEL-651RA instruction manual for additional troubleshooting steps.

Troubleshooting Manual Commissioning Command Line Issues

- Step 1. If manual MACsec Commissioning fails, the SEL-651RA displays the response shown in *Figure 4.78*.

```
=>>MCS M <Enter>

WARNING: This command should not be issued over the Ethernet link to be
secured, unless the integrity of the cable can be verified. Failure to follow
this practice may result in compromised security.

Continue with MACsec Commissioning process (Y/N)? Y <Enter>

Enter Connectivity Association Key (CAK), with or without dashes
? 4eee-11a8-5d91-9c8f-c515-52af-5f5a-2915 <Enter>

Listening for MACsec Key Agreement (MKA) Key Server Activity..

A Key Server (KS) was found at 00:30:a7:0c:92:70

Continue (Y/N)? N <Enter>

MACsec Commissioning Process Failed

=>>
```

Figure 4.78 MACsec Commissioning Failed

- Step 2. Issue the **SLR** command on the SEL-651RA terminal window to determine which step(s) in the MACsec commissioning were not successful.
- Step 3. Verify the physical integrity of the Ethernet cable between the SEL-3622 and the SEL-651RA.

Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control

- Step 4. Open the SEL-3622 web interface and copy the MACsec manual commissioning key (under **Embedded Client**).
- Step 5. Re-enter the connection information by executing the **MCS M** command on the SEL-651RA terminal. Paste the SEL-3622 MACsec manual commissioning key in the SEL-651RA terminal when prompted.
- Step 6. See *Figure 4.79* for an example of an **SLR** command response that shows successful commissioning with encryption enabled (most recent events are at the top).

```
=>>SLR <Enter>
Serial Number: 1130390591
FEEDER 1 Date: 11/23/2021 Time: 10:17:27.489
STATION A Time Source: internal
FEEDER 1 Date: 05/17/2022 Time: 00:32:40.555
STATION A Time Source: internal
FID=SEL-651R-2-X700-V0-Z012003-D20220515 CID=CF9E
Date Time Tag Severity Facility Message
05/17/2022 00:32:35.236 3 6 4 SAK Installation Successful
05/17/2022 00:32:34.140 3 5 4 Rx SAK from 00:30:a7:08:d5:b8
05/17/2022 00:26:36.297 1 2 4 Commissioning Successful
05/17/2022 00:26:36.171 3 6 4 SAK Installation Successful
05/17/2022 00:26:36.171 1 2 4 MSOK=1,block non-secure comms
05/17/2022 00:26:36.168 0 2 4 MS_EANDI=1,encryption enabled
05/17/2022 00:26:35.114 3 5 4 Rx SAK from 00:30:a7:08:d5:b8
05/17/2022 00:26:32.018 3 6 4 CAK Installation Successful
05/17/2022 00:26:32.017 3 5 4 Rx CAK from 00:30:a7:08:d5:b8
05/17/2022 00:26:23.631 1 2 4 Commissioning in Progress
```

Figure 4.79 Successful SLR Command Response

Refer to the SEL-651RA instruction manual for additional troubleshooting steps.

S E C T I O N 5

Settings and Commands

Introduction

This section explains the settings and commands of the SEL-3610, SEL-3620, and SEL-3622. Except as otherwise noted, references to the SEL-3620 refer also to the SEL-3622.

- *Commissioning Page* on page 5.2
- *System* on page 5.4
 - *Date/Time*
 - *Usage Policy*
 - *File Management*
 - *Management Interface*
 - *Device Reset*
 - *Physical Sensors*
- *Network* on page 5.18
 - *Network Settings*
 - *Disable Unused Ports*
 - *Static Routes*
 - *Syslog*
 - *SNMP*
- *Serial Ports* on page 5.33
 - *Serial Port Settings*
 - *Serial Port Profiles*
 - *Bit Based Processing Mode*
 - *Port Mappings*
- *Security* on page 5.49
 - *X.509 Certificates*
 - *Allowed Clients*
 - *SSH Protocol*
 - *SSH Host Key*
 - *exe-GUARD*
- *Reports* on page 5.59
 - *System Logs*
 - *Diagnostics*

Commissioning Page

The device commissioning page is at the device default IP address: 192.168.1.2 for the front Ethernet port or https://172.29.131.1 for the USB-B port. For you to access the commissioning page, the device must be unconfigured. The device is in the unconfigured state when you receive it from the factory and after a factory-default reset. To connect to the device in the unconfigured state, open your preferred web browser and enter **https://192.168.1.2** for the front Ethernet port or **https://172.29.131.1** for the USB-B port into the address bar.

NOTE: You must enter the HTTPS prefix in the address bar to specify communication to port 443. Without the HTTPS prefix, your web browser will default to communicating to port 80 and the device will deny connection attempts.

The device authenticates itself to your web browser with a self-signed X.509 certificate. This is necessary to communicate over HTTPS. The self-signed certificate will likely cause your web browser to generate a security alert, similar to the one in *Figure 5.1*. This occurs because the web browser considers self-signed X.509 certificates nonsecure. Such alerts are unavoidable during commissioning, but you can prevent a subsequent alert of this type by adding a security exception to your browser. Your web browser will provide instructions to create the security exception. By generating or installing a new certificate after commissioning, you can eliminate this security alert.

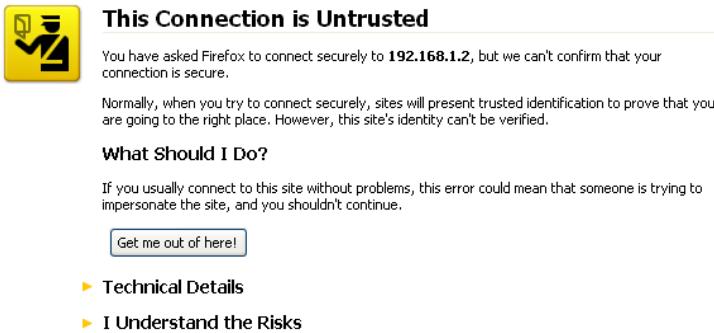


Figure 5.1 Security Exception

You must create an administrative-level user account to commission the device. The device does not contain any accounts in the unconfigured state. This ensures that only you have the knowledge necessary to access this device. The commissioning page (*Figure 5.2*) provides username and password boxes to create the initial administrative account. These are the only boxes you must complete during commissioning.

Figure 5.2 Commissioning Page

The commissioning page contains optional boxes in which you can enter global network configurations for the device. Completion of these boxes is unnecessary to access the management interface, but doing so can prevent the need for later configuration changes. *Table 5.1* shows the configurable boxes on the device commissioning page, acceptable values for these boxes, and brief box descriptions. For more detailed information on each of the network configuration boxes, see *Network Settings* on page 5.18.

Table 5.1 Commissioning Settings

Name	Values	Description
Username	As many as 128 characters	The username for the initial administrative-level account on this system. All usernames on this system must be unique.
Password	8 to 128 characters	Passwords must consist of at least eight characters and have characters from each of the following character sets: lowercase letters, uppercase letters, digits, and nonalphanumeric characters. Passwords must be entered twice to ensure correctness.
Hostname	1 to 63 characters	The unique name identifying this device on the domain. The Hostname must begin with a letter and can contain letters, digits, and hyphen (-). This defaults to the device serial number.
Default Ethernet Port	www.xxx.yyy.zzz/aa	A unique IP address used to communicate to the front Ethernet port of this device. The protected address is the address accessible by the internal (trusted) network. Class D and Class E addresses are not allowed. This defaults to 192.168.1.2/24.
Domain Name	As many as 253 characters	Defines the domain of which this device is a member. You can consider the domain the network to which this device is attached. The domain name must be of the form [X.]X.Y where X follows the hostname rules and Y is from two to six characters in length and begins with a letter (optional).
Default Router	www.xxx.yyy.zzz/aa	Defines the IP address of the default router by which packets transfer to another network. Class D and Class E addresses are not allowed. If this is left blank and a packet is destined for another network, the device will drop that packet (optional).
VLAN	0–4095	Identifies the VLAN to associate with the protected interface. If left blank, this device will not process VLAN tags on that interface (optional).

System

The System link on the navigation panel opens the System Settings Description page. This page gives an overview of the Date/Time, Usage Policy, File Management, Management Interface, and Device Reset functions of the device.

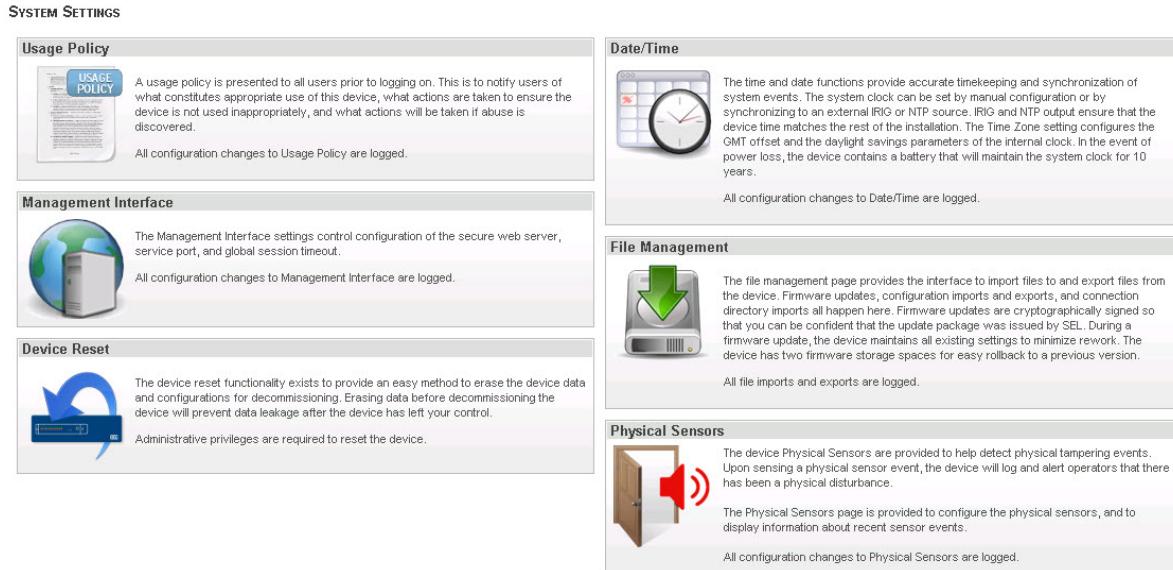


Figure 5.3 System Settings

Date/Time

The time and date functions of the device allow for accurate timekeeping for all internally generated system events. The device can synchronize its internal clock to an IRIG-B or Network Time Protocol (NTP) time from an Ethernet source, and use these data to time-stamp all internally generated logs and system events.

Another powerful feature the device provides is time distribution. The device can distribute IRIG-B000 (Even Parity) from its BNC output port (not available on the SEL-3622) and all 17 serial ports (four on the SEL-3622), and it can simultaneously transmit NTP time from any enabled Ethernet interface.

The device is flexible in how it supplies IRIG-B and NTP. This flexibility allows the device to use a satellite-synchronized clock as an IRIG-B source, and in turn supply NTP to all networked devices. Conversely, the device can synchronize with a remote or local NTP server for high-stratum NTP data and then supply IRIG-B to all physically connected devices. If an event disrupts the IRIG-B or NTP time input, the device will continue to supply IRIG-B and/or NTP time from its internal clock. In the event of power loss, the device contains a battery that will maintain its internal clock for ten years.

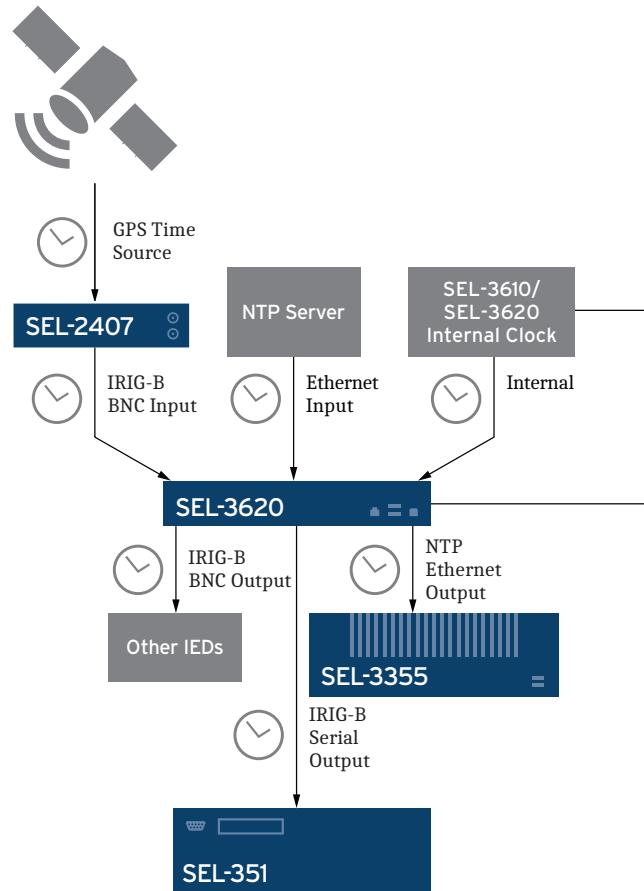


Figure 5.4 Time Synchronization With NTP and/or IRIG-B

From the Date/Time configuration page, you can manually configure date/time and time zone settings on the device, as well as configure time input and output for either IRIG-B or NTP. You can configure only one time source at any one time: IRIG, NTP, or Local. The NTP input to the device is disabled when you set IRIG as the time source. When NTP or IRIG inputs are enabled, the device ignores all manual updates to the internal system clock. The device logs all configuration changes to the system date or time.

The screenshot shows the 'DATE/TIME' configuration page. On the left, under 'Date/Time Settings', there is a dropdown menu for 'Time Zone' set to 'US/Pacific'. Below it are two input fields: 'Date: [] (D/M/Y)' and 'Time: [] (HH:MM:SS)'. A note below these fields states: 'This device provides an option for manually setting the system's date and time. Manual setting of the date and time is not as accurate as an IRIG signal and should only be used in the absence of an IRIG-B signal. IRIG-B output is not available when the time is set manually.' At the bottom of this section is a 'Update' button. On the right, under 'Synchronization Settings', there is a radio button group for 'Time Source': 'IRIG' (unselected), 'NTP' (unselected), and 'LOCAL' (selected). Below this are two input fields: 'Input IRIG Offset: []' and 'Output IRIG Offset: []'. A note states: 'This device provides for an IRIG offset function in order to maintain a specified difference between the system's internal clock and the received IRIG-B time signal. The range of this offset is -1439 to 1439 minutes.' Below these are two checkboxes: 'Enable IRIG output on this device' (unchecked) and 'Enable NTP output on this device' (unchecked). Under 'NTP Server', there are three sets of input fields for 'NTP Server 1', 'NTP Server 2', and 'NTP Server 3', each consisting of four input boxes. A note for 'NTP Stratum' says: 'NTP Stratum: [10] Range (1-15)'. At the bottom is a 'Set Time Settings' button.

Figure 5.5 Date/Time Configuration Page

Manually Updating Date/Time

The device provides an extensive time zone list to allow you to select the time zone appropriate for your location. Identification of many of these time zones is according to cities that lie in those zones, while common time zone names, such as Coordinated Universal Time (UTC), identify others. Time zone selection is important in how the device determines daylight-saving adjustments. To select a time zone, find the appropriate time zone entry in the dropdown list labeled **Time Zone**, and select **Update**. The list arranges time zones in alphabetical order and by region.

In installations where IRIG-B or NTP sources are unavailable, you will need to manually enter device date and time settings. Enter the current date and time in the respective boxes and formats indicated, and select **Update**.

This is a zoomed-in view of the 'Date/Time Settings' dialog box. It shows the 'Time Zone' dropdown set to 'US/Pacific' and the note about manual time setting. Below are the 'Date:' and 'Time:' input fields. A note below them states: 'This device provides an option for manually setting the system's date and time. Manual setting of the date and time is not as accurate as an IRIG signal and should only be used in the absence of an IRIG-B signal. IRIG-B output is not available when the time is set manually.' At the bottom is a 'Update' button.

Figure 5.6 Manual Time Input

IRIG-B

When connected to an IRIG-B source, the device time system compares its internal clock against the IRIG signal once per second. If the difference is less than 5 seconds, it gradually adjusts the internal clock until it is back in alignment. If the difference is greater than 5 seconds, it immediately adjusts the internal clock to match the IRIG-B time.

To enable IRIG-B input functionality, ensure the physical connection of a demodulated IRIG-B source to the front-panel connector of the SEL-3622, or of a modulated or demodulated IRIG-B source to the IRIG-B BNC Input port on the rear of the SEL-3610/SEL-3620. Select **IRIG** as the time source, and select **Set Time Settings**. Ensure that **Enable IRIG output on this device** is selected. The device can automatically select between IRIG-B000 and IRIG-B002 formats, and between EVEN or ODD parity for IRIG-B000.

When you select **Enable IRIG output on this device**, the device supplies demodulated IRIG-B000 (Even Parity) to all serial ports and the IRIG-B Output BNC port. The device sets IRIG-B output signal quality bits according to *Table 5.2*.

NOTE: The device does not synchronize its own clock to the input IRIG signal unless time quality is <1 microseconds (TQ4). If you receive an error when selecting Sync Now, check your IRIG source time quality.

Table 5.2 IRIG-B Output Quality Settings

Input Source	IRIG-B Output Quality (TQ)
IRIG-B	Same as input
NTP	6
Local	7

The device provides an IRIG Offset to maintain a specific difference between the system internal clock and the IRIG-B time signal the device receives. You can set this IRIG Offset to between -1439 and +1439 minutes. This range corresponds to ±23 hours 59 minutes.

The Output IRIG Offset is additive to the Input IRIG Offset. If you apply an Input IRIG Offset of 180 minutes, and you then configure an Output IRIG Offset of -60 minutes, all downstream devices will see a cumulative 120-minute offset from the time source entering the device.

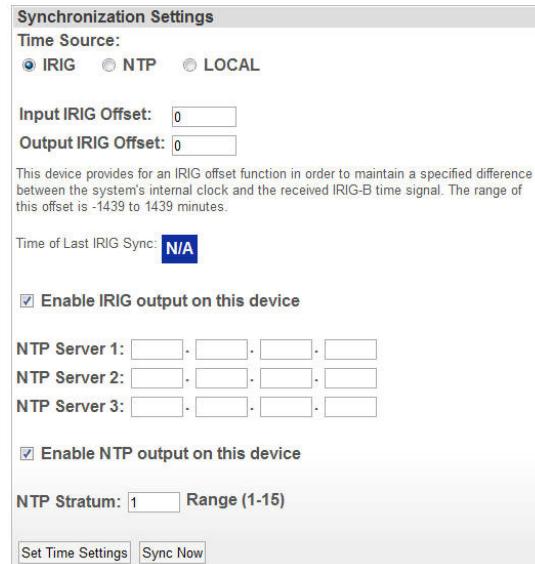


Figure 5.7 Time Synchronization Settings

Network Time Protocol

NTP is a method for synchronizing computer system clocks over packet-switched, variable-latency data networks such as Ethernet. NTP uses UDP on Port 123 as its transport layer. NTPv4 typically maintains accuracies of 10 ms across public networks and 200 µs or better in private networks under ideal conditions.

NTP uses a hierarchical, layered “stratum” system of clock source levels. Stratum numbering begins with zero at the top and increments with layers from the reference clock. The stratum scheme exists to prevent cyclical dependencies in the hierarchy. A lower stratum number for the NTP source does not necessarily mean it is more accurate. The number delineates how many computer layers separate that information from a stratum 0 clock source. NTP supports 16 strata.

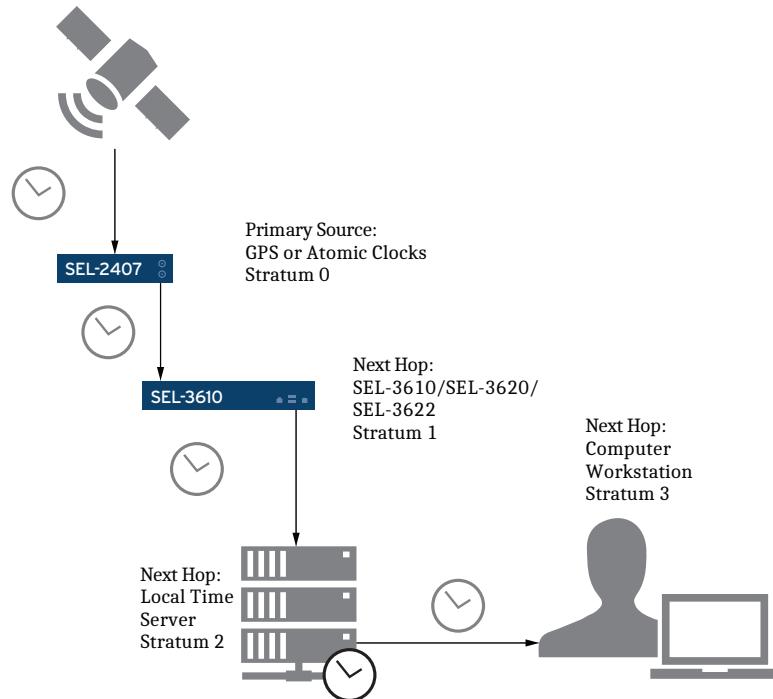


Figure 5.8 NTP Stratum Levels

To enable NTP input to the device, ensure availability of an NTP server on the Ethernet network to which you have connected the device. You must select **Time Source** as NTP and configure the NTP server settings according to the parameters in *Table 5.3*. Then select **Set Time Settings**.

Table 5.3 NTP Server Settings

Name	Values	Description
NTP Servers 1, 2, 3	www.xxx.yyy.zzz	Defines the IP address of the primary NTP server to which the local time will synchronize. Class D and E range IP addresses are not allowed.

NOTE: The device ignores the user-configured NTP stratum level when the input source is IRIG-B or NTP.

NOTE: To ensure downstream NTP devices will synchronize to the local clock of the device, set the NTP stratum to 7 or lower.

To enable NTP output, select the **Enable NTP output on this device** check box. When you select this box, the device supplies NTP from all enabled Ethernet ports. Settings for the output NTP stratum level are according to *Table 5.3*.

Table 5.4 NTP Output Stratum Setting

Input Source	NTP Output Stratum
IRIG-B	Output stratum is 1
NTP	Output stratum is 1 plus the input stratum level
Local	You can configure the output stratum to be at any level from 1 to 15

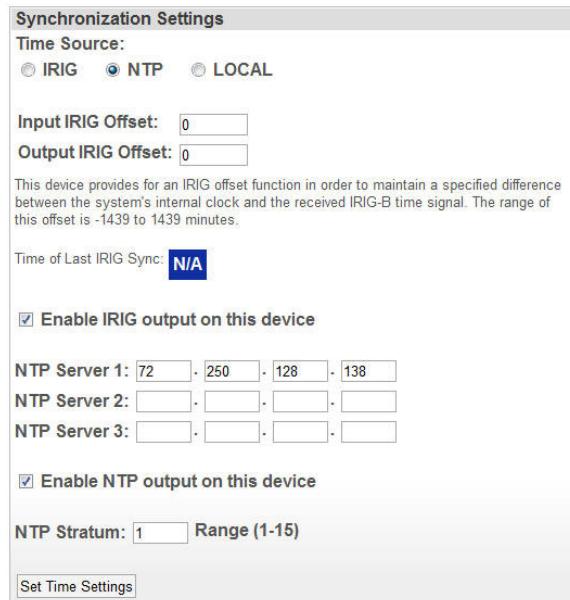


Figure 5.9 NTP Synchronization Settings

Usage Policy

The device login page displays a usage policy that notifies all users about what constitutes appropriate use of this device, actions to ensure appropriate use, and actions for any abuse. The usage policy is as follows:

This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such activity to law enforcement officials.

You can customize this usage policy to include any message consisting of as many as 4096 characters. Select the **Usage Policy** link from the navigation panel to modify this policy.

Only an administrative user can perform changes to the usage policy, and the device logs all policy configuration changes.

File Management

From the File Management configuration page, you can upload new device firmware and integrate connection directories (SEL-3620/SEL-3622 only). You can also import new system configuration files and export current configuration files. This feature is useful for commissioning large numbers of devices with the same master configuration file or for backing up configuration files for disaster recovery scenarios. Administrator privileges are necessary for any file import (upload), export, or generation operations. The device logs all file operations.

FILE MANAGEMENT

IMPORTANT: If you select Firmware Update, the system restarts as part of the upgrade process.

[File Upload](#) [Connection Directory](#) [System Settings](#) [Single File Backup](#)

File Upload

Select the appropriate radio button for the type of file you would like to import. Select Browse and choose the file to upload. For system settings uploads, enter the password associated with the selected configuration file. When the correct file has been selected, click Upload File to begin the upload and install process. The message bar below will notify you of important messages during the upload and install process.

Warning: a system reboot will be performed as part of any file management task.

Firmware Update Connection Directory System Settings Backup File

Choose a file to upload: [Choose File](#) **No file chosen**

[Upload File](#)

Figure 5.10 File Management Window

The Firmware Version window displays the current and previous firmware versions of the device. You can upload later firmware versions or revert to previous firmware versions should you need to do so. If there is no previous firmware version, the **Revert** button does not display. To learn more about how to configure firmware updates, see *Appendix B: Firmware Upgrade Instructions*.

Firmware Version

These are the current and previous firmware versions currently stored on the device. To make the previous firmware active, select the **Revert** button.

If there is no previous version the **Revert** button will be hidden.

Current Firmware Version:	Previous Firmware Version:	Action:
X125	X124	Revert

Figure 5.11 Firmware Version Window

In the Connection Directory (SEL-3620 only) window, you can upload new connection directories with QuickSet for scripted IED management. When a connection directory is loaded on the device, the File Management page displays the SHA1 hash of the presently installed directory. To learn more about connection directories, see *Section 6: SEL-3620 and SEL-3622 Security Services*.

Connection Directory

Use the SEL-5030 AcSElerator QuickSet software to generate the connection directory for use in the SEL-3620 Ethernet Security Gateway.

SHA1 hash of currently installed connection directory (N/A if no installed directory):

N/A

Figure 5.12 Connection Directory Window

NOTE: The device will only accept a settings file generated from the same firmware version.

You can import new system configuration files and export current system configuration files in the System Settings window. There are two types of system settings files that can be exported, full system settings and syslog settings. The syslog settings export will only export the settings configured on the Syslog page. This allows for easy replication of the syslog settings between SEL-3610, SEL-3620, and SEL-3622 devices without affecting other settings on the device. When a settings file is imported, the unit only modifies the settings that are different from the current configuration. To ensure that there have been no changes to configuration files, you can generate SHA1 checksums for configuration files presently stored on the device by selecting **Generate** in the System Settings window.

The device encrypts all settings files and requires that you enter a password to generate the settings file. This password must be at least eight characters long and use a combination of uppercase and lowercase letters, numbers, and special characters. Note that the hash value shown on the webpage is for the settings file. Because the file is encrypted when it is exported, the resulting file will have a different hash value. After uploading a new settings file, the device requires you to log in again. After logging in, restart the device via the Diagnostics webpage to ensure that system settings, such as hostname, are properly loaded.

To export a generated system settings file, enter the password for the settings file in the System Settings window, select **Generate**, **Type**, and then **Export**. Download the SystemSetting.bkp file. To upload (import to the device) a settings file, select **System Settings** in the File Management window, choose the SystemSettings.bkp file, enter the password of the file, then select **Upload File**.

NOTE: The Export function includes sensitive settings information. Encryption of the settings file of the device prevents unauthorized individuals from reading this information.

NOTE: To prevent issues, do not have more than one user at a time perform this function. It can cause an invalid file.

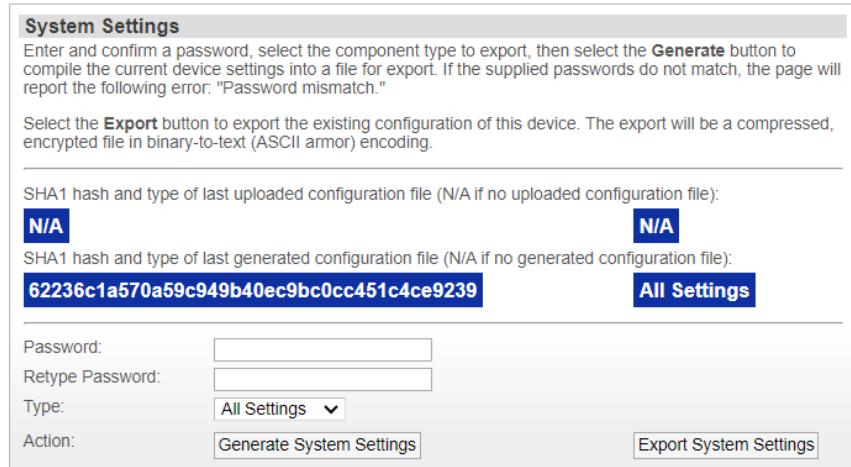


Figure 5.13 System Settings

The Single File Backup window allows you to generate and upload single-backup files. These files combine the connection directory, passwords, and configuration files into a single file to simplify backup and restoration.

To export a generated single-file backup, enter the password for the single-file backup file in the window and select **Generate Backup File**, then **Export Backup File**. Download the Hostname_FWVersion_Systembackup_Date.bkp file. To upload the single-file backup, select **Single File Backup**, choose the Hostname_FWVersion_Systembackup_Date.bkp file, enter the password of the file, and select **Upload File**.

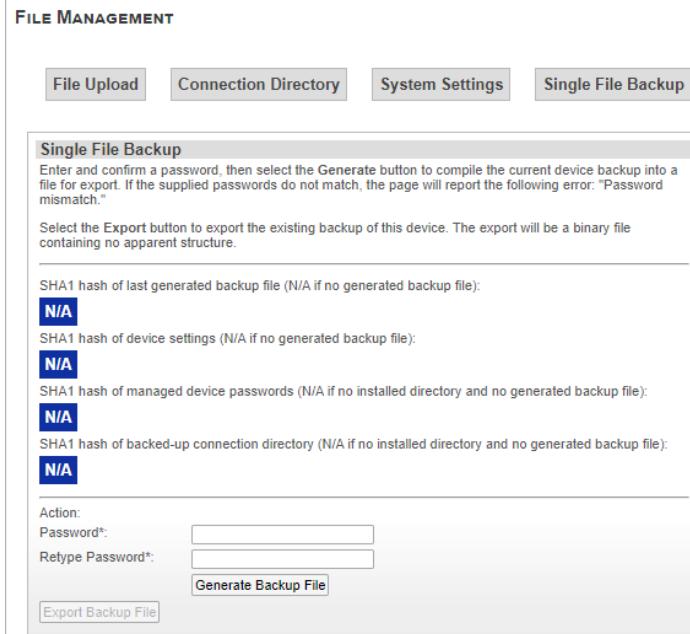


Figure 5.14 Single File Backup Window

The Messages window displays information about system setting file generation and the status of file imports, firmware upgrades, or reversions. The device logs all file management tasks.

Management Interface

The management interface section provides settings for both the web interface and the service-port interface (*Figure 5.15*). The web server communicates via HTTPS to allow use from any web browser without the need for additional software. The web server has user-configurable settings for local network addresses, the communications port number, and an X.509 certificate. The service port interface is accessible via SSH protocol and is disabled by default. A user can enable the service port and change its communications port number.

The device logs all configuration changes.

MANAGEMENT INTERFACE SETTINGS

Settings	Global Settings	Management Interface Address	
Web Server Port: <input type="text" value="443"/>	Global Session Timeout: <input type="text" value="60"/> This device terminates user sessions after the given number of minutes of inactivity. The valid range is 1-60 minutes.	Network Addresses: <input type="button" value="None"/> <input type="button" value="Add"/> Listed above are the local device addresses that will accept new user management sessions. Please select your desired address and click Add.	
This device's secure user management uses Hypertext Transfer Protocol Secure (HTTPS). This device accepts HTTPS connections only and will reject all HTTP connection requests. HTTPS connects on Port 443 by default. This can be set to any port between 1 and 65535.	This setting also applies to port mapping groups. Changing this setting will close existing port mapping connections and force users to reconnect.	To add or edit a device management address please navigate to the Network Settings page.	
X.509 Certificate: <input type="button" value="Default_Web_Cert"/>	Service Port <input checked="" type="checkbox"/> Enabled Port: <input type="text" value="1022"/> The service port is an SSH SELASCII interface on the specified port of the management interface. This can be set to any unused port between 1 and 65535.		
Note: Only valid X.509 certificates will appear in the drop down box. If an expected certificate does not appear in the drop down box, verify that the current system date and time is set correctly and falls within the validity period of the certificate.			
<input type="button" value="Set Configuration"/>			
Management Interface Addresses			
Alias	IP	VLAN	Options
LAN	192.168.10.21/24	10	<input type="button" value="Delete"/>
NATIVE	192.168.1.21/24		<input type="button" value="Delete"/>

Figure 5.15 Management Interface

Management Interface Web Server

The web server listens to a TCP port for incoming connection requests. The default port number, and the standard port number for HTTPS connections, is 443. To change the port number, enter the new port number in the box labeled **Port**, and select **Set Configuration**.

HTTPS connections require authentication to confirm that the server with which you are communicating is correct. Such authentication occurs through the use of X.509 certificates. By default, the device has a self-signed X.509 certificate that can cause your web browser to issue a security alert. Before you can continue, you will need to create a security exception in your web browser.

To prevent this security alert from appearing, install a certificate authority (CA)-signed X.509 certificate on your web browser and set this as the default Web Server Certificate.

You can select any presently installed X.509 certificate for the Web Server Certificate. Select from the X.509 dropdown list the certificate you want, and select **Set Configuration**.

For more information on X.509 certificates, see *Appendix K: X.509*.

The device web server has a default time-out of 10 minutes (configurable via the Global Session Timeout option). If no activity from a logged-on account is seen within this time frame, the server closes the user's session. If this happens, no more work can be done until the user logs back in by providing credentials.

The Global Session Timeout is a configurable value between 1 and 60 minutes. It may be necessary in some installations to temporarily set the time-out value to 60 minutes to successfully upload a large file, such as a firmware update, over a slow connection link.

The Global Session Timeout applies to all users and all account types on the device, including web UI sessions and port mapping connections.

At the bottom of the File Management page is a list of network addresses that you can use to communicate with the device web server and service port. By default, this list includes the addresses associated with the default Ethernet and USB-B interfaces. To add more addresses, select the appropriate address from the dropdown list labeled **Network Address**. This dropdown list is populated with the addresses you have assigned to configured ports. If the address you want is not in the list, you will need to configure one of your network ports with that address. The list will display the new address when you return to this page.

NOTE: If your network routes traffic for the management interface to a different physical interface, the interface will still be accessible. To prevent unauthorized hosts from being able to contact the management interface, define all authorized hosts on the Allowed Clients page.

Table 5.5 Web Server Settings

Setting	Values	Default Value
Port	1–65535	443
Global Session Timeout	1–60	10
X.509 Certificate	Any installed X.509 certificate	Default_Web_Cert
Network Addresses	Any configured device interfaces	192.168.1.2/24

Management Interface Service Port

The Service Port is available in firmware versions R203 and later and currently allows an Administrative user to view a read-only version of the current device settings and generate a hash value of those settings. Users of any access level may retrieve device information via the **ID** command. The interface is meant to allow a user to quickly verify and/or troubleshoot device settings, and also to allow for automated scripts to perform continual settings baseline analysis. All user-editable data can be viewed in the Service Port interface. For security and confidentiality purposes, the Service Port is accessible via SSH only. The Service Port does not expose the private portion of asymmetric key pairs, such as X.509 certificates or SSH signatures.

Table 5.6 Service Port Settings

Setting	Values	Default Value
Enabled (check box)	Checked/Unchecked	Unchecked
Port	1–65535	None

The Service Port can have as many as 10 active connections at one time. *Table 5.7* shows the commands available on the Service Port.

Table 5.7 Service Port Commands (Sheet 1 of 2)

Command	Example	Description
ID	**id	Displays the device Firmware ID String (FID), Hostname, Device Code, MOT Part Number, Serial Number, Config Number, and Special Option Number
SHOW	**sho	Displays all current device settings except for private asymmetric keys
EXIT	**exit	Exits the Service Port

Table 5.7 Service Port Commands (Sheet 2 of 2)

Command	Example	Description
HELP	**hel	Displays available commands
HASH	**has	Displays a string representing the current state of the settings on the device, currently managed device passwords, and the currently installed connection directory ^a

^a The SEL-3610 does not support password management so will not display a hash for managed passwords or the connection directory.

Device Reset

The device provides a Factory-Default Reset function to restore the unit to its factory configuration. You should only use this feature when you decommission the device. You will need administrative privileges to activate the reset command.

Factory-Default Reset erases the device log files and is a potential avenue for an attacker wanting to disguise unauthorized activity. To prevent such activity, you should configure the device to forward all log messages to an external Syslog server. This also ensures that logs are retained during decommissioning.

Factory-Default Reset removes all user-configurable settings from both firmware partitions and returns them to factory defaults. After a Factory-Default Reset, you can access the device at the default address of <https://192.168.1.2> on the front Ethernet port or <https://172.29.131.1> for the USB-B port.

Physical Sensors

The device physical sensors provide notification of changes in the security gateway's physical environment with respect to movement, light levels, and an external binary sensor such as a door contact. The combination of these three sensors can provide notification of intruders to your secured areas (such as recloser control cabinets) via the Syslog Protocol, SNMP, and the alarm output contact.

Use the Physical Sensors page to configure the physical sensors and also to view recent events.

The device logs all configuration changes to the physical sensor settings.

The SEL-3622 supports all the physical sensors. The SEL-3610 and SEL-3620 support only the input contact.

At the top of the Physical Sensor page are the Global Settings options for the physical sensors. This is where you can enable or disable all of the Physical settings at once. The **Global Settings Enabled** check box must be selected for the device to receive any notifications from any of the physical sensors. By default, the Physical Sensors are globally disabled.

You must select **Submit** at the bottom of the page to save settings changes to the Physical Sensors Global Settings.

NOTE: The SEL-3622 supports all the physical sensors. The SEL-3610 and SEL-3620 support only the input contact.

Input Contact

The Input Contact is available on the SEL-3610, SEL-3620, and the SEL-3622. The input contact receives a trigger from an external sensor such as a door contact. When a state change occurs in the external sensor, the device generates and sends the proper notification via Syslog and SNMP Trap. It then pulses the alarm

contact and logs the event on this page. For input contact wiring instructions, see the discussion of discrete input connections in Section 1 of the instruction manual for the device you have.

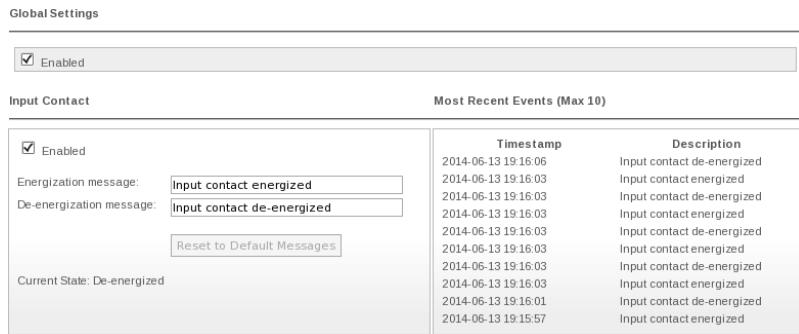


Figure 5.16 Input Contact Settings and Recent Events

See *Table 5.8* for the Input Contact Settings.

Table 5.8 Input Contact Settings

Setting	Values	Default Value
Enabled	Check box	Selected
Energization Message	Any string (as many as 128 characters)	Input contact energized
De-energization Message	Any string (as many as 128 characters)	Input contact de-energized

SEL-3622 Light Sensor

The light sensor is available on the SEL-3622, and its aperture is located on the front panel of the device. Changes in orientation of the SEL-3622 with respect to light sources can significantly affect the behavior of the light sensor. For best results, the light sensor should be oriented towards the light source to be detected or towards the area in which movement needs to be detected (see the circle in *Figure 5.17* for the location of the light sensor). The light sensor has three sensitivity levels: low, medium, and high.



Figure 5.17 Light Sensor

The three different sensitivity levels are designed for different use cases. The high sensitivity level is designed for applications where the SEL-3622 is installed in a normally dark environment, such as a recloser control cabinet, for which light level changes you want to detect may be very slight. If excessive LED flickering within the cabinet causes false positives, a medium sensitivity level should be used instead.

The medium sensitivity level is designed for situations where the SEL-3622 is installed in a normally dark environment that has less consistent light levels than a small enclosure. Examples could be a poorly illuminated and irregularly accessed substation control house or a radio house. Again, if the medium sensitivity level produces too many false positives, use the low sensitivity setting.

The low sensitivity level is designed for spaces that see more and fairly regular activity. An example of an environment for which this sensitivity level is designed would be a substation control house where people move around. This sensitivity level will detect significant light changes such as the house lights turning on, but it should not trigger for movement of workers.

Table 5.9 Light Sensor Settings

Setting	Values	Default Value
Enabled	Check box	Selected
Sensitivity Level	High, Medium, Low	High

SEL-3622 Motion Sensor

The motion sensor is available on the SEL-3622. The motion sensor is designed to detect two types of motion: quick hits or impacts, and tilts. A tilt is a change in orientation with respect to gravity of greater than 45 degrees on any single axis and is intended to detect someone physically handling the SEL-3622 itself. Sustained 0.5 g acceleration on any axis will also trigger a tilt event. A spike in acceleration of 1.25 g will record an impact event such as from someone hammering on the cabinet in which the SEL-3622 is installed.

The screenshot shows the SEL-3622 configuration interface with four main sections:

- Global Settings:** Contains a checked "Enabled" checkbox.
- Input Contact:** Contains an "Enabled" checkbox, "Energization message" field (Input contact energized), "De-energization message" field (Input contact de-energized), and a "Reset to Default Messages" button. To the right is a "Most Recent Events (Max 10)" table with the following data:

Timestamp	Description
2014-06-04 23:52:42	Input contact de-energized
2014-06-04 23:52:31	Input contact energized
2014-06-04 23:52:24	Input contact de-energized
2014-06-04 23:52:19	Input contact energized
2014-06-04 23:52:14	Input contact de-energized
2014-06-04 23:52:12	Input contact energized

- Light Sensor:** Contains an "Enabled" checkbox, a "Sensitivity" dropdown with "Low" selected, and a "Most Recent Events (Max 10)" table with the following data:

Timestamp	Description
2014-06-04 23:59:05	Light sensor detected a change
2014-06-04 23:57:41	Light sensor detected a change
2014-06-04 23:53:53	Light sensor detected a change

- Motion Sensor:** Contains an "Enabled" checkbox, a "Sensitivity" dropdown with "Impact and Tilt" selected, and a "Most Recent Events (Max 10)" table with the following data:

Timestamp	Description
2014-06-04 23:59:18	Motion sensor detected tilt
2014-06-04 23:59:07	Motion sensor detected tilt
2014-06-04 23:58:51	Motion sensor detected movement or impact
2014-06-04 23:51:10	Motion sensor detected tilt
2014-06-04 23:50:38	Motion sensor detected tilt

Figure 5.18 Motion Sensor Settings and Recent Events

See *Table 5.10* for the Motion Sensor settings.

Table 5.10 Motion Sensor Settings

Setting	Values	Default Value
Enabled	Check box	Selected
Sensitivity	Tilt Only or Impact and Tilt	Tilt Only

If you have set the motion sensor to detect both impacts and tilts, then the SEL-3622 may detect both an impact and a tilt for a large impact event or for repeated successive impact events.

Network

Selecting the **Network** link on the navigation page opens the Network Settings page. This page provides an overview of the network settings, static routes, hosts, firewall (SEL-3620/SEL-3622 only), and Syslog functions of the device. See *Section 6: SEL-3620 and SEL-3622 Security Services* for more information about firewall.

Network Settings

The Network Settings page provides the configuration options for the global network settings and Ethernet network interface ports. The device logs all configuration changes to the network settings.

The screenshot displays the Network Settings page with the following sections:

- Network Settings:** Describes global network settings and physical network interface ports. It includes icons for a globe and wrench, and a note that all configuration changes are logged.
- Network Address Translation (NAT):** Describes NAT, which hides private addresses. It includes an icon of a server with arrows and a note that all configuration changes to NAT are logged.
- Static Routes:** Describes static routes for traffic to foreign networks. It includes an icon of a network diagram and a note that all configuration changes to Static Routes are logged.
- Hosts:** Describes hostnames to IP address mappings. It includes an icon of three servers and a note that all configuration changes to Hosts are logged.
- Address & Port Groups:** Describes grouping CIDR addresses or port ranges. It includes an icon of two servers and a note that all configuration changes to Address Groups and Port Groups are logged.
- Syslog:** Describes log storage and routing. It includes an icon of a document labeled "LOGS" and a note that every log includes severity level, message facility, tag, timestamp, and content fields. All configuration changes to Syslog are logged.
- Firewall:** Describes inspecting traffic. It includes an icon of a globe with a fire icon and a note that traffic can be filtered by transport protocol, IP address, port number, and encryption state. All configuration changes to Firewall are logged.
- SNMP Settings:** Describes Simple Network Management Protocol. It includes an icon of a stack of books and a note that these settings control remote access using SNMP and trap servers.

Figure 5.19 Network Settings

The top section of the Network Settings page (see *Figure 5.19*) displays the current configuration of the device global settings. Selecting **Edit Global Settings** at the top of the page causes the right panel on the device display to present the Network Global Settings form, from which you can modify Global Settings. See *Table 5.11* for a description of these settings.

Table 5.11 Global Network Settings

Name	Values	Description
Hostname	1 to 63 characters	The unique name identifying this device on the domain. The Hostname must begin with a letter and can contain letters, digits, and hyphens. This defaults to the serial number of the device.
Domain Name	As many as 253 characters	Defines the domain in which this device is a member. Consider the domain the network to which this device is attached. The domain name must be of the form [X.]X.Y, where X follows the hostname rules and Y is from two to six characters in length and begins with a letter. (Optional)
Manual Default Gateway	www.xxx.yyy.zzz	Defines the IP address of the default router the device uses to transfer packets to another network. Class D and Class E addresses are not allowed. If you leave this blank and a packet is destined for another network, the device will drop that packet. (Optional)
DHCP Gateways	Use manual gateway or list of Dynamic Host Configuration Protocol (DHCP) gateways	Selects the DHCP gateway that the device will use as the default router. The device will fall back to the manually configured default router if the selected DHCP gateway goes offline. (Optional)

There are hard-coded TCP keepalive values in the device that are applied globally. These settings are not user-configurable. *Table 5.12* describes the TCP keepalive settings.

Table 5.12 TCP Keepalive Settings

Name	Values	Description
TCP Keepalive Time	30	The device will send out the first TCP keepalive probe after 30 seconds of no activity for each unique TCP connection.
TCP Keepalive Interval	15	If the device does not get a reply to a keepalive probe, it will send a new probe in 15 seconds.
Maximum TCP Keepalive Probes	6	If the device does not see any TCP ACKs for any particular TCP connection after six consecutive lost keepalive probes, then it will mark the TCP connection as broken and drop it.

In the middle of the Network Settings page is the Network Interfaces diagram. This is the same diagram of the Ethernet interfaces that displays on the Dashboard. Each of these icons is color-coded to indicate the configuration state of that interface. *Table 5.13* shows the interface icon colors and their meanings.

Table 5.13 Network Interface Icon Colors

Interface	Status
	Enabled (Configured)
	Enabled (Not Configured)
	Disabled (Configured)
	Disabled (Not Configured)

**Figure 5.20 Network Interfaces**

On the device, you can enable/disable each physical Ethernet network interface, configure the maximum transmission unit (MTU) setting, change aliases, and add network addresses. See *Table 5.14* for device-specific network interface configuration information.

Table 5.14 Network Interface Capabilities

NOTE: MACsec is not supported on a bridged interface.

Network Interface Function	Supported on SEL-3610	Supported on SEL-3620 and SEL-3622
Enable/Disable	Yes	Yes
Change the MTU	Yes	Yes
Act as DHCP Client	Yes	Yes
VLAN Tagging	Yes, either one VLAN tagged network address or one native network address per network interface	Yes, as many as four total network addresses, including three VLAN tagged networks and one native network per network interface
Port Bridging	Yes, a combination of two or all three Ethernet interfaces may be configured as a bridge	Yes, a combination of two or all three Ethernet interfaces may be configured as a bridge
MACsec	No	Yes

Select the **Update** link below an Ethernet icon to configure settings unique to each Ethernet interface. Selecting this link will cause the device to display the Ethernet Interface form, from which you can enable or disable the interface, set the alias for the interface, provide a description of the interface, and set the interface MTU. Once you have entered any settings, select **Submit** at the bottom of the form to submit the changes. See *Table 5.15* for a description of each of these settings.

Table 5.15 Ethernet Interface Settings

Setting	Values	Description
Enabled	Check box	To disable an interface without losing your configuration settings, clear the Enabled box. This allows you to quickly reenable the interface when you need it.
Alias	As many as 32 characters	A name that is associated with the physical network interface. Aliases must be unique to each network interface.
MTU	68 to 1500	The maximum transmission unit defines the maximum size datagram the device will transmit. If left blank, the MTU defaults to 1500. If you enable bridging, the bridge MTU is the lowest MTU of all interfaces that are members of the bridge. For some WAN networks (such as cellular networks), you may have to set MTU to a lower value, such as 1440.

To add an Ethernet address to a network interface, select **Add Ethernet Address** at the top of the page. This causes the device to display the Add Network Address form (*Figure 5.21*) on the right side of the page.

On the SEL-3610, each interface can have only a single address. On the SEL-3620 and SEL-3622, each interface can be configured to have as many as four addresses, either as four VLAN addresses, or one native address and as many as three VLAN addresses. Note that the VLANs must occur in different broadcast domains. See *VLAN Tagging* in *Table 5.14*.

The Add Network Address form contains a dropdown list from which you can select the interface you want, boxes for the manual IP address, a configurable VLAN identifier, and an alias for the logical interface. If you have enabled the DHCP client on any interface, the user-configurable manual IP Address acts as the fallback address if the device cannot find a DHCP server. The device will poll periodically (every 30 seconds) for a DHCP server when you use the fallback address. See *Table 5.16* for a description of each of these settings.

The screenshot shows the 'Add Network Address' configuration page. The 'Interface' dropdown is set to 'Eth F'. The 'Enable DHCP Client' checkbox is unchecked. The 'Manual IP Address' field contains an IP address and a subnet mask. The 'VLAN' radio button is selected. The 'Native' radio button is selected. The 'Alias' field is empty. A note at the bottom says '*required'. A 'Submit' button is at the bottom right.

Figure 5.21 Add Network Address Form**Table 5.16 Network Address Form Settings**

Name	Values	Description
Interface	Physical network interface alias (default = Eth F, Eth 1, or Eth 2)	The physical network interface to which users add a Manual IP Address. Each interface can have a native IP address and/or one or more VLAN addresses (see <i>Table 5.14</i>).
Enable DHCP Client	Check box	If selected, the device will poll a DHCP server for the address the selected interface will use.
Manual IP Address	www.xxx.yyy.zzz/aa	An IP address to associate with the physical Ethernet interface. Class D and Class E addresses are not allowed. The device uses class interdomain routing (CIDR) notation to assign the subnet mask. If the device uses DHCP, this will be the fallback address if the device cannot find a DHCP server.
VLAN/Native	0 to 4095, or Native	Defines the Manual IP Address as native or associates it with a VLAN identifier. If you have selected Native, this device will not process VLAN tags on that interface.
Alias	As many as 32 characters	A name that is associated with the logical network interface. Aliases must be unique to each configured Ethernet address.

A combination of two or three Ethernet ports on the device can join a bridge. Bridging ports establishes switch-like functionality that you can use to hook multiple devices into a ring network without the need for an external switch. Once you add an Ethernet interface to the bridge, it shares the same IP address as other ports on the bridge but maintains its own MAC address. If the bridged Ethernet interface receives a packet destined for itself, it processes that packet normally. If the bridged Ethernet interface receives a packet destined for another address, it forwards that packet to its destination from the port best suited to sending it. The bridge interface runs Spanning Tree Protocol (STP) to determine which port forwards packets.

The bridge STP configuration parameters are Bridge Priority = 32768, Hello time = 2 seconds, Max age = 20 seconds, and Forward Delay = 15 seconds.

NOTE: Interfaces with MACsec configured will not be selectable.

To add a bridge to the device, select **Add Bridge** at the top of the page. This causes the device to display the Add Bridge Interface form (*Figure 5.22*) on the right side of the page. The Add Bridge Interface form contains boxes for the manual IP address, a list of physical interfaces, and a box for the bridge alias. See *Table 5.17* for a description of each of these settings.

The screenshot shows the 'Add Bridge Interface' configuration window. It includes fields for enabling DHCP, specifying a manual IP address (172.16.10.1/24), selecting physical interfaces (Eth F, Eth 1, Eth 2), and defining an alias ('bridge'). A note indicates that the alias field is required.

Figure 5.22 Add Bridge Interface Form

Table 5.17 Bridge Interface Form Settings

Name	Values	Description
Enable DHCP Client	Check box	If selected, the device will poll a DHCP server for the address it will use on the bridge interfaces.
Manual IP Address	www.xxx.yyy.zzz/aa	An IP address to associate with the network bridge. Class D and Class E addresses are not allowed. The device uses CIDR notation to assign the subnet mask. If you use DHCP, this address will be the fallback address if the device cannot find a DHCP server.
Physical Interfaces	Physical network interface aliases (default = Eth F, Eth 1, or Eth 2)	The physical network interfaces to add the network bridge. Two interfaces must be added to a bridge. Addition of a third interface can occur after initial bridge configuration when you are logged into the web management interface from the bridge IP address.
Alias	As many as 32 characters	A name that is associated with the bridge.

Below the diagram of Ethernet network interfaces is the list of configured Ethernet addresses on the device. Note that you cannot assign the same IP address to multiple network interfaces unless these interfaces are on the same interface bridge.

Network Addresses Address Alias	Interface Alias	IP Address	VLAN	MACsec	Web Server	Options
front	Eth F	192.168.1.10/24		Yes		<button>Update</button> <button>Delete</button>
USB	USB B	172.29.131.1/24		Yes		
bridge		10.10.10.1/24				<button>Update</button> <button>Delete</button>
	Eth 2					<button>Update</button>
	Eth 1					<button>Update</button>

Figure 5.23 Configured Addresses

You can perform two actions through use of the buttons associated with each entry in this list: update and delete. If you delete an entry the device provides a confirmation page displaying the entry to be deleted and other items that depend on that entry. Note that deletion of an entry causes deletion of all settings that depend upon that entry.

Disable Unused Ports

To disable unused ports, navigate to the Network Settings page. Select **Update** for the interface you want to disable. Clear the **Enabled** check box in the Ethernet Interface USB B Settings window, and select **Submit**.



Figure 5.24 Disable Unused Ports

Static Routes

The device supports static routes to allow communication between networks that are not directly connected. The device also provides the ability to silently drop all traffic to a network or to reject traffic to a network and define it as unreachable. The device provides graphical representation of static routes to verify that configurations are correct. An administrative user can configure as many as 100 routes. The device logs all configuration changes to static routes.

Be aware that static routes offer no extra security, and you should only configure such routes if encryption is unavailable at an address necessary for normal operation. The SEL-3620 and SEL-3622 offer virtual private network (VPN) functionality that automatically defines encrypted, authenticated static routes with Internet Protocol Security (IPsec).

To view, edit, delete, or add static routes, select the **Static Routes** link in the left navigation panel. If you have already configured static routes, you will see something similar to *Figure 5.25*. If not, you will only see the **Add Static Route** button.

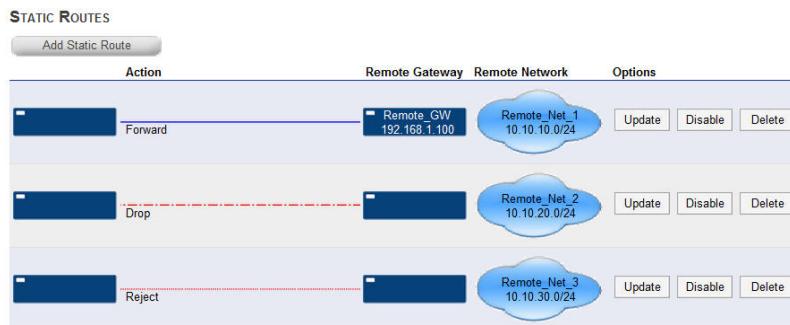


Figure 5.25 Static Routes

Figure 5.25 shows diagrams illustrating the configuration of static routes. The box on the left side of each diagram represents the local device. The box on the right side of each diagram represents the remote gateway. The cloud next to each remote gateway is a representation of the remote network. These diagrams provide a visual method for verifying that you have configured a static route correctly. For descriptions of each of the symbols in these diagrams, see *Table 5.18*.

Table 5.18 Static Route Symbols

Symbol	Description
	Represents the remote network and that the rule is enabled.
	Represents the remote network and that the rule is disabled.
	The local SEL-3610 or SEL-3620.
	The remote gateway.
	Indicates the traffic is forwarded to the remote network.
	Indicates the traffic is rejected. Packets are discarded, and the device generates an Internet Control Message Protocol (ICMP) message indicating an unreachable path.
	Indicates the traffic is dropped. Packets are discarded.

To add static routes to the device, select **Add Static Route** at the top of the page. This causes the Static Route form (see *Figure 5.26*) to display in the right-side panel. Refer to *Table 5.19* for a description of form settings.

Add Static Route

Remote Network

Enabled

IP*: 10 . 10 . 50 . 0 / 24

Alias*: Remote_Network

Action: Forward

Remote Gateway:** Remote_GW

or add new remote gateway:

IP++: 192 . 168 . 1 . 10

Alias**: Network_Gateway

*required
**If Action = Forward, then the Remote Gateway or IP/Alias must be entered

Submit

Figure 5.26 Static Route Form

Table 5.19 Static Route Settings (Sheet 1 of 2)

Setting	Values	Description
Enabled	Check box	Enables processing of the static route rule.
IP	www.xxx.yyy.zzz/aa	The network ID of the remote network. This must be the base address in the network. The device uses CIDR notation to assign the subnet mask.
Alias	As many as 32 characters	A name that is associated with this remote network. Aliases must be unique to each remote network.
Action	Forward, Drop, or Reject	Select the action that this rule should perform.
Remote Gateway	Any preconfigured remote gateway	A quick-select dropdown list that contains all of the previously configured remote gateways.

Table 5.19 Static Route Settings (Sheet 2 of 2)

Setting	Values	Description
IP	www.xxx.yyy.zzz/aa	The IP address of the remote gateway. The device uses CIDR notation to assign the subnet mask.
Alias	As many as 32 characters	A name that is associated with this remote gateway. Aliases must be unique to each mote gateway.

Address and Port Group

The SEL-3610 only supports address groups while the SEL-3620 and SEL-3622 support both address groups and port groups. This feature makes it easier to specify security policies by allowing one policy to include items that are not in a continuous range. Address groups can be used within the firewall rules, NAT/Port forwarding rules, and the allowed clients. Port groups also efficiently manage networks by grouping TCP and UDP port numbers, and by simplifying complex and large-scale networks.

The screenshot shows the 'ADDRESS & PORT GROUPS' section of the SEL-3620 configuration interface. On the left, there are two tabs: 'Add Address Group' and 'Add Port Group'. Below them are two tables:

- Address Groups:** Shows two entries: 'Rack_Devices' (IP: 192.168.4.0/24, 192.168.3.21/32, 192.168.23.20/31) and 'RTAC_Remote' (IP: 192.168.4.20/32, 10.10.10.0/24, 172.16.28.0/22, 172.29.131.10/32). Each entry has 'Update' and 'Delete' buttons.
- Port Groups:** Shows one entry: 'Substation_port_group' (Ports: 1025-1100, 443, 5001, 1700-1901). It also has 'Update' and 'Delete' buttons.

To the right, a modal dialog box titled 'Add Port Group' is open. It contains fields for 'Name*' (with 'RTAC_Group' entered), 'Description' (empty), and four port ranges ('Port 1*', 'Port 2*', 'Port 3*', 'Port 4*') each with 'From:' and 'To:' input fields. There is also an 'Add Another Port' button and a 'Submit' button at the bottom.

Figure 5.27 Address and Port Group

The SEL-3620 limits the creation of address and port groups to 100 for each group type. Each group can consist of a maximum of as many as 16 members.

Syslog

Syslog is a specification that describes both the method and format in which the device stores logs locally and routes them to a collector. The device can send its log information to three destinations and store no more than 60,000 event logs locally in nonvolatile memory. Each destination, including the local memory, has a configurable severity level filter. The device logs all configuration changes to Syslog. For more information about Syslog, refer to *Appendix F: Syslog*.

The device logs many different types of events such as system startup, login attempts, and configuration changes. Selecting the **Syslog** link from the navigation panel causes the device to display a screen similar to *Figure 5.28*. The information this display presents includes statistics for the local Syslog storage and a list of the configured Syslog servers to which the device sends events.

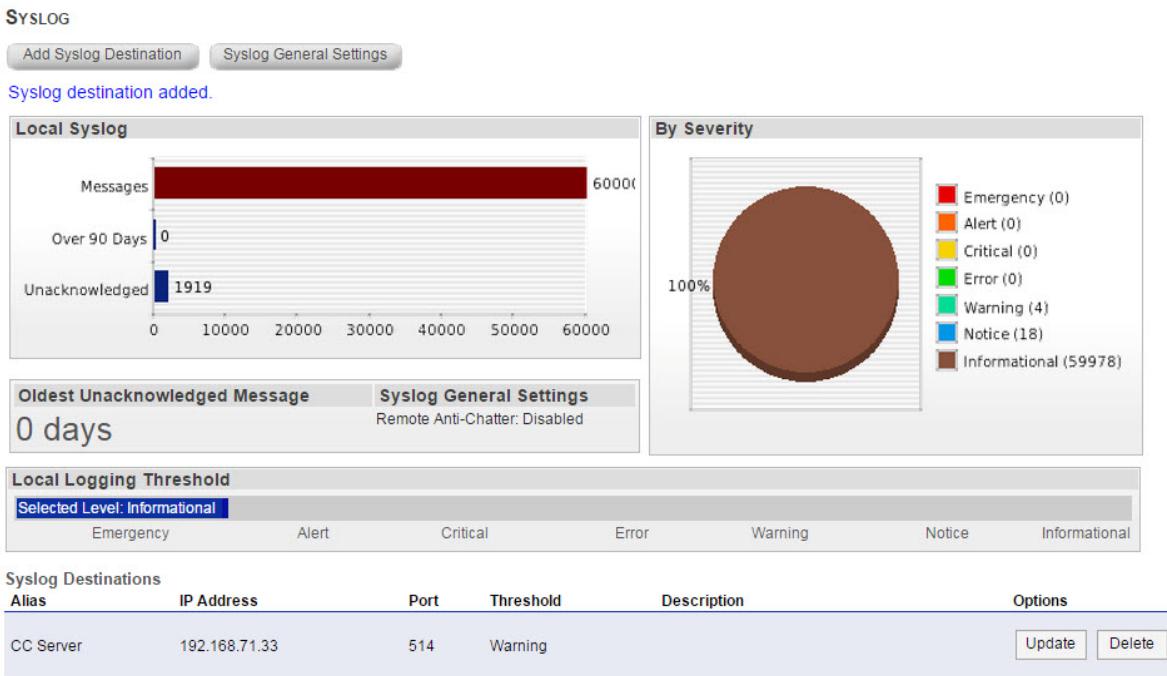


Figure 5.28 Syslog

The bar graph on the left of the display indicates the number of messages presently stored locally, the number of messages older than 90 days, and the number of unacknowledged messages. The pie graph on the right indicates the percentage of messages within each severity level. The device supports seven severity levels from informational to emergency. For a description of these severity levels, refer to *Appendix F: Syslog*.

The oldest unacknowledged message indicates the number of days since a user last examined the internal logs of the device. For more information about log acknowledgment, refer to *System Logs* on page 5.59. Under Syslog General Settings, the device will display whether or not the Remote Anti-Chatter feature is enabled or disabled (disabled by default).

Beneath the graphs is a logging threshold setting. This bar indicates the minimum severity that a Syslog message must have before the device stores that message locally.

The display lists Syslog destinations under the logging threshold setting. These destinations are the Syslog servers that will store and process the Syslog messages remotely. You can configure as many as three destinations. To configure a Syslog destination, select **Add Syslog Destination** located at the top of the page. Selecting this button causes the device to display the Syslog Destination form on the right side of the page.

The SEL-3620 offers higher granularity for the different types of Syslog message tags generated for each facility (Kernel, User, System, and Security) that are being sent to the Syslog destination (see *Table F.2*). See *Table 5.20* for descriptions of the Syslog destination settings.

NOTE: For security and auditing purposes, notifications about changes made to Syslog destinations are sent to the remote Syslog server before the actual changes are implemented to the device.

Add Syslog Destination

Destination

Alias*:

Description:

IP Address*: . . .

Port*: 514

Filters**

Enable Advanced Filtering

Minimum Priority Threshold Filters:

Kernel:

User:

System:

Security:

Enable Tag/Severity Filtering

Tag/Severity Allowlist Filters:

Search for tags ...

AddressGroupsConfig, Notice
 AllowedClients, Warning
 AllowedClientsConfig, Warning
 AllowedClientsConfig, Notice
 AllowedClientsConfig, Informational

*required
**at least one filter required

Figure 5.29 Add Syslog Destination**Table 5.20 Syslog Destination Settings**

Setting	Values	Description
Alias	As many as 32 characters	A name that is associated with this Syslog destination. Aliases must be unique to each destination.
Description	As many as 255 characters	A description of the usage or purpose of this Syslog destination.
IP Address	www.xxx.yyy.zzz	The IP address of the Syslog destination.
Port	1–65535	The Syslog UDP port number is 514 by default. This must match your Syslog server configuration.
Minimum Severity Threshold Filter	Informational, Notice, Warning, Error, Critical, Alert, Emergency	The minimum severity level necessary before the device will forward a message to this destination.
Enable Advanced Filtering	Disabled, Informational, Notice, Warning, Error, Critical, Alert, Emergency	Sets the minimum severity level for the Kernel, User, System, and Security facilities that will be forwarded to the Syslog destination.
Enable Tag/Severity Filtering	A maximum of 50 tags per Syslog destination	Selects individual Syslog tags for each severity level.

Syslog Destinations	Alias	Description	IP Address	Port	Filters	Options
Remote Syslog			129.138.12.1	514	Minimum Priority Threshold Filters KERNEL: Critical USER: Info SYSTEM: Emergency SECURITY: Informational Tag/Severity Allowlist Filters Firewall: Informational FirewallConfig: Warning Firmware: Critical FirmwareConfig: Warning Firmware: Notice HostsConfig: Notice IPsecConfig: Notice IPsecConfig: Informational JumperConfig: Error MACsecConfig: Notice MACsecConfig: Alert: Notice NATConfig: Notice PhysicalSensorsConfig: Warning PhysicalSensorsConfig: Notice PortMapping: Warning PortMapping: Notice Update: Critical Update: Error Update: Warning UserConfig: Error	<input type="button" value="Update"/> <input type="button" value="Delete"/>

Figure 5.30 Updated Syslog Destination Table

Syslog General Settings

Under Syslog General Settings (see *Figure 5.31*), you can set the device Minimum Local Logging Threshold, and enable or disable the Remote Anti-Chatter feature. Select your desired logging threshold from one of the following options: Informational, Notice, Warning, or Error. Setting the threshold too low may result in the device generating an excess of logs, some of which may be irrelevant to your business needs. Setting the threshold too high may result in the device failing to record important messages. The logging threshold is set at Notice by default.

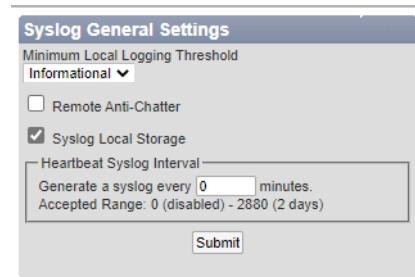


Figure 5.31 Syslog General Settings

The Remote Anti-Chatter feature is designed to prevent the device from consuming a large amount of bandwidth when sending logs of the same Tag Name, Severity, and Facility to remote Syslog servers. While Remote Anti-Chatter is enabled, the device exhibits the following behavior:

1. Five messages within five seconds that have the same combination of Tag Name, Severity, and Facility will trigger a suppression period. The device will no longer send messages that match that combination to any remote Syslog destinations.
2. The suppression period will end when at least five seconds pass during which no matching messages are received. The device will resume sending all messages to remote Syslog destinations.
3. When a suppression period ends, the device will send a message indicating the total number of messages that were suppressed and the Tag Name of the packets.

IMPORTANT: If the verbose logs are local and set to All, premature flash failure could occur. Consider using a remote Syslog to prevent this from occurring.

The device can keep track of multiple suppressed combinations of Tag Name, Severity, and Facility. While the suppression period is active, the device will continue to log messages locally to static storage. See *Table 5.21* for details.

Table 5.21 Syslog General Settings

Setting	Value	Description
Minimum Local Logging Threshold	Error, Warning, Notice, Informational	The minimum severity level necessary for the device to log a message to local storage (Notice by default).
Remote Anti-Chatter	Enabled or Disabled	Prevents the device from sending a large number of logs with the same Tag Name, Severity, and Facility to remote Syslog servers.
Local Storage	Enabled or Disabled	Set the check box for Syslog Local Storage to allow local storage of verbose firewall logs.
Heartbeat Syslog Interval	0–2880 minutes (0 = Disabled)	Set the Heartbeat Syslog Interval so that the heartbeat message appears in the logs at the specified interval. Example: System Heartbeat: --MARK--

SNMP

General

The SNMP (Simple Network Management Protocol) provides the ability to remotely read some device status information and to send notification of certain device status changes to an SNMP Trap Server on the network. SNMP clients can authenticate to the device by using SNMP v1/v2c or SNMP v3 credentials to read status values provided by the device. SNMP traps are conditions that are trapped by an SNMP-enabled device and result in notifications to trap servers that record or act upon these events.

Selecting the SNMP Settings link in the Network group on the navigation panel causes the device to display the SNMP Settings page (*Figure 5.32*).

The screenshot shows the SNMP Settings page with the following sections:

- SNMP SETTINGS** header with buttons: Add Profile, Add Trap Server, SNMP Status, MIB Download.
- SNMP Engine ID:** 80007C4F053131330323130323739
- SNMP Status** section with a checked checkbox for Enable SNMP and a Submit button.
- SNMP Profiles** table:

Profile Name	SNMP Version	Protocol	Protocol	Permissions	Options
V3Sample	v3	SHA1	AES-128	Read, Trap	<button>Update</button> <button>Delete</button>
V2V1Sample	v1/v2c			Read, Trap	<button>Update</button> <button>Delete</button>

Note: To allow SNMP access only from specific hosts, use the Allowed Clients page to add those hosts as SNMP clients. If no SNMP clients are added there, all hosts with the correct credentials will be allowed access.
- SNMP Trap Servers** table:

Server Name	IP Address	Associated Profile	Traps	Options
V3Server	192.168.10.53	V3Sample	Configuration Physical Sensor	<button>Update</button> <button>Delete</button>
V2V1Server	192.168.10.52	V2V1Sample	Configuration Physical Sensor	<button>Update</button> <button>Delete</button>

Figure 5.32 SNMP Setting Page

The SNMP Engine ID uniquely identifies the device. Its value is the sequence of bytes (shown in hex) 80007C4F05 followed by the serial number of the unit. So, with the serial number 1234ABCD, it will have an SNMP Engine ID of 80 00 7C 4F 05 31 32 33 34 41 42 43 44.

The device provides configuration information about data values and trap events for remote SNMP clients or trap servers. This information is provided in an MIB information file that can be downloaded by using the **MIB Download** button on the SNMP Settings page.

Setting Up Clients

Remote clients or trap servers use authentication to ensure the identity of the other party in an SNMP transaction. The simpler v2c authentication technique uses a “community string” known to all SNMP devices. The v3 scheme improves security by adding cryptographic options for authentication and encryption of messages.

Remote clients can use either v1/v2c or v3 profiles to access SNMP data on the device. Profile data defines the operations permitted for the remote host, as well as the authentication and/or encryption information.

Use the **Add Profile** button to set up a profile for use by clients or trap servers. *Figure 5.33* shows the configuration information needed to set up a v1/v2c profile for use by v2c clients. *Figure 5.34* shows the configuration information for v3 clients.

The screenshot shows the 'Add SNMP Profile' dialog box. It has a title bar 'Add SNMP Profile'. Below it are three main sections: 'Profile Name *:' with a text input field, 'Permissions:' with two checked checkboxes ('Read' and 'Trap'), and 'SNMP Community String' with two text input fields ('String *:' and 'Confirm String *:'). At the bottom right is a 'Submit' button.

Figure 5.33 Adding an SNMP v1/v2c Profile

Table 5.22 SNMP v1/v2c Parameters

Name	Value
Profile Name	1 to 31 letters or numbers
Permissions	Read, Trap, or both
SNMP Community String	As many as 128 ASCII characters

This screenshot shows the 'Add SNMP Profile' dialog for v3 clients, which is similar to Figure 5.33 but with additional sections. It includes 'Authentication' and 'Encryption' sections. The 'Authentication' section contains a 'Protocol' dropdown set to 'SHA1' and password fields. The 'Encryption' section contains a 'Protocol' dropdown set to 'AES-128' and password fields. A note at the bottom states: '* Required' and '** Required unless the related protocol is 'None'.'

Figure 5.34 Adding an SNMP v3 Profile

Table 5.23 SNMP v3 Parameters

Name	Value
Profile Name	1 to 31 letters or numbers
Permissions	Read, Trap, or both
Authentication Protocol	None, MD5, or SHA1
Authentication Password	8–128 upper- or lowercase letters, numerals, or symbols. Tabs and newline characters are permitted.
Encryption Protocol	None, DES, or AES-128
Encryption Password	8–128 upper- or lowercase letters, numerals, or symbols. Tabs and newline characters are permitted.

Setting Up Trap Servers

Trap servers receive notification events in response to certain device status changes. To set up a trap server, you must supply the name of the server and its IP address, and choose the authentication type (profile) for messages to the server. *Figure 5.35* shows the Add Trap Server dialog.

**Figure 5.35 Adding a Trap Server**

SEL SNMP MIBs and Testing

The device supports the MIBs in *Table 5.24* in poll or trap form.

Table 5.24 Supported MIBs (Sheet 1 of 2)

MIB	OID	Name	Type	Value (Example)
RFC1213-MIB (SNMPV2-MIB)	.1.3.6.1.2.1.1.1.0	sysDescr.0	OctetString	SEL-3622
RFC1213-MIB (SNMPV2-MIB)	.1.3.6.1.2.1.1.2.0	sysObjectID.0	OID	sel3622 (.1.3.6.1.4.1.31823.1.3622)
RFC1213-MIB (DISMAN-EVENT-MIB)	.1.3.6.1.2.1.1.3.0	sysUpTime.0	TimeTicks	32 hours 25 minutes 30 seconds (11673007)
RFC1213-MIB (SNMPV2-MIB)	.1.3.6.1.2.1.1.4.0	sysContact.0	OctetString	"
RFC1213-MIB (SNMPV2-MIB)	.1.3.6.1.2.1.1.5.0	sysName.0	OctetString	sel3622lt
RFC1213-MIB (SNMPV2-MIB)	.1.3.6.1.2.1.1.6.0	sysLocation.0	OctetString	"
SEL-3600-MIB	.1.3.6.1.4.1.31823.1.3600.1.1.3.0.1.0	sel3600SELinuxAudit-Message	Trap	Message

Table 5.24 Supported MIBs (Sheet 2 of 2)

MIB	OID	Name	Type	Value (Example)
SEL-3600-MIB	.1.3.6.1.4.1.31823.1.3600.1.2.1.0	sel3600Autoscopy-Enabled.0	Integer	false (0)
SEL-3600-MIB	.1.3.6.1.4.1.31823.1.3600.1.2.2.0	sel3600SELinuxEnabled.0	Integer	true (1)
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.0.1	sel3600PhysicalSensor-InputContactEvent	Trap	Message
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.0.2	sel3600PhysicalSensor-LightSensor	Trap	Message
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.0.3	sel3600PhysicalSensor-MotionSensorEvent	Trap	Message
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.1.0	sel3600PhysicalSensor-InputContactEnabled.0	Integer32	false (0)
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.2.0	sel3600PhysicalSensor-LightSensorEnabled.0	Integer32	false (0)
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.3.0	sel3600PhysicalSensor-MotionSensorEnabled.0	Integer32	false (0)
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.4.1.0	sel3600PhysicalSensor-InputContactEvents.0	Counter32	0
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.4.2.0	sel3600PhysicalSensor-LightSensorEvents.0	Counter32	100
SEL-3600-PHYSICAL-SENSOR-MIB	.1.3.6.1.4.1.31823.1.3600.2.1.4.3.0	sel3600PhysicalSensor-MotionSensorEvents.0	Counter32	1
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.1.0	selCommonWhitelist-Enabled.0	Integer	true (1)
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.1.0	selCommonWhitelist-FilesHashed.0	Counter32	538
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.2.0	selCommonWhitelist-CacheHits.0	Counter32	266721452
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.3.0	selCommonWhitelist-IntegrityFailures.0	Counter32	0
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.4.0	selCommonWhitelist-CacheInvalidates.0	Counter32	122
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.5.0	selCommonWhitelist-CacheSuccess.0	Counter32	178366795
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.6.0	selCommonWhitelist-UnknownFileHits.0	Counter32	0
SEL-COMMON-WHITELIST-MIB	.1.3.6.1.4.1.31823.3.1.1.2.7.0	selCommonWhitelist-ConfigCount.0	Counter32	3891
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1.1.0	snmpEngineID.0	OctetString	0x80 00 7C 4F 05 31 31 34 31 31 34 30 33 31 30
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1.2.0	snmpEngineBoots.0	Integer	8
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1.3.0	snmpEngineTime.0	Integer	116730
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1.4.0	snmpEngineMax-MessageSize.0	Integer	1500

You can poll the device via SNMP by using snmpwalk (Linux) or Windows-based MIB browsers such as iReasoning MIB Browser. To poll the SEL-3620 via Linux, you can use a command such as the following:

```
snmpwalk -v 2c -c public 192.168.1.2 .1.3.6.1.4.1.31823.3.1.1.2
```

Serial Ports

The SEL-3610 and SEL-3620 contain 17 serial ports that you can configure to EIA-232/EIA-422/EIA-485 at speeds from 1200 to 115200 bps. The SEL-3622 has four serial ports, two EIA-232 ports, and two ports configurable as EIA-232/EIA-422/EIA-485. The Serial Port section discusses all configuration options for the physical serial ports. Also included in this section is information about port mapping capabilities that enable a variety of serial-to-Ethernet applications, including secure engineering access, Modbus TCP to Modbus RTU/ASCII conversion, bit-based serial-to-Ethernet conversion, and much more. The device logs all configuration changes to the serial port settings or port mappings.

PORT SETTINGS

Port Settings

The Serial Port Settings page provides you the ability to name, enable/disable, and assign profiles to the device's serial ports. Be sure to configure your Serial Port Profiles before visiting this page.

All configuration changes to Port Settings are logged.

Port Profiles

A Port Profile is a collection of serial port settings that can be applied to multiple serial ports via the Serial Port Settings page.

Port Profile settings include:

- Name
- Baud Rate
- Data Bits
- Parity
- Stop Bits
- Max Frame Length
- Communication Interface
- Flow Control
- Port Power
- Framing
- Intercharacter Delay
- Minimum Interframe Deadtime
- Push To Talk

All configuration changes to Port Profiles are logged.

Port Mappings

The device accepts both incoming and outgoing connections from any serial or TCP/UDP port to any serial or TCP/UDP port. Assign and map port connections on the Port Mappings page.

Port mappings are organized in groups. Each port (serial, TCP or UDP) can only be a member of one group at a time. Groups can have a master port which acts as a terminal server that can redirect any incoming connection to any one of the grouped ports at a time.

Changes to mappings containing any TCP port will take effect only after any present connections or communications associated with that TCP port are terminated.

All configuration changes to Port Mappings are logged.

Figure 5.36 Serial Ports Page

Serial Port Settings

⚠ CAUTION

Settings for serial ports that are part of connection directories downloaded from QuickSet should not be edited, enabled, or disabled. Use QuickSet to update the settings on these ports.

The Serial Ports page provides a list of the serial ports and the present configuration of each port. Selecting **Update** for the corresponding serial port causes the device to display the Serial Interface Settings form for the respective serial port. This form allows you to enable or disable the interface, select a Use Profile, and set the Alias of the interface. Once you have entered any settings, select **Update** at the bottom of the form to submit the changes. See *Table 5.25* for a description of each of these settings.

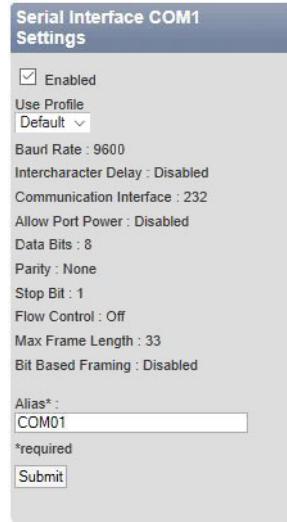


Figure 5.37 Serial Interface Settings Form

Table 5.25 Serial Interface Settings

Name	Values	Description
Enabled	Check box	To disable an interface without losing your configuration settings, clear the Enabled check box. This allows you to quickly reenable the interface when necessary.
Use Profile	Default or User-Defined Profile	A default or user-defined user profile. User profiles contain serial port settings such as baud rate, data bits, parity, flow control, and the type of serial communications interface.
Alias	As many as 32 characters	A name that is associated with the physical serial interface. Aliases must be unique to each serial interface.

Serial ports are color-coded to illustrate when they are enabled or disabled. The device uses these colors in any display of serial ports or port mappings, such as on the Dashboard, the Port Settings page, and Port Mappings page.

Table 5.26 Serial Port Icon Colors

Interface	Status
	Enabled (Configured)
	Disabled (Not Configured)

Serial Port Profiles

The Port Profiles page provides configuration options through which you can create serial port profiles containing common settings. You would typically incorporate these user-defined serial port profiles when you apply the same serial port settings across multiple serial ports. When you configure settings for a serial port, you select the user-defined serial port profile and apply the settings within the profile to the serial interface. You can then configure a serial port profile once and apply the settings many times, saving configuration time. See *Table 5.27* for a description of the settings the serial port profiles use.

NOTE: A user cannot edit or remove any port profile currently in use by a serial port. To remove or edit a profile, remove any active serial port using the profile from all serial port mappings.

NOTE: The RTS line of the SEL-3600 serial port is usually HIGH, unless Push-to-Talk is enabled in Bit Based Processing mode.

Table 5.27 Serial Interface Settings

Name	Values	Description
Name	As many as 32 characters	The name of the user-defined profile
Baud Rate	1200–115200 (1200–9600 if Bit Based Processing is enabled)	Sets the baud rate of this interface in bits per second (bps). The device supports standard baud rates from 1200 to 115200.
Communication Interface	232, 422, or 485	The type of serial communications interface. Either EIA-232, EIA-422 (four-wire), or EIA-485 (two-wire).
Allow Port Power	Check box	5 V power supplied on Pin 1 of the DB-9 connector of the specified serial port. Note that the SEL-3622 is not capable of providing 5 V Pin 1 power on any serial ports.
Data Bits	7 or 8	Number of bits per character. Not available under Bit Based Processing mode.
Parity	None, Even, Odd	Error detection bit. Not available under Bit Based Processing mode.
Stop Bits	1 or 2	The number of stop bits. Not available under Bit Based Processing mode.
Flow Control	Off, RTS/CTS, XON/XOFF	Enable or disable hardware (RTS/CTS) or software (XON/XOFF) flow control. Not available under Bit Based Processing mode.
Max. Frame Length	1–255	Maximum serial buffer size in bytes. Set this to 255 if you want to package as much serial data as possible into a single Ethernet packet. This minimizes the splitting of serial data into multiple messages and can lower the chance of dropped messages. Note that if data less than the maximum frame length are received on the serial port, the device will automatically impose an 8-bit time delay for received data (64 bit-times for transmitted data) before processing the data in the buffer. Not available under Bit Based Processing mode.
Intercharacter Delay	Check box	Add intercharacter delay time to obtain an effective 2400 bps transmission rate. This improves compatibility with older relays that have limited serial-buffering capabilities.
Bit Based Processing	Check box	Turns off byte processing and turns on bit mode for the serial port.
Min. Interframe Deadtime	10–20000	Specifies number of bit time mark bits that are observed before terminating sending or receiving of bit-based data.
Push-To-Talk	Check box	If selected, the device keeps the RTS line deasserted at all times unless data are sent. Before data are sent out the serial port, the RTS line is raised for a 45-millisecond Pre-Transmission Mark time, kept high while bit-based data are sent, then lowered after an 8-millisecond Post-Transmission Mark time. Push-To-Talk is only available if the Communication Interface is set to 232.

Bit Based Processing Mode

NOTE: Bit Based Processing mode is not supported on EIA-485 two-wire connections.

Bit Based Processing mode is designed to be able to transport bit-based protocols such as Conitel, Redac, Van Comm, and others over Ethernet. Bit mode works by detecting a start bit, then sampling and sending data bits until the Interframe Dead Time number of mark bits (logical 0s) have been received. At this point, the serial port transitions back into an idle state, waiting for a new start bit to restart the Interframe Dead Time timer and begin recording data bits again.

Push-to-Talk

The Bit Based Processing Push-to-Talk (PTT) function is designed to integrate with existing analog lease-line modems, or devices that require dynamic RTS behavior to communicate properly, such as device with built-in modems or existing lease-line modem hardware. The PTT function of the device raises the RTS for a Pre-Transmission Mark period of time (fixed at 45 milliseconds) before data transmission, keeps the RTS line raised during data transmission, then drops the RTS after a Post-Transmission Mark period of time (8 milliseconds OR Inter-frame Dead Time bit-times, whichever is greater) after data transmission is finished.

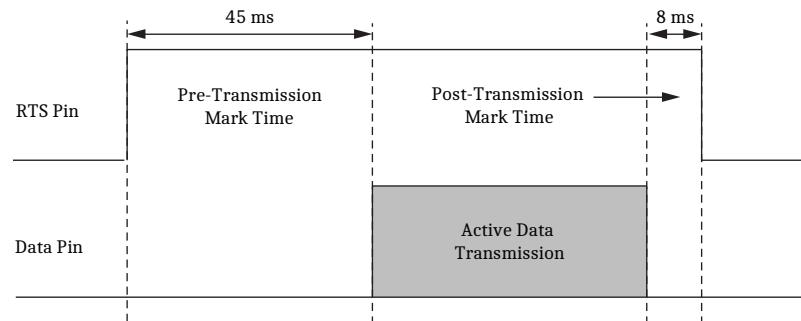


Figure 5.38 Push-to-Talk RTS vs. Data Pin Behavior

Bit Based Processing Latency

The device introduces an 8 bit-time delay when receiving serial data, and a 64 bit-time delay when transmitting serial data. For a round-trip over an Ethernet network, the total expected bit-time delay will be 144 bit-times ($8 + 64 + 8 + 64$) + Ethernet network latency. Because the far-end serial data transmission hold-back is 64 bit-times, the jitter tolerance on the Ethernet network is either 64 bit-times or 64 bit-times + PTT Pre-Mark Time (if PTT is enabled on the far end). See *Table 5.28* for one-way bit-time latency through two SEL-3620/SEL-3622 devices.

Table 5.28 One-Way Bit-Time Delays

One-Way Latency for SEL-3620/SEL-3622 Bit-Based Conversion Through an IPsec Tunnel			
Baud Rate (bps)	Bit-Times	Time (ms)	Jitter Tolerance (ms)
1200	72	60	53.33 (98.33 w/PTT)
2400	72	30	26.67 (71.67 w/PTT)
4800	72	15	13.33 (58.33 w/PTT)
9600	72	7.5	6.67 (51.67 w/PTT)

Other Considerations

The SEL-3610 and SEL-3620 can operate all 16 DB-9 serial ports in Bit Based Processing mode at 1200 bps. Because of CPU constraints, the number of simultaneous serial ports operational in Bit Based Processing mode at higher baud rates is limited. The maximum number of supported serial ports at given baud rates over an IPsec tunnel is shown in *Table 5.29*.

Table 5.29 Maximum Number of Supported Bit-Based Serial Ports

Speed (bps)	Simultaneous Number of Serial Ports
1200 bps	16 (SEL-3610/SEL-3620), 4 (SEL-3622)
2400 bps	8 (SEL-3610/SEL-3620), 4 (SEL-3622)
4800 bps	4 (SEL-3610/SEL-3620), 4 (SEL-3622)
9600 bps	1 (SEL-3610/SEL-3620), 1 (SEL-3622)

When both encryption and bit-based conversion modes are used together, the high CPU usage can result in errors in bit-based data transmission. For this reason, SEL suggests avoiding using SSH as the Ethernet transport method, and suggests avoiding the use of IPsec when providing bit-based conversion at 9600 bps.

Port Mappings

Introduction to Port Mappings

The device can configure highly flexible port mappings between two or more physical serial ports, two or more logical Ethernet ports, and between logical Ethernet ports and physical serial ports. Port mappings on the device enable intuitive, authenticated human-to-machine interaction with the Master Port function, and direct human-to-machine and machine-to-machine information transfer with Port Switch functionality. Ethernet connections into and originating from port mapping can use Raw TCP, UDP, SSH, Telnet, or Modbus protocols.

You can use port switch functionality with multiple communications media, data rates, and protocols to transfer data between connected devices. You can map EIA-232 and EIA-485 serial devices to each other, independently of baud rate or flow controls. You can also use serial-to-Ethernet port mappings to tunnel data from serial devices over Ethernet networks to SCADA application software. An Ethernet device can broadcast to multiple serial or Ethernet clients and then listen selectively to responses from a single client.

Another capability of port mappings is master port functionality. A master port is a console-based authentication portal for interactive user access to one or more serial or Ethernet devices connected to the device. You can configure a physical serial port or logical Ethernet port to act as a master port in a port mapping. The device logs and authenticates all access to a master port by the local or centralized user-based accounts of the device. You can configure the master port to use scripting, through which the device can manage passwords for multiple connected IEDs (SEL-3620 and SEL-3622 only).

Primary Applications of Port Mappings

A primary application of port mappings is in authenticated interactive access to remote consoles. Through such access, engineers can securely monitor or configure IEDs connected to the device. Engineers can securely access a master port over Ethernet, dial-up, or through a direct connection to a serial port on the device. After you authenticate your identity to the device, the master port pres-

ents you a list of authorized devices from which you can select. The device will connect you transparently to any device you select and hold the connection open until you terminate the session or a time-out occurs.

Benefits of authenticated local and/or remote engineering access include increased security and added traceability. With a master port, administrators can add centralized user-based accounts to all IEDs in a substation environment by passing all engineering access through a master port authentication portal before allowing access to IEDs behind the device. See *Section 6: SEL-3620 and SEL-3622 Security Services* and *Section 7: Proxy Services and Password Management* for more details about automated password management available on the SEL-3620.

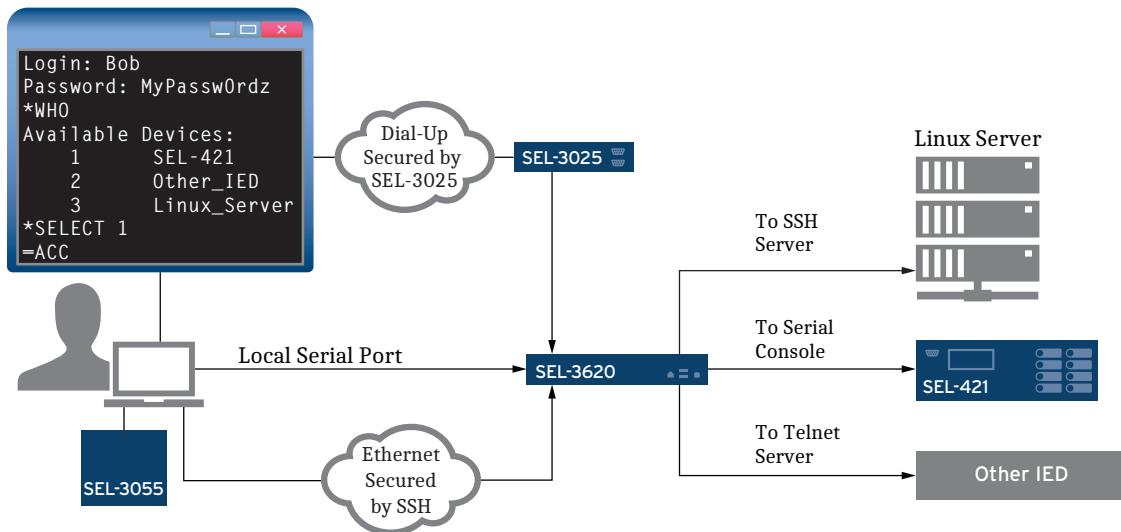


Figure 5.39 Master Port for Engineering Access

Another application is configurable machine-to-machine data transfer. You can mix and match physical serial ports and logical Ethernet ports, then use filtering to determine which ports listen and which ports respond. Uses for this scenario include Modbus TCP to Modbus RTU/ASCII conversion, expansion of the number of serial ports available over an Ethernet network, multi-master architectures, and the broadcasting of SCADA data to multiple serial devices while filtering for one or more responses.

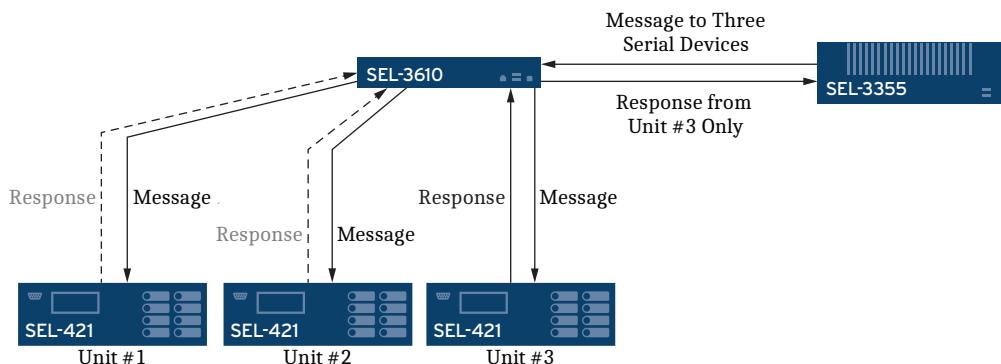


Figure 5.40 Easy Connection Filtering

Engineers can also use port switch functionality to achieve, supervise, and provide redundancy of data streams without physically manipulating wires or changing external device settings. The selective listen/transmit abilities in the device

allow you to simultaneously send multiple read-only copies of a data stream between two or more devices to an archive server, provide troubleshooting capabilities by mirroring such a transmission to an engineering computer, and to forward copies of a data stream to redundant devices, all without moving a single physical wire.

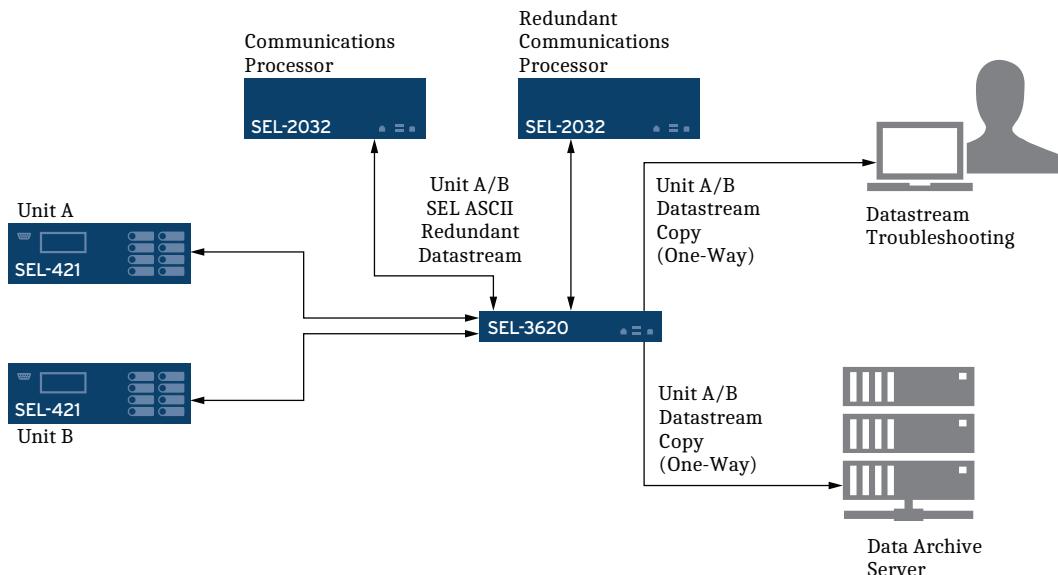


Figure 5.41 Archiving, Supervision, and Data Redundancy

Functional Components of Port Mapping

Various configured port mappings on the device are called port groups. To add a group, select **Add Group** at the top of the Port Mappings page. An Add New Group form appears on the right side of the page. You must provide a unique alias with as many as 32 characters to the port group. Select **Submit** to create the new port group.

PORT MAPPINGS	
Add Group	
Name	Action

Add New Group

Alias *:

* Required

Figure 5.42 Add Group Form

Every group on the device contains one or more functional components called devices. Three types of devices can form a group: Serial, Ethernet Listen Local, and Ethernet Connect Remote.

Add Device

Group : PortGroup

Serial
 Ethernet Listen Local
 Ethernet Connect Remote

Figure 5.43 Add Device Form

Serial Device

A serial device is a physical serial port alias, such as those you configured on the Port Settings page. You can configure a serial device as either serial protocol or Modbus RTU/ASCII protocol. Refer to *Table 5.30* for a description of each setting. A serial device is unique to each group. You cannot use the same serial device in another group.

NOTE: All serial devices in the same group must use the same port profile.

Figure 5.44 Add Serial Form

Table 5.30 Add Serial Form Settings

Name	Values	Description
Serial Port	Alias:Profile	Name of the physical port alias followed by the name of the current profile it uses.
Protocol	Serial or Modbus	The protocol of the serial port as configured in port settings, or Modbus RTU or ASCII.
Master Port	Check box	Select to configure the serial port as a master port. See <i>Table 5.31</i> (Add Serial Master Port Form) for more information.
Listening Ports	Check box for every configured device in the group	The port you are presently configuring will receive data from any selected device in this list. The device will ignore listening ports if you select Master Port or choose Modbus Protocol.

If you select the Master Port box, the Add Serial form will expand to allow extra options, including Modem, Termination String, and Leading Time configuration. Refer to *Table 5.31* for a description of each setting.

The screenshot shows a configuration window titled 'Update Serial Driver'. It includes fields for 'Group : PortGroup' and 'Serial Port : COM01'. Under 'Protocol **', 'Serial' is selected. Under 'Master Port **', both 'Master Port' and 'Modem' are checked. In the 'Master Port Settings' section, 'Allow Script' is checked. The 'Termination String' is set to 'Ctrl-Q'. The 'Leading Time *' is set to '1 (1-10)'. A note at the bottom states: '* Required' and '** Listening ports selection is ignored if Master port is set or Protocol is Modbus'. A 'Submit' button is at the bottom.

Figure 5.45 Add Serial Master Port Form**Table 5.31 Add Serial Master Port Form Settings**

Name	Values	Description
Modem	Check box	This feature is only available on the SEL-3620 and SEL-3610 COM1 port. This feature is not available on the SEL-3622. When this box is selected, the device will watch the serial DCD line and close any open session when the DCD line is deasserted. Note that you will need to add a hardware jumper to activate this feature. See <i>Section 1: Introduction and Specifications</i> for more information.
Allow Script (SEL-3620 and SEL-3622 only)	Check box	Allows the master port to use user scripts and automatic password management functionality specific to the SEL-3620. For more information about the Script option, see <i>Section 7: Proxy Services and Password Management</i> .
Termination String	Ctrl+Q Ctrl+W Ctrl+E	This termination string ends a present connection of a master port to a remote device. Use this when you need to return to the master port menu from a device into which you have tunneled.
Leading Time	1–10	Number of seconds of inactivity necessary before the master port recognizes the termination string. This helps prevent accidental disconnect while the device forwards data.

Using Modems

Selecting the Modem option for COM1 allows you to connect a modem to receive incoming modem calls to the SEL-3610/SEL-3620. The modem should be configured for auto-answer (ATS0 = 1), and to disconnect on loss of DTR (AT&D2). It should be also configured for no local echo (ATE0), and no status messages (ATQ1) so that the only characters received by the device will be data sent through the modem on the other end of the connection. Note that the SEL-3622 does not have a special COM port for connecting to modems.

Ethernet Listen Local Device

NOTE: Only one session per master port is allowed unless the master port is script-enabled.

The Ethernet listen local device is a logical Ethernet TCP or UDP port on the device that allows incoming connections into a port group. You can configure the logical port to use Raw TCP, UDP, Telnet, SSH, or Modbus TCP protocols. Once

you have established an incoming connection with a TCP-based Ethernet listen local device, two-way communications on the TCP port you specified occur as usual.

With UDP Ethernet listen local devices, when a UDP packet is received on the port, the system will hold open the connection until a time-out has occurred, and will respond back to the source IP address and source UDP port. A user may configure UDP Ethernet listen local devices to override the original incoming source data IP address and UDP port for responses.

When a TCP-based Ethernet listen local device is part of a port group, device members cannot communicate with each other until the TCP Ethernet listen local device has accepted a new TCP connection. Once you have established this connection, all group devices can communicate normally. This restriction is removed for UDP Ethernet listen local devices; connections to UDP Ethernet listen local devices are not required for other port group members to communicate. Furthermore, when UDP Response Destination Override is enabled, and both IP and port are set, then data from the port group can be sent to the override response destination IP and port without an incoming connection being required. Refer to *Table 5.32* for a description of each setting. An Ethernet listen local device is unique to each group. You cannot use the same Ethernet listen local device in another group.

NOTE: Timeouts for Ethernet listen local and Ethernet connect remote are user-configurable between 1-60 minutes. To configure this time-out, configure the Global Session Timeout setting under the Management Interface webpage on the device.

The screenshot shows the 'Add Ethernet Local Driver' configuration interface. The 'Group' field is set to 'PortGroup'. The 'Alias' field contains 'SSH'. The 'Network Interface' dropdown is set to 'Listen on All'. The 'Port' field is set to '5000'. The 'Protocol' dropdown is set to 'SSH'. There is a checked checkbox for 'Master Port **'. Below these fields is a large text input area labeled 'Listening Ports' which is currently empty. At the bottom of the form, there is a note: '* Required' and '** Listening ports selection is ignored if Master port is set or Protocol is Modbus.' A 'Submit' button is located at the bottom right.

Figure 5.46 Add Ethernet Listen Local Form

Table 5.32 Add Ethernet Listen Local Form Settings (Sheet 1 of 2)

Name	Values	Description
Alias	As many as 32 characters	Name of the Ethernet listen local device. Once you have configured this alias, you cannot use it in another group.
Network Interface	Listen on All, or select the network interface	The specific configured network interface on which to listen for connections to the Ethernet listen local device. The device can listen on all configured network interfaces or on a single specific network interface.
Port	1–65535	The device TCP and/or UDP port on which the Ethernet listen local device listens for incoming connections. The port cannot conflict with any other listening port on the system.

Table 5.32 Add Ethernet Listen Local Form Settings (Sheet 2 of 2)

Name	Values	Description
Protocol	Raw TCP, UDP, Telnet, SSH, Modbus TCP	The configured protocol for the specified Ethernet listen local device. When configured as SSH, the device will act like an SSH server, and it will authenticate any incoming connections to local or centralized user-based accounts on itself. The device will authenticate itself to incoming connections with its SSH host key. For more information about Modbus configuration, see <i>Performing Modbus Conversion</i> on page 5.47. For Telnet, the device will negotiate either 7- or 8-bit mode.
Master Port	Check box	Select to configure the Ethernet listen local device as a master port. See <i>Table 5.33 (Add Ethernet listen local master port form)</i> for more information. Master ports are not available as Modbus, bit-based serial, or UDP.
UDP Response Destination	Check box	If the UDP Response Destination Override is enabled and port is set, the system will respond to the source IP address on the specified port. If the UDP Response Destination Override is enabled and both the port and IP address are set, then the system will ignore source IP and source UDP port data and send any responses to the specified IP address and UDP port.
Listening Ports	Check box for every configured device in the group	The port you are presently configuring will receive data from any device you have selected in this list. The device will ignore listening ports if you select Master Port or choose Modbus Protocol.

NOTE: You can have only one TCP-based Ethernet listen local device (SSH, Telnet, Raw TCP, or Modbus TCP) per port group.

If while configuring the Ethernet listen local device you select the Master Port check box, the Add Ethernet Listen Local form expands to allow extra options, including configurations for Allow Script, Termination String, and Leading Time. Refer to *Table 5.33* for a description of each setting. You can have only one master port per group. Master ports cannot be added to port groups with bit-based serial devices or UDP devices.

Figure 5.47 Add Ethernet Listen Local Master Port Form

Table 5.33 Add Ethernet Listen Local Master Port Form Settings

Name	Values	Description
Allow Script (SEL-3620 and SEL-3622 only)	Check box	Allows multiple user access to the master port for user scripts and automatic password management functionality specific to the SEL-3620. For more information about the Script option, see <i>Section 7: Proxy Services and Password Management</i> .
Termination String	Ctrl-Q, Ctrl-W, Ctrl-E	This termination string ends a present connection of a master port to a remote device. Use this when you need to return to the Master Port menu from a device into which you have tunneled.
Leading Time	1–10	Number of seconds of inactivity necessary before the master port recognizes the termination string. This helps prevent accidental disconnect while the device forwards data.

Ethernet Connect Remote Device

An Ethernet connect remote device creates an outgoing connection from the port group on the SEL-3610/SEL-3620 to a logical Ethernet port on another networked device. You can configure the device to connect to a port that uses Raw TCP, UDP, Telnet, SSH, or Modbus TCP protocols. Once you have established an outgoing connection from a TCP Ethernet connect remote device to a networked device, two-way communications on the specified TCP occur as usual. For UDP Ethernet connect remote devices, data are sent to the remote UDP destination, and the source port is held open until a time-out occurs. Refer to *Table 5.34* for a description of each setting. You can use an Ethernet connect remote device in more than one port group.

An Ethernet connect remote device remains disconnected until there exist enough data to write to it. When sufficient data are available, the device attempts to connect to the specified IP address on the specified port with the configured protocol. The device will remain connected until a remote device closes it or a session time-out occurs.

The screenshot shows the 'Add Ethernet Remote Driver' configuration window. It has several sections:

- Group :** PortGroup
- Alias *:** SSH-Secured
- Remote IP Address *:** 192 . 168 . 1 . 55
- Port *:** 5000
- Protocol **:** SSH
- SSH Credentials** section:
 - Prompt for Credentials
 - Username *:** bob_engineer
 - Password *:** [redacted]
- Listening Ports :** (Empty list box)

At the bottom, there are notes: * Required and ** Listening ports selection is ignored if Protocol is Modbus. A **Submit** button is at the very bottom right.

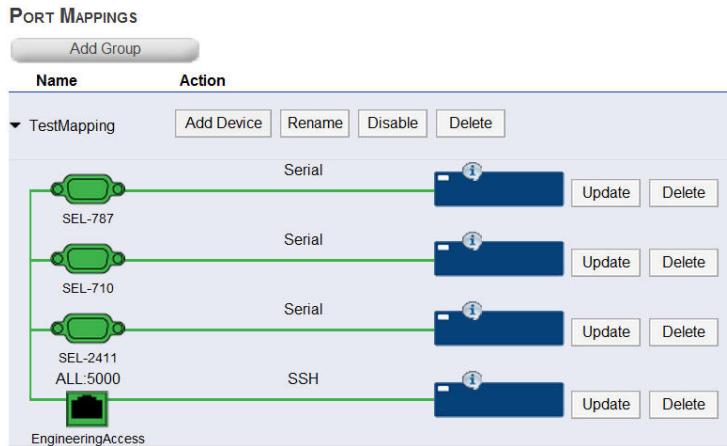
Figure 5.48 Add Ethernet Connect Remote Form

Table 5.34 Add Ethernet Connect Remote Form Settings

Name	Values	Description
Alias	As many as 32 characters	Name of the Ethernet connect remote device. Once you configure this alias, you cannot use it in another group.
Remote IP Address	www.xxx.yyy.zzz	The Ethernet connect remote device will attempt to connect to the IP address you specify here. The device will automatically use the most appropriate network interface.
Port	1–65535	The port of the device to which the Ethernet connect remote device will connect.
Protocol	Raw TCP, Telnet, SSH, Modbus TCP, UDP	The configured protocol for the specified Ethernet connect remote device. When configured as SSH, the device acts like an SSH client and authenticates to the remote SSH server by using either the username and password you entered into the SSH Credentials boxes or by prompting you for credentials.
SSH Credentials: Prompt for Credentials	Check box	If you select this box, the device prompts you for credentials before it connects to the remote SSH Server. If you configure multiple SSH Ethernet connect remote devices in the same group to prompt for credentials, the device only prompts for credentials once and then uses those same credentials for all connections you have selected for prompting.
SSH: Username/Password	As many as 128 characters for each box	Enter the username and password for the remote SSH server to which the Ethernet connect remote device will connect. The device automatically accepts any host key the remote SSH server offers to it. Password strength requirements depend on the remote SSH server.
Listening Ports	Check box for every configured device in the group	The port you are presently configuring will receive data from any device you have selected in this list.

Above each Port Group diagram, you have the option to add a device to the group, rename, disable, or delete the group. On the right side of each device, you can choose to update or delete the device.

Figure 5.49 is an example of a port map with three serial devices and one Ethernet listen local device with SSH that is configured as a master port. For details about the maximum number of port groups, devices, and capabilities specific to the device, see Table 5.35 below.

**Figure 5.49 Example Port Mapping****Table 5.35 Device Capability Matrix**

Functional Component	SEL-3610 Port Server	SEL-3620 Ethernet Security Gateway	SEL-3622 Security Gateway
Maximum Number of Port Groups	As many as 25	As many as 25	As many as 25
Maximum Devices Per Group	As many as 18	As many as 32	As many as 32
Max Serial Devices	As many as 17 per group	As many as 17 per group	As many as 4

Table 5.35 Device Capability Matrix

Functional Component	SEL-3610 Port Server	SEL-3620 Ethernet Security Gateway	SEL-3622 Security Gateway
Max TCP Ethernet Listen Local Devices	One per group	One per group	One per group
Max UDP Ethernet Listen Local Devices	One per group	Many	Many
Max Ethernet Connect Remote Devices	One per group	Many	Many
Sessions per Ethernet Listen Local to Connect Remote	Many	Many	Many
Maximum Number of Master Ports	One per group	One per group	One per group
Scripting	No	Yes	Yes
Sessions per Master Port	n/a	1	1
Sessions per Scripted Master Port	n/a	10	10
Modbus Serial/Ethernet Conversion	Yes	Yes	Yes
DNP3 Serial/Ethernet Conversion	Yes	Yes	Yes
Bit-Based Serial/Ethernet Conversion	Yes	Yes	Yes

Using the Master Port

With a master port (not available with the UDP protocol), you can authenticate to the device and choose from a list of any Ethernet connect remote device or serial device belonging to the same group. To connect to a master port such as that in *Figure 5.49* (Example Port Mapping), open a terminal program and connect to the corresponding Ethernet TCP port or serial COM port. In this example, we are connecting to TCP Port 5000 at IP address 192.168.1.20 with SSH. When connecting to a master port, the device will display the usage policy from the web management page. You must then enter a valid username and password to authenticate to the device.

```

login as: admin
Pre-authentication banner message from server:
This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
End of banner message from server
admin@172.29.131.1's password:

*help
WHO      - Display the list of ports available for connection.
SElect   - Select a port and initiate a connection.
CHEck <OUT|IN> <target> - Set to initial device passwords, or restore device passwords.
EXIT     - Log out of this master port.
HELP     - Display help information.

*

```

Figure 5.50 Terminal Access to Master Port

Successful authentication results in display of “*”. You then have four commands available: **WHO**, **SELECT**, **EXIT**, and **HELP**. Special **SELECT SELF**, **CHECK OUT**, and **CHECK IN** commands are available if you have enabled master port scripting. See *Section 6: SEL-3620 and SEL-3622 Security Services* for more information about the **SELECT SELF** case. See *Section 7: Proxy Services and Password Management* for more information about the **CHECK OUT** and **CHECK IN** commands. *Table 5.36* contains a description of master port commands.

Table 5.36 Master Port Commands

Command	Usage	Example	Description
WHO	who	*who	Displays a numerically listed set of aliases for other ports in the same group as the master port.
SELECT	SELECT (Device Alias) or SELECT (# in List of Devices)	*sel SEL-2411 or *sel 1	Selects a device to which you will tunnel. Allows you to interact directly with the device interface.
CHECK OUT	CHE OUT (Device Alias) or CHE OUT (# in List of Devices)	*che out SEL-787 or *che out 1	Checks out a device and resets device passwords back to initial values based on user permissions.
CHECK IN	CHE IN (Device Alias) or CHE IN (# in List of Devices)	*che in SEL-787 or *che in 1	Checks in a device and restores secure passwords. Only usable by the user who checked out the device.
EXIT	exi	*exit	Logs out and disconnects you from the master port.
HELP	hel	*hel	Displays a list of valid commands.

Use the **WHO** command to see a numerically ordered list of configured devices in the port group. Use the **SELECT <ALIAS>** or **SELECT #NUMBER** command to enter the interface of the respective device. See an example of this in *Figure 5.51*.

```
*who
Available Devices:
 1      SEL-2411
 2      SEL-710
 3      SEL-787

*sel 1

=id

"FID=SEL-2411-R104-V0-Z001001-D20080606", "08D0"
"BFID=BOOTLDR-R300-V0-Z000000-D20051214", "0944"
"CID=19C7", "0261"
"DEVID=SEL-2411", "03F2"
"DEVCODE=64", "0311"
"PARTNO=241101A3A2X71851130", "0683"
"CONFIG=111120", "0389"

=
```

Figure 5.51 Device List and Connect

Once the master port connects you transparently to the device, you can view status, download settings through the use of YMODEM and QuickSet, and perform operations as usual. To exit the session with the device, you can enter the termination sequence (default = <Ctrl+W>) to return to the master port level.

Performing Modbus Conversion

The Modbus conversion capability allows serial Modbus RTU/ASCII products to communicate with Ethernet Modbus TCP products. In this mode, the port server supports a one-to-one map between a serial Modbus server address and Modbus TCP unit ID. One Modbus TCP source can communicate with multiple serial Modbus addresses on one serial port of the port server in configurations where the physical serial port is set to EIA-422 or EIA-485.

To configure Modbus protocol conversion, you must add Modbus serial devices and either an Ethernet listen local or Ethernet connect remote configured with Modbus TCP protocol. To add a Modbus TCP unit ID to Modbus serial server address mappings, select **Modbus** near the Ethernet device mapping diagrams. You can either add or update new mappings (see *Figure 5.52*).

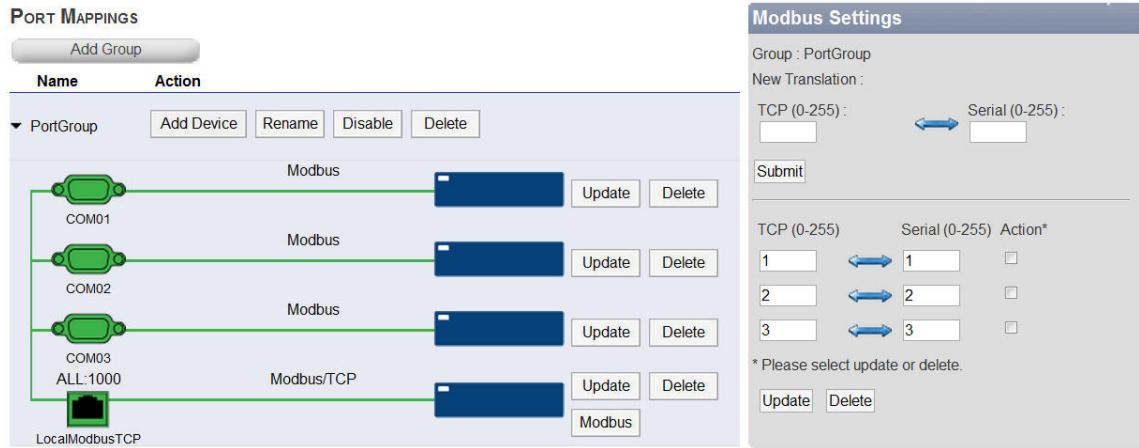


Figure 5.52 Modbus Conversion Configuration

Port Group Diagnostics

For easy visualization of port mapping status, the device can display diagnostic information for each configured serial or Ethernet device in a port group. This diagnostic information appears when you hover your mouse over a diagnostic bubble for each device representation on the Port Mappings page.

For Ethernet devices, the device shows diagnostic information such as Connection Status, Inactivity Status, Bytes Received, Bytes Sent, and Bytes Dropped. See *Table 5.37* for an explanation of these diagnostics.

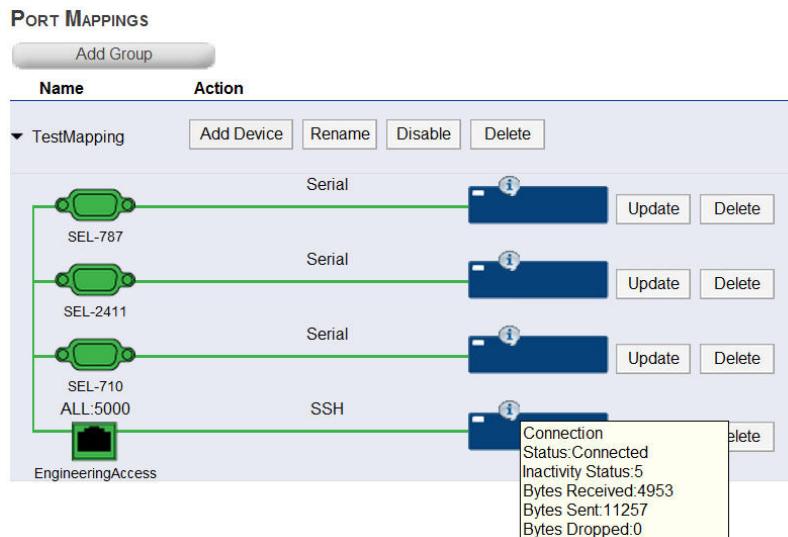


Figure 5.53 Ethernet Device Diagnostics

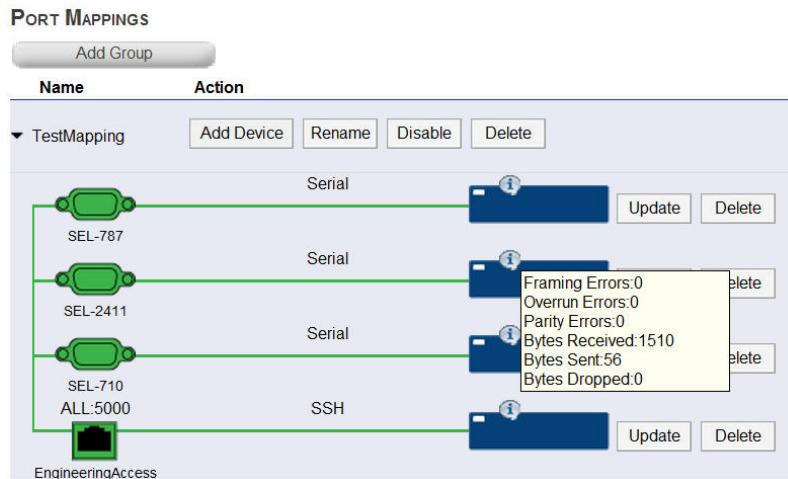
Table 5.37 Ethernet Diagnostics Explanation

Diagnostic	Description
Connection Status	This will show Connected or Disconnected.
Inactivity Status	Amount of time in seconds since receipt of the last packet from the local/remote device.
Bytes Received	Total number of data bytes received.

Table 5.37 Ethernet Diagnostics Explanation

Diagnostic	Description
Bytes Sent	Total number of data bytes transmitted.
Bytes Dropped	Number of bytes dropped as a result of internal buffering.

For serial devices, the device shows diagnostic information such as Framing Errors, Overrun Errors, Parity Errors, Bytes Received, Bytes Sent, and Bytes Dropped. See *Table 5.38* for an explanation of these diagnostics.

**Figure 5.54 Serial Device Diagnostics****Table 5.38 Serial Diagnostics Explanation**

Diagnostic	Serial Port Mode (Byte or Bit)	Description
Framing Errors	Byte mode only	Number of framing errors that have occurred since initialization.
Overrun Errors	Byte and Bit modes	Number of overrun errors that have occurred since initialization.
Parity Errors	Byte mode only	Number of parity errors that have occurred since initialization.
Bytes Received	Byte and Bit modes	Total number of data bytes received.
Bytes Sent	Byte and Bit modes	Total number of data bytes transmitted.
Bytes Dropped	Byte and Bit modes	Number of bytes dropped as a result of internal buffering.

Security

Selecting the **Security** link in the navigation panel causes the device to display the Security Settings description page. This provides an overview of some of the security features the device uses to protect itself and the traffic passing through it. These security features include the following:

- ▶ X.509 Certificates
- ▶ Allowed Clients
- ▶ SSH Host Key

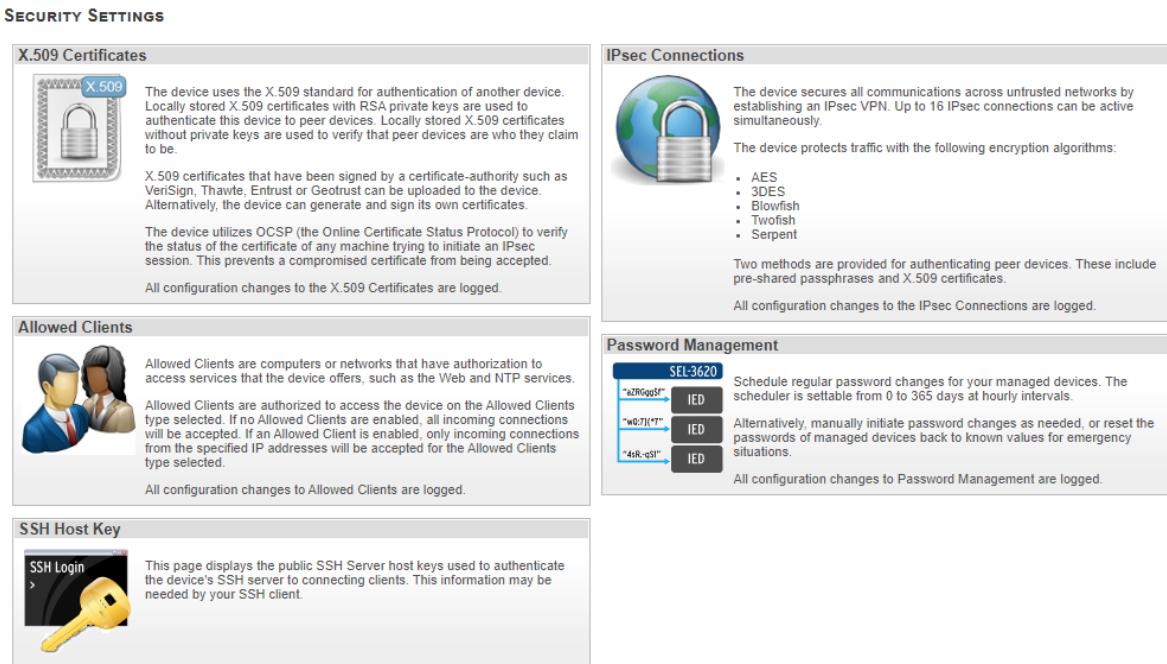


Figure 5.55 Security Settings

X.509 Certificates

The device uses the X.509 standard for authentication of another device over an untrusted network. Use of the X.509 standard ensures that the device at the opposite end of the tunnel is one with which the device has authorization to communicate.

NOTE: All X.509 certificates generated by the device utilize industry-standard Rivest, Shamir and Adleman (RSA) encryption with user-selectable key strengths.

You can upload X.509 certificates signed by either a private CA or one such as VeriSign, Entrust, or Geotrust to the device. Alternatively, the device can generate and sign its own certificates for you to load onto a peer machine. The device logs all configuration changes to X.509 certificates.

The device uses Online Certificate Status Protocol (OCSP) to verify the status of the CA-signed certificate of any machine trying to initiate an IPsec session. This prevents acceptance of a compromised certificate.

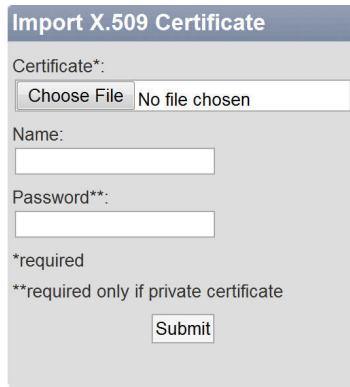
Selecting the **X.509 Certificates** link from the navigation panel causes the device to display a list of all installed X.509 certificates. *Figure 5.56* shows an example.

X.509 CERTIFICATES									
		Import	Generate						
Name	Country	CA	Valid Start	Valid End	OCSP Options				
Default_Web_Cert	US	No	2008-02-26 13:47:52-08	2018-02-23 13:50:01-08	No	View	Export	Rename	Delete
New_Web_Certificate	US	No	2011-06-21 10:55:42.960959-07	2021-06-18 10:55:42.960959-07	No	View	Export	Rename	Delete
Win2008_CA		Yes	2011-05-15 16:51:23-07	2016-05-15 17:01:20-07	No	View	Export	Rename	Delete
ActiveDirectory_Cert		No	2011-05-16 12:01:10-07	2012-05-16 12:11:10-07	No	View	Export	Rename	Delete

Figure 5.56 Installed X.509 Certificates

You can install new certificates onto the device either through an import or generate action. Selecting **Import** located above the X.509 certificate list causes the device to display the Import X.509 Certificate form (see *Figure 5.59*). The device

only supports importing of Privacy Enhanced Mail (PEM) certificates. You can identify these certificates by their .pem, .cer, .crt, and .key file name extensions. To import a PEM certificate, use the following steps.



The form is titled "Import X.509 Certificate". It has a "Certificate*" field with a "Choose File" button and a message "No file chosen". Below it is a "Name:" input field. Underneath is a "Password**:" input field. At the bottom left is a note "*required" and at the bottom right is a note "**required only if private certificate". A "Submit" button is at the bottom center.

Figure 5.57 Import X.509 Certificate Form

- Step 1. Select **Browse** on the Import X.509 Certificate form.
- Step 2. Locate the appropriate PEM certificate on your computer. Select the .pem, .cer, .crt or .key file and select **Open**.
- Step 3. (Optional) Add a name with as many as 128 characters for the certificate. If you supply no name, the device uses the common name (CN) on the certificate, with the serial number of the certificate appended, as the name of the certificate.
- Step 4. If this is a certificate with an encrypted private key, enter the decryption password in the Password box.
- Step 5. Select **Submit**.

The imported certificate will now display in the list.

To generate an X.509 certificate, select **Generate** above the X.509 Certificate list. This causes the device to display the Generate X.509 Certificate form, as in *Figure 5.58*. Enter the necessary information and select **Submit** to generate and store a new X.509 certificate. The device generates the new certificate and add it to the X.509 Certificates list.

NOTE: The SEL-3600 does not support importing of PKCS#12 certificate containers at this time, or DER-encoded X.509 certificates.

Figure 5.58 X.509 Certificate Generation Form

For a description of each setting in the form, refer to *Table 5.39*.

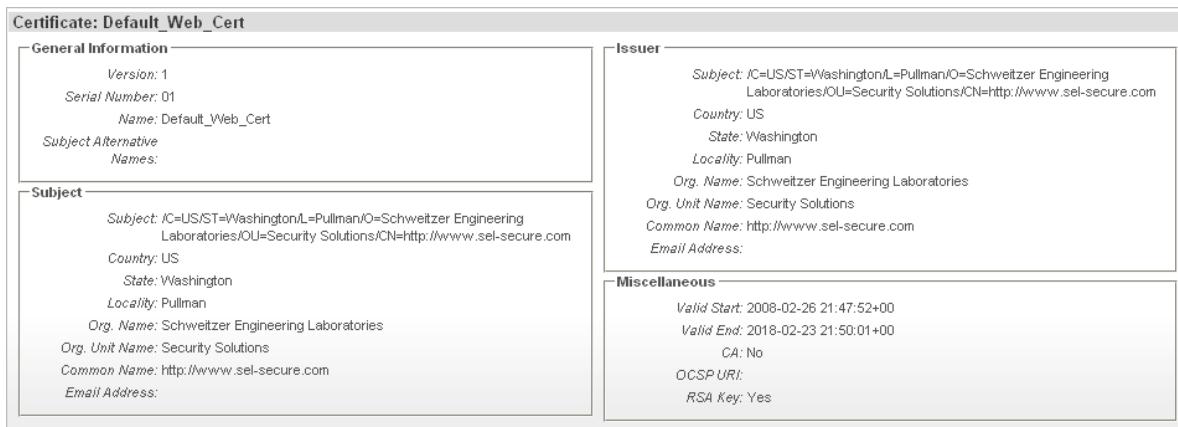
Table 5.39 X.509 Generation Settings

Setting	Values	Description
Name	As many as 128 characters	The name of the X.509 certificate and private key. If you enter nothing, the device generates a name from the common name and serial number of the certificate (optional).
RSA Key Size	1024, 2048, 4096	The X.509 certificate key size. Smaller key sizes are faster to generate and process. Larger key sizes are more secure.
Country Abbreviation	Two-letter country codes	The country in which the owner of the certificate resides.
Common Name	As many as 128 characters	The common name of the certificate should match the domain and host name of the owning device or the IP address of the owning device.
Valid Time Period	30 days, 90 days, 180 days, 1 year, 5 years, 10 years, 20 years	The length of time until the X.509 certificate naturally expires.
State/Province	As many as 128 characters	The state or province in which the organization resides (optional).
Locality	As many as 128 characters	The locality of the organization (optional).
Organization Name	As many as 64 characters	The name of the organization that owns the certificate (optional).
Organization Unit Name	As many as 64 characters	The organizational unit that owns the certificate (optional).
Email Address	As many as 64 characters	A contact point for questions or concerns regarding the certificate (optional).

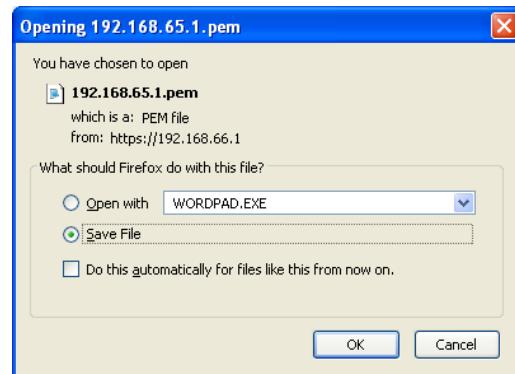
Four actions are available on specific certificates: view, export, rename, and delete. Perform these actions by selecting the appropriate button for each certificate.

NOTE: Neither the device default X.509 certificate or generated certificates will attempt to verify the certificate by using OCSP.

Select the view button to show the View X.509 Certificate page. *Figure 5.59* shows an example of this page. This page provides details of the selected certificate. You can select **Export this Certificate** at the top of the page to verify that you are exporting the correct certificate.

**Figure 5.59 View X.509 Certificate**

Select **Export this Certificate** from the View X.509 Certificate page, or select the export icon from the X.509 Certificate list to download the certificate to your management personal computer (PC) (see *Figure 5.60*). The device will export the certificate in PEM format, and your web browser will handle this as a normal download. Open the file, or save it as necessary.

**Figure 5.60 Export X.509 Certificate**

Select the rename button corresponding to a certificate in the X.509 Certificates list to rename that certificate. This setting only applies to how you would reference this certificate on the device. The device will not export this name with the certificate. Selecting the rename icon shows the Rename X.509 Certificate form.

To delete an X.509 certificate from the device, select the delete icon corresponding to the certificate that you want to delete. The device will display the Confirm Deletion page (see *Figure 5.61*) on which you should see the certificate to be deleted and all settings that rely on the certificate. Selecting **Delete** deletes the certificate and all settings that rely on that certificate. Select **Cancel** to cancel the deletion.

**Figure 5.61 Confirm Deletion**

Allowed Clients

Allowed clients are hosts or networks that have authorization to access Ethernet-based services running on the device. Administrative users can configure allowed clients to access the web management service, the VPN service (SEL-3620 and SEL-3622 only), the port switch, the device time, the SNMP service, the SSH service port, or combinations of any of the five services. The device logs all configuration changes to Allowed Clients.

You can consider allowed clients to be an IP whitelisting of incoming connections to services running on the device. If an administrator has not defined an allowed client for a specific service, then the device will allow any IP address/IP address group name to connect to that specific service. Once an administrator has defined an allowed client for a service, then only that allowed client can use the service, unless the administrator adds more allowed clients for that service.

The allowed client functionality has no control over connections originating from the device itself, such as outgoing IPsec connections and Syslog messages. However, incoming IPsec connections and clients connecting for NTP time updates from the device follow allowed client rules. You can specify as many as 128 separate allowed client entries.

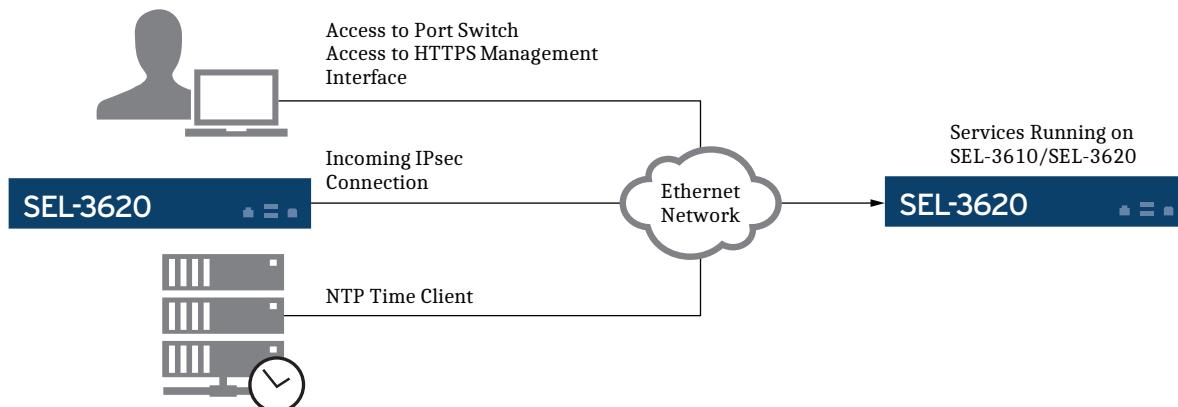


Figure 5.62 Allowed Client Services

Allowed web clients are networks or computers that have authorization to access the HTTPS web management and service port interfaces of the device. If no allowed web clients are enabled, the device will accept all incoming management connection requests. If an allowed web client is enabled, the device will only accept incoming connections from the specified hosts or networks.

Allowed VPN clients (SEL-3620 and SEL-3622 only) are network devices that have authorization to access the IPsec VPN service for the device. If no allowed VPN clients are enabled, the device will only allow IPsec initiation from the enabled Remote Gateways configured on the IPsec Connections page.

Allowed port switch clients are networks or computers that have authorization to access an Ethernet listen local device in any of the port mappings of the device. This includes any master port connection or other Raw TCP, UDP, SSH, Telnet, or Modbus TCP connections into any port mapping. If no allowed port switch clients are enabled, the device accepts all incoming port switch connection requests. If an allowed port switch client is enabled, the device will only accept incoming connections from hosts or networks you specify.

Allowed time clients are networks or computers that have authorization to synchronize NTP time from the device. If no allowed time clients are enabled, the device will allow any client to connect to it for updated NTP time data. If an allowed time client is enabled, the device will only accept incoming connections from NTP clients or networks you specify.

Allowed SNMP clients are networks or hosts that have authorization to poll the device by using SNMPv1/v2c/3 protocol for information found in the device SNMP MIB files. If you have no allowed SNMP clients enabled, the device will allow any client to poll it for SNMP status information. If an allowed SNMP client is enabled, the device will only accept incoming connections from hosts or networks you specify.

Select the **Allowed Clients** link from the navigation panel to show the list of allowed clients (*Figure 5.63*). If you have configured no allowed clients, the list will be empty. Otherwise, you will see all configured allowed clients. To view the Web, VPN, Time, Port Switch, or all configured clients, select the appropriate button above the list.

ALLOWED CLIENTS					
<input type="button" value="Add Client"/> Client Added <input type="button" value="ALL"/> <input type="button" value="Port Switch"/> <input type="button" value="SNMP"/> <input type="button" value="Time"/> <input type="button" value="VPN"/> <input type="button" value="Web"/>					
All Clients	Alias	Address Group Name/IP Address	Description	Types	Options
	Allowed client Test	Address_groups_test		<input checked="" type="checkbox"/> Port Switch <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> VPN <input checked="" type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	User_1	192.168.1.0/24		<input checked="" type="checkbox"/> Port Switch <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> VPN <input type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	User_3	192.168.1.209/32		<input checked="" type="checkbox"/> Port Switch <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> Time <input checked="" type="checkbox"/> VPN <input checked="" type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	User_4	192.168.1.220/32		<input checked="" type="checkbox"/> Port Switch <input type="checkbox"/> SNMP <input type="checkbox"/> Time <input checked="" type="checkbox"/> VPN <input type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	User_5	192.168.1.210/32		<input type="checkbox"/> Port Switch <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> VPN <input type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>
	Allowed client web group	Address_groups_test		<input type="checkbox"/> Port Switch <input type="checkbox"/> SNMP <input type="checkbox"/> Time <input type="checkbox"/> VPN <input checked="" type="checkbox"/> Web	<input type="button" value="Update"/> <input type="button" value="Delete"/>

Figure 5.63 Allowed Clients

Select **Add Client** to display the Add Client form on the right side of the page (*Table 5.64*).

Add Client					
Alias*:	<input type="text" value="User Alias"/>				
Address Group Name/IP Address*:	<input type="button" value="IP Address"/> <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="4"/> . <input type="text" value="50"/> / <input type="button" value="24"/>				
IP Address*:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="4"/> . <input type="text" value="50"/> / <input type="button" value="24"/>				
Client Types*:	<input checked="" type="checkbox"/> Port Switch <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> VPN				
Description:	<input type="text"/>				
<small>*required</small>					
<input type="button" value="Submit"/>					
Your current IP Address is: 192.168.4.59 Not allowing this address as a Web Client will block your current access to the device. This IP address may be the address of your local computer or the address of a proxy between your local computer and the device.					

⚠ CAUTION

If you enable a new web client and your present computer is not in the Allowed Web Clients list, you will be locked out of the web interface.

Figure 5.64 Add Client

NOTE: The IP address from which you are presently accessing the web interface is shown to prevent you from locking yourself out of the web interface when you create a new web client. The address that displays may be your local address or the address of a proxy between your local host and the device.

Enter the appropriate information and select **Submit** to configure a new allowed client. See *Table 5.40* for a description of each of these settings.

Table 5.40 Allowed Client Settings

Setting	Values	Description
Alias	As many as 32 characters	A unique identifier for the allowed client.
Description	As many as 255 characters	A description of the usage and purpose of the allowed client.
IP Address Groups	As many as 16 group members	IP address groups for the allowed client.
IP Address	www.xxx.yyy.zzz/aa	The IP address or network ID of the allowed web clients. If you are selecting the entire network, you must enter the base address of the subnet. Use CIDR notation to assign the subnet mask.
Client Types	Port Switch, SNMP, Time, VPN, Web	Indicates the type of client. Clients can be Port Switch, SNMP, Time, VPN, Web, combinations of the four, or all.

You can either update or delete from the Allowed Clients list. To perform one of these actions, select the appropriate button associated with the entry you want to modify.

Select **Update** to display the Update Client form on the right side of the page. Edit the boxes that need changes, and select **Submit**.

Select **Delete** to remove an allowed client from the device. You will need to confirm the deletion before the device removes the allowed client.

SSH Protocol

NOTE: SSH protocol is implemented in software, so you may experience degraded performance during periods of high processor burden.

The Secure Shell protocol is used to protect port mapping communication when chosen as the Ethernet Listen Local or Ethernet Connect Remote Protocols. SSHv2 will be used to protect either the outgoing or incoming link. All SSH sessions are protected with a username and password combination. Any username-password combination that allows access to the SEL-3600 web or proxy interfaces will be accepted when an Ethernet Listen Local port mapping device is configured with SSH. A username password combination to access the remote SSH server must be entered when configuring an Ethernet Connect Remote port mapping device. The SEL-3600 devices do not support SSH key-based authentication. The following list shows the SSHv2 ciphers the SEL-3600 supports in order of priority. The protocol uses the highest priority cipher that the SSHv2 peer accepts.

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes256-cbc
- aes128-cbc
- blowfish-cbc
- 3des-cbc

The SEL-3600 supports two secure key exchange algorithms: diffie-hellman group14-sha256 and elliptic-curve-diffie-hellman, ecdh-sha2 nistp256. The SEL-3600 also supports legacy key exchange algorithms diffie-hellman-group14-sha1 and diffie-hellman-group1-sha1. SEL recommends using the secure ciphers, the legacy algorithms are provided for compatibility. These are used to initialize the cryptographic sessions between the server and the client.

The device supports two message digest algorithm: hmac-sha1 and hmac-sha2-256.

Key Exchange Algorithms

To establish a successful SSH connection, the SEL-3600 must agree with the SSH peer on many parameters including the key exchange algorithm, public/private keys, ciphers, and Hash Message Authentication Code (HMAC). *Table 5.41* shows the advertised host keys, ciphers, and HMACs for the SEL-3600 SSH protocol's selectable key exchange algorithm. If multiple key exchange algorithms are selected, the advertised host keys, ciphers, and HMACs are cumulative (without duplicates).

Table 5.41 Key Exchange Algorithm

Kex	Host Key	Cipher	HMAC
ecdh-sha2-nistp256	ecdsa-sha2-nistp256, rsa-sha2-256	aes128-ctr,aes192-ctr,aes256-ctr	hmac-sha2-256
kex-diffie-hellman-group14-sha256	rsa-sha2-256, ssh-rsa	aes128-ctr,aes192-ctr,aes256-ctr	hmac-sha2-256
kex-diffie-hellman-group14-sha1,kex-diffie-hellman-group1-sha1	ssh-rsa, ssh-dss	aes128-ctr,aes192-ctr,aes256-ctr,aes256-cbc,aes128-cbc,blowfish-cbc,3des-cbc	hmac-sha1

SSH Host Key

NOTE: The device SSH Host Key is regenerated upon factory-default reset.

You can use either device as an SSH server to authenticate and encrypt incoming connections to the port switch of the device. The device presents the SSH host key for incoming user connections to any configured SSH Ethernet listen local driver. You can find this key on the web configuration interface under SSH Host Key in the navigation window on the left side of the page. The RSA, DSA, and ECC keys are 1024 bits in length, and it displays in read-only PEM format.

SSH MANAGEMENT		
Type	Key	Options
DSA Public Key (SHA1 Hashing)	<pre>-----BEGIN PUBLIC KEY----- MIIBtjCCASgByqGSM44BAAwgEeAoGBALamyATzF12o1Av018H0SPva3gT7Hm2N KHa0lu6vbp8+Zc6AlxURJrBHuu+4xh0fsuVk4E+FxrRM6vf60q0xPLYTQ+NGBK FUZLlh4tcIaJ6chivC53nxev31yBjhLnx+SXdt+BR7r60js64hvkvG3bkE7gqkN hByf08c/s7DFAHUA7BDm02swNeZusfrab+bNwYeFb0CgY0SzF5mghdjeZgqkN Ivk3GijsVrezo/cQEh6At3CFeJyvF1BBF3BgMr4t4bA6/opub3fvBd+haQjriz q0dgdiuNZASRLSKAe5FDG4RFR0+OcyQfhPolnDDEAF91gkcmHId9EHNHeD20+ zwABP883If1M1CVFKQg0Pn+gOBhACgAvolN31+s8yEgA1aMM4jsBEVjinxv5 3hX5p14u1kd1QTVbhVFRKx8c+9VswRMq51JwenRuEhwyub/hddbosdocTMvrrh RemFuubndjfUI6jyx3MEMStz+CyklzukJtSgeC/khC5N19DgpcQ8eTSe3LnCMChZ yHJ6ATIhkxAI4u== -----END PUBLIC KEY-----</pre>	<button>Generate New SSH Keys</button>
RSA Public Key (SHA1 Hashing)	<pre>-----BEGIN PUBLIC KEY----- MIICjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAv9dmkqu85Q/hcA3VtMub 4nsvcKvhTYdxGsVKJTv3fIz113MiMECIQLmUrQEYuVe15jA605NgVpr60mjpu1 DUmgOHnmzb4xWMuIZzR0/S3bv4khkp4r5CptfIVk1b9CKEvf25Ynvd1fl83brv r92vuLyDj61mDvbwlwOrU6Fs8xXmYqz7dhNkt8d/19uii/7FGa2jMpnRdQ7+BP 7BVvvwA+IrZmXugvJZyp1lN/gy3kdnIFcpLSYmXQq47zccuVYS5kA9UFh2GfJ1o U1b+149ND84kyHLhtosaYuVluP3JKQ2mq47auUkPHTxzvheiBYJqpLXQZF+6w YwIDAQAB -----END PUBLIC KEY-----</pre>	<button>Generate New SSH Keys</button>
RSA Public Key (SHA2-256 Hashing)	<pre>-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAv9dmkqu85Q/hcA3VtMub 4nsvcKvhTYdxGsVKJTv3fIz113MiMECIQLmUrQEYuVe15jA605NgVpr60mjpu1 DUmgOHnmzb4xWMuIZzR0/S3bv4khkp4r5CptfIVk1b9CKEvf25Ynvd1fl83brv r92vuLyDj61mDvbwlwOrU6Fs8xXmYqz7dhNkt8d/19uii/7FGa2jMpnRdQ7+BP 7BVvvwA+IrZmXugvJZyp1lN/gy3kdnIFcpLSYmXQq47zccuVYS5kA9UFh2GfJ1o U1b+149ND84kyHLhtosaYuVluP3JKQ2mq47auUkPHTxzvheiBYJqpLXQZF+6w YwIDAQAB -----END PUBLIC KEY-----</pre>	<button>Generate New SSH Keys</button>
ECC Public Key (SHA2-256 Hashing)	<pre>-----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQdBQgAEkJRJf36hQcMu9ZL019ucYqqUvD0 ChrjX1qvtQ3HzPUQi7yBR58+16gcPc2dnns9s77/esih3yGwV9oCQ=</pre>	<button>Generate New SSH Keys</button>

Figure 5.65 Device SSH Host Key

NOTE: You can export or import the SSH host key as part of the System Settings function under File Management. If you export the system settings of one device and import them into another device, the new device will have the same SSH host key as the old device.

When users connect to the device, they can verify the SSH host key of the remote server against the known key value the web configuration page provides. This helps prevent possible man-in-the-middle attacks against the SSH connection, where a malicious entity could potentially masquerade as the legitimate end device by presenting an alternate key. Users can generate new RSA, DSA, and ECC host keys by selecting **Generate New DSA SSH Keys**, **Generate New RSA SSH Keys**, or **Generate New ECC SSH Keys**. When new SSH keys are generated, or different key exchange algorithms are selected, all existing connections are immediately closed.

exe-GUARD

SEL integrates embedded exe-GUARD antivirus technology for SEL-3620 Ethernet Security Gateway, SEL-3622 Security Gateway, and SEL-3610 Port Server devices. exe-GUARD provides Host Intrusion Prevention (HIP) protections against past, present, and future malware threats via a potent whitelist defensive architecture. This technology eliminates the need for signature updates and adds zero settings to the device.

SEL designed and built exe-GUARD as part of a cooperative project with the U.S. Department of Energy (DOE), Dominion Virginia Power (DVP), and Sandia National Laboratories (SNL). exe-GUARD provides protection against rootkits, contains kernel-level whitelisting with secured memory privileges, and implements mandatory access controls (MACs). exe-GUARD also provides powerful resistance to code injection with executable whitelisting. exe-GUARD helps support NERC CIP compliance efforts.

exe-GUARD is always enabled on the device on firmware versions R200 and later and cannot be disabled. To check the running status of exe-GUARD, navigate to **Diagnostics**, and select **Update Diagnostics**. After the device refreshes the page, navigate to the bottom of the diagnostics output and review the following lines:

NOTE: Autoscopv was removed in firmware R210. For prior firmware releases R200 to R208, Autoscopv Status was 1.

1. SELinux Audit Failures: (blank)
2. SELinux Enabled: Enforcing
3. Autoscopv Status: 0
4. Whitelist Enabled: 1

You can also poll the device via SNMP to gain information about the state of exe-GUARD on the system. The SNMP Management Information Bases (MIBs) pertaining to items 1–4 are as follows:

- .1.3.6.1.4.1.31823.3.1.1.2.3 (Number of Audit Failures)
- .1.3.6.1.4.1.31823.1.3600.1.2.2 (SE Linux Status)
- .1.3.6.1.4.1.31823.1.3600.1.2.1 (Autoscopv Status)
Autoscopv was removed in firmware R210, so this MIB will not be present in R210 or later.
- .1.3.6.1.4.1.31823.3.1.1.1 (Whitelist Status)

For more about SNMP, see *SNMP* on page 5.29.

If you see anything different than what is listed, contact an SEL representative immediately. The device sends violations that exe-GUARD discovers via both SNMP Traps and Syslog. The text in those logs is documented in *Appendix F: Syslog*.

Reports

Selecting the **Reports** link in the navigation panel causes the device to display the Reports description page. This provides an overview of the reporting capabilities of the device, including the system logs to monitor events on the device and internal diagnostics to troubleshoot device functionality.

The screenshot shows the 'REPORTS' page with the following sections:

- System Logs**: Describes the Syslog message format and its fields (Severity, Facility, Tag, Time, Message). It also mentions the 7 severity levels and the timestamp field.
- Diagnostics**: Provides actions for troubleshooting, such as Update Diagnostics, Halt System, Restart System, Ping, and Lamp Test. It includes a warning about physical access required for system restart.
- Proxy Reports**: Details the Proxy Reports page, which allows users to collect and export audit reports for management and user activity.
- Summary**: A brief overview of the available reports: Commands and Devices, Password Updates, and Managed Device Passwords. It notes that the Managed Device Passwords report is only available to users with administrative privileges.

Figure 5.66 Reports Settings

System Logs

The device uses the Syslog message format to record event data. The device can store 60,000 of these messages. The device can also forward Syslog messages to three destinations.

The Syslog message format includes five fields:

- Severity
- Facility
- Tag Name
- Time Stamp
- Message

A message can have seven different severity ratings, ranging from informational to emergency. There are three possible facilities on the device: user, system, and security. User and System messages are user- or non-user-initiated events unrelated to security, while security messages relate to changes in secure communication. The Tag Name box indicates which part of the system generated the message. The Time Stamp and Message fields include the time stamp from when the device generated the message and the message description. For more information about Syslog messages, refer to *Appendix F: Syslog*.

Select the **System Logs** link from the navigation panel, to show the internal system logs (*Figure 5.67*).

The screenshot shows a table titled "SYSTEM LOGS" with the following data:

Ack	Time Stamp	Tag Name	Severity	Facility	Message
<input type="checkbox"/>	2011-06-21 07:43:44	WebServer	Warning	SECURITY	Login while the default Web server authentication certificate was active
<input type="checkbox"/>	2011-06-21 07:43:44	Login	Notice	SECURITY	Login to Web: successful by admin at 192.168.1.111
<input type="checkbox"/>	2011-06-20 16:57:37	Login	Notice	SECURITY	Timeout Web: admin at 192.168.1.111
<input type="checkbox"/>	2011-06-20 16:46:36	WebServer	Warning	SECURITY	Login while the default Web server authentication certificate was active
<input type="checkbox"/>	2011-06-20 16:46:36	Login	Notice	SECURITY	Login to Web: successful by admin at 192.168.1.111
<input type="checkbox"/>	2011-06-20 16:41:27	Login	Notice	SECURITY	Timeout Web: admin at 192.168.1.111

Figure 5.67 System Logs

Device system logs are displayed in the order of their generation. Select a box label at the top of the list to reorder the messages according to the value of that box. For example, selecting the severity label reorders the list by severity.

Event messages in the device have two states: unacknowledged and acknowledged. Unacknowledged messages always appear before acknowledged messages in the list. These two states help make identification of abnormal event generation easier. Large numbers of unacknowledged messages can indicate high levels of activity on the device.

Message acknowledgment also exists to assist log documentation. In your periodic examination of logs, be certain to acknowledge the existing logs. In future log examinations, you can limit the logs of concern to only those the device generated since your last examination.

You can filter the device system logs to track certain events. Configure the filters with the form above the System Logs list (*Figure 5.68*).

**Figure 5.68 System Log Filters**

The three dropdown combo lists are filters for the Severity, Facility, and Tag boxes. Select the appropriate boxes and values to filter out all messages but those that match your selections. Select **Filter** to process the filters and display the results.

Other filters are based on message content and the time box. Enter a start time and end time to display all events that occurred within the times of interest. Enter a message string to display all events that have a matching message. Select **Filter** to process the filters and display the results.

Select **Clear** to clear the filters and display all system logs.

There are two action buttons above the System Logs list: Acknowledge All and Download All. Select **Acknowledge All** to acknowledge all unacknowledged system logs. Select **Download All** to download all system logs in comma-separated values (CSV) format.

You cannot remove system logs from the device without issuing a factory-default reset. For more information about using the Factory-Default Reset feature, refer to *Diagnostics* on page 5.61.

Diagnostics

The diagnostics page contains information, such as the present state of the device, that may be useful for troubleshooting.

If you have administrative privileges, you can perform the following actions from the diagnostics page. These actions can help resolve problems you encounter while using the device.

- Update Diagnostics
- Halt System
- Reboot System
- Lamp Test
- Ping Host

CAUTION

Halting the system requires physical access to the device to restart it.

CAUTION

To avoid losing system logs during a factory-default reset, configure the device to forward Syslog messages.

A nonadministrative user will not be able to see the **Halt System** button.

The Update Diagnostics action updates the diagnostics to the present running state. The Reboot System action restarts the device. The Halt System action shuts down the device. The Lamp Test action causes the device to cycle its LEDs through each supported color and state. The Ping Host action will issue ICMP ping messages to the entered IP address and will return a message indicating whether the host is up (if ping responses are received) or down (if no responses are received).

For more information about the Diagnostics page, refer to *Section 8: Testing and Troubleshooting*.

This page intentionally left blank

S E C T I O N 6

SEL-3620 and SEL-3622 Security Services

Introduction

This section explains the security-specific settings of the SEL-3620 and the SEL-3622. Except as otherwise noted, references to the SEL-3620 refer also to the SEL-3622.

- *Firewall* on page 6.1
- *Network Address Translation* on page 6.6
- *IPsec Connections* on page 6.10
- *MACsec Connections* on page 6.16

Firewall

The SEL-3620 configurable, stateful firewall inspects all traffic as it passes through, denying or permitting packets according to a set of defined rules. The firewall follows a deny-by-default security posture. You can use the firewall to filter traffic according to the following.

- Transport Protocol
- IP Address or IP Address Group
- Port Number or Port Group
- Encryption State

The device logs all configuration changes to the firewall. Additionally, the device can log all connections closed, rejected, dropped, or established to, or through, the firewall.

A stateful firewall protects the internal network by monitoring the state of network connections, such as TCP streams, that route through the network. This operation minimizes processing necessary for packets that are part of an existing session, so the firewall functions very efficiently. By default, the SEL-3620 denies all connection attempts. You must create rules to explicitly allow traffic through the firewall. Selecting the Firewall link from the navigation panel causes the device to display the firewall rules in *Figure 6.1*.

The screenshot shows the SEL-3620 Firewall Rules configuration. It includes two main sections: Global Rules and Eth 1 Interface Rules.

- Global Rules:**

Global Order	Interface	Alias Status	Verbose Logging	Source Port	Description Protocol Rule	Destination Port	Options
1	All Interfaces	RTAC_Group Enabled		Address_groups_test test_port_groups	TCP ACCEPT	0.0.0.0/0 1-65535	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
3	All Interfaces	Allow All Enabled		0.0.0.0/0 1-65535	TCP/UDP ACCEPT	0.0.0.0/0 1-65535	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>

Graphical representation: A cloud icon (representing all IP addresses) is connected to a server icon (representing the destination port range).
- Eth 1 Interface Rules:**

Eth 1 Interface Rules	Network Address Alias	Alias Status	Verbose Logging	Source Port	Description Protocol Rule	Destination Port	Options
2	Eth 1	Allow RTAC Enabled		0.0.0.0/0 1-21000	TCP ACCEPT	Address_groups_test test_port_groups	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>

Graphical representation: A cloud icon is connected to a server icon.

To the right of the interface rules is a modal window titled "Add Firewall Rule" for creating a new rule. It includes fields for Alias*, Description, Action (ACCEPT), Protocol (TCP), Address Alias (All), Verbose Logging Enabled, Source (IP Address: 0.0.0.0/0), Destination (IP Address: 0.0.0.0/0), and Port Range (From: 1 To: 65535). There are also checkboxes for Invert and required, and a "Submit" button.

Figure 6.1 Firewall Rules

Figure 6.1 shows an example of the firewall rules in the SEL-3620. For descriptions of each of the symbols, see Table 6.1.

Table 6.1 Firewall Symbols

Symbol	Description
	Represents all IP addresses.
	Represents a specified range of IP addresses.
	Represents a specific IP address.
	The device will forward to its destination any traffic matching this rule.
	The device will block traffic matching this rule from reaching its destination.
	The device will block traffic matching this rule from reaching its destination and send a message to the source that the ICMP destination is unreachable.

On the right side of the page is the General Rule Settings form. You can use the check boxes in this form to quickly set the firewall and change the view of the rules table. Table 6.2 contains a description of each of these features.

Table 6.2 General Rule Settings

Check Box	Description
Drop Ping	Drops all ping packets to or through the SEL-3620. Drop Ping is enabled by default.
Drop Traceroute	Drops all ICMP traceroute packets through the SEL-3620. Drop Traceroute is enabled by default.

Table 6.2 General Rule Settings

Check Box	Description
Must Be Encrypted	Drops all packets that are not going into or coming out of an established IPsec tunnel.
Allow All Encrypted	Allows all packets that are going into or coming out of an established IPsec tunnel.
Verbose Logging	Logs all connections established, closed, dropped, or rejected to the device or through the device. Note: This option can substantially increase the number of logs on the device and can prevent some messages from being sent remotely.
Text-only View	Changes the view of the firewall rules to a text-only view.
Integrated View	Reorders the firewall rules by priority, regardless of interface.

There are two buttons above the firewall rule list: **Add Firewall Rule** and **General Rule Settings**. Selecting the **Add Firewall Rule** button replaces the General Rule Settings form with the Add Firewall Rule form on the right side of the page. All settings you enter into this form will apply to a single firewall rule. Refer to *Table 6.3* for a description of each of these settings. Select **General Rule Settings** to restore the General Rule Settings form.

Table 6.3 Firewall Rule Settings

Setting	Value	Description
Enabled	Check box	Enables processing of the firewall rule.
Alias	As many as 32 characters	A unique identifier for the firewall rule.
Description	As many as 255 characters	A description of the usage and purpose of the firewall rule.
Action	Accept, Drop, Reject	Accept will accept any packet to which this rule applies. Drop will discard any packet to which this rule applies. Reject will discard any packet to which this rule applies and inform the packet source of such rejection.
Protocol	TCP, UDP, TCP/UDP, ESP/AH	Identifies the transport protocol.
Address Alias	All or any physical interface	Identifies the physical interface. This can be any single physical interface or all physical interfaces.
Verbose Logging Enabled	Check box	Enables verbose logging for the firewall rule.
Source IP Group Name/Source IP	www.xxx.yyy.zzz/aa	The IP address or IP address group name of the source of the packet.
Source Port Group Name/Port Range	1–65535	The packet port of origin. ^a
Destination IP Group Name/IP/Network	www.xxx.yyy.zzz/aa	The IP address or IP address group of the destination of the packet.
Destination Port Group Name/Port Range	1–65535	The port of the destination of the packet. ^a
Invert	Check box	Used to invert the entry of the corresponding IP address or port number. An example use for this setting would be to accept all except the address or port you specify.

^a Port settings do not apply to rules regarding the ESP/AH protocol.

Rule processing happens in order of priority. Look at the Order column in the firewall rule table to determine a rule's priority. Alternatively, select **Integrated View** to see all firewall rules in order of priority. When a packet reaches the device, the firewall rule with the highest priority is processed first. If that rule does not apply to the packet, the device processes the rule with the next highest

priority. This continues until either a rule applies to the packet, or the device has exhausted the firewall rule list. If the device has exhausted the firewall rule list, it drops the packet. The global QuickSet rules take precedence over all other rules.

NOTE: When the port and IP address groups are used to create firewall rules, the IP Table rules will multiply but will be limited to fewer than 1,000 user firewall rules, as shown in the diagnostics page.

The priority of firewall rules is very important and can greatly impact packet handling. For example, take the case where you need to allow all UDP traffic except that from a specific interface. For that, you need two rules: one interface-specific rule denying UDP traffic on that interface, and one global rule applied to all interfaces allowing UDP traffic. If the global rule allowing UDP traffic has the higher priority, the device applies that rule to packets on all interfaces that will allow the packet to pass before processing the next rule that denies the UDP traffic from the specific interface.

Automatic Firewall Rules

The system creates automatic firewall rules. When created, these automatic rules are not displayed in the Firewall link of the web user interface.

If the Management Interface Service Port is enabled on a specific port, the firewall will automatically create rules to accept TCP traffic addressed to the device on that port. If the Service Port is disabled but configured to a specific port, the firewall will drop TCP traffic addressed to the device on that port.

The firewall automatically creates rules to allow remote IPsec clients to connect to the local Internet Key Exchange (IKE) connection.

Table 6.4 describes additional conditions under which the firewall automatically creates rules to open specific ports.

Table 6.4 Ports Automatically Opened by Firewall

Port	Protocol	Use	Notes
Configurable	TCP	Service Port	See description above.
20	TCP	FTP	<p>By default, the firewall blocks all access to the FTP data channel port (Port 20). To establish an FTP connection on the control port, the user will need to create a firewall rule that opens Port 21 (the default FTP control port) with the server side as the destination. If so configured, the firewall creates a rule to allow traffic through the FTP data channel port. This automatic rule is created whether the FTP connection is active or passive.</p> <p>If the user chooses to establish an FTP control channel on a port other than Port 21, Port 20 will not be automatically opened and the user will need to create an additional firewall rule to open that port.</p>
123	UDP	NTP	Only open when NTP is enabled and NTP initiates an outbound connection.
161	UDP	SNMP	Only open when SNMP is enabled.
443	TCP	Web Server (Apache)	Default 443. User configurable web server port.
500	UDP	IKE (ISAKMP)	Always open but filtered.

Verbose Logging

As of firmware versions R202 and later, the firewall can optionally log all communication that is meant to go to, or through, the device. If the Verbose Logging feature is enabled, the firewall logs the following information directly to Syslog:

- All established, closed, rejected, and dropped ICMP, UDP, or TCP connections
- Information about the protocol of the packet, and, if applicable, the source and/or destination IP and port
- What action was taken (dropped, rejected, established, or closed)

As of firmware R208 and later, you can select from the following new radio buttons:

- Off
- Dropped/Rejected
- All
- Custom

This change allows granular control (an easy transition to logging everything, when desired) and allows disabling (or enabling) granular logging without editing every rule. This change also gives users the ability to configure per-firewall-rule logging verbosity and disable local verbose logging to obtain more granularity in monitoring and debugging the network.

Main Setting Status	Description
Off	No logging occurs
Blocked	Logging for rules that block occurs
All	Logging for all rules occurs
Custom	Logging for rules that have the logging option set occurs

Two rules that are on by default are Log Default Blocks (e.g., Deny by default rule) and Log Default Accepts (e.g., Web Interface, Port Mappings, Service Port, IPsec, etc.).

The Verbose Logging feature may result in a large number of messages on the device. When you are connected to a public network, the number of messages per day may exceed the 60,000 stored log limit, depending on the activity level of the network interfaces. Take this into account when enabling Verbose Logging.

The device further limits the logging of packets during periods of frequent activity to prevent the logging feature from overwhelming system resources. If the device is connected to one or more remote Syslog servers, you can enable the Remote Anti-Chatter feature on the **Syslog** page to prevent high utilization for logging on bandwidth-constrained links.

When Verbose Logging is enabled, the device will limit the real-time logging of the total number of connections established, closed, rejected, or dropped depending on network conditions. This limit prevents system resources from being overwhelmed in case of a denial-of-service condition. This feature does not limit the real-time bandwidth or throughput capabilities of the device.

Network Address Translation

Network Address Translation (NAT) is available on the SEL-3620 and SEL-3622 as of firmware version R202, and allows the device to effectively hide (or “masquerade”) IP networks behind a user-selectable “public” network interface. The device implements NAT in two ways: Outbound NAT and Port Forwarding. The default NAT webpage is shown in *Figure 6.2*.



Figure 6.2 Default NAT Webpage

Outbound NAT

Outbound NAT is a feature in which IP traffic originating on one or more network interfaces has all source IP addresses changed to match that of the one public network interface. Outbound NAT is a form of Source Network Address Translation (SNAT), and is similar to the NAT functions of a home cable or DSL modem that allows a device on a “private” network to access a public internet destination. An example of Outbound NAT is shown in *Figure 6.3*.

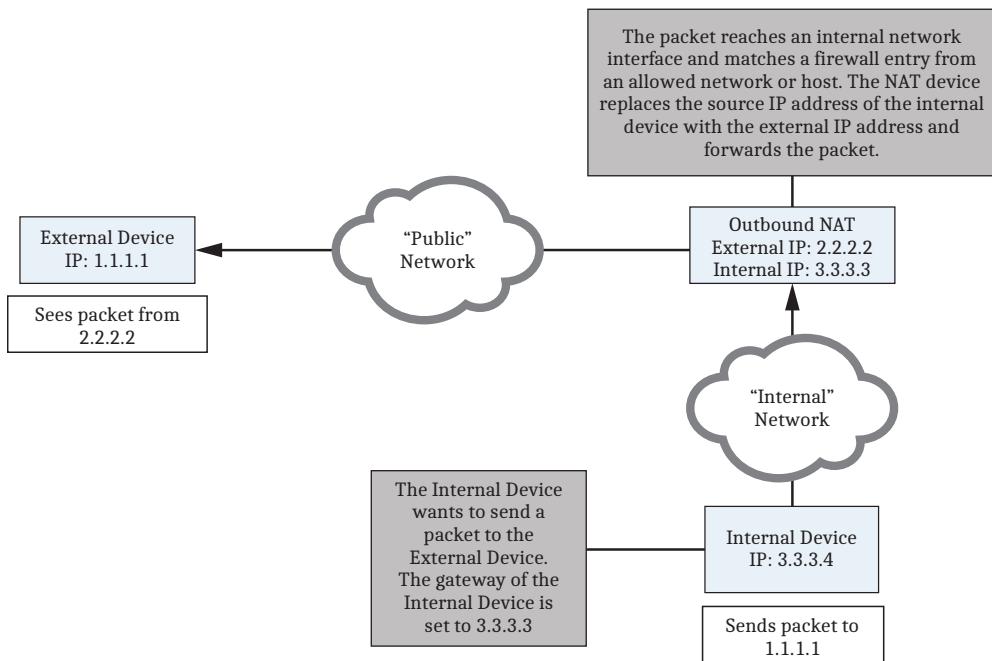


Figure 6.3 Outbound NAT Example

The communications coming from internal networks must match ACCEPT firewall rule entries before the device will forward packets out of the public network interface.

Port Forwarding

Port Forwarding is a feature in which IP traffic originating from a network on or external to the public network interface has its destination IP address changed and forwarded to a device that is accessible via one or more non-public network interfaces on the device. For Port Forwarding to occur, a user must enter one or more Port Forwarding entries, and the incoming traffic originating from the public network interface must match one or more of those entries. Port Forwarding is a form of Destination Network Address Translation (DNAT), and is similar to the NAT functions of a home cable or DSL modem that allow a source on the public internet to send data directly to a device on a “private” network. An example of Port Forwarding is shown in *Figure 6.4*.

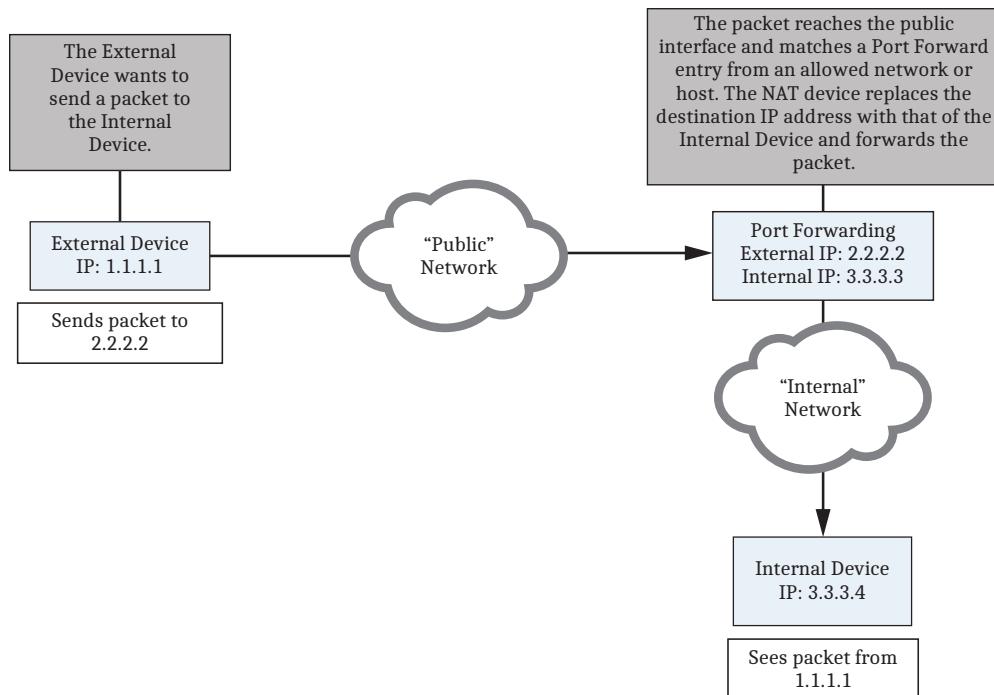


Figure 6.4 Port Forwarding Example

Before the device will forward packets from the public network interface that match a port forward rule, the device will check if the internal destination is reachable via its internal routing table, and that the public source matches an allowed network or host for the entry.

NAT Global Settings

From the NAT page, select **Edit Global Settings** to open the Edit Global Settings dialog box (see *Figure 6.5*).

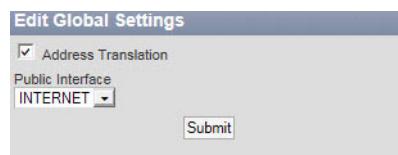


Figure 6.5 Edit Global NAT Settings Dialog Box

In the Edit Global NAT Settings dialog box, **Address Translation** may be enabled or disabled, and the **Public Interface** may be selected for the device. See *Table 6.5* for more details on setting these parameters.

Table 6.5 Global NAT Settings

Setting	Value	Description
Address Translation	Check box	Enables (selected) or disables (cleared) NAT on the device, including Outbound NAT and all configured Port Forwards.
Public Interface	Any configured device interfaces	Lists all configured network interfaces on the device. The chosen network interface will be designated as the Public Interface.

When NAT is enabled, all packets sent through the designated Public Interface—including those from IPsec encrypted network—will have the source IP addresses or address groups replaced with that of the Public Interface. Likewise, all packets arriving into the Public Interface will have the destination IP addresses or address groups replaced with that of the matching port forward private address port.

The **Reset Connections** button at the top of the NAT webpage will clear any Outbound NAT or Port Forward connections that are currently active on the device.

Port Forwarding

From the NAT page, select **Add Port Forwarding Rule** to open the Add Port Forwarding Rule dialog box (see *Figure 6.6*).

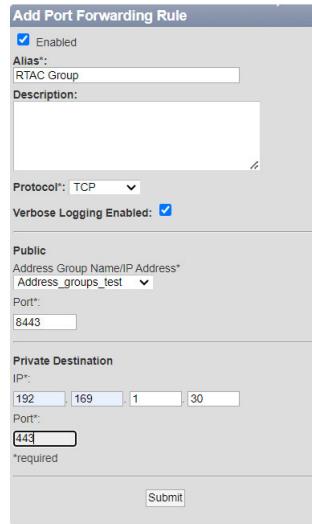


Figure 6.6 Add Port Forwarding Rule Dialog Box

From this dialog box, a Port Forwarding entry may be added. See *Table 6.6* for more details.

Table 6.6 Port Forwarding Rule Settings

Setting	Value	Description
Enabled	Check box	Enables or disables the port forward entry.
Alias	As many as 32 characters	A unique identifier for the port forward entry.
Protocol	TCP, UDP, TCP/UDP	Identifies the transport protocol for the port forward entry.
Public IP Address/Address Group Name	www.xxx.yyy.zzz/aa	The host IP address(es) or network(s) that is/are allowed to access the port forward entry. Set to 0.0.0.0/Any by default.
Public Port	1-65535	The incoming TCP and/or UDP port that will be redirected to the private destination.
Private Destination IP	www.xxx.yyy.zzz	The IP address of the internal host to which the connection is to be forwarded.
Private Destination Port	1-65535	The TCP and/or UDP port of the private host to which the connection is to be forwarded.

Select **Submit** to submit the new Port Forwarding Entry.

All configured port forward entries are listed under Port Forwarding at the bottom of the NAT webpage (see *Figure 6.7*).

Port Forwarding						
Alias	Description	Protocol	Public Source (Address Group Name/IP Address:Port)	Private Destination (IP:Port)	Verbose Logging	Options
FWD_RTAC_GROUP		TCP	Rack_Devices:1234	192.168.1.25:443	Enabled	<button>Update</button> <button>Disable</button> <button>Delete</button>
Port Forward to RTAC web		TCP	0.0.0.0/8442	192.168.1.35:443	Enabled	<button>Update</button> <button>Disable</button> <button>Delete</button>
FWD_to_Remote_RTU		TCP	RTAC_Remote:15010	192.168.1.30:2000	Enabled	<button>Update</button> <button>Disable</button> <button>Delete</button>
TO SEL-2411_Modbus_TCP		TCP	66.77.88.99/32:502	192.168.1.201:20000	Enabled	<button>Update</button> <button>Disable</button> <button>Delete</button>

Figure 6.7 Configured Port Forward Entries

Each rule can be independently updated, enabled, disabled, or deleted. When updating connections, the device will show a dialog window similar to *Table 6.6*. Deleting a port forward entry will result in a confirmation dialog box. Enabling or disabling a connection will change the color of the port forward entry, which represents the current state of the port forward entry. See *Figure 6.8* for an example of the three different port forward states.

RULE 1	TCP	0.0.0.0/50001	192.168.1.250:50001	<button>Update</button> <button>Disable</button> <button>Delete</button>
RULE 2	TCP	0.0.0.0/50002	192.168.1.251:50002	<button>Update</button> <button>Enable</button> <button>Delete</button>
⚠ RULE 3	TCP	0.0.0.0/50003	172.16.1.50:50003	<button>Update</button> <button>Disable</button> <button>Delete</button>

Figure 6.8 Port Forward, Enabled, Disabled, and System Disabled States

In *Figure 6.8*, there are three rules: an enabled rule, a disabled rule, and a system disabled rule.

- The enabled rule (in black; **RULE 1**) is enabled and functioning.
- The disabled rule (in gray; **RULE 2**) has been disabled by the user and is non-functioning.
- The system disabled rule (in gray with exclamation mark; **RULE 3**) has been disabled by the system, because the private destination is not a directly connected network.

The system will disable a port forward entry if network interface changes result in a non-accessible private host, or if a rule is added for a private host that is non-accessible.

NAT Implementation Specifics

Note the following specific details of the NAT implementation of the device:

- Certain system-reserved ports cannot be port forwarded. For example, UDP Port 4500 (IPsec NAT-T) is used by the device, and therefore cannot be forwarded to another interface.
- The device does not support NAT reflection. NAT reflection allows traffic originating from a network interface other than the designated public network interface to access user-created Port Forward mappings. Only IP communications that originate on the designated public network interface can access Port Forwards.
- Only one device network interface can be designated as the public network interface at any one time.
- The device cannot port forward to a device that is not on a local network.
- If your IPsec gateway network interface and NAT public network interface are the same, traffic originating from encrypted subnets (“Local Networks” in the IPsec Connection page) will be translated and forwarded with the source IP address of the outbound NAT interface.
- Global firewall rule settings such as **Allow All Encrypted** and **Must Be Encrypted** affect both Outbound NAT and Port Forwarding rules.
- As many as 200 port forward entries can be added.
- The device allows multiple sources to connect to the same destination.

IPsec Connections

The SEL-3620 and SEL-3622 secure all communications across untrusted networks by establishing an IPsec virtual private network (VPN) between another SEL-3620 or SEL-3622, a Lemnos-compliant device, or a Cisco Layer 3 device. As many as 16 IPsec connections can be active simultaneously on the SEL-3620, and as many as four IPsec connections on the SEL-3622.

NOTE: IPsec is not available on the SEL-3610.

The device provides two methods for authenticating peer IPsec devices. These include pre-shared passphrases and X.509 certificates. The device logs all changes to IPsec Connections.

Select the **IPsec Connections** link from the navigation panel to access the IPsec Connections page (see *Figure 6.9*). This page displays a list of the presently configured IPsec connections.

The IPsec Connections form on the right side of the page contains check boxes you can select to globally enable or disable IPsec on the SEL-3620, and to drop IPsec connections when your X.509 Online Certificate Status Protocol server is inaccessible.

IPsec connections are globally enabled by default, but you can disable these connections to prevent a network compromise from spreading to other networks.

Dropping connections on loss of Online Certificate Status Protocol (OCSP) is disabled by default.

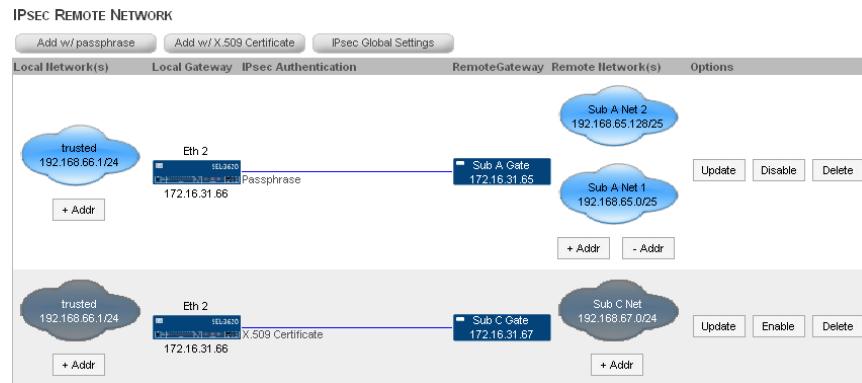


Figure 6.9 IPsec Connections

Select **Add w/Passphrase** to show the Add IPsec using Passphrase form (Figure 6.10) on the right side of the page. IPsec passphrases are pre-shared keys that must match between both endpoints of the VPN tunnel. The device requires strong passphrases for protection against brute force and dictionary attacks. Limit knowledge of all passwords and passphrases to authorized persons and systems.

Figure 6.10 Add IPsec Using Passphrase Form

NOTE: Adding a new IPsec connection to an interface where one or more IPsec connections already exist results in a loss of connectivity.

Complete the Add IPsec using Passphrase form, and select **Submit** to configure a new IPsec Using Passphrase connection. *Table 6.7* describes these settings.

Table 6.7 IPsec Settings

Setting	Values	Description
IPsec Profile	Lemnos IKEv2, Lemnos IKEv1, Cisco, and SEL Secure (2022)	Select the correct IPsec profile to communicate with the remote gateway.
Initiate Connection	Check box	Select this box to have the device request IPsec sessions from the remote device. If cleared, the device must receive a connection request from the peer machine before a tunnel can be established. Only one gateway of the IPsec connection should initiate. NOTE: Normally, the device should not be configured as the initiator. If this option is selected for any connection, and the device is unable to successfully initiate the connection, all IPsec connections will be reset every 200 seconds until all initiated connections are successfully established.
Enabled	Check box	Enable or disable the IPsec connection. This box must be selected for the IPsec connection to be used.
Remote Network IP	www.xxx.yyy.zzz/aa	The network ID of the remote network. This must be the base address in the network. CIDR notation is used to assign the subnet mask.
Remote Network Alias	As many as 32 characters	A name that is associated with this remote network. Aliases must be unique to each remote network.
Remote Gateway	All configured remote gateways	A quick-select dropdown list that contains all of the previously configured remote gateways.
Remote Gateway IP	www.xxx.yyy.zzz	The IP address of the remote gateway.
Remote Gateway Alias	As many as 32 characters	A name that is associated with this remote gateway. Aliases must be unique to each remote gateway.
Description	As many as 255 characters	A description of the usage or purpose of this remote network or gateway.
Local Gateway	All configured local interfaces	Select the appropriate local interface that is connected to the non-secured network.
Local Network	All configured local interfaces	Select the appropriate local interface that is connected to the protected network.

Table 6.8 IPsec Using Passphrase Settings

Setting	Values	Description
Passphrase	As many as 128 characters	The passphrase is a strong passphrase and must be at least eight characters in length. Additionally, the passphrase must contain at least one lowercase letter, one uppercase letter, one digit, and one special character.

Select **IPsec with X.509** to show the Add IPsec Using X.509 Cert. form on the right side of the page. This configuration uses X.509 certificates rather than a pre-shared passphrase for authentication of the peer gateway. The device supports both pre-shared X.509 certificates and CA-signed X.509 certificates. Use CA-signed X.509 certificates to gain the full security advantages of authenticating via X.509 certificates. The device will not be able to detect if pre-shared X.509 certificates are invalid, expired, or stolen. Refer to *Appendix K: X.509* for more information about X.509 certificates.

Use the X.509 Cert. form to complete the Add IPsec Using X.509 Cert. form, and select **Add** to configure a new IPsec Using X.509 connection. *Table 6.9* describes these settings.

Table 6.9 IPsec Using X.509 Certificates Settings

Setting	Values	Description
Remote X.509 Certificate	All installed X.509 certificates	The X.509 certificate that the remote gateway will use to authenticate itself to the SEL-3620.
Treat Remote Certificate as CA	Check box	Identifies the selected Remote X.509 certificate as being the certificate that signed the peer's certificate. Must be the root certificate. An intermediate certificate will not work.
Local X.509 Certificate	All installed X.509 certificates	The X.509 certificate that the SEL-3620 will use to authenticate itself to the remote gateway.

The device comes with preconfigured IPsec profiles to simplify VPN configuration. If the peer gateway is an SEL or Lemnos device with support for IKEv2, select the Lemnos IKEv2 device profile. Any two devices using this profile can communicate with each other through use of the most secure IPsec parameters supported. *Table 6.10* lists the Lemnos IKEv2 profile parameters.

Table 6.10 Lemnos IKEv2 Profile

Parameter	Values
IKE Version	2
IKE Mode	Main
Phase 1 Encryption	AES-256, AES-128, 3DES
Phase 1 Hash	SHA2-256, SHA1
Diffie-Hellman Group	Group 5 (modp1536)
Phase 2 Encryption	AES-256, AES-128, 3DES
Phase 2 Hash	SHA2-256, SHA1
Perfect Forward Secrecy	Group 5 (modp 1536)
IKE Lifetime	10800 s
IPsec Lifetime (ESP Lifetime)	3600 s
Dead Peer Detection	Yes (DPD Delay Time = 60 s, DPD Timeout = 150 s, DPD Action = Clear, DPD Action When Initiating Connection = Restart)

If the peer gateway is a Lemnos device that only supports IKEv1, select the Lemnos IKEv1 profile on the device. All Lemnos devices support the parameters of this profile. You will need to configure the Lemnos device with the necessary parameters to communicate with the device. *Table 6.11* lists the Lemnos IKEv1 profile parameters.

Using IKEv2 profile will result in communications loss or buffering for 2–3 seconds every three hours or so. This is because the SEL IKEv2 implementation uses IPsec break-before-make methodology when the protocol rekeys. If your particular application demands maximum reliability, use either the IKEv1 or Cisco profile because IKEv1 implements make-before-break methods.

Table 6.11 Lemnos IKEv1 Profile

Parameter	Values
IKE Version	1
IKE Mode	Main
Phase 1 Encryption	AES-256, AES-128, 3DES
Phase 1 Hash	SHA2-256, SHA1

Table 6.11 Lemnos IKEv1 Profile

Parameter	Values
Diffie-Hellman Group	Group 5 (modp 1536), Group 2 (modp 1024)
Phase 2 Encryption	AES-256, AES-128, 3DES
Phase 2 Hash	SHA2-256, SHA1
Perfect Forward Secrecy	Group 2 (modp 1024)
IKE Lifetime	10800 s
IPsec Lifetime (ESP Lifetime)	3600 s
Dead Peer Detection	Yes (DPD Delay Time = 60 s, DPD Timeout = 150 s, DPD Action = Clear, DPD Action When Initiating Connection = Restart)

If the peer gateway is a Cisco ASA, PIX, or router, select the Cisco profile. *Table 6.12* lists the Cisco profile parameters.

Table 6.12 Cisco Profile

Parameter	Values
IKE Version	1
IKE Mode	Main
Phase 1 Encryption	AES-256, AES-128, 3DES
Phase 1 Hash	SHA1
Diffie-Hellman Group	Group 5 (modp 1536)
Phase 2 Encryption	AES-256, AES-128, 3DES
Phase 2 Hash	SHA1
Perfect Forward Secrecy	Group 5 (modp 1536)
IKE Lifetime	10800 s
IPsec Lifetime (ESP Lifetime)	3600 s
Dead Peer Detection	Yes (DPD Delay Time = 60 s, DPD Timeout = 150 s, DPD Action = Clear, DPD Action When Initiating Connection = Restart)

For those who want to protect their data in transit with the latest recommended cipher suites from NIST, select the **SEL - Secure (2022)** profile. *Table 6.13* lists the SEL - Secure (2022) profile parameters.

Table 6.13 SEL - Secure (2022) Profile

Parameter	Values
IKE Version	2
IKE Mode	Main
Phase 1 Encryption	AES-256-GCM-16
Phase 1 Hash	SHA2_512
Diffie-Hellman Group	Group 21 (ecp521)
Phase 2 Encryption	AES-256-GCM-16
Phase 2 Hash	SHA2_512
Perfect Forward Secrecy	Group 21 (ecp521)
IKE Lifetime	10800 s

Table 6.13 SEL - Secure (2022) Profile

Parameter	Values
IPsec Lifetime (ESP Lifetime)	3600 s
Dead Peer Detection	Yes (DPD Delay Time = 60 s, DPD Timeout = 150 s, DPD Action = Clear, DPD Action When Initiating Connection = Restart)

The SEL-3620 only accepts the protocols explicitly specified for the SEL - Secure (2022) profile. If the remote endpoint lacks one or more of these protocols, the SEL-3620 will not negotiate other protocols and will not successfully establish a VPN tunnel. If the SEL-3620 is the initiator of this connection, the diagnostics page of its web UI will show repeated messages for each attempted connection. Otherwise, look to the remote endpoint for information on the cause of the failure.

With the exception of the SEL - Secure (2022) Profile, you can create VPNs with devices other than those with supported profiles on the device. To do this, select a device profile that has parameters the peer device supports. Configure the peer device to use those parameters for communication. If the peer device does not support any of these parameters, the device will autonegotiate to other Phase 2 parameters. These other parameters will lack hardware-accelerated encryption.

SEL recommends not using a device Default Gateway (located on the Network Settings page) in conjunction with IPsec. This prevents the transmission of unencrypted packets when the IPsec tunnel is not established. It also forces the security gateway to source all its own client-side requests (such as Syslog, RADIUS, and LDAP requests) from the inside tunnel address when connecting to server services located inside a far-end IPsec protected network. If the remote IPsec endpoint is located behind another router (like in scenarios when connecting over the internet), use Static Routes to ensure connectivity with the remote gateway instead of a system default route.

The IPsec Connections list will display a configured IPsec connection. The device displays a graphical representation of each connection to help you verify that each connection configuration is correct. See *Table 6.14* for explanation of these graphical representations.

Table 6.14 IPsec Symbols

Symbol	Description
	Represents the remote network and that the rule is enabled
	Represents the remote network and that the rule is disabled
	The local device
	The remote gateway
	A connection where the traffic is forwarded to the remote network
	Represents a nonexistent path to an unreachable network
	Indicates that traffic is not allowed to flow on that path

MACsec Connections

The SEL-3620 and SEL-3622 can secure all device-to-device communications by establishing a MACsec Layer 2 connection between another embedded client like the SEL-651R. There can be as many simultaneously active MACsec connections as there are physical Ethernet ports.

NOTE: MACsec is not available on the SEL-3610.

When MACsec is commissioned, a bi-directional secure link is established after an initial exchange and verification of security keys between the two connected devices. These keys are known as the Secure Association Key (SAK), and Connectivity Association Key (CAK). The MACsec Key Agreement (MKA) protocol is used to generate and distribute these keys at configurable intervals to maintain security. It is also used to facilitate and automate commissioning, management, and scalability of MACsec on the LAN. To safeguard transmitted data and prevent replay attacks, integrity checks are constantly performed. MACsec connections can optionally encrypt all transmitted data as well. The SEL-3620 and SEL-3622 log all MACsec connection events per *Table F.3*. They have been engineered to gracefully recover from disruptions including loss of power or denial-of-service attempts.

From the navigation panel, select the **MACsec Connections** link under the **Security** heading to access the MACsec Connections page (see *Figure 6.11*). This page displays a list of configured MACsec connections and their states and allows for the creation of new connections.

The screenshot shows the SEL-3620/3622 web interface. The top bar includes the SEL logo, device ID (SEL2010057199), user (admin), and server time (Wed, May 18, 2022 09:44 UTC). The left sidebar has a 'Security' section with 'MACsec Connections' highlighted. The main content area is titled 'MACSEC CONNECTIONS' and shows three entries:

Key Server	Status	Alias	Embedded Client	Options
00:30:a7:01:9f:32	Commissioned	CA-4	00:30:a7:06:bd:ac	Update Delete
00:30:a7:01:9f:33	Waiting to be Commissioned	CA-2	Not Adopted Automatic Key Start of Commissioning Window: Wed, May 18, 2022 09:31 UTC Valid Until: Wed, May 18, 2022 17:31 UTC	Update Delete
00:30:a7:01:9f:34	Waiting to be Commissioned	CA-3	Not Adopted Manual Key - b5b5-6b47-e523-b92e-e9de-ac01-cbfb-f32c Start of Commissioning Window: Wed, May 18, 2022 09:32 UTC Valid Until: Wed, May 18, 2022 17:32 UTC	Update Delete

Figure 6.11 MACsec Connections

To commission a new MACsec connection, select **New Connection** to show the Commissioning Options dialog box on the right side of the webpage (see *Figure 6.12*). Select the **Interface** from the drop down, pick a start date and time, and set the number of hours to define the commissioning window.

This screenshot shows a simplified version of the 'Commissioning Options' dialog. It includes fields for 'Interface' (set to 'Eth 1'), 'Security Type' (set to 'Integrity + Encryption'), 'Commissioning key' (set to 'Automatic'), and a 'Commissioning Window' section with a start date/time of '05/16/2022 03:18 PM' and a duration of 'Hours: 8'. There are 'More Options' and 'Submit' buttons at the bottom.

Figure 6.12 Initial MACsec Form (Fewer Options)

Select **More Options** to show advanced Commissioning Options (see *Figure 6.13*). This allows more customization of the MACsec connection, such as disabling or enabling optional encryption, selection of the commissioning method, or customizing the maximum key lifetime. See *Table 6.15* for a descriptions of these options. Once the desired customization is complete, clicking on the **Submit** button initiates the process for commissioning.

This screenshot shows the expanded 'Commissioning Options' dialog. It includes all the fields from the previous version plus additional ones: 'Alias' (set to 'CA-1'), 'Security Type' (radio buttons for 'Integrity + Encryption' and 'Integrity Only'—the former is selected), 'Commissioning key' (radio buttons for 'Automatic' and 'Manual'—the latter is selected), and 'Maximum Key Lifetimes' sections for 'SAK Lifetime' (set to '24 Hours') and 'CAK Lifetime' (set to '168 Hours'). There are 'Less Options' and 'Submit' buttons at the bottom.

Figure 6.13 MACsec Form (More Options)

Table 6.15 provides descriptions of the MACsec Commissioning Options and their default values.

Table 6.15 MACsec Settings (Sheet 1 of 2)

Setting	Values	Default Value	Description
Interface	Network Interface Aliases		This selects the desired Ethernet port for the new MACsec connection. Only enabled ports not already configured for VLANs or members of a bridge can be selected.
Alias	As many as 32 characters	CA-#	Descriptive name for this MACsec connection. This is automatically populated with “CA-#” (where # is automatically incremented based on previously configured MACsec connections) in the Commissioning Options form when More Options is picked. Can be customized by the user.
Security Type			
Security Type Radio Buttons	Integrity + Encryption Integrity Only	Integrity + Encryption	Integrity + Encryption – this setting encrypts all MACsec frames as well as provide authentication and integrity. Integrity Only—this option allows the MACsec frames to be sent without encryption, for example, to an Intrusion Detection System.

Table 6.15 MACsec Settings (Sheet 2 of 2)

Setting	Values	Default Value	Description
Commissioning Key			
Commissioning Key Radio Buttons	Automatic Manual	Automatic	<p>Select the desired commissioning method of the SEL Connectivity Association (CA):</p> <ul style="list-style-type: none"> ► Automatic commissioning uses a derived Connectivity Association Key (dCAK) on both members to enable simple commissioning with minimal user interaction. ► Manual commissioning utilizes the SEL-362X randomly generated key, also known as a pre-shared Connectivity Association Key (pCAK), that shall be copied to the other CA member. Note that the SEL-362X generates a new random key if it restarts during an active pairing window. <p>Refer to <i>Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control</i> on page 4.33 for guidance on when to use each commissioning mode.</p>
Commissioning Window			
Start Date/Time	Date and time are stored in YYYY-MM-DD HH:MM format but may be displayed differently by the web browser. See <i>Figure 6.12</i> for an example of the date and time shown by the Google Chrome browser.	Current SEL-362X date and time	Click on the calendar button and select the date and time from the pop-up or manually type in the desired values. This setting, along with the Hours setting, defines the window for commissioning. This must be set to a date and time less than one hour in the past or to a future date and time.
Hours	1–8 (drop-down list of integers)	16 hours	The number of hours after the Start Date/Time that the SEL-362X attempts to commission a CA with an embedded client. Note that if no device is commissioned while the commissioning window is active, the connection is removed.
Maximum Key Lifetimes			
SAK Lifetime	0 to 200 hours	24 hours	This defines the desired maximum time between SAK rotations. SAK Rotation may occur earlier if CA traffic causes the SAK to expire due to Packet Number (PN) exhaustion. Entering 0 results in SAK rotations solely based on the PN.
CAK Lifetime	0 to 200 hours	168 hours	This defines the maximum time between CAK rotations. Entering 0 or leaving blank results in a CAK that is only rotated upon SEL-362X reboot.

The MACsec Connections webpage displays a graphical representation of each configured MACsec connection. This can help verify that each connection is correct and otherwise aid in troubleshooting.

During the commissioning process, the MACsec webpage displays the local interface, last three octets of its hardware MAC address, CA status, alias, and embedded client commissioning status. It also shows the commissioning settings under the Embedded Client column until an embedded client is added to the CA. See *Figure 6.14* for an example of a commissioning in progress.

**Figure 6.14 MACsec Connections Commissioning**

NOTE: No factory-default keys, salts, or passwords are used for MACsec communication after commissioning.

NOTE: The MAC address of the embedded client disappears if it loses contact. It reappears when the embedded client comes back online. Note that even if the embedded client goes offline, the line between the Key Server, Embedded Client, and the icon that represents the physical network remains green in color.

The SEL-362X automatically adopts the MACsec connectivity association once the Commissioning Options are submitted. At this point, the commissioning continues with the device at the other end of the MACsec CA. The remote device is responsible for adopting the SEL-362X. See *Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control* on page 4.33. Note that when commissioning with a manual key, if Commissioning Options are changed via the **Update** button or the SEL-362X is rebooted prior to commissioning completion, a new manual key is generated which must then be used on the embedded client to complete commissioning.

Once commissioned, the initial CAK used to establish the CA is rotated and replaced by a new CAK and SAK to complete commissioning. The webpage is updated to identify each commissioned MACsec connection by the last three octets of the MAC address of each device and by its CA alias. The Rotate SAK and Rotate CAK buttons are made available for manual key rotations (see *Figure 6.15*). Rotate SAK forces the rotation of the SAK, while Rotate CAK forces the rotation of both the CAK and the SAK. Rotations can be done on a set schedule by setting the SAK Lifetime and CAK Lifetime intervals as desired and is the recommended method.

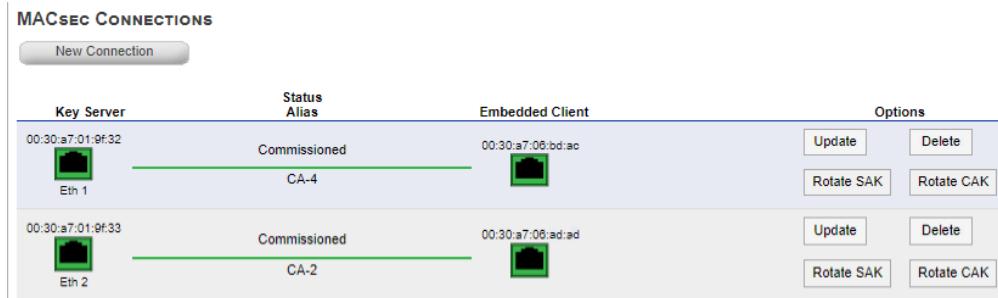


Figure 6.15 Commissioned MACsec Connections

Select the **Update** button to change the parameters of any existing MACsec connection (see *Figure 6.16*). Note that updating a commissioned MACsec connection may result in a temporary loss of connectivity. Selecting the **Delete** button removes the selected MACsec connection from the SEL-362X. You are asked to confirm deletion of a connection after the Delete button is selected. Ensure that the CA is also removed or cleared on the embedded client after deleting a MACsec connection on the SEL-362X or the connection may show an unexpected state on the embedded client.

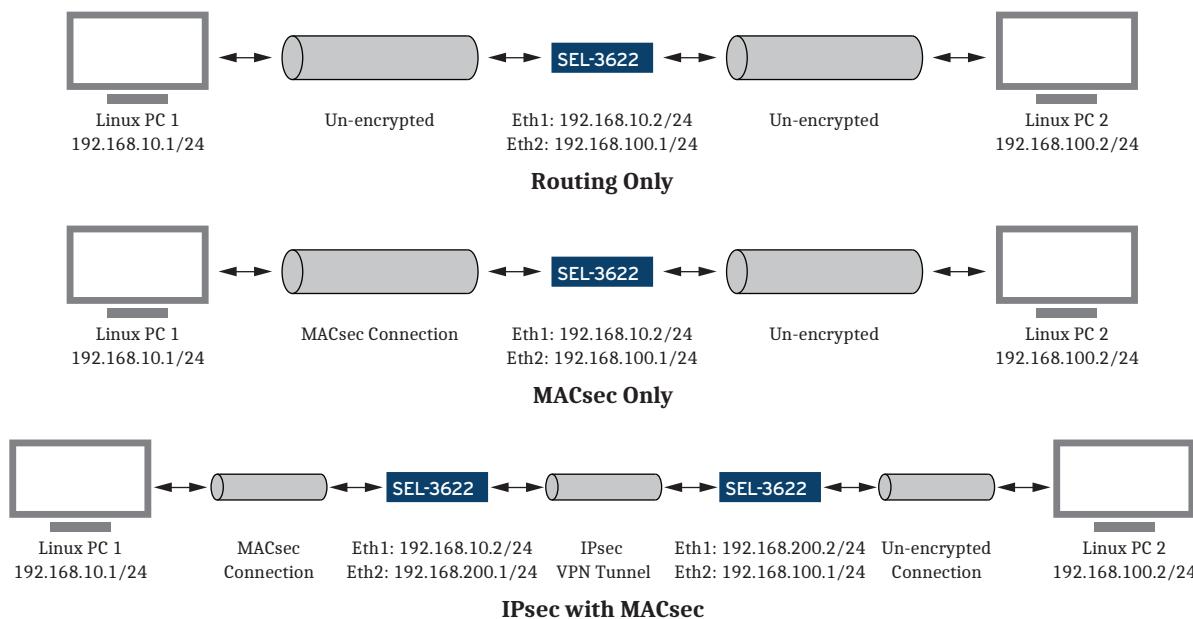
Figure 6.16 Updating an Existing MACsec Connection

If the remote end of a commissioned MACsec CA is cleared or deleted on the embedded client, the SEL-362X MACsec Connections page still shows the status as “Commissioned”, but the MAC address of the embedded client is blank when the page is refreshed (see *Figure 6.17*). This is the same behavior as when an embedded client temporarily loses connectivity. If the embedded client is permanently disconnected from this CA and you wish to use the same interface for a new MACsec connection, the CA must first be deleted by using the Delete button. Note that the line between Key Server, Embedded Client, and the icon that represents the physical network remains green in color.

Figure 6.17 Embedded Client Removed From Existing MACsec Connection

Throughput and Latency Considerations

MACsec is implemented in software, so throughput and latency can be affected by system burden, enabled features, and the extent to which they are utilized. Throughput and latency testing was performed on an SEL-3622 and an SEL-3620. In *Figure 6.18*, for each instance where an SEL-3622 was placed, an SEL-3620 was swapped to compare the differences in latency and throughput as shown in the results in *Table 6.16* and *Table 6.17*.

**Figure 6.18 Test Configurations**

Throughput was measured from end to end with no other services running.
Latency was measured by Ping round-trip-times (RTT) with packet sizes of 64 and 1440-bytes. Results will vary depending on system load.

Table 6.16 SEL-3622 Test Results

Configuration	Throughput (Mbps)	Ping RTT (ms) 64-bytes	Ping RTT (ms) 1440-bytes
Routing Only	4.84	0.824	1.186
IPsec Only (MACsec disabled)	4.82	2.839	2.905
MACsec w/ Integrity	4.80	2.927	4.441
MACsec w/ Integrity and Encryption	4.58	4.571	7.454
IPsec with MACsec Integrity	3.24	4.986	8.471
IPsec with MACsec Integrity and Encryption	3.03	5.170	8.826

Table 6.17 SEL-3620 Test Results

Configuration	Throughput (Mbps)	Ping RTT (ms) 64-bytes	Ping RTT (ms) 1440-bytes
Routing Only	92	2.115	2.594
IPsec Only (MACsec disabled)	43.9	3.374	4.563
MACsec w/ Integrity	35.1	2.523	3.489
MACsec w/ Integrity and Encryption	23.9	2.602	3.823
IPsec with MACsec Integrity	23.3	3.505	5.175
IPsec with MACsec Integrity and Encryption	17.3	3.712	5.400

This page intentionally left blank

S E C T I O N 7

Proxy Services and Password Management

Terms and Definitions

NOTE: Both the SEL-3620 Ethernet Security Gateway and the SEL-3622 Security Gateway have the same proxy services and password management functionality. For the purposes of this appendix, SEL-3620 refers to both the SEL-3620 and the SEL-3622.

- IED: Intelligent Electronic Device.
- Centralized Authentication Server (CAS): The server that provides centralized authentication, authorization, and accountability functions, such as an LDAP or RADIUS server.
- Centralized Authentication Client (CAC): The client that connects to a CAS to check the credentials of a user requesting access.
- Connection Directory: The database of IEDs, scripts, user permissions, and connection settings that is used by the SEL-3620 for password management and proxy services operations.
- Global Device ID: Unique identifier used by QuickSet and the SEL-3620 to alias IEDs in the QuickSet Device Manager Connection Directory.
- Pass Through Port: The serial port of the parent device used to access the current device in Device Manager.
- Scripting-Enabled Master Port (SMP): The primary TCP port (Telnet, Raw TCP, or SSH) through which an authorized user may gain access to managed IEDs through the SEL-3620 proxy.
- TEAM: ACCELERATOR TEAM SEL-5045 Software, used for some enterprise configuration and security management features.

Navigating This Section

NOTE: There are safety tips spread throughout this document, typically marked with a large visible tag (). Where this appears, read the note prior to continuing with the section.

If You Are...

New to the SEL-3620 Ethernet Security Gateway or SEL-3622 Security Gateway and want to walk through configuration of Proxy Services and Automated IED Password Management:
Already familiar with the SEL-3620/SEL-3622 password management and Proxy Services, and would like to explore different scenarios:

See...

Initial Configuration on page 7.8 and *Implementing Password Management* on page 7.50.
Management of Ethernet-Connected IEDs on page 7.74, *Management of SEL Communications Processors* on page 7.87, *Management of GE Devices* on page 7.112, and *Using TEAM With the SEL-3620 Proxy* on page 7.128.

If You Are...	See...
In charge of a currently running SEL-3620 system and would like to check status or make changes:	<i>Initial Configuration</i> on page 7.8 through <i>Implementing Password Management</i> on page 7.50 for general guidelines and information about how to find system status.
Interested in disaster recovery scenarios for password management:	<i>Appendix C: Best Practices for Emergency Readiness</i> , and read <i>Implementing Password Management</i> on page 7.50 for more information about the password management system.
A compliance officer in charge of auditing:	<i>Using the SEL-3620 Proxy Services</i> on page 7.26 for information about auditing SEL-3620 access logs. <i>Initial Configuration</i> on page 7.8 and <i>Configuring Group Access Permissions for Proxy Services</i> on page 7.14 may also be of use as they detail important information about SEL-3620 access control and authorizations theory.

Introduction

The SEL-3620 is a router, virtual private network (VPN) endpoint, and firewall device that can perform security proxy services for serial and Ethernet-based intelligent electronic devices (IEDs).

The SEL-3620 Proxy Services function helps create a user audit trail through strong and centralized user-based authentication and authorization support for modern and legacy IEDs. The SEL-3620 Automated IED Password Management technology manages protected IED passwords, ensuring that passwords are changed regularly, and that they conform to complexity rules for stronger security. Enforcing strong passwords on IEDs and having the passwords automatically changed on a configurable schedule satisfies regulatory password requirements, and ensures that no weak or default passwords are in use.

This guide provides step-by-step instructions for configuring SEL-3620 or SEL-3622 Security Gateways for Proxy Services and Automated IED Password Management in a variety of common situations including directly connecting to serial or Ethernet IEDs, using SEL Communications Processors, or Modbus-enabled products of a third-party manufacturer.

During the course of this section, you will need the following:

- A computer with administrative-level access to a Windows operating system and QuickSet with Device Manager plug-in, version 5.15.0.4 or later (installed and functioning)
- Terminal application software, such as HyperTerminal, Tera Term, or PuTTY
- SEL-3620 Ethernet Security Gateway or SEL-3622 Security Gateway with firmware version R200 or later
- Ethernet networking RJ45 cables (such as an SEL-C627 cable) and null-modem serial cables with RTS/CTS control lines (such as an SEL-C273A cable)
- SEL IED for testing, such as an SEL-351 relay
- Optional: SEL-5827 Virtual Connect Client 1.2.0.0 or later installed and functioning

- Optional: TEAM DDC Client 1.22.0.0 or later installed and functioning
- Optional: SEL-5828 Virtual Connect Service installed and functioning

This appendix assumes that you have basic Ethernet networking skills and experience with SEL-based IEDs and SEL Communications Processors or SEL Real-Time Automation Controllers (RTAC).

Proxy Services

One of the security features of the SEL-3620 is the implementation of Proxy Services. The SEL-3620 Proxy Services present additional authentication, authorization, and accountability options when accessing critical IEDs, including multifactor authentication and strict granular per-device permissions.

When normally accessing a critical IED, the user must access the relay by using a global shared account (Access Level 1 for read-only, Access Level 2 for read-write, etc.). Under this scenario, the password for the relay must be shared because the account is not unique to the user. Furthermore, there may not be any audit trail to show when a user has accessed the relay, other than changed settings or an alarm contact pulse (see *Figure 7.1*).

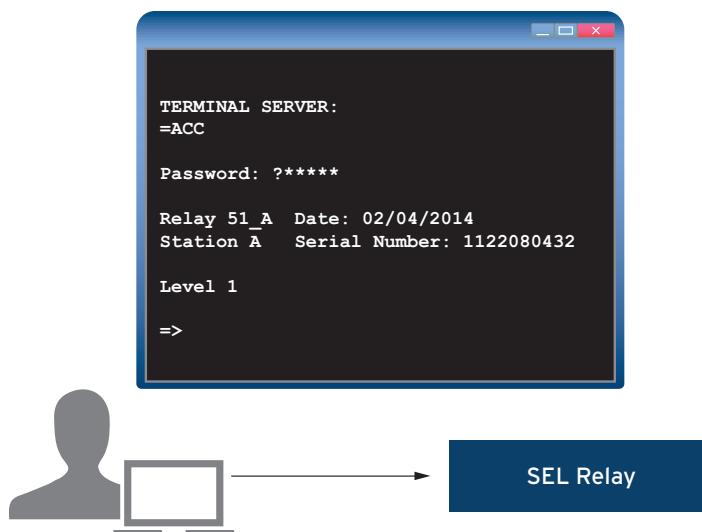


Figure 7.1 User Accessing a Global Shared IED Account

The SEL-3620 enforces user-based access controls before allowing communication with IEDs. When a user logs in to the SEL-3620 proxy, the SEL-3620 can authenticate the user by using a Centralized Authentication Server via LDAP or RADIUS. The SEL-3620 can receive user authorizations directly from the CAS, and then manage the entry of the password of the IED so the user never needs to know it (see *Figure 7.2*).

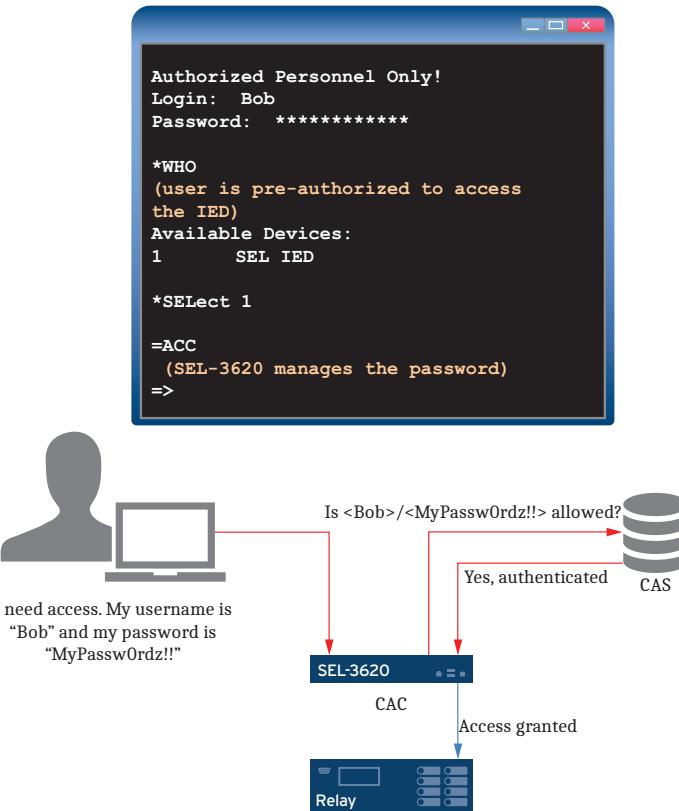


Figure 7.2 Accessing an IED with the SEL-3620 Proxy

The SEL-3620 proxy does not pass user-initiated commands directly to the device(s) to which it is connected (unless it is in binary mode). Instead, it records the command and checks it for predefined scripts that interact with the end-managed IED. If there is a match of a command to a script, such as **ACC** to access Access Level 1 of an SEL IED, then a script is invoked for the destination device. In effect, the entry of a command becomes the execution of a script by the SEL-3620. The results returned by the device as the script is executed are passed back to the person or computer process that initiated the exchange. If the user input does not match a script command, then the user input gets passed directly to the managed device.

For situations where users need direct access to managed devices, the SEL-3620 provides a device checkout feature that will temporarily revert the passwords of the checked-out devices to their initial values. This can be useful when testing with equipment that needs to be directly connected to managed devices. When devices are checked back in, the last used secure password is restored to prevent loss of password synchronization.

Virtual Client Software

The SEL-3620 Security Gateway may use optional virtual port software, such as SEL-5827 Virtual Connect Client and SEL-5828 Virtual Port Service, to enhance the usefulness of the SEL-3620 Proxy for existing Windows-based software applications.

Virtual Connect software creates virtual serial and/or Ethernet ports on a client computer, which may be used by existing software to “tunnel” plaintext data (such as Telnet) over a Secure Shell (SSH) connection to the SEL-3620. The Virtual Connect clients may be used to allow legacy software to use SEL-3620 proxy

services functionality (as in the case of SEL-5020 Settings Assistant Software), or to enhance the functionality of existing software (such as with GE EnerVista software). More information about using Virtual Connect software may be found in the following sections.

Theory of Operation

The following steps are required to configure the SEL-3620 Proxy Services:

- Step 1. Users and/or groups must be created or defined in Device Manager and/or the SEL-3620 (see *Figure 7.3*).

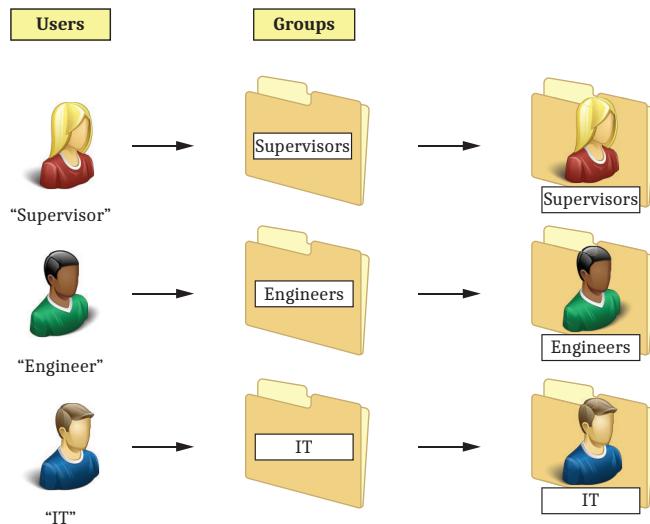


Figure 7.3 Users and Groups

- Step 2. Groups of users in Device Manager must be mapped to Connection Directory IED permissions (see *Figure 7.4*). The Connection Directory must then be uploaded to the SEL-3620.

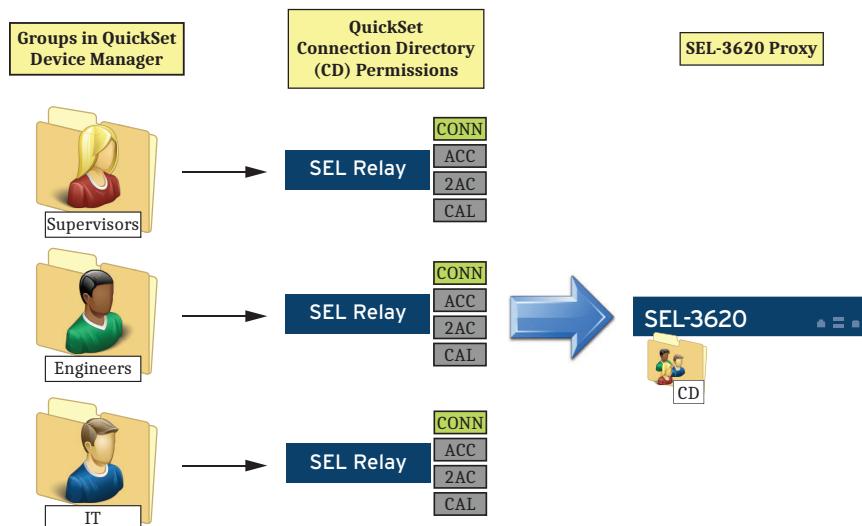


Figure 7.4 Groups Are Mapped to IED Permissions

Step 3. A user may then log in to the SEL-3620 proxy and access IEDs, if he or she has proper authorizations (see *Figure 7.5*).

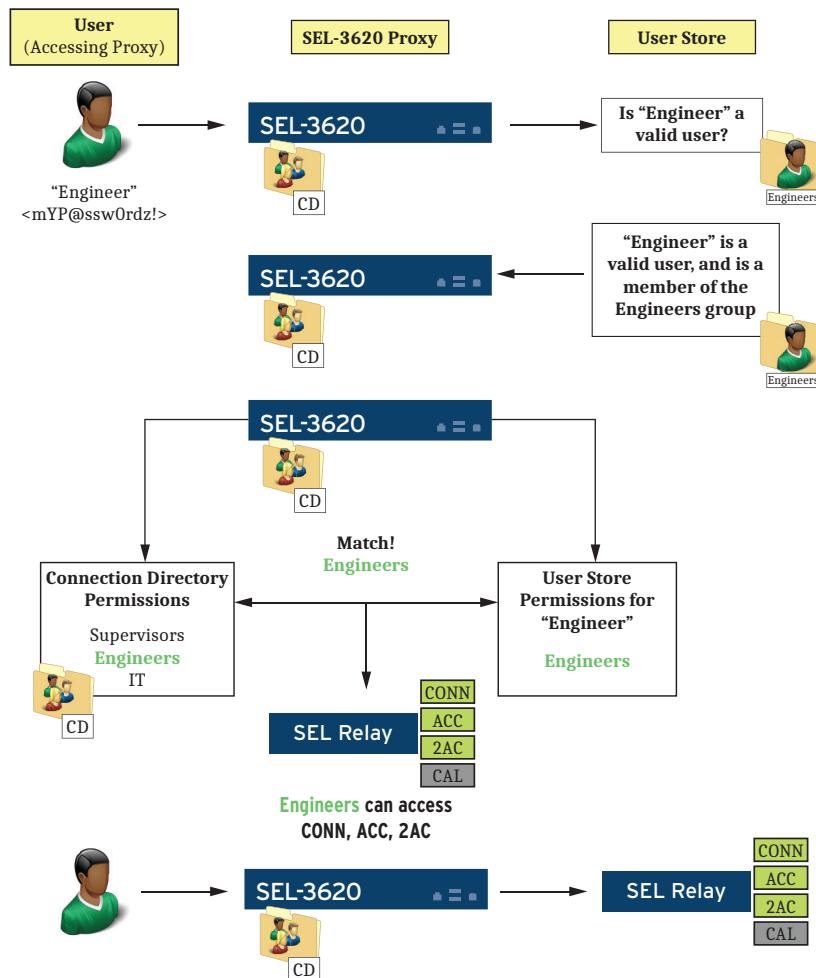


Figure 7.5 SEL-3620 Proxy Login Scenario

General Information About SEL-3620 Password Management, IED Proxy, and QuickSet User Authentication Capabilities

LDAP, RADIUS, and local accounts are acceptable forms of authentication to the SEL-3620 and the SEL-3620 IED proxy services. The SEL-3620 also supports user-based access controls and granular privilege levels based on centralized group mappings.

The QuickSet database supports both LDAP and local accounts for user authentication in an all-or-nothing manner (authenticated users have read/write privileges).

The SEL-3620 can manage passwords (e.g., generate and apply new complex passwords) for SEL IEDs, GE Multilin relays, and other IEDs with ASCII-based command-line interfaces. The SEL-3620 can also manage passwords for devices that only support password management via SSH, such as Siemens Ruggedcom switches. On some IEDs, the SEL-3620 can automate the entry of local shared account passwords, thus

General Information About SEL-3620 Password Management, IED Proxy, and QuickSet User Authentication Capabilities

avoiding the need for accessing users to know the actual IED passwords. Refer to *Table 7.1* for a noncomprehensive SEL-3620 password management compatibility chart.

Table 7.1 SEL-3620 Password Management Capabilities

IED Type	Manage Password	Automate Password Entry
SEL IEDs supported by QuickSet	Yes	Yes
SEL IEDs not supported by QuickSet	Yes ^a	Yes ^a
SEL-3500 Real-Time Automation Controllers	Use LDAP	N/A
SEL-3600 Port Servers and Security Gateways	Use LDAP/RADIUS	N/A
SEL-2730M Ethernet Switch	Use LDAP	N/A
GE Relays	Yes ^b	No
Third-party IEDs with ASCII interface	Maybe ^c	No
Third-party IEDs with non-ASCII interface	Maybe ^d	No
Third-party IEDs with ASCII interface over SSH	Maybe ^c	No

^a SEL IED must have an ASCII interface.

^b GE Multilin relays only.

^c Scripts can be readily built for third-party IEDs with ASCII interfaces using QuickSet. Contact SEL if you have questions about support for a particular IED.

^d Scripts can be created by SEL for third-party IEDs with binary interfaces. Contact SEL if you have questions about support for a particular IED.

The SEL-3620 provides a proxy for user access to critical IEDs, including software that requires serial and Ethernet connections. Refer to *Table 7.2* for a non-comprehensive SEL-3620 IED proxy compatibility chart.

Table 7.2 SEL-3620 IED Proxy Capabilities

Access Type	Can Be Proxied	Protocol(s) Proxied
SEL-5010 Relay Assistant Software	Yes ^a ; use with SEL-5827	Serial, Telnet
SEL-5020 Settings Assistant Software	Yes; use with SEL-5827	Serial, Telnet
ACCELERATOR QuickSet SEL-5030 Software	Yes	Serial, Telnet, SSH, FTP
SEL-5032 ACCELERATOR Architect	Yes	FTP
ACCELERATOR RTAC SEL-5033 Software	No; use NAT (port forwarding)	N/A
ACCELERATOR Report Server SEL-5040 Software	Yes ^a ; use with SEL-5827 or SEL-5828	Serial, Telnet, SSH
ACCELERATOR TEAM SEL-5045 Software	Yes; optionally use with SEL-5828	Serial, Telnet, SSH
GE EnerVista	Yes; use with SEL-5827	Modbus RTU, Modbus TCP
Terminal (PuTTY, Tera Term, HyperTerminal)	Yes	Serial, Telnet, SSH
FTP clients	Yes ^b	FTP
SNMP software	No; use NAT (port forwarding)	N/A
Web browser	No; use NAT (port forwarding)	N/A
Windows Remote Desktop	No; use NAT (port forwarding)	N/A
Other third-party software	Maybe ^c	Raw TCP, FTP, Telnet, SSH, Modbus RTU, Modbus TCP

^a FTP connections from this software cannot be proxied.

^b Many SEL IEDs can only have one FTP connection open at any one time, which might not be supported by some FTP client software.

^c Contact SEL if you have questions about support for protocol or software clients.

Initial Configuration

Introduction

This section walks through the creation of a “quickset” user account on the SEL-3620 Security Gateway and QuickSet that will be used in subsequent sections for configuration uploads.

Assumptions for this section include the following:

- You have already commissioned the SEL-3620 Ethernet Security Gateway with an initial administrative user account.
- You have an SEL IED—such as an SEL-787—with an available serial port connected to the SEL-3620. This example uses serial COM port 11 on the SEL-3620.
- QuickSet software with the Device Manager plug-in is already installed and functioning on your computer, and you have already logged in to Device Manager (the default username is admin and the default password is blank).
- You are connected via Ethernet to the commissioned SEL-3620 Ethernet Security Gateway from the computer that is hosting QuickSet.

Scenario Configuration

Figure 7.6 shows the current configuration for this section. You may replace the network addresses with your own, depending on your SEL-3620 network settings. The figures in this section display an SEL-787 relay as the IED. You may use your own SEL IED connected to the SEL-3620 via a null-modem serial cable (such as an SEL-C273A).

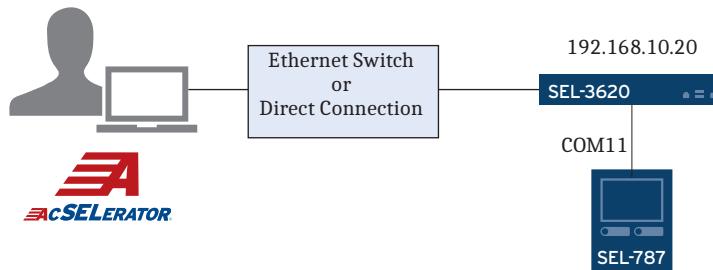


Figure 7.6 Initial Configuration Network Diagram

Creating a Dedicated QuickSet User on the SEL-3620

Because only one instance of a user account may be logged in to the SEL-3620 web server at a time, SEL recommends that you create a dedicated quickset user account on the SEL-3620 to be used for uploading IED connection attribute information, also known as the Connection Directory, from QuickSet to the SEL-3620. This will prevent you from being disconnected from the SEL-3620 web server during a Connection Directory upload. To create a dedicated user account for QuickSet on the SEL-3620, perform the following steps:

- Step 1. Log in to the SEL-3620 as an administrative user. In the navigation panel, under **Users**, select **Accounts** to go to the **User Accounts** page.
- Step 2. Select **Add User** at the top of the page to show the Add User form.

NOTE: In SEL-3620 firmware versions R133-R138, users needed to have an account with administrative privileges in the SEL-3620 to upload Connection Directories. If this applies to you, ensure the **Admin** check box is selected for the QuickSet user. As of firmware version R139 and later, the user account only needs to be Technician-level privilege or higher.

- Step 3. Add a user called **quickset**, provide a strong password, and give the user Technician privileges (do not select the **Admin** check box at the bottom of the form). The **Accounts** page should now look similar to *Figure 7.7*.

Username	First Name	Last Name	Admin	Account State	Creation Date Last Login Password Changed	Options
admin			Yes	ENABLED	2013-11-27 16:54:55 2014-08-01 11:12:10 2013-11-27 16:54:55	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>
quickset			No	ENABLED	2013-11-27 16:54:55 2014-05-28 10:45:58 2013-11-27 16:54:55	<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>

Figure 7.7 SEL-3620 Users Page With QuickSet Account

Testing Connectivity Between QuickSet and the SEL-3620

To test the connectivity between QuickSet and the SEL-3620, perform the following steps:

- Step 1. Right-click anywhere in the **Connection Explorer** window, and select **Add > Device**. QuickSet will present a list of devices. Select SEL-3620 from the list and select **OK**. This will place a new device in the **Connection Explorer** window. You may choose to give this device a more descriptive name.

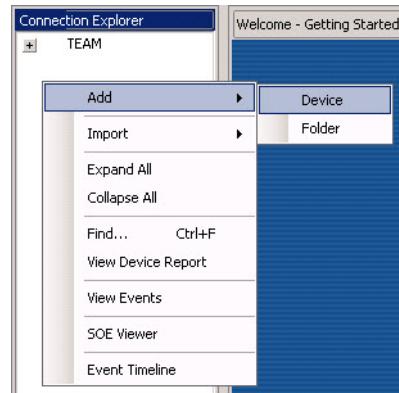


Figure 7.8 Adding a Device Template

- Step 2. In the **Connection Explorer** window, double-click the SEL-3620 to show the SEL-3620 device in the QuickSet main panel. Select **Edit** in the lower right of the main panel to edit the device.
- Step 3. On the left side of the main panel, select the **Device** tab, and select the **Is Managed** check box. This enables password management features for all devices under the SEL-3620 in the Connection Directory.

Device Type	SEL-3620
In Service	<input type="checkbox"/>
Is Managed	<input checked="" type="checkbox"/>
Enable RADIUS Authentication	<input type="checkbox"/>
Device Name	SEL-3620

Figure 7.9 Select the Is Managed Check Box in the SEL-3620 Template

Step 4. Configure the Connection tab as shown in *Figure 7.10*. You should only need to change the **Host IP Address** and the **Connection Type**. You may leave all other settings as the default values provided (for now). When finished, select **Apply** in the lower right corner of the QuickSet main panel.

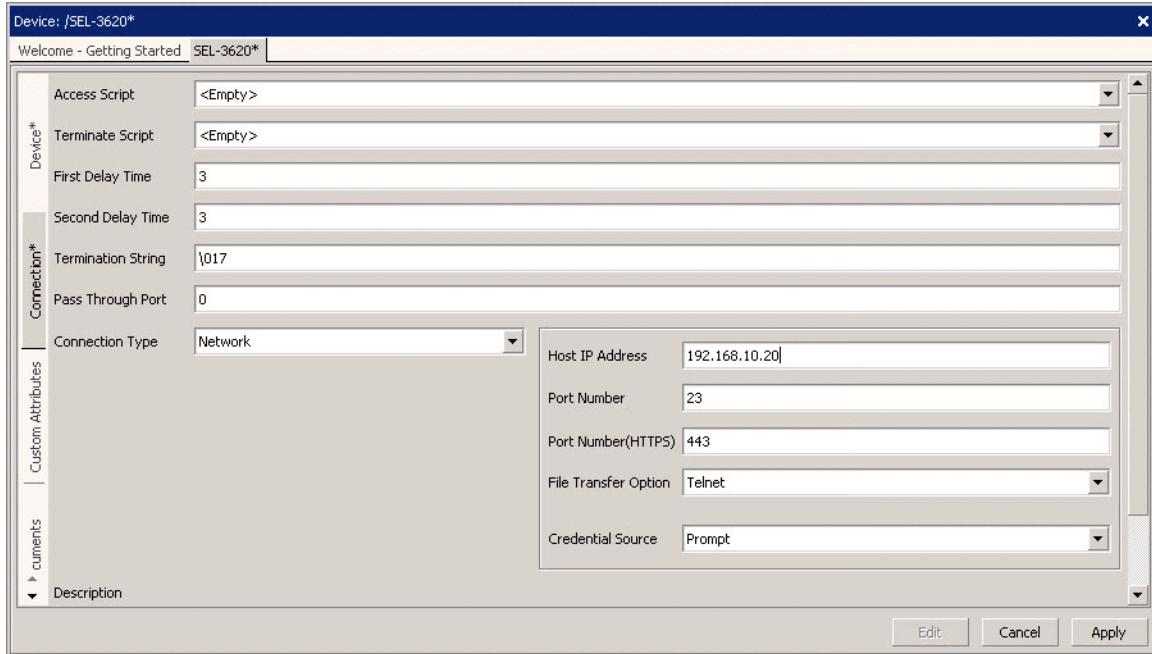


Figure 7.10 SEL-3620 Template Connection Tab

NOTE: The SEL-787 represents a single device Connection Directory. The Connection Directory is an “address book” of devices, their attributes, and scripts that the SEL-3620 scripting engine uses to manage passwords on (and access to) the device. The graphical representation of the Connection Directory shows the logical structure of the connections between devices.

NOTE: The SEL-3620 recognizes the Global Device ID of the relay (not the Device Name). To make the Global Device ID more user-friendly on the SEL-3620, change it to match the Device Name. This allows users to intuitively identify the device. Take care to have a single GDID for each device, because the GDID cannot be reused.

Step 5. In the **Connection Explorer** window, right-click on SEL-3620, select **Add > Device**, and select **OK** (this example uses an SEL-787). This will place a new device in the **Connection Explorer** window under the SEL-3620. Do not change any settings on the device (device settings will be updated in a subsequent section).

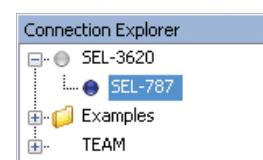


Figure 7.11 Adding SEL-787 Beneath the SEL-3620 Template

Step 6. In the left pane, select the **Device** tab, and select **Edit**. Change the **Global Device ID (GDID)** so that it matches the **Device Name**. You can use the following characters: space, tab, newline, a–z, A–Z, 0–9, #, &, (,), +, -, ., /, :, =, ?, @, ^, [,], _, ~. However, do not begin a GDID with a number.

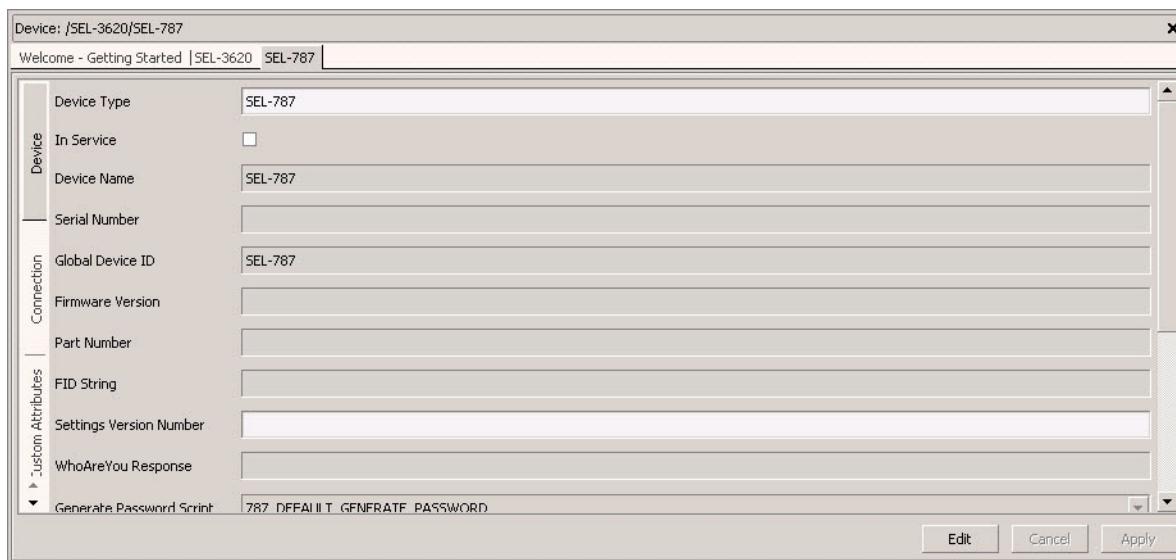


Figure 7.12 SEL-787 Global Device ID

- Step 7. If the SEL IED passwords are currently set to default values (**OTTER**, **TAIL**, etc.), then skip to *Step 8*. Otherwise, enter the current level (Access Level 1, Access Level 2, Access Level C, etc.) passwords into the **Device Passwords** boxes.
- Step 8. Select the **Connection** tab. Change the **Pass Through Port** to match the COM port that the IED connects to on the SEL-3620 (11 in this case to indicate COM11).
- Step 9. Change the serial device characteristics to match those of the IED. In this case:
 - > **Data Speed:** 9600
 - > **Data Bits:** 8
 - > **Stop Bits:** 1
 - > **Parity:** None
 - > **RTS/CTS:** On
 - > **DTR, RTS, and XON/XOFF:** Off
- Step 10. Leave the other settings in the Connection tab with the default values.

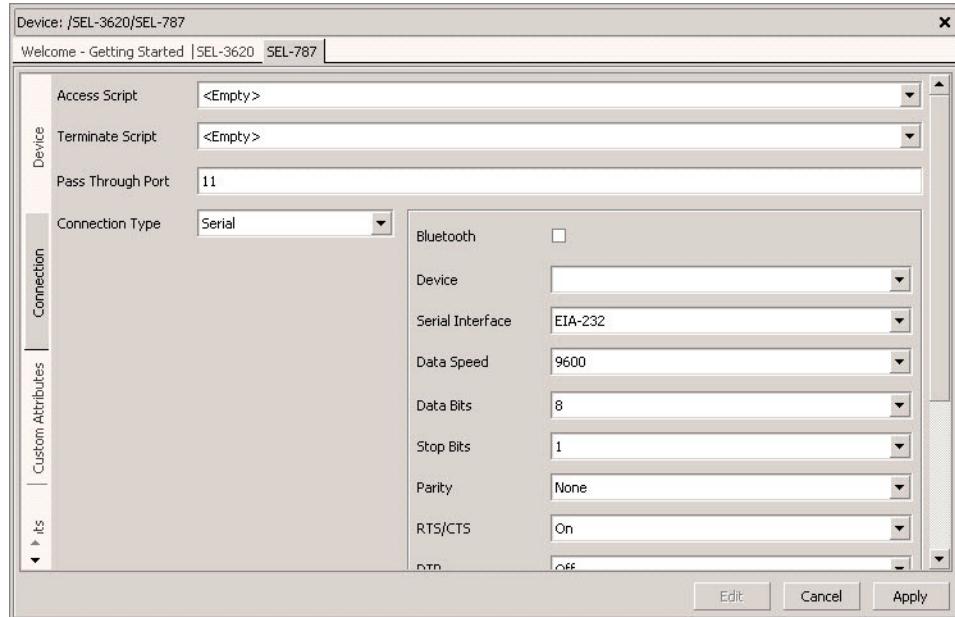


Figure 7.13 SEL-787 Connection Tab Parameters

Step 11. In the **Connection Explorer** window, right-click **SEL-3620**, and select **Device Tasks > Send**. This will send the test Connection Directory to the SEL-3620. In QuickSet version 6.0.0.0 and later, you will be prompted by a warning when uploading the Connection Directory to the SEL-3620. If you are prompted to continue, select **OK**.

Step 12. You will be prompted for your SEL-3620 username and password. Enter the username and password of the “quickset” user previously created on the SEL-3620. If you encounter an error, see *Troubleshooting* on page 7.13.

Step 13. Log in to the SEL-3620 web interface. Under **Reports**, in **System Logs**, verify that the SEL-3620 logs show that the Connection Directory was successfully uploaded.

2013-05-02 20:43:21	ProxyConfig	Notice	SYSTEM	Connection Directory: update successful
2013-05-02 20:43:18	ProxyConfig	Notice	USER	Connection Directory: update initiated by quickset at 192.168.10.57
2013-05-02 20:43:18	Login	Notice	SECURITY	Login to Web: successful by quickset at 192.168.10.57

Figure 7.14 Successful Upload of the Connection Directory From QuickSet

Troubleshooting

Invalid SSL Certificate Message



Figure 7.15 Invalid Certificate Message

QuickSet will display this message whenever it receives a default X.509 certificate from the SEL-3620 web server that it has not seen previously in the current QuickSet session.

"Failed to send data to device: 400" Message



Figure 7.16 Failed: 400 Message

A "Failed to send data to device: 400" message is most likely because of a credential mismatch between users currently logged into the QuickSet Database, or the user does not have administrative access to the SEL-3620 (if using firmware version R139 or earlier). Ensure the username/password currently logged in to the QuickSet Database matches a username/password (case-sensitive) on the SEL-3620, or, if using firmware version R139 or earlier, that the user has administrative privileges in the SEL-3620.

"Failed to send data to device: 10058" Message

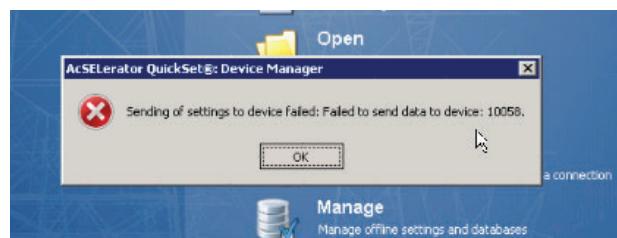


Figure 7.17 Failed: 10058 Message

A "Failed to send data to device: 10058" message is an indication that the underlying Windows operating system returned a network socket error, and that the sending/receiving process was shut down. Check your network settings, the reliability of the network link, or your network interface card drivers. In some cases, a simple system reboot will fix this error by forcing the networking subsystem in the host to be properly initialized.

Winsock Error Code: -1

A “Winsock Error Code: -1” message can indicate a couple of different problems. If the response is immediate, then there is most likely a problem with the connection directory configuration itself. Check your connection directory settings, especially FTP proxy port numbers, to ensure proxy ports are not set to the same number (such as two different devices using an FTP proxy port of 20001). This Winsock error is also an indication that the underlying Windows operating system cannot find a network path to the SEL-3620. Check your network settings, the reliability of the network link, or your network interface card drivers. In some cases, a simple system reboot will fix this error by forcing the networking subsystem in the host to be properly initialized. Note that this error can also indicate that the SEL-3620 web server is not enabled at the IP address to which you are attempting to send the CD. Ensure that the SEL-3620 web server is enabled for the particular interface.

“500” Error From Your Web Browser When Accessing the SEL-3620

A “500” error when attempting to access the SEL-3620 may be because of attempting to log in to the web interface with the same user you recently used to upload a Connection Directory to the same Security Gateway from QuickSet. To fix this problem, you must restart the web browser and connect again.

Other Connection Errors When Sending the Connection Directory

If you receive errors when trying to send the Connection Directory to the SEL-3620, ensure the IP Address and HTTPS port (default port 443) match those of the SEL-3620 web server.

QuickSet Reports “Settings can only be sent to a Security Gateway when it is managed and has child devices”

If you receive the message **Settings can only be sent to a Security Gateway when it is managed and has child devices** when attempting to upload a CD, ensure that the **Is Managed** check box on the SEL-3620 Device tab is selected.

Configuring Group Access Permissions for Proxy Services

Introduction

This section walks through setting group access permissions to devices in the Connection Directory by using either local groups or centralized groups. Groups of users who are given access to Connection Directory devices can then access those devices through the SEL-3620 Proxy Services mechanism. Users can access the SEL-3620 Proxy Services directly from a terminal prompt connected to an SEL-3620 Script-Enabled Master Port (SMP), or from QuickSet to an SEL-3620 Script-Enabled Master Port.

Groups in the SEL-3620 are defined by particular job activities. These job activities typically require specific administrative abilities when interacting with IEDs. In the following scenarios, three example groups are configured, each with their own authorizations:

- **Supervisors:** Users that have complete access to all privileges (i.e., Access Levels) on Connection Directory devices.
- **Engineers:** Users that have read (Access Level 1) and write (Access Level 2) privileges on Connection Directory devices.
- **IT (Information Technology):** Users that have connect-level (basic) privileges on Connection Directory devices.

Scenario Configuration

The following shows an example configuration. You may replace the network addresses with your own, depending on your SEL-3620 network settings. In this section, an SEL-787 relay is used for testing. You may use your own SEL IED connected to the SEL-3620 via a null-modem serial cable (such as an SEL-C273A). Note that the use of the CAS is optional. The following configuration steps outline how to integrate centralized users and groups.

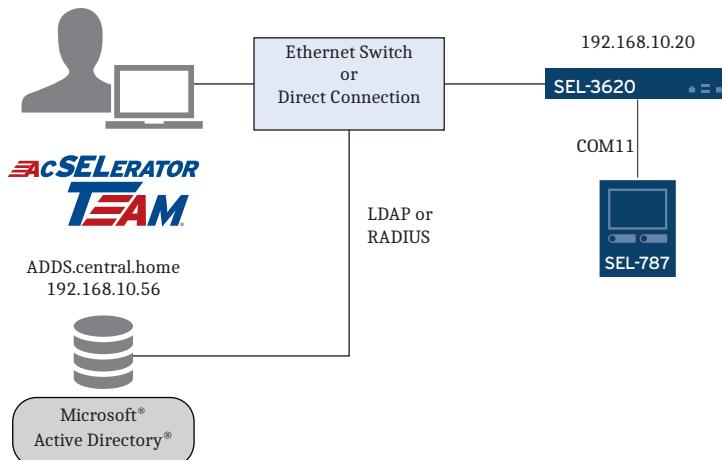
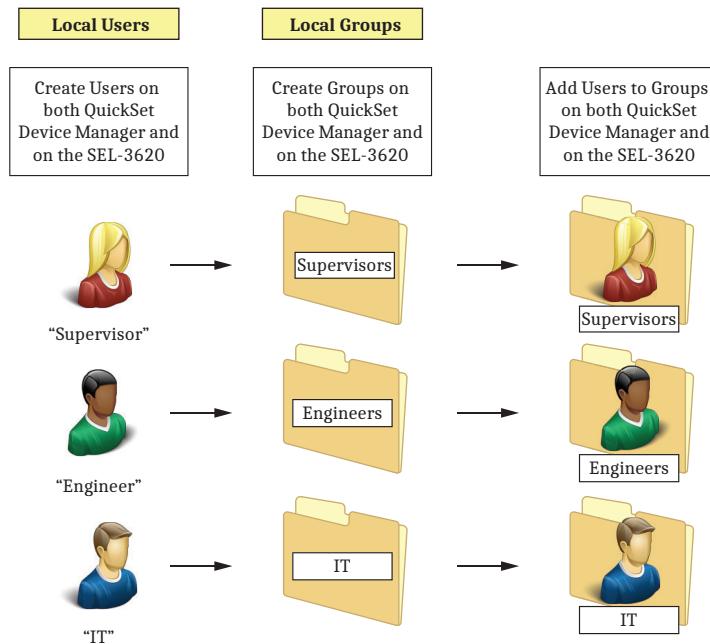


Figure 7.18 Initial Configuration Network Diagram

Local User Groups in QuickSet and the SEL-3620

Both QuickSet and the SEL-3620 support local authentication capabilities that require the use of a correct username/password combination and local group privilege before allowing access. All the local groups and local users contained in them must be synchronized between the SEL-3620 and Device Manager (see *Figure 7.19*).

**Figure 7.19 Local Users and Groups on the SEL-3620 and Device Manager**

SEL recommends having at least one local group and local user for emergency access in case of loss of wide-area network connectivity for centralized authentication. For more information about managing local users on the SEL-3620, see Application Guide AG2013-26, *Using Emergency Accounts for Access When the Network Is Unavailable*.

Creating Local Proxy Services Groups on the SEL-3620

To create local users and local groups on the SEL-3620 for access to the SEL-3620 Proxy Services, perform the following steps:

- Step 1. Log in to the SEL-3620 as an administrative user. In the navigation panel, under **Users**, select **Accounts** to go to the User Accounts page.
- Step 2. Create three users: supervisorlocal, engineerlocal, and itlocal (see *Figure 7.20*). You do not need to give the users administrative privileges in the SEL-3620 (Technician privileges suffice for the proxy).

Add User

Username*: supervisorlocal

First Name: Local Last Name: Supervisor

New Password*: Retype New Password*:

Title: Division:

Employee Identification:

Address:

City: State:

Country: Postal Code:

Work Phone: Mobile Phone:

Email: supervisorlocal@central.home

Admin: Enabled:

*required

Submit

Figure 7.20 Creating the Local Users

- Step 3. In the navigation panel, under **Users**, on the **Local Groups** page, select **Add Local Group** and create three groups: SupervisorsLocal, EngineersLocal, and ITLocal.
- Step 4. Under the **SupervisorsLocal** group, in the **Local Users** box, select the **supervisorlocal** check box to place that user into the group.
- Step 5. Under the **EngineersLocal** group, in the **Local Users** box, select the **engineerlocal** check box to place that user into the group.
- Step 6. Under the **ITLocal** group, in the **Local Users** box, select the **itlocal** check box to place that user into the group.

The Local Groups page should now look similar to *Figure 7.21*.

LOCAL GROUPS		
Add Local Group		
Local Groups		
Alias	Options	
▼ SupervisorsLocal	Update	Delete
supervisorlocal		Delete
▼ EngineersLocal	Update	Delete
engineerlocal		Delete
▼ ITLocal	Update	Delete
itlocal		Delete

Figure 7.21 Local User Groups on the SEL-3620

The following step is optional:

- Step 7. Log in to the web server of the SEL-3620 as each user to ensure that each user is active and correctly configured.

Creating Local Proxy Services Groups in Device Manager

To create local users and local groups in Device Manager for access to the SEL-3620 Proxy Services, perform the following steps:

- Step 1. Log in to Device Manager as the quickset user.
- Step 2. From the **Tools** menu, select **Device Manager > Users** to access the User Manager.
- Step 3. Right-click the **Local Users** folder and add three users: **supervisorlocal**, **engineerlocal**, and **itlocal**. All three usernames (case-sensitive) and passwords must match the three local users created previously on the SEL-3620.

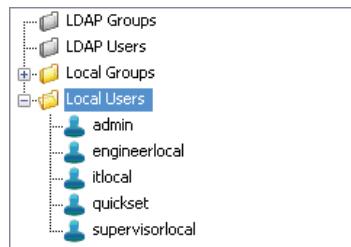


Figure 7.22 Three Local QuickSet Users

- Step 4. Right-click the **Local Groups** folder, and create three groups: **SupervisorsLocal**, **EngineersLocal**, and **ITLocal**. All three group names (case-sensitive) must match the associated local group created earlier on the SEL-3620. Add the supervisorlocal, engineerlocal, and itlocal users to their respective groups. For each group, you may select the **Allow log on to ACCELERATOR Database** check box to allow users read/write access to the Connection Directory (see *Figure 7.23*).

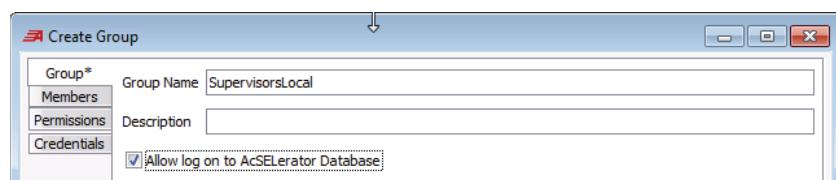


Figure 7.23 Allow Log in to ACCELERATOR Database Check Box

NOTE: For Proxy Services, it is important that the local usernames, passwords, and groups match **exactly** between the SEL-3620 and QuickSet, including spellings and uppercase/lowercase letters. Mismatches in usernames, passwords, or groups between the SEL-3620 and QuickSet will result in connectivity and authentication issues.

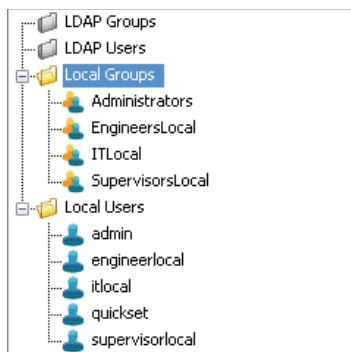


Figure 7.24 QuickSet Local Groups and Users

Centralized User Groups in QuickSet and the SEL-3620

While localized users and groups work well for a finite number of SEL-3620 gateways, local authentication becomes unreasonable as the number of username/password combinations, or the number of active SEL-3620 gateways, grow beyond manageable numbers.

To ease this burden, QuickSet and the SEL-3620 support centralized authentication via the LDAP and RADIUS. LDAP and RADIUS allow user access privileges to be controlled and configured from a single point: a CAS. In a centralized authentication system, the SEL-3620 acts as a Central Authentication Client (CAC), which authenticates an accessing user by passing the credentials back to the CAS. The CAC will only allow the user access if the CAS reports that its credentials are valid and that the user has access permissions. Adding or revoking access is easier because all credentials are managed at the CAS instead of every CAC, and revoking access to an IED in the Connection Directory anywhere on the system is now a single operation on the CAS.

NOTE: When using centralized accounts as your primary user management method, it is still a good idea to have local accounts configured for emergency access if communication to your CAS fail.

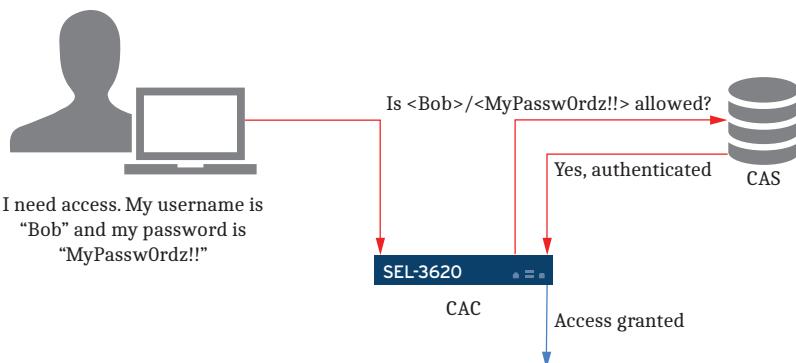


Figure 7.25 Centralized User Access to the SEL-3620 Proxy Services

A further benefit to using centralized users is that the accessing user does not need to have any authorization privilege to the SEL-3620 web interface. This is different from local users that need to have Technician authorizations to the SEL-3620 web interface (at minimum) to use the proxy.

LDAP on QuickSet and the SEL-3620

Both QuickSet and the SEL-3620 support LDAP authentication capabilities that require the use of a correct LDAP username/password combination and LDAP group privilege before allowing access. Both QuickSet and the SEL-3620 must be able to communicate with an LDAP server, and LDAP groups must be referenced in Device Manager (see *Figure 7.26*).

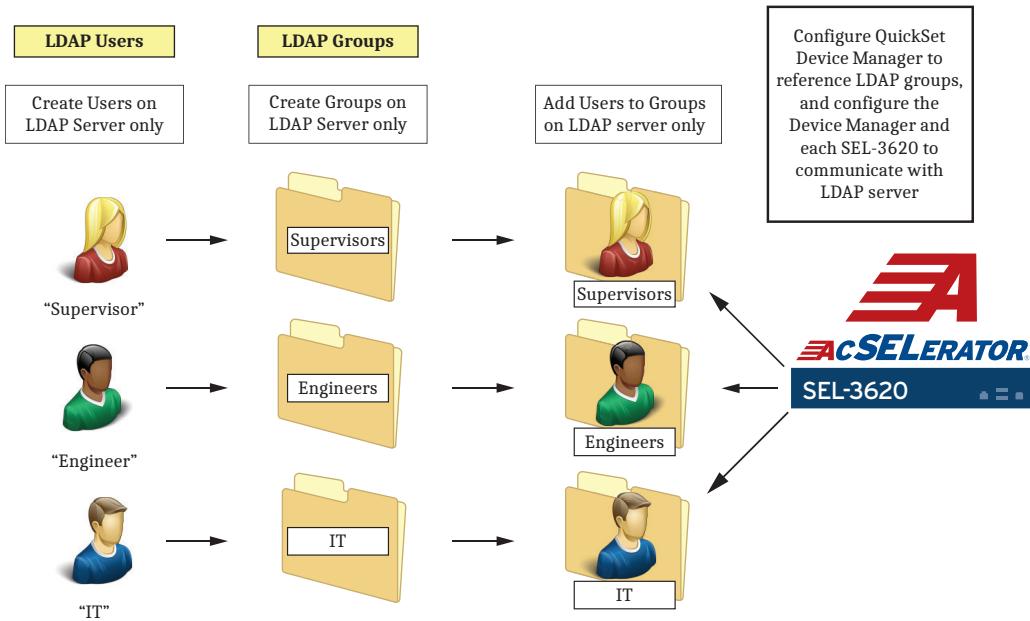


Figure 7.26 LDAP Users and Groups

NOTE: As of firmware version R210, the SEL-3620 no longer supports TLSv1.1 authentication. Ensure that the CAS supports TLSv1.2 or TLSv1.3 authentication.

Ensure that both the SEL-3620 and Device Manager can bind to an LDAP-enabled CAS. This example uses Windows Server 2008 R2 Standard as the CAS (see *Figure 7.18*). See *Centralized User Accounts With LDAP* on page 3.8 for more information about configuring LDAP settings.

The LDAP parameters in Quickset can be set within Device Manager by selecting **Tools > Configure LDAP** (see *Figure 7.27*).

For detailed information about commissioning an LDAP server, refer to Application Guide AG2013-14, *Configuring a Windows Server for Centralized Authentication With LDAP-Enabled SEL Devices*.

Creating LDAP Proxy Services Groups on the SEL-3620

Once the SEL-3620 is successfully configured for LDAP, no further users or groups will need to be manually added to the Security Gateway. Any additional Proxy Services permissions and privileges are set from within Device Manager.

Creating LDAP Proxy Services Groups in Device Manager

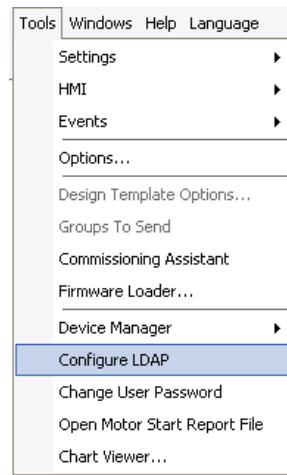


Figure 7.27 QuickSet Configure LDAP

The following will add three preexisting centralized accounts in Device Manager for access to the SEL-3620 Proxy Services.

- Step 1. Log in to Device Manager as the quickset user.
- Step 2. In the **Tools** menu, select **Device Manager > Users** to access the User Manager.
- Step 3. Right-click the **LDAP Groups** folder, and select **Add**. Create a group called **SupervisorsCentral**. Select the **Associate with LDAP Group** check box, and navigate to the appropriate centralized group (in this case **CN=Supervisors,DC=central,DC=home**). You may select the **Allow log on to ACSELERATOR Database** check box to allow the specified LDAP users read/write access to the Connection Directory (see *Figure 7.28*).

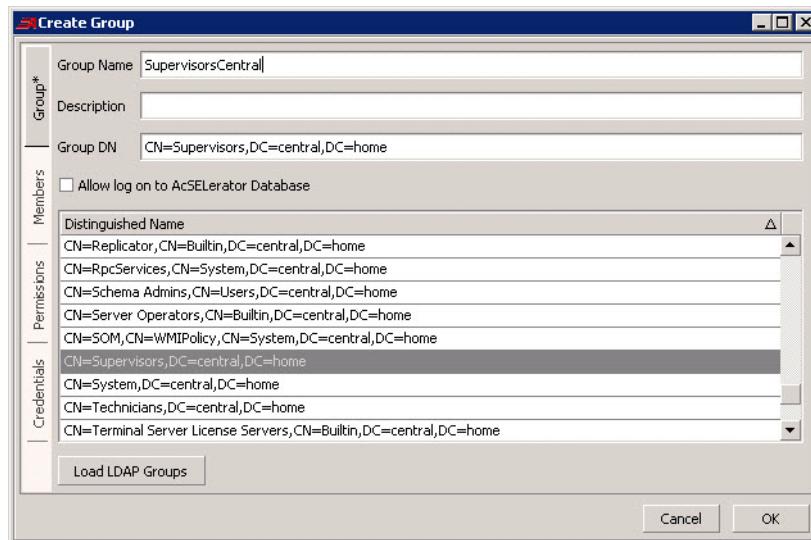


Figure 7.28 Parsing the LDAP Groups to Find the Supervisors Group

- Step 4. In the left pane, select the **Members** tab to list all members of the central **SupervisorsLocal** group, including a user with the name "Supervisor" and login name of "supervisorcentral" to verify that they have been added correctly.

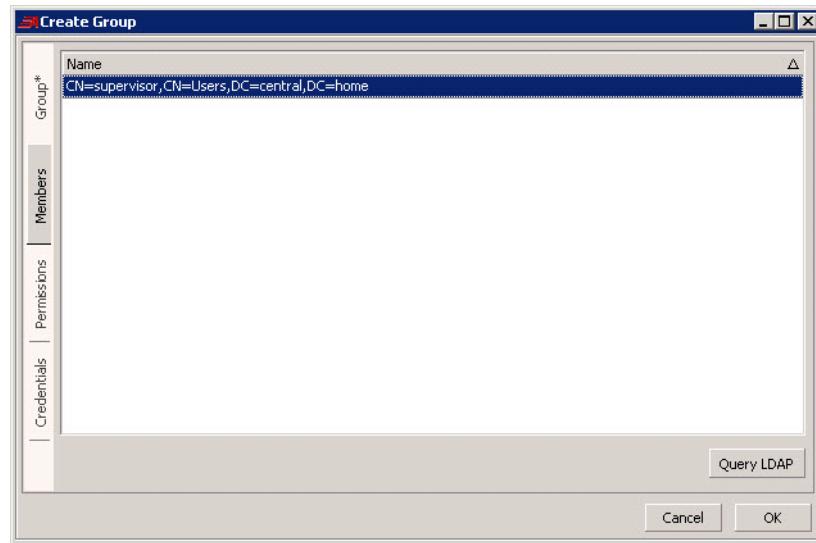


Figure 7.29 Supervisor Users Within the Centralized Supervisors Group

Step 5. Repeat Step 3–Step 4 for each new centralized group. This creates an **EngineersCentral** and an **ITCentral** group, each with a respective engineercentral and itcentral user.

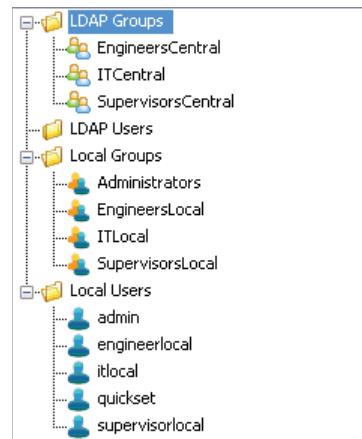


Figure 7.30 LDAP User Groups

RADIUS in QuickSet and the SEL-3620

The SEL-3620 supports RADIUS authentication capabilities that require the use of a correct RADIUS username/password combination and correct SEL-PROXY-GROUP Vendor-Specific Attribute (VSA) before allowing access. The SEL-3620 must be able to communicate with a RADIUS server (see *Figure 7.31*). Because QuickSet cannot communicate with a RADIUS server, local groups must be created in Device Manager that match the string sent along with the SEL-PROXY-GROUP VSA that is sent back to the SEL-3620 with a successful Access-Accept.

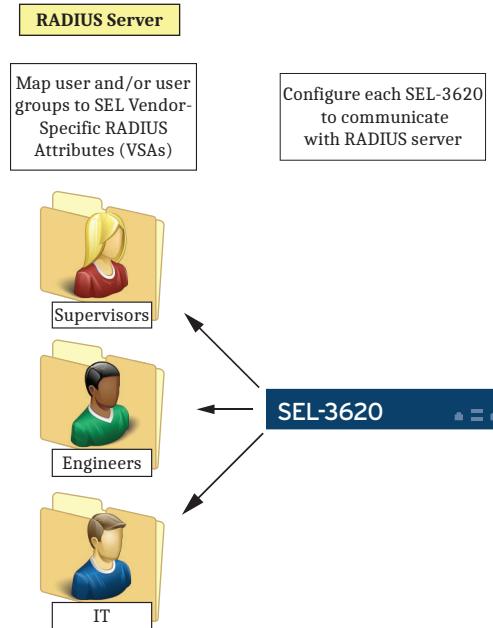


Figure 7.31 RADIUS Authorizations in Device Manager

Creating RADIUS Proxy Services Groups on the SEL-3620

NOTE: As of firmware version R210, the SEL-3620 no longer supports TLSv1.1 authentication. Ensure that the CAS supports TLSv1.2 or TLSv1.3 authentication.

Ensure that the SEL-3620 can successfully authenticate to a RADIUS-enabled CAS. This example uses Windows Server 2008 R2 Standard with Network Policy Service (NPS). See *Using RADIUS* on page 3.15. For detailed information about configuring a RADIUS server, refer to the following Application Guides:

- AG2014-10, *Integrating RADIUS Authentication With the SEL-3620 in a Cisco Secure ACS Environment*
- AG2014-11, *Integrating RADIUS Authentication With the SEL-3620 in a FreeRADIUS Environment*
- AG2014-12, *Integrating RADIUS Authentication With the SEL-3620 in an RSA Authentication Manager 7.1 SP4 Environment*
- AG2014-13, *Integrating RADIUS Authentication With the SEL-3620 in a Microsoft Windows NPS Environment*

Once the SEL-3620 is successfully configured for RADIUS, no further users or groups will need to be manually added to the Security Gateway. Any additional Proxy Services permissions and privileges are set from Device Manager and the RADIUS server itself.

Creating RADIUS Proxy Services Groups in Device Manager

In the case of RADIUS, you may simply use the existing Local Groups (e.g., **SupervisorsLocal**) that have been previously defined in Device Manager. Unlike with the LDAP configuration (which can be configured entirely client-side), you will need to configure your RADIUS server with information about the SEL-3620 (such as IP address), and the *exact* names of your local groups. This is necessary so the RADIUS server can send the SEL-3620 the names of groups as part of the SEL-PROXY-GROUP attribute (e.g., SEL-PROXY-GROUP = "SupervisorsLocal").

For more information about RADIUS and SEL RADIUS dictionary configuration information, see *Using RADIUS* on page 3.15.

Associating Groups With IED Permissions in the QuickSet Connection Directory

To define what groups of users have access to Access Level 1, Access Level 2, or other authorization levels on an IED in the Connection Directory, we must specifically associate a group with privileges on the IED.

For LDAP connectivity, we must associate the LDAP groups in Device Manager with permissions on the IED in the QuickSet Connection Directory (see *Figure 7.32*).

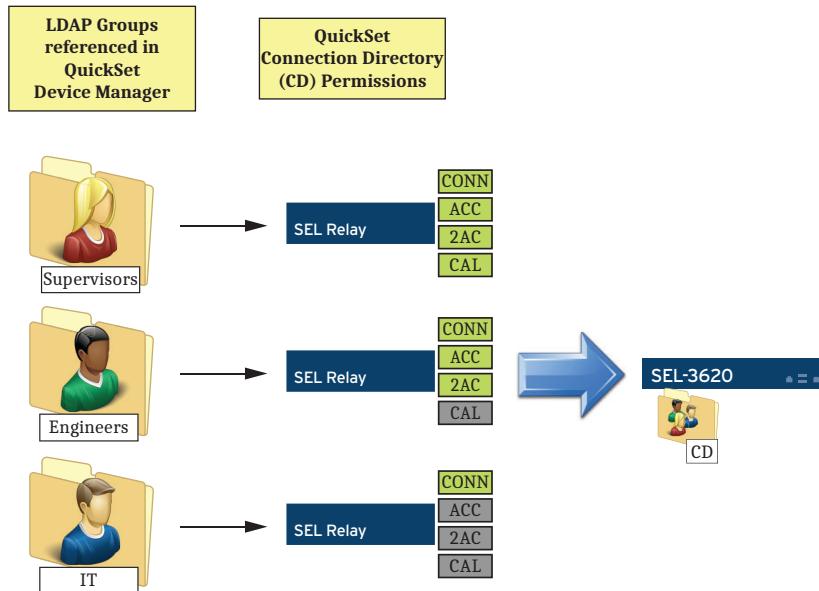


Figure 7.32 Associate LDAP Groups With IED Permissions

For Local and RADIUS connectivity, we must associate the Local groups in Device Manager with permissions on the IED in the QuickSet Connection Directory (see *Figure 7.33*).

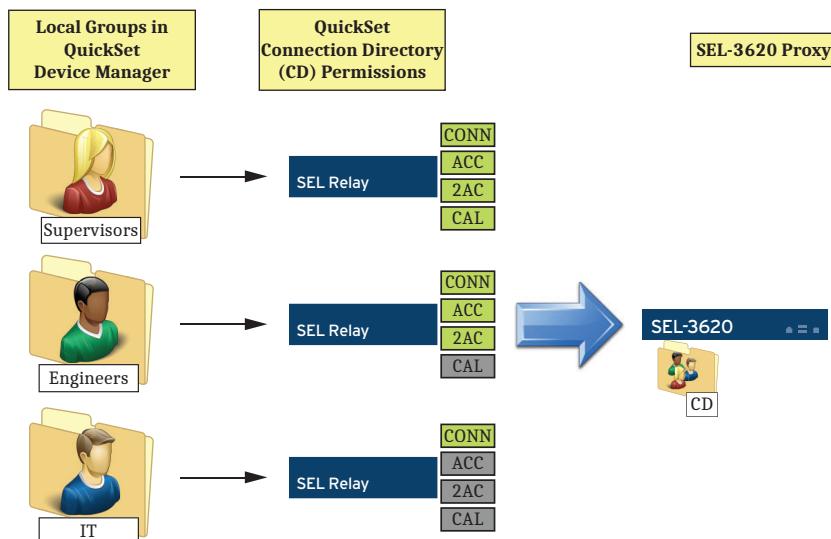


Figure 7.33 Associate Local/RADIUS Groups With IED Permissions

To associate groups in Device Manager with IED permissions, complete the following steps:

- Step 1. Log in to Device Manager as the quickset user.
- Step 2. Expand the previously created Connection Directory with the SEL-3620 and the SEL-787 (or your own serial IED).
- Step 3. Expand the SEL-787 IED by double-clicking the template.
- Step 4. Under the **Permissions** tab in the left pane, select **Add**, and select the groups that you would like to give access to the IED (you may select multiple groups by holding the <Ctrl> key while selecting). Select **OK** when finished.

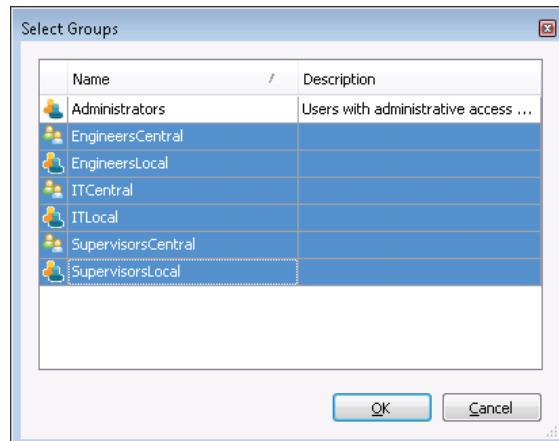


Figure 7.34 Selecting Groups in the IED Permissions Tab

- Step 5. For each group, select the **Allow** check box on each SEL authorization level to which you would like to give the respective group access. In this example, we choose the following permissions:

- **Supervisors:** All permissions
- **Engineers:** Connect, Access Level 1 and Access Level 2 permissions
- **IT:** Connect permissions only

7.26 | Proxy Services and Password Management
Using the SEL-3620 Proxy Services

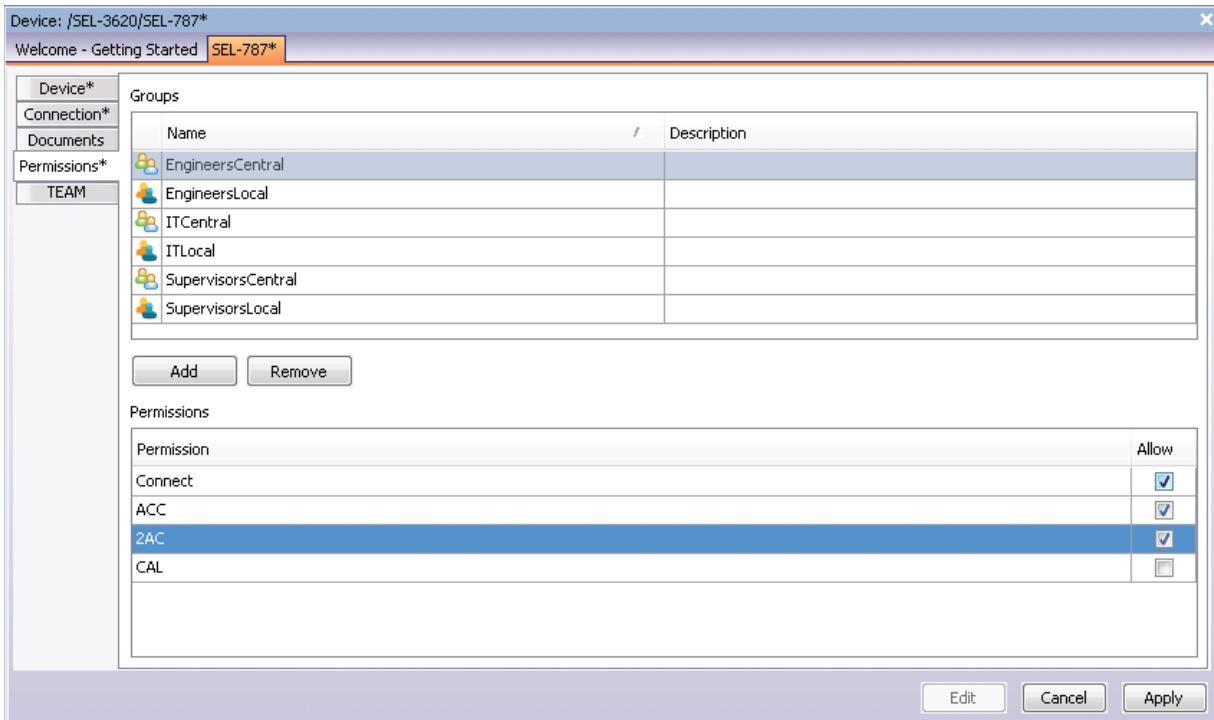


Figure 7.35 IED Permissions Tab Settings

Step 6. When finished, select **Apply**.

Step 7. Right-click on **SEL-3620** in the **Connection Explorer** window, and select **Device Tasks > Send** from the displayed menu. This will send the test Connection Directory to the SEL-3620. Ensure the upload completes without errors.

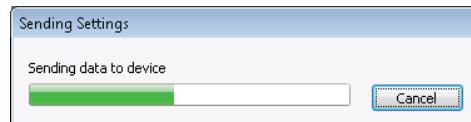


Figure 7.36 Uploading the Connection Directory to the SEL-3620

Step 8. Log in to the SEL-3620 web interface. Under **Reports**, in **System Logs**, verify that the SEL-3620 Syslog shows that the Connection Directory was successfully uploaded.

Using the SEL-3620 Proxy Services

Introduction

This section details the following configuration and testing steps:

- Creating an SMP on the SEL-3620
- Navigating the SEL-3620 Proxy Services via a terminal application
- Using the SEL-3620 Proxy Services via QuickSet
- Proxy Services privileges and blacklisted commands

- Proxy Services audit trail with Syslog and the Commands and Devices Report
- Troubleshooting

Scenario Configuration

Figure 7.37 shows the current configuration for this section. You may replace the network addresses with your own IP address, depending on your SEL-3620 network settings. This example uses an SEL-787 relay for testing. You may use your own SEL IED connected to the SEL-3620 via a null-modem serial cable (such as an SEL-C273A). Note that the use of the CAS is optional.

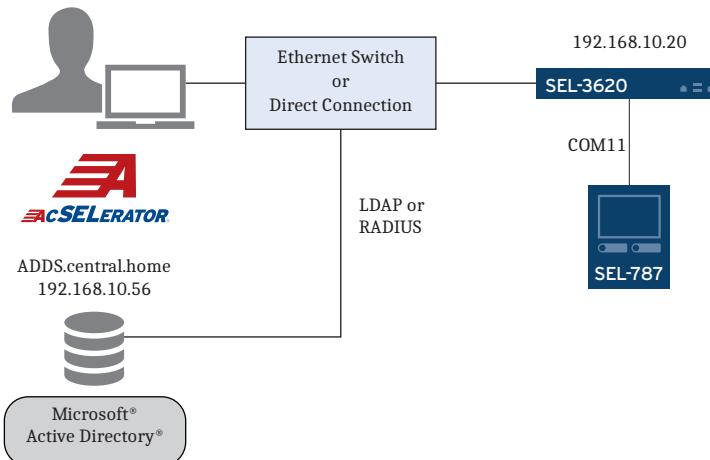


Figure 7.37 Initial Configuration Network Diagram

Creating an SMP on the SEL-3620

In this section, an access point is created on the SEL-3620 through which to reach the Connection Directory IEDs previously uploaded to the SEL-3620. This Proxy Services access point, known as a Scripting-Enabled Master Port (SMP) on the SEL-3620, can be configured to be accessible via Secure Shell (SSH), Telnet, Raw TCP, Serial, or Modem. Only one communication method may be used; for example, an SMP configured for use with Telnet cannot also support communication via Raw TCP.

This example uses SSH because the communications stream is encrypted between the client and the SEL-3620. The SMP is an ASCII-driven interface that is accessible from most any terminal program, such as HyperTerminal, Tera Term, or PuTTY.

To create an SMP, complete the following steps:

- Step 1. Log in to the SEL-3620 web server as an administrative user, and select **Port Mappings** in the navigation panel.
- Step 2. Select **Add Group** from the top of the page to create a new port mapping group. Provide the new group with an Alias such as “Engineering Access.” Select **Submit** when finished.

Figure 7.38 Adding a New Group

- Step 3. Select **Add Device** in the newly created group to add a remote access communications driver. In the **Add Device** form, select **Ethernet Listen Local** from the dropdown list and select **Submit**.
- Step 4. Complete the Add Ethernet Local Driver form as shown in *Figure 7.39*. When finished, select **Submit**.

Figure 7.39 Ethernet Listen Local Driver

NOTE: The SMP emulates a terminal interface, and therefore requires a Termination String with a Leading Time to prevent binary file transfers from “triggering” a disconnection sequence. The default Termination String is <Ctrl-W>, or \017 in hexadecimal. At this time, SEL does not suggest using <Ctrl-Q>, or \011 for the termination string because of conflicts with software flow control (XON/XOFF).

- Step 5. In the Engineering Access Port Group you just created, you should now be able to see the Connection Directory that you previously uploaded from QuickSet (see *Figure 7.40*). If your port group does not look similar to the figure below, see *Troubleshooting* on page 7.41 for more information.

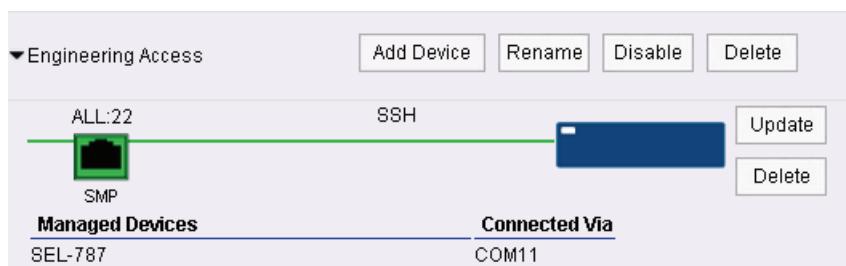


Figure 7.40 Engineering Access SMP

Accessing the SEL-3620 SMP

Now that we have created a Proxy Services Access Point on the SEL-3620, we can now access our Connection Directory IEDs, protected by the SEL-3620 Authentication and Authorizations features (as dictated by the QuickSet permissions in *Configuring Group Access Permissions for Proxy Services* on page 7.14), and the detailed accountability trail provided by the SEL-3620 Commands and Devices report.

For SEL IEDs, the SEL-3620 SMP allows authenticated users to access connected devices at the access levels that are authorized in the QuickSet Connection Directory. These users will be granted access without needing knowledge of the access-level passwords. Users that are not authorized to access specific SEL IED access levels will still be granted access, if they have knowledge of the access passwords of the device.

For Local authentication and authorization, the connection scenario will look similar to that shown in *Figure 7.41*. The SEL-3620 will authenticate using a local account, and then allow access to the IED(s), based on its group membership, so long as it matches the permissions given in the Connection Directory.

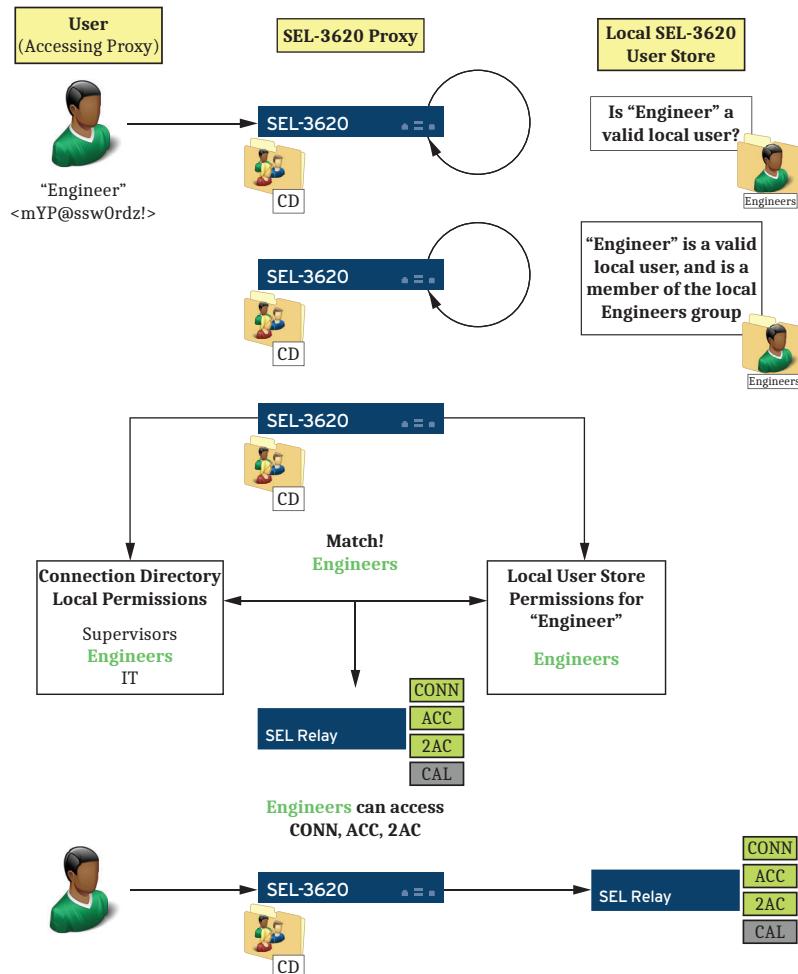


Figure 7.41 Local Access to the SEL-3620 Proxy

For LDAP authentication and authorization, the connection scenario will look similar to that shown in *Figure 7.42*. The SEL-3620 will send the username and password to an LDAP server. The SEL-3620 will then allow access to the IED(s),

7.30 | Proxy Services and Password Management Using the SEL-3620 Proxy Services

based on authorizations received from the LDAP server, as long as they match the permissions given in the Connection Directory. Note that in the figure, the group membership attribute “memberOf” can be configured by a user in both QuickSet and the SEL-3620.

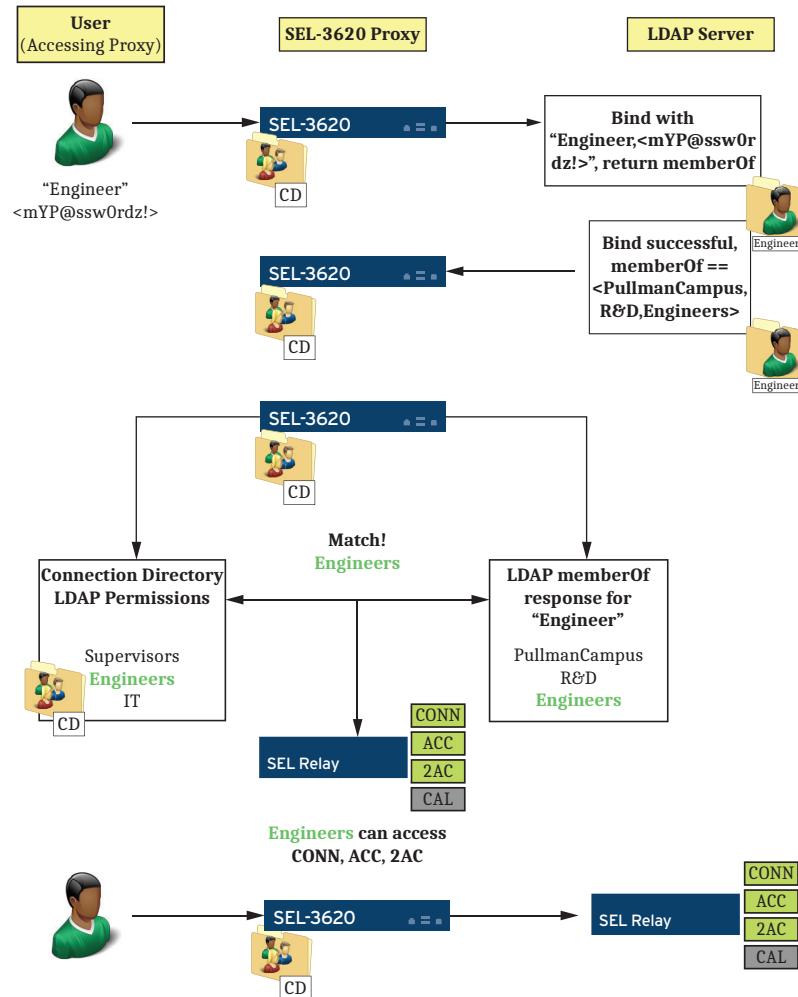


Figure 7.42 LDAP Access to the SEL-3620 Proxy

For RADIUS authentication and authorization, the connection scenario will look similar to that shown in *Figure 7.43*. The SEL-3620 will send the username and password to a RADIUS server. The SEL-3620 will then allow access to the IED(s), based on authorizations received from the RADIUS server, so long as they match the permissions given in the Connection Directory.

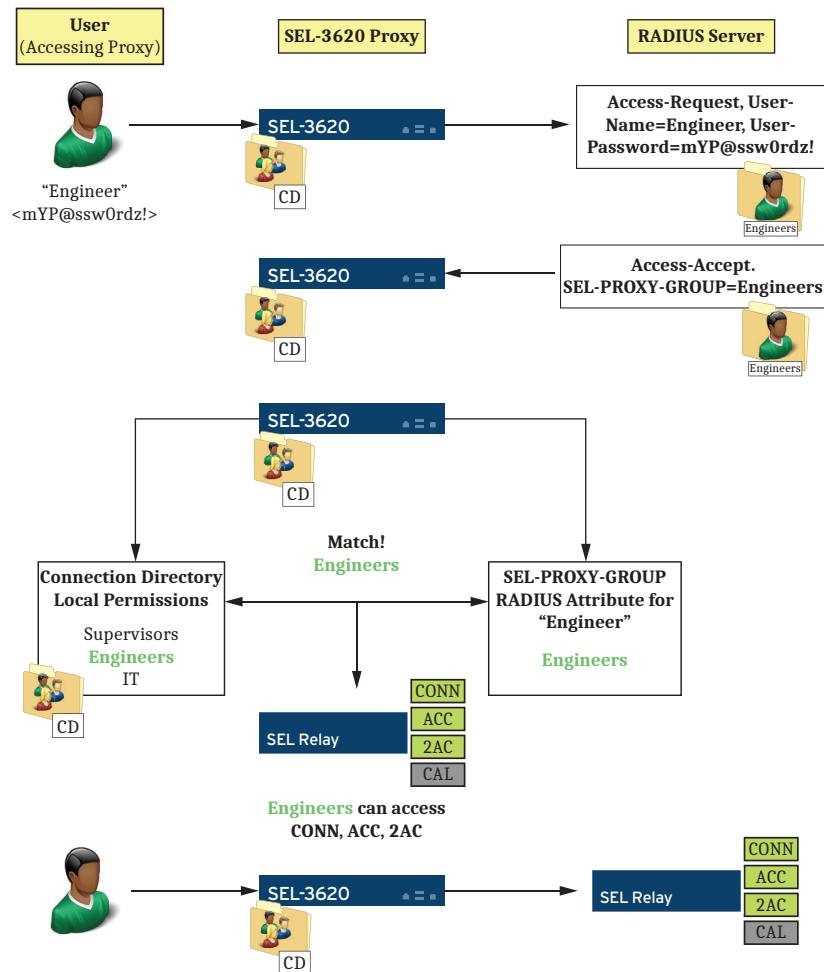


Figure 7.43 RADIUS Access to the SEL-3620 Proxy

Navigating the SEL-3620 SMP via a Terminal Application

To access our Connection Directory devices via the SMP through use of a terminal application, complete the following steps:

- Step 1. Open your terminal application software and open a connection to the SMP you just created. In this case, the IP is 192.168.10.20 and the TCP port is 22 (for access via the SSH protocol). Log in to the SMP by using the supervisorlocal name and password (you can choose to use the central **supervisorcentral** account if you have LDAP connectivity from the SEL-3620). If you are unable to successfully log in to the SEL-3620, see *Troubleshooting* on page 7.41.

NOTE: You may receive a security message from your terminal software regarding the SSH key presented by the SEL-3620. This is normal for first-time connections. You may wish to check the SSH Host Key section of the SEL-3620 webpage to ensure the signature matches. If there are no signature mismatches, select **Accept** to continue. If the message shows up again in the future when connecting from the same computer, then it could mean that your terminal software is connecting to the wrong device. If this happens, notify your cybersecurity manager for guidance.



Figure 7.44 Tera Term Connection to SMP

- Step 2. If you have successfully connected to the SEL-3620 SMP, you should see a star prompt *. Type **WHO** to see the list of Connected Directory devices that are accessible by the supervisorlocal user (created in *Configuring Group Access Permissions for Proxy Services* on page 7.14). If the result from the **WHO** command is empty, see *Troubleshooting* on page 7.41.

```
*who
Available Devices:
1      SEL-787
*
```

Figure 7.45 WHO Command From the SMP

- Step 3. Type **SEL 1** into the terminal prompt, and press <Enter> to select the SEL-787. You should now be connected to the interface of the selected IED. If you are unable to connect to the IED and receive a prompt, see *Troubleshooting* on page 7.41 (if you get no IED prompt, type <Ctrl+W> to navigate back to the SMP prompt).

```
*who
Available Devices:
1      SEL-787
*sel 1
=
```

Figure 7.46 SEL IED Interface on the SMP

- Step 4. Next, you should ensure that you can access the authorization SEL IED access levels (Access Level 1, Access Level 2, etc.) without the need for knowledge of individual passwords. Type **ACC** into the terminal prompt, and ensure that you can access Access Level 1 without needing to know the Access Level 1 password. Also navigate to Access Level 2, Access Level C, or other access levels on the device to ensure access to those levels are supported by scripts from the SEL-3620 Proxy Services, and you do not need knowledge of the individual passwords. If you are unable to connect to certain access levels, or you receive unexpected prompts from the SEL-3620, see *Troubleshooting* on page 7.41.

```
*who
Available Devices:
1      SEL-787

*sel 1

=acc

=>

=>2ac

=>>

=>>cal

=>>>

=>>>
```

Figure 7.47 SEL IED Access Levels

Active Proxy Session: Special Commands

SEL IED ASCII commands are available and usable through the SEL-3620 SMP. YMODEM read/write commands and binary file transfers are available as well. Some special ASCII commands (case agnostic) are treated differently:

- **KILL**: The **KILL** command will halt the SEL-3620 script engine and disconnect the user from the SEL-3620 SMP for about 60 seconds. This command is meant to give the user control to terminate stalled script execution that the SEL-3620 SMP is executing.
- **PAS**: The **PAS** command is blocked by the SEL-3620 SMP. Executing the **PAS** command will result in the SEL-3620 SMP returning the message `Command not allowed` (see *Figure 7.48*).
- **ACC, 2AC, CAL, PAC, BAC, OAC, AAC, EAC, EZA, BRE**: If the user has been given permissions to the specified access level in Device Manager, these keywords trigger the SEL-3620 to change levels from the current level to the desired authorization level (e.g., transition from Access Level 1 to Access Level 2, etc.). If the user has not been permitted to access the desired level, the SEL-3620 will not script the change, but instead pass the command on to the end IED.
- **<Ctrl+W>** (hex \017), **<Ctrl+Q>** (hex \011), **<Ctrl+E>** (hex \005): These special commands are interpreted as termination strings by the SEL-3620. These termination strings—and respective Leading Times—are defined on the Port Mappings page for the specific SMP. From an active proxy session, typing the termination string (**<Ctrl+W>** by default) after the specified Leading Time will terminate the active proxy session and bring the terminal back to the SMP Prompt. Note that **<Ctrl+Q>** (hex \011) for the termination may conflict with software flow control (XON/XOFF).

```
=>>pas
Command not allowed

=>>
```

Figure 7.48 SEL-3620 SMP Blocks the PAS Command

Active Proxy Session: Binary Mode

As of firmware versions R139 and later, the SEL-3620 supports a special Binary Transfer Mode on Telnet and SSH proxy sessions. When binary mode is activated, the SEL-3620 will send all data directly to the end device without looking for special commands. The only exception to this is the Termination String (e.g., <Ctrl+W>) which is available to terminate a connection. Use this mode only under special circumstances, such as when accessing GE relays.

Most terminal emulators support the use of the break command. See *Figure 7.49* for an example of how to send the break command during an active proxy session.

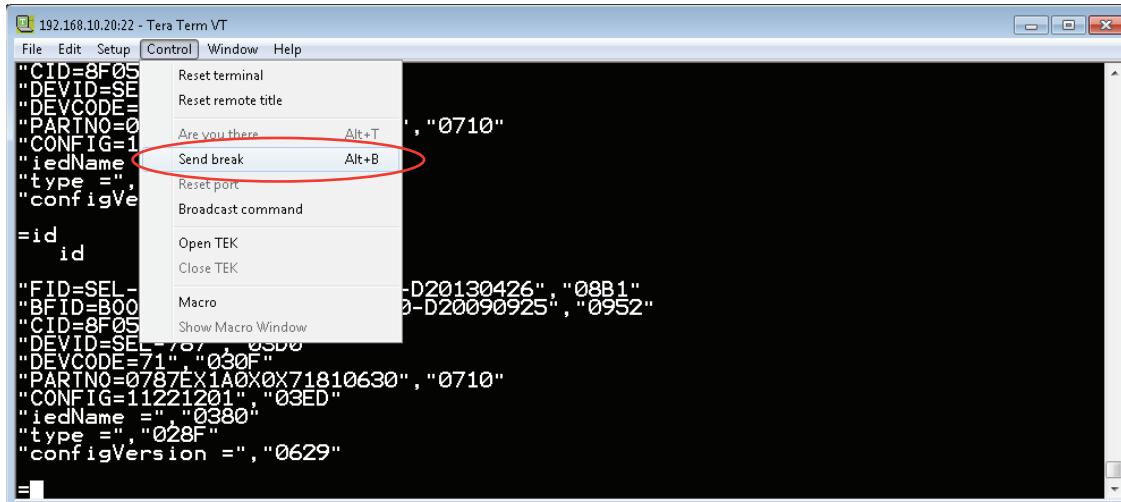


Figure 7.49 Binary Mode Control

Binary mode is especially useful when connecting to third-party IEDs that require binary protocols (e.g., Modbus).

Access and Terminate Scripts on Managed IEDs

NOTE: Because of the sensitive nature of the managed IEDs, ensure that Access and Terminate scripts only come from trusted sources and are properly verified and vetted.

Access scripts are executed as soon as a connection to a device is established. Terminate scripts are executed immediately before disconnecting from a device. Access and Terminate scripts are very useful at getting devices into a desired state before executing normal functions (e.g., changing a password). In some scenarios, Access and Terminate scripts are required for proper behavior (see *Management of SEL Communications Processors* on page 7.87).

Access and Terminate scripts on IEDs below an SEL-3620 (in the Connection Directory) are run by the SEL-3620 under three different circumstances:

1. Whenever a user accesses or terminates from the IED from the SEL-3620 SMP.
2. Whenever the SEL-3620 accesses or terminates from the device for password management.
3. If the device is accessed to access another device (i.e., the device is a terminal server or a communications processor [like an SEL-2032]).

Access and Terminate scripts on the SEL-3620 itself are not run by the SEL-3620. Instead, these scripts are used by QuickSet when accessing IEDs in Device Manager through the SEL-3620.

NOTE: Because the Connection Directory contains sensitive information, SEL recommends that its creation, maintenance, export, import, and handling are protected by secure practices.

Users can write their own Access and Terminate scripts and use them with IEDs in the Connection Directory. For information about how to write scripts in Device Manager, see the QuickSet documentation.

Access and Terminate scripts on the SEL-3620 itself are run from within the context of QuickSet itself. They are useful for automating access to IEDs managed by the SEL-3620 (reducing the number of clicks required).

Navigating the SEL-3620 SMP via QuickSet

Users may also choose to use QuickSet software to access IEDs directly from Device Manager Connection Directory. Users can then use QuickSet to download/upload settings, check the HMI, and download event reports automatically.

For maximum compatibility between QuickSet and the SEL-3620 proxy, it is highly recommended that you configure the following features before you begin:

1. **Enable Control Characters on the QuickSet Terminal:** Open the QuickSet terminal (<Ctrl+T> or select **Communications** and then **Terminal**). Select the **Send Ctrl Characters** check box. This will ensure QuickSet can send termination characters to the SEL-3620 (see *Figure 7.50*).

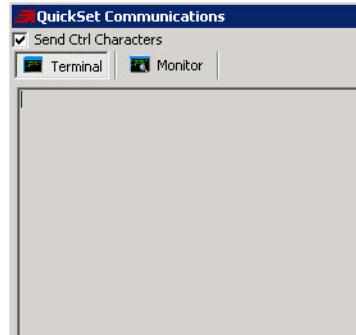


Figure 7.50 Allow Ctrl Characters on QuickSet Terminal

2. **Enable Monitoring on the QuickSet Terminal:** Under **Tools**, select **Options**. Under the **Options** window, in the **Communications** tab, select the **Enable Advanced Communications Settings** check box. Select to clear the **Auto-Detect Connection** check box, and select the **Enable Monitoring** check box. This helps with troubleshooting any proxy issues (see *Figure 7.51*).

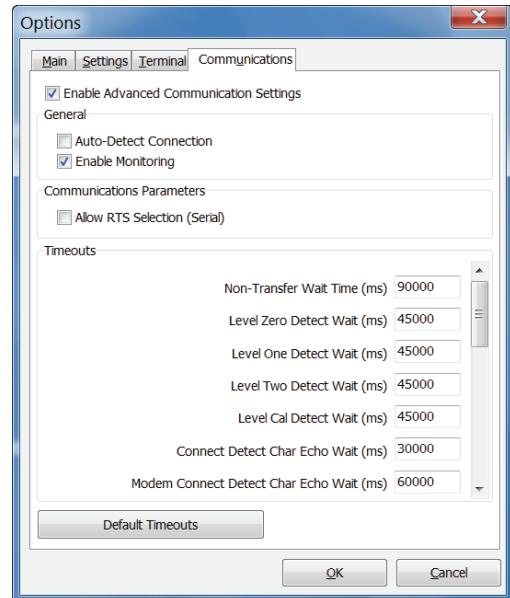


Figure 7.51 QuickSet Communications Options

To access the SEL-787 through the SEL-3620 Proxy Services with QuickSet, use the following steps:

Step 1. Under the **Connection Explorer** window, on the SEL-3620 page, in the **Connection** tab, select **Edit**. Fill in the settings as shown below. Select **Apply** when finished.

- **Access Script:** GENERAL_362X_ACCESS_SCRIPT
- **Terminate Script:** GENERAL_362X_TERMINATE_SCRIPT
- **First Delay Time:** 1
- **Second Delay Time:** 1
- **Termination String:** \017 (this matches the <Ctrl+W> terminate sequence of the SMP)
- **Pass Through Port:** 0

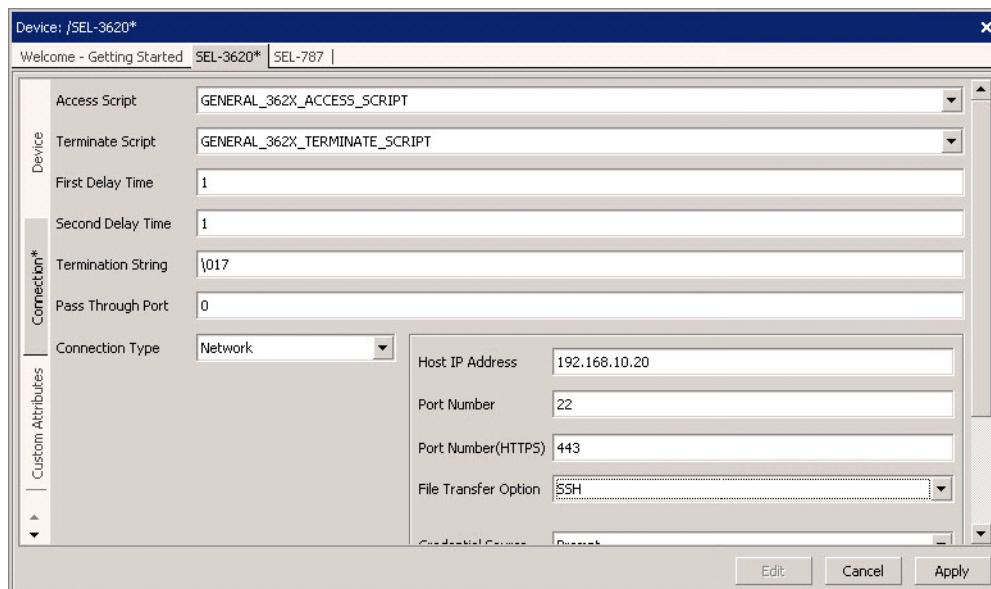


Figure 7.52 SEL-3620 Connection Settings

- Step 2. Next, log in to the QuickSet Database as a user who has privileges on the SEL-787 IED, such as **supervisorlocal**.
- Step 3. In the **Connection Explorer** window, right-click on **SEL-787**, and select **Connect**.

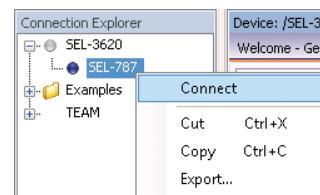


Figure 7.53 Connecting to the SEL-787

NOTE: The Device Manager in QuickSet will use the credentials of the current user in QuickSet to authenticate to the SEL-3620 proxy.

- Step 4. Receiving a Device Authentication prompt from QuickSet is normal for SSH connections between QuickSet and the SEL-3620. You may choose **Trust** to permanently trust the SEL-3620 SSH signature or **Trust Once** to temporarily trust the SEL-3620 SSH signature.
- Step 5. Green dots next to the SEL-3620 and SEL-787 templates indicate a successful connection has been made. If you do not connect successfully to the SEL-787, see *Troubleshooting* on page 7.41.

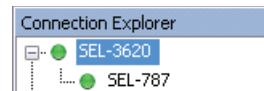


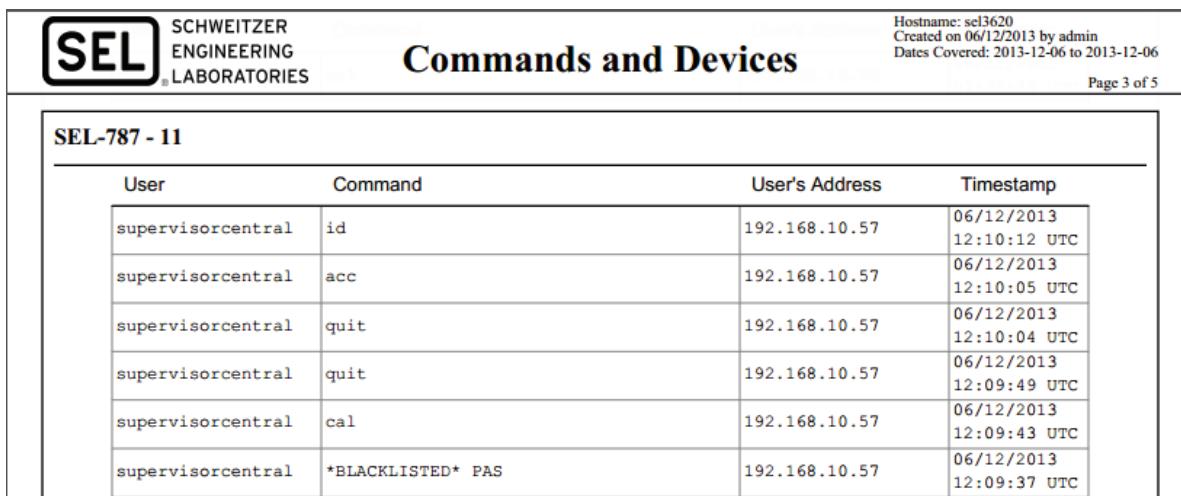
Figure 7.54 Successful Proxy Services Connection Through QuickSet

From this state, you can download/upload device settings, check the current running HMI, and download event reports (right-click on the active SEL-787 template to see a list of options).

- Step 6. To disconnect from the SEL-787 IED, right-click on **SEL-787**, and select **Disconnect**.

SEL-3620 Commands and Devices Report

All connections to the SEL-3620 SMP are logged via the SEL-3620 Syslog logging function, and all ASCII commands executed on IEDs when connected through the SEL-3620 SMP are logged to the SEL-3620 Commands and Devices report. This report contains information about the user who executed the commands, the commands themselves, the user's IP address or serial COM port number, and UTC time stamp to the second. *Figure 7.55* shows an example of this information.

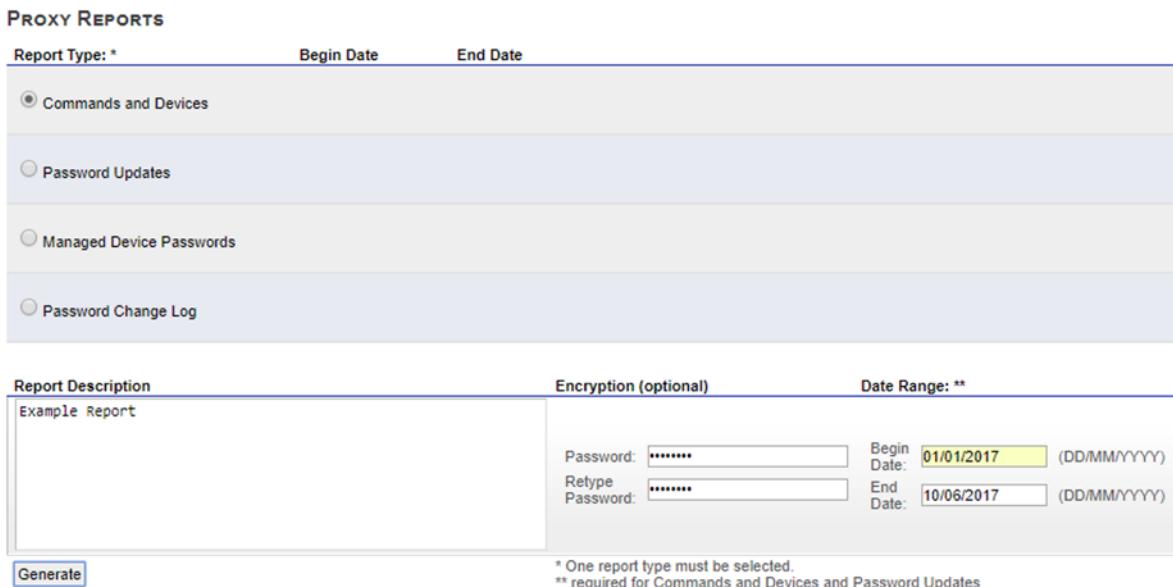


The screenshot shows the SEL-3620 Commands and Devices report. At the top left is the SEL logo and "SCHWEITZER ENGINEERING LABORATORIES". The title "Commands and Devices" is centered above a table. At the top right, it shows "Hostname: sel3620", "Created on 06/12/2013 by admin", "Dates Covered: 2013-12-06 to 2013-12-06", and "Page 3 of 5". The table has columns: User, Command, User's Address, and Timestamp. The data shows six entries from a user named "supervisorcentral".

User	Command	User's Address	Timestamp
supervisorcentral	id	192.168.10.57	06/12/2013 12:10:12 UTC
supervisorcentral	acc	192.168.10.57	06/12/2013 12:10:05 UTC
supervisorcentral	quit	192.168.10.57	06/12/2013 12:10:04 UTC
supervisorcentral	quit	192.168.10.57	06/12/2013 12:09:49 UTC
supervisorcentral	cal	192.168.10.57	06/12/2013 12:09:43 UTC
supervisorcentral	*BLACKLISTED* PAS	192.168.10.57	06/12/2013 12:09:37 UTC

Figure 7.55 Commands and Devices Report

In the navigation panel, on the SEL-3620 **Reports** page, select **Proxy Reports** to open the Commands and Devices report. To generate a report, select **Commands and Device**, and enter the date range for which you want to view user command data (in day/month/year format—see *Figure 7.56*). You can optionally choose to encrypt the report with a provided password. Select **Generate** to create the report.



The screenshot shows the "PROXY REPORTS" configuration page. Under "Report Type:", "Commands and Devices" is selected. Below that, there are four options: "Password Updates", "Managed Device Passwords", and "Password Change Log", each with a radio button. At the bottom, there are fields for "Report Description" (containing "Example Report"), "Encryption (optional)" (with "Password:" and "Retype Password:" fields), and "Date Range: **" (with "Begin Date" set to "01/01/2017" and "End Date" set to "10/06/2017"). A note at the bottom states: "* One report type must be selected." and "** required for Commands and Devices and Password Updates". A "Generate" button is at the bottom left.

Figure 7.56 Commands and Devices Report Generation

NOTE: As of firmware version R139, the SEL-3620 will generate a report with as many as 20,000 events. If there are more than 20,000 events for the given date range, the SEL-3620 will only show the most recent 20,000 events. Attempting to generate Commands and Devices reports on previous firmware versions of more than 20,000 events may result in extremely long generation times.

The SEL-3620 generates reports in both PDF and JSON formats. The PDF format is best for readability, while the JSON file is better suited for subsequent processing of the information by external processing. You should save both file types to secure offline storage for safekeeping.

SEL-3620 Encrypted Proxy Reports

If you chose to generate an encrypted report, you will need to decrypt it offline before viewing it by using direct decryption with openSSL.

To decrypt with openSSL, run the following command:

openssl enc -d -a -aes-256-cbc -md md5 <fileIn> -pass pass:<password> -out <fileOut>.gzip. <fileIn>, <fileOut>, and <password> should be replaced with the respective input file name, output file name, and the password used to encrypt the file originally. The resultant file is compressed with gzip and will need to be uncompressed using software such as gunzip or 7-zip. Then the appropriate extension, such as .pdf or .json, must be applied to the file. At this point, the file can be opened in the desired viewer.

SEL-3620 Proxy Syslog Messages

While the Commands and Devices report captures granular user-session data, the SEL-3620 also captures more general security information about user connection to the Proxy via Syslog. An SEL-3620 administrative user can configure as many as three different Syslog server destinations, which can be common Security Information Event Management (SIEM) servers, such as Splunk, QRadar, Log-Rhythm, and others.

Proxy Services FAQ

Can I use the SEL-3620 proxy with legacy SEL PC Software?

The SEL-3620 proxy supports the use of the following SEL PC software:

- ▶ SEL-5010 Relay Assistant Software
- ▶ SEL-5020 Settings Assistant Software
- ▶ ACSELERATOR Report Server SEL-5040 Software

Use of SEL-5010, SEL-5020, and Report Server requires the use of SEL-5827 Virtual Connect Client or SEL-5828 Virtual Connect Service to fully integrate with the SEL-3620 proxy. See *Using the SEL-3620 Proxy With SEL-5020 Settings Assistant Software* on page 7.99 for more information about SEL-5827 software. Note that the SEL-3620 proxy does not support server-to-client connections with Report Server, and does not support FTP with SEL-5010 and Report Server.

Does the SEL-3620 proxy change how the IED interface looks when connected via terminal?

Because of the hold-back nature of the SEL-3620 proxy, it does slightly change the look of the IED interface when viewed through a proxy. See *Figure 7.57* and *Figure 7.58* for an example of the difference in the look of a directly connected IED compared to one that is proxied through the SEL-3620. In the latter case, the SEL-3620 proxy echoes back the echo from the SEL IED.

```
=id
"FID=SEL-787-R207-VO-Z003001-D20111107", "08AB"
"BFID=BOOTLDR-R500-VO-Z000000-D20090925", "0952"
"CID=2E90", "025D"
"DEVID=SEL-787", "03D0"
"DEVCODE=71", "030F"
"PARTNO=0787EX1AOX0X71810630", "0710"
"CONFIG=11221201", "03ED"
"iedNAME =", "028f"
"type =", "028F"
"configVersion =", "0629"
=
```

Figure 7.57 Direct Terminal Connection to SEL IED

```
=id
    id
"FID=SEL-787-R207-VO-Z003001-D20111107", "08AB"
"BFID=BOOTLDR-R500-VO-Z000000-D20090925", "0952"
"CID=2E90", "025D"
"DEVID=SEL-787", "03D0"
"DEVCODE=71", "030F"
"PARTNO=0787EX1AOX0X71810630", "0710"
"CONFIG=11221201", "03ED"
"iedNAME =", "028f"
"type =", "028F"
"configVersion =", "0629"
=
```

Figure 7.58 Terminal Connection to SEL IED (Proxied)

Can I use the SEL-3620 proxy with TEAM?

Yes, the SEL-3620 proxy supports the use of TEAM software. See *Using TEAM With the SEL-3620 Proxy* on page 7.128 for more details.

Can I access third-party IEDs through the SEL-3620 proxy?

In many cases, the SEL-3620 supports connecting to third-party IEDs through the proxy. If the IED you are trying to access has an ASCII-based terminal, you may create your own Access and Terminate scripts in Device Manager to navigate that device and to change the password of the IED. Accessing the IED may require the use of SEL-5827 Virtual Connect Client to work properly with the SEL-3620 proxy. See *Using the SEL-3620 Proxy With SEL-5020 Settings Assistant Software* on page 7.99 for more information about SEL-5827 software.

Can I access a computer using Windows Remote Desktop Protocol (RDP) through the SEL-3620 proxy?

At this time, the SEL-3620 proxy does not support RDP connections.

Can I access FTP servers through the SEL-3620 proxy?

Yes, see *Management of Ethernet-Connected IEDs* on page 7.74 for more details.

Troubleshooting

There Is No Connection Directory Information in My SMP

If you do not see any Managed Devices in your SMP, select **Update** next to the Ethernet Listen Local member and ensure that both the **Master Port** and **Allow Script** check boxes are selected.

The Managed Device in My SMP Has a Name That Looks Scrambled

If the Global Device ID (GDID) of the Connection Directory IED has not been changed to match the Device Name, the SMP on the SEL-3620 may look similar to *Figure 7.59*.

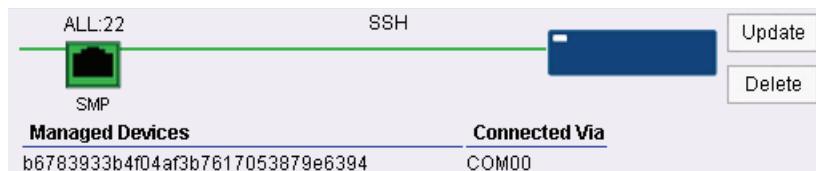


Figure 7.59 “Scrambled” Connection Directory IED

To fix this, change the GDID of your IED in the Connection Directory to match the Device Name, and reupload the Connection Directory to your SEL-3620.

Unable to Successfully Log In to the SEL-3620 SMP

If a user is not able to successfully authenticate to the SEL-3620 SMP, check the following.

For Centralized Users

- Ensure the SEL-3620 has connectivity to the CAS.
- Ensure the centralized user is not disabled, or that the user does not need to change passwords on the next login.
- For LDAP, ensure the centralized user is a member of a centralized group that has been given access to at least one of the Connection Directory IEDs. Use the Device Manager User Manager page in QuickSet to discover all Connection Directory authorization information. *Figure 7.60* shows the centralized group **SupervisorsCentral** with its respective centralized users, with the list of its Connection Directory permissions.
- For RADIUS troubleshooting, see *Using RADIUS* on page 3.15.

NOTE: As of firmware version R210, the SEL-3620 no longer supports TLSv1.1 authentication. Ensure that the CAS supports TLSv1.2 or TLSv1.3 authentication.

7.42 | Proxy Services and Password Management
Using the SEL-3620 Proxy Services

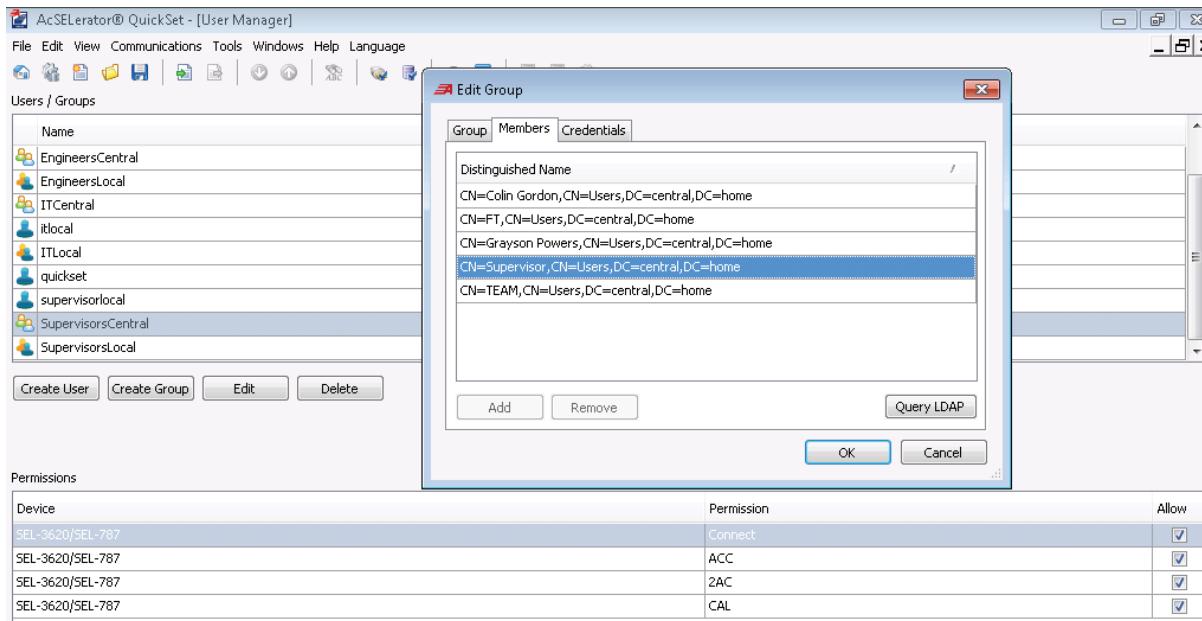


Figure 7.60 User Manager With Groups and Permissions

For Localized Users

- Ensure the usernames and passwords *match exactly* between the QuickSet User Manager and the SEL-3620 with the SMP.
- Ensure the local user account is not currently disabled on the SEL-3620.

No Available Devices When I Use the WHO Command on the SMP

When logged in to an SEL-3620, you might not see any Available Devices when running the **WHO** command.

```
*who
Available Devices:
*
```

Figure 7.61 No Available Devices

The primary reason the SEL-3620 SMP would return an empty list is because the user authorizations are not configured to allow the current user to access the SEL-3620. Check the following:

- Ensure the accessing user is a member of a group that has been given access to at least one of the Connection Directory IEDs in Device Manager. Use the Device Manager User Manager page in QuickSet to discover all Connection Directory authorization information (see *Figure 7.60*).
- For LDAP users, ensure your group has been given authorization to one or more IEDs in the Connection Directory.
- For RADIUS users, ensure the RADIUS SEL-PROXY-GROUP attribute being passed to the SEL-3620 matches the name of at least one local group to which you have granted permissions to one or more IEDs in the Connection Directory. For more information about RADIUS, see *Using RADIUS* on page 3.15.

- Ensure that the **Connect** check box has been selected for the accessing user's group in the Connection Directory Permission tab on the IED. At the very minimum, the **Connect** level needs to be allowed for the accessing user to view the Connection Directory (see *Figure 7.62*).

Permissions	
Permission	Allow
Connect	<input checked="" type="checkbox"/>
ACC	<input checked="" type="checkbox"/>
2AC	<input checked="" type="checkbox"/>
CAL	<input checked="" type="checkbox"/>

Figure 7.62 Connection Directory Permissions Tab

Unable to Connect to the IED While on the SMP Prompt

If you are unable to connect to the connection directory device (similar to *Figure 7.63*), check the following:

- Ensure the connection parameters for the IED in the QuickSet Connection Directory are accurate. If there is a mismatch in baud rate or bit types, you will have connection issues.
- Ensure the serial cable is connected from the correct COM port on the SEL-3620 to the SEL IED, and that the SEL IED can “talk” to a terminal connected to its serial port.
- Ensure the **Pass Through Port** setting on the IED Connection Directory template matches the COM port on the SEL-3620 you are connecting to the SEL IED.
- Ensure you are currently not using the serial port on the SEL-3620 as part of any other existing Port Group in the Port Mappings page.

```
*who
Available Devices:
1      SEL-787
*sel 1
```

Figure 7.63 Unable to Connect to a Serial Connection Directory Device

SEL-3620 SMP Reports “Device failed to gain access level”

In some instances, the SEL-3620 SMP may report the message **Device failed to gain access level** (see *Figure 7.64*).

```
=>>cal
Device failed to gain access level CAL
```

Figure 7.64 SEL-3620 SMP Reports “Device failed to gain access to level”

This message is most likely because of the MAXACC setting of the SEL IED port being set to block access to the access level that is the user is attempting to navigate to. You may consider changing the MAXACC setting on the SEL IED to allow access to the specific access level.

Another cause for this error is the SEL-3620 attempting to change access levels while the relay is in an account-lockout window (typically 30 seconds). This can happen if an SEL-3530 RTAC has attempted to enter Access Level 1 for autoconfiguration purposes on the same serial port and locked out the relay. Exit the proxy session and attempt to establish another connection.

This error could also be attributed to the end IED having an emergency access password bypass jumper enabled. If the password bypass jumper is currently in place on an SEL IED, it can cause issues with the SEL-3620 script engine.

```
=>>set p MAXACC
      set p MAXACC
Port 5
Ethernet Port Settings:
Maximum Access Level(0,1,B,2,C)          MAXACC = 2      ? C
```

Figure 7.65 Setting MAXACC on the Port

SEL-3620 SMP Reports “Device responded with: ‘Invalid Password’”

In some instances, the SEL-3620 SMP may report back the message Device responded with: ‘Invalid Password’ when the user attempts to navigate to an access level (see *Figure 7.66*).

```
=>2ac
      Device responded with: "Invalid Password", when trying to gain access level
      2AC
```

Figure 7.66 SEL-3620 SMP Reports “Device responded with: ‘Invalid Password’”

This message is most likely because of a password mismatch between the SEL-3620 IED password database and the actual IED password. To fix the mismatched password, complete the following steps:

- Step 1. Generate a Managed Device Passwords report on the SEL-3620. Check the access level password of the IED in question as recorded on the report.
- Step 2. Check the actual password of the IED. Refer to the IED product literature about how to do this.
- Step 3. Under the SEL-3620, on the **Password Management** page, select **Assign Password** to update the SEL-3620 IED password database with the correct IED password.

SEL-3620 SMP Reports “Traceback”

Under specific circumstances, the SEL-3620 SMP may report a Traceback when attempting to connect to a device, similar to the message shown in *Figure 7.67*.

```
*who

Available Devices:
1       SEL-787

*sel 1
      Traceback (most recent call last):
      File "/python/main_wrapper.py", line
      169, in (module)
            sys.exit(main())
```

Figure 7.67 SEL-3620 SMP “Traceback”

This is most likely because of an unsupported Access Script having been configured on the device in QuickSet. An example of an unsupported Access Script would include GENERAL_362X_ACCESS_SCRIPT, which should only be used on an SEL-3620 template (see *Figure 7.68*).

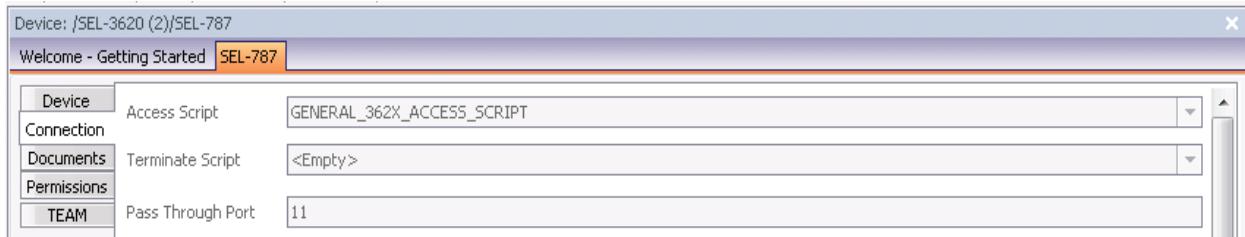


Figure 7.68 Unsupported Access Script on IED

Fixing the issue is typically just a matter of removing the unsupported Access Script from the IED, and resending the Connection Directory to the SEL-3620. If this problem persists, contact your local SEL representative.

SEL-3620 SMP Interferes With Valid Use of BAC and Other Trigger Commands

In rare instances, the SEL-3620 SMP will “catch” valid settings that are also trigger words, such as **2AC**, **CAL**, etc., which normally tell the SEL-3620 to pause the terminal and perform a specific action. One example of this is the IPConn setting in the SEL-651R, which can be set to **BAC** (BAC also corresponds to a valid access level on the relay).

```
=2ac

=>>set g ipconn
      set g ipconn

Current and Voltage Connection Settings:
I123 Terminal Conn.(ABC,ACB,BAC,BCA,CAB,CBA)      IPCONN := ABC      ? BAC

CT Polarity(POS,NEG)                                CTPOL := POS      ?
=>>set g ipconn

Current and Voltage Connection Settings:
I123 Terminal Conn.(ABC,ACB,BAC,BCA,CAB,CBA)      IPCONN := ABC      ? BAC

Enable Ground Current Switch(Y,N)                  EGNDSW := Y      ?
```

Figure 7.69 SEL-3620 SMP Interfering With BAC

NOTE: In Figure 7.69, the terminal pauses for around a minute after entering the BAC on the IPConn line. However, the setting is not changed (it stays ABC).

The two possible solutions to this problem are as follows:

1. Using the terminal, send the “break” command (available in R139 or later versions of firmware) before entering **BAC**. This tells the device to go into binary mode and to treat the **BAC** command as a normal string. This will work for Telnet or SSH terminal sessions. Be sure to resend the “break” command after you have finished setting the command to reenable scripted mode.
2. If the first solution does not work, you may manually edit the connection directory to remove user access permissions to Access Level B, and reupload the connection directory to the SEL-3620. If a user does not have permission to Access Level B, the SEL-3620 will not treat the command as special.

SEL-3620 SMP Responds With “The expected specified response to <string> was not encountered”

In cases where an IED has been misconfigured or is not currently reachable, and the IED has an Access script and/or Termination script configured, the SEL-3620 SMP may respond with The expected specified response to <string> was not encountered. This is because these scripts may “want” to see a valid response before succeeding. An example of such script would be the following:

```
SEL.WriteLine("QUIT", ['*', '='], 5)
```

In this example, the script wants to see either ‘*’ or ‘=’ after sending “QUIT.” If a serial link is disconnected, the relay will not respond with the correct string, and you may see a response similar to that shown in *Figure 7.70*.

```
*who

Available Devices:
1      SEL-2032_DIRECT_SERIAL
2      SEL-351-7_DIRECT_SERIAL
3      SEL-451-5_DIRECT_SERIAL
4      SEL-651R-2_DIRECT_SERIAL
5      SEL-787_DIRECT_SERIAL

*sel 1

*The expected specified response to 'QUIT' was not encountered.
```

Figure 7.70 SMP Unexpected Response String

SEL-3620 SMP Responds With “Unable to connect. Port busy.”

If you receive the Unable to connect. Port busy. message similar to that shown in *Figure 7.71*, this is an indication that another proxy user is connected to the SMP and is using the port. All SEL devices only support one connection to a serial port, and most support as many as three simultaneous connections to a Telnet interface (the SEL-3620 currently supports ten simultaneous connections to the SMP). Note that if the connection from the SEL-3620 is connecting to a serial device, only one connection to that device is supported at a time.

```
*who

Available Devices:
1      SEL-2032_DIRECT_SERIAL
2      SEL-351-7_DIRECT_SERIAL
3      SEL-451-5_DIRECT_SERIAL
4      SEL-651R-2_DIRECT_SERIAL
5      SEL-787_DIRECT_SERIAL

*sel 5

Unable to connect. Port busy.
```

Figure 7.71 SMP Port Busy Response

The SEL-3620 SMP Connects at an Elevated IED Access Level

In scenarios where the SEL-3620 is accessing an IED connected via serial, the SEL-3620 may sometimes connect to the IED at an elevated authorization level (see *Figure 7.72*).

```
*who  
  
Available Devices:  
1 SEL-787  
  
*sel 1  
  
==>>
```

Figure 7.72 SMP Connects at Elevated Access Level

This is most likely because of the SEL-3620 terminating from the IED after last accessing the elevated authorization level. There are two ways to solve this issue. Using both methods is recommended.

1. Configure the SEL IED serial port to properly time out after a reasonable amount of time (see T_OUT or TIMEOUT setting on the serial port). When the serial time-out time is reached, the serial port will automatically back itself down to the CONNECT level of the SEL relay.
2. Configure the IED in the QuickSet Connection Directory to use a special Terminate script that will send the QUIT command whenever the Terminate sequence is run. This QUIT script is very simple, and looks similar to that shown in *Figure 7.73*. Simply apply the script as a Terminate script to the IED exhibiting the issue, and reupload the Connection Directory.

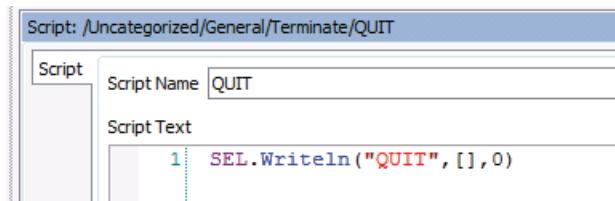


Figure 7.73 Simple IED “QUIT” Terminate Script

Errors Connecting to the SEL-3620 Proxy From Device Manager

If you are unable to access the SEL-3620 proxy from Device Manager, the following tips may help.

Incorrect or Missing Access Script on the SEL-3620

To proxy automatically to a device, you will need to enable the GENERAL_362X_ACCESS_SCRIPT on the SEL-3620 from the Connection tab. If you do not have this script enabled, you can still access an IED below the SEL-3620 by opening the QuickSet Terminal and logging in to the SEL-3620 manually.

Incorrect Username and Password

If you are using “Active User” to connect to the SEL-3620 from Device Manager, make sure the credentials you used to log in to the QuickSet Database have proper authorizations on the SEL-3620 proxy.

QuickSet Attempts to Auto-Detect Connection Settings

Sometimes QuickSet will fail to auto-detect the current connection, which may cause failures to connect to the SEL-3620 proxy. To disable auto-detection of connections, follow these steps:

Step 1. From QuickSet, select **Tools > Options** (see *Figure 7.74*).

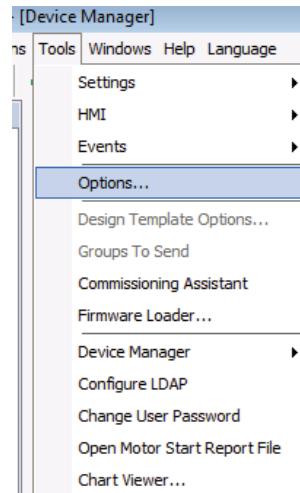


Figure 7.74 QuickSet Options Menu

Step 2. Under the **Options** window, in the **Communications** tab, select the **Enable Advanced Communication Settings** check box. Select **Yes** on the popup window, then clear the **Auto-Detect Connection** check box (see *Figure 7.75*).

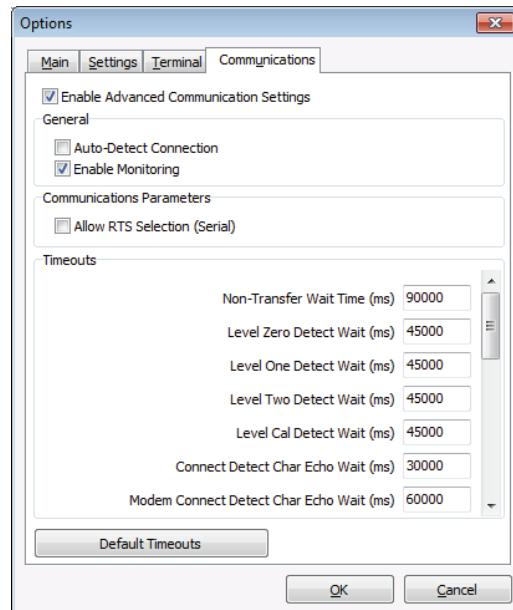


Figure 7.75 Advanced Communication Options Window

Unknown Global Device ID

If you change the Global Device ID (GDID) of an IED in the Connection Directory, and attempt to connect to the IED automatically through QuickSet without first uploading the new Connection Directory to the SEL-3620, you will not be

able to access the new device name from the SEL-3620 proxy. Upload the new Connection Directory first to the SEL-3620 (be careful about this; see *Safety Tips for SEL-3620 Password Management* on page 7.54).

<Ctrl+Q> Termination String \011 Leads to Termination of the Sessions Prematurely

Sometimes QuickSet will send hex character \011 as part of a software hand-shake sequence (XON/XOFF) when reading settings or performing other functions on relays through the SEL-3620 SMP. If the termination sequence for the SMP is set to <Ctrl+Q>, this can lead to premature termination of the session. Ensure the termination string is set to a sequence other than <Ctrl+Q> on the SEL-3620 SMP (e.g., <Ctrl+E> or <Ctrl+W>).

SSH Connection Times Out

In some instances where the SEL-3620 is authenticating to an LDAP server over a slow connection, the SSH authentication session between QuickSet and the SEL-3620 can time out. To lengthen the default QuickSet SSH authentication time-out, navigate to **Tools > Options > Communications** and set **SSH Authentication Timeout (ms)** to a value higher than the default (15 seconds) as shown in *Figure 7.76*.

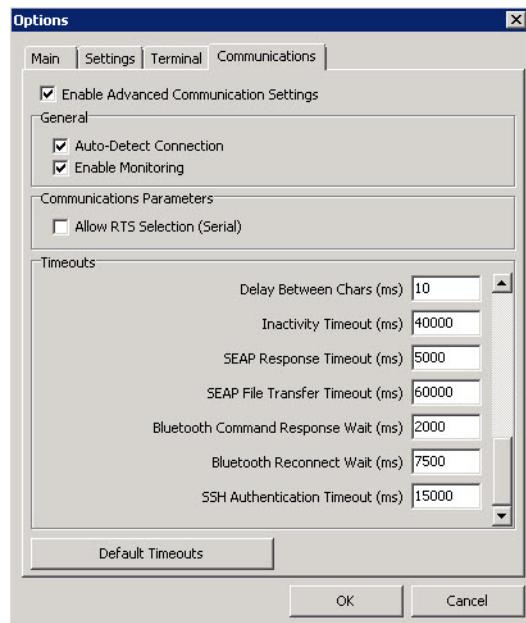


Figure 7.76 SSH Authentication Timeout

Other QuickSet Connection Errors

If you encounter an unknown error in QuickSet when attempting to access an IED from the SEL-3620 proxy, enable monitoring (see *Figure 7.75*) and attempt to connect again. You may view the QuickSet Terminal (see *Figure 7.77*) during the connection process to view the connection attempt. You may send copies of the terminal session log to your local SEL representative if you need help.



Figure 7.77 QuickSet Terminal

Errors Disconnecting From the SEL-3620 Proxy From Device Manager

If you seem unable to disconnect from the SEL-3620 proxy from Device Manager, check the following:

QuickSet Terminal Does Not Allow Sending Control Characters

If the SEL-3620 seems to not respond to a valid termination string, ensure that the QuickSet Terminal allows sending control characters (right-click on the QuickSet Terminal and ensure **Send Ctrl Characters** is selected).

Incorrect or Missing Terminate Script on the SEL-3620

You will need to enable the GENERAL_362X_TERMINATE_SCRIPT on the SEL-3620 from the Connection tab to proxy automatically disconnect from the IED. If you do not have this script enabled, you can still terminate from the IED manually by opening the QuickSet terminal and sending the terminate character (e.g., <Ctrl+W>) to the SEL-3620 manually.

Incorrect or Missing Termination String on the SEL-3620

To automatically disconnect from the IED, you will need to ensure you have a valid Termination String set on the SEL-3620. This string is in hexadecimal, and should match whatever ASCII termination character you are using (e.g., the <Ctrl+W> Termination String would be \017).

Custom Scripts Created by User

Proxy scripts must be Python 3-compliant.

Implementing Password Management

Introduction

This section details the following configuration and testing steps:

- Password management connection directory scripts
- Safety tips for SEL-3620 password management
- Using the Managed Device Passwords report
- Using the Managed Device List
- Generating IED passwords
- Applying IED passwords
- Reverting Passwords
- Assigning Passwords
- Including/Excluding Managed Devices

- Managing Password Persistence
- Checking out managed devices
- Disaster recovery
- Troubleshooting

Password management should only be undertaken when the proxy is working as expected. If you are still encountering errors or are unclear about how the SEL-3620 proxies access to secured IEDs, review the previous sections.

Scenario Configuration

The following scenario shows the current configuration for this section that is used in this example. You may replace the network addresses with your own, depending on your SEL-3620 network settings. The following example uses an SEL-787 relay for testing. You may use your own SEL IED connected to the SEL-3620 via a null-modem serial cable (such as an SEL-C273A). Note that the use of the CAS is optional.

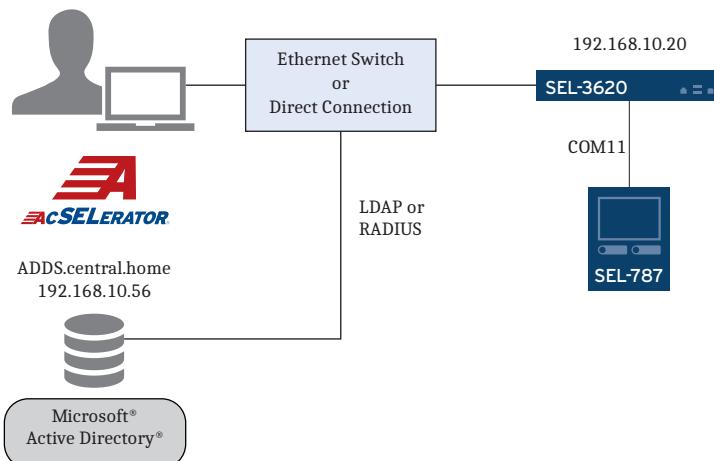


Figure 7.78 Password Management Network Diagram

Password Management Theory of Operation

The SEL-3620 manages IED passwords by using information sent to it in the QuickSet Connection Directory. The SEL-3620 always separates out the steps of Generating new IED passwords and Applying IED passwords. It can generate and apply new passwords to the IED, check out the IED, or revert the IED passwords to their default state in extenuating circumstances (e.g., a natural disaster).

The SEL-3620 can change IED passwords in the following ways:

- **Manually Initiated Password Change:** A user with administrative privileges in the SEL-3620 can manually initiate the following:
 - Password change of any set of managed IEDs
 - Password change for any set of passwords on IEDs
 - Password update to the SEL-3620 database for any set of passwords on IEDs
- **Automatic Password Change:** A user with administrative privileges in the SEL-3620 can configure the Security Gateway to automatically generate and apply passwords for all connected IEDs based on a regular time period (e.g., every 90 days).

- **Manually Initiated Device Check Out/In:** A user with managed device access permissions can manually initiate a device check-out or check-in.
- **Externally Triggered Password Change:** An external software package such as ACCELERATOR TEAM can trigger password changes on a set schedule.

At any one time, the SEL-3620 can store as many as three separate passwords for each IED account level. These passwords are the Initial Password, Current Password, and Proposed Password:

- **Initial Password:** When a QuickSet Connection Directory is first uploaded with at least one IED with a new GDID, the SEL-3620 uses the current password boxes found in that IED as the initial passwords. The SEL-3620 will remember these very first passwords, even after generation and application of multiple new passwords for the IED, or uploads of new Connection Directories with the same GDID. The SEL-3620 can revert to the original Initial Password(s) for each IED. The only way to override an initial password is to upload a Connection Directory twice: once with the specified IED GDID changed or removed, then again with the same IED GDID re-added with the new passwords set in the Connection Directory.
- **Current Password:** This is the current password that the SEL-3620 “knows” to be on the IED (this may be the initial password if the GDID of the device is new). When the SEL-3620 rotates passwords on the IED, the Current Password will be updated.
- **Proposed Password:** The Proposed Password is created when new passwords are generated for the IED. Then, when the passwords are applied, the new Proposed Passwords are entered into each IED. If the password change is successful, the Proposed Password will become the new Current Password.

The diagrams below illustrate how these different password states are used during password management. After a Connection Directory is uploaded with a new GDID, the password management cycle looks similar to *Figure 7.79*.

NOTE: If a QuickSet Connection Directory is not uploaded to the device, the Password Management page of the web UI will not be populated.

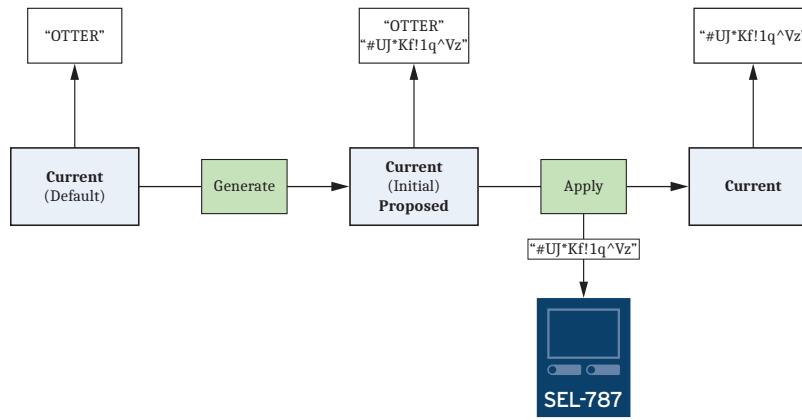
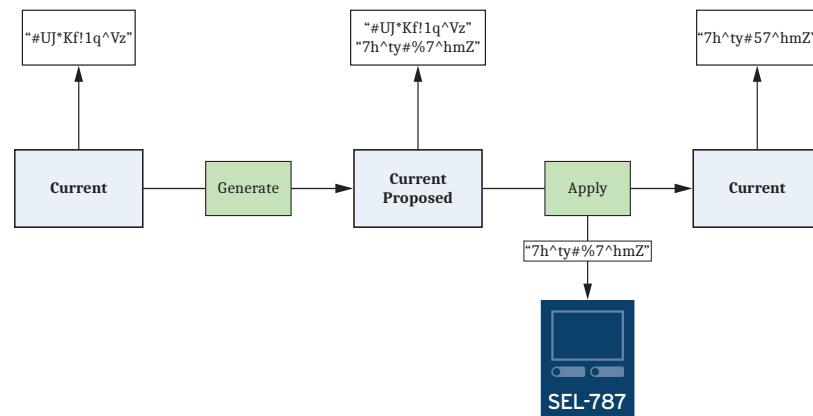
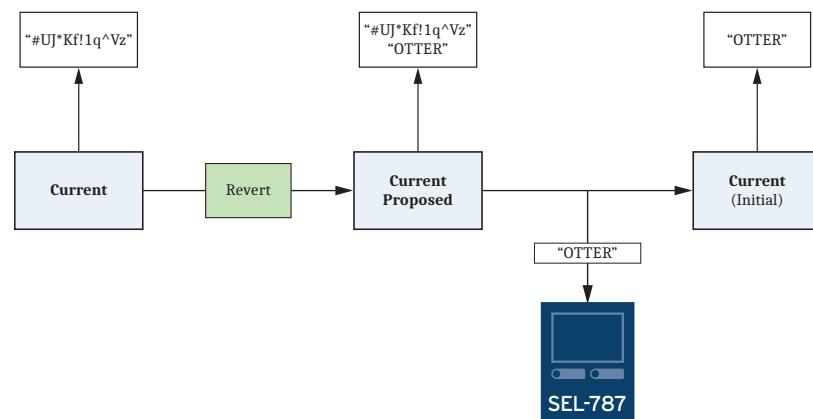


Figure 7.79 Password Management Cycle With New IED

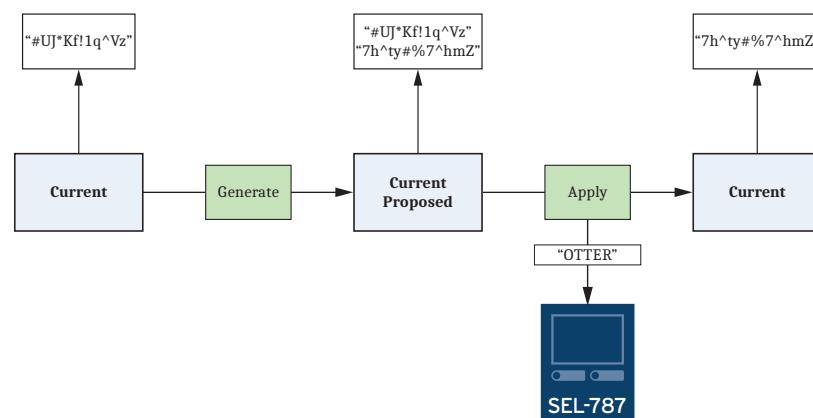
During normal password management after the first application cycle, password management looks similar to *Figure 7.80*.

**Figure 7.80 Normal Password Management Cycle**

In case default passwords must be restored to the IED, the passwords can be reverted, as in *Figure 7.81*.

**Figure 7.81 Revert Password Cycle**

A checked-out device is in a special state where the managed device is using its initial passwords, but the current and proposed passwords in the SEL-3620 database are not changed.

**Figure 7.82 Device Checkout Cycle**

Safety Tips for SEL-3620 Password Management



Read this section before performing ANY password changes with your SEL-3620.

When managing passwords on IEDs, the SEL-3620 Security Gateway keeps copies of both generated passwords and current passwords on devices to prevent loss of password information during extraordinary events (power failure during password changes, etc.). However, an SEL-3620 operator should be aware that there are several user-initiated scenarios during which current IED password information could become desynchronized (the current passwords could become “lost”) on the SEL-3620:

- Changing the Global Device ID of the IED in the Connection Directory, and uploading the Connection Directory to the SEL-3620
- Removing the IED from beneath the SEL-3620 in the Connection Directory, and uploading the Connection Directory to the SEL-3620
- Performing a Factory-Default Reset of an SEL-3620
- Reverting to a previous firmware version after a firmware upgrade, then upgrading from the reverted state (you will get the version of the IED passwords as they were before reverting)
- Updating individual IED passwords in the SEL-3620 database by using the Assign Password function (old Current Password is overwritten)
- Manually editing the SEL-3620 IED password record
- Directly editing passwords of a managed device

Copies of IED passwords are kept in the Managed Device Passwords report found on the SEL-3620. It is highly recommended that the SEL-3620 operators *always* keep a current copy of this report (and its associated JSON file) offline in secure storage for use in case of an extraordinary circumstance. To prevent loss of IED passwords, always use the following safety steps:

- Before any SEL-3620 firmware changes (updates or reverts), generate and download the Managed Device Passwords PDF and JSON report to a secure location.
- Before uploading a System Settings file to the SEL-3620, generate and download the Managed Device Passwords PDF and JSON report to a secure location.
- Before uploading any Connection Directory to the SEL-3620 from QuickSet, generate and download the Managed Device Passwords PDF and JSON report to a secure location.
- Before changing or updating any IED passwords on the SEL-3620, generate and download the Managed Device Passwords PDF and JSON report to a secure location.

Following the preceding safety steps will help prevent the need to physically recover IED passwords.

Password Management Connection Directory Scripts

When performing password management in combination with proxy access, the SEL-3620 requires two additional pieces of information: a Generate Password Script and a Set Password Script for each IED access level. These scripts are found on the **Device** tab of the IED in Device Manager (see *Figure 7.83*).

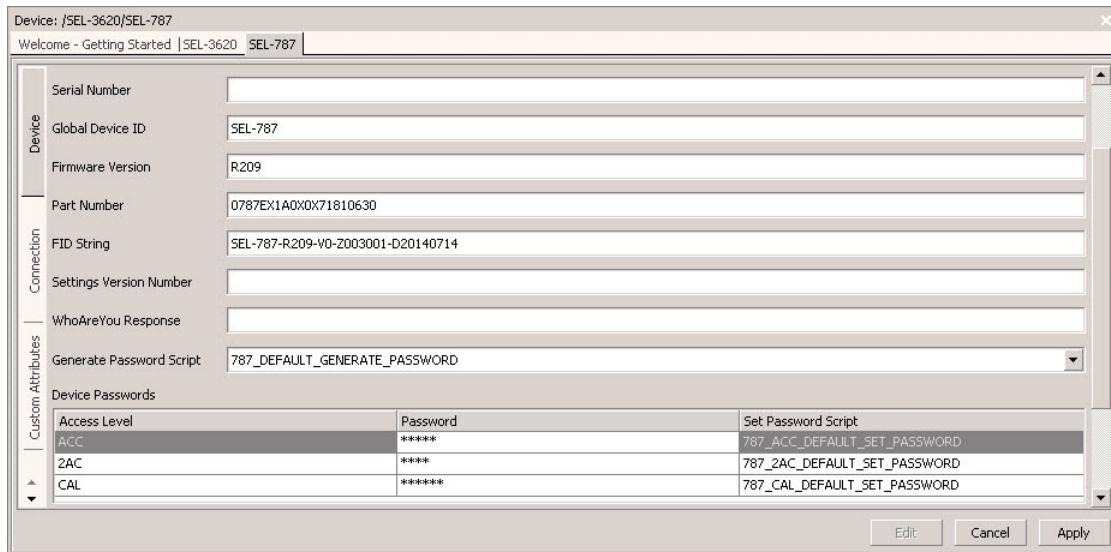


Figure 7.83 Set Password and Generate Password Scripts

Generate Password Script

The Generate Password scripts can be found in Device Manager (**Tools > Device Manager > Scripts**). The following is the 787_DEFAULT_GENERATE_PASSWORD script:

```
SEL.GeneratePassword(12, ['ABCDEFGHIJKLMNPQRSTUVWXYZ', 'abcdefghijklmnopqrstuvwxyz', '0123456789', '!\"#$%&()*,.:/;<=>?@[\\\]^_{|}`'])
```

This script tells the SEL-3620 the length and character types to include in a new, randomly generated password for the IED. In the above script, the SEL-3620 will generate a random 12-character password with at least one or more uppercase alpha character, lowercase alpha character, number, and special character.

The Generate Password script defaults to the allowed password complexity for the latest iteration of the SEL device firmware. Some SEL IEDs support a different password complexity on earlier firmware versions. To reduce the complexity of the Generate Password script, you can right-click the script, and copy it, and then paste and edit it to meet the password requirements of the device.

Set Password Script

The Set Password scripts tell the SEL-3620 how to update the password for a particular account level on the IED. For SEL devices, most relays come with three separate Set Password scripts; ACC_DEFAULT_SET_PASSWORD, 2AC_DEFAULT_SET_PASSWORD, and CAL_DEFAULT_SET_PASSWORD. These scripts can be found in Device Manager (**Tools > Device Manager > Scripts**). The following is the 787_ACC_DEFAULT_SET_PASSWORD script:

```
SEL.SetPassword('ACC', SEL._ProposedPassword(), 'pas',[ 'Changed'],[ 'Invalid'])
```

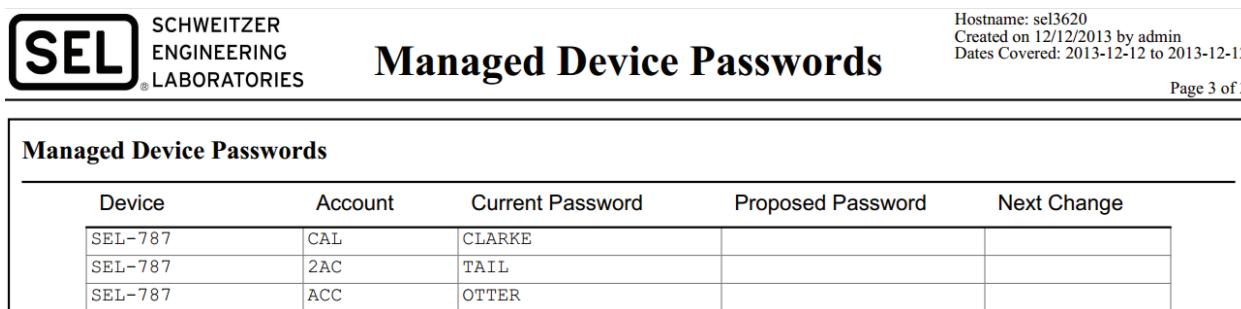
Most of the complexity of the script is abstracted into a Python function call. SEL does not suggest editing these prewritten scripts. However, you could create your own Python script to navigate ASCII prompts and update passwords.

Viewing the Managed Device Passwords Report

The SEL-3620 Managed Device Passwords contains a record of Current Passwords and Proposed Passwords for each IED account. In the SEL-787 example, the account levels are Access Level 1, Access Level 2, and Access Level C. To generate the Managed Device Password Report, perform the following steps:

- Step 1. On the SEL-3620 web interface, in the navigation table under **Reports**, select **Proxy Reports**.
- Step 2. Select **Managed Device Passwords**.
- Step 3. (Optional) Enter and confirm a password to encrypt the Managed Device Passwords report. If the report is encrypted, it will not be readable offline without a method to decrypt and knowledge of the password. For decryption instructions, refer to *SEL-3620 Encrypted Proxy Reports* on page 7.39.
- Step 4. After the report has generated, select the new **Download PDF** button next to the **Managed Device Passwords** option to view the report.

Figure 7.84 shows the default passwords of the IED with no passwords generated.



Managed Device Passwords

Device	Account	Current Password	Proposed Password	Next Change
SEL-787	CAL	CLARKE		
SEL-787	2AC	TAIL		
SEL-787	ACC	OTTER		

Figure 7.84 Default Managed Device Passwords Report

Managed Device List

The Managed Device List, underneath the heading Manual Password Management, on the Password Management webpage, is a list of all the devices that the SEL-3620 is managing. This list is always shown, even when manual password operations are disabled in favor of scheduled password changes. In all cases, this list provides the device names and feedback on the current state of the passwords for each device. The Managed Device List has four columns: Select, Last Operation Status, Device Status, and Global Device ID.

Selection				Action			
	All	Initial Passwords	Included	Excluded	Clear	Select Action	Perform Action
Select	Last Operation Status	Device Status	Global Device ID				
<input type="checkbox"/>			SEL-2030-001				
<input type="checkbox"/>			SEL-421-3-001				
<input type="checkbox"/>			SEL-421-3-002				
<input type="checkbox"/>			SEL-3505-001				
<input type="checkbox"/>			SEL-311C-001				
<input type="checkbox"/>			SEL-351A-001				

Figure 7.85 Managed Device List

The Select column contains check boxes that are only enabled when the SEL-3620 password management is configured to Manual Operation or Check Out Allowed. These check boxes are used to select one or more devices in the list on which to perform an action.

The Last Operation Status column contains icons and mouse-overs to indicate the success or failure of the last password change operation that was attempted on each managed device. The icons you may see in the Last Operation Status column are:

	Indicates the last password change operation was successful.
	Indicates the last password change operation failed.
	Indicates the last password change operation was aborted by a user.

If any icons other than ✓ show in the Last Operation Status column, it means your devices may not be in a desired or secure state and further investigation should be performed.

The Device Status column contains icons to show various states the device or management of the device could be in. The icons you may see in the Device Status column are:

	Indicates the managed device is currently using its initial passwords.
	Indicates proposed passwords exist and have not yet been applied.
	Indicates the device is checked out by a user.
	Indicates the device has passwords set to be persistent.

When you hold your mouse cursor over any icons, a popup should show, indicating what the icon means. This pop-up may not be available on all web browsers.

The device column contains the Global Device IDs of all the managed devices. Indents in this column indicate hierarchy where children devices are indented underneath parent devices. This list is sorted in the following order: numerical, lowercase alphabetical, and uppercase alphabetical. Parent devices are sorted first, then children devices are sorted underneath their parent.

All password operations that are performed on more than one device will be performed in the order devices are shown in this list. While password operations are occurring the Managed Device List can be used to determine operation progress. The icons associated with each device will change as passwords are generated for or applied to each device. Following the progress in the Managed Device List can provide an idea of where in the password operation the SEL-3620 is currently at.

Manual Password Management

Manual Password Management can be enabled by setting Automated Password Management to Manual Operation or Check Out Allowed. Manual operation is useful for user-initiated password changes, and passwords changes triggered by external machines, applications, or scripts.

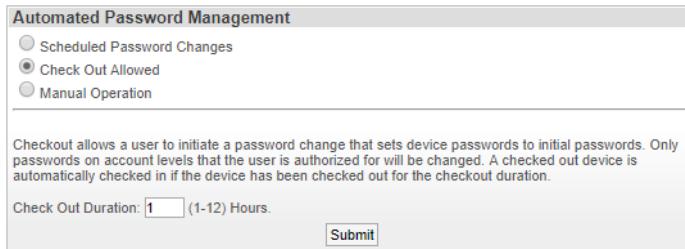


Figure 7.86 Manual Password Management

When the SEL-3620 is configured for manual password management, the commands on the managed device list are enabled. This allows you to select devices to perform actions on, and to perform the desired actions. There are six methods for selecting or clearing devices.

- **Select:** Checks the select box of each managed device you want to select.
- **All Button:** Selects all managed devices.
- **Initial Passwords Button:** Selects all managed devices that are currently using initial passwords.
- **Included Button:** Selects all managed devices that are actively being managed by the SEL-3620.
- **Excluded Button:** Selects all managed devices that currently excluded from management actions.
- Deselect: Clears the select box of each managed device you do not want selected.
- **Clear Button:** Clears the entire selection.

When devices are selected, you can perform actions on them. You can perform actions on any combination of managed devices: one, some or all. The possible actions are:

- **Generate:** Generates new passwords for all accounts of all selected devices.
- **Change Now:** Applies all proposed passwords.
- **Revert:** Changes passwords back to their initial values.
- **Abort:** Aborts the current operation.
- **Include:** Enables management of the device by the SEL-3620. This includes password functions and proxy functions.
- **Exclude:** Disables management of the device by the SEL-3620. Excluded devices will not have any password operations performed on them and are not available for access via the proxy.
- **Assign:** Assigns or applies user-entered password for any accounts common to all selected devices.
- **Manage Persistence:** Locks the passwords on specific managed device accounts so they cannot be changed.
- **Clear Proposed Passwords:** Clears all proposed passwords.

NOTE: The **Change Now** action does not honor the selected devices and will do all proposed passwords.

Generating IED Passwords

To generate a new set of complex passwords for the IED, follow these steps:

Step 1. Under the **Security** section of the navigation panel, select **Password Management**.

Step 2. In the **Automated Password Management** box, ensure that **Manual Operation** or **Check Out Allowed** is selected. Select **Submit** if you change the setting.

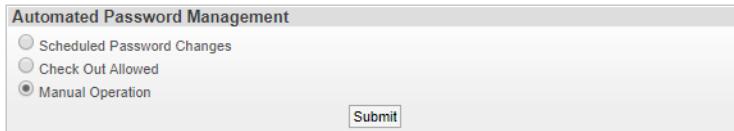


Figure 7.87 Automated Password Management Box

Step 3. In the **Manual Password Management** box, select the managed devices for which you want to generate new passwords. You can do this by selecting individual check boxes or by selecting the **All** or **Initial Passwords** buttons. The **Initial Passwords** button selects all devices currently using their initial passwords.

Selection				Action		
All	Initial Passwords	Included	Excluded	Clear	Select Action	Perform Action
Select	Last Operation Status	Device Status	Global Device ID			
<input checked="" type="checkbox"/>	(1)		SEL-787			

Figure 7.88 Password Management Device Selection

Step 4. Select **Generate** from the **Select Action** dropdown list.

Step 5. Select **Perform Action**.

You should see the message “Password generation in progress” at the top of the page. The page reloads every 5 seconds until the operation is completed. Every update, the message at the top of the page informs you which device is currently having its passwords changed. When all passwords have been generated the message changes to “Passwords generated successfully.” If you get the message “Password generation failed”, then there is likely an error in the password generation scripts.

Navigate to **Proxy Reports** and generate a new Managed Device Passwords report. You should now see the **Proposed Password** column has been filled in with new complex passwords generated for the IED by the SEL-3620 (see *Figure 7.89*).

Managed Device Passwords				
Device	Account	Current Password	Proposed Password	Next Change
SEL-787	CAL	CLARKE	~*[8asZhU>,J	
SEL-787	ACC	OTTER	O]6?!wV_v6jY	
SEL-787	2AC	TAIL	f6C01RH5m?*	

Figure 7.89 Managed Device Passwords Report With Proposed Passwords

Applying IED Passwords

Now that you have generated a new set of complex passwords for the IED, you can instruct the SEL-3620 to apply the new passwords to the IED. To perform this function, follow these steps:

- Step 1. On the **Password Management** page, in the **Manual Password Management** box, select the relevant managed device(s).
- Step 2. Select **Change Now** from the **Select Action** dropdown list.
- Step 3. Select **Perform Action**.

You should see the message “Password change in progress” at the top of the page. The page reloads every 5 seconds until the operation is completed. Every update the message at the top of the page informs you which device is currently having its passwords changed. When you have changed all passwords, the message changes to “Passwords changed successfully.” If you get the message “Password change failed”, then there is at least one password in the operation that was not successfully applied. This could be because of incorrect scripts, incorrect connection settings, down communications channels, or other scenarios.

- Step 4. Navigate to the **Proxy Reports** page, and regenerate the Managed Device Passwords report. On the report, you should now see that the Current Passwords column has changed to what the Proposed Passwords were previously, and the Proposed Passwords column is now empty (see *Figure 7.90*).

Managed Device Passwords				
Device	Account	Current Password	Proposed Password	Next Change
SEL-787	CAL	~*[8asZhU>,J		
SEL-787	ACC	O]6?!wV_v6jY		
SEL-787	2AC	f6C01RH5m?`*		

Figure 7.90 Managed Device Passwords Report With New Complex Passwords

Reverting IED Passwords to Default

Now that you have generated and applied a new set of complex passwords, you can instruct the SEL-3620 to revert the IED to our original set. To perform this function, follow these steps:

- Step 1. On the **Passwords Management** page, select the managed device(s) you would like to revert from the managed device list.
- Step 2. Select **Revert** from the **Select Action** dropdown list and select **Perform Action**.

When the passwords have all been reverted, you will see a new warning banner at the top of the SEL-3620 webpage (see *Figure 7.91*). This banner will only disappear if you do one of the following:

- a. Generate and apply a new set of IED passwords, and ensure that the password change is successful.
- b. Change the Set Password Scripts of the IED in the Connection Directory to **empty**, reupload the Connection Directory to the SEL-3620, and generate and apply passwords again.
- c. Use the **Edit Password** function (see *Assigning Password* on page 7.61) and change the password to what it is currently.
- d. Perform a Factory-Default Reset of the SEL-3620.

WARNING: Managed Devices Using Initial Passwords

Figure 7.91 SEL-3620 Default Passwords Warning Banner

- Step 3. When the passwords have been successfully reverted, navigate to the **Proxy Reports** page, and regenerate the Managed Device Passwords report. On the report, you should now see that the Current Passwords column has changed back to the default set of passwords (see *Figure 7.84*).

Assigning Password

In addition to the functions on the SEL-3620 that allow for managing all passwords on all devices simultaneously, the SEL-3620 also features the ability to set user-entered passwords on IEDs. This function is useful for both changing passwords on managed devices and for updating the database of the password manager with the correct password of the IED (for example, when the IED has been replaced). Both of these actions are available for the following scenarios:

- Changing/updating a single password on a single managed device.
- Changing/updating multiple passwords on a single managed device.
- Changing/updating common passwords between multiple devices.

To assign or update managed device password(s), follow these steps:

- Step 1. Generate and download a Managed Device Passwords report for safekeeping.
- Step 2. Navigate to the **Password Management** webpage on the SEL-3620. At the bottom of the page, in the managed device list, select the IED(s) that you want to assign password(s) to.
- Step 3. Select the **Assign** action from the **Select Action** dropdown list and select **Perform Action**.

Step 4. An **Edit Password(s) For Managed Device(s)** box should now be displayed. Enter and confirm passwords for the account(s) you want to change or update password(s) for.

Step 5. Select **Change password(s) on the managed device(s)** if you want to change the password(s) on the IED(s). Select **Update local copy of password(s) for the managed device(s)** if you want to update the SEL-3620 password list without making any changes to the IED itself. Select **Apply** to perform the action.

Edit Password(s) For Managed Device(s)		
Accounts**:		
2AC	New Password**:	Retype New Password**:
ACC	New Password**: *****	Retype New Password**: *****
CAL	New Password**:	Retype New Password**:

Action Type*:

Change password(s) on the managed device(s)
 Update local copy of password(s) for the managed device(s)

* Required
** One or more passwords must be entered

Apply Cancel

Figure 7.92 Managed Device Password Editing Window

Step 6. After a minute or so, you should see the message “Password change successful” at the top of the page.

Perform *Step 2–Step 4* again to change the single password back to its previous value. If you see a fail message, see *Troubleshooting* on page 7.71.

Aborting a Password Operation

Password operations can take a long time to complete if there are a large number of managed devices and/or slow communications channels. While a password operation is in progress, managed devices are not accessible via the SMP. If there is an immediate need to access a managed device, or a mistake was made in generating or applying passwords, the process can be aborted to gain quick access to the managed device or correct the operation.

To abort a password operation, navigate to the SEL-3620 Password Management webpage with an administrative level user and select **Abort**. This action aborts the current operation and does not need any devices to be selected.

Including and Excluding Managed Devices

By default, when a connection directory is uploaded, all devices are included in the management scheme. This means that they can have passwords generated and applied. It also means they are accessible to users via the SEL-3620 SMP. The SEL-3620 has the option to exclude a device from the management scheme. An excluded device still exists in the SEL-3620 database, but no operations are performed on it, and users cannot access it via the SMP. This prevents users from accidentally accessing a device that has not yet been configured. It also prevents script time-outs and error messages on managed devices that are known to be offline.

There are two primary reasons to exclude devices. One is that a user knows ahead of time that many devices will be managed by the SEL-3620. To simplify commissioning, all managed devices are added to the SEL-3620 connection directory at commissioning, even if they do not yet exist in the installation. The unavailable

devices can then be excluded from device management until they have been added to the installation. The second reason for device exclusion is that an environment might be very dynamic, where devices regularly go offline and come online.

Perform the following steps to exclude devices:

- Step 1. Navigate to the SEL-3620 Password Management page.
- Step 2. Select the devices in the managed device list that you want to exclude.
- Step 3. Select **Exclude** from the **Select Action** dropdown list and select **Perform Action**.

The excluded devices will appear in the list with their rows grayed out, will not be accessible via the SMP to users, and will not have passwords generated or changed for them.

Perform the following steps to include devices:

- Step 1. Navigate to the SEL-3620 Password Management page.
- Step 2. Select the excluded devices in the managed device list you want to include.
- Step 3. Select **Include** from the **Select Action** dropdown list and select **Perform Action**.

The selected devices will re-activate for full device management.

Excluded devices are selectable in the Managed Device List, however the only action that can be performed on them is to Include them. All other actions will generate an error message at the top of the Password Management Web Page.

If a parent device, such as an SEL-2032 Communications Processor, is excluded, all of its children devices will automatically be excluded as well.

Managing Password Persistence

Managed device passwords can be marked as persistent, meaning they will not change. The only way to change a password that is marked persistent is to remove the persistence and then change the password.

There are two use cases for persistence. One is to protect passwords from accidental change. If the SEL-3620 is managing specific devices/accounts that do not have a requirement to be changed periodically, it is recommended to mark those devices/accounts as persistent to prevent a user from accidentally changing them. This can help prevent both users and automated tasks from being locked out of devices to which they should have direct access.

The second case is to set common passwords. This case also relies on the previously mentioned Assign action. It is desirable at some installations to set a common password among all devices at Access Level 1. This password can then be provided to technicians and scripts for direct read access to managed devices. At the same time, the rest of the passwords at the installation are required to be periodically set to random values. By assigning a common password to all devices at Access Level 1, and then marking those passwords as persistent, the SEL-3620 can maximize ease of use for relay technicians while still maintaining a high level of password security.

Perform the following steps to mark password(s) as persistent:

- Step 1. Navigate to the SEL-3620 Password Management page.
- Step 2. Select the devices in the managed device list that you want to have password(s) marked persistent.

- Step 3. Select **Manage Persistence** from the **Select Action** dropdown list and select **Perform Action**. This brings up the Edit Persistence for Managed Device(s) form on the right side of the page, as shown in *Figure 7.93*.

Edit Persistence For Managed Device(s)		
Common Account Level(s)		
Select	Deselect	Level(s)
<input type="checkbox"/>	<input type="checkbox"/>	2AC
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ACC
<input type="checkbox"/>	<input type="checkbox"/>	BAC
<input type="checkbox"/>	<input type="checkbox"/>	CAL
<input type="checkbox"/>	<input type="checkbox"/>	All
Device		Persistent
SEL-421-3-001		<input type="checkbox"/> 2AC <input type="checkbox"/> AAC <input checked="" type="checkbox"/> ACC <input checked="" type="checkbox"/> BAC <input type="checkbox"/> CAL <input type="checkbox"/> OAC <input type="checkbox"/> PAC
SEL-421-3-002		
SEL-311C-001		
SEL-351A-001		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Figure 7.93 Edit Persistence Form

- Step 4. If you want to mark common access levels as persistent, select the desired common access levels from the top half of the form. This will select those access levels for all of the selected devices. If there is a mix of access levels to be marked, select each device/access level in the list on the bottom half of the form.

The top half of the form is marked Common Account Level(s). Only account levels shown in the Edit Persistence form are those that are common to all selected devices. If the selected devices do not all have the same access levels, then the non-overlapping access levels will not be shown. To mark non-overlapping access levels as persistent, select those access levels from each desired device in the bottom half of the form.

- Step 5. Select **Apply**. The page reloads with the Managed Device List showing the icon indicating that persistence is set on those devices.

Perform the following steps to remove persistence from password(s):

- Step 1. Navigate to the SEL-3620 Password Management page.
- Step 2. Select the devices in the managed device list from which you want to remove persistence.
- Step 3. Select **Manage Persistence** from the **Select Action** dropdown list and select **Perform Action**. This brings up the Edit Persistence for Managed Device(s) form on the right side of the page.
- Step 4. Clear the desired access levels to remove persistence.
- Step 5. Select **Apply**.

When passwords are marked persistent, the Managed Device Passwords report reflects the persistence in the Next Scheduled Change column. See *Figure 7.94*.



SCHWEITZER
ENGINEERING
LABORATORIES

Managed Device Passwords

Hostname: sel3620
Created on 28/04/2018 by admin

Page 4 of 5

Managed Device Passwords				
Device	Account	Current Password	Proposed Password	Next Change
SEL-2030-001	ZAC	TAIL		
SEL-2030-001	ACC	klab.1		PERSISTENT
SEL-2030-001	CAL	CLARKE		

Figure 7.94 Persistence Report

Clearing Proposed Passwords

When the SEL-3620 is requested to apply proposed password either by automated script or by user request, it changes the passwords for all managed devices/accounts that have proposed passwords, as long as they are not marked persistent, and not excluded. If there are devices that have proposed passwords that you do not want to change, you will need to first clear their proposed passwords.

Perform the following steps to clear proposed passwords:

- Step 1. Select the managed devices that have proposed passwords that you want to clear.
- Step 2. Select **Clear Proposed Passwords** from the **Select Action** dropdown list.
- Step 3. Select **Perform Action**.

Password Change Scheduler

The SEL-3620 Password Change Scheduler will automatically perform the password generation and password application at user-defined intervals (e.g., every 60 days). The password scheduler is useful in scenarios where yearly (or shorter intervals) password changes are required for compliance purposes, and an administrative user does not want to manually perform the process.

The Password Change Scheduler has an offset between the generation cycle and application cycle so a user can download the Managed Device Passwords report. Follow the next steps to configure the Password Change Scheduler to generate new passwords every 60 days at 3:00 a.m., and change the passwords 48 hours (two days) after generation:

NOTE: While the Password Change Scheduler is enabled, you will not be able to manually generate or apply passwords. You may consider disabling the scheduler while following the remainder of this guide.

- Step 1. Navigate to the SEL-3620 **Password Management** page. You will see the Password Change Scheduler group.
- Step 2. Select **Scheduled Password Changes** in the Automated Password Management box. In the Generate managed device passwords every box, enter **60**. In the (1-365) days on hour box, enter **3**. In the Change managed device passwords box, enter **48** (see *Figure 7.95*).

Figure 7.95 Password Change Scheduler Options

Step 3. Select **Submit**. You should now see “Managed device password scheduler enabled successfully” and “Managed device password scheduler data updated successfully” messages. The **Next Scheduled Password Change** box will also show dates for the next generation and application cycles (see *Figure 7.96*).



Figure 7.96 Next Scheduled Password Change Box

Step 4. Navigate to the **Proxy Reports** page, and generate a current Managed Device Passwords report. When generated, the report should now show the **Next Change** column has been configured with the scheduled password change date (see *Figure 7.97*).

Managed Device Passwords				
Device	Account	Current Password	Proposed Password	Next Change
SEL-787	ACC	OTTER		2014-03-18 03:00:00
SEL-787	CAL	CLARKE		2014-03-18 03:00:00
SEL-787	2AC	TAIL		2014-03-18 03:00:00

Figure 7.97 Managed Device Passwords Report With Next Change Date

You may also choose to use TEAM to provide automated password changes and proxy report downloads. For more information about TEAM software, see *General Considerations for SEL-3620 and TEAM Software Interaction* on page 7.128.

Managed Device Check Out

Device check-out provides a method for users to directly access IEDs using the IEDs’ initial passwords. This is useful when direct access to a specific IED is preferred and sometimes even necessary. It allows a privileged user direct IED access without the need to type in a complex password, without compromising the security of the password list, and without rolling the managed site to a nonse-

cure state. This feature is useful for users who want direct access to an IED so they can be sure they are collecting the correct event data. Another purpose is to simplify direct connection of test equipment to managed devices.

When a managed device is checked out, the SEL-3620 sets the IED passwords back to their initial values. The SEL-3620 sets all access levels for which the user has access permission back to their initial values. For example, consider a user with access permission for Access Level 1 on an SEL-787. The user does not have permission to access Access Level 2 or Access Level C. If the user requests a check-out of the SEL-787, the SEL-3620 sets the SEL-787 Access Level 1 password to the initial value configured in QuickSet. The Access Level 2 and Access Level C passwords are not changed.

The SEL-3620 stores the secure passwords for all checked-out devices and access levels. Upon check in, those secure passwords are restored. This prevents the need to generate and download Managed Device Passwords reports before, during, and after every check-out. Upon check in, the passwords of the managed device are restored to the state they were in prior to the check-out.

Device check-out has a configurable automatic checkout timer. When this timer expires, the SEL-3620 automatically checks the managed device in. This check-out timer is configurable by administrative level users of the system and can be set from 1 to 12 hours.

Device check-in can only be performed on devices that have been checked out. Device check-in can only be performed by the user that checked a device out or the automatic checkout timer expiration. A device that is checked out cannot be accessed via the scripted master port.

Device check-outs are disabled by default and must be enabled from the SEL-3620 web interface. To enable device check-outs, follow these steps:

- Step 1. Log in to the SEL-3620 web interface with an Administrative level user.
- Step 2. Navigate to the **Password Management** webpage.
- Step 3. In the **Automated Password Management** box, select **Check Out Allowed**.
- Step 4. Set the **Check Out Duration**.
- Step 5. Select **Submit**.

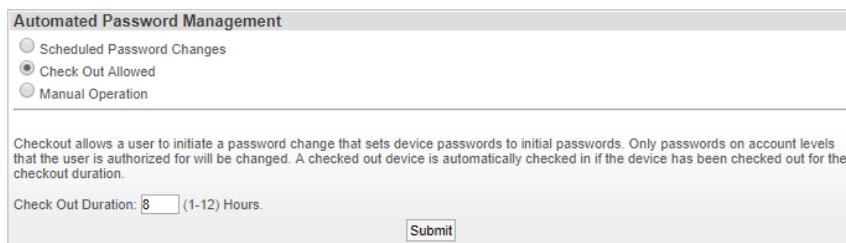


Figure 7.98 Check Out Allowed

Device check-outs can only be performed from the scripted master port. To check out a device, follow these steps:

- Step 1. Log in to the scripted master port command-line interface of the SEL-3620 with a user that has permission to access the IED.
- Step 2. Issue the command **CHECK OUT device_id**, where *device_id* is the device GGUID or the index of the device as provided by the **WHO** command.

You will receive a message that the checkout has been requested, a success or failure message, and the list of access levels and associated initial passwords that have been set.

```
*WHO
Available Devices:
1 SEL-787

*CHE OUT 1

Checking device out.

Level Password
ACC OTTER

Device check out successful.

* [green square icon]
```

Figure 7.99 Device Check Out

To check in a device, follow these steps:

- Step 1. Log in to the scripted master port with the same user that checked the device out.
- Step 2. Issue the command **CHECK IN *device_id*** where *device_id* is the device GGUID or the index of the device as provided by the **WHO** command.

You will receive a device check-in success or failure message when the operation is complete.

The SEL-3620 SELF Controller

The SEL-3620 features a limited command-line interface (CLI) that allows users to perform some password management functions from a terminal. This interface is called the SELF Controller and can be accessed by any user that has administrative privileges on the SEL-3620.

The SELF controller is accessed by logging in to the Scripting-Enabled Proxy Port and using the **SEL SELF** command (see *Figure 7.100*). See *Table 7.3* for a list of available commands from the SELF controller.

Table 7.3 SELF Controller Menu Options

Command	Parameters	Description
HELP	None	Displays a list of commands available on the SELF controller.
PWGENERATE	None	Generates passwords that you can apply to managed devices. This command is unavailable when the password change schedule is enabled.
PWAPPLY	None	Apply generated passwords to managed devices. This command is unavailable if there are no proposed passwords or when the password change scheduler is enabled.
PWREVERT	None	Revert managed devices to default passwords. This command is unavailable if the SEL-3620 is already showing that managed devices are using initial passwords.
GENERATE	<report type> <begin date> <end date> dd/mm/yyyy	Generate the given report type. Report types are COMMANDS_AND_DEVICES, PASSWORD_UPDATES, and MANAGED_DEVICE_PASSWORDS. The begin and end dates are in DD/MM/YYYY format.
FILE DIR	None	Displays the reports available for download.
FILE READ	File name	Initiates a YMODEM transfer on the file name.
EXIT	None	Exits the SELF controller to the normal master port menu.

To perform password management functions from the SELF Controller, perform the following steps:

- Step 1. Log in to the Scripting-Enabled Proxy Port that was created in the previous section.
- Step 2. After successfully logging in, type **SEL SELF** from the interface. Typing **HELP** will show you a number of new options (see *Figure 7.100*).

```
*SEL SELF

*HELP
    PWGenerate
        - Generate passwords for each account on each protected device.
    PWApply
        - Apply generated passwords to the protected device accounts.
    PWRevert
        - Revert the passwords of all protected device accounts back to their
          initial values as defined in the connection directory.
          This command will place the device in emergency mode.
    GENerate <report type> <begin date> <end date>
        - Generate <report type> report with the specified date range.
        Valid report types are COMMANDS_AND_DEVICES, PASSWORD_UPDATES,
        and MANAGED_DEVICE_PASSWORDS. The date range format is DD/MM/YYYY.
    FILE DIR - List the available reports.
    FILE READ <filename>
        - Initiate file transfer of <filename>.
    EXIT      - Return to the master port connection menu.
    HELp      - Display help information.

*
```

Figure 7.100 SELF Controller

- Step 3. If your terminal has YMODEM capabilities, you can generate and download the Managed Device Passwords report (recommended). Generate this report by entering the following command:
GEN MANAGED_DEVICE_PASSWORDS 16/01/2014 16/01/2014 (replace the beginning and end dates with your own). Note that the date format is DD/MM/YYYY.
- Step 4. Download the Managed Device Passwords report with the following commands: **FILE READ managed_device_passwords.pdf** and **FILE READ managed_device_passwords.json** (see *Figure 7.101*).

```
*GEN_MANAGED_DEVICE_PASSWORDS 16/01/2014 16/01/2014
                                Command Executed

*FILE READ managed_device_passwords.pdf
#000 Ready to send file
#001 Transfer Complete

*FILE READ managed_device_passwords.json
#000 Ready to send file
#001 Transfer Complete

*
```

Figure 7.101 Generating and Downloading Reports From SELF Controller

- Step 5. To generate a new set of complex passwords, type **PWG**. Note that the terminal will not respond to any input until the password generation is complete.
- Step 6. Generate and download the Managed Device Passwords reports (recommended).
- Step 7. To apply the new passwords to the managed IEDs, type **PWA**. When the password change is complete, the terminal will respond with the message **Passwords of the managed devices have been changed** (see *Figure 7.102*).

```
*pwg
Generating passwords. This process could take several minutes. The terminal
will not respond until script execution has completed.

*
*pwa
Applying new passwords. This process could take several minutes. The terminal
will not respond until script execution has completed.

*
Passwords of managed devices have been changed. New passwords can be found in the
Managed Device Passwords reports.
```

Figure 7.102 Generating and Applying Passwords

Step 8. Generate and download the Managed Device Passwords reports (recommended).

The SELF Controller makes it easier to create scripts to automatically handle the password management capabilities of the SEL-3620 using common scripting methods through Python, Tera Term, and others. For more about the automated password management solution using TEAM, see *General Considerations for SEL-3620 and TEAM Software Interaction* on page 7.128.

Password Change FAQ

Can I turn off password changes for specific levels (e.g., Access Level 1)?

Yes, you can turn off password changes for specific levels from the QuickSet Connection Directory. To turn off password changes for Access Level C, navigate to the **Device** tab for the specific device in Device Manager, and change the **Set Password** script to <Empty>, then reupload the Connection Directory (see *Figure 7.103*).

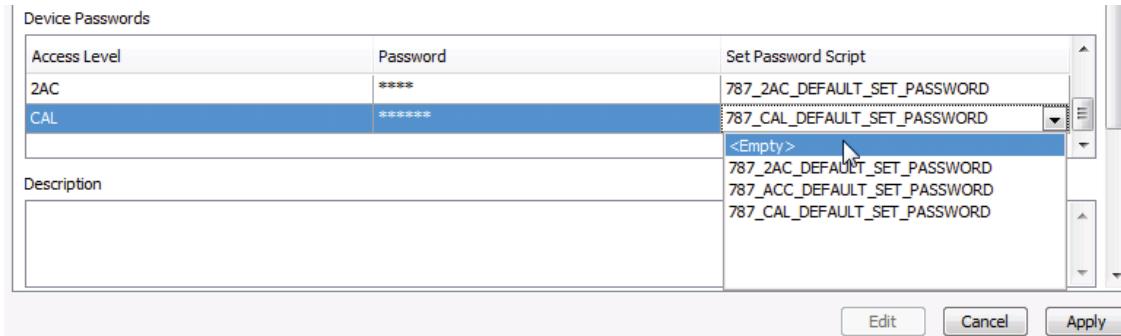


Figure 7.103 Empty Set Password Script

Note that this SEL-3620 will still generate new passwords for the specific IED level. However, during a password apply cycle, the proposed password will never be entered into the device.

Can I make all passwords the same on all devices?

Yes, you can modify the Generate Password script for the specific IED in the Connection Directory to generate the same password for all access levels. Simply create a new Generate Password script and add the following contents:

```
SEL.Return('<xml><Method>PASSWORD</Method></xml>')
```

Simply replace `PASSWORD` in the above statement to what you want the password to be, and configure the IED to use your new Generate Password script. Note that there is no way at this time to have unique per-level Generate Password scripts.

Will SCADA notice when the SEL-3620 performs password changes?

Most SEL IEDs will trigger their physical alarm contacts during the following events:

- When a privileges access level is reached (Access Level 2, Access Level C)
- When a setting is written to the relay

If you have tied the SEL IED alarm contacts to SCADA points, you will see many SEL IED alarm contact triggers when the SEL-3620 changes passwords for IEDs. You should warn SCADA operators or control personnel before changing passwords to prevent confusion.

Do password updates disable protection on SEL IEDs?

Writing new settings to static memory on SEL IEDs may temporarily disable protection for a number of milliseconds. While the risk of a protection event happening during this time is extraordinarily low, be advised of the risk.

Disaster Recovery

For detailed information about disaster recovery of an SEL-3620, see *Appendix C: Best Practices for Emergency Readiness*. For the best disaster recovery readiness, always follow these guidelines:

- Maintain a current SEL-3620 System Settings file. The Single File Backup process combines the connection directory, passwords, and configuration files into a single encrypted file to simplify backup and restoration.
- Execute the **HASH** command immediately after performing a single-file backup and save the response in a safe and accessible location. Use the **HASH** command after restoration to determine if the previous settings were correctly restored.
- Maintain a backup copy of your QuickSet Connection Directory.
- Always have a current version of both the PDF and JSON versions of the Managed Device Passwords report. If you do not use a single-file backup, you may use an automated script from SEL to restore Managed Device Passwords back into a backup SEL-3620. For this script, see *Reloading Managed Device Passwords From an Exported JSON File* (SEL Application Guide AG2014-06).

Following these guidelines will ensure the fastest recovery from any unexpected event.

Troubleshooting

General Tips for Maximizing the Reliability of Your IED Password Management

- After uploading any new Connection Directory into the SEL-3620 and before changing IED passwords, always verify your devices and that all levels are reachable from the SMP. This will find most configuration or device errors before a password change occurs.

- Always save a PDF and JSON copy of the Managed Device Passwords report before and after every password change.
- Check both the SEL-3620 System Logs (Syslogs) and the Managed Device Password report if you have an issue, and follow the troubleshooting steps included here. If the normal troubleshooting steps do not alleviate the problem, contact your local SEL representative.

Password Change Attempt Quickly Fails on Serial IEDs

If your password change attempt fails quickly, check the Pass Through Port setting on the serial IEDs in the Device Manager and ensure none are set to 0.

“ERROR: User(s) logged into managed device(s)” Message After Attempting to Change Passwords

If you receive the “ERROR: User(s) logged into managed device(s)” message, then you probably have an open connection to the SMP. All active sessions to IEDs from the SMP must be disconnected before attempting to change passwords.

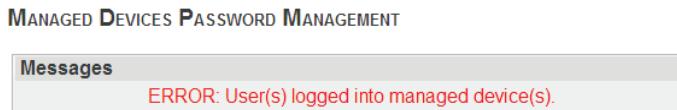


Figure 7.104 SMP Busy Error

“Password change failed” Message After Attempting to Change Passwords

There are a number of reasons why the SEL-3620 can fail during a password change operation. The following is a list of the possible reasons.

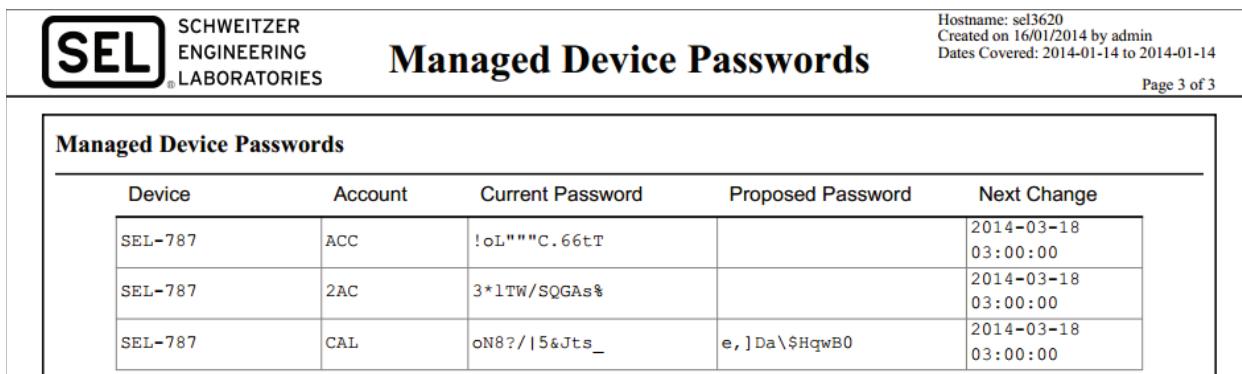
The Proposed Password for the IED Is Too Long or Contains Unsupported Characters

Many legacy SEL devices only support passwords with a maximum six character length, uppercase/lowercase alpha, numbers, and two special characters: dot (.) and dash (-). Some legacy devices will only support the dot character as the special character. However, the device templates in Device Manager by default contain the Password Generate scripts for the very latest firmware.

This problem typically manifests itself if the SEL-3620 System Logs show that all the password changes failed for the particular IED. To solve this issue, navigate to the IED template within Device Manager, and change its Generate Password Script box to GENERAL_GENERATE_PASSWORD. This script contains the minimum character set supported by SEL IEDs. Reupload the Connection Directory, generate a set of fresh passwords, and attempt the apply process again.

Access Level C Failed to Change

When you look at the Managed Device Passwords report after a failed password change attempt, you may notice that the Access Level C password failed to change (see *Figure 7.105*).



The screenshot shows a report titled "Managed Device Passwords". At the top right, it displays the hostname "sel3620", creation date "Created on 16/01/2014 by admin", and the date range "Dates Covered: 2014-01-14 to 2014-01-14". Below this, it says "Page 3 of 3". The main table has columns: Device, Account, Current Password, Proposed Password, and Next Change. The data is as follows:

Device	Account	Current Password	Proposed Password	Next Change
SEL-787	ACC	!oL""C.66tT		2014-03-18 03:00:00
SEL-787	2AC	3*1TW/SQGAs%		2014-03-18 03:00:00
SEL-787	CAL	oN8?/ 5&Jts_	e,]Da\\$HqwB0	2014-03-18 03:00:00

Figure 7.105 Failed Access Level C Password Change

To solve this issue, check the MAXACC settings of the IED to which you are attempting to change passwords. MAXACC should be set to **C** if possible. On some SEL IEDs, Access Level C can only be accessed from the front serial port. If this is the case, and the front serial port cannot be used, the only solution is to turn off the Access Level C password change script for the IED in Device Manager by setting the **Set Password Script** to <Empty>.

Current Password Is Incorrect

The password change may process when there is a difference between what the SEL-3620 “thinks” to be the password on the IED, and what the password actually is. You can verify this situation by logging in to the SEL-3620 proxy and attempting to access the level in question (if there is a difference, the SEL-3620 should warn of an incorrect password). To alleviate this issue, check the following:

- If passwords on the IED are default, ensure that you are using the correct default password. See the particular IED product manual for details.
- If there is a mismatch in passwords, update the internal copy of the password of the SEL-3620 by using the **Manual Password Update** function (see *Assigning Password* on page 7.61).
- If there is a password mismatch because of an error during password change, use the saved Managed Device Passwords report to correct the issue.

IED Device Template in Device Manager Is Incorrect

A password change error may be induced by using an incorrect template in the QuickSet Device Manager. Make sure you are using the correct template for your IED (e.g., an SEL-451 template for an SEL-451).

Lack of Hardware Flow Control on Serial Links (RTS/CTS)

If possible, always use hardware flow control (RTS/CTS) on IEDs connected via serial links. This will ensure the highest possible reliability of the serial data stream. This is especially true when using IEDs connected to SEL Communications Processors (SEL-2020, SEL-2030, and SEL-2032).

Use of Front Serial Ports on Legacy Relays

The front serial ports of some SEL legacy relays are not designed to be used at any speed faster than a human being can type. In these cases, the front serial ports can only be used accurately at speeds as fast as 4800 bps. Choosing a serial speed

faster than 4800 bps on the front serial ports of these relays (e.g., an older SEL-321 relay) will cause errors during attempted password changes by the SEL-3620.

Password Changes on Very Slow Links or Links With High Latency

Attempts to change passwords on IEDs over serial connections of less than 1200 bps can cause failures during password changes. Likewise, password changes attempted over high-latency or very jittery communications links can also cause failures during password changes. Check your communications links, replace the link with a more reliable/faster one, or consider moving the SEL-3620 to the same physical location as the device that it is managing.

Password Change Script Is Bad

If you have edited or created your own Password Set script in Device Manager, check the script for errors. Send the script to your local SEL representative if you have syntax questions.

Communications Cable Is Disconnected or Loose

If any communication cables are disconnected or loose, this will also cause password changes to fail. Verify your connection directory before attempting password changes.

Password Change Log

To assist with troubleshooting password application failures, a Password Change Log can be generated from the Proxy Reports webpage. The Password Change Log is a JSON file that can be generated and downloaded by an Administrative level user of the system. The Password Change Log contains all communications between the SEL-3620 and the managed devices that were a part of the last password change operation. When used with the SEL-3620 generated Syslog messages, this report can help pinpoint the cause of password application failures. This report contains the passwords used to access the managed devices and the passwords the managed devices were changed to, so it should be protected as sensitive information.

Management of Ethernet-Connected IEDs

Introduction

This section details the following configuration and testing steps:

- General considerations for Ethernet IED support
- Device Manager configuration for Ethernet devices
- Proxy configuration and use for Ethernet devices
- Password management for Ethernet devices
- Troubleshooting

Password management should *only* be undertaken when the proxy is working as expected. If you are still encountering errors or are unclear about how the SEL-3620 manages IEDs, see *Troubleshooting* on page 7.71.

Assumptions for this section include the following:

- You are using the SSH SMP created in a previous section.
- You have QuickSet installed and operational.

Scenario Configuration

NOTE: For additional security, implement the Ethernet IED on a different subnet (e.g., 192.168.100.x) from your WAN or test network. This allows you to take full advantage of the firewall capabilities of the SEL-3620. The example above (Using the SEL-3620 Proxy Services on page 7.26, where the IED and Engineering Access segments are on the same network) is for learning/laboratory purposes only.

The following shows the present configuration used in the following example. You may replace the network addresses with your own, depending on your SEL-3620 network settings. The following example uses an Ethernet-enabled SEL-787 relay (used in previous sections). You may use your own SEL IED if desired. Note that the use of the CAS is optional.

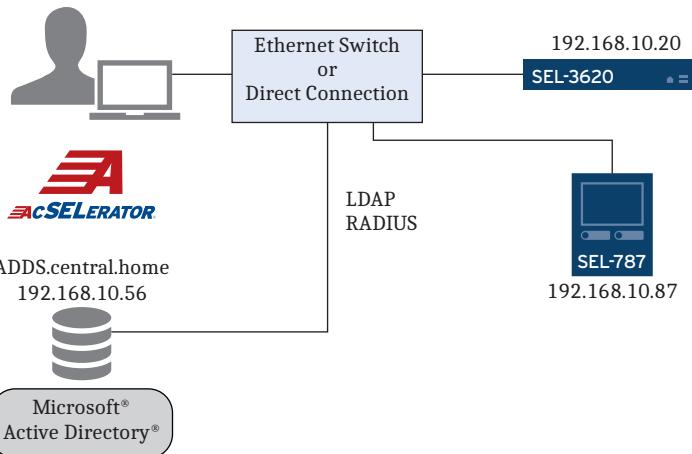


Figure 7.106 Password Management Over Ethernet Network Diagram

General Considerations for SEL-3620 Ethernet IED Support

Configuring and implementing SEL-3620 password management and proxy services for Ethernet-enabled IEDs are very similar to that of serial devices. There are three ways to transfer settings to SEL IEDs over Ethernet: YMODEM, ASCII, and FTP. Prior to firmware revision R138, the SEL-3620 could only proxy transfer settings files over ASCII or YMODEM.

As of R139 and later firmware revisions, the SEL-3620 has implemented support for FTP proxying sessions for settings and event report transfers. Where FTP proxying is in use, the SEL-3620 will use multiple TCP ports for proxying ports to the managed IEDs: one TCP port (SSH/Telnet/Raw TCP) for the primary SMP for terminal access to the IEDs, and an additional dedicated TCP port for each IED that uses FTP (see *Figure 7.107*). The dedicated FTP proxy port for each FTP-enabled IED is required because FTP ports cannot be multiplexed, unlike terminal access for the IEDs.

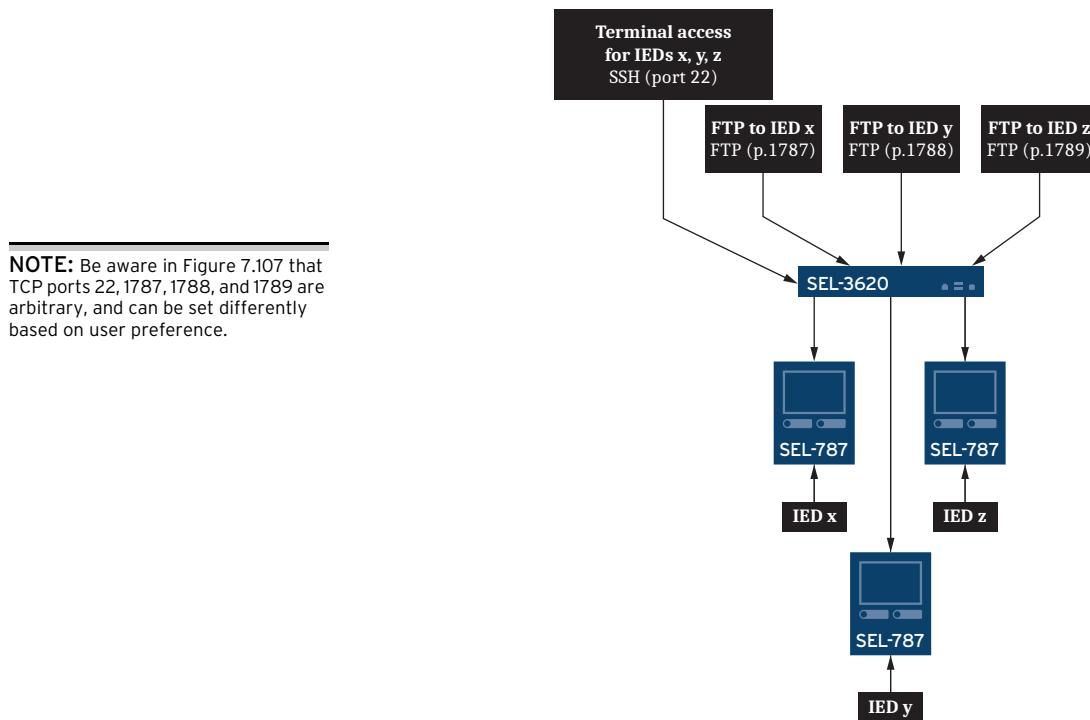


Figure 7.107 SEL-3620 SMP and FTP Proxy Ports

The SEL-3620 FTP proxy is capable of both active and passive FTP data transfer modes. Reference the manuals of your IED for their specific requirements.

Device Manager Configuration of Ethernet IEDs

This section will guide the user through configuring an Ethernet-enabled IED in the QuickSet Device Manager. To do this, perform the following steps:

- Step 1. In the **Connection Explorer** window, right-click on **SEL-3620**, and select **Add > Device**. Scroll down to the bottom of the **Select Device Type** window, and choose **SEL-787**.
- Step 2. Expand the SEL-787 device by double-clicking the template. Open the **Device** tab.
- Step 3. Select **Edit** and change the **Global Device ID** (GDID) so that it matches the **Device Name**.
- Step 4. If the SEL IED passwords are currently set to default values (**OTTER**, **TAIL**, etc.), then go to the next step. Otherwise, enter the current level (Access Level 1, Access Level 2, Access Level C, etc.) passwords into the **Device Passwords** boxes.
- Step 5. Under the **Connection** tab, change the **Connection Type** to **Network** and the **File Transfer Option** to **FTP**.
- Step 6. You should now see a number of new options available. Fill them in according to *Figure 7.108*.

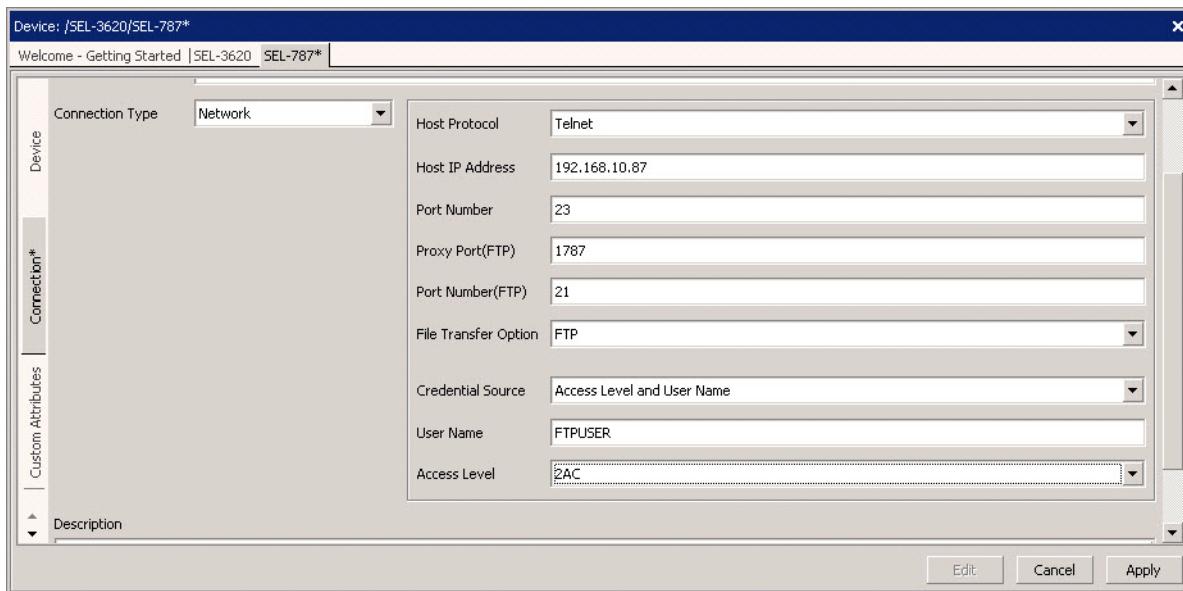


Figure 7.108 Ethernet-Connected IED Connection Tab

An explanation of some of the options are as follows:

- **Host Protocol:** The protocol that the end device is using for engineering access. This will always be Telnet for SEL IEDs, unless you are accessing the IED through a port server.
- **Port Number:** This is the port number used in conjunction with the Host Protocol. This will usually be 23 for SEL IEDs, unless you are accessing the IED through a port server.
- **Proxy Port(FTP):** This is the TCP port of the SEL-3620 FTP proxy for the particular IED. Use a port number that will not conflict with any other open port on the SEL-3620, and does not conflict with any other FTP Proxy Port of any other managed IED.
- **Port Number(FTP):** This is the TCP port of the FTP implementation on the IED. This is usually port 21 for SEL IEDs.
- **File Transfer Option:** For SEL IEDs, this will almost always be either Telnet (for YMODEM over Telnet) or FTP, unless you are accessing the IED through a port server.
- **Credential Source:** This must be set to Access Level and User Name if you are using the SEL-3620 to proxy FTP requests to the SEL-3620.
- **User Name:** For SEL IEDs, the FTP username is typically 'FTPUSER'. However, the username might also be "2AC," "anonymous," or another custom name. You can find the FTP username setting from the interface of the IED or the product manual.
- **Access Level:** Most SEL IEDs associate FTP access with Access Level 2. However, on some SEL IEDs (e.g., SEL-2032) the access level for FTP access is settable. Check with your device terminal or product manual for information about the access level FTP is associated with. The SEL-3620 uses this box to know what managed password to send to the IED when proxying the FTP connection.

Step 7. You may leave the other settings in the **Connection** tab with the default values.

Step 8. Under the **Permissions** tab, select **Add**, and select the Groups that you would like to give access to the IED (you may select multiple groups by hold the <Ctrl> key while selecting). Select **OK** when finished.

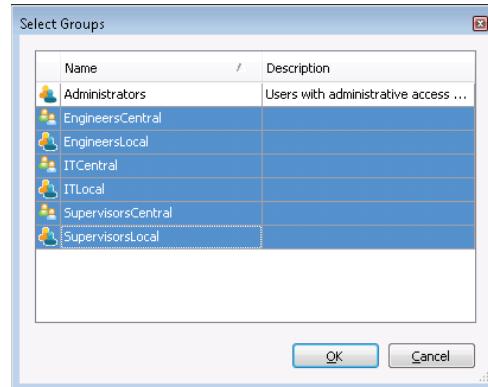


Figure 7.109 Selecting Groups on the IED Permissions Tab

Step 9. For each group, select the **Allow** check box on each SEL authorization level to which you would like to give the respective group access. In this example, we select the following permissions:

- **Supervisors:** All permissions
- **Engineers:** Connect, Access Level 1 and Access Level 2 permissions
- **IT:** Connect permissions only

Step 10. When finished, select **Apply**.

Step 11. In the **Connection Explorer** window, right-click on **SEL-3620**, and then select **Device Tasks > Send**. This will send the test Connection Directory to the SEL-3620. Ensure the upload completes without errors. If you do get errors, see *Troubleshooting* on page 7.83.

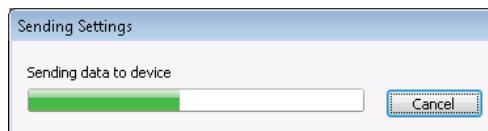


Figure 7.110 Uploading the Connection Directory to the SEL-3620

Step 12. Log in to the SEL-3620 web interface. Under **Reports**, in **System Logs**, verify that the SEL-3620 Syslog shows that the Connection Directory was successfully uploaded.

Step 13. Assuming you have previously configured an SMP, navigate to the **Port Mappings** page and verify that you see both the SSH port and the FTP port for the SEL-787 (see *Figure 7.111*).

Engineering Access		Add Device	Rename	Disable	Delete
ALL:22		SSH		-	
Protocol	Port	Managed Devices	Connected Via		
FTP	1787	SEL-787	192.168.10.87:21		
SSH	22	SEL-787	192.168.10.87:23		

Figure 7.111 SMP With FTP Proxy Port

Navigating the SEL-3620 FTP Proxy via Terminal

This section will first guide you through proxying access to an Ethernet-enabled SEL IED over FTP using a Windows terminal, and then by using QuickSet (see *Using the SEL-3620 Proxy Services* on page 7.26).

When logging in to the SEL-787 FTP proxy of the SEL-3620, the SEL-3620 will prompt the user for valid local or centralized credentials. If authentication succeeds, the user is then authorized to access the Access Level configured in the Connection Directory for the IED FTP proxy settings (see *Figure 7.108*).

To proxy using FTP through use of a Windows terminal, perform the following steps:

- Step 1. Open a Windows terminal (select **Start**, type **cmd**, and press **<Enter>**).

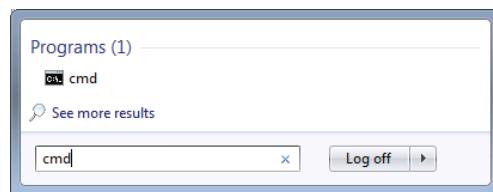


Figure 7.112 Windows Command Line Terminal

- Step 2. To access FTP from the Windows command line, type **FTP**.
- Step 3. To access the SEL-787 FTP proxy of the SEL-3620 on TCP Port 1787, type **OPEN 192.168.10.20 1787**. You should now see the FTP login prompt of the SEL-3620 (see *Figure 7.113*).

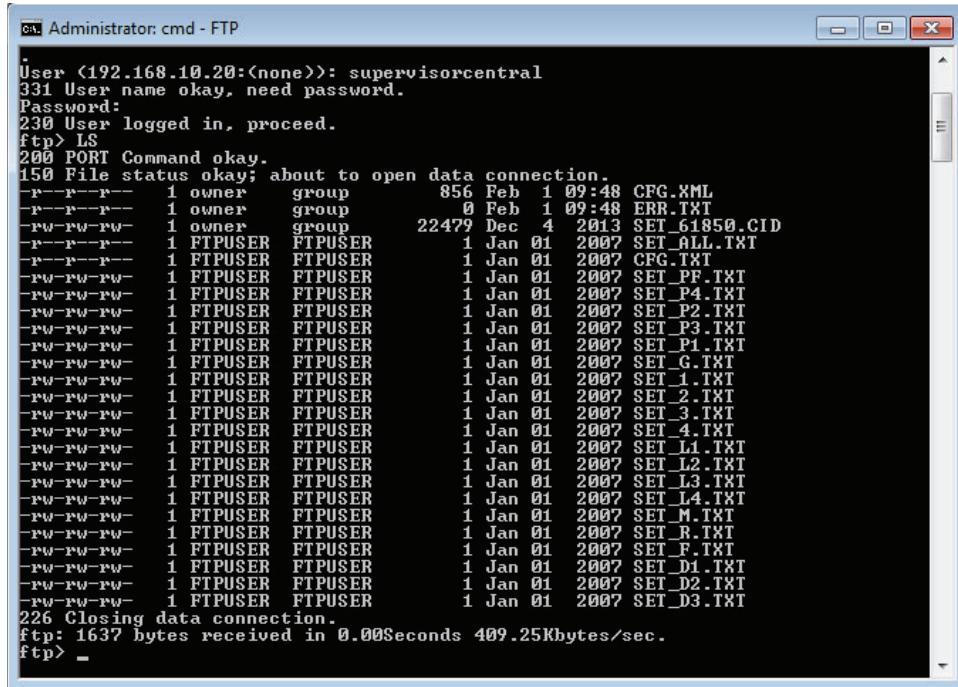
A screenshot of a Windows Command Line Terminal window titled 'Administrator: cmd - FTP'. The window shows a command-line session:

```
C:\>Users\Colin\Desktop>FTP
ftp> OPEN 192.168.10.20 1787
Connected to 192.168.10.20.
220 This system is for the use of authorized users only. Individuals using this
system without authority, or in excess of their authority, are subject to having
all their activities on this system monitored and recorded by system personnel.
Anyone using this system expressly consents to such monitoring and is advised t
hat if such monitoring reveals possible evidence of criminal activity, system pe
rsonnel may provide the evidence of such monitoring to law enforcement officials
User <192.168.10.20:<none>>: -
```

The terminal window has a dark background with white text. The title bar is blue with white text.

Figure 7.113 FTP Login Prompt

- Step 4. Log in to the SEL-787 FTP proxy of the SEL-3620 with your user-name and password. Once successfully authenticated, you should be able to use the **LS** command to view a list of files available on the Ethernet-enabled IED (see *Figure 7.114*).



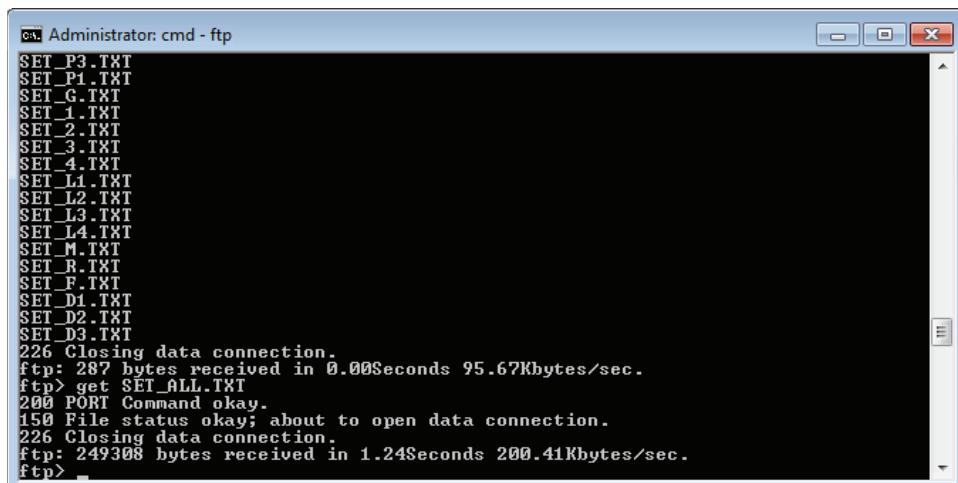
```

Administrator: cmd - FTP
User <192.168.10.20:<none>>: supervisorcentral
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> LS
200 PORT Command okay.
150 File status okay; about to open data connection.
-r--r--r-- 1 owner group 856 Feb 1 09:48 CFG.XML
-r--r--r-- 1 owner group 0 Feb 1 09:48 ERR.TXT
-rw-rw-rw- 1 owner group 22479 Dec 4 2013 SET_61850.CID
-r--r--r-- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_ALL.TXT
-r--r--r-- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 CFG.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_PF.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_P4.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_P2.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_P3.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_P1.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_G.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_1.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_2.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_3.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_4.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_L1.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_L2.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_L3.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_L4.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_M.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_R.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_F.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_D1.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_D2.TXT
-rw-rw-rw- 1 FTIPUSER FTIPUSER 1 Jan 01 2007 SET_D3.TXT
226 Closing data connection.
ftp: 1637 bytes received in 0.00Seconds 409.25Kbytes/sec.
ftp> _

```

Figure 7.114 FTP LS Command

Step 5. You can now download/upload files over FTP by using the **GET** and **PUT** commands, respectively (see *Figure 7.115*).



```

Administrator: cmd - ftp
SET_P3.TXT
SET_P1.TXT
SET_G.TXT
SET_1.TXT
SET_2.TXT
SET_3.TXT
SET_4.TXT
SET_L1.TXT
SET_L2.TXT
SET_L3.TXT
SET_L4.TXT
SET_M.TXT
SET_R.TXT
SET_F.TXT
SET_D1.TXT
SET_D2.TXT
SET_D3.TXT
226 Closing data connection.
ftp: 287 bytes received in 0.00Seconds 95.67Kbytes/sec.
ftp> get SET_ALL.TXT
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp: 249308 bytes received in 1.24Seconds 200.41Kbytes/sec.
ftp> _

```

Figure 7.115 FTP Proxy GET Command

Step 6. To exit the FTP session, use the **QUIT** command.

Note that there are neither special commands nor a binary mode available on the SEL-3620 when connected to the FTP proxy. Access scripts and Terminate scripts are not triggered or used while in the FTP proxy session.

Navigating the SEL-3620 FTP Proxy via QuickSet

Users may also choose to use QuickSet software to access IEDs directly from the Device Manager Connection Directory, and use QuickSet to download/upload settings over FTP.

To access the SEL-787 through the SEL-3620 Proxy Services with QuickSet, use the following steps:

- Step 1. In the Device Manager **Connection Explorer** window, select the **SEL-3620 Connection** tab and ensure the settings shown in *Figure 7.52* are used.
- Step 2. Ensure that you are logged in to the QuickSet Database as a user who has privileges on the SEL-787 IED, such as supervisorlocal.
- Step 3. After logging in to the QuickSet Database, right-click on **SEL-787** in the **Connection Explorer** window, and select **Connect**.

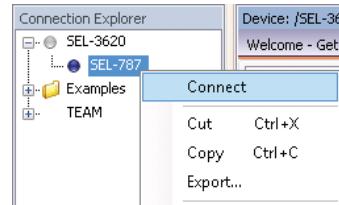


Figure 7.116 Connecting to the SEL-787

- Step 4. It is normal to receive a Device Authentication prompt from QuickSet for SSH connections between QuickSet and the SEL-3620. You may choose **Trust** to permanently trust the SEL-3620 SSH signature or **Trust Once** to temporarily trust the SEL-3620 SSH signature.
- Step 5. Green dots next to the SEL-3620 and SEL-787 templates indicate a successful connection has been made. If you do not connect successfully to the SEL-787, see *Troubleshooting* on page 7.83.



Figure 7.117 Successful Proxy Services Connection Through QuickSet

From this state, you can download/upload device settings, check the current running HMI, and download event reports (right-click on the active SEL-787 template to see a list of options).

- Step 6. To download settings via FTP, right-click on **SEL-787** and select **Device Tasks > Read** (make sure the **File Transfer Protocol** on the IED is set to **FTP**). During settings download over FTP, QuickSet will typically download CFG.XML and SET_ALL.TXT files (see *Figure 7.118*).

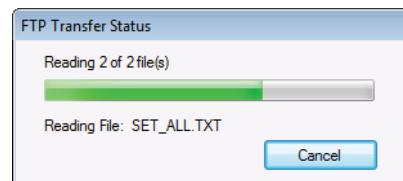


Figure 7.118 QuickSet FTP File Transfer

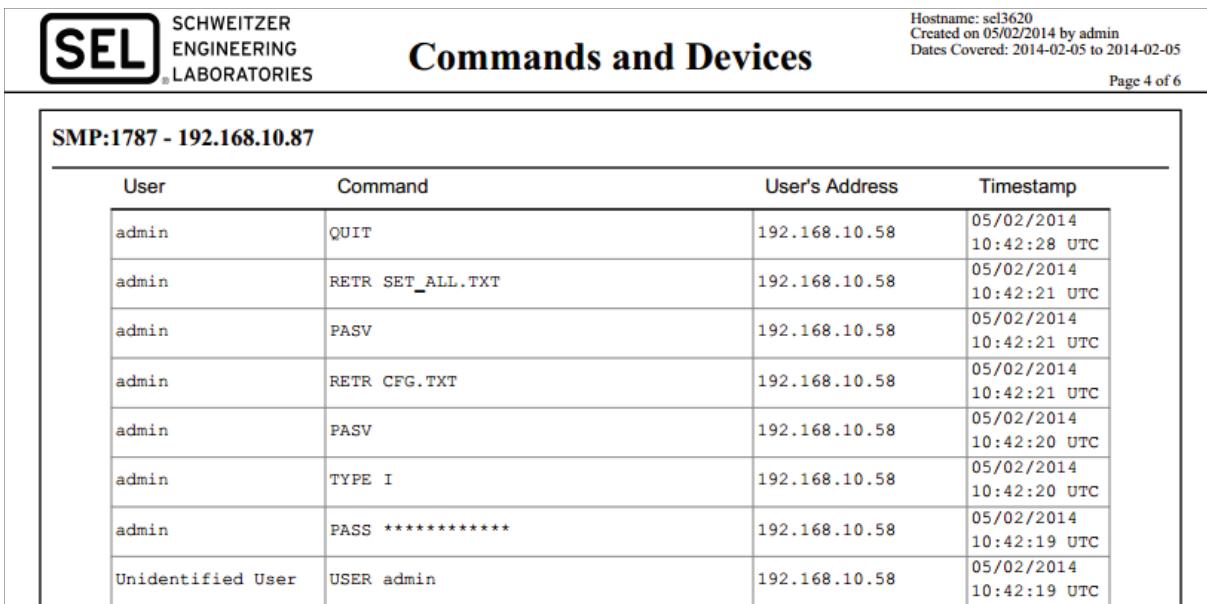
- Step 7. To disconnect from the SEL-787 IED, right-click **SEL-787** and select **Disconnect**.

Using Multifactor Authentication With QuickSet and FTP Proxy

A recent version of QuickSet introduced the ability to reauthenticate to the FTP Proxy when using RADIUS for one-time token (OTP) based challenges. When you select the **Enable RADIUS Authentication** check box on the **Device** tab (see *Figure 7.9*), QuickSet will challenge a user for their password before attempting an FTP transaction.

SEL-3620 Commands and Devices Report (FTP)

All connections to the SEL-3620 FTP Proxy are logged via the SEL-3620 Syslog logging function, and all ASCII commands executed on IEDs when connected through the SEL-3620 SMP are logged to the SEL-3620 Commands and Devices report. This report contains information about the user who executed the FTP commands, the commands themselves, the user's IP, and the UTC time stamp to the second. *Figure 7.119* shows an example of this information.

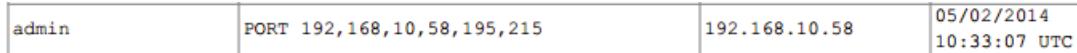


The screenshot shows a report titled "Commands and Devices" from the SEL-3620. The header includes the SEL logo, the text "SCHWEITZER ENGINEERING LABORATORIES", and details about the report: Hostname: sel3620, Created on 05/02/2014 by admin, Dates Covered: 2014-02-05 to 2014-02-05, and Page 4 of 6. The main table has columns for User, Command, User's Address, and Timestamp. The data shows several commands from user "admin" at IP 192.168.10.58, including QUIT, RETR SET_ALL.TXT, PASV, RETR CFG.TXT, and PASS. There is also a single entry for an "Unidentified User" who logged in as "admin".

User	Command	User's Address	Timestamp
admin	QUIT	192.168.10.58	05/02/2014 10:42:28 UTC
admin	RETR SET_ALL.TXT	192.168.10.58	05/02/2014 10:42:21 UTC
admin	PASV	192.168.10.58	05/02/2014 10:42:21 UTC
admin	RETR CFG.TXT	192.168.10.58	05/02/2014 10:42:21 UTC
admin	PASV	192.168.10.58	05/02/2014 10:42:20 UTC
admin	TYPE I	192.168.10.58	05/02/2014 10:42:20 UTC
admin	PASS *****	192.168.10.58	05/02/2014 10:42:19 UTC
Unidentified User	USER admin	192.168.10.58	05/02/2014 10:42:19 UTC

Figure 7.119 Commands and Devices Report (FTP)

Certain FTP commands captured in the report may contain information about which ports were dynamically opened on the SEL-3620 firewall to accommodate Active FTP data transfer sessions (see *Figure 7.120*).



The screenshot shows a single row of a table with four columns. The first column contains "admin", the second contains "PORT 192,168,10,58,195,215", the third contains "192.168.10.58", and the fourth contains "05/02/2014 10:33:07 UTC".

admin	PORT 192,168,10,58,195,215	192.168.10.58	05/02/2014 10:33:07 UTC
-------	----------------------------	---------------	----------------------------

Figure 7.120 Active FTP Session Command

From the **PORT** command (see *Figure 7.120*), we can see that the Windows terminal FTP client instructed the SEL-3620 FTP proxy to connect to the Windows computer (192.168.10.58) on TCP port 50135 ([195 x 256] + 215) to download the data from the proxied IED FTP connection.

SEL-3620 Proxy Syslog Messages

While the Commands and Devices report captures granular FTP command session data, the SEL-3620 also captures more general security information about user connection to the proxy via Syslog. An SEL-3620 administrative user can configure as many as three different Syslog server destinations, which can be common SIEM servers, such as Splunk, QRadar, LogRhythm, and others.

SEL-3620 Password Management for Ethernet-Enabled IEDs

There is essentially no difference in the SEL-3620 password management for Ethernet-enabled IEDs when compared to serial IEDs.

Troubleshooting

See *Safety Tips for SEL-3620 Password Management* on page 7.54 for general password management and proxy troubleshooting tips.

QuickSet Reports “A duplicate Proxy Port (FTP) value was found” When Uploading a Connection Directory

If you receive a “Duplicate Proxy Port” message from QuickSet (see *Figure 7.121*), then you have multiple IEDs in the Connection Directory with the same Proxy Port (FTP) value. Check your IEDs and ensure each has a unique TCP port value set for the Proxy Port (FTP), and attempt the Connection Directory upload again.

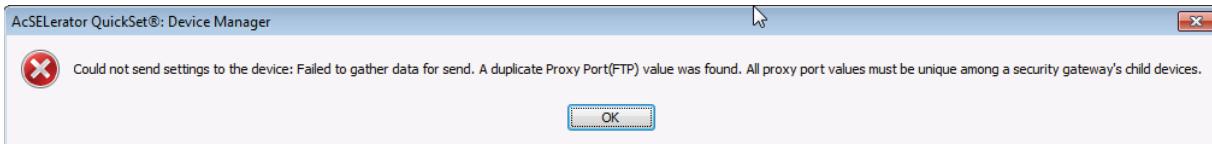


Figure 7.121 Duplicate Proxy Port (FTP) Value

Unable to Connect to the SEL-3620 FTP Proxy Port

Under specific conditions, you may not be able to connect to the SEL-3620 FTP proxy ports. To troubleshoot the connectivity of the FTP proxy ports, perform the following checks:

- Step 1. Ensure that you are connecting to a valid FTP proxy port (check the Port Mappings page on the SEL-3620 webpage).
- Step 2. Ensure that the Port Mapping that contains the FTP proxy port is currently enabled.
- Step 3. If you still encounter errors, check the SEL-3620 Diagnostics page (**Reports >Diagnostics**). From the Diagnostics page, select **Update Diagnostics**, and wait until you see the message **Diagnostics Updated**. In the diagnostics dump under **Chain USER_INPUT**, you should see information similar to *Figure 7.122*.

Chain USER_INPUT (1 references)							
pkts	bytes	target	prot	opt	in	source	destination
0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0
3	156	ACCEPT	tcp	--	*	*	0.0.0.0/0
0	0	ACCEPT	tcp	--	*	*	10.203.18.23
							0.0.0.0/0
							tcp dpt:33389 flags: 0x17/0x2
							tcp dpt:1787 flags: 0x17/0x2
							tcp dpt:500 flags: 0x17/0x2

Figure 7.122 SEL-3620 Diagnostics Dump

Figure 7.122 shows that FTP Proxy Port 1787 is open and accepting connections. If you cannot find your FTP proxy ports under the **Chain USER_INPUT** section, then it is possible that the ports did not open correctly. Perform the following troubleshooting steps to fix this problem:

- Step 1. Disable the FTP Proxy Port map from the **Port Mappings** page, wait 10 seconds, then reenable the port map. Check diagnostics again (see *Step 3*) to see if the ports were opened.
- Step 2. If the ports are still not opened, reboot the SEL-3620 from the **Diagnostics** page (select **Reboot system**). Recheck diagnostics after the SEL-3620 has rebooted to ensure that the FTP proxy ports are open and accepting connections.

FTP Proxy Responds With “421 Service not available”

A “421 Service not available” message from the FTP proxy after logging in means that the downstream SEL relay has responded that it cannot currently accept new FTP connections (see *Figure 7.123*).

```
Administrator: cmd - ftp
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Colin\Desktop>ftp
ftp> open 192.168.10.20 1787
Connected to 192.168.10.20.
220 This system is for the use of authorized users only. Individuals using this
system without authority, or in excess of their authority, are subject to having
all their activities on this system monitored and recorded by system personnel.
Anyone using this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity, system personnel may
provide the evidence of such monitoring to law enforcement officials.

User (192.168.10.20:<none>): admin
331 User name okay, need password.
Password:
421 Service not available, closing control connection.
Login failed.
ftp> _
```

Figure 7.123 FTP Proxy 421 Error

Most SEL relays can only accept either one or two FTP connections simultaneously. Some common FTP clients require the use of more than one open FTP command channels, and therefore may be incompatible with SEL IED FTP implementations. Check your FTP client documentation and/or SEL IED documentation for information about simultaneous FTP connections.

FTP Proxy Responds With “530 Invalid User Credentials”

If you receive the “530 Invalid User Credentials” message from the FTP proxy after attempting to log in (*Figure 7.124*), then either your username/password combination was not correct, or you do not have permissions to access the FTP proxy for the current IED.



```
C:\Users\Colin\Desktop>ftp
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Colin\Desktop>ftp> open 192.168.10.20 1787
Connected to 192.168.10.20.
220 This system is for the use of authorized users only. Individuals using this
system without authority, or in excess of their authority, are subject to having
all their activities on this system monitored and recorded by system personnel.
Anyone using this system expressly consents to such monitoring and is advised t
hat if such monitoring reveals possible evidence of criminal activity, system pe
rsonnel may provide the evidence of such monitoring to law enforcement officials
.

User (192.168.10.20:<none>): engineercentral
331 User name okay, need password.
Password:
530 Invalid User Credentials.
Login failed.
ftp> -
```

Figure 7.124 FTP Proxy 530 Error

Check your current username and password, and ensure that you have been given authorization to the IED access level in the connection directory (see *Figure 7.108*).

Other FTP Proxy Connectivity Issues

NOTE: On the SEL-3610, SEL-3620, and SEL-3622 devices, we use the following ranges for ephemeral ports:

Firmware R208 and earlier:
Ports 32768-61000

Firmware R210 and later:
Ports 32768-60999

If you continue experiencing FTP proxy connectivity issues, ensure that any firewalls between your FTP client, the SEL-3620 FTP proxy, and the downstream IEDs allow passive and/or active FTP connections.

For active FTP connections, you need to ensure any firewall between the FTP client and the FTP server allows the following:

- Step 1. The FTP client can connect to the FTP server at the proper FTP command channel port (FTP Proxy Port).
- Step 2. The FTP server can connect back to the FTP client at an ephemeral (short-lived use) port number (see *Figure 7.125*).

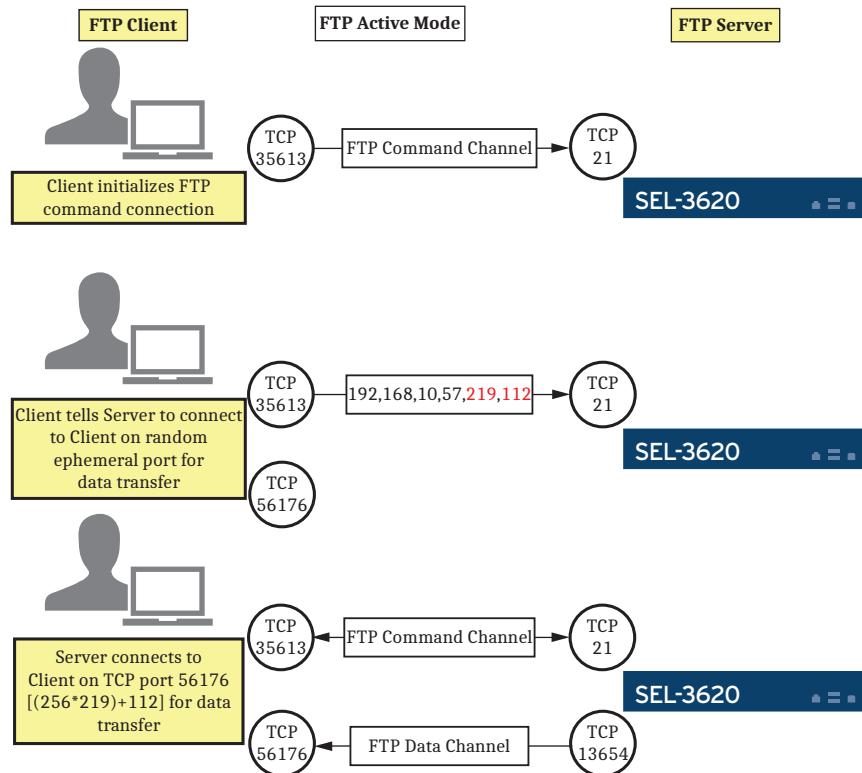


Figure 7.125 FTP Active Mode

For passive FTP connections, you need to ensure any firewall between the FTP client and the FTP server allows the following:

- Step 1. The FTP client can connect to the FTP server at the proper FTP command channel port (FTP Proxy Port).
- Step 2. The FTP client can connect to the FTP server at an ephemeral (short-lived use) port number (see *Figure 7.126*).

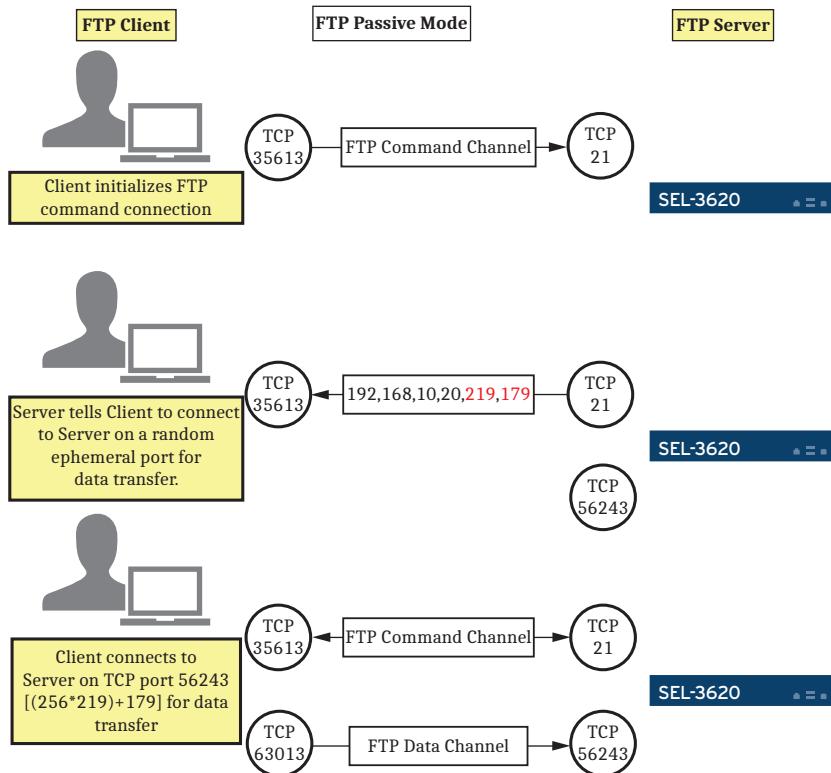


Figure 7.126 FTP Passive Mode

QuickSet uses FTP passive mode by default. The Windows terminal client uses FTP active mode by default. In most cases, you can instruct the FTP server to use the passive mode by sending the **PASV** command. Check with your FTP client documentation for information about whether it supports FTP active or passive mode. In many instances, firewalls are less restrictive about FTP passive mode.

Management of SEL Communications Processors

Introduction

NOTE: The communications processor family encompasses the SEL-2020, SEL-2030, and SEL-2032. For information about how the SEL-3620 interacts with SEL-3530 Series Real-Time Automation Controllers (RTACs), see Managing IED Passwords With the SEL-3620 Ethernet Security Gateway and SEL RTAC Using SEL Server Connections (SEL Application Guide AG2013-22).

This section details the following configuration and testing steps:

- Theory of operation
- Password management process
- General configuration tips for SEL communications processors
- Safety tips and best practices for SEL communications processors
- QuickSet Device Manager configuration
- Using the SEL-3620 Proxy with SEL communications processors
- Password management with SEL communications processors
- FAQ
- Troubleshooting

Password management should only be undertaken when the proxy is working as expected. If you encounter errors that are not answered in *Troubleshooting* on page 7.83 or are unclear about how the SEL-3620 proxies access secured IEDs, review the previous sections.

Scenario Configuration

The following scenario shows the present configuration. You may replace the network addresses and serial COM port numbers with your own, depending on your system settings. This example uses an SEL-2032 Communications Processor, and SEL-351 and SEL-451-5 relays for testing. You may use your own single or multiple SEL IEDs connected via serial to an SEL-2020, SEL-2030, or SEL-2032. The SEL-2032 may then be connected via serial to an SEL-2020, SEL-2030, or SEL-2032. The SEL-2032 may then be connected via serial or Ethernet to the SEL-3620. Note that the use of the CAS is optional.

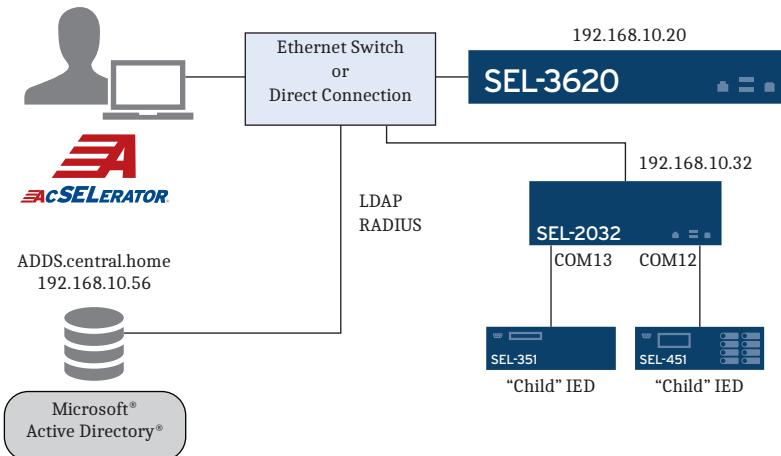


Figure 7.127 Communications Processor Password Management Network Diagram

SEL-3620 Management of Communications Processors Theory of Operation

The SEL-3620 manages IEDs connected to communications processors by using information sent to it in a QuickSet Connection Directory. The scenario with a communications processor is complicated by the fact that when a communications processor uses SEL Protocols to poll a child SEL IED, it must have knowledge of the Access Level 1 (and sometimes Access Level 2) password of the child relay to perform event retrieval, fast breaker, and other command operations. If the SEL-3620 performs a password update on the SEL device, the SEL-3620 must update the communications processor internal database with the child's new Access Level 1 (and sometimes Access Level 2) password or risk the communications processor losing operational (i.e., SCADA) visibility on the child relay.

The solution to this child password synchronization issue is simple: you must configure the SEL-3620 to update the internal database of the communications processor with the new Access Level 1/Access Level 2 child password for each IED it polls via SEL Protocols. We do this by configuring the communications processor in Device Manager with a special Child Password Update Script.

Notes on SEL-2030 and SEL-2032 Firmware Versions

In 2015, SEL introduced later firmware versions for SEL-2030 (R126-V1) and SEL-2032 (R115-V1). The later firmware introduces the ability to update child passwords in the static memory of the communications processors without the need to run an autoconfiguration process. The autoconfiguration process is required for SEL-2020 communications processors, SEL-2030 communications processors firmware R125 and earlier, and SEL-2032 communications processors firmware R114 and earlier when updating passwords for child SEL devices,

because the communications processors may use the Access Level 1 password (and Access Level 2 in some instances) of the child device when performing normal SEL ASCII functions. It is strongly recommended to update any SEL-2030 and SEL-2032 communications processors to R126-V1 and R115-V1 (respectively) to greatly reduce the time needed for password changes and increase the reliability of the operation.

Password Change Process on SEL Communications Processors

To change the password of a communications processor with two children, do the following:

- Step 1. Ensure a connection between an SEL-3620 and a communications processor.
- Step 2. The SEL-3620 tunnels to the IED by going to Access Level 1 on the communications processor, and entering the **PORT x D** command to open a direct connection to the child IED. *At this point, SCADA will stop polling the IED.*
- Step 3. The SEL-3620 will change all passwords on the child IED.
- Step 4. The SEL-3620 will terminate from the child IED by using the termination string of the communications processor.
- Step 5. The SEL-3620 will update the child IED password(s) on the communications processor.
 - a. For all SEL-2020 communications processors, SEL-2030 communications processors with firmware version R125 or earlier, and SEL-2032 communications processors with firmware version R114 or earlier, the SEL-3620 will update the child IED password(s) on the communications processor by accessing Access Level 2 of the communications processor, and use the **SET P x TERSE** command to trigger an autoconfiguration. During the port autoconfiguration, the SEL-3620 will enter the new password(s) of the child IED when prompted by the communications processor.
 - b. For SEL-2030 communications processors with firmware version R126-V1 or later and SEL-2032 communications processors with firmware version R115-V1 or later, the SEL-3620 will update the child IED password(s) on the communications processor by accessing Access Level 2 of the communications processor, and use the **SET P x y <PASSWORD>** command to update port x IED, password level y <PASSWORD> (e.g., Level 1 OTTER, Level 2 TAIL).
- Step 6. If using SEL-2032 firmware R114 and below, or SEL-2030 firmware R125 and below: The SEL-3620 will finish the autoconfiguration sequence, then reestablish a connection to the IED, then terminate. *At this point, SCADA will begin polling the IED again.*
- Step 7. The SEL-3620 will proceed to update the communications processor passwords.
- Step 8. The SEL-3620 will repeat Step 1 on page 7.89–Step 6 on page 7.89 for each child IED.

The SEL-3620 requires the configuration of special Access and Terminate scripts on the IED in Device Manager to know how to properly tunnel to the IED and terminate correctly.

Figure 7.128 illustrates this process.



Figure 7.128 SEL-3620 Communications Processor and Child Password Change Process

The proxying of a user to an IED through a communications processor is similar to the previous Steps 1 and 2:

- Step 1. A user selects an IED to connect to from the SEL-3620 proxy interface.
- Step 2. The SEL-3620 connects to the communications processor.
- Step 3. The SEL-3620 tunnels to the IED by going to Access Level 1 on the communications processor, and entering the **PORT x D** command to open a direct connection to the child IED.

While the user is connected to the IED, the SEL-3620 prevents the user from entering the communications processor termination string to gain access to the communications processor interface.

Before You Begin

For SEL-3620 communications processor password management and proxy applications, there are a number of recommendations and limitations to be aware of:

- On SEL-2020 communications processors, SEL-2030 communications processors with firmware version R125 and earlier, and SEL-2032 communications processors with firmware version R114 and earlier, individual child password updates on the communications processors can take as long as 20 minutes in some extreme cases (e.g., where the child IED serial baud rate is very slow) because of lengthy autoconfiguration sessions. Be aware of this before you attempt to change all passwords on IEDs below communications processors, as the total password change time could take several hours. SEL strongly recommends that you update your SEL-2030 and SEL-2032 communications processors to firmware version R126-V1 or later and R115-V1 or later, respectively, to take advantage of much faster child password updates.
- The communications processor master port time-out (the port you are using to communicate with the SEL-3620) should be set to 30 minutes, at minimum, to account for lengthy child password updates. For safety purposes, do not disable time-outs altogether.
- If the SEL-3620 is connecting to the SEL-2032 over Ethernet, you will need to set your **ComProc TIDLE** setting to **disabled**, or to a time that is equal to or greater than the **TIMEOUT** setting. This is because the TIDLE setting causes the SEL-2032 to generate Telnet keep-alive messages to which the SEL-3620 does not respond to, and this may accidentally disconnect an active session.
- For child IEDs connected to the communications processor via a serial connection, use hardware flow control (RTS/CTS) as much as possible. RTS/CTS will maximize the reliability of serial IED connections, and prevent password change failures or errors. Lack of RTS/CTS is commonly the cause of Access Level C password change failures because of the size of the warning banner upon entering Access Level C on SEL IEDs. XON/XOFF software flow control is not an alternative to hardware flow control. XON/XOFF should be disabled when using RTS/CTS signals.
- For child IEDs connected to the communications processor via serial, configure those particular serial ports on the communications processor with time-outs set to a reasonable number of minutes (e.g., 30 minutes). This will prevent tunneled connections from being “stuck,” because the IED will naturally terminate the tunneled connection once the time-out is reached.
- The SEL-3620 does not support engineering access or password changes for child IEDs with serial baud rates lower than 1200 bps, because of script time-outs and instabilities at lower baud rates.
- The SEL-3620 does not support engineering access or password changes for child IEDs that are polled by a communications processor over Ethernet (e.g., require a **PORT 17 192.168.10.123 D** command, Port 17 or Port 18 being SEL-2701/2702 cards).
- Heavily loaded communications processors (i.e., those that have high poll rates for child IEDs) may be “laggy” and unresponsive to commands on the master port at times. These “loaded” communications processors may exhibit failures during password changes or engineering access sessions.

- Ensure that the firmware of your communications processor is up-to-date. For SEL-2032 communications processors, firmware versions R108 and earlier may exhibit failures during autoconfiguration attempts for child password updates for some SEL relays.
- Do not use the front serial port (COM F) as the master port between the communications processor and the SEL-3620. The front serial port on communications processors is incapable of using direct transparent mode for binary file transfers (refer to *Direct Transparent Mode* in the SEL-2032 manual). If you are using the front COM port in an attempt to transfer files, use a different master port instead (COM ports 1–16 or Ethernet ports 17–18).

Before configuring Device Manager for a communications processor scenario, you will need the following information from the master port (the port that will be connected to the SEL-3620) of the communications processor:

- **Termination String (TERSTRING):** The termination string is a special character that triggers the communications processor to terminate an active tunneled session to an IED child.
- **Termination Time 1 (TERTIME1):** This time-out setting can be found on the port settings of the master port on the communications processor (Ethernet or serial) that you intend to use for the SEL-3620 connection (see *Figure 7.129*). TERTIME1 is the time (in seconds) that the master port of the communications processor must be idle before checking for the termination string during an active tunneled session to a child IED.
- **Termination Time 2 (TERTIME2):** This time-out setting can be found on the port settings of the master port on the communications processor (Ethernet or serial) that you intend to use for the SEL-3620 connection (see *Figure 7.129*). TERTIME2 is the time (in seconds) that the master port of the communications processor must be idle after the termination string is entered before the communications processor will terminate an active tunneled session to a child IED.
- **Serial Baud Rates:** If the master port of the communications processor is serial, you will need serial port parameters to configure in Device Manager.

```

PORT: 17
SENDTIME= Y
XON_XOFF= Y
TIMEOUT = 30.0
TERTIME1= 1
TERSTRING="\004"
TERTIME2= OFF
    IPADDR = "192.168.10.32"
    SUBNETM = "255.255.255.0"
    DEFRTTR = "192.168.10.20"
    NETPORT = "B"
    FAILVR = "N"
        FTIME = 5
    NETASPB = "A"
    NETBSPD = "A"

    FTPSERV = "Y"
    FTPCBAN = "FTP SERVER:"
    FTPIDLE = 5
    FTPANMS = "Y"
    FTPAUSR = "2AC"

    T1CBAN = "HOST TERMINAL SERVER:"

```

Figure 7.129 SEL-2032 Master Port Settings

Safety Tips for SEL-3620 Management of Communications Processors



Read this section before performing ANY password changes with your SEL-3620 on communications processors and their child IEDs.

When using the SEL-3620 to manage passwords on communications processors with child IEDs, you must verify the uploaded Connection Directory that you configured in the Device Manager in QuickSet. To perform this function, follow the next steps for each child IED from the SEL-3620 proxy:

- Step 1. Select the child IED, connect to it, and ensure that the SEL-3620 connects to the interface of the correct IED.
- Step 2. Disconnect from the child IED back to the SEL-3620 proxy by using the proxy termination string (<Ctrl+W> by default). Wait ten seconds to ensure that the SEL-3620 disconnects successfully and does not give an error.

If you receive any errors above, or you connect to the wrong IED interface, go back to the QuickSet Device Manager and ensure that you are using correct Access and Terminate scripts, correct serial port parameters, etc.

- For all SEL-2020 communications processors, SEL-2030 communications processors with firmware version R125 or earlier, and SEL-2032 communications processors with firmware version R114 or earlier, SEL suggests that you manually attempt an autoconfiguration of a child IED to ensure the communications processor firmware is new enough to correctly handle autoconfiguration for newer SEL child IEDs. You may perform this autoconfiguration function by entering the **SET P x TERSE** command, and following the prompts to perform a new autoconfiguration. If you receive errors during this process, you should consider upgrading the communications processor firmware before attempting a system-wide password change on the communications processor.
- You are strongly urged to save a copy of the configuration of the communications processor to a secure storage location by using SEL-5020 Settings Assistant Software. You may perform this function through the SEL-3620 proxy by using the SEL-5827 Virtual Connect Client software (see below for guidance on how to do this).
- SEL-2032 communications processors with firmware versions R114 or earlier may lose port settings for certain SEL IEDs during the autoconfiguration process. Backup all SEL Communications Processor port settings (Math/Move, etc.) before attempting to run password changes using the SEL-3620.

Following the preceding safety steps will help prevent the need to physically recover IED passwords, and will help prevent errors during the SEL-3620 password change process.

Device Manager Configuration of Communications Processor Systems

This section will guide you through configuring an Ethernet-enabled SEL-2032 with two child IEDs in the QuickSet Device Manager. To do this, perform the following steps:

- Step 1. In the **Connection Explorer** window, right-click on **SEL-3620**, and select **Add > Device**. Scroll down to the bottom of the **Select Device Type** window, and choose **SEL-2032**.
- Step 2. Expand the SEL-2032 device by double-clicking the template. Select the **Device** tab.
- Step 3. Select **Edit** and change the **Global Device ID** (GDID) so that it matches the **Device Name**.
- Step 4. If the SEL-2032 passwords are currently set to default values (**OTTER**, **TAIL**, etc.), then go to the next step. Otherwise, enter the current level (Access Level 1, Access Level 2, Access Level C, etc.) passwords into the **Device Passwords** box. Note that the **Update Child Password Script** should be enabled by default (see *Figure 7.130*).

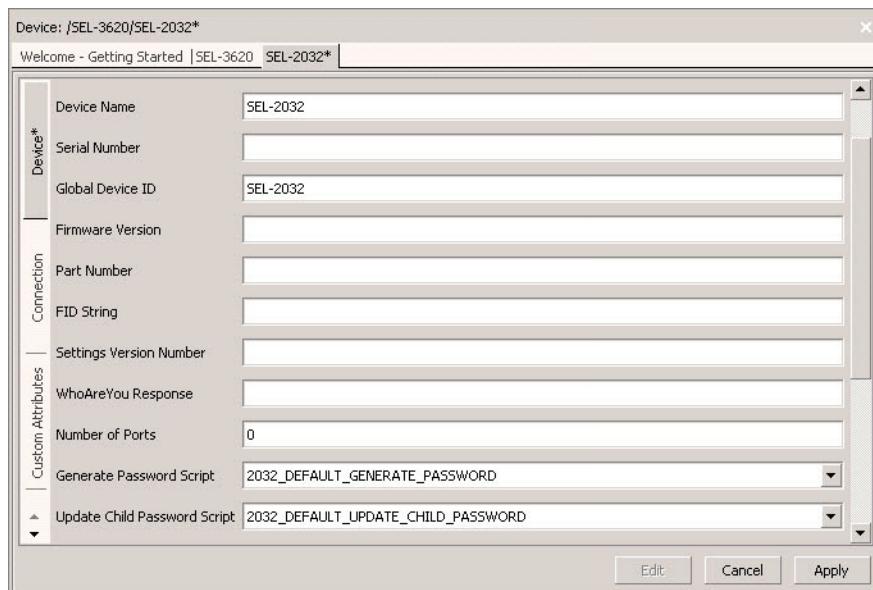


Figure 7.130 SEL-2032 Device Tab

Select the **Connection** tab. Fill in the boxes according to *Figure 7.131*. An explanation of some of the options are as follows:

- **First Delay Time:** This is the same as the TERTIME1 setting on the communications processor master port. Enter the actual TERTIME1 setting here (one second by default).
- **Second Delay Time:** This is the same as the TERTIME2 setting on the communications processor master port. Enter the actual TERTIME2 setting here (zero seconds by default).
- **Termination String:** This is the same as the TERSTRING setting on the communications processor master port. Enter the actual TERSTRING setting here (004 or <Ctrl+D> by default).

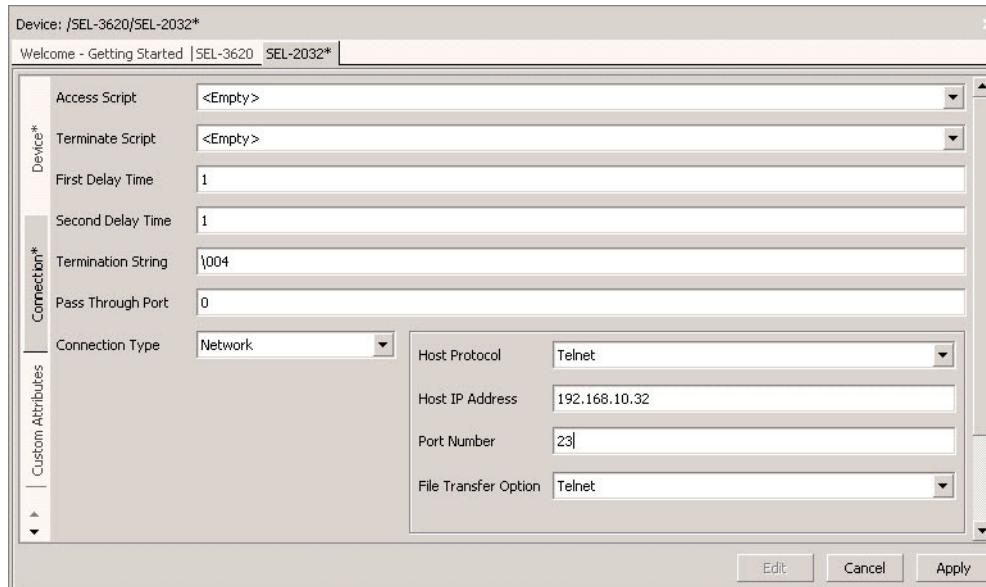


Figure 7.131 SEL-2032 Connection Tab

- Step 5. You may leave the other settings in the **Connection** tab with the default values.
- Step 6. Under the **Permissions** tab, select **Add**, and select the Groups that you would like to give access to the IED (you may select multiple groups by hold the **<Ctrl>** key while selecting). Select **OK** when finished.

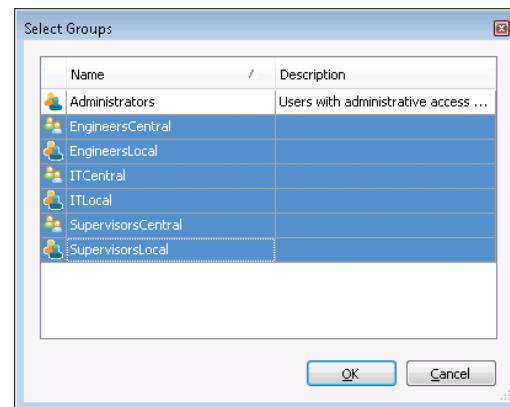


Figure 7.132 Selecting Groups on the IED Permissions Tab

- Step 7. For each group, select the **Allow** check box on each SEL authorization level to which you would like to give the respective group access. In this example, we select the following permissions:

- **Supervisors:** All permissions
- **Engineers:** Connect Access Level 1 and Access Level 2 permissions
- **IT:** Connect permissions only

- Step 8. When finished, select **Apply**.

Next, we will add the SEL-351 and SEL-451 relays as child IEDs below the SEL-2032 in Device Manager.

- Step 1. In the **Connection Explorer** window, right-click on **SEL-2032** below the SEL-3620, and select **Add > Device** (see *Figure 7.133*). Scroll down to the bottom of the **Select Device Type** window, and choose **SEL-451**.

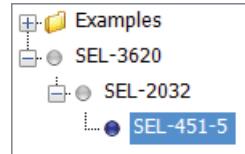


Figure 7.133 Tiered SEL-2032 and SEL-451-5

- Step 2. Double-click on **SEL-451-5** to open it, and select the **Device** tab.
- Step 3. Select **Edit** and change the Global Device ID (GDID) so that it matches the **Device Name**.
- Step 4. If the SEL-451-5 passwords are currently set to default values (**OTTER**, **TAIL**, etc.), then go to the next step. Otherwise, enter the current level (Access Level 1, Access Level 2, Access Level C, etc.) passwords into the **Device Passwords** boxes.
- Step 5. Under the **Connection** tab, fill the boxes in according to *Figure 7.134*. An explanation of some of the options are as follows:
- **Access Script:** The GENERAL_20XX_ACCESS_SCRIPT is required for IEDs that are children of SEL-2032 Communications Processors. This special script tells the SEL-3620 how to tunnel to the IED through the SEL-2032 (by using **PORT x D**, where *x* is the Pass Through Port of the child IED).
 - **Terminate Script:** The GENERAL_20XX_TERMINATE_SCRIPT is required for IEDs that are children of SEL-2032 Communications Processors. This special script tells the SEL-3620 how to terminate active sessions to the IED through the SEL-2032 (by using the Termination String of the parent communications processor).
 - **Pass Through Port:** This number is the physical COM port on the parent communications processor to which the child IED is attached. In this case, the SEL-451 relay is connected to the SEL-2032 on COM port 12.

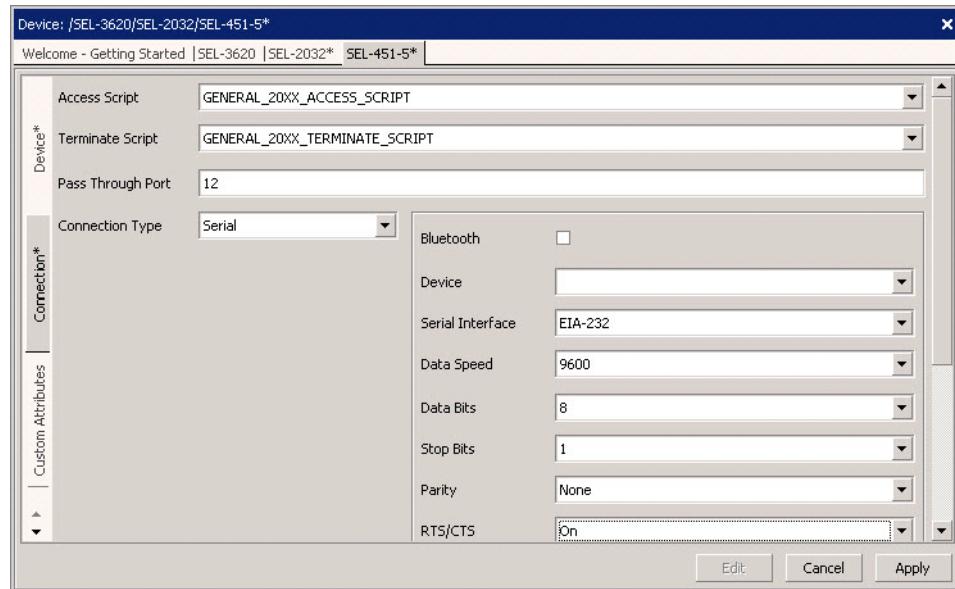


Figure 7.134 SEL-451 Tiered Connection Tab

- Step 6. You may leave the other settings in the Connection tab with the default values. Note that the SEL-3620 does not actually need to know the serial port settings of the child IED below the communications processor, because it cannot program them itself into the communications processor. However, you might want to configure them for record-keeping purposes.
- Step 7. Under the **Permissions** tab, select **Add**, and select the Groups that you would like to give access to the IED (you may select multiple groups by hold the **<Ctrl>** key while selecting). Select **OK** when finished.

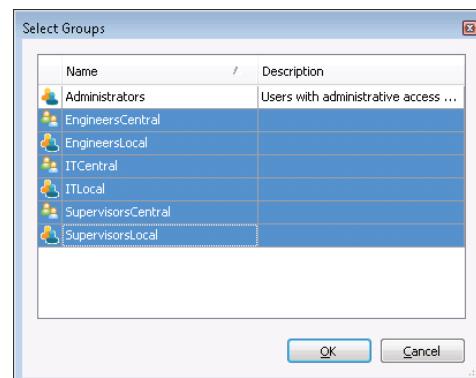


Figure 7.135 Selecting Groups on the IED Permissions Tab

- Step 8. For each group, select the **Allow** check box on each SEL authorization level to which you would like to give the respective group access. In this example, we select the following permissions:
- **Supervisors:** All permissions
 - **Engineers:** Connect, Access Level 1 and Access Level 2 permissions
 - **IT:** Connect permissions only
- Step 9. When finished, select **Apply**.

Step 10. Repeat *Step 1* on page 7.96–*Step 9* on page 7.97 for the SEL-351. The Pass Through Port of the SEL-351 Relay is 13. The final Connection Directory should be similar to *Figure 7.136*.

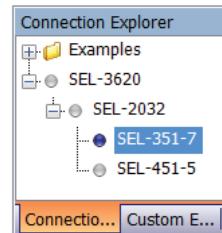


Figure 7.136 SEL-2032, SEL-351, SEL-451 Tiered Scenario

Step 11. In the **Connection Explorer** window, right-click on **SEL-3620**, and select **Device Tasks > Send** from the displayed menu. This will send the test Connection Directory to the SEL-3620. Ensure the upload completes without errors. If you get any errors, see *Troubleshooting* on page 7.105.

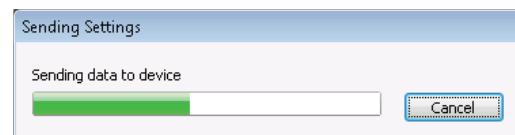


Figure 7.137 Uploading the Connection Directory to the SEL-3620

Step 12. Log in to the SEL-3620 web interface. Under **Reports**, in the **System Log**, verify that the SEL-3620 Syslog shows that the Connection Directory was successfully uploaded.

Step 13. Assuming you have previously configured an SMP, navigate to the **Port Mappings** page and verify that you see the SEL-2032, SEL-351, and SEL-451 IEDs. Both the SEL-351 and SEL-451 should be shown in a tier below the SEL-2032 (see *Figure 7.138*).

Engineering Access			
<input type="button" value="Add Device"/> <input type="button" value="Rename"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>			
ALL:22		SSH	
 SMP			
Protocol	Port	Managed Devices	Connected Via
SSH	22	SEL-2032	192.168.10.32:23
SSH	22	SEL-451-5	Tiered - SEL-2032
SSH	22	SEL-351-7	Tiered - SEL-2032

Figure 7.138 SMP With a Communications Processor Tiered Scenario

Navigating the SEL-3620 Proxy to Communications Processors via Terminal and QuickSet

There is essentially no difference between navigating the SEL-3620 proxy to connect to serial, Ethernet, or communications processor tiered IEDs. Connecting to child IEDs through a communications processor may take as long as one minute in some cases because of baud rate, lag, or a number of other factors associated with tunneling through a communications processor.

Be aware that when downloading or uploading IED settings files of child IEDs via QuickSet, the process may take some time because the maximum serial baud rate for child IEDs is 19200 bps.

Using the SEL-3620 Proxy With SEL-5020 Settings Assistant Software

This section will guide the user through proxying access to a communications processor by using SEL-5020 Settings Assistant Software and SEL-5827 Virtual Connect Client software. SEL-5827 software is suggested for this scenario because SEL-5020 software was not built to support the SEL-3620 proxy authentication and device selection interface. To use SEL-5827 and SEL-5020 software to communicate with a communications processor behind the SEL-3620 proxy, follow these steps:

- Step 1. Open the SEL-5827 Virtual Connect Client software, and select **Communications > Connect**.
- Step 2. Configure the following settings (see *Figure 7.139*):
 - **Virtual Port Settings:** Telnet
 - **Network IP:** 127.0.0.1
 - **TCP Port:** 2032
 - **MODBUS:** Uncheck
 - **Connection Settings:** SSH
 - **Network Host name / IP:** 192.168.10.20 (this is the SEL-3620)
 - **TCP Port:** 22 (this is the SMP)
 - **Enable break on application connect:** Uncheck

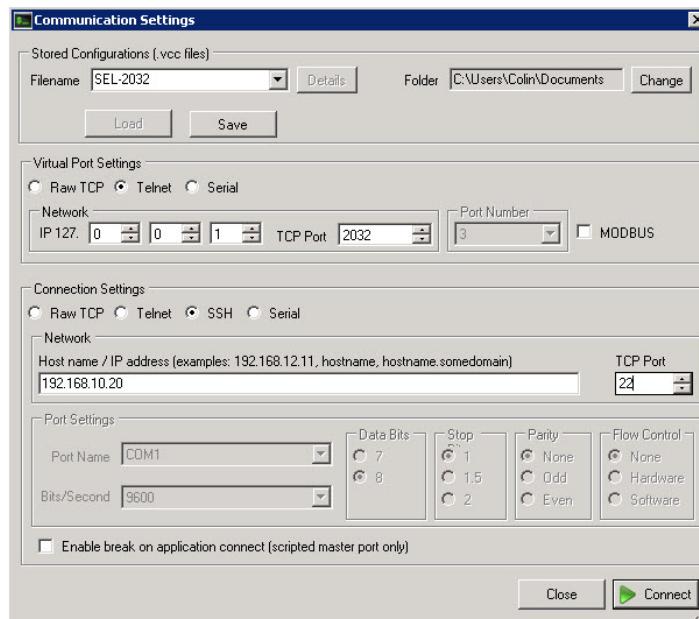


Figure 7.139 SEL-5827 Settings for SEL-5020 Integration

- Step 3. Select **Connect**. If you selected SSH under Connection Settings, you should now see a window asking for your login information (see *Figure 7.140*). You may also see an **SSH Key** window display asking you to verify the remote SSH key. If you see this window the first time you connect to the remote SEL-3620, select **Continue**.

7.100 | Proxy Services and Password Management
Management of SEL Communications Processors

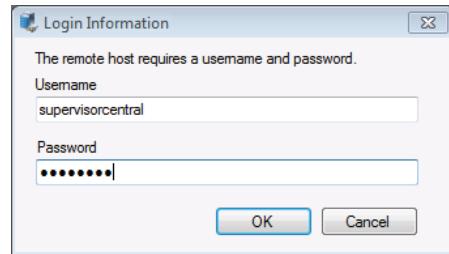


Figure 7.140 SEL-5827 Login Information Window

Step 4. You should now see a “Connection: Connected” message in the lower left corner of the SEL-5827 window. You may now navigate the SMP as if you are using a normal terminal. Type **WHO** to find the communications processor. Next, type **SELECT x** to tell the SEL-3620 to connect to the communications processor interface (see *Figure 7.141*).

A screenshot of the SEL-5827 Virtual Connect Client terminal window. The title bar says "SEL-5827 Virtual Connect Client - 192.168.10.20:22". The menu bar includes File, Communication, and Help. The main window shows a terminal session with the following text:

```
This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Any one using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

*who
Available Devices:
1      SEL-2032
2      SEL-351-7
3      SEL-451-5

*SELECT 1
      HOST TERMINAL SERVER:

*id
  id
"VID=SEL-2032-R114-V0-Z003001-D20110701","08C8"
"VID=SLBT-2030-R103-V0-Z000000-D20010122","094F"
"CID=DDD9","0282"
"DEVID=","0219"
"DEVCODE=52","030E"
"PARTNO=","0281"
"CONFIG=000000","0383"
"SPECIAL=","02AE"

*
```

The status bar at the bottom shows "Connection: Connected | Virtual Port: 127.0.0.1:2032 Open | Rx: 371 Tx: 16".

Figure 7.141 SEL-5827 Terminal Interface for a Communications Processor

Step 5. Next, open the SEL-5020 software, and navigate to **Configuration > Connection Directory**.

Step 6. From the Connection Directory, **Add** a new device. Configure the communication settings to connect to the virtual port that you configured for the SEL-5827 software (see *Figure 7.142*).

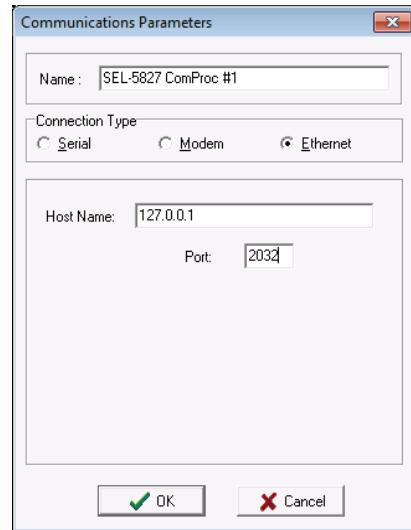


Figure 7.142 SEL-5827 Connection Directory Entry

Step 7. Navigate to **Configuration > Options**, and ensure that you have the SEL-5827 Connection Directory entry selected (see *Figure 7.143*). Select **OK** when finished.

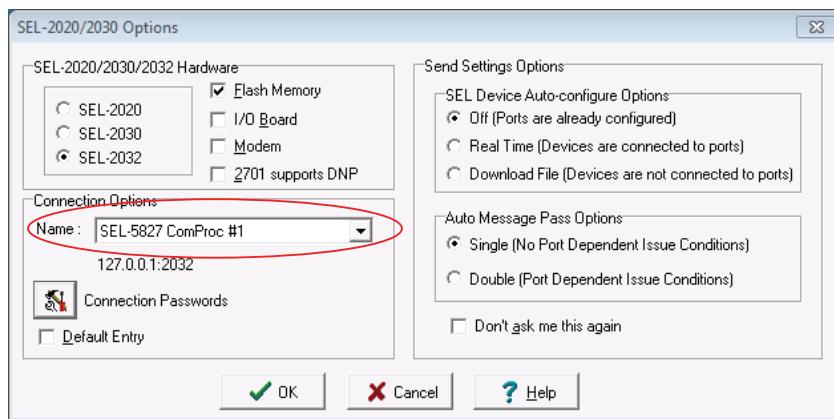


Figure 7.143 SEL-5020 Configuration Options

Step 8. Select **Connect** to access the SEL-2032 interface at the SEL-5827 virtual port (127.0.0.1:2032). You should now be able to check configurations of your SEL-2032, download and upload settings, and perform other duties as if you were directly connected to the SEL-2032. Navigate to **Communications > Terminal** to watch the progress of the SEL-5020 software (see *Figure 7.144*).

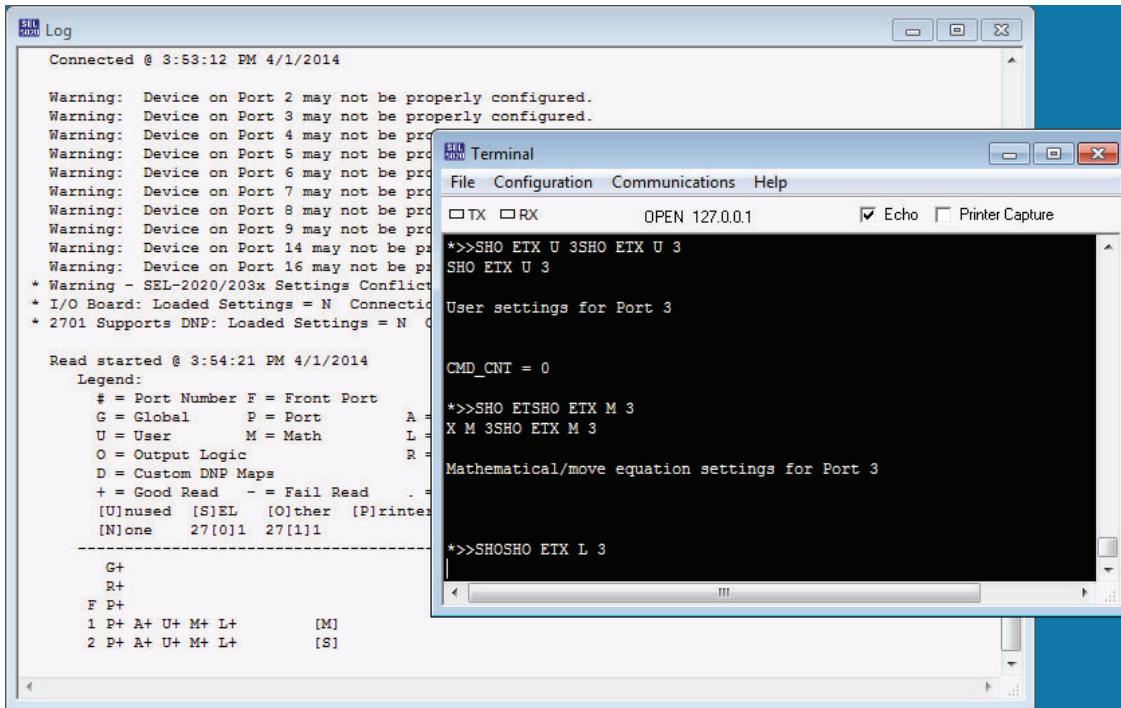


Figure 7.144 SEL-5020 Terminal Through the SEL-5827 Virtual Port

SEL-3620 Password Management of Communications Processor Scenarios



Verify that you can reliably connect and disconnect to/from every child IED (see Safety Tips for SEL-3620 Management of Communications Processors on page 7.93) before attempting password management.

The password management procedure for communications processor scenarios is similar to that of normal Ethernet and serial IEDs. However, password changes for communications processors may take as long as several hours depending on a number of factors.

To keep track of how the SEL-3620 is changing passwords, you may refresh the Syslogs webpage to keep track of progress (see *Figure 7.145*). If you notice a number of failures and wish to cancel the current password change, you may select **Abort** on the **Password Management** page at any time during the process.

<input type="checkbox"/>	2014-04-01 16:02:54	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-451-5
<input type="checkbox"/>	2014-04-01 16:02:33	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-2032
<input type="checkbox"/>	2014-04-01 16:02:21	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-2032
<input type="checkbox"/>	2014-04-01 16:02:12	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-2032
<input type="checkbox"/>	2014-04-01 16:01:59	ProxyServices	Warning	SYSTEM	Authentication Proxy: password updated for child password on SEL-2032
<input type="checkbox"/>	2014-04-01 15:59:24	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-351-7
<input type="checkbox"/>	2014-04-01 15:59:13	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-351-7
<input type="checkbox"/>	2014-04-01 15:59:05	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-351-7
<input type="checkbox"/>	2014-04-01 15:58:57	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on SEL-351-7

Figure 7.145 Communications Processor Password Change Logs

Additional Notice Regarding Child Password Updates



Read this section before performing ANY password changes with your SEL-3620 on communications processors and their child IEDs.

Note that child password updates for every child IED will always run during the following events:

- Any scheduled password changes
- Any manually triggered password changes
- Any manually triggered password changes for individual IED passwords, regardless of type or access level

As of firmware version R201, there is not a way in the SEL-3620 to change an IED password without triggering autoconfigurations for all configured child IEDs to run; so even a manual password update for a single access level (e.g., Access Level 1) can result in several hours of child password updates being run. SEL will enhance this behavior in a future SEL-3620 firmware update. Be aware of the child password update behavior before attempting any password changes. Update any SEL-2030 or SEL-2032 communications processors to firmware revisions R126-V1 and R115-V1 (respectively) or later for the lowest possible child password update times.

Communications Processor Scenario FAQ

The password change on the communications processor and child IEDs is taking forever. How do I stop the process?

The password management procedure for communications processor scenarios is similar to that of normal Ethernet and serial IEDs. However, password changes for communications processors may take as long as several hours depending on a number of factors.

If you are physically present near the communications processor while the password change is occurring, you should be able to tell if the communications processor is performing an autoconfiguration by looking at the serial activity lights on the front of the communications processor. The serial activity lights should be flashing for a child IED that is undergoing autoconfiguration.

If you notice a number of failures and wish to cancel the current password change, you may select **Abort** on the SEL-3620 Password Management page at any time during the process.

Why does the SEL-2032 child password update script trigger an autoconfiguration instead of just updating the IED Port Startup String of the communications processor?

On SEL-2032 firmware version R114 and below, modification of the Port Password Array (EEPROM memory on the communications processor where downstream IED Access Level 1 and Access Level 2 passwords are stored) is limited to the autoconfiguration process only. Modifying the port Startup String (via the **SET A** port command) will not influence the passwords sent to the IED when the communications processor connects back to the IED for SCADA polling or command operations. An autoconfiguration must be performed when changing passwords on child IEDs to properly update the Communications Processor's Port Password Array. In R115-V1 and above, the SEL-2032 will update the startup string based on the current child Access Level 1 and/or Access Level 2 password value found in EEPROM memory.

Will password changes of child IEDs on communications processors disrupt SCADA?

If the communications processor is polling the child IED by using SEL Protocols, then SCADA will be disrupted for each child IED when the SEL-3620 is tunneled into the child IED, and when the SEL-3620 is running the autoconfiguration process for the child IED password update in the communications processor.

Why does my startup string password look different than my password in the SEL-3620?

Running a **SHOW A x** command for a particular serial port yields the startup string for the relay associated with that port, including the Access Level 1 (and sometimes Access Level 2) password(s). Because quotes ("") and backslashes (\) are special characters in the startup string, these characters are escaped using an additional backslash. Therefore, quotes in the child relay passwords will appear as (\") and backslashes will appear as (\\). For example, an Access Level 2 password for a child IED of **76gh\8a** will appear in the startup string for the particular port as **76gh\\8a** (see *Figure 7.146*).

```
USER      = 40
*>>SET A 1
Automatic message settings for Port 1

Save Unsolicited Messages (Y/N)          AUTOBUF = N      ?
Port Startup String
STARTUP ="ACC\nOTTER\n2AC\n76gh\8a\n"
? ACC\nOTTER\n2AC\n76gh\8a\n
Invalid escape character
Port Startup String
STARTUP ="ACC\nOTTER\n2AC\nTAIL\n"
? ACC\nOTTER\n2AC\n76gh\\8a\n
Send Operate command on Logic bit transition (Y/N)SEND_OPER= Y      ? end
AUTOBUF = N
STARTUP ="ACC\nOTTER\n2AC\n76gh\\8a\n"
```

Figure 7.146 Escape Character

Troubleshooting

See previous sections for general password management and proxy troubleshooting tips.

Note that if you get persistent errors after attempting troubleshooting steps, you may wish to implement a serial or Ethernet sniffer to monitor password changes or engineering access attempts between the SEL-3620 and the downstream communications processor. For information about how to do this, see Application Guide AG2013-23, *Using Port Stream Mirroring in the SEL-362x to Monitor Data Traffic*.

For general communications processor troubleshooting, the **STA** command results will provide information about active IED ports, and if the communications processor is heavily loaded (see *Figure 7.147*). See the SEL-2032 manual for additional troubleshooting information.

7.106 | Proxy Services and Password Management
Management of SEL Communications Processors

```
*>>sta
Date: 06/14/14      Time: 17:18:59
FID=SEL-2032-R114-VO-Z003001-D20110701      FID=SLBT-2030-R103-VO-Z000000-D20010122

SELF-TESTS

RAM      SRAM      CODE      ARCH      EEPROM      P.S.      SET      BATTERY      SETM
512 kb   1024 kb  OK        1792 kb  OK        OK        OK        OK        OK        OK

IRIG-B Input: Absent
I/O Board: Installed

Port    Status      Success Rate    SET M      Database Delays
1       Active      None
2       Inactive    None
3       Inactive    None
4       Inactive    None
5       Inactive    None
6       Inactive    None
7       Inactive    None
8       Inactive    None
9       Inactive    None
10      Active      None
11      pInactive  None
12      Active      None
13      Active      None
14      Inactive    None
15      Active      None
16      Inactive    None
17      Normal(0h) NORM      None
F       Active      None
17      Active VT2  100%
```

Last Status Reset: 05/23/14 13:22:22

*>>

Figure 7.147 Communications Processor STA Command

In SEL-2032 firmware version R115-V1 and above, and SEL-2030 firmware version R126-V1 and above, you can use the **PAS P ALL** command to view current Access Level 1 and/or Access Level 2 passwords for all child devices for which the communications processor has a corresponding startup string. Similarly, you can use the **PAS P x**, where *x* is a port number on the communications processor, to view Access Level 1 and/or Access Level 2 password(s) for a single child device. See *Figure 7.148* for an example of the **PAS P x** command.

```
*>>pas p all
Date: 08/06/15      Time: 12:27:11

Port#  Identification          Password#1      Password#2
1      SEL-311L              "OTTER"         ""
2      Relay 1                "OTTER"         ""
3      Relay 1                "OTTER"         ""
4      10014                   "OTTER"         ""
5      FEEDER 1               "OTTER"         ""
6      FEEDER 1               "OTTER"         ""
7      FEEDER 1               "OTTER"         ""
8      SEL-311L              "OTTER"         ""
9      FEEDER 1               "OTTER"         ""
10     SEL-311L              "OTTER"         ""
11     SEL-311L              "OTTER"         ""
12     FEEDER 1               "OTTER"         ""
13     XFMR 1                 "587"           ""
14     FEEDER 1               "OTTER"         ""
15     FEEDER 1               "OTTER"         ""

*>>pas p 1
1: "OTTER"
2: ""

*>>
```

Figure 7.148 SEL-2032 PAS P Command

The **PAS P** command only shows child passwords for devices that have the corresponding Access Level 1 and/or Access Level 2 password in the communications processor startup string. To see the startup string for a child device, enter the **SHO A x** command, where *x* is a port on the communications processor.

QuickSet Warns “Unable to access port 0” When Connecting to an IED in a Communications Processor Scenario

If QuickSet responds with “Unable to access port 0” (see *Figure 7.149*), then ensure that the Global Device ID of the IED matches that used on the Connection Directory of the SEL-3620. You can view the SEL-3620 output in the QuickSet Terminal (activated with the <Ctrl+T> command) to verify the GDID of the IED in question.

Output			
Timestamp	Severity	Context	Message
6/14/2014 2:33:32 PM	✖ Error		Unable to access port 0.
6/14/2014 2:33:33 PM	✖ Error	Script Error	Script encountered an error. Please verify script contents.
6/14/2014 2:33:33 PM	ⓘ Info	GENERAL_362X_TERM...	Starting
6/14/2014 2:33:33 PM	ⓘ Info	SEL-3620_ETH_2032...	Disconnecting
6/14/2014 2:33:36 PM	ⓘ Info	SEL-3620_ETH_2032...	Disconnected
6/14/2014 2:33:36 PM	ⓘ Info	SEL-3620_ETH_2032...	Disconnecting
6/14/2014 2:33:36 PM	ⓘ Info	SEL-3620_ETH_2032...	Disconnected

Figure 7.149 QuickSet “Unable to access port 0” Message

Errors When Transferring Child IED Files Through the SEL-3620 Proxy

If you receive errors during file transfers through the SEL-3620 proxy from child IEDs, they are most likely attributable to the following causes:

- **No RTS/CTS:** For maximum link reliability, use hardware flow control between child IEDs and the communications processor parent. You will also need serial cables that support RTS/CTS signals (such as the SEL-C273A).
- **Incorrect time-outs:** Ensure that you have a TERTIME1 setting on the communications processor master port that is greater than 0, so that the communications processor does not trigger on the termination string while passing normal binary data through the communications processor master port. If you still receive errors, consider configuring a longer TERTIME1 setting on the communications processor master port (e.g., three seconds).
- **Using front COM port:** The front serial port on communications processors is incapable of using direct transparent mode for binary file transfers (Refer to *Direct Transparent Mode* in the SEL-2032 manual). If you are using the front COM port in an attempt to transfer files, use a different master port instead (COM Ports 1–16 or Ethernet Ports 17–18).

Errors When Connecting to a Child IED Through the SEL-3620 Proxy

If you receive errors while attempting to connect through the SEL-3620 proxy to child IEDs, they are most likely attributable to the following causes:

- **Error in the QuickSet Connection Directory:** It is possible that the SEL-3620 cannot connect to the child IED because of an error in the QuickSet Connection Directory settings. Check the IED Pass Through Port setting, Access and Terminate scripts, and the communications processor termination time-outs and termination strings.
- **The communications processor child IED port may be busy:** “Port Busy” errors messages are common on heavily loaded communications processors, or when another session is currently established to the port, or if the communications processor is attempting an autoconfiguration on the port. Wait a few minutes and attempt the connection again. If the problem persists, you can run the STA command and view the result for help with troubleshooting.
- **Child IED serial cable may be disconnected:** While rare, it is possible that the child IED serial cable may be disconnected. Try logging in to the communications processor and manually attempting to establish a tunneled connection to the IED.
- **Communications processor may be unresponsive:** Sometimes a heavily loaded communications processor will simply not respond to a command on the master port. It might require more than one attempt to connect to a child IED.
- **Communications processor SEL-2700 series Ethernet card may be unresponsive:** Quickly disconnecting then reconnecting to a communications processor SEL-2700 series Ethernet card may result in a “Service is not available” message (see *Figure 7.150*). To prevent fast disconnect/reconnect scenarios to the Ethernet-enabled communications processors from causing problems, you can create a custom Access Script on the communications processor with the code “SEL.Sleep(10)”, which will cause the SEL-3620 to pause for ten seconds before entering commands on the communications processor. Make sure to upload the Connection Directory with the new Access Script to the SEL-3620.

```
Direct Transparent Communications to Port 10 established

=QUIT
QUIT

SEL-787                               Date: 06/27/2014    Time: 07:11:13.955
TRNSFRMR RELAY                         Time Source: External

=
Direct Transparent Communications to Port 10 terminated

*> sent 0, rcvd 506
listening on [any] 7777...
192.168.10.20: inverse host lookup failed: Unknown host
connect to [192.168.10.177] from (UNKNOWN) [192.168.10.20] 50636

Service is not available at this time. try back later.
```

Figure 7.150 SEL-2700-Series Ethernet Card “Service is not available” Message

When Connecting to a Child IED, the Session Ends Up on the Wrong Child IED Prompt

If the SEL-3620 proxy session ends up on the wrong child IED prompt, this may be because of the following errors:

- **Communications processor termination time-out is incorrect:** If the communications processor termination time-outs are incorrect in the QuickSet Connection Directory, you may get “stuck” in a previous child IED tunnel session. Ensure that the TERTIME1 setting for the master port on the communications processor that you are using matches the First Delay Time setting on the communications processor in the QuickSet Connection Directory. It may be useful in some instances to increase the First Delay Time by one additional second beyond the TERTIME1 setting.
- **Communications processor termination string is incorrect:** If the communications processor termination string is incorrect in the QuickSet Connection Directory, you may get “stuck” in a previous child IED tunnel session.
- **Previous Child IED Termination Script:** If the 20XX_GENERAL_TERMINATE script is missing from the QuickSet Connection Directory for the previously connected child IED, you may get “stuck” in a previous child IED tunnel session.
- **Child IED Pass Through Port is incorrect:** Ensure that the child IED Pass Through Port is correct in the QuickSet Connection Directory.

Check your Connection Directory settings. If you are “stuck” in a Child IED proxy session, you can try the following fixes:

- Try entering binary mode by sending the break command to the SEL-3620 proxy (when connected via Telnet or SSH), and then manually sending the communications processor termination string (typically <Ctrl+D>).
- If you are unable to disconnect from the tunneled IED session by putting the SEL-3620 proxy in binary mode, you can attempt to wait for the time-out on the communications processor Pass Through Port to time out and disconnect the tunneled session.
- If there is no time-out set for the communications processor Pass Through Port, you have two options:
 - Manually log in to the communications processor master port and terminate the session by issuing the terminate string of the master port (typically <Ctrl+D>)
 - Log in to a different communications processor master port and issue the STA command to discern which port is currently blocked. You can then issue the TOGGLE x NOCONN command (where x is the port that is blocked) twice (once to terminate the active session of the port, and again to clear the NOCONN bit).

The SEL-3620 Proxy Gives an Error Message When Disconnecting From a Child IED

If the SEL-3620 proxy gives an error when terminating from a child IED to the proxy interface, this may be because of the following errors:

- **Communications processor termination time-out is incorrect:** If the communications processor termination time-outs are incorrect in the QuickSet Connection Directory, you may get “stuck” in a previous child IED tunnel session, which would cause the SEL-3620 scripting engine to show an error.
- **Communications processor termination string is incorrect:** If the communications processor termination string is incorrect in the QuickSet Connection Directory, you may get “stuck” in a previous child IED tunnel session, which also may cause the SEL-3620 scripting engine to show an error.

When Connecting to a Child IED, the Session Ends Up on the SEL Communications Processor Interface Instead

If the SEL-3620 proxy session ends up on the communications processor prompt instead of that of the child IED you selected, this may be because of the following errors:

- **Previous Child Access Script is not set:** If the 20XX_GENERAL_ACCESS script is missing from the QuickSet Connection Directory for the child IED, the SEL-3620 will not correctly tunnel to the child IED.
- **Child IED Pass Through Port is incorrect:** Ensure that the child IED Pass Through Port is correct in the QuickSet Connection Directory.

Ensure that all Connection Directory port settings are correct.

Password Change for the SEL Communications Processor Fails

If you receive a password change “failed” message when attempting to change communications processor and child IED passwords, you first need to know what type of password change failed. To determine this, examine the SEL-3620 system logs on the Syslog page.

Review previous sections for individual IED password change failure troubleshooting tips in addition to the ones below.

Note that you should always verify the SEL-3620 proxy Connection Directory by first connecting to and disconnecting from every child IED before running a password change attempt.

Child Password Update (CPU) Failure—Possible Causes

NOTE: If the parent device of a connected child device fails to store the password of that child device, the failure symbol will be indicated in the Last Operation Status column.

For easy troubleshooting of child password failures, use the **PAS P ALL** command to quickly check child passwords on the most recent firmware versions of communications processors.

- Most CPU failures are because of time-outs being set incorrectly. Ensure TIDLE (if connected by Ethernet) and master port TIMEOUT settings are set to at least 30 minutes.

NOTE: Updating SEL-2030 communications processors to R126-V1 or later and SEL-2032 communications processors to R115-V1 or later and setting the appropriate child password update script in the Connection Directory will alleviate most child password update issues.

- Sometimes a CPU failure may be because of heavily loaded communications processors being unable to process an autoconfiguration in a timely manner. This will cause the Connection Directory CPU script to fail.
- Older communications processor firmware can also contribute to CPU failures. If you receive consistent CPU failures after following all troubleshooting steps, check the communications processor firmware to ensure it is above version R108.
- CPU updates will fail if there is a password mismatch between the child IED and the SEL-3620 internal database. Ensure that passwords are matched correctly between the SEL-3620 and the child IED.
- In very rare instances, a complex password generated by the SEL-3620 could cause a startup string error on the communications processor during autoconfiguration. If the SEL-3620 randomly generates a password with a valid child IED command (e.g., ACC, CON, etc.), the generated password can cause issues when the communications processor attempts to run the startup string on the IED. You can check the startup string by using the **SHO A x** command on the communications processor, where *x* is the serial port of the communications processor connected to the child IED.

Other Password Change Failures

For other password change failures on IEDs or communications processors, review previous sections for individual IED password change failure troubleshooting tips in addition to the following:

- Sometimes a password change failure may be because of heavily loaded communications processors being unable to open a tunnel to a child IED. This will cause all child IED password change attempts to fail.
- Sometimes an Access Level C password will fail to change on a child IED. This is most likely because of a lack of hardware flow control between the communications processor and child IED. Ensure that you are using hardware flow control, and are using serial cables that support hardware flow control (such as the SEL-C273A cable).
- A password change can fail because the script engine received an unexpected prompt. To correct this, you can create custom password change scripts that set the device back to the Access Level 1 prior to each attempted password change (see *Figure 7.151*).

Script Name

Script Text

```
1 SEL.GotoLevel('ACC')
2 SEL.GotoLevel('2AC')
3 SEL.SetPassword('2AC',SEL._ProposedPassword(),'pas',['Changed'],['Invalid'])
```

Figure 7.151 Custom Password Change Script for SEL Communications Processor IEDs

Management of GE Devices

Introduction

This section details the following configuration and testing steps:

- General considerations for GE IED support
- Device Manager configuration for GE devices
- Proxy configuration and use for GE devices
- Password management for GE devices
- Troubleshooting

Password management should only be undertaken when the proxy is working as expected. If you still are encountering errors or are unclear about how the SEL-3620 manages IEDs, see *Troubleshooting* on page 7.105.

Assumptions for this section include the following:

- This example reuses the SSH SMP created in a previous section.
- You have GE's EnerVista Software installed and operational.
- You have a copy of the SEL-5827 Virtual Connect Client installed and operational. You can find this software on the SEL website. If you have difficulty locating this software, contact your local SEL representative.

Note: Ensure that you have SEL-5827 software version 1.3.0.0 or later.

Scenario Configuration

The following scenario shows the present configuration. You may replace the network addresses with your own, depending on your SEL-3620 network settings. The following example uses a GE UR T60 relay for testing. You may use your own GE IED connected to the SEL-3620 via an appropriate serial cable (such as a C387 connected to the front serial port of the GE device). Note that the use of the CAS is optional.

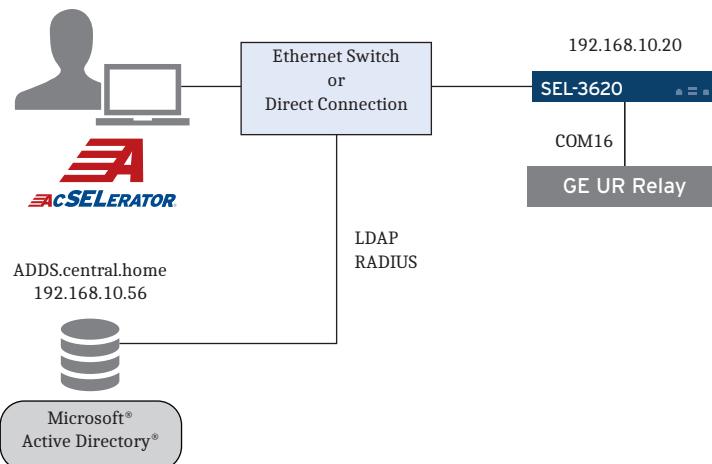


Figure 7.152 GE Password Management Network Diagram

General Considerations for SEL-3620 GE IED Support

It is important to know that SEL does not support all GE devices for proxy services and password management (see *Table 7.4*). SEL supports proxying Modbus RTU/TCP access from GE EnerVista software (or other GE software) to several different types of GE devices. SEL also supports password management for the GE UR series relays. Support for GE devices may vary depending on the endianness of the Modbus implementations, password change opcodes, and other factors. Ask your local SEL representative if you have questions about whether a particular GE device is supported by the SEL-3620.

Table 7.4 GE Product Support for Proxy and Password Management

GE Device	Proxy Services Supported	Password Mgmt. Supported
Multilin Series	Yes	No
UR Series	Yes	Yes
UR+ Series	Yes	Partial—custom scripts required
CyberSentry Series (GE Multilin series firmware 7.x and above)	N/A (RADIUS)	N/A (RADIUS)

There are also other considerations to know when using the SEL-3620 to manage GE device access and passwords:

- GE's EIA-232 front serial port is the DCE variant, rather than the typical DTE ports found on SEL devices. When connecting GE front serial ports to the SEL-3620, you will need to choose a straight-through cable (e.g., SEL-C387).
- Multidrop EIA-485 scenarios (multiple GE devices on the same serial port) have not been tested, and are not officially supported. SEL suggests testing any multidrop scenarios in the lab before any live implementation.
- Some GE UR devices only accept numbers in the passwords. More recent GE devices (UR+, etc.) accept both letters and numbers (CyberSentry versions accept the entire character space).

Finally, Modbus has a different protocol structure depending on if it is serial (Modbus RTU) or Ethernet (Modbus TCP). If the protocol is Modbus TCP, the Modbus address must be used in the TCP header. If the protocol is Modbus RTU, the Modbus address is in the serial frame. This means that Modbus TCP is not a serial message wrapped in a TCP packet. Instead, true protocol conversion has to happen. This is why it is important to know if the SEL-3620 is communicating via Modbus RTU or Modbus TCP to the end GE relay, and use either serial or Ethernet with SEL-5827, accordingly. Simply put, what the message starts with should be what it ends with (EnerVista and the relay should use the same format: if the relay uses serial, then use serial in SEL-5827, and vice-versa).

Device Manager Configuration of GE IEDs

This section will guide the user through configuring a GE IED in the QuickSet Device Manager. To do this, perform the following steps:

- Step 1. In the **Connection Explorer** window, right-click on **SEL-3620**, and select **Add > Device**. Scroll down to the bottom of the **Select Device Type** window and choose the GE relay (this example uses a GE T60) for the SEL-3620 to manage.
- Step 2. The GE IED will be added as a new device. Rename the IED to a different name (this example uses “GE T60”).
- Step 3. Expand the GE IED by double-clicking the template. Open the **Device** tab.
- Step 4. Select **Edit** and enter a matching **Global Device ID** (GDID) and **Device Name** (see *Figure 7.153*).

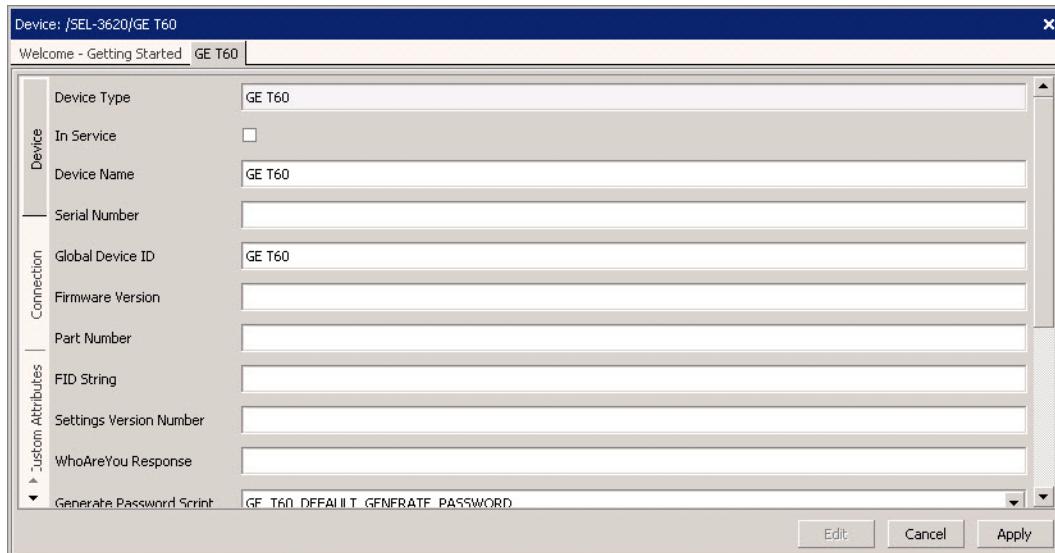


Figure 7.153 GE T60 Global Device ID

- Step 5. If the GE IED passwords are currently empty, you may edit the Password boxes for the **Command** and **Setting** passwords to add your password. GE UR passwords are typically “0” or empty by default.
Note: The SEL-3620 requires an initial password (the password cannot be empty).
- Step 6. Next, you need to edit the **Generate Password Script** and **Set Password Script** boxes to select the password management and application scripts defined in Device Manager. This example uses the following (default) scripts:
 - **Generate Password Script:**
GE_T60_DEFAULT_GENERATE_PASSWORD
 - **Set Password Script (Command):**
GE_T60_COMMAND_DEFAULT_SET_PASSWORD
 - **Set Password Script (Setting):**
GE_T60_SETTING_DEFAULT_SET_PASSWORD
- Step 7. Under the **Connection** tab, change the **Pass Through Port** to match the COM port that the IED connects to on the SEL-3620 (“16” in this case).

Step 8. Change the serial device characteristics to match those of the GE IED (see *Figure 7.154*). In this case:

- **Pass Through Port:** 16
- **Protocol:** Modbus RTU
- **Serial Interface:** EIA-232 (can also be EIA-422 or EIA-485)
- **Data Speed:** 9600
- **Data Bits:** 1
- **Parity:** None
- **RTS/CTS, DTS, RTS, and XON/XOFF:** Off
- **Unit ID:** 100

Step 9. Leave the other settings in the Connection tab with the default values.

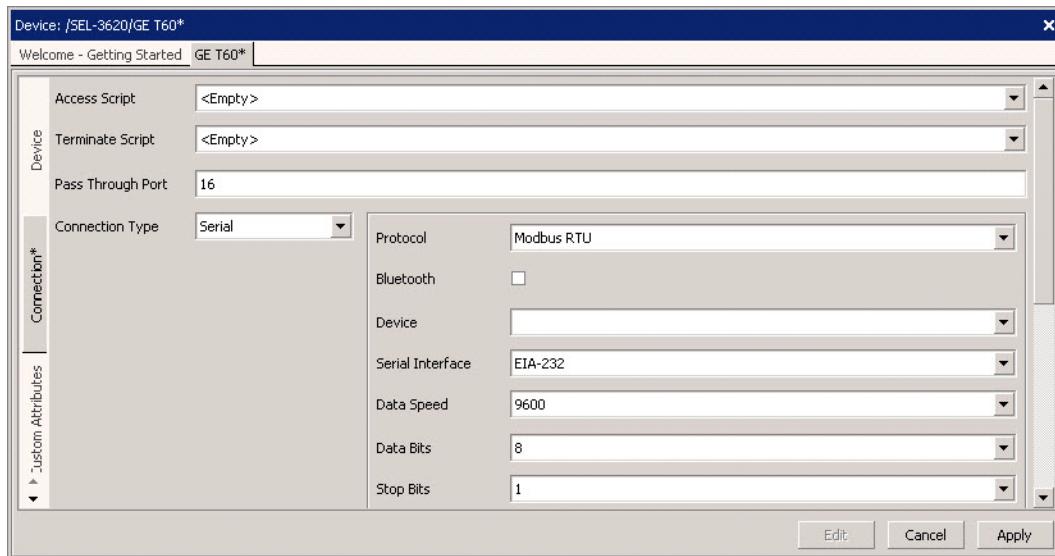


Figure 7.154 Serial GE T60 Connection Tab Parameters

Step 10. For Ethernet-connected GE IEDs, you will want to use the following settings (see *Figure 7.155*):

- **Pass Through Port:** 0
- **Host Protocol:** Raw TCP (does not matter)
- **Protocol:** Modbus TCP
- **Host IP Address:** the IP of the GE IED (in this case 192.168.10.60)
- **Port Number:** the TCP port of the GE IED (default is 502)
- **File Transfer Option:** does not matter
- **Unit ID:** 100

**7.116 | Proxy Services and Password Management
Management of GE Devices**

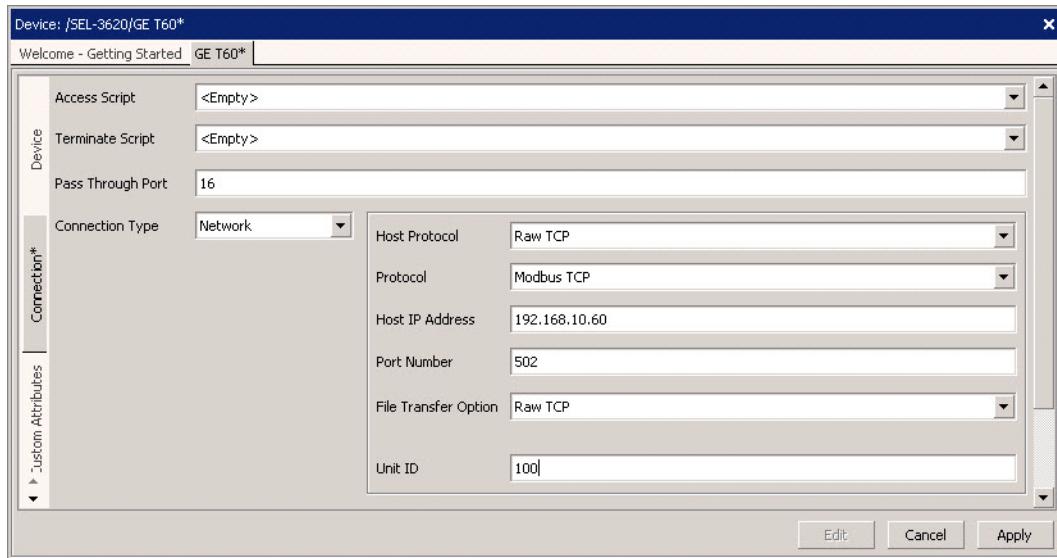


Figure 7.155 Ethernet GE T60 Connection Tab Parameters

Step 11. Under the **Permissions** tab, select **Add**, and select the Groups that you would like to give access to the GE IED (you may select multiple groups by holding the **<Ctrl>** key while selecting). Select **OK** when finished.

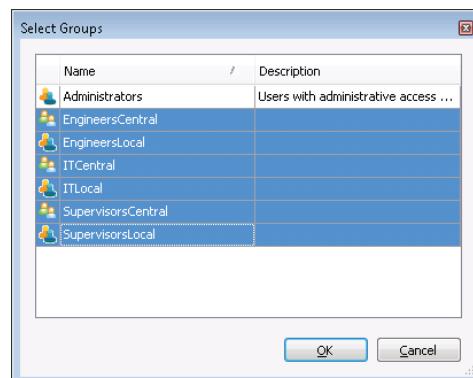


Figure 7.156 Selecting Groups on the IED Permissions Tab

Step 12. For each group, select the **Allow** check box on each GE authorization level (**Command** and **Setting**) to which you would like to give the respective group access. This example selects the following permissions:

- **Supervisors:** All permissions
- **Engineers:** All permissions
- **IT:** Connect only

Step 13. When finished, select **Apply**.

Step 14. In the **Connection Explorer** window, right-click on **SEL-3620** and select **Device Tasks > Send**. This will send the test Connection Directory to the SEL-3620. Ensure the upload completes without errors.

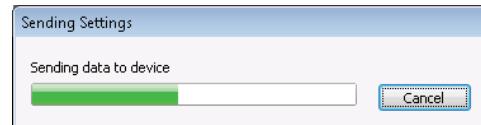


Figure 7.157 Uploading the Connection Directory to the SEL-3620

Step 15. Log in to the SEL-3620 web interface. Under **Reports**, in **System Logs**, verify that the SEL-3620 logs show that the Connection Directory was successfully uploaded.

SEL-3620 Proxy Configuration and Usage for Serial-Connected GE IEDs

This section will guide the user through proxying access to a serial-connected (Modbus RTU) GE IED through the use of GE EnerVista software and SEL-5827 Virtual Connect Client. To configure the SEL-3620 proxy for GE IEDs, follow these steps:

- Step 1. Open SEL-5827 Virtual Connect Client software, and select **Communications > Connect**.
- Step 2. Configure the following settings (see *Figure 7.158*):
 - **Virtual Port Settings:** Serial
 - **Port Number:** 100 (you may use others)
 - **MODBUS:** Check
 - **Connection Settings:** SSH
 - **Network Host name / IP:** 192.168.10.20 (this is the SEL-3620)
 - **TCP Port:** 22 (this is the SMP)
 - **Enable break on application connect:** Check (this sends the break command as soon as EnerVista connects to the virtual port).

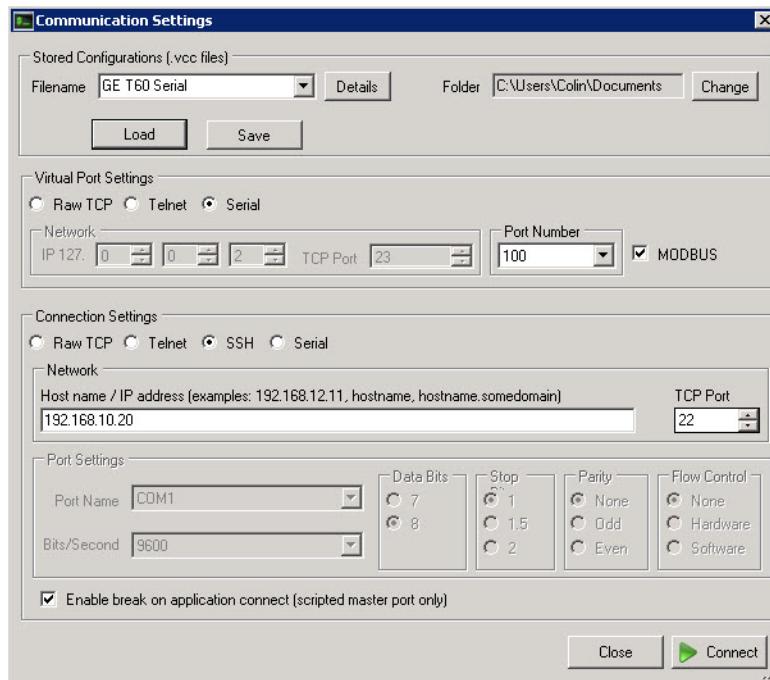


Figure 7.158 SEL-5827 Settings for Serial GE IED

Step 3. Select **Connect**. If you selected SSH as the Connection Settings, you should now see a window asking for your login information (see *Figure 7.159*). You may also see an **SSH Key** window display asking you to verify the remote SSH key. If you see this window the first time you connect to the remote SEL-3620, select **Continue**.

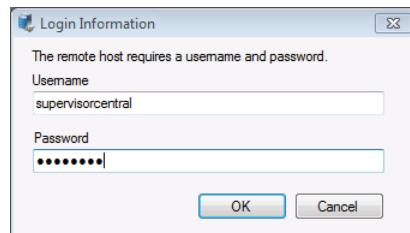


Figure 7.159 SEL-5827 Login Information Window

Step 4. You should now see **Connection: Connected** in the lower left-hand corner of the SEL-5827 window. You may now navigate the SMP as if you are using a normal terminal. Type **WHO** to find the available GE IED(s). Next, type **SELECT 1** to tell the SEL-3620 to connect to the GE IED interface (see *Figure 7.160*).

A screenshot of a terminal window titled "SEL-5827 Virtual Connect Client - 192.168.10.20:22". The window shows a system message about monitoring, followed by command history: "*who", "Available Devices: 1 GE T60", and "*SELECT 1". The cursor is at the end of the last command.

Figure 7.160 SEL-5827 Terminal Interface

Step 5. Next, open GE EnerVista Software, add a UR T60 IED (if you have not done so already), and open the UR setup window. Select **Device Setup** from the **Online Window** options (see *Figure 7.161*).

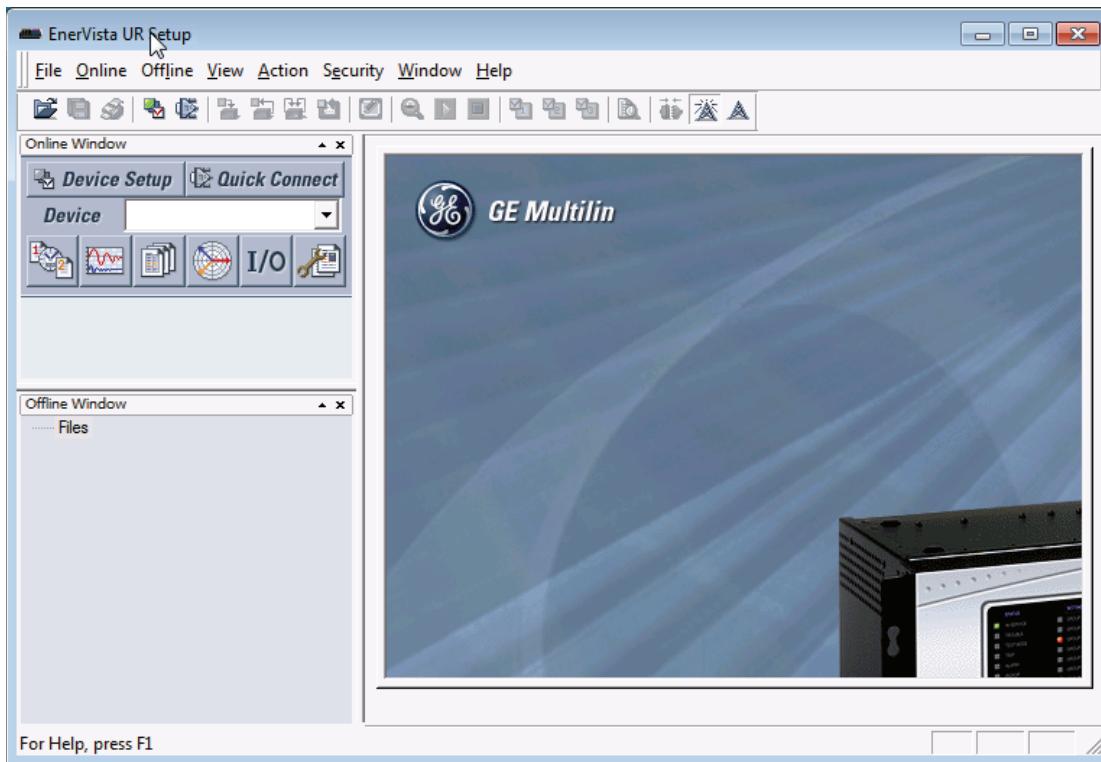


Figure 7.161 GE EnerVista UR Setup Window

Step 6. From the Device Setup window, add a new Site and a new Device (if you have not done so already). On the Device setup window, add the following information:

- **Device Name:** T60 (you can use another name)
- **Interface:** Serial
- **Slave Address:** 100 (matching the Unit ID in Device Manager)
- **COM Port:** 100 (use the virtual COM port configured in SEL-5827)
- All other settings can be default (see *Figure 7.162*)

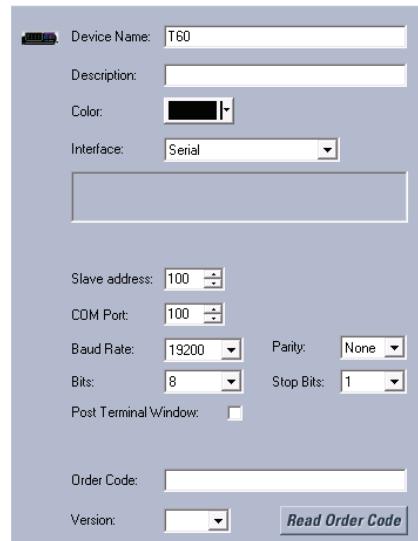


Figure 7.162 Device Setup Window

NOTE: When GE EnerVista Software accesses the SEL-5827 virtual communications port, the SEL-5827 screen should turn a blue color, indicating that virtual port is in use.

- Step 7. Select **Read Order Code**. At this point, GE EnerVista software should correctly read the Order Code from the IED. If this does not occur, or you get an error, see *Troubleshooting* on page 7.125.
- Step 8. To ensure that the connection to the GE IED through SEL-5827 and the SEL-3620 is fully connected, navigate to **Settings > Product Setup > Installation** on the GE IED, and check the Relay Settings status. If the GE IED has been commissioned, the status should say **Programmed** (see *Figure 7.163*). If not, then see *Troubleshooting* on page 7.125.

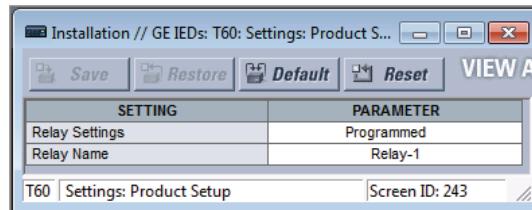


Figure 7.163 GE EnerVista Installation Status Window

- Step 9. You should now be able to communicate with the GE relay, including polling for data, downloading or uploading settings, etc. To disconnect the session, you can close out the device window, and disconnect SEL-5827 by selecting **Communications > Disconnect**.

SEL-3620 Proxy Configuration and Usage for Ethernet-Connected GE IEDs

This section will guide the user through proxying access to an Ethernet-connected (Modbus TCP) GE IED through the use of GE EnerVista software and SEL-5827 Virtual Connect Client. To configure the SEL-3620 proxy for GE IEDs, follow these steps:

- Step 1. Open SEL-5827 Virtual Connect Client software, and select **Communications > Connect**.
- Step 2. Configure the following settings (see *Figure 7.158*):
 - **Virtual Port Settings:** Raw TCP
 - **Network IP:** 127.0.0.1
 - **TCP Port:** 1060
 - **MODBUS:** Check
 - **Connection Settings:** SSH
 - **Network Host name / IP:** 192.168.10.20 (this is the SEL-3620)
 - **TCP Port:** 22 (this is the SMP)
 - **Enable break on application connect:** Check (this sends the break command as soon as EnerVista connects to the virtual port)

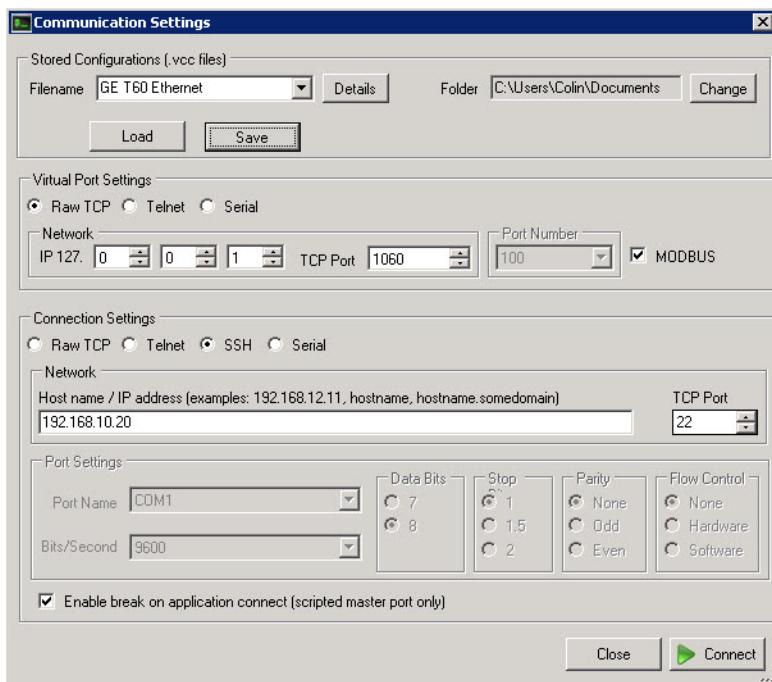


Figure 7.164 SEL-5827 Settings for Ethernet GE IED

Step 3. Select **Connect**. If you selected SSH as the Connection Settings, a window displays asking you for your login information (see *Figure 7.165*). You may also see an SSH Key window asking you to verify the remote SSH key. If you see this window the first time you connect to the remote SEL-3620, select **Continue**.

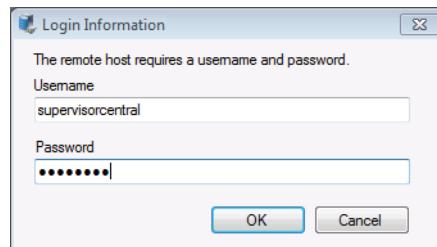


Figure 7.165 SEL-5827 Login Information Window

Step 4. You should now see **Connection: Connected** in the lower left corner of the SEL-5827 window. You may now navigate the SMP as if you are using a normal terminal. Type **WHO** to find the available GE IED(s). Then type **SELECT 1** to tell the SEL-3620 to connect to the GE IED interface (see *Figure 7.166*).

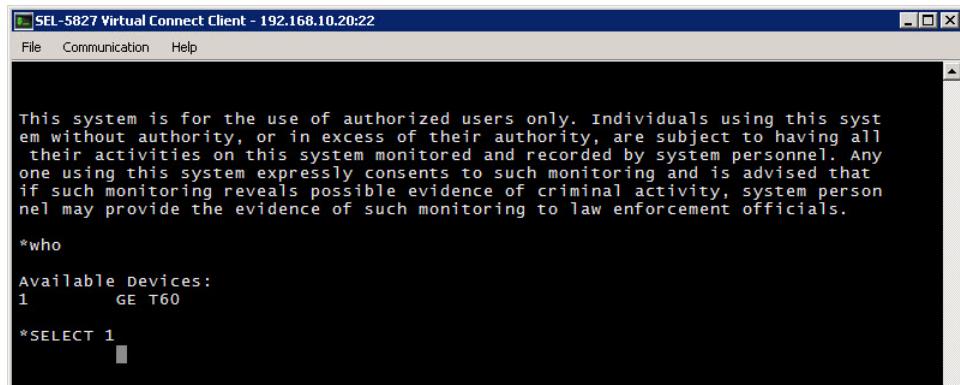


Figure 7.166 SEL-5827 Terminal Interface

Step 5. Next, open GE EnerVista software, add a UR T60 IED (if you have not done so already), and open the UR setup window. Select **Device Setup** from the **Online Window** options (see *Figure 7.167*).

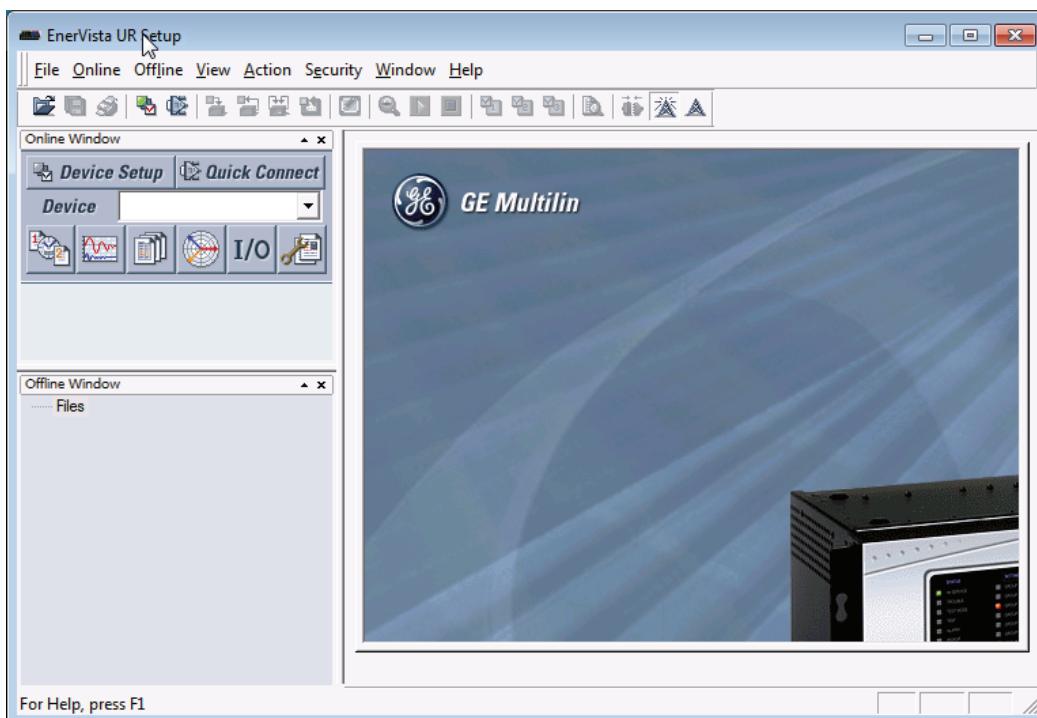


Figure 7.167 GE EnerVista UR Setup Window

Step 6. From the Device Setup window, add a new Site and a new Device (if you have not done so already). On the Device Setup window, add the following information (see *Figure 7.168*):

- **Device Name:** T60 (you can use another name)
- **Interface:** Ethernet
- **IP Address:** 127.0.0.1
- **Slave Address:** 100 (matching the Unit ID in Device Manager)
- **Modbus Port:** 1060
- **Connected via Ethernet / Serial Gateway:** No
- All other settings can be default

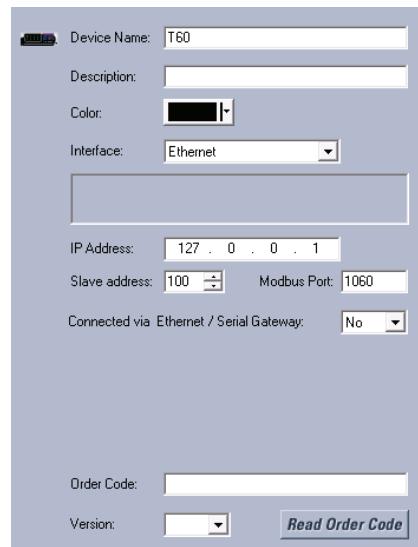


Figure 7.168 GE Device Setup Window

NOTE: When GE EnerVista software accesses the SEL-5827 virtual communications port, the SEL-5827 screen turns blue, indicating that virtual port is in use.

- Step 7. Select **Read Order Code**. The GE EnerVista software should correctly read the Order Code from the IED. If this does not occur, or you get an error, see *Troubleshooting* on page 7.125.
- Step 8. To ensure that the connection to the GE IED through SEL-5827 and the SEL-3620 is fully connected, select **Settings > Product Setup > Installation** on the GE IED, and check the **Relay Settings** status. If the GE IED has been commissioned, the status should say **Programmed** (see *Figure 7.169*). If not, see *Troubleshooting* on page 7.125.

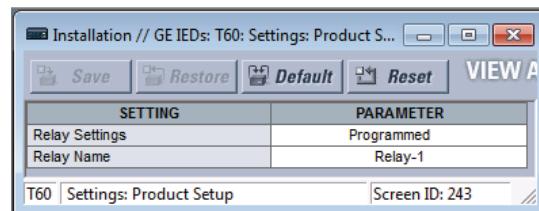


Figure 7.169 GE EnerVista Installation Status Window

NOTE: If prompted for a password, you may retrieve the current password from the Managed Devices Passwords report on the SEL-3620. To access this password, you must have administrative privileges in the SEL-3620.

- Step 9. You should now be able to communicate with the GE relay, including poll for data, download and upload settings, etc. To disconnect the session, you can close out the device window, and select **Communications > Disconnect** to disconnect the SEL-5827.

SEL-3620 Password Management for GE IEDs



See Safety Tips for SEL-3620 Password Management on page 7.54 before attempting to change any passwords.

To generate a new set of complex passwords for the GE IED, follow these steps:

- Step 1. On the SEL-3620 webpage, under the **Security** section of the navigation panel, select **Password Management**.
- Step 2. In the **Change All Passwords Now** (*Figure 7.170*) box, select **Generate** to generate passwords for the IED.

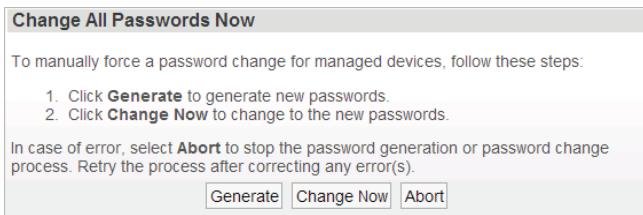


Figure 7.170 Change All Passwords Now Box

NOTE: You can halt the generation of passwords at any time by selecting **Abort** in the **Change All Passwords Now** box.

- Step 3. You should see the message **Password generation in progress** at the top of the page. After a moment, the message should change to **Passwords generated successfully**.

Navigate to **Proxy Reports** and generate a new Managed Device Passwords report. You should now see the Proposed Password column has been filled in with new complex passwords generated for the GE IED by the SEL-3620 (see *Figure 7.171*).

SCHWEITZER ENGINEERING LABORATORIES

Managed Device Passwords

Hostname: SEL2009280577
Created on 21/01/2014 by admin
Dates Covered: 2014-01-21 to 2014-01-21
Page 3 of 3

Managed Device Passwords

Device	Account	Current Password	Proposed Password	Next Change
GE T60	Command	0	3263990745	
GE T60	Setting	0	2933960448	

Figure 7.171 Managed Device Passwords Report With GE Proposed Passwords

Now that you have generated a new set of complex passwords for the IED, you can instruct the SEL-3620 to apply the new passwords to the GE IED. To perform this function, follow these steps:

NOTE: You can halt the changing of passwords at any time by selecting **Abort** in the **Change All Passwords Now** box.

- Step 1. On the **Password Management** page, in the **Change All Passwords Now** box, select **Change Now**.
- Step 2. You should see the message **Password change in progress** at the top of the page. This message will persist while the SEL-3620 is actively changing the GE IED passwords.
- Step 3. After a minute or so, you should see a **Password changed successfully** message. Navigate to the **System Logs** page to view the password change logs. For each password changed, the SEL-3620 will log either a failure or a success message. This is a good way of tracking the status of the password change operation while active (see *Figure 7.172*).

Time Stamp	Tag Name	Severity	Facility	Message
2014-01-21 17:23:41	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on GE T60
2014-01-21 17:23:39	ProxyServices	Warning	SYSTEM	Authentication Proxy: changed password(s) on GE T60
2014-01-21 17:23:36	ProxyConfig	Warning	USER	Authentication Proxy: password change initiated by admin at XXX.XXX.XX.XX

Figure 7.172 Password Change Syslogs for GE IED

Step 4. Navigate to the **Proxy Reports** page, and regenerate the Managed Device Passwords report. On the report, you should now see that the Current Passwords column has changed to what the Proposed Passwords were previously, and the Proposed Passwords column is now empty (see *Figure 7.173*).

Managed Device Passwords				
Device	Account	Current Password	Proposed Password	Next Change
GE T60	Setting	2747316217		
GE T60	Command	1958229502		

Figure 7.173 Managed Device Passwords Report With New Complex Passwords for GE IED

All other password management functions that the SEL-3620 can perform with SEL devices can also be done with GE IEDs, including Revert, Abort, and Manual Password Edits, Scheduler, and use of the SELF Controller. For more about how to use those functions, see the previous sections.

Troubleshooting

See previous sections for general password management troubleshooting tips. Not all GE devices are supported at this time (see *Table 7.4* on page 7.113). Talk to your local SEL representative if you have questions about supported GE devices.

GE EnerVista Software Fails to Connect

If GE EnerVista software fails to connect to the GE IED, check the following:

- Ensure that you are using SEL-5827 Virtual Connect Client Software, and that the virtual Ethernet TCP port of virtual serial port match the port you are attempting to connect to in EnerVista. When a service is connected to the SEL-5827 virtual port, the screen of SEL-5827 should turn blue. If you do not see this color change, this is an indication you are not using the right port from EnerVista.
- Ensure that SEL-5827 is connected to the SEL-3620 and that you have selected the correct IED from the SMP.
- Ensure that the SEL-5827 connection to the SEL-3620 SMP has not timed out.

GE EnerVista Software Connects But Gives Errors When Attempting to View or Access Settings

If the reliability of the connection is intermittent, ensure the **Enable break on application connect** check box is selected from within the SEL-5827 Communications window (see *Figure 7.174*), and that you are using SEL-5827 version 1.2.0.0 or later.

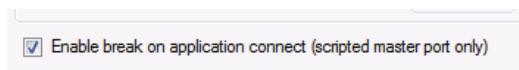


Figure 7.174 SEL-5827 Enable Break Option

The other cause of intermittent connection errors is mixing/matching Modbus RTU and Modbus TCP. If the end relay is connected to the SEL-3620 via Modbus TCP (Ethernet), then you must use an Ethernet virtual port with SEL-5827, and if the end relay is connected to the SEL-3620 via Modbus RTU (serial), then you must use a serial virtual port with SEL-5827. Read *General Considerations for SEL-3620 GE IED Support* on page 7.113 for an explanation of Modbus TCP and Modbus RTU differences.

GE Passwords Fail to Change After Password Change Initiated

If the GE relay passwords fail to change after a password change attempt, ensure that the GE relay has a password currently set. The SEL-3620 cannot change passwords on GE Multilin relays that have an empty (or null) password.

Password Management on SSH Devices

The SEL-3620 authentication proxy through the QuickSet Device Manager provides password management for Ruggedcom switches and other devices that require an SSH connection.

Navigate to the QuickSet Device Manager Device tab. Add SSH managed devices as you would add any device whose passwords you want to manage with the SEL-3620. See *Figure 7.175* for an example of adding a new SSH device. If the Ruggedcom template is not available for QuickSet, select SEL-587 for the Device Type field. Fill in the Device Name and Global Device ID fields with the appropriate values.

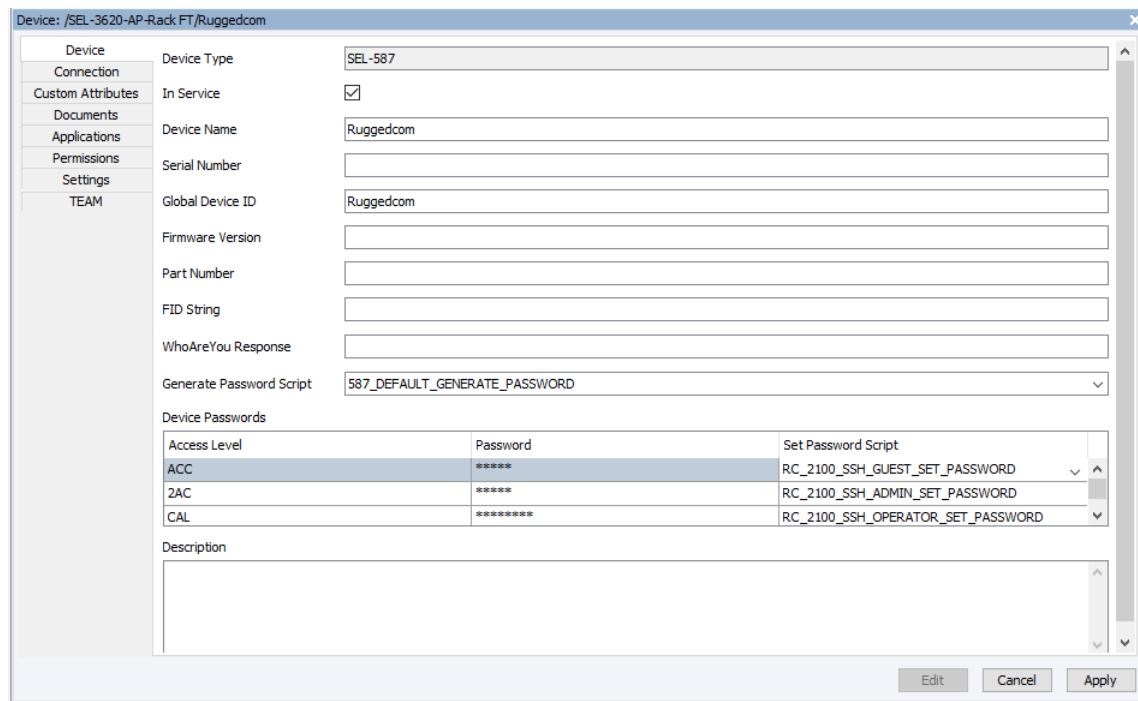


Figure 7.175 Add a New SSH Device to the QuickSet Device Manager

If you want the SEL-3620 to generate and change passwords for this device, you must create and upload a custom password generation script to the Device Manager. This will ensure that the SEL-3620 generates proper passwords for each access level and changes passwords correctly on the SSH devices. See *Figure 7.176* for an example password generation script for the admin user.

```
SEL.WriteLine("passwd admin " +  
SEL._ProposedPassword() ['2AC'], [>"], 15)  
SEL.LogMessage('<xml><Method>True</Method></xml>')
```

Figure 7.176 Example Password Generation Script for Admin User

NOTE: Although you can use identical scripts, you must have a separate script for each of the three Ruggedcom access levels: guest, admin, and operator. These access levels correspond to the SEL-3620 ACC, 2AC, and CAL access levels, respectively. You only need one Terminate script.

Custom access scripts are needed for each access level of the Ruggedcom switch. See *Figure 7.177* and *Figure 7.178* for example Access and Terminate scripts.

```
CR = "\x0d"  
SEL.Write(CR, ["Enter", "S-Shell"], 60)  
SEL.Write(CR, ["Main Menu", "S-Shell"], 10)  
SEL.Write("\x13", [>"], 10)
```

Figure 7.177 Example Access Script

```
SEL.WriteLine("logout", [], 0)
```

Figure 7.178 Example Terminate Script

QuickSet Device Manager allows us to configure a managed device connection with Telnet, Raw TCP, or SSH host protocols. To configure an SSH connection, navigate to the Connection tab and set the Host Protocol (file transport source) to **SSH** and the Credential Source to **Access Level** and **User Name**. You can then specify the user name for the SSH connection to select the desired access level. See *Figure 7.179* for an example of configuring a connection with the Ruggedcom admin user, which corresponds to the 2AC access level.

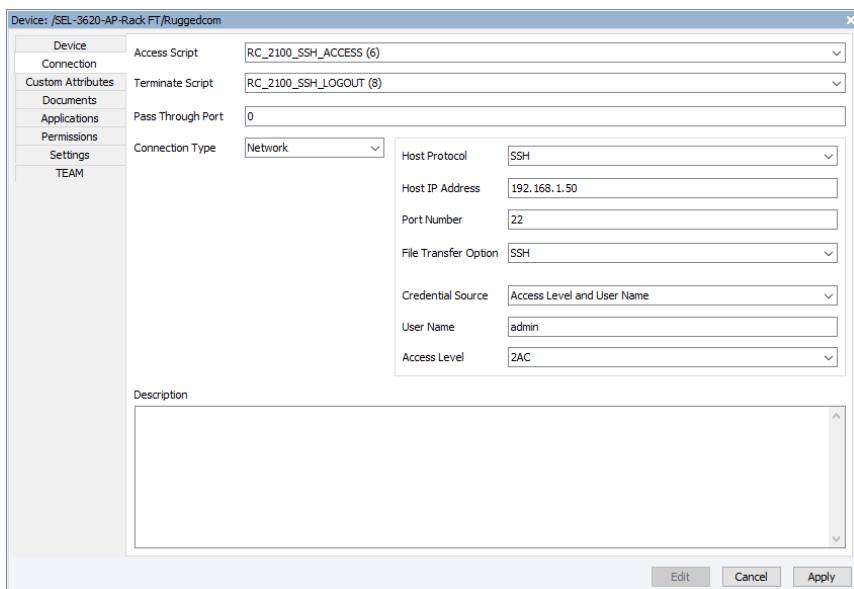


Figure 7.179 Configure an SSH Connection in the QuickSet Device Manager

SSH password-managed devices are displayed on the SEL-3620 user interface Password Management page along with the other password-managed devices.

Using TEAM With the SEL-3620 Proxy

Introduction

This section details the following configuration and testing steps:

- General considerations for TEAM support
- Device Manager configuration for TEAM polling of an SEL-3620
- Device Manager configuration for TEAM polling of IEDs through the SEL-3620 proxy
- Troubleshooting

Assumptions for this section include the following:

- You are reusing the SSH SMP created in a previous section.
- You have TEAM version 1.22.0.0 or later installed and operational.

Scenario Configuration

The following scenario shows the present configuration. You may replace the network addresses with your own, depending on your SEL-3620 network settings. This example uses an SEL-787 relay testing. You may use your own SEL IED connected to the SEL-3620 via an appropriate serial cable (such as SEL-C273A). Note that the use of the CAS is optional.

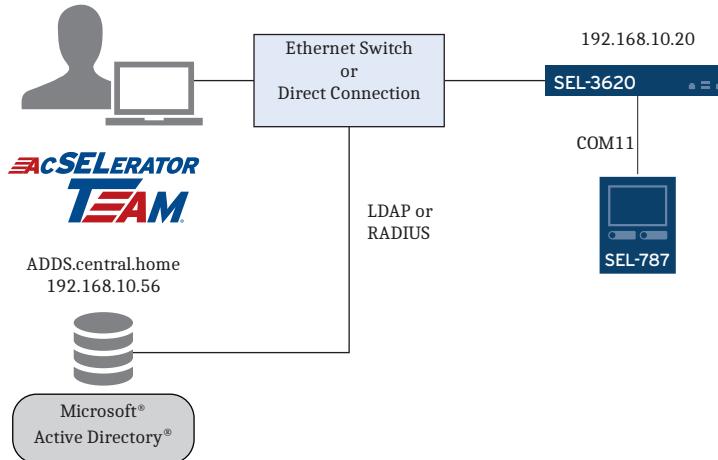


Figure 7.180 SEL-3620 TEAM Software Network Diagram

General Considerations for SEL-3620 and TEAM Software Interaction

The SEL-3620 supports TEAM for two types of scenarios:

1. TEAM gathering of SEL Password Management and Proxy reports (both PDF and JSON files) from the SEL-3620 Security Gateway itself.
2. TEAM Event Report polling of IEDs through the SEL-3620 proxy.

TEAM introduced support for SSH connection in version 1.22.0.0 of its DDC client, so use that version to avoid extra complication with TEAM's configuration and usage.

SEL strongly recommends that the TEAM software instance be installed on a completely separate physical or virtual Windows operating system instance from that used for configuring the SEL-3620 Connection Directories. Following this recommendation will help maximize the reliability and applicability of the TEAM software service.

This example assumes that there is already a licensed and functional TEAM instance already installed. For questions about installing TEAM, see the TEAM instruction manual, or contact your local SEL support person.

Configuring a New QuickSet Instance From a Backup Connection Directory

QuickSet supports importing/exporting the Connection Directory for easy commissioning of new QuickSet instances. The same import/export can be used to quickly commission a Team instance of an existing QuickSet Connection Directory.

To export an existing Connection Directory, see the following steps:

- Step 1. From an existing QuickSet Device Manager Connection Directory, right-click on **SEL-3620** in the left pane, and select **Export > Export to DMX** (see *Figure 7.181*).

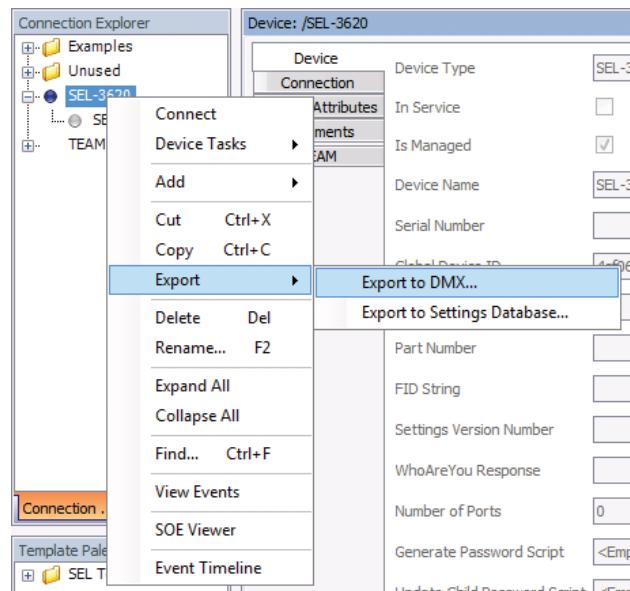


Figure 7.181 Exporting a QuickSet Connection Directory

- Step 2. Select the destination for the exported Connection Directory, and select **OK**. On the **Select Data** screen, select all check boxes that apply (see *Figure 7.182*), and select **OK**.

**7.130 | Proxy Services and Password Management
Using TEAM With the SEL-3620 Proxy**

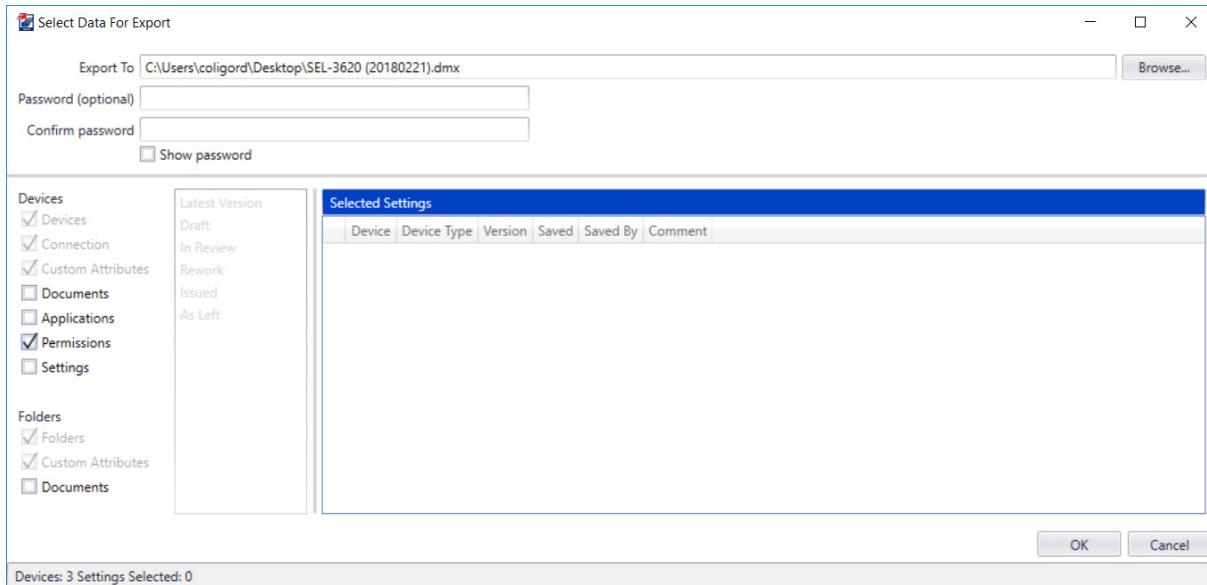


Figure 7.182 Connection Directory Export Select Data Window

You should now have an exported QuickSet Connection Directory DMX file on your desktop.

To import the exported Connection Directory into another QuickSet instance, see the following steps:

- Step 1. Copy the DMX file into the computer with QuickSet, and ensure the QuickSet instance has the current Device Manager plug-in installed.
- Step 2. Right-click in the **Connection Explorer** window, and select **Import > Import from DMX** (see *Figure 7.183*).

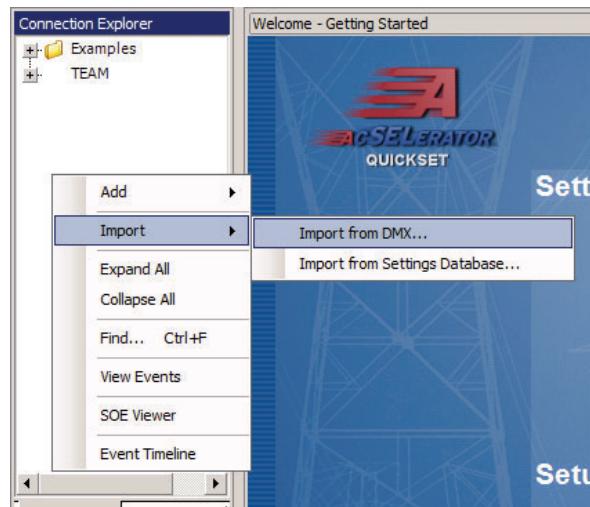


Figure 7.183 Import an Existing DMX File

- Step 3. Select the DMX file you exported previously, and on the **Select Data** window choose any data that you want to apply to this new QuickSet instance.
- Step 4. (Optional) Select **Configure Options** on the import dialog and select **Permissions** to import relay group permissions. See *Figure 7.184*.

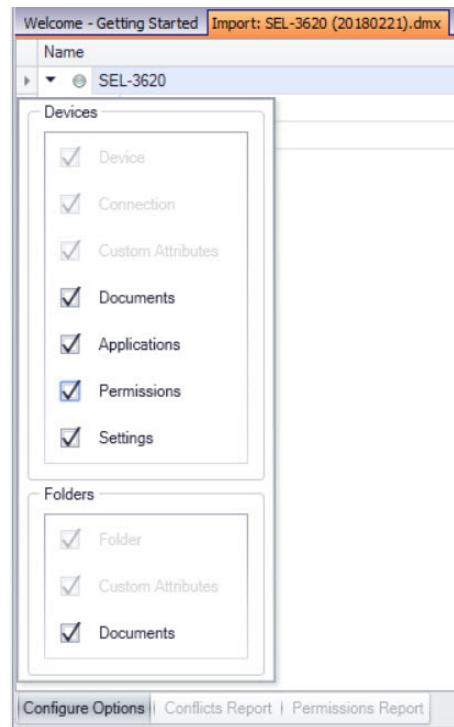


Figure 7.184 New Imported Connection Directory

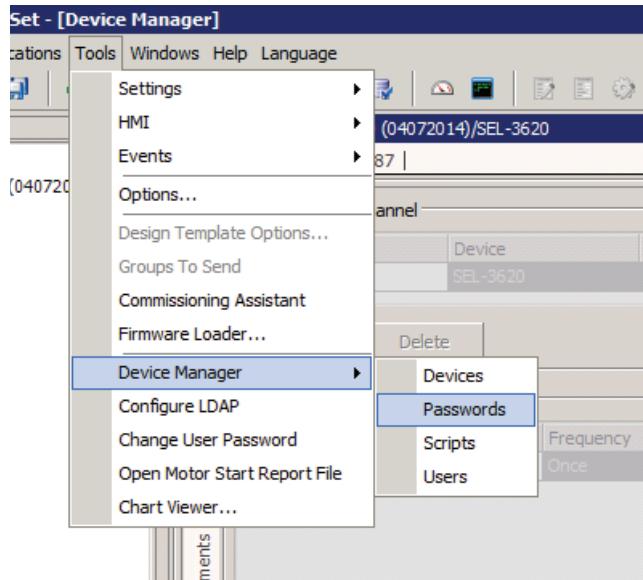
Collecting SEL-3620 Reports and Scheduling Password Changes via TEAM

The following sections require that TEAM has already been configured with appropriate DDC Connections and Archive Directories.

TEAM can be configured to gather Managed Device Passwords, Password Updates, and Commands and Devices reports (both PDF and JSON) from the SEL-3620 Security Gateway itself.

First, we need to configure a username/password combination to be used by TEAM when logging in to the SEL-3620:

- Step 1. In the QuickSet Device Manager, under the **Tools** menu, select **Device Manager > Password** (see *Figure 7.185*).



NOTE: You can configure a local administrative user ("TEAM") with password on the SEL-3620 by following directions from Initial Configuration on page 7.8. Whatever credentials used by TEAM to generate and download reports from the SEL-3620 require administrative privileges in the SEL-3620. However, the TEAM user does not need privileges on the SEL-3620 IED proxy for this particular function (if the TEAM account is used to gather reports directly from IEDs, then this privilege will be necessary).

Figure 7.185 Device Manager Passwords

- Step 2. Under the QuickSet Password Manager, right-click in the left pane, and select **Add > Password**. Type **TEAM** for the password.
- Step 3. Double-click the TEAM password. Enter your credentials for an administrative-level account on the SEL-3620. In the case of this example, there is a centralized user "TEAM" that has administrative privileges in the SEL-3620 (see *Figure 7.186*).

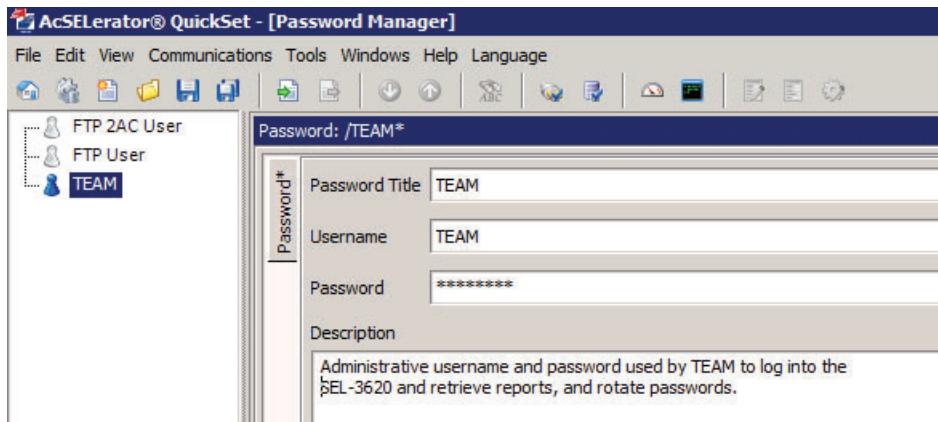


Figure 7.186 TEAM Username and Password

- Step 4. Select **Apply**. We strongly suggest checking the username and password by attempting to log in to the configured SMP with the TEAM username/password combination before continuing with the following steps.

To configure TEAM to gather reports from the SEL-3620, see the following steps:

- Step 1. Open the SEL-3620 device template in the Connection Directory (imported previously). Select the **Device** tab, and then select **Edit**, and ensure that the **In Service** check box is selected (see *Figure 7.187*).

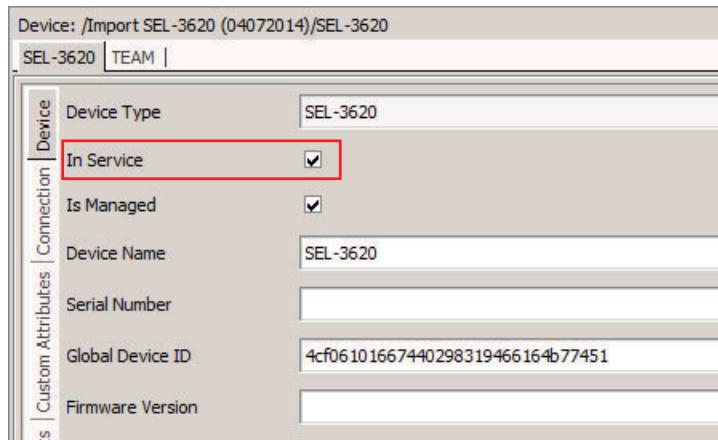


Figure 7.187 SEL-3620 In Service Check Box

- Step 2. Select the **TEAM** tab. Under **Communication Channel**, select **Add**. You will be prompted to go through the Server Configuration Wizard, during which you will need to select the appropriate host/service and network connection. You will need to ensure that you select a non-listening network connection (see *Figure 7.188*).

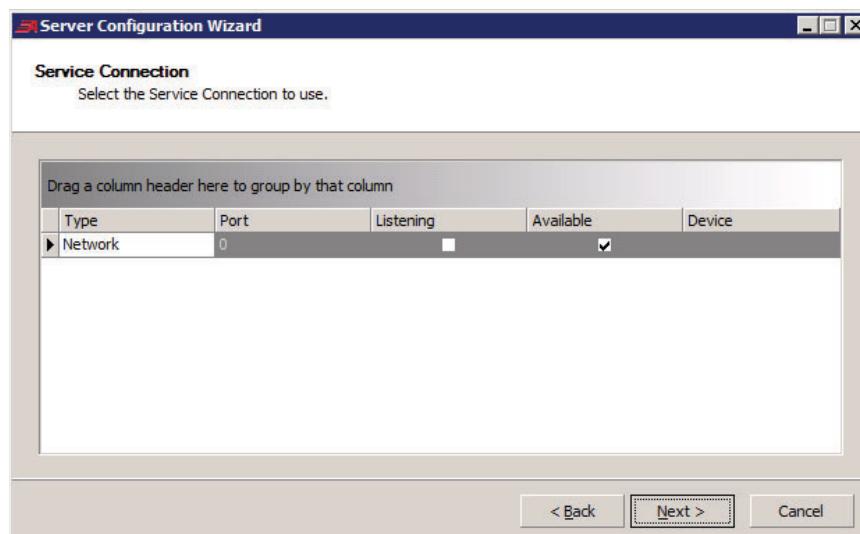


Figure 7.188 Select a Non-Listening Network Connection

- Step 3. When you have finished the Server Configuration Wizard, add a **Polling Job** and follow the Polling Job Wizard. The wizard will prompt you for the service and polling job type. For the job, select **3620 Log Collector Job** (see *Figure 7.189*).

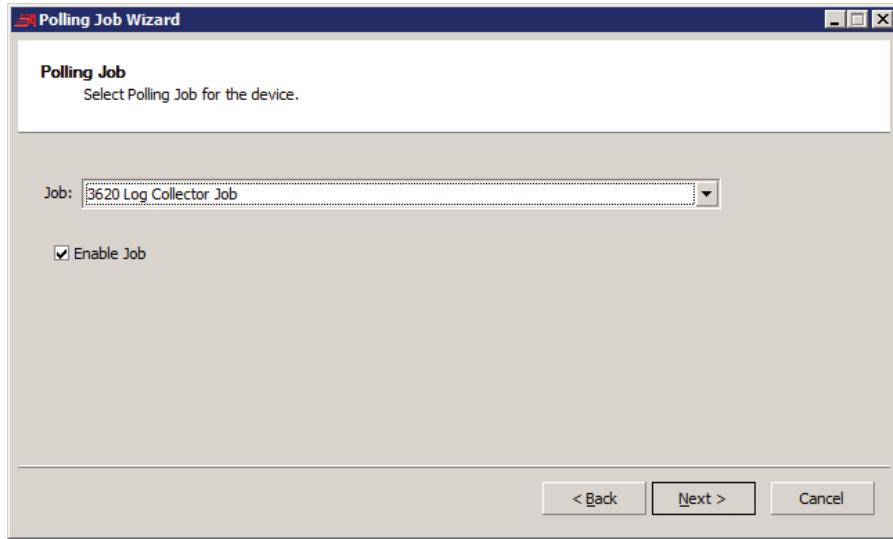


Figure 7.189 3620 Log Collector Job

Step 4. On the next screen (**Configure Job**), configure the following (see *Figure 7.190*):

- **3620 Database Credentials (Username / Password):** TEAM (previously configured user)
- **Generate and apply new passwords:** Unchecked

For testing, the **Generate and apply new passwords** box should be unchecked. However, you may choose to enable TEAM to generate and apply new passwords on a regular schedule. This will ensure that you always have the latest Managed Device Passwords reports, because they are collected by TEAM three times when it runs a password change job: immediately prior to generating new passwords, immediately after passwords are generated, and then again after passwords are changed on the IED.

- **Report Collection Data Range:** All- Collect all Event Reports

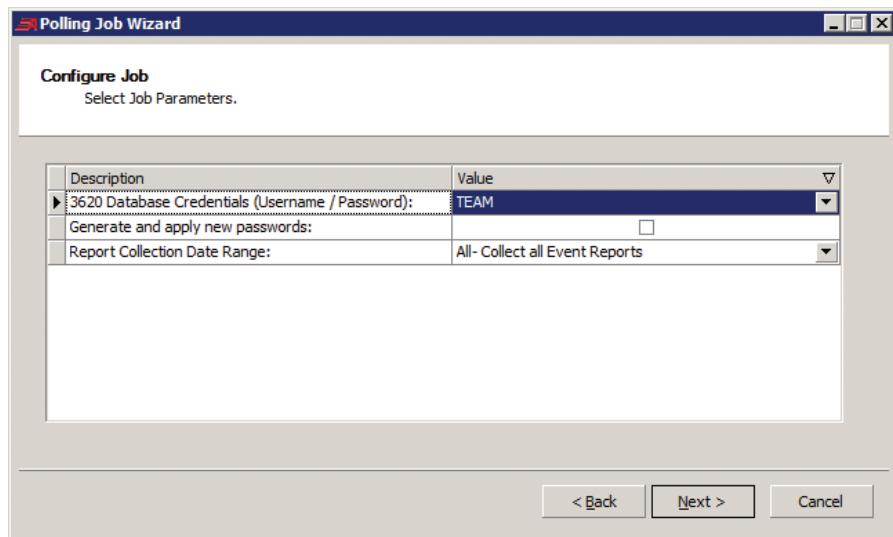


Figure 7.190 3620 Configure Job

Step 5. Select **Next**. On the **Polling Frequency** screen, you can select the schedule for which TEAM will grab reports (and possibly execute password changes) on the SEL-3620. For testing, we suggest using **Once**, and then selecting a schedule when the system commissioning is complete. Select **Next** to continue the wizard.

Step 6. If you have selected **Once**, then the next screen will be the Job Start Date. For testing, you can set this time to several minutes out (give yourself a buffer of four to five minutes; see *Figure 7.191*).

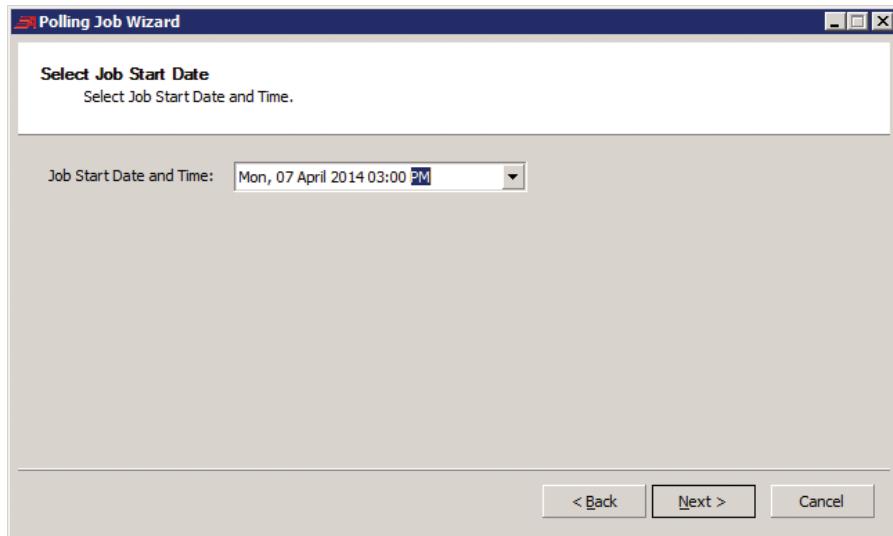


Figure 7.191 3620 Job Start Date

Step 7. Select **Next** and then **Finish** to complete the wizard. Select **Apply** on the SEL-3620 TEAM tab to lock in the TEAM changes you just made.

The process for TEAM will take five to ten minutes to complete once started (or longer, depending on how many events there are to generate). TEAM will save both PDF and JSON copies of the reports in the Events folder (initially configured during TEAM install) under the name of your SEL-3620 (“SEL-3620” in this example). See *Figure 7.192* for an example of the downloaded reports.

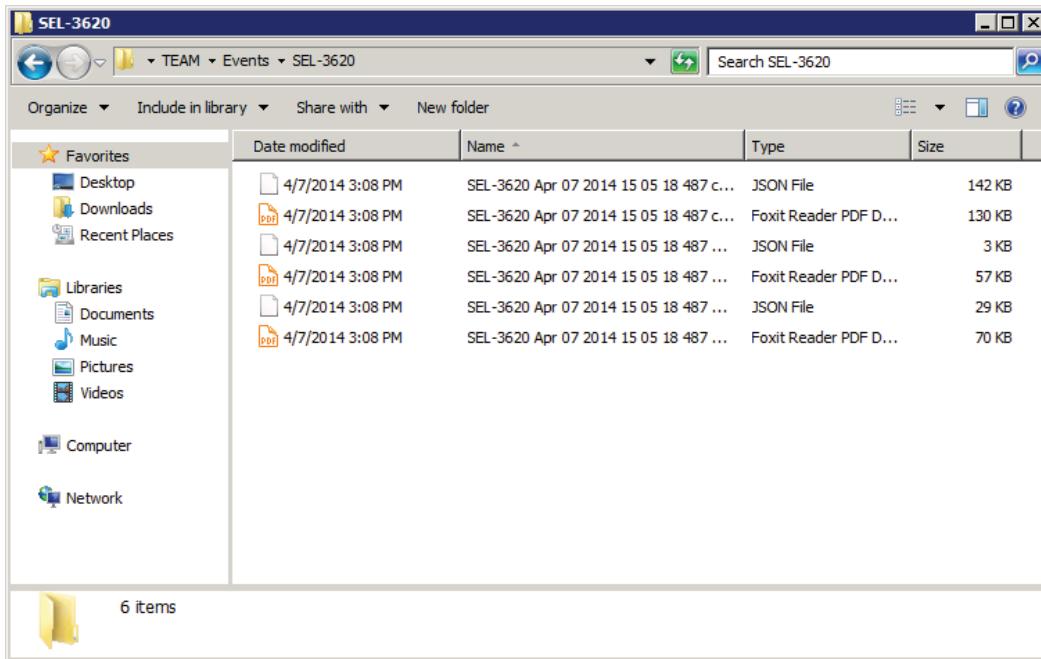


Figure 7.192 SEL-3620 Reports Folder

Collecting Event Reports From IEDs Through an SEL-3620 Proxy via TEAM

TEAM can be configured to collect Event Reports from IEDs by proxying through the SEL-3620 scripting-enabled master port. To perform this function, TEAM needs three things:

1. The SEL-3620 template needs to be configured to use a Titled Password as its credential source, and it must be configured to use the “General” SEL-362X Access and Terminate scripts.
2. A TEAM user that is a member of a local or central group that has Access Level 1 privileges (at minimum) on IEDs from which it needs to collect reports.
3. TEAM needs to be configured to poll a Default Event Collection job on the IEDs.

See the following steps to collect Event Reports from IEDs by proxying through the SEL-3620 SMP:

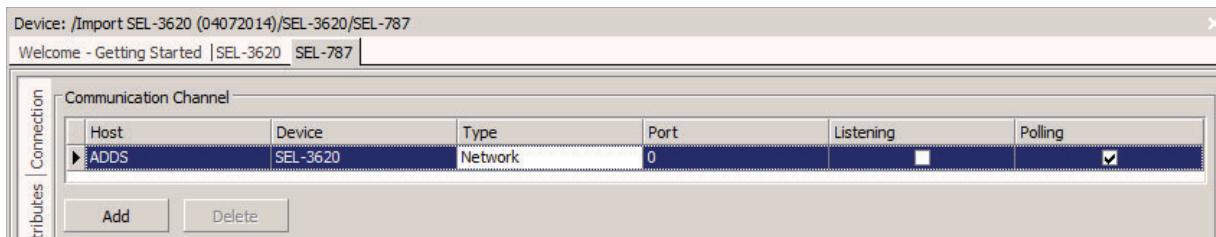
Step 1. Select the **Connection** tab of the SEL-3620 template used during the previous example. Ensure the following are configured (see *Figure 7.193*), and then select **Apply**:

- **Access Script:** GENERAL_362X_ACCESS_SCRIPT
- **Terminate Script:** GENERAL_362X_TERMINATE_SCRIPT
- **Credential Source:** Device Manager: Prompt; TEAM: Titled Password
- **Credentials:** TEAM (username and password from previous example)

Figure 7.193 SEL-3620 TEAM Configuration

The TEAM username and password used in the configuration will require authorization to access Access Level 1 of the SEL-787 relay. Our previous example added the TEAM user as a local user in QuickSet and in the SEL-3620, and added the TEAM user to the EngineersLocal group in the original QuickSet Connection Directory and on the SEL-3620. Ensure that you can successfully access the test IED with the TEAM credentials before continuing with this guide.

- Step 2. On the SEL-787 template, select the **Device** tab, and ensure that the **In Service** check box is selected.
- Step 3. On the SEL-787 IED TEAM tab, ensure that the Communication Channel from the previous section is already added (it should be inherited from the SEL-3620; see *Figure 7.194*).

**Figure 7.194 SEL-787 Team Tab Inherited Communication Channel**

- Step 4. Under Polling Jobs, Add a new job. During the Polling Job Wizard, ensure that **SEL Default Event Collection Job** is selected, and that the **Enable Job** check box is selected (see *Figure 7.195*).

**7.138 | Proxy Services and Password Management
Using TEAM With the SEL-3620 Proxy**

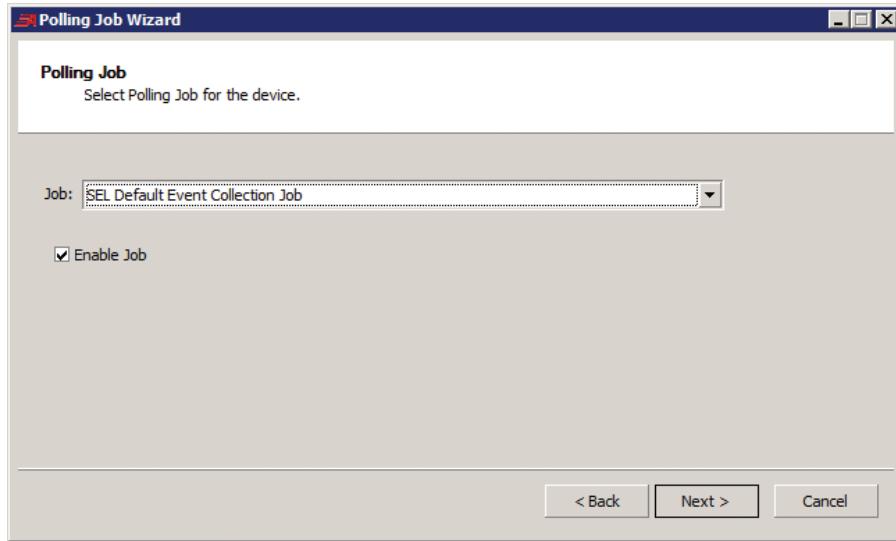


Figure 7.195 SEL Default Event Collection Job

- Step 5. Select **Next**. On the Polling Frequency screen, you can select the schedule for which TEAM will grab reports on the SEL-787 IED. For testing, we suggest using **Once**, and configuring a schedule later when the system commissioning is complete. Select **Next** to continue the wizard.
- Step 6. If you have selected **Once**, then the next screen will be the Job Start Date. For testing, you can set this time to several minutes out (give yourself a buffer of four to five minutes).
- Step 7. Select **Next**, and then **Finish** to complete the wizard. Select **Apply** on the SEL-787 IED TEAM tab to lock in the TEAM changes you just made.

The process for TEAM will take five to ten minutes to complete once started (or longer, depending on how many events there are to generate). TEAM will collect the IED event reports and store copies in the TEAM Events folder (initially configured during TEAM install) under the name of your SEL IED (“SEL-787” in this example). See *Figure 7.196* for an example of the downloaded reports.

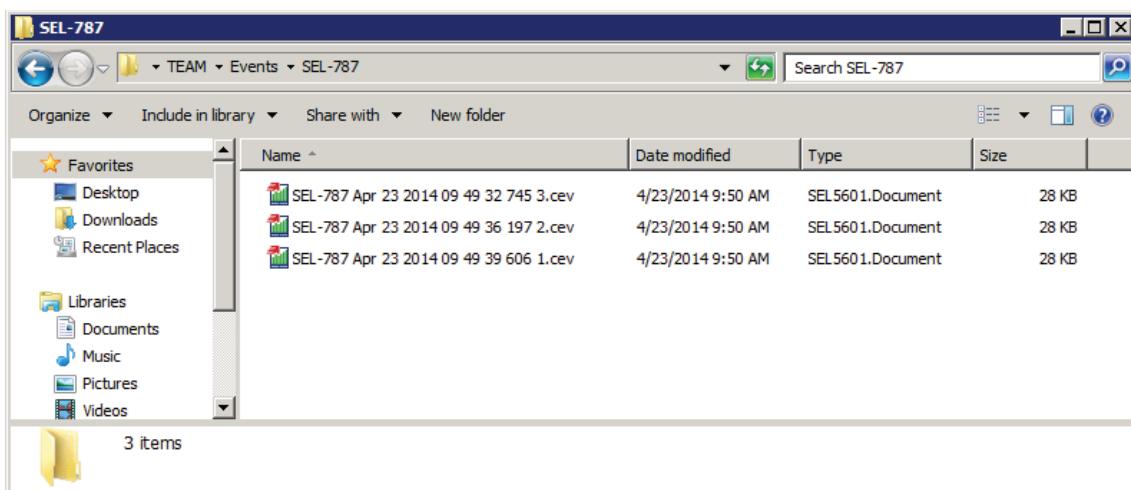


Figure 7.196 SEL-787 Reports Folder

Troubleshooting

When troubleshooting or commissioning TEAM software, you may manually start and stop the service in debugging mode. To use TEAM in debugging mode, see the Troubleshooting section of Application Guide AG2013-06, *Event Collection From SEL-3530 RTAC Using ACCELERATOR TEAM*.

Also ensure that the **Enable Logging** check box is selected on the TEAM configuration. It is useful to be able to keep records of TEAM's attempts to access the SEL-3620 scripting-enabled master port for troubleshooting (see *Figure 7.197*).

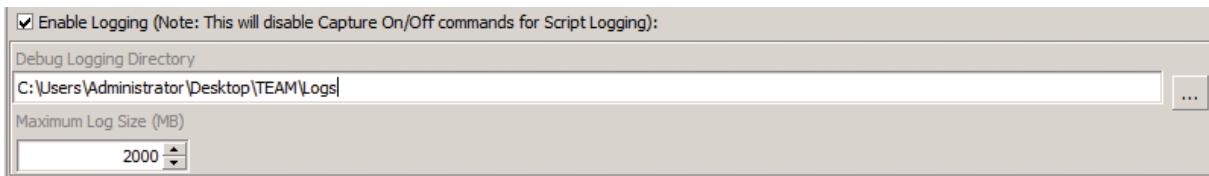


Figure 7.197 TEAM Logging Directory

TEAM Cannot Connect via SSH to the SEL-3620

If TEAM seems unable to connect to the SEL-3620 via SSH, ensure that QuickSet has accepted and remembered the SEL-3620 SSH public key. If this is the first time that QuickSet or TEAM has connected to the SEL-3620, right-click on an IED below SEL-3620 and select **Connect**, and then accept and trust the SSH public key that presents itself.

Error on Connection Directory Import Into QuickSet

If you receive an error while attempting to import a DMX file into QuickSet, ensure the QuickSet version of the QuickSet instantiation from which you exported the DMX file matches that of the QuickSet instantiation to which you are attempting to import.

TEAM Is Not Able to Download Reports From the SEL-3620 or From Proxied IEDs

If TEAM is not able to download reports from the SEL-3620 or from proxied IEDs, ensure that the TEAM username/password combination has sufficient privileges on the SEL-3620. The username/password used by TEAM for report generation and collection on the SEL-3620 requires administrative privileges in the SEL-3620. For a collection of reports from an IED below an SEL-3620, the TEAM username/password is required to be a member of a group that has (at minimum) Access Level 1 access on the SEL-3620.

Check your SEL-3620 system logs to see if you are receiving authentication attempts on your SMP. This can be an indicator that the TEAM username/password is incorrect.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

S E C T I O N 8

Testing and Troubleshooting

Introduction

This section provides guidelines for testing and troubleshooting the SEL-3610, SEL-3620, and SEL-3622. Except as otherwise noted, references to the SEL-3620 refer also to the SEL-3622.

- *Testing Philosophy* on page 8.1
- *LED Indicators* on page 8.2
- *Diagnostics Page* on page 8.4
- *Troubleshooting* on page 8.5
- *Technical Support* on page 8.8

Testing Philosophy

Device testing can be divided into three categories: acceptance, commissioning, and maintenance testing. The categories are differentiated by when they take place in the life cycle of the product and by test complexity. The following paragraphs describe when you should perform each type of test, the goals of testing at that time, and the functions that you need to test at each point.

This information is intended as a guideline for testing a device.

Acceptance Testing

Perform acceptance testing when qualifying a device for use in an IP-based communications network that requires encryption.

Goals of Acceptance Testing

- Ensure that the device meets published critical performance specifications.
- Ensure that the device meets the requirements of the intended application.
- Improve your familiarity with device capabilities.

What to Test

Acceptance test all settings parameters critical to your intended application.

SEL performs detailed acceptance testing on all SEL-3610/SEL-3620 models and versions. It is important for you to perform acceptance testing on an SEL-3610/SEL-3620 if you are unfamiliar with device operating theory or settings. Such testing helps you ensure that the device settings are correct for your application.

Commissioning Testing

Perform commissioning testing when installing a new device.

Goals of Commissioning Testing

- Ensure that power connections are correct.
- Ensure that the alarm output connection is correct.
- Ensure that the device functions with your settings according to your expectations.

What to Test

Perform commissioning testing on all connected Ethernet ports, serial ports, IRIG ports, and alarm contacts.

SEL performs a complete functional check of each device before shipment. Device commissioning tests should verify that the power supply, Ethernet cables, serial cables, IRIG cables, and alarm contacts are connected properly.

Maintenance Testing

The device requires minimal maintenance testing. Verification of the expiration dates of internally stored X.509 certificates can prevent loss of communication because of expired certificates.

LED Indicators

The device has extensive self-test capabilities. You can determine the status of your device with the LED indicators located on the front panel. These indicators are mirrored on the User Interface Dashboard.

The device monitors IPsec VPN status for availability of the IPsec service, and the number of current IPsec connections. These can be used to determine if there are communications channel problems.

The device also monitors the UP/DOWN state of Ethernet interfaces on the User Interface Dashboard for quick connection troubleshooting. Serial and Ethernet devices within Port Mappings have easy-to-access diagnostic information that includes connection state and error detection.

The device monitors the status of its internal logs. This provides a method to determine if there is unwanted activity on the device and to maintain the integrity of the internal logs.

SEL-3610/SEL-3620 LED Indicators

The device has several LED indicators. Descriptions of these LED indicators are in *Table 8.1* and *Table 8.2*.

The LED indicators found in *Table 8.1* are located on the device front panel next to the **Lamp Test** button. These indicators are not mirrored on the web management interface Dashboard page.

Table 8.1 System LED Indicators

Indicator Light	Green Condition	Red Condition
Enabled	Normal operations	System is halted, system is booting, or an error condition has occurred.
Alarm	N/A	When the alarm contact triggers or watchdog timer expires.

The LED indicators found in *Table 8.2* are located on the device front panel and are mirrored on the User Interface Dashboard.

Table 8.2 Subsystem LED Indicators

Indicator Light	Green Condition	Red Condition	Off Condition
VPN SYNC	The VPN functionality is available and not configured, or available and all host-host and net-net SAs of all configured VPN tunnels have been established	The VPN functionality is available, but not all host-host and net-net SAs of all configured VPN tunnels have been established	The device does not use IPsec, or IPsec is disabled
TIME SYNC	System time is synchronized with an external source	System time is configured, but not synchronized with an external IRIG-B or NTP source	There is no configured time source
X.509 ERROR	The system is running without the default X.509 certificate, and all configured X.509 certificates are currently valid (not expired)	The system is running with the default X.509 certificate, or if any configured X.509 certificates have expired	N/A
LOG WARN	The Syslog message queue is not in the warning state	Unacknowledged messages comprise >65% of the Syslog message queue	N/A
LOG ERROR	The Syslog message queue is not in the error state	Unacknowledged messages comprise >80% of the Syslog message queue	N/A
SYS ERROR	The device is operating normally	A system flash memory partition is more than 90% full, or the password jumper is currently installed	N/A
USER ACTIVE	A user session is active on the web management port or a master port	N/A	There is no active user session on the device web management server or master port
USER LOCK	The device is operating normally	One or more accounts is in the lockout state as a result of repeated invalid login attempts.	N/A
FILE IMPORT	The device is operating normally	The device is processing a firmware upgrade, system settings file import, or connection directory import (SEL-3620 only).	N/A

SEL-3622 LED Indicators

The SEL-3622 has fewer LED indicators and because of space limitations, they are labeled differently. In particular, the LOG and the USER lights operate differently than the corresponding indicators on the SEL-3620.

The LED indicators found in *Table 8.3* are located on the device front panel. These indicators are not mirrored on the web management interface Dashboard page.

Table 8.3 System LED Indicators

Indicator Light	Green Condition	Red Condition
EN	Normal Operations	The device is halted or booting, or an error condition has occurred
AL	N/A	The alarm contact has triggered or the watchdog timer has expired

The LED indicators found in *Table 8.4* are located on the device front panel and are mirrored in the web management interface Dashboard page.

Table 8.4 Subsystem LED Indicators

Indicator Light	Green Condition	Red Condition	Blinking Condition
VPN	VPN function is enabled and not configured, or enabled and all configured VPN tunnels have been established	VPN function is enabled and not all configured VPN tunnels have been established	N/A
CERT	The system is running with an X.509 certificate other than the default, and that certificate is not expired	The system is running with the default X.509 certificate, or a configured certificate is expired	N/A
LOG	The Syslog message queue is in neither warning nor error state	The Syslog message queue is in the error state	The Syslog message queue is in the warning state (blinks red)
SYS	The device is operating normally	A system flash memory partition is more than 90 percent full, or the password jumper is installed	N/A
USER	A user is active on the web management interface or a master port (serial or Ethernet)	A user account is in lockout as a result of repeated invalid login attempts	N/A
FILE	The device is operating normally	The device is processing a firmware upgrade, a setting file import, or connection directory import	N/A

Diagnostics Page

While the device status LED indicators are useful for getting status information at a glance, they will only alert you to normal vs. abnormal operating conditions. For more detailed diagnostics information, visit the Diagnostics page by selecting the **Diagnostics** link from the navigation panel.

There are five actions provided by the Diagnostics page.

- Update Diagnostics
- Halt System
- Reboot System
- Lamp Test (SEL-3622 only)
- Ping Host

Update Diagnostics

Select **Update Diagnostics** to populate the Diagnostics page with detailed information about the device. Before examining the diagnostics output, be sure to refresh the diagnostics information by selecting the **Update Diagnostics** button.

Halt System

⚠️ WARNING

The Halt System function should only be used in emergencies. If this feature is used, the only way to restore the unit to service is to physically cycle the power applied. This requires physical access to the unit.

The Halt System function exists to provide a method to stop dangerous traffic from traversing the device. If a local or remote network that communicates through the device has been compromised, the Halt System function will prevent the other network from being compromised as well.

Reboot System

The Reboot System function provides a method to remotely power cycle the device.

Lamp Test

The **Lamp Test** button is only available on the SEL-3622 Diagnostics page. Select **Lamp Test** to cycle through and flash the LEDs on the front panel of the SEL-3622. Use this function to ensure that all LEDs are operating correctly.

Ping Host

With firmware version R202 and above, the device can ping a host for quick troubleshooting purposes. Select **Ping Host** to display the option to enter the IP address of a host device that you want to ping. When executing the ping host function, the device will send three ICMP echo request packets to the IP address destination. If any positive replies are received within five seconds, the device will report **Host is up** (see *Figure 8.1*). If no replies are received, the device will report **Host is down**.



Figure 8.1 Successful Ping Host

Troubleshooting

Inspection Procedure

Complete the following procedure before disturbing the device. After you finish the inspection, refer to *Table 8.5*.

- Step 1. If the web interface is accessible, update and record the diagnostics from the diagnostics page.
- Step 2. Measure and record the power supply voltage at the power input terminals.
- Step 3. Record the state of the light indicators.

Table 8.5 Troubleshooting Procedure (Sheet 1 of 2)

Problem	Possible Causes	Solution
The Enabled/EN indicator light is dark.	Input power is not present.	Verify that input power is present.
The X.509 Error/CERT indicator light is red.	The device still has security-related default configurations that should be changed.	Generate and assign a new certificate for the web server.
VPN SYNC/VPN indicator light is red.	A VPN cannot be established because the peer is not present.	Verify that the peer gateway is turned on and working properly.
	A VPN cannot be established because there is no network path between the two peers.	Verify that routes exist between the two Ethernet gateways.
	A VPN cannot be established because there is a configuration error on one or both of the peers.	Verify the configuration of both peer devices.
	A VPN tunnel is only partially established.	Configure the peer device for a host-to-host connection between the two gateways.
The Login page is inaccessible.	Input power is not present.	Verify that input power is applied.
	HTTP connections to the device are being attempted to port 80.	Prefix the IP address with https:// in your web browser.
	The computer trying to connect to the web interface is not on the correct network.	Configure the IP address of the management computer to the same network as the device.
	The computer trying to connect to the web interface is not in the allowed web clients list.	Install the password jumper and use the front Ethernet port as a management port.
	Network errors are preventing communication.	Verify the physical and logical connections between the management computer and the device.
A user cannot log in.	The user's account has been locked because of repeated incorrect passwords.	If the user's account is centrally managed, have an administrator unlock the user's account, or, if the domain lockout policy provides for a lockout interval, wait for the lockout interval to elapse.
	The user's password is incorrect.	An administrative user must change the password.
An administrative user cannot log in.	The administrative user's account has been locked because of repeated incorrect passwords.	If the administrative user's account is centrally managed, have an administrator unlock the user's account, or, if the domain lockout policy provides for a lockout interval, wait for the lockout interval to elapse.
	The administrative user's password is incorrect.	Have another administrative-level user change the password, or install the password jumper.
LDAP connection to LDAP server fails.	An LDAP host entry has not been made.	Configure the hostname and IP address of the LDAP server in the Hosts section of the device web configuration page, and ensure it matches the LDAP server in the LDAP settings page.
	Proper X.509 certificates are not installed.	The certificate chain of the LDAP server must be present on the device. In most cases, the root CA certificate imported into the SEL device is enough for LDAP to function correctly.
	X.509 certificate date range is no longer valid.	Check the validity date range of the X.509 certificate current installed for LDAP functionality, and make sure the current date of the SEL device matches the validity period.
Ethernet Listen Local port group member (or another setting) is missing after device power cycle.	The device has not had time to synchronize the new setting to the database.	Before powering down the device, navigate to the Diagnostics page, and select Halt system . Wait a minute or two, then turn off the unit.
Cannot establish a MACsec connection.	A MACsec connection cannot be established because there is no physical connection between the CA members.	Verify the physical integrity of the Ethernet cable.

Table 8.5 Troubleshooting Procedure (Sheet 2 of 2)

Problem	Possible Causes	Solution
	A MACsec connection cannot be established because there is a configuration error on one or both CA members.	Verify the configuration of both CA members.
	A MACsec connection cannot be established because there is a mismatch in commissioning options between CA members.	Verify the commissioning options selected for both CA members.
	A MACsec connection cannot be established because an unused MACsec session is still configured.	Clear the existing MACsec session.
	A MACsec connection cannot be established because of an unsuccessful SAK or CAK rotation.	
An established MACsec connection fails.	An established MACsec connection fails because there is no physical connection between the CA members.	Verify the physical integrity of the Ethernet cable.

Password Jumper

The device contains a jumper that can be applied to set the front Ethernet port to a known address and enable an emergency administrative account. This feature should only be used in the situation where the device is inaccessible because of unknown IP addresses or unknown administrative passwords. Perform the following steps to enable this feature. Do not have the password jumper enabled during a factory-default reset. If you attempt to log in using the emergency administrative account after a factory-default reset without first removing and readding the password jumper, you will not be able to log in using the emergency administrative account.

SEL-3610/SEL-3620

- Step 1. De-energize the device and remove it from the rack or panel.
- Step 2. Remove the retaining screws, ground plug, plug-in connectors, and connected cables.
- Step 3. Remove the panel that covers the top and rear.
- Step 4. Locate JMP 6.
- Step 5. Place a jumper across the C position in the JMP 6 block.
- Step 6. Apply power to the unit.
- Step 7. Connect an Ethernet cable from your management computer to the device front port.
- Step 8. Assign IP address 192.168.100.2/24 to your management computer.
- Step 9. Open your web browser and enter <https://192.168.100.1> in the address bar.
- Step 10. Log in to the device with a known username. If there is no known username, log in to the device with the username **Edison**. Any password will be accepted while the password jumper is enabled.

SEL-3622

- Step 1. De-energize the device, disconnect it, and remove it for servicing.
- Step 2. Remove the four case screws (two on each side).

- Step 3. Remove the panel that covers the top and rear of the unit by lifting the cover about an inch at the front, and then sliding the cover toward the rear of the unit.
- Step 4. Locate JMP1 near the **ETH F** connector at the front of the unit.
- Step 5. Place a jumper on position C (the middle one).
- Step 6. Apply power to the unit.
- Step 7. Set your management computer network interface to **192.168.100.2/24**.
- Step 8. Connect your management computer to ETHF on the device. If the firmware version on your SEL-3622 unit is earlier than firmware version R200, you will need to connect your management computer to ETH1 on the device instead of ETHF.
- Step 9. Open your web browser and enter **https://192.168.100.1** in the address bar.
- Step 10. Log in to the device with a known username. If there is no known username, log in as **Edison**. Any password will be accepted while the password jumper is enabled.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

A P P E N D I X A

Firmware and Manual Versions

Firmware

The firmware version will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

A standard release is identified by a change in the R-number of the device FID number.

Existing firmware:

FID=SEL-3620-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID=SEL-3620-**R101**-V0-Z001001-Dxxxxxxxx

A point release is identified by a change in the V-number of the device FID number.

Existing firmware:

FID=SEL-3620-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID=SEL-3620-R100-**V1**-Z001001-Dxxxxxxxx

The date code is after the D. For example, the following is firmware version number R100, date code November 13, 2009.

FID=SEL-3620-R100-V0-Z001001-**D20091113**

The following tables list the firmware versions, revision descriptions, and corresponding instruction manual date codes:

- *SEL-3610 Firmware Revision History* on page A.2
- *SEL-3620 Firmware Revision History* on page A.7
- *SEL-3622 Firmware Revision History* on page A.14

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with “[Cybersecurity]”. Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with “[Cybersecurity Enhancement]”.

SEL-3610 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3610-R215-V0-Z018006-D20241001	<ul style="list-style-type: none"> ➤ [Cybersecurity Enhancement] Added current user verification on user enable/disable/edit/delete. ➤ [Cybersecurity Enhancement] Updated the hashing algorithm used to store user account passwords. ➤ [Cybersecurity Enhancement] Improved security controls on the web interface with enhanced input checking and a new content security policy. ➤ [Cybersecurity Enhancement] Addressed an issue where users with complex passwords could not complete user verification through the user account modifications. ➤ [Cybersecurity Enhancement] Updated third-party packages to ensure continuity of support. ➤ [Cybersecurity Enhancement] Updated the syslog destination configuration to allow for more granular filtering of each syslog facility's severity level selection. ➤ [Cybersecurity Enhancement] Updated the SSH key exchange algorithms and configuration options. ➤ [Cybersecurity Enhancement] Added secure configuration suggestions to the user web interface. ➤ Added address group functionality for allowed clients. ➤ Modified the system settings file export to generate a syslog only settings file in addition to the pre-existing full settings file. ➤ Improved the import processing for LDAP, Port Mappings, and syslog settings. ➤ Clarified web interface feedback messages. 	20241001
SEL-3610-R214-V0-Z017006-D20231212	<ul style="list-style-type: none"> ➤ [Cybersecurity] Added current user verification on password change attempts. ➤ [Cybersecurity] Added current user verification for new user creation. 	20231212
SEL-3610-R213-V2-Z017006-D20231004	No functional changes from R213-V1.	20231004
SEL-3610-R213-V1-Z017006-D20230601	<p>Includes all the functions of SEL-3610-R213-V0-Z017006-D20230109 with the following addition:</p> <ul style="list-style-type: none"> ➤ Added support for updated hardware to replace an obsolete component. Devices shipped with R213-V1 and later cannot be downgraded to any previous firmware version, but existing devices upgraded to R213-V1 can revert to previously installed firmware R210 and later. 	20230601
SEL-3610-R213-V0-Z017006-D20230109	<ul style="list-style-type: none"> ➤ Addressed an issue where firmware upgrades from R208 or earlier to R210 or later could result in a device with loss of variant and functionality. ➤ Addressed an issue where IRIIG would lose sync after a short period of time. ➤ Addressed an issue where “\” characters in certain settings could result in an extra “\” being added to the setting. ➤ Modified firmware to prevent invalid firmware reversions. 	20230112
SEL-3610-R212-V0-Z017006-D20221003	<ul style="list-style-type: none"> ➤ Addressed an issue where Administrator device role LDAP group mappings would be converted to Technician device role when settings are imported. <p>The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20221003

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3610-R211-V0-Z016006-D20220712	<ul style="list-style-type: none"> ➤ Added a feature to block the downgrade of firmware prior to R211 to prevent compatibility issues with updated hardware. ➤ [Cybersecurity] Addressed security vulnerabilities that could degrade performance. ➤ Added support for updated hardware to replace an obsolete component. ➤ Improved performance of bit-based RS-232 communications with the Push-to-Talk feature. <p>R211 cannot downgrade to any earlier firmware versions. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220712
SEL-3610-R210-V0-Z015006-D20220429	<ul style="list-style-type: none"> ➤ [Cybersecurity] Updated the operating system and third-party packages to ensure a continued ability to remediate potential security vulnerabilities. ➤ [Cybersecurity] Removed support for TLSv1.1. ➤ [Cybersecurity Enhancement] Added support for TLSv1.3. <p>The downgrade or reversion of firmware from R210 to earlier versions is not possible due to the significance of the system changes in the R210 release. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220429
SEL-3610-R209-V0	This firmware version did not production release.	—
SEL-3610-R208-V3-Z014006-D20210426	<p>Includes all the functions of SEL-3610-R208-V2-Z014006-D20201216 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. 	20210426
SEL-3610-R208-V2-Z014006-D20201216	<p>Includes all the functions of SEL-3610-R208-V0-Z014006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where the HASH command could return differing hash values or the hash for a backup file could differ for the same data because of the nondeterministic ordering of some list-based settings. 	20201216
SEL-3610-R208-V1	This firmware version was created and released only for the SEL-3620 and SEL-3622. It did not production release for the SEL-3610.	—
SEL-3610-R208-V0-Z014006-D20200624	<ul style="list-style-type: none"> ➤ Provided a new single-file backup for disaster recovery. ➤ Updated several third-party packages used in the product. ➤ Implemented a system heartbeat system log. 	20200624
SEL-3610-R207-V3-Z013006-D20210426	<p>Includes all the functions of SEL-3610-R207-V1-Z013006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. <p>Note: R207-V2 firmware was created and released only for the SEL-3620 and SEL-3622.</p>	20210426
SEL-3610-R207-V1-Z013006-D20200624	<p>Includes all the functions of SEL-3610-R207-V0-Z013006-D20191031 with the following addition:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. 	20200624
SEL-3610-R207-V0-Z013006-D20191031	<ul style="list-style-type: none"> ➤ Enabled the front-panel USB port for use as an Ethernet out-of-band management port. ➤ Added the ability to add character pacing to EIA-232 communications. 	20191031
SEL-3610-R206-V2-Z012006-D20200624	<p>Includes all the functions of SEL-3610-R206-V1-Z012006-D20180803 with the following addition:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. 	20200624
SEL-3610-R206-V1-Z012006-D20180803	<p>Includes all the functions of SEL-3610-R206-V0-Z012006-D20180525 with the following addition:</p> <ul style="list-style-type: none"> ➤ Adjusted the intrusion detection triggers on password input fields to better handle complex passwords entered on the web interface. ➤ Adjusted white-space trimming on some user input fields. 	20180803

A.4 Firmware and Manual Versions

Firmware

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3610-R206-V0-Z012006-D20180525	<ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. ➤ Added support for RADIUS Calling-Station-ID. ➤ Added support for RADIUS unknown user roles. ➤ Expanded input contact support to all hardware variants. ➤ Updated RADIUS dictionary.sel. 	20180525
SEL-3610-R205-V2-Z011006-D20180803	<p>Includes all the functions of SEL-3610-R205-V0-Z011006-D20171026 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3610-R205-V1	This firmware version did not production release.	—
SEL-3610-R205-V0-Z011006-D20171026	<ul style="list-style-type: none"> ➤ Modified web server configuration to prevent security scanner false positives. ➤ Enabled HTTP Strict Transport Security. ➤ Added protection against HTTP slow denial of service. ➤ Added HTTPOnly flag to web session cookies. ➤ Removed support for TLSv1.0. ➤ Updated support web server cipher list. ➤ Updated settings file export/import processing. ➤ Added RADIUS Calling-Station-Id attribute. 	20171026
SEL-3610-R204-V4-Z010006-D20180803	<p>Includes all the functions of SEL-3610-R204-V3-Z010006-D20170714 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3610-R204-V3-Z010006-D20170714	<p>Includes all the functions of SEL-3610-R204-V1-Z010006-D20170321 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3610-R204-V2	This firmware version did not production release.	—
SEL-3610-R204-V1-Z010006-D20170321	<p>Includes all the functions of SEL-3610-R204-V0-Z010006-D20160728 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170321
SEL-3610-R204-V0-Z010006-D20160728	<ul style="list-style-type: none"> ➤ Enhanced the Service Port SHOW command to ensure data properly returned for some SSH clients. ➤ Changed the device default web certificate to use 2048-bit RSA keys and be signed with a SHA-256-based signature. ➤ Changed the signing algorithm to SHA-256 for X.509 certificates generated on the device. 	20160728
SEL-3610-R203-V5-Z010006-D20180803	<p>Includes all the functions of SEL-3610-R203-V4-Z010006-D20170714 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3610-R203-V4-Z010006-D20170714	<p>Includes all the functions of SEL-3610-R203-V2-Z010006-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3610-R203-V3	This firmware version did not production release.	—

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3610-R203-V2-Z010006-D20170407	<p>Includes all the functions of SEL-3610-R203-V1-Z010006-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3610-R203-V1-Z010006-D20160203	<p>Includes all the functions of SEL-3610-R203-V0-Z010006-D20151230 with the following addition:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. 	20160203
SEL-3610-R203-V0-Z010006-D20151230	<ul style="list-style-type: none"> ➤ Added configurable SSH interface to view settings. ➤ Changed “Web Server” section name to “Management Interface.” ➤ Updated open-source software components to current versions that addressed applicable CVEs. ➤ Added the ability to ping an IP address from the device web interface diagnostics page. ➤ Added an optional Anti-Chatter message throttling function for the syslog client on the device. ➤ Modified Telnet implementation to negotiate 7-bit or 8-bit connections. ➤ Improved import and export handling of port group Ethernet Listen Local associated interface setting. 	20151230
SEL-3610-R201-V3-Z008004-D20170714	<p>Includes all the functions of SEL-3610-R201-V2-Z008004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3610-R201-V2-Z008004-D20170407	<p>Includes all the functions of SEL-3610-R201-V1-Z008004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3610-R201-V1-Z008004-D20160203	<p>Includes all the functions of SEL-3610-R201-V0-Z008004-D20150227 with the following addition:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. 	20160203
SEL-3610-R201-V0-Z008004-D20150227	<ul style="list-style-type: none"> ➤ Added bit-based serial conversion capabilities. ➤ Added UDP Ethernet transport to port mapping capabilities. ➤ Enhanced reliability of DHCP client capabilities for Ethernet interfaces. ➤ Enhanced stability of port group members by syncing changes to flash immediately. ➤ Addressed POODLE vulnerability in OpenSSL implementation CVE-2014-3566. 	20150227
SEL-3610-R200-V3-Z007004-D20170714	<p>Includes all the functions of SEL-3610-R200-V2-Z007004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3610-R200-V2-Z007004-D20170407	<p>Includes all the functions of SEL-3610-R200-V1-Z007004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3610-R200-V1-Z007004-D20160203	<p>Includes all the functions of SEL-3610-R200-V0-Z007004-D20140616 with the following addition:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. 	20160203

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3610-R200-V0-Z007004-D20140616	<ul style="list-style-type: none"> ➤ Added support for new hardware version that replaced some obsolete components. ➤ Added feature to block downgrade of firmware below R200 because of hardware incompatibility. ➤ Added backwards-compatible support for hardware change to replace obsolete component. ➤ Added the Global Session Timeout setting to the web interface. ➤ Modified IRIG processing. ➤ Modified SSH processing. ➤ Modified ymodem passthrough behavior. ➤ Removed IM from the firmware image. 	20140616
SEL-3610-R142-V0-Z005004-D20140409	<ul style="list-style-type: none"> ➤ Updated OpenSSL. 	20140409
SEL-3610-R140-V0-Z005004-D20140107	<ul style="list-style-type: none"> ➤ Updated open-source software components to current revisions. ➤ Added 2-wire EIA-485 support. ➤ Added whitelisting and self-diagnostic features to safeguard system integrity. ➤ Added SNMP management support. ➤ Added support for central authentication using RADIUS. ➤ Fixed delay between clock reference and IRIG signal output. 	20140107
SEL-3610-R137-V0-Z005003-D20121207	<ul style="list-style-type: none"> ➤ Added EIA-485 2-wire support. ➤ Added Max Frame Length to Serial Port Profile settings. 	20121207
SEL-3610-R133-V0-Z003003-D20111014	<ul style="list-style-type: none"> ➤ Updated serial flow control functionality. ➤ Modified EIA-485 signal correlation. 	20111014
SEL-3610-R132-V0-Z003003-D20110902	<ul style="list-style-type: none"> ➤ Modified settings import processing. 	20110902
SEL-3610-R130-V0-Z003003-D20110729	<ul style="list-style-type: none"> ➤ Added port switch functions. ➤ Added Master Port. ➤ Modified Status LED functions. ➤ Modified Time Processing. ➤ Added settings import/export. ➤ Removed Network Address Translation Traversal. ➤ Removed Half Duplex Serial Flow Control. ➤ Updated Linux packages to current versions. 	20110729
SEL-3610-R122-V0-Z003002-D20100907	<ul style="list-style-type: none"> ➤ Corrected Modbus connection recovery process. 	20100907
SEL-3610-R121-V0-Z003002-D20100524	<ul style="list-style-type: none"> ➤ Made enhancement to include Ethernet port bridging. 	20100524
SEL-3610-R110-V0-Z002002-D20100222	<ul style="list-style-type: none"> ➤ Made Modbus serial to TCP transceiver and web security enhancements. 	20100222
SEL-3610-R100-V0-Z001001-D20091209	<ul style="list-style-type: none"> ➤ Initial version. 	20091209

SEL-3620 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R215-V0-Z018006-D20241001	<ul style="list-style-type: none"> ➤ [Cybersecurity] Adjusted FTP processing to prevent usage of the SEL-3620 in FTP Bounce attacks. ➤ [Cybersecurity Enhancement] Added current user verification on user enable/disable/edit/delete. ➤ [Cybersecurity Enhancement] Updated the hashing algorithm used to store user account passwords. ➤ [Cybersecurity Enhancement] Improved security controls on the web interface with enhanced input checking and a new content security policy. ➤ [Cybersecurity Enhancement] Updated third-party packages to ensure continuity of support. ➤ [Cybersecurity Enhancement] Addressed an issue where users with complex passwords could not complete user verification through the user account modifications. ➤ [Cybersecurity Enhancement] Updated permissions to allow technicians to create, delete, and modify the NAT/Port Forwarding Rules. ➤ [Cybersecurity Enhancement] Updated the syslog destination configuration to allow for more granular filtering of each syslog facility's severity level selection. ➤ [Cybersecurity Enhancement] Updated the SSH key exchange algorithms and configuration options. ➤ [Cybersecurity Enhancement] Updated the Managed Device(s) scheduled password rotation to occur at local time instead of UTC. ➤ [Cybersecurity Enhancement] Added secure configuration suggestions to the user web interface. ➤ Added group functionality to the sources and destinations of the firewall, allowed clients, and NAT port forwarding rules. ➤ Improved the System Setting import processing for the LDAP, Port Mappings, and syslog settings. ➤ Clarified web interface feedback messages. ➤ Addressed an issue where the ACCELERATOR QuickSet HMI does not connect to the relay through an SEL-3620 when FTP is used as the file transfer option. ➤ Added a description field to the NAT port forwarding rules. ➤ Modified system settings file export to generate syslog only settings file in addition to preexisting full settings file. 	20241001
SEL-3620-R214-V0-Z017006-D20231212	<ul style="list-style-type: none"> ➤ [Cybersecurity] Added current user verification on password change attempts. ➤ [Cybersecurity] Added current user verification for new user creation. 	20231212
SEL-3620-R213-V2-Z017006-D20231004	<p>Includes all the functions of SEL-3620-R213-V1-Z017006-D2023060 with the following addition:</p> <ul style="list-style-type: none"> ➤ [Cybersecurity] Resolved an issue with password rotation for GE relays that use non-numeric passwords in versions R210 through R213-V1. 	20231004
SEL-3620-R213-V1-Z017006-D20230601	<p>Includes all the functions of SEL-3620-R213-V0-Z017006-D20230109 with the following addition:</p> <ul style="list-style-type: none"> ➤ Added support for updated hardware to replace an obsolete component. Devices shipped with R213-V1 and later cannot be downgraded to any previous firmware version, but existing devices upgraded to R213-V1 can revert to previously installed firmware R210 and later. 	20230601

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R213-V0-Z017006-D20230109	<ul style="list-style-type: none"> ➤ Addressed an issue where firmware upgrades from R208 or earlier to R210 or later could result in a device with loss of variant and functionality. ➤ Addressed an issue where IRIG would lose sync after a short period of time. ➤ [Cybersecurity Enhancement] Addressed an issue where “\” characters in certain settings, including managed device passwords, could result in an extra “\” being added to the setting. ➤ Modified firmware to prevent invalid firmware reversions. 	20230112
SEL-3620-R212-V0-Z017006-D20221003	<ul style="list-style-type: none"> ➤ Addressed an issue where Administrator device role LDAP group mappings would be converted to Technician device role when settings are imported. ➤ Addressed issue in previous firmware, in which the VPN LED turned green when Phase 1 negotiation succeeded even if Phase 2 negotiation failed and no tunnel was established. Now the VPN LED only turns green when a VPN tunnel is successfully established. ➤ [Cybersecurity Enhancement] Added “SEL - Secure (2022)” IPSec Profile. The firmware is only available on units from the factory. It is not available as a field upgrade. 	20221003
SEL-3620-R211-V0-Z016006-D20220712	<ul style="list-style-type: none"> ➤ Added a feature to block the downgrade of firmware prior to R211 to prevent compatibility issues with updated hardware. ➤ [Cybersecurity] Addressed security vulnerabilities that could degrade performance. ➤ Added support for updated hardware to replace an obsolete component. ➤ Improved performance of bit-based RS-232 communications with the Push-to-Talk feature. ➤ [Cybersecurity Enhancement] Added support for Media Access Control Security (MACsec) and MACsec Key Agreement (MKA) protocol. ➤ [Cybersecurity Enhancement] Addressed an issue with password generation after initial boot. <p>R211 cannot downgrade to any earlier firmware versions. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220712
SEL-3620-R210-V0-Z015006-D20220429	<ul style="list-style-type: none"> ➤ [Cybersecurity] Updated the operating system and third-party packages to ensure a continued ability to remediate potential security vulnerabilities. ➤ [Cybersecurity] Updated IPsec Key Exchange (IKE) for better compliance with RFC 4945, section 5.1.3.2. This can cause IPsec connections with some non-compliant certificates to fail. See <i>X.509 Certificates</i> in Appendix K: X.509 of the instruction manual for more information. ➤ [Cybersecurity] Updated the Python interpreter used to execute Authentication Proxy scripts from Python 2 to Python 3. ➤ [Cybersecurity] Modified firmware to open UDP ports 500 and 4500 only when IPsec is configured and enabled. Previously, UDP and TCP ports 500 and 4500 were always open but in a non-listening state if IPsec was disabled. ➤ [Cybersecurity] Enhanced authentication proxy to support SSH-connected managed devices. ➤ [Cybersecurity] Removed support for TLSv1.1. ➤ [Cybersecurity Enhancement] Added support for TLSv1.3. <p>The downgrade or reversion of firmware from R210 to earlier versions is not possible due to the significance of the system changes in the R210 release. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220429
SEL-3620-R209-V0	This firmware version did not production release.	—

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R208-V3-Z014006-D20210426	<p>Includes all the functions of SEL-3620-R208-V2-Z014006-D20201216 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. 	20210426
SEL-3620-R208-V2-Z014006-D20201216	<p>Includes all the functions of SEL-3620-R208-V1-Z014006-D20200918 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where the HASH command could return differing hash values or the hash for a backup file could differ for the same data because of the nondeterministic ordering of some list-based settings. ➤ Corrected verbose firewall logging behavior where traffic is rejected but no syslog is created. 	20201216
SEL-3620-R208-V1-Z014006-D20200918	<p>Includes all the functions of SEL-3620-R208-V0-Z014006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Allowed selection of managed devices configured for XON/XOFF in QuickSet Device Manager. 	20200918
SEL-3620-R208-V0-Z014006-D20200624	<ul style="list-style-type: none"> ➤ Implemented a firewall logging enhancement that enables more granular logging control. ➤ Provided a new single-file backup for disaster recovery. ➤ Updated several third-party packages used in the product. ➤ Extended the existing limit for the maximum managed device checkout duration. ➤ Implemented a system heartbeat system log. ➤ Removed extra spacing from Authentication proxy PDF reports. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624
SEL-3620-R207-V3-Z013006-D20210426	<p>Includes all the functions of SEL-3620-R207-V2-Z013006-D20200918 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. 	20210426
SEL-3620-R207-V2-Z013006-D20200918	<p>Includes all the functions of SEL-3620-R207-V1-Z013006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Allowed selection of managed devices configured for XON/XOFF in QuickSet Device Manager. 	20200918
SEL-3620-R207-V1-Z013006-D20200624	<p>Includes all the functions of SEL-3620-R207-V0-Z013006-D20191031 with the following additions:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624
SEL-3620-R207-V0-Z013006-D20191031	<ul style="list-style-type: none"> ➤ Enabled the front-panel USB port for use as an Ethernet out-of-band management port. ➤ Added the ability to add character pacing to EIA-232 communications. ➤ Enhanced DNAT to allow multiple sources to connect to the same destination. 	20191031
SEL-3620-R206-V2-Z012006-D20200624	<p>Includes all the functions of SEL-3620-R206-V1-Z012006-D20180803 with the following additions:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624

A.10 | Firmware and Manual Versions

Firmware

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R206-V1-Z012006-D20180803	<p>Includes all the functions of SEL-3620-R206-V0-Z012006-D20180525 with the following additions:</p> <ul style="list-style-type: none"> ➤ Adjusted the intrusion detection triggers on password input fields to better handle complex passwords entered on the web interface. ➤ Adjusted white-space trimming on some user input fields. ➤ Improved FTP proxy initialization to eliminate erroneous white list notification. 	20180803
SEL-3620-R206-V0-Z012006-D20180525	<ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. ➤ Added support for RADIUS Calling-Station-ID. ➤ Added support for RADIUS unknown user roles. ➤ Updated RADIUS dictionary.sel. ➤ Improved SEMP reliability. ➤ Improved password operation performance. ➤ Added password persistence. ➤ Expanded input contact support to all hardware variants. ➤ Added device selection for password operations. ➤ Added ability to exclude devices from management operations. ➤ Added status feedback to managed device list. ➤ Added Syslog messages. ➤ Added order to the managed device list. ➤ Added encryption option to proxy report generation. 	20180525
SEL-3620-R205-V2-Z011006-D20180803	<p>Includes all the functions of SEL-3620-R205-V1-Z011006-D20180122 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3620-R205-V1-Z011006-D20180122	<p>Includes all the functions of SEL-3620-R205-V0-Z011006-D20171026 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved handling of malformed connection directories. ➤ Improved connection directory import process. 	20180122
SEL-3620-R205-V0-Z011006-D20171026	<ul style="list-style-type: none"> ➤ Modified web server configuration to prevent security scanner false positives. ➤ Enabled HTTP Strict Transport Security. ➤ Added protection against HTTP slow denial of service. ➤ Added HTTPOnly flag to web session cookies. ➤ Removed support for TLSv1.0. ➤ Updated support web server cipher list. ➤ Updated settings file export/import processing. ➤ Added RADIUS Calling-Station-Id attribute. ➤ Added device check out/in. ➤ Improved password application performance. ➤ Added password change log. 	20171026
SEL-3620-R204-V4-Z010006-D20180803	<p>Includes all the functions of SEL-3620-R204-V3-Z010006-D20170714 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3620-R204-V3-Z010006-D20170714	<p>Includes all the functions of SEL-3620-R204-V2-Z010006-D20170510 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R204-V2-Z010006-D20170510	<p>Includes all the functions of SEL-3620-R204-V1-Z010006-D20170321 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated network address translation functionality to add firewall access control lists for port forwarding destinations. 	20170510
SEL-3620-R204-V1-Z010006-D20170321	<p>Includes all the functions of SEL-3620-R204-V0-Z010006-D20160728 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170321
SEL-3620-R204-V0-Z010006-D20160728	<ul style="list-style-type: none"> ➤ Enhanced the Service Port SHOW command to ensure data properly returned for some SSH clients. ➤ Changed the device default web certificate to use 2048-bit RSA keys and be signed with a SHA-256-based signature. ➤ Changed the signing algorithm to SHA-256 for X.509 certificates generated on the device. 	20160728
SEL-3620-R203-V5-Z010006-D20180803	<ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3620-R203-V4-Z010006-D20170714	<p>Includes all the functions of SEL-3620-R203-V3-Z010006-D20170510 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3620-R203-V3-Z010006-D20170510	<p>Includes all the functions of SEL-3620-R203-V2-Z010006-D20170407 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated network address translation functionality to add firewall access control lists for port forwarding destinations. 	20170510
SEL-3620-R203-V2-Z010006-D20170407	<p>Includes all the functions of SEL-3620-R203-V1-Z010006-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3620-R203-V1-Z010006-D20160203	<p>Includes all the functions of SEL-3620-R203-V0-Z010006-D20151230 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3620-R203-V0-Z010006-D20151230	<ul style="list-style-type: none"> ➤ Added configurable SSH interface to view settings. ➤ Changed “Web Server” section name to “Management Interface.” ➤ Updated open-source software components to current versions that addressed applicable CVEs. 	20151230
SEL-3620-R202-V0-Z009005-D20150916	<ul style="list-style-type: none"> ➤ Added Network Address Translation (NAT) capabilities, including Outbound NAT (SNAT) and Port Forwarding (DNAT). ➤ Added optional Verbose Logging capabilities to the device firewall to alert on all ICMP, UDP, and TCP connection attempts. ➤ Added the ability to ping an IP address from the device web interface diagnostics page. ➤ Added an optional Anti-Chatter message throttling function for the syslog client on the device. ➤ Added the PWRevert command to the SEL SELF controller. ➤ Enhanced IPsec byte counters on the device dashboard to capture all IPsec communications. ➤ Modified Telnet implementation to negotiate 7-bit or 8-bit connections. ➤ Improved import and export handling of port group Ethernet Listen Local associated interface setting. 	20150916

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R201-V3-Z008004-D20170714	<p>Includes all the functions of SEL-3620-R201-V2-Z008004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3620-R201-V2-Z008004-D20170407	<p>Includes all the functions of SEL-3620-R201-V1-Z008004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3620-R201-V1-Z008004-D20160203	<p>Includes all the functions of SEL-3620-R201-V0-Z008004-D20150227 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3620-R201-V0-Z008004-D20150227	<ul style="list-style-type: none"> ➤ Added bit-based serial conversion capabilities. ➤ Added UDP Ethernet transport to port mapping capabilities. ➤ Enhanced reliability of DHCP client capabilities for Ethernet interfaces. ➤ Enhanced stability of port group members by syncing changes to flash immediately. ➤ Addressed POODLE vulnerability in OpenSSL implementation CVE-2014-3566. ➤ Addressed issue in which IPsec did not function with offline-generated X.509 certificates. 	20150227
SEL-3620-R200-V3-Z007004-D20170714	<p>Includes all the functions of SEL-3620-R200-V2-Z007004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3620-R200-V2-Z007004-D20170407	<p>Includes all the functions of SEL-3620-R200-V1-Z007004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3620-R200-V1-Z007004-D20160203	<p>Includes all the functions of SEL-3620-R200-V0-Z007004-D20140616 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3620-R200-V0-Z007004-D20140616	<ul style="list-style-type: none"> ➤ Added support for new hardware version that replaced some obsolete components. ➤ Added feature to block downgrade of firmware below R200 because of hardware incompatibility ➤ Added backwards-compatible support for hardware change to replace obsolete component. ➤ Added the Global Session Timeout setting to the web interface. ➤ Modified IRIG processing. ➤ Modified SSH processing. ➤ Modified ymodem passthrough behavior. ➤ Removed IM from the firmware image. ➤ Enabled the contact input sensor. ➤ Added Ethernet link-loss detection and alerting. 	20140616

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-3620-R142-V0-Z005004-D20140409	➤ Updated OpenSSL.	20140409
SEL-3620-R141-V0-Z005004-D20140404	➤ Improved master port handling of multiple simultaneous scripts. ➤ Improved Syslog daemon boot process. ➤ Removed unnecessary DNS requests.	20140404
SEL-3620-R139-V0-Z005004-D20131122	➤ Updated open-source software components to current revisions. ➤ Added 2-wire EIA-485 support. ➤ Added Modbus/TCP protocol conversion. ➤ Added Modbus options to serial port configuration. ➤ Added whitelisting and self-diagnostic features to safeguard system integrity. ➤ Added SNMP management support. ➤ Added support for central authentication using RADIUS. ➤ Limited size of generated proxy report. ➤ Added Proxy functionality for FTP. ➤ Fixed delay between clock reference and IRIG signal output.	20131122
SEL-3620-R138-V0-Z004003-D20130501	➤ Improved logic for proxy access to devices through an SEL Communications Processor. ➤ Improved child password updates using an SEL Communications Processor. ➤ Improved robustness for password updates in tiered systems.	20130501
SEL-3620-R135-V0-Z004003-D20120928	➤ Upgraded Linux Kernel. ➤ Added ability to handle multiple master port connections. ➤ Fixed master port scripting handling of ^X^X^X sequence. ➤ Improved master port support for tiered device connections. ➤ Improved support for ACCELERATOR Quickset SEL-5030 and ACCELERATOR TEAM SEL-5045 Software. ➤ Updated for ACCELERATOR TEAM integration.	20120928
SEL-3620-R134-V0-Z003003-D20120815	➤ Corrected operation of password change scheduler.	20120815
SEL-3620-R133-V0-Z003003-D20111014	➤ Modified proxy services to not strip nonalphanumeric characters from the beginning of strings. ➤ Modified proxy services to enhance performance. ➤ Updated serial flow control functionality. ➤ Modified EIA-485 signal correlation.	20111014
SEL-3620-R132-V0-Z003003-D20110902	➤ Modified settings import processing.	20110902
SEL-3620-R130-V0-Z003003-D20110729	➤ Added NTP support. ➤ Modified Time Processing. ➤ Added serial port switch. ➤ Added proxy services. ➤ Added SSH support. ➤ Added settings import/export. ➤ Modified Status LED functions. ➤ Modified supported Allowed Clients. ➤ Updated Linux packages to current versions.	20110729
SEL-3620-R120-V0-Z002002-D20100831	➤ Added LDAP for centralized access control. ➤ Added DHCP client mode. ➤ Added Network Address Translation Traversal. ➤ Modified the default Ethernet Port to Eth F. ➤ Updated Linux packages to current versions.	20100831
SEL-3620-R112-V0-Z001001-D20100204	➤ Modified Firewall behavior and implemented security enhancements.	20100204
SEL-3620-R110-V0-Z001001-D20091217	➤ Modified IPsec rekey behavior.	20091217
SEL-3620-R100-V0-Z001001-D20091113	➤ Initial version.	20091113

SEL-3622 Firmware Revision History

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R215-V0-Z018006-D20241001	<ul style="list-style-type: none"> ➤ [Cybersecurity] Adjusted FTP processing to prevent usage of the SEL-3622 in FTP Bounce attacks. ➤ [Cybersecurity Enhancement] Added current user verification on user enable/disable/edit/delete. ➤ [Cybersecurity Enhancement] Updated the hashing algorithm used to store user account passwords. ➤ [Cybersecurity Enhancement] Improved security controls on the web interface with enhanced input checking and a new content security policy. ➤ [Cybersecurity Enhancement] Updated third-party packages to ensure continuity of support. ➤ [Cybersecurity Enhancement] Addressed an issue where users with complex passwords could not complete user verification through the user account modifications. ➤ [Cybersecurity Enhancement] Updated permissions to allow technicians to create, delete, and modify the NAT/Port Forwarding Rules. ➤ [Cybersecurity Enhancement] Updated the syslog destination configuration to allow for more granular filtering of each syslog facility's severity level selection. ➤ [Cybersecurity Enhancement] Updated the SSH key exchange algorithms and configuration options. ➤ [Cybersecurity Enhancement] Updated the Managed Device(s) scheduled password rotation to occur at local time instead of UTC. ➤ [Cybersecurity Enhancement] Added secure configuration suggestions to the user web interface. ➤ Added group functionality to the sources and destinations of the firewall, allowed clients, and NAT port forwarding rules. ➤ Improved the System Setting import processing for the LDAP, Port Mappings, and syslog settings. ➤ Clarified web interface feedback messages. ➤ Addressed an issue where the ACCELERATOR QuickSet HMI does not connect to the relay through an SEL-3622 when FTP is used as the file transfer option. ➤ Added a description field to the NAT port forwarding rules. ➤ Modified system settings file export to generate syslog only settings file in addition to preexisting full settings file. 	20241001
SEL-3622-R214-V0-Z017006-D20231212	<ul style="list-style-type: none"> ➤ [Cybersecurity] Added current user verification on password change attempts. ➤ [Cybersecurity] Added current user verification for new user creation. ➤ Adjusted downgrade blockers to allow SEL-3622 downgrades from R214 to R213, R212, and R211. 	20231212
SEL-3622-R213-V2-Z017006-D20231004	<p>Includes all the functions of SEL-3622-R213-V1-Z017006-D20230601 with the following addition:</p> <ul style="list-style-type: none"> ➤ [Cybersecurity] Resolved an issue with password rotation for GE relays that use non-numeric passwords in versions R210 through R213-V1. 	20231004
SEL-3622-R213-V1-Z017006-D20230601	<p>Includes all the functions of SEL-3622-R213-V0-Z017006-D20230109 with the following addition:</p> <ul style="list-style-type: none"> ➤ Added support for updated hardware to replace an obsolete component. Devices shipped with R213-V1 and later cannot be downgraded to any previous firmware version, but existing devices upgraded to R213-V1 can revert to previously installed firmware R210 and later. 	20230601

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R213-V0-Z017006-D20230109	<ul style="list-style-type: none"> ➤ Addressed an issue where firmware upgrades from R208 or earlier to R210 or later could result in a device with loss of variant and functionality. ➤ Addressed an issue where IRIG would lose sync after a short period of time. ➤ [Cybersecurity Enhancement] Addressed an issue where “\” characters in certain settings, including managed device passwords, could result in an extra “\” being added to the setting. ➤ Modified firmware to prevent invalid firmware reversions. 	20230112
SEL-3622-R212-V0-Z017006-D20221003	<ul style="list-style-type: none"> ➤ Addressed an issue where Administrator device role LDAP group mappings would be converted to Technician device role when settings are imported. ➤ Addressed issue in previous firmware, in which the VPN LED turned green when Phase 1 negotiation succeeded even if Phase 2 negotiation failed and no tunnel was established. Now the VPN LED only turns green when a VPN tunnel is successfully established. ➤ [Cybersecurity Enhancement] Added “SEL - Secure (2022)” IPSec Profile. The firmware is only available on units from the factory. It is not available as a field upgrade. 	20221003
SEL-3622-R211-V0-Z016006-D20220712	<ul style="list-style-type: none"> ➤ Added a feature to block the downgrade of firmware prior to R211 to prevent compatibility issues with updated hardware. ➤ [Cybersecurity] Addressed security vulnerabilities that could degrade performance. ➤ Added support for updated hardware to replace an obsolete component. ➤ Improved performance of bit-based RS-232 communications with the Push-to-Talk feature. ➤ [Cybersecurity Enhancement] Added support for Media Access Control Security (MACsec) and MACsec Key Agreement (MKA) protocol. ➤ [Cybersecurity Enhancement] Addressed an issue with password generation after initial boot. <p>R211 cannot downgrade to any earlier firmware versions. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220712
SEL-3622-R210-V0-Z015006-D20220429	<ul style="list-style-type: none"> ➤ [Cybersecurity] Updated the operating system and third-party packages to ensure a continued ability to remediate potential security vulnerabilities. ➤ [Cybersecurity] Updated IPsec Key Exchange (IKE) for better compliance with RFC 4945, section 5.1.3.2. This can cause IPsec connections with some non-compliant certificates to fail. See <i>X.509 Certificates in Appendix K: X.509</i> of the instruction manual for more information. ➤ [Cybersecurity] Updated the Python interpreter used to execute Authentication Proxy scripts from Python 2 to Python 3. ➤ [Cybersecurity] Modified firmware to open UDP ports 500 and 4500 only when IPsec is configured and enabled. Previously, UDP and TCP ports 500 and 4500 were always open but in a non-listening state if IPsec was disabled. ➤ [Cybersecurity] Enhanced authentication proxy to support SSH-connected managed devices. ➤ [Cybersecurity] Addressed an issue where the SEL-3622 front Ethernet port could become unresponsive under certain traffic conditions. ➤ [Cybersecurity] Removed support for TLSv1.1. ➤ [Cybersecurity Enhancement] Added support for TLSv1.3. <p>The downgrade or reversion of firmware from R210 to earlier versions is not possible due to the significance of the system changes in the R210 release. The firmware is only available on units from the factory. It is not available as a field upgrade.</p>	20220429
SEL-3622-R209-V0	This firmware version did not production release.	—

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R208-V3-Z014006-D20210426	<p>Includes all the functions of SEL-3622-R208-V2-Z014006-D20201216 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. 	20210426
SEL-3622-R208-V2-Z014006-D20201216	<p>Includes all the functions of SEL-3622-R208-V1-Z014006-D20200918 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where the HASH command could return differing hash values or the hash for a backup file could differ for the same data because of the nondeterministic ordering of some list-based settings. ➤ Corrected verbose firewall logging behavior where traffic is rejected but no syslog is created. 	20201216
SEL-3622-R208-V1-Z014006-D20200918	<p>Includes all the functions of SEL-3622-R208-V0-Z014006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Allowed selection of managed devices configured for XON/XOFF in QuickSet Device Manager. 	20200918
SEL-3622-R208-V0-Z014006-D20200624	<ul style="list-style-type: none"> ➤ Implemented a firewall logging enhancement that enables more granular logging control. ➤ Provided a new single-file backup for disaster recovery. ➤ Updated several third-party packages used in the product. ➤ Extended the existing limit for the maximum managed device checkout duration. ➤ Implemented a system heartbeat system log. ➤ Removed extra spacing from Authentication proxy PDF reports. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624
SEL-3622-R207-V3-Z014006-D20210426	<p>Includes all the functions of SEL-3622-R207-V2-Z014006-D20200918 with the following addition:</p> <ul style="list-style-type: none"> ➤ Addressed an issue affecting USB networking on some computers. 	20210426
SEL-3622-R207-V2-Z013006-D20200918	<p>Includes all the functions of SEL-3622-R207-V1-Z013006-D20200624 with the following addition:</p> <ul style="list-style-type: none"> ➤ Allowed selection of managed devices configured for XON/XOFF in QuickSet Device Manager. 	20200918
SEL-3622-R207-V1-Z013006-D20200624	<p>Includes all the functions of SEL-3610-R207-V0-Z013006-D20191031 with the following additions:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624
SEL-3622-R207-V0-Z013006-D20191031	<ul style="list-style-type: none"> ➤ Enabled the front-panel USB port for use as an Ethernet out-of-band management port. ➤ Added the ability to add character pacing to EIA-232 communications. ➤ Enhanced DNAT to allow multiple sources to connect to the same destination. 	20191031
SEL-3622-R206-V2-Z012006-D20200624	<p>Includes all the functions of SEL-3622-R206-V1-Z012006-D20180803 with the following additions:</p> <ul style="list-style-type: none"> ➤ Removed the downgrade block so users can downgrade through a point release to a previous version. ➤ Updated authentication proxy to prevent malicious configuration changes from allowing unauthorized access. 	20200624
SEL-3622-R206-V1-Z012006-D20180803	<p>Includes all the functions of SEL-3622-R206-V0-Z012006-D20180525 with the following additions:</p> <ul style="list-style-type: none"> ➤ Adjusted the intrusion detection triggers on password input fields to better handle complex passwords entered on the web interface. ➤ Adjusted white-space trimming on some user input fields. ➤ Improved FTP proxy initialization to eliminate erroneous white list notification. 	20180803

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R206-V0-Z012006-D20180525	<ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. ➤ Added support for RADIUS Calling-Station-ID ➤ Added support for RADIUS unknown user roles ➤ Updated RADIUS dictionary.sel ➤ Improved SEMP reliability ➤ Improved password operation performance ➤ Added password persistence ➤ Added device selection for password operations ➤ Added ability to exclude devices from management operations ➤ Added status feedback to managed device list ➤ Added Syslog messages ➤ Added order to the managed device list ➤ Added encryption option to proxy report generation 	20180525
SEL-3622-R205-V2-Z011006-D20180803	<p>Includes all the functions of SEL-3622-R205-V1-Z011006-D20180122 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3622-R205-V1-Z011006-D20180122	<p>Includes all the functions of SEL-3622-R205-V0-Z011006-D20171026 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved handling of malformed connection directories. ➤ Improved connection directory import process. 	20180122
SEL-3622-R205-V0-Z011006-D20171026	<ul style="list-style-type: none"> ➤ Modified web server configuration to prevent security scanner false positives. ➤ Enabled HTTP Strict Transport Security. ➤ Added protection against HTTP slow denial of service. ➤ Added HTTPOnly flag to web session cookies. ➤ Removed support for TLSv1.0. ➤ Updated support web server cipher list. ➤ Updated settings file export/import processing. ➤ Added RADIUS Calling-Station-Id attribute. ➤ Added device check out/in. ➤ Improved password application performance. ➤ Added password change log. 	20171026
SEL-3622-R204-V4-Z010006-D20180803	<p>Includes all the functions of SEL-3622-R204-V3-Z010006-D20170714 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3622-R204-V3-Z010006-D20170714	<p>Includes all the functions of SEL-3622-R204-V2-Z010006-D20170510 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3622-R204-V2-Z010006-D20170510	<p>Includes all the functions of SEL-3622-R204-V1-Z010006-D20170321 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated network address translation functionality to add firewall access control lists for port forwarding destinations. 	20170510
SEL-3622-R204-V1-Z010006-D20170321	<p>Includes all the functions of SEL-3622-R204-V0-Z010006-D20160728 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170321

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R204-V0-Z010006-D20160728	<ul style="list-style-type: none"> ➤ Enhanced the Service Port SHOW command to ensure data properly returned for some SSH clients. ➤ Changed the device default web certificate to use 2048-bit RSA keys and be signed with a SHA-256-based signature. ➤ Changed the signing algorithm to SHA-256 for X.509 certificates generated on the device. 	20160728
SEL-3622-R203-V5-Z010006-D20180803	<ul style="list-style-type: none"> ➤ Update kernel and UBIFS drivers to resolve the file system reliability issue introduced in R200. 	20180803
SEL-3622-R203-V4-Z010006-D20170714	<p>Includes all the functions of SEL-3622-R203-V3-Z010006-D20170510 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3622-R203-V3-Z010006-D20170510	<p>Includes all the functions of SEL-3622-R203-V2-Z010006-D20170407 with the following addition:</p> <ul style="list-style-type: none"> ➤ Updated network address translation functionality to add firewall access control lists for port forwarding destinations. 	20170510
SEL-3622-R203-V2-Z010006-D20170407	<p>Includes all the functions SEL-3622-R203-V1-Z010006-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3622-R203-V1-Z010006-D20160203	<p>Includes all the functions of SEL-3622-R203-V0-Z010006-D20151230 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3622-R203-V0-Z010006-D20151230	<ul style="list-style-type: none"> ➤ Added configurable SSH interface to view settings. ➤ Changed “Web Server” section name to “Management Interface.” ➤ Updated open-source software components to current versions that addressed applicable CVEs. 	20151230
SEL-3622-R202-V0-Z009005-D20150916	<ul style="list-style-type: none"> ➤ Added Network Address Translation (NAT) capabilities, including Outbound NAT (SNAT) and Port Forwarding (DNAT). ➤ Added optional Verbose Logging capabilities to the device firewall to alert on all ICMP, UDP, and TCP connection attempts. ➤ Added the ability to ping an IP address from the device web interface diagnostics page. ➤ Added an optional Anti-Chatter message throttling function for the syslog client on the device. ➤ Added the PWRevert command to the SEL SELF controller. ➤ Enhanced IPsec byte counters on the device dashboard to capture all IPsec communications. ➤ Modified Telnet implementation to negotiate 7-bit or 8-bit connections. ➤ Improved import and export handling of port group Ethernet Listen Local associated interface setting. 	20150916
SEL-3622-R201-V3-Z008004-D20170714	<p>Includes all the functions of SEL-3622-R201-V2-Z008004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R201-V2-Z008004-D20170407	<p>Includes all the functions SEL-3622-R201-V1-Z008004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3622-R201-V1-Z008004-D20160203	<p>Includes all the functions of SEL-3622-R201-V0-Z008004-D20150227 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3622-R201-V0-Z008004-D20150227	<ul style="list-style-type: none"> ➤ Added bit-based serial conversion capabilities. ➤ Added UDP Ethernet transport to port mapping capabilities. ➤ Enhanced reliability of DHCP client capabilities for Ethernet interfaces. ➤ Enhanced stability of port group members by syncing changes to flash immediately. ➤ Addressed POODLE vulnerability in OpenSSL implementation CVE-2014-3566. ➤ Addressed issue in which IPsec did not function with offline-generated X.509 certificates. 	20150227
SEL-3622-R200-V3-Z007004-D20170714	<p>Includes all the functions of SEL-3622-R200-V2-Z007004-D20170407 with the following additions:</p> <ul style="list-style-type: none"> ➤ Improved performance of FTP proxy services. ➤ Improved performance of Modbus RTU/TCP translations. ➤ Updated SSH ciphers. ➤ Revoked administrator ability to create local passwords for central accounts. 	20170714
SEL-3622-R200-V2-Z007004-D20170407	<p>Includes all the functions SEL-3622-R200-V1-Z007004-D20160203 with the following addition:</p> <ul style="list-style-type: none"> ➤ Improved a file system reliability issue introduced in R200 that affects a small number of units. 	20170407
SEL-3622-R200-V1-Z007004-D20160203	<p>Includes all the functions of SEL-3622-R200-V0-Z007004-D20140616 with the following additions:</p> <ul style="list-style-type: none"> ➤ Resolved an issue where device access from SSH-enabled master ports could be attributed to the wrong user in activity logs. ➤ Resolved an issue with how privileges are assigned to users authenticating to an SSH scripting-enabled master port. 	20160203
SEL-3622-R200-V0-Z007004-D20140616	<ul style="list-style-type: none"> ➤ Enabled the physical sensors. ➤ Enabled the Eth F interface. ➤ Added Ethernet link-loss detection and alerting. ➤ Enabled Ethernet bridging. ➤ Added the Global Session Timeout setting to the web interface. ➤ Modified IRIG processing. ➤ Modified SSH processing. ➤ Modified ymodem passthrough behavior. ➤ Removed IM from the firmware image. 	20140616
SEL-3622-R142-V0-Z005004-D20140409	<ul style="list-style-type: none"> ➤ Updated OpenSSL. 	20140409
SEL-3622-R141-V0-Z005004-D20140404	<ul style="list-style-type: none"> ➤ Improved master port handling of multiple simultaneous scripts. ➤ Improved Syslog daemon boot process. ➤ Removed unnecessary DNS requests. 	20140404

Firmware ID (FID) Number	Summary of Revisions	Manual Date Code
SEL-3622-R139-V0-Z005004-D20131122	<ul style="list-style-type: none"> ➤ Updated open-source software components to current revisions. ➤ Added 2-wire EIA-485 support. ➤ Added Modbus/TCP protocol conversion. ➤ Added Modbus options to serial port configuration. ➤ Added whitelisting and self-diagnostic features to safeguard system integrity. ➤ Added SNMP management support. ➤ Added support for central authentication using RADIUS. ➤ Limit size of generated proxy report. ➤ Add Proxy functionality for FTP. ➤ Fixed delay between clock reference and IRIG signal output. 	20131122
SEL-3622-R138-V0-Z004003-D20130501	<ul style="list-style-type: none"> ➤ Improved logic for proxy access to devices through an SEL Communications Processor. ➤ Improved child password updates using an SEL Communications Processor. ➤ Improved robustness for password updates in tiered systems. 	20130501
SEL-3622-R136-V0-Z004003-D20121009	<ul style="list-style-type: none"> ➤ Initial version. 	20121009

Manual

The date code at the bottom of each page of this manual reflects the creation or revision date.

The following table lists the combined instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Manual Revision History

Date Code	Summary of Revisions
20241010	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Serial Ports, DC Output Ratings, and AC Output Ratings</i> in <i>SEL-3622 Specifications</i>.
20241001	<p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Commissioning Device</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 3.1: Administrative Accounts Features/Roles</i>. ➤ Updated <i>Removing a User and Enabling or Disabling a User</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 4.5: Add Syslog Destination</i> and <i>Figure 4.20: Add Syslog Destination</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 5.19: Network Settings</i>. ➤ Added <i>Address Groups and Port Groups, Syslog, Allowed Clients, SSH Protocol, and SSH Host Key</i>. ➤ Updated <i>Table 5.27: Serial Interface Settings</i>. ➤ Added <i>Key Exchange Algorithm</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>Firewall, NAT Global Settings, and Port Forwarding</i>. ➤ Updated <i>Figure 6.2: Default NAT Webpage</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 7.1: SEL-3620 Password Management Capabilities</i>.

Date Code	Summary of Revisions
	<p>Section 8</p> <ul style="list-style-type: none"> ➤ Updated <i>Password Jumper</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R215-V0 for the SEL-3610, the SEL-3620, and the SEL-3622. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
20231212	<p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Adding a User</i>, <i>Editing a User</i> and <i>Resetting a Password</i>, and <i>Changing a User Password</i>. ➤ Updated <i>Figure 3.2: Add User Form</i>, <i>Figure 3.3: Update User Form</i>, and <i>Figure 3.5: Change Password</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ [Cybersecurity] Updated for firmware version R214-V0 for the SEL-3610, the SEL-3620, and the SEL-3622. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.3: SEL-3622 Firmware</i>. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
20231004	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R213-V2 for the SEL-3610, the SEL-3620, and the SEL-3622.
20230601	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R213-V1 for the SEL-3610, the SEL-3620, and the SEL-3622. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Downgrading Firmware to an Earlier Revision</i>.
20230112	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R213-V0 for the SEL-3610, the SEL-3620, and the SEL-3622. ➤ Removed table captions and added the following headings: <i>SEL-3610 Firmware Revision History</i>, <i>SEL-3620 Firmware Revision History</i>, <i>SEL-3622 Firmware Revision History</i>, and <i>Manual Revision History</i>. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>, <i>Table B.2: SEL-3620 Firmware</i>, and <i>Table B.3: SEL-3622 Firmware</i>.
20221003	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Specifications</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Commissioning Device</i>, <i>Navigating the interface</i>, and <i>The Device Dashboard</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 3.1: Administrative Accounts Features/Roles</i>. ➤ Updated <i>Figure 3.15: Group Mappings</i>. ➤ Updated <i>Using RADIUS</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Manage Users and Collect Logs at a Central Location</i>. ➤ Updated <i>Figure 4.12: Add New Profile</i>, <i>Figure 4.13: Assign Serial Interface Settings</i>, <i>Figure 4.29: Port Profile DNP Port Settings</i>, <i>Figure 4.30: Serial Port Enabled and Updated</i>, and <i>Figure 4.49: Adding the Firewall Rule</i>.

Date Code	Summary of Revisions
	<p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Commissioning Page</i>. ➤ Updated <i>IRIG-B</i>. ➤ Updated <i>Settings and Commands</i>. ➤ Updated <i>Table 5.11: Network Interface Capabilities</i>. ➤ Modified <i>Disable Unused Ports</i>. ➤ Updated <i>Table 5.16: Static Route Settings</i>. ➤ Updated <i>Syslog</i>. ➤ Updated <i>Table 5.18: Syslog General Settings</i>. ➤ Updated <i>Figure 5.26: Serial Ports Page</i>. ➤ Updated <i>Table 5.21: Serial Interface Settings</i>. ➤ Updated <i>Table 5.27: Add Ethernet Listen Local Master Port Form Settings</i>. ➤ Updated <i>Table 5.29: Device Capability Matrix</i>. ➤ Updated <i>Figure 5.40: Terminal Access to Master Port</i>. ➤ Added <i>Figure 5.52: Security Settings</i>. ➤ Updated <i>SSH Host Key</i>. ➤ Updated <i>Figure 5.56: Adding an SNMP v1/v2c Profile</i> and <i>Figure 5.57: Adding an SNMP v3 Profile</i>. ➤ Updated <i>Reports</i>. ➤ Updated <i>Diagnostics</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 6.2: General Rule Settings</i>. ➤ Added <i>Table 6.13: SEL - Secure (2022) Profile</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Management of GE Devices</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R212-V0 for the SEL-3610, the SEL-3620, and the SEL-3622. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>, <i>Table B.2: SEL-3620 Firmware</i>, and <i>Table B.3: SEL-3622 Firmware</i>.
20220712	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>SEL-3620 and SEL-3622 Features in Product Features</i>. ➤ Updated <i>Figure 1.11: SEL-3622 Communication Encryption</i>. ➤ Updated <i>Ethernet Protocols in SEL-3610 and SEL-3620 Specifications</i>. ➤ Updated <i>Ethernet Protocols in SEL-3622 Specifications</i>. ➤ Added <i>MACsec to Security in SEL-3622 Specifications</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 2.14: Device Status Dashboard</i>. ➤ Updated <i>Figure 2.17: Device Dashboard</i>. ➤ Updated <i>Ethernet Connections in The Device Dashboard</i>. ➤ Updated <i>Figure 2.20: System Statistics</i>. ➤ Updated <i>Table 2.3: System Statistics</i>. ➤ Updated <i>Figure 2.23: Connection Status</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 3.1: Administrative Accounts Features/Roles</i>. ➤ Updated <i>Centralized User Accounts With LDAP</i>. ➤ Updated <i>Configuring Your RADIUS Server in Using RADIUS</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Introduction</i>. ➤ Updated <i>Figure 4.48: Completed SEL-3620 Interface</i>. ➤ Added <i>Job Done Example 8: Commissioning MACsec With an SEL-651RA Recloser Control</i>.

Date Code	Summary of Revisions
	<p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 5.11: Network Interface Capabilities</i>. ➤ Added Notes in <i>Network Settings</i>. ➤ Updated <i>Figure 5.20: Configured Addresses</i>. ➤ Updated <i>Figure 5.21: Disable USB B</i>. ➤ Updated <i>Settings and Commands</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Added <i>MACsec Connections</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>LDAP on QuickSet and the SEL-3620 in Centralized User Groups in QuickSet and the SEL-3620</i>. ➤ Updated <i>Creating RADIUS Proxy Services Groups on the SEL-3620 in RADIUS in QuickSet and the SEL-3620</i>. ➤ Updated <i>For Centralized Users in Unable to Successfully Log In to the SEL-3620 SMP</i>. <p>Section 8</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 8.5: Troubleshooting Procedure</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R211-V0 for the SEL-3610, the SEL-3620, and the SEL-3622. ➤ Updated general description of firmware revision R210-V0 and removed an incorrect firmware revision statement for a [Cybersecurity] vulnerability that was addressed during firmware R210-V0 development and was not present in any released firmware. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>, <i>Table B.2: SEL-3620 Firmware</i>, and <i>Table B.3: SEL-3622 Firmware</i>. ➤ Updated <i>Downgrading Firmware to an Earlier Revision</i>. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Added <i>MACsec Configuration</i> to <i>Table F.3: Syslog Messages</i>. <p>Appendix O</p> <ul style="list-style-type: none"> ➤ Added <i>Appendix O: Media Access Control Security (MACsec)</i>. <p>Glossary</p> <ul style="list-style-type: none"> ➤ Added MACsec terms.
20220429	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Common Features in Product Features</i>. ➤ Updated <i>Ethernet Filtering in SEL-3620 Applications</i>. ➤ Updated <i>Table 1.9: Serial DB-9 Port Pinout</i>. ➤ Updated <i>Discrete Input Connections (SEL-3610/SEL-3620 Only)</i>. ➤ Updated <i>SEL-3610 and SEL-3620 Specifications</i>. ➤ Updated <i>SEL-3622 Specifications</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated device requirements in <i>Connecting to the Device</i>. ➤ Updated <i>The Physical Network in Connecting to the Device</i>. ➤ Updated <i>Figure 2.4: Ethernet Commissioning Network</i>. ➤ Added <i>Figure 2.5: USB Commissioning Network</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 3.1: Administrative Accounts Features/Roles</i>.

Date Code	Summary of Revisions
	<p>Section 5</p> <ul style="list-style-type: none"> ➤ Added note in <i>Bit Based Processing Mode</i>. ➤ Updated <i>Bit Based Processing Latency</i> in <i>Bit Based Processing Mode</i>. ➤ Updated <i>Table 5.7: Service Port Commands</i>. ➤ Updated <i>Table 5.22: One-Way Bit-Time Delays</i>. ➤ Updated <i>Using the Master Port in Port Mappings</i>. ➤ Updated <i>Table 5.30: Master Port Commands</i>. ➤ Updated <i>SSH Protocol</i> in <i>Security</i>. ➤ Updated <i>SSH Host Key</i> in <i>Security</i>. ➤ Updated <i>Table 5.37: Supported MIBs</i>.
	<p>Section 6</p> <ul style="list-style-type: none"> ➤ Added <i>Automatic Firewall Rules</i> under <i>Firewall</i>. ➤ Updated <i>IPsec Connections</i>.
	<p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>General Information About SEL-3620 Password Management, IED Proxy, and QuickSet User Authentication Capabilities</i>. ➤ Updated <i>Table 7.1: SEL-3620 Password Management Capabilities</i>. ➤ Updated <i>Access and Terminate Scripts on Managed IEDs</i> in <i>Using the SEL-3620 Proxy Services</i>. ➤ Updated <i>Disaster Recovery</i> in <i>Implementing Password Management</i>. ➤ Updated <i>FTP Proxy Responds With “530 Invalid User Credentials”</i> in <i>Management of Ethernet-Connected IEDs</i>. ➤ Updated <i>Other FTP Proxy Connectivity Issues</i> in <i>Management of Ethernet-Connected IEDs</i>. ➤ Updated <i>Child Password Update (CPU) Failure—Possible Causes</i> in <i>Management of SEL Communications Processors</i>. ➤ Added <i>Password Management</i> on <i>SSH Devices</i> in <i>Management of GE Devices</i>.
	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R210-V0 and R209-V0 for SEL-3610, SEL-3620, and SEL-3622, and R208-V1 for SEL-3610.
	<p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>. ➤ Updated <i>Table B.2: SEL-3620 Firmware</i>. ➤ Updated <i>Table B.3: SEL-3620 Firmware</i>. ➤ Added <i>Special Firmware Upgrade Process</i>. ➤ Updated <i>Downgrading Firmware to an Older Revision</i>.
	<p>Appendix C</p> <ul style="list-style-type: none"> ➤ Updated <i>Maintain Backups</i> in <i>Replacing a Damaged SEL-3620</i>. ➤ Updated <i>Configuring a Replacement Unit</i> in <i>Replacing a Damaged SEL-3620</i>.
	<p>Appendix D</p> <ul style="list-style-type: none"> ➤ Added <i>File Transfer Protocol</i> in <i>Ethernet Services—Client</i>.
	<p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
	<p>Appendix K</p> <ul style="list-style-type: none"> ➤ Updated <i>X.509 Certificates</i>.
	<p>Appendix N</p> <ul style="list-style-type: none"> ➤ Updated <i>Introduction</i>. ➤ Updated <i>TLS</i>. ➤ Updated <i>Table N.1: TLSv1.2 Cipher List</i>. ➤ Added <i>Table N.2: TLSv1.3 Cipher List</i>.

Date Code	Summary of Revisions
20210622	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>SEL-3610 and SEL-3620 Specifications</i>. ➤ Updated <i>SEL-3622 Specifications</i>.
20210426	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R208-V3 and R207-V3 for SEL-3610, SEL-3620, and SEL-3622.
20210324	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated UL certification in <i>SEL-3622 Specifications</i>.
20201216	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R208-V2 for SEL-3610, SEL-3620, and SEL-3622.
20200918	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Added <i>Example EIA-485 Wiring Scenarios</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R207-V2 and R208-V1 for SEL-3620 and SEL-3622.
20200629	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Added bullet to R206-V2, R207-V1, and R208 entries in <i>Table A.2: SEL-3620 Firmware Revision History</i> and <i>Table A.3: SEL-3622 Firmware Revision History</i>.
20200624	<p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 4.19: Syslog Configuration Page</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 5.10: File Management Window</i>. ➤ Added information regarding single-file backup in <i>File Management</i>. ➤ Added <i>Disable USB B</i> under <i>Network</i>. ➤ Updated <i>Figure 5.25: Syslog General Settings</i>. ➤ Updated <i>Table 5.15: Syslog General Settings</i>. ➤ Updated <i>Table 5.30: Master Port Commands</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 6.1: Firewall Rules</i>. ➤ Updated <i>Table 6.3: Firewall Rules Settings</i>. ➤ Updated <i>Verbose Logging</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Added <i>Custom Scripts Created by User</i> under <i>Network Address Translation</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R206-V2, R207-V1, and R208-V0 for SEL-3610, SEL-3620, and SEL-3622. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Downgrading Firmware to an Older Revision</i>. ➤ Updated <i>Figure B.1: File Management Window</i>.
20200416	<ul style="list-style-type: none"> ➤ Updated for information incorrectly removed from 20200326 version.
20200326	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Added UL MX certification to <i>SEL-3622 Specifications</i>.
20191031	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Common Features</i>. ➤ Updated <i>Figure 1.18: SEL-3622 Rear-Panel Diagrams</i>. ➤ Updated <i>SEL-3610 and SEL-3620 Specifications</i>. ➤ Updated <i>SEL-3622 Specifications</i>.

Date Code	Summary of Revisions
	<p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 2.13: Device Status Dashboard</i>, <i>Figure 2.16: Device Dashboard</i>, <i>Figure 2.17: Network Interfaces</i>, and <i>Figure 2.22: Connection Status</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 5.16: Network Interfaces</i>. ➤ Updated <i>Figure 5.25: Serial Interface Settings Form</i>. ➤ Updated <i>Table 5.21: Serial Interface Settings</i>. ➤ Updated <i>Table 5.37: Supported MIBs</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R207-V0. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
20180803	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Virtual Private Networks (SEL-3620 Only)</i> in <i>Specifications</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R206-V1, R205-V2, R204-V4, and R203-V5. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
20180525	<p>Preface</p> <ul style="list-style-type: none"> ➤ Updated <i>Technical Support</i>. <p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 1.17: SEL-3622 Front-Panel Diagram</i> and <i>Figure 1.18: SEL-3622 Rear-Panel Diagrams</i>. ➤ Updated <i>Proxy Services (SEL-2620 only)</i> in <i>SEL-3610 and SEL-3620 Specifications</i> and <i>Proxy Services in SEL-3622 Specifications</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 3.2: Description of RADIUS Settings</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>X.509 Certificate Chain of the LDAP Server</i> and <i>Add the Hostname and IP Address Mapping of the LDAP Server</i>. ➤ Added <i>Job Done Example 7: Using VLANs on the SEL-3620 With a Managed Ethernet Switch</i>. ➤ Added <i>Figure 4.49: Add the Firewall Rule</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>IRIG-B, File Management and SSH Protocol under System</i>. ➤ Updated <i>Table 5.1: Commissioning Settings</i>, <i>Table 5.2: IRIG-B Output Quality Settings</i>, <i>Table 5.3: NPT Server Settings</i>, and <i>Table 5.8: Global Network Settings</i>. ➤ Added <i>Table 5.9: TCP Keep-Alive Settings</i>. ➤ Updated <i>Table 5.13: Network Address Form Settings</i>, <i>Table 5.14: Bridge Interface Form Settings</i>, <i>Table 5.19: Serial Interface Settings</i>, and <i>Table 5.21: Serial Interface Settings</i>. ➤ Added <i>Port Mappings</i> heading above <i>Introduction to Port Mappings</i>. ➤ Updated <i>Table 5.24: Add Serial Form Settings</i>, <i>Table 5.25: Add Serial Master Port Form Settings</i>, <i>Table 5.26: Add Ethernet Listen Local Form Settings</i>, <i>Table 5.27: Add Ethernet Listen Local Master Port Form Settings</i>, and <i>Table 5.28: Add Ethernet Connect Remote Form Settings</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 6.3: Firewall Rule Settings</i>. ➤ Updated <i>Figure 6.3: Outbound NAT Example</i>. ➤ Updated <i>IPsec Connections</i>.

Date Code	Summary of Revisions
	<p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 7.1: SEL-3620 Password Management Capabilities.</i> ➤ Updated <i>Winsock Error Code: -1 under Troubleshooting.</i> ➤ Updated <i>Introduction, Password Management Theory of Operation, and Safety Tips for SEL-3620 Password Management under Implementing Password Management.</i> ➤ Added <i>Managed Device List, Manual Password Management, Aborting a Password Operation, Including and Excluding Managed Devices, Managing Password Persistence, and Clearing Proposed Passwords under Password Management Connection Directory Scripts.</i> ➤ Added <i>Figure 7.85: Managed Device List.</i> ➤ Added <i>Figure 7.86: Manual Password Management.</i> ➤ Updated <i>Figure 7.88: Password Management Device Selection.</i> ➤ Updated <i>Generating IED Passwords, Applying IED Passwords, Reverting IED Passwords to Default, and Assigning Password under Password Management Connection Directory Scripts.</i> ➤ Updated <i>Communications Processor Scenario FAQ under Management of SEL Communications Processors.</i> ➤ Updated <i>Figure 7.177: Connection Directory Export Select Data Window.</i> ➤ Updated <i>Configuring a New QuickSet Instance From a Backup Connection Directory.</i> ➤ Updated <i>Figure 7.179: New Imported Connection Directory and Figure 7.188: SEL-3620 Team Configuration.</i> <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R206. <p>Appendix K</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure K.4: Digital Signatures.</i>
20180122	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R205-V1.
20171026	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Web Management in SEL-3610 and SEL-3620 Specifications and SEL-3622 Specifications.</i> <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Configuring Your RADIUS Server.</i> <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Using the Master Port.</i> <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 6.8: IPsec Using X.509 Certificates Settings.</i> <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Proxy Services.</i> ➤ Updated <i>Password Management Theory of Operation.</i> ➤ Updated <i>Generating IED Passwords.</i> ➤ Updated <i>Applying IED Passwords.</i> ➤ Updated <i>Reverting IED Passwords to Default.</i> ➤ Renamed <i>Manual Password Updates to Assigning Passwords</i> and updated. ➤ Updated <i>Password Change Scheduler.</i> ➤ Added <i>Managed Device Check Out.</i> ➤ Updated <i>Troubleshooting.</i> <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R205. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages.</i> <p>Appendix M</p> <ul style="list-style-type: none"> ➤ Updated Appendix.

Date Code	Summary of Revisions
	Appendix N ► Added new <i>Appendix N: Web Server Security With Transport Layer Security.</i>
20170714	Section 1 ► Added <i>Proxy Services</i> in <i>SEL-3610 and SEL-3620 Specifications</i> and <i>SEL-3622 Specifications</i> . ► Updated <i>Ethernet Protocols</i> and <i>System Speeds</i> in <i>SEL-3610 and SEL-3620 Specifications</i> and <i>SEL-3622 Specifications</i> . Section 5 ► Added <i>SSH Protocol</i> . ► Added <i>SSH ciphers</i> . Appendix A ► Updated for firmware versions R200-V3, R201-V3, R203-V4, R204-V3.
20170605	Section 1 ► Updated <i>Table 1.6: Conditions for SEL-3610/SEL-3620 Alarm Contacts</i> . ► Updated <i>Table 1.12: Conditions for SEL-3622 Alarm Contacts</i> . ► Added <i>RCM Mark</i> in <i>SEL-3610 and SEL-3620 Specifications</i> .
20170512	Preface ► Updated <i>Safety Information</i> . Section 1 ► Updated <i>Discrete Input Connections (SEL-3610/SEL-3620 Only)</i> . ► Updated <i>Power Supply Connections</i> . ► Updated <i>Discrete Input Connections (SEL-3622 Only)</i> . Section 5 ► Updated <i>Table 5.32: X.509 Generation Settings</i> . ► Updated <i>exe-GUARD</i> . ► Added <i>SEL SNMP MIBs and Testing</i> . Section 6 ► Updated <i>IPsec Connections</i> .
20170510	Appendix A ► Updated for firmware versions R203-V3 and R204-V2.
20170407	Appendix A ► Updated for firmware version R200-V2, R201-V2, and R203-V2.
20170321	Appendix A ► Updated for firmware version R204-V1. Appendix B ► Updated <i>Table B.1: SEL-3610 Firmware</i> , <i>Table B.2: SEL-3620 Firmware</i> , and <i>Table B.3: SEL-3622 Firmware</i> .
20160728	Section 1 ► Added <i>Firewall</i> in <i>SEL-3610 and SEL-3620 Specifications</i> and <i>SEL-3622 Specifications</i> . ► Updated <i>Digital Inputs</i> in <i>SEL-3610 and SEL-3620 Specifications</i> . Section 2 ► Updated <i>Figure 2.11: Device Commissioning Page</i> . Section 3 ► Added <i>Table 3.1: Administrative Accounts Features/Roles</i> . Section 5 ► Added <i>exe-GUARD</i> .

Date Code	Summary of Revisions
	<p>Section 7</p> <ul style="list-style-type: none"> ➤ Added GDID character list in <i>Testing Connectivity Between QuickSet and the SEL-3620</i>. <p>Section 8</p> <ul style="list-style-type: none"> ➤ Changed “access jumper” to “password jumper” throughout the section. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R204. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>, <i>Table B.2: SEL-3620 Firmware</i>, and <i>Table B.3: SEL-3622 Firmware</i>. <p>Appendix D</p> <ul style="list-style-type: none"> ➤ Updated the network port table.
20160212	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>SEL-3622 Specifications</i>. ➤ Added <i>Table 1.6: Conditions for SEL-3610/SEL-3620 Alarm Contacts</i> and <i>Table 1.12: Conditions for SEL-3622 Alarm Contacts</i>. ➤ Updated <i>SEL-3622 Connections and LED Indicators</i> for new options.
20160203	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware versions R203-V1, R201-V1, and R200-V1. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.1: SEL-3610 Firmware</i>, <i>Table B.2: SEL-3620 Firmware</i>, and <i>Table B.3: SEL-3622 Firmware</i> for firmware versions R200-V1, R201-V1, and R203-V1.
20151230	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Added Service Port to <i>Common Features</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 2.13: Front Dashboard Page</i>, <i>Figure 2.14: User Accounts</i>, and <i>Figure 2.16: Device Dashboard</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 3.8: LDAP Login Process</i> and <i>Figure 3.16: RADIUS Settings</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 5.3: System Settings</i>. ➤ Changed name of <i>Web Server to Management Interface</i> and updated the section. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>NAT Implementation Specifics</i> to include maximum number of port forward entries. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 7.9: Select the Is Managed Check Box in the SEL-3620 Template</i>. ➤ Added <i>Using Multifactor Authentication with QuickSet and FTP Proxy</i>. ➤ Updated firmware versions called out in <i>Management of SEL Communications Processors</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R203. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>. <p>Appendix L</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure L.1: LDAP Transaction</i>.

Date Code	Summary of Revisions
20150916	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated <i>Product Features</i>. ➤ Updated <i>Specifications</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 2.13: SEL-3620 Front Dashboard Page</i>. ➤ Updated <i>Figure 2.16: Device Dashboard</i>. ➤ Updated <i>Configuring Your RADIUS Server</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 4.4: Syslog Configuration Page</i>. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 5.22: Syslog</i>. ➤ Added <i>Syslog General Settings</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Added <i>Verbose Logging</i>. ➤ Added <i>Network Address Translation</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 7.2: SEL-3620 IED Proxy Capabilities</i>. ➤ Added <i>Testing the Connectivity Between QuickSet and the SEL-3620</i>. ➤ Updated <i>Troubleshooting</i>. ➤ Updated <i>The SEL-3620 SELF Controller</i>. ➤ Updated <i>Communications Processor Scenario FAQ</i>. <p>Section 8</p> <ul style="list-style-type: none"> ➤ Updated <i>Diagnostics Page</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R202 (SEL-3620 and SEL-3622 only). <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Table B.2: SEL-3620 Firmware</i> and <i>Table B.3: SEL-3622 Firmware</i> for firmware version R202. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i>.
20150227	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Added UDP option for sending serial data over Ethernet. ➤ Updated <i>Product Features</i>. ➤ Updated <i>Discrete Input Connections</i>. ➤ Added <i>Table 1.12: Jumper Location</i> and <i>Figure 1.21: JMP1 Location</i>. ➤ Updated <i>Specifications</i>. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 2.22: Connection Status</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 3.11: LDAP Settings</i>. ➤ Updated <i>Group Mappings</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Create a Serial Port Profile</i>. ➤ Removed <i>Job Done Example 4: Automated IED Password Management</i> and <i>Job Done Example 5: Secure Engineering Access</i>. ➤ Added <i>Job Done Example 4: Secure DNP serial to DNP UDP Conversion over a Cellular Network</i>.

Date Code	Summary of Revisions
	<p>Section 5</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 5.8: Network Interface Capabilities</i>. ➤ Updated screen shots throughout section. ➤ Updated <i>Table 5.17: Serial Interface Settings</i>. ➤ Added UDP protocol. ➤ Updated <i>Ethernet Listen Local Device</i> and <i>Ethernet Connect Remote Device</i>. ➤ Updated <i>Table 5.26: Serial Diagnostics Explanation</i>. ➤ Updated <i>Allowed Clients</i>. ➤ Added <i>Physical Sensors</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Moved <i>Physical Sensors</i> to <i>Section 5</i>. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Moved <i>Appendix M: Proxy Services and Password Management</i> to become the new <i>Section 7</i>. ➤ Updated <i>Troubleshooting</i>. ➤ Updated <i>Proxy Services FAQ</i>. ➤ Added <i>Notes on SEL-2030 and SEL-2032 Firmware Versions</i>. ➤ Added explanations of the effects of SEL-2030 firmware version R126 and later and SEL-2032 firmware version R115 or later on the process of updating passwords. ➤ Updated <i>Communications Processor Scenario FAQ</i>. <p>Section 8</p> <ul style="list-style-type: none"> ➤ Updated <i>Table 8.5: Troubleshooting Procedure</i>. ➤ Updated <i>Access Jumper</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R201. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R201. ➤ Added <i>Obtaining GPLv2 Code from SEL</i>. <p>Appendix M</p> <ul style="list-style-type: none"> ➤ Added new <i>Appendix M: SEL RADIUS Dictionary</i>.
20150126	<p>Preface</p> <ul style="list-style-type: none"> ➤ Updated <i>Safety Information</i>. <p>Section 1</p> <ul style="list-style-type: none"> ➤ Changed <i>Certifications to Compliance</i> and moved it to the beginning of <i>Specifications</i>.
20141201	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Updated certification information in SEL-3622 specifications.
20140616	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Clarified rear connector pin designations. ➤ Added physical sensors description. ➤ Applied bridging to SEL-3622. ➤ Added exe-GUARD description. ➤ Modified alarm contact behavior description. ➤ Clarified auto-crossover description for SEL-3622. ➤ Removed maximum centralized accounts from specifications. ➤ Added spanning tree to SEL-3622 specifications. ➤ Added Eth F to SEL-3622.

Date Code	Summary of Revisions
	<p>Section 2</p> <ul style="list-style-type: none"> ➤ Added light sensor physical description. ➤ Clarified differences among the SEL-3610, SEL-3620, and SEL-3622. ➤ Changed SEL-3622 commissioning instructions. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Clarified differences among the SEL-3610, SEL-3620, and SEL-3622. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Job Done Example 6: Secure a Remote Connection for the SEL-5020 Settings Assistant</i> to use SEL-5828 software. ➤ Added Job Done example to detect physical tampering. ➤ Clarified differences among the SEL-3610, SEL-3620, and SEL-3622. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Clarified differences among the SEL-3610, SEL-3620, and SEL-3622. ➤ Added description of Global Session Timeout setting. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Added physical sensors settings and descriptions. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware revision R200. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Added information about downgrading firmware below R200. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Added new Syslog messages. <p>Appendix M</p> <ul style="list-style-type: none"> ➤ Added new <i>Appendix M: Proxy Services and Password Management</i>. <p>Glossary</p> <ul style="list-style-type: none"> ➤ Added new terms.
20140409	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware revision R142.
20140404	<p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware revision R141.
20140107	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Moved exe-GUARD, RADIUS, and SNMP to <i>Common Features</i>. ➤ Updated protocol lists in <i>Specifications</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 3.19: Selecting the RADIUS Authentication Type</i> to show correct RADIUS options. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware revision R140. ➤ Updated description of firmware revision R139. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i> adding Syslog messages for RADIUS and SNMP support.

Date Code	Summary of Revisions
20131122	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Added Modbus translation and RADIUS support for the SEL-3620 and SEL-3622 and exe-GUARD to SEL-3620 to feature list in <i>Product Features</i>. ➤ Updated <i>Table 1.1: Serial DB-9 Port Pinout</i>, <i>Table 1.2: Isolated Port Pinout</i>, <i>Table 1.7: Serial DB-9 Port Pinout</i>, and <i>Table 1.8: Ethernet Port Option</i>. ➤ Added <i>Discrete Input Connections (3620/3622 Only)</i> in <i>SEL-3622 Connections and LED Indicators</i>. ➤ Updated <i>SEL-3610 and SEL-3620 Specifications</i> and <i>SEL-3622 Specifications</i> to add SNMP and RADIUS protocols and fiber-optic interface specifications information, and added accelerated and nonaccelerated cryptographic protocols to <i>SEL-3622 Specifications</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated <i>LDAP Settings</i>. ➤ Added <i>Using RADIUS With the SEL-3620</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure 4.30: Change All Passwords Now Dialog Box</i>. ➤ Updated <i>Job Done Example 1–5</i> and added <i>Job Done Example 6</i> for user interface changes made to SEL-3610, SEL-3620, and SEL-3622 and to ACCELERATOR QuickSet. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Added bridge STP configuration parameters to <i>Network Settings</i>. ➤ Added <i>Using Modems in Serial Ports</i>. ➤ Added <i>SNMP (SEL-3620/SEL-3622 Only)</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Updated <i>IPsec Information</i>. ➤ Updated <i>Figure 6.3: Add IPsec Using Passphrase Form</i>. ➤ Updated <i>Table 6.7: Lemnos IKEv2 Profile</i>, <i>Table 6.8: Lemnos IKEv1 Profile</i>, and <i>Table 6.9: Cisco Profile</i>. ➤ Added <i>FTP Proxy to Proxy Services</i>. ➤ Updated <i>Figure 6.8: Change All Passwords Now</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware revision R139. <p>Appendix B</p> <ul style="list-style-type: none"> ➤ Updated <i>Figure B.2: Select Firmware File</i>. <p>Appendix C</p> <ul style="list-style-type: none"> ➤ New <i>Appendix C: Best Practices for Emergency Readiness</i>. <p>Appendix D</p> <ul style="list-style-type: none"> ➤ New <i>Appendix D: Open Network Ports</i>. <p>Appendix F</p> <ul style="list-style-type: none"> ➤ Updated <i>Table F.3: Syslog Messages</i> to show new input contact syslog messages. <p>Glossary</p> <ul style="list-style-type: none"> ➤ Added RADIUS definition.
20130604	<p>Appendix B</p> <ul style="list-style-type: none"> ➤ Added <i>Upgrading Firmware From Older Versions</i>. ➤ Removed <i>Table B.1: SEL-3610/SEL-3620/SEL-3622 Watershed Revisions</i>.

Date Code	Summary of Revisions
20130501	Appendix A ► Updated for firmware version R138.
20121207	Section 4 ► Updated <i>Figure 4.12: Add New Profile</i> . Section 5 ► Add Maximum Frame Length to <i>Table 5.17: Serial Interface Settings</i> . Appendix A ► Updated for firmware version R137.
20121009	Appendix A ► Updated for SEL-3622 release.
20120928	Section 1 ► Added SEL-3622 description and specifications. Section 2 ► Added SEL-3622 installing information. Section 4 ► Added SEL-3622 as alternative to the SEL-3620. Section 5 ► Added SEL-3622. ► Removed references to 2-wire RS-485. Section 7 ► Added description of the SEL-3622 indicators. Appendix A ► Updated for firmware version R135. Appendix B ► Added firmware update instructions for SEL-3622. ► Added information about nondowngradable versions.
20120815	Appendix A ► Updated for firmware version R134.
20120119	Section 1 ► Updated Type Test information in <i>Specifications</i> . Section 2 ► Changed port name to which the default IP address is assigned in <i>Commissioning the Device</i> . Section 3 ► Updated <i>Figure 3.12: Edit LDAP Settings</i> . ► Revised description of LDAP search base and User ID form in <i>LDAP Settings</i> .

Date Code	Summary of Revisions
	<p>Section 4</p> <ul style="list-style-type: none"> ➤ Added port information to <i>Step 6</i> in <i>Create Serial Mappings</i>. ➤ Updated <i>Figure 4.14: Add Ethernet Local Driver</i>. ➤ Revised <i>Step 11</i> in <i>Create Serial Mappings</i>. ➤ Added new <i>Job Done Example 3</i>. ➤ Updated version number of ACCELERATOR QuickSet in <i>Defining the Solution in Job Done Example 4</i>. ➤ Added new <i>Step 1</i> in <i>Configure the Local Users and Groups</i>. ➤ Updated <i>Build the Connection Directory</i> in ACCELERATOR QuickSet. ➤ Added <i>Configuring the Device Users and Groups</i> in <i>Job Done Example 4</i>. ➤ Updated <i>Figure 4.43: Assign Technician Permissions</i>. ➤ Added <i>Figure 4.45: Communication With the SEL-351 Via the SEL-3620 Using SSH</i>.
20111014	<p>Section 1</p> <ul style="list-style-type: none"> ➤ Removed two-wire information from <i>Table 1.1: Serial DB-9 Port Pinout</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R133.
20110902	<p>Section 3</p> <ul style="list-style-type: none"> ➤ Added Local User Groups. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R132.
20110729	<p>General</p> <ul style="list-style-type: none"> ➤ Combined SEL-3610 and SEL-3620 into one manual. <p>Section 1</p> <ul style="list-style-type: none"> ➤ Clarified DNP conversion functions. ➤ Added <i>Modem Support</i>. ➤ Updated <i>Specifications</i>. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Added Local User Groups. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Created new Job Done examples to reflect new features. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Added and Modified Serial Configuration. ➤ Moved Security Settings to <i>Section 6</i>. <p>Section 6</p> <ul style="list-style-type: none"> ➤ Changed title to <i>Security Settings</i>. ➤ Added proxy function descriptions. <p>Section 7</p> <ul style="list-style-type: none"> ➤ Moved Troubleshooting and Diagnostics information to <i>Section 7</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R130. <p>Appendix D</p> <ul style="list-style-type: none"> ➤ Added new Syslog messages.
20110415	<p>SEL-3610</p> <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added 24/48 Vdc and single-mode fiber hardware options. ➤ Updated certification information in <i>Specifications</i>. ➤ Added UL listing information in <i>Specifications</i>.

Date Code	Summary of Revisions
20110210	<p>SEL-3620</p> <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added 24/48 Vdc and single-mode fiber hardware options.
20100831	<p>SEL-3620</p> <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added text for mixed Ethernet port option. <p>Section 2</p> <ul style="list-style-type: none"> ➤ Modified text to account for change in default Ethernet port. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Added text and images for LDAP. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Modified and added images for Job Done 2. <p>Section 5</p> <ul style="list-style-type: none"> ➤ Added text for NAT-T. ➤ Modified text for Allowed Client changes. ➤ Added text for DHCP. ➤ Modified text for Factory Reset. ➤ Added firewall image descriptions. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R120. <p>Appendix D</p> <ul style="list-style-type: none"> ➤ Added list of Syslog messages. <p>Appendix J</p> <ul style="list-style-type: none"> ➤ Added <i>Appendix J</i> for LDAP settings form.
20100907	<p>SEL-3610</p> <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R122.
20100524	<p>SEL-3610</p> <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added Ethernet port bridging options. <p>Section 3</p> <ul style="list-style-type: none"> ➤ Updated job done execution steps. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R121. <p>Appendix C</p> <ul style="list-style-type: none"> ➤ Added <i>Appendix C: Syslog Logs</i>.
20100222	<p>SEL-3610</p> <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added Modbus TCP/IP option information. ➤ Updated complex password information in <i>SSH</i>. ➤ Updated Password Length in <i>Specifications</i>.

Date Code	Summary of Revisions
	<p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated Username and Password character lengths in <i>Table 4.1: Commissioning Settings</i>. ➤ Updated <i>Manage Port Mappings</i>. ➤ Added <i>Figure 4.17: Modbus Settings</i>. ➤ Added Modbus as a protocol in <i>Table 4.14: Serial Port Mapping Settings</i>. <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R110.
20100212	<p>SEL-3610 General</p> <ul style="list-style-type: none"> ➤ Changed ETH 1 to ETH F throughout. <p>Section 1</p> <ul style="list-style-type: none"> ➤ Added <i>Table 1.1: Non-Isolated Female DB-9 Ports EIA-232 EIA-485/EIA-422</i> and <i>Table 1.2: Isolated Port Pinout EIA-232 EIA-485/EIA-422</i>. ➤ Updated Serial Ports data rate in <i>Specifications</i>. <p>Section 4</p> <ul style="list-style-type: none"> ➤ Updated baud rate information in <i>Table 4.13: Serial Interface Settings</i>.
20100204	<p>SEL-3620</p> <p>Appendix A</p> <ul style="list-style-type: none"> ➤ Updated for firmware version R112.
20091209	<p>SEL-3610 General</p> <ul style="list-style-type: none"> ➤ Initial version.
20091113	<p>SEL-3620 General</p> <ul style="list-style-type: none"> ➤ Initial version.

This page intentionally left blank

APPENDIX B

Firmware Upgrade Instructions

Introduction

SEL occasionally offers firmware upgrades to improve the performance of your device. Your device stores firmware in nonvolatile memory, therefore, changing physical components is not necessary. These instructions give a step-by-step procedure to upgrade the device firmware by uploading a file from a personal computer to the gateway via the web interface. All firmware updates are logged.

Firmware releases are enhancements to improve functionality that change the way your device is configured or maintained and can be installed in increasing or decreasing order. All existing settings will be transferred to later firmware versions. Settings may not be transferred to an earlier firmware version. After a firmware update, it is possible to revert to the previously installed firmware version.

To perform an upgrade, you will need the appropriate firmware upgrade file(s) and access to an administrative account on the device.

Firmware Files

The firmware upgrade file has the tar.gz extension. An example firmware file name is 3620.R120.tar.gz.

Firmware files are cryptographically signed to enable the device to recognize official SEL firmware. Any uploaded files that cannot be verified as being produced by SEL will not be processed.

Upgrading Firmware From Earlier Revisions

Some firmware versions have special needs or restrictions on their upgrade path. It is important to know the current firmware version for your device and what requirements or restrictions your later firmware has. To aid you in this, the following tables list the released firmware for the SEL-3610, SEL-3620, and SEL-3622. The first column of each table lists the released firmware versions for each device. The second column lists the upgrade path, which includes any special files that may need to be applied before the later firmware will be accepted. The third column lists the target firmware. The fourth column provides restriction information on downgradability.

B.2 | Firmware Upgrade Instructions
Upgrading Firmware From Earlier Revisions

Table B.1 SEL-3610 Firmware

Firmware Version	Upgrade Path	Latest Firmware	Restrictions
R100	Direct	R122	None
R110			
R120			
R121	Preload-R132.tar.gz	R132	None
R122			
R132	Direct	R142	R132 and later cannot downgrade or revert to a version earlier than R132.
R133			
R137			
R140			
R142 or later	Upgrade incrementally no more than five versions at a time, then to R208-V3, and finally to R213 or later.	R213	R200 or later cannot downgrade to a version earlier than R200, but R208 and earlier can revert to a previous version. R210 or later cannot downgrade or revert to R208 or to any other previous version. R211 or later can only revert to R210 or later if it was previously installed.

Table B.2 SEL-3620 Firmware

Firmware Version	Upgrade Path	Latest Firmware	Restrictions
R110	Direct	R120	None
R112			
R120	Preload-R132.tar.gz	R132	None
R132	Direct	R142	R132 and later cannot downgrade or revert to a version earlier than R132.
R133			
R134			
R135			
R138			
R139			
R141			
R142 or later	Upgrade incrementally no more than five versions at a time, then to R208-V3, and finally to R213 or later.	R213	R200 or later cannot downgrade to a version earlier than R200, but R208 and earlier can revert to a previous version. R210 or later cannot downgrade or revert to R208 or to any other previous version. R211 or later can only revert to R210 or later if it was previously installed.

Table B.3 SEL-3622 Firmware

Firmware Version	Upgrade Path	Latest Firmware	Restrictions
R136	Direct	R142	None
R138			
R139			
R141			
R142 or later	Upgrade incrementally no more than five versions at a time, then to R208-V3, and finally to R213 or later.	R213	R200 or later cannot downgrade to a version earlier than R200, but R208 and earlier can revert to a previous version. R210 or later cannot downgrade or revert to R208 or to any other previous version. R211 or later can revert to R210 or later if it was previously installed. R214 can be downgraded to R213, R212, and R211.

There is a special upgrade process for upgrading to version R132 because of special startup requirements when installing that version. **Note that this process will reset your device to factory-default settings. Make certain to manually copy down your device settings or take screenshots before beginning the process.** You must carefully perform the following procedure to upgrade to R132:

- Step 1. Upgrade to the latest version of R12x firmware for your device.
- Step 2. From the device webpage, perform a factory-default reset by navigating to the **Reset** webpage.
- Step 3. Commission the device after performing the factory-default reset.
Load the Preload-R132.tar.gz file for your product from the CD.
- Step 4. Load the R132 firmware file (i.e., 3610.R132.tar.gz or 3620.R132.tar.gz). Note that this file must be loaded without rebooting the device after installing the preload file.
- Step 5. Wait for the system to start R132 by itself, and then wait ten full minutes.
- Step 6. Log in to the device and reboot the unit from the diagnostics page of the web UI (do not cycle power).

See *Firmware File Loading Procedure* on page B.4 for instructions on how to load individual upgrade files.

Special Firmware Upgrade Process

NOTE: Do not turn off the unit until the firmware upgrade is complete, or it may become non-functional.

Firmware revision R211-V1 requires a one-way upgrade path. Users will not be able to use the revert feature after performing the upgrade from a earlier firmware version to R211-V1. This upgrade process takes much longer than the normal upgrade process. To provide users with feedback on the status of the upgrade, the lights on the unit have been programmed to show that the upgrade process is working. The VPN, SYS, and CERT LEDs on the device front panel will flash green on and off in sequence during the upgrade of an SEL-3622. The VPN SYNC, TIME SYNC, and X.509 ERROR LEDs on the device front panel will flash green on and off in sequence during the upgrade of an SEL-3610 or SEL-3620. Once the firmware has been upgraded to the later version, subsequent firmware upgrades will go back to the normal process.

The upgrade could take up to 40 minutes with a large, complex connection directory of devices on the SEL-3620 and SEL-3622. Do not power off the unit during the upgrade process. This could prevent the unit from rebooting, and you would need to return the unit to SEL.

Beginning with firmware version R210, certificates used for IPsec Key Exchange (IKE) on the SEL-3620 and SEL-3622 that contain a keyUsage extension must also have either the digitalSignature or nonRepudiation bits set. This change makes the SEL-3620 and SEL-3622 more compliant with RFC 4945, section 5.1.3.2. Certificates that do not comply may cause the IKE process to fail, preventing a connection from being established. Ensure that any X.509 certificates used for IKE are compliant with RFC 4945, section 5.1.3.2 prior to upgrading to firmware version R211-V1 or later.

Downgrading Firmware to an Earlier Revision

Some firmware versions have unique requirements or restrictions on their downgrade or reversion path. It is important to know the current firmware version for your device and what requirements or restrictions might block downgrades or reversions. *Upgrading Firmware From Earlier Revisions* on page B.1 includes tables that provided information on downgrade restrictions. This section provides additional information on those restrictions.

NOTE: All device settings are removed during this process.

Firmware revision R200 was released with a new version of the SEL-3610, SEL-3620, and SEL-3622 circuit boards that replaced a number of obsolete components. Because these components require support from the firmware, the device would become inoperable if an earlier version of firmware were to be installed.

For this reason, firmware version R200 includes a feature that prevents loading a previous version of the firmware, though you can revert to an earlier version if it is already present on the device.

Firmware version R208 may be downgraded directly to R207 (any version) or to R206-V2. Versions R207 and later require using R206-V2 as the first step in a downgrade. Once R206-V2 has been installed, you may install any desired firmware version R200 through R206-V2.

Firmware version R210 includes many new features, such as an updated settings database. For this reason, R210 may not be downgraded or reverted to any earlier firmware version.

Firmware version R211 through R213-V1 includes support and drivers for new hardware components. For this reason, R211 through R213-V1 may not be downgraded to any earlier firmware version but may be reverted to the most recently installed version of R210 or later.

Table B.4 Firmware Downgrades and Reversions

Current Firmware Version	Downgradable to Versions	Reversion Allowed?
R211 through R213-V1	None	Yes (R210 or later)
R210	None	No
R208	R207, R206-V2, R200 to R206 ^a	Yes
R207	R206-V2, R200 to R206 ^a	Yes
R201 through R206-V2	R200 to R206	Yes
R200	None	Yes
R100 through R146 ^b	Not recommended	Not recommended

^a Downgrading from R207 or R208 to R206 or earlier requires an intermediate installation of R206-V2.

^b Contact SEL for more information.

Firmware File Loading Procedure

Perform the following steps to load a firmware file:

- Step 1. Access the device by using an account with administrative-level privileges. Nonadministrative accounts cannot perform firmware upgrades.
- Step 2. Select the **File Management** link from the navigation panel. This will show the File Management page, where firmware upgrades may be performed.

Step 3. In the File Management window, select **Firmware Update**, and select **Browse** to show a file browser window (see *Figure B.1*).

IMPORTANT: If you select **Firmware Update**, the system restarts as part of the upgrade process.

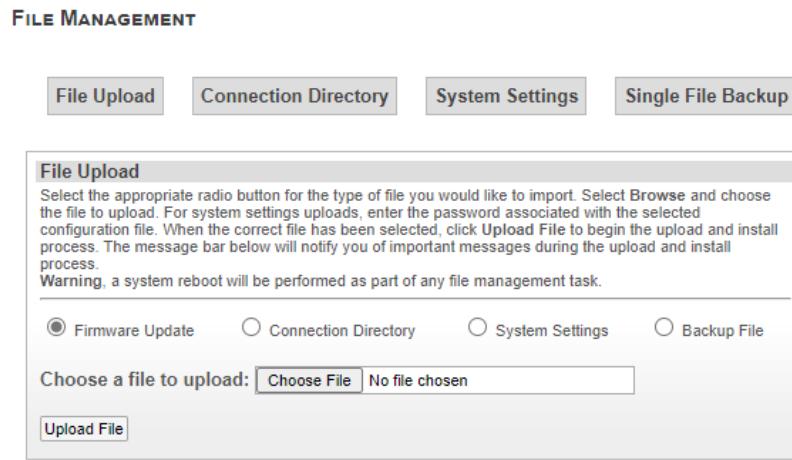


Figure B.1 File Management Window

Step 4. Navigate to the location the correct upgrade files are stored, and select it (see *Figure B.2*).

Step 5. Select **Open**.

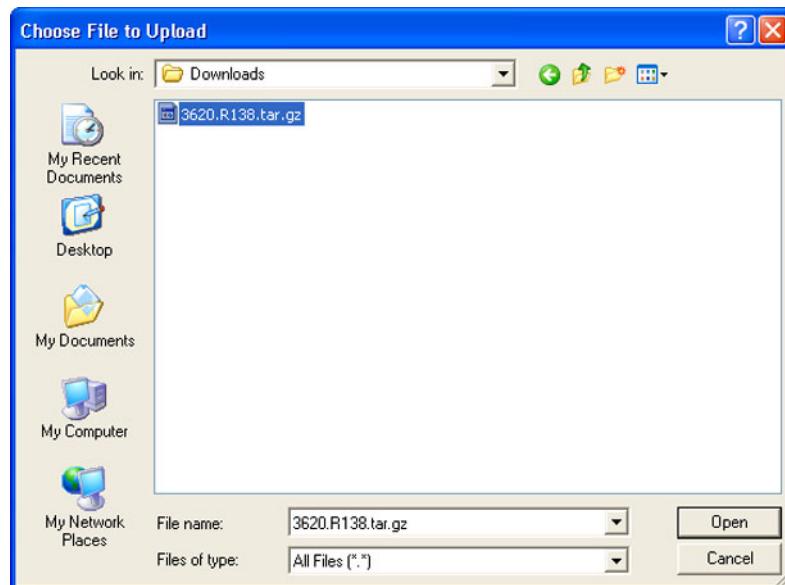


Figure B.2 Select Firmware File

Step 6. Select **Upload File** to upload and install the later firmware. Status messages will be displayed in the bar at the bottom of the page. These status messages will indicate success or failure.

During the firmware upgrade, the earlier firmware will be placed into the Previous Firmware slot. This firmware stays on the device until another firmware upgrade occurs. This feature allows for a quick recovery if a firmware upgrade causes system instability. Installing an upgrade can take between five and ten minutes to complete.

Reverting to Previous Firmware

Perform the following steps to revert the device to the previous firmware version. Settings will not transfer from your current firmware version to the backup firmware version. For easy reconfiguration, be sure to record the current system settings before reverting firmware. Firmware versions prior to R130 do not allow importing of system settings. Firmware versions R211 and later may only be reverted to R210 and later if the desired firmware was previously installed on the device.

Remember to refer to *Table B.1*, *Table B.2*, or *Table B.3* for downgrade or reversion restrictions that your firmware may have.

- Step 1. Access the device by using an account with administrative-level privileges. Nonadministrative accounts cannot perform firmware revisions.
- Step 2. Select the **File Management** link from the navigation panel. This will show the File Management page.
- Step 3. In the Firmware Version window, select **Revert** to change the firmware of the device to the Previous Firmware Version. After the process is completed, the previous firmware will become the current firmware and the current firmware will become the previous firmware, as in *Figure B.3*.

⚠ CAUTION

If you revert the firmware to a previous version, and then go through a firmware upgrade process, your device will inherit the settings that were on the unit immediately before the revert function was activated. Be aware of this behavior before upgrading firmware if you have previously activated the revert function.



Figure B.3 Firmware Versions

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

A P P E N D I X C

Best Practices for Emergency Readiness

These recommended practices provide for continued IED access through the SEL-3620/SEL-3622 in the event of system failures. In this discussion, mention of the SEL-3620 also applies to the SEL-3622.

Replacing a Damaged SEL-3620

Ideally, an SEL-3620 that has failed or been destroyed should be replaced with a new unit that exactly duplicates the settings, keys, and account password information of the old unit. To duplicate this information, you must maintain backups of the information before it is needed.

Maintain Backups

The operational state of the SEL-3620 can be saved in three parts: the device settings, the managed device passwords, and the connection directory.

NOTE: If the SEL-3620 is part of a configured MACsec Connectivity Association (CA), the MACsec Connectivity Association Key (CAK) is exported in system settings and in the single-file backup. In order to avoid having to re-commission the MACsec CA after restoration, always perform a backup after a CAK rotation occurs. The Syslog information contains messages of CAK rotation completion, which can be used along with the CAK Lifetime setting to determine when to execute a backup.

- SEL-3620 Settings:** The SEL-3620 provides for export of the device system settings file or a backup of the entire SEL-3620 configuration, connection directory, and managed passwords as a single file on the File Management page of the web interface. SEL recommends the single-file backup for the most complete and efficient backup method. This process is described here. Use the **Export** button in the System Settings section of the page to export a file containing settings, local accounts and their passwords, and keys for the device. Navigate to the Single File Backup section of the page and select **Export** to create a single-file backup which combines the SEL-3620 system settings and configuration files, connection directory, and managed passwords. The export process of either method requires using a password to encrypt the exported file to help keep the sensitive information (passwords and keys) in the settings file safe. If you want to be able to commission a new device to replace a damaged unit, export the preferred backup file(s) and save the file(s) and the file password in a secure location whenever settings on the device are changed.
- QuickSet Connection Directories:** If you are using the SEL-3620 to manage IED passwords, the connection directory information that defines the connections and interconnections to your SEL-3620 is maintained by, and can be reloaded from, QuickSet.
- Managed Device Password Reports:** If you are using the SEL-3620 to manage IED passwords, then you should generate, download, and store the Managed Device Passwords report from the Proxy Reports page of the SEL-3620 web interface between every new password generation and password application. This report provides the strong passwords currently set for each of the devices managed by the

SEL-3620. The Managed Device Passwords report can be exported from the SEL-3620 web or proxy interface either as a PDF file or a JSON file. A JSON file is a computer-readable file that can be used (e.g., with a Python script) to automate reloading IED passwords into an SEL-3620.

Configuring a Replacement Unit

Configuring a new unit requires commissioning it in the usual way, and then logging on as administrator and restoring the three configuration components just discussed.

1. **Restore the settings file.** Use the Backup File option in the File Upload area on the File Management page. Enter the correct password for the file, select the file, and select **Upload File**.
2. **Reload the connection directory.** Upload the connection directory from your QuickSet installation. In the QuickSet Device Manager view, right-click on the SEL-3620, select **Device Tasks**, and select **Send** to send the connection directory information to the new device.
3. **Restore the managed device passwords.** If you are using the SEL-3620 to manage IED passwords, you can use the Define Passwords section of the Password Management page (see *Figure C.1*) to restore the current values of each of the managed device passwords.

The screenshot shows the 'Define Passwords' page. It contains the following text and controls:

- Define Passwords**
- To manually set the passwords a given device uses, select the device from the drop down box and click the **Assign Passwords** button.
- Clicking on the **Assign Passwords** button will cause the **Edit Passwords for Managed Device** form to be displayed. This form will include the following inputs:

 - Account - The device account to be edited
 - New Password - The new password for the device account (limited to 128 characters)
 - Retype New Password - Confirmation of the new password (limited to 128 characters)
 - Action Type - Radio button with two possible selections (neither selected by default):
 - Change managed devices' passwords
 - Update local copy of managed devices' passwords

- All inputs are required for successful form submission. The following error messages can be generated by the **Edit Passwords for Managed Devices** form:

 - Both password fields must be filled.
 - Password mismatch.
 - Action type is not set.

Device: SEL-2032_DIRECT_ETHERNET

Figure C.1 Define Passwords

Select the relevant device from the **Device** dropdown list, and select **Assign Passwords** to show the Edit Password For Managed Device form as shown in *Figure C.2*. For each device, set the appropriate access level account (Access Level C, Access Level 2, Access Level 1, Access Level B) password, select **Update local copy of managed device's password**, and select **Edit**. Repeat this process for each account on each device and for each access level in the Managed Device Passwords Report.



Figure C.2 Editing Passwords for Device Accounts

Restoring Passwords Using the JSON File and a Script

If you exported the Managed Device Passwords report as a JSON file, you can use a computer application, such as a script written in Python, to read the file, and automate the process of entering the password information for the IEDs managed by the SEL-3620.

SEL provides a sample Python script that processes the JSON file and automates the process of restoring the IED passwords for an SEL-3620 connection directory. The following figure shows a sample run of the Python script to set IED password information.

```
C:\InstallDirectory>python restore.py 192.168.10.20 admin Asdf123$ good_192_168_10_20.json
Starting SEL 3622 managed device passwords restore.
Retrieving managed password data from file 'good_192_168_10_20.json'...  OK
Logging into device...  OK
Loading web page...  OK
Restoring SEL-2032_DIRECT_ETHERNET, acct: CAL, password: CLARKE...  OK
Restoring SEL-2032_DIRECT_ETHERNET, acct: ACC, password: OTTER...  OK
Restoring SEL-2032_DIRECT_ETHERNET, acct: 2AC, password: TAIL...  OK
Restoring SEL-351-7_DIRECT_ETHERNET, acct: ACC, password: OTTER...  OK
Restoring SEL-351-7_DIRECT_ETHERNET, acct: 2AC, password: TAIL...  OK
Restoring SEL-351-7_DIRECT_ETHERNET, acct: BAC, password: EDITH...  OK
Restoring SEL-351-7_DIRECT_ETHERNET, acct: CAL, password: CLARKE...  OK
Restoring SEL-451-5_DIRECT_ETHERNET, acct: OAC, password: WATT...  OK
.
.
.
Restoring SEL-787_DIRECT_ETHERNET, acct: 2AC, password: TAIL...  OK
Restoring SEL-787_DIRECT_ETHERNET, acct: ACC, password: OTTER...  OK

Restore finished with 0 errors.

Logging out of device...  OK
C:\InstallDirectory>
```

The script for restoring password information, together with an application guide describing its use, can be downloaded from the **Documentation** tab at selinc.com/products/3620/.

Emergency Access When LDAP Is Unavailable

Best Practices for Emergency Access When the Network Is Unavailable

Use of centralized (LDAP) authentication in the SEL-3620 supports secure individual accounts, granular control of privileges, and timely termination of access when an employee changes assignments or leaves the company. However, centralized authentication requires that the SEL-3620 be able to contact the directory service when an employee logs in. This might be a problem when widespread

physical damage results in network outages. This section describes recommended practices to ensure continued access through the SEL-3620 when a network outage makes contact with the directory service impossible.

Emergency access uses a local emergency access account on each SEL-3620 device, so that technicians can log in to the SEL-3620 locally using the emergency account and be able to use the authentication proxy feature to gain access to devices managed by the SEL-3620.

The recommended practice is to use the same account name (e.g., “Emergency”) and a strong password on all devices. To assign the emergency account password, consider using a strong password generator—several can be found on the internet. Change the emergency account password after it is used, and change the password regularly as required by NERC CIP regulations.

Creating the emergency account on multiple devices and changing the account password when required can be automated (for instance, by using a Python script). SEL provides two sample scripts, one for adding emergency access accounts and one for changing the passwords for those accounts on each of a list of SEL-3620 gateways in a file of IP addresses.

The following figure shows a sample run of the Python script to change passwords.

```
C:\YourWorkingDirectory>python ChangeEmergencyPasswords.py myips.txt EmergencyPasswords.txt admin Asdf123$  
User account: Emergency  
Old password: 2f895.aj  
New password: XnDGR*r5  
Opening https://192.168.10.20 Logging in... OK. Opening... Changing password... OK. Logging out... OK  
Opening https://192.168.10.20 Logging in... Failed  
...
```

NOTE: These sample scripts are designed to be run from a secure workstation because they show the administrative account password on the command line, and they store a password file containing the emergency account password on the computer in the directory from which the scripts are run.

The scripts for creating emergency accounts and for updating emergency account passwords, plus application guides describing their use, can be downloaded from the **Documentation** tab at selinc.com/products/3620/.

A P P E N D I X D

Open Network Ports

The following information is intended to help security auditors verify that the network hosts and open ports on a control network are what is expected.

The following table lists the network ports that may be presented by the device. Configuring port mappings with Ethernet endpoints using Raw TCP, SSH, or Telnet protocols will open additional ports.

Physical Port	# Ports	Default		Able to be Disabled			
Ethernet Services—Server	Device Function	Protocol	Default Listening Port	Port Settable	Default State	Able to be Disabled	
Serial Ports	17	Disabled		Yes (all)			
Ethernet Ports	3	Eth F Enabled, Eth 1–2 Disabled		Yes (all)			
Hypertext Transfer Protocol Secure (HTTPS)	Web Server	TCP	443	Yes	Enabled	Yes	
Network Time Protocol (NTP) Server	Date/Time	UDP	123	No	Disabled	Yes	
Raw TCP Server	Port Mappings	TCP	None	Yes	Disabled	Yes	
Secure Shell (SSH) Server	Port Mappings Service Port	TCP	None	Yes	Disabled	Yes	
Telnet Server	Port Mappings	TCP	None	Yes	Disabled	Yes	
Modbus TCP Server	Port Mappings	TCP	None	Yes	Disabled	Yes	
Simple Network Management Protocol (SNMP)	System	UDP	161	No	Disabled	Yes	
UDP Server	Port Mappings	UDP	None	Yes	Disabled	Yes	
Encapsulating Security Payload (ESP)	IPsec	ESP	N/A: IP protocol 50	N/A	Disabled	Yes	
Authentication Header (AH)	IPsec	AH	N/A: IP protocol 51	N/A	Disabled	Yes	
Internet Key Exchange (IKEv1/v2) and Internet Security Association and Key Management Protocol (ISAKMP)	IPsec	UDP/TCP	500	No	Enabled	Yes	
IPsec NAT-T	IPsec	UDP/TCP	4500	No	Enabled	Yes	
Internet Control Message Protocol (ICMP)	System	ICMP	N/A: IP protocol 1	N/A	Disabled	Yes	
Ethernet Services—Client	Device Function	Protocol	Default Destination Port	Port Settable	Default State	Able to be Disabled	
File Transfer Protocol	Firewall	TCP	20	No	Disabled	Yes ^a	
Lightweight Directory Access Protocol (LDAP) Client	LDAP	TCP	389	Yes	Disabled	Yes	
Network Time Protocol (NTP) Client	Date/Time	UDP	123	No	Disabled	Yes	

Raw TCP Client	Port Mappings	TCP	None	Yes	Disabled	Yes
Secure Shell (SSH) Client	Port Mappings	TCP	None	Yes	Disabled	Yes
Telnet Client	Port Mappings	TCP	None	Yes	Disabled	Yes
Modbus TCP Client	Port Mappings	TCP	None	Yes	Disabled	Yes
UDP Client	Port Mappings	UDP	None	Yes	Disabled	Yes
Syslog Client	Syslog	UDP	514	Yes	Disabled	Yes
Encapsulating Security Payload (ESP)	IPsec	ESP	N/A: IP protocol 50	N/A	Disabled	Yes
Authentication Header (AH)	IPsec	AH	N/A: IP protocol 51	N/A	Disabled	Yes
Internet Key Exchange (IKEv1/v2) and ISAKMP	IPsec	UDP	500	No	Disabled	Yes
Online Certificate Revocation Protocol (OCSP) Client	X.509 Management	TCP	None	Yes	Disabled	Yes
Dynamic Host Configuration Protocol (DHCP) Client	Networking	UDP	68	No	Disabled	Yes
Simple Network Management Protocol (SNMP)	System	UDP	162	No	Disabled	Yes
Internet Control Message Protocol (ICMP)	System	ICMP	N/A: IP protocol 1	N/A	Disabled	Yes
File Transfer Protocol	FTP Control	TCP	21	Yes	Disabled	Yes
File Transfer Protocol	FTP Data	TCP	20	No	Disabled	Yes
Ethernet Services—Non-IP Protocols	Device Function	Protocol	Default Destination Port	Port Settable	Default State	Able to be Disabled
Address Resolution Protocol (ARP)	Networking	ARP	N/A	N/A	Enabled	No
802.1Q Virtual Local Area Networking (VLAN)	Networking	VLAN	N/A	N/A	Disabled	Yes
Spanning Tree Protocol	Networking	STP	N/A	N/A	Disabled	Yes
Ethernet Services—Used Internally by the Device^b	Device Function	Protocol	Default Listening Port	Port Settable	Default State	Able to be Disabled
Postgresql	Internal Only	TCP/UDP	5432	N/A	N/A	N/A

^a Disabled by FTP automatic rule.^b Inaccessible from any external network device.

Though not actually discoverable as an open port, the response to ICMP PING requests also affects the discoverability of the device. ICMP PING response is disabled by default. This can be changed on the Firewall page in the web management interface.

APPENDIX E

User-Based Accounts

Introduction

Local accounts are the engineering access accounts that reside on SEL products. SEL has historically used global accounts like Access Level 1 and Access Level 2 and a password associated with each to control access to our devices. With global accounts, every user has the same login credentials (username and password), which weakens the security of the system. To strengthen authentication, authorization, and accountability, this SEL product uses a user-based account structure.

Benefits of User-Based Accounts

User-based accounts allow for a stronger security posture than global accounts. One of the drawbacks of global accounts is that when the privileges of an individuals are revoked, either everyone who uses that account is temporarily without access or there exists an unauthorized individual with secret knowledge that they can use or sell for malicious purposes. User-based accounts correct this problem with the ability to disable or remove the account of one individual without affecting the access of anybody else.

Similarly when password changes are required, either because of a compromised system, routine maintenance, or regulatory requirements, users will not be required to remember several new and different global passwords. They will only need to remember their own personal passwords changes. This increases security by reducing the need to write passwords down and by reducing the chance that an active password will be leaked.

Three key parts of strong access control are authentication, authorization, and accountability. Authentication is the process of verifying that an entity is who they claim to be. This is very difficult to reliably do with global accounts because of the nature of shared passwords. User-based accounts allow for the reliable authentication of individual users of a system. This creates more trust that someone who accesses the system is who they claim to be.

Authorization is the process of granting privileges to users of a system. Authorization can be done with global accounts when the accounts are organized into access roles, such as with Access Level 1 and Access Level 2. However, unless you have a large number of roles (and therefore a large number of shared passwords), global accounts are difficult to granularly assign privileges. User-based accounts can be used to specifically assign privileges to users of a system.

Accountability is the idea that an individual user can be held responsible for their actions on a system. The lack of authentication with global accounts creates too much opportunity to cast doubt on one's activities, making accountability difficult to enforce. The ability to clearly authenticate a user to the individual level allows all actions to be assigned to specific users. Accountability is very important to event tracking and forensic investigations.

Administration of User-Based Accounts

This product comes from the factory not configured. This means there are no user accounts installed. To access the product, an administrative account must be created. Create this account through the commissioning page. An administrative account is an account with full access to the system. This account is authorized to add, remove, enable, and disable system users. It is recommended that knowledge of this account password be restricted to only the individual who creates this account.

The ability to create other accounts with administrative privileges does exist. This device supports as many as 30 unique user accounts. It is recommended that administrative privileges be granted to only those users with a need to manage user accounts.

User accounts are stored in nonvolatile memory. This allows account status to be maintained through power cycles and other unexpected events.

SEL Use Banner

Before logging in to this SEL product, any potential user is presented a use banner. The use banner is a programmable message indicating what constitutes appropriate use of this device and potential consequences for abusing this device. The default use banner for SEL products is the same as the recommended use banner of the National Institute of Standards and Technology:

This system is for the use of authorized users only. Individuals using this system without authority or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such activity to law enforcement officials.

Logging in With SEL User-Based Accounts

Upon connection to this SEL product, a user will be presented with a use banner and a login prompt. The login prompt includes boxes to enter a username and the password associated with that username. To log in to this SEL product, the user must enter a valid username and the appropriate password. Usernames are case-sensitive and unique to each individual with the authority to access the device. If a valid username and the matching password are entered, the user will be granted access to the device.

If the username or password is determined to be invalid, then the device will reject the access attempt and provide an alert to the user. This alert will inform the user that the login credentials were incorrect. After three failed login attempts, this SEL product will disallow access attempts using the locked username for 30 seconds. Additionally, this device will pulse the alarm contact three times to provide an alert to the control center that a failed login attempt has occurred. These security features are designed to prevent and slow down password guessing attacks. Login failure can happen for three reasons: the username was invalid, the password was incorrect, or the user's account is disabled. Check

the spelling of the username and password if an access attempt fails. If you are certain the username and password were correctly entered, contact your system administrator to verify that your account has not been disabled.

Passphrases

Passphrases provide a user with the ability to create strong and easy to remember passwords that protect access to a system. A strong passphrase includes many different characters, from many different character sets. Longer passphrases provide greater security than shorter passphrases. SEL user-based accounts support complex passphrases that must include at least one character from each of the following character sets.

- ▶ Uppercase letters
- ▶ Lowercase letters
- ▶ Digits
- ▶ Special characters

Additionally, passphrases must be at least eight characters in length. This SEL product supports passphrases as many as 127 characters in length. Spaces are allowed in passphrases.

Users with administrative access can set or change passphrases for any user of the system. Users without administrative access can only change their own passphrases. For the protection of your account, this SEL product will not ever display, transmit, or store a passphrase in cleartext.

This page intentionally left blank

A P P E N D I X F

Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport to allow a device to send system event notification messages across IP networks to remote Syslog servers. Syslog is commonly used to send system logs such as security events, system events, and status messages useful in troubleshooting, auditing, and event investigations. The Syslog packet size is limited to 1024 bytes and is formatted into three parts: PRI, HEADER, and MSG.

1. **PRI:** The priority part of a Syslog packet is a number enclosed in angle brackets that represents both the Facility and Severity of the message. The Priority value is calculated by multiplying the Facility numerical code by 8 and adding the numerical value of the Severity. For example, a kernel message (Facility = 0) with a Severity of Emergency (Severity = 0) would have a Priority of 0. Also, a “local use 4” message (Facility = 20) with a Severity of Notice (Severity = 5) would have a Priority value of 165. In the PRI part of the Syslog message, these values would be placed between the angle brackets as <0> and <165> respectively.

The severity code (*Table F.1*) is a number indicative of how critical the message is.

Table F.1 Syslog Message Severities

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

The Facility code (*Table F.2*) defines from which application group the message originated.

Table F.2 Syslog Message Facilities (Sheet 1 of 2)

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons

Table F.2 Syslog Message Facilities (Sheet 2 of 2)

Numerical Code	Facility
4	Security/authorization messages ^a
5	Messages generated internally by Syslog
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon ^b
10	Security authorization messages ^a
11	FTP daemon
12	NTP subsystem
13	Log audit ^a
14	Log audit ^b
15	Clock daemon ^b
16	Local use 0 (local 0)
17	Local use 1 (local 1)
18	Local use 2 (local 2)
19	Local use 3 (local 3)
20	Local use 4 (local 4)
21	Local use 5 (local 5)
22	Local use 6 (local 6)
23	Local use 7 (local 7)

^a Various operating systems have been found to utilize Facilities 4, 10, 13, and 14 for security/authorization, audit, and alert messages that seem to be similar.

^b Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.

Source: <http://www.faqs.org/rfcs/rfc3164.html>

2. **HEADER:** The header of a Syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message originator. Time stamps are based on the time of the originating host, so it is critical to have time-synchronized across devices for the entire network to accurately perform log analysis and event correlation.
3. **MSG:** The message part of a Syslog packet contains the source program that triggered the message and the human-readable body of the message.

A sample Syslog message has been provided below. This particular message shows an invalid login attempt on July 09, 2009 at 08:17:29 to “myhostname” for user root from the IP address 192.168.1.1. The priority of this message is 34.

```
<34>Jul 09 2009 08:17:29 myhostname Invalid login attempt by:  
root at 192.168.1.1
```

The Syslog message has been divided into each respective part as shown in the table.

PRI	HEADER	MSG
<34>	Jul 09 2009 08:17:29 myhostname	Invalid login attempt by: root at 192.168.1.1

Remote Syslog Servers

Syslog messages are stored locally and optionally sent to remote Syslog servers. The local buffers are circular so that newer messages overwrite older messages after the buffer is filled. Support for multiple remote Syslog servers provides the added benefits of centralized logging including larger storage capacity, centralized event analysis and correlation, and archival of event logs. In *Figure F.1*, remote devices are configured to send Syslog messages to the remote Syslog server on the other end of the VPN tunnel. Syslog compatible devices can send logs to the central Syslog server in this example for centralized logging, reporting, and event correlation. The Syslog Protocol uses User Datagram Protocol (UDP) port 514 to send Syslog messages to remote Syslog servers.

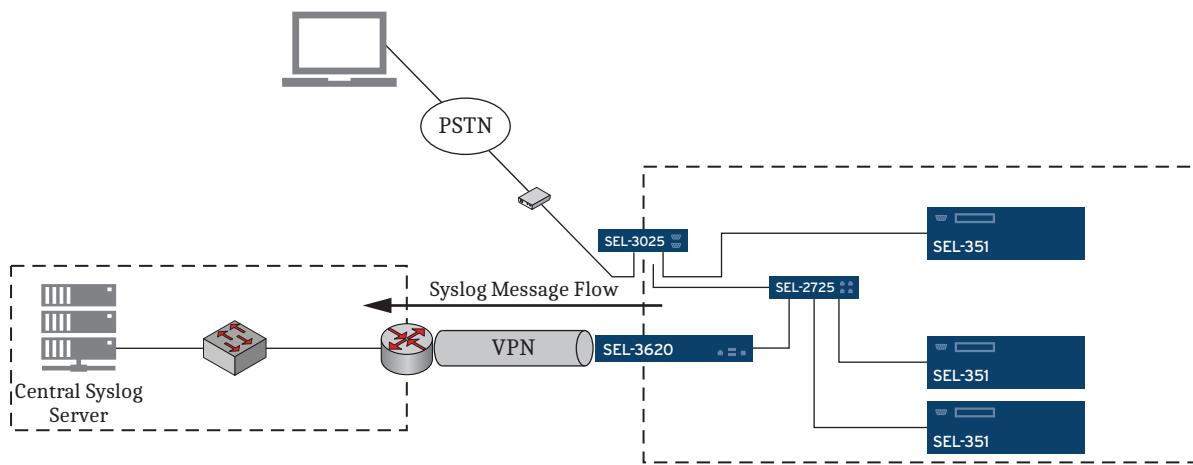


Figure F.1 Central Syslog Server

Open Source Syslog Servers

Most Linux and UNIX distributions include a native Syslog server that can be used for a central Syslog server solution. Syslog-*ng* (<http://balabit.com>) is also an excellent solution with added functionality that can be used if not already included in your distribution. Syslog server solutions for Microsoft Windows are typically commercial or have limited feature sets if offered at no charge.

Event Logs

The device records and time-stamps all events in the Syslog format consistent with the Syslog description from RFC 3164. This appendix is a listing of all the events that the device logs and the record that is generated with each of these events.

Log messages may contain words or phrases in brackets such as <Username>. This notation indicates that the word or phrase inside the brackets will be replaced with the value of the entity being logged. In this case the username of the user who performed an action.

Note that logs pertaining to physical sensors (motion and light) are for the SEL-3622 only. Firewall, IPsec, and Proxy logs pertain to the SEL-3620/SEL-3622 only. All other logs are common to all three devices.

Table F.3 Syslog Messages (Sheet 1 of 17)

Message	Tag Name	Severity	Facility
Address Group Configuration			
Address Group <ip_address_group_name>: created by <username> at <user_ip>	AddressGroupsConfig	5-Notice	1-User
Address Group <ip_address_group_name>: deleted by <username> at <user_ip>	AddressGroupsConfig	5-Notice	1-User
Address Group <ip_address_group_name>: modified by <username> at <user_ip>	AddressGroupsConfig	5-Notice	1-User
Address Group <pre_name> name: changed to <post_name> by <username> at <user_ip>	AddressGroupsConfig	5-Notice	1-User
Allowed Clients Configuration			
Allowed <types> Client <alias>: changed by <username> at <user_ip>	AllowedClientsConfig	4-Warning	4-Security/ Authorization
Allowed <types> Client <alias>: created by <username> at <user_ip>	AllowedClientsConfig	4-Warning	4-Security/ Authorization
Allowed <types> Client <alias>: deleted by <username> at <user_ip>	AllowedClientsConfig	4-Warning	4-Security/ Authorization
Allowed <types> Client <alias_1>: modified due to Address Group <alias_2> update by <username> at <user_ip>	AllowedClientsConfig	4-Warning	4-Security/ Authorization
Allowed <types> Client <alias_1>: removed due to Address Group <alias_2> deletion by <username> at <user_ip>	AllowedClientsConfig	4-Warning	4-Security/ Authorization
Commissioning			
Attempt to access Device Configuration page after commissioning from <user_ip>	Commissioning	2-Critical	4-Security/ Authorization
Attempt to access pre-commissioning page from <user_ip>	Commissioning	2-Critical	4-Security/ Authorization
Device commissioned by <username> at <user_ip>	Commissioning	5-Notice	4-Security/ Authorization
Device reset initiated by <username> at <user_ip>	Commissioning	2-Critical	4-Security/ Authorization
Configuration File Imports and Exports			
Configuration File: export initiated by <username> at <user_ip>	ConfigFile	4-Warning	1-User
Configuration File: generation failed	ConfigFile	3-Error	3-System
Configuration File: generation initiated by <username> at <user_ip>	ConfigFile	5-Notice	1-User
Configuration File: generation successful	ConfigFile	5-Notice	3-System
Configuration File: import initiated by <username> at <user_ip>	ConfigFile	4-Warning	1-User
Configuration File: update failed	ConfigFile	3-Error	3-System
Configuration File: update successful	ConfigFile	5-Notice	3-System
Date/Time Configuration			
IRIG Input Offset: changed from <pre_config> to <post_config> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
IRIG Output Offset: changed from <pre_config> to <post_config> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
IRIG: output disabled by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
IRIG: output enabled by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
NTP Server <server_ip>: created by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
NTP Server <server_ip>: deleted by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User

Table F.3 Syslog Messages (Sheet 2 of 17)

Message	Tag Name	Severity	Facility
NTP Stratum: changed from <pre_config> to <post_config> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
NTP: output disabled by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
NTP: output enabled by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
System Time: changed from <pre_timestamp> to <post_timestamp> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
Time Source: set to <source_type> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
Time Zone: changed from <pre_tz> to <post_tz> by <username> at <user_ip>	DateTimeConfig	5-Notice	1-User
Date/Time Operations			
System Time: lost synchronization to external source	DateTime	4-Warning	3-System
System Time: synchronization to external source failed	DateTime	4-Warning	3-System
System Time: synchronized to external source by <username> at <user_ip>	DateTime	5-Notice	1-User
System Time: synchronized via IRIG	DateTime	5-Notice	3-System
System Time: synchronized via NTP	DateTime	5-Notice	3-System
Firewall Configuration			
Firewall Allow All Encrypted: disabled by <username> at <user_ip>	FirewallConfig	5-Notice	4-Security/ Authorization
Firewall Allow All Encrypted: enabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Drop Ping: disabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Drop Ping: enabled by <username> at <user_ip>	FirewallConfig	5-Notice	4-Security/ Authorization
Firewall Drop Traceroute: disabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Drop Traceroute: enabled by <username> at <user_ip>	FirewallConfig	5-Notice	4-Security/ Authorization
Firewall Must Be Encrypted: disabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Must Be Encrypted: enabled by <username> at <user_ip>	FirewallConfig	5-Notice	4-Security/ Authorization
Firewall Rule <pre_alias> Alias: changed to <post_alias> by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <rule_alias>: changed by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <rule_alias>: created by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <rule_alias>: deleted by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <rule_alias>: disabled by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <rule_alias>: enabled by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule Priority: <alias_1> was moved above <alias_2> by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule Priority: <alias> was moved to the end by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Verbose Logging: All enabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 3 of 17)

Message	Tag Name	Severity	Facility
Firewall Verbose Logging: Custom enabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Verbose Logging: Default Rule logging disabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Verbose Logging: Default Rule logging enabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Verbose Logging: disabled by <username> at <user_ip>	FirewallConfig	5-Notice	4-Security/ Authorization
Firewall Verbose Logging: Dropped/Rejected enabled by <username> at <user_ip>	FirewallConfig	4-Warning	4-Security/ Authorization
Firewall Rule <alias_1>: modified due to Address Group <alias_2> update by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <alias_1>: modified due to Port Group <alias_2> update by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <alias_1>: removed due to Address Group <alias_2> deletion by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Rule <alias_1>: removed due to Port Group <alias_2> deletion by <username> at <user_ip>	FirewallConfig	5-Notice	1-User
Firewall Operations			
<count> connection/connections established	Firewall	6-Informational	3-System
<count> connection/connections terminated	Firewall	6-Informational	3-System
<count> packet/packets dropped	Firewall	6-Informational	3-System
<count> packet/packets rejected	Firewall	6-Informational	3-System
<protocol> connection from <source_ip> to <destination_ip> established by Rule: <rule name>	Firewall	6-Informational	3-System
<protocol> connection from <source_ip> to <destination_ip> terminated by Rule: <rule name>	Firewall	6-Informational	3-System
<protocol> connection from <source_ip>:<source_port> to <destination_ip>:<destination_port> established	Firewall	6-Informational	3-System
<protocol> connection from <source_ip>:<source_port> to <destination_ip>:<destination_port> terminated	Firewall	6-Informational	3-System
<protocol> packet from <source_ip>:<source_port> to <destination_ip>:<destination_port> dropped	Firewall	6-Informational	3-System
<protocol> packet from <source_ip>:<source_port> to <destination_ip>:<destination_port> rejected	Firewall	6-Informational	3-System
Logging throttled: High event rate	Firewall	6-Informational	3-System
Firmware			
The firmware update from <Rxxx> to new version failed with an error of <z>. Please contact Schweitzer Engineering Laboratories, Inc. for assistance	Update	2-Critical	3-System
Boot did not succeed; automatically reverted to previous version	Firmware	2-Critical	3-System
Firmware update from <Rxxx> to <Ryyy> succeeded without error	Update	4-Warning	3-System
Firmware: update initiated by <username> at <user_ip>	Firmware	5-Notice	1-User

Table F.3 Syslog Messages (Sheet 4 of 17)

Message	Tag Name	Severity	Facility
The firmware version downgrade is not compatible with the current firmware	Update	3-Error	3-System
The installed firmware update package is corrupted; unable to decrypt the firmware update package or validate the signature on the firmware update package	Update	3-Error	3-System
Hosts Configuration			
Hostname <remote_hostname> Address: created by <username> at <user_ip>	HostsConfig	5-Notice	1-User
Hostname <remote_hostname> Address: deleted by <username> at <user_ip>	HostsConfig	5-Notice	1-User
Input Contact			
Note: The Input Contact messages listed here are the default. These messages are user-configurable.			
Input contact de-energized	InputContact	5-Notice	4-Security/ Authorization
Input contact energized	InputContact	5-Notice	4-Security/ Authorization
IPsec Configuration			
IPsec Connection <local-gateway> - <remote-gateway> Local Network: <local-network> created by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway> Local Network: <local-network> deleted by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway> Passphrase: changed by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway> Remote Network: <remote-network> created by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway> Remote Network: <remote-network> deleted by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway>: changed by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway>: deleted by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway>: disabled by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway>: enabled by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Connection <local-gateway> - <remote-gateway>: generated by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec Drop on OCSP Loss: disabled by <username> at <user_ip>	IPsecConfig	4-Warning	1-User
IPsec Drop on OCSP Loss: enabled by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
IPsec: disabled by <username> at <user_ip>	IPsecConfig	4-Warning	1-User
IPsec: enabled by <username> at <user_ip>	IPsecConfig	5-Notice	1-User
MACsec Configuration			
MACsec Connection <int> added by <username> at <user_ip>	MACsecConfig	5-Notice	1-User
MACsec Connection <int> deleted by <username> at <user_ip>	MACsecConfig	5-Notice	1-User
MACsec Connection <int> updated by <username> at <user_ip>	MACsecConfig	5-Notice	1-User

Table F.3 Syslog Messages (Sheet 5 of 17)

Message	Tag Name	Severity	Facility
CAK Rotation performed on <int>	MACsecManagement	5-Notice	4-Security/ Authorization
SAK Rotation performed on <int>	MACsecManagement	5-Notice	4-Security/ Authorization
MKA actor with Member Identifier <mka_mi> is now associated with Verbose Identity <verbose_id>	MACsecManagement	6-Informational	4-Security/ Authorization
MKA actor with Member Identifier <mka_mi> is now associated with Short Identity <mka_id>	MACsecManagement	6-Informational	4-Security/ Authorization
MKA CAK generation and distribution initiated by <src> on interface <int>	MACsecManagement	5-Notice	4-Security/ Authorization
MACsec SAK generation and distribution initiated by <src> on interface <int>	MACsecManagement	5-Notice	4-Security/ Authorization
MACsec enabled on interface <int> by <src>	MACsecManagement	5-Notice	4-Security/ Authorization
MACsec disabled on interface <int> by <src>	MACsecManagement	5-Notice	4-Security/ Authorization
MACsec commissioning process succeeded on <int>	MACsecManagement	2-Critical	4-Security/ Authorization
MACsec commissioning process failed on <int>	MACsecManagement	2-Critical	4-Security/ Authorization
MACsec commissioning process enabled on <int>	MACsecManagement	2-Critical	4-Security/ Authorization
Remote MACsec actor <mka_id> was successfully adopted on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
Remote MACsec actor <mka_id> was successfully verified on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
Remote MACsec actor <mka_id> was not successfully adopted on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
MACsec key was successfully synchronized with remote MACsec actor <mka_id> on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
MACsec key management key was successfully synchronized with remote MACsec actor <mka_id> on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
MACsec key management functions are now active on interface <int>	MACsecManagement	2-Critical	4-Security/ Authorization
Interface <int> is no longer secured with MACsec and will allow non-secured communications	MACsecManagement	2-Critical	4-Security/ Authorization
Local actor with Member Identifier <mka_mi> was generated by the device	MACsecCommissioning	6-Informational	4-Security/ Authorization
Local actor <mka_id> was disassociated from the commissioning Connectivity Association on interface <int>	MACsecCommissioning	6-Informational	4-Security/ Authorization
Commissioning Connectivity Association version <dver> was successfully enabled on interface <int> by the device	MACsecCommissioning	5-Notice	4-Security/ Authorization
Commissioning Connectivity Association version <dver> has been disabled on interface <int> by the device	MACsecCommissioning	5-Notice	4-Security/ Authorization
Remote actor with identity <mka_mi> advertising MACsec commissioning version <dver> was discovered on interface <int>	MACsecCommissioning	5-Notice	4-Security/ Authorization
Remote actor <mka_id> on interface <int> was successfully verified	MACsecCommissioning	5-Notice	4-Security/ Authorization
Remote actor <mka_id> on interface <int> was successfully adopted	MACsecCommissioning	5-Notice	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 6 of 17)

Message	Tag Name	Severity	Facility
Local actor <mka_id> was associated with the commissioning Connectivity Association on interface <int>	MACsecCommissioning	5-Notice	4-Security/ Authorization
Active initiation has timed out on interface <int>	MACsecCommissioning	5-Notice	4-Security/ Authorization
Active initiation enabled on interface <int> by the device	MACsecCommissioning	5-Notice	4-Security/ Authorization
Active initiation disabled on interface <int> by the device	MACsecCommissioning	5-Notice	4-Security/ Authorization
Remote actor with identity <mka_mi> advertising unsupported MACsec commissioning version <dver> was discovered on interface <int>	MACsecCommissioning	4-Warning	4-Security/ Authorization
Commissioning attempt failed for the remote actor <mka_id> on interface <int>	MACsecCommissioning	4-Warning	4-Security/ Authorization
Commissioning attempt failed for remote actor <mka_id> on interface <int> due to an incorrect secret	MACsecCommissioning	4-Warning	4-Security/ Authorization
Remote actor <mka_id> is no longer available on the interface <int> due to timeout	MACsecCommissioning	4-Warning	4-Security/ Authorization
Commissioning Connectivity Association was not successfully enabled on interface <int>	MACsecCommissioning	3-Error	4-Security/ Authorization
MKA CAK with Connectivity Association Key Name <ckn> was generated by the device	MACsecKeyManagement	6-Informational	4-Security/ Authorization
MKA CAK <ckn> has been distributed by local actor <mka_id> from interface <int>	MACsecKeyManagement	5-Notice	4-Security/ Authorization
MKA CAK <ckn> has been added to the CAK cache for interface <int> by the device	MACsecKeyManagement	6-Informational	4-Security/ Authorization
MACsec SAK <sak_id> with Association Number <sak_an> and Confidentiality Offset <sak_co> was generated for interface <int> by the device	MACsecKeyManagement	6-Informational	4-Security/ Authorization
MACsec SAK <sak_id> with a Lowest Acceptable Packet Number of <sak_llpn> has been successfully installed as the current MACsec key on local interface <int>	MACsecKeyManagement	6-Informational	4-Security/ Authorization
MACsec SAK <sak_id> has been marked as expired and is no longer used as a key on interface <int>	MACsecKeyManagement	6-Informational	4-Security/ Authorization
MACsec SAK <sak_id> has been distributed by local actor <mka_id> from interface <int>	MACsecKeyManagement	5-Notice	4-Security/ Authorization
Frames secured by MACsec SAK <sak_id> enforce MACsec Confidentiality	MACsecKeyManagement	5-Notice	4-Security/ Authorization
Frames secured by MACsec SAK <sak_id> do not enforce MACsec Confidentiality	MACsecKeyManagement	4-Warning	4-Security/ Authorization
MKA CAK <ckn> cannot be used on interface <int>	MACsecKeyManagement	3-Error	4-Security/ Authorization
MACsec SAK <sak_id> was not installed as the current key on interface <int>	MACsecKeyManagement	3-Error	4-Security/ Authorization
Remote actor <mka_id> was added to the Live Peer List of local actor <mka_id> on interface <int>	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Remote actor <mka_id> MKA Life Time expired	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Local actor with Member Identifier <mka_mi> was generated by the device	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Local actor <mka_id> was elected Key Server for Connectivity Association <ckn> on interface <int>	MACsecKeyAgreement	6-Informational	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 7 of 17)

Message	Tag Name	Severity	Facility
Local actor <mka_id> was associated with Connectivity Association <ckn> on interface <int>	MACsecKeyAgreement	5-Notice	4-Security/ Authorization
Connectivity Association <ckn> has been enabled on interface <int> by the device	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Connectivity Association <ckn> has been disabled on interface <int> by the device	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Remote actor <mka_id> was removed from the Live Peer List of local actor <mka_id> on interface <int>	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Frame validation failed for dropped ingressing frame number <mka_mn> from <mka_id> on interface <int>	MACsecKeyAgreement	6-Informational	4-Security/ Authorization
Frame validation failed due to delay for dropped ingressing frame number <mka_mn> from <mka_id> on interface <int>	MACsecKeyAgreement	4-Warning	4-Security/ Authorization
Frame generation failed for Connectivity Association <ckn> on interface <int>	MACsecKeyAgreement	3-Error	4-Security/ Authorization
Connectivity Association <ckn> was not successfully enabled on interface <int>	MACsecKeyAgreement	3-Error	4-Security/ Authorization
Confidentiality enabled for secured frames on interface <int> by the device	MACsec	2-Critical	4-Security/ Authorization
Confidentiality enabled for secured frames on interface <int> by the device	MACsec	2-Critical	4-Security/ Authorization
Jumper Configuration			
Password jumper installed	JumperConfig	3-Error	4-Security/ Authorization
Password jumper removed	JumperConfig	3-Error	4-Security/ Authorization
LDAP Configuration			
LDAP Bind DN Password: changed by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP Group Mapping: <privilege_level> mapping created by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP Group Mapping: <privilege_level> mapping deleted by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP Server <hostname>: created by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP Server <hostname>: deleted by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP Server <previous_hostname> Hostname: changed to <post_hostname> by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
LDAP User Attribute Mappings: changed by <username> at <user_ip>	LDAPConfig	5-Notice	4-Security/ Authorization
LDAP: settings changed by <username> at <user_ip>	LDAPConfig	4-Warning	4-Security/ Authorization
Light Sensor			
Light sensor detected a change	LightSensor	5-Notice	4-Security/ Authorization
Link Up/Down			
Port <alias> changed link state to up	Link Up/Down	4-Warning	3-System

Table F.3 Syslog Messages (Sheet 8 of 17)

Message	Tag Name	Severity	Facility
Port <alias> changed link state to down	Link Up/Down	4-Warning	3-System
Local User Configuration			
Local Group <created_group>: created by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
Local Group <deleted_group>: deleted by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
Local Group <group_name>: users added by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
Local Group <group_name>: users removed by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
Local Group <pre_alias> Alias: changed to <post_alias> by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
User <changed_username> Attributes: changed by <username> at <user_ip>	UserConfig	5-Notice	4-Security/ Authorization
User <changed_username> Password: set by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
User <changed_username>: password change attempt failed by unverified user <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
User <created_username>: created by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
User <new_username>: account creation attempt failed by unverified user <username> at <user_ip>	User Config	4-Warning	4-Security/ Authorization
User <deleted_username>: deleted by <username> at <user_ip>	UserConfig	4-Warning	4-Security/ Authorization
User <disabled_user>: disabled by <username> at <user_ip>	UserConfig	5-Notice	4-Security/ Authorization
User <enabled_user>: enabled by <username> at <user_ip>	UserConfig	5-Notice	4-Security/ Authorization
Username <pre_username>: changed to <post_username> by <username> at <user_ip>	UserConfig	3-Error	4-Security/ Authorization
User <changed_username>: account update attempt failed by unverified user <username> at <user_ip>	UserConfig	4-Notice	4-Security/ Authorization
User <enabled/disabled_username>: account enable/disable attempt failed by unverified user <username> at <user_ip>	UserConfig	4-Notice	4-Security/ Authorization
User <deleted_username>: account deletion attempt failed by unverified user <username> at <user_ip>	UserConfig	4-Notice	4-Security/ Authorization
Logging			
Audit Report <report_type>: deleted by <username> at <user_ip>	Logging	4-Warning	1-User
Audit Report <report_type>: downloaded by <username> [at <user_ip>]	Logging	5-Notice	1-User
Audit Report <report_type>: generated from local log items by <username> [at <user_ip>]	Logging	6-Informational	1-User
Login			
Login Lockout on <driver_alias>: <username> [at <user_ip>]	Login	5-Notice	4-Security/ Authorization
Login to <alias>: failed [from <user_ip>]	Login	5-Notice	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 9 of 17)

Message	Tag Name	Severity	Facility
Login to <alias>: successful by <username> [at <user_ip>]	Login	5-Notice	4-Security/ Authorization
Login to Web: failed from <user_ip>	Login	5-Notice	4-Security/ Authorization
Login to Web: successful by <username> at <user_ip>	Login	5-Notice	4-Security/ Authorization
Logout <driver_alias>: <username> [at <user_ip>]	Login	5-Notice	4-Security/ Authorization
Logout Web: <username> at <user_ip>	Login	5-Notice	4-Security/ Authorization
Timeout <driver_alias>: <username> [at <user_ip>]	Login	5-Notice	4-Security/ Authorization
Timeout Web: <username> at <user_ip>	Login	5-Notice	4-Security/ Authorization
Miscellaneous Configuration			
DSA SSH Host Keys generation failed	Config	5-Notice	4-Security/ Authorization
New DSA SSH Host Keys generated	Config	5-Notice	4-Security/ Authorization
New DSA SSH Host Keys generation initiated by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
New RSA SSH Host Keys generated	Config	5-Notice	4-Security/ Authorization
New RSA SSH Host Keys generation initiated by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
RSA SSH Host Keys generation failed	Config	5-Notice	4-Security/ Authorization
Usage Policy: changed by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
New RSA-SHA2-256 SSH Host Keys generation initiated by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
New ECC SSH Host Keys generation initiated by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
New RSA-SHA2-256 SSH Host Keys generated	Config	5-Notice	4-Security/ Authorization
RSA-SHA2-256 SSH Host Keys generation failed	Config	5-Notice	4-Security/ Authorization
New ECC SSH Host Keys generated	Config	5-Notice	4-Security/ Authorization
ECC SSH Host Keys generation failed	Config	5-Notice	4-Security/ Authorization
Available SSH key exchange algorithms updated by <username> at <user_ip>	Config	5-Notice	4-Security/ Authorization
Motion Sensor			
Motion Sensor detected movement or impact	MotionSensor	5-Notice	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 10 of 17)

Message	Tag Name	Severity	Facility
Motion sensor detected tilt	MotionSensor	4-Warning	4-Security/ Authorization
NAT Configuration			
Address Translation: disabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Address Translation: enabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> created by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> deleted by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> disabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> enabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> updated by <username> at <user_ip>	NATConfig	5-Notice	1-User
Public Interface: changed from <A> to by <username> at <user_ip>	NATConfig	5-Notice	1-User
Public Interface: changed to <X> by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> modified due to Address Group <alias> update by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <X> removed due to Address Group <alias> deletion by <username> at <user_ip>	NATConfig	5-Notice	1-User
NAT Operations			
Connections reset by <X> at <IP>	NAT	5-Notice	1-User
Networking Configuration			
Global Network Settings: changed by <username> at <user_ip>	NetworkConfig	5-Notice	1-User
Network Address <alias>: changed by <username> at <user_ip>	NetworkConfig	5-Notice	1-User
Network Address <alias>: created by <username> at <user_ip>	NetworkConfig	5-Notice	1-User
Network Address <alias>: deleted by <username> at <user_ip>	NetworkConfig	5-Notice	1-User
Network Interface <alias> IP Address: <pre_config> changed to <post_config> by DHCP	NetworkConfig	5-Notice	3-System
Network Interface <alias>: changed by <username> at <user_ip>	NetworkConfig	5-Notice	1-User
Network Interface <alias>: DHCP lease cannot be obtained.	NetworkConfig	4-Warning	3-System
Ping Messages			
Ping <A> succeeded by <X> at <IP>	Config	6-Informational	1-User
Ping <A> failed by <X> at <IP>	Config	6-Informational	1-User
Physical Sensor Configuration			
Input Contact: disabled by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User
Input Contact: enabled by <username> at <user_ip>	PhysicalSensorsConfig	5-Notice	1-User
Input Contact: Syslog message changed by <username> at <user_ip>	PhysicalSensorsConfig	5-Notice	1-User
Light Sensor: changed from <pre_config> to <post_config> by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User
Light Sensor: disabled by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User
Light Sensor: enabled by <username> at <user_ip>	PhysicalSensorsConfig	5-Notice	1-User
Motion Sensor: changed from <pre_config> to <old_config> by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User
Motion Sensor: disabled by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User
Motion Sensor: enabled by <username> at <user_ip>	PhysicalSensorsConfig	5-Notice	1-User
Physical Sensors: disabled by <username> at <user_ip>	PhysicalSensorsConfig	4-Warning	1-User

Table F.3 Syslog Messages (Sheet 11 of 17)

Message	Tag Name	Severity	Facility
Physical Sensors: enabled by <username> at <user_ip>	PhysicalSensorsConfig	5-Notice	1-User
Port Forwarding Configuration			
<protocol> connection from <source_ip>:<source_port> to <destination_ip>:<destination_port> established by Rule: <rule name>	Firewall	6-Informational	3-System
<protocol> connection from <source_ip>:<source_port> to <destination_ip>:<destination_port> terminated by Rule: <rule name>	Firewall	6-Informational	3-System
Port Forwarding: rule <alias> created by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <alias> deleted by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <alias> disabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding: rule <alias> enabled by <username> at <user_ip>	NATConfig	5-Notice	1-User
Port Forwarding Operations			
Port Forwarding: connection rejected to port <alias> from <IP A>	NAT	5-Notice	3-System
Port Forwarding: connection established to port <alias> from <IP A>	NAT	5-Notice	3-System
Port Forwarding: connection terminated to port <alias> from <IP A>	NAT	5-Notice	3-System
Port Mapping Configuration			
Port Mapping Group <alias>: created by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <alias>: deleted by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <alias>: disabled by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <alias>: enabled by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Connect Remote Driver <driver_alias> SSH credentials: modified by <username>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Connect Remote Driver <driver_alias>: created by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Connect Remote Driver <driver_alias>: deleted by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Connect Remote Driver <driver_alias>: modified by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Connect Remote Driver <pre_driver_alias>: changed to <post_driver_alias> by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Listen Local Driver <driver_alias>: created by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Listen Local Driver <driver_alias>: deleted by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Listen Local Driver <driver_alias>: modified by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Ethernet Listen Local Driver <pre_driver_alias>: changed to <post_driver_alias> by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Modbus Translation(s): deleted by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Modbus Translation(s): updated by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User

Table F.3 Syslog Messages (Sheet 12 of 17)

Message	Tag Name	Severity	Facility
Port Mapping Group <group_alias> Modbus Translation: created by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Serial Driver <driver_alias>: created by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Serial Driver <driver_alias>: deleted by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group <group_alias> Serial Driver <driver_alias>: modified by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Group Alias <pre_alias>: changed to <post_alias> by <username> at <user_ip>	PortMappingConfig	5-Notice	1-User
Port Mapping Operations			
Connection from <driver_alias>: timeout [from <remote_ip>]	PortMappingConfig	4-Warning	3-System
Connection to <driver_alias>: disconnected [from <remote_ip>]	PortMappingConfig	5-Notice	3-System
Incoming Connection to <driver_alias>: established [from <remote_ip>]	PortMappingConfig	5-Notice	3-System
Master Port <driver_alias>: connected to <port_alias> by <username> [at <remote_ip>]	PortMappingConfig	5-Notice	1-User
Master Port <driver_alias>: disconnected from <port_alias> by <username> [at <remote_ip>]	PortMappingConfig	5-Notice	1-User
Master Port <driver_alias>: transitioned into binary mode by <username>	PortMappingConfig	5-Notice	1-User
Master Port <driver_alias>: transitioned out of binary mode by <username>	PortMappingConfig	5-Notice	1-User
Outgoing Connection from <driver_alias>: established to <remote_IP>	PortMappingConfig	5-Notice	3-System
Port Group Configuration			
Port Group <port_group_name>: created by <username> at <user_ip>	PortGroupsConfig	5-Notice	1-User
Port Group <port_group_name>: deleted by <username> at <user_ip>	PortGroupsConfig	5-Notice	1-User
Port Group <port_group_name>: modified by <username> at <user_ip>	PortGroupsConfig	5-Notice	1-User
Port Group <pre_name> name: changed to <post_name> by <username> at <user_ip>	PortGroupsConfig	5-Notice	1-User
Power			
Device halted by <username> at <user_ip>	Power	2-Critical	1-User
Device initialization completed	Power	2-Critical	3-System
Device rebooted by <username> at <user_ip>	Power	3-Error	1-User
Proxy Configuration			
Authentication Proxy Device Checkout: disabled by <username> at <user_ip>	ProxyConfig	5-Notice	1-User
Authentication Proxy Device Checkout: enabled by <username> at <user_ip>	ProxyConfig	5-Notice	1-User
Authentication Proxy Password Change Scheduler: disabled by <username> at <user_ip>	ProxyConfig	4-Warning	1-User
Authentication Proxy Password Change Scheduler: enabled by <username> at <user_ip>	ProxyConfig	5-Notice	1-User
Authentication Proxy Password Change Scheduler: modified by <username> at <user_ip>	ProxyConfig	5-Notice	1-User
Authentication Proxy Password Change: device <device global name> for privilege level <access level> changed by <username> at <user_ip>	ProxyConfig	4-Warning	1-User

Table F.3 Syslog Messages (Sheet 13 of 17)

Message	Tag Name	Severity	Facility
Authentication Proxy Password Change: device <device global name> for privilege level <access level> changed in the Authentication Proxy by <username> at <user_ip>	ProxyConfig	4-Warning	1-User
Authentication Proxy: password change initiated by <username> [at <user_ip>]	ProxyConfig	4-Warning	1-User
Authentication Proxy: password generation initiated by <username> [at <user_ip>]	ProxyConfig	5-Notice	1-User
Authentication Proxy: passwords for managed devices reverted to initial values by <username> [at <user_ip>]	ProxyConfig	4-Warning	1-User
Connection Directory: update failed	ProxyConfig	3-Error	3-System
Connection Directory: update initiated by <username> at <user_ip>	ProxyConfig	5-Notice	1-User
Connection Directory: update successful	ProxyConfig	5-Notice	3-System
Proxy Operations			
Authentication Proxy Session: attempt to elevate privileges on <managed_device> by <username> at <user_ip>	ProxyServices	4-Warning	1-User
Authentication Proxy Session: attempt to issue blacklisted command <command> by <username> at <user_ip>	ProxyServices	4-Warning	3-System
Authentication Proxy Session: connection to <managed_device> closed by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy Session: connection to <managed_device> established by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy Session: connection to <managed_device> timed out	ProxyServices	4-Warning	3-System
Authentication Proxy: <managed_device> is inaccessible	ProxyServices	3-Error	3-System
Authentication Proxy: automatic check in initiated by system	ProxyServices	5-Notice	3-System
Authentication Proxy: changed password(s) on <managed_device>	ProxyServices	4-Warning	3-System
Authentication Proxy: device <managed_device> access level <access_level> password persistence cleared by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> access level <access_level> password set to persist by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> check in by <username> [at <user_ip>] failed	ProxyServices	3-Error	1-User
Authentication Proxy: device <managed_device> check in by system failed	ProxyServices	3-Error	3-System
Authentication Proxy: device <managed_device> check out by <username> [at <user_ip>] failed	ProxyServices	3-Error	1-User
Authentication Proxy: device <managed_device> checked in by <username> [at <user_ip>] successfully	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> checked in by system successfully	ProxyServices	5-Notice	3-System
Authentication Proxy: device <managed_device> checked out by <username> [at <user_ip>] successfully	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> excluded from device management by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> exclusion from device management by <username> at <user_ip> failed	ProxyServices	3-Error	1-User

Table F.3 Syslog Messages (Sheet 14 of 17)

Message	Tag Name	Severity	Facility
Authentication Proxy: device <managed_device> failed to clear access level <access_level> password persistence by <username> at <user_ip>	ProxyServices	3-Error	1-User
Authentication Proxy: device <managed_device> failed to set access level <access_level> password to persist by <username> at <user_ip>	ProxyServices	3-Error	1-User
Authentication Proxy: device <managed_device> included in device management by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy: device <managed_device> inclusion in device management by <username> at <user_ip> failed	ProxyServices	3-Error	1-User
Authentication Proxy: password change aborted	ProxyServices	5-Notice	3-System
Authentication Proxy: password change complete	ProxyServices	5-Notice	3-System
Authentication Proxy: password change initiated by scheduler	ProxyServices	4-Warning	3-System
Authentication Proxy: password for <managed_device> is incorrect	ProxyServices	3-Error	3-System
Authentication Proxy: password generation aborted	ProxyServices	5-Notice	3-System
Authentication Proxy: password generation complete	ProxyServices	5-Notice	3-System
Authentication Proxy: password generation initiated by scheduler	ProxyServices	5-Notice	3-System
Authentication Proxy: password process being aborted by <username> at <user_ip>	ProxyServices	5-Notice	1-User
Authentication Proxy: password update for child password on <managed_device> failed	ProxyServices	3-Error	3-System
Authentication Proxy: password update for local change for <managed_device> failed	ProxyServices	3-Error	3-System
Authentication Proxy: password update on <managed_device> failed	ProxyServices	3-Error	3-System
Authentication Proxy: password updated for child password on <managed_device>	ProxyServices	4-Warning	3-System
Authentication Proxy: password updated locally for <managed_device>	ProxyServices	4-Warning	3-System
Authentication Proxy: proposed password(s) cleared by <username> at <user_ip>	ProxyServices	5-Notice	1-User
RADIUS			
RADIUS Authentication Connection: Active server changed to server <N>	RADIUS	3-Error	4-Security/ Authorization
RADIUS Authentication Connection: Request timed out	RADIUS	3-Error	4-Security/ Authorization- Authorization
RADIUS Authentication Server <N> Authorization: Access-Accept does not contain SEL-User-Role attribute for <username>	RADIUS	3-Error	4-Security/ Authorization
RADIUS Authentication Server <N> Authorization: Access-Accept received with invalid SEL-User-Role attribute for <username>	RADIUS	3-Error	4-Security/ Authorization
RADIUS Authentication Server <N> X.509: certificate does not match the server name or address	RADIUS	3-Error	4-Security/ Authorization
RADIUS Authentication Server <N> X.509: certificate is expired or it is not yet valid	RADIUS	3-Error	4-Security/ Authorization
RADIUS Authentication Server <N> X.509: unknown or untrusted certificate authority	RADIUS	3-Error	4-Security/ Authorization

Table F.3 Syslog Messages (Sheet 15 of 17)

Message	Tag Name	Severity	Facility
RADIUS Configuration			
RADIUS disabled by <username> at <user_ip>	RADIUSConfig	4-Warning	4-Security/ Authorization
RADIUS enabled by <username> at <user_ip>	RADIUSConfig	4-Warning	4-Security/ Authorization
RADIUS settings changed by <username> at <user_ip>	RADIUSConfig	5-Notice	4-Security/ Authorization
RADIUS Accounting^a			
RADIUS Accounting Connection: Accounting server does not respond	RADIUS	4-Warning	4-Security/ Authorization
RADIUS Accounting Connection: Active server changed to server <N>	RADIUS	4-Warning	4-Security/ Authorization
RADIUS Accounting disabled by <username> at <user_ip>	RADIUSConfig	4-Warning	4-Security/ Authorization
RADIUS Accounting enabled by <username> at <user_ip>	RADIUSConfig	4-Warning	4-Security/ Authorization
RADIUS Accounting settings change by <username> at <user_ip>	RADIUSConfig	4-Warning	4-Security/ Authorization
Routing Configuration			
Static Route <alias> Settings: changed by <username> at <user_ip>	RouteConfig	5-Notice	1-User
Static Route <alias>: created by <username> at <user_ip>	RouteConfig	5-Notice	1-User
Static Route <alias>: deleted by <username> at <user_ip>	RouteConfig	5-Notice	1-User
SELinux			
<audit_message>	avc	4-Warning	4-Security/ Authorization
SEL Whitelist			
File <filename> failed integrity check	SELWhitelist	4-Warning	4-Security
Serial Configuration			
Serial Interface <pre_alias> Alias: changed to <post_alias> by <username> at <user_ip>	SerialConfig	5-Notice	1-User
Serial Port <alias> Profile: <profile_alias> assigned by <username> at <user_ip>	SerialConfig	5-Notice	1-User
Serial Port <alias>: disabled by <username> at <user_ip>	SerialConfig	5-Notice	1-User
Serial Port <alias>: enabled by <username> at <user_ip>	SerialConfig	5-Notice	1-User
Serial Profile Configuration			
Serial Port Profile <alias> Settings: changed by <username> at <user_ip>	SerialProfileConfig	5-Notice	1-User
Serial Port Profile <alias>: deleted by <username> at <user_ip>	SerialProfileConfig	5-Notice	1-User
Service Port			
Management Interface Service Port: attempt to issue SHoW by <username> at <user_ip>	ServicePort	4-Warning	1-User
Management Interface Service Port: attempt to issue HAsH by <username> at <user_ip>	ServicePort	4-Warning	1-User
Service Port Configuration			
Management Interface Service Port: disabled by <username> at <user_ip>	ServicePortConfig	4-Warning	1-User

Table F.3 Syslog Messages (Sheet 16 of 17)

Message	Tag Name	Severity	Facility
Management Interface Service Port: enabled on port <port> by <username> at <user_ip>	ServicePortConfig	4-Warning	1-User
Single File Backup			
Single File Backup: export initiated by <username> at <user_ip>	BackupFile	4-Warning	1-User
Single File Backup: generation failed	BackupFile	3-Error	3-System
Single File Backup: generation on device serial number <device_serial> initiated by <username> at <user_ip>	BackupFile	5-Notice	1-User
Single File Backup: generation successful	BackupFile	5-Notice	3-System
Single File Backup: import initiated by <username> at <user_ip>	BackupFile	4-Warning	1-User
Single File Backup: update failed	BackupFile	3-Error	3-System
Single File Backup: update on device serial number <device_serial> successful	BackupFile	5-Notice	3-System
SNMP			
SNMP disabled by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP enabled by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Profile <alias> added by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Profile <alias> changed by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Profile <alias> deleted by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Trap Server <alias> added by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Trap Server <alias> changed by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Trap Server <alias> deleted by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
SNMP Trap Server <ip_address> changed to <new_ip_address> by <username> at <user_ip>	SNMPConfig	5-Notice	1-User
Syslog Configuration			
Local Firewall Storage Settings: modified by <username> at <user_ip>	SyslogConfig	4-Warning	1-User
Remote anti-chatter: disabled by <username> at <user_ip>	SyslogConfig	5-Notice	1-User
Remote anti-chatter: enabled by <username> at <user_ip>	SyslogConfig	5-Notice	1-User
Syslog Destination <alias> Settings: modified by <username> at <user_ip>	SyslogConfig	4-Warning	1-User
Syslog Destination <alias>: created by <username> at <user_ip>	SyslogConfig	5-Notice	1-User
Syslog Destination <alias>: deleted by <username> at <user_ip>	SyslogConfig	4-Warning	1-User
Syslog Settings: changed by <username> at <user_ip>	SyslogConfig	5-Notice	1-User
System Heartbeat Settings: modified by <username> at <user_ip>	SyslogConfig	4-Warning	1-User
Syslog Operations			
Local Syslog Event Queue contains <ecp%> unacknowledged events	Syslog	5-Notice	3-System
Local Syslog Event Queue contains <wcp%> unacknowledged events	Syslog	5-Notice	3-System
Local Syslog Event Queue contains >= ep% unacknowledged events	Syslog	2-Critical	3-System
Local Syslog Event Queue contains >= wp% unacknowledged events	Syslog	4-Warning	3-System
Suppressed <count> times	Syslog	Varies	Varies
Syslog event export initiated by <username> at <user_ip>	Syslog	6-Informational	1-User
Syslog events acknowledged by <username> at <user_ip>	Syslog	5-Notice	1-User
System Heartbeat: -- MARK --	Syslog	5-Notice	3-System

Table F.3 Syslog Messages (Sheet 17 of 17)

Message	Tag Name	Severity	Facility
Watchdog Alerts			
Watchdog timer expired	Watchdog	0-Emergency	0-Kernel
Web Server Configuration			
Web Server Settings: changed by <username> at <user_ip>	WebServerConfig	4-Warning	1-User
Web Server Operations			
Login while the default Web server authentication certificate was active	WebServer	4-Warning	4-Security/ Authorization
X.509 Configuration			
X.509 Certificate/Private Key <alias> has expired; communications requiring X.509 based authentication may have stopped	X.509Config	1-Alert	3-System
X.509 Certificate/Private Key <alias> will expire in <days_until_expiration> days; communications requiring X.509 based authentication may be affected when it expires	X.509Config	2-Critical	3-System
X.509 Certificate/Private Key <alias> will expire in <days_until_expiration> days; communications requiring X.509 based authentication may be affected when it expires	X.509Config	4-Warning	3-System
X.509 Certificate/Private Key <alias> will expire in <days_until_expiration> days; communications requiring X.509 based authentication may be affected when it expires	X.509Config	5-Notice	3-System
X.509 Certificate/Private Key <alias>: deleted by <username> at <user_ip>	X.509Config	5-Notice	4-Security/ Authorization
X.509 Certificate/Private Key <alias>: exported by <username> at <user_ip>	X.509Config	5-Notice	1-User
X.509 Certificate/Private Key <alias>: generated by <username> at <user_ip>	X.509Config	5-Notice	4-Security/ Authorization
X.509 Certificate/Private Key <alias>: imported by <username> at <user_ip>	X.509Config	5-Notice	4-Security/ Authorization
X.509 Certificate/Private Key <old_alias> Alias: changed to <new_alias> by <username> at <user_ip>	X.509Config	5-Notice	1-User

^a Available if RADIUS Accounting is enabled.

APPENDIX G

Networking Fundamentals

Introduction

A telecommunications network can be as simple as two devices linked together for sharing information or can be as complex as the internet involving many devices serving a multitude of purposes. In either case, networking devices need a common model for interconnectivity across a diverse set of communications media, manufacturer equipment, protocols, and applications. The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model to serve this purpose. The OSI model has been in use for decades as a reference model that describes the fundamental concepts and approach to interconnecting heterogeneous systems by abstracting the model into seven logical layers. This appendix provides an introduction to networking fundamentals and illustrates how device communication occurs across disparate networks.

OSI Model

The OSI model consists of seven conceptual layers as shown in *Figure G.1*. Each layer performs a specific task, operating relatively independently of the other layers, and only communicating with the layers adjacent to it as shown in *Figure G.1*. This independence has allowed manufacturers to develop implementations at their respective OSI layer and still be interoperable with implementations at a completely different layer. For example, a program interfacing at the Application layer does not need to know if the data being transmitted will traverse over an Ethernet, serial, or radio physical medium.

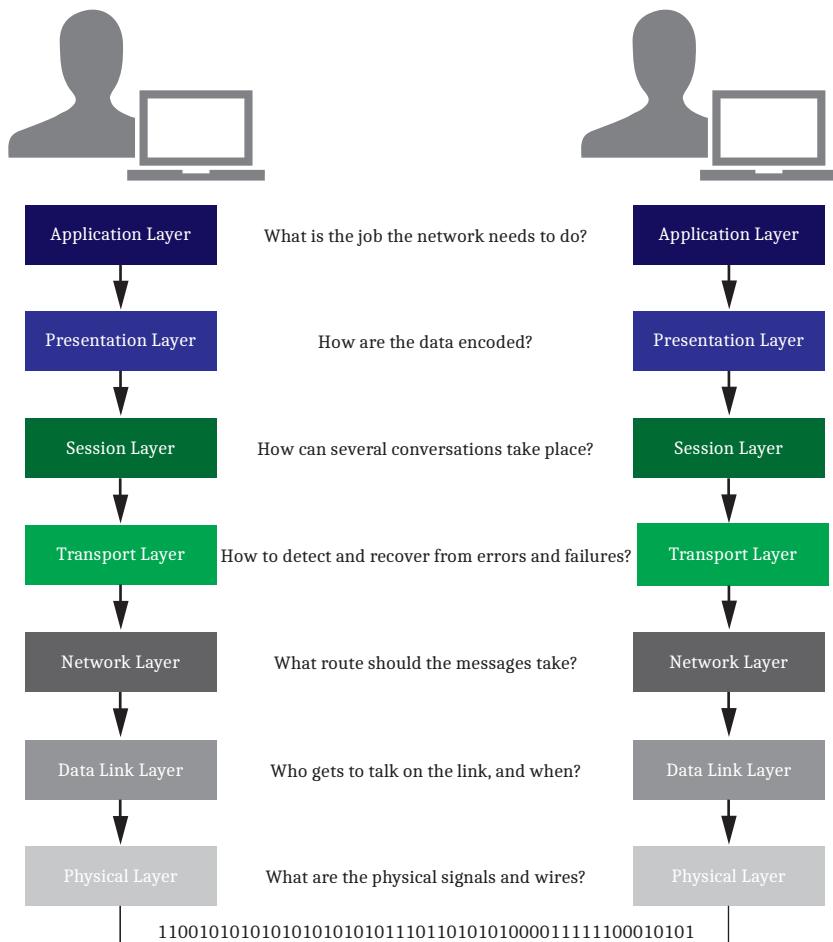


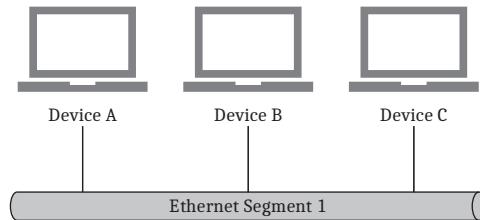
Figure G.1 OSI Model

Physical Layer (Layer 1)

The primary responsibility of the Physical Layer is transmitting data across a communications medium from one device to another. This layer defines the electrical and mechanical interfaces such as the hardware used in network interface cards used to interface with the physical medium that carries the bit stream. A Physical Layer device simply transmits or receives data and lacks any knowledge of the data that it transmits. Copper and fiber Ethernet are both examples of commonly used physical mediums. Network hubs and repeaters are devices commonly found at this layer.

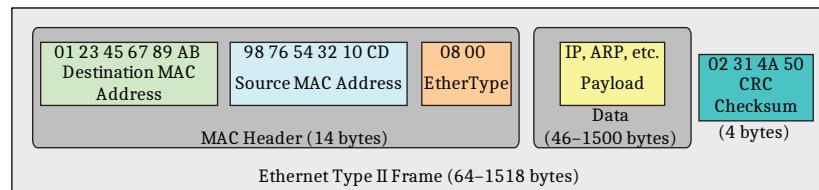
Data Link Layer (Layer 2)

The Data Link Layer is responsible for providing reliable transit of data across physical mediums by controlling frame synchronization, flow control, error detection, and providing physical addressing. Devices directly connected (*Figure G.2*) communicate at this layer without the need for a Layer 3 device, such as a router.

**Figure G.2 Ethernet Segment**

The Data Link Layer is subdivided into the Logical Link Control (LLC) and the Media Access Control (MAC) sub-layers. The LLC sub-layer manages communication between devices and handles the frame synchronization, flow control, and error checking mentioned above. The MAC sub-layer manages physical addressing at the Data Link layer. MAC addresses are physical addresses that are embedded into the hardware and determine how devices should uniquely identify each other on the same network segment. MAC addresses are also known as hardware addresses and are represented in the form of 01-23-45-67-89-ab.

Data received at this layer are organized into frames that encapsulate the data with descriptive information, called headers. An example of an Ethernet frame is depicted in *Figure G.3*.

**Figure G.3 Ethernet Frame**

The Ethernet frame in *Figure G.3* includes the following components:

- ▶ **MAC Header:** Includes the source and destination MAC addresses that determine which devices are communicating on the network. Also included is the EtherType, which defines the type of Ethernet framing used.
- ▶ **Data:** The data field includes the payload type as well as the actual data transmitted.
- ▶ **CRC Checksum:** The CRC checksum provides error checking to verify that the data are received exactly as sent.

Network Layer (Layer 3)

The Network Layer is responsible for transmitting data from one device to another device that is on a separate network segment. The separate network segment could be within close proximity, such as within the same building, or could be in a completely different country, as seen with the internet.

Addressing, routing, fragmentation, error handling, and congestion control are all functions of the Network Layer.

Layer 3 addressing is different from Layer 2 addressing in that addresses used at Layer 3 are logical. Logical addresses are hardware independent, unlike MAC addresses that are assigned to specific hardware. The Network Layer manages mappings between these logical addresses and physical addresses. Address Resolution Protocol (ARP) performs this mapping in IP networks.

The most common Layer 3 addressing scheme is IP addressing. IP addresses are 32-bit addresses, commonly denoted in dotted-decimal notation, that identify devices across different network segments.

Table G.1 shows an example IP address of 192.168.254.1 in dotted-decimal notation, with the equivalent 32-bit binary notation. Each 8-bit octet value is equivalent to the decimal value in the dotted-decimal notation. For example, the first binary octet of 11000000 is equivalent to 192 in the first octet of the dotted-decimal notation.

Table G.1 Sample IP Address

Dotted-Decimal Notation	192.168.254.1
32-Bit Binary Notation	11000000. 10101000. 11111110. 00000001

Routing is needed to define the path of the traffic between two networks. In *Figure G.4*, there are two IP networks, 192.168.254.0/24 and 10.10.10.0/24, with a router between the two networks. The router provides the ability for Device A, Device B, and Device C to communicate with Device D, Device E, and Device F. Without this router, these devices would not be able to communicate with each other. Device A, Device B, and Device C can all communicate among each other without the need for a router as described in *Data Link Layer (Layer 2)* on page G.2. The same is true for communication among Device D, Device E, and Device F.

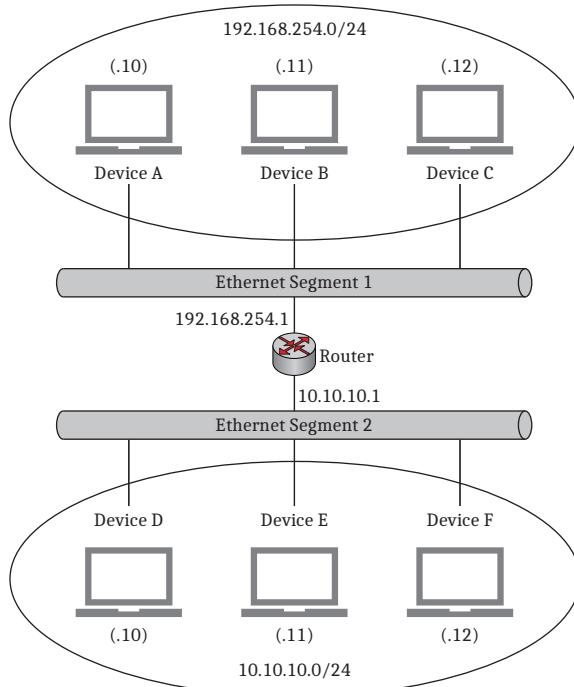


Figure G.4 Layer 3 IP Network

Transport Layer (Layer 4)

When data arrive at a network device that the Network Layer determines is the final destination, the Network Layer formats the data and passes them to the Transport Layer. This layer is responsible for end-to-end control and ensures successful data transfer. The main Transport Layer functions are flow control and error recovery.

Flow control manages the amount of data transmitted between communicating devices so that the sending device does not send more data than the receiving device can process.

Error recovery is handled differently with each Transport Layer protocol but typically involves requesting data retransmission if an error has been detected.

Transmission Control Protocol (TCP) is the Transport Layer protocol used in the TCP/IP suite to provide reliable, end-to-end communication. User Datagram Protocol (UDP) is also included as a connectionless protocol, meaning data are sent with no guarantee of successful delivery.

Connection-Oriented vs. Connectionless

Connection-oriented protocols, such as TCP, establish a connection between the sending device and the receiving device prior to data transmission. A connection is made between two devices through a three-way handshake (*Figure G.5*). The three steps in the handshake are as follows:

1. The sending device sends a Synchronization (SYN) packet to the receiving device.
2. The receiving device sends back a Synchronization/Acknowledgment (SYN/ACK) packet to the sending device.
3. The sending device completes the three-way handshake by sending an Acknowledgment (ACK) to the receiving device.

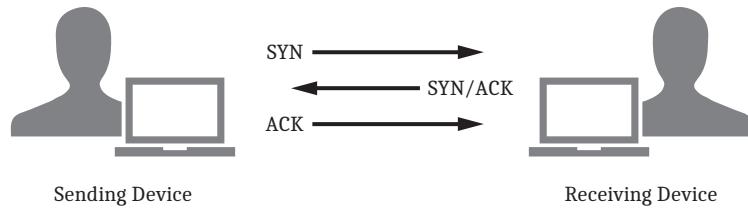


Figure G.5 TCP Three-Way Handshake

Once the three-way handshake completes, a connection is established and the two devices can begin transmitting and receiving data. The connection is maintained between the two devices throughout the session, providing a reliable connection and verification of data transmission.

In a connectionless protocol, such as UDP, no connection is established prior to data transmission, nor is a connection maintained at any point during data transmission. Because the protocol is connectionless, routing information must be sent with each data packet to provide information on how the data should traverse the network. Connectionless protocols provide no means for data transmission verification and are often referred to as unreliable protocols for this reason.

Session Layer (Layer 5)

The Session Layer handles session establishment, management, and termination between two end-user software application processes. This is the first layer that switches focus from the actual networking details and deals primarily with sessions consisting of service requests and responses that occur between applications installed on communicating devices.

Presentation Layer (Layer 6)

The Presentation Layer provides for standard data presentation for applications to exchange data in a meaningful manner across a network. The sending device converts data into a standard format for transmission on the network. The receiving device converts the data sent in this standard format to a format recognizable by the application of the receiving device. This processing occurs transparently to ensure that the data from the sending device is readable by the receiving device.

Application Layer (Layer 7)

The Application Layer is the layer closest to the end-user of a system. Software applications provide a means for end-users to interface with a device to transmit and receive data. The Application Layer provides the interface between the end-user and software applications that are used to process data over the network. Application Layer protocols define rules for communicating with network applications in a standardized format.

A P P E N D I X H

Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR) was developed as a method to help alleviate the exhaustion of IPv4 addresses available on the internet and also to reduce and simplify global routing tables across internet routers.

CIDR is an addressing scheme that allows for better utilization of IP addresses that traditionally fell into the old Class A, B, and C address schemes. In the traditional address scheme, Class A, B, and C addresses were categorized with 8, 16, and 24 bits used for the subnet mask, respectively. The smallest block of IP addresses in this addressing scheme is 254. This led to unused and wasted addresses in scenarios where someone needed 10 IP addresses but had to purchase the entire Class C block of 254 usable addresses. In situations where someone needed more than 254 addresses, they either had to purchase another Class C block or jump to a Class B or Class A network. The jump from Class C (254 usable addresses) to Class B (65,534 usable addresses) to Class A (16,777,214 usable addresses) provided no middle ground for IP addressing.

The solution was to allow network bits other than 8, 16, and 24, which resulted in providing that middle ground in the addressing scheme. For example, someone that needed only 10 IP addresses could be given a block of 14 usable IP addresses by using 28 network bits instead of 24 in the subnet mask.

CIDR allows blocks of contiguous addresses to be combined through route aggregation to create a larger, classless set of IP addresses. These aggregated routes can then be summarized into routing tables, resulting in fewer route advertisements.

In the example that follows, a route would need to be advertised for each classful network.

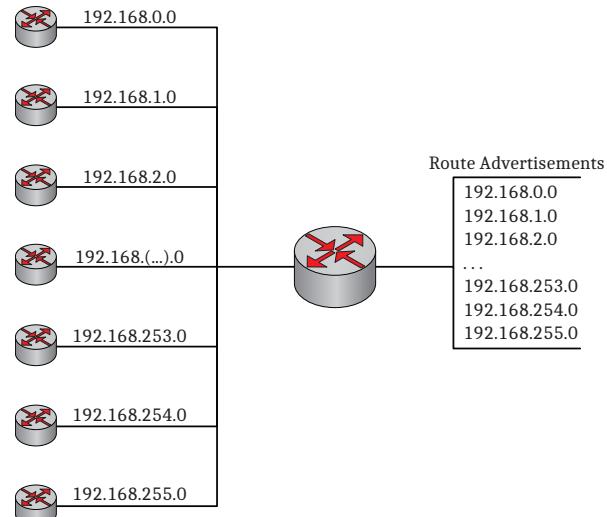


Figure H.1 Classful Route Advertisements

By using CIDR notation, multiple routes can be combined using route aggregation, as seen in the following figure. High-level route entries can represent many lower-level routes in the global routing table, simplifying routing and management of route tables.

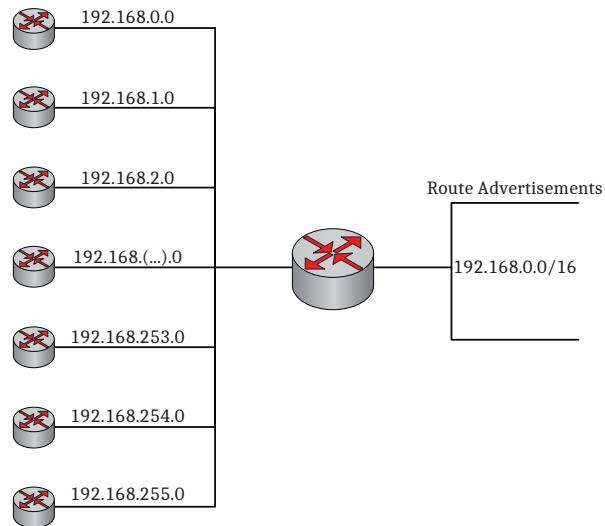


Figure H.2 CIDR Route Advertisements

CIDR has carried over to use in RFC 1918 addresses used in private networks by using CIDR notation when defining the subnet mask as well as simplifying internal routing tables. CIDR notation uses the format where the network ID and associated subnet mask are listed as $\text{xxx.xxx.xxx.xxx}/n$, where n is the number of leftmost bits set to a value of “1” in the mask. A traditional classful depiction of a network ID and subnet mask would be as follows:

Network ID: 192.168.1.0

Subnet Mask: 255.255.255.0 (dotted-decimal notation)

To take the above example and convert it to CIDR notation, you would need to count the number of leftmost bits set to a value of “1” in the binary notation of the subnet mask. The binary notation of the subnet mask of 255.255.255.0 would be 11111111 11111111 11111111 00000000. As you can see there are 24 bits set to a value of “1,” and therefore n would equal 24. The CIDR notation would be 192.168.1.0/24. The following table provides additional information about CIDR and the equivalent dotted-decimal notation.

Table H.1 CIDR to Dotted-Decimal Mapping (Sheet 1 of 2)

Subnet Mask (CIDR)	Subnet Mask (Dotted-Decimal)	# of Bits for Network ID	# of Bits for Host ID	# of Hosts per Network
/1	128.0.0.0	1	31	2,147,483,646
/2	192.0.0.0	2	30	1,073,741,822
/3	224.0.0.0	3	29	536,870,910
/4	240.0.0.0	4	28	268,435,454
/5	248.0.0.0	5	27	134,217,726
/6	252.0.0.0	6	26	67,108,862
/7	254.0.0.0	7	25	33,554,430
/8	255.0.0.0	8	24	16,777,214
/9	255.128.0.0	9	23	8,388,606

Table H.1 CIDR to Dotted-Decimal Mapping (Sheet 2 of 2)

Subnet Mask (CIDR)	Subnet Mask (Dotted-Decimal)	# of Bits for Network ID	# of Bits for Host ID	# of Hosts per Network
/10	255.192.0.0	10	22	4,194,302
/11	255.224.0.0	11	21	2,097,150
/12	255.240.0.0	12	20	1,048,574
/13	255.248.0.0	13	19	524,286
/14	255.252.0.0	14	18	262,142
/15	255.254.0.0	15	17	131,070
/16	255.255.0.0	16	16	65,534
/17	255.255.128.0	17	15	32,766
/18	255.255.192.0	18	14	16,382
/19	255.255.224.0	19	13	8,190
/20	255.255.240.0	20	12	4,094
/21	255.255.248.0	21	11	2,046
/22	255.255.252.0	22	10	1,022
/23	255.255.254.0	23	9	510
/24	255.255.255.0	24	8	254
/25	255.255.255.128	25	7	126
/26	255.255.255.192	26	6	62
/27	255.255.255.224	27	5	30
/28	255.255.255.240	28	4	14
/29	255.255.255.248	29	3	6
/30	255.255.255.252	30	2	2

This page intentionally left blank

A P P E N D I X I

Virtual Local Area Networks

Virtual Local Area Networks (VLANs) are logical groupings of devices that communicate with one another as though they are part of the same broadcast domain on a physical network segment. Devices within the same broadcast domain can send data directly to other devices within the same broadcast domain without sending traffic through a routing device. *Figure I.1* illustrates a network with two broadcast domains. Device A, Device B, and Device C are all within Broadcast Domain A and can communicate directly with one another. Similarly, Device D, Device E, and Device F are all within Broadcast Domain B and can communicate directly with one another. For devices to communicate between Broadcast Domains A and B, data must pass through the router. In this network configuration, all devices on the 2nd floor must be part of Broadcast Domain A, and all devices on the 1st floor must be part of Broadcast Domain B. This might work well in some configurations, but utilizing VLANs provides the flexibility to assign a device to a broadcast domain regardless of the physical location.

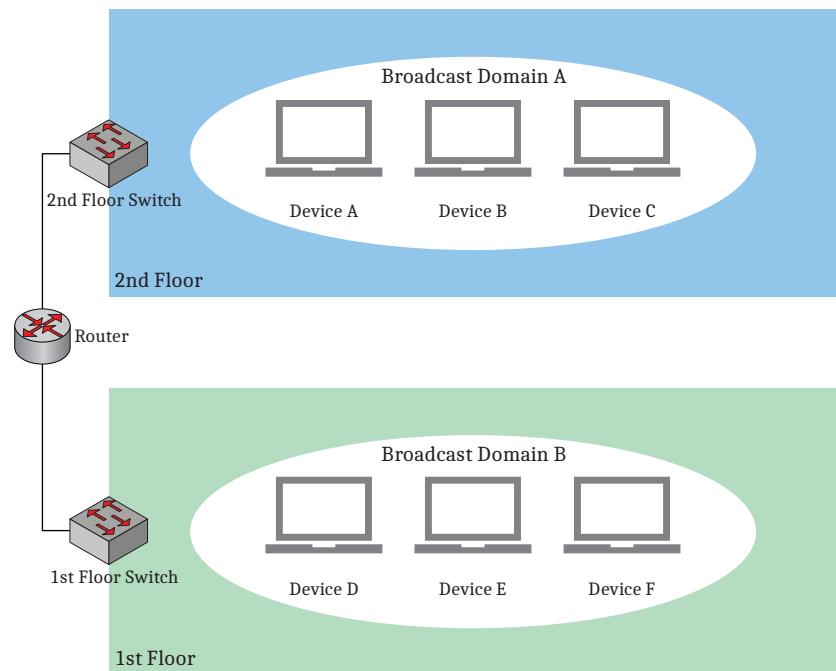
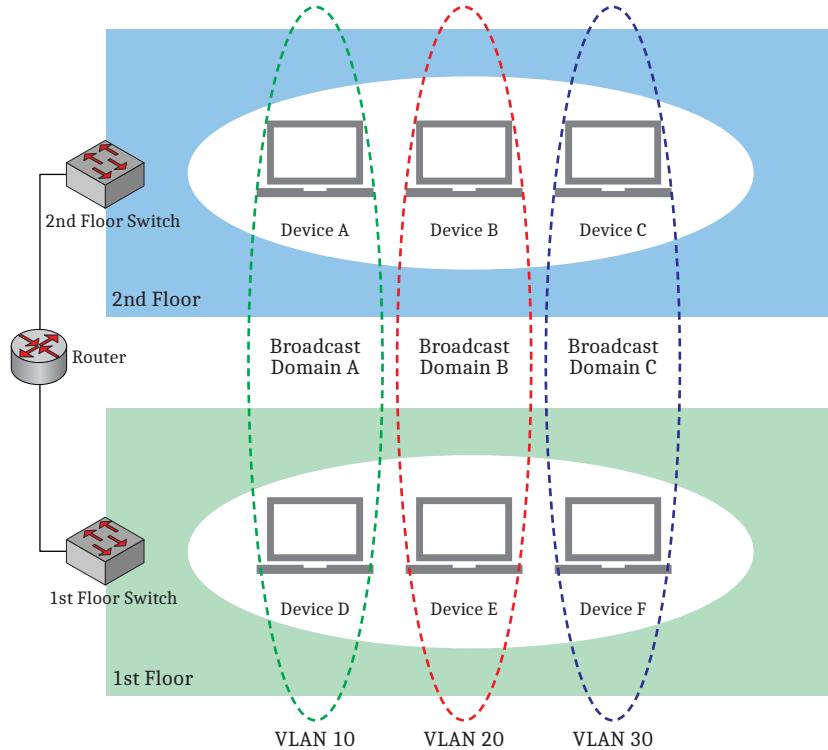


Figure I.1 Network Illustration Not Utilizing VLANs

Figure I.2 shows the same physical network utilizing VLANs. Broadcast Domain A now consists of Device A and Device D without requiring Device A to physically move to the 2nd floor. This can be useful when assigning VLANs to functional or departmental roles within an organization. Let's assume VLAN 10 was created for the Human Resources department that contains network resources spread throughout the 1st and 2nd floors. Without the use of VLANs, all network resources for the Human Resources department would need to be physically located on the same floor. As you can see in *Figure I.2*, VLAN membership is independent of physical location.

**Figure I.2 Network Illustration Utilizing VLANs**

VLANs also increase network performance in large broadcast domains. As the name implies, broadcast domains “broadcast” certain types of traffic to every device within the respective broadcast domain. As the number of devices increases within the broadcast domain, so does the amount of network traffic, which causes network congestion. By separating certain devices into different VLANs, the broadcast traffic is also separated and isolated to each VLAN. While this separation provided by VLANs is great for isolating broadcast traffic, VLANs should not be confused as a security mechanism for secure network segregation. Highly secure networks should use a switch independent of the switch used by a less secure network. For example, it is not recommended to include a publicly accessible DMZ network segment on the same switch as an internal LAN segment. While these two network segments may be on completely different networks and separated using a VLAN for the DMZ network segment and a VLAN for the LAN network segment, there are attacks that could bypass this network separation.

A P P E N D I X

Internet Protocol Security

Introduction

You have probably used Internet Protocol Security (IPsec) at some point, and maybe without realizing it. Virtual private networks (VPN) are one benefit of IPsec and many companies use them to provide secure corporate network access to remote workers. This is one way you have likely used IPsec. A VPN is a means to create a network extension that behaves as if it is connected to a larger enterprise-wide network service, and is one of the more common uses of IPsec.

IPsec is a suite of protocols designed to secure IP-based communication that strives to be as flexible as possible to allow for use in a variety of environments. This unfortunately brings with it a tremendous amount of complexity. IPsec provides security through authentication and encryption. Authentication is the verification of the source of a message or the integrity of a message. Encryption keeps a message confidential. Both of these functions are enabled through cryptographic technologies.

Security Provided

IPsec provides security in many forms. The security benefits the network (IP) layer of the OSI model and above. It does not protect the physical or data link layers.

Access control is the first protection mechanism that IPsec offers. There are multiple options in IPsec for access control that range from pre-shared secret knowledge, a key, which is required to access the protected system, to X.509 certificates, which can be linked to a specific person or system. Access controls are necessary to ensure that an attacker cannot gain access to your protected networks.

Data confidentiality is the idea that a message cannot be read and understood by anyone who is not the sender or the intended recipient of the message. It is provided in IPsec through a variety of supported encryption algorithms such as AES, DES, 3DES, CAST, IDEA, RC5, and Blowfish. Data confidentiality will greatly limit the amount of information an attacker can gain through passive attacks such as line sniffing.

Traffic flow confidentiality keeps the source and destination of a message secret. IPsec provides limited traffic flow confidentiality when gateways are used, preventing an attacker from learning the identities of the parties involved in the communication. The attacker can still learn the identities of the gateways though.

Connectionless integrity, also known as message authentication, verifies that a message has not been modified in transit. This modification can come from either natural corruption of a packet or through intentional manipulation. Cryptographic hash functions such as MD5 and SHA provide this to IPsec. This prevents an assailant from causing any damage through active attacks such as bit-flipping.

Other active attacks that IPsec protects against are spoofing and replay attacks. Spoofing attacks are characterized by an attacker pretending they are someone else, usually a trusted party. IPsec protects against spoofing attacks through a data origin authentication mechanism. Attackers will capture messages and resend those same messages at a later time in a replay attack. To protect against replay attacks, IPsec uses message sequencing.

Protected Paths

There are three different types of communications paths that IPsec can protect. These are host-to-host, host-to-gateway, and gateway-to-gateway. In IPsec, a host is an end device and a gateway is an intermediate device. A host-to-host IPsec connection protects all data between two end devices. A host-to-gateway IPsec connection is similar to the corporate VPN mentioned previously where an end device (laptop) connects to a network through a VPN gateway. A gateway-to-gateway IPsec connection is also known as a site-to-site VPN, and generally protects messages flowing between two separate networks.

Two Protection Protocols

IPsec has two core protocols that are applied to a packet to protect it and the information in it. These are the Authentication Header (AH) and the Encapsulating Security Payload (ESP). Both of these protocols serve different purposes and are used in different situations.

Authentication Header

As its name implies, the AH protocol will only provide authentication services to the protected communication. Confidentiality is not a concern with this protocol. AH provides the following services:

- Connectionless integrity
- Data Origin authentication
- Antireplay
- Access control

Some of these security services are dependent upon the mode being used. The modes of use are described in *Two Modes of Use* on page J.3.

The AH protocol protects communication through modification of the datagram by extending the IP header. Only two fields in this extension provide security to the original datagram: the sequence number and the authentication data. All other fields provide the necessary information for network devices to process the datagram.

Encapsulating Security Payload

Unlike the AH protocol that only modifies the message header and does not touch the payload, ESP actively modifies the payload through encryption. This provides confidentiality to the message. ESP provides the following security services:

- Data confidentiality
- Limited traffic flow confidentiality

- Connectionless integrity
- Data origin authentication
- Antireplay
- Access control

Some of these security services are dependent upon the mode being used. The modes of use are described in *Two Modes of Use* on page J.3.

ESP has two flavors: with authentication and without authentication. ESP without authentication does not provide connectionless integrity.

Two Modes of Use

IPsec has two modes of use that apply to the AH and the ESP protocols. These modes of use are transport mode and tunnel mode. The factors that go into choosing the mode of use are the two endpoints of the IPsec session. If the IPsec session is between two host devices, then transport mode is typically used. If the IPsec session involves a gateway, then Tunnel mode must be used to prevent issues with packet fragmentation and reassembly.

Transport Mode

Transport mode is for the protection of upper-layer protocols between the two hosts. Protection is provided through authentication, encryption, or both. Transport mode does not provide a VPN, but it does provide a secure IP connection.

Transport mode functions by slightly modifying the original IP header to indicate that the datagram is either protected by AH or ESP. This modification is done to the protocol field. The only other modification is performed to the packet length field, to add the length of the AH or ESP information.

Tunnel Mode

Tunnel mode provides protection to tunneled Network Layer (IP Layer) protocols. If an IPsec session includes a gateway, then tunnel mode must be used. This prevents issues with packet fragmentation and reassembly.

Tunnel mode functions by encapsulating the entire IP datagram within a new IP datagram. A completely new header is built with the two endpoints of the tunnel as the new source and destination addresses. Only the type of service field is copied from the original IP header. VPNs are built using IPsec ESP with authentication in tunnel mode.

Internet Key Exchange

Encryption and authentication algorithms require all parties involved to have some pre-shared secret information or keys that are used to decode messages. IPsec supports two methods for doing this. One method is manually sharing the

keys. This requires an out-of-band method and the user is entirely responsible for the security of the keys. The manual method is also not very scalable. The second method is an automated in-band mechanism known as Internet Key Exchange (IKE).

IKE is the protocol that IPsec uses to securely negotiate cryptographic sessions. IKE uses a Diffie-Hellman key exchange to securely transport the keys that both parties use for IPsec encryption and authentication.

IKE has two modes: main mode and aggressive mode. Main mode is the more secure of the two and requires six packet exchanges to securely exchange session material. Aggressive mode uses only half the number of exchanges because some information is sent in cleartext. One complete IKE session is required to establish one security association.

Security Associations

A security association (SA) includes all of the information needed to specify a simplex (one-way) IPsec session. This includes information identifying the session and information to process the session traffic. There is a limit of one SA per AH or ESP connection and a limit of one AH or ESP connection per SA.

SA session identification information includes the peer IP address, the IPsec protocol being used (ESP or AH), and the Security Parameters Index (SPI). The SPI exists for the case where the same two peers establish multiple IPsec connections.

SA processing information identifies the encryption or authentication algorithms to apply to packets identified by their addresses and SPIs. SA processing information also includes IP filtering policies and key exchange parameters.

An SA describes a simplex communications channel. This means that bidirectional-protected communication between two peers requires at least two SAs.

APPENDIX K

X.509

Introduction

In cryptography, X.509 is an International Telecommunication Union standard for public-key infrastructure (PKI). The standard specifies formats for public-key certificates and validation paths for authentication. The device uses X.509 certificates both in the web server for secure device management and for IPsec authentication.

Public-Key Cryptography

Public-key cryptography is distinguished by the use of asymmetric keys instead of the more traditional symmetric keys. Asymmetric keys are mathematically related so that whatever one key encrypts, the other key must be used to decrypt. There is no way to derive one key from knowledge of its paired key. These key pairs are known as public and private keys. The private key must be kept secret, while the public key can be freely distributed. This allows for many methods of protecting and authorizing messages that are not possible with symmetric key cryptography.

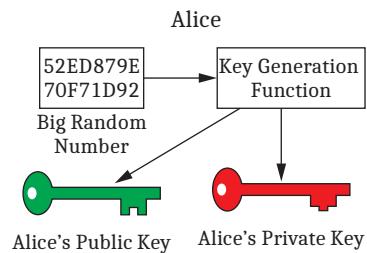


Figure K.1 Asymmetric Keys

Symmetric key cryptography, which has been used in various forms for thousands of years, uses a single key that both encrypts and decrypts the message. This key must be shared between the sender and receiver in advance. If the key cannot be securely shared, the confidentiality of any transmission encrypted with that key cannot be known.

In public-key cryptography, the encryption key is not the same as the decryption key. If a message is encrypted with the publicly known key, only the private key can be used to decrypt it. Because this private key is known only to the owner of the key pair, the message will be known only to the sender and the intended receiver, ensuring confidentiality.

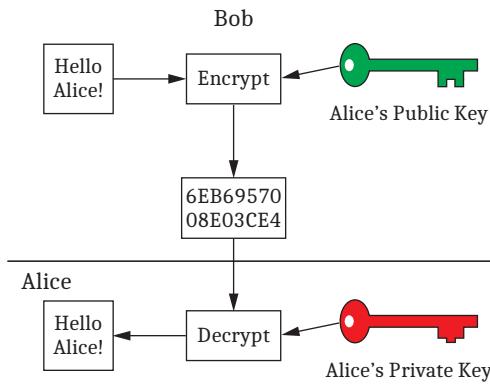


Figure K.2 Confidentiality With Asymmetric Keys

Public-key cryptography is much more computation intensive than symmetric key cryptography. This makes it unfeasible to send large amounts of data or secure a series of transmissions by using this technology. The benefit from the confidentiality that public-key cryptography offers is the ability to securely and confidentially exchange symmetric keys. This is known as hybrid cryptography and is one way that IPsec uses public-key cryptography.

Public-key cryptography can also be used for authentication. This is done by using a private key as the encryption key, rather than the public key. The public key used to decrypt the message will identify who the sender was. This is known as an electronic signature.

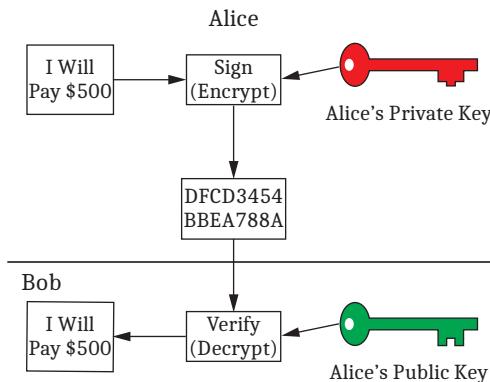


Figure K.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public-key certificates, provide a formal method for tracking pairs of asymmetric keys and who they belong to. These electronic documents, through the use of digital signatures, are used to bind public keys to their owners. Digital certificates are primarily used in three different ways involving public-key infrastructure, web of trust, and simple public-key infrastructure. These three methods are distinguished by the certificate issuer.

Beginning with firmware version R210, certificates used for IPsec Key Exchange (IKE) on the SEL-3620 and SEL-3622 that contain a keyUsage extension must also have either the digitalSignature or nonRepudiation bits set. This change

makes the SEL-3620 and SEL-3622 more compliant with RFC 4945, section 5.1.3.2. Certificates that do not comply may cause the IKE process to fail, preventing a connection from being established.

Digital Signatures

A digital signature is a more formal method of authentication than an electronic signature. They can be likened to the wax seals that were placed on envelopes before email was available. A digital signature is created by computing a hash of the certificate and encrypting that hash with the private key of the issuer. This signature is then attached to the certificate. To verify the authenticity of the certificate, the certificate and signature are first separated. A hash of the certificate is computed and the signature is decrypted by using the public key of the issuer. These two results are compared, and if they match, we know the certificate is authentic.

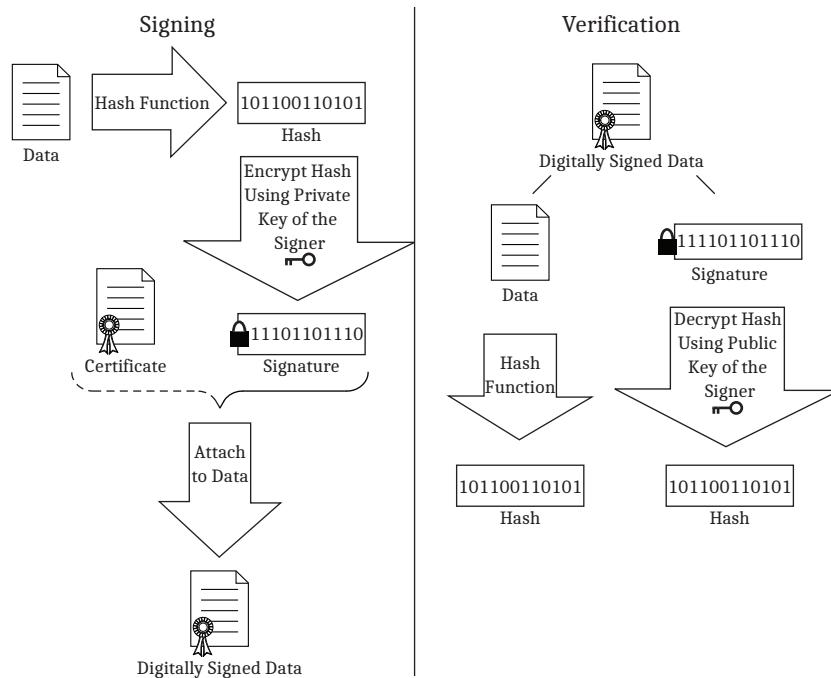


Figure K.4 Digital Signatures

Public-Key Infrastructure

One of the three ways that digital certificates are commonly used is in a PKI. PKI is a formal, hierarchical system where a digital certificate is signed by a more trusted certificate. At the top of the PKI hierarchy is the most trusted certificate, the root certificate. This certificate is self-signed, highly protected, and should only be used to sign CA certificates. If the root certificate is compromised, all certificates below it must be assumed to be compromised as well.

A certificate authority (CA) is an entity that issues, or signs, other certificates. To obtain a certificate, an entity will generate a key pair, and send the public key and credentials to a CA. The CA will verify the authenticity of the credentials and

issue the certificate containing those credentials, the public key and the CA digital signature. A CA is responsible for confirming that this person is who they claim to be. CAs are authenticated by other CAs or by the root certificate.

Be aware that this process can be subverted. This happens when an attacker requests a certificate and provides valid credentials for the victim. The CA, thinking everything is good, will issue a certificate to the attacker, in the name of the victim. Care must be taken in communicating with the CA to ensure that this will not happen.

Web of Trust

Another of the three common uses of digital certificates is in the web of trust. This is a less formal method of authentication than PKI provides, but is still in common use. The largest use of the web of trust model is in Pretty Good Privacy (PGP) used for email security. This model is very similar to PKI in that a trusted third party is verifying the authenticity of a certificate. The difference is that this trusted third party is not a CA, but rather a person who endorses the authenticity of another person. Signing the public key of the person requiring endorsement (or trust) with the private key of the endorser (trusted entity) establishes a web of trust. *Figure K.5* illustrates a simple example of a web of trust: if Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

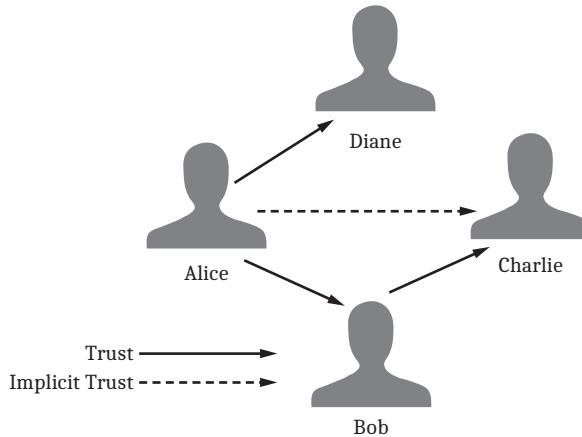


Figure K.5 Web of Trust

Simple Public-Key Infrastructure

The third common use of digital certificates is in the simple public-key infrastructure (SPKI). This model evolved from the need to limit the complexity inherent in PKI and the web of trust. There is no trusted third party in SPKI as the owner and issuer of the certificate are the same entity. For SPKI to be secure, certificates must be pre-shared among all entities who communicate on that system. This ensures that all knowledge for security decisions resides locally.

Online Certificate Status Protocol (OCSP)

In consideration of the case where an authentic certificate has been stolen, there are methods to revoke certificates. One method is the certificate revocation list (CRL). The CRL method has a few problems that allow a revoked certificate to still be used. This arises from the lag associated with producing CRLs. Also, a certificate will be accepted by default, even if revoked, if the CRL is not accessible.

The online certificate status protocol (OCSP) was created to fix some of these problems. OCSP requires less bandwidth than CRLs and enables near real-time status checks to verify the status of a certificate. OCSP also allows a certificate to be denied by default if the OCSP server is not accessible.

OCSP is a request/response protocol that provides real-time revocation status information for X.509 certificates. When an OCSP-enabled certificate is presented to an application, such as a web browser, the browser checks the certificate that is using OCSP to ensure it is valid before proceeding with the session. OCSP uses the following response indicators for use in determining certificate revocation status:

- Good: Indicates that the certificate is valid and has not been revoked
- Revoked: Indicates that the certificate has been revoked
- Unknown: Indicates that the responder does not know about the certificate being requested

A real-time revocation check for each certificate is performed so that if a certificate is compromised or for some other reason requires revocation, it will no longer appear as valid.

Sample X.509 Certificate

```
Certificate:  
Data:  
    Version: 3 (0x2)  
    Serial Number: 1 (0x1)  
    Signature Algorithm: md5WithRSAEncryption  
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,  
           OU=Certification Services Division,  
           CN=Thawte Server CA/Email=server-certs@thawte.com  
    Validity  
        Not Before: Aug 1 00:00:00 1996 GMT  
        Not After: Dec 31 23:59:59 2020 GMT  
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,  
             OU=Certification Services Division,  
             CN=Thawte Server CA/Email=server-certs@thawte.com  
    Subject Public Key Info:  
        Public Key Algorithm: rsaEncryption  
        RSA Public Key: (1024 bit)  
            Modulus (1024 bit):  
                00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:  
                68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:  
                85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:  
                6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:  
                6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:  
                29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:  
                6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:  
                5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:  
                3a:c2:b5:66:22:12:d6:87:0d  
            Exponent: 65537 (0x10001)  
    X509v3 extensions:  
        X509v3 Basic Constraints: critical  
            CA:TRUE  
    Signature Algorithm: md5WithRSAEncryption  
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:  
        a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:  
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:  
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:  
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:  
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:  
        b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:  
        70:47
```

This page intentionally left blank

A P P E N D I X L

Lightweight Directory Access Protocol

SEL LDAP Client Implementation

LDAP allows the device to bind with existing centralized account directories, such as Microsoft Active Directory, for user authentication and authorization. The specific LDAP implementation uses the StartTLS method for securing LDAP data from the device to the centralized account server. See *Figure L.1* for information about the LDAP interaction between the SEL LDAP client and the centralized server.

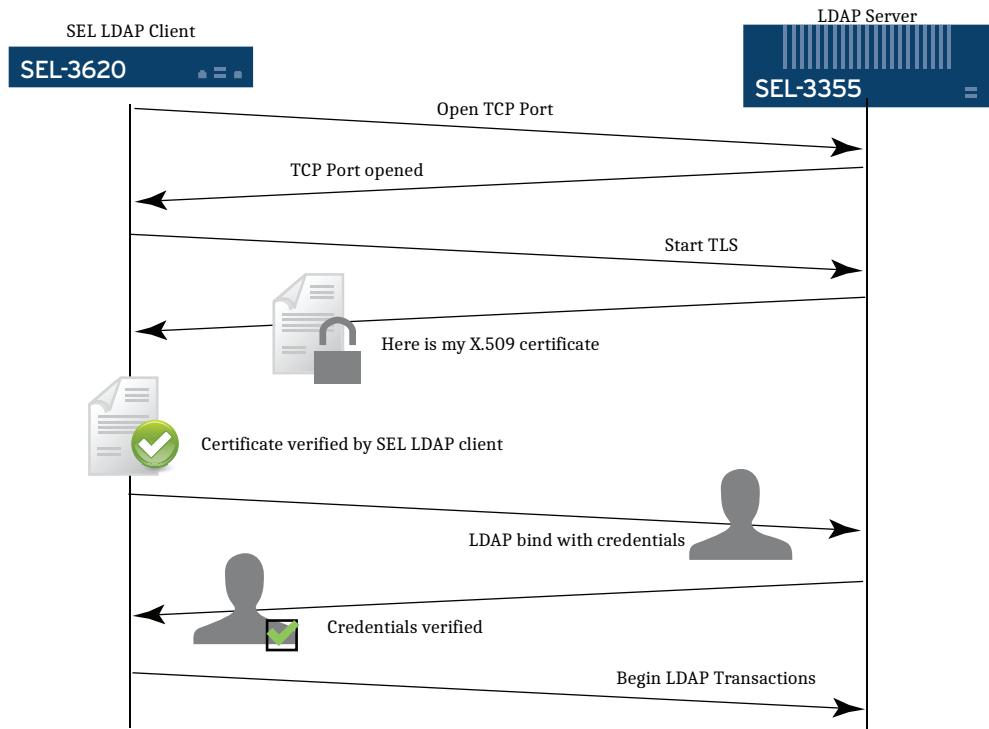


Figure L.1 LDAP Transaction

Certificate Chain

When an SEL device receives an X.509 certificate from an LDAP server during a StartTLS exchange prior to LDAP bind, you will need to have the certificate chain stored locally. The certificate chain, also known as the certification path, is a list of certificates used to authenticate the LDAP server. The chain, or path, begins with the certificate of the LDAP server (the one the SEL device receives), and each certificate in the chain is signed by the CA identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in

the chain must be verified by the SEL LDAP client until the root CA certificate is reached. The Distinguished Name (DN) of the X.509 certificate that the LDAP server uses to authenticate to the SEL LDAP client must match the LDAP server name (i.e., LDAP server “3355.x509.local” must match its certificate DN “3355.x509.local”).

LDAP Settings Form

LDAP Hosts

(Input these settings on the Hosts page, need at least one):

Hostname:

IP Address:

Hostname:

IP Address:

Hostname:

IP Address:

LDAP Settings

(Input these settings on the LDAP Settings page):

Search Base:

User ID Attribute:

Group Member Attribute:

Bind DN (optional, if left blank will use anonymous binds):

Bind DN Password (optional, required only if not using anonymous binds):

LDAP Servers

(Input these settings on the LDAP Settings page, need at least one):

Hostname:

Port Number:

Hostname:

Port Number:

Hostname:

Port Number:

Attribute Mappings

(Optional, input these settings on the LDAP Settings Page):

First Name Attribute:

Last Name Attribute:

Email Attribute:

Telephone Attribute:

Device Roles

(Required to map user privileges, input these settings on the LDAP settings page):

Administrator Group/User DN:

Engineer Group/User DN:

A P P E N D I X M

SEL RADIUS Dictionary

```
#####
# COPYRIGHT (c) 2017 Schweitzer Engineering Laboratories, Inc.
#
# FILE DESCRIPTION: SEL VENDOR SPECIFIC ATTRIBUTES
# VERSION: 1.1
#####

# THIS FILE CONTAINS TWO DICTIONARY FORMATS, ONE FOR FREERADIUS, AND ONE FOR THE
# RSA RADIUS SERVER. THE SETTINGS FOR THE RSA RADIUS SERVER HAVE BEEN
# 'COMMENTED OUT'. TO USE THIS FILE WITH THE RSA RADIUS SERVER, COMMENT OUT THE
# LINES BETWEEN: FREERADIUS STARTS HERE AND FREERADIUS END, AND UNCOMMENT THE
# LINES BETWEEN: RSA STARTS HERE AND RSA END

#####
# SEL-USER-ROLE IS USED TO ASSIGN A DEVICE ROLE TO A USER FOR SYSTEM ACCESS.
# VALID FOR ACCESS-ACCEPT MESSAGES ONLY.
# A MINIMUM OF ONE SEL-USER-ROLE PER USER IS REQUIRED.
# THE PREDEFINED VALUES ARE (CASE SENSITIVE):
# Administrator
# Technician

# SEL-PROXY-GROUP IS USED TO ASSIGN PROXY GROUPS TO A USER FOR ACCESSING MANAGED
# DEVICES. THE VALUE OF SEL-PROXY-GROUP SHOULD BE THE NAME OF A PROXY GROUP THE
# USER IS A MEMBER OF.
# VALID FOR ACCESS-ACCEPT MESSAGES ONLY.
# SEL-PROXY-GROUP IS REQUIRED ONLY FOR MANAGED DEVICE ACCESS.
# MULTIPLE SEL-PROXY-GROUP ATTRIBUTES MAY BE USED.
# ONLY ONE PROXY GROUP ALLOWED PER ATTRIBUTE.

# SEL-SYSLOG-MESSAGE IS USED TO PROVIDE USER ACTIONS ON THE SYSTEM.
# THE VALUE OF SEL-SYSLOG-MESSAGE WILL BE THE SYSLOG MESSAGE.
# VALID FOR ACCOUNTING-REQUEST MESSAGES ONLY.
# ONLY ONE SEL-SYSLOG-MESSAGE PER MESSAGE IS ALLOWED.

# SEL-ACCT-INFO IS USED TO PROVIDE INFORMATIONAL MESSAGES.
# THE VALUE OF SEL-ACCT-INFO WILL BE A TEXT MESSAGE.
# VALID FOR ACCOUNTING-REQUEST MESSAGES ONLY.
# ONLY ONE SEL-ACCT-INFO PER MESSAGE IS ALLOWED.

#-----
# FREERADIUS STARTS HERE
```

VENDOR	SCHWEITZER-ENGINEERING-LABORATORIES-INC.	31823
--------	--	-------

BEGIN-VENDOR SCHWEITZER-ENGINEERING-LABORATORIES-INC.

ATTRIBUTE	SEL-USER-ROLE	1	STRING
ATTRIBUTE	SEL-PROXY-GROUP	2	STRING
ATTRIBUTE	SEL-SYSLOG-MESSAGE	11	STRING
ATTRIBUTE	SEL-ACCT-INFO	12	STRING

END-VENDOR SCHWEITZER-ENGINEERING-LABORATORIES-INC.

```
# FREERADIUS END
#-----
# RSA STARTS HERE

# @radius.dct

# MACRO      SEL-VSA(TYPE,SYNTAX)    26          [VID=31823 TYPE1=%TYPE%  
LEN1=+2 DATA=%SYNTAX%]
# ATTRIBUTE   SEL-USER-ROLE        SEL-VSA(1, string)  R
# ATTRIBUTE   SEL-PROXY-GROUP     SEL-VSA(2, string)  R
# ATTRIBUTE   SEL-SYSLOG-MESSAGE  SEL-VSA(11, string) C
# ATTRIBUTE   SEL-ACCT-INFO       SEL-VSA(12, string) C

# RSA END
#-----
```

APPENDIX N

Web Server Security With Transport Layer Security

Introduction

The web server in the SEL-3600 family of devices has many levels of protection implemented in it to keep the device and your configuration traffic secure. One technology used, Transport Layer Security (TLS), can directly affect user interaction with the product. The computer and web browser you use to configure and interact with the web server of the SEL-3600 family must support TLSv1.2 or TLSv1.3. TLSv1.0 and Secure Socket Layer (SSL) are no longer considered secure and the SEL-3600 family will not use them.

TLS is a protocol suite that authenticates peer devices, encrypts communications, and verifies message integrity. The TLS protocol suite relies on many other standards and technologies to function correctly, including X.509, HTTP session cookies, encryption ciphers, message hashing algorithms, and others. For more information on X.509, see *Appendix K: X.509*.

HTTP Session Cookies

HTTP session cookies are provided by the SEL-3600 web server when your browser contacts the login or commissioning pages of the web server to initiate a new secure session. The cookie consists of a unique identifying string and flags to indicate to the browser how the cookie should be used. The browser then uses the cookie for all communications to the web server, so the web server can verify the integrity of the web session. The cookie persists until the web browser is closed.

The user's web browser must be capable of supporting cookies and must have support for cookies enabled. SEL strongly recommended that you use a web browser that also accepts the `HTTPOnly` flag found in the SEL-3600 web server cookie. This flag prevents certain types of web server attacks, such as JavaScript attacks and cross-site request forgeries.

TLS

The SEL-3600 family web server supports TLSv1.2 and TLSv1.3 to encrypt and authenticate web session traffic with browsers that support TLSv1.2 and TLSv1.3. *Table N.1* lists the TLSv1.2 ciphers supported by the SEL-3600 family web server in order of priority. *Table N.2* lists the TLSv1.3 ciphers supported by

the SEL-3600 family web server in order of priority. The web server used must also support at least one of these ciphers. The SEL-3600 family web server will use the highest priority cipher that the browser supports.

Table N.1 TLSv1.2 Cipher List

Cipher Name	Key Exchange Method	Server Authentication Method	Symmetric Encryption Algorithm	Message Authentication Algorithm
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AEAD (GCM-AES-128)	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AEAD (GCM-AES-256)	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE	RSA	AEAD (GCM-AES-128)	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE	RSA	AES	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE	RSA	AES	SHA-1
ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	AEAD	SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE	RSA	AES	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE	RSA	AES	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES	SHA-1

Table N.2 TLSv1.3 Cipher List

Cipher Name	Key Exchange Method	Server Authentication Method	Symmetric Encryption Algorithm	Message Authentication Algorithm
TLS_AES_256_GCM_SHA384	RSA	RSA	AEAD (GCM-AES-256)	SHA384
TLS_CHACHA20_POLY1305_SHA256	RSA	RSA	AEAD	SHA256
TLS_AES_128_GCM_SHA256	RSA	RSA	AEAD (GCM-AES-128)	SHA256

APPENDIX O

Media Access Control Security (MACsec)

Overview

MACsec is made up of two distinct components and several SEL inventions:

- *IEEE 802.1AE MACsec Protocol* on page O.2
- *IEEE 802.1X-2010 Clause 9: MKA Protocol* on page O.4

MACsec Abbreviations and Definitions

- **aCAK:** automatic Connectivity Association Key.
- **AES:** Advanced Encryption Standard.
- **AN:** Association Number.
- **CA:** for Connectivity Association.
- **CAK:** Connectivity Association Key.
- **CKN:** Connectivity Association Key Name.
- **CO:** Confidentiality Offset.
- **EAPoL-MKA:** Extensible Authentication Protocol over LAN as defined by IEEE 802.1X, that incorporates MACsec Key Agreement.
- **EC:** Embedded Client.
- **GCM:** Galois Counter Mode.
- **ICV:** Integrity Check Value.
- **IED:** intelligent electronic device.
- **IPsec:** Also known as IP security, IPsec is a suite of cryptographic protocols that can be used to establish VPNs. IPsec is identified by a series of RFCs including RFC 4301 and RFC 4309.
- **IV:** Initialization Vector.
- **KDF:** Key Derivation Function.
- **KS:** Key Server.
- **LAN:** Local Area Network.
- **LPN:** the Lowest-acceptable Packet Number.
- **MACsec:** Media Access Control Security.
- **MKA:** MACsec Key Agreement.
- **MSDU:** MACsec Service Data Unit.
- **NAC:** Network Access Control.
- **OSI Model:** The Open Systems Interconnection model has seven layers to identify how and when certain communications functions should be performed.
- **pCAK:** pre-shared Connectivity Association Key.
- **PNs:** Packet Number associated with each MACsec Packet.

- **RNG:** Random Number Generator.
- **SA:** Secure Association.
- **SAK:** Secure Association Key.
- **SCI:** Secure Channel Identifier.
- **SecTag:** Security Tag.
- **SSL/TLS:** Secure Sockets Layer and Transport Layer Security. TLS is the successor to SSL. Both provide cryptographic protection for communication over Ethernet networks. TS is often used in conjunction with HTTP to provide secure communication over the internet. TLS is identified in RFC 5246.

IEEE 802.1AE MACsec Protocol

Introduction

MACsec is a non-routable “hop-by-hop” cryptographic protocol that protects Ethernet frames starting at the data-link layer (OSI Layer 2). When MACsec is enabled, a bi-directional secure link is established after an exchange and verification of security keys between the two connected devices. MACsec protocol provides the following security attributes, as shown in *Figure O.1*:

- **Confidentiality:** Optional obfuscation of the Ethernet frame’s data payload through encryption.
- **Integrity:** Prevention of manipulation of any section of the Ethernet frame using an ICV.
- **Authenticity:** Providing proof of the identity of the hosts on the LAN and proof of the identity of the hosts within the CA with symmetrical encryption keys.
- **Replay Prevention:** Mitigation of replay attacks using consecutive PNs.

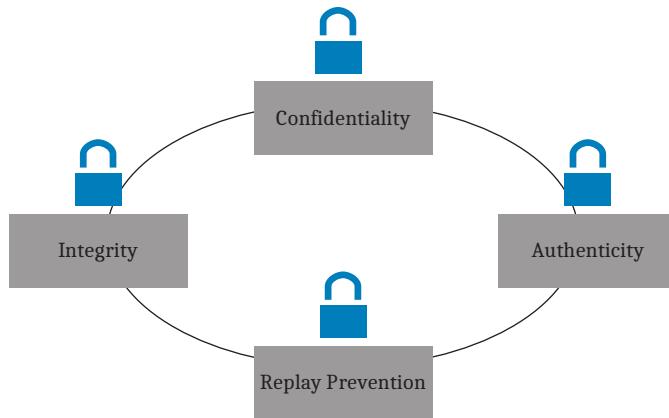
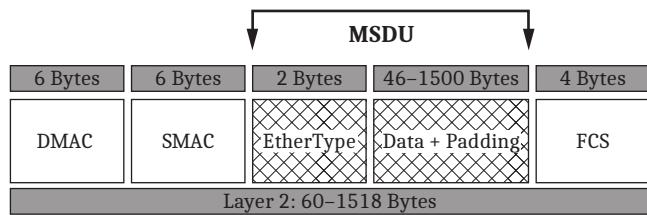
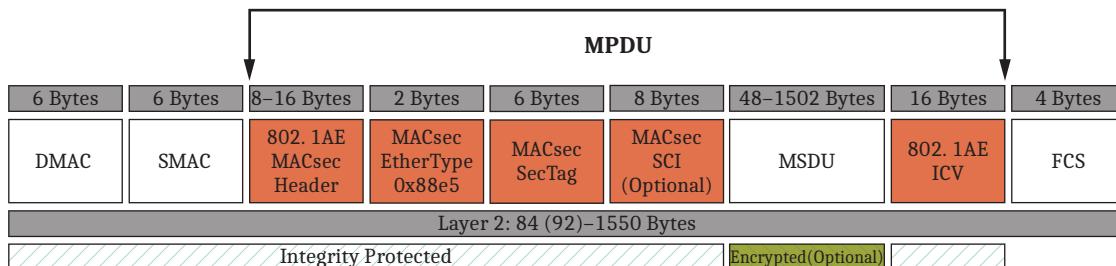


Figure O.1 MACsec Protocol Attributes

MACsec works by taking the original Ethernet frame and adding two components to it: a MACsec SecTag and an ICV. *Figure O.2* is an example of a normal Ethernet II frame, where the original EtherType and payload comprise the MSDU of the original frame.

**Figure O.2 Ethernet II Frame**

In MACsec protection, an additional header and the SecTag are inserted in the frame after the MAC addresses and before the original EtherType. The ICV is inserted after the MSDU and before the Frame Check Sequence (FCS). SecTag and ICV allow the receiver of the frame to verify the authenticity and integrity of the frame and prevent replay attacks. *Figure O.3* shows the normal Ethernet II frame with the addition of MACsec.

**Figure O.3 MACsec-Enabled Ethernet II Frame**

By default, MACsec uses Galois Counter Mode Advanced Encryption Standard with a 128-bit key (GCM-AES-128). GCM-AES is an Authenticated Encryption with Additional Data (AEAD) cipher which performs both encryption and authentication of the original data using a single key. AEAD ciphers are useful for the SEL MACsec solution because they enable the device to secure all parts of an Ethernet frame. Unlike TLS or IPsec, this means that MACsec can optionally encrypt the data payload and still provide integrity and replay protection for the entire Ethernet frame, including the original source and destination MAC addresses (which are never encrypted). GCM-AES-128 has its own NIST standard, SP 800-38D.

Cryptographic Keys

NOTE: MACsec parameters for the SEL-3620 use the Cryptographic Cipher of GCM-AES-128, a Confidentiality Offset of 0, and a replay-widow size of 0.

When hosts on a LAN want to securely communicate with each other using MACsec, they use a 32- or 64-byte symmetric SAK to secure the connection. To prevent packet loss when transitioning to a new SAK, each device must be able to support two SAKs simultaneously, each distinguished by an AN ranging from 0–3. Depending on the devices in the CA, all frames between the two devices can then be secured with MACsec, with the assumption that no attacker is able to communicate successfully on the network with other hosts without knowing the correct SAK.

MACsec on Point-to-Point ICS LAN



Figure O.4 MACsec on Point-to-Point ICS LAN

For two MACsec-supporting devices to communicate, they must be configured with the following:

- One or more keys (passwords), called SAKs, along with the respective AN used to distinguish individual keys
- A Cryptographic Cipher, which for IEEE 802.1AE is GCM-AES-128
- A CO, that indicates how much of the Ethernet payload is to be encrypted

In this scenario, hosts using MACsec can communicate directly with each other or through traditional unmanaged Ethernet switches, SDN switches, or even Ethernet radios.

Scalability, Maintainability, and Ease-of-Use

For point-to-point scenarios, MACsec configuration is simpler than either TLS or IPsec. Generally, the user must program two SAKs with their respective ANs and include a CO (if desired).

However, there are some maintainability and ease-of-use concerns:

- **SAK Rotation:** SAKs need to be retired after 2^{32} packets due to the use of the PN as an initialization vector (IV) (repeated IVs due to PN rollover after 2^{32} frames break GCM-AES). On a Sampled Values network with 4000 packets per second, an SAK would be exhausted after 12 days [$(2^{32}) / (3600 * 24 * 4000)$]. Networks that only run DNP for SCADA or intermittent engineering access traffic would not see packet numbers to this level.
- **Commissioning:** A point-to-point configuration is simpler than TLS or IPsec (using SAKs, ANs, and COs).

IEEE 802.1X-2010 Clause 9: MKA Protocol

Introduction

The goal of MKA protocol is to facilitate and automate the commissioning, management, and scalability of MACsec on a LAN. MKA provides these ease-of-use attributes:

- **Network Discovery:** hosts can discover other MKA-supporting devices attached to the same LAN.
- **Mutual Authentication:** hosts can confirm mutual possession of a CAK and prove a past mutual authentication.

- **Key Management:** MKA automatically manages the generation of new SAKs for all authorized MACsec hosts joining a LAN and rotates SAKs when they near expiration. MKA can also distribute new CAKs to ensure that CAKs are refreshed on a regular basis.
- **MACsec Parameter Management:** MKA enables the automatic creation of SCIs and facilitates the synchronization of the cipher suites and COs used by all authorized MACsec hosts.

MKA automates most of the commissioning and management overhead of MACsec protocol for all authorized hosts on a LAN. Devices implementing MKA will either act as a KS (devices that distribute keys and decide the cipher suite) or as an EC (devices that receive keys and follow the direction of the KS).

The MKA protocol is an extension to the IEEE 802.1X Port-Based NAC standard and is specific to MACsec implementations. Two or more MACsec-authorized hosts use MKA to advertise and synchronize with each other on a LAN through an 802.1X-specific multicast MAC address. During synchronization, the hosts exchange details and negotiate which device becomes the MACsec KS on the LAN. When the negotiation is complete, the MACsec KS is responsible for automating SAK distribution to authorized members, synchronizing MACsec cipher suite details, and rotating SAKs when their expiration nears. Some devices are configured to either be just a KS, or just a client, where no negotiation is required.

Cryptographic Keys

All hosts wanting to use MKA with each other require a CAK with an associated CKN. Using the CAK with the GCM-AES cipher, MKA protocol authenticates hosts on the LAN and securely distributes encrypted SAKs to MACsec-authorized devices. Once all necessary SAKs are distributed, hosts can securely communicate with each other using MACsec.

NOTE: The SEL-3620 supports the AES-CMAC-128 algorithm for MKA control packets.

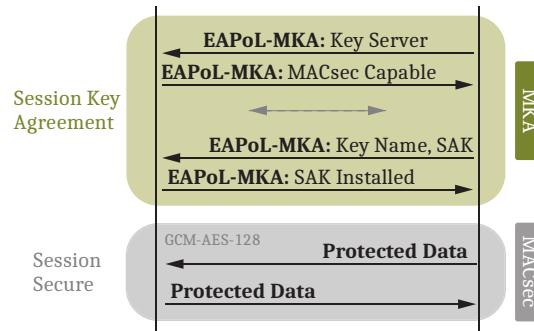


Figure 0.5 Secure Communication Using MACsec

MKA on ICS LANs

NOTE: Communicating through managed switches is not currently supported by MKA protocol. IEEE Standard 802.1Q requires blocking the forwarding of received group bridge frames.

For two or more MACsec and MKA-supporting devices to be able to communicate, they must be configured with a CAK with an associated CKN. Hosts integrating MACsec and MKA can communicate directly with each other or through existing unmanaged switching infrastructure.

MACsec Architecture

Definitions

- **Connectivity Association (CA):** A set of MACsec attributes used to create secure channels for inbound and outbound traffic between devices.
- **Embedded Client (EC):** A device that will never act as a key server (e.g., the SEL-651R Advanced Recloser Control).
- **Key Server (KS):** A device that can generate and distribute keys (SAKs and CAKs) used in the MACsec system (e.g., an SEL-3622 Security Gateway).

Point-to-Point



Figure O.6 Point-to-Point Architecture

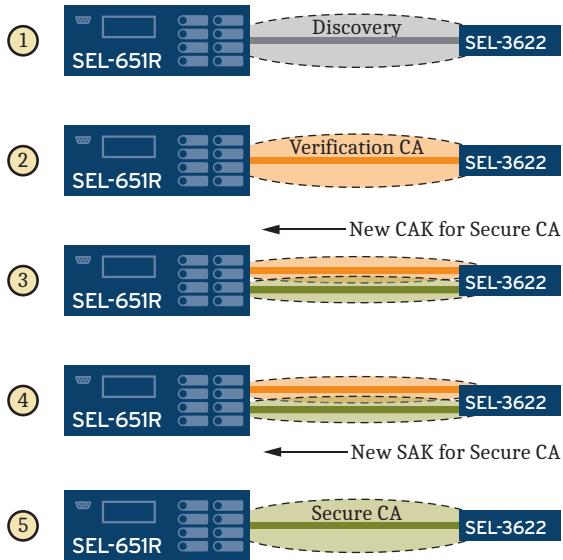
Point-to-point architectures are the simplest MACsec implementation. Users can easily implement this architecture between a KS and EC. In this implementation, only the EC and the KS communicate with each other, and they form a single MACsec CA. The cryptographic relationship between the KS and EC are not shared with any other device.

SEL Innovations

In addition to MACsec and MKA (industry standards), SEL enhanced MACsec with several crucial innovations that serve to make the implementation easier and more secure.

Device Verification

SEL's implementation of MACsec uses a process of MKA verification to maximize the simplicity of commissioning scenarios. MKA verification removes the need for a user to initially input a CAK/CKN pair to complete the host adoption process. *Figure O.7* shows how MKA verification works in SEL devices.

**Figure O.7 MKA Verification**

1. The SEL devices discover each other using an initial verification CA that is advertised by the KS and distinguished through the use of a unique, SEL specific, CKN which is “SELVER_00000000000000000000000000000000”.
2. The SEL devices verify each other differently depending on which commissioning mode is selected. Manual adoption is then completed by the user, confirming the KS on the user interface of the client, via the Command Line Interface (CLI) or front panel.
 - a. Auto-commissioning mode involves utilization of a CAK (dCAK) derived on both devices from the same input by the same derivation function.
 - b. Manual commissioning mode involves utilization of a pre-shared CAK (pCAK) that the KS generates and displays to the user, which the user then manually inputs into the client interface using CLI as a verification.
3. After verification is complete, the KS generates and distributes a new unique group automatic CAK (aCAK) and CKN tuple to the client. The CAK is randomly generated by the KS, as is the CKN.
4. The client and KS bring up the new secure CA and confirm each other on the new CAK/CKN live members list. At this point, the KS distributes a SAK on the new CA.
5. The KS and client delete each other from the live members list on the verification CA. The client ceases advertising on the verification CA. Members begin secure MACsec-protected communications on the new CA.

For the user, MKA verification allows the KS and the client to securely communicate using MACsec with minimal settings and zero management overhead.

Automatic CAK Rotation

Once a CAK is configured for MKA, there is no standards-based method to automatically rotate that key beyond CAK caching. However, IEEE 802.1X-2010 subclause 9.12 specifies a method for using an MKA key server to distribute a

NOTE: See Maintain Backups in Appendix C: Best Practices for Emergency Readiness for considerations on performing system backups when implementing automatic or manual CAK rotation.

subsequent group CAK/CKN pair for use with a different CA. Automatic MKA CAK rotation operates similarly to SEL's MKA verification implementation, as shown in *Figure O.8*.

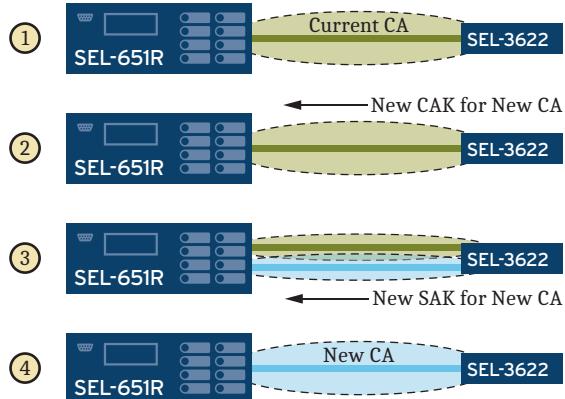


Figure O.8 Automatic MKA CAK Rotation

1. During an active CA, an end-user desires to change the CAK. This can be triggered in three ways:
 - a. The end-user has configured the KS to automatically rotate the CAK on a schedule, and that scheduled change now takes place.
 - b. An end-user manually initiates a CAK change via the SEL-3622 web interface.
 - c. KS reboots and a new CAK is distributed to the EC.
2. The KS (SEL-3622) generates and distributes the new CAK/CKN tuple to the client.
3. The client and KS bring up the new CA and confirm each other on the new CAK/CKN live members list. At this point, the KS distributes an SAK on the new CA, allowing members to begin secure MACsec-protected communications.
4. The KS and client delete each other from the live members list on the old CA. Both client and KS cease advertising on the old CA.

Cryptographic Considerations

- **Key Generation:** IEDs without secure key generation capabilities should use an MKA protocol priority of 255, indicating that they should never become a KS.
- **SAK Exhaustion:** SAKs would need to be considered expired when 64GB of data has been encrypted with the key, and when the PN value of 0xC000 0000 (decimal 3,221,225,472) has been reached (per the MKA protocol). MKA automatically rotates SAKs based on PN. Note that the maximum SAK lifetime may occur prior to SAK exhaustion by configuring the SAK Lifetime setting in the SEL-3622 web interface.
- **Relay Entropy:** Relays do not need RNGs with good entropy sources to securely communicate using MACsec, so long as relays (ECs) never act as KSSs, which are responsible for generating and distributing keys.

APPENDIX P

Cybersecurity Features

The SEL-3610 is primarily a serial-to-serial and Ethernet-to-serial cryptographic port server. Its cybersecurity features include the ability to allow serial devices to communicate securely through Ethernet network tunnels via SSH. It also supports centralized user-based access controls with LDAP or RADIUS. The focus of the remainder of this appendix is on the cybersecurity features of the SEL-3620 and SEL-3622.

The SEL-3620 Ethernet Security Gateway is a router, virtual private network (VPN) endpoint, and firewall device that can perform security proxy services for serial and Ethernet-based intelligent electronic devices (IEDs). The SEL-3620 helps create a user audit trail through strong, centralized, user-based authentication and authorization to modern and legacy IEDs. The SEL-3620 secures control system communications with a stateful deny-by-default firewall, strong cryptographic protocols, and logs for system awareness. The SEL-3620 also manages protected IED passwords, ensuring that passwords are changed regularly and conform to complexity rules for stronger security. The integrated security proxy also provides user-based single sign-on access to Ethernet and serial devices. The SEL-3622 Security Gateway provides the same cybersecurity features as the SEL-3620 in a smaller form factor and is interchangeable with the SEL-3620 throughout this appendix.

Version Information

Device Firmware

The device firmware identification (FID) number can be obtained through the web interface of the SEL-3620. The SEL-3620 firmware is provided in a single digitally signed and encrypted file.

Ports and Services

Physical Ports

The SEL-3620 has one front Ethernet port and two rear Ethernet ports used for management and data, and one USB port that can be used for out-of-band management and configuration. There are 16 rear serial ports (4 on the SEL-3622) that can be used for secure serial communications over an Ethernet network via IPsec or SSH. The front Ethernet and USB ports are enabled by default. All serial and rear Ethernet ports are disabled by default.

Logical Ports

See Appendix D: Open Network Ports.

Centralized User-Based Access to Protected IEDs

The authentication proxy technology integrated in the SEL-3620 provides single sign-on engineering access to protected IEDs. The strong authentication in the SEL-3620 includes centralized user-based credentials with LDAP or RADIUS and verification of the source of user communications. Thorough logging of all user activities on protected devices provides simple audit reports from which you can know who did what when.

Password Management

User-based accounts increase log granularity and make password management easy and effective. The SEL-3620 includes support for centralized authentication and authorization to simplify management and enforcement of user accounts, strong passwords, and user privileges for all protected devices from an active directory server.

Firewall

An integrated stateful, deny-by-default firewall prevents unauthorized communications from entering or exiting the protected network. The SEL-3620 filters incoming and outgoing TCP, UDP, ICMP, AH, and ESP communications based on a user-configurable set of rules.

X.509 Certificates

The SEL-3620 can use either X.509 certificates or preshared keys for authentication of another party over a network. The X.509 certificate confirms that the party at the opposite end of the tunnel is an entity with whom the SEL-3620 has approval to communicate. The SEL-3620 accepts both self-signed X.509 certificates and X.509 certificates that have been signed by a Certificate Authority (CA). The SEL-3620 uses OCSP to check the status of X.509 certificates.

Physical Access Controls (SEL-3622 Only)

The SEL-3622 is designed to make it difficult to physically tamper with the device without generating a log and alarm. The SEL-3622 can detect changes in light intensity with an embedded light sensor, motion with an embedded accelerometer, and opening of cabinet doors with a discrete input contact.

Cryptographic Message Protection

IPsec

The SEL-3620 performs the following steps when it connects to any peer IPsec-enabled device: the two peers must authenticate each other, the IKE security associations (SAs) must be established, and the IPsec SAs must be established. Upon establishment of the IPsec SAs, the SEL-3620 transmits all messages that route through this “tunnel” within an Encapsulating Security Payload. An IPsec SA defines the communications parameters that will be in use for communication

across a VPN. The SEL-3620 contains preconfigured settings in “Profiles” to simplify connecting to non-SEL devices. The supported profiles are the following:

- Lemnos IKEv2
- Lemnos IKEv1
- Lemnos - Cisco
- SEL - Secure (2022)

MACsec

MACsec provides industry-standard security through the use of secured point-to-point Ethernet LAN links. The point-to-point links are secured after matching security keys are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption.

Encryption ensures that communications are confidential and only readable by authorized parties. The SEL-3620 uses MACsec Security Protocols to protect the communication.

The SEL-3620 will participate as an MKA key server only, not as a client. MACsec is configured in connectivity associations. Key management is automated for simplicity with MACsec and MKA.

Alerts and Logging

Security Events

The SEL-3620 uses the syslog format to log events in nonvolatile memory, and it generates, stores, and forwards syslog messages to multiple destinations. These logs contain several fields that indicate event severity, event origin, the type of event that occurred, and details regarding the cause of the event. Additionally, the event message contains such event tracking information as the entity that triggered the event and the time and date of the event. For slow communications links, the SEL-3620 can throttle the number of outgoing syslog messages.

Internal Log Storage

The SEL-3620 formats, stores, and forwards logs according to the syslog specification to enable quick notification, central collection, and interoperable reporting of security events. IRIG-B and NTP time synchronizes these events. The SEL-3620 records IED user activity to provide you with auditable tracking within your system. Internal storage can hold as many as 60,000 events in non-volatile memory. If storage is full, new events replace the oldest events.

Backup and Restore

Saving and Restoring Settings

The SEL-3620 web interface provides two methods to backup and restore settings. The single file backup provides the entire SEL-3620 configuration, connection directory, and managed passwords as a single file that can be exported from the Single File Backup tab of the File Management page of the web interface. The file exported from the Single File Backup process can be used to restore an entire device in the event of an emergency or catastrophic failure.

Decommissioning

Preparing for Recycling or Disposal

It is often desirable to delete settings from the product when it is removed from service.

To delete the SEL-3620 settings, factory reset the SEL-3620 through the web interface.

Malware Protection Features

Operating System and Firmware

The SEL-3620 is an embedded device that does not allow additional software to be installed. The SEL-3620 exe-GUARD feature provides whitelist architected antivirus and other malware protections, including a secure kernel that prevents unauthorized access or modification of system data and monitors critical system services to detect unexpected activity caused by unauthorized modifications to the device program. The SEL-3620 only accepts digitally signed firmware upgrades. See “The SEL Process for Mitigating Malware Risk to Embedded Devices” at selinc.com/malware_protection/ for more details.

Revision Management

Appendix A: Firmware and Manual Versions contains a description of each firmware update.

See “The SEL Process for Disclosing Security Vulnerabilities” at selinc.com/security_vulnerabilities for details on vulnerability disclosure.

Firmware Update Verification

The SEL-3620 automatically checks the firmware authenticity and integrity and only loads firmware files that have been signed by SEL. The authenticity and integrity of firmware updates also can be verified by checking the firmware hash. For instructions and firmware hash values, see selinc.com/products/firmware.

Contact SEL

For further questions or concerns about product security, contact SEL Security at:
security@selinc.com or +1.509.332.1890.

This page intentionally left blank

Glossary

3DES	3DES, or triple DES, is a more secure form of the DES encryption algorithm.
aCAK	Abbreviation for automatic Connectivity Association Key.
AD	Abbreviation for Additional Data.
AE	Abbreviation for Authenticated Encryption.
AES	Abbreviation for Advanced Encryption Standard. AES is the U.S. government-approved algorithm to encrypt military data.
Alias	An alternative name assigned to ports and configurations to allow for quick and descriptive identification.
AN	Abbreviation for Association Number.
Blowfish	Blowfish is an encryption algorithm.
CA	Abbreviation for Connectivity Association.
CAK	Abbreviation for Connectivity Association Key.
CIDR	Abbreviation for classless inter-domain routing. CIDR simplifies network addressing and allows for better utilization of IP addresses. CIDR is used on the SEL-3620 rather than subnet masks.
CKN	Abbreviation for Connectivity Association Key Name.
CO	Abbreviation for Confidentiality Offset.
Communications Protocol	A language for communication between devices.
Dead Peer Detection	Dead peer detection provides a method for an IPsec gateway to detect if peer gateways have become inaccessible.
DES	Abbreviation for Data Encryption Standard. DES is no longer considered secure.
Diffie-Hellman	A cryptographic protocol that allows two parties with no pre-shared knowledge to establish a shared secret key over an untrusted IP-based network.
Diffie-Hellman Group	Groups in the Diffie-Hellman algorithm define the size and type of the secret material that is used to exchange material securely.
EA	Abbreviation for Energy automation.
EAPoL-MKA	Abbreviation for Extensible Authentication Protocol over LAN as defined by IEEE 802.1X, that incorporates MACsec Key Agreement.
EC	Abbreviation for Embedded Client.
EMS	Abbreviation for Energy management system.

ESP	Abbreviation for Encapsulating Security Payload. ESP is part of the IPsec suite and provides encryption and optional authentication for IPsec protected traffic. ESP is identified in RFC 4303.
Ethernet	A network architecture defined by IEEE 802.2 and IEEE 802.3.
exe-GUARD	exe-GUARD is a whitelist-based anti-malware technology developed under a U.S. Department of Energy project to develop anti-malware technology for use in embedded devices.
Firewall	A firewall blocks or allows Ethernet traffic by filtering the traffic based on a set of rules.
Firmware	The nonvolatile program stored in the relay that defines relay operation.
Flash Memory	A type of nonvolatile memory used for storing data.
g	The acceleration of an object resulting from the gravitational pull of the Earth. A value of 1 g is roughly 9.8 m/s ² .
GCM	Abbreviation for Galois Counter Mode.
HTTP	Abbreviation for Hypertext Transfer Protocol. HTTP is the primary communications protocol used on the internet and allows communication between web browser and servers. HTTP is identified in RFC 2616.
HTTPS	Abbreviation for Hypertext Transfer Protocol Secure. HTTPS is a combination of HTTP and SSL/TLS to provide cryptographically protected communication between a web browser and a server. HTTPS is identified in RFC 2818.
ICMP	Abbreviation for Internet Control Message Protocol. ICMP is used for diagnostic and routing purposes. ICMP is identified in RFC 792.
ICMP Ping	A type of ICMP packet that allows a system to determine whether it can communicate with a specific host.
ICMP Traceroute	A type of ICMP packet that allows a system to determine the route to a specific host.
ICV	Abbreviation for Integrity Check Value.
IEEE 802.1Q	IEEE 802.1Q is a method for creating VLANs by attaching a tag to Ethernet packets. These tags identify the VLAN the packet belongs to.
IKE	Abbreviation for Internet Key Exchange. IKE is the cryptographic protocol used to securely establish the security associations used in the IPsec protocol suite. IKE is identified in RFC 2409.
IP Address	An identifier for a computer or device on a TCP/IP network.
IPsec	Also known as IP security, IPsec is a suite of cryptographic protocols that can be used to establish VPNs. IPsec is identified by a series of RFCs including RFC 4301 and RFC 4309.
IRIG-B	A time-code signal that can be used to synchronize devices.
ISAKMP	Internet Security Association and Key Management Protocol. ISAKMP is used for establishing secure cryptographic communication over an untrusted IP-based network. ISAKMP is defined by RFC 2408.

ITU-T X.509	X.509 is a standard that describes the standard formats for public-key certificates.
IV	Abbreviation for Initialization Vector.
KDF	Abbreviation for Key Derivation Function.
KS	Abbreviation for Key Server.
LED	Light-emitting diode. Used as indicators on the front panel.
Lemnos	Lemnos is a Department of Energy project to identify a common set of technologies, parameters, metrics, and vocabulary to enable interoperable security for control systems.
LPN	Abbreviation for the Lowest-acceptable Packet Number.
Lux	The SI unit of illuminance. A value of 1 lux is equal to 1 lumen per square meter.
MAC Address	The Media Access Control (hardware) address of a device used to identify Ethernet devices at the data link layer of the OSI model.
MACsec	Abbreviation for Media Access Control Security.
MKA	Abbreviation for MACsec Key Agreement.
MODP	A type of Diffie-Hellman group.
MSDU	Abbreviation for MACsec Service Data Unit.
NAC	Abbreviation for Network Access Control.
NAT	Abbreviation for Network Address Translation. NAT modifies the addressing information of a packet to provide the ability to remap a given address space to another.
OCSP	Abbreviation for Online Certificate Status Protocol. OCSP is used to determine the status of X.509 certificates.
OPSAID	Abbreviation for Open PCS Security Architecture for Interoperable Design. The OPSAID program was a Department of Energy initiative to promote interoperable security solutions for control systems. The work done in the OPSAID program led into the Lemnos program.
OSI Model	The Open Systems Interconnection model has seven layers to identify how and when certain communications functions should be performed.
PC	Abbreviation for personal computer.
pCAK	Abbreviation for pre-shared Connectivity Association Key.
Perfect Forward Secrecy	Perfect forward secrecy prevents knowledge of past or current cryptographic key material from providing any insight into the current or future cryptographic key material.
PNs	Abbreviation for Packet Number associated with each MACsec Packet.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is a UDP-based protocol widely deployed for authenticating users by testing user credentials against a remote authentication server.

RNG	Abbreviation for Random Number Generator.
SA	Abbreviation for Secure Association.
SAK	Abbreviation for Secure Association Key.
SCADA	Abbreviation for Supervisory Control and Data Acquisition.
SCI	Abbreviation for Secure Channel Identifier.
SecTag	Abbreviation for Security Tag.
Self-Test	A function that verifies the correct operation of a critical device subsystem and indicates the detection of an out-of-tolerance condition.
Serpent	Serpent is an encryption algorithm.
SLIP	Abbreviation for Serial Line Internet Protocol. SLIP is a communications protocol that provides IP-based communication over serial channels. SLIP is identified in RFC 1055.
SNMP	Abbreviation for Simple Network Management Protocol. SNMP provides a method to poll devices for status information.
SSL/TLS	Abbreviations for Secure Sockets Layer and Transport Layer Security. TLS is the successor to SSL. Both provide cryptographic protection for communication over Ethernet networks. TLS is often used in conjunction with HTTP to provide secure communication over the internet. TLS is identified in RFC 5246.
Stateful Firewall	A firewall that is aware of the state of established connections. A stateful firewall can process traffic more quickly by limiting the number of rules that need to be applied to an existing connection.
Strong Password	A mix of at least eight valid password characters that include a lowercase letter, an uppercase letter, a digit, and other printable characters such as \$.
Subnet Mask	The subnet mask divides the local node IP address into two parts, a network identifier and a node address on that network. A subnet mask is four bytes of information and is expressed in the same format as an IP address. The SEL-3620 uses CIDR notation in place of subnet masks.
Syslog	Syslog is a standard for forwarding log messages in an IP network. The term Syslog is used both to identify the communications protocol and the applications that employ the communications protocol. Syslog is identified by RFC 5424.
TCP	Abbreviation for Transmission Control Protocol. Along with IP, TCP is one of the two original components of the Internet Protocol Suite. This connection-aware protocol resides at Layer 4 of the OSI model and uses error detection, flow control, and congestion control to provide reliable communication. TCP is identified in RFC 793.
Twofish	Twofish is an encryption algorithm.
UDP	Abbreviation for User Datagram Protocol. Like TCP, UDP is a transport protocol that resides at Layer 4 of the OSI model. UDP is a connectionless protocol. UDP is defined in RFC 768.

VLAN	Abbreviation for Virtual Local Area Network. VLANs provide a method to logically segregate network traffic that traverses the same physical network. Various standards describe VLANs including IEEE 802.1Q.
VPN	Abbreviation for virtual private network. A VPN is a cryptographically protected communications channel over a packet-switched network that provides authentication and encryption services. VPNs provide confidentiality, authentication, and integrity of message data.

This page intentionally left blank