MX-ROS V3

User Manual

Version 1.17

October 2026

Table of Contents

Overview 26

Introduction 27

What's in This Document 28

Who This Document Is For 29

Supported Series and Firmware Versions 30

Supported Features List 32

Document Conventions 41

Quick Start 42

Using a Web Browser to Configure the Industrial Secure Router 43

UI Reference 47

UI Reference Overview 48

The MX-ROS User Interface 49

Options Menu 50

Options Menu - User Privileges 50

Change Language 51

Reboot 51

Reset to Defaults 51

Save Custom Default 52

Log Out 53

Device Summary 54

Model Information 54

Panel Status 55

Panel View 56

System Event Summary 57

CPU Usage History (%) 58

Memory Usage History (%) *59*

Setup Wizard **60**

Port Type 60

Interface 61

LAN IP Configuration *61*

WAN IP Configuration *62*

PPTP Dialup *62*

PPPoE Dialup *63*

Service *63*

Confirm *64*

System **65**

System - User Privileges 65

System Management 66

Information Settings *67*

Firmware Upgrade *68*

Software Package Management *72*

Configuration Backup and Restore *74*

Account Management 86

User Accounts *87*

Password Policy *95*

License Management 97

License Management - Overview *97*

License History *104*

Management Interface 104

Out of Band Management *105*

User Interface *106*

Ping Response *109*

Hardware Interface (all products except TN Series) *114*

Hardware Interface (TN Series only) *115*

SNMP *116*

Moxa Remote Connect *124*

MXsecurity *130*

Time 131

System Time *132*

NTP/SNTP Server *141*

Power Management 142

Power Management - General *143*

Power Management - Scheduling *144*

Power Management - Ignition *154*

SMS 156

SMS - General *157*

Remote Control List *160*

Send SMS *162*

GNSS 163

GNSS - General *163*

GNSS Client *164*

GNSS Server *165*

GNSS - Status *166*

Setting Check 167

Setting Check Configuration *167*

Cellular 169

Cellular - User Privileges 169

Cellular - General 169

SIM Settings 171

Reordering SIM Card Priority *171*
Changing the Active SIM Card *171*
SIM Card List *171*
GuaranLink 174
GuaranLink Settings *175*
GuaranLink Recovery Settings *176*
Cellular - Status 178
Cellular Status *178*
Cellular Module Information *180*
Carrier and SIM *180*
Signal Status *181*
Serial 183
Serial - User Privileges 183
Serial Device Server 183
Operation Mode *184*
Serial - Port Settings *196*
Data Packing *198*
Serial - Status *201*
Serial Data Logs *203*
SCATS 203
SCATS - Settings *204*
SCATS - Status *205*
Network Configuration 208
Network Configuration - User Privileges 208
Ports 209
Port Settings *209*
Link Aggregation *213*

Link Fault Passthrough *220*
LAN Bypass Gen3 ..... *222*
PoE *223*
Layer 2 Switching 236
VLAN *236*
MAC Address Table *243*
QoS *245*
Rate Limit *255*
Multicast *257*
Network Interfaces 265
LAN *266*
WAN/WAN1 ..... *271*
WAN2/DMZ *290*
Bridge *301*
MTU Configuration *307*
Secondary IP *308*
Virtual Interface *311*
Redundancy 314
Redundancy - User Privileges 314
Layer 2 Redundancy 315
Spanning Tree *315*
Turbo Ring V2 ..... *319*
Turbo Chain *324*
Layer 3 Redundancy 326
VRRP *326*
WAN Redundancy 337
WAN Redundancy - Settings *337*

WAN Redundancy - Status *341*
High Availability 342
HA Interface *342*
High Availability - Settings *344*
High Availability - Status *346*
Auto Provisioning *347*
Network Service 351
Network Service - User Privileges 351
DHCP Server 351
DHCP Server - General *352*
DHCP *352*
DHCP Server - MAC-based IP Assignment *358*
DHCP Server - Port-based IP Assignment *363*
DHCP Server - Lease Table *368*
DHCP Relay Agent *369*
DHCP Server - Classless Static Route *371*
Dynamic DNS 375
DNS Server 376
DNS Server - Global *376*
DNS Server - Settings *377*
DNS Server - Status *380*
DNS Server - DNS Forwarding *381*
Routing 385
Routing - User Privileges 385
Unicast Route 386
Static Routes *386*
RIP *389*

OSPF *392*

Routing Table *410*

Multicast Route 411

Multicast Route Settings *412*

Static Multicast Route *412*

Multicast Forwarding Table *416*

Broadcast Forwarding 417

Broadcast Forwarding Settings *417*

Broadcast Forwarding List *417*

Directed Forwarding 420

Directed Forwarding Settings *420*

Directed Forwarding Rule List *420*

Tunneling 426

Tunneling - User Privileges 426

VXLAN L2 Tunneling 426

VXLAN Interface List *427*

GRE L3 Tunneling 430

Create GRE Interface Entry *430*

Edit GRE Interface Entry *431*

Delete GRE Interface *432*

NAT 433

NAT - User Privileges 433

NAT Setting 433

NAT Rule List *434*

ALG Settings 454

PN-DCP Forwarding 455

PN-DCP Forwarding Settings *455*

PN-DCP Forwarding List *456*

Translated IP List *458*

Object Management **461**

Object Management - User Privileges 461

Object Member 461

Create Object *462*

Object Member Grouping 478

IP Address Grouping *479*

User-defined Service *482*

Interface Grouping 485

Create Interface Grouping *486*

Edit Interface Grouping *487*

Delete Interface Grouping *488*

Firewall **490**

Network Configuration - User Privileges 490

Layer 2 Policy 491

Add Layer 2 Policy *492*

Edit Layer 2 Policy *495*

Delete Layer 2 Policy *498*

Reorder Layer 2 Policies *498*

Layer 3 Policy 499

Layer 3 Policy Settings *500*

Layer 3 Policy List *500*

Layer 3-7 Policy 512

Layer 3-7 Policy Settings *513*

Layer 3-7 Policy List *514*

Malformed Packets 522

Session Control 523
Create Session Control Policy 524
Edit Session Control Policy 526
Delete Session Control Policy 529
Reorder Session Control Policies 529
DoS Policy 529
DoS Policy - Global 530
Device Policy 532
Soft Lockdown Mode 538
Soft Lockdown Status 539
Soft Lockdown Mode Settings 539
Device Lockdown 541
Device Lockdown - Settings 541
Device Lockdown - Learning Table 543
Advanced Protection 547
Dashboard 547
Configuration 550
Protocol Filter Policy 606
ADP 613
IPS 615
Domain Protection 622
VPN 626
VPN - User Privileges 626
IPSec 626
IPSec - General 627
IPSec Connections 628
IPSec Status 653

OpenVPN Client 654
OpenVPN Client - Settings *654*
OpenVPN Client - Status *655*
L2TP Server 656
Server Setting (WAN) *656*
User Name Settings *657*
Certificate Management 660
Certificate Management - User Privileges 660
Local Certificate 661
Generate Certificate *662*
Delete Certificate *663*
Trusted CA Certificate 663
Generate CA Certificate *664*
Delete CA Certificate *665*
Certificate Signing Request 665
Key Pair Generate *665*
CSR Generate *667*
Security 670
Security - User Privileges 670
Device Security 671
Login Policy *671*
Trusted Access *673*
SSH & SSL *681*
Network Security 682
IEEE 802.1X *683*
Authentication 692
Login Authentication *693*

RADIUS *694*

TACACS+ *695*

LDAP *697*

2-Factor Authentication *704*

RADIUS Server 707

RADIUS Server - General *707*

RADIUS Client List *708*

RADIUS User List *711*

MXview Alert Notification 713

Security Notification Setting *714*

Security Status *715*

Diagnostics 717

Diagnostics - User Privileges 717

System Status 718

Utilization *718*

Fiber Check *720*

Network Status 724

Network Statistics *724*

LLDP Settings *728*

ARP Table *729*

Connection Management *730*

Duplicate IP Detection *734*

Event Logs and Notifications 734

Event Log *735*

Event Notifications *760*

Syslog *778*

SNMP Trap/Inform *780*

Email Settings *786*

SMS Settings *788*

Tools 790

Diagnostic Support *791*

Port Mirroring *800*

Ping *802*

NetFlow *802*

Asset Recognition 807

Asset Recognition - Global Settings *807*

Asset Type and Current Asset Status *808*

Asset Recognition Summary *808*

Industrial Application 810

Industrial Application - User Privileges 810

IEC 61375 Setting 810

Ethernet Train Backbone *811*

Communication Profile *823*

Operational Status *830*

Other Features 839

Firmware Image Recovery Overview 840

Methodology 840

How Dual-imaging Works 841

Soft Lockdown 843

Soft Lockdown Criteria 843

Entering Soft Lockdown Mode 844

When in Soft Lockdown Mode 844

Leaving Soft Lockdown Mode 845

Serial Operation Modes 846

Operation Mode - Real COM 847

Operation Mode - RFC 2217 848
Operation Mode - TCP Server 848
Operation Mode - TCP Client 849
Operation Mode - UDP 849
Device Applications 850
Device Applications Overview 851
Network Segmentation 852
About Network Segmentation 852
Layer-2 Segments 852
Layer-3 Segments 852
VLANs in Depth 852
VLAN Standards and Implementation 853
Benefits of VLANs 853
Scenario: Layer 2 Segmentation of 3 Factories 854
Example: Creating VLANs for Layer 2 Segmentation of 3 Factories 856
Example: Assigning VLANs to Ports on Switch A 856
Example: Assigning VLANs to Ports on Switch B 858
Scenario: Layer 3 Segmentation of Two Services 860
Example: Creating VLANs for Layer 3 Segmentation 862
Example: Assigning VLANs to Ports for Layer 3 Segmentation 863
Example: Assigning IPs to Router Interfaces 865
Example: Configuring Static Routing for Layer 3 Segmentation 866
About Redundancy 869
What kinds of redundancy protocols are there? 869
About Layer 2 Redundancy Protocols 869
About Scenarios for Turbo Chain and Turbo Ring 871
About Turbo Ring v2 872
About Ring Coupling 873

Scenario: Using Turbo Ring in a Manufacturing Plant *874*

Scenario: Using Turbo Ring in an On-board Train Application *878*

About RSTP 882

How RSTP Works *883*

Scenario: RSTP on 4 Network Devices *884*

About Turbo Chain 887

Example: Configuring Turbo Chain *890*

About VRRP 891

Benefits of VRRP *891*

About VRRP States *892*

VRRP in Depth *893*

Scenario: VRRP on Two Routers *894*

Routing 898

About Routing 898

Routing and Packet Delivery *899*

About Static Routing *899*

About Multicast Routing *900*

About Selecting a Routing Protocol *901*

Example: Adding a Static Unicast Route for Factory Automation 902

Example: Adding Static Multicast Route for Passenger Speed Display 904

About OpenVPN Client 907

Scenario: Using a Site-to-Site OpenVPN Tunnel 907

Configuring the Router as an OpenVPN Client *907*

Example: Configuring NAT to Translate over OpenVPN *908*

About NetFlow 911

NetFlow In Depth 911

NetFlow Exporter *911*

NetFlow Collector *911*

NetFlow Analyzer *911*

Scenario: Using NetFlow to Collect LAN Interface Data 912

Example: Configuring the Router as a NetFlow Exporter *914*

About Loopback Interfaces 916

Scenario: Connecting Two Subnets 916

Sample Topology *917*

Setup *917*

Example: Configuring a Loopback Interface for IPSec Tunnel #1 ..... *918*

Example: Configuring NAT to Translate to the Loopback Interface *919*

About NAT 922

NAT in Depth 922

Types of NAT 922

NAT Advantages 923

Scenario: NAT for Renewable Power Generators 923

Example: Configuring 1-to-1 NAT for Device Management *924*

Scenario: Isolated Product Network with Limited Internet Access (NAT N-to-1) 927

Example: Configuring Interfaces for DMZ *929*

Example: Creating Firewall Rules for DMZ *930*

Example: Configuring NAT Rules for DMZ *932*

About L2TP 934

Scenario: Configuring L2TP with IPSec for Corporate VPN 934

Example: Configuring L2TP Server *935*

Example: Configuring IPSec for L2TP Server *935*

About IPSec 937

Remote Access to Control Systems 937

Interconnecting Facilities 937

Regulatory Compliance 937
Sensitive Data Handling 938
Cybersecurity Enhancement 938
Interfacing with IoT Devices 938
Disaster Recovery and Backup 938
Scenario: Using IPSec to Configure Site-to-site VPNs 938
Example: Configuring Field Site Device as a Server for Site-to-site VPN Access 940
Example: Configure Remote Site Device as a Client for Site-to-site VPN Access 940
Railway Applications 942
Overview of IEC 61375 for Rail Applications 943
Ease of Coupling/Decoupling 943
Simplify On-board Device Communication 943
Failover Supports Redundancy 944
Getting to Know IEC 61375 945
About Communication Profiles (IEC 61375-2-3) 945
Train Real-time Data Protocol (TRDP) 946
Train Topology Database (TTDB) 946
ETB Control Service Provider (ECSP) and Client (ECSC) 946
TCN Domain Name System (TCN-DNS) 947
TCN Uniform Resource Identifier (TCN-URI) 947
Safe Data Transmission (SDTv2) 947
IEC 61375-2-3 Terms 947
About Ethernet Train Backbones (IEC 61375-2-5) 948
Ethernet Train Backbone Node (ETBN) 948
Train Topology Discovery Protocol (TTDP) 948
About Ethernet Consist Networks (IEC 61375-3-4) 949

Ethernet Device (ED) *949*

Railway-Network Address Translation (R-NAT) *949*

Scenario: 2 Consists, Each with 2 Redundant ETBNs/ECSPs 950

About Traffic Flows in ETBNs 950

Network Topology *950*

T=0 Getting Camera IP *951*

T=1 DIP/SIP *952*

T=2 R-NAT Translation from Consist 1 ..... *952*

T=3 R-NAT Translation to Consist 2 ..... *953*

Example: Configuring 2 Consists with 2 Redundant ETBN Routers Each 954

Example: Configuring TTDP for ETBN Router 1 on Consist 1 ..... *955*

Example: Configuring TTDP for ETBN Router 2 on Consist 1 ..... *958*

Example: Configuring TTDP for ETBN Router 1 on Consist 2 ..... *960*

Example: Configuring TTDP for ETBN Router 2 on Consist 2 ..... *963*

Checking End-Device IPs 965

Getting ECSP Data with a Network Analyzer 966

Getting ECSP Data with the Web GUI 968

Scenario: 2 Consists, with 1 ETBN/ECSP Each 970

Example: Configuring 2 Consists with 1 ETBN/ECSP Each 970

Example: Configuring TTDP for ETBN Router on Consist 1 ..... *972*

Example: Configuring TTDP for ETBN Router on Consist 2 ..... *974*

Example: Configuring Communication Profiles for ETBNs/ECSPs 977

Security Hardening Guide 979

Security Hardening Guide Overview 980

Security Best Practices 981

Introduction to Defense in Depth 981

Product Security 981

Physical Installation Guidelines *981*

Account Management Guidelines *982*
Protecting Vulnerable Network Ports *983*
Maintaining Communication Integrity 983
Communication Integrity Features *984*
Device Access Control Best Practices 985
Configuring Allowlists in Compliance with IEC 61162-460 ..... *987*
About Device Integrity and Authenticity *988*
Securing USB Interfaces on Network Devices *989*
Device Resource Management and Monitoring 990
Device Resource Monitoring *990*
Event Logs *990*
Denial of Service (DoS) Protection *991*
Session Control *991*
Recommended Settings for Services and Features 992
Common Threats and Countermeasures 993
Recommended Operational Roles and Duties 994
Administrator *994*
Supervisor *995*
Auditor *995*
Recommended Patching and Backup Practices 996
Firmware Upgrade *996*
Configuration Backup *997*
Recommendations for Vulnerability Management 997
Recommendations for Decommissioning 998
Recommendations for Decommissioning *998*
Using Security Features 999
Introduction to IPS 999

What is the difference between IDS and IPS? *999*
IPS Applications 1000
IPS Limitations *1000*
Example: Updating the Network Security Package via the Web GUI 1001
Example: Updating the Network Security Package via MXsecurity 1002
Example: Configuring IPS Rules via MXsecurity 1003
Example: Configuring IPS rules via WebGUI 1004
Introduction to Firewalls 1004
Stateful vs. Stateless firewalls *1005*
Categories of Firewall *1005*
When to Use Firewalls *1006*
Scenario: Airport Integrated Solutions 1006
Sub-Systems in an Airport Network: *1007*
Interoperability and Security *1007*
Moxa's Solution *1007*
Allowlist Firewall Configuration *1007*
Example: Allowing ATMS-ALCMS traffic *1008*
Example: Configuring Blocked Traffic (Air) *1009*
Scenario: Railway Integrated Solutions 1010
Understanding Railway Network Topology *1010*
Allowlist Firewall Configuration *1011*
Example: Allowing TCMS traffic *1012*
Example: Allowing the T2G to access TCMS and PA/PIS *1013*
Example: Configuring Blocked Traffic (Rail) *1015*
Security Standards and Concepts 1017
AAA 1017
About AAA - Authentication, Authorization, and Accounting *1017*

About Authentication Types *1018*

ISA/IEC 62443 Standards and Architecture 1024

Security Reference Standards *1024*

ISA/IEC 62443 Standards and Architecture *1025*

Establishing Foundational Requirements *1027*

FR 1 Applications: User Identification and Authentication *1028*

Product Lifecycle and Security *1030*

Product Security Context 1031

Security Context of an Industrial Secure Router *1031*

Security Context of an Industrial Ethernet Switch *1032*

Appendix 1033

All Settings for Example Scenario: 2 Consists with 1 ETBN/ECSP Each ... 1034

All Settings for Example Scenario: 2 Consists with 2 Redundant ETBN Routers Each 1036

CIP Object List 1038

Destination Ports for Layer 3 – 7 Protocol 1044

Ethernet Protocol Default Ports 1046

EtherTypes for Layer 2 1049

Fiber Check Threshold Values for Auto Mode 1051

Glossary 1054

1-to-1 NAT 1054

Broadcast Forwarding 1054

CoS Mapping 1054

Dead Interval 1054

Double NAT 1054

DSCP Mapping 1055

Hello Interval 1055

Hello Packet 1055

IEC 61735 1055
IKE 1056
Link-State Advertisement Packet (LSA) 1056
MTU (Maximum Transmission Unit) 1056
N-to-1 NAT 1056
NAT Loopback 1056
Network Address Translation (NAT) 1056
Port Address Translation (PAT) 1057
VRRP Binding 1057
IEC 61162-460 Supplementary Declaration 1058
Preface 1058
Explanation 1058
Supplementary Declaration 1058
IEC 61375-2-3 Communication Identifiers 1060
IEC-104 Cause of Transmission List 1063
IEC-104 Type Identification List 1065
Process information in monitor direction 1065
Process telegrams with long time tag (7 octets) 1066
Process information in control direction 1066
Command telegrams with long time tag (7 octets) 1067
System information in monitor direction 1067
System information in control direction 1068
Parameter in control direction 1068
File transfer 1068
LED Behavior 1070
EDF-G1002 Series LED Behavior 1070
EDR-8010 Series LED Behavior 1071

EDR-G9004 Series LED Behavior 1072
EDR-G9010 Series LED Behavior 1074
NAT-102 Series LED Behavior 1075
NAT-108 Series LED Behavior 1076
NAT-G102 Series LED Behavior 1076
OnCell G4302-LTE4 Series LED Behavior 1077
OnCell G4308-LTE4 Series LED Behavior 1079
TN-4900 Series LED Behavior 1081
System LEDs 1081
Port LEDs 1082
NAT-108 Series LED Behavior 1083
MIB Groups 1084
MIB Tree Structure 1084
MMS Command Type List 1100
MMS Service Operation List 1101
PoE Configuration Suggestions 1105
Sample Local Consist Info File 1106
Installation 1107
Physical Installation 1107
Acoount Management 1107
Vulnerable Network Ports 1108
Operation 1108
Maintenance 1111
Decommission 1112
Severity Level List 1113
SMS Remote Control Commands 1114
Status Codes 1115

PoE Status Codes 1115
Classification 1115
Device Type 1115
Configuration Suggestion 1116
Structure and Syntax of Local Consist Info Files 1117
consistinfo 1117
Attributes 1117
Child Elements 1117
functioninfo 1118
Attributes 1118
Child Elements 1118
vehicleinfo 1119
Attributes 1119
Child Elements 1119
System Event List 1121
TRDP Message Type List 1125
Configuration attribute requirements - msgType 1125
Configuration attribute requirements - msgType Profile 1125
TRDP Protocol Filter Profile List 1126
User Role Privileges 1127
Options Menu 1127
System 1127
Cellular 1129
Serial 1129
Network Configuration 1129
Redundancy 1130
Network Service 1130

Routing 1131
Tunneling 1131
NAT 1131
Object Management 1132
Firewall 1132
VPN 1133
Certificate Management 1133
Security 1133
Diagnostics 1134
Industrial Application 1135

Chapter 1

Overview

Introduction

Welcome to the Moxa RouterOS (MX-ROS) manual. This comprehensive guide is designed to help you understand and navigate the UI features, technical concepts, and tasks you may encounter while using your MX-ROS device. The goal is to simplify your experience and make the setup process easier.

What's in This Document

This document includes the following sections:

- **Overview**: This section introduces this document and how to use it.
- **Quick Start**: This section tells you how to connect to your device so you can start using and configuring it.
- **UI Reference**: This section goes through the web user interface (UI) of your device to help you quickly understand what settings are available. This section also shows you the valid ranges and defaults for settings, and any limitations there may be when configuring your device.
- **Other Features**: This section helps you understand features for your device that may not have a related user interface.
- **Device Applications**: This section goes through various applications and helps you understand the related technologies, product features, and best practices so you can better configure the device for your own needs.
- **Security Hardening Guide**: This section gives you an overview of industrial network security and the related product features and best practices needed to help you better secure your application.
- **Appendix**: This section provides additional reference information for your device.

Who This Document Is For

We want you to get the most out of your Moxa device, so we designed this document with these audiences in mind:

- **OT engineers learning how to configure OT network devices**: For frontline personnel operating in OT environments, keeping your MX-ROS configuration up-to-date is crucial. We created the **Security** section to help you better understand how you can use this device effectively for your application.
- **Experienced OT network engineers integrating Moxa devices into OT network infrastructure**: For those who already have a solid understanding of networking concepts, the **UI Reference** section is designed to give you a quick reference for all the device settings, options, default settings, and limitations. You may also find the **Security** section useful for learning how to get more out of your Moxa device and to optimize your application.

Supported Series and Firmware Versions

Note

When updating your device's firmware, we recommend you also update your device to the latest built-in network security package to ensure access to the most recent features and pattern updates.

Moxa Router Series	Firmware Version	Network Security Package Version
EDF-G1002 Series	v3.30	v19.0.12
EDR-8010 Series	v3.30	v19.0.12
EDR-G9004 Series	v3.30	v19.0.12
EDR-G9010 Series	v3.30	v19.0.12
NAT-102 Series **Note** Before upgrading a NAT-102 Series device from v1.x to v3.x, we suggest saving the previous version's configuration first, then redoing the device's configuration after the upgrade to prevent compatibility issues.	v3.30	v19.0.12
NAT-108 Series	v3.30	v19.0.12
NAT-G102 Series	v3.30	v19.0.12
OnCell G4302-LTE4 Series	v3.30	v19.0.12
OnCell G4308-LTE4 Series	v3.30	v19.0.12
TN-4900 Series	v3.30	v19.0.12

The information in this document is applicable to other products and firmwares that use MX-ROS V3, but the appearance and availability of features and settings may vary. The versions listed here may be released after publication of this document. For more

information about which features are supported by each product series, refer to the Supported Features List.

MX-ROS support may expand to other products in the future; please check the Moxa website for the latest information.

Supported Features List

Support for various features varies depending on the product and model. Refer to the table below for an overview of which features are supported by different product series.

Note

Please note that there may still be functional differences between different models within the same product series.

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
Options		YES	YES	YES	YES	YES
	Change Language	YES	YES	YES	YES	YES
	Reboot	YES	YES	YES	YES	YES
	Reset to Defaults	YES	YES	YES	YES	YES
	Save Custom Default	-	-	-	-	YES
	Log Out	YES	YES	YES	YES	YES
Device Summary		YES	YES	YES	YES	YES
Setup Wizard		-	YES	YES	YES	YES
System		YES	YES	YES	YES	YES
	System Management	YES	YES	YES	YES	YES
	Information Settings	YES	YES	YES	YES	YES
	Firmware Upgrade	YES	YES	YES	YES	YES
	Software Package Management	YES	YES	-	YES	YES
	Configuration Backup and Restore	YES	YES	YES	YES	YES
	Account Management	YES	YES	YES	YES	YES
	User Accounts	YES	YES	YES	YES	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
	Password Policy	YES	YES	YES	YES	YES
	License Management	YES	YES	-	YES	YES
	Management Interface	YES	YES	YES	YES	YES
	Out of Band Management	YES	-	-	-	-
	User Interface	YES	YES	YES	YES	YES
	Ping Response	YES	YES	YES	YES	YES
	Hardware Interface	YES	YES	-	YES	YES
	SNMP	YES	YES	YES	YES	YES
	Moxa Remote Connect	-	-	-	YES	YES
	MXsecurity	YES	YES	-	YES	YES
	Time	YES	YES	YES	YES	YES
	System Time	YES	YES	YES	YES	YES
	NTP/SNTP Server	-	YES	YES	YES	YES
	Power Management	-	-	-	YES	-
	SMS	-	-	-	YES	-
	GNSS	-	-	-	YES	-
	Setting Check	YES	YES	YES	YES	YES
Cellular		-	-	-	YES	-
Serial		-	-	-	YES	-
	Serial Device Server	-	-	-	YES	-
	SCATS	-	-	-	YES	-

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
Network Configuration		YES	YES	YES	YES	YES
	Ports	YES	YES	YES	YES	YES
	Port Settings	YES	YES	YES	YES	YES
	Link Aggregation	-	YES	-	-	YES
	Link Fault Passthrough	YES	YES[1]	-	-	-
	LAN Bypass Gen3	YES	YES[1]	-	-	-
	PoE	-	-	-	-	YES
	Layer 2 Switching	-	YES	YES	YES	YES
	VLAN	-	YES	YES	YES[2]	YES
	MAC Address Table	-	YES	YES	YES	YES
	QoS	-	YES	-	-	YES
	Rate Limit	-	YES	-	-	YES
	Multicast	-	YES	-	YES	YES
	IGMP Snooping	-	YES	-	-	YES
	Static Multicast Table	-	YES	-	YES	YES
	Network Interfaces	YES	YES	YES	YES	YES
Redundancy		-	YES	-	-	YES
	Layer 2 Redundancy	-	YES	-	-	YES
	Spanning Tree	-	YES	-	-	YES
	Turbo Ring V2	-	YES	-	-	YES
	Turbo Chain	-	YES	-	-	-
	Layer 3 Redundancy	-	YES	-	YES	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
	VRRP	-	YES	-	YES	YES
	WAN Redundancy	-	YES	-	YES	-
	High Availability	-	YES[3]	-	-	-
Network Service		-	YES	YES	YES	YES
	DHCP Server	-	YES	YES	YES	YES
	Dynamic DNS	-	YES	-	YES	YES
	DNS Server	-	-	-	-	YES
Routing		-	YES	YES	YES	YES
	Unicast Route	-	YES	YES	YES	YES
	Static Routes	-	YES	YES	YES	YES
	RIP	-	YES	-	YES	YES
	OSPF	-	YES	-	YES	YES
	Routing Table	-	YES	YES	YES	YES
	Multicast Route	-	YES	-	YES	YES
	Multicast Route Settings	-	YES	-	YES	YES
	Static Multicast Route	-	YES	-	YES	YES
	Multicast Forwarding Table	-	YES	-	YES	YES
	Broadcast Forwarding	-	YES	-	YES	YES
	Directed Forwarding	-	YES	-	-	YES
Tunneling		-	YES	-	-	YES
	VXLAN L2 Tunneling	-	YES	-	-	-
	GRE L3 Tunneling	-	YES	-	YES[4]	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
NAT		-	YES	YES	YES	YES
	NAT Setting	-	YES	YES	YES	YES
	ALG Settings	-	-	-	-	YES
	PN-DCP Forwarding	-	-	YES	-	-
Object Management		YES	YES	-	YES	YES
Firewall		YES	YES	YES	YES	YES
	Layer 2 Policy	YES	YES	-	YES	YES
	Layer 3 Policy	-	-	YES	-	-
	Layer 3-7 Policy	YES	YES	-	YES	YES
	Malformed Packets	YES	YES	-	YES	YES
	Session Control	YES	YES	-	YES	YES
	DoS Policy	YES	YES	-	YES	YES
	Soft Lockdown Mode	-	-	-	-	YES
	Device Lockdown	-	-	YES	-	-
	Advanced Protection	YES	YES	-	YES	YES
	Dashboard	YES	YES	-	YES	YES
	Configuration	YES	YES	-	YES	YES
	Protocol Filter Policy	YES	YES	-	YES	YES
	ADP	YES	YES	-	YES	-
	IPS	YES	YES	-	-	YES
	Domain Protection	YES	YES	-	YES	-
VPN		-	YES	-	YES	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
	IPSec	-	YES	-	YES	YES
	OpenVPN Client	-	YES	-	YES	YES
	L2TP Server	-	YES	-	-	YES
Certificate Management		YES	YES	YES	YES	YES
	Local Certificate	YES	YES	YES	YES	YES
	Trusted CA Certificate	YES	YES	YES	YES	YES
	Certificate Signing Request	YES	YES	YES	YES	YES
Security		YES	YES	YES	YES	YES
	Device Security	YES	YES	YES	YES	YES
	Login Policy	YES	YES	YES	YES	YES
	Trusted Access	YES	YES	YES	YES	YES
	SSH & SSL	YES	YES	YES	YES	YES
	Network Security	-	YES	-	-	YES
	IEEE 802.1X	-	YES	-	-	YES
	Authentication	YES	YES	YES	YES	YES
	Login Authentication	YES	YES	YES	YES	YES
	RADIUS	YES	YES	YES	YES	YES
	TACACS+	YES	YES	YES	YES	YES
	LDAP	YES	YES	-	-	YES
	2-Factor Authentication	YES	YES	-	-	YES
	RADIUS Server	-	-	-	-	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
	MXview Alert Notification	YES	YES	YES	YES	YES
Diagnostics		YES	YES	YES	YES	YES
	System Status	YES	YES	YES	YES	YES
	Utilization	YES	YES	YES	YES	YES
	Fiber Check	-	YES	-	-	-
	Network Status	YES	YES	YES	YES	YES
	Network Statistics	YES	YES	YES	YES	YES
	LLDP	YES	YES	YES	YES	YES
	ARP Table	YES	YES	YES	YES	YES
	Connection Management	YES	YES	-	YES	YES
	Duplicate IP Detection	-	YES	-	YES	YES
	Event Log and Notifications	YES	YES	YES	YES	YES
	Event Log	YES	YES	YES	YES	YES
	Event Notifications	YES	YES	YES	YES	YES
	Syslog	YES	YES	YES	YES	YES
	SNMP Trap/Inform	YES	YES	YES	YES	YES
	Email Settings	YES	YES	YES	YES	-
	SMS Settings	YES	-	-	YES	-
	Tools	YES	YES	YES	YES	YES
	Diagnostic Support	YES	YES	YES	YES	YES
	Port Mirroring	-	YES	-	-	YES
	Ping	YES	YES	YES	YES	YES

Configuration Section	Function	EDF Series	EDR Series	NAT Series	OnCell Series	TN Series
	Netflow	YES	YES	-	-	YES
	Asset Recognition	YES	YES	-	YES	YES
Industrial Application		-	-	-	-	YES
	IEC 61375	-	-	-	-	YES
	Ethernet Train Backbone	-	-	-	-	YES
	TTDP Settings	-	-	-	-	YES
	Local ETBN Status	-	-	-	-	YES
	ETB Status	-	-	-	-	YES
	TCN Multicast Table	-	-	-	-	YES
	Communication Profile	-	-	-	-	YES
	ECSP Settings	-	-	-	-	YES
	SDTv2 Settings	-	-	-	-	YES
	ECSP Status	-	-	-	-	YES
	SDTv2 Status	-	-	-	-	YES
	Operational Status	-	-	-	-	YES
	Consist Info	-	-	-	-	YES
	Train Directory	-	-	-	-	YES
	Operational Train Directory	-	-	-	-	YES
	TCN-URI Table	-	-	-	-	YES

[1] For EDR Series devices, only the EDR-G9004 Series supports Link Fault Passthrough and LAN Bypass Gen3.

[2] OnCell Series will add support for 802.1ad VLAN in a later version.

[3] For EDR Series devices, only the EDR-8010 Series and EDR-G9010 Series support High Availability.

[4] GRE tunneling for the OnCell Series is currently in **Network Configuration** > **Network Interfaces** > **GRE Interface**.

Document Conventions

This document uses the following formatting conventions:

Convention/Format	Description
Bold	Used for UI elements you see on-screen, including page name, tab name, field labels, drop-down options, menu path, etc.
Italics	Used to highlight important information in a paragraph or a table, such as indicating that a UI setting is only shown under certain conditions.
`Code/commands/CLI`	Used for code snippets, blocks, commands, and CLI output.

Chapter 2

Quick Start

Using a Web Browser to Configure the Industrial Secure Router

The device's web interface provides a convenient way to modify the router's configuration and access the built-in monitoring and network administration functions.

Note

When using the device's web interface, we recommend using the following browsers and versions. Please note that Internet Explorer (IE) is not supported.

- Chrome: 2 most recent versions
- Firefox: Latest version and the Extended Support Release (ESR)
- Edge: 2 most recent major versions
- Safari: 2 most recent major versions
- iOS: 2 most recent major versions
- Android: 2 most recent major versions

Perform the following steps to access the device's web interface:

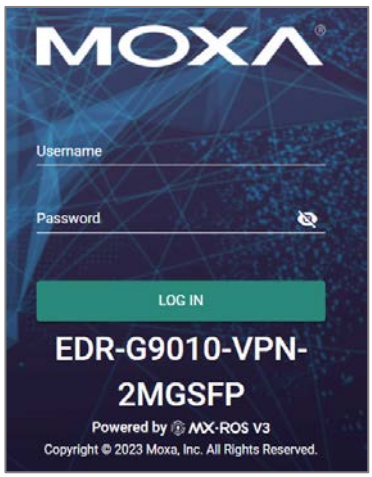
1. Make sure your PC host is connected to your device's LAN port, and is on the same subnet as your device.
2. Open a web browser and type the device's LAN IP address (**192.168.127.254** by default) into the address bar and press Enter.

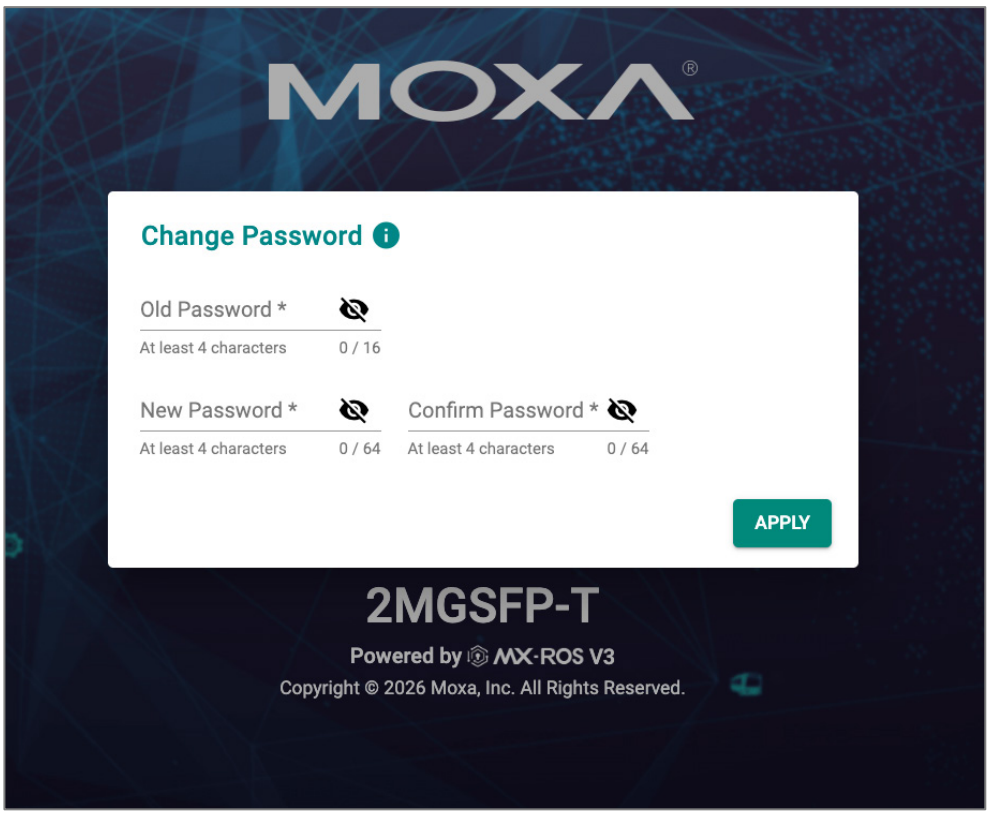
3. The web login page will open. Enter the username (**admin** or **user**) and password (the same as the Console password) and select **LOG IN** to continue.

Note

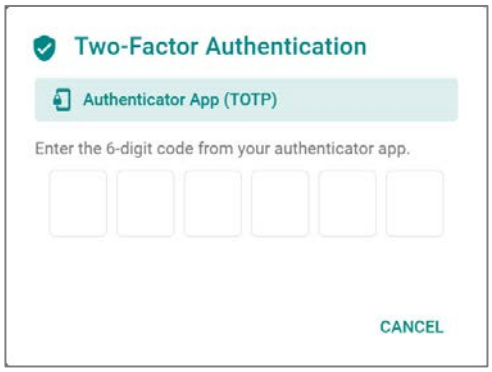
The default username is admin and the default password is moxa.

After logging in with the default credentials, you are required to change the password before proceeding.

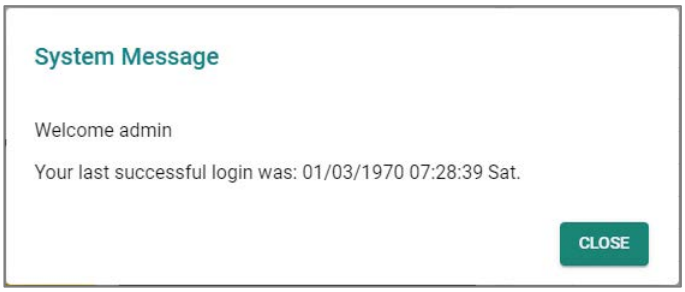




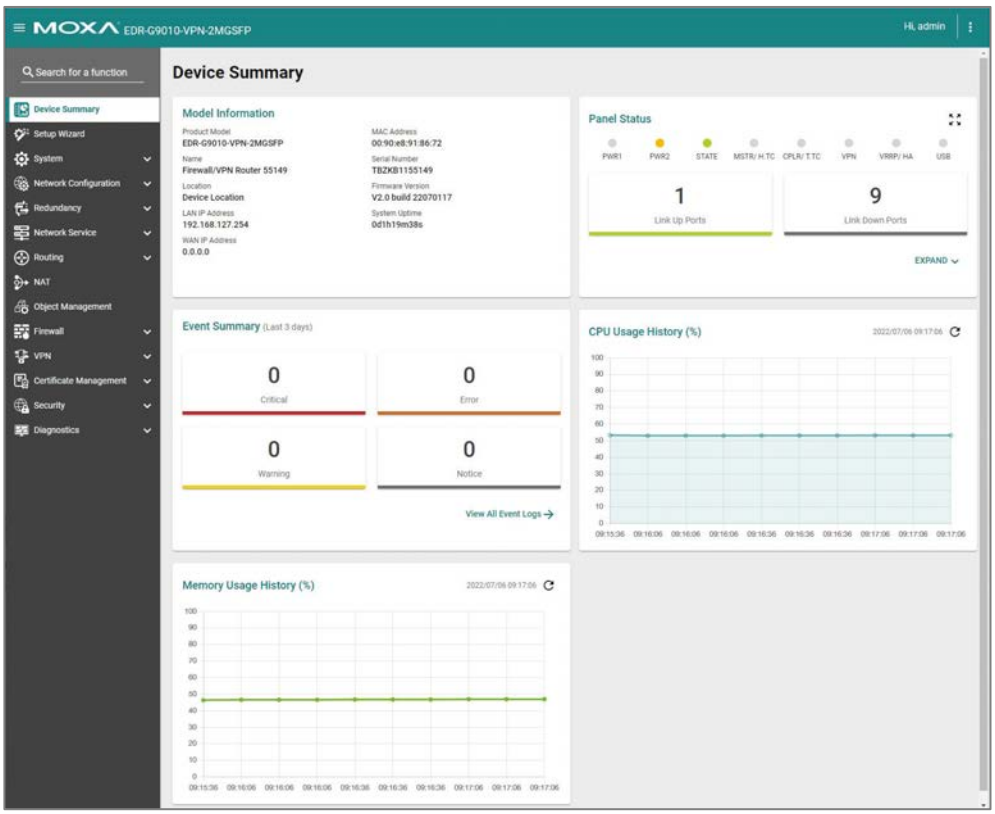
If 2FA is enabled for the account, you will need to enter the authentication code from an authenticator application or from your email, depending on how TOTP is set up for the account. Refer to 2-Factor Authentication and User Accounts for more information.



You may need to wait a few moments for the web interface to appear. If you have logged in before, a system message will appear showing the details of the last successful login. Select **CLOSE** to close this message.



4. After successfully connecting to the router, the **Device Summary** screen will automatically appear. Use the menu tree on the left side of the window to open the function pages to access each of the router's functions.


EDR-G9010-VPN-2MGSFP
Hi, admin
Search for a function
Device Summary
Setup Wizard
System
Network Configuration
Redundancy
Network Service
Routing
NAT
Object Management
Firewall
VPN
Certificate Management
Security
Diagnostics
Device Summary
Model Information
Product Model
EDR-G9010-VPN-2MGSFP
MAC Address
00:90:e8:91:86:72
Name
Firewall/VPN Router 55149
Serial Number
TBZKB1155149
Location
Device Location
Firmware Version
V2.0 build 22070117
LAN IP Address
192.168.127.254
System Uptime
0d1h19m38s
WAN IP Address
0.0.0.0
Panel Status
PWR1
PWR2
STATE
MSTR/ H.TC
CPLR/ T.TC
VPN
VRRP/ HA
USB
1
Link Up Ports
9
Link Down Ports
EXPAND
Event Summary (Last 3 days)
0
Critical
0
Error
0
Warning
0
Notice
View All Event Logs
CPU Usage History (%)
2022/07/06 09:17:06
Memory Usage History (%)
2022/07/06 09:17:06

Chapter 3

UI Reference

UI Reference Overview

This section provides you with a quick reference to the different settings and options of your device.

To help you understand how to use the user interface, the following sections are included:

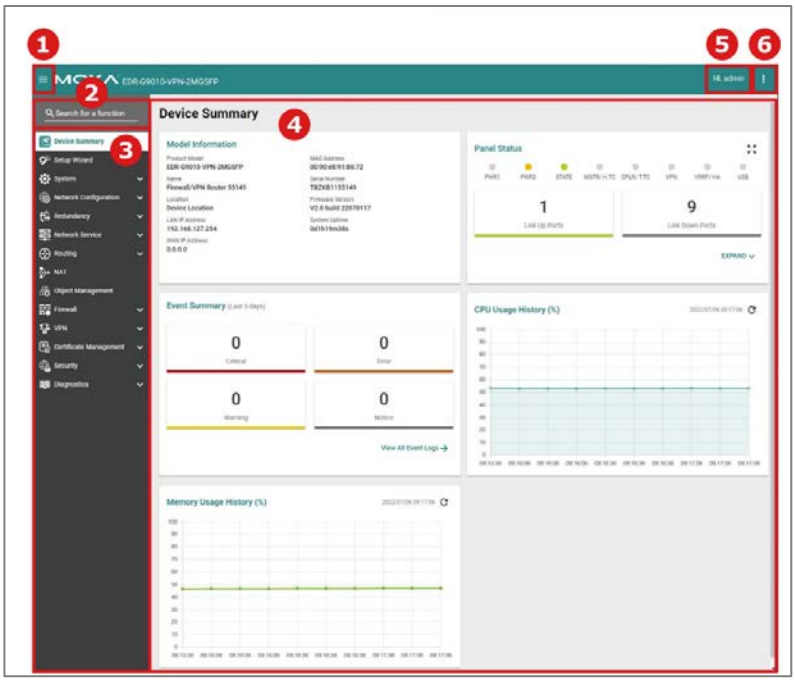
- The MX-ROS User Interface
- Options Menu

The rest of this section follows the order of the menu areas in the user interface:

- Device Summary
- Setup Wizard
- System
- Cellular
- Serial
- Network Configuration
- Redundancy
- Network Service
- Routing
- NAT
- Object Management
- Firewall
- VPN
- Certificate Management
- Security
- Diagnostics
- Industrial Application

The MX-ROS User Interface

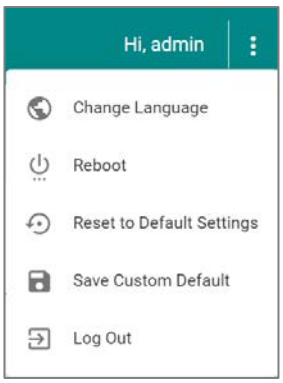
Here is an overview of the MX-ROS user interface.

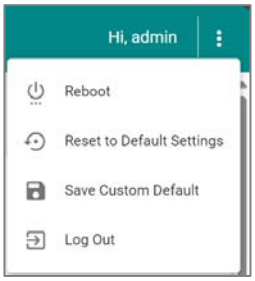


1. Clicking the **Menu (☰)** icon in the top-left will toggle display of the function menu.
2. Enter the name of a function in the **Search Bar** to quickly find a specific function page.
3. Click on a page name in the **Function Menu** on the left-hand side to go to its function page.
4. All the configuration options and information of the selected function page will be shown here.
5. The name of the currently logged-in user is shown here.
6. Clicking the **Options (⋮)** icon in the top-right will expand the Options menu.

Options Menu

Clicking the **Options (▾)** icon in the upper-right corner of the page will open the options menu.





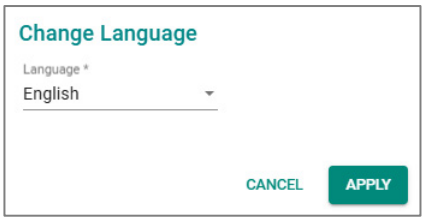
Options Menu - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Change Language	R/W	R/W	R/W
Reboot	R/W	R/W	-
Reset to Defaults	R/W	-	-
Save Custom Default	R/W	-	-
Log Out	R/W	R/W	R/W

Change Language

To change the language of the interface, click the **Options (▾)** icon in the upper-right corner of the page, and select **Change Language**.



Reboot

To manually reboot the device, click the **Options (▾)** icon in the upper-right corner of the page, and select **Reboot**.

Reset to Defaults

To reset the device to its default settings, click the **Options (⋮)** icon in the upper-right corner of the page, and select **Reset to Defaults**.

Select whether to reset to **Factory Default** settings, or the saved **Custom Default** settings, then click **RESET**.

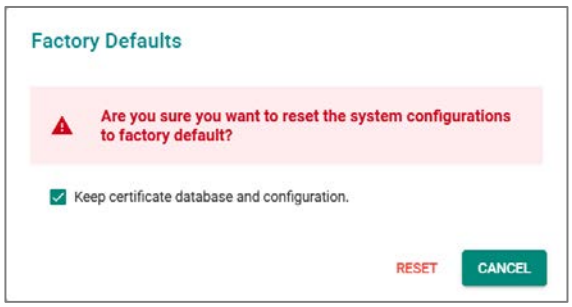
Refer to Save Custom Default for more information about custom default settings.

> **Note**
> Custom Default is only available for the TN-4900 Series.

Warning

When resetting your device to the factory default settings, all your current configuration settings will be permanently deleted.

Check the Keep certificate database and configuration option to keep the certificate database and configuration information. Leaving this option unchecked will delete all information on the device and reset everything to its factory default value.



Save Custom Default

You can save a custom default configuration for your device. This allows you to reset the device to a trusted configuration without uploading a configuration file to restore from.

After saving a custom default, the custom default configuration will become part of the startup configuration and can be backed up and restored with the startup configuration.

Refer to Reset to Default Settings for more information.

Note

Save Custom Default is only available for the TN-4900 Series.

Note

- Ensure that the current startup configuration works as expected and that the user account settings are correct before saving the configuration as a custom default.
- The configuration name can be modified on the Config Backup and Restore page. We recommend using a unique name when backing up a configuration to differentiate it for easy identification and management.
- Each device can only have one set of custom default settings.
- Custom default settings can only save and restore configuration settings. They do not include other uploaded files, such as SSL certificate files, SSH keys, etc.
- Refer to Configuration Types for more information about the different configurations your device uses.

To save the current startup configuration as a custom default, click the **Options ( )** icon in the upper-right corner of the page, and select **Save Custom Default**.

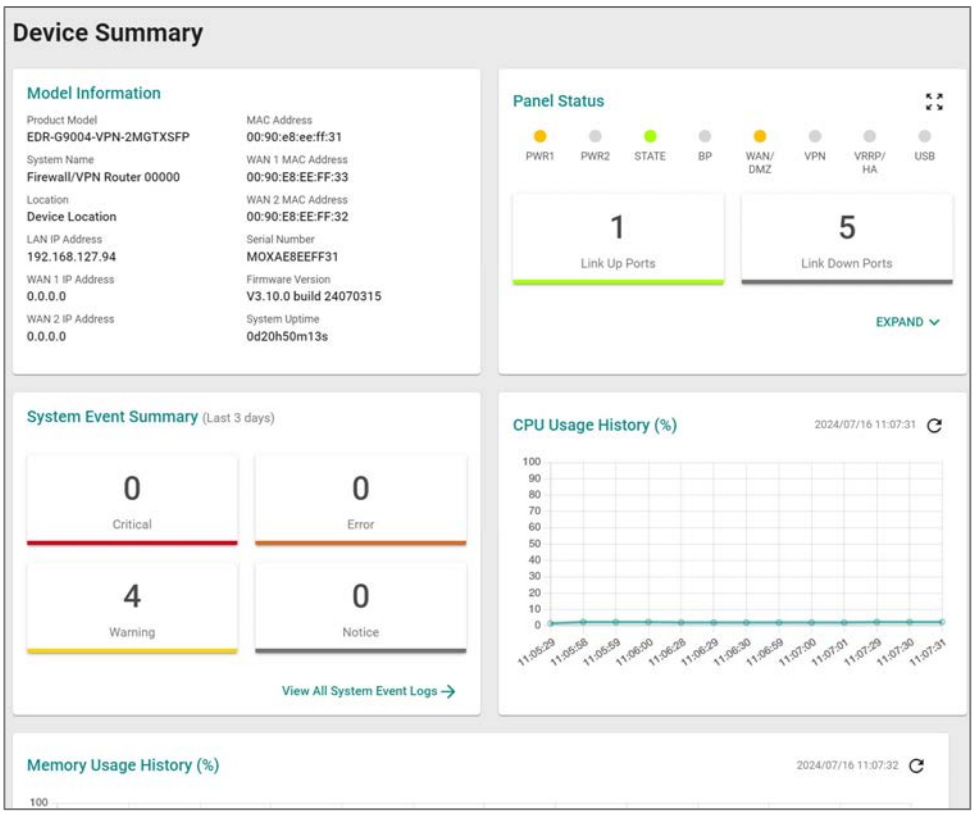
Log Out

To log out of the device, click the **Options ( )** icon in the upper-right corner of the page, and select **Log Out**.

Device Summary

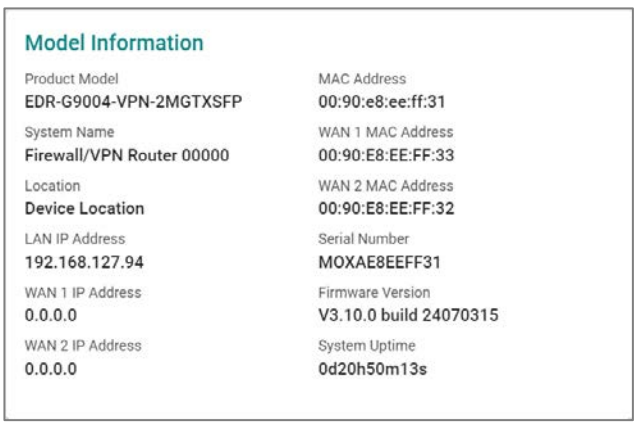
Menu Path: Device Summary

This page lets you see displays with information about your device and current status.



Model Information

This display shows basic information about your device.

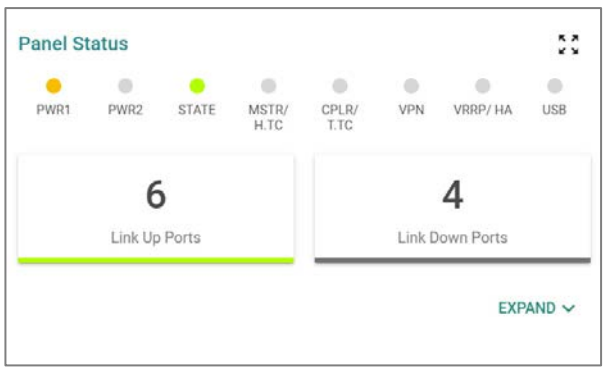


UI Setting	Description
Product Model	Shows the product model of the device.
System Name	Shows the name of the device. Refer to Information Settings for more information.
Location	Shows the location of the device. Refer to Information Settings for more information.
LAN IP Address	Shows the LAN IP address of the device. This can be configured in the Setup Wizard.
WAN IP Address	Shows the WAN IP address of your device. This can be configured in the Setup Wizard.
MAC Address	Shows the MAC address of your device.
Serial Number	Shows the serial number of your device.
Firmware Version	Shows the firmware version of your device.
System Uptime	Shows the amount of time your device has been continuously running for.

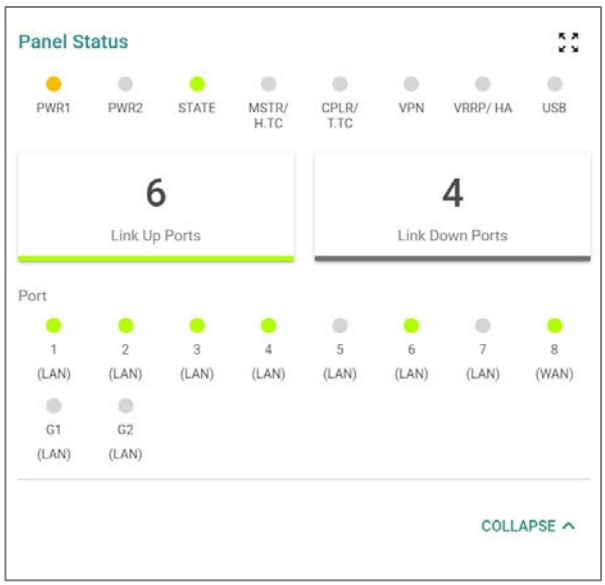
Panel Status

This display shows the status LEDs of your device. For example, connected ports will be shown in green, while disconnected ports will be shown in gray.

Click **EXPAND** to view more detailed information.



Click **COLLAPSE** to hide the details.



Panel View

Clicking the **Expand ( )** icon in the **Panel Status** display will show your device's port status on a representative image of the device. This image will vary depending on your device. Click the **Close ( )** icon in the upper-right corner to close the **Panel View**.

Note

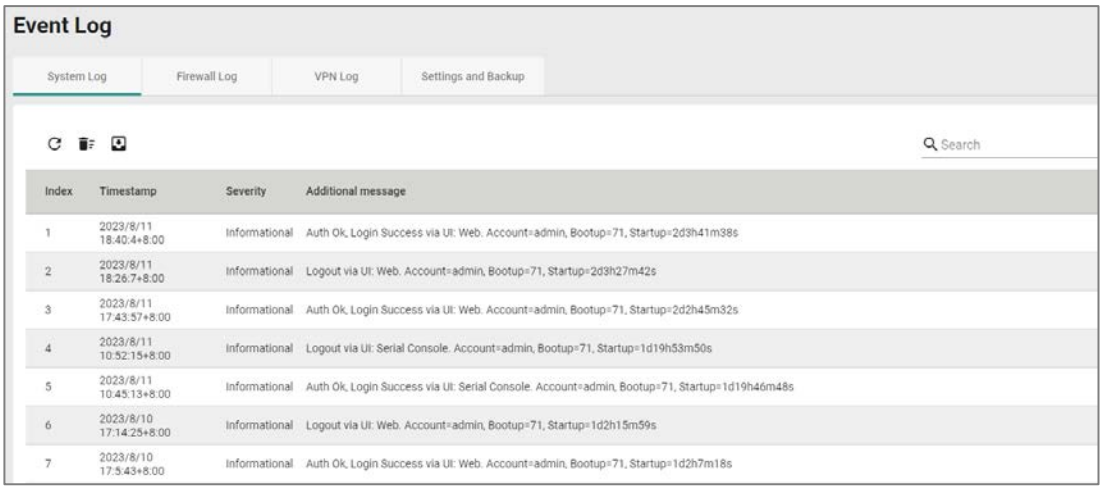
Available LEDs may vary across different versions of devices. For more information about status LEDs and their behavior, refer to LED Behavior.

System Event Summary

This display shows the event summary for the last 3 days or last 24 hours.

The default option is Last 3 days.

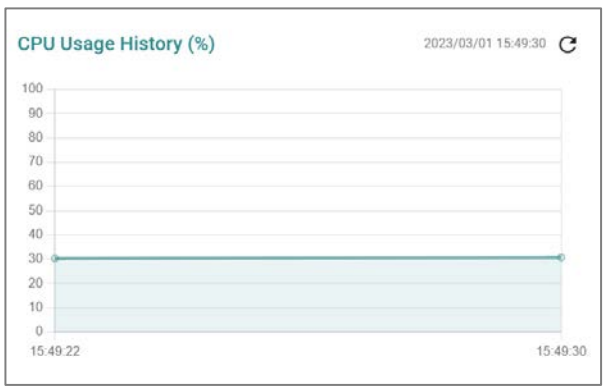
Click **View All System Event Logs** to go to the Event Log page to view event logs in more detail.



Refer to Event Log for more information.

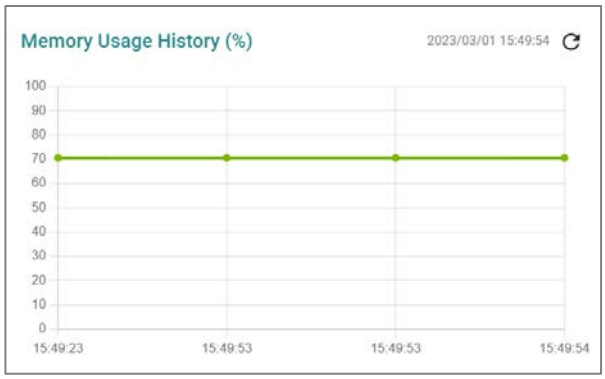
CPU Usage History (%)

This display shows the device's CPU usage. The data will be shown as a percentage over time. Click the **Refresh (↻)** icon to refresh the graph.



Memory Usage History (%)

This display shows the device's memory usage. The data will be shown as a percentage over time. Click the **Refresh (↻)** icon to refresh the graph.



Setup Wizard

Menu Path: Setup Wizard

The Setup Wizard helps guide you through basic setup of your device through four steps:

1. Port Type
2. Interface
3. Service
4. Confirm

> **Note**
> Available settings will vary depending on your product model.

Port Type

In this step, you can set each port of your device to act as a LAN, WAN, or Bridge port.

UI Setting	Description	Valid Range	Default Value
MG1 / MG2	Select whether to use this fiber port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN
1 / 2 / 3 / 4 / 5 / 6 / 7 / 8	Select whether to use this Ethernet port as a LAN, WAN, or Bridge port.	LAN / WAN / Bridge	LAN

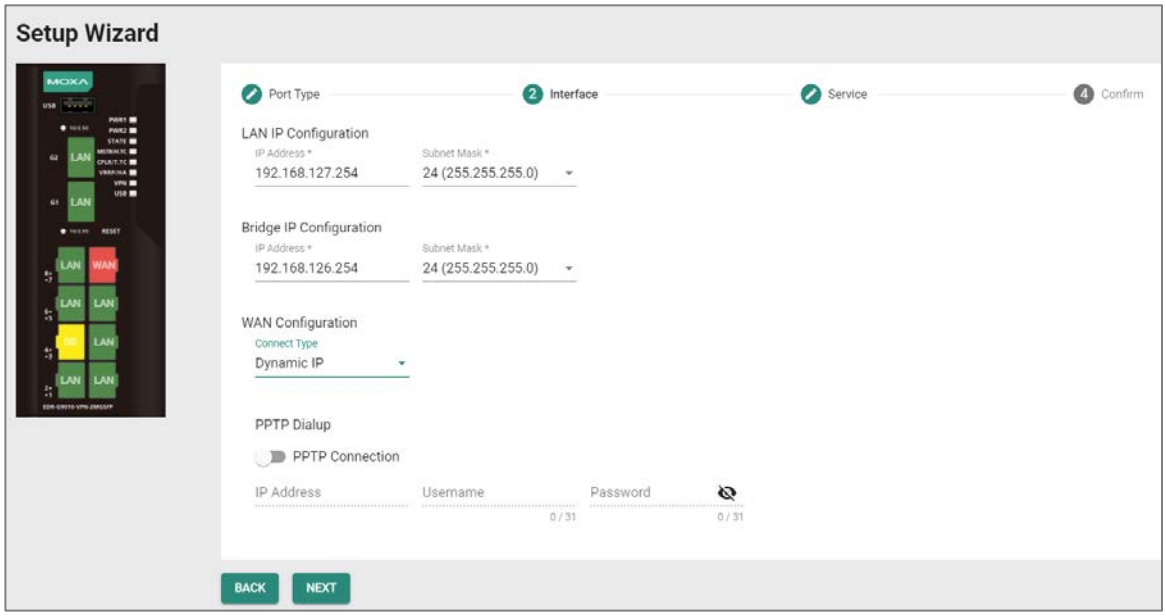
Interface

In this step, you can set up the connection interfaces for your device:

- LAN IP Configuration
- Bridge IP Configuration
- WAN Configuration

Note

Some of these settings may not appear if there are no ports set to LAN, WAN, or Bridge.



LAN IP Configuration

Set the LAN connection details for your device. If you're not familiar with your LAN interface, seek assistance from the network administrator. Network administrators usually determine the LAN interface configuration.

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for your LAN port. **Note** The IP Address should be inputted as unicast IP address.	Valid IP address	192.168.127.245
Subnet Mask	Specify the subnet mask for your LAN port.	Valid subnet mask	255.255.255.0

WAN IP Configuration

Set the WAN connection details for your device. If you're not familiar with your WAN interface, seek assistance from the network administrator. Network administrators usually determine the WAN interface configuration.

UI Setting	Description	Valid Range	Default Value
Connect Type	Select the connection type to use for your WAN port.	Dynamic IP / Static IP / PPPoE	Dynamic IP

If you choose **Static IP** as your **Connection Type**, these settings will also appear:

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for your WAN port.	Valid IP address	N/A
Gateway	Specify the gateway for your WAN port.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for your WAN port.	Valid subnet mask	N/A

PPTP Dialup

Set the PPTP Dialup connection details for your device. This section only appears if **Static IP** or **Dynamic IP** is set for **WAN Configuration > Connect Type**.

Note

Availability of this feature may vary depending on your product model and version.

UI Setting	Description	Valid Range	Default Value
PPTP Connection	Enable or disable using a PPTP connection.	Enabled / Disabled	Disabled
IP Address	Specify the IP address of your PPTP connection.	Valid IP address	N/A
Username	Specify the username for your PPTP connection.	1 to 31 characters	N/A
Password	Specify the password for your PPTP connection.	1 to 31 characters	N/A

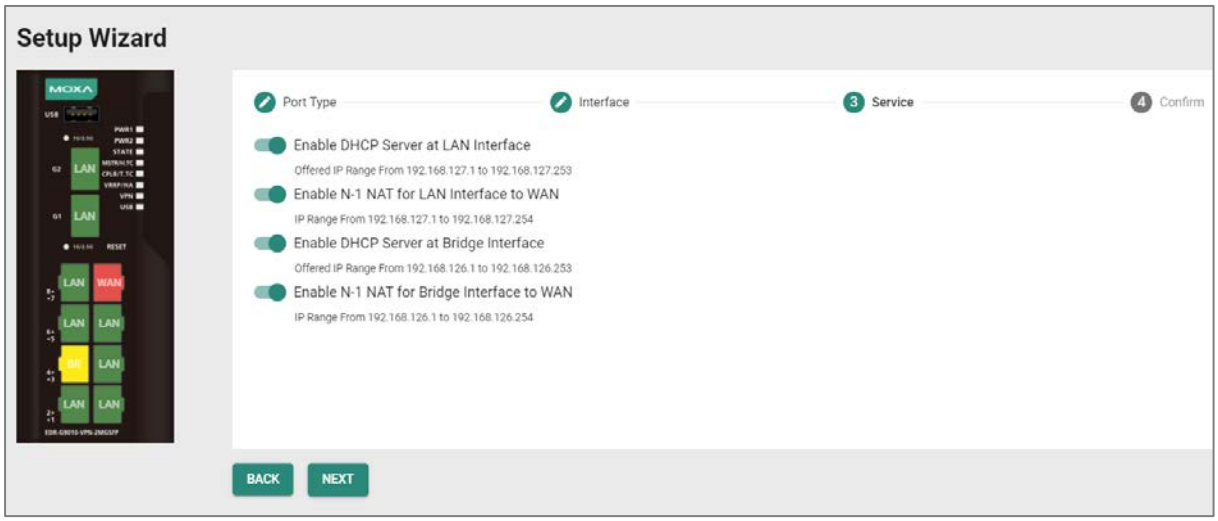
PPPoE Dialup

Set the PPPoE Dialup connection details for your device. This section only appears if **PPPoE** is set for **WAN Configuration > Connect Type**.

UI Setting	Description	Valid Range	Default Value
Username	Specify the username for your PPPoE connection.	1 to 31 characters	N/A
Password	Specify the password for your PPTP connection.	1 to 31 characters	N/A
Host Name	Specify the host name for your PPPoE connection.	1 to 31 characters	N/A

Service

In this step, you can enable or disable services for your device.



UI Setting	Description	Valid Range	Default Value
Enable DHCP Server at LAN Interface	Enable or disable using a DHCP server for the LAN interface.	Enabled / Disabled	Enabled
Enable N-1 NAT for LAN Interface to WAN	Enable or disable using N-1 NAT for LAN interfaces to WAN.	Enabled / Disabled	Enabled
Enable DHCP Server at Bridge Interface **(if Bridge Mode is Port)**	Enable or disable using a DHCP server for bridge interfaces.	Enabled / Disabled	Enabled
Enable N-1 NAT for Bridge Interface to WAN **(if Bridge Mode is Port)**	Enable or disable using N-1 NAT for bridge interfaces to WAN.	Enabled / Disabled	Enabled

Confirm

Confirm your settings, then click **APPLY** to save and apply your changes.

System

Menu Path: System

The System settings area lets you configure the main system settings for your device.

This settings area includes these sections:

- System Management
- Account Management
- License Management
- Management Interface
- Time
- Power Management
- SMS
- GNSS
- Setting Check

System - User Privileges

Privileges to System settings are granted to the different authority levels as follows.
Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Software Package Management	R/W	-	-
Configuration Backup and Restore	R/W	-	-
Account Management			
User Accounts	R/W	-	-

Settings	Admin	Supervisor	User
Password Policy	R/W	-	-
License Management	R/W	R/W	R
Management Interface			
Out of Band Management	R/W	R/W	R
User Interface	R/W	R/W	R
Ping Response	R/W	R/W	R
Hardware Interface	R/W	R/W	R
SNMP	R/W	-	-
Moxa Remote Connect	R/W	-	-
MXsecurity	R/W	R/W	-
Time			
System Time	R/W	R/W	R
NTP/SNTP Server	R/W	R/W	R
Power Management	R/W	R/W	R
SMS	R/W	R/W	R
GNSS	R/W	R/W	R
Setting Check	R/W	R/W	R

System Management

Menu Path: System > System Management

This section lets you manage your device's identification, firmware, and configuration backup settings.

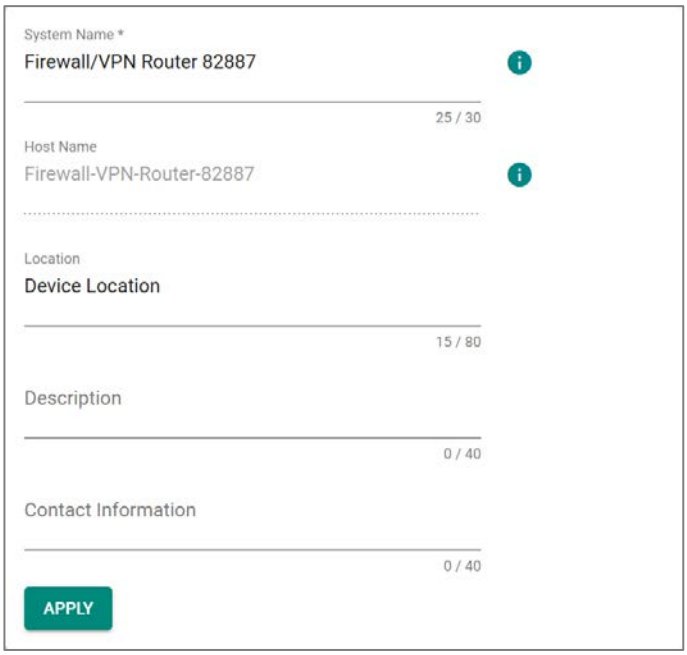
This section includes these pages:

- Information Settings
- Firmware Upgrade
- Software Package Management
- Configuration Backup and Restore

Information Settings

Menu Path: System > System Management > Information Settings

This page lets you add additional information about the device to make it easier to identify on the network.



UI Setting	Description	Valid Range	Default Value
System Name	Enter a name to help identify the device.	1 to 30 characters	Firewall/VPN Router-xxxxx (where xxxxx is the last 5 characters of the device's serial number)

UI Setting	Description	Valid Range	Default Value
Host Name	Shows the host name for the device, which is used with various protocols. This cannot be changed. **Note** The Host Name will automatically update to match the System Name, with the following changes to create a valid host name: • The Host Name will start with the first letter or number in the System Name • The Host Name will end with the last letter or number in the System Name • All spaces and symbols in between the first and last character will be changed to a hyphen - character After changing the System Name, the updated Host Name will appear after the page is refreshed.	**System Name** with spaces and symbols changed	N/A
Location	Enter a location for the device.	1 to 80 characters	Device Location
Description	Enter a description for the device.	1 to 40 characters	N/A
Contact Information	Enter the contact information of the person in charge of the device.	1 to 40 characters	N/A

Firmware Upgrade

Menu Path: System > System Management > Firmware Upgrade

This page lets you upgrade the firmware of your device.

You can upgrade the firmware through the following methods:

- Local
- TFTP
- USB
- SCP
- SFTP

- Moxa service (refer to the MXview One Series User Manual)

Note

As of v3.12, the device will retain all configuration settings when upgrading to newer firmware.

However, as a precaution, we still recommend backing up your configuration before upgrading firmware. Refer to System > System Management > Configuration Backup and Restore for more information.

Note

If it is necessary to verify the integrity and signature of the application when the system is running, the administrator can use the show integrity check CLI command.

The device provides specific CLI commands that allow authenticated users to access the CLI interface through SSH at any time and execute commands to obtain the integrity status of the commands and configurations stored on the device. Therefore, it is recommended that system administrators design scripts or programs to connect to the device via SSH regularly.

Users can integrate these CLI commands into system-level scripts for automation or manually verify whether the internal commands and configurations of the device have been modified without authorization.

Warning

Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will provide you with the necessary assistance.

Before performing a firmware upgrade, make sure you take the following precautions:

- Back up your configuration before upgrading the firmware
- Ensure that the device has power during the entire process
- Ensure that your computer stays connected to the device you are upgrading the firmware on
- Make sure the connection to the firmware source is not interrupted during the upgrade process

Firmware Upgrade - Local

If you select **Local** as your **Method**, these settings will appear. The Local method lets you upload firmware directly from local storage on the host device.

UI Setting	Description	Valid Range	Default Value
Select File	Navigate to and upload the firmware file from the local host device.	N/A	N/A

Firmware Upgrade - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you upload and install firmware stored on a remote TFTP server.

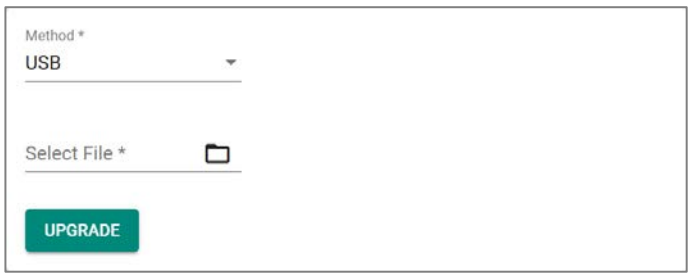
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address	N/A
File Name	Specify the filename of the firmware file.	File name	N/A

Firmware Upgrade - USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to install firmware directly from a USB drive attached to your device.

Note

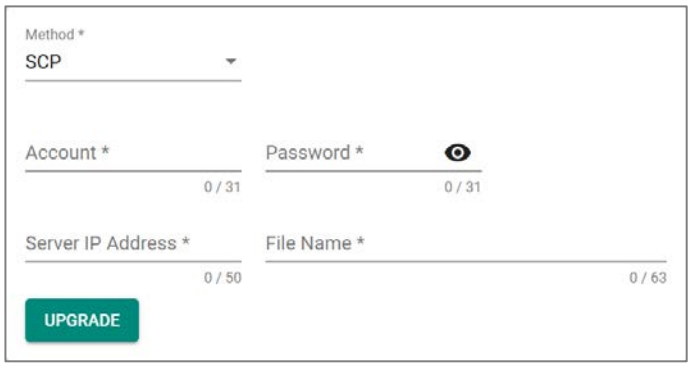
To use this feature, USB Function must be enabled in Hardware Interface.



UI Setting	Description	Valid Range	Default Value
Select File	Select the firmware file on the USB device.	N/A	N/A

Firmware Upgrade - SCP

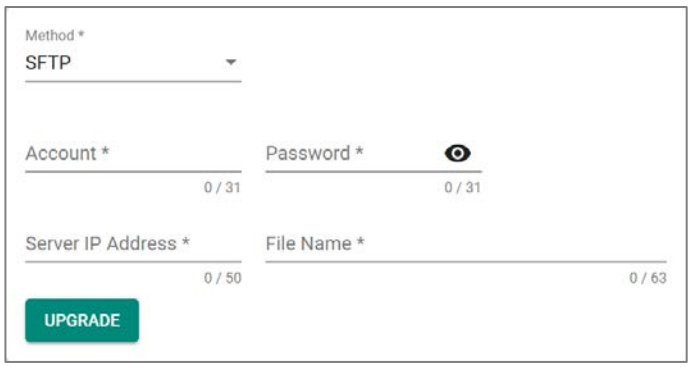
If you select **SCP** as your **Method**, these settings will appear. The SCP (secure copy protocol) method lets you upload and install firmware from a remote system.



UI Setting	Description	Valid Range	Default Value
Account	Enter the remote system account name.	1 to 31 characters	N/A
Password	Enter the remote system account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the remote system.	Valid IP address	N/A
File Name	Specify the filename of the firmware file.	1 to 63 characters	N/A

Firmware Upgrade - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you upload and install firmware stored on a remote SFTP server.



UI Setting	Description	Valid Range	Default Value
Account	Enter the SFTP server account name.	1 to 31 characters	N/A
Password	Enter the SFTP server account password.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server.	Valid IP address	N/A
File Name	Specify the filename of the firmware file.	1 to 63 characters	N/A

Software Package Management

Menu Path: System > System Management > Software Package Management

This page lets you upgrade your Network Security Package and MXsecurity Agent Package, enhancing your device's security capabilities. To upgrade a software package, you can either use the package included with the currently installed firmware, or you can download the latest version from the resource section on the Moxa website at www.moxa.com.

Note

Keeping your software packages updated is critical to keep your device and network secure against the latest cyberattacks.

- **Network Security Package**: Helps you protect your device and network with IPS (Intrusion Prevention System) patterns and a DPI (Deep Packet Inspection) engine.

> **Note**
>
> Products that do not support a firewall will not be compatible with the Network Security Package. Most Moxa routers support firewall functionality, except for products with model names that include '-ETBN-' but do not include '-F-', such as the TN-4908-ETBN-4GTX-4GTXBP-WV-CT-T.

- **MXsecurity Agent Package**: Provides centralized visibility and security management to streamline management of your device. It helps you monitor and identify cyberthreats, and also helps prevent security misconfigurations to create a robust threat defense.

Network Security Package

UI Setting	Description	Valid Range	Default Value
Source	Select a source to use to upgrade the software package. • **Local**: Use a file stored on the local host. • **Firmware**: Use the package included with the current firmware.	Local / Firmware	N/A
Select File (If Source is Local)	Select network secruity package downloaded from Moxa's website. **Note** Moxa will periodically release new security packages on the Moxa official website. Users can download the latest security package and then import it into their device.	N/A	N/A
Package Version **(If Source is Firmware)**	Shows the included package version of the current firmware.	N/A	Current Package Version

MXsecurity Agent Package

UI Setting	Description	Valid Range	Default Value
Source	Select a source to use to upgrade the software package. • **Local**: Use a file stored on the local host. **Note** The Local option is not commonly used in standard environments. However, if you experience issues with your device and MXsecurity, please reach out to Moxa Technical Support. They can utilize the Local option as a troubleshooting interface. • **Firmware**: Use the package included with the current firmware. **Note** Starting from v3.10, the MXsecurity Agent Package will be automatically upgraded when the firmware is upgraded. When upgraded, a "Successfully installed MXSecurity agent package" notification will appear when logging in, and a notification can be found in the **Event Log > System Log**.	Local / Firmware	N/A
Select File (If Source is Local)	This is a troubleshooting interface in case you encounter issues with your device and MXsecurity.	N/A	N/A
Package Version **(If Source is Firmware)**	This shows the included package version of the current firmware.	N/A	Current Package Version

Configuration Backup and Restore

Menu Path: System > System Management > Configuration Backup and Restore

This page helps you back up and restore your device configuration.

This page includes these tabs:

- Backup
- Restore
- File Encryption

> **Note**
>
> For the TN-4900 Series, configuration files from firmware version v1.2 are not compatible with firmware v3.0 and higher due to substantial changes made between v1.2 and v3.0. Please create and import a new configuration file when changing from firmware v1.2 to v3.0 or higher. If you encounter any issues, please contact Moxa technical support.

Backup

Menu Path: System > System Management > Configuration Backup and Restore - Backup

This section lets you create a backup of the current device configuration.

There are multiple methods of backing up the device configuration:

- Local
- TFTP
- USB
- SCP
- SFTP

> **Note**
>
> For security reasons, we strongly recommend that you back up the system configuration to a secure storage location periodically.

Backup - Local

If you select **Local** as your **Method**, these settings will appear.

Select **BACK UP** to back up the device configuration to a file on your local host.

UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local

Backup - TFTP

If you select **TFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **BACK UP** to back up the device configuration to a file on the specified TFTP server.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local
Server IP Address	Specify the IP address of the TFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	N/A	N/A

Backup - USB

If you select **USB** as your **Method,** these settings will appear.

Insert a Moxa ABC-02 configuration tool into the USB port of the device, then select **BACK UP** to back up the device configuration to the ABC-02.

Note

To use this feature, USB Function must be enabled in Hardware Interface.

UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local

Auto Configuration Backup

If you select **USB** as your **Method,** these settings will appear.

Auto configuration backup lets you automatically back up the device configuration to an inserted ABC-02 configuration tool whenever the startup configuration changes.

To enable automatic backup, select **Enabled** from the drop-down list, then click **APPLY.**

Note

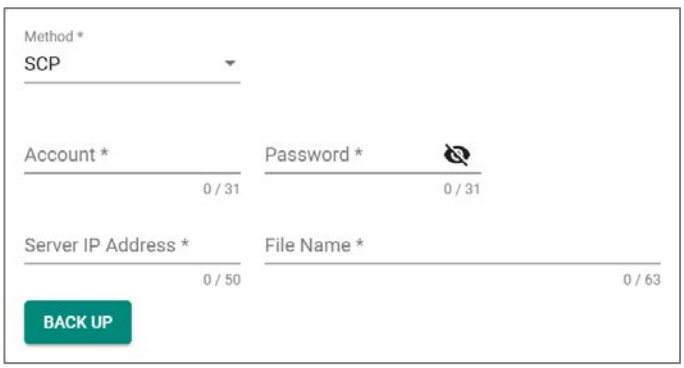
To use this feature, USB Function must be enabled in Hardware Interface.

UI Setting	Description	Valid Range	Default Value
Automatically Back Up	When enabled, this will back up the device configuration to an inserted ABC-02 configuration tool whenever the device configuration changes.	Enabled / Disabled	Enabled

Backup - SCP

If you select **SFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **BACK UP** to back up the device configuration to a file on the specified SCP server.



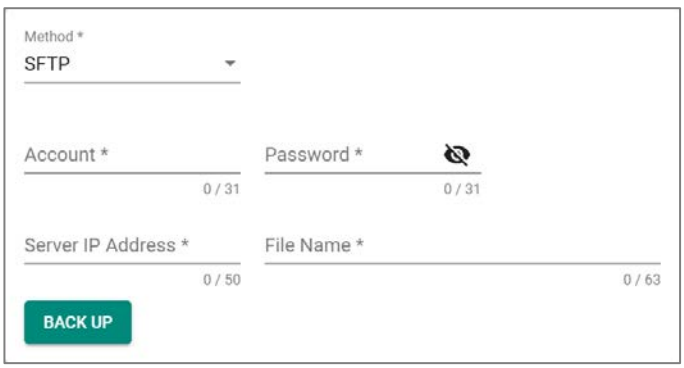
UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local

UI Setting	Description	Valid Range	Default Value
Account	Enter the SCP server account name to use to connect to the SFTP server.	1 to 31 characters	N/A
Password	Enter the SCP server account password to use to connect to the SFTP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SCP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	1 to 63 characters. File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A

Backup - SFTP

If you select **SFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **BACK UP** to back up the device configuration to a file on the specified SFTP server.



UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local

UI Setting	Description	Valid Range	Default Value
Account	Enter the SFTP server account name to use to connect to the SFTP server.	1 to 31 characters	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	1 to 63 characters. File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A

Restore

Menu Path: System > System Management > Configuration Backup and Restore - Restore

This page lets you restore a previously backed up configuration.

Note

To ensure that configuration files can be imported successfully, do not modify the configuration files manually.

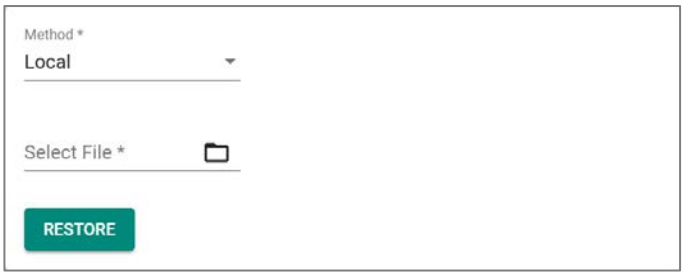
There are multiple methods of restoring the device configuration:

- Local
- TFTP
- USB
- SCP
- SFTP

Restore - Local

If you select **Local** as your **Method**, these settings will appear. The Local method will restore from a configuration file on the local host.

Select a file, then select **RESTORE** to restore the configuration from a local file.



UI Setting	Description	Valid Range	Default Value
Method	Select a method for restoring the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local
Select File	Select the configuration file to use from your computer.	Select a file from your computer	N/A

Restore - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you download and install a configuration stored on a remote TFTP server.

Specify the required settings, then select **RESTORE** to restore the device configuration from the specified file on the TFTP server.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

UI Setting	Description	Valid Range	Default Value
Method	Select a method for restoring the device's configuration.	Local / TFTP / USB / SCP / SFTP	TFTP
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address up to 50 characters	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 63 characters, including file extension. File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

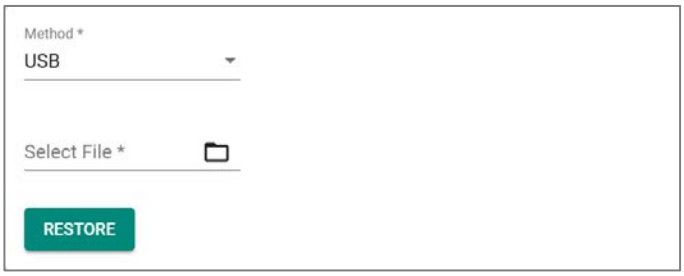
Restore - USB

If you select **USB** as your **Method**, these settings will appear.

Select a file from an ABC-02 configuration tool inserted into the USB port of the device, then select **RESTORE** to restore the device configuration from the file.

Note

To use this feature, USB Function must be enabled in Hardware Interface.



UI Setting	Description	Valid Range	Default Value
Method	Select a method for restoring the device's configuration.	Local / TFTP / USB / SCP / SFTP	Local
Select File	Select the configuration file to use from the ABC-02 device inserted into the USB port.	Select a file from the ABC-02 device	N/A

Auto Configuration Restore

If you select **USB** as your **Method,** these settings will appear.

Auto configuration restore lets you restore the device's configuration from an inserted ABC-02 configuration tool whenever the device is rebooted.

To enable automatic restore, select **Enabled** from the drop-down list, then click **APPLY**.

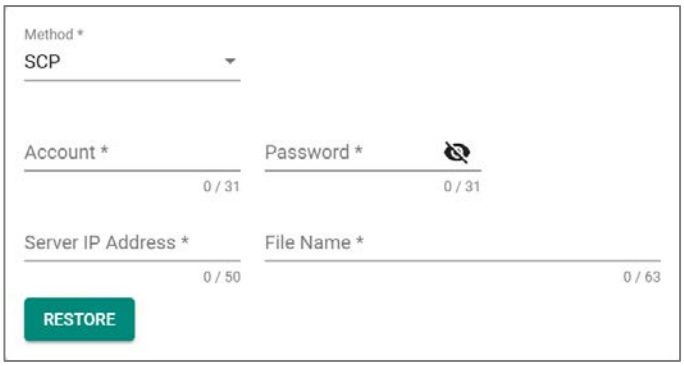
> **Note**
> To use this feature, USB Function must be enabled in Hardware Interface.

UI Setting	Description	Valid Range	Default Value
Automatically Restore	When enabled, this will restore the device's configuration from an inserted ABC-02 configuration tool whenever the device is rebooted.	Enabled / Disabled	Enabled

Restore - SCP

If you select **SCP** as your **Method**, these settings will appear.

Specify the required settings, then select **RESTORE** to restore the device configuration from the specified file on the SCP server.

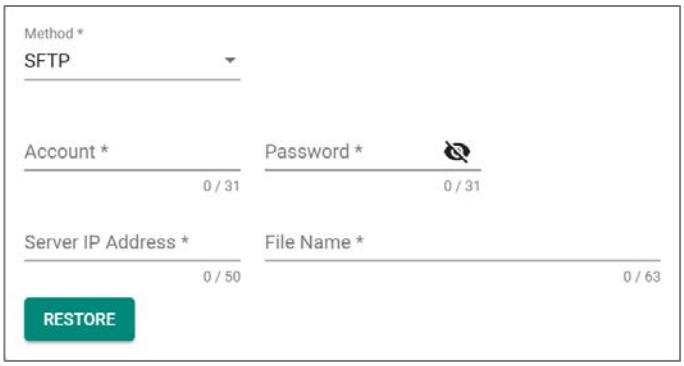


UI Setting	Description	Valid Range	Default Value
Method	Select a method for restoring the device's configuration.	Local / TFTP / USB / SCP / SFTP	TFTP
Account	Enter the account name to use to connect to the SCP server.	1 to 31 characters	N/A
Password	Enter the account password to use to connect to the SCP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SCP server where the configuration file is stored.	Valid IP address up to 50 characters	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 63 characters File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

Restore - SFTP

If you select **SFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **RESTORE** to restore the device configuration from the specified file on the SFTP server.

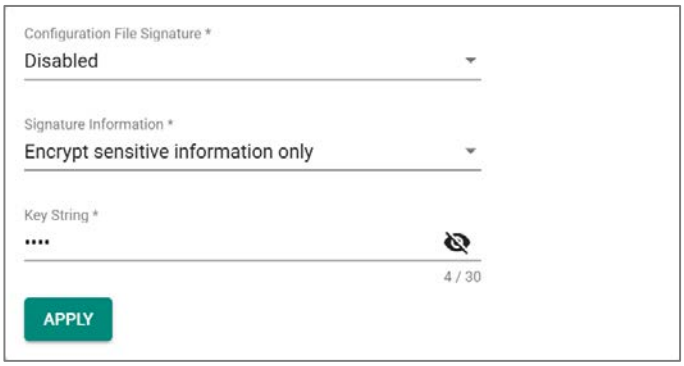


UI Setting	Description	Valid Range	Default Value
Method	Select a method for restoring the device's configuration.	Local / TFTP / USB / SCP / SFTP	TFTP
Account	Enter the account name to use to connect to the SFTP server.	1 to 31 characters	N/A
Password	Enter the account password to use to connect to the SFTP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server where the configuration file is stored.	Valid IP address up to 50 characters	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 63 characters File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

File Encryption

Menu Path: System > System Management > Configuration Backup and Restore - File Encryption

This page lets you configure data encryption settings for exported configuration files.



UI Setting	Description	Valid Range	Default Value
Configuration File Signature	Enables or disables the use of a digital signature for checking the integrity of a configuration file.	Enabled / Disabled	Disabled
Signature Information	Select the type of data to encrypt. **Encrypt sensitive information only:** Only sensitive information will be encrypted in the configuration file. **Encrypt all information:** The entire configuration file will be encrypted. **Note** Sensitive information includes passwords used for authentication and the encryption key used to encrypt data.	Encrypt sensitive information only / Encrypt all information	Encrypt sensitive information only
Key String	Specify an encryption key string. The key string is used to decrypt encrypted configuration files.	1 to 30 characters	moxa

Account Management

Menu Path: System > Account Management

This section lets you manage the user accounts used to access the device.

This section includes these pages:

- User Accounts
- Password Policy

User Accounts

Menu Path: System > Account Management > User Accounts

This page allows you create, manage, modify, and remove user accounts.

Note

1. We strongly recommend changing the default password for the admin account after logging in for the first time.
2. The default admin account cannot be deleted and is enabled by default.
3. Only admin accounts may change the password for supervisor and user accounts.
4. For security reasons, it is recommended for the administrator to keep a record of the account list and associated users.

Warning

Due to the constraints of the IEC 62443-4-2 integrity verification standard, User Accounts will be reset to Factory Default under certain conditions. Specifically, all non-Factory Default user accounts will be entirely removed by the system when the following conditions are all met:

1. The original firmware version of the user device is V.3.0 or higher.
2. The user downgrades the firmware below to V.3.0 and performs any action on this firmware.
3. The firmware version is subsequently upgraded back to V.3.0 or higher.

In cases where all these conditions are satisfied, all user-created non-factory default accounts will be removed.

However, if a user's original firmware version was below V.3.0 and they later upgrade to V.3.0 or subsequent versions, this issue will not arise.

Warning

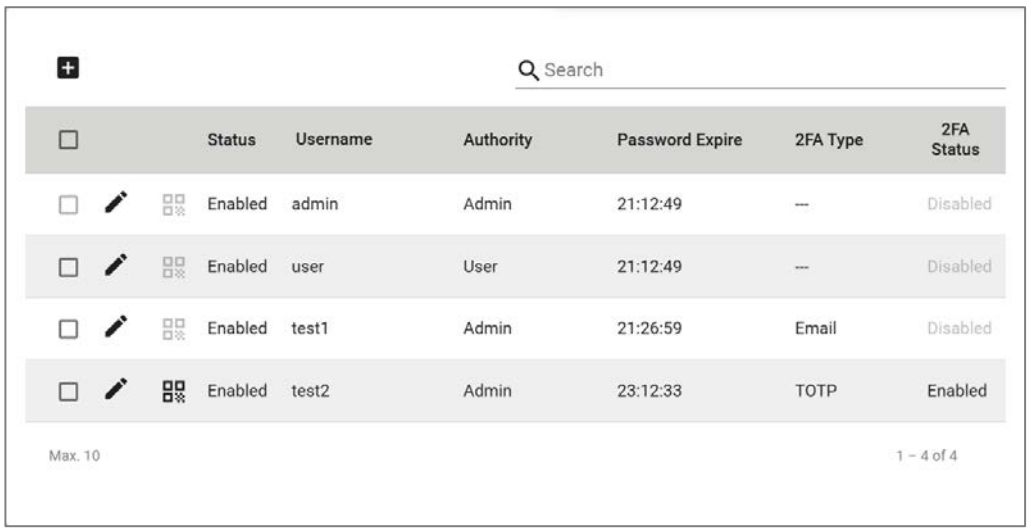
Starting from firmware v3.17:

- Only the admin account is included in the factory default settings. If you need supervisor or user accounts, you will need to create them manually.
- If you upgrade to firmware v3.17 or later without modifying any of the default user account settings, the system will automatically remove supervisor and user accounts. If any changes have been made to user account settings, such as changing the admin password, then all user accounts will be kept when upgrading the firmware.
- In compliance with the EU Radio Equipment Directive (RED), if the device includes wireless functionality, users must change the password upon first login.

Limitations

You can create up to 10 users.

If 2FA is enabled for an account, you can select its **QR code ( )** icon to view its TOTP binding information.

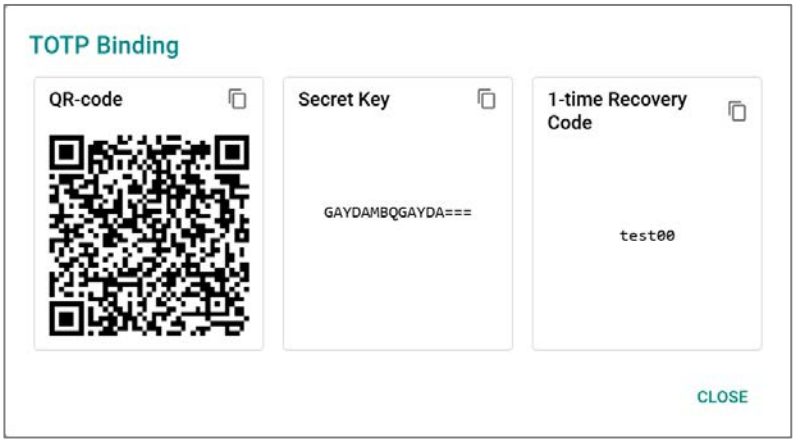


UI Setting	Description
Status	Shows whether the account is enabled or disabled.
Username	Shows the username of the account.
Authority	Shows the authority level of the account.
Password Expire	Shows the number of days left before the password expires for the account. A — means the password will not expire. The password expiration time is determined by the **Password Max-life-time** setting on the **Password Policy** page. Refer to Password Policy for more information.
2FA Type	Shows the 2FA type this account uses.
2FA Status	Shows whether 2FA is enabled or disabled for the account.

TOTP Binding

Selecting the **QR code ( )** icon for an account on the **System > Account Management > User Accounts** page will open this dialog.

Select the **Copy ( )** for an item to copy it to your host's clipboard.



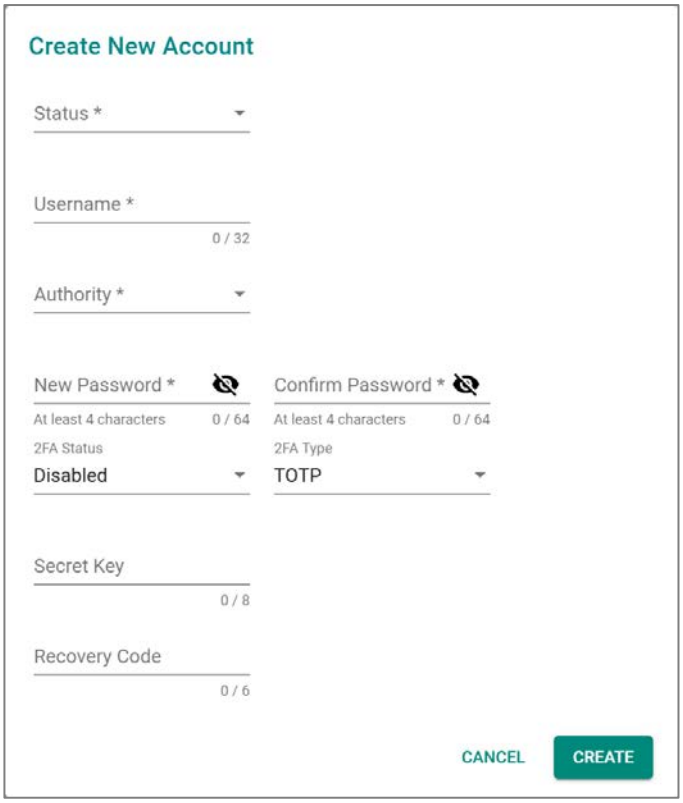
UI Setting	Description
QR-code	Scan this QR code with an authenticator application to add a TOTP entry for the account.
Secret Key	Shows the secret key for the account in Base32 format. Input this key into an authenticator application to add a TOTP entry for the account. Important Select the 2FA algorithm used in your authenticator application to match the algorithm used in 2-Factor Authentication when manually inputting the secret key into your authenticator. Different algorithms generate different 2FA codes, and the secret key does not contain information about which algorithm is used.
1-time Recovery Code	Shows the 1-time recovery code for the account. The recovery code may be used instead of a 2FA code if the 2FA code cannot be generated or retrieved. **Caution** Protect the Recovery Code to prevent unauthorized access. Inputting the Recovery Code bypasses account 2FA requirements. **Important** Re-enable a used **Recovery Code** for an account by editing the account. A 2FA recovery code can only be used once before it is disabled.

Create New Account

Menu Path: System > Account Management > User Accounts

Clicking the **Add (⊕)** icon on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you create a new user account.

Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this user account.	Enabled / Disabled	N/A
Username	Enter a user name for this account.	4 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Authority	Select an authority role for this account. • **Admin**: The account will have read/write access to all configuration parameters. • **Supervisor**: The account will have read/write access to all configuration parameters except create, delete, and modify accounts. • **User**: The account can only view configurations and cannot make any modifications. **Note** Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.	Admin / Supervisor / User	N/A
New Password	Enter a password for this account. **Note** The new password must follow any requirements set on the Password Policy page.	4 to 64 characters, additional requirements are based on settings in **Password Policy**	N/A
Confirm Password	Enter the password again to confirm.	4 to 64 characters	N/A
2FA Status	Enable or disable 2FA for this user account. When enabled, a 2FA code will be required in addition to the username and password to log in to the account.	Enabled / Disabled	Disabled
2FA Type	Select the 2FA method for this account. • **TOTP**: A time-based one-time password generated by an authenticator will be used as the 2FA code. • **Email**: An email with a one-time 2FA code will be sent to the specified email address.	TOTP / Email	TOTP
Secret Key **(If 2FA Type is TOTP)**	Specify the secret key used to generate 2FA codes for the account. **Caution** Use a different Secret Key for each account to protect against potential unauthorized access. Using the same Secret Key for different accounts results in identical codes across accounts.	8 characters	N/A

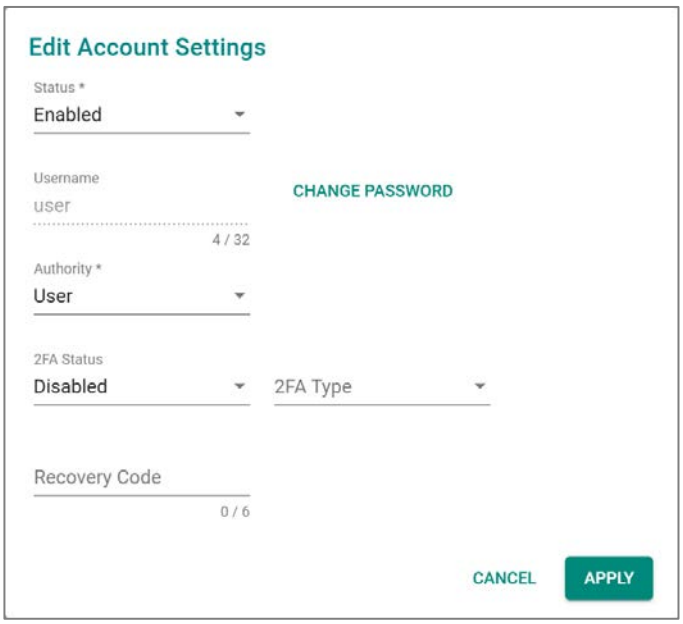
UI Setting	Description	Valid Range	Default Value
Email **(If 2FA Type is Email)**	Specify the email to send 2FA codes to for the account. **Note** To use this feature, your device must be configured to use a mail server. Refer to Email Settings for more information.	Valid email address up to 128 characters	N/A
Recovery Code	Specify a one-time recovery code for the account. The recovery code may be used instead of a 2FA code if the 2FA code cannot be generated or retrieved. **Caution** Protect the Recovery Code to prevent unauthorized access. Inputting the Recovery Code bypasses account 2FA requirements. **Important** Re-enable a used **Recovery Code** for an account by editing the account. A 2FA recovery code can only be used once before it is disabled.	6 characters	N/A

Edit Account Settings

Menu Path: System > Account Management > User Accounts

Clicking the **Edit ( )** icon for an account on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you edit an existing account.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this user account.	Enabled / Disabled	N/A
Username	Shows the username for this account. The username cannot be changed. Select **CHANGE PASSWORD** to change the password for the account.	4 to 32 characters	N/A
Authority	Select an authority role for this account. • **Admin**: The account will have read/write access to all configuration parameters. • **Supervisor**: The account will have read/write access to all configuration parameters except create, delete, and modify accounts. • **User**: The account can only view configurations and cannot make any modifications. **Note** Refer to User Role Privileges for a list of what read/write access privileges are granted for the different authority levels.	Admin / Supervisor / User	N/A
2FA Status	Enable or disable 2FA for this user account. When enabled, a 2FA code will be required in addition to the username and password to log in to the account.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
2FA Type	Select the 2FA method for this account. • **TOTP**: A time-based one-time password generated by an authenticator will be used as the 2FA code. • **Email**: An email with a one-time 2FA code will be sent to the specified email address.	TOTP / Email	TOTP
Secret Key **(If 2FA Type is TOTP)**	Specify the secret key used to generate 2FA codes for the account. **Caution** Use a different Secret Key for each account to protect against potential unauthorized access. Using the same Secret Key for different accounts results in identical codes across accounts.	8 characters	N/A
Email **(If 2FA Type is Email)**	Specify the email to send 2FA codes to for the account. **Note** To use this feature, your device must be configured to use a mail server. Refer to Email Settings for more information.	Valid email address up to 128 characters	N/A
Recovery Code	Specify a one-time recovery code for the account. The reovery code may be used instead of a 2FA code if the 2FA code cannot be generated or retrieved. **Caution** Protect the Recovery Code to prevent unauthorized access. Inputting the Recovery Code bypasses account 2FA requirements. **Important** Re-enable a used **Recovery Code** for an account by editing the account. A 2FA recovery code can only be used once before it is disabled.	6 characters	N/A

Delete User Account

Menu Path: System > Account Management > User Accounts

You can delete user accounts by using the checkboxes to select the accounts you want to delete, then clicking the **Delete ( )** icon.

> **Note**
> The default admin account is enabled by default and cannot be deleted.

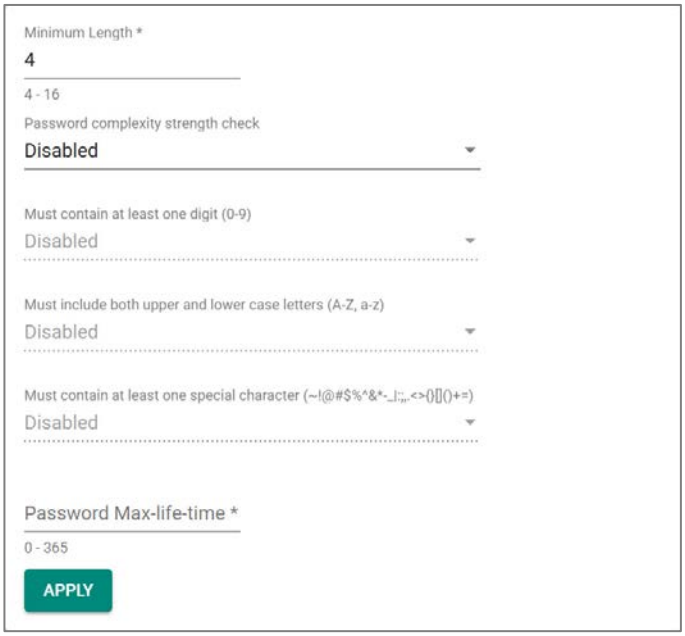
Password Policy

Menu Path: System > Account Management > Password Policy

This page allows you to set password complexity rules for user accounts to improve security.

Click **APPLY** to save your changes.

> **Note**
> To improve the security of your device and network, we recommend that you:
>
> - Set the Minimum Length for passwords to 16.
> - Enable the Password complexity strength check and enable all the requirement options.
> - Set a Password Max-life-time to ensure that users change their password regularly.



UI Setting	Description	Valid Range	Default Value
Minimum Length	Set the minimum required password length.	4 to 16 characters	4
Password complexity strength check	Enable or disable the password complexity strength check.	Enabled / Disabled	Disabled
Must contain at least one digit (0-9) **(If Password complexity strength check is Enabled)**	Enable or disable requiring the password to contain at least one digit.	Enabled / Disabled	Disabled
Must include both upper and lower case letters (A-Z, a-z) **(if Password complexity strength check is Enabled)**	Enable or disable requiring the password to include both uppercase and lowercase letters.	Enabled / Disabled	Disabled
Must contain at least one special character (~!@#$%^&*-|:;,.<>{}[]()) **(If Password complexity strength check is Enabled)**	Enable or disable requiring the password to contain at least one special character.	Enabled / Disabled	Disabled
Password Max-life-time	Specify how long in days passwords will be valid for. When the password expires, the system will require the user to change their password. If this is set to 0, passwords will not expire.	0 to 365	0

License Management

Menu Path: System > License Management

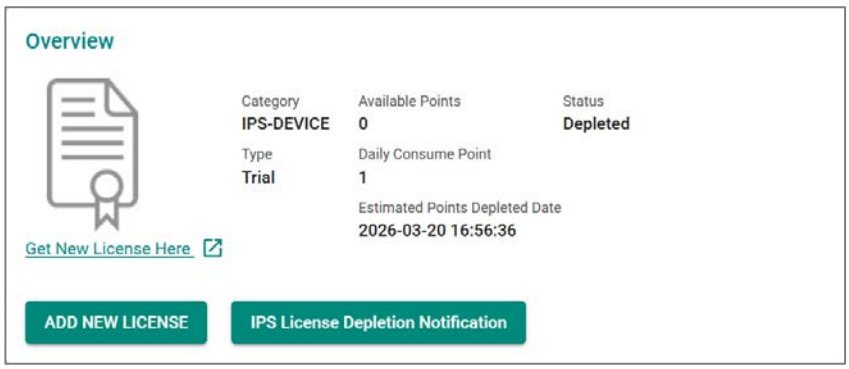
This page lets you add new licenses and view details about existing ones.

This page includes these sections:

- Overview
- License History

License Management - Overview

- Select **ADD NEW LICENSE** to add a new IPS license to your device. Refer to Adding a New License for more details.
- Select **IPS License Depletion Notification** to set up notifications to alert you before the device's IPS license runs out. Refer to Event Notifications - System for more details.



UI Setting	Description
Category	Shows the license category assigned to this device. • **IPS-DEVICE**: License is for standalone IPS use. • **IPS-MGMT**: License is for IPS use managed by MXsecurity or the MXview One Security addon.
Type	Shows the license type (Standard or Trial).
Available Points	Shows the total number of IPS points remaining in the license pool for the device.
Daily Consume Point	Shows the number of license points the device consumes each day when IPS protection is active.

UI Setting	Description
Estimated Points Depleted Date	Shows the projected date and time when available points for the device will reach zero, based on the Daily Consume Point value.
Status	Shows the current status of the license. • **Valid:** The license is valid and the device will receive IPS pattern updates. • **Depleted:** The license is out of available points. The IPS function will continue to work, but will not receive IPS pattern updates.

Adding a New License

Goal

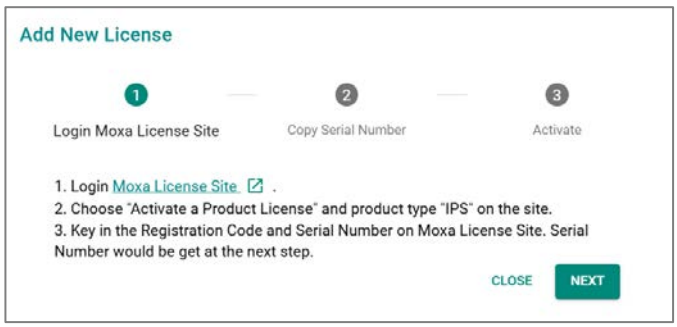
This section provides step-by-step instructions on how to add a new license for your Moxa device.

Prerequisites

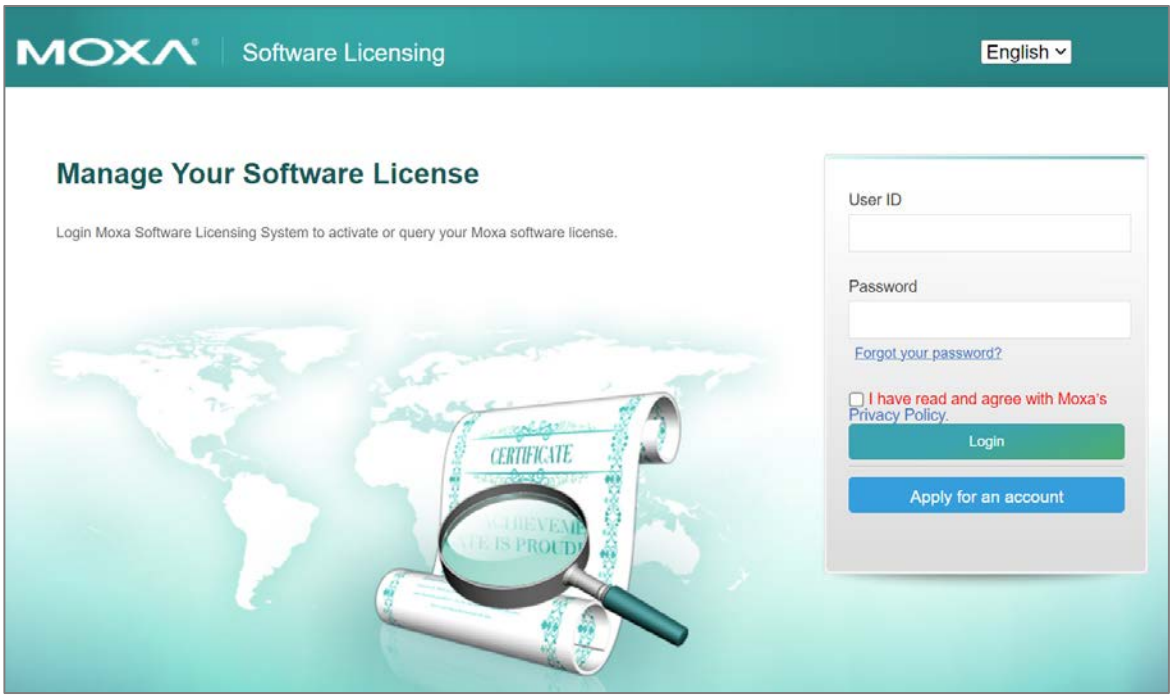
- You need to create an account on the Moxa Software Licensing site (https://netsecuritylicense.moxa.com).
- You need to purchase the license to add from the Moxa Software Licensing site and have the registration code for your license, which is sent to you by email after purchasing the license.

Procedure

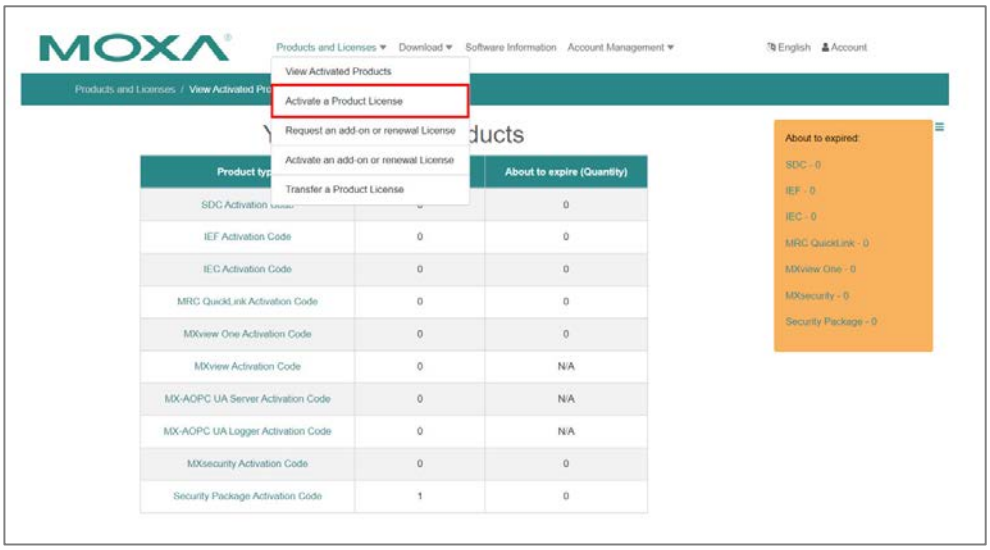
1. Log in to your Moxa device through a web browser.
2. In **System** > **License Management**, select the **Add New License** button. A new page with instructions will appear.



3. Select the **Moxa License Site** link. The Moxa Software Licensing site will open in a new browser window.



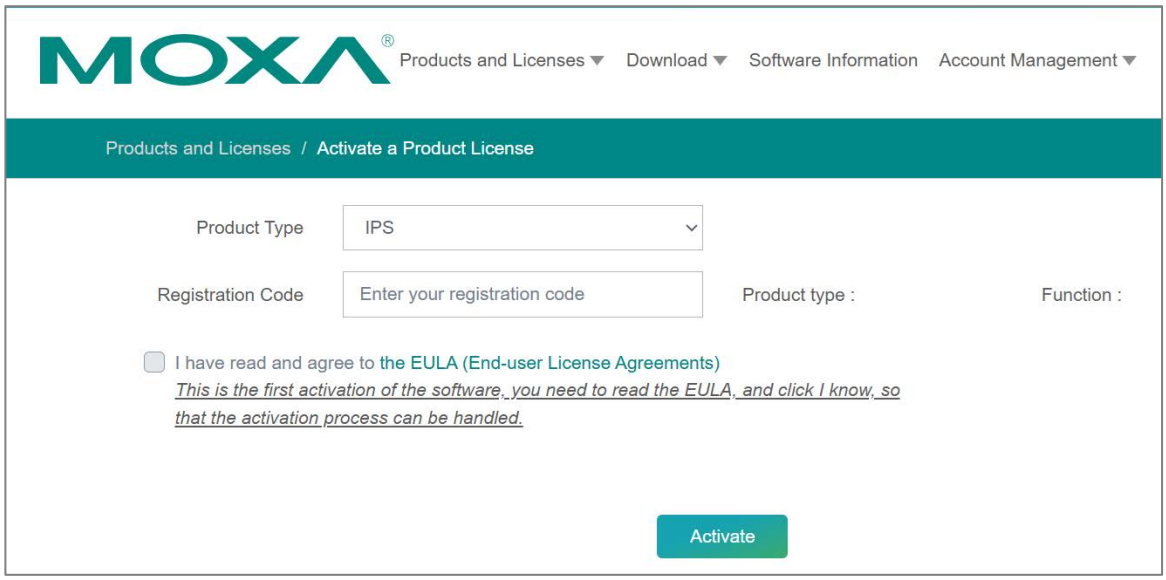
4. In the Moxa Software Licensing window, log in to your account.
5. Select **Products and Licenses** > **Activate a Product License**.



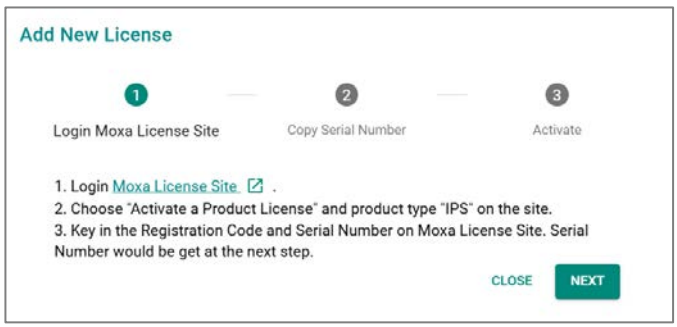
6. Specify the **Product Type** and **Registration Code** of the license.

Note

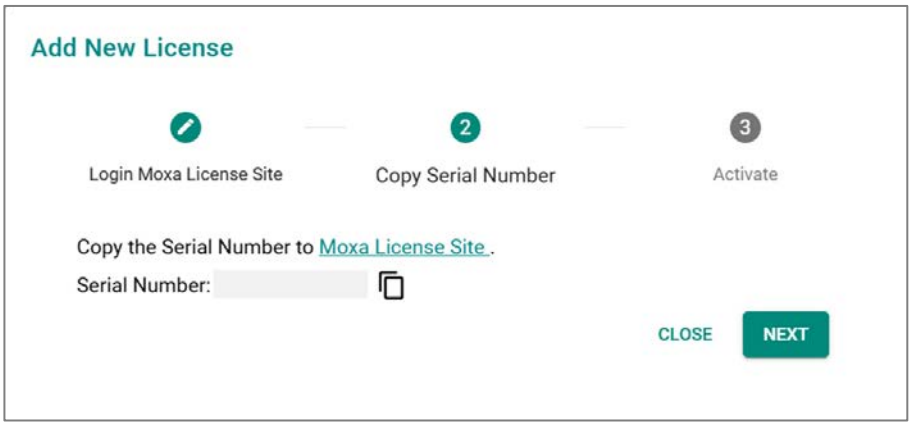
The Registration Code is sent to you in an e-mail after purchasing a license.



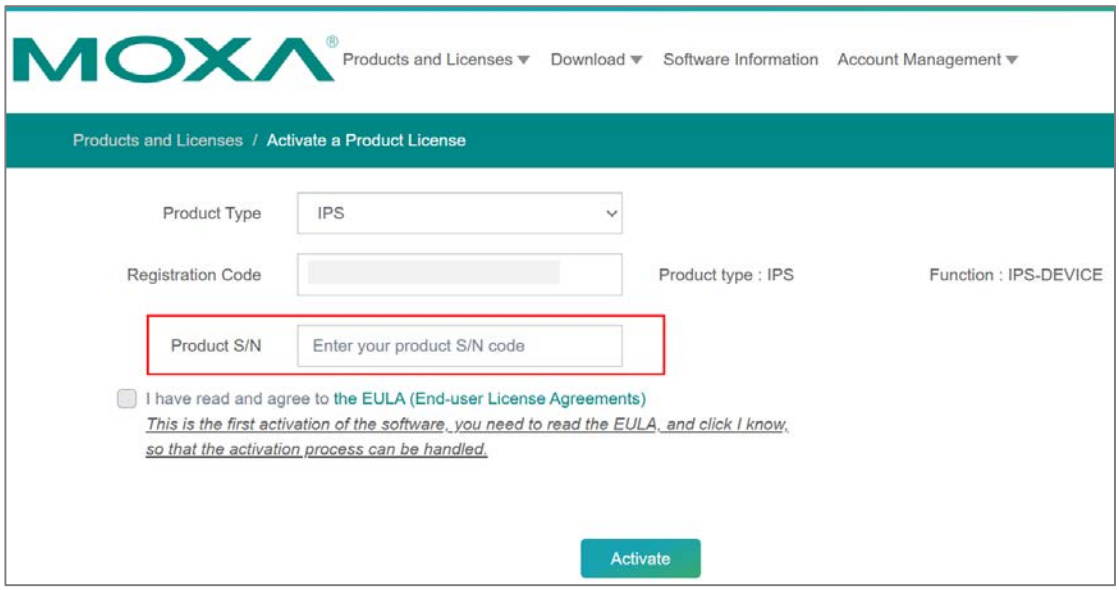
7. In the Moxa device Add New License window, select **NEXT**.



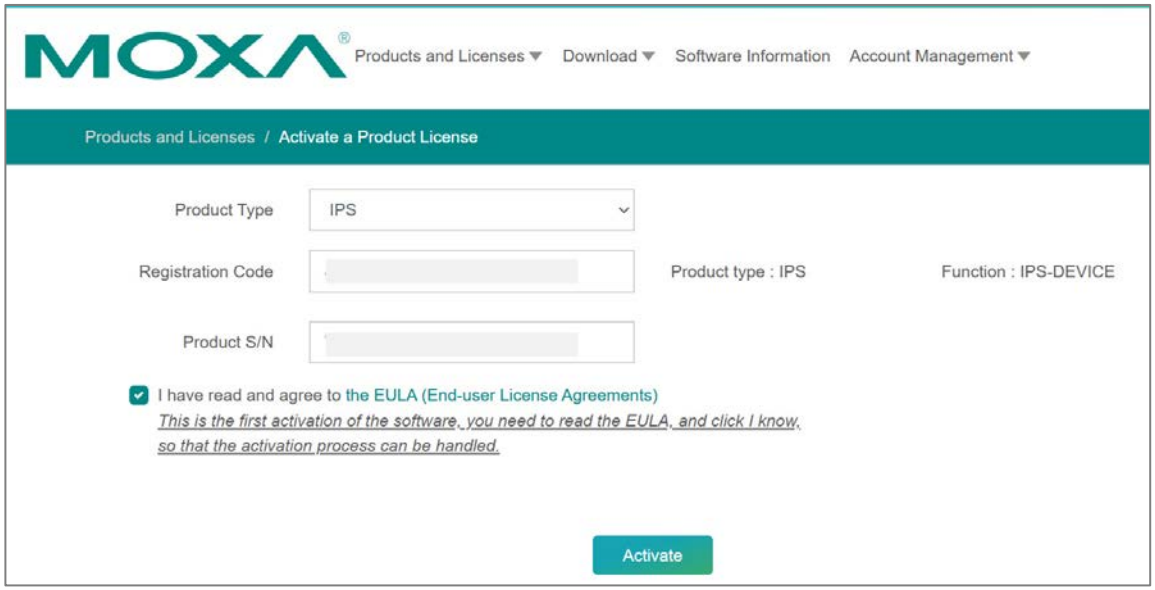
8. Copy the **Serial Number**.



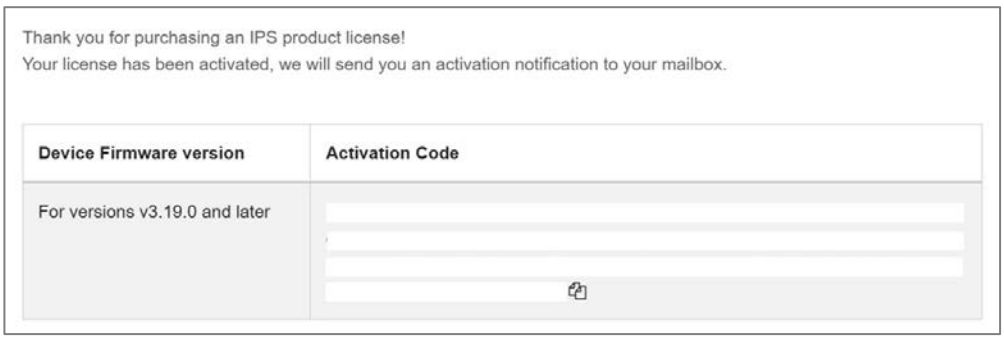
9. In the Moxa Software Licensing window, paste the Serial Number into the **Product S/N** field.



10. Tick the checkbox to indicate you have read and agree to the EULA, then click **Activate**. After activating your license, an activation confirmation page will appear.



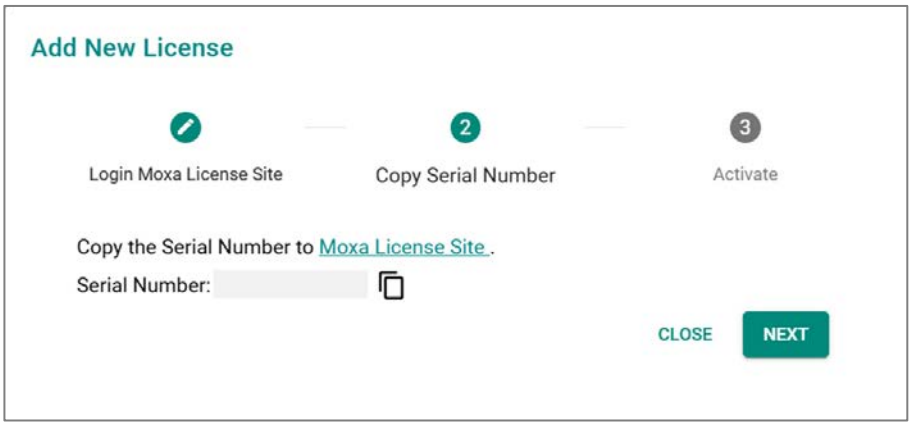
11. Copy the **Activation Code** from the confirmation page.



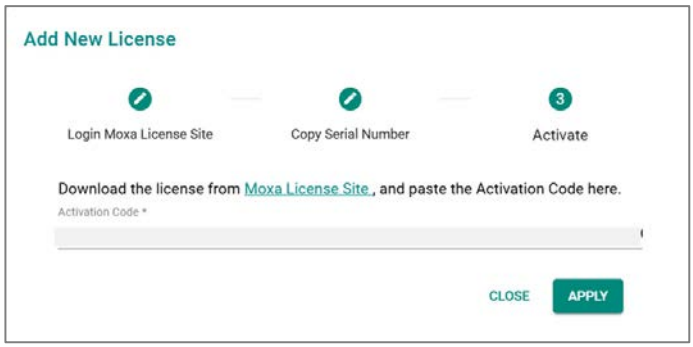
Note

If you forget to copy the activation code, you can retrieve it from the Moxa Software Licensing site in Products and Licenses > View Activated Products.

12. In the Moxa device Add New License window, select **NEXT**.



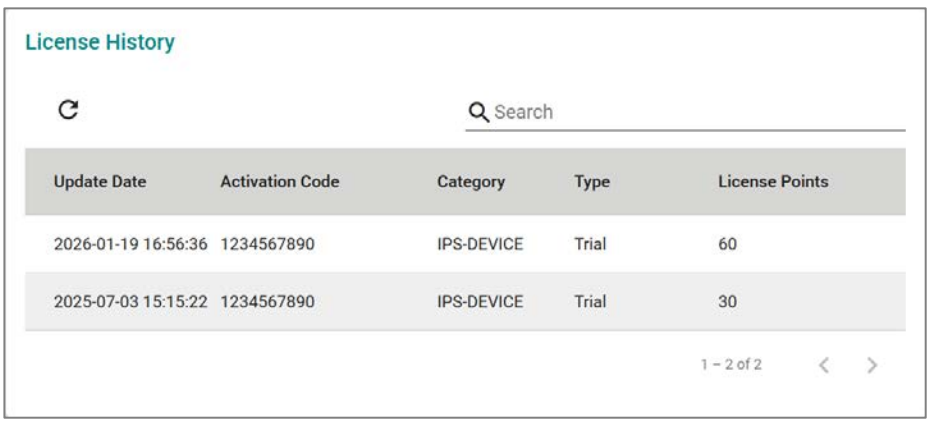
13. Paste in the **Activation Code**.



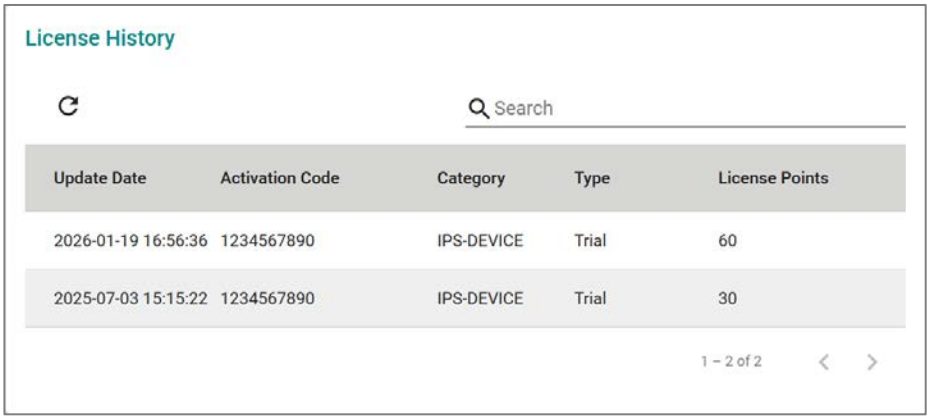
14. Select **APPLY**.

End Result

You will now see the new license in the **License History** section.



License History



UI Setting	Description
Update Date	Shows date of the license update.
Activation Code	Shows the activation code used for the license.
Category	Shows the category of the license. • **IPS-DEVICE**: License is for standalone IPS use. • **IPS-MGMT**: License is for IPS use managed by MXsecurity or the MXview One Security addon.
Type	Shows the license type (Standard or Trial).
License Points	Shows the number of points the license contains.

Management Interface

Menu Path: System > Management Interface

This section lets you configure the interfaces use to manage the device.

This section includes these pages:

- Out of Band Management
- User Interface
- Ping Response
- Hardware Interface

- SNMP
- Moxa Remote Connect
- MXsecurity

Out of Band Management

Menu Path: System > Management Interface > Out of Band Management

This page lets you enable and monitor your device's out of band management port, which segregates traffic from the LAN port to provide a fully isolated and more secure Ethernet connection. This port uses an independent IP address so users can securely connect and configure devices without interfering with operational traffic.

> **Note**
> Availability of this feature may vary depending on your product model and version.

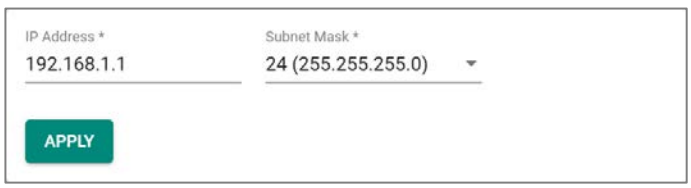
This page includes these tabs:

- Settings
- Status

Out of Band Management - Settings

Menu Path: System > Management Interface > Out of Band Management - Settings

This page lets you configure the settings of your device's out of band management port.



UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address to use for the out of band management port.	Valid IP address	192.168.1.1
Subnet Mask	Specify the subnet mask to use for the out of band management port.	Valid subnet mask	24 (255.255.255.0)

Out of Band Management - Status

Menu Path: System > Management Interface > Out of Band Management - Settings

This page lets you view the status of your device's out of band management port.

UI Setting	Description
Admin Status	Shows whether the out of band management port is enabled or disabled. Refer to Hardware Interface for more information.
Link Status	Shows the link status of the out of band management port.

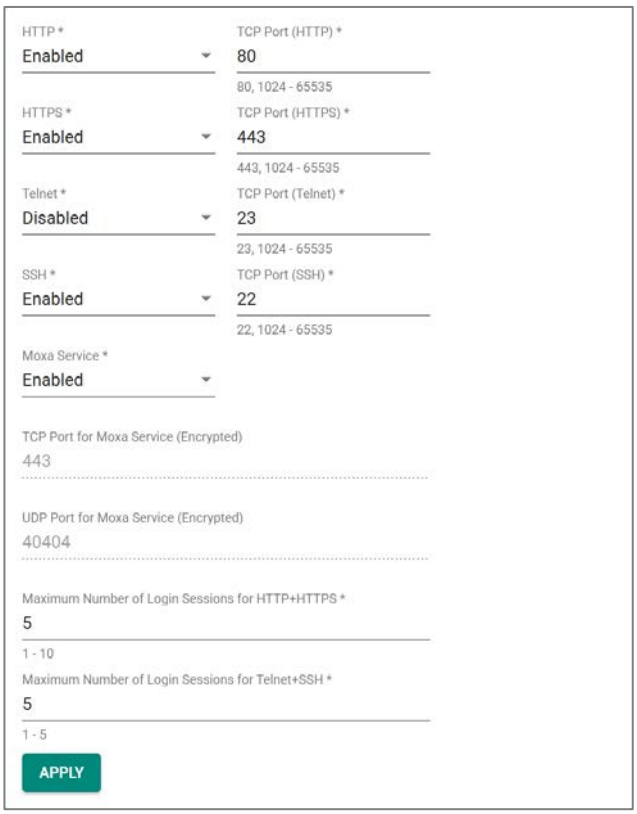
User Interface

Menu Path: System > Management Interface > User Interface

This page lets you configure which interfaces can be used to access the device.

Note

For security reasons, users should access the device using the secure HTTPS and SSH interfaces.



UI Setting	Description	Valid Range	Default Value
HTTP	Enable or disable HTTP connections.	Enabled / Disabled	Enabled
TCP Port (HTTP)	Set the TCP port number for HTTP.	80, 1024 to 65535	80

UI Setting	Description	Valid Range	Default Value
HTTPS	Enable or disable HTTPS connections. **Note** The administrator can manually import a self-signed certificate (in .p12 format) for web server (HTTPS) services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When the browser verifies the signature and accesses the device, it will return the subject name which the administrator can use to confirm the connected device is authorized. **Note** The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations. The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.	Enabled / Disabled	Enabled
TCP Port (HTTPS)	Set the TCP port number for HTTPS.	443, 1024 to 65535	443
Telnet	Enable or disable HTTPS connections.	Enabled / Disabled	Disabled
TCP Port (Telnet)	Set the TCP port number for Telnet.	23, 1024 to 65535	23
SSH	Enable or disable HTTPS connections.	Enabled / Disabled	Enabled
TCP Port (SSH)	Set the TCP port number for SSH.	22, 1024 to 65535	22

UI Setting	Description	Valid Range	Default Value
MOXA Service	Enable or disable the MOXA Service. **Note** Moxa Service is only used for Moxa network management software, and is only available for user accounts with admin privileges.	Enabled / Disabled	Enabled
TCP Port for Moxa Service (Encrypted)	The TCP port number for Moxa Service. This setting cannot be changed.	443	443
UDP Port for Moxa Service (Encrypted)	The UDP port number for Moxa Service. This setting cannot be changed.	40404	40404
Maximum Number of Login Sessions for HTTP+HTTTPS	Set the maximum combined number of users that can be logged in to the Moxa Router using HTTP and HTTPS.	1 to 10	5
Maximum Number of Login Sessions for Telnet+SSH	Set the maximum combined number of users that can be logged in to the Moxa Router using Telnet and SSH.	1 to 5	5

Ping Response

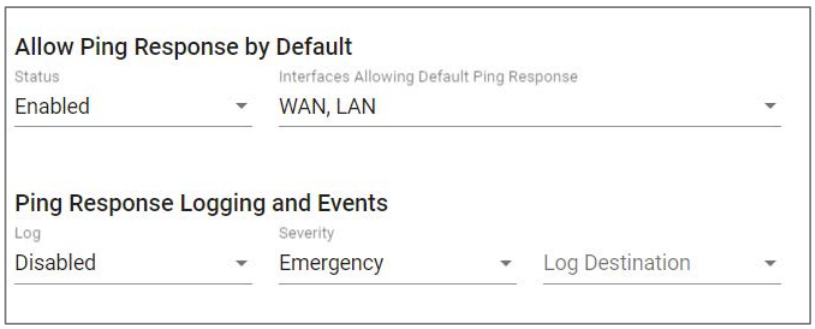
Menu Path: System > Management Interface > Ping Response

This page allows you to configure and manage ping response policies that let you control how your device handles incoming ping requests.

Limitations

You can create up to 16 ping response policies.

Ping Response Settings



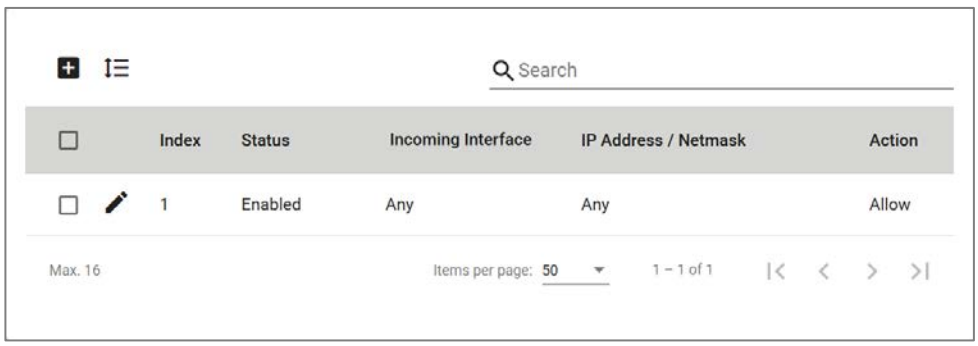
Allow Ping Response by Default

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable allowing ping responses to ping requests through the specified interfaces by default. **Note** If Status is set to Disabled, ping responses will be denied for all ping requests by default. **Note** Ping response policies will override the default behavior.	Enabled / Disabled	Disabled
Interfaces Allowing Default Ping Response	Select the interfaces to allow ping responses for by default.	Drop-down list of interfaces	Existing interfaces

Ping Response Default Rule Event Setting

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable global policy event logging. This will allow event logging for actions taken due to the global policy.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Select the default action log destination.	Syslog / Trap / Local Storage	N/A

Ping Response Policy List



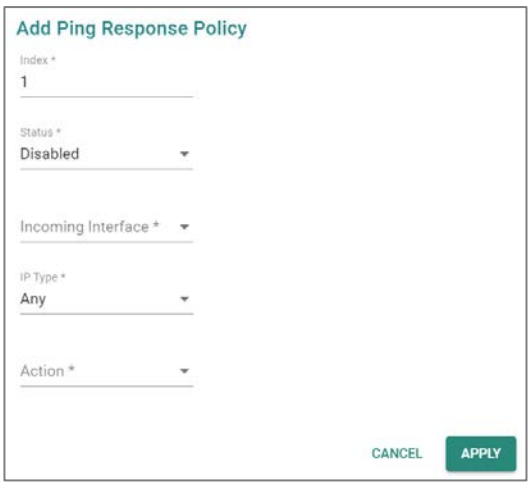
UI Setting	Description
Index	Shows the index of the ping response policy.
Status	Shows whether the policy is enabled.
Incoming Interface	Shows the interface this policy will monitor for ping requests through this policy.
IP Address/Netmask	Shows the IP address and netmask to monitor for ping requests through this policy.
Action	Shows whether the device will allow or deny ping responses for matching ping requests through this policy.

Create Ping Response Policy

Menu Path: System > Management Interface > Ping Response

Clicking the **Add (⊕)** icon on the **System > Management Interface > Ping Response** page will open this dialog box. This dialog lets you create a new ping response policy.

Click **CREATE** to save your changes and add the new policy.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index for the ping response policy.	1 to 16	Next available index
Status	Enable or disable the ping response policy.	Enabled / Disabled	Disabled
Incoming Interface	Select the interface this policy will monitor for ping requests.	Drop-down list of interfaces	N/A
IP Type	Select the IP type to monitor for ping requests for this policy.	Any / Single IP / Subnet	Any
IP Address **(If IP Type is Single IP or Subnet)**	Specify the IP address to monitor for ping requests through this policy.	Valid IP Address	N/A
Netmask **(If IP Type is Subnet)**	Specify the netmask to monitor for ping requests through this policy.	Drop-down list of netmask	N/A

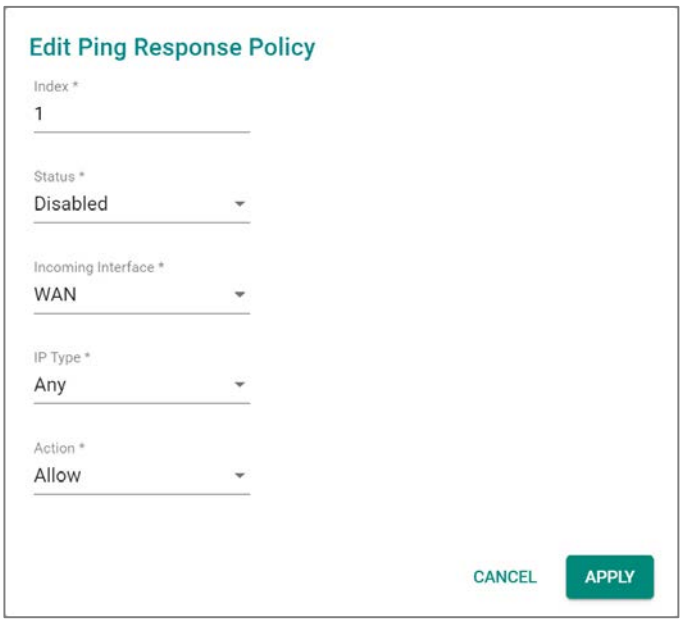
UI Setting	Description	Valid Range	Default Value
Action	Select whether the device will allow or deny ping responses for matching ping requests through this policy.	Allow / Deny	N/A

Edit Ping Response Policy

Menu Path: System > Management Interface > Ping Response

Clicking the **Edit ( )** icon for a policy on the **System > Management Interface > Ping Response** page will open this dialog box. This dialog lets you edit an existing policy.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index for the ping response policy.	1 to 16	Next available index
Status	Enable or disable the ping response policy.	Enabled / Disabled	Disabled
Incoming Interface	Select the interface this policy will monitor for ping requests.	Drop-down list of interfaces	N/A

UI Setting	Description	Valid Range	Default Value
IP Type	Select the IP type to monitor for ping requests for this policy.	Any / Single IP / Subnet	Any
IP Address **(If IP Type is Single IP or Subnet)**	Specify the IP address to monitor for ping requests through this policy.	Valid IP Address	N/A
Netmask **(If IP Type is Subnet)**	Specify the netmask to monitor for ping requests through this policy.	Drop-down list of netmask	N/A
Action	Select whether the device will allow or deny ping responses for matching ping requests through this policy.	Allow / Deny	N/A

Delete Ping Response Policy

Menu Path: System > Management Interface > Ping Response

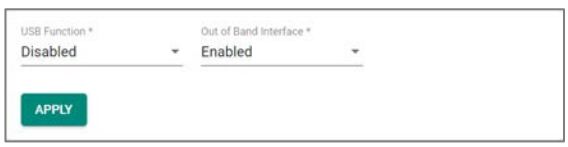
You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Hardware Interface (all products except TN Series)

Menu Path: System > Management Interface > Hardware Interface

This section lets you configure the additional hardware interfaces for your device.

> **Note**
> Available settings will vary depending on your product model.



UI Setting	Description	Valid Range	Default Value
USB Function	Enable or disable the USB interface on the device. **⚠ Warning** USB ports may be used to load unauthorized configuration files or other device data. Establishing careful control procedures can minimize this risk. Consider restricting personnel to only connecting Moxa ABC-02 configuration devices to USB ports, and regularly scanning the ABC-02 with antivirus software.	Enabled / Disabled	Enabled
Out of Band Interface	Enable or disable the out of band port on the device.	Enabled / Disabled	Enabled

Hardware Interface (TN Series only)

Menu Path: System > Management Interface > Hardware Interface

This page lets you configure the additional hardware interfaces for your device.

This page includes these tabs:

- USB
- Fault LED

USB

Menu Path: System > Management Interface > Hardware Interface - USB

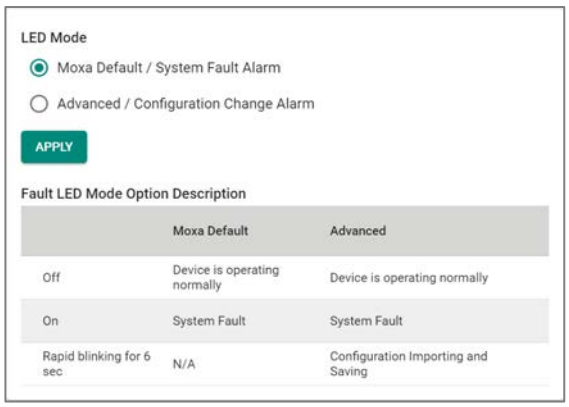
This page lets you enable or disable the USB interface on your device for use with a USB drive.

UI Setting	Description	Valid Range	Default Value
USB Function	Enable or disable the USB interface on the device.	Enabled / Disabled	Enabled

Fault LED

Menu Path: System > Management Interface > Hardware Interface - Fault LED

This page lets you select the behavior of the Fault LED.



UI Setting	Description	Valid Range	Default Value
LED Mode	Select the behavior mode to use for the Fault LED. • **Moxa Default / System Fault Alarm:** The Fault LED will be off when the device is operating normally, and on when there is a system fault. • **Advanced / Configuration Change Alarm:** The Fault LED will be off when the device is operating normally, and on when there is a system fault. When the device configuration is being imported and saved, the Fault LED will blink rapidly for 6 seconds.	Moxa Default / Advanced	Moxa Default

SNMP

Menu Path: System > Management Interface > SNMP

This section lets you configure SNMP settings for your device.

There are two tabs in this section:

- General
- SNMP Account

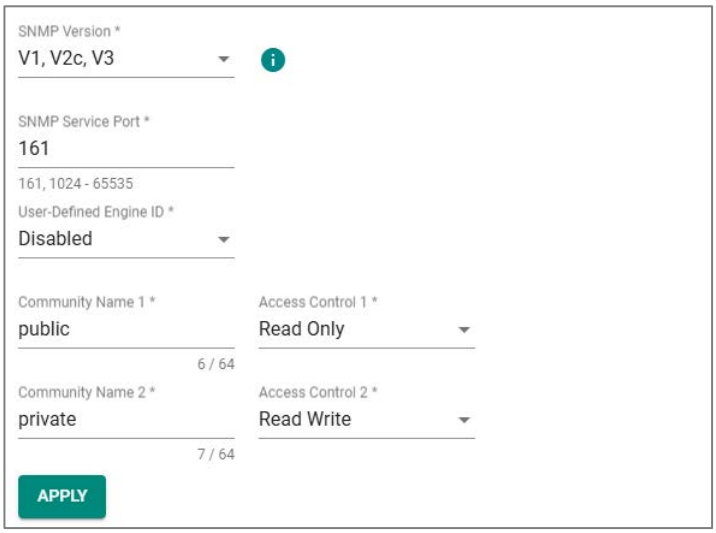
SNMP - General

Menu Path: System > Management Interface > SNMP - General

This page lets you enable or disable SNMP. SNMP versions V1, V2c, and V3 are supported.

Limitations

You can specify up to 2 SNMP community names with corresponding access controls.



UI Setting	Description	Valid Range	Default Value
SNMP Version	Specify the SNMP protocol version used to manage your device. • **Disabled**: Disable SNMP. • **V1, V2c, V3**: Enable SNMP V1, V2c, and V3. • **V1, V2c**: Enable SNMP V1, V2c only. • **V3 only**: Enable SNMP V3 only.	Disabled / V1, V2c, V3 / V1, V2c / V3 only	Disabled
SNMP Service Port	Specify the port number used by the SNMP service.	161, 1024 to 65535	161
User-Defined Engine ID **(If SNMP Version is V1, V2c, V3 or V3 only)**	Enable or disable use of a user-defined engine ID. If disabled, the system will use the default engine ID.	Disabled / Enabled	Disabled

UI Setting	Description	Valid Range	Default Value
Engine ID **(If SNMP Version is V1, V2c, V3 or V1, V2c)**	Specify an engine ID to manage your device. If **User-Defined Engine ID** is disabled, the engine ID will be view-only.	2 to 54 hexadecimal character string. The length of the string must be even.	800021f305
Community Name 1 **(If SNMP Version is V1, V2c, V3 or V1, V2c)**	Specify a community string name match to use for authentication.	1 to 64 characters	public
Community Name 2 **(If SNMP Version is V1, V2c, V3 or V1, V2c)**	Specify a community string name match to use for authentication.	1 to 64 characters	private
Access Control 1 **(If SNMP Version is V1, V2c, V3 or V1, V2c)**	Specify the access control type to use when Community String 1 is matched.	Read Write / Read only / No Access	Read Only
Access Control 2 **(If SNMP Version is V1, V2c, V3 or V1, V2c)**	Specify the access control type to use when Community String 2 is matched.	Read Write / Read only / No Access	Read Write

SNMP - SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

This page lets you configure SNMP management access for the device. You can configure SNMP access for your device's admin and user-level authority user accounts, or you can create custom SNMP accounts.

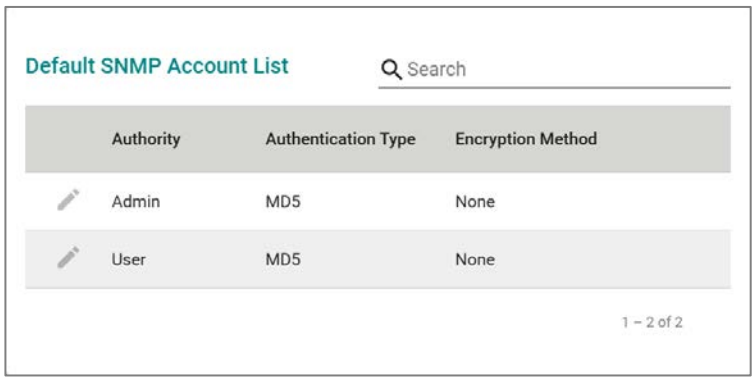
Limitations

You can create up to 5 custom SNMP accounts.

SNMP Mode Settings

UI Setting	Description	Valid Range	Default Value
SNMP Mode	Select the SNMP mode to use. • **Default:** SNMP access will be provided for the device's admin and user-level user accounts. Refer to User Accounts for more information. • **Custom**: You can specify your own SNMP accounts. The device's user accounts will not be used for SNMP access.	Default / Custom	Default

If **SNMP Mode** is **Default**, this will appear.



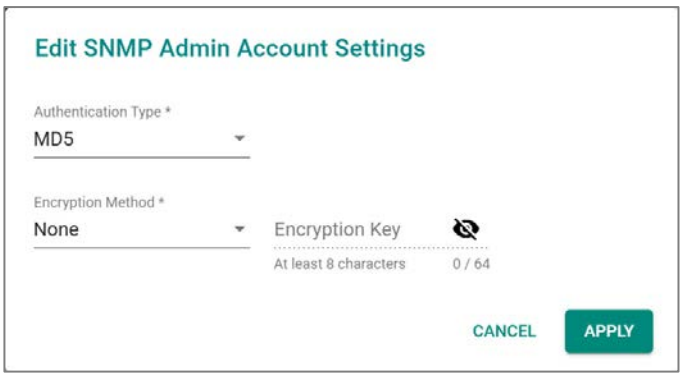
UI Setting	Description
Authority	Shows the user account authority level the settings are for.
Authentication Type	Shows the authentication type used for the user account authority level.
Encryption Method	Shows the encryption method used for the user account authority level.

Edit SNMP Account Settings

Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Edit ( )** icon for an authority level on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you modify SNMP settings for the selected user account authority level.

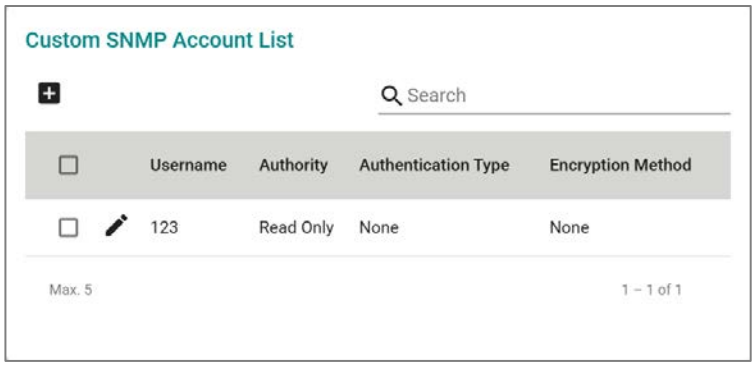
Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Authentication Type	Select which authentication method to use for the user account authority level. • **None**: No authentication will be used. • **MD5**: Use MD5 authentication. • **SHA**: Use SHA authentication. • **SHA-256**: Use SHA-256 authentication. • **SHA-512**: Use SHA-512 authentication. **Note** The authentication key will be the password for the user account. Refer to User Accounts for more information on changing user account passwords.	None / MD5 / SHA / SHA-256 / SHA-512	None
Encryption Method	Select which encryption method to use for the user account authority level.	None / DES / AES	None
Encryption Key **(If Encryption Method is DES or AES)**	Specify an encryption password for the user account authority level.	8 to 64 characters	N/A

Custom SNMP Account List

If **SNMP Mode** is **Custom**, this will appear.



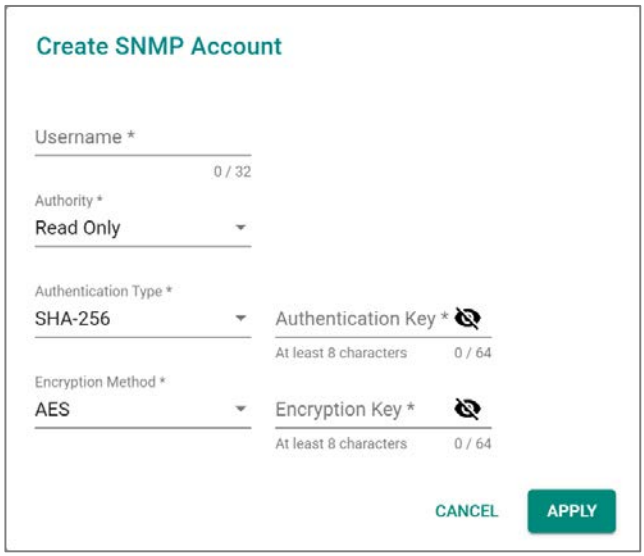
UI Setting	Description
Username	Shows the username for the account.
Authority	Shows the authority level of the account.
Authentication Type	Shows the authentication type used for the account.
Encryption Method	Shows the encryption method used for the account.

Create SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Add (+)** icon on the **System > Management Interface > SNMP - SNMP Account** page when **SNMP Mode** is **Custom** will open this dialog box. This dialog lets you create a new SNMP account.

Click **APPLY** to save your changes and add the new account.



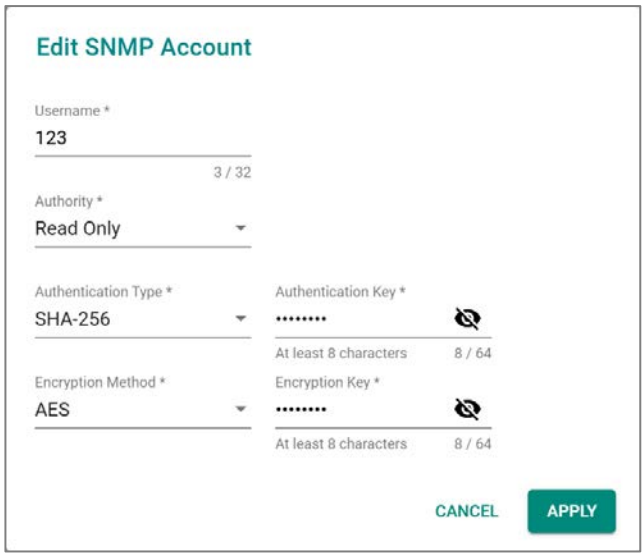
UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the account.	1 to 32 characters	N/A
Authority	Specify the authority for the account.	Read Write / Read Only	Read Only
Authentication Type	Select which authentication method to use for the account. • **None**: No authentication will be used. • **MD5**: Use MD5 authentication. • **SHA**: Use SHA authentication. • **SHA-256**: Use SHA-256 authentication. • **SHA-512**: Use SHA-512 authentication.	None / MD5 / SHA / SHA-256 / SHA-512	None
Authentication Key **(If Authentication Type is not None)**	Specify the authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Select which encryption method to use for the account.	None / DES / AES	None
Encryption Key **(If Encryption Method is not None)**	Specify the encryption key to use for the account.	8 to 64 characters	N/A

Edit SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Edit ( )** icon on the **System > Management Interface > SNMP - SNMP Account** page when **SNMP Mode** is **Custom** will open this dialog box. This dialog lets you edit an existing SNMP account.

Click **APPLY** to save your changes.



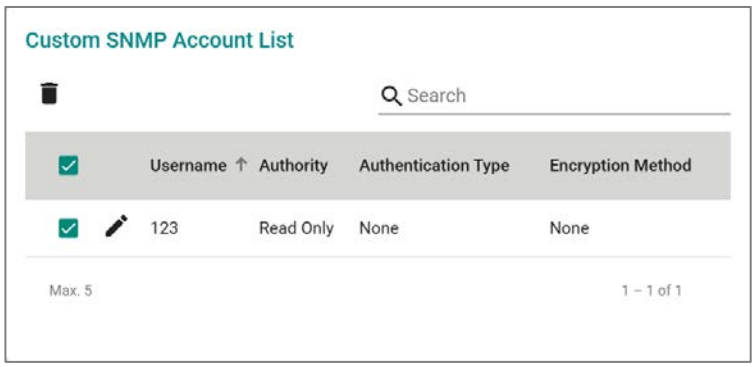
UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the account.	1 to 32 characters	N/A
Authority	Specify the authority for the account.	Read Write / Read Only	Read Only
Authentication Type	Select which authentication method to use for the account. • **None**: No authentication will be used. • **MD5**: Use MD5 authentication. • **SHA**: Use SHA authentication. • **SHA-256**: Use SHA-256 authentication. • **SHA-512**: Use SHA-512 authentication.	None / MD5 / SHA / SHA-256 / SHA-512	None

UI Setting	Description	Valid Range	Default Value
Authentication Key **(If Authentication Type is not None)**	Specify the authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Select which encryption method to use for the account.	None / DES / AES	None
Encryption Key **(If Encryption Method is not None)**	Specify the encryption key to use for the account.	8 to 64 characters	N/A

Delete SNMP Account

Menu Path: System > Management Interface > SNMP - SNMP Account

You can delete an account by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Moxa Remote Connect

Menu Path: System > Management Interface > Moxa Remote Connect

This section lets you establish a connection to the MRC Quick Link cloud platform to monitor and remotely access your device. Visit the Moxa Remote Connect Suite page for more information.

Note

Availability of this feature may vary depending on your product model and version.

There are two tabs in this section:

- Settings
- Status

Moxa Remote Connect - Settings

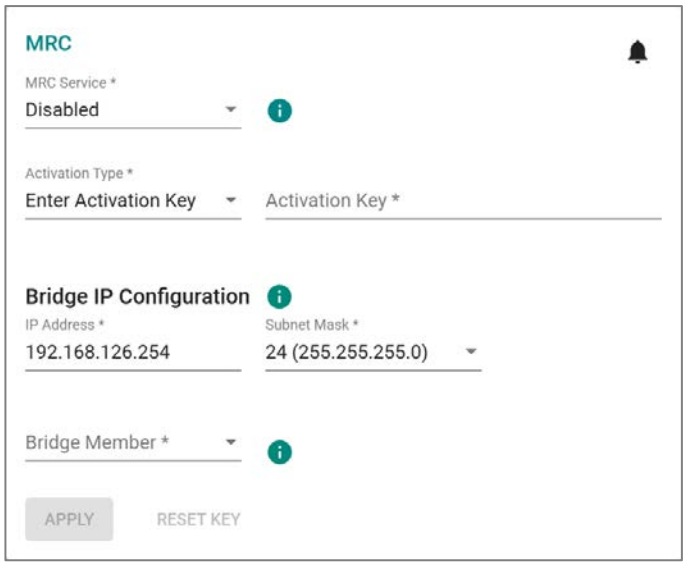
Menu Path: System > Management Interface > Moxa Remote Connect - Settings

This page lets you enable or disable MRC service and configure its connection parameters.

MRC

- Click **APPLY** to activate the device in MRC Quick Link.
- Click **RESET KEY** to unbind the device from MRC Quick Link.

> **Note**
>
> When the gateway exhibits any of the following behaviors, it will appear as offline in MRC Quick Link:
>
> - Clicking RESET KEY in the MRC settings page of the gateway web console
> - Clicking Reset to Defaults in the gateway web console
> - Physically pressing the reset button on the hardware
>
> To reactivate the gateway, you will need to perform the deactivate function and download a new activation key in MRC Quick Link and then enter it into the gateway, or create a new gateway in MRC Quick Link and enter a new key into the gateway.



UI Setting	Description	Valid Range	Default Value
MRC Service	Enable or disable the MRC service for establishing remote access connections.	Enabled / Disabled	Disabled
Activation Type	Select how to add the activation key. • **Enter Activation Key:** Manually enter an activation key for authentication. • **Import from USB drive**: Insert a USB drive that has an activation key on it for authentication. **Note** To use this feature, USB Function mus enabled in Hardware Interface.	Enter Activation Key / Import from USB	Enter Activation Key
Activation Key **(If Activation Type is Enter Activation Key)**	Specify the activation key for authentication.	Valid activation key	N/A

Bridge IP Configuration

UI Setting	Description	Valid Range	Default Value
IP Address	Specify an IP address for the bridge.	Valid IP address	192.168.126.254
Subnet Mask	Select a subnet mask for the bridge.	Drop-down list of subnet masks	24(255.255.255.0)

UI Setting	Description	Valid Range	Default Value
Bridge Member	Select which ports will be members of the bridge. **Note** Only devices connected to the Bridge port can be remotely accessed via MRC service. Please ensure that the device's IP and the Bridge IP are set within the same subnet. **Note** Bridge members are limited to LAN ports only. If any port is used as a WAN port, please do not add that port as a bridge member to avoid affecting the WAN network settings.	Drop-down list of ports	N/A

Tunnel Control Settings

UI Setting	Description	Valid Range	Default Value
Tunnel Control	Select the Tunnel Control Type. • **Persistent Connection**: Always establish a tunnel for remote access. • **Controlled by Key file from USB drive**: Establish a tunnel for remote access only when a USB containing the key is inserted into the device. **Note** To use this feature, USB Function must be enabled in Hardware Interface. • **Controlled by DI**: Establish a tunnel for remote access only when the Digital Input is detected as On.	Persistent Connection / Controlled by USB Key / Controlled by DI	Permanent Connection

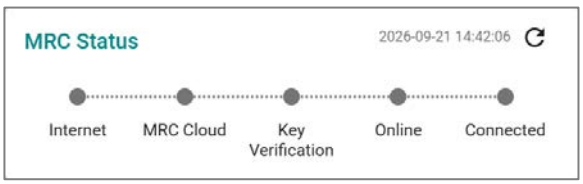
Moxa Remote Connect - Status

Menu Path: System > Management Interface > Moxa Remote Connect - Status

This page lets you view the status and details of your Moxa Remote Connect connection.

MRC Status

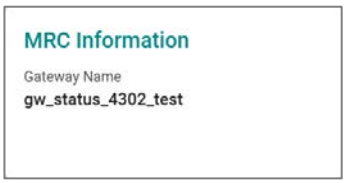
This shows the current status of your MRC connection.



UI Setting	Description
Internet	Shows the status of your device's Internet connection. • **Green**: The device is connected to the Internet. • **Red**: The device failed to connect to the Internet. • **Gray**: The device has not been activated yet.

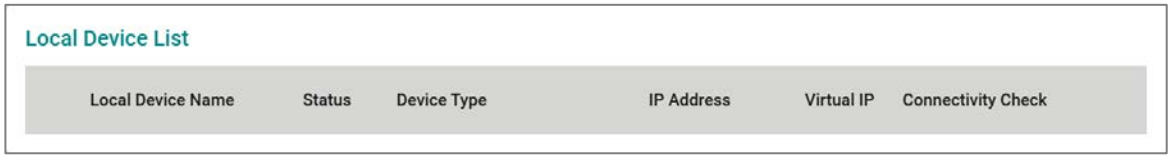
UI Setting	Description
MRC Cloud	Shows the status of your device's MRC Cloud connection. • **Green**: Connected to MRC Cloud successfully. • **Red:** Failed to connect to MRC Cloud. • **Gray**: Have not tried to connect to MRC Cloud yet.
Key Verification	Shows the status of your device's key verification. • **Green**: Successfully verified the activation key. • **Red:** Failed to verify the activation key. • **Gray**: Have not tried to verify the activation key yet.
Online	Shows the status of your device in MRC Quick Link. • **Green**: Device online. • **Red:** Device offline. • **Gray**: Device not authenticated yet.
Connected	Shows the status of your device's remote connection. • **Green**: Remote connection established successfully. • **Red:** Failed to establish remote connection. • **Gray**: Remote connection not yet established yet.

MRC Information



UI Setting	Description
Gateway Name	Shows the name of this device in MRC Quick Link.

Local Device List



UI Setting	Description
Local Device Name	Shows the name of the local device connected to this device.
Status	Shows the connection status of the local device.
Device Type	Shows the type of the local device. (IP Ethernet Device / Layer 2 Ethernet Device / Serial Device)
IP Address	Shows the IP address of the local device.
Virtual IP	Shows the virtual IP address of the local device that is assigned by the MRC Quick Link server.
Connectivity Check	Shows how the local device's alive status will be checked for connectivity.

MXsecurity

Menu Path: System > Management Interface > MXsecurity

TThis page lets you establish a connection to an MXsecurity instance to monitor and manage the device.

Note

To manage your the device through MXsecurity, the MXsecurity Agent Package must be installed and enabled first. Refer to the Software Package Management section for more information and instructions.

MXsecurity - Connection Status

UI Setting	Description
Status	Shows the MXsecurity connection status.

UI Setting	Description
Package Version	Shows the MXsecurity package version.
Service address (IP Address / FQDN)	Shows the service address of the MXsecurity connection.
Profile Synchronization	Shows the MXsecurity profile synchronization status.

MXsecurity - New Connection

To set up a new MXsecurity connection, specify the required settings, then select **CONNECT**.

UI Setting	Description	Valid Range	Default Value
Service Address (IP Address / FQDN)	Set the MXsecurity server IP address or domain name.	Valid IP address or domain name	N/A
HTTPS Port	Specify the HTTPS port number for MXsecurity.	1 to 65535	443
Communication Port	Specify the communication port number for MXsecurity.	1 to 65535	8833

Time

Menu Path: System > Time

This section lets you configure the system time settings for your device.

This section includes these pages:

- System Time
- NTP/SNTP Server

System Time

Menu Path: System > Time > System Time

This section lets you set up time settings for the device itself.

This page includes these tabs:

- Time
- Time Zone
- NTP Authentication

> **Note**
>
> This device does not include a real-time clock. If there is no NTP/SNTP server on the network or if the device is not connected to the Internet, the Current Time and Current Date must be manually reconfigured after each reboot.

System Time - Time

Menu Path: System > Time > System Time - Time

This page lets you set the system time and date.

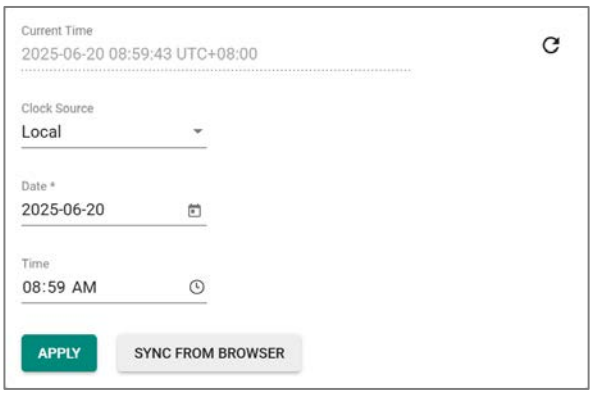
You can set your system time using these clock sources:

- Local
- SNTP
- NTP

System Time Settings - Local

If you select **Local** as your **Clock Source**, these settings will appear. Local lets you set your device's system time manually, or you can copy the time from your local host by clicking **SYNC FROM BROWSER**.

Click **APPLY** to save your changes.

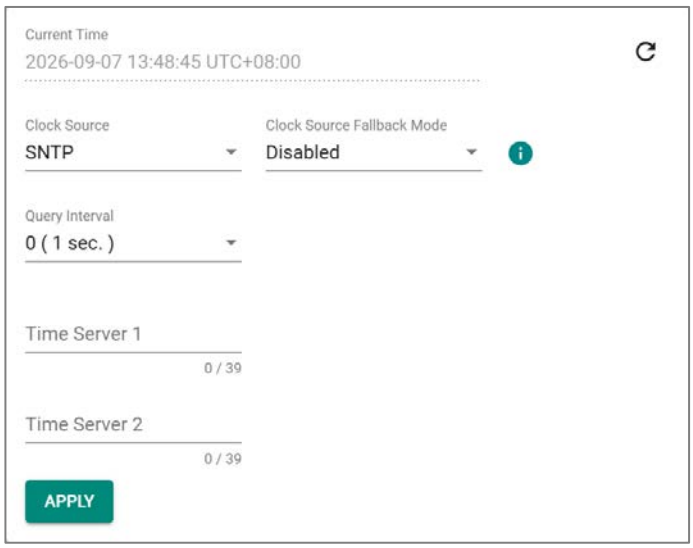


UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Date	Specify the date manually in YYYY-MM-DD format.	YYYY-MM-DD	Current date
Time	Specify the time manually in HH:MM AM/PM format.	HH:MM AM/PM	Current time

System Time Settings - SNTP

If you select **SNTP** as your **Clock Source**, these settings will appear. SNTP allows your device to update its system time from a Simplified Network Time Protocol (SNTP) time server.

Click **APPLY** to save your changes.



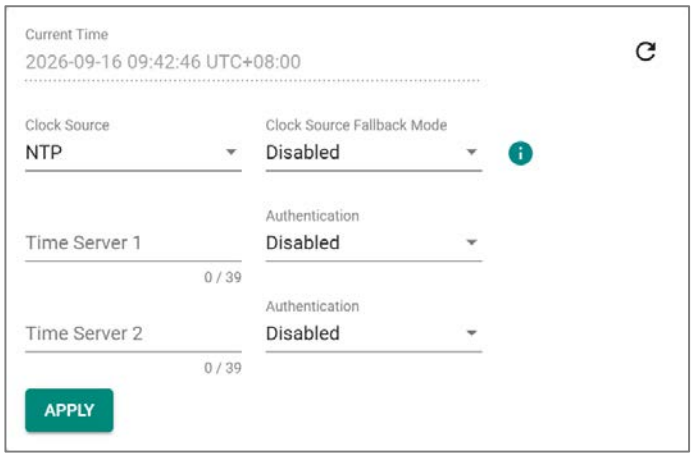
UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Clock Source Fallback Mode	Specify whether the system should switch to the "Local" clock source when the configured clock source becomes unavailable. Enabling this setting ensures timekeeping continuity if external time synchronization fails. **Note** Make sure the "Local" time is correct before enabling Clock Source Fallback Mode to avoid time errors after fallback.	Disabled / Enabled	Disabled
Query Interval	Select the amount of time to wait in between SNTP requests.	0 (1 sec.) / 1 (2 sec.) / 2 (4 sec.) / 3 (8 sec.) / 4 (16 sec.) / 5 (32 sec.) / 6 (64 sec.) / 7 (128 sec.) / 8 (256 sec.) / 9 (512 sec.) / 10 (1024 sec.) / 11 (2048 sec.) / 12 (4096 sec.) / 13 (8192 sec.)	0 (1 sec.)
Time Server 1	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Valid IP address or domain, 1 to 39 characters	N/A
Time Server 2	Set the IP or domain address of the secondary time server. This will be used by the device if it cannot connect to the primary time server.	Valid IP address or domain, 1 to 39 characters	N/A

System Time Settings - NTP

If you select **NTP** as your **Clock Source**, these settings will appear. NTP allows your device to update its system time from a Network Time Protocol (NTP) server.

Click **APPLY** to save your changes.

> **Note**
>
> When synchronizing device time using NTP, we recommend using NTP authentication to reduce cybersecurity risks.



UI Setting	Description	Valid Range	Default Value
Current Time	This shows the device's current system date, time, and time zone.	N/A	N/A
Clock Source Fallback Mode	Specify whether the system should switch to the "Local" clock source when the configured clock source becomes unavailable. Enabling this setting ensures timekeeping continuity if external time synchronization fails. **Note** Make sure the "Local" time is correct before enabling Clock Source Fallback Mode to avoid time errors after fallback.	Disabled / Enabled	Disabled
Time Server 1	Set the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Valid IP address or domain up to 39 characters	N/A

UI Setting	Description	Valid Range	Default Value
Time Server 2	Set the IP or domain address of the secondary time server. This will be used by the device if it cannot connect to the primary time server.	Valid IP address or domain up to 39 characters	N/A
Authentication	Specify whether to use a key ID for NTP server authentication. **Note** To use authentication, set up the Key ID value in the NTP Authentication tab first. After setting it up, it will become available in the Authentication drop-down.	Disabled / Key IDs created in the **NTP Authentication** tab	Disabled

System Time - Time Zone

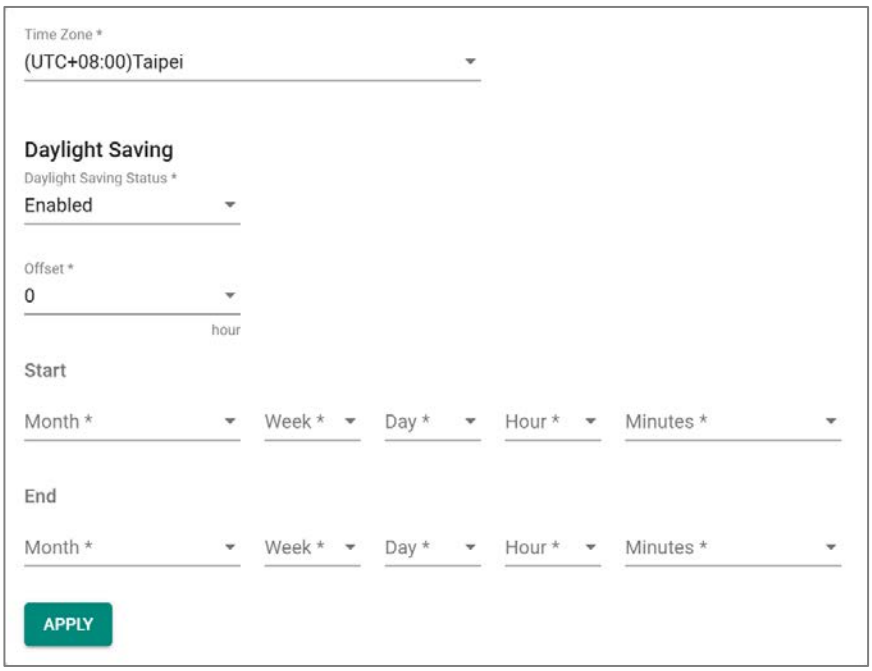
Menu Path: System > Time > System Time - Time Zone

This page lets you set the time zone settings of your device.

Click **APPLY** to save your changes.

Note

Changing the time zone will automatically adjust the device's system time. Be sure to set the time zone before setting the system time.



UI Setting	Description	Valid Range	Default Value
Time Zone	Select a time zone from the list of UTC (Coordinated Universal Time) time zones.	Drop-down list of UTC time zones	N/A
Daylight Saving Status	Enable or disable Daylight Saving time adjustment.	Enabled / Disabled	Disabled
Offset **(If Daylight Saving Status is Enabled)**	Select the offset in hours to add to the time when Daylight Saving time is active.	0 / 0.5 / 1 / 1.5 / 2 / 2.5 / 3 / 3.5 / 4 / 4.5 / 5 / 5.5 / 6 / 6.5 / 7 / 7.5 / 8 / 8.5 / 9 / 9.5 / 10 / 10.5 / 11 / 11.5 / 12	0
Month **(If Daylight Saving Status is Enabled)**	Select the month Daylight Saving Time starts/ends.	Drop-down list of months	N/A
Week **(If Daylight Saving Status is Enabled)**	Select the week Daylight Saving time starts/ends.	1st / 2nd / 3rd / 4th / Last	N/A
Day **(If Daylight Saving Status is Enabled)**	Select the day of the week Daylight Saving time starts/ends.	Drop-down list of days of the week	N/A

UI Setting	Description	Valid Range	Default Value
Hour **(If Daylight Saving Status is Enabled)**	Select the hour Daylight Saving time starts/ends.	00 to 23	N/A
Minutes **(If Daylight Saving Status is Enabled)**	Select the minute Daylight Saving time starts/ends.	00 to 59	N/A

System Time - NTP Authentication

Menu Path: System > Time > System Time - NTP Authentication

This section describes how to configure NTP Authentication. After creating a key, it will be available for use in the **Time** tab.

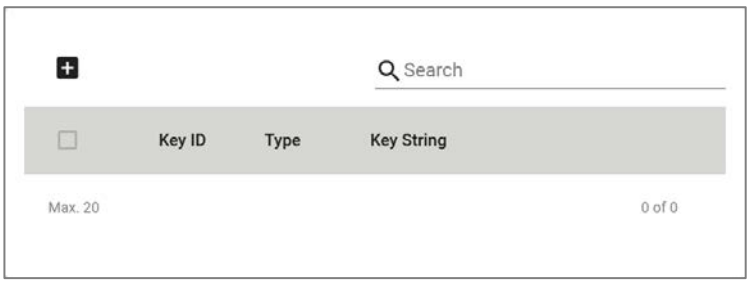
Click **APPLY** to save your changes.

Note

When synchronizing device time using NTP, we recommend using NTP authentication to reduce cybersecurity risks.

Limitations

You can create up to 20 NTP authentication entries.



UI Setting	Description
Key ID	Shows the key ID for the authentication key.
Type	Shows the type of NTP authentication the key uses. • **MD5**: Uses authentication based on MD5 algorithms. • **SHA**: Uses authentication based on SHA-512 algorithms.
Key String	Shows the key string used by the authentication key.

NTP Authentication - Create Entry

Menu Path: System > Time > System Time - NTP Authentication

Clicking the **Add (⊕)** icon on the **System > Time > System Time - NTP Authentication** page will open this dialog box. This dialog lets you create a new NTP authentication key.

Click **CREATE** to save your settings and create the new authentication key.

UI Setting	Description	Valid Range	Default Value
Key ID	Specify the key ID to use for the authentication key.	1 to 65535 characters	N/A
Type	Specify the type of NTP authentication the key should use. • **MD5**: Sets authentication based on MD5 algorithms. • **SHA**: Sets authentication based on SHA-512 algorithms.	MD5 / SHA-512	N/A

UI Setting	Description	Valid Range	Default Value
Key String	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

NTP Authentication - Edit Entry

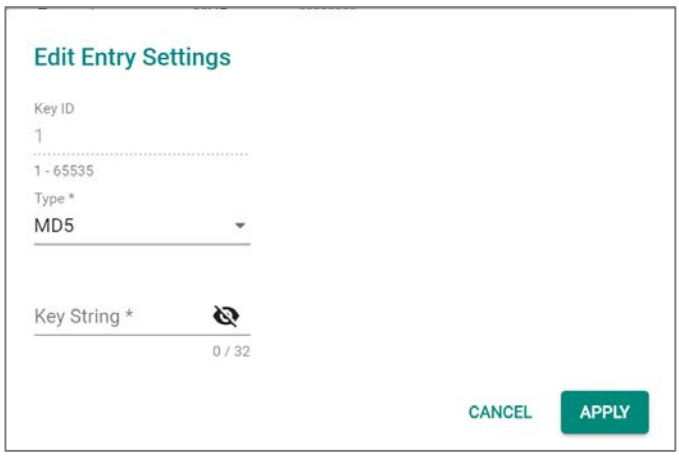
Menu Path: System > Time > System Time - NTP Authentication

Clicking the **Edit ( )** icon for a key on the **System > Time > System Time - NTP Authentication** page will open this dialog box. This dialog lets you edit an existing authentication key.

Click **APPLY** to save your settings.

Note

All key parameters can be modified, except for the key ID. To modify the key ID, you must create a new authentication key.



UI Setting	Description	Valid Range	Default Value
Key ID	Shows the key ID for this authentication key. The key ID cannot be changed.	N/A	Current key ID

UI Setting	Description	Valid Range	Default Value
Type	Specify the type of NTP authentication the key should use. • **MD5**: Sets authentication based on MD5 algorithms. • **SHA**: Sets authentication based on SHA-512 algorithms.	MD5 / SHA-512	N/A
Key String	Specify the key string to use for the authentication key.	1 to 32 characters	N/A

NTP Authentication - Delete Entry

Menu Path: System > Time > System Time - NTP Authentication

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

NTP/SNTP Server

Menu Path: System > Time > NTP/SNTP Server

This page lets you enable NTP/SNTP functionality for clients.

Select **APPLY** to save your changes.

NTP/SNTP Server Settings

UI Setting	Description	Valid Range	Default Value
NTP/SNTP Server	Enable or disable NTP/SNTP server functionality for clients.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Client Authentication	Enable or disable client authentication for the NTP/SNTP server. **Note** Before enabling Client Authentication, you will need to create NTP authentication keys first. Refer to NTP Authentication for more information.	Enabled / Disabled	Disabled

Power Management

Menu Path: System > Power Management

This page lets you configure the power management features of your device.

Note

Availability of this feature may vary depending on your product model and version.

Important

Possible loss of management access to device. Enabling a power management mode immediately applies the relevant settings and rules. This may cause the device to enter power-saving mode immediately, preventing management access without a physical power cycle or until the device enters wake up mode.

To access a device that is in power-saving mode, power the device off then on again. The device will stay in wake up mode for 15 minutes before using the configured power management mode and rules to determine when to enter power-saving mode again.

This page includes these tabs:

- General
- Scheduling
- Ignition

Power Management - General

Menu Path: System > Power Management - General

This page lets you lets you enable power management for your device. If enabled, you can control how and when the device enters power-saving mode. Power-saving mode minimizes power usage by stopping all communication and activity until the device leaves power-saving mode.

UI Setting	Description	Valid Range	Default Value
Power Management	Select a power management setting for your device. • **Disabled**: Disables power management; the device will never enter power-saving mode. • **Scheduling**: Enables power-saving mode based on a schedule you define. Refer to Power Management - Scheduling for more information. • **Ignition:** Enables power-saving mode based on signals sent to the digital input, allowing the device to enter power-saving mode when a vehicle ignition is off. Refer to Power Management - Ignition for more information. Important Possible loss of management access to device. Enabling a power management mode immediately applies the relevant settings and rules. This may cause the device to enter power-saving mode immediately, preventing management access without a physical power cycle or until the device enters wake up mode. To access a device that is in power-saving mode, power the device off then on again. The device will stay in wake up mode for 15 minutes before using the configured power management mode and rules to determine when to enter power-saving mode again.	Disabled / Scheduling / Ignition	Disabled

Power Management - Scheduling

Menu Path: System > Power Management - Scheduling

This page lets you create both repeating cycle rules and one-time rules to determine when the device should enter and leave power-saving mode. One-time rules will have priority over cycle rules.

Limitations

You can create up to 2 cycle rules, and up to 12 one-time rules.

- Both cycle rules must use the same Cycle Type. If the Cycle Type is changed, all existing cycle rules will be deleted.
- If the Cycle Type is set to Weekly or Monthly, the start and end times must be within the same day. If you need the start and end times to be on different days, create a One Time Rule.
- Enabled one-time rules cannot have overlapping schedules.

Note

This feature requires Power Management settings to be set to Scheduling. Refer to Power Management - General for more information.

Important

Possible loss of management access to device. Applying changes to power management settings may cause the device to enter power-saving mode immediately, preventing management access without a physical power cycle or until the device enters wake up mode.

To avoid triggering rules while changing power management settings, disable power management first. Refer to Power Management - General for more information.

To access a device that is in power-saving mode, power the device off then on again. The device will stay in wake up mode for 15 minutes before using the configured power management mode and rules to determine when to enter power-saving mode again.

Note

When using scheduling for power management, the default power mode of the device depends on whether there are enabled cycle rules that are currently applicable.

- If the system time is inside the rule start/end period of an enabled cycle rule, the device will be in power-saving mode by default, and will only wake up according to cycle rules and one-time wake up rules.
- If no cycle rules are enabled, or if the system time is outside the rule start/end period of all enabled cycle rules, the device will be in wake up mode by default, and will only enter power-saving mode according to one-time power saving rules.

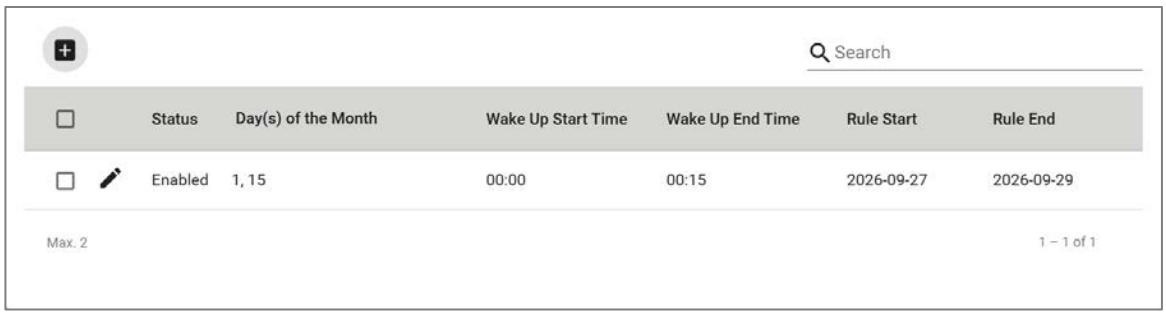
Note

Scheduling rules are not adjusted when making changes to the system time.

Wakeup Cycle Rules

UI Setting	Description	Valid Range	Default Value
Cycle Type	Select a wakeup cycle to use for power-saving mode scheduling. • **Hourly**: The device will enter and leave power-saving mode according to specific times every hour. • **Daily**: The device will enter and leave power-saving mode according to specific times every day. • **Weekly**: The device will enter and leave power-saving mode according to specific times on specific days of the week. Multiple days of the week may be selected. • **Monthly**: The device will enter and leave power-saving mode according to specific times on specific days of the month. Multiple days of the month may be selected.	Hourly / Daily / Weekly / Monthly	Daily

Wakeup Cycle Rule List



UI Setting	Description
Status	Shows the status of the wakeup cycle rule.
Day(s) of the Week **(If Cycle Type is Weekly)**	Shows the days of the week the wakeup cycle rule will run on.
Day(s) of the Month **(If Cycle Type is Monthly)**	Shows the days of the month the wakeup cycle rule will run on.
Wake Up Start Time	Shows when the device will leave power-saving mode. HH indicates this will happen every hour. **Note** The units shown will vary depending on the wakeup cycle type used.
Wake Up End Time	Shows when the device will enter power-saving mode. HH indicates this will happen every hour. **Note** The units shown will vary depending on the wakeup cycle type used.
Rule Start	Shows when the wakeup cycle rule will start taking effect.
Rule End	Shows when the wakeup cycle rule will no longer take effect.

Add Cycle Rule

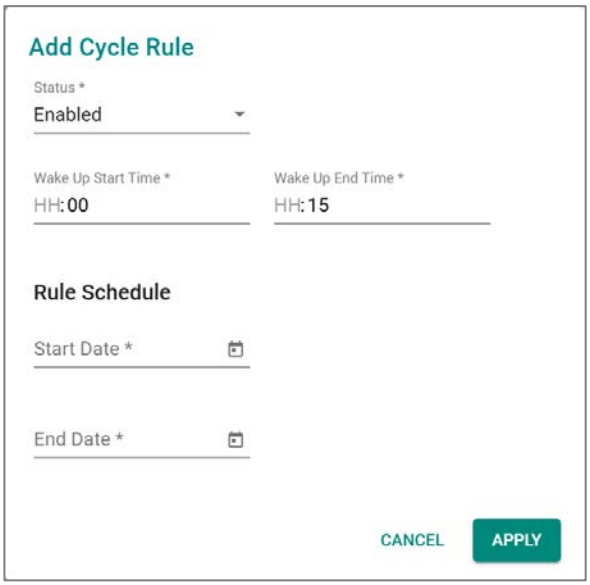
Menu Path: System > Power Management - Scheduling

Clicking the **Add (⊕)** icon in the **Wakeup Cycle Rule List** on the **System > Power Management - Scheduling** page will open this dialog box. This dialog lets you create a new wakeup cycle rule. The options shown will vary depending on what **Cycle Type** is selected.

Click **CREATE** to save your changes and add the new rule.

Add Cycle Rule - Hourly

If the **Cycle Type** is set to **Hourly**, these options will appear.

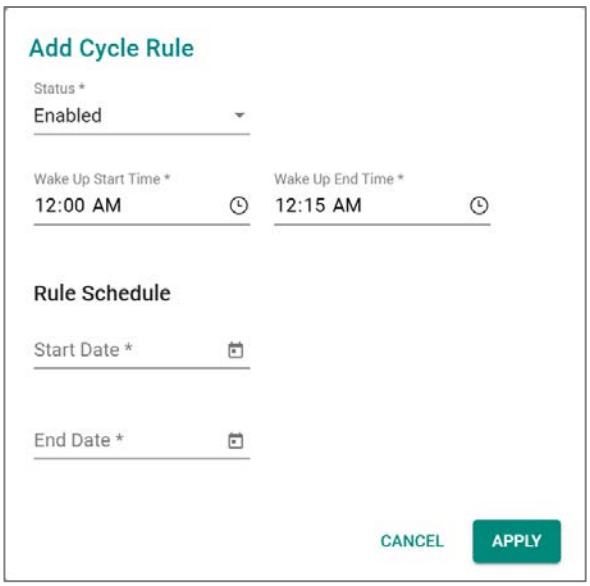


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
Wakeup Start Time	Specify the minute when the device will leave power-saving mode each hour.	00 to 59	00
Wakeup End Time	Specify the minute when the device will enter power-saving mode each hour.	00 to 59	15

UI Setting	Description	Valid Range	Default Value
Start Date	Specify when this cycle rule will take effect. You can also click the **calendar (** **)** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
End Date	Specify when this cycle rule will end. You can also click the **calendar (** **)** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A

Add Cycle Rule - Daily

If the **Cycle Type** is set to **Daily**, these options will appear.

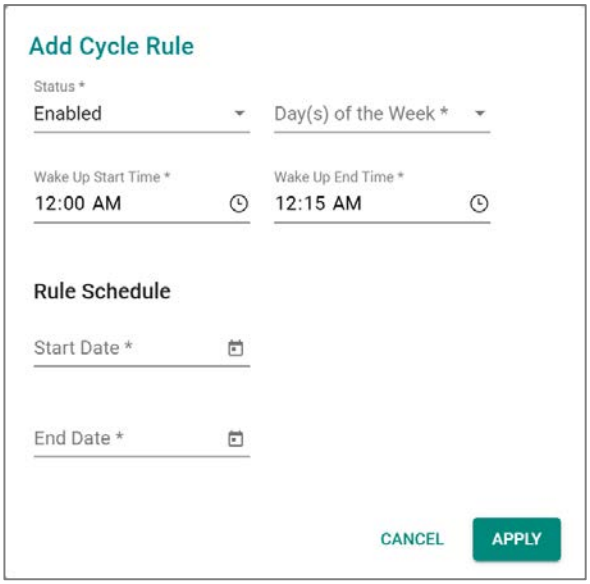


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
Wakeup Start Time	Specify the hour and minute when the device will leave power-saving mode every day. You can also click the **clock (** **)** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:00 AM
Wakeup End Time	Specify the hour and minute when the device will enter power-saving mode every day. You can also click the **clock (** **)** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:15 AM

UI Setting	Description	Valid Range	Default Value
Start Date	Specify when this cycle rule will take effect. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
End Date	Specify when this cycle rule will end. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A

Add Cycle Rule - Weekly

If the **Cycle Type** is set to **Weekly**, these options will appear.

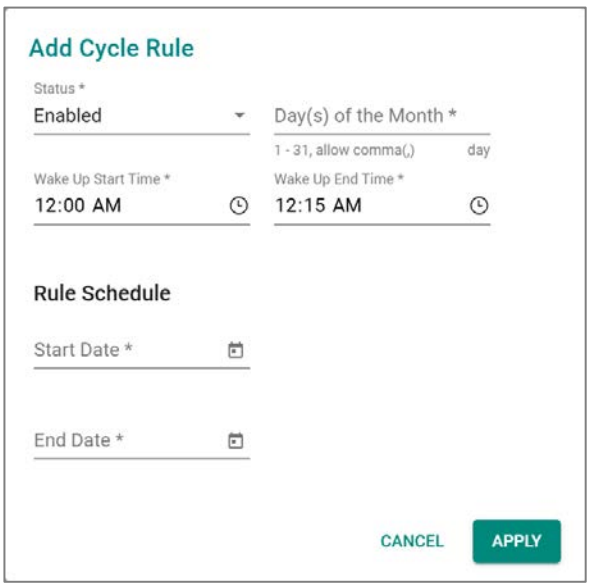


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the cycle rule.	Enabled / Disabled	Enabled
Day(s) of the Week	Select which days of the week this rule will apply to. You can select multiple days.	Drop-down list of days of the week	N/A
Wakeup Start Time	Specify the hour and minute when the device will leave power-saving mode on the specified **Day(s) of the Week**. You can also click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:00 AM

UI Setting	Description	Valid Range	Default Value
Wakeup End Time	Specify the hour and minute when the device will enter power-saving mode on the specified **Day(s) of the Week**. You can also click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:15 AM
Start Date	Specify when this cycle rule will take effect. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
End Date	Specify when this cycle rule will end. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A

Add Cycle Rule - Monthly

If the **Cycle Type** is set to **Monthly**, these options will appear.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the cycle rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Day(s) of the Month	Select which days of the month this rule will apply to. You can select multiple days by entering a comma in between each day (e.g., 1,2,16). **Note** If a month does not have a specified day in it, the rule will be ignored for that day.	1 to 31, multiple days should be separated by a comma	N/A
Wakeup Start Time	Specify the hour and minute when the device will leave power-saving mode on the specified **Day(s) of the Month**. You can also click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:00 AM
Wakeup End Time	Specify the hour and minute when the device will enter power-saving mode on the specified **Day(s) of the Month**. You can also click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	12:15 AM
Start Date	Specify when this cycle rule will take effect. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
End Date	Specify when this cycle rule will end. You can also click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A

Delete Cycle Rule

Menu Path: System > Power Management - Scheduling

You can delete a cycle rule by using the checkboxes to select the cycle rules you want to delete, then clicking the **Delete ( )** icon.

One Time Rule List

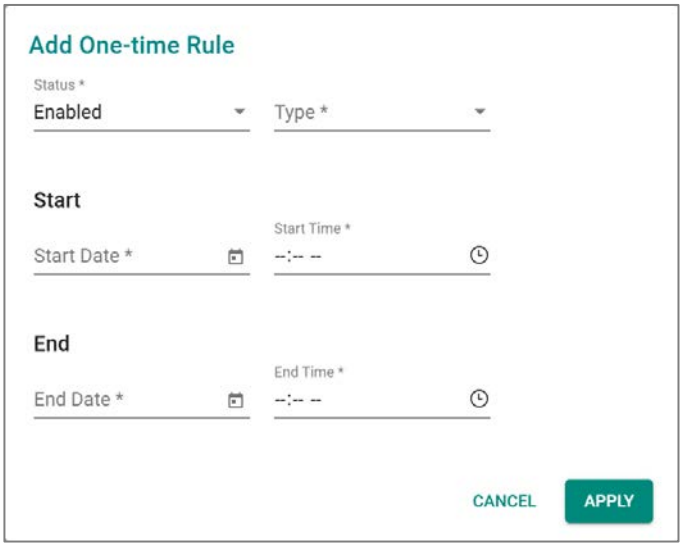
UI Setting	Description
Status	Shows the status of the one-time rule.
Type	Shows the type of the one-time rule. • **Power Saving:** The device will enter power-saving mode when the rule starts, and leave power-saving mode when the rule ends. • **Wake Up:** The device will leave power-saving mode when the rule starts, and enter power-saving mode when the rule ends.
Rule Start	Shows the rule start date and time.
Rule End	Shows the rule end date and time.

Add One-time Rule

Menu Path: System > Power Management - Scheduling

Clicking the **Add (⊕)** icon in the **One Time Rule** list on the **System > Power Management - Scheduling** page will open this dialog box. This dialog lets you create a new one-time rule.

Click **CREATE** to save your changes and add the new rule.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the one-time rule. **Note** You cannot enable a one-time rule if its schedule would overlap with another one-time rule.	Enabled / Disabled	Enabled
Type	Select the type for the one-time rule. • **Power Saving:** The device will enter power-saving mode when the rule starts, and leave power-saving mode when the rule ends. • **Wake Up:** The device will leave power-saving mode when the rule starts, and enter power-saving mode when the rule ends. **Note** To enable a one-time Wake Up rule, you must have at l one wakeup cycle rule. If there are no wakeup cycle rules enabled, the device be in wake up mode by default, and one-time wake up rules will not have any effect.	Power Saving / Wake up	Power Saving
Start Date	Specify the date this one-time rule will take effect. You can click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
Start Time	Specify the time this one-time rule will take effect. You can click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	N/A

UI Setting	Description	Valid Range	Default Value
End Date	Specify the date this one-time rule will end. You can click the **calendar ( )** icon to select the date from a date picker.	Valid date (yyyy-mm-dd)	N/A
End Time	Specify the time this one-time rule will end. You can click the **clock ( )** icon to select the time from a drop-down list.	Valid time in 12-hour format	N/A

Delete One-time Rule

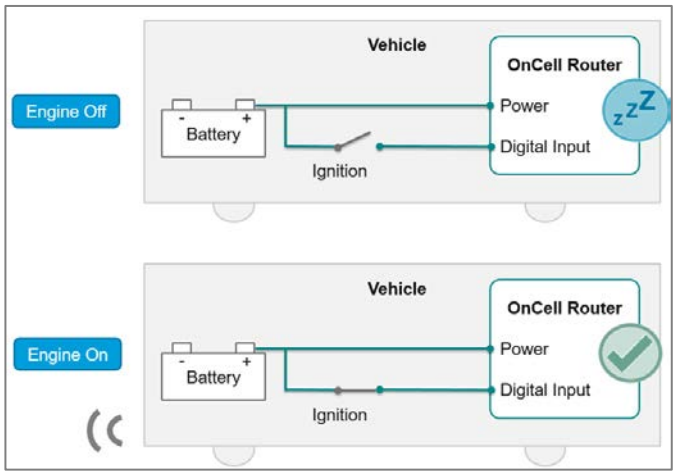
Menu Path: System > Power Management - Scheduling

You can delete a one-time rule by using the checkboxes to select the one-time rules you want to delete, then clicking the **Delete ( )** icon.

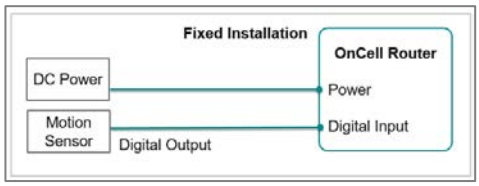
Power Management - Ignition

Menu Path: System > Power Management - Ignition

This page lets you configure the Ignition feature, which lets you use the digital input to determine when the device should enter and leave power-saving mode. This allows the device to enter and leave power-saving modes automatically when a vehicle starts or turns off. The device detects the ignition status through the digital input, and will enter power saving mode when the vehicle ignition is off to save battery power.



This feature can also be used for fixed installations with an I/O to monitor an external device, such as a motion sensor. You can configure the I/O line to either wake the device or put the device in power-saving mode, based on your needs.



Note

The Ignition feature is only applicable to OnCell G4302 hardware rev 1.1 and higher.

Note

This feature requires Power Management settings to be set to Ignition. Refer to Power Management - General for more information.

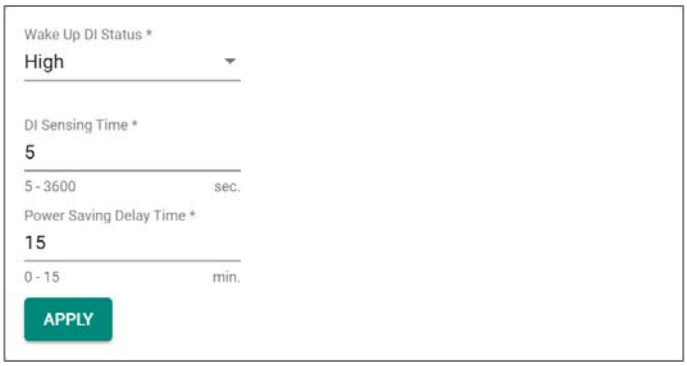
Important

Possible loss of management access to device. Applying changes to power management settings may cause the device to enter power-saving mode immediately, preventing management access without a physical power cycle or until the device enters wake up mode.

To avoid triggering rules while changing power management settings, disable power management first. Refer to Power Management - General for more information.

To access a device that is in power-saving mode, power the device off then on again. The device will stay in wake up mode for 15 minutes before using the configured power management mode and rules to determine when to enter power-saving mode again.

Ignition Settings



UI Setting	Description	Valid Range	Default Value
Wakeup DI Status	Select the DI status that will wake the device. • **High**: The device will leave power-saving mode when it detects the DI is high, and enters power-saving mode when it detects the DI is low. • **Low**: The device will leave power-saving mode when it detects the DI is low, and enters power-saving mode when it detects the DI is high.	High / Low	High
DI Sensing Time	Enter the number of seconds the DI status must remain changed for before the device determines there is a change in DI status. This is useful for avoiding erratic behavior when the DI signal is unstable.	5 to 3600	5
Power Saving Delay Time	Enter the number of minutes to delay entering enter power-saving mode after the vehicle's ignition shuts off. This is useful if you want to maintain a network connection while the vehicle's engine is off for a short period of time.	0 to 15	15

SMS

Menu Path: System > SMS

This page lets you configure your device's SMS remote control feature. When a cellular connection is not available or if there is limited service, SMS remote control provides an emergency recovery mechanism and a way to perform out-of-band management. SMS remote control lets you send specific SMS messages to the device to perform various

operations, such as getting the current cellular status of the device or restarting the system. Refer to SMS Remote Control Commands for a list of available commands.

To ensure the security of out-of-band communication, SMS remote control supports password protection and trusted number authentication. With wireless out-of-band management, engineers can control and troubleshoot remote devices, avoiding costly onsite visits by service technicians while minimizing downtime.

This page includes these tabs:

- General
- Remote Control List
- Send SMS

Note

Availability of this feature may vary depending on your product model and version.

Note

The cellular module must be enabled for this feature. Refer to Cellular for more information.

SMS - General

Menu Path: System > SMS - General

This page lets you configure basic SMS settings and the trusted number list.

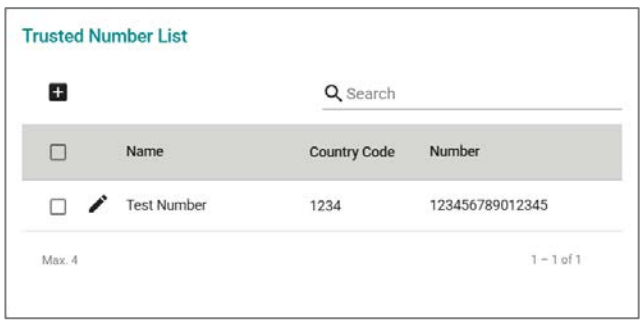
Limitations

You can add up to 4 trusted numbers.

SMS Settings

UI Setting	Description	Valid Range	Default Value
SMS Remote Control	Enable or disable SMS remote control. If enabled, the device can be controlled remotely through specific SMS messages. **Note** Your SIM card must support receiving SMS messages for this feature.	Enabled / Disabled	Enabled
Password	Specify the password required to authorize SMS remote control commands. Important Do not leave the password blank. Leaving the password blank allows the device to process unauthorized SMS remote control commands.	0 to 15 characters	N/A
Trusted Number Authentication	Enable or disable trusted number authentication. If enabled, the device will only accept SMS messages from numbers added to the Trusted Numbers List. If disabled, the device can be controlled by messages sent from any number.	Enabled / Disabled	Enabled

Trusted Number List



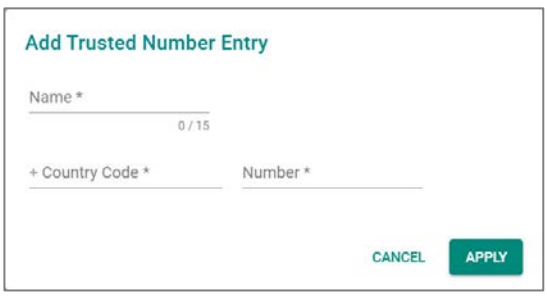
UI Setting	Description
Name	Shows the name used to identify the trusted number.
Country Code	Shows the country code for the trusted number.
Number	Shows the trusted number.

Add Trusted Number Entry

Menu Path: System > SMS - General

Clicking the **Add (⊕)** icon on the **System > SMS - General** page will open this dialog box. This dialog lets you add a new entry.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name to help identify the trusted number. This is for reference only.	1 to 15 characters	N/A
Country Code	Specify the country code of the trusted phone number.	1 to 4 digits	N/A
Number	Specify the trusted phone number.	1 to 15 digits	N/A

Edit Trusted Number Entry

Menu Path: System > SMS - General

Clicking the **Edit (✎)** icon on the **System > SMS - General** page will open this dialog box. This dialog lets you edit an existing entry.

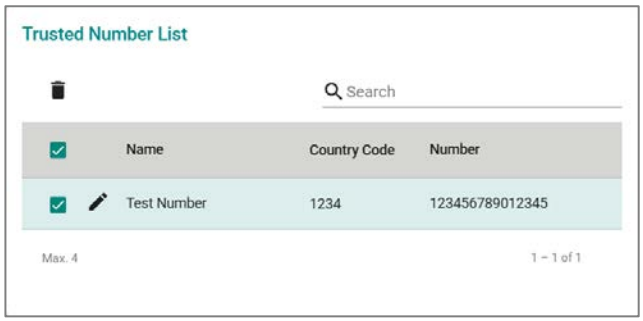
Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name to help identify the trusted number. This is for reference only.	1 to 15 characters	N/A
Country Code	Specify the country code of the trusted phone number.	1 to 4 digits	N/A
Number	Specify the trusted phone number.	1 to 15 digits	N/A

Delete Trusted Number Entry

Menu Path: System > SMS - General

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Remote Control List

Menu Path: System > SMS - Remote Control List

This page lets you manage which SMS remote control commands your device will respond to.

Note

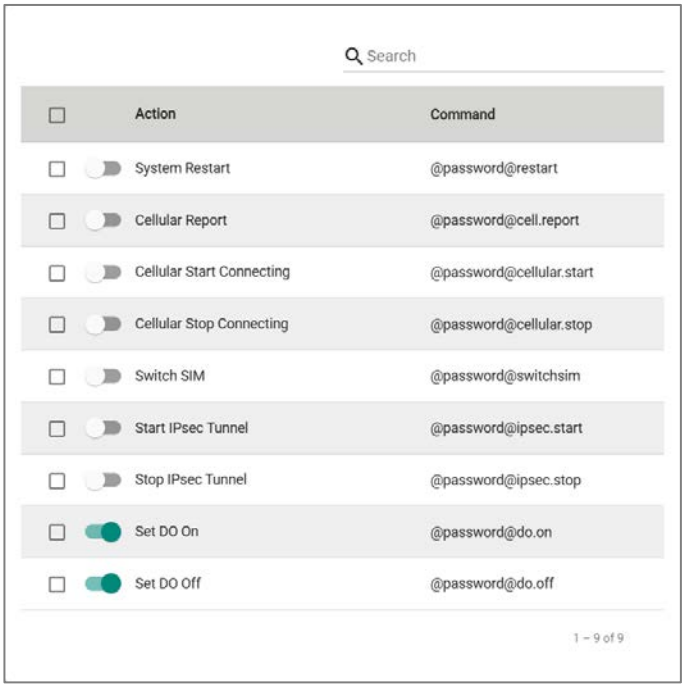
When sending remote control SMS messages to the device, wait 30 seconds between each message to ensure optimal system stability.

Remote Control List Settings

UI Setting	Description	Valid Range	Default Value
SMS Receipt	Enable or disable SMS receipts. If enabled, the device will send a reply SMS to the sender for confirmation after receiving a command SMS.	Enabled / Disabled	Enabled

Remote Control Command List

Use the toggle buttons to enable or disable the corresponding SMS command. Alternatively, check the boxes of the commands you want to manage and use the **Settings ( )** icon to enable or disable the selected commands. Refer to SMS Remote Control Commands for a list of available commands.



UI Setting	Description
Action	Shows the action the device will take when receiving the SMS command.
Command	Shows the text to use for the SMS command. When sending an SMS command to the device, replace `password` with the **Password** specified on the SMS - General page.

Send SMS

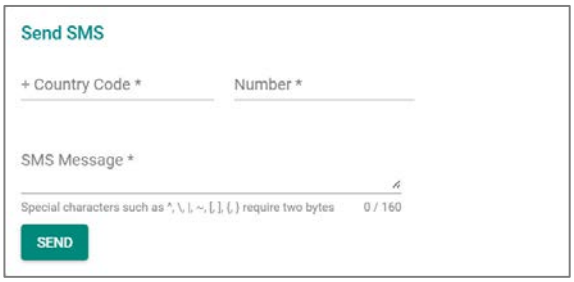
Menu Path: System > SMS - Send SMS

This page lets you send a custom SMS message from the device to a specified recipient, which can be useful for testing the device's SMS connection.

Input the required settings then select **SEND** to send the SMS message.

Note

Ensure your SIM card plan supports sending SMS messages before using this feature. If SMS service is unavailable on the SIM card, it may cause unexpected cellular communication errors. If this occurs, disable all SMS functions and restart the device to recover normal operation.



UI Setting	Description	Valid Range	Default Value
Country Code	Specify the country code of the recipient's phone number.	1 to 4 digits	N/A
Number	Specify the recipient's phone number.	1 to 15 digits	N/A
Message	Specify the text of the message to send.	1 to 160 characters	N/A

GNSS

Menu Path: System > GNSS

This page lets you configure the GNSS settings of your device.

> **Note**
> Availability of this feature may vary depending on your product model and version.

This page includes these tabs:

- General
- GNSS Client
- GNSS Server
- Status

GNSS - General

Menu Path: System > GNSS - General

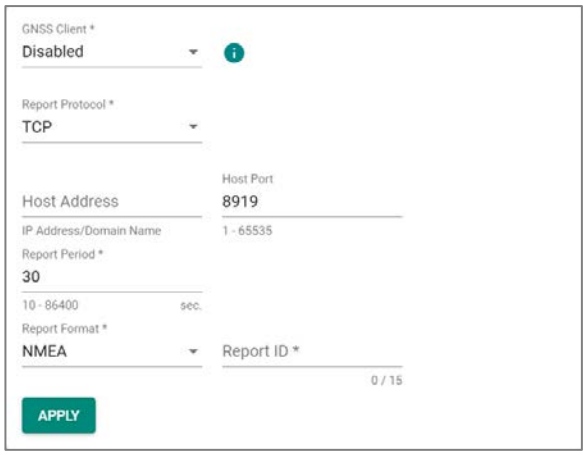
This page lets you enable or disable GNSS functionality.

UI Setting	Description	Valid Range	Default Value
GNSS	Enable or disable GNSS functionality. If enabled, the device will use satellite positioning to show its real-time physical location on a map. **Note** The cellular module must be enabled for this feature. Refer to Cellular for more information.	Enabled / Disabled	Enabled

GNSS Client

Menu Path: System > GNSS - GNSS Client

This page lets you configure GNSS client settings to allow the device to send GNSS data to a user-configured server.



UI Setting	Description	Valid Range	Default Value
GNSS Client	Enable or disable GNSS client functionality. If enabled, the device will send GNSS data to the configured server at the specified interval.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Report Protocol	Select the report protocol to use. • **TCP**: Send reports over TCP. This requires a receipt from the server to confirm the data was delivered. • **UDP**: Send reports over UDP. This does not require a receipt from the server.	TCP / UDP	TCP
Host Address	Specify the IP address or host name of the server that will receive the GNSS data.	Valid IP address	N/A
Host Port	Specify the TCP or UDP port number of the server that will receive the GNSS data.	1 to 65535	8919
Report Period	Specify the interval (in seconds) at which GNSS data reports are generated.	10 to 86400	30
Report Format	Select the report format to use. • **NMEA**: Send GNSS data in standard NMEA format. • **General**: Send GNSS data in latitude-longitude format.	NMEA / General	NMEA
Report ID	Enter the ID to use in the GNSS data report header. The Report ID and device MAC address will be included in both report formats.	1 to 15 characters	N/A

GNSS Server

Menu Path: System > GNSS - GNSS Server

This page lets you configure the the device to act as a GNSS server to allow clients to request GNSS data reports.

UI Setting	Description	Valid Range	Default Value
GNSS Server	Enable or disable GNSS server functionality. If enabled, clients will be able to request GNSS data reports from this server.	Enabled / Disabled	Disabled
Server Port	Specify the UDP port number for clients to access the server.	1 to 65535	8919
Report Period	Specify the interval in seconds at which GNSS data reports are generated.	10 to 86400	30
Report Format	Select the report format. • **NMEA**: Send GNSS data in standard NMEA format. • **General**: Send GNSS data in latitude-longitude format.	NMEA / General	NMEA
Report ID	Enter the ID to use in the GNSS data report header. The Report ID and device MAC address will be included in both report formats.	1 to 15 characters	N/A

GNSS - Status

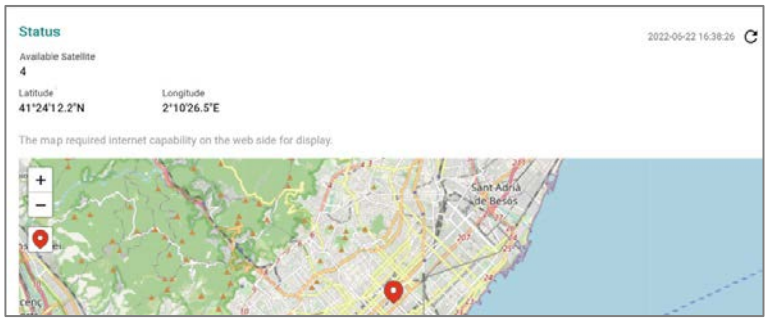
Menu Path: System > GNSS - Status

The Status screen shows the current geolocational information of the device, as well the device's current physical location on an interactive map.

Note

The device's physical location and coordinates will only appear if GNSS is enabled.

- Select the refresh icon ( ) to refresh the map.
- Select the **+** and **-** icons to zoom in and out of the map.
- Select the pin ( ) icon to center the map on the device's location.



UI Setting	Description
Available Satellite	Shows the number of available satellites to receive information from.
Latitude	Shows the north–south position of the device.
Longitude	Shows the east–west position of the device.

Setting Check

Menu Path: System > Setting Check

This page provides a double confirmation mechanism that allows you to verify configuration changes made by remote users before they are applied.

Setting Check Configuration

UI Setting	Description	Valid Range	Default Value
Layer 3-7 Policy	Enable or disable Setting Check for Layer 3-7 policy changes.	Enabled / Disabled	Disabled
Network Address Translate	Enable or disable Setting Check for NAT policy changes.	Enabled / Disabled	Disabled
Trusted Access	Enable or disable Setting Check for Trusted IP address changes.	Enabled / Disabled	Disabled
Timer	Set the time in seconds the user will have to confirm changes. If the user does not confirm the changes within the specified time period, the system will automatically undo the changes.	10 to 3600	180

Cellular

Menu Path: Cellular

This page lets you configure mobile network connection settings.

This page includes these tabs:

- General
- SIM Settings
- GuaranLink
- Status

> **Note**
> These features are only available on devices with cellular capabilities.

Cellular - User Privileges

Privileges to Cellular settings are granted to the different authority levels as follows.
Refer to User Accounts for more information on user accounts.

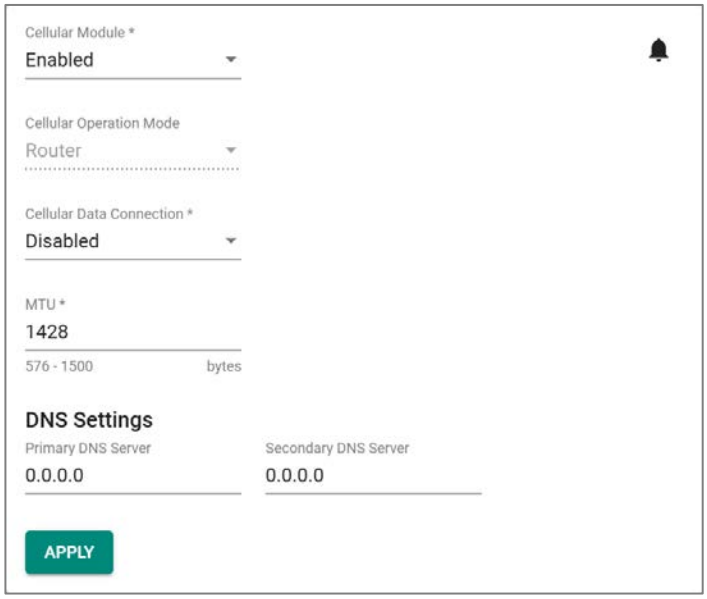
Settings	Admin	Supervisor	User
Cellular	R/W	R/W	R

Cellular - General

Menu Path: Cellular - General

This page lets you configure basic cellular settings for your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Cellular Module	Enable or disable the cellular module for establishing cellular connections, sending SMS messages, and using GNSS services.	Enabled / Disabled	Enabled
Cellular Operation Mode	The device will function as an IP router for IP data communication.	Router	Router
Cellular Data Connection	Enable or disable cellular data connections. If enabled, cellular connections may incur data usage costs based on your cellular service and ISP.	Enabled / Disabled	Enabled
MTU	Specify the Maximum Transmission Unit (MTU) value in bytes for router mode. The recommended MTU size may vary depending on the cellular carrier. Make sure the end device is set to the same MTU value for optimal performance.	576 to 1500	1428
Primary DNS Server	Specify the IP address of the primary DNS server used by your network.	Valid IP address	N/A
Secondary DNS Server	Specify the IP address of the secondary DNS server used by your network. The device will use the secondary DNS server if the primary DNS server fails to connect.	Valid IP address	N/A

SIM Settings

Menu Path: Cellular - SIM Settings

This section lets you enable or disable SIM cards and manage the SIM card settings including the priority, cellular bands, and authentication method.

Reordering SIM Card Priority

The device will always connect to the Internet using the SIM card designated with priority 1. The secondary SIM card will act as a redundant backup.

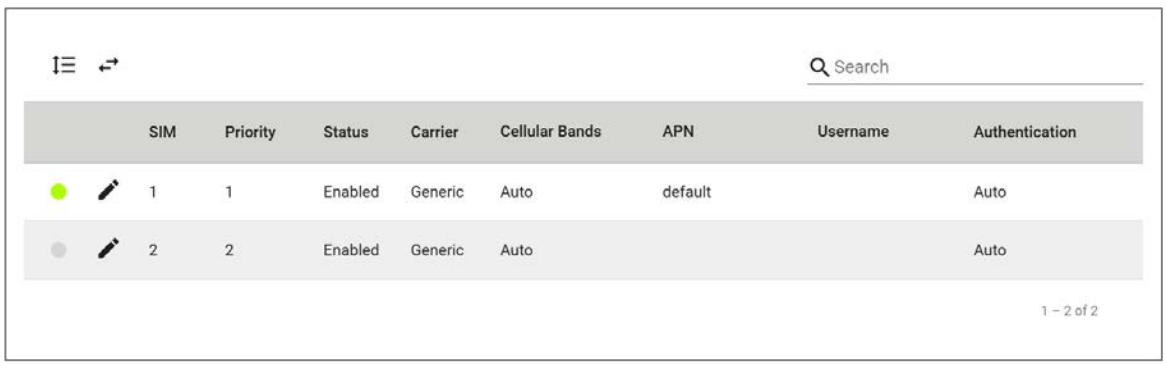
To change the priority of the SIM cards, click the **Reorder Priorities ( )** icon then click and drag the SIM card to the desired priority. Click the **Finish Reorder ( )** icon to confirm the change.

Changing the Active SIM Card

The green dot icon indicates the SIM card is active and connected to the Internet. By default, the SIM card designated with priority 1 will be used to connect to the Internet while the SIM with priority 2 acts as a backup.

If necessary, you can manually change the active SIM card. Click the **Change SIM ( )** icon to swap the active SIM card.

SIM Card List



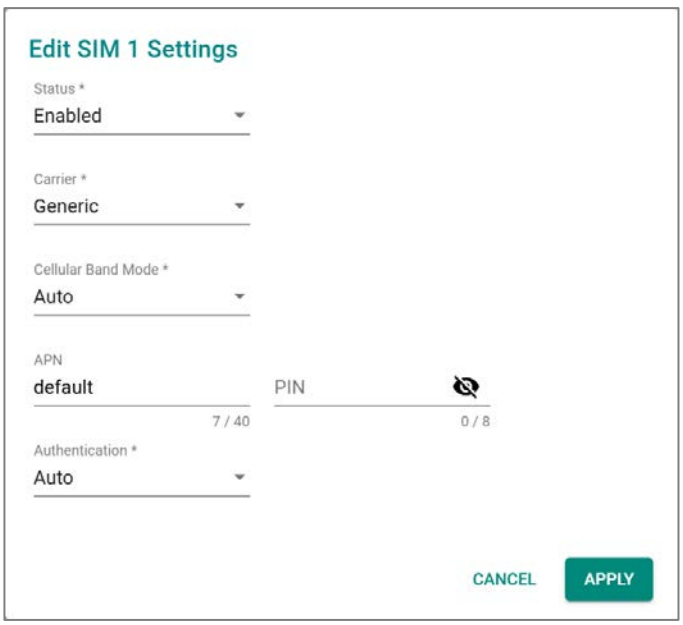
UI Setting	Description
SIM	Shows which SIM slot the entry is for.
Priority	Shows the priority of the SIM card.
Status	Shows the configured status of the SIM card.
Carrier	Shows the carrier for the SIM card.
Cellular Bands	Shows the cellular bands the SIM card will use.
APN	Shows the access point network (APN) information.
Username	Shows the username for PAP authentication.
Authentication	Shows the authentication method.

Edit SIM Settings

Menu Path: Cellular - SIM Card Settings

Clicking the **Edit ( )** icon for an entry on the **Cellular - SIM Card Settings** page will open this dialog box. This dialog lets you edit the settings for the SIM card.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the SIM card.	Enabled / Disabled	Enabled
Carrier	Select the carrier to use with the SIM card.	Generic	Generic
Cellular Band Mode	Select the cellular band mode. • **Auto**: The device will automatically negotiate the optimal cellular band frequency to use with the base station. • **Manual**: Manually specify the cellular band frequencies to use.	Auto / Manual	Auto
Cellular Bands **(If Cellular Band is Manual)**	Select the cellular bands to use. You can select multiple options. Available options depend on the product model.	Drop-down list of cellular bands	N/A
APN	Specify the access point network (APN) information provided by your cellular carrier if they require it.	0 to 40 characters	N/A
PIN	Enter the PIN number to unlock the SIM card. **Note** If you have already set up a PIN code, select CHANGE PIN to change the PIN. **Warning** SIM cards become permanently locked after 3 failed PIN attempts. To help prevent a SIM card from becoming locked, this device will stop making attempts when only 1 retry remains. • 2 attempts remaining: The device will proceed and attempt to use the new PIN. • 1 attempt remaining: The device will not attempt to use the new PIN. You must insert the SIM into a phone, enter the correct PIN to reset the retry counter, then re-insert it into this device. • 0 attempts remaining: The SIM is locked. Please contact your service provider for assistance. You can view PIN errors and the number of remaining attempts in the **System Log**.	0 to 8 characters	N/A

UI Setting	Description	Valid Range	Default Value
Authentication	Select the authentication method for the SIM card. • **Auto**: Set up a session without specifying the authentication method. • **PAP**: Use PAP (Password Authentication Protocol) authentication. PAP will send the username and password to the server for authentication against the server's database. • **CHAP**: Use CHAP (Challenge-Handshake Authentication Protocol) authentication. CHAP will generate a password which is changed frequently for improved identity security.	Auto / PAP / CHAP	Auto
Username **(If Authentication is PAP or CHAP)**	Specify the username for authentication.	0 to 32 characters	N/A
Password **(If Authentication is PAP or CHAP)**	Specify the password for authentication.	0 to 32 characters	N/A

GuaranLink

Menu Path: Cellular - GuaranLink

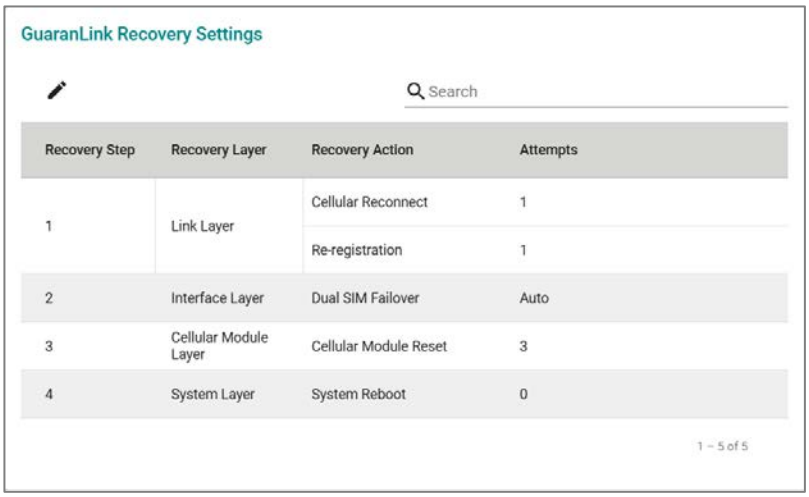
This page lets you set up Moxa's GuaranLink feature, which enables reliable connectivity with 3 different connection checks and 4 levels of recovery actions. A number of factors can contribute to connection failures in cellular communications, including loss of cellular signal, interference, connection errors caused by the base station, or termination by the operator for unknown reasons. GuaranLink is designed to address various needs, including minimizing cellular costs by optimizing the number of cellular packets sent to check connection status and optimizing the time it takes to swap to a backup SIM.

GuaranLink Settings

UI Setting	Description	Valid Range	Default Value
GuaranLink	Enable or disable GuaranLink. If enabled, the device will monitor cellular connections. If a connection failure is detected, the device will attempt to automatically recover the connection. **Note** Enabling this function will send additional alive check cellular messages, which may incur additional cellular costs.	Enabled / Disabled	Enabled
Check Time	Specify the check time. • **Always**: The device will constantly send out alive check packets to check for cellular connection issues. • **Idle Transmission**: The device will only send alive check packets when the device has not received any data transmissions during the specified Ping Interval period. • **Poor Signal**: The device will only send alive check packets when the device identifies poor signal quality.	Always / Idle Transmission / Poor Signal	Always
Ping Interval **(If Check Time is Always)**	Specify the interval in seconds at which the device will send out an alive check packet.	1 to 86400	10
Ping Interval **(If Check Time is Idle Transmission)**	Specify the interval in minutes the device will wait for data transmissions. If no data transmissions take place during the interval, the device will perform a connection alive check.	1 to 600	5

UI Setting	Description	Valid Range	Default Value
Signal Checking Interval **(If Check Time is Poor Signal)**	Specify the interval in minutes the device will check the host for poor signal quality. If the device detects poor signal quality from the host, the device will perform a connection alive check.	1 to 600	5
Ping Host 1 / 2	Enter the IP address or domain name of the remote host to ping. If both ping host 1 and 2 are configured, the device will perform connection alive checks for both hosts simultaneously. The device will only consider the connection to have failed if the device receives no response from both hosts.	Valid IP address / Domain name	N/A
Ping Failure Retry Times	Specify the number of times the device will perform the connection alive check. If the check fails the specified number of retry times, the device will determine that the cellular connection has failed and will initiate the GuaranLink recovery process.	1 to 10	3

GuaranLink Recovery Settings



UI Setting	Description
Recovery Step	Shows whiich recovery step the entry is for. When a connection fails, recovery steps will be attempted from the lowest step to the highest step.
Recovery Layer	Shows the architectural layer of the recovery step.
Recovery Action	Shows the recovery action that will be taken for the step.

UI Setting	Description
Attempts	Shows the number of times the action will be attempted before moving to the next step.

Edit Recovery Action Settings

Menu Path: Cellular - GuaranLink

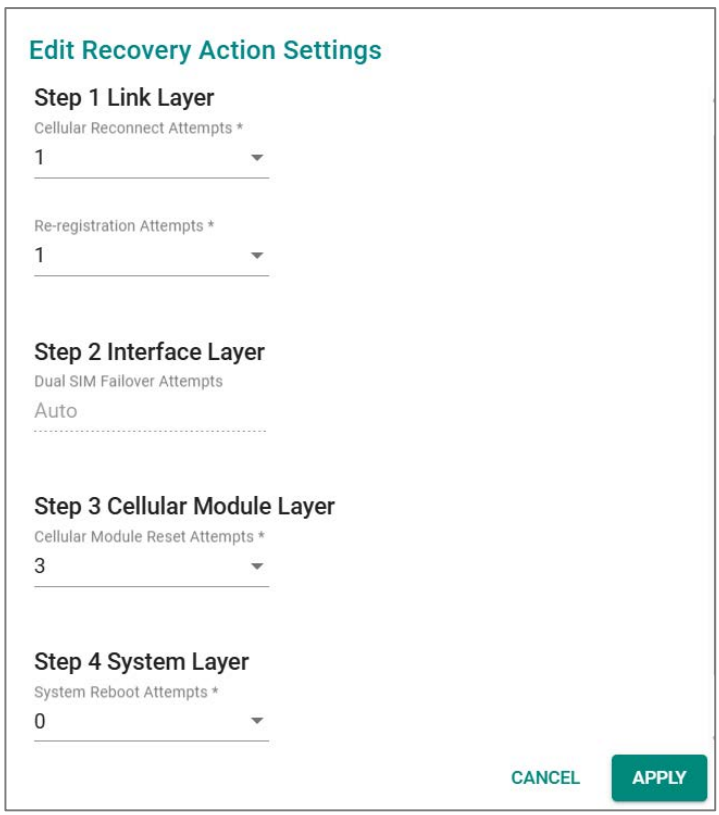
Clicking the **Edit ( )** icon for an action on the **Cellular - GuaranLink** page will open this dialog box. This dialog lets you specify the number of times to attempt each recovery action before moving to the next recovery action.

Click **APPLY** to save your changes.

Note

Upon disconnection, the device will automatically determine the appropriate method (Cellular Reconnect or Re-registration) to recover the link layer connection (Step 1).

- If one of these methods is set to 0, only the other method will be tried.
- If both methods are set to 0, the device will skip this entire step and move on to the next step (Step 2).



UI Setting	Description	Valid Range	Default Value
Cellular Reconnect Attempts	Specify the number of times the device will try to disconnect and re-establish the cellular connection before moving on to the next recovery step. If set to 0, the device will not use this method and will try the other method or move on to the next recovery step, depending on your settings.	0 to 5	1
Re-registration Attempts	Specify the number of times the device will try to re-register with the ISP to obtain a new IP address from the base station to re-establish the cellular connection before moving on to the next recovery step. If set to 0, the device will not use this method and will try the other method or move on to the next recovery step, depending on your settings.	0 to 5	1
Dual SIM Failover Attempts	If two SIM cards are inserted into the device, the device will attempt to use the other SIM card and restart the recovery process from step 1. If the connection is not restored after this, the device will move on to the next recovery step. If only one SIM card is inserted into the device, the device will move on to the next recovery step.	Auto	Auto
Cellular Module Reset Attempts	Specify the number of times the device will try to reset the cellular module to re-establish the cellular connection before moving on to the next recovery step. If set to 0, the device will skip this step and move on to the next recovery step.	0 to 10	3
System Reboot Attempts	Specify whether the device will reboot in order to re-establish the cellular connection before restarting the recovery process from step 1. If set to 0, the device will not perform a system reboot, and will restart the recovery process from step 1.	0 to 1	0

Cellular - Status

Menu Path: Cellular - Status

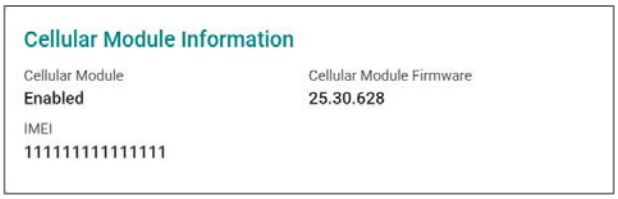
This section lets you see the current status of the cellular connection as well as information about the cellular carrier and SIM card, cellular module, and signal strength.

Cellular Status

This section shows you the cellular connection status of your device.

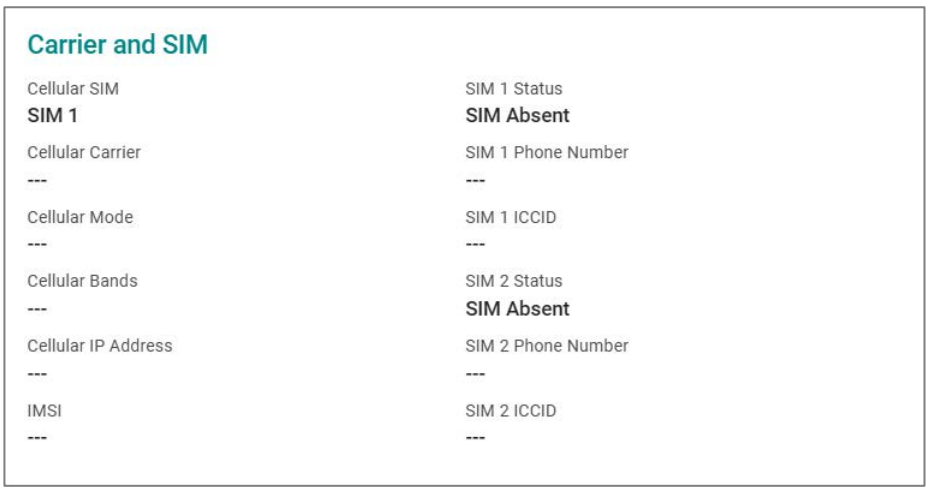
UI Setting	Description
SIM	Shows the status of the SIM card. • **Green**: The SIM card is active. • **Red**: The SIM card is inactive. • **Gray**: No SIM card inserted.
Signal	Shows the status of the device's cellular signal. • **Green**: Good cellular signal. • **Amber**: Fair cellular signal. • **Red:** Poor cellular signal. • **Gray**: No cellular signal.
Register	Shows the status of the device's cellular registration. • **Green**: The device successfully registered with the base station. • **Red**: The device failed to register with the base station. • **Gray**: The registration phase has not been reached yet.
Connection	Shows the status of the device's network connection. • **Green**: The device obtained an IP address from the base station. • **Red**: The device failed to obtain an IP address from the base station. • **Gray**: The connection phase has not been reached yet.
Internet	Shows the status of the device's Internet connection. • **Green**: The device is connected to the Internet. • **Red**: The device failed to connect to the Internet. • **Gray**: Alive checks are not being performed. **Note** GuaranLink must be enabled to perform connection alive checks. Refer to GuaranLink for more information.

Cellular Module Information



UI Setting	Description
Cellular Module	Shows the current status of the cellular module.
Cellular Module Software	Shows the firmware version of the cellular module.
IMEI	Shows the International Mobile Equipment Identity (IMEI) number of the cellular module.

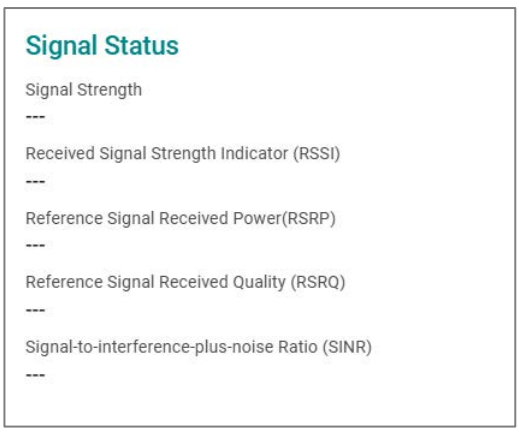
Carrier and SIM



UI Setting	Description
Cellular SIM	Shows the SIM card used for establishing the cellular connection.
Cellular Carrier	Shows the cellular service provider being used.
Cellular Mode	Shows the cellular connection technology being used, such as LTE or HSPA.
Cellular Band	Shows the cellular band frequency being used.

UI Setting	Description
Cellular IP Address	Shows the cellular IP address assigned by the cellular carrier.
IMSI	Shows the International Mobile Subscriber Identity number.
SIM 1 Status	Shows the status of the SIM card installed in SIM slot 1.
SIM 1 Phone Number	Shows the phone number of the SIM card in SIM slot 1.
SIM 1 ICCID	Shows the Integrated Circuit Card ID of the SIM card in SIM slot 1.
SIM 2 Status	Shows the status of the SIM card installed in SIM slot 2.
SIM 2 Phone Number	Shows the phone number of the SIM card in SIM slot 2.
SIM 2 ICCID	Shows the Integrated Circuit Card ID of the SIM card in SIM slot 2.

Signal Status



UI Setting	Description
Signal Strength	Shows the current overall signal strength of the device.
RSRP (Reference Signal Received Power)	Shows the current RSRP. • **Good**: Higher than -80 dBm • **Average**: -80 to -90 dBm • **Poor**: -90 to -100 dBm • **Inadequate**: Less than-100 dBm

UI Setting	Description
RSSI (Received Signal Strength Indicator)	Shows the current RSSI. • **Good**: Higher than -73 dBm • **Average**: -73 to -89 dBm • **Poor**: -89 to -113 dBm • **Inadequate**: Less than -113 dBm
RSRQ (Reference Signal Received Quality)	Shows the current RSRQ. • **Good**: Higher than -10 dB • **Average**: -10 to -15 dB • **Poor**: -15 to -20 dB • **Inadequate**: Less than -20 dB
SINR (Signal to Interference and Noise Ratio)	Shows the current SINR. • **Good**: Higher than 20 dB • **Average**: 13 to 20 dB • **Poor**: 0 to 13 dB • **Inadequate**: Less than 0 dB

Serial

Menu Path: Serial

This page lets you configure your device's serial settings.

> **Note**
> Availability of this feature may vary depending on your product model and version.

This settings area includes these sections:

- Serial Device Server
- SCATS

Serial - User Privileges

Privileges to Serial settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Serial Device Server	R/W	R/W	R
SCATS	R/W	R/W	R

Serial Device Server

Menu Path: Serial > Serial Device Server

This page lets you configure your device's serial settings.

> **Note**
> Availability of this feature may vary depending on your product model and version.

This page includes these tabs:

- Operation Mode
- Port Settings

- Data Packing
- Status
- Serial Data Logs

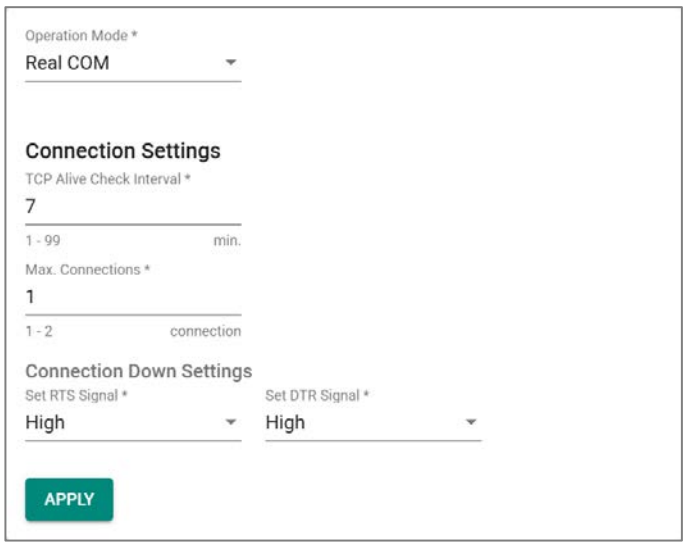
Operation Mode

Menu Path: Serial > Serial Device Server - Operation Mode

This page lets you set up and configure a serial operation mode. Refer to Serial Operation Modes for more information about the different modes.

Operation Mode - Real COM

If you select **Real COM** as your **Operation Mode**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Operation Mode	Select the operation mode for the serial device server. Available settings will change based on the selected mode.	Disabled / Real COM / RFC 2217 / TCP Server / TCP Client / UDP	Disabled

Connection Settings

UI Setting	Description	Valid Range	Default Value
TCP Alive Check Interval	Specify the interval in minutes at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any “keep alive” packets. **Note** Disabling this option can help free up device resources.	1 to 99	7
Max. Connections	Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.	1 to 2	1

Connection Down Setings

UI Setting	Description	Valid Range	Default Value
Set RTS Signal	Select the RTS signal method to use. • **High**: The cellular or Ethernet connection status will not affect RTS signals. • **Low**: If the cellular or Ethernet connection is lost, RTS signals will change to low.	High / Low	High
Set DTR Signal	Select the DTR signal method to use. • **High**: The cellular or Ethernet connection status will not affect DTR signals. • **Low**: If the cellular or Ethernet connection is lost, DTR signals will change to low.	High / Low	High

Operation Mode - RFC 2217

If you select **RFC 2217** as your **Operation Mode**, these settings will appear.

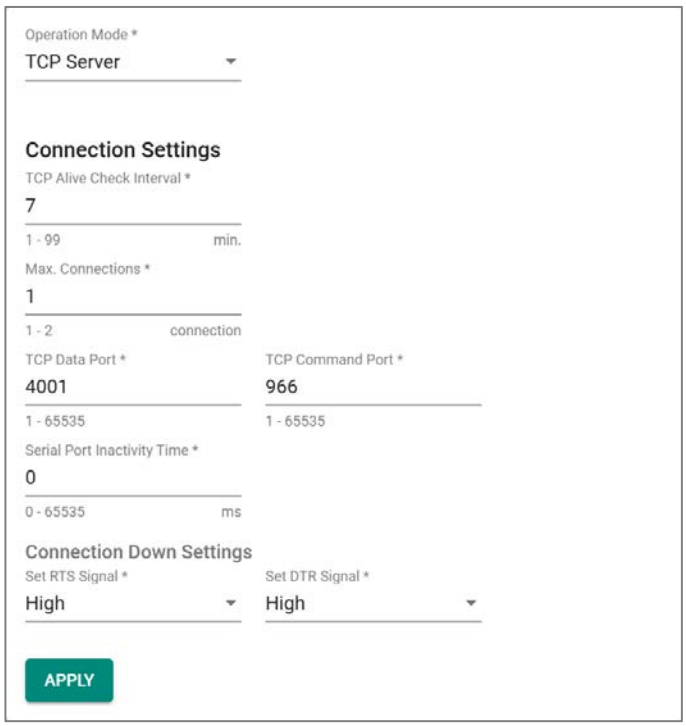
UI Setting	Description	Valid Range	Default Value
Operation Mode	Select the operation mode for the serial device server. Available settings will change based on the selected mode.	Disabled / Real COM / RFC 2217 / TCP Server / TCP Client / UDP	Disabled

Connection Settings

UI Setting	Description	Valid Range	Default Value
TCP Alive Check Interval	Specify the interval in minutes at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any “keep alive” packets. **Note** Disabling this option can help free up device resources.	1 to 99	7
TCP Data Port	Specify the TCP port number for the serial port used to listen to connections and for other devices to contact. To avoid conflicts with well-known TCP ports, the default port is 4001.	1 to 65535	4001

Operation Mode - TCP Server

If you select **TCP Server** as your **Operation Mode**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Operation Mode	Select the operation mode for the serial device server. Available settings will change based on the selected mode.	Disabled / Real COM / RFC 2217 / TCP Server / TCP Client / UDP	Disabled

Connection Settings

UI Setting	Description	Valid Range	Default Value
TCP Alive Check Interval	Specify the interval in minutes at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any “keep alive” packets. **Note** Disabling this option can help free up device resources.	1 to 99	7
Max. Connections	Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.	1 to 2	1

UI Setting	Description	Valid Range	Default Value
TCP Data Port	Specify the TCP port number for the serial port used to listen to connections and for other devices to contact. To avoid conflicts with well-known TCP ports, the default port is 4001.	1 to 65535	4001
TCP Command Port	Specify the TCP port number for MOXA IP-Serial Library commands. **Note** It is not necessary to reference this port number in your application when using the Moxa IP-Serial Library since the library automatically obtains the number from the device server. Only change this setting if there is a port number conflict with another application or device.	1 to 65535	9006
Serial Port Inactivity Time	Specify the time limit in milliseconds to keep the connection open if there is no data going to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity. For many applications, this option should be set to 0, as the serial device may be idle for long periods of time. **Warning** Serial Port Inactivity Time setting should be greater than the Force Transmit Interval in Data Packing settings. Otherwise, the connection may be closed before the data in the buffer can be transmitted. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.	1 to 65535	0

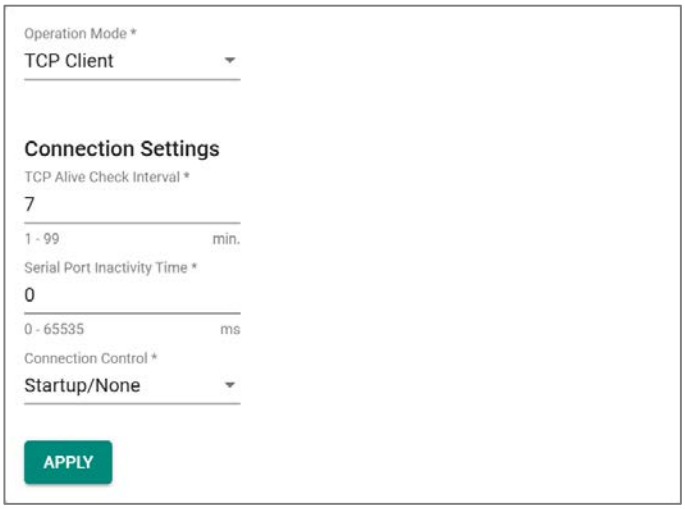
Connection Down Setings

UI Setting	Description	Valid Range	Default Value
Set RTS Signal	Select the RTS signal method to use. • **High**: The cellular or Ethernet connection status will not affect RTS signals. • **Low**: If the cellular or Ethernet connection is lost, RTS signals will change to low.	High / Low	High

UI Setting	Description	Valid Range	Default Value
Set DTR Signal	Select the DTR signal method to use. • **High**: The cellular or Ethernet connection status will not affect DTR signals. • **Low**: If the cellular or Ethernet connection is lost, DTR signals will change to low.	High / Low	High

Operation Mode - TCP Client

If you select **TCP Client** as your **Operation Mode**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Operation Mode	Select the operation mode for the serial device server. Available settings will change based on the selected mode.	Disabled / Real COM / RFC 2217 / TCP Server / TCP Client / UDP	Disabled

Connection Settings

UI Setting	Description	Valid Range	Default Value
TCP Alive Check Interval	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any “keep alive” packets. **Note** Disabling this option can help free up device resources.	1 to 99	7
Serial Port Inactivity Time	Specify the time limit in milliseconds to keep the connection open if there is no data going to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity. For many applications, this option should be set to 0, as the serial device may be idle for long periods of time. **Note** The serial port inactivity time is only applied when the Connection Control option is set to Any Character/Inactivity Time. **Warning** **Serial Port Inactivity Time** setting should be greater than the **Force Transmit Interval** in **Data Packing** settings. Otherwise, the connection may be closed before the data in the buffer can be transmitted. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.	1 to 65535	0

UI Setting	Description	Valid Range	Default Value
Connection Control	Select a connection control method. • **Startup / None**: A TCP connection will be established on startup and will remain active indefinitely. • **Any Character / None**: A TCP connection will be established when any character is received from the serial interface and will remain active indefinitely. • **Any Character / Inactivity Time**: A TCP connection will be established when any character is received from the serial interface and will be disconnected after the specified Serial Port Inactivity Time. • **DSR On / DSR Off**: A TCP connection will be established when a DSR "On" signal is received and will be disconnected when a DSR "Off" signal is received. • **DSR On / None**: A TCP connection will be established when a DSR "On" signal is received and will remain active indefinitely. • **DCD On / DCD Off**: A TCP connection will be established when a DCD "On" signal is received and will be disconnected when a DCD "Off" signal is received. • **DCD On / None**: A TCP connection will be established when a DCD "On" signal is received and will remain active indefinitely.	Startup/None / Any Character/None / Any Character/Inactivity Time / DSR On/DSR Off / DSR On/None / DCD On/DCD Off / DCD On/None	Startup/None

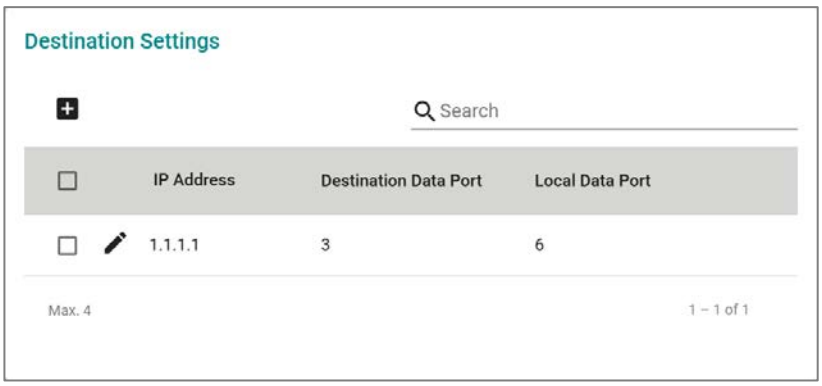
TCP Client - Destination Settings

Limitations

You can create up to 4 TCP client destination entries.

⚠ Warning

Though up to 4 TCP client destination entries are supported, a low connection speed or throughput on one of the connections will affect the performance of the other active connections.



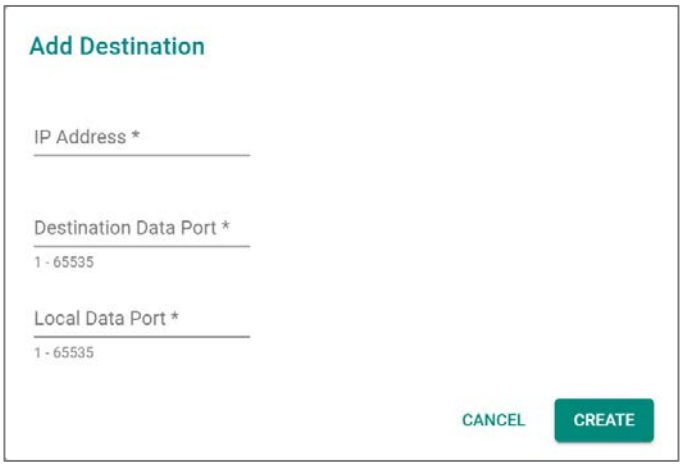
UI Setting	Description
IP Address	Shows the IP address of the remote host.
Destination Data Port	Shows the TCP port number of the remote host.
Local Data Port	Shows the designated local port.

Add a Destination Entry (TCP Client)

Menu Path: Serial > Serial Device Server - Operation Mode (TCP Client)

Clicking the **Add (⊞)** icon on the **Serial > Serial Device Server - Operation Mode (TCP Client)** page will open this dialog box. This dialog lets you add a destination entry.

Click **CREATE** to save your changes and add the new entry.

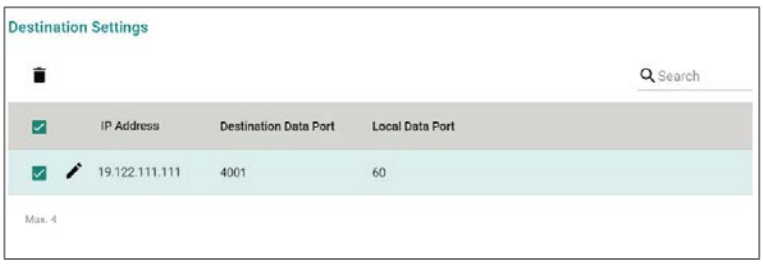


UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the remote host.	Valid IP address	N/A
Destination Data Port	Specify the TCP port number of the remote host.	1 to 65535	N/A
Local Data Port	Specify a designated local port.	1 to 65535	N/A

Delete a Destination Entry (TCP Client)

Menu Path: Serial > Serial Device Server - Operation Mode (TCP Server)

You can delete a destination entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Operation Mode - UDP

If you select **UDP** as your **Operation Mode**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Operation Mode	Select the operation mode for the serial device server. Available settings will change based on the selected mode.	Disabled / Real COM / RFC 2217 / TCP Server / TCP Client / UDP	Disabled

Connection Settings

UI Setting	Description	Valid Range	Default Value
UDP Data Port	Enter the UDP port number for contacting the serial device.	1 to 65535	4001

UDP - Destination Settings

Limitations

You can create up to 4 UDP destination entries.

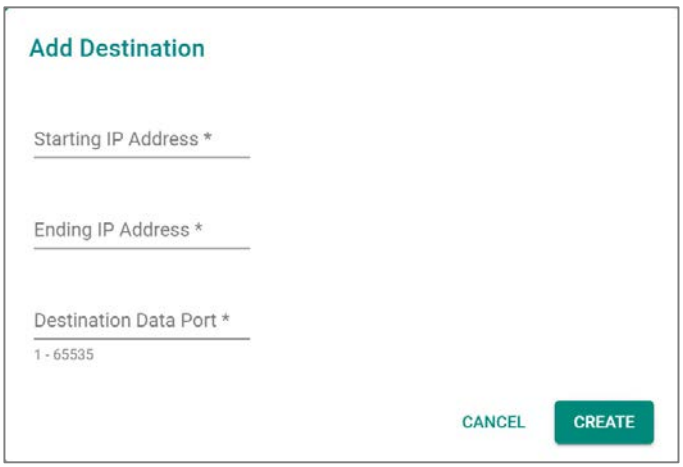
UI Setting	Description
Starting IP Address	Shows the starting IP address of the remote host IP range.
End IP Address	Shows the ending IP address of the remote host IP range.
Destination Data Port	Shows the UDP port number of the remote host.

Add a Destination Entry (UDP)

Menu Path: Serial > Serial Device Server - Operation Mode (UDP)

Clicking the **Add (⊕)** icon on the **Serial > Serial Device Server - Operation Mode (UDP)** page will open this dialog box. This dialog lets you add a destination entry.

Click **CREATE** to save your changes and add the new entry.

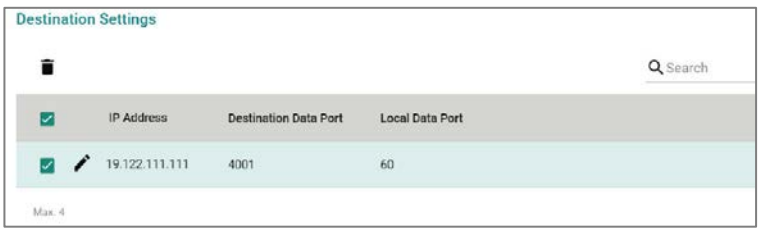


UI Setting	Description	Valid Range	Default Value
Starting IP Address	Enter the starting IP address of the remote host IP range. **Note** The maximum IP address range size is 64 addresses. However, when using multicast, you may enter IP addresses in the form xxx.xxx.xxx.255 in the Starting IP Address field. For example, enter 192.168.127.255 to allow the system to broadcast UDP packets to all hosts with IP addresses between 192.168.127.1 and 192.168.127.254.	Valid IP address, IP addresses in the form xxx.xxx.xxx.255 are allowed	N/A
End IP Address	Enter the ending IP address of the remote host IP range.	Valid IP address	N/A
Destination Data Port	Enter the UDP port number of the remote host.	1 to 65535	N/A

Delete a Destination Entry (UDP)

Menu Path: Serial > Serial Device Server - Operation Mode (UDP)

You can delete a destination entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



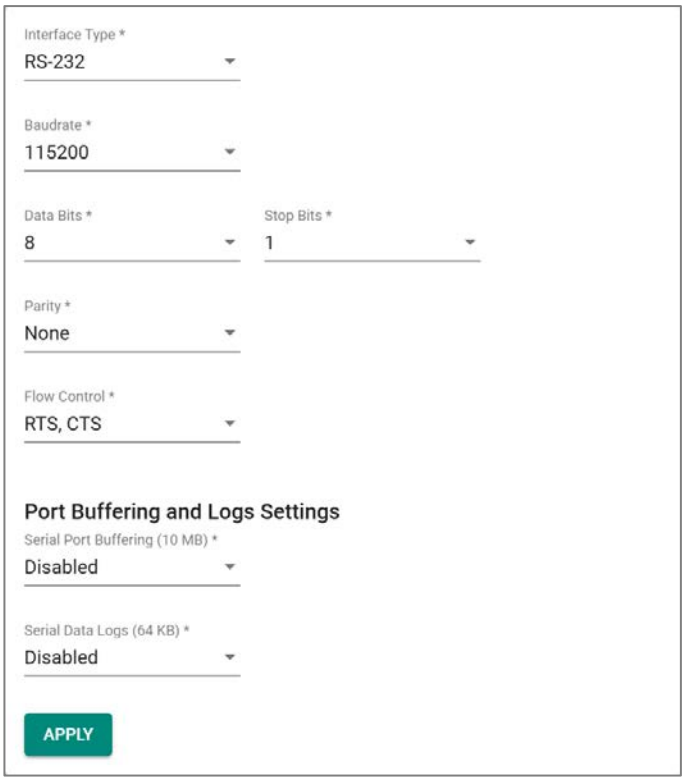
Serial - Port Settings

Menu Path: Serial > Serial Device Server - Port Settings

This page lets you enable or disable the serial port and configure the serial communication parameters. When enabled, the device allows for traditional serial (RS-232/422/485) devices to transmit data over the cellular network.

Note

The serial port settings on the device should match the parameters configured for the connected serial device. Refer to your serial device's user manual to determine the appropriate serial communication parameters.



UI Setting	Description	Valid Range	Default Value
Interface Type	Select the serial interface type to use for the serial device.	RS-232 / RS-422 / 2-wire-RS-485/ 4-wire-RS-485	RS-232
Baudrate	Specify the data transmission rate to and from the serial device.	300 / 600 / 1200 / 1800 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 / 460800 / 921600	115200
Data Bits	Specify the size for data characters.	5 to 8	8
Stop Bits	Specify the size for stop characters.	1 / 1.5 / 2	1
Parity	Select the parity mode. Even and odd parity provide rudimentary error-checking.	None / Odd / Even	None

UI Setting	Description	Valid Range	Default Value
Flow Control	Select the flow control method. This determines how the system will suspend and resume data transmissions to prevent data loss. RTS, CTS (hardware) flow control is recommended.	None / RTS, CTS / XON, XOFF	RTS, CTS

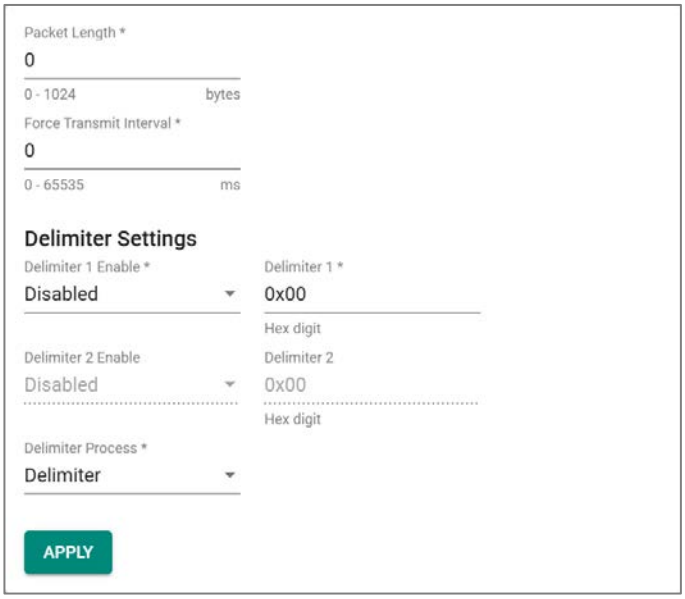
Port Buffering and Logs Settings

UI Setting	Description	Valid Range	Default Value
Serial Port Buffering (10 MB)	Enable or disable serial port buffering. When enabled, if the WAN connection goes down, the router will keep the serial data and retransmit the buffered data when the WAN connection is back. If disabled, serial data will be lost if the WAN connection goes down. **Note** • Port buffering can be used in Real COM, RFC 2217, TCP Server, and TCP Client modes. • For other modes, the port buffering settings will have no effect. • The maximum buffer size is 10 MB. • Buffer data exceeding 10 MB will overwrite previous data.	Enabled / Disabled	Disabled
Serial Data Logs (64 KB)	Enable or disable serial data logs. If enabled, the router will store the serial data logs in system RAM. **Note** The device's system RAM can save up to 64 kb of serial data logs. Serial log data will be cleared when the router is powered off.	Enabled / Disabled	Disabled

Data Packing

Menu Path: Serial > Serial Device Server - Data Packing

This page lets you configure the conditions and delimiter settings for serial port data buffering and transmission.



UI Setting	Description	Valid Range	Default Value
Packet Length	Specify the Packet Length in bytes for the serial port buffer. The packet length refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. • At the default packet length of 0, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. • If a packet length of 1 to 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.	0 to 1024	0
Force Transmit Interval	Specify the interval in milliseconds to force transmission of serial port data if no activity is recorded. This setting controls data packing by the amount of time that elapses between bits of data. As serial data is received, it accumulates in the device port's buffer. If serial data is not received for the specified amount of time, the data that is currently in the buffer is packed for network transmission. A setting of 0 means that data in the buffer will not be automatically packed when additional data is not received from the device.	0 to 65535	0

Delimiter Settings

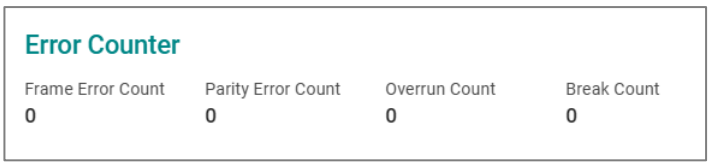
UI Setting	Description	Valid Range	Default Value
Delimiter 1/2 Enable	Enable or disable delimiter 1 or 2. • **Enabled**: The serial port will queue data in the buffer and send it to the cellular or Ethernet port when a specific hex character is received. When both Delimiter 1 and 2 are enabled and specified, both of them will be used to control when data should be sent. • **Disabled**: The serial port will not check for specific characters for data transmission. **Note** When Delimiter is enabled, we recommend setting the Packet Length to 0 to ensure serial data output is as expected. **Note** **Delimiter 2** can only be used when **Delimiter 1** is enabled. When there is only one Delimiter to set, use **Delimiter 1**.	Disabled / Enabled	Disabled
Delimiter 1/2	Specify the character that acts as the delimiter to control when data should be sent. **Note** When the device port buffer is full, the data will be packed for network transmission regardless of the Delimiter 1, Delimiter 2, and Force Transmit Interval settings.	0x00 to 0xFF	0x00
Delimiter Process	Select the delimiter process. • **Delimiter**: Data in the buffer will be transmitted when the delimiter is received. • **Delimiter +1**: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter. • **Delimiter +2**: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter. • **Strip Delimiter**: Data in the buffer is stripped of the delimiter before being transmitted.	Delimiter / Delimiter +1 / Delimiter +2 / Strip Delimiter	Delimiter

Serial - Status

Menu Path: Serial > Serial Device Server - Status

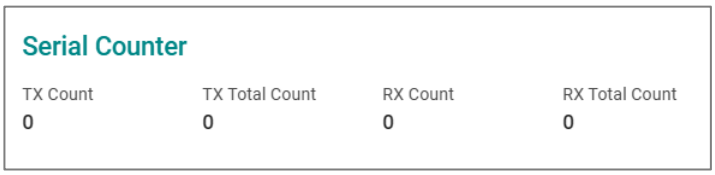
This page lets you see detailed statistics and information about the serial port data and connections.

Error Counter



UI Setting	Description
Frame Error Count	Shows the number of frame errors since the device was powered on.
Parity Error Count	Shows the number of parity errors since the device was powered on.
Overrun Count	Shows the number of overrun errors since the device was powered on.
Break Count	Shows the number of break errors since the device was powered on.

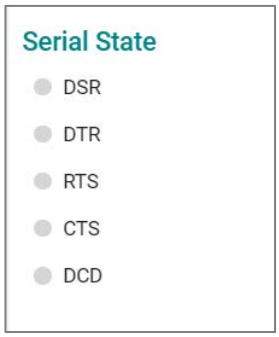
Serial Counter



UI Setting	Description
TX Count	Shows the number of packets transmitted.
TX Total Count	Shows the total total number of packets transmitted since the device was powered on.
RX Count	Shows the number of packets received.

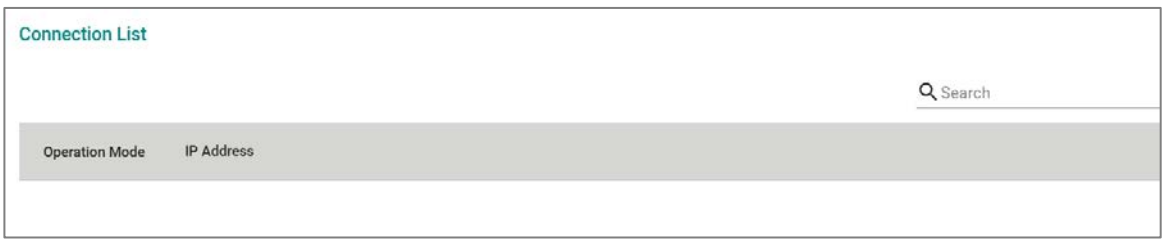
UI Setting	Description
RX Total Count	Shows the total total number of packets received since the device was powered on.

Serial State



UI Setting	Description
Serial State	Shows the status of the serial signal. • **Green**: The signal pins are connected. • **Grey**: The signal pins are disconnected.

Serial - Connection List



UI Setting	Description
Operation Mode	Shows the operation mode for the connection.
IP Address	Shows the IP address of the connection.

Serial Data Logs

Menu Path: Serial > Serial Device Server - Serial Data Logs

This page lets you see the device's serial data logs in ASCII or HEX format.

- Click the **Refresh icon ( )** icon to refresh the serial data logs.
- Click the **Clear Data Log icon ( )** icon to delete all serial data logs.
- Click the **Export icon ( )** icon to export all serial data logs to a file.
- Click **ASCII** or **HEX** to change the format of the logs.

SCATS

Menu Path: Serial > SCATS

This page lets you configure your device's SCATS (Sydney Coordinated Adaptive Traffic System) settings.

> **Note**
> Availability of this feature may vary depending on your product model and version.

This page includes these tabs:

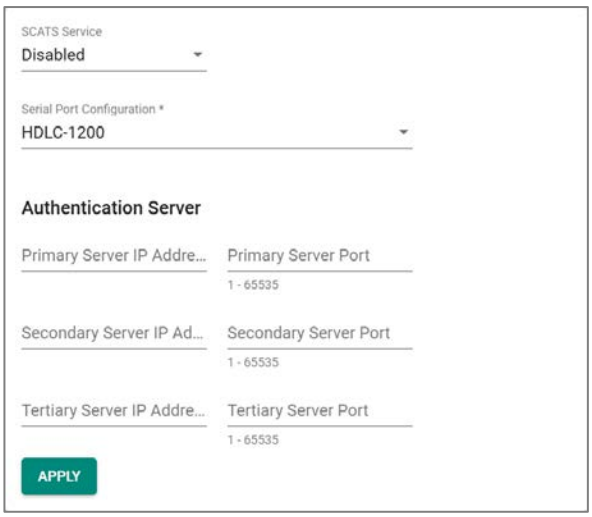
- Settings
- Status

SCATS - Settings

Menu Path: Serial > SCATS - Settings

This page lets you configure the SCATS settings for your device.

SCATS Settings



UI Setting	Description	Valid Range	Default Value
SCATS Service	Enable or disable the SCATS service. When enabled, the device will transmit serial traffic controller information to a SCATS traffic signal management system.	Disabled / Enabled	Disabled

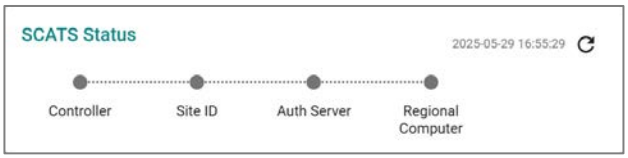
UI Setting	Description	Valid Range	Default Value
Serial Port Configuration	Select one or more serial port configurations to use for the connected traffic signal controller. • **HDLC-1200:** HDLC (High-Level Data Link Control) protocol with a 1200 baud rate. • **Non-HDLC-1200:** Non-HDLC (raw or custom protocol) communication at 1200 baud rate. • **HDLC-9600:** HDLC (High-Level Data Link Control) protocol with a 9600 baud rate. • **Non-HDLC-300:** Non-HDLC (raw or custom protocol) communication at 300 baud rate. **Note** If multiple options are selected, the device will automatically negotiate and use the first compatible configuration when establishing a connection. The negotiation order of the configurations is HDLC-1200 > Non-HDLC-1200 > HDLC-9600 > Non-HDLC-300.	HDLC-1200 / Non-HDLC-1200 / HDLC-9600 / Non-HDLC-300	HDLC-1200
Primary/Secondary/Tertiary Server IP Address	Enter the IP address of the primary/secondary/tertiary SCATS authentication server.	Valid IP address	N/A
Primary/Secondary/Tertiary Server Port	Specify the TCP port number of the primary/secondary/tertiary SCATS authentication server.	1 to 65535	N/A

SCATS - Status

Menu Path: Serial > SCATS - Status

This page lets you see the status of your device's SCATS function.

SCATS Status

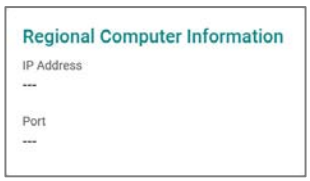


UI Setting	Description
Controller	Shows the connection status with the Traffic Signal Controller. • **Green**: The device successfully connected to the Traffic Signal Controller. • **Red**: The device failed to connect to the Traffic Signal Controller. • **Gray**: SCATS is disabled.
Site ID	Shows the status of obtaining a Traffic Control Site ID from the Traffic Signal Controller. • **Green**: The device successfully obtained a Traffic Control Site ID from the Traffic Signal Controller. • **Red:** The device failed to obtain a Traffic Control Site ID from the Traffic Signal Controller. • **Gray**: This phase has not been reached yet.
Auth Server	Shows the status of obtaining information from the authentication server. • **Green**: The device successfully obtained the IP and port information of the Regional Computer from the Authentication Server. • **Red**: The device failed to obtain the IP and port information of the Regional Computer from the Authentication Server. • **Gray**: This phase has not been reached yet.
Regional Computer	Shows the connection status with the Regional Computer. • **Green**: The device successfully connected to the Regional Computer. • **Red**: The device failed to connect to the Regional Computer. • **Gray**: This phase has not been reached yet.

Controller Information

UI Setting	Description
Site ID	Shows the Traffic Control Site ID of the Traffic Signal Controller.
Serial Port Configuration	Shows the serial communication protocol and baud rate for the connected Traffic Signal Controller.

Regional Computer Information



UI Setting	Description
IP Address	Shows the IP address of the Regional Computer.
Port	Shows the port of the Regional Computer.

Network Configuration

Menu Path: Network Configuration

The Network Configuration settings area lets you configure settings related to your device's networking ports.

This settings area includes these sections:

- Ports
- Layer 2 Switching
- Network Interfaces

Network Configuration - User Privileges

Privileges to Network Configuration settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Ports			
Port Settings	R/W	R/W	R
Link Aggregation	R/W	R/W	R
Link Fault Passthrough	R/W	R/W	R
LAN Bypass Gen3	R/W	R/W	R
PoE	R/W	R/W	R
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS	R/W	R/W	R
Rate Limit	R/W	R/W	R

Settings	Admin	Supervisor	User
Multicast	R/W	R/W	R
IGMP Snooping	R/W	R/W	R
Static Multicast Table	R/W	R/W	R
Network Interfaces	R/W	R/W	R

Ports

Menu Path: Network Configuration > Ports

This section includes these pages:

- Port Settings
- Link Aggregation
- Link Fault Passthrough
- LAN Bypass Gen3
- PoE

Port Settings

Menu Path: Network Configuration > Ports > Port Settings

This page includes these tabs:

- Settings
- Status

Port Settings - Settings

Menu Path: Network Configuration > Ports > Port Settings - Settings

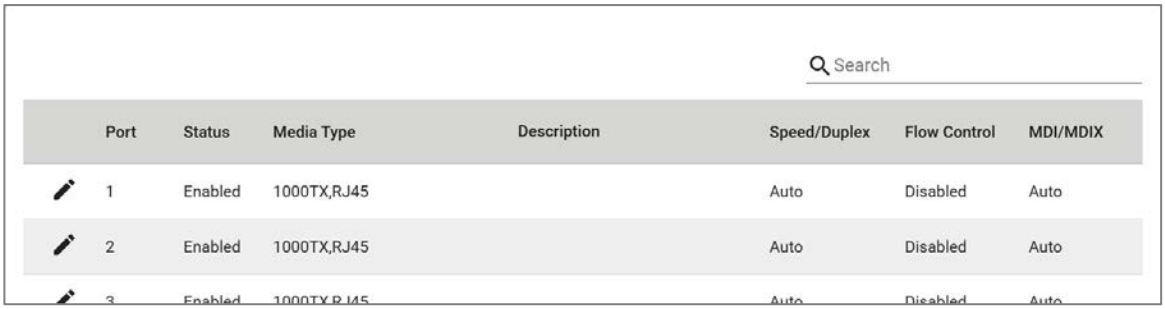
This page lets you view and adjust the settings for each port.

Edit Port Settings

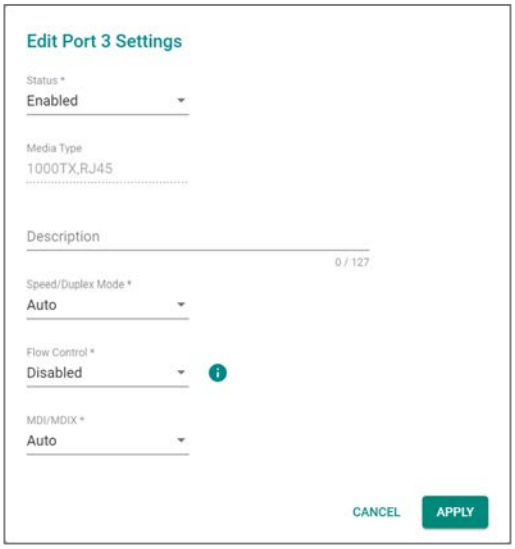
Menu Path: Network Configuration > Ports > Port Settings - Settings

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Ports > Port Settings - Settings** page will open this dialog box. This dialog lets you change the settings for a port.

Click **APPLY** to save your changes.



UI Setting	Description
Port	Shows which port this row describes.
Status	Shows the status of the port.
Media Type	Shows the port's media type.
Description	Shows the description for the port.
Speed/Duplex	Shows the speed and duplex mode for the port.
Flow Control	Shows the whether flow control is enabled or disabled for the port.
MDI/MDIX	Shows the MDI/MDIX setting for the port.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the port.	Enabled / Disabled	Enabled
Media Type	Displays the port's media type. This setting cannot be changed.	N/A	Port's media type
Description	Enter a description for the port to make it easier to identify.	1 to 127 characters	N/A
Speed / Duplex	Select the speed and duplex mode for the port. • **Auto**: Allows the port to use IEEE 802.3u protocol to negotiate the best port speed and duplex mode to use for the connected device. • **100M-Full**: This will force the port to connect using 100 Mbps at full-duplex. • **100M-Half**: This will force the port to connect using 100 Mbps at half-duplex. • **10M-Full**: This will force the port to connect using 10 Mbps at full-duplex. • **10M-Half**: This will force the port to connect using 10 Mbps at half-duplex.	Auto / 100M-Full /100M-Half / 10M-Full / 10M-Half	Auto

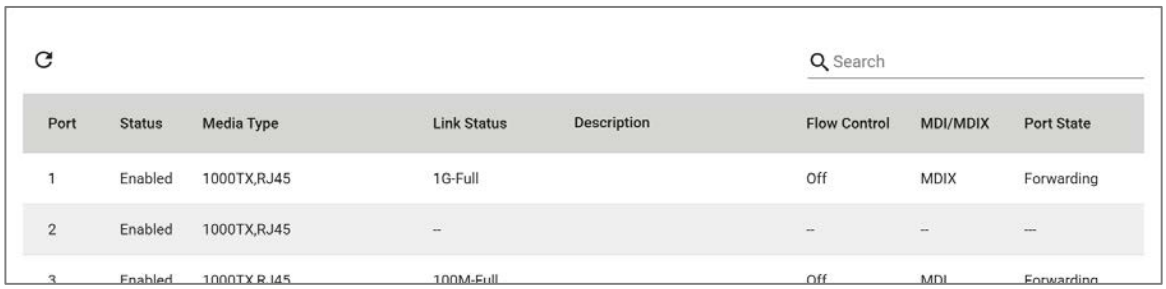
UI Setting	Description	Valid Range	Default Value
Flow Control	Enable or disable flow control for this port when the port's **Speed / Duplex** setting is set to **Auto**. Flow control helps manage the data transfer rate between the device and the connected Ethernet devices. **Note** Flow Control can be enabled or disabled but is only effective in full-duplex. Back Pressure is enabled by default but works only in half-duplex. When using the SFP ports for WAN1 or WAN2 on the EDR-G9004, Flow Control will be ineffective. **Note** If **Speed / Duplex** is set to something other than **Auto**, **Flow Control** will be disabled.	Enabled / Disabled	Disabled
MDI / MDIX	Select whether the port should use MDI or MDIX. The correct setting depends on both the connected device and the cabling used to connect to the device. • **Auto**: Allow the port to auto-detect whether to use MDI or MDIX for connected devices. • **MDI**: Force the port to use MDI (also known as "straight-through"). • **MDIX**: Force the port to use MDIX (also known as "crossover"). **Note** Only choose MDI or MDIX if your connected Ethernet device has trouble auto-negotiating the correct port type.	Auto / MDI / MDIX	Auto

Port Settings - Status

Menu Path: Network Configuration > Ports > Port Settings - Status

This page lets you monitor the status of each port.

Select the **Refresh (↻)** button to refresh the table.



UI Setting	Description
Port	Shows which port this row describes.
Status	Shows the status of the port.
Media Type	Shows the port's media type.
Link Status	Shows the speed and duplex mode the connection is currently using. If the link is not active, a – will be shown.
Description	Shows the description for the port.
Flow Control	Shows the whether flow control is currently on or off for the port. If the link is not active, a – will be shown.
MDI/MDIX	Shows whether the port is using MDI or MDIX for its connection. If the link is not active, a – will be shown.
Port State	Shows the port state for the port. If the link is not active, a – will be shown.

Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation

This page lets you manage link aggregation for your device.

This page includes these tabs:

- Settings
- Status

Link Aggregation - Settings

Menu Path: Network Configuration > Ports > Link Aggregation - Settings

This page lets you configure link aggregation for your device. Link aggregation (or port trunking) is the process of combining multiple physical network links into a single logical link to increase bandwidth, improve redundancy and availability, and provide load balancing across links.

Note

Ports in the same link aggregation must have the same speed.

Note

If a port is being used for Turbo Ring or Turbo Chain, it will not appear in the Link Aggregation list.

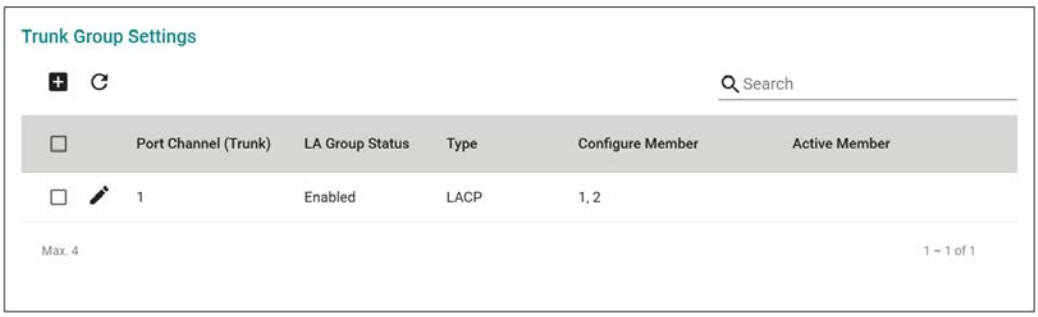
Note

For TN-4916 models with only 4 Gigabit ports, ports 1 to 8 cannot be aggregated with ports 9-12 due to design limitations.

Limitations

You can create up to 4 trunk group entries.

Trunk Group Settings



UI Setting	Description
Port Channel (Trunk)	Shows the Port Channel (Trunk) number of the link aggregation group.
LA Group Status	Shows whether the link aggregation group is enabled.
Type	Shows the method for configuring the link aggregation group.
Configure Member	Shows the configured member ports in the link aggregation group.
Active Member	Shows the active member ports in the link aggregation group.

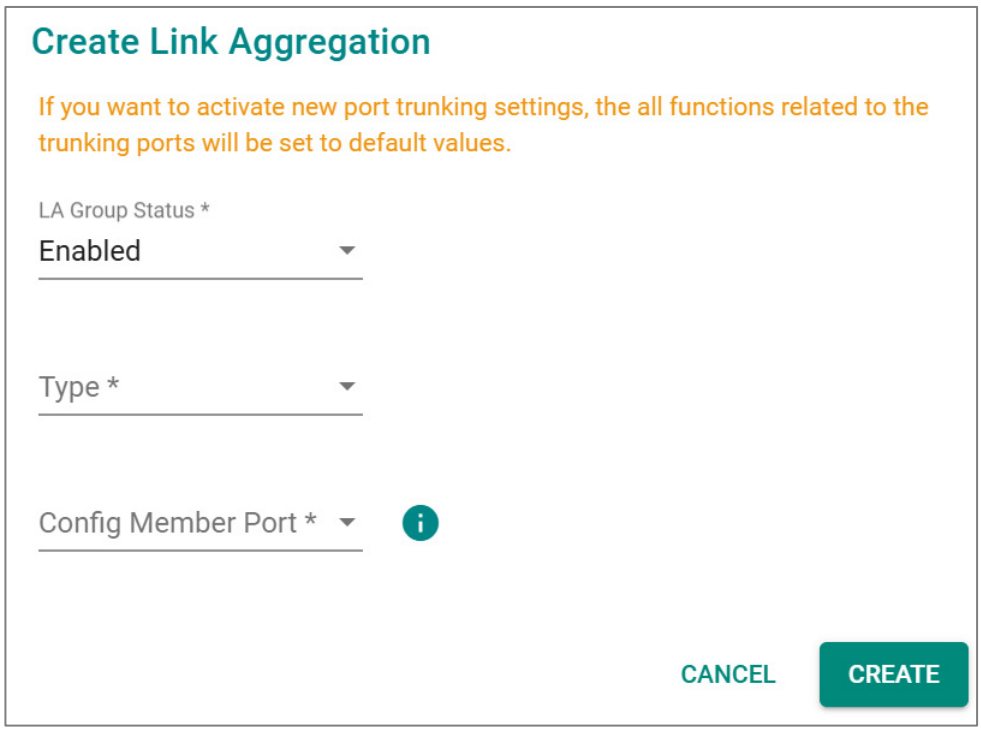
Create Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation - Settings

Clicking the **Add (⊞)** icon on the **Network Configuration > Ports > Link Aggregation - Settings** page will open this dialog box. This dialog lets you create a new link aggregation.

Click **CREATE** to save your changes and add the new aggregation.

> **Note**
> Please note that settings and available options may vary depending on the product model.



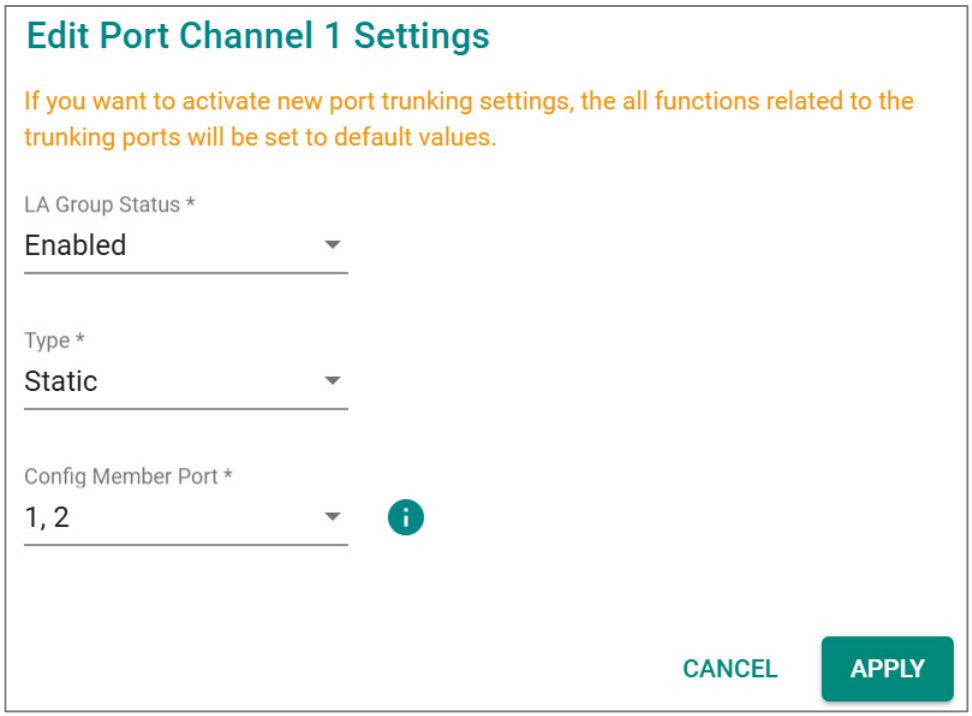
UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled
Type	Select the method to use for configuring the link aggregation group. • **Static**: This allows you to specify the ports to be included in the LA Group. • **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Static / LACP	N/A
Config Member Port	Select the ports you want to include in the link aggregation group.	Drop-down list of ports	N/A

Edit Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation - Settings

Clicking the **Edit ( )** icon for a link aggregation on the **Network Configuration > Ports > Link Aggregation - Settings** page will open this dialog box. This dialog lets you edit an existing link aggregation.

Click **APPLY** to save your changes.



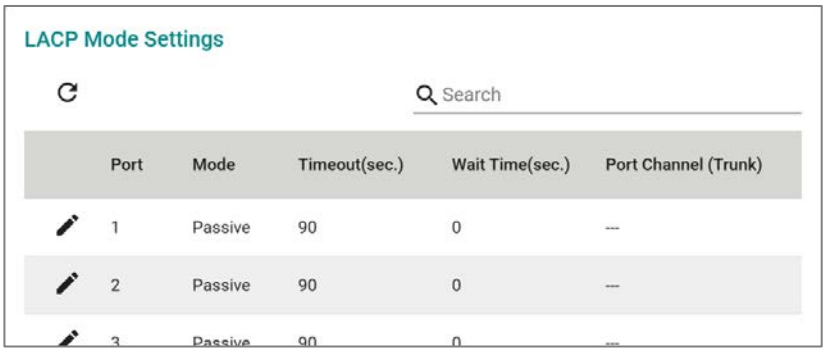
UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled
Type	Select the method to use for configuring the link aggregation group. • **Static**: This allows you to specify the ports to be included in the LA Group. • **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Static / LACP	N/A
Config Member Port	Select the ports you want to include in the link aggregation group.	Drop-down list of ports	N/A

Delete Link Aggregation

Menu Path: Network Configuration > Ports > Link Aggregation - Settings

You can delete link aggregations by using the checkboxes to select the link aggregations you want to delete, then clicking the **Delete (🗑)** icon.

Link Aggregation - LACP Mode Settings



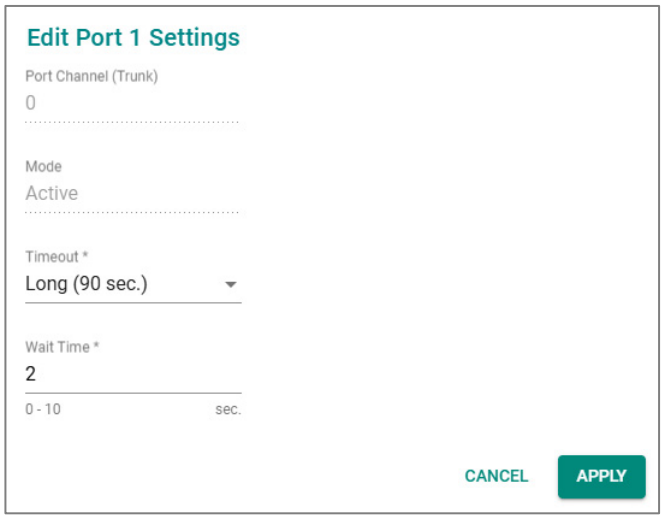
UI Setting	Description
Port	Shows which port the entry describes.
Mode	Shows the LACP mode for the port. • **Active:** Ports will actively query link partners for LACP by sending LACP PDUs. If the partner is also LACP-enabled, the ports will establish an LACP link.
Timeout (sec.)	Shows the LACP inactivity timeout in seconds for the port.
Wait Time (sec.)	Shows the LACP wait time in seconds for the port.
Port Channel (Trunk)	Shows the link aggregation group (Port channel) number for the port.

Edit LACP Mode Settings

Menu Path: Network Configuration > Ports > Link Aggregation - Settings

Clicking the **Edit ( )** icon by a port on the **Network Configuration > Ports > Link Aggregation** page will open this dialog box. This dialog lets you edit the port settings for LACP parameters if your link aggregation type is set to LACP.

Click **APPLY** to save your changes.

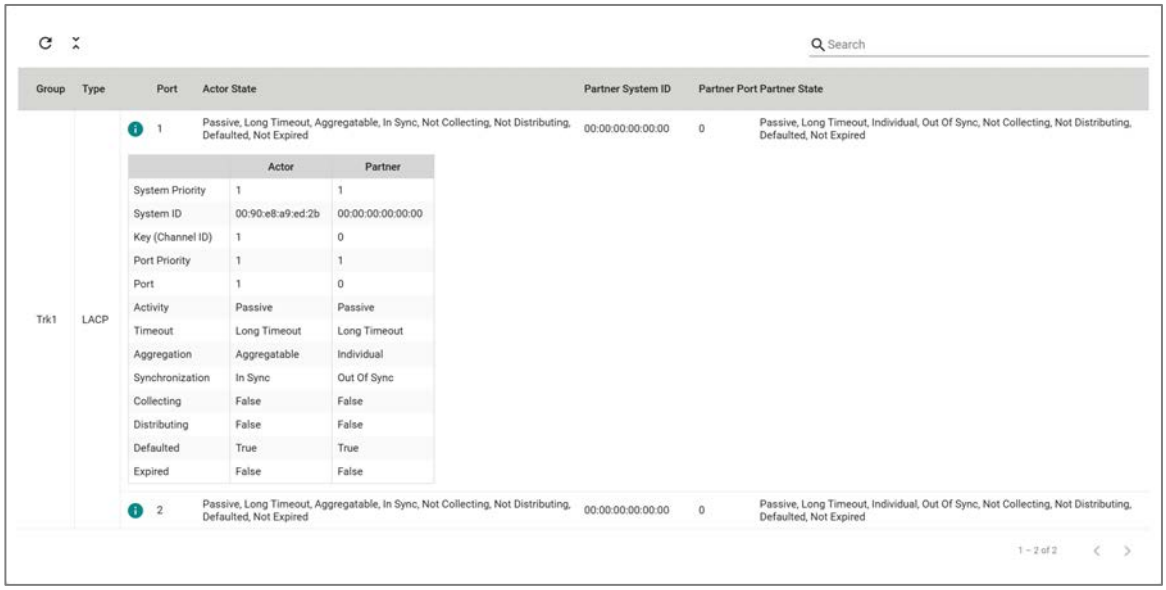


UI Setting	Description	Valid Range	Default Value
Port Channel (Trunk)	Shows the link aggregation group (Port channel) number of the port. This setting cannot be changed.	Port Channel Number	N/A
Mode	Shows the LACP mode for the port. This setting cannot be changed.	Active	Active
Timeout	Specify the LACP inactivity timeout in seconds. This is the amount of time that must elapse without receiving any LACP PDUs before a link is considered to have failed.	Short (3 sec.) / Long (90 sec.)	Long (90 sec.)
Wait Time	Specify the LACP wait time in seconds. This is the amount of time that must elapse after a LACP link comes up before it is added to the link aggregation group.	0 to 10	0

Link Aggregation - Status

Menu Path: Network Configuration > Ports > Link Aggregation - Status

This page lets you check the status of link aggregation for your device.



UI Setting	Description
Group	Shows the Port Channel (Trunk) number of the link aggregation group.
Type	Shows the method for configuring the link aggregation group.
Port	Shows the port in the link aggregation group the entry is for. Click the **Show info icon ( )** to show more details about the state of the Actor and Partner for the port.
Actor State	Shows the state of the Actor, which is a Link Aggregation Control (LAG) instance responsible for transmitting LACP Data Units (LACPDUs) to establish and maintain a link aggregation connection.
Partner System ID	Shows the Partner's System ID, represented as a MAC address. A value of 00:00:00:00:00:00 indicates that no partner port is linked to the corresponding port on this device.
Partner Port	Shows the Partner port for the link aggregation group. A value of 0 indicates that no partner port is linked to the corresponding port on this device.
Partner State	Shows the state of the Partner, which is a Link Aggregation Control (LAG) instance that receives LACPDUs from the Actor and includes its own Actor information in response, facilitating link negotiation and aggregation.

Link Fault Passthrough

Menu Path: Network Configuration > Ports > Link Fault Passthrough

This page lets you enable and configure the Link Fault Passthrough function.

Note

Availability of this feature may vary depending on your product model and version.

Note

When Link Fault Passthrough is enabled, both ports need to be linked up. Otherwise, traffic between LAN ports or access from LAN ports to the device's web console might be shut down.

Note

Available ports may vary depending on the model, and port selection may be fixed for some models.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the Link Fault Passthrough function. When enabled, when any of the port links are down, the other port will be shut down.	Enabled / Disabled	Disabled
Port 1	Specify which port to use as Port 1 in the Link Fault Passthrough pair.	Drop-down list of ports	1
Port 2	Specify which port to use as Port 2 in the Link Fault Passthrough pair.	Drop-down list of ports	2

LAN Bypass Gen3

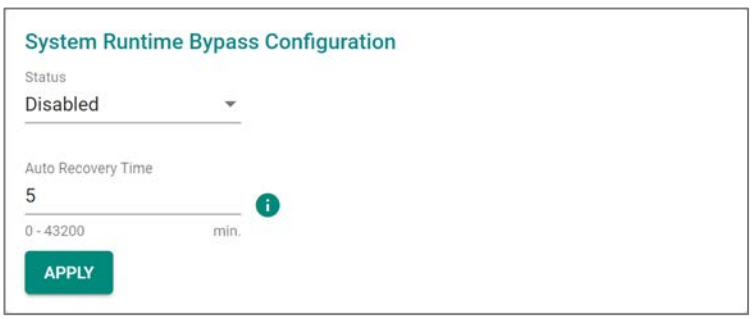
Menu Path: Network Configuration > Ports > LAN Bypass Gen3

This page lets you enable and configure different LAN bypass modes for your device.

System Failure Bypass Configuration

UI Setting	Description	Valid Range	Default Value
Mode	Specify which system failure bypass mode to use. When triggered, system failure bypass allows traffic to continue to flow between LAN ports during system failure events, minimizing disruption and maintaining operational integrity. • **Disabled:** Disable system failure bypass. Traffic will not pass between LAN ports during device failure. • **Shutdown**: Enable system failure bypass only when there is a hardware failure, such as a power outage. • **Shutdown and Halted**: Enable bypass function for both hardware failures and software issues, such as the CPU becoming unresponsive.	Disabled / Shutdown / Shutdown and Halted	Shutdown and Halted

System Runtime Bypass Configuration



UI Setting	Description	Valid Range	Default Value
Status	Enable/ Disable the system runtime bypass feature. When system runtime bypass is enabled, this will temporarily allow traffic to flow through LAN ports unimpeded, ensuring continuous network operation.	Disabled / Enabled	Disabled
Auto Recovery Time	Specify the number of minutes after which the device will automatically disable system runtime bypass after it is enabled, and will then recover to normal LAN port behavior. If this is set to 0, the device will not exit system runtime bypass after it is enabled.	0 to 43200	5

PoE

Menu Path: Network Configuration > Ports > PoE

This section lets you configure your device's Power over Ethernet (PoE) settings. PoE allows your Moxa device to power other connected PoE Ethernet devices—such as security cameras, wireless access points, and sensors—through the Ethernet cable.

> **Note**
> PoE functionality is only available on specific PoE-enabled Moxa device models. Connected PoE devices must support the IEEE 802.3af/at standard in order to use this feature.

This page includes these tabs:

- General
- PD Failure Check
- Scheduling
- Status

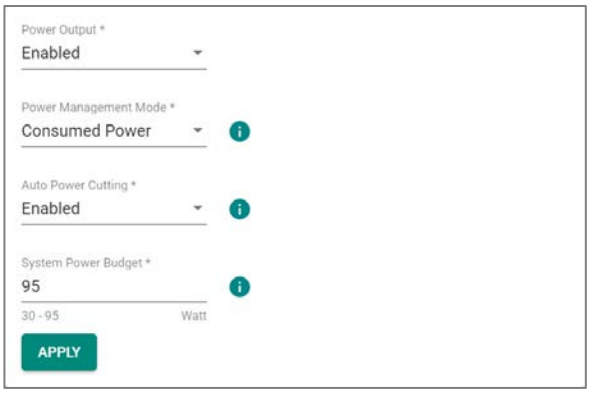
PoE - General

Menu Path: Network Configuration > Ports > PoE - General

This page lets you enable or disable various PoE related features.

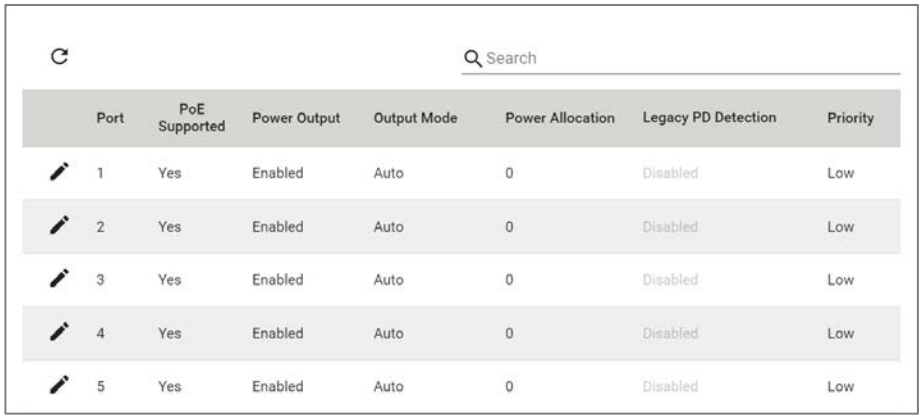
Click **APPLY** to save your changes.

PoE Settings



UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE for the device.	Enabled / Disabled	Enabled
Power Management Mode	Specify how the power budget for all ports should be calculated. • **Allocated Power**: This calculates the power budget based on the power allocation settings of all ports. For more information on per-port power allocation, refer to PoE - General - Edit Port Settings. • **Consumed Power**: This calculates the power budget based on actual power consumed by all ports.	Allocated Power / Consumed Power	Consumed Power
Auto Power Cutting	Enable or disable Auto Power Cutting, which allows PoE to be disabled for ports when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority.	Enabled / Disabled	Disabled
System Power Budget	Specify the "total measured power" budget in watts to use for all PoE ports combined. This is used as a threshold for the Auto Power Cutting feature.	(Depends on your device model)	(Depends on your device model) TN-4916 PoE models: 95 W TN-4908 PoE models: 50 W

PoE Port List



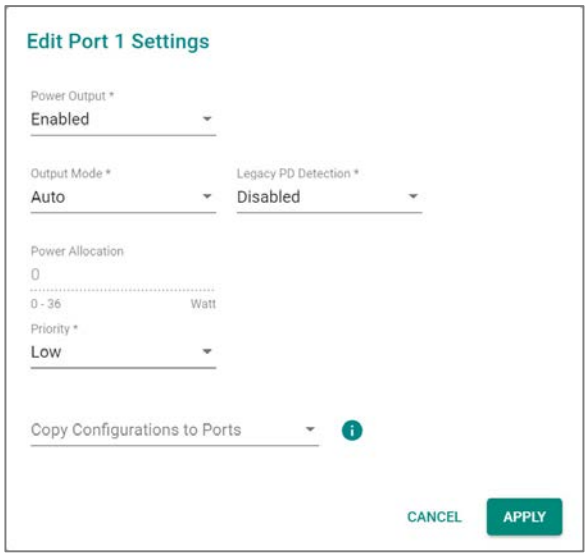
UI Setting	Description
Port	Shows which port the entry is for.
PoE Supported	Shows whether PoE is supported for the port.
Power Output	Shows whether PoE is enabled for the port.
Output Mode	Shows the PoE output mode for the port.
Power Allocation	Shows how much power in watts is allocated to the port. **Note** If the Output Mode for the port is set to Auto, the port's power allocation will be displayed as 0.
Legacy PD Detection	Shows whether legacy PD detection is enabled for the port.
Priority	Shows the priority of the port for use with the Auto Power Cutting feature. PoE will be disabled for ports with lower priority first when total power consumption exceeds the system power budget threshold.

PoE - General - Edit Port Settings

Menu Path: Network Configuration > Ports > PoE - General

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Ports > PoE - General** page will open this dialog box. This dialog lets you configure the PoE settings for a specific port.

Click **APPLY** to save your changes.



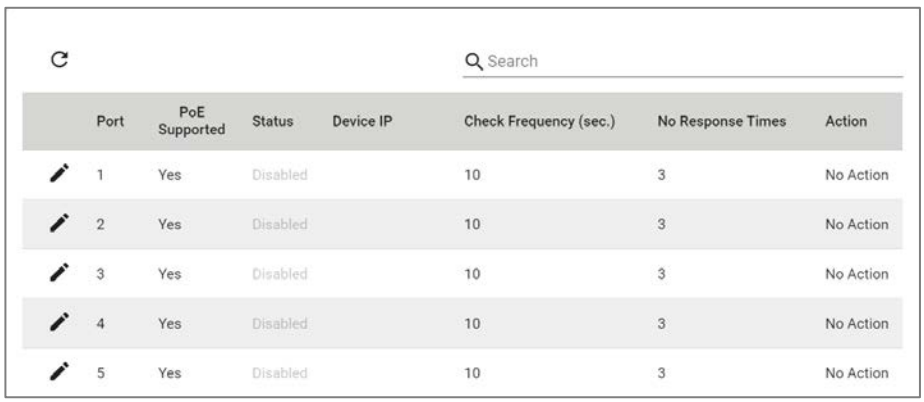
UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE for the port.	Enabled / Disabled	Enabled
Output Mode	Specify whether to set the PoE output mode to Auto or Force. • **Auto**: Power output will be determined by using 802.3at auto-detection. • **High Power**: 36 watts will be allocated to the PD connected to the port if it requires more than 30 watts of power. • **Force**: Power output will be determined by the **Power Allocation** setting for the port. This may be necessary for PDs that do not follow 802.3af/at standards.	Auto / High Power / Force	Auto
Legacy PD Detection	Enable or disable Legacy PD Detection. Legacy PD Detection will trigger the system to output power to the connected PD when the capacitance of the PD is higher than 2.7 µF and less than 10 µF. It will take a few seconds for PoE power to be output through the port (if triggered) after enabling Legacy PD Detection.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Power Allocation	Specify the power in watts to allocate to a connected PD when the **Output Mode** is set to **Force**. **Note** This setting cannot be adjusted if the Output Mode is set to Auto or High Power. It will be fixed as 0 in Auto mode, and as 36 in High Power mode.	0 to 36	0
Priority	Specify the priority of the port to use with the **Auto Power Cutting** feature. If Auto Power Cutting is enabled, PoE will be disabled for ports when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority. Refer to PoE Settings for more information.	Critical / High / Low	Low
Copy Config to Ports	Specify which ports you want to copy this configuration to.	Select port(s) from the drop-down list	None

PoE PD Failure Check

Menu Path: Network Configuration > Ports > PoE - PD Failure Check

This page lets you monitor the status of a powered device (PD) through its IP address. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process will be restarted. This function is extremely useful for ensuring network reliability and simplifying management.



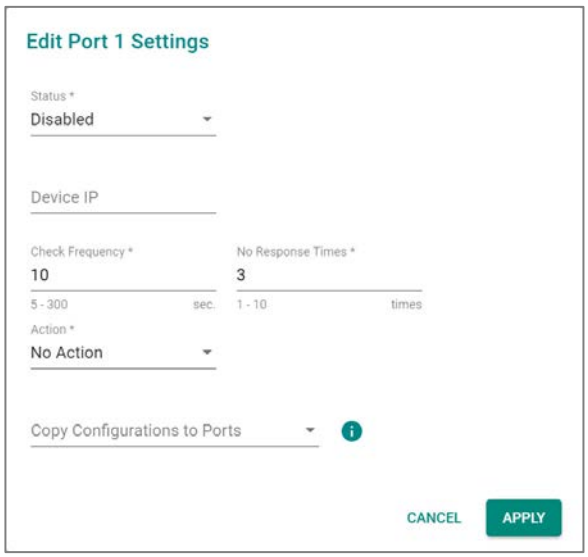
UI Setting	Description
Port	Shows which port the entry is for.
PoE Supported	Shows whether the port supports PoE.
Status	Shows whether PD failure checking is enabled or disabled for the port.
Device IP	Shows the IP that will be monitored for PD failure checks for the port.
Check Frequency (sec.)	Shows the frequency in seconds to perform PD failure checks for the port.
No Response Times	Shows how many consecutive PD failure checks must fail before determining a PD is not responding.
Action	Shows what action will be taken if a PD failure is detected for the port.

PoE - PD Failure Check - Edit Port Settings

Menu Path: Network Configuration > Ports > PoE - PD Failure Check

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Ports > PoE - PD Failure Check** page will open this dialog box. This dialog lets you configure the PD failure check settings for each port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PD failure checking for the port.	Enabled / Disabled	Disabled
Device IP	Specify the IP that will be monitored for PD failure checks for the port. This is normally set to the connected PD's IP. PD failure checks will ping this IP, and will result in a "fail" if there is no response from the IP.	Valid IP address	None
Check Frequency	Specify the frequency in seconds to perform PD failure checks for the port.	5 to 300	10
No Response Times	Specify how many consecutive PD failure checks must fail before determining a PD is not responding and executing the specified action for the rule.	1 to 10	3
Action	Decide what action to take when a PD failure is determined. • **No Action**: The PD failure will be logged, but no action will be taken. • **Restart PD**: PoE power for the port will be stopped, and then start again to restart the connected PD. • **Shut down PD**: PoE power for the port will be stopped.	No Action / Restart PD / Shut down PD	No Action
Copy Configurations to Ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

PoE - Scheduling

Menu Path: Network Configuration > Ports > PoE - Scheduling

This page lets you set schedules for each PoE port. Switch to Advanced Mode, click the Scheduling tab, and then click the + icon to create the scheduling settings.

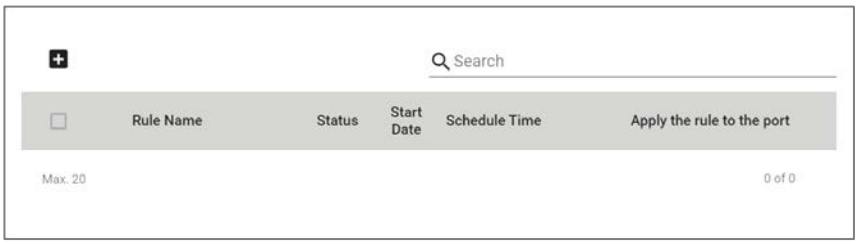
Limitations

You can create up to 20 PoE scheduling rules.

System Time Status

UI Setting	Description
System Time	Shows the device's current system time.
Local TimeZone	Shows the device's local time zone.
Daylight Saving Time	Shows whether a daylight saving time adjustment is currently applied to the system time.

PoE Scheduling Rule List



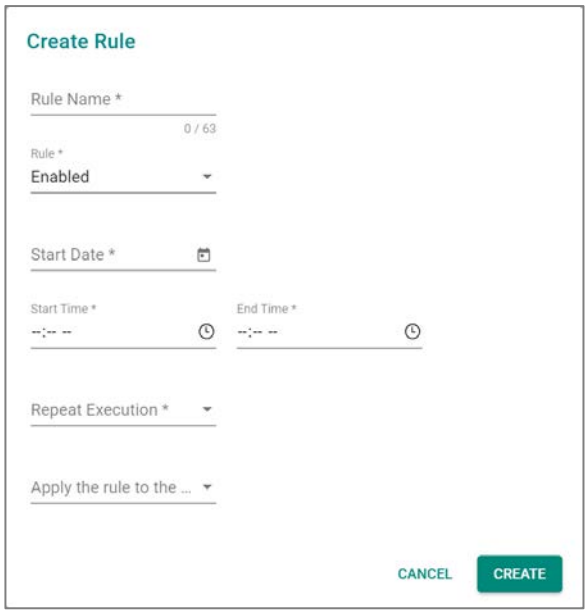
UI Setting	Description
Rule Name	Shows the name for the scheduling rule the entry is for.
Status	Shows whether the rule is enabled or disabled.
Start Date	Shows what date the rule will start on.
Schedule Time	Shows when PoE will be enabled for ports using the rule.
Apply the rule to the port	Shows which ports will use this rule.

PoE - Scheduling - Create Rule

Menu Path: Network Configuration > Ports > PoE - Scheduling

Clicking the **Add (⊕)** icon on the **Network Configuration > Ports > PoE - Scheduling** page will open this dialog box. This dialog lets you create a PoE scheduling rule.

Click **CREATE** to save your changes and add the new rule.



UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Enable	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled
Start Date	Specify a start date for the rule. You can click the calendar icon to open a date picker to select a date.	yyyy-mm-dd	N/A
Start Time	Specify a start time for the rule. PoE power to the specified ports will be supplied after the start time. You can click the clock icon to open a time picker to select a time.	hh:mm AM/PM	N/A
End Time	Specify an end time for the rule. PoE power to the specified ports will be stopped after the end time. You can click the clock icon to open a time picker to select a time.	hh/mm AM/PM	N/A

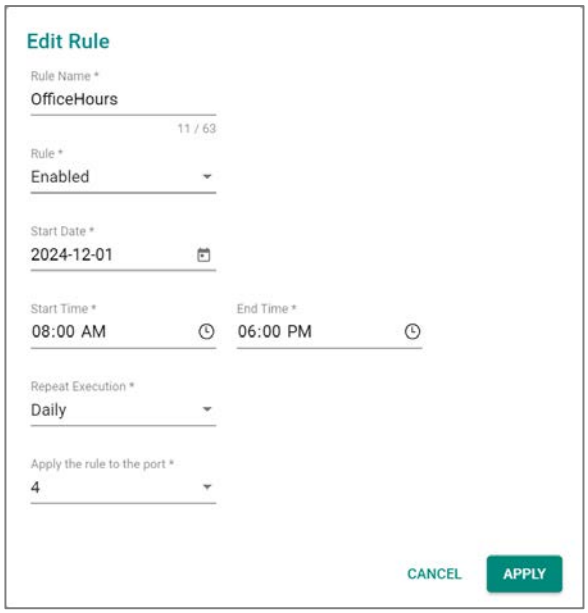
UI Setting	Description	Valid Range	Default Value
Repeat Execution	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	N/A
Apply the rule to port	Specify which ports should use this rule.	Drop-down list of ports	N/A

PoE - Scheduling - Edit Rule

Menu Path: Network Configuration > Ports > PoE - Scheduling

Clicking the **Edit ( )** icon on the **Network Configuration > Ports > PoE - Scheduling** page will open this dialog box. This dialog lets you edit an existing PoE scheduling rule.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Enable	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Start Date	Specify a start date for the rule. You can click the calendar icon to open a date picker to select a date.	yyyy-mm-dd	N/A
Start Time	Specify a start time for the rule. PoE power to the specified ports will be supplied after the start time. You can click the clock icon to open a time picker to select a time.	hh:mm AM/PM	N/A
End Time	Specify an end time for the rule. PoE power to the specified ports will be stopped after the end time. You can click the clock icon to open a time picker to select a time.	hh/mm AM/PM	N/A
Repeat Execution	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	N/A
Apply the rule to port	Specify which ports should use this rule.	Drop-down list of ports	N/A

PoE - Scheduling - Delete Rule

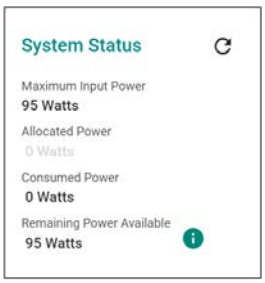
You can delete a rule by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

PoE - Status

Menu Path: Network Configuration > Ports > PoE - Status

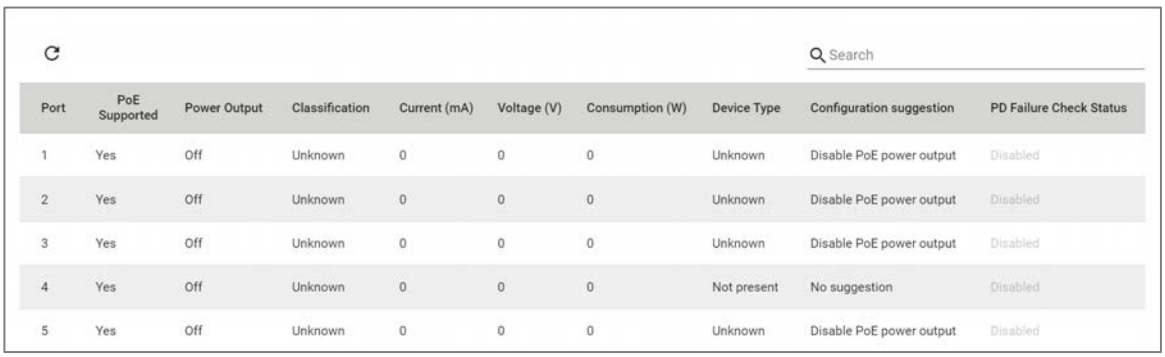
This page lets you view the current PoE status of your ports.

PoE - System Status



UI Setting	Description
Maximum Input Power	Shows the maximum power budget of the device.
Allocated Power	Shows the total allocated PoE power.
Consumed Power	Shows the total consumed PoE power.
Remaining Power Available	Shows the remaining power available for the device. **Note** Remaining Power Available is calculated as Maximum Input Power minus Allocated Power.

PoE Port Status List



UI Setting	Description
Port	Shows the number of the PoE port the entry is for.
PoE Supported	Shows whether the port supports PoE.
Power Output	Shows whether PoE power output is on or off for the port.

UI Setting	Description
Classification	Shows the PoE power classification of the port. Each PoE power classification has a different maximum power (in watts) by PSE output as follows: • **0**: 15.4 watts • **1**: 4 watts • **2**: 7 watts • **3**: 15.4 watts • **4**: 30 watts
Current (mA)	Shows the amount of current in mA being supplied to the port.
Voltage (V)	Shows the voltage in V being used for the port.
Consumption (W)	Shows the power consumption in W of the device connected to the port.
Device Type	Shows the device type of the device currently connected to the port. • **Not Present**: There are no active connections to the port. • **802.3at**: An IEEE 802.3at PD is connected to the port. • **802.3af**: An IEEE 802.3af PD is connected to the port. • **NIC**: A NIC is connected to the port. • **Unknown**: An unknown PD is connected to the port. • **N/A**: PoE is disabled for the port.
Configuration Suggestion	Shows configuration suggestions based on detected conditions. • **Disable PoE power output**: A NIC or unknown PD was detected; you may want to disable PoE power output for the port. • **Select Force Mode**: A higher/lower resistance or higher capacitance was detected; you may want to select **Force Mode** for the port. • **Select high power output**: An unknown classification was detected; you may want to select **High Power** output for the port. • **Raise the external power supply voltage to greater than 46 VDC**: When the external supply voltage is detected as less than 46 V, the system suggests raising the voltage. • **Enable PoE function for detection**: The system suggests enabling PoE. • **Select IEEE 802.3at auto mode**: When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode. • **Select IEEE 802.3af auto mode**: When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.
PD Failure Check	Shows the results of the last PD failure check, if checking is enabled. Refer to PD Failure Check for more information. • **Disable**: PD failure checking is not enabled for the port. • **Alive**: The port is alive, and passed the last PD failure check. • **Not Alive**: The port is not alive, and failed the last PD failure check.

Layer 2 Switching

Menu Path: Network Configuration > Layer 2 Switching

This section lets you configure the Layer 2 switching settings for your device.

This section includes these pages:

- VLAN
- MAC Address
- QoS
- Rate Limit
- Multicast

VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN

This page lets you configure global VLAN settings so you can partition your network into separate VLANs.

This page includes these tabs:

- Global
- Settings
- Status
- VLAN Standard

VLAN Settings - Global

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Global

This page lets you configure the settings for the management VLAN and management port. Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Management VLAN	Specify the management VLAN ID from the drop-down menu.	Drop-down list of VLAN IDs	1
Management Port	Specify a management port for this device to allow for quick and easy configuration of VLAN settings for multiple ports.	(Depends on your device model)	N/A

The following settings will appear after selecting a **Management Port**:

UI Setting	Description	Valid Range	Default Value
Mode	Specify which VLAN mode the port should use: • **Access**: Define the port as an Access port. This is used when connecting to single devices without tags. • **Trunk**: Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware router. • **Hybrid**: Define the port as a Hybrid port. This is used when connecting to another 802.1Q VLAN-aware router, or another LAN that combines tagged and/or untagged devices and/or other routers or hubs. **Note** If you do not intend to use the device purely as a Layer 2 switch, it is strongly recommended that you do not use trunk VLANs for most use cases.	Access / Trunk / Hybrid	Access
PVID	Set the default VLAN ID to use for traffic from untagged devices that connect to the port.	Drop-down list of VLAN IDs	1

UI Setting	Description	Valid Range	Default Value
Tagged VLAN **(If Mode is Trunk or Hybrid)**	If the **Mode** is set to **Trunk** or **Hybrid**, you can specify what VLAN IDs tagged devices that connect to the port will use. Use commas to separate different VIDs.	All Member VIDs / Drop-down list of VLAN IDs	N/A
Untagged VLAN **(If Mode is Hybrid)**	Assign a VLAN ID for untagged devices that connect to the port and remove tags upon egress. Use commas to separate different VLAN IDs.	All Member VIDs / Drop-down list of VLAN IDs	1

VLAN - Settings

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

This page lets you configure management VLAN and port settings.

Click **APPLY** to save your changes.

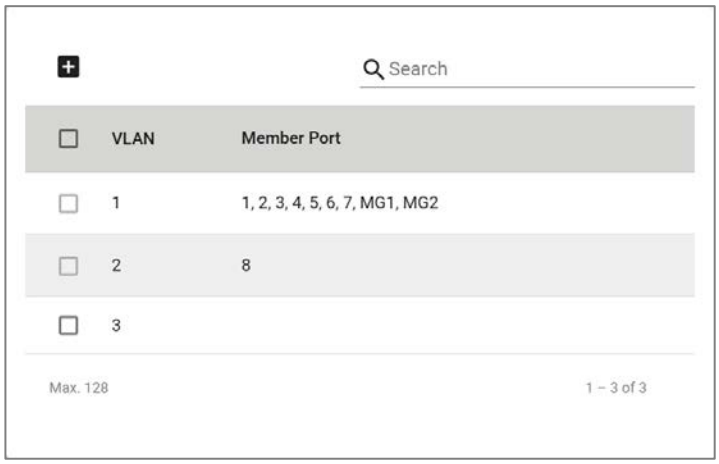
Note

Please note that port numbers may vary depending on product model.

Limitations

- EDR, OnCell, and TN Series: You can create up to 128 VLANs.
- NAT Series: You can create up to 10 VLANs.

VLAN List



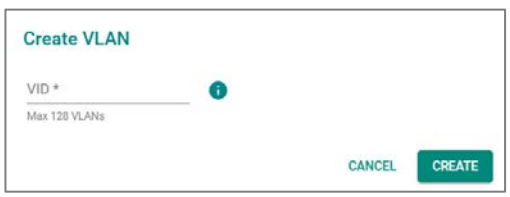
UI Setting	Description
VLAN	Shows the VID for the VLAN.
Member Port	Shows which ports are in the VLAN.

VLAN - Settings - Create VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

Clicking the **Add (+)** icon on the **Network Configuration > Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you create a VLAN.

Click **CREATE** to save your changes and add the new VLAN.

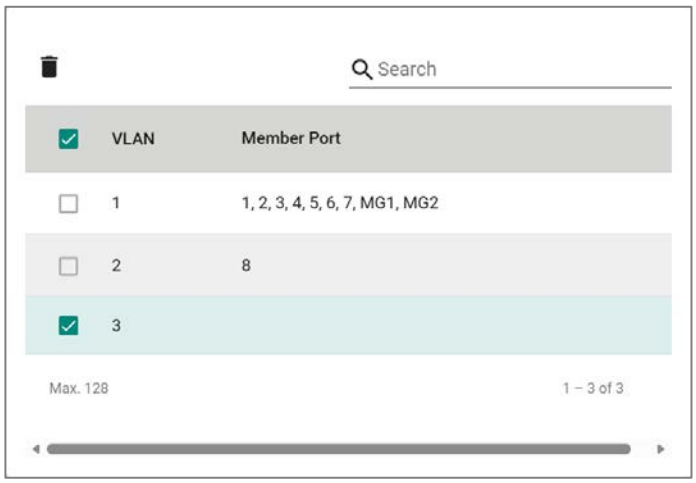


UI Setting	Description	Valid Range	Default Value
VID	Specify the VID to use for the VLAN. You can create multiple VLANs at once by entering single VIDs or VID ranges separated by commas, such as 2, 4-8, 10-13.	1 to 4094 You can enter multiple VIDs and/or VID ranges, separated by commas.	N/A

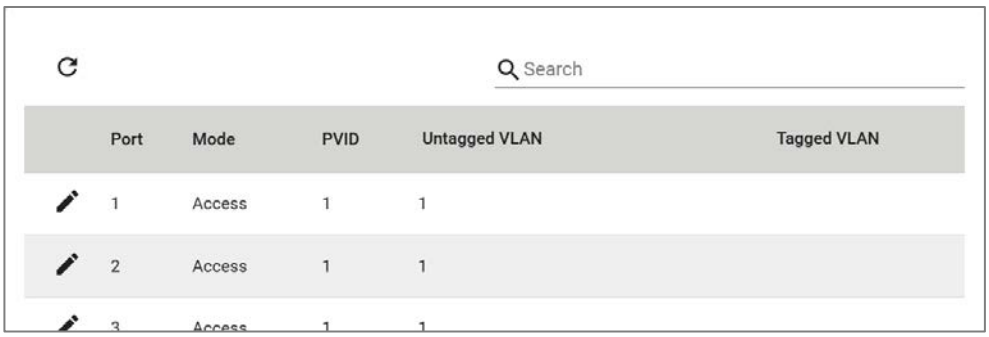
VLAN - Settings - Delete VLAN

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

You can delete VLANs by using the checkboxes to select the VLANs you want to delete, then clicking the **Delete ( )** icon.



VLAN Port List



UI Setting	Description
Port	Shows which port this row describes.

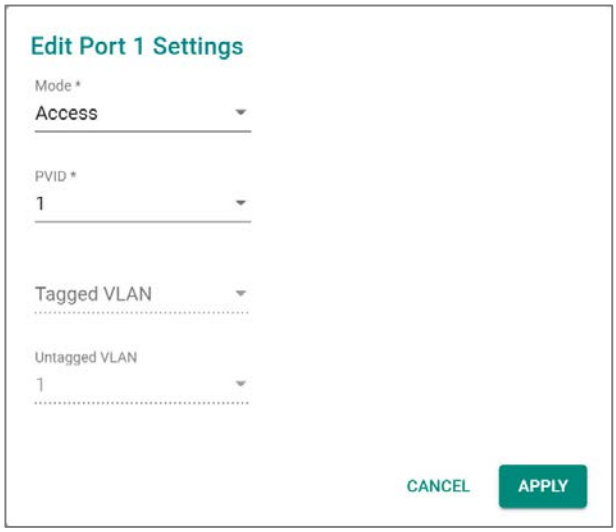
UI Setting	Description
Mode	Shows the VLAN mode for the port.
PVID	Shows the VLAN ID used for the port.
Untagged VLAN	Shows the Untagged VLAN for the port.
Tagged VLAN	Shows the Tagged VLAN for the port.

VLAN - Settings - Edit Port Settings

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Settings

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you edit the VLAN settings for a port.

Click **APPLY** to save your changes.

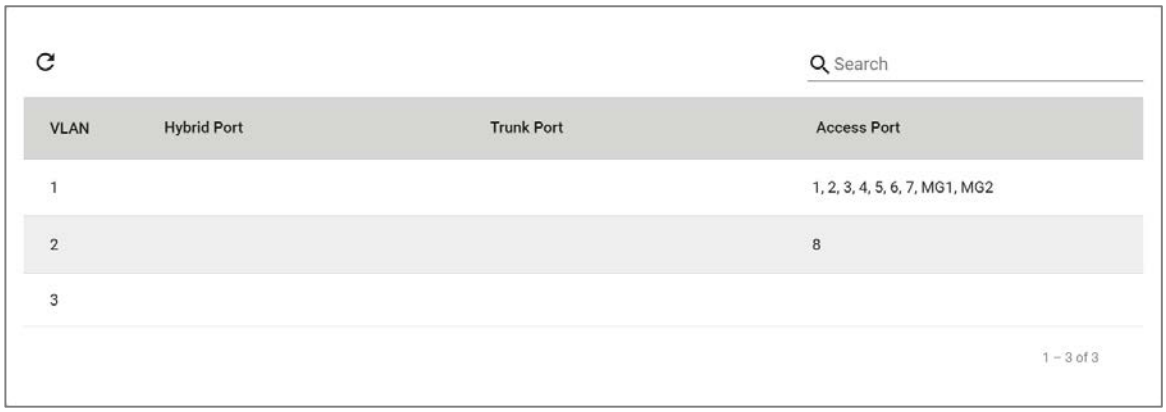


UI Setting	Description	Valid Range	Default Value
Mode	Specify which VLAN mode the port should use: • **Access**: Define the port as an Access port. This is used when connecting to single devices without tags. • **Trunk**: Define the port as a Trunk port. This is used when connecting to another 802.1Q VLAN-aware router. • **Hybrid**: Define the port as a Hybrid port. This is used when connecting to another 802.1Q VLAN-aware router, or another LAN that combines tagged and/or untagged devices and/or other routers or hubs.	Access / Trunk / Hybrid	Access
PVID	Set the default VLAN ID to use for traffic from untagged devices that connect to the port.	1 to 4094	1
Tagged VLAN **(When editing settings for the Management Port)**	If the **Mode** is set to **Trunk** or **Hybrid**, you can specify what VLAN IDs tagged devices that connect to the port will use. Use commas to separate different VIDs.	All Member VIDs / 1 to 4094	N/A
Untagged VLAN **(When editing settings for the Management Port)**	If the **Mode** is set to **Access**, assign a VLAN ID for untagged devices that connect to the port and remove tags upon egress. Use commas to separate different VLAN IDs.	All Member VIDs / 1 to 4094	N/A

VLAN - Status

Menu Path: Network Configuration > Layer 2 Switching > VLAN - Status

This page lets you monitor the status of the VLANs on your device.



UI Setting	Description
VLAN	Shows the VID of the VLAN.
Hybrid Port	Shows ports acting as a Hybrid Port for the VLAN.
Trunk Port	Shows ports acting as a Trunk Port for the VLAN.
Access Port	Shows ports acting as an Access Port for the VLAN.

VLAN Standard

Menu Path: Network Configuration > Layer 2 Switching > VLAN - VLAN Standard

This page lets you specify which VLAN standard the device will use.

UI Setting	Description	Valid Range	Default Value
VLAN Standard	Select which VLAN standard the device will use. **Note** Changing the VLAN mode will automatically configure all interfaces to use the new mode, and then reboot the device to ensure the new configuration takes effect.	802.1Q / 802.1ad	802.1Q

MAC Address Table

Menu Path: Network Configuration > Layer 2 Switching > MAC Address Table

This page lets you view your device's MAC address table and set the aging time for MAC address entries.

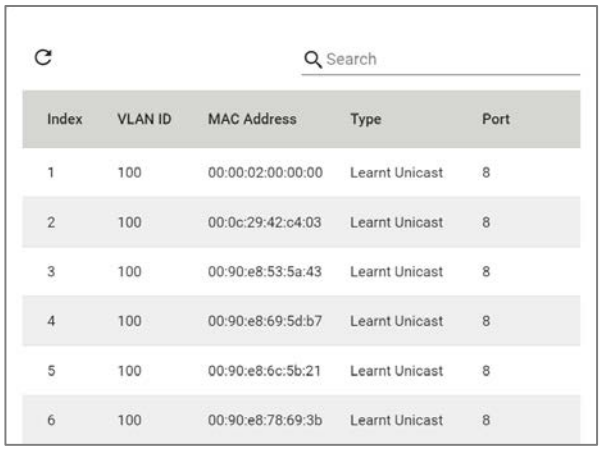
Limitations

The MAC address table can hold up to 8192 entries.

MAC Address Table Settings

UI Setting	Description	Valid Range	Default Value
Aging Time	Specify the aging time for MAC address entries in seconds. The aging time determines how long entries will be kept in the MAC address table in the device's memory before expiring.	5 to 300	300
Log	Enable or disable logging of MAC address entries.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Informational
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Any changes to the MAC Address Table will be logged under the Neighbor MAC Change classification. Refer to Event Log for more information.	Syslog / Trap / Local Storage	None

MAC Address Table



UI Setting	Description
Index	Shows the index number of the MAC address.
VLAN ID	Shows which VLAN ID is being used for the MAC address.
MAC Address	Shows the MAC address.
Type	Shows what kind of MAC address entry this is: • **Learnt Unicast**: Used for all learnt unicast MAC addresses. • **Learnt Multicast**: Used for all learnt multicast MAC addresses. • **Static Unicast**: Used for all static unicast MAC addresses. • **Static Multicast**: Used for all static multicast MAC addresses.
Port	Shows which port on the device the MAC address is connected to.

QoS

Menu Path: Network Configuration > Layer 2 Switching > QoS

This page lets you configure QoS settings to control network traffic prioritization.

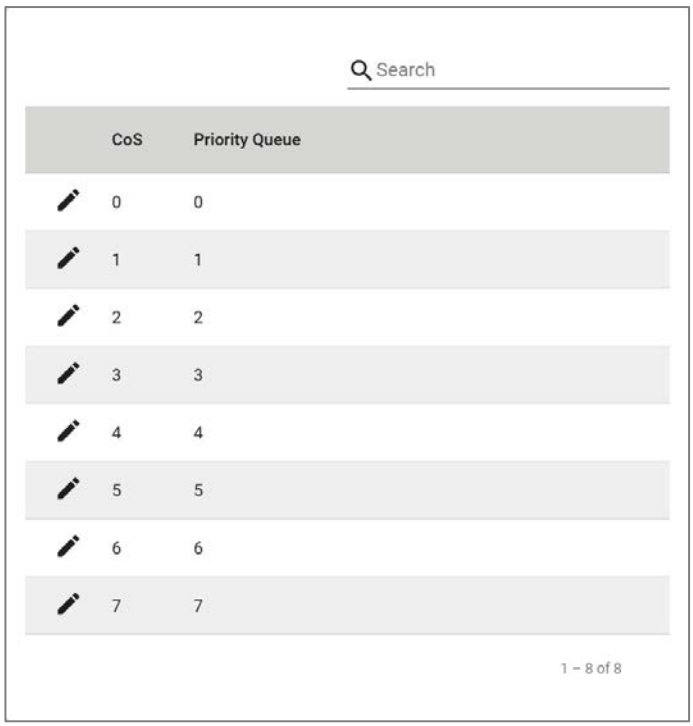
This page includes these tabs:

- CoS Mapping
- DSCP Mapping
- Port Classification
- DSCP Remark

CoS Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - CoS Mapping

This page lets you configure CoS Mapping, which allows you to map 802.1p/1Q Layer 2 CoS tags to priority queues on the device.



UI Setting	Description
CoS	Shows the CoS level. Higher numbers indicate higher priority.
Level	Shows the device priority queue the CoS level is mapped to. Higher numbers indicate higher priority.

Edit CoS Settings

Menu Path: Network Configuration > Layer 2 Switching > QoS - CoS Mapping

Clicking the **Edit ( )** icon for a CoS level on the **Network Configuration > Layer 2 Switching > QoS - CoS Mapping** tab will open this dialog box. This dialog lets you map the CoS level to a device priority queue.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Priority Queue	Select the device priority queue to use for the CoS level. Higher numbers indicate higher priority.	0 to 7	0

DSCP Mapping

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Mapping

This page lets you map Layer 3 DSCP levels to priority queues on the device.

UI Setting	Description
DSCP	Shows the DSCP level. Higher numbers indicate higher priority.
Level	Shows the device priority queue the DSCP level is mapped to. Higher numbers indicate higher priority.

Edit DSCP Settings

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Mapping

Clicking the **Edit ( )** icon for an DSCP mapping on the **Network Configuration > Layer 2 Switching > QoS - DSCP Mapping** page will open this dialog box. This dialog lets you map the DSCP level to a device priority queue.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Priority Queue	Select the device priority queue to use for the DSCP level. Higher numbers indicate higher priority.	0 to 7	0

Port Classification

Menu Path: Network Configuration > Layer 2 Switching > QoS - Port Classification

This page lets you configure QoS queueing mechanisms for each port.

Note

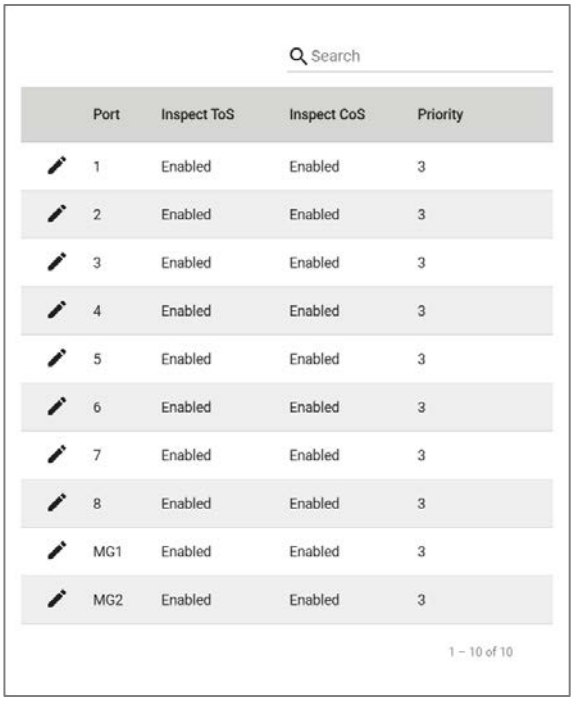
For TN-4900 Series 16-port models, port priority must be handled in 2 separate groups as follows, due to design limitations:

- Ports 1 to 8
- Ports G1 to G8
  or
  Ports 9 to 12 and G1 to G4
  (depends on your model)

Port Classification Settings

UI Setting	Description	Valid Range	Default Value
Scheduling Mechanism	Specify the scheduling mechanism to use for your device: • **Weight Fair(8:4:2:1)**: In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priority levels on the device. This approach prevents lower priority frames from being starved of opportunities for transmission with only a slight delay to higher priority frames. • **Strict(High Priority First Always)**: In the strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunities for transmitting any frames, but ensures that all high priority frames will egress the switch as soon as possible.	Weight Fair(8:4:2:1) / Strict(High Priority First Always)	Weight Fair(8:4:2:1)

Port Classification - Port List



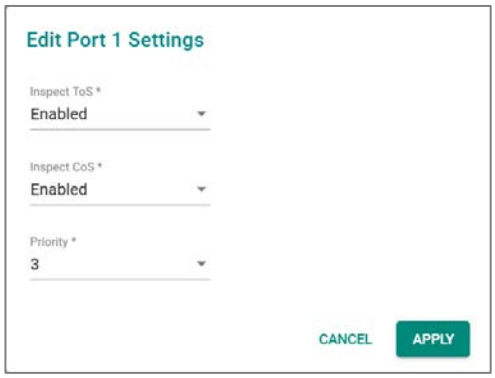
UI Setting	Description
Port	Shows which port this row describes.
Inspect ToS	Shows whether ToS is enabled or disabled for the port.
Inspect CoS	Shows whether CoS inspection is enabled or disabled for the port.
Priority	Shows the priority for the port. Higher numbers indicate higher priority.

Port Classification - Edit Port Settings

Menu Path: Network Configuration > Layer 2 Switching > QoS - Port Classification

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Layer 2 Switching > QoS - Port Classification** page will open this dialog box. This dialog lets you configure the classifications settings for the port.

Click **APPLY** to save your changes.



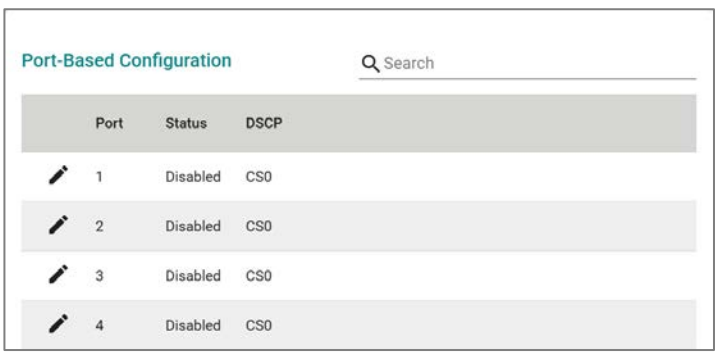
UI Setting	Description	Valid Range	Default Value
Inspect ToS	Enable or disable inspection of Type of Service (ToS) bits in the IPV4 frame to determine the priority of each frame.	Enabled or Disabled	Enabled
Inspect CoS	Enable or disable inspection of 802.1p CoS tags in the MAC frame to determine the priority of each frame.	Enabled or Disabled	Enabled
Priority	Specify the priority of the port. Higher numbers indicate higher priority.	0 to 7	3

DSCP Remark

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Remark

This page lets you configure the DSCP remark feature for the device.

DSCP Remark - Port-based Configuration



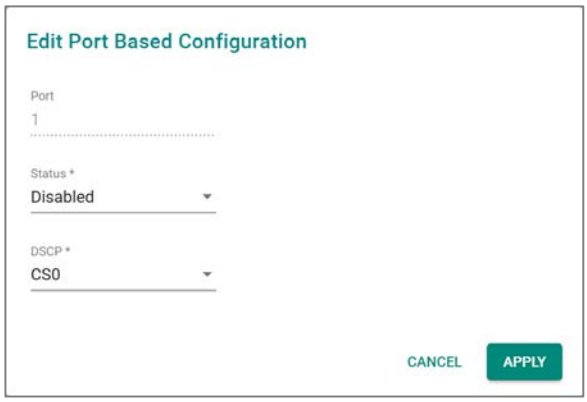
UI Setting	Description
Port	Shows which port this entry describes.
Status	Shows whether DHCP Remark is enabled for the port.
DSCP	Shows the DSCP level for the port. Higher numbers indicate higher priority.

DSCP Remark - Edit Port-based Configuration

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Remark

Clicking the **Edit ( )** icon for a port-based configuration on the **Network Configuration > Layer 2 Switching > QoS - DSCP Remark** page will open this dialog box. This dialog lets you edit the configuration.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port (View-only)	Shows which port the configuration is for. This setting cannot be edited.	N/A	N/A
Status	Enable or disable the DSCP Remark feature for the configuration.	Enabled / Disabled	Enabled
DSCP	Specify the DSCP level for the configuration. Higher numbers indicate higher priority.	CS0 / CS1 / CS2 / CS3 / CS4 / CS5 / CS6 / CS7	CS0

DSCP Remark - Subnet-based Configuration

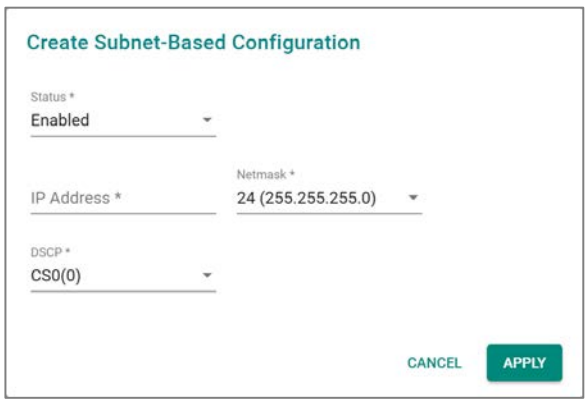
UI Setting	Description
Enabled	Shows whether DSCP remark is enabled or disabled for the configuration.
IP Address	Shows the IP address for the configuration.
Netmask	Shows the subnet mask for the configuration.
DSCP	Shows the DSCP level for the configuration. Higher numbers indicate higher priority.

DSCP Mapping - Create a Subnet-based Configuration

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Remark

Clicking the **Add (⊞)** icon for the Subnet-based Configuration table on the **Network Configuration > Layer 2 Switching > QoS - DSCP Remark** page will open this dialog box. This dialog lets you create a new configuration.

Click **APPLY** to save your changes.



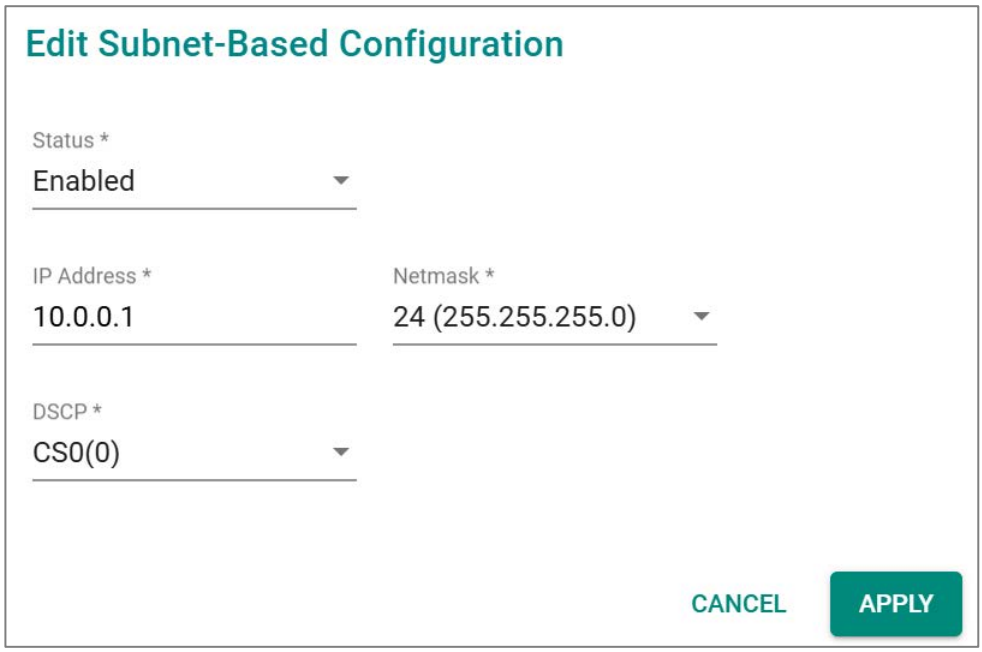
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the DSCP Remark feature for the configuration.	Enabled / Disabled	Enabled
IP Address	Specify the IP address of the configuration.	Valid IP address	N/A
Netmask	Specify the subnet mask of the configuration.	Valid subnet mask	24 (255.255.255.0)
DSCP	Specify the DSCP level for the configuration. Higher numbers indicate higher priority.	CS0 / CS1 / CS2 / CS3 / CS4 / CS5 / CS6 / CS7	CS0

DSCP Remark - Edit Subnet-based Configuration

Menu Path: Network Configuration > Layer 2 Switching > QoS - DSCP Remark

Clicking the **Edit ( )** icon for a subnet-based configuration on the **Network Configuration > Layer 2 Switching > QoS - DSCP Remark** page will open this dialog box. This dialog lets you edit the configuration.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the DSCP Remark feature for the configuration.	Enabled / Disabled	Enabled
IP Address	Specify the IP address of the configuration.	Valid IP address	N/A
Netmask	Specify the subnet mask of the configuration.	Valid subnet mask	24 (255.255.255.0)
DSCP	Specify the DSCP level for the configuration. Higher numbers indicate higher priority.	CS0 / CS1 / CS2 / CS3 / CS4 / CS5 / CS6 / CS7	CS0

Rate Limit

Menu Path: Network Configuration > Layer 2 Switching > Rate Limit

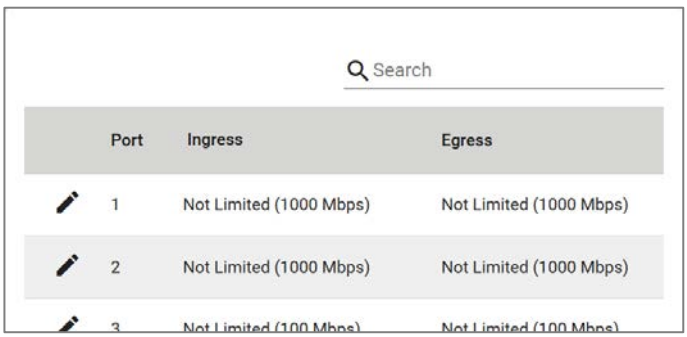
This page lets you control the bandwidth of ingress (incoming) and egress (outgoing) traffic through the device to protect end-devices that may not have the capability to handle large amounts of traffic.

> **Note**
> Please note that available options may vary depending on the product model.

Rate Limit Settings

UI Setting	Description	Valid Range	Default Value
Ingress Policy	Select which kind of traffic ingress rate limiting will be applied to. • **Limit All**: Rate limit will be applied to all traffic. • **Limit Broadcast, Multicast and Flooded Unicast**: Rate limit will be applied to broadcast, multicast, and flooded unicast traffic only. • **Limit Broadcast, Multicast**: Rate limit will be applied to broadcast and multicast traffic only. • **Limit Broadcast**: Rate limit will be applied to broadcast traffic only.	Limit All / Limit Broadcast, Multicast and Flooded Unicast / Limit Broadcast, Multicast / Limit Broadcast	Limit Broadcast
Ingress Action	Select the ingress action. • **Drop Packet**: The rate limit will discard incoming packets that do not comply with the ingress policy. • **Port Disable**: The rate limit will disable the port that do not comply with the ingress policy.	Drop Packet / Port Disable	Drop Packet
Port Disabled Period **(If Ingress Action is Port Disable)**	Select the port disable period during which the port will be disabled. Once this period is over, the port will be re-enabled. However, if the port does not comply with the ingress policy again, it will be disabled then.	1 to 65535	300

Rate Limit Port List



UI Setting	Description
Port	Shows which port this row describes.

UI Setting	Description
Ingress	Shows the ingress bandwidth rate limit method and bandwidth.
Engress	Shows the egress bandwidth rate limit method and bandwidth.

Rate Limit - Edit Port Settings

Menu Path: Network Configuration > Layer 2 Switching > Rate Limit

Clicking the **Edit ( )** icon for a port on the **Network Configuration > Layer 2 Switching > Rate Limit** page will open this dialog box. This dialog lets you configure rate limit settings for each port.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Ingress	Select the ingress rate limit (% of max. throughput) for all packets.	Not Limited / 3% / 5% / 10% /15% / 25% / 35% / 50% / 65% / 85%	Not Limited
Egress	Select the egress rate limit (% of max. throughput) for all packets.	Not Limited / 3% / 5% / 10% /15% / 25% / 35% / 50% / 65% / 85%	Not Limited

Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast

This section lets you adjust various settings for handling multicast traffic.

This section includes these pages:

- IGMP Snooping

- Static Multicast Table

IGMP Snooping

Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping

This page lets you configure IGMP snooping, which enables intelligent forwarding of multicast traffic in local area networks (LANs). By listening to IGMP messages sent between hosts and multicast routers, IGMP snooping can learn which multicast groups are active on the network and maintain a database of multicast group membership.

This page includes these tabs:

- VLAN Settings
- Group Table
- Forwarding Table

VLAN Settings

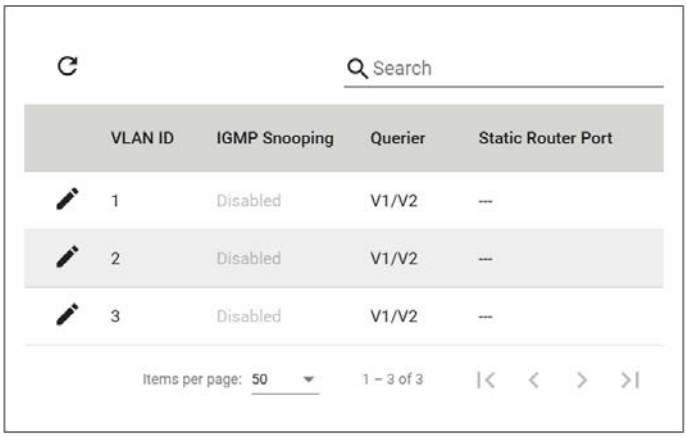
Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

This page lets you configure IGMP snooping settings for each VLAN.

IGMP VLAN Settings

UI Setting	Description	Valid Range	Default Value
Query Interval	Specify the query interval of the querier function globally.	20 to 600 seconds	125 seconds

IGMP VLAN List



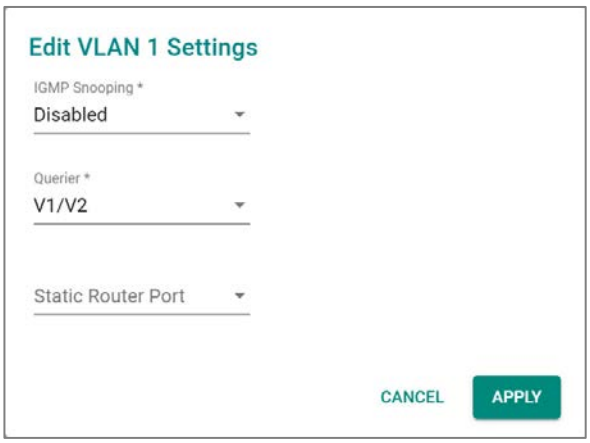
UI Setting	Description
VLAN ID	Shows which VLAN ID this row describes.
IGMP Snooping	Shows whether IGMP snooping is enabled or disabled for the VLAN.
Querier	Shows which version of IGMP snooping the VLAN will use.
Static Router Port	Shows the static router port the VLAN will use to connect to the multicast router for IGMP snooping.

VLAN Settings - Edit VLAN Settings

Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

Clicking the **Edit ( )** icon for a VLAN on the **Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings** page will open this dialog box. This dialog lets you enable and configure IGMP snooping for each VLAN.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP Snooping function for the VLAN.	Enabled / Disabled	Disabled
Querier	Specify which version of IGMP snooping to use: • **None**: This device will not act as a querier for the network. Important When selecting None for Querier, there must be at leas one other device on the VLAN acting as a querier or el IGMP will not work properly. • **V1/V2**: Enable the device to send IGMP snooping version 1 and 2 queries. • **V3**: Enable the device to send IGMP snooping version 3 queries.	None / V1/V2 / V3	V1/V2
Static Router Port	Select which ports will be used to connect to multicast routers for IGMP Snooping. The device will receive all multicast packets from the selected ports. **Note** If a router or Layer 3 switch is connected to the network, it will act as the querier, and the querier function will be disabled on all Moxa Layer 2 switches. If all switches on the network are Moxa Layer 2 switches, then only one Layer 2 switch will act as the querier.	Drop-down list of ports	N/A

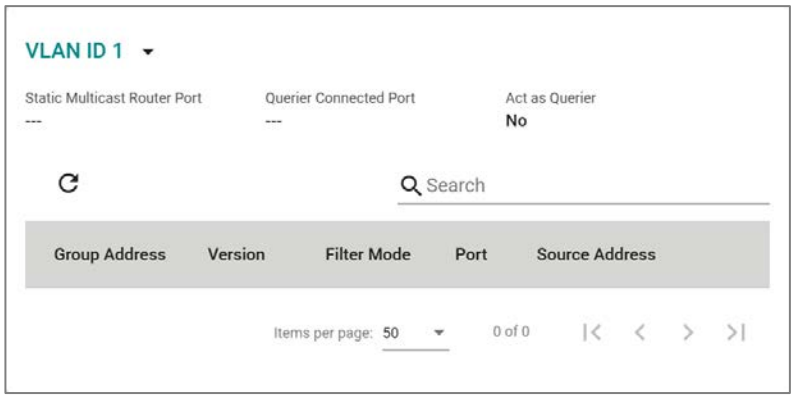
Group Table

Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - Group Table

This page lets you see all currently active IGMP groups that were detected for each VLAN.

VLAN Group Table List

You can use the VLAN drop-down to select which VLAN's group table is displayed.



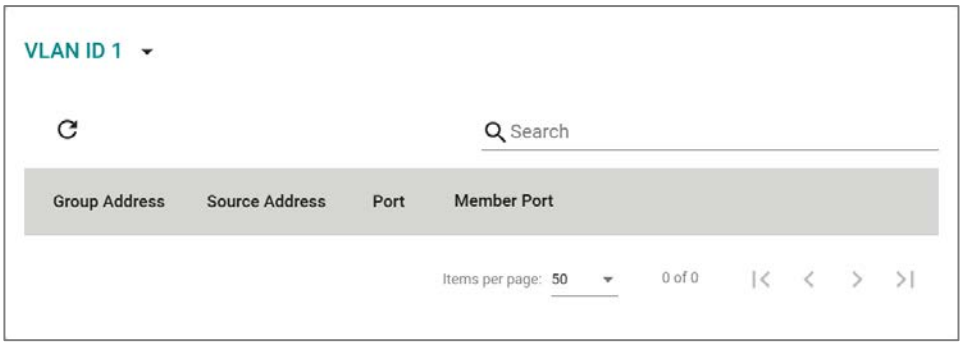
UI Setting	Description
Static Multicast Router Port	Shows the static multicast querier port(s) for the VLAN.
Querier Connected Port	Shows the port which is connected to the querier for the VLAN.
Act as a Querier	Shows whether or not this VLAN has been selected to act as a querier.
Group Address	Shows the multicast group address for the VLAN.
Version	Shows the IGMP snooping version for the group address.
Filter Mode	If IGMP v3 is enabled for the VLAN ID, this shows whether the group address is Included or Excluded.
Port	Shows which port is a member of the group address. Multiple ports will be shown on separate rows.
Source Address	When IGMP v3 is enabled, this shows the multicast source address for the group address.

Forwarding Table

Menu Path: Network Configuration > Layer 2 Switching > Multicast > IGMP Snooping - Forwarding Table

This page lets you see the multicast stream forwarding status for each VLAN.

You can use the VLAN drop-down to select which VLAN's forwarding table is displayed.



UI Setting	Description
Group Address	Shows the multicast group IP address.
Source Address	Shows the IP address the multicast group will receive multicast streams from.
Port	Shows the port receiving the multicast stream.
Member Port	Shows the port the multicast stream is forwarded to.

Static Multicast Table

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

This page lets you manage your device's static multicast entries.

> **Note**
>
> 01:00:5E:XX:XX:XX addresses on this page are for IP multicast MAC addresses. We recommend enabling IGMP Snooping for automatic classification.

Note

Please note that settings and available options will vary depending on the product model.

Note

Moxa's Router Series devices manage MAC address learning for VLANs using IVL (Independent VLAN Learning), which uses separate MAC address tables for each VLAN so that MAC address learning for different VLANs do not interfere with each other. This allows the same MAC address to be used in multiple VLANs without causing forwarding issues.

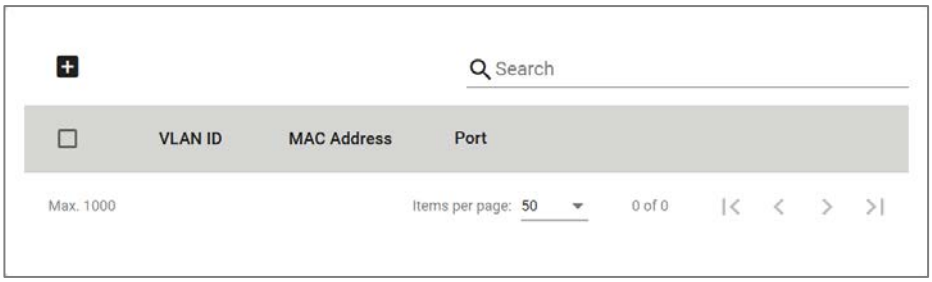
This may lead to a larger MAC address table size, as each VLAN maintains its own individual address table, and the number of MAC address entries will increase based on the number of VLAN member ports used.

Limitations

You can create up to 256 static multicast entries, though some models may support up to 1000 static multicast entries.

The number of entries is calculated as follows: Number of MAC address entries * Number of VLAN IDs

For example, if the static multicast table contains 30 MAC addresses and is connected to 4 VLAN IDs, then the number of MAC address entries would be 30 MAC addresses * 4 VLAN IDs = 120 static multicast entries.



UI Setting	Description
VLAN ID	Shows the VLAN ID used for the static multicast entry.
MAC Address	Shows the MAC address used for the static multicast entry.
Port	Shows which ports are included for the static multicast entry.

Static Multicast Table - Create Static Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

Clicking the **Add (+)** icon on the **Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table** page will open this dialog box. This dialog lets you add a static multicast entry.

Click **CREATE** to save your changes and add the new static multicast entry.

UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static multicast MAC address.	Valid multicast MAC address	N/A
Port	Specify which ports you want to include in the static multicast group.	Drop-down list of ports	N/A

Static Multicast Table - Edit Static Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

Clicking the **Edit (✎)** icon for an account on the **Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table** page will open this dialog box. This dialog lets you edit an existing static multicast entry.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static multicast MAC address.	Valid multicast MAC address	N/A
Port	Specify which ports you want to include in the static multicast group.	Drop-down list of ports	N/A

Static Multicast Table - Delete Static Multicast

Menu Path: Network Configuration > Layer 2 Switching > Multicast > Static Multicast Table

You can delete user accounts by using the checkboxes to select the accounts you want to delete, then clicking the **Delete (🗑)** icon.

Network Interfaces

Menu Path: Network Configuration > Network Interfaces

This page lets you configure the settings for the various interfaces of your device.

This page includes these tabs:

- LAN
- WAN/WAN1
- WAN2/DMZ
- Bridge
- MTU Configuration

- Secondary IP
- Virtual Interface

LAN

Menu Path: Network Configuration > Network Interfaces - LAN

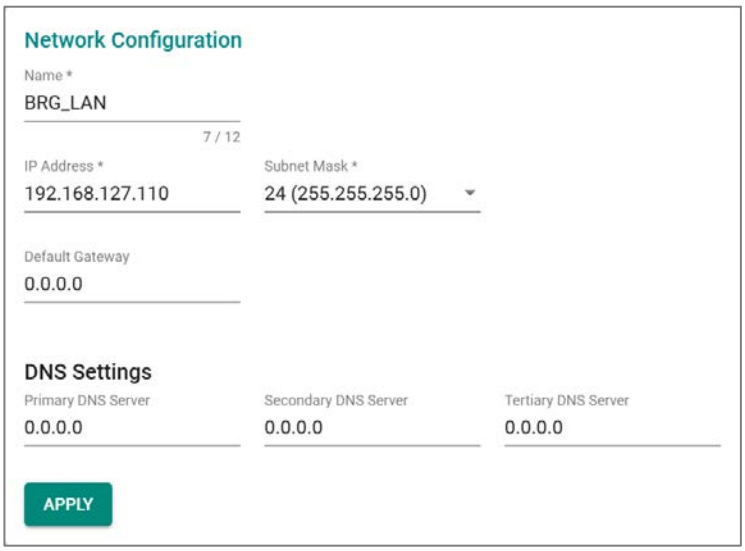
This page lets you manage your LAN interfaces.

> **Note**
>
> The VLAN ID of the first LAN interface configured will be set as the management VLAN ID.

> **Limitations**
>
> EDR, NAT, OnCell, and TN Series: You can create up to 32 LAN interfaces by configuring each port with unique VLAN ID numbers.

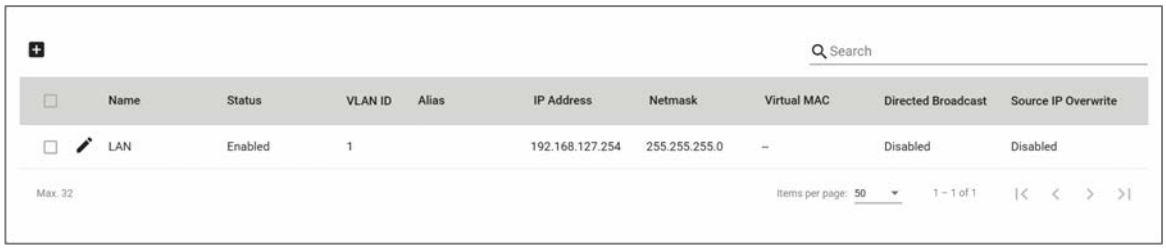
> **Note**
>
> For the TN-4900 Series, when the Connection Type is set to Dynamic IP for an interface, the interface's information including the IP and the file name/file server (Option 66/67) can be checked through the CLI interface.

Network Configuration (EDF Series)



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
IP Address	Specify the IP address of the interface.	Valid IP address	N/A
Subnet Mask	Select the subnet mask of the interface.	Drop-down list of subnet masks	24 (255.255.255.0)
Default Gateway	Specify the IP address of the default gateway for the interface.	Valid IP address	0.0.0.0
Primary/Secondary/Tertiary DNS Server	Specify the IP address of the primary/secondary/tertiary DNS server for the interface.	Valid IP address	0.0.0.0

LAN Interface List (EDR, NAT, OnCell, TN Series)



UI Setting	Description
Name	Shows the name of the interface.
Status	Shows the status of the interface.
VLAN ID	Shows the VLAN ID used for the interface.
Alias	Shows the alias for the interface.
IP Address	Shows the IP address of the interface.
Netmask	Shows the subnet mask of the interface.
Virtual MAC	Shows the virtual MAC address of the interface.
Directed Broadcast	Shows whether directed broadcast is enabled for the interface.

UI Setting	Description
Source IP Overwrite	Shows whether source IP overwrite is enabled for the interface.

LAN - Create LAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - LAN

Clicking the **Add (⊞)** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you create new LAN interface entries for your device.

Click **CREATE** to save your changes and add the new interface.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A

UI Setting	Description	Valid Range	Default Value
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00
Connection Type (TN Series)	Select the connection type for the interface.	Static IP / Dynamic IP	Static IP
Directed Broadcast	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled
IP Address (If Connection Type is Static IP)	Specify the IP address of the interface.	Valid IP address	N/A
Netmask (If Connection Type is Static IP)	Select the subnet mask of the interface.	Drop-down list of subnet masks	24 (255.255.255.0)
DHCP Client Option 66/67 (If Connection Type is Dynamic IP)	Enable or disable DHCP Client Option 66/67 for the interface, if the device supports it.	Enabled / Disabled	Disabled
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	Disabled

LAN - Edit LAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - LAN

Clicking the **Edit ( )** icon on the **Network Configuration > Network Interfaces - LAN** page will open this dialog box. This dialog lets you edit an existing LAN interface entry for your device.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface.	1 to 12 characters	N/A
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	1 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address of the interface.	Valid MAC address	00:00:00:00:00:00
Connection Type (TN Series)	Select the connection type for the interface.	Static IP / Dynamic IP	Static IP
Directed Broadcast	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
IP Address **(If Connection Type is Static IP)**	Specify the IP address of the interface.	Valid IP address	N/A
Netmask **(If Connection Type is Static IP)**	Select the subnet mask of the interface.	Drop-down list of subnet masks	24 (255.255.255.0)
DHCP Client Option 66/67 **(If Connection Type is Dynamic IP)**	Enable or disable DHCP Client Option 66/67 for the interface, if the device supports it.	Enabled / Disabled	Disabled
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	Disabled

Delete LAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - LAN

You can delete interfaces by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete (🗑)** icon.

WAN/WAN1

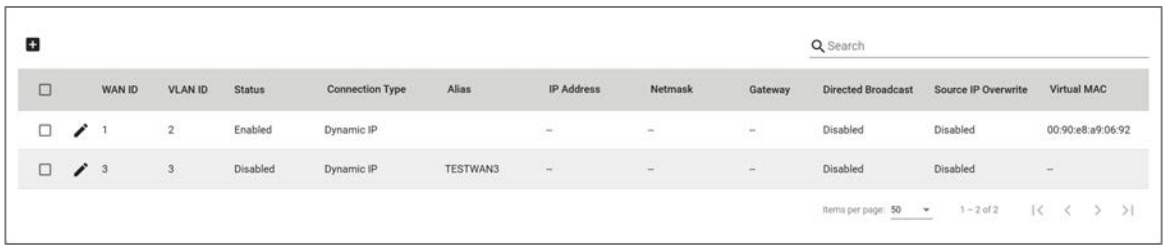
Menu Path: Network Configuration > Network Interfaces - WAN/WAN1

This page lets you configure the settings for the WAN interfaces of your device. WAN interfaces are VLAN-based; when WAN is enabled for a VLAN ID, all ports associated with that VLAN ID will act as a single WAN interface.

> **Note**
> This page may appear as WAN or WAN1 depending on your product model.

There are multiple types of WAN you can select for your **Connection Type**:

- Static IP
- Dynamic IP
- PPPoE



UI Setting	Description
WAN ID	Shows the WAN ID of the interface.
VLAN ID	Shows the VLAN ID used for the interface.
Status	Shows the status of the interface.
Connection Type	Shows the interface's connection type.
Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.
Netmask	Shows the subnet mask of the interface.
Gateway	Shows the gateway of the interface.
Directed Broadcast	Shows whether directed broadcast is enabled for the interface.
Source IP Overwrite	Shows whether source IP overwrite is enabled for the interface.
Virtual MAC	Shows the virtual MAC address of the interface.

Create WAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - WAN/WAN1

Clicking the **Add (⊞)** icon on the **Network Configuration > Network Interfaces - WAN/WAN1** page will open this dialog box. This dialog lets you create new WAN interface entries for your device.

Click **CREATE** to save your changes and add the new interface.

Create WAN Interface - Static IP

If you select **Static IP** as your **Connection Type**, these settings will appear.

VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

Address Information

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for the interface.	Valid IP address	0.0.0.0
Netmask	Select the subnet mask for the interface.	Drop-down list of subnet masksk	N/A
Gateway	Specify the gateway address for the interface.	Valid IP address	0.0.0.0

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

DNS Settings

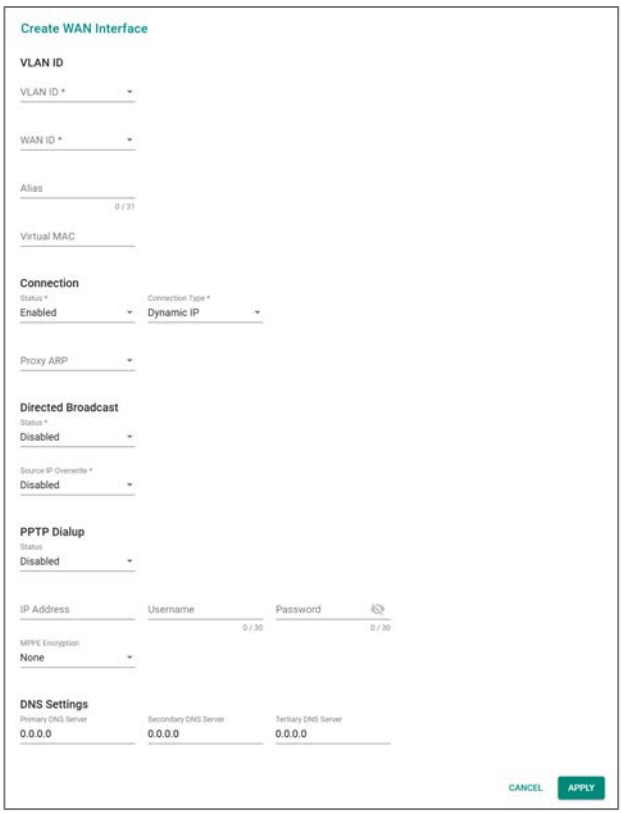
> **Note**
>
> Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Create WAN Interface - Dynamic IP

If you select **Dynamic IP** as your **Connection Type**, these settings will appear.

> **Note**
>
> Please note that settings and available options will vary depending on the product model.



VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

DHCP Client Option 66/67 (TN Series)

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP client option 66/67.	Enabled / Disabled	Disabled

DNS Settings

Note

When using Dynamic IP, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the DHCP server.

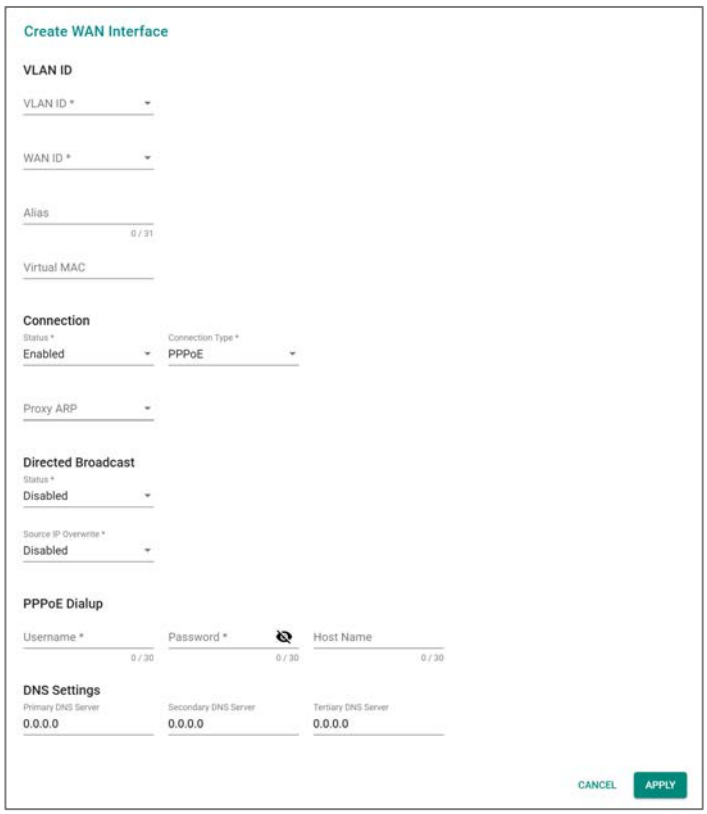
Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Create WAN Interface - PPPoE

If you select **PPPoE** as your **Connection Type**, these settings will appear.



VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPPoE Dialup

UI Setting	Description	Valid Range	Default Value
User Name	Specify the username used to connect to the PPPoE service.	1 to 30 characters	N/A
Password	Specify the password used to connect to the PPPoE service.	1 to 30 characters	N/A
Host Name	Specify the hostname of the PPPoE server.	1 to 30 characters	N/A

DNS Settings

Note

When using PPPoE, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the PPPoE server.

Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Edit WAN Interface Entry

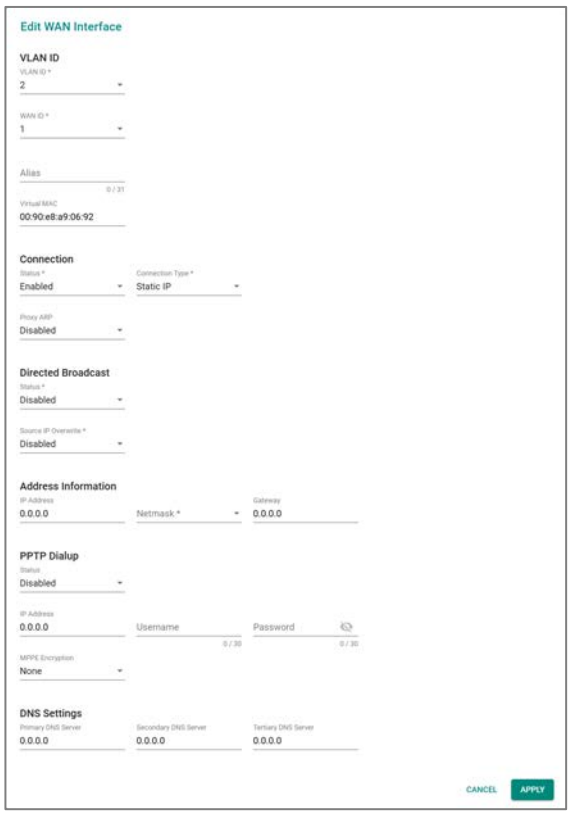
Menu Path: Network Configuration > Network Interfaces - WAN/WAN1

Clicking the **Edit ( )** icon on the **Network Configuration > Network Interfaces - WAN/WAN1** page will open this dialog box. This dialog lets you edit an existing WAN interface for your device.

Click **APPLY** to save your changes.

Edit WAN Interface - Static IP

If you select **Static IP** as your **Connection Type**, these settings will appear.



VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

Address Information

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for the interface.	Valid IP address	0.0.0.0
Netmask	Select the subnet mask for the interface.	Drop-down list of subnet masksk	N/A
Gateway	Specify the gateway address for the interface.	Valid IP address	0.0.0.0

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

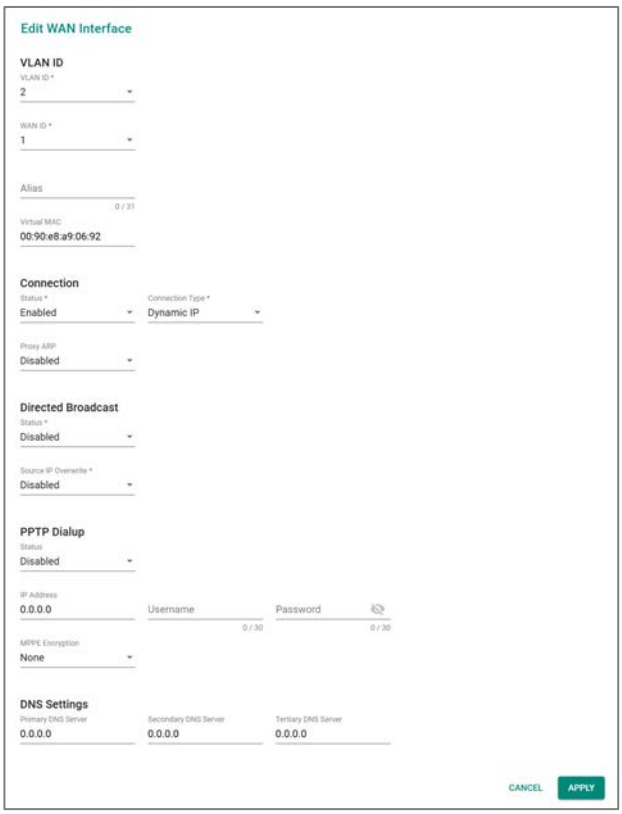
DNS Settings

> **Note**
>
> Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Edit WAN Interface - Dynamic IP

If you select **Dynamic IP** as your **Connection Type**, these settings will appear.



VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

DHCP Client Option 66/67 (TN Series)

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP client option 66/67.	Enabled / Disabled	Disabled

DNS Settings

Note

When using Dynamic IP, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the DHCP server.

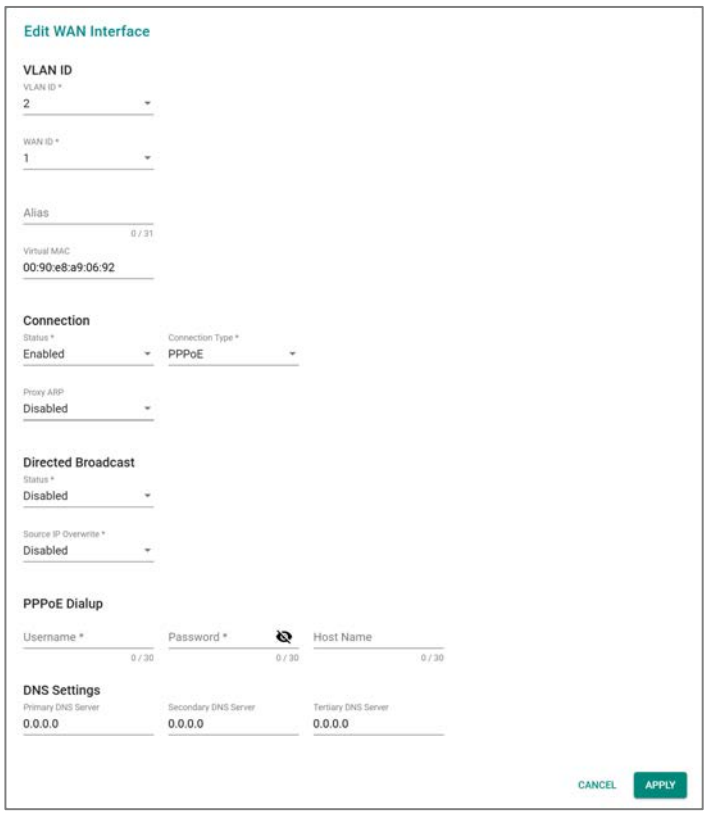
Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Edit WAN Interface - PPPoE

If you select **PPPoE** as your **Connection Type**, these settings will appear.



VLAN ID

UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID to use for the WAN interface.	Drop-down list of VLAN IDs	N/A
WAN ID	Select a WAN ID to use for the interface.	Drop-down list of WAN IDs	N/A
Alias	Specify an alias to help identify the interface.	0 to 31 characters	N/A
Virtual MAC	Specify the virtual MAC address for the interface.	Valid MAC address	00.00.00.00.00.00

Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable proxy ARP for the interface.	Enabled / Disabled	N/A

Directed Broadcast

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed broadcast for the interface.	Enabled / Disabled	Disabled
Source IP Overwrite	Enable or disable source IP overwrite for the interface.	Enabled / Disabled	Disabled

PPPoE Dialup

UI Setting	Description	Valid Range	Default Value
User Name	Specify the username used to connect to the PPPoE service.	1 to 30 characters	N/A
Password	Specify the password used to connect to the PPPoE service.	1 to 30 characters	N/A
Host Name	Specify the hostname of the PPPoE server.	1 to 30 characters	N/A

DNS Settings

Note

When using PPPoE, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the PPPoE server.

Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Delete WAN Interface Entry

Menu Path: Network Configuration > Network Interfaces - WAN/WAN1

You can delete interfaces by using the checkboxes to select the interfaces you want to delete, then selecting the **Delete ( )** icon.

WAN2/DMZ

Menu Path: Network Configuration > Network Interfaces - WAN2/DMZ

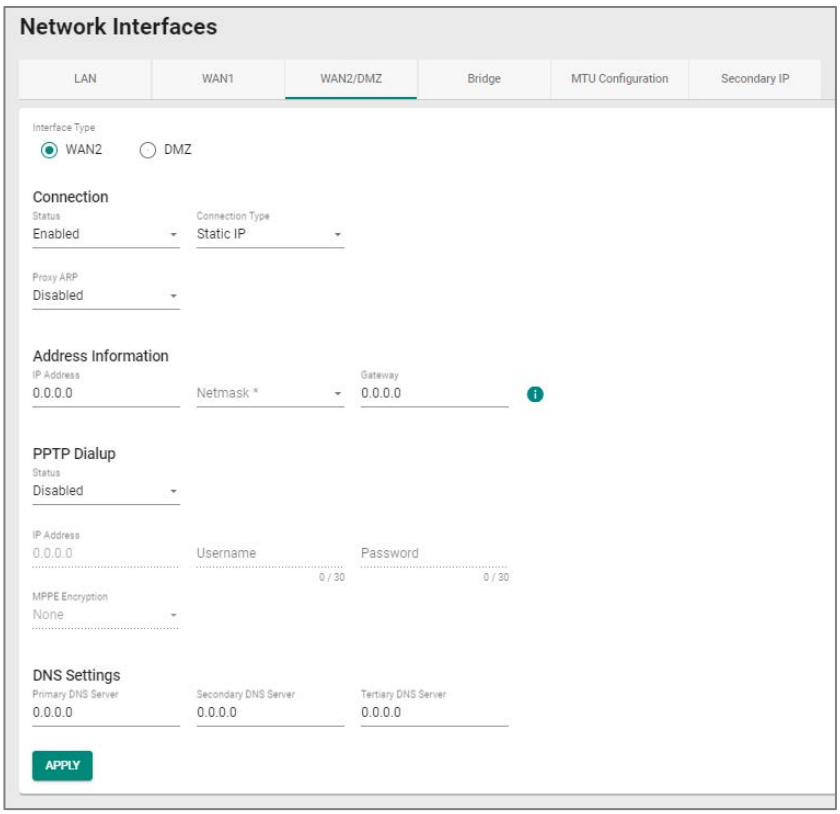
This page lets you configure the settings for the WAN2 or DMZ interfaces of your device. WAN interfaces are VLAN-based; when WAN is enabled for a VLAN ID, all ports associated with that VLAN ID will act as a single WAN interface.

Note

Availability of this feature may vary depending on your product model and version.

Static IP

If you select **WAN2** as the **Interface Type** and **Static IP** for the **Connection Type**, these settings will appear.



Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable the Proxy ARP.	Enabled / Disabled	Disabled

Address Information

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for the interface.	Valid IP address	0.0.0.0
Netmask	Select the subnet mask for the interface.	Drop-down list of subnet masksk	N/A
Gateway	Specify the gateway address for the interface.	Valid IP address	0.0.0.0

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

DNS Settings

Note

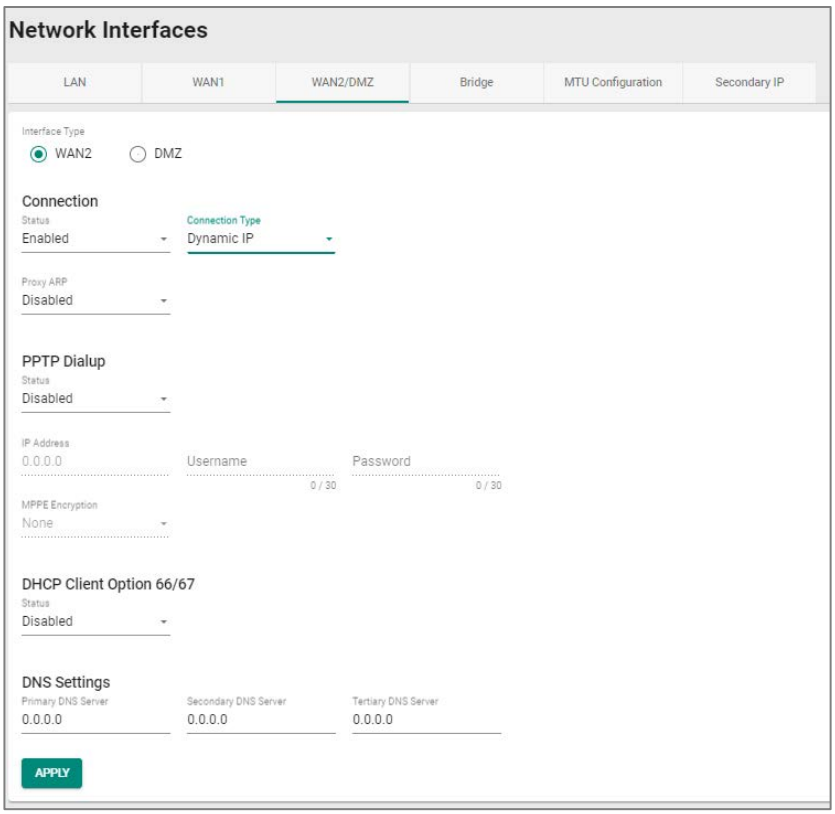
Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

Dynamic IP

If you select **WAN2** as the **Interface Type** and **Dynamic IP** for the **Connection Type**, these settings will appear.



Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable the Proxy ARP.	Enabled / Disabled	Disabled

PPTP Dialup

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PPTP connection for the interface.	Enabled / Disabled	Disabled
IP Address	Specify the PPTP service IP address.	Valid IP address	0.0.0.0
User Name	Enter the username to use for dialing in to the PPTP service.	1 to 30 characters	N/A
Password	Enter the password to use for dialing in to the PPTP service.	1 to 30 characters	N/A
MPPE Encrytion	Enable or disable MPPE encryption.	None / Encrypt	None

DHCP Client Option 66/67 (TN Series)

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP client option 66/67.	Enabled / Disabled	Disabled

DNS Settings

Note

When using Dynamic IP, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the DHCP server.

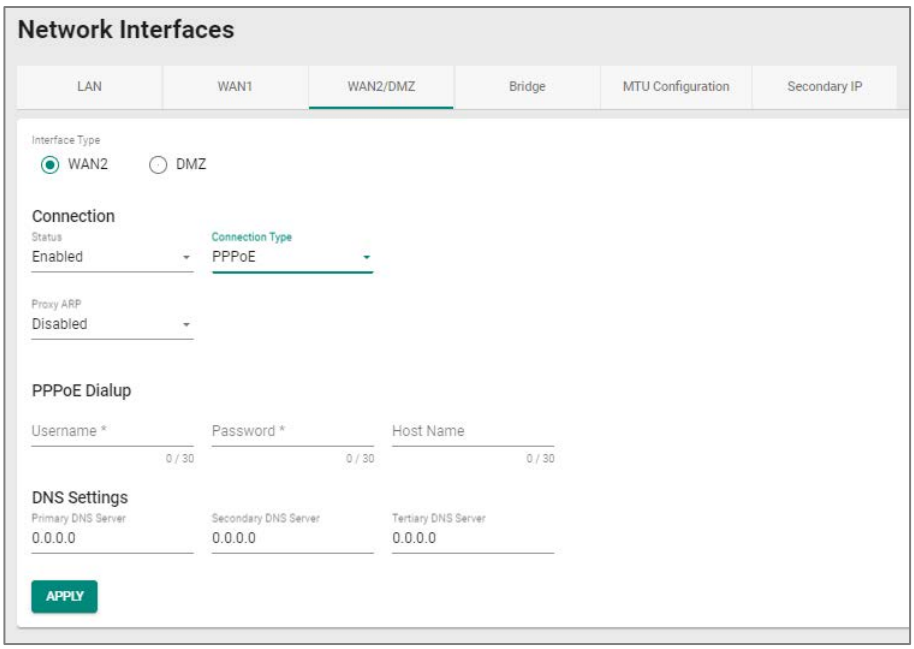
Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

PPPoE

If you select **WAN2** as the **Interface Type** and **PPPoE** for the **Connection Type**, these settings will appear.



Connection

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the WAN interface.	Enabled / Disabled	Enabled
Connection Type	Specify the connection type to use for the connection.	Static IP / Dynamic IP / PPPoE	Dynamic IP
Proxy ARP	Enable or disable the Proxy ARP.	Enabled / Disabled	Disabled

PPPoE Dialup

UI Setting	Description	Valid Range	Default Value
User Name	Specify the username used to connect to the PPPoE service.	1 to 30 characters	N/A

UI Setting	Description	Valid Range	Default Value
Password	Specify the password used to connect to the PPPoE service.	1 to 30 characters	N/A
Host Name	Specify the hostname of the PPPoE server.	1 to 30 characters	N/A

DNS Settings

Note

When using PPPoE, you can manually configure DNS servers here. Manually configured DNS servers will have a higher priority than DNS servers coming from the PPPoE server.

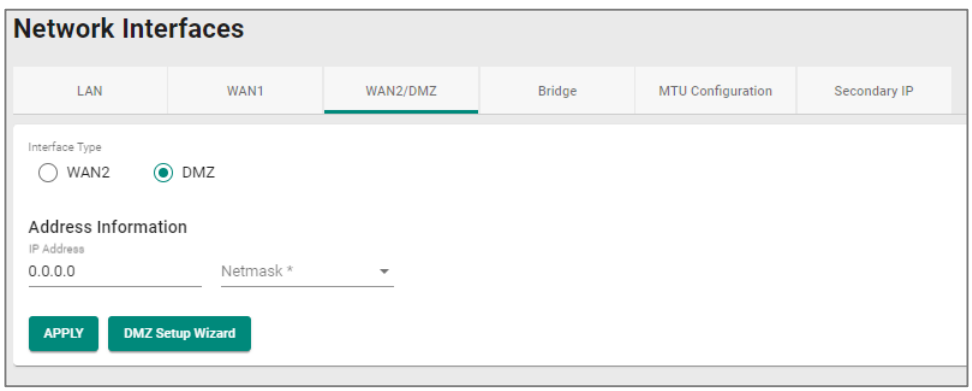
Note

Duplicate DNS server addresses other than 0.0.0.0 are not allowed.

UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the primary DNS IP address.	IP Address	0.0.0.0
Secondary DNS Server	Specify the secondary DNS IP address.	IP Address	0.0.0.0
Tertiary DNS Server	Specify the tertiary DNS IP address.	IP Address	0.0.0.0

DMZ

If you select **DMZ** as the **Interface Type**, these settings will appear.



Address Information

UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address for the interface.	Valid IP address	0.0.0.0
Netmask	Specify the subnet mask for the interface.	Valid subnet mask	N/A

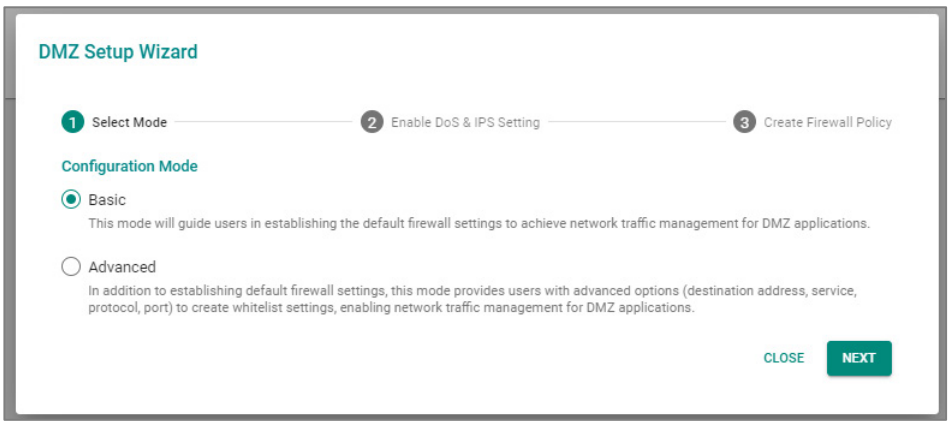
DMZ Setup Wizard

Menu Path: Network Configuration > Network Interfaces - WAN2/DMZ

Clicking the **DMZ Setup Wizard** button on the **Network Configuration > Network Interfaces - WAN2/DMZ** page will start a wizard to help you configure security policies for the DMZ.

Step 1: Select Mode

Select between basic or advanced configuration mode.



Step 2: Enable DoS & IPS Setting

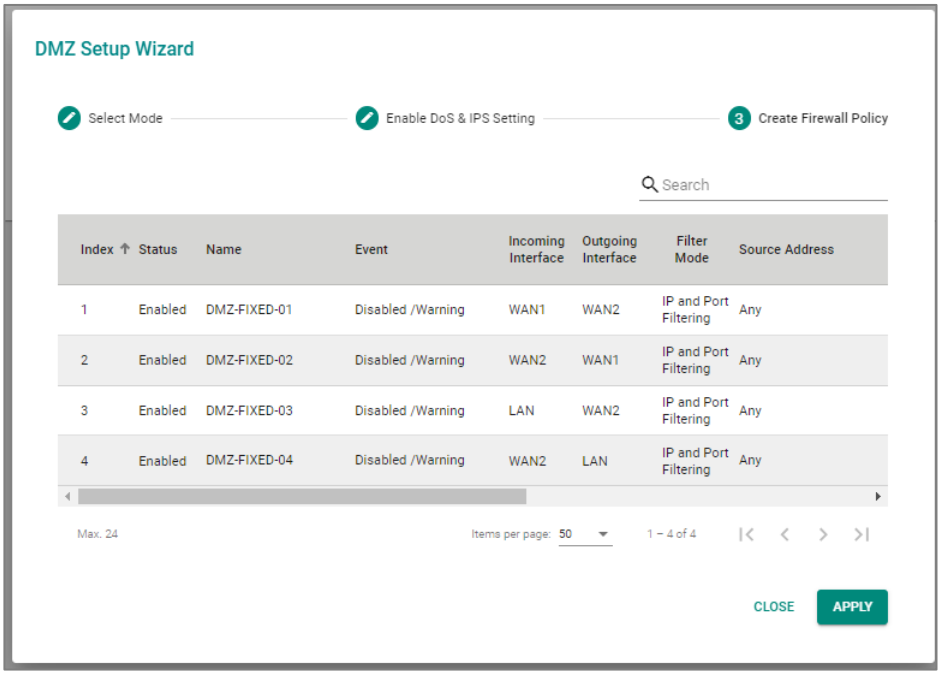
Select whether to enable DoS protection and IPS functionality.

Step 3: Create Firewall Policy

Basic Mode

In basic mode, four policies are preconfigured for you so you don't need to set them manually.

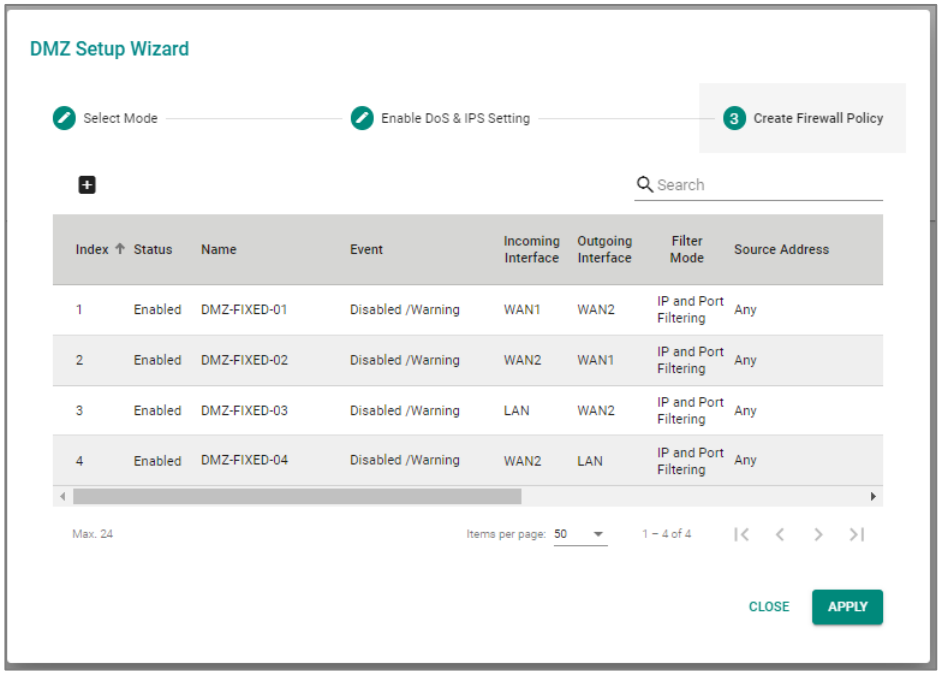
- WAN1 to DMZ (Allow)
- DMZ to WAN1 (Allow)
- LAN to DMZ (Allow)
- DMZ to LAN (Deny)



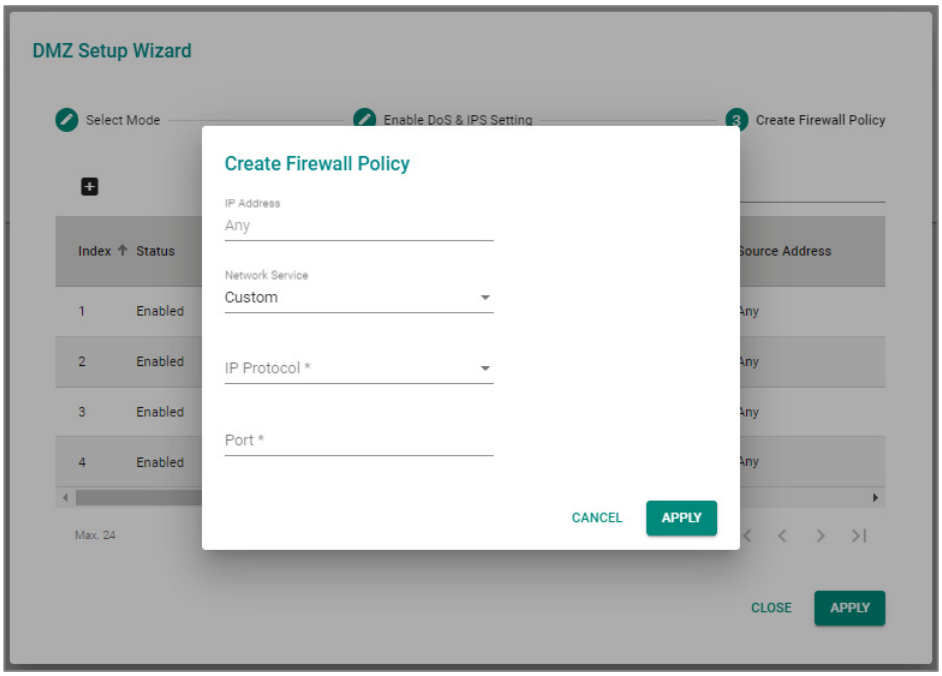
Advanced Mode

In advanced mode, you will need to set up the correct destination address, service, protocol, and port whitelist policies according to each policy's requirements.

- WAN1 to DMZ (Deny)
- DMZ to WAN1 (Allow)
- LAN to DMZ (Deny)
- DMZ to LAN (Deny)



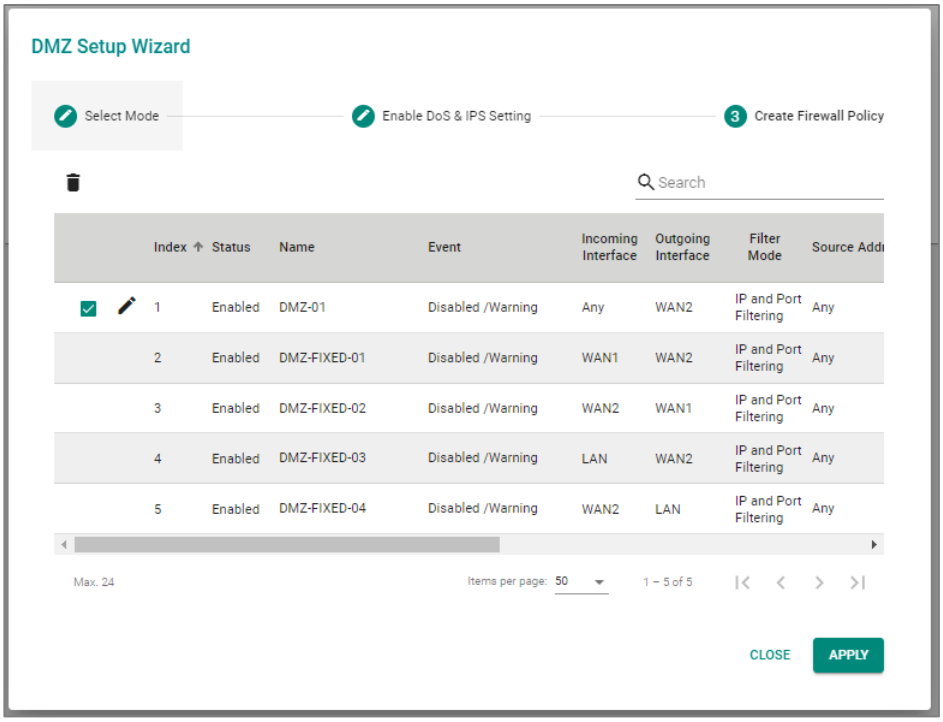
You can also click the **Add (⊞)** button to add additional firewall policies.



UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address.	Valid IP address	Any
Network Service	Specify the network service.	Custom / TELNET / SSH / SMTP / FTP / HTTP / HTTPS / DNS	Custom

UI Setting	Description	Valid Range	Default Value
IP Protocol	Specify the IP protocol.	TCP / UDP / TCP and UDP	N/A
Port	Specify the port number.	Valid port number	N/A

To delete a firewall policy, select the checkbox next to it and click the **Delete (🗑)** button.



After confirming your changes, click the **APPLY** button to save your changes and finish the setup wizard.

Bridge

Menu Path: Network Configuration > Network Interfaces - Bridge

This page lets you configure a bridge for your device.

You can set up these kinds of bridges:

- Port-based
- Zone-based

Limitations

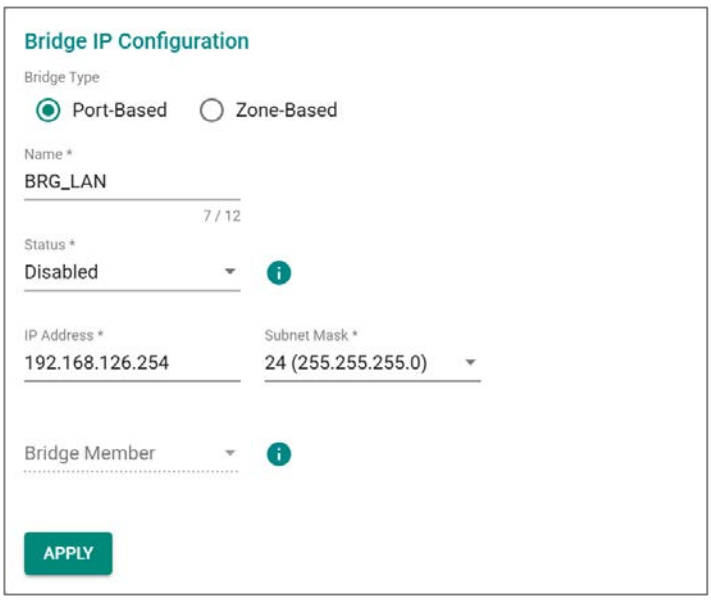
You can create up to 8 sets of zone-based bridges.

Port-Based

If you select **Port-Based** as your **Bridge Type**, these settings will appear. Port-based bridges allow the device's firewall to filter traffic moving between bridge member ports.

Note

If a port is configured as a bridge interface member, it cannot be used for L2 redundancy features (Turbo Ring, Turbo Chain, or RSTP).

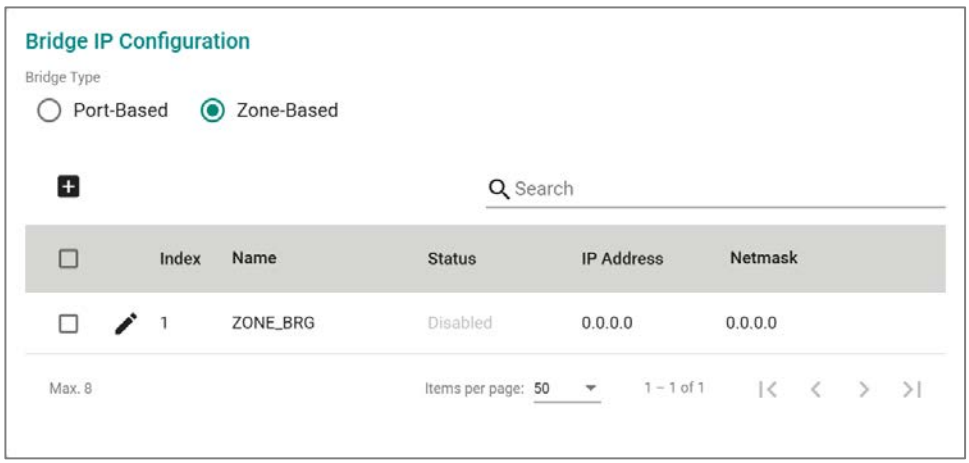


UI Setting	Description	Valid Range	Default Value
Bridge Type	Select which bridge type you want to use.	Port-Based / Zone-Based	N/A
Name	Specify a name for the bridge.	1 to 12 characters	BRG_LAN

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the bridge.	Enabled / Disabled	Disabled
IP Address	Specify an IP address for the bridge.	Valid IP address	192.168.126.254
Subnet Mask	Specify a subnet mask for the bridge.	Valid subnet mask	24(255.255.255.0)
Bridge Member	Select which ports will be members of the bridge.	Drop-down list of ports	N/A

Zone-based Bridges List

If you select **Zone-Based** as your **Bridge Type**, these settings will appear. Zone-based bridges allow you to create zones based on VLANs. The device's firewall can filter traffic moving between different zones.



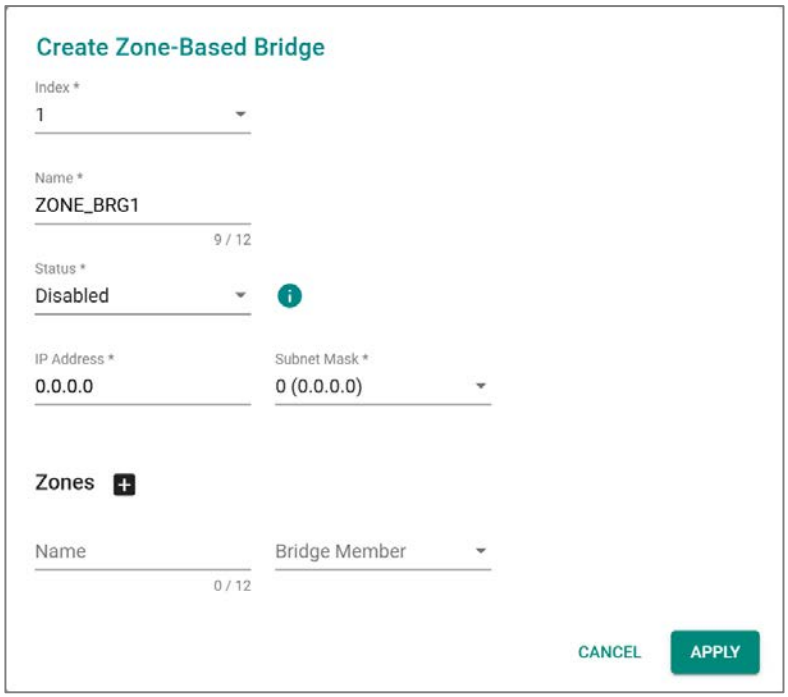
UI Setting	Description
Index	Shows the index for the bridge.
Name	Shows the name of the bridge.
Status	Shows the status of the bridge.
IP Address	Shows the IP address of the bridge.
Netmask	Shows the netmask of the bridge.

Create Zone-Based Bridge

Menu Path: Network Configuration > Network Interfaces - Bridge

Clicking the **Add (⊕)** icon on the **Network Configuration > Network Interfaces - Bridge** page will open this dialog box. This dialog lets you create new Zone-Based Bridge interface entries for your device.

Click **CREATE** to save your changes and add the new interface.



UI Setting	Description	Valid Range	Default Value
Index	Specify an index for the bridge.	1 to 8	1
Name	Specify a name for the bridge.	1 to 12 characters	ZONE_BRG
Status	Enable or disable the bridge. **Note** When a bridge interface is disabled, the associated policies are also removed.	Enabled / Disabled	Disabled
IP Address	Specify an IP address for the bridge.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Subnet Mask	Specify a subnet mask for the bridge.	Drop-down list of subnet masks	0 (0.0.0.0)

Zones

You can configure multiple zones for the bridge. Click the add icon ( ) to add a new entry. Select the delete icon ( ) for an entry to delete it.

Limitations

You can configure up to 8 zones per zone-based bridge.

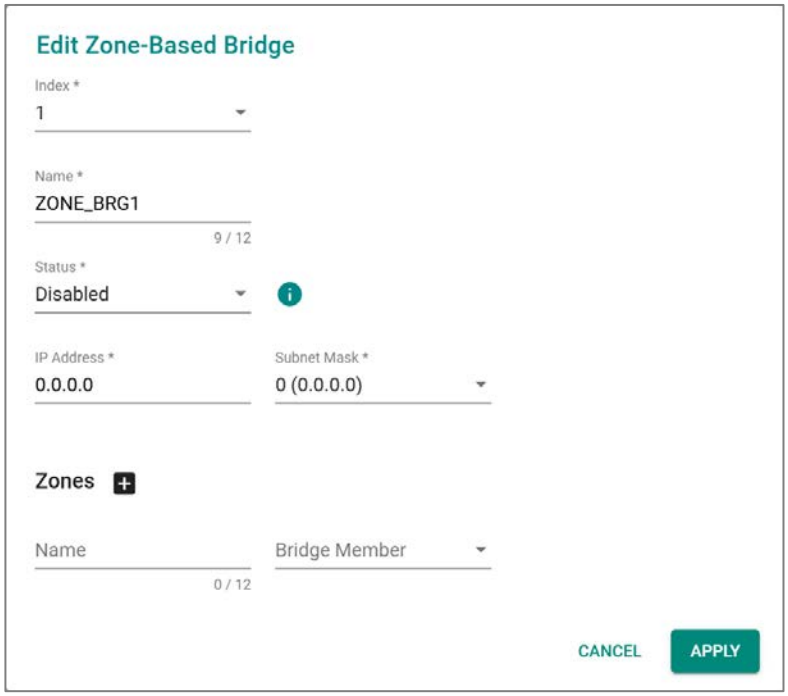
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the bridge zone.	1 to 12 characters	N/A
Bridge Member	Select which VLAN will determine the members of this zone.	Drop-down list of VLANs	N/A

Edit Zone-Based Bridge

Menu Path: Network Configuration > Network Interfaces - Bridge

Clicking the **Edit ( )** icon on the **Network Configuration > Network Interfaces - Bridge** page will open this dialog box. This dialog lets you edit an existing Zone-Based Bridge interface entry for your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify an index for the bridge.	1 to 8	1
Name	Specify a name for the bridge.	1 to 12 characters	ZONE_BRG
Status	Enable or disable the bridge. **Note** When a bridge interface is disabled, the associated policies are also removed.	Enabled / Disabled	Disabled
IP Address	Specify an IP address for the bridge.	Valid IP address	0.0.0.0
Subnet Mask	Specify a subnet mask for the bridge.	Drop-down list of subnet masks	0 (0.0.0.0)

Zones

You can configure multiple zones for the bridge. Click the add icon ( ) to add a new entry. Select the delete icon ( ) for an entry to delete it.

Limitations

You can configure up to 8 zones per zone-based bridge.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the bridge zone.	1 to 12 characters	N/A
Bridge Member	Select which VLAN will determine the members of this zone.	Drop-down list of VLANs	N/A

Delete Zone-Based Bridge

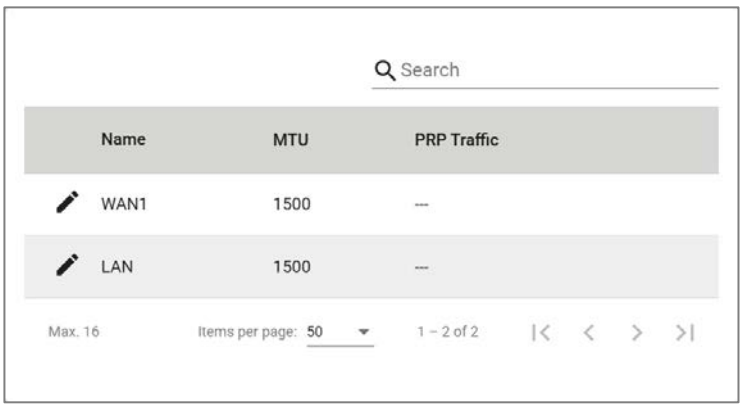
Menu Path: Network Configuration > Network Interfaces - Bridge

You can delete interfaces by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete ( )** icon.

MTU Configuration

Menu Path: Network Configuration > Network Interfaces - MTU Configuration

This page lets you configure the MTU settings for your interfaces.



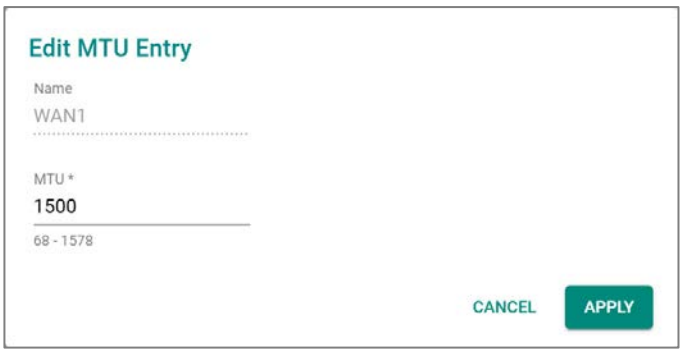
UI Setting	Description
Name	Shows the name of the interface.
MTU	Shows the MTU size used for the interface.
PRP Traffic	Shows the PRP traffic status for the interface.

MTU Configuration - Edit MTU Entry

Menu Path: Network Configuration > Network Interfaces - MTU Configuration

Clicking the **Edit ( )** icon for an interface on the **Network Configuration > Network Interfaces - MTU Configuration** page will open this dialog box. This dialog lets you edit the MTU settings for an interface.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Shows the name of of this interface. This setting cannot be changed here.	N/A	Name of interface
MTU	Specify the MTU size to use for the interface. **Note** Jumbo Frames are not currently supported.	68 to 1578	1500

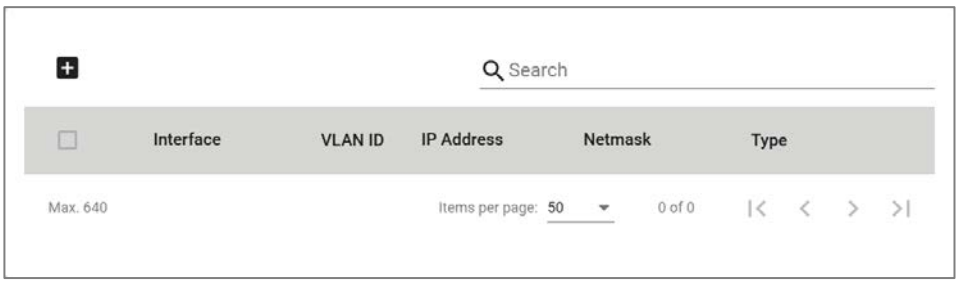
Secondary IP

Menu Path: Network Configuration > Network Interfaces - Secondary IP

This page lets you create secondary IPs for your interfaces. The Layer 3 interface can act as a secondary IP for a network interface, allowing a single interface to communicate with multiple networks, increasing network flexibility and availability.

Limitations

- EDR, OnCell, and TN Series: You can create up to 640 secondary IPs.
- NAT Series: you can create up to 256 secondary IPs.



UI Setting	Description
Interface	Shows which interface the secondary IP is for.
VLAN ID	Shows the VLAN ID used for the interface.
IP Address	Shows the secondary IP address for the interface.
Netmask	Shows the subnet mask of the secondary IP.
Type	Shows the type of the secondary IP.

Secondary IP - Create Secondary IP Entry

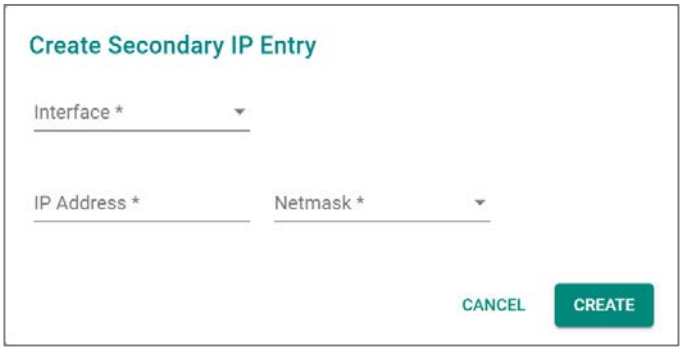
Menu Path: Network Configuration > Network Interfaces - Secondary IP

Clicking the **Add (+)** icon on the **Network Configuration > Network Interfaces - Secondary IP** page will open this dialog box. This dialog lets you create a secondary IP for an interface.

Click **CREATE** to save your changes and add the new secondary IP.

Limitations

- EDR, OnCell, and TN Series: You can create up to 640 secondary IPs.
- NAT Series: you can create up to 256 secondary IPs.



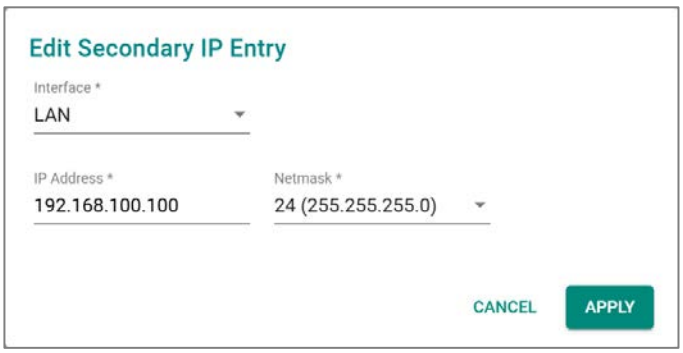
UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Select the subnet mask of the secondary interface.	Drop-down list of subnet masks	N/A

Secondary IP - Edit Secondary IP Entry

Menu Path: Network Configuration > Network Interfaces - Secondary IP

Clicking the **Edit ( )** icon on the **Network Configuration > Network Interfaces - Secondary IP** page will open this dialog box. This dialog lets you edit an existing secondary IP entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Interface	Select which interface the secondary IP is for.	Drop-down list of interfaces	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Select the subnet mask of the secondary interface.	Drop-down list of subnet masks	N/A

Delete Secondary IP

Menu Path: Network Configuration > Network Interfaces - Secondary IP

You can delete secondary IP entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Virtual Interface

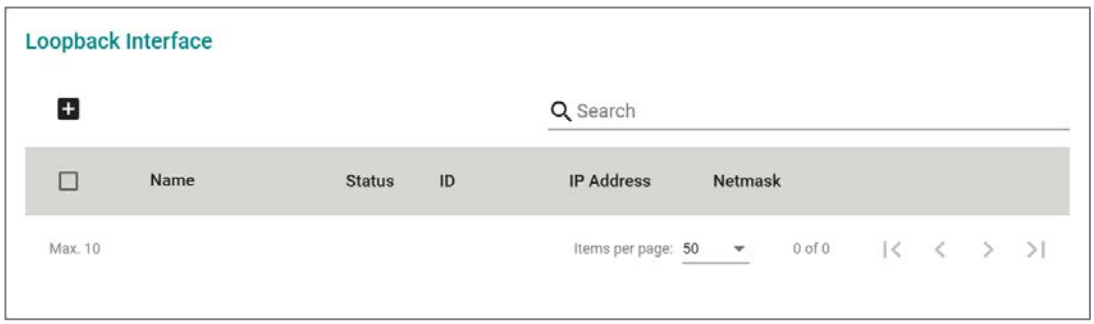
Menu Path: Network Configuration > Network Interfaces - Virtual Interface

This page lets you create virtual interfaces for your device.

Limitations

You can create up to 10 loopback interfaces.

Loopback Interface List



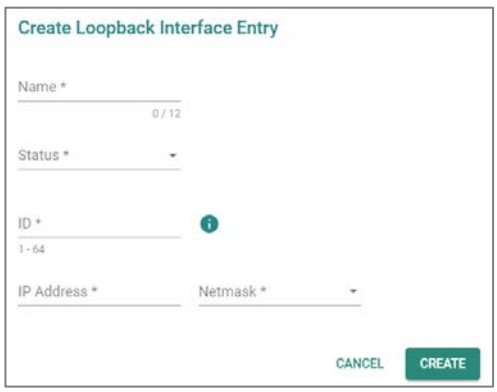
UI Setting	Description
Name	Shows the name of the loopback interface.
Status	Shows whether the loopback interface is enabled or disabled.
ID	Specify the ID of the loopback interface.
IP Address	Specify the IP address of the loopback interface.
Netmask	Specify the subnet mask of the loopback interface.

Create Loopback Interface Entry

Menu Path: Network Configuration > Network Interfaces - Virtual Interface

Clicking the **Add (⊞)** icon on the **Network Configuration > Network Interfaces - Virtual Interface** page will open this dialog box. This dialog lets you create a loopback interface.

Click **CREATE** to save your changes and add the new interface.

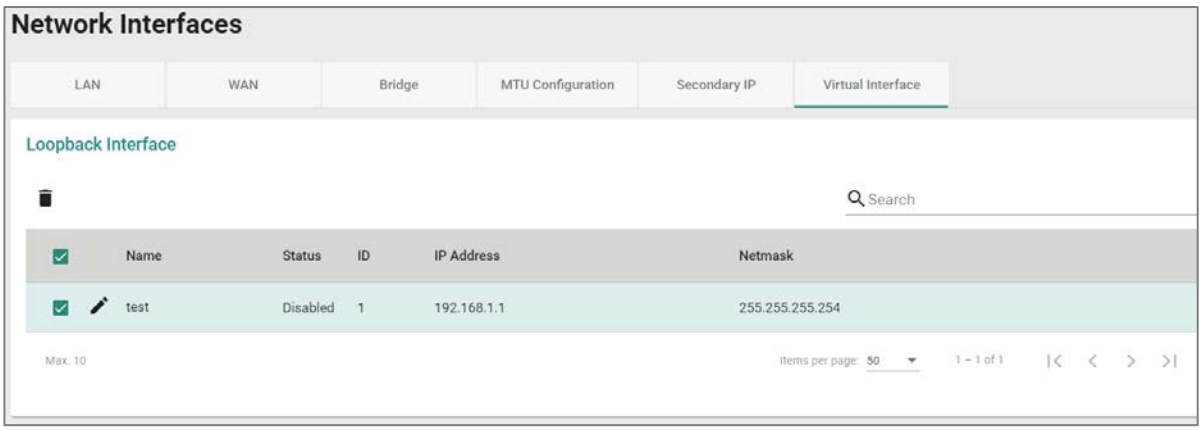


UI Setting	Description	Valid Range	Default Value
Name	Specify the name of the loopback interface.	1 to 12 characters	N/A
Status	Enable or disable the loopback interface.	Enabled / Disabled	N/A
ID	Specify the ID for the loopback interface.	1 to 64	N/A
IP Address	Specify the IP address of the secondary interface.	Valid IP address	N/A
Netmask	Specify the subnet mask of the secondary interface.	Valid subnet mask	N/A

Delete Loopback Interface

Menu Path: Network Configuration > Network Interfaces - Virtual Interface

You can delete an interface by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete ( )** icon.



Redundancy

Menu Path: Redundancy

The Redundancy settings area lets you configure redundancy settings to help you ensure network availability.

This settings area includes these sections:

- Layer 2 Redundancy
- Layer 3 Redundancy
- WAN Redundancy
- High Availability

Redundancy - User Privileges

Privileges to Redundancy settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring V2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
Layer 3 Redundancy			
VRRP	R/W	R/W	R
WAN Redundancy	R/W	R/W	R

Layer 2 Redundancy

Menu Path: Redundancy > Layer 2 Redundancy

This section lets you manage various Layer 2 redundancy features for your device.

This section includes these pages:

- Spanning Tree
- Turbo Ring V2
- Turbo Chain

Spanning Tree

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree

This page lets you configure Spanning Tree Protocol (STP) settings for redundancy.

This page includes these tabs:

- General
- Status

Spanning Tree - General

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - General

This page lets you configure spanning tree settings for your device.

Spanning Tree Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Spanning Tree Protocol for the device.	Enabled / Disabled	Enabled
Bridge Priority	Select the bridge priority. Lower numbers represent higher priority. A device with a higher bridge priority has a greater chance of being established as the root of the spanning tree topology.	0 to 61440, in multiples of 4096	32768
Forward Delay Time	Specify the forwarding delay time in seconds. This is the amount of time this device will wait before checking to see if it should change to a different state.	4 to 30	15
Hello Time	Specify the interval in seconds at which the device, if it is currently the root of the spanning tree topology, will send out periodic “Hello” messages to other devices on the network to check if the topology is healthy.	1 to 2	2
Max Age	Specify the maximum age duration in seconds to wait for a "Hello" message from the root of the spanning tree topology before the device will reconfigure itself as root. If two or more devices on the network are recognized as a root, the devices will negotiate to determine which will act as the new root.	6 to 40	20

Spanning Tree List

Note

We recommend that you disable Spanning Tree Protocol on a port if it is connected to a device (such as a PLC or RTU) instead of network equipment, as this may cause unnecessary negotiation.

UI Setting	Description
Port	Shows the port number.

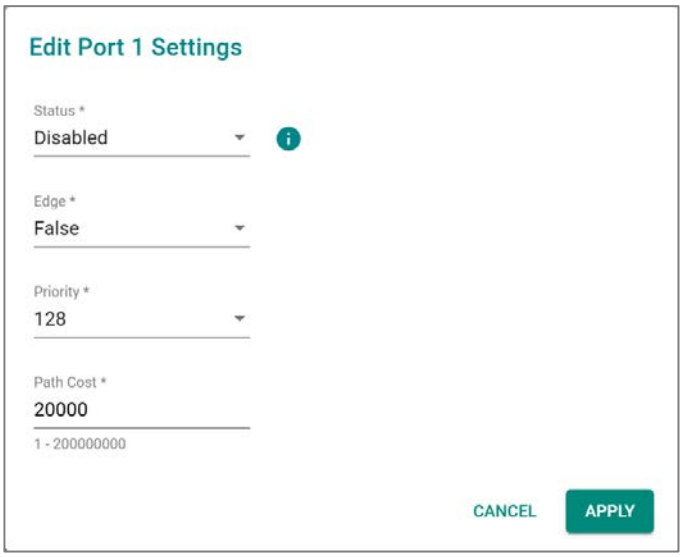
UI Setting	Description
Status	Shows the status of the port as a node in the spanning tree topology.
Edge	Shows whether the port is an edge port or not. • **Force Edge**: The port is fixed as an edge port and will always be in the forwarding state. • **False**: The port is not an edge port.
Priority	Shows the priority of the port. Lower numbers indicate higher priority.
Path Cost	Shows the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.

Spanning Tree - Edit Port Settings

Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - General

Clicking the **Edit ( )** icon for a port on the **Redundancy > Layer 2 Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you configure the spanning tree settings for a port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the port as a node in the spanning tree topology.	Enabled / Disabled	Disabled
Edge	Specify whether the port is an edge port or not. • **Force Edge**: The port is fixed as an edge port and will always be in the forwarding state. • **False**: The port is not an edge port.	Force Edge / False	False
Priority	Specify the priority of the port. Lower numbers indicate higher priority.	0 to 240, in multiples of 16	128
Path Cost	Specify the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.	1 to 200000000	20000 **Note** The default value may vary depending on the maximum speed supported by the port.

Spanning Tree - Status

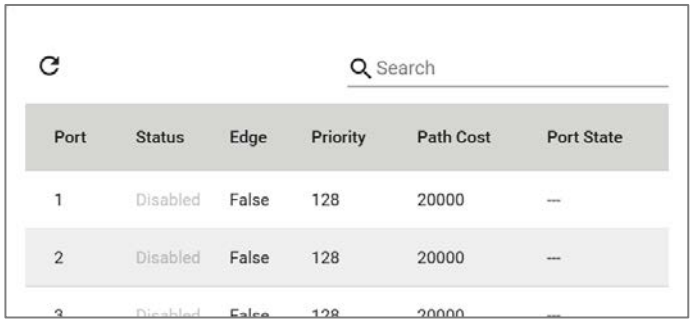
Menu Path: Redundancy > Layer 2 Redundancy > Spanning Tree - Status

This page lets you see the current spanning tree status of your device and its ports.

Root Information

UI Setting	Description
Root State	Shows whether the device is currently acting as the root of the spanning tree topology.

Spanning Tree Port List



UI Setting	Description
Port	Shows the port number.
Enable	Shows whether Spanning Tree Protocol is enabled for the port.
Edge	Shows whether the port is an edge port or not. • **Force Edge**: The port is fixed as an edge port and will always be in the forwarding state. • **True**: The port is currently designated as an edge port. • **False**: The port is not an edge port.
Priority	Shows the priority of the port. Lower numbers indicate higher priority.
Path Cost	Shows the path cost for the port. Higher path costs indicate that this port is less suitable as a node for the spanning tree topology. If set to 0, the path cost will be automatically calculated based on different port speeds.
Port State	Shows the current spanning tree status of the port. • **Forwarding**: Indicates the port is allowing transmissions normally. • **Blocking**: Indicates the port is blocking transmissions.

Turbo Ring V2

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2

This page lets you manage the Turbo Ring V2 redundancy feature for your device.

This page includes these tabs:

- General
- Status

Turbo Ring V2 - General

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General

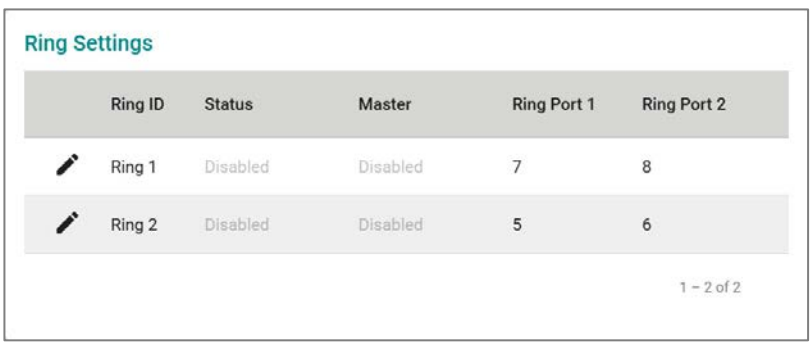
This page lets you configure the Turbo Ring settings for your device.

Turbo Ring Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled

Ring Settings

> **Note**
> To set up a Dual-Ring architecture, you must enable both Ring 1 and Ring 2.



UI Setting	Description
Ring ID	Shows the ring ID.
Status	Shows the status of the ring.

UI Setting	Description
Master	Shows whether this device is designated as the master for the ring.
Ring Port 1	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
Ring Port 2	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection, and will be blocked normally.

Edit Ring Settings

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General

Clicking the **Edit ( )** icon for a ring on the **Redundancy > Layer 2 Redundancy > Turbo Ring V2 - General** page will open this dialog box. This dialog lets you adjust your device's settings for the ring.

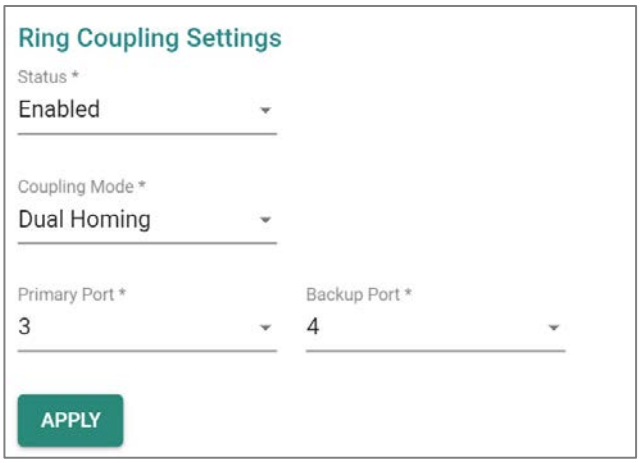
Click **APPLY** to save your changes.

Note

TN Series: Though ports that belong to a port-based bridge may be selected as ring ports, we do not recommend enabling redunancy protocols on these ports as this may cause recovery times to exceed their specification targets. For further details, contact Moxa Technical Support.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
Master	Enable or disable whether this device will be designated as the master for the ring.	Enabled / Disabled	Disabled
Ring Port 1	Specify which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.	Drop-down list of ports	7
Ring Port 2	Specify which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection, and will be blocked normally.	Drop-down list of ports	8

Ring Coupling Settings



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled

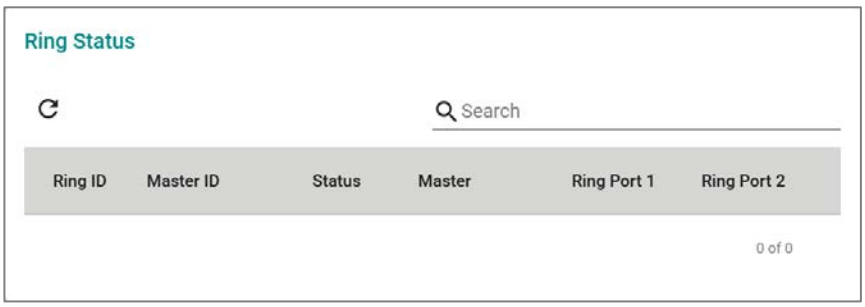
UI Setting	Description	Valid Range	Default Value
Coupling Mode **(If Status is Enabled)**	Specify the coupling mode for the device. • **Dual Homing**: This device will handle both the primary path and backup path for ring coupling. • **Backup Path**: This device only handles the backup path for ring coupling; the primary path will be handled by another device. • **Primary Path**: This device only handles the primary path for ring coupling; the backup path will be handled by another device.	Dual Homing / Backup Path / Primary Path	N/A
Primary Port **(If Coupling Mode is Dual Homing)**	Specify the port that connects to the primary path for ring coupling.	Select a port from the drop-down menu	3
Backup Port **(If Coupling Mode is Dual Homing)**	Specify the port that connects to the backup path for ring coupling.	Select a port from the drop-down menu	N/A
Coupling Port **(If Coupling Mode is Primary Path or Backup Path)**	Specify the port that connects to primary path or backup path for ring coupling.	Select a port from the drop-down menu	3

Turbo Ring V2 - Status

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Ring V2 - Status

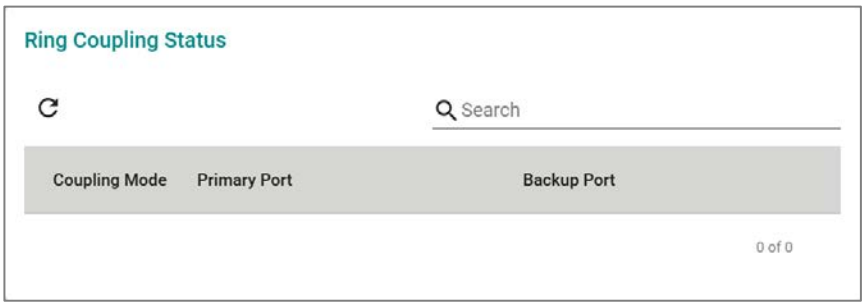
This page lets you see the current status of your rings and ring couplings.

Ring Status



UI Setting	Description
Ring ID	Shows the ID number of the ring.
Master ID	Shows the MAC address of the ring master.
Status	Shows the current status of the ring. • **Healthy**: The ring and its related ports are working properly. • **Break**: One or more rings are broken.
Master	Shows whether this device is acting as a master or slave in the ring.
Ring Port 1	Shows which port is acting as the first ring port.
Ring Port 2	Shows which port is acting as the second ring port.

Ring Coupling Status



UI Setting	Description
Coupling Mode	Shows the mode being used for the ring coupling.
Primary Port	Shows the primary port for the ring coupling.
Backup Port	Shows the backup port for the ring coupling.

Turbo Chain

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain

This page lets you configure Turbo Chain settings for redundancy.

This page includes these tabs:

- Settings
- Status

Turbo Chain - Settings

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain - Settings

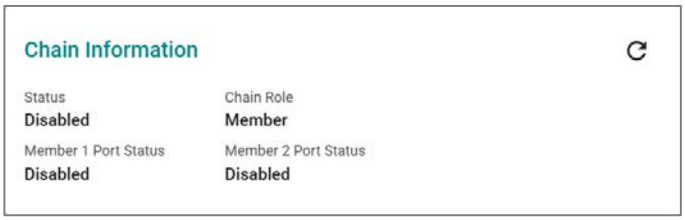
This section lets you enable and configure Turbo Chain for your device.

UI Setting	Description	Valid Range	Default Value
Turbo Chain	Enable or disable Turbo Chain.	Enabled / Disabled	Disabled
Chain Role	Select the chain role of the device.	Head / Member / Tail	Member
Member Port 1	Select which port will be Member Port 1.	Drop-down menu of ports	Depends on model
Member Port 2	Select which port will be Member Port 2.	Drop-down menu of ports	Depends on model

Turbo Chain - Status

Menu Path: Redundancy > Layer 2 Redundancy > Turbo Chain - Status

This page lets you view the current status of Turbo Chain for your device.



UI Setting	Description
Turbo Chain	Shows the status of Turbo Chain.
Chain Role	Shows the chain role for your device.
Member Port 1 Status	Shows the status of Member Port 1.
Member Port 2 Status	Shows the status of Member Port 2.

Layer 3 Redundancy

Menu Path: Redundancy > Layer 3 Redundancy

This section lets you configure the Layer 3 redundancy features of your device.

This section includes these pages:

- VRRP

VRRP

Menu Path: Redundancy > Layer 3 Redundancy > VRRP

This page lets you configure the VRRP settings for your device.

This page includes these tabs:

- Settings
- Status

VRRP - Settings

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

This page lets you configure the VRRP settings for your device.

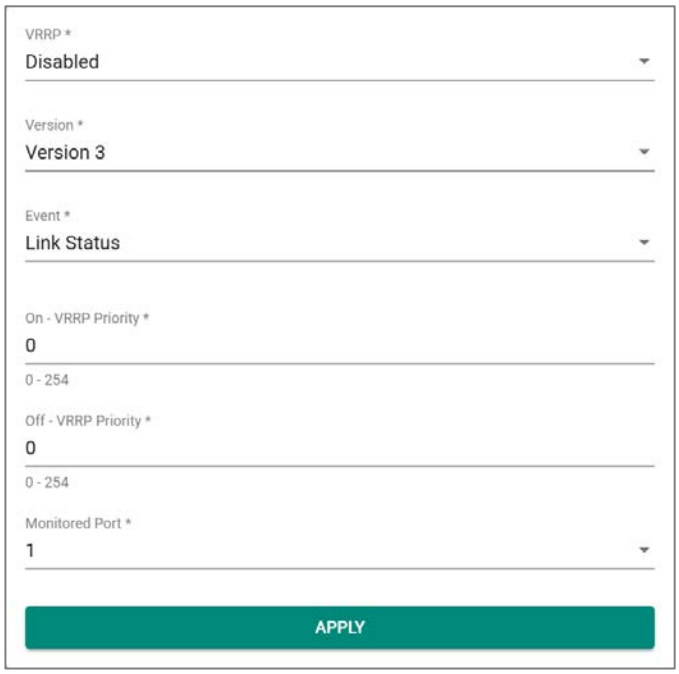
Note

Virtual Router Redundancy Protocol (VRRP) helps solve some problems with static configurations. VRRP enables a group of routers to form a single virtual router with a virtual IP address. The LAN clients can then be configured with the virtual router's virtual IP address as their default gateway. This virtual router consisting of a group of routers is also known as a VRRP group.

Limitations

You can create up to 16 virtual routers.

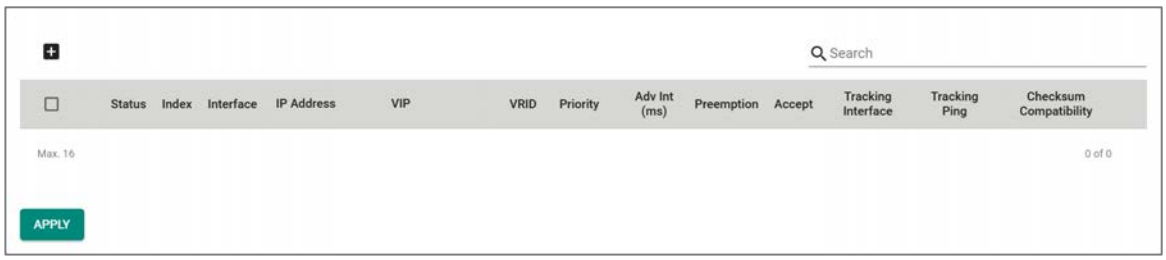
VRRP Settings



UI Setting	Description	Valid Range	Default Value
VRRP	Enable or disable VRRP for the device.	Enabled / Disabled	Disabled
Version	Select the VRRP version to use.	Version 2 / Version 3	Version 3
Event	Select the event for VRRP.	No Event / DI Status / Link Status	No Event

UI Setting	Description	Valid Range	Default Value
On - VRRP Priority **(If Event is Link Status or DI Status)**	Specify the VRRP Priority when the event is On. Higher numbers indicate higher priority, **Note** If this is 0, the device will use the priority assigned to each VRRP interface.	0 to 254	0
Off - VRRP Priority **(If Event is Link Status or DI Status)**	Specify the VRRP Priority when the event is Off. Higher numbers indicate higher priority, **Note** If this is 0, the device will use the priority assigned to each VRRP interface.	0 to 254	0
Monitored Port **(If Event is Link Status)**	Select the port to monitor.	Drop-down list of ports	1

VRRP List



UI Setting	Description
Status	Shows the status of the VRRP interface.
Index	Shows the index number used to identify the VRRP interface.
Interface	Shows which network interface is used for the VRRP interface.
IP Address	Shows the IP address of the VRRP interface.
VIP	Shows the virtual router IP address for the VRRP interface.

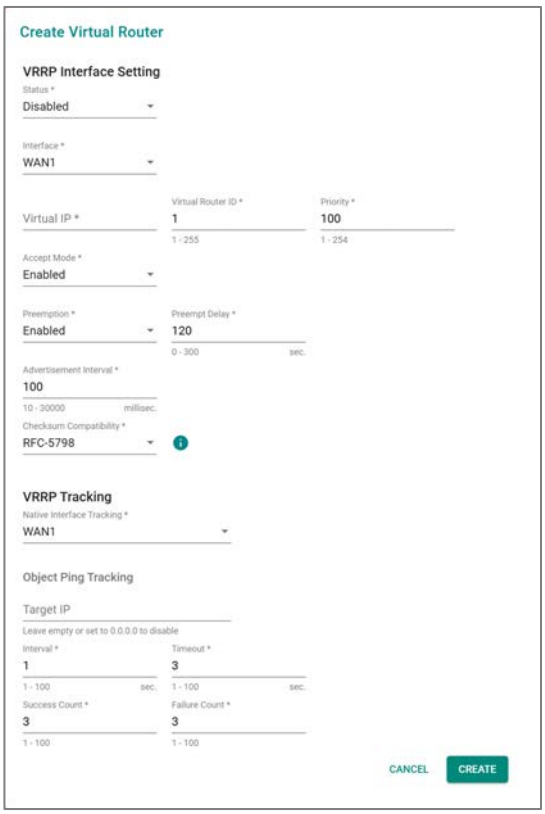
UI Setting	Description
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
Priority	Shows the priority of the VRRP interface. Higher numbers indicate higher priority.
Adv Int (ms)	Shows the advertisement interval for the VRRP interface in milliseconds.
Preemption	Shows the preemption status of the VRRP interface.
Accept	Shows whether Accept Mode is enabled for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.
Tracking Interface	Shows whether Native Interface Tracking is enabled for the VRRP interface.
Tracking Ping	Shows the tracking ping status of the VRRP interface.
Checksum Compatibility **(If VRRP Version is Version 3)**	Shows the checksum calculation mode used for VRRPv3 advertisement packets.

VRRP - Create Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

Clicking the **Add (+)** icon on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you create a new virtual router for your device.

Click **CREATE** to save your changes and add the new account.



VRRP Interface Setting

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the VRRP interface.	Enabled / Disabled	Disabled
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	
Virtual IP	Specify the virtual router IP address for the VRRP interface. **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Virtual Router ID	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group. **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1 to 255	1
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority. **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1 to 254	100
Accept Mode	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	Enabled
Preemption	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	Enabled
Preempt Delay (If Preemption is Enabled)	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	0 to 300	120
Advertisement Interval	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	10 to 30000	100

UI Setting	Description	Valid Range	Default Value
Checksum Compatibility **(If VRRP Version is Version 3)**	Select the checksum calculation method used for VRRPv3 advertisement packets. • **RFC-5798**: Moxa legacy-compatible method. Includes an IPv4 pseudo-header in the checksum calculation for compatibility. • **RFC-9568**: Standard method. Does not include an IPv4 pseudo-header, as per the updated RFC. **Note** Some newer packet-capture tools (Wireshark ≥ v4.4.0) validate VRRPv3 checksums against RFC-9568 by default, and will flag RFC-5798-calculated packets as invalid even though they aren't actually errors. Selecting Standard (RFC-9568) avoids this false-positive warning; Moxa Legacy Compatibility (RFC-5798) is kept as default for backward compatibility with existing deployments.	RFC-5798 / RFC-9568	RFC-5798

VRRP Tracking

Note

If either Native Interface Tracking or Object Ping Tracking determines a connection failure, the VRRP status will be switched to INIT mode.

UI Setting	Description	Valid Range	Default Value
Native Tracking Interface	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
Target IP	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface. **Note** Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.	Valid IP address	N/A
Interval	Specify the interval in seconds the device will use for pinging the target IP.	1 to 100	1

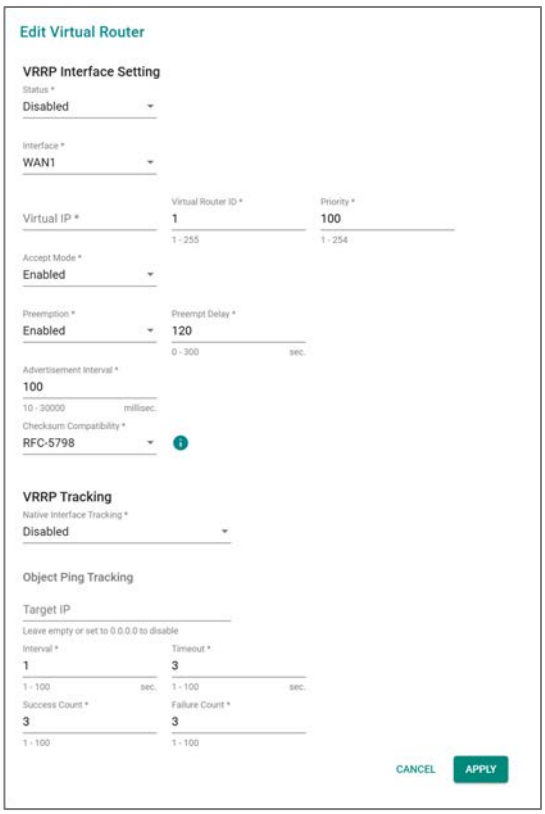
UI Setting	Description	Valid Range	Default Value
Timeout	Specify the timeout duration in seconds the device will wait for a response before timing out.	1 to 100	3
Success Count	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1 to 100	3
Failure Count	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1 to 100	3

VRRP - Edit Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

Clicking the **Edit ( )** icon for a VRRP interface on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you edit an existing virtual router.

Click **APPLY** to save your changes.



VRRP Interface Setting

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the VRRP interface.	Enabled / Disabled	Disabled
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	
Virtual IP	Specify the virtual router IP address for the VRRP interface. **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A
Virtual Router ID	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group. **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1 to 255	1
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority. **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1 to 254	100
Accept Mode	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	Enabled
Preemption	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	Enabled
Preempt Delay **(If Preemption is Enabled)**	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	0 to 300	120

UI Setting	Description	Valid Range	Default Value
Advertisement Interval	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	10 to 30000	100
Checksum Compatibility **(If VRRP Version is Version 3)**	Select the checksum calculation method used for VRRPv3 advertisement packets. • **RFC-5798**: Moxa legacy-compatible method. Includes an IPv4 pseudo-header in the checksum calculation for compatibility. • **RFC-9568**: Standard method. Does not include an IPv4 pseudo-header, as per the updated RFC. **Note** Some newer packet-capture tools (Wireshark ≥ v4.4.0) validate VRRPv3 checksums against RFC-9568 by default, and will flag RFC-5798-calculated packets as invalid even though they aren't actually errors. Selecting Standard (RFC-9568) avoids this false-positive warning; Moxa Legacy Compatibility (RFC-5798) is kept as default for backward compatibility with existing deployments.	RFC-5798 / RFC-9568	RFC-5798

VRRP Tracking

Note

If either Native Interface Tracking or Object Ping Tracking determines a connection failure, the VRRP status will be switched to INIT mode.

UI Setting	Description	Valid Range	Default Value
Native Tracking Interface	Disable or specify which interface to use for Native Interface Tracking for the VRRP interface. When enabled, if all interfaces on the device are disconnected, it will be considered to be a disconnection.	Disabled / Drop-down list of interfaces	Disabled
Target IP	Specify the target IP to ping to verify if the connection to the destination is working. Leaving this field empty or entering 0.0.0.0 will disable object ping tracking for the VRRP interface. **Note** Moxa devices will decide which interface/source IP to use for pinging the target IP based on the routing table.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Interval	Specify the interval in seconds the device will use for pinging the target IP.	1 to 100	1
Timeout	Specify the timeout duration in seconds the device will wait for a response before timing out.	1 to 100	3
Success Count	Specify the success count, which indicates how many responses the device must receive to consider the connection as working.	1 to 100	3
Failure Count	Specify the failure count, which indicates how many times the target IP fails to respond before the device considers the connection as not working.	1 to 100	3

Delete Virtual Router

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

You can delete VRRP interfaces by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete ( )** icon.

VRRP - Status

Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Status

This page lets you see the status of your device's VRRP interfaces.

UI Setting	Description
Status	Shows the status of the VRRP interface.
Index	Shows the index number used to identify the VRRP interface.
Interface	Shows which network interface is used for the VRRP interface.

UI Setting	Description
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
State	Shows the state of the VRRP interface. • **Init State**: This is the initial state when a virtual router starts up. • **Master State**: The virtual router is acting as a master, and is responsible for forwarding packets sent to the virtual IP address and acting as the default gateway for the devices in the network. • **Backup State**: The virtual router is in the backup state, and waiting to take over the master role if the current master fails.
Master Address	Shows IP address of the current master for the VRRP interface.

WAN Redundancy

Menu Path: Redundancy > WAN Redundancy

This section lets you configure the WAN Rdundancy features of your device.

This page includes these tabs:

- Settings
- Status

> **Note**
> Please note that settings and available options will vary depending on the product model.

WAN Redundancy - Settings

Menu Path: Redundancy > WAN Redundancy - Settings

This page lets you configure the WAN Redundancy settings for your device.

WAN Redundancy Settings

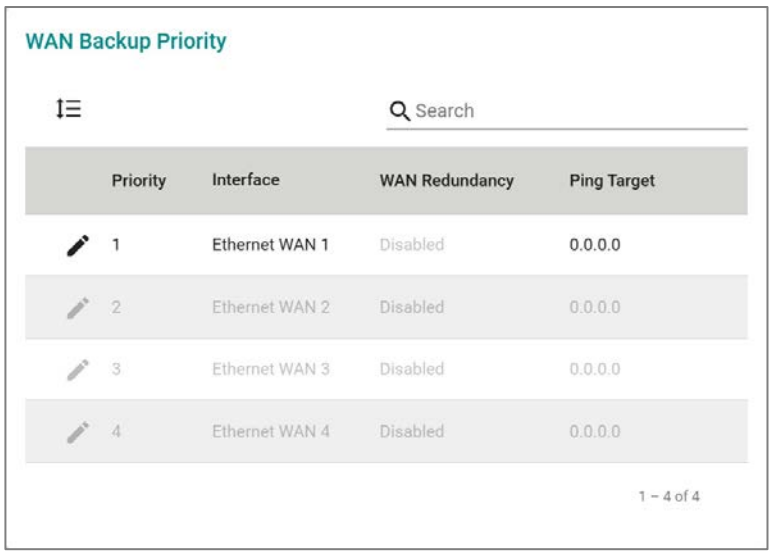
UI Setting	Description	Valid Range	Default Value
WAN Redundancy Mode	Select the WAN redundancy mode to use for your device. • **Disabled:** Disable redundancy. If the connection on the WAN interface becomes unavailable, the WAN connection will be lost. • **Backup:** If the connection on the active WAN interface becomes unavailable, the system will automatically switch to another WAN interface to maintain a WAN connection.	Disabled / Backup	Disabled
WAN Switching Mode	Select the WAN switching mode to use for your device. • **Failover:** The system will switch its WAN connection to the next-highest priority backup WAN interface when the current WAN interface becomes unavailable. • **Failback:** The system will switch its WAN connection to the next highest-priority WAN interface when the current WAN interface becomes unavailable. When a higher priority WAN interface recovers, the system will switch its WAN connection back to it.	Failover / Failback	Failback
Ping Check	Enable or disable ping checks to determine whether an interface's connection is still alive. • **Link Check Only**: An interface's connection will be determined to be unavailable if its link goes down. • **Link and Ping Check**: An interface's connection will be determined to be unavailable if its link goes down, or if the number of consecutive failed ping checks to the interface's **Ping Target** reaches the **Ping Failure Retry Attempts** threshold.	Enabled / Disabled	Disabled
Ping Interval	Specify the interval in seconds between ping checks to the current interface's **Ping Target**.	1 to 3600	5

UI Setting	Description	Valid Range	Default Value
Ping Failure Retry Times	Specify the number of consecutive failed ping checks to an interface's **Ping Target** before the interface's connection is determined to be unavailable.	1 to 10	3
Ping Success Retry Times	Specify the number of consecutive successful ping checks to an interface's **Ping Target** before the interface's connection is determined to be available. In **Failback** mode, if a higher priority interface is determined to be available, the device will switch its WAN connection back to that interface.	1 to 10	3
Ping Timeout	Specify the timeout duration in seconds the device will wait for a response before timing out and determining the ping check has failed.	1 to 10	5

WAN Backup Priority List

Note

To change the priority of entries in the table, select the Reorder ( ) icon, then drag the Reorder Handle ( ) icons for the entries to reorder them in order of priority.



UI Setting	Description
Priority	Shows the priority of the interface. Lower numbers have higher priority.

UI Setting	Description
Interface	Shows the interface the entry is for.
WAN Redundancy	Shows whether WAN redundancy is enabled for the interface.
Ping Target	Shows the ping target used to check connectivity for the interface.

WAN Backup Priority - Editing Ethernet Interface Settings

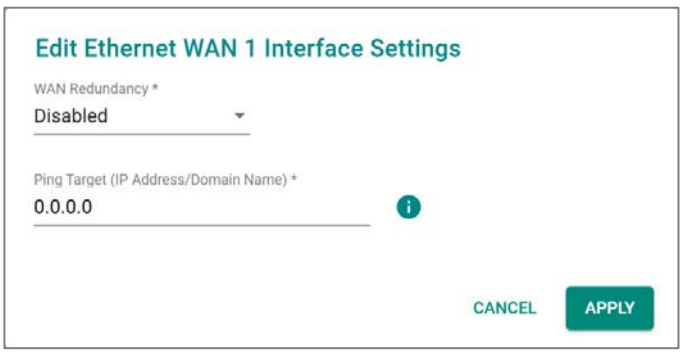
Menu Path: Redundancy > WAN Redundancy - Settings

Clicking the **Edit ( )** icon for an interface on the **Redundancy > WAN Redundancy - Settings** page will open this dialog box. This dialog lets you edit the interface's WAN backup priority settings.

Click **APPLY** to save your changes.

Note

To change the priority of entries in the table, select the Reorder ( ) icon, then drag the Reorder Handle ( ) icons for the entries to reorder them in order of priority.



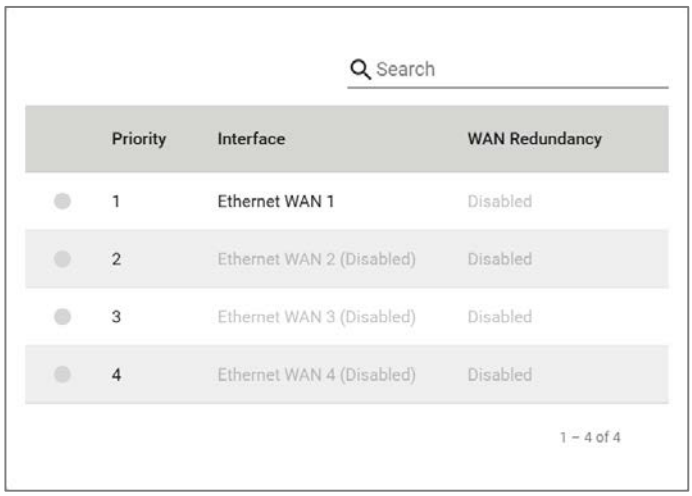
UI Setting	Description	Valid Range	Default Value
WAN Redundancy	Enable or disable use of this interface as a WAN redundancy interface.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Ping Target (IP Address/Domain Name)	Specify the IP address or domain name for performing ping checks to determine if the interface's WAN connection is available. **Note** If you enter a domain name, please ensure that you have already set a DNS server for the interface.	Valid IP address / Domain name	0.0.0.0

WAN Redundancy - Status

Menu Path: Redundancy > WAN Redundancy - Status

This page lets you see the WAN Redundancy status of your device's interfaces.



UI Setting	Description
Status	Shows the usage status of the interface. • **Green:** The WAN interface is in use. • **Gray:** The WAN interface is not in use. This can happen when the interface connection is unavailable, the interface is acting as a WAN Redundancy backup, or when the interface is not used for WAN Redundancy (WAN Redundancy is disabled for the interface).
Priority	Shows the WAN Redundancy priority for the interface. Lower numbers have higher priority.

UI Setting	Description
Interface	Shows the interface the entry is for.
WAN Redundancy	Shows whether WAN Redundancy is enabled for the interface.

High Availability

Menu Path: Redundancy > High Availability

This page lets you manage the HA (High Availability) feature of the device. HA allows a backup device to take over traffic routing if the primary device fails.

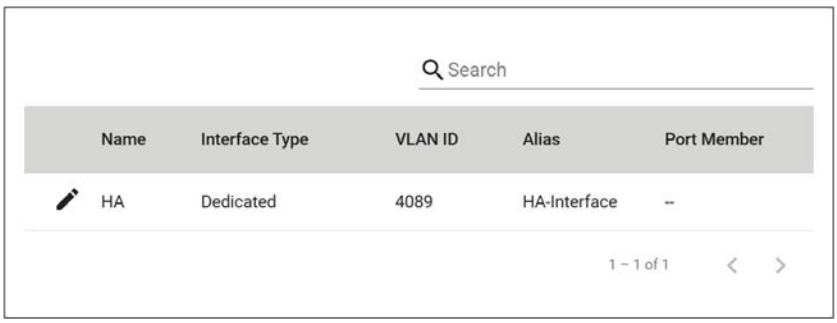
This page includes these tabs:

- HA Interface
- Settings
- Status
- Auto Provisioning

HA Interface

Menu Path: Redundancy > High Availability - HA Interface

This page lets you configure an HA interface for the device.



UI Setting	Description
Name	Shows the name of the interface.

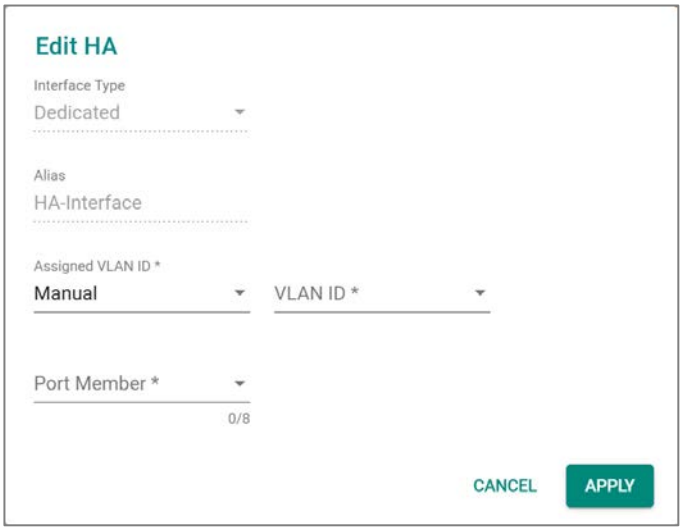
UI Setting	Description
Interface Type	Shows the interface type.
VLAN ID	Shows the VLAN ID assigned to this interface.
Alias	Shows the alias for the interface.
Port Member	Shows the ports that are members of this interface.

Edit HA

Menu Path: Redundancy > High Availability - HA Interface

Clicking the **Edit ( )** icon for an interface on the **Redundancy > High Availability - HA Interface** page will open this dialog box. This dialog lets you edit the interface's settings.

Click **APPLY** to save your changes.



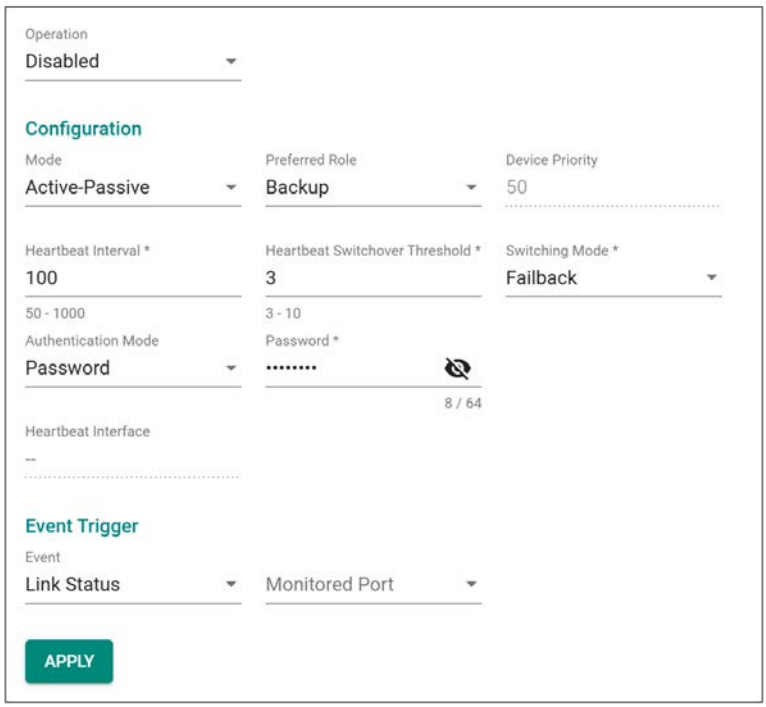
UI Setting	Description	Valid Range	Default Value
Interface Type	Shows the interface type. This is fixed to **Dedicated**.	Dedicated	Dedicated
Alias	Shows the alias for the interface. This is fixed to **HA-Interface**.	HA-Interface	HA-Interface

UI Setting	Description	Valid Range	Default Value
Assigned VLAN ID	Select **Auto** to automatically assign a VLAN ID to use for the interface. Select **Manual** to manually assign a VLAN ID to use for the interface.	Auto / Manual	Auto
VLAN ID **(If Assigned VLAN ID is Manual)**	Select a VLAN ID to use for the interface.	Drop-down list of VLAN IDs	N/A
Port Member	Select which ports will be members of the interface.	Drop-down list of ports	N/A

High Availability - Settings

Menu Path: Redundancy > High Availability - Settings

This page lets you configure the main HA settings of your device.



UI Setting	Description	Valid Range	Default Value
Operation	Enable or disable high availability (HA) for the device.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Mode	Select the HA mode your network uses. • **Active-Passive**: Only the Primary device processes traffic while the Backup device remains idle, taking over traffic routing only if the Primary device fails. • **Active-Active w/o Load Balancing**: Both the Primary and Backup devices are used to distribute traffic for improved performance and zero-downtime failover.	Active-Passive / Active-Active w/o Load Balancing	Active-Passive
Preferred Role	Select the preferred HA role for the device.	Primary / Backup	Backup
Device Priority	Shows the priority of the device when electing a Primary node. Higher numbers have higher priority. This value is fixed based on the **Preferred Role** setting.	If **Preferred Role** is **Primary:** 100 If **Preferred Role** is **Backup:** 50	If **Preferred Role** is **Primary:** 100 If **Preferred Role** is **Backup:** 50
Heartbeat Interval	Specify the interval in milliseconds between heartbeat packets sent from the device to check the status of its HA peer.	50 to 1000	N/A
Heartbeat Switchover Threshold	Specify how many consecutive heartbeat packets can be sent without receiving a response before triggering a switchover.	3 to 10	N/A
Switching Mode	Select the mode used for switchover. • **Failover**: If the Primary device fails, the Backup device will take on the Primary role and take over traffic routing for the Primary device. The Backup device will continue in this role even if the Primary device recovers, and the Primary device will take on the Backup role. • **Failback**: If the Primary device fails, the Backup device will take on the Primary role and take over traffic routing for the Primary device. If the Primary device recovers, traffic will be redirected to it and the Backup device will return to its Backup role.	Failover / Failback	N/A
Authentication Mode	Select the mode to use to authenticate heartbeat packets. • **None**: No authentication will be used. • **Password**: Heartbeat packets must use the specified password to be used. Heartbeat packets without the specified password will be dropped.	None / Password	None

UI Setting	Description	Valid Range	Default Value
Password	Specify the password to use for heartbeat authentication with the HA peer.	1 to 64 characters	N/A
Heartbeat Interface	Shows the interface used for heartbeat packets. This is fixed to the port members of the HA interface.	HA interface port members	HA interface port members
Event	Select the events to monitor. • **No Event**: No events will be monitored. • **Link Status**: Link status changes on the monitored ports will trigger a System event.	No Event / Link Status	No Event
Monitored Port **(If Event is Link Status)**	Select the ports to monitor for link status changes. You can select multiple ports.	Drop-down list of ports	N/A

High Availability - Status

Menu Path: Redundancy > High Availability - Status

This page lets you view the HA status of your device.

UI Setting	Description
HA State	Shows the HA state of the device.
Priority	Shows the HA priority of the device.
Mode	Shows the HA mode of the device.
System name	Shows the system name of the device.
Serial No.	Shows the serial number of the device.
Role Configuration	Shows the preferred role of the device.
Running Role	Shows the current role of the device.

UI Setting	Description
System Uptime	Shows the system uptime of the device.
Sessions	Shows the number of HA sessions.
Heartbeat	Showss the HA heartbeat interface for the device.
Cluster Uptime	Shows the cluster uptime of the device.
CPU Usage	Shows the CPU usage of the device.
Link Up Ports	Shows the device's link up ports.
Link Down Ports	Shows the device's link down ports.
RAM	Shows the RAM usage of the device.
Cluster Link Packets (Tx / Rx)	Shows the cluster link packets (transmitted/received).
Cluster Link Bytes (Tx / Rx)	Shows the cluster link size in bytes (transmitted/received).

Auto Provisioning

Menu Path: Redundancy > High Availability - Auto Provisioning

This page lets you configure the auto provisioning feature of your device. Auto provisioning simplifies high availability (HA) deployment by automatically copying the device's firmware and configuration to an unconfigured target device.

Note

HA must be enabled to use Auto Provisioning. Refer to High Availability - Settings for more information.

Note

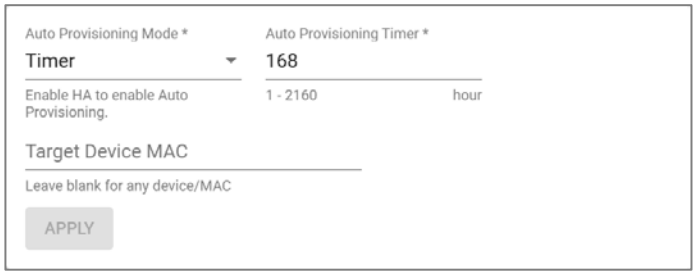
Target devices for Auto Provisioning must be unconfigured and set to the factory default settings.

Note

The staged firmware version must match the device's installed firmware version to use Auto Provisioning.

If they do not match, the correct matching firmware must be staged before using Auto Provisioning.

Auto Provisioning Settings



UI Setting	Description	Valid Range	Default Value
Auto Provisioning Mode	Select the auto provisioning mode to use for the device. • **Disabled**: Auto provisioning will be disabled. • **Timer**: Auto provisioning will be run on eligible devices connected through this device's HA link within the amount of time specified by **Auto Provisioning Timer**. • **DI**: Auto provisioning will be run when a DI signal is received on the device's DI port.	Disabled / Timer / DI	Disabled
Auto Provisioning Timer **(If Auto Provisioning Mode is Timer)**	Specify the amount of time in hours to allow auto provisioning of eligible devices that connect to this device's HA link after selecting the **APPLY** button.	1 to 2160	168
Target Device MAC	Specify the MAC address of the target device to auto provision. Leave this blank to allow auto provisioning of any eligible device connected through the HA link. **Note** Target devices for Auto Provisioning must be unconfigured and set to the factory default settings.	Valid MAC address, may be left blank	Blank

Provisioning Status

Select the **Refresh (↻)** icon to refresh the provisioning status.

UI Setting	Description
Mode	Shows the current auto provisioning mode.
State	Shows the current state of the auto provisioning process.

Staged Firmware Status - Staged

If the current staged firmware matches the device's currently installed firmware version, this will appear.

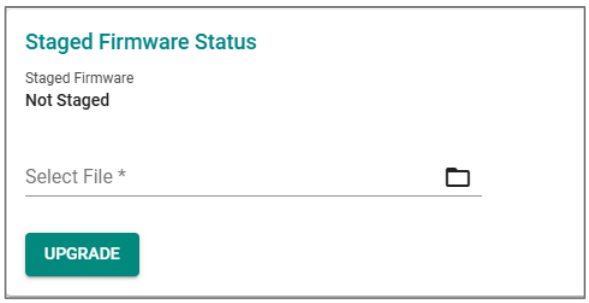
UI Setting	Description
Staged Firmware	Shows the staged firmware version, which matches the device's currently installed firmware version.

Staged Firmware Status - Not Staged

If the current staged firmware does not match the device's currently installed firmware, this will appear. After selecting the matching firmware file from your host PC, select **UPGRADE** to upload and stage the firmware.

Note

The staged firmware version must match the device's installed firmware version to use Auto Provisioning. If they do not match, the correct matching firmware must be staged before using Auto Provisioning.



UI Setting	Description	Valid Range	Default Value
Select File	Select the firmware file that matches your device's current firmware from your host PC.	Valid firmware file	N/A

Network Service

Menu Path: Network Service

The Network Service settings area lets you configure the main system settings for your device.

This settings area includes these sections:

- DHCP Server
- Dynamic DNS
- DNS Server

Network Service - User Privileges

Privileges to Network Service settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R
Dynamic DNS	R/W	R/W	R
DNS Server	R/W	R/W	R

DHCP Server

Menu Path: Network Service > DHCP Server

This page lets you manage the DHCP server settings of your device.

This page includes these tabs:

- General
- DHCP
- MAC-based IP Assignment
- Port-based IP Assignment

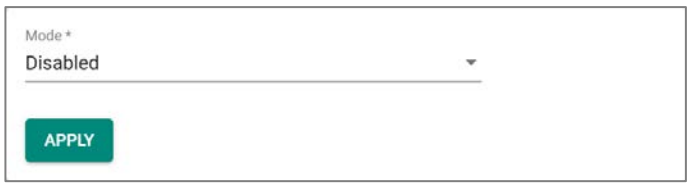
- Lease Table
- DHCP Relay Agent

DHCP Server - General

Menu Path: Network Service > DHCP Server - General

This page lets you enable the DHCP server feature of your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Mode	Select the DHCP server mode to use.	Disabled / DHCP/MAC-based assignment / Port-based IP assignment	Disabled

DHCP

Menu Path: Network Service > DHCP Server - DHCP

This page lets you set up your device's DHCP server settings to automatically assign an IP address from a user-configured IP address pool to connected Ethernet devices.

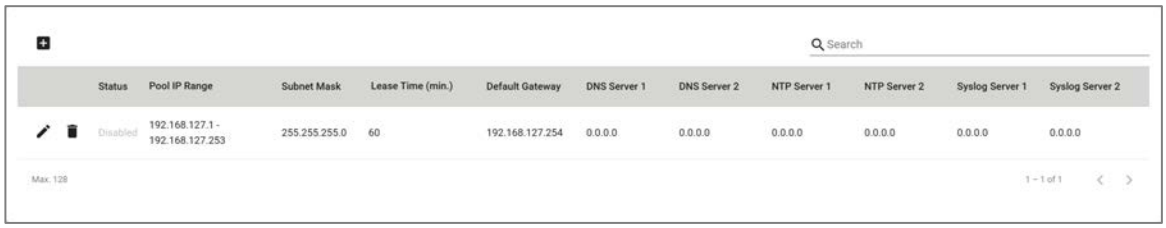
Note

The DHCP Server is only available for LAN interfaces. The DHCP pool's Starting/Ending IP Address must be in the same LAN subnet.

Limitations

- EDR, OnCell, and TN Series: You can create up to 128 DHCP server pools.
- NAT Series: You can create up to 10 DHCP server pools.

DHCP Server Pools

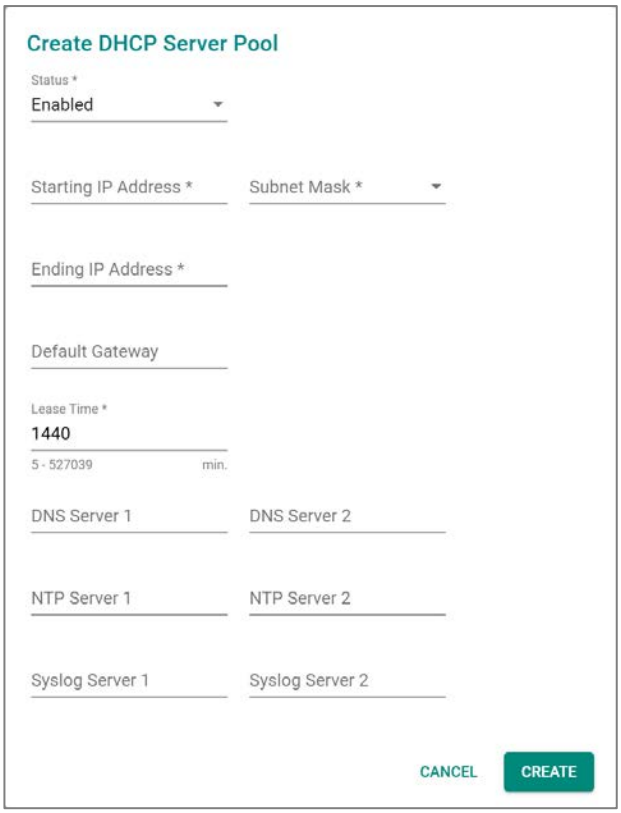


UI Setting	Description
Status	Shows the status of the DHCP server pool.
Pool IP Range	Shows the IP range of the pool.
Subnet Mask	Shows the subnet mask to use for DHCP clients in the pool.
Lease Time	Shows the lease time to use for IP addresses assigned by the DHCP server for the pool.
DNS Server 1	Shows the IP address to use for the first DNS server for DHCP clients in the pool.
DNS Server 2	Shows the IP address to use for the second DNS server for DHCP clients in the pool.
NTP Server 1	Shows the IP address to use for the first NTP server for DHCP clients in the pool.
NTP Server 2	Shows the IP address to use for the second NTP server for DHCP clients in the pool.
Syslog Server 1 (TN Series only)	Shows the IP address to use for the first syslog server for DHCP clients in the pool.
Syslog Server 2 (TN Series only)	Shows the IP address to use for the second syslog server for DHCP clients in the pool.

DHCP - Create DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP

Clicking the Add (/) icon on the **Network Service > DHCP Server - DHCP** page will open this dialog box. This dialog lets you create a new DHCP server pool.
Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A

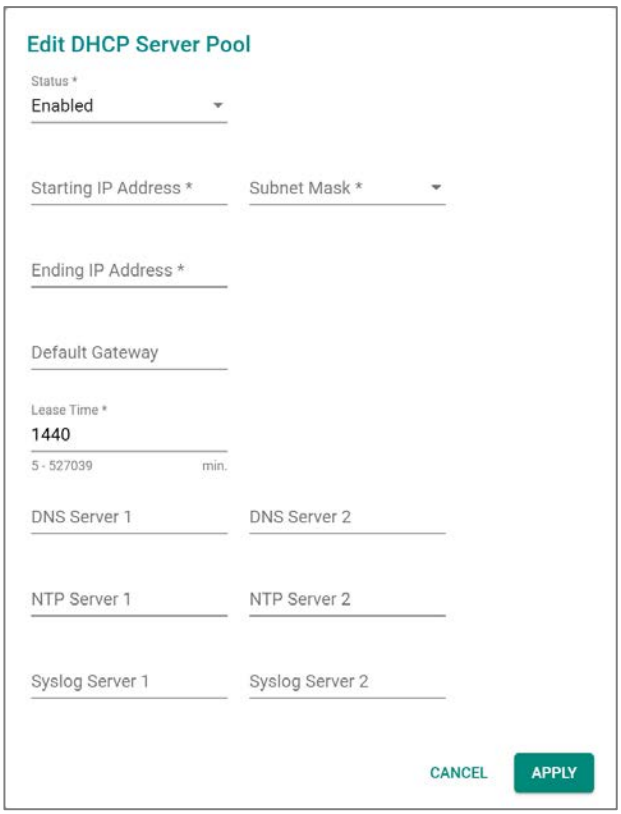
UI Setting	Description	Valid Range	Default Value
Subnet Mask	Specify the subnet mask for DHCP clients in the pool. **Note** When configuring the DHCP Server, ensure the subnet mask is correctly set and the starting IP address, ending IP addresses, and IP addresses of all devices in the pool fall within this range. Exclude the reserved .0 (network) and .255 (broadcast) addresses to avoid conflicts.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes to use for IP addresses assigned to DHCP clients in the pool.	5 to 527039	1440
DNS Server 1	Specify the IP address to use for the first DNS server for DHCP clients in the pool.	Valid IP address	N/A
DNS Server 2	Specify the IP address to use for the second DNS server for DHCP clients in the pool.	Valid IP address	N/A
NTP Server 1	Specify the IP address to use for the first NTP server for DHCP clients in the pool.	Valid IP address	N/A
NTP Server 2	Specify the IP address to use for the second NTP server for DHCP clients in the pool.	Valid IP address	N/A
Syslog Server 1 **(TN Series only)**	Specify the IP address to use for the first syslog server for DHCP clients in the pool.	Valid IP address	N/A
Syslog Server 2 **(TN Series only)**	Specify the IP address to use for the second syslog server for DHCP clients in the pool.	Valid IP address	N/A

Edit DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP

Clicking the **Edit ( )** icon for an pool on the **Network Service > DHCP Server - DHCP** page will open this dialog box. This dialog lets you edit an existing DHCP server pool.

Click **APPLY** to save your changes.



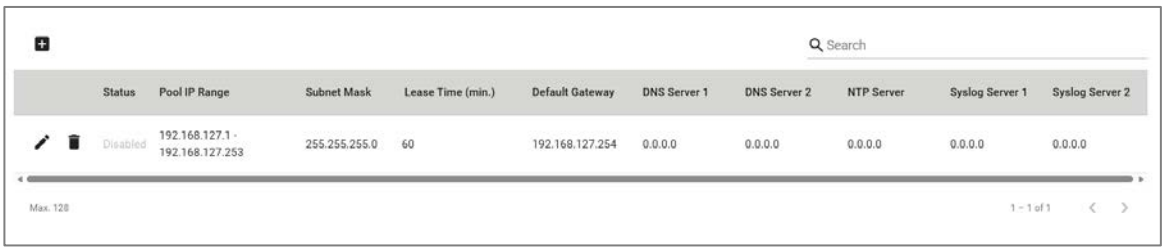
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable DHCP server functionality.	Enabled / Disabled	N/A
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Subnet Mask	Specify the subnet mask for DHCP clients in the pool. **Note** When configuring the DHCP Server, ensure the subnet mask is correctly set and the starting IP address, ending IP addresses, and IP addresses of all devices in the pool fall within this range. Exclude the reserved .0 (network) and .255 (broadcast) addresses to avoid conflicts.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes to use for IP addresses assigned to DHCP clients in the pool.	5 to 527039	1440
DNS Server 1	Specify the IP address to use for the first DNS server for DHCP clients in the pool.	Valid IP address	N/A
DNS Server 2	Specify the IP address to use for the second DNS server for DHCP clients in the pool.	Valid IP address	N/A
NTP Server 1	Specify the IP address to use for the first NTP server for DHCP clients in the pool.	Valid IP address	N/A
NTP Server 2	Specify the IP address to use for the second NTP server for DHCP clients in the pool.	Valid IP address	N/A
Syslog Server 1 **(TN Series only)**	Specify the IP address to use for the first syslog server for DHCP clients in the pool.	Valid IP address	N/A
Syslog Server 2 **(TN Series only)**	Specify the IP address to use for the second syslog server for DHCP clients in the pool.	Valid IP address	N/A

DHCP - Delete DHCP Server Pool

Menu Path: Network Service > DHCP Server - DHCP

You can delete a DHCP server pool by clicking the **Delete ( )** icon for the pool.



DHCP Server - MAC-based IP Assignment

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

This page lets you manage the DHCP server's MAC-based IP assignments.

Note

MAC-based IP assignment is a method of managing IP address allocation on a DHCP server by associating specific IP addresses with the unique MAC addresses of devices on a network. This approach allows network administrators to ensure that certain devices always receive the same IP address, regardless of their connection order or lease duration. By configuring the DHCP server with a table of MAC addresses and their corresponding IP addresses, administrators can have greater control over IP address allocation and enhance network security and management.

Limitations

You can create up to 256 MAC-based IP assignments.

UI Setting	Description
Status	Shows the status of the MAC-based IP assignment.
Name	Shows the name to help identify the IP assignment.
IP Address	Shows the IP address to assign.
Subnet Mask	Shows the subnet mask to assign.

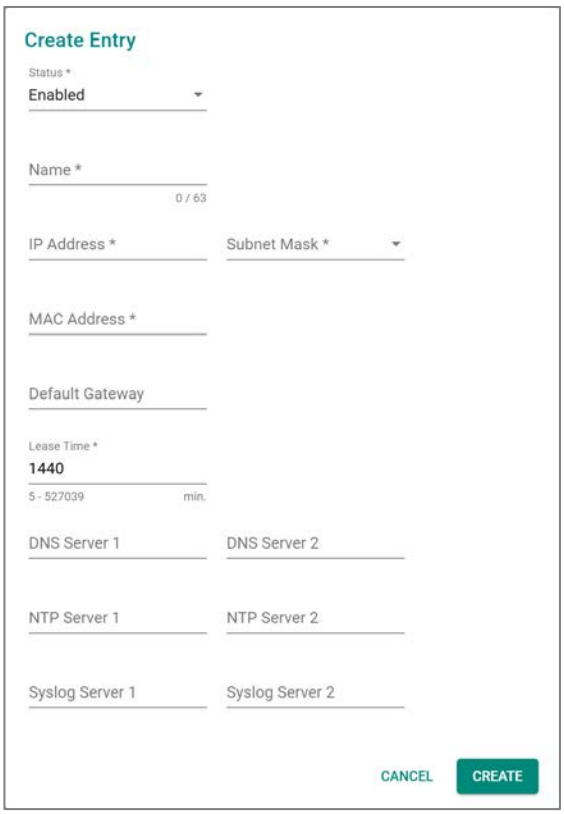
UI Setting	Description
MAC Address	Shows the MAC address of the device that this IP assignment will apply to.
Default Gateway	Shows the default gateway for the IP assignment.
Lease Time (min.)	Shows the lease time in minutes for the IP assignment.
DNS Server 1	Shows the IP address of the primary DNS server for the IP assignment.
DNS Server 2	Shows the IP address of the secondary DNS server for the IP assignment.
NTP Server 1	Shows the IP address of the primary NTP server for the IP assignment.
NTP Server 1	Shows the IP address of the secondary NTP server for the IP assignment.
Syslog Server 1 (TN Series only)	Shows the IP address of the primary syslog server for the IP assignment.
Syslog Server 2 (TN Series only)	Shows the IP address of the secondary syslog server for the IP assignment.

MAC-based IP Assignment - Create Entry

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

Clicking the **Add (+)** icon on the **Network Service > DHCP Server - MAC-based IP Assignment** page will open this dialog box. This dialog lets you add a new MAC-based IP assignment.

Click **CREATE** to save your changes and add the new assignment.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
Name	Enter a name to help identify the IP assignment.	1 to 63 characters	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Select a subnet mask for the IP assignment.	Drop-down list of subnet masks	N/A
MAC Address	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	N/A
Default Gateway	Specify the default gateway for the IP assignment.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes for the IP assignment.	5 to 527039	1440
DNS Server 1	Specify the IP address of the primary DNS server for the IP assignment.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
DNS Server 2	Specify the IP address of the secondary DNS server for the IP assignment.	Valid IP address	N/A
NTP Server 1	Specify the IP address of the primary NTP server for the IP assignment.	Valid IP address	N/A
NTP Server 2	Specify the IP address of the secondary NTP server for the IP assignment.	Valid IP address	N/A
Syslog Server 1	Specify the IP address of the primary syslog server for the IP assignment.	Valid IP address	N/A
Syslog Server 2	Specify the IP address of the secondary syslog server for the IP assignment.	Valid IP address	N/A

MAC-based IP Assignment - Edit Entry

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

Clicking the **Edit ( )** icon for an assignment on the **Network Service > DHCP Server - MAC-based IP Assignment** page will open this dialog box. This dialog lets you edit an existing IP assignment.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this MAC-based IP assignment.	Enabled / Disabled	N/A
Name	Enter a name to help identify the IP assignment.	1 to 63 characters	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Select a subnet mask for the IP assignment.	Drop-down list of subnet masks	N/A
MAC Address	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	N/A
Default Gateway	Specify the default gateway for the IP assignment.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes for the IP assignment.	5 to 527039	1440
DNS Server 1	Specify the IP address of the primary DNS server for the IP assignment.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
DNS Server 2	Specify the IP address of the secondary DNS server for the IP assignment.	Valid IP address	N/A
NTP Server 1	Specify the IP address of the primary NTP server for the IP assignment.	Valid IP address	N/A
NTP Server 2	Specify the IP address of the secondary NTP server for the IP assignment.	Valid IP address	N/A
Syslog Server 1	Specify the IP address of the primary syslog server for the IP assignment.	Valid IP address	N/A
Syslog Server 2	Specify the IP address of the secondary syslog server for the IP assignment.	Valid IP address	N/A

MAC-based IP Assignment - Delete Entry

Menu Path: Network Service > DHCP Server - MAC-based IP Assignment

You can delete a MAC-based IP assignment by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

DHCP Server - Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

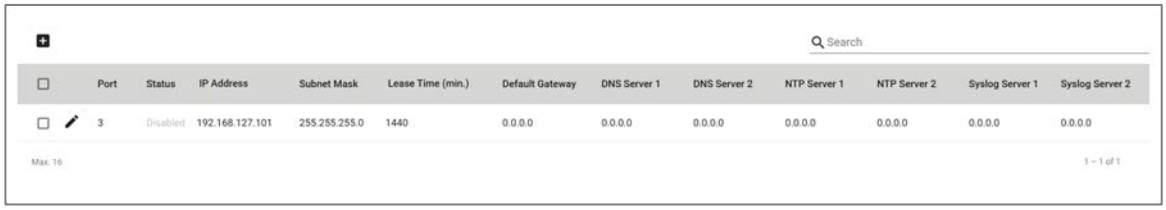
This page lets you manage port-based IP assignment for your device's DHCP server.

Note

Port-based IP assignment is a method of managing IP address allocation on a DHCP server by associating specific IP addresses with the physical ports on network equipment, such as switches or routers. This approach provides network administrators with the ability to assign predetermined IP addresses to devices based on the network port they are connected to.

Limitations

You can create a port-based IP assignment for each port on the device.



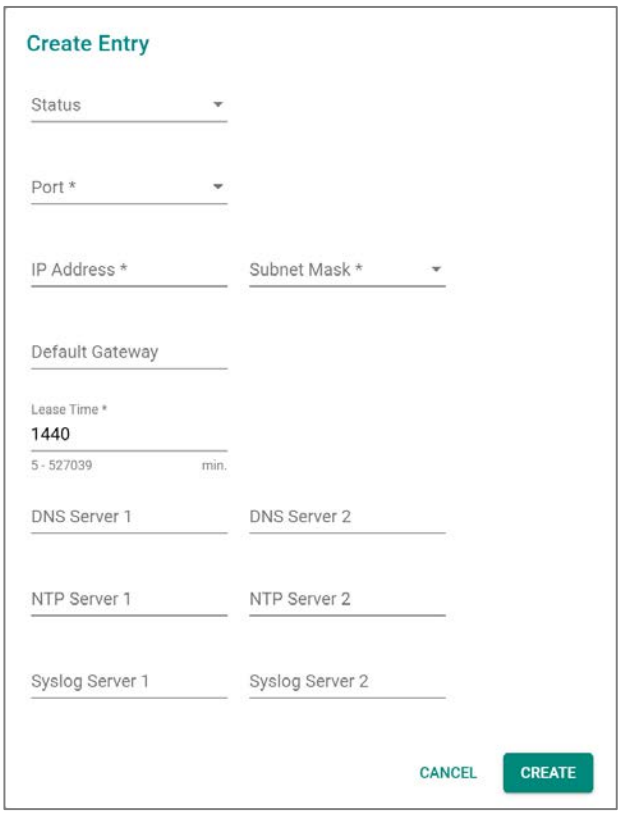
UI Setting	Description
Port	Shows the physical port on the device to assign the IP to.
Status	Shows the status of the port-based IP assignment.
IP Address	Shows the IP address to assign.
Subnet Mask	Shows the subnet mask to assign.
Default Gateway	Shows the default gateway to assign.
Lease Time (min.)	Shows the lease time in minutes for the IP assignment.
DNS Server 1	Shows the IP address of the primary DNS server for the IP assignment.
DNS Server 2	Shows the IP address of the secondary DNS server for the IP assignment.
NTP Server 1	Shows the IP address of the primary NTP server for the IP assignment.
NTP Server 2	Shows the IP address of the secondary NTP server for the IP assignment.
Syslog Server 1 (TN Series only)	Shows the IP address of the primary syslog server for the IP assignment.
Syslog Server 2 (TN Series only)	Shows the IP address of the secondary syslog server for the IP assignment.

Create Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

Clicking the **Add (⊞)** icon on the **Network Service > DHCP Server - Port-based IP Assignment** page will open this dialog box. This dialog lets you create a new port-based IP assignment.

Click **CREATE** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this port-based IP assignment.	Enabled / Disabled	N/A
Port	Select the physical port on the device to assign the IP to.	Drop-down list of ports	N/A
IP Address	Shows the IP address to assign.	Valid IP address	N/A
Subnet Mask	Shows the subnet mask to assign.	Drop-down list of subnet masks	N/A
Default Gateway	Shows the default gateway to assign.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes for the IP assignment.	5 to 527039	1440
DNS Server 1	Shows the IP address of the primary DNS server for the IP assignment.	Valid IP address	N/A
DNS Server 2	Shows the IP address of the secondary DNS server for the IP assignment.	Valid IP address	N/A

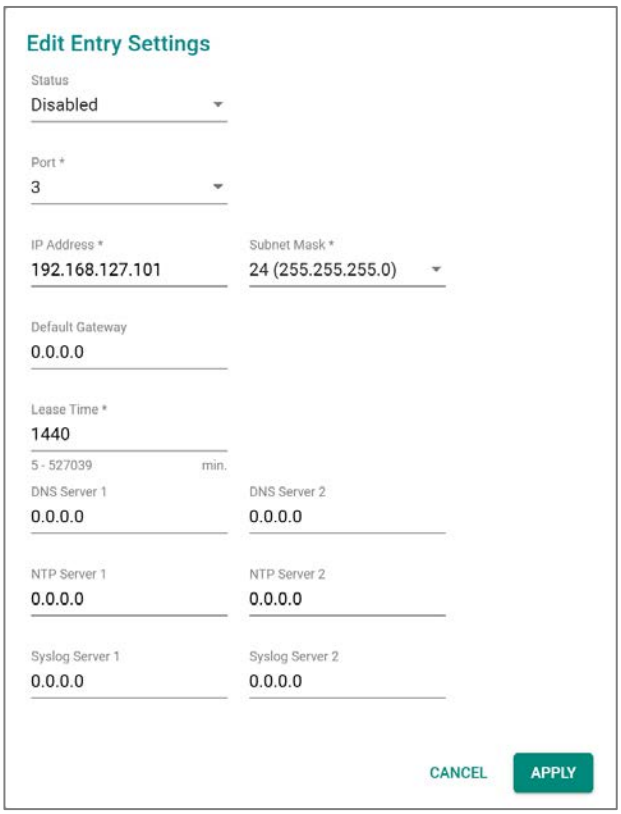
UI Setting	Description	Valid Range	Default Value
NTP Server 1	Shows the IP address of the primary NTP server for the IP assignment.	Valid IP address	N/A
NTP Server 2	Shows the IP address of the secondary NTP server for the IP assignment.	Valid IP address	N/A
Syslog Server 1 **(TN Series only)**	Shows the IP address of the primary syslog server for the IP assignment.	Valid IP address	N/A
Syslog Server 2 **(TN Series only)**	Shows the IP address of the secondary syslog server for the IP assignment.	Valid IP address	N/A

Edit Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

Clicking the **Edit ( )** icon for an entry on the **Network Service > DHCP Server - Port-based IP Assignment** page will open this dialog box. This dialog lets you edit an existing port-based IP assignment.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this port-based IP assignment.	Enabled / Disabled	N/A
Port	Select the physical port on the device to assign the IP to.	Drop-down list of ports	N/A
IP Address	Shows the IP address to assign.	Valid IP address	N/A
Subnet Mask	Shows the subnet mask to assign.	Drop-down list of subnet masks	N/A
Default Gateway	Shows the default gateway to assign.	Valid IP address	N/A
Lease Time	Specify the lease time in minutes for the IP assignment.	5 to 527039	1440
DNS Server 1	Shows the IP address of the primary DNS server for the IP assignment.	Valid IP address	N/A
DNS Server 2	Shows the IP address of the secondary DNS server for the IP assignment.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
NTP Server 1	Shows the IP address of the primary NTP server for the IP assignment.	Valid IP address	N/A
NTP Server 2	Shows the IP address of the secondary NTP server for the IP assignment.	Valid IP address	N/A
Syslog Server 1 **(TN Series only)**	Shows the IP address of the primary syslog server for the IP assignment.	Valid IP address	N/A
Syslog Server 2 **(TN Series only)**	Shows the IP address of the secondary syslog server for the IP assignment.	Valid IP address	N/A

Delete Port-based IP Assignment

Menu Path: Network Service > DHCP Server - Port-based IP Assignment

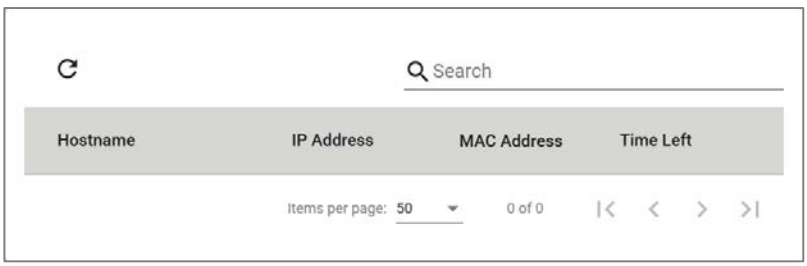
You can delete a port-based IP assignment by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

DHCP Server - Lease Table

Menu Path: Network Service > DHCP Server - Lease Table

This page lets you see an overview of the device's current DHCP clients.

Lease Table



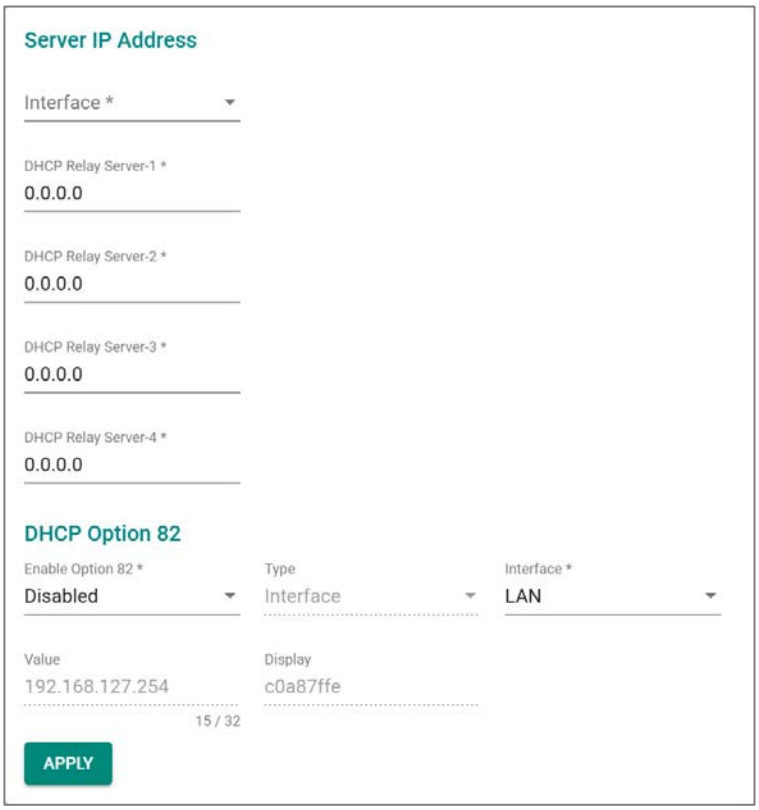
UI Setting	Description
Hostname	Shows the hostname of the DHCP lease.
IP Address	Shows the IP address of the DHCP lease.
MAC Address	Shows the MAC address of the DHCP lease.
Time Left	Shows the time left for the DHCP lease.

DHCP Relay Agent

Menu Path: Network Service > DHCP Server - DHCP Relay Agent

This page allows you to configure the DHCP relay agent, including the settings for remote DHCP server(s) and option-82 related attributes.

DHCP Relay Agent Settings



Server IP Address

UI Setting	Description	Valid Range	Default Value
Interface	Select a preconfigured network interface.	Drop-down menu of interfaces	None
DHCP Relay Server-1	Specify the IP address of the 1st DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-2	Specify the IP address of the 2nd DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-3	Specify the IP address of the 3rd DHCP server.	Valid IP address	0.0.0.0
DHCP Relay Server-4	Specify the IP address of the 4th DHCP server.	Valid IP address	0.0.0.0

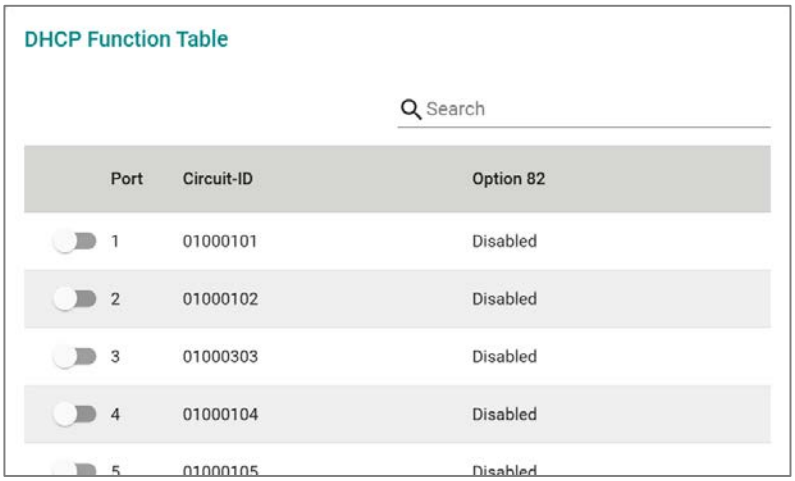
DHCP Option 82

UI Setting	Description	Valid Range	Default Value
Enable Option 82	Enable or disable DHCP Option 82.	Enabled / Disabled	Disabled
Type	Specify the type of DHCP Option 82 to use. This will determine what is used for the remote ID sub. • **Interface:** The IP address of the selected **Interface** will be used. • **MAC**: The MAC address of the device will be used. • **Client ID**: The client ID of the device will be used. The client ID is created by combining the device's MAC address with the device's WAN IP address in hexadecimal format. • **Other**: A user-designated value will be used.	Interface / MAC / Client-ID / Other	Interface
Interface	Select the interface to use for DHCP Option 82.	Drop-down menu of interfaces	N/A
Value	Shows the value to use as the remote ID sub for DHCP Option 82. The value used depends on the selected **Type.** If **Type** is **Other**, specify the value to use.	If **Type** is **Other**: 1 to 32 characters	Depends on the selected **Type**

UI Setting	Description	Valid Range	Default Value
Display (View-only)	Shows the **Value** in hexadecimal. If **Type** is **Other**, this will update after selecting **APPLY** to save changes.	N/A	N/A

DHCP Function Table

Use the toggle ( ) for a port to enable or disable DHCP relay (Option 82) for the port.



UI Setting	Description
Port	Shows the number of the port the entry is for.
Circuit-ID	Shows the Circuit-ID of the port.
Option 82	Shows whether DHCP relay (Option 82) is enabled or disabled for the port.

DHCP Server - Classless Static Route

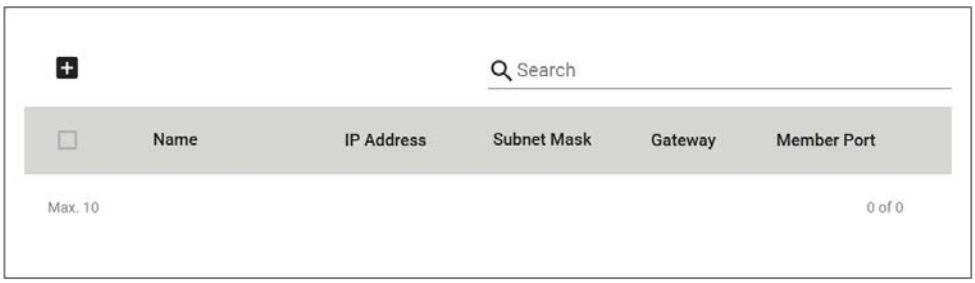
Menu Path: Network Service > DHCP Server - Classless Static Route Table

This page lets you enable the Classless Static Route feature (DHCP option 121) of your device. Click **APPLY** to save your changes.

Limitations

You can create up to 10 classless static route entries.

UI Setting	Description	Valid Range	Default Value
Mode	Select the DHCP Server Classless Static Route mode to use.	Disabled / Port-based IP assignment	Disabled
Default Gateway	Enable or disable use of the default gateway configured in DHCP Server - Port-based IP Assignment for classless static routes.	Enabled / Disabled	Disabled



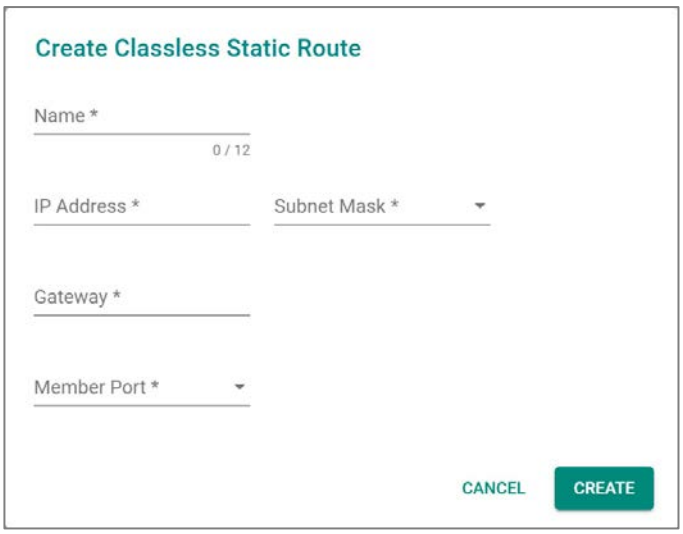
UI Setting	Description
Name	Shows name of the classless static route entry.
IP Address	Shows the IP address of the classless static route.
Subnet Mask	Shows the subnet mask of the classless static route.
Gateway	Shows the default gateway of the classless static route.
Member Port	Shows the member ports to apply this rule to.

Create Classless Static Route Entry

Menu Path: Network Service > DHCP Server - Classless Static Route Table

Clicking the **Add (⊕)** icon on the **Network Service > DHCP Server - Classless Static Route Table** page will open this dialog box. This dialog lets you create a new Classless Static Route entry.

Click **CREATE** to save your changes.



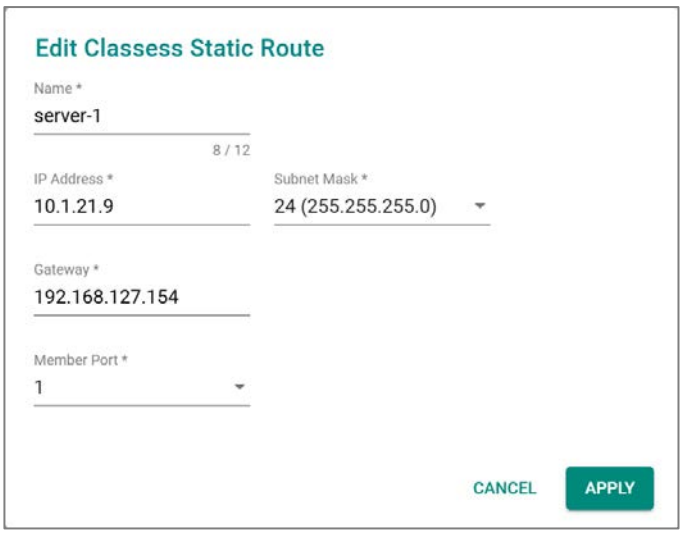
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the classless static route.	1 to 12 characters	N/A
IP Address	Specify the IP address of the classless static route.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask of the classless static route.	Drop-down list of subnet masks	N/A
Gateway	Specify the default gateway of the classless static route.	Valid IP address	N/A
Member Port	Select the member ports to apply this rule to. You can select multiple ports.	Drop-down list of ports	N/A

Edit Classless Static Route Entry

Menu Path: Network Service > DHCP Server - Classless Static Route Table

Clicking the **Edit ( )** icon for an entry on the **Network Service > DHCP Server - Classless Static Route Table** page will open this dialog box. This dialog lets you edit an existing Classless Static Route entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the classless static route.	1 to 12 characters	N/A
IP Address	Specify the IP address of the classless static route.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask of the classless static route.	Drop-down list of subnet masks	N/A
Gateway	Specify the default gateway of the classless static route.	Valid IP address	N/A
Member Port	Select the member ports to apply this rule to. You can select multiple ports.	Drop-down list of ports	N/A

Delete Classless Static Route Entry

Menu Path: Network Service > DHCP Server - Classless Static Route Table

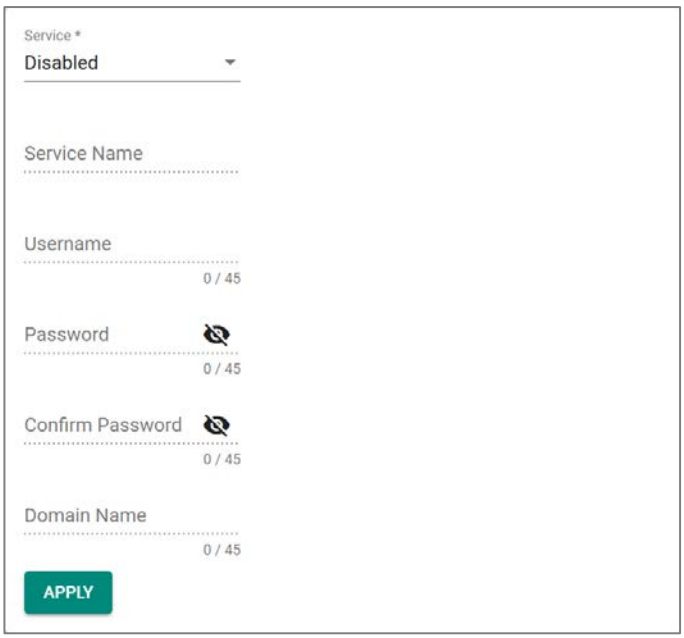
You can delete a classless static route entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Dynamic DNS

Menu Path: Network Service > Dynamic DNS

This page lets you configure your device to use a free dynamic DNS service to enable you to access your device through a domain name rather than an IP.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Service	Select a dynamic DNS service to use, or disable dynamic DNS.	Disabled / freedns.afraid.org / 3322.org / DynDns.org / NO-IP.com	Disabled
Service Name (View-only)	Shows the name of the selected dynamic DNS service.	freedns.afraid.org / www.3322.org / members.dyndns.org / dynupdate.no-ip.com	N/A
Username	Specify the username to connect to the dynamic DNS service.	1 to 45 characters	N/A
Password	Specify the password to connect to the dynamic DNS service.	1 to 45 characters	N/A
Confirm Password	Confirm the password to connect to the dynamic DNS service.	1 to 45 characters	N/A

UI Setting	Description	Valid Range	Default Value
Domain Name	Specify the domain name to use to connect to your device through the dynamic DNS service.	1 to 45 characters	N/A

DNS Server

Menu Path: Network Service > DNS Server

This page lets you configure the DNS server settings.

This page includes these tabs:

- Global
- Settings
- Status

> **Note**
> Availability of this feature may vary depending on your product model and version.

DNS Server - Global

Menu Path: Network Service > DNS Server - Global

This page lets you configure the DNS server related settings.

Click **APPLY** to save your changes.

DNS Server Settings

UI Setting	Description	Valid Range	Default Value
DNS Server	Enable or disable the DNS server for your device.	Enabled / Disabled	Disabled
DNS Reverse Lookup	Enable or disable DNS reverse lookup for your device. DNS reverse lookup allows the router to identify the hostname (device name) associated with a known IP address on the network.	Enabled / Disabled	Disabled

DNS Server - Settings

Menu Path: Network Service > DNS Server - Settings

This page lets you configure the DNS server zone settings.

Limitations

You can create up to 16 DNS zones.

Limitations

You can create up to 256 resource records for each zone.

Zone Table

Zones provide a structured way to manage and organize DNS records for a domain. They allow administrators to group related records together and apply consistent configurations across the domain.

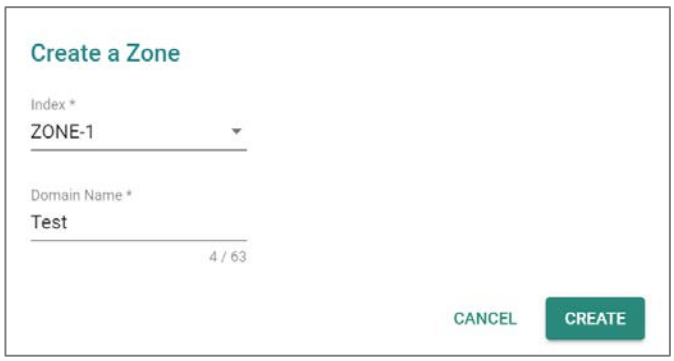
UI Setting	Description
Index	Shows the number of the zone the entry is for.
Domain Name	Shows the domain name of the zone.

Create a Zone

Menu Path: Network Service > DNS Server - Settings

Clicking the **Add (⊕)** icon on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create a zone for the DNS server.

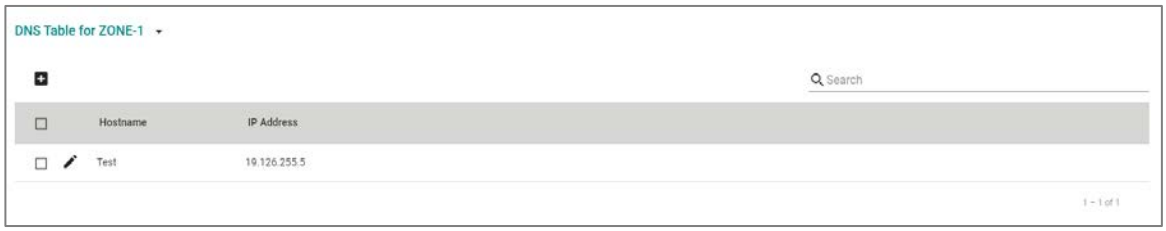
Click **CREATE** to save your changes and add the new zone.



UI Setting	Description	Valid Range	Default Value
Index	Select a zone to create.	Drop-down list of zones	N/A
Domain Name	Specify a domain name for the zone. **Note** Domains used for local DNS zones cannot be used for DNS forwarding zones. Refer to DNS Server - DNS Forwarding for more information on configuring DNS forwarding zones.	1 to 63 characters	N/A

DNS Table

Select a zone from the drop-down list to see its DNS table.



UI Setting	Description
Hostname	Shows the hostname of the resource record.
IP Address	Shows the IP address of the resource record.

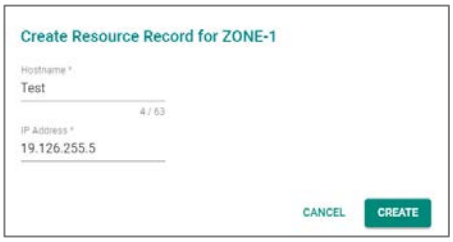
Create a Resource Record

Menu Path: Network Service > DNS Server - Settings

Clicking the **Add (⊕)** icon in a DNS table on the **Network Service > DNS Server - Settings** page will open this dialog box. This dialog lets you create resource records for the displayed zone.

Click **CREATE** to save your changes and add the resource record for the displayed zone.

> **Note**
> Resource records cannot be created for a zone until the corresponding zone has been created.



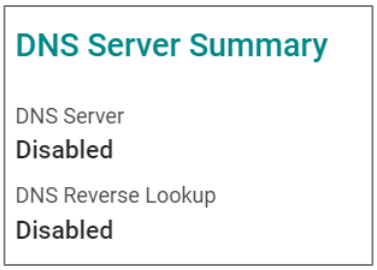
UI Setting	Description	Valid Range	Default Value
Hostname	Specify the host name for the resource record.	1 to 63 characters	N/A
IP Address	Specify the IP address for the resource record.	Valid IP address	N/A

DNS Server - Status

Menu Path: Network Service > DNS Server - Status

This page lets you see the DNS server's overall status.

DNS Server Summary

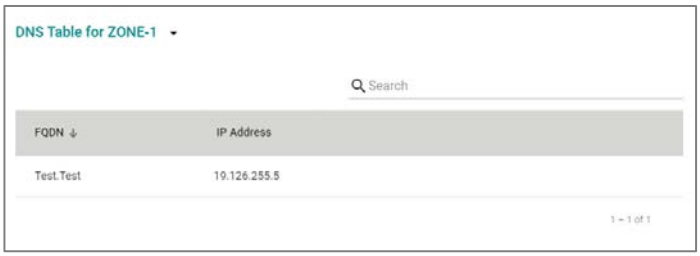


UI Setting	Description
DNS Server	Shows whether the DNS server is enabled for the device.
DNS Reverse Lookup	Shows whether DNS reverse lookup is enabled for the device

Status - Zone Table

UI Setting	Description
Index	Shows the index of the zone the entry is for.
Domain Name	Shows the domain name of the zone.

Status - DNS Table



UI Setting	Description
FQDN	Shows the full qualified domain name (FQDN) of the resource record, which is in the format "Hostname.Domain Name". For example, if the hostname is "door1" and the domain name for the zone is "train1", the FQDN will be "door1.train1".
IP Address	Shows the IP address of the resource record.

DNS Server - DNS Forwarding

Menu Path: Network Service > DNS Server - DNS Forwarding

This page lets you configure the DNS Forwarding feature.

Click **APPLY** to save your changes.

DNS Forwarding Settings

Note

Local authoritative and forwarding DNS resolution can conflict. If only one feature is active, it will follow its correct role. However, when multiple modes are enabled simultaneously, DNS queries are processed in the following order:

1. Local Authoritative Data (if DNS server is enabled)
2. Forward to specific zone servers if the query matches a configured zone (if DNS Forwarding is enabled)
3. Forward to WAN interface DNS servers if conditions 1 and 2 are not met (if WAN DNS server is configured)

UI Setting	Description	Valid Range	Default Value
DNS Forwarding	Enable or disable the DNS forwarding function.	Enabled / Disabled	Disabled

DNS Forwarders Table

UI Setting	Description
Zone	Shows the specific domain that DNS queries will be forwarded to.
Forwarder IP Address	Shows the IP address of the designated DNS server.

Create Zone Forwarder

Menu Path: Network Service > DNS Server - DNS Forwarding

Clicking the **Add (⊞)** icon on the **Network Service > DNS Server - DNS Forwarding** page will open this dialog box. This dialog lets you create a forwarding entry.

Click **CREATE** to save your changes and add the entry.

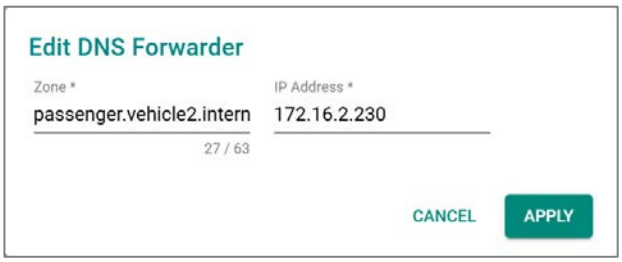
UI Setting	Description	Valid Range	Default Value
Zone	Specify the specific domain that DNS queries will be forwarded to. **Note** Domains used for local DNS zones cannot be used for DNS forwarding zones. Refer to DNS Server - Settings for more information on configuring local DNS zones.	1 to 63 characters • Allowed characters: a-zA-Z0-9.- • Characters , and . cannot be at the beginning or end • The character . may not appear consecutively	N/A
IP Address	Specify the IP address of the designated DNS server.	Valid IP address	N/A

Edit Zone Forwarder

Menu Path: Network Service > DNS Server - DNS Forwarding

Clicking the **Edit ( )** icon on the **Network Service > DNS Server - DNS Forwarding** page will open this dialog box. This dialog lets you edit an existing forwarding entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Zone	Specify the specific domain that DNS queries will be forwarded to. **Note** Domains used for local DNS zones cannot be used for DNS forwarding zones. Refer to DNS Server - Settings for more information on configuring local DNS zones.	1 to 63 characters • Allowed characters: a-zA-Z0-9.- • Characters , and . cannot be at the beginning or end • The character . may not appear consecutively	N/A
IP Address	Specify the IP address of the designated DNS server.	Valid IP address	N/A

Delete Zone Forwarder

Menu Path: Network Service > DNS Server - DNS Forwarding

You can delete forwarding entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Routing

Menu Path: Routing

The Routing settings area lets you configure settings related to how your device routes network traffic.

This settings area includes these sections:

- Unicast Route
- Multicast Route
- Broadcast Forwarding

Routing - User Privileges

Privileges to Routing settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Unicast Route			
Static Routes	R/W	R/W	R
RIP	R/W	R/W	R
OSPF	R/W	R/W	R
Routing Table	R	R	R
Multicast Route			
Multicast Route Settings	R/W	R/W	R
Static Multicast Route	R/W	R/W	R
Multicast Forwarding Table	R	R	R
Broadcast Forwarding	R/W	R/W	R
Directed Forwarding	R/W	R/W	R

Unicast Route

Menu Path: Routing > Unicast Route

This section lets you manage unicast routes for your device.

This section includes these pages:

- Static Routes
- RIP
- OSPF
- Routing Table

Static Routes

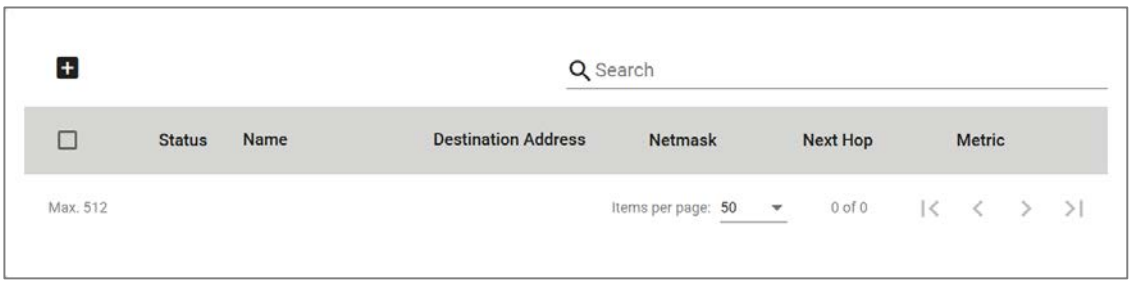
Menu Path: Routing > Unicast Route > Static Routes

This page lets you manage static routes for your device, which allows you to specify the next hop (or router) that the device will forward data to for a specific subnet. Static routes will be added to the routing table and stored on the device.

Limitations

- EDR, OnCell, and TN Series: You can create up to 512 static routes.
- NAT Series: You can create up to 32 static routes.

Static Route List



UI Setting	Description
Status	Shows the status of the static route.

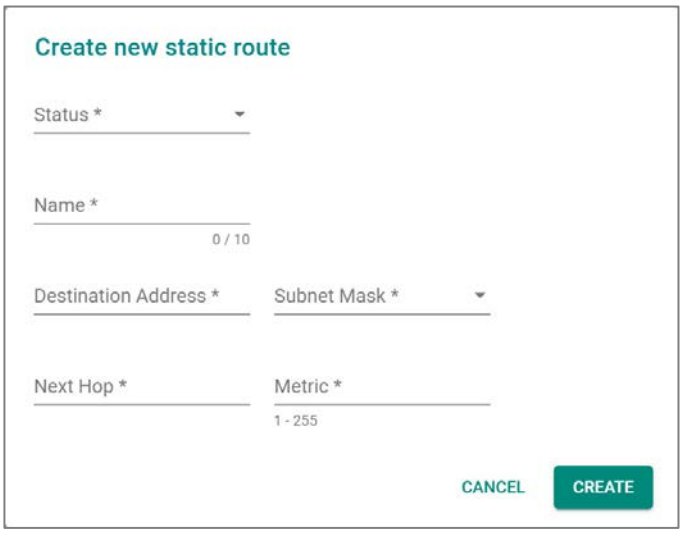
UI Setting	Description
Name	Shows the name of the static route.
Destination Address	Shows the destination IP address for the static route.
Netmask	Shows the subnet mask for the destination IP address.
Next Hop	Shows the next router on the path to the destination IP address.
Metric	Shows the metric value used to determine the priority of the static route. Lower values have higher priority.

Create New Static Route

Menu Path: Routing > Unicast Route > Static Routes

Clicking the **Add (⊞)** icon on the **Routing > Unicast Route > Static Routes** page will open this dialog box. This dialog lets you create a new static route.

Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the static route.	Enabled / Disabled	N/A
Name	Specify a name for the static route.	1 to 10 characters	N/A

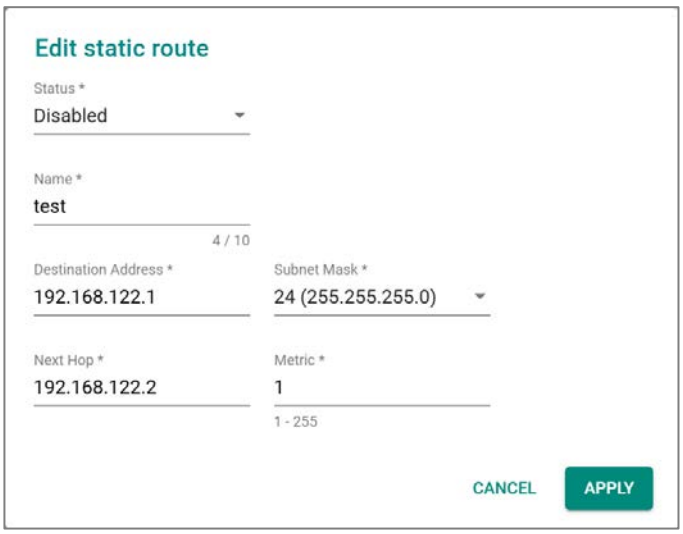
UI Setting	Description	Valid Range	Default Value
Destination Address	Specify the destination IP address for the static route.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
Next Hop	Specify the next router on the path to the destination IP.	Valid IP address	N/A
Metric	Specify the metric value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A

Edit a Static Route

Menu Path: Routing > Unicast Route > Static Routes

Clicking the **Edit ( )** icon for an entry on the **Routing > Unicast Route > Static Routes** page will open this dialog box. This dialog lets you edit an existing static route.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the static route.	Enabled / Disabled	N/A
Name	Specify a name for the static route.	1 to 10 characters	N/A

UI Setting	Description	Valid Range	Default Value
Destination Address	Specify the destination IP address for the static route.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
Next Hop	Specify the next router on the path to the destination IP.	Valid IP address	N/A
Metric	Specify the metric value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A

Delete Static Route

Menu Path: Routing > Unicast Route > Static Routes

You can delete entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

RIP

Menu Path: Routing > Unicast Route > RIP

This page lets you configure RIP (Routing Information Protocol), a distance-vector routing protocol that employs the hop count as a routing metric. RIP prevents routing from looping by implementing a limit on the number of hops allowed in a path from the source to a destination.

Click **APPLY** to save your changes.

RIP Settings

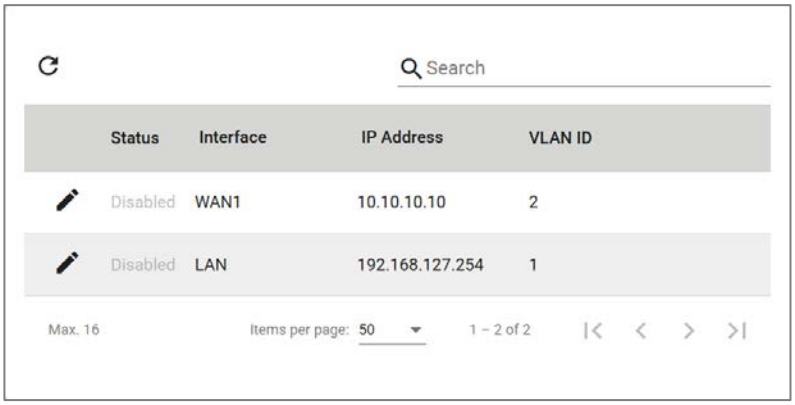
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable RIP protocol.	Enabled / Disabled	Disabled
Version	Set the RIP protocol version: • **V1**: RIP V1 uses classful routing. This means that network addresses are assigned to specific classes, and the subnet mask is determined by the class of the network address. • **V2**: RIP V2 uses classless routing. This means that network addresses can be assigned in a more flexible way, and the subnet mask can be specified independently of the network address class.	V1 / V2	V2
Redistribute	Set which rules to enable for RIP redistribution. You can enable multiple redistribution rules. • **Connected**: Entries learned from directly connected interfaces will be re-distributed. • **Static**: Entries set in a static route will be re-distributed. • **OSPF**: Entries learned from the OSPF will be re-distributed. **Note** Redistribute in RIP refers to the process of importing routing information from other routing protocols into the RIP routing table, allowing for interconnectivity between different protocols and complex networks.	Connected / Static / OSPF	N/A

RIP Interface List

This list shows all of your device interfaces and the RIP settings applied to each one.

Note

Interfaces and their settings can be configured in Network Interfaces. VLAN IDs can be configured in VLAN.



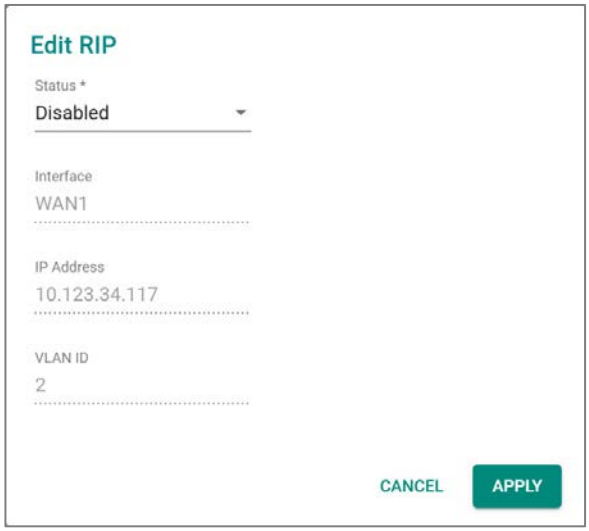
UI Setting	Description
Status	Shows whether RIP is enabled or disabled for the interface.
Interface	Shows the name of the interface.
IP Address	Shows the IP address of the interface.
VLAN ID	Shows the VLAN ID of the interface.

Edit RIP

Menu Path: Routing > Unicast Route > RIP

Clicking the **Edit ( )** icon for an interface on the **Routing > Unicast Route > RIP** page will open this dialog box. This dialog lets you edit the RIP settings for the interface.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable RIP for the interface.	Enabled / Disabled	Disabled
Interface (View-only)	Shows the name of the interface.	Interface name	N/A
IP Address (View-only)	Shows the IP address of the interface.	Interface IP address	N/A
VLAN ID (View-only)	Shows the VLAN ID of the interface.	Interface VLAN ID	N/A

OSPF

Menu Path: Routing > Unicast Route > OSPF

This section lets you configure OSPF (Open Shortest Path First) routing for your device.

This section includes these pages:

- OSPF Settings
- OSPF Status

OSPF Settings

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings

This page lets you configure OSPF settings for your device.

This page includes these tabs:

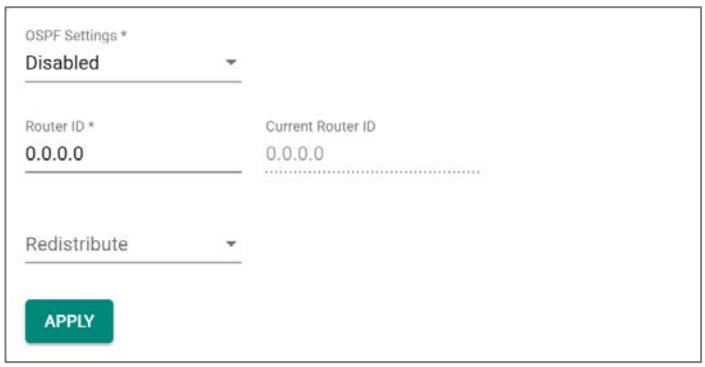
- General
- Area
- Interface
- Aggregation
- Virtual Link

OSPF Settings - General

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - General

This page lets you adjust the basic settings for OSPF.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
OSPF Settings	Enable or disable OSPF for your device.	Enabled / Disabled	Disabled
Router ID	Specify the Router ID of your Moxa router. **Note** The router ID, which must be established for every OSPF instance, should be written in the dot-decimal format of an IP address (e.g., 1.2.3.4) and does not need to be part of any routable subnet on the network, since it is an IP address.	Router ID	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Current Router ID **(View-only)**	Specify the current Router ID of your Moxa router. **Note** When the Router ID is set to 0.0.0.0, the Current Router ID will automatically use the highest interface IP address.	Current Router ID	0.0.0.0
Redistribute	Specify the OSPF redistribution method: • **Connected**: Entries learned from the directly connected interfaces will be redistributed. • **Static**: Entries set in a static route will be redistributed. • **RIP**: Entries learned from RIP will be redistributed. **Note** Redistributing in OSPF refers to the process of importing routing information from other routing protocols–such as RIP, EIGRP, etc.–into the OSPF routing table.	Connected / Static / RIP	N/A

OSPF Settings - Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

This page lets you define OSPF areas.

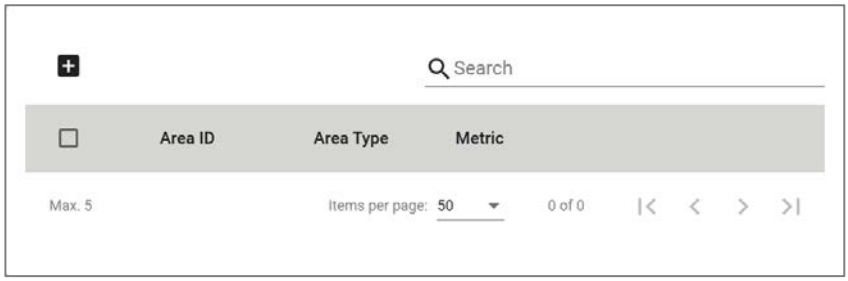
Note

Areas are used to divide a large network into smaller network areas. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside of the area. This reduces the amount of routing traffic between parts of an autonomous system.

Limitations

You can create up to 5 OSPF areas.

OSPF Area List



UI Setting	Description
Area ID	Shows the area's ID.
Area Type	Shows the type of OSPF routing used for the area.
Metric	Shows the metric value/cost for OSPF in the area if **Area Type** is **Stub** or **NSSA**.

Create Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

Clicking the **Add ( )** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Area** page will open this dialog box. This dialog lets you create a new OSPF area. Click **CREATE** to save your changes and add the new area.

UI Setting	Description	Valid Range	Default Value
Area ID	Specify an ID for this OSPF area.	N/A	N/A
Area Type	Specify the type of OSPF routing to use for this area: • **Normal**: A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing. • **Stub**: A stub area is an OSPF area that does not allow external routes to be imported into the area. • **NSSA**: An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.	Normal / Stub / NSSA	Normal
Metric **(If Area Type is Stub or NSSA)**	Specify the metric value/cost to use for this area. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

Edit Area

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

Clicking the **Edit ( )** icon for an OSPF area on the **Routing > Unicast Route > OSPF > OSPF Settings - Area** page will open this dialog box. This dialog lets you modify an existing OSPF area.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Area ID	Specify an ID for this OSPF area.	N/A	N/A
Area Type	Specify the type of OSPF routing to use for this area: • **Normal**: A normal (or standard) area is an OSPF area that allows both intra-area and inter-area routing. • **Stub**: A stub area is an OSPF area that does not allow external routes to be imported into the area. • **NSSA**: An NSSA (Not-So-Stubby Area) is a special type of OSPF area that allows external routing information to be imported into the area, but does not allow the area to propagate that information to other areas.	Normal / Stub / NSSA	Normal
Metric **(If Area Type is Stub or NSSA)**	Specify the metric value/cost to use for this area. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

Delete Area

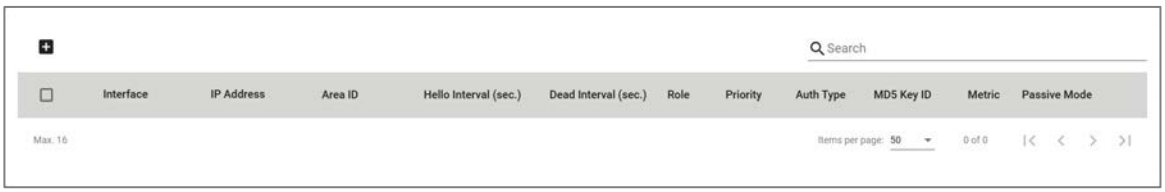
Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area

You can delete an OSPF area by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

OSPF Settings - Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

This page lets you configure the OSPF settings for each of your interfaces. To manage your interfaces, refer to Network Interfaces.



UI Setting	Description
Interface	Shows which interface this entry describes.
IP Address	Shows the IP address of the interface.
Area ID	Shows the OSPF area ID used for the interface.
Hello Interval (sec.)	Shows the hello message interval for the interface.
Dead Interval (sec.)	Shows the dead interval for the interface.
Role	Shows the role of the interface.
Priority	Shows the priority of the interface. Higher numbers have higher priority.
Auth Type	Shows the authentication type used to authenticate OSPF neighbors.
MD5 Key ID **(If Auth Type is MD5)**	Shows the MD5 key ID used to authenticate OSPF neighbors.
Metric	Shows the metric value/cost to OSPF. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.
Passive Mode	Shows the status of passive mode.

OSPF Settings - Create Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

Clicking the **Add ( )** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Interface** page will open this dialog box. This dialog lets you select an interface and configure OSPF settings for it.

Click **CREATE** to save your changes and add the new entry.

Note

You cannot create new interfaces in this dialog; you can only select existing interfaces. To create a new interface, refer to Network Interfaces.

UI Setting	Description	Valid Range	Default Value
Interface	Specify which interface to assign to an OSPF area.	Drop-down list of interfaces	N/A
Area ID	Select an OSPF area ID to assign to the interface. **Note** To manage OSPF areas, refer to Routing > Unicast Route > OSPF > OSPF Settings - Area.	Drop-down list of area IDs	N/A
Priority	Specify the priority of the interface. Higher numbers have higher priority.	0 to 255	1
Hello Interval	Specify the hello message interval in seconds for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535	10

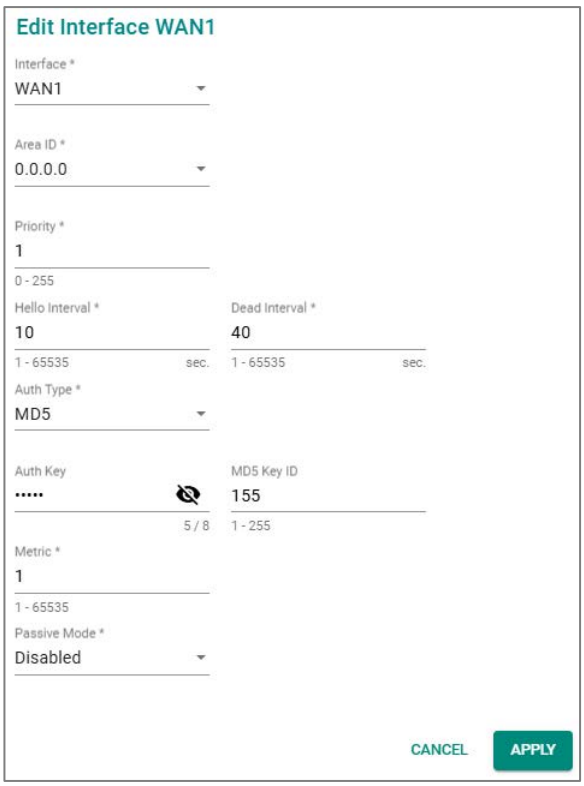
UI Setting	Description	Valid Range	Default Value
Dead Interval	Specify the dead interval in seconds for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535	40
Auth Type	Specify the authentication type to use when authenticating OSPF neighbors. • **None**: No authentication method will be used for neighbor authentication. • **Simple**: Neighbors will be authenticated using an auth key. • **MD5**: Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
Auth Key **(If Auth Type is Simple or MD5)**	Specify the auth key to use for neighbor authentication. • If **Auth Type** is **Simple**, the auth key will be a pure-text password. • If **Auth Type** is **MD5**, the auth key will be an encrypted password.	1 to 8 characters	N/A
MD5 Key ID **(If Auth Type is MD5)**	Specify the MD5 key ID to use for neighbor authentication. **Note** MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
Metric	Specify the metric value/cost for OSPF. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1
Passive Mode	Specify the status of passive mode.	Enabled / Disabled	Disabled

OSPF Settings - Edit Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

Clicking the **Edit ( )** icon for an entry on the **Routing > Unicast Route > OSPF > OSPF Settings - Interface** page will open this dialog box. This dialog lets you edit existing OSPF settings for an interface.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Interface	Specify which interface to assign to an OSPF area.	Drop-down list of interfaces	N/A
Area ID	Select an OSPF area ID to assign to the interface. **Note** To manage OSPF areas, refer to Routing > Unicast Route > OSPF > OSPF Settings - Area.	Drop-down list of area IDs	N/A

UI Setting	Description	Valid Range	Default Value
Priority	Specify the priority of the interface. Higher numbers have higher priority.	0 to 255	1
Hello Interval	Specify the hello message interval in seconds for the interface. The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.	1 to 65535	10
Dead Interval	Specify the dead interval in seconds for the interface. The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.	1 to 65535	40
Auth Type	Specify the authentication type to use when authenticating OSPF neighbors. • **None**: No authentication method will be used for neighbor authentication. • **Simple**: Neighbors will be authenticated using an auth key. • **MD5**: Neighbors will be authenticated more securely by using an auth key and an MD5 key ID.	None / Simple / MD5	N/A
Auth Key **(If Auth Type is Simple or MD5)**	Specify the auth key to use for neighbor authentication. • If **Auth Type** is **Simple**, the auth key will be a pure-text password. • If **Auth Type** is **MD5**, the auth key will be an encrypted password.	1 to 8 characters	N/A
MD5 Key ID **(If Auth Type is MD5)**	Specify the MD5 key ID to use for neighbor authentication. **Note** MD5 authentication method uses MD5 to calculate a hash value from the contents of the OSPF packet and the authentication key. This hash value is transmitted in the packet, along with a key ID.	1 to 255	1
Metric	Specify the metric value/cost for OSPF. **Note** Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.	1 to 65535	1

UI Setting	Description	Valid Range	Default Value
Passive Mode	Specify the status of passive mode.	Enabled / Disabled	Disabled

OSPF Settings - Delete Interface

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Note

Please note that this will delete the OSPF settings for the interface, but it will not delete the interface itself.

OSPF Settings - Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

This page lets you aggregate different OSPF areas into a single routing table entry.

Limitations

You can create up to 5 OSPF aggregations.

UI Setting	Description
Area ID	Shows the area ID.

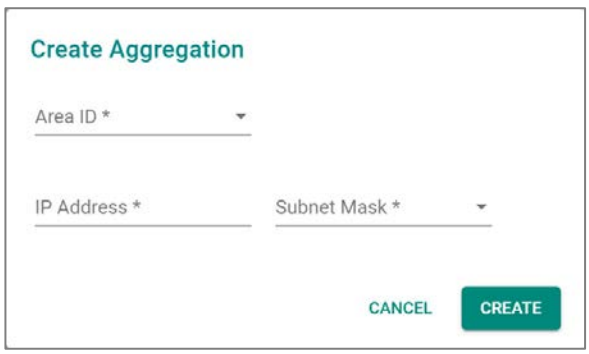
UI Setting	Description
IP Address	Shows the IP address of the area.
Subnet Mask	Shows the network subnet mask.

Create an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

Clicking the **Add (⊕)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you create an OSPF aggregation.

Click **CREATE** to save your changes and add the new aggregation.



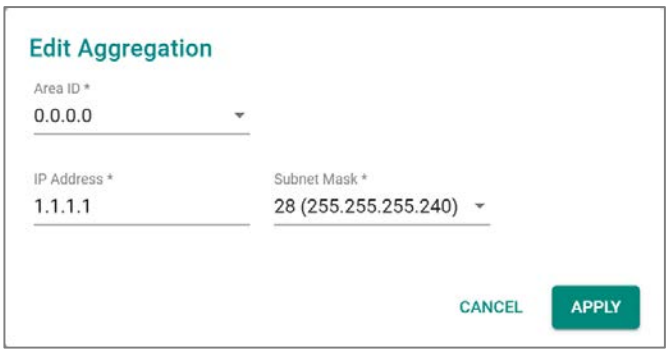
UI Setting	Description	Valid Range	Default Value
Area ID	Select the area ID that you want to use for the aggregation.	Drop-down list of area IDs	N/A
IP Address	Specify the IP address to use for the area.	Valid IP address	N/A
Subnet Mask	Select the network subnet mask to use for the area.	Drop-down list of subnet masks	N/A

Edit an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

Clicking the **Edit ( )** icon for an entry on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you modify an existing aggregation.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Area ID	Select the area ID that you want to use for the aggregation.	Drop-down list of area IDs	N/A
IP Address	Specify the IP address to use for the area.	Valid IP address	N/A
Subnet Mask	Select the network subnet mask to use for the area.	Drop-down list of subnet masks	N/A

Delete an Aggregation

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Virtual Link

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

This page lets you configure virtual links, which can be used to connect areas in an OSPF autonomous system when physical connection to the backbone area is not possible.

Limitations

You can create up to 5 OSPF virtual links.

Virtual Link List

UI Setting	Description
Area ID	Shows the area ID for the virtual link.
Router ID	Shows the router ID for the virtual link.

Create a Virtual Link

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

Clicking the **Add ( )** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link** page will open this dialog box. This dialog lets you create an OSPF virtual link.

Click **CREATE** to save your changes and add the entry.

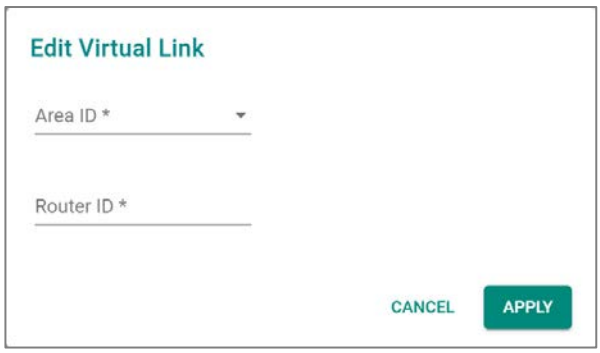
UI Setting	Description	Valid Range	Default Value
Area ID	Select the area to use for the virtual link.	Drop-down list of area IDs	N/A
Router ID	Specify the router ID for the virtual link. **Note** To establish a virtual link in OSPF, you must input the corresponding router ID obtained from the Area Border Router (ABR) configuration. For Moxa routers, the router ID can be found in OSPF Settings - General.	Valid router ID	N/A

Edit Virtual Link

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

Clicking the **Edit ( )** icon for an entry on the **Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link** page will open this dialog box. This dialog lets you modify an existing virtual link.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Area ID	Select the area to use for the virtual link.	Drop-down list of area IDs	N/A

UI Setting	Description	Valid Range	Default Value
Router ID	Specify the router ID for the virtual link. **Note** To establish a virtual link in OSPF, you must input the corresponding router ID obtained from the Area Border Router (ABR) configuration. For Moxa routers, the router ID can be found in OSPF Settings - General.	Valid router ID	N/A

Delete Virtual Link

Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

OSPF Status

Menu Path: Routing > Unicast Route > OSPF > OSPF Status

This page lets you view the OSPF routing status of your device.

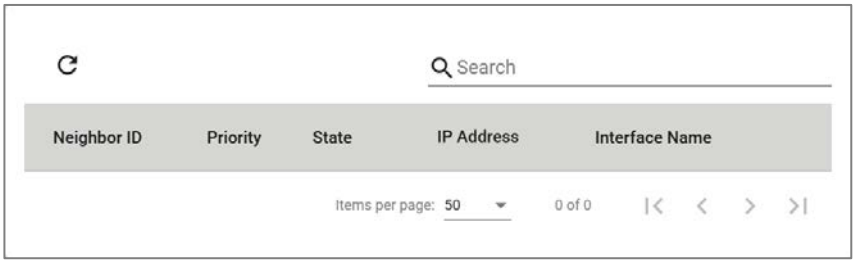
This page includes these tabs:

- Neighbor
- Database

Neighbor

Menu Path: Routing > Unicast Route > OSPF > OSPF Status - Neighbor

This page lets you see the status of OSPF neighbors. OSPF neighbors are devices that share their link-state information with other devices in the network.

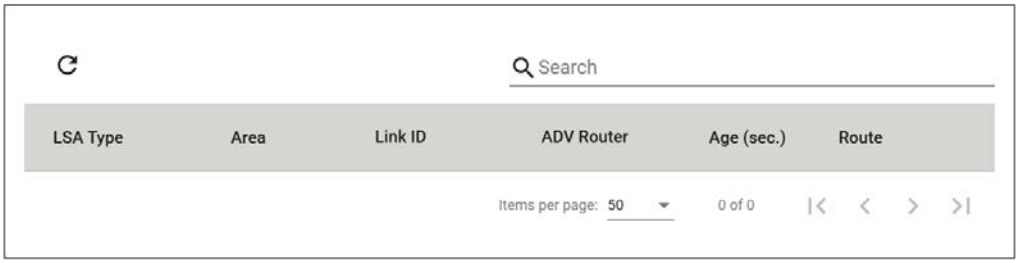


UI Setting	Description
Neighbor ID	Shows the unique identifier for the OSPF neighbor.
Priority	Shows priority value that the neighbor has assigned to itself.
State	Shows the current state of the OSPF neighbor relationship: • **Down:** The initial state before any OSPF communication has occurred between two routers. • **Init**: The state where the local router has sent an OSPF Hello packet to a neighbor but has not yet received a response. • **2-way**: The state where both routers have exchanged Hello packets and can become neighbors, but they have not yet established a bidirectional relationship. • **Exstart**: The state where the routers determine which one will be the master and which one will be the slave during the database exchange process. • **Exchange**: The state where the routers exchange link-state advertisement (LSA) headers and determine which LSAs need to be sent. • **Loading**: The state where the routers exchange LSAs to synchronize their link-state databases. • **Full**: The final state where the routers have a complete and accurate view of the network topology and are ready to forward traffic.
IP Address	Shows the IP address of the neighbor router's interface used for OSPF communication.
Interface Name	Shows the name of the local interface used for OSPF communication with the neighbor.

Database

Menu Path: Routing > Unicast Route > OSPF > OSPF Status - Database

This page lets you see the list of link-state advertisements (LSAs) that describe the network topology, which is used to calculate the shortest path to a destination.

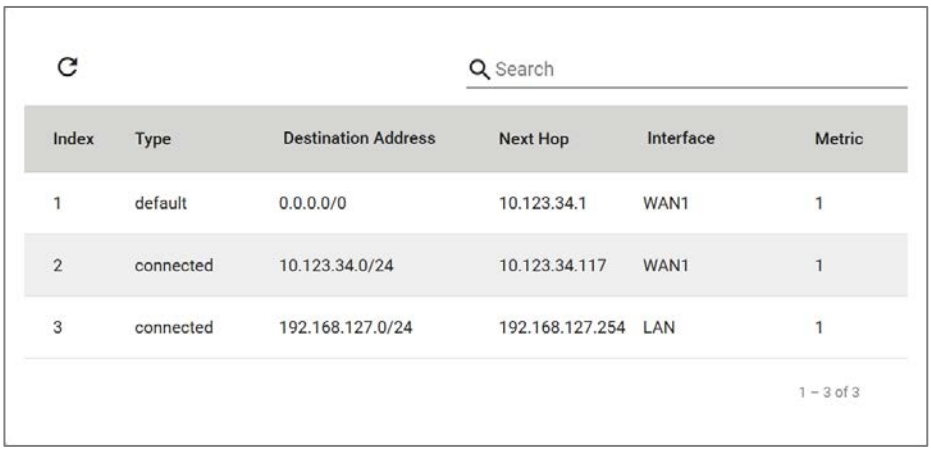


UI Setting	Description
LSA Type	Shows the type of the LSA, which describes the contents of the OSPF LSA packet. • **Router LSA**: Describes the links attached to a router and is flooded within the same area as the router. • **Network LSA**: Describes the routers attached to a multi-access network. • **Summary LSA**: Advertises reachability information between OSPF areas. • **AS External LSA**: Advertises routes to networks outside the OSPF domain. • **NSSA External LSA**: Similar to the Type 5 LSA, but used in a Not-So-Stubby Area (NSSA) to advertise external routes. • **Link-local LSA**: Used to advertise IPv6 link-local addresses and is flooded throughout the same link-local scope.
Area	Shows the area of the network to which the LSA belongs.
Link ID	Shows the endpoint of the link described by the LSA.
ADV Router	Shows the router that the LSA originated from.
Age (sec.)	Shows the age of the LSA in seconds.
Route	Shows the shortest route calculated by OSPF based on the information in the LSA.

Routing Table

Menu Path: Routing > Unicast Route > Routing Table

This page lets you see the current routing table for your device.



UI Setting	Description
Index	Shows the unique identifier for the routing table entry.
Type	Shows the source type of the route.
Destination Address	Shows the address of the destination network for the route.
Next Hop	Shows the IP address of the next hop router or gateway that the packet should be forwarded to.
Interface	Shows the outgoing interface that should be used to reach the destination network.
Metric	Shows the metric value/cost of the route to the destination network.

Note

Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

Multicast Route

Menu Path: Routing > Multicast Route

This section lets you configure multicast routing for your device.

This section includes these pages:

- Multicast Route Settings

- Static Multicast Route
- Multicast Forwarding Table

Multicast Route Settings

Menu Path: Routing > Multicast Route > Multicast Route Settings

This page lets you enable or disable multicast routing.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Mode	Enable or disable multicast routing.	Disabled / Static Multicast Route	Disabled

Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

This page lets you manage multicast routes for your device.

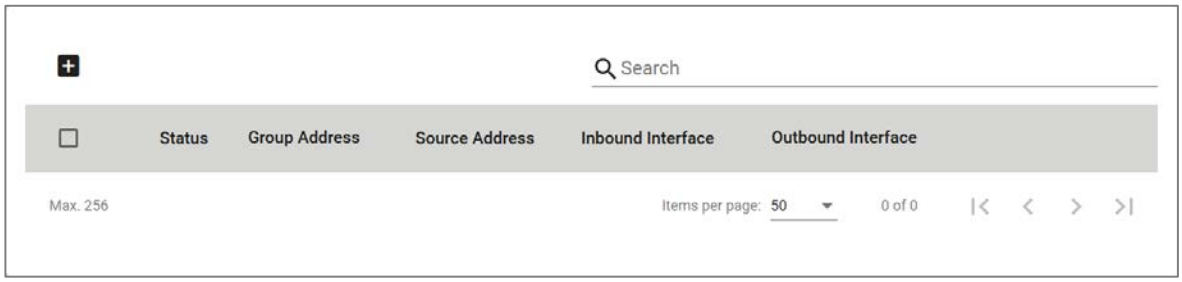
Limitations

You can create up to 256 static multicast routes.

Static Multicast Route Settings

UI Setting	Description	Valid Range	Default Value
VRRP-Master-Only	Enable or disable VRRP-Master-Only. When enabled, only the VRRP master will forward the multicast stream.	Enabled / Disabled	Disabled

Static Multicast Route List



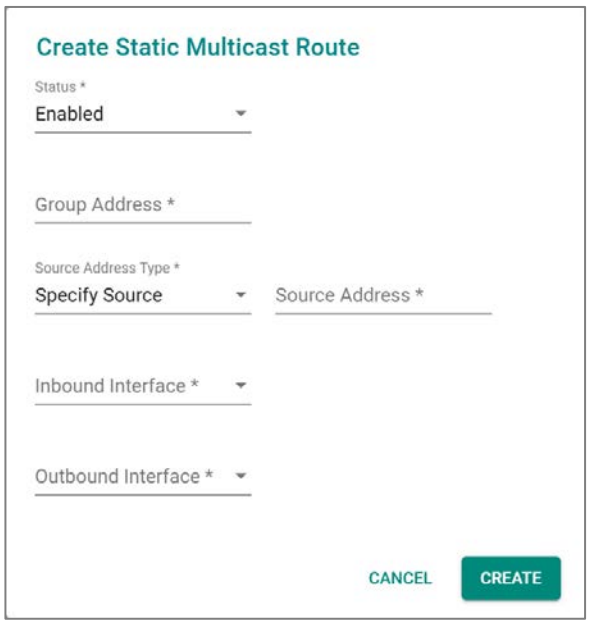
UI Setting	Description
Status	Shows whether the static multicast route is enabled or disabled.
Group Address	Shows the group IP address for the route.
Source Address	Shows the source address for the route.
Inbound Interface	Shows the inbound interface for the route.
Outbound Interface	Shows the outbound interfaces for the route.

Create Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

Clicking the **Add (⊞)** icon on the **Routing > Multicast Route > Static Multicast Route** page will open this dialog box. This dialog lets you add a new static multicast route.

Click **CREATE** to save your changes and add the new account.



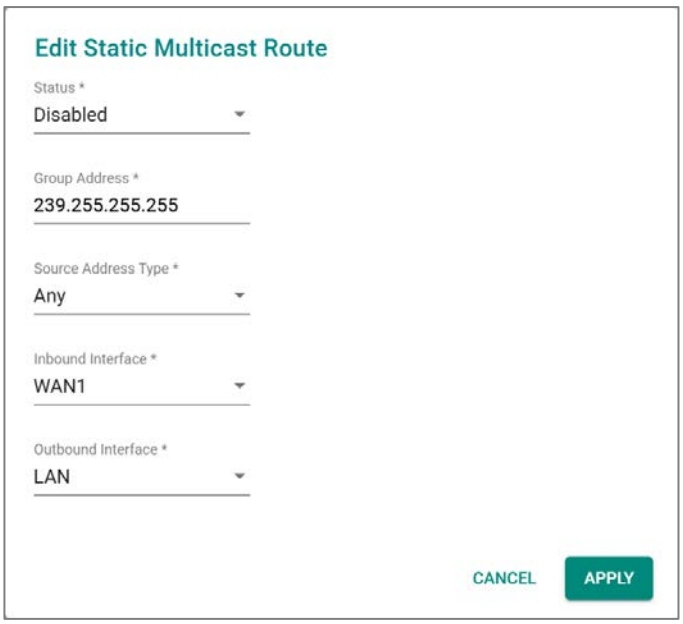
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this route.	Enabled / Disabled	Enabled
Group Address	Specify the group IP address for this route.	N/A	N/A
Source Address Type	Specify the type of source address to use for this route. • **Any**: Allow any IP to be the source address. • **Specify Source**: Use the specified **Source Address**.	Any / Specify Source	Any
Source Address **(If Source Address Type is Specify Source)**	Specify the source IP address to use for this route.	N/A	N/A
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interfaces the broadcast packets will be routed to.	Drop-down list of interfaces	N/A

Edit Static Multicast Route

Menu Path: Routing > Multicast Route > Static Multicast Route

Clicking the **Edit ( )** icon for an entry on the **Routing > Multicast Route > Static Multicast Route** page will open this dialog box. This dialog lets you modify an existing static multicast route.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this route.	Enabled / Disabled	Enabled
Group Address	Specify the group IP address for this route.	N/A	N/A
Source Address Type	Specify the type of source address to use for this route. • **Any**: Allow any IP to be the source address. • **Specify Source**: Use the specified **Source Address**.	Any / Specify Source	Any
Source Address **(If Source Address Type is Specify Source)**	Specify the source IP address to use for this route.	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interfaces the broadcast packets will be routed to.	Drop-down list of interfaces	N/A

Delete Static Multicast Route

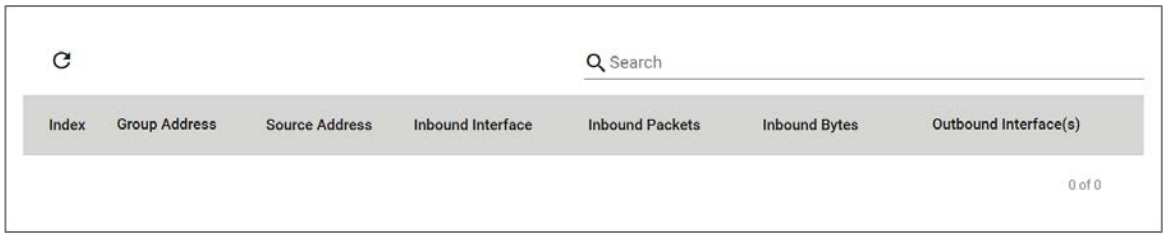
Menu Path: Routing > Multicast Route > Static Multicast Route

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Multicast Forwarding Table

Menu Path: Routing > Multicast Route > Multicast Forwarding Table

This page lets you see the multicast forwarding table for your device.



UI Setting	Description
Index	Shows the index of the entry.
Group Address	Shows the group IP address of the entry.
Source Address	Shows the source address of the entry.
Inbound Interface	Shows the inbound interface of the entry.
Inbound Packets	Shows the number of inbound packets for the entry.
Inbound Bytes	Shows the size of the inbound payload (in bytes) for the entry.
Outbound Interface(s)	Shows the outbound interfaces of the entry.

Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

This page lets you set up broadcast forwarding. Broadcast forwarding enables users to specify the interface and UDP ports that broadcast packets will use to pass through the router, allowing devices to be queried on the network, such as Modbus devices.

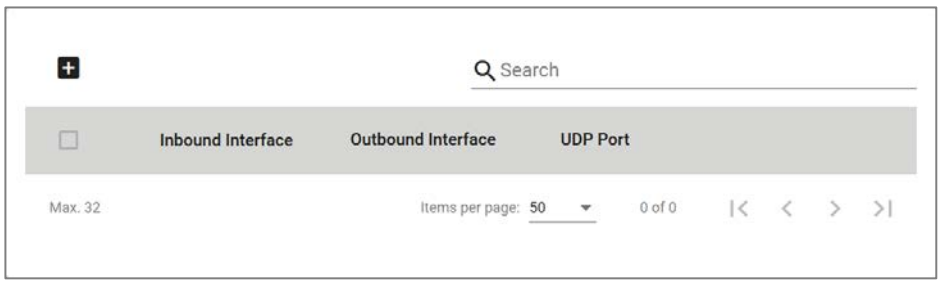
Limitations

You can create up to 32 broadcast forwarding entries.

Broadcast Forwarding Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable broadcast forwarding.	Enabled / Disabled	Disabled

Broadcast Forwarding List



UI Setting	Description
Inbound Interface	Shows which interface broadcast packets will come from.
Outbound Interface	Shows which interface broadcast packets will pass through.

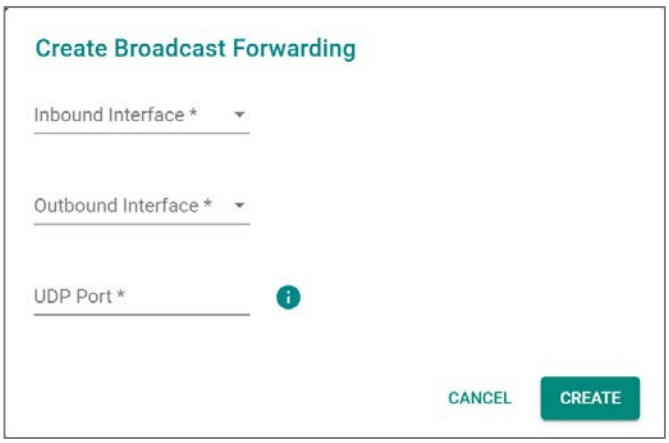
UI Setting	Description
UDP Port	Shows the UDP ports the device will listen to for broadcast packets.

Create Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

Clicking the **Add (⊕)** icon on the **Routing > Broadcast Forwarding** page will open this dialog box. This dialog lets you create a new broadcast forwarding rule.

Click **CREATE** to save your changes and add the new rule.



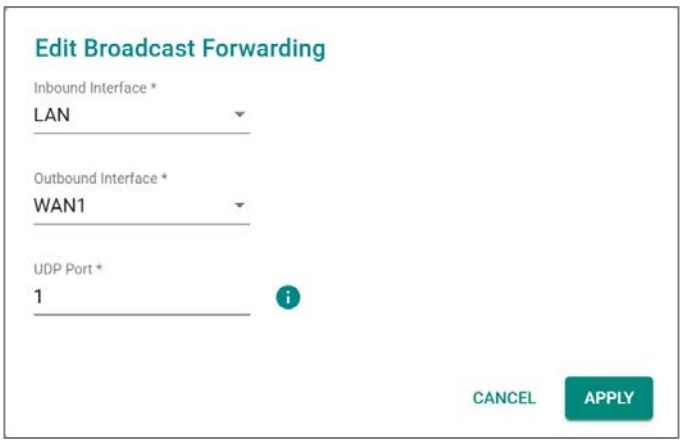
UI Setting	Description	Valid Range	Default Value
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interface broadcast packets will pass through.	Drop-down list of interfaces	N/A
UDP Port	Specify which UDP ports the device will listen to for broadcast packets. You can enter up to 8 ports, separated by commas.	1 to 65535, up to 8 ports separated by commas	N/A

Edit Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

Clicking the **Edit ( )** icon for an entry on the **Routing > Broadcast Forwarding** page will open this dialog box. This dialog lets you modify an existing broadcast forwarding rule.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Inbound Interface	Select which interface broadcast packets will come from.	Drop-down list of interfaces	N/A
Outbound Interface	Select which interface broadcast packets will pass through.	Drop-down list of interfaces	N/A
UDP Port	Specify which UDP ports the device will listen to for broadcast packets. You can enter up to 8 ports, separated by commas.	1 to 65535, up to 8 ports separated by commas	N/A

Delete Broadcast Forwarding

Menu Path: Routing > Broadcast Forwarding

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Directed Forwarding

Menu Path: Routing > Directed Forwarding

This page lets you manage your device's directed forwarding rules.

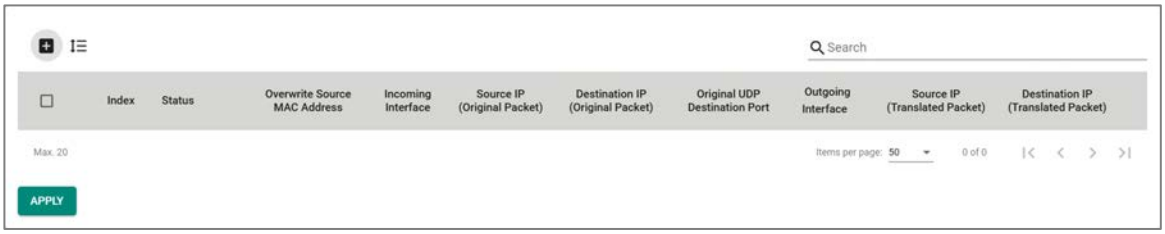
Limitations

You can create up to 20 directed forwarding rules.

Directed Forwarding Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable directed forwarding.	Enabled / Disabled	Disabled

Directed Forwarding Rule List



UI Setting	Description
Index	Shows the index of the rule this entry is for.
Status	Shows whether the rule is enabled.
Overwrite Source MAC Address	Shows whether the overwrite source MAC address option is enabled for the rule.
Incoming Interface	Shows which interface forwarding packets will come from for the rule.

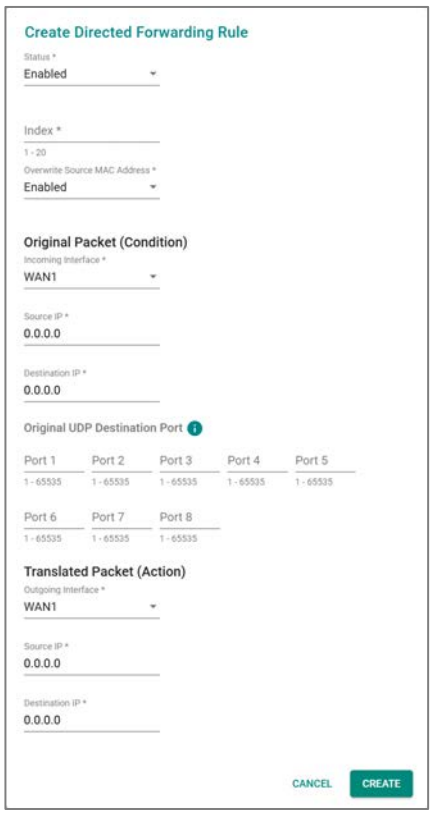
UI Setting	Description
Source IP (Original Packet)	Shows the source IP this rule will apply to.
Destination IP (Original Packet)	Shows the destination IP this rule will apply to.
Original UDP Destination Port	Shows the UDP ports the device will listen to for forwarding packets.
Outgoing Interface	Shows which interface forwarding packets will pass through.
Source IP (Translated Packet)	Shows the source IP this rule will translate to.
Destination IP (Translated Packet)	Shows the destination IP this rule will translate to.

Create Directed Forwarding Rule

Menu Path: Routing > Directed Forwarding

Clicking the **Add (+)** icon on the **Routing > Directed Forwarding** page will open this dialog box. This dialog lets you create a new directed forwarding rule.

Click **CREATE** to save your changes and add the new rule.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	1 to 20	N/A
Index	Specify the index of this rule.	Disabled / Enabled	Enabled
Overwrite Source MAC Address	Enable or disable the overwrite source MAC address option.	Disabled / Enabled	Enabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Shows which interface forwarding packets will come from.	Drop-down list of interfaces	N/A
Source IP	Specify the source IP this rule will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination IP	Specify the destination IP this rule will apply to.	Valid IP address	0.0.0.0
Original UDP Destination Port 1-8	Shows the UDP ports the device will listen to for forwarding packets.	1 to 65535, up to 8 ports	N/A

Translated Packet (Action)

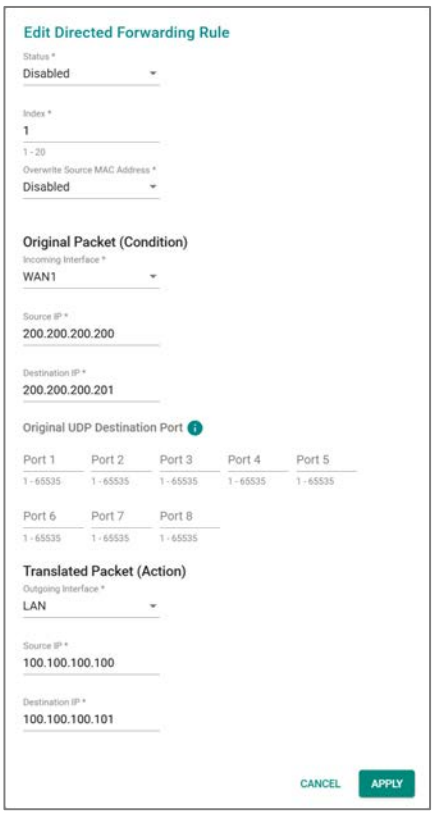
UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Shows which interface forwarding packets will pass through.	Drop-down list of interfaces	N/A
Source IP	Specify the source IP this rule will translate to.	Valid IP address	0.0.0.0
Destination IP	Specify the destination IP this rule will translate to.	Valid IP address	0.0.0.0

Edit Directed Forwarding Rule

Menu Path: Routing > Directed Forwarding

Clicking the **Edit ( )** icon for an entry on the **Routing > Directed Forwarding** page will open this dialog box. This dialog lets you modify an existing broadcast forwarding rule.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index of this rule.	1 to 20	N/A
Status	Enable or disable this rule.	Disabled / Enabled	Enabled
Overwrite Source MAC Address	Enable or disable the overwrite source MAC address option.	Disabled / Enabled	Enabled
Incoming Interface	Shows which interface forwarding packets will come from.	Drop-down list of interfaces	N/A
Source IP (Original Packet)	Specify the source IP this rule will apply to.	Valid IP address	0.0.0.0
Destination IP (Original Packet)	Specify the destination IP this rule will apply to.	Valid IP address	0.0.0.0
Original UDP Destination Port	Shows the UDP ports the device will listen to for forwarding packets.	1 to 65535, up to 8 ports	N/A
Outgoing Interface	Shows which interface forwarding packets will pass through.	Drop-down list of interfaces	N/A

UI Setting	Description	Valid Range	Default Value
Source IP (Translated Packet)	Specify the source IP this rule will translate to.	Valid IP address	0.0.0.0
Destination IP (Translated Packet)	Specify the destination IP this rule will translate to.	Valid IP address	0.0.0.0

Delete Directed Forwarding Rule

Menu Path: Routing > Directed Forwarding

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Tunneling

Menu Path: Tunneling

The Tunneling settings area lets you configure tunneling interfaces for your device.

This settings area includes these sections:

- VXLAN L2 Tunneling
- GRE L3 Tunneling

Tunneling - User Privileges

Privileges to Tunneling settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
VXLAN L2 Tunneling	R/W	R/W	R
GRE L3 Tunneling	R/W	R/W	R

VXLAN L2 Tunneling

Menu Path: Tunneling > VXLAN L2 Tunneling

This section lets you VXLAN interfaces for your device.

Limitations

You can create up to 20 VXLAN interface entries.

VXLAN Interface List

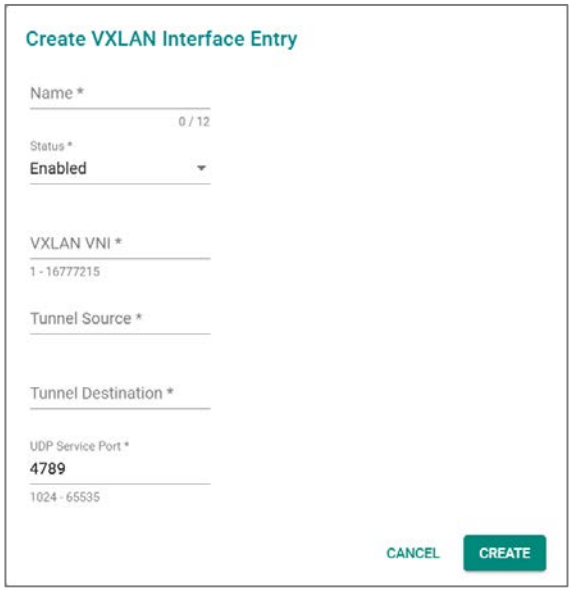
UI Setting	Description
Name	Shows the name of the interface.
Status	Shows whether the interface is enabled or disabled.
VXLAN VNI	Shows the VXLAN VNI value of the interface.
Tunnel Source	Shows the tunnel source of the interface.
Tunnel Destination	Shows the tunnel destination of the interface.
UDP Service Port	Shows the UDP service port of the interface.

Create a VXLAN Interface Entry

Menu Path: Tunneling > VXLAN L2 Tunneling

Clicking the **Add (⊞)** icon on the **Tunneling > VXLAN L2 Tunneling** page will open this dialog box. This dialog lets you create a new VXLAN interface for your device.

Click **CREATE** to save your changes and add the new interface.



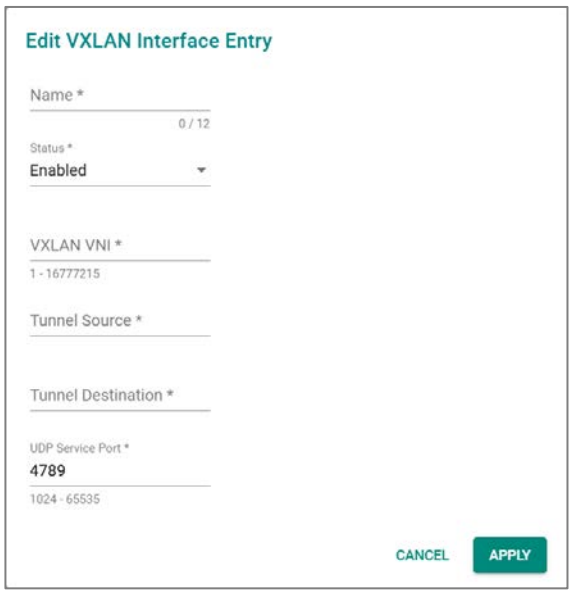
UI Setting	Description	Valid Range	Default Value
Name	Specify the name for the interface.	1 to 12	N/A
Status	Enabled or disable the interface.	Enabled / Disabled	Enabled
VXLAN VNI	Specify a VXLAN VNI for the interface.	1 to 16777215	N/A
Tunnel Source	Specify the tunnel source IP address for the interface.	Valid IP address	N/A
Tunnel Destination	Specify the tunnel destination IP address for the interface.	Valid IP address	N/A
UDP Service Port	Specify the UDP service port for the interface.	1024 to 65535	4789

Edit a VXLAN Interface Entry

Menu Path: Tunneling > VXLAN L2 Tunneling

Clicking the **Edit ( )** icon for an interface on the **Tunneling > VXLAN L2 Tunneling** page will open this dialog box. This dialog lets you edit an existing interface.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify the name for the interface.	1 to 12	N/A
Status	Enabled or disable the interface.	Enabled / Disabled	Enabled
VXLAN VNI	Specify a VXLAN VNI for the interface.	1 to 16777215	N/A
Tunnel Source	Specify the tunnel source IP address for the interface.	Valid IP address	N/A
Tunnel Destination	Specify the tunnel destination IP address for the interface.	Valid IP address	N/A
UDP Service Port	Specify the UDP service port for the interface.	1024 to 65535	4789

Delete a VXLAN Interface Entry

Menu Path: Tunneling > VXLAN L2 Tunneling

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

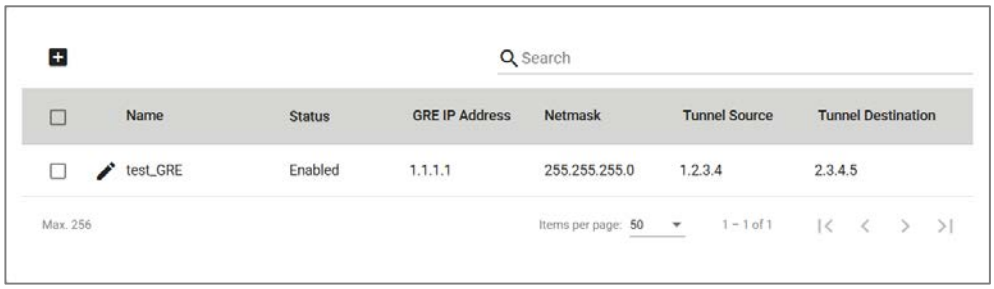
GRE L3 Tunneling

Menu Path: Tunneling > GRE L3 Tunneling

This page lets you create GRE interfaces for your device.

Limitations

You can add up to 256 GRE interface entries.



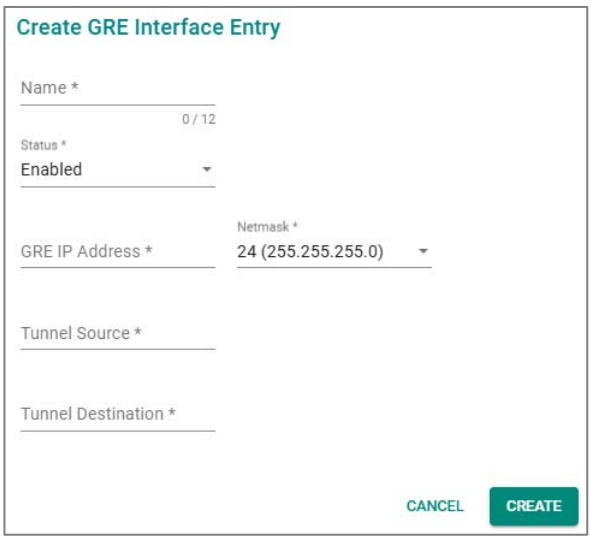
UI Setting	Description
Name	Shows the name of the GRE interface.
Status	Shows whether the GRE interface is enabled or disabled.
GRE IP Address	Shows the IP address of the GRE interface.
Netmask	Shows the netmask of the GRE interface.
Tunnel Source	Shows the tunnel source of the GRE interface.
Tunnel Destination	Shows the tunnel destination of the GRE interface.

Create GRE Interface Entry

Menu Path: Tunneling > GRE L3 Tunneling

Clicking the **Add (⊞)** icon on the **Tunneling > GRE L3 Tunneling** page will open this dialog box. This dialog lets you create a GRE interface.

Click **CREATE** to save your changes and add the new interface.



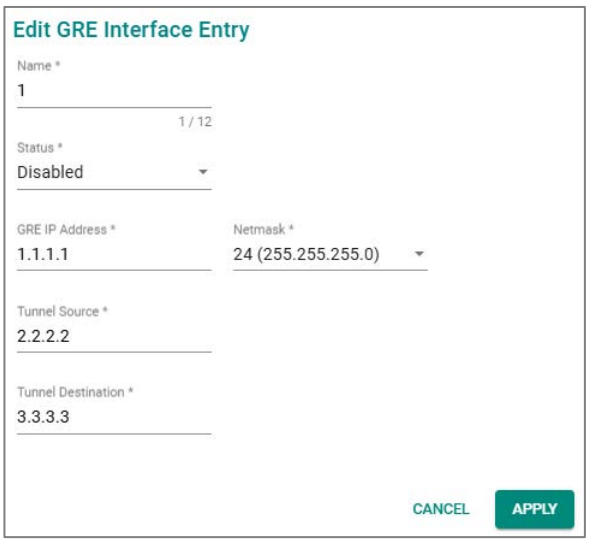
UI Setting	Description	Valid Range	Default Value
Name	Specify the name of the GRE interface.	1 to 12 characters	N/A
Status	Specify whether the GRE interface is enabled or disabled.	Enabled / Disabled	Enabled
GRE IP Address	Specify the IP address of the GRE interface.	Valid IP address	N/A
Netmask	Specify the netmask of the GRE interface.	Drop-down list of subnet masks	24 (255.255.255.0)
Tunnel Source	Specify the tunnel source of the GRE interface.	Valid IP address	N/A
Tunnel Destination	Specify the tunnel destination of the GRE interface.	Valid IP address	N/A

Edit GRE Interface Entry

Menu Path: Tunneling > GRE L3 Tunneling

Clicking the **Edit ( )** icon for an interface on the **Tunneling > GRE L3 Tunneling** page will open this dialog box. This dialog lets you edit an existing interface.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify the name of the GRE interface.	1 to 12 characters	N/A
Status	Specify whether the GRE interface is enabled or disabled.	Enabled / Disabled	Enabled
GRE IP Address	Specify the IP address of the GRE interface.	Valid IP address	N/A
Netmask	Specify the netmask of the GRE interface.	Drop-down list of subnet masks	24 (255.255.255.0)
Tunnel Source	Specify the tunnel source of the GRE interface.	Valid IP address	N/A
Tunnel Destination	Specify the tunnel destination of the GRE interface.	Valid IP address	N/A

Delete GRE Interface

Menu Path: Tunneling > GRE L3 Tunneling

You can delete an interface by using the checkboxes to select the interfaces you want to delete, then clicking the **Delete ( )** icon.

NAT

Menu Path: NAT

This section allows you to manage your device's Network Address Translation (NAT) features.

This section includes these pages:

- NAT Setting
- ALG Settings
- PN-DCP Forwarding

> **Note**
> NAT Series devices currently support the following ALG protocols: FTP, TFTP, SNMP.

NAT - User Privileges

Privileges to NAT settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
NAT Setting	R/W	R/W	R
ALG Settings	R/W	R/W	R
PN-DCP Forwarding	R/W	R/W	R

NAT Setting

Menu Path: NAT > NAT Setting

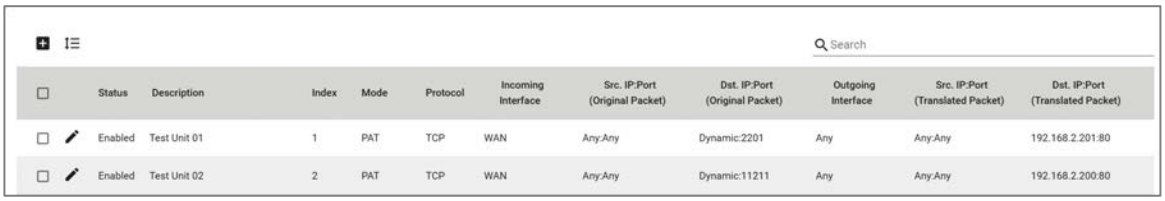
This page lets you manage your device's NAT rules.

Click **APPLY** to save your changes.

Limitations

- EDR, OnCell, and TN Series: You can create up to 512 NAT rules.
- NAT Series: You can create up to 128 NAT rules.

NAT Rule List



UI Setting	Description
Status	Shows whether the NAT rule is enabled or disabled.
Description	Shows the name of the NAT rule.
Index	Shows the index of the NAT rule.
Mode	Shows the NAT mode used by the rule.
Protocol	Shows the protocols included in the NAT rule.
Incoming Interface	Shows the incoming interface.
Src. IP:Port (Original Packet)	Shows the original source IP address and ports for incoming packets.
Dst. IP:Port (Original Packet)	Shows the original destination IP address and ports for incoming packets.
Outgoing Interface	Shows the outgoing interface.
Src. IP:Port (Translated Packet)	Shows the translated source IP address and ports.
Dst. IP:Port (Translated Packet)	Shows the translated destination IP address and ports.

Create Index

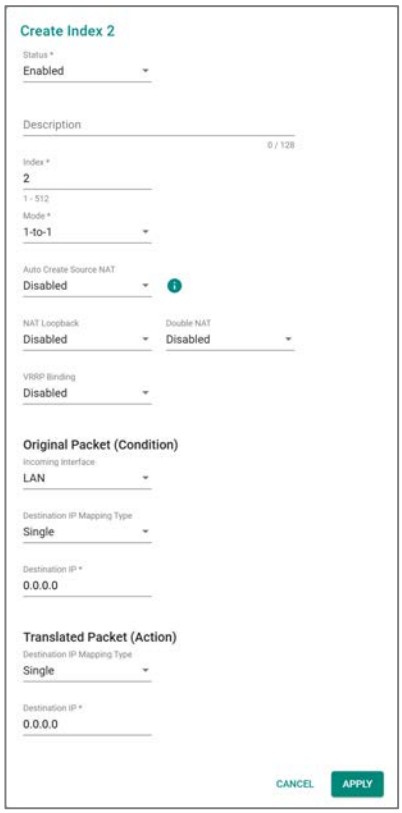
Menu Path: NAT > NAT Setting

Clicking the **Add (⊕)** icon on the **NAT > NAT Setting** page will open this dialog box. This dialog lets you create a new NAT rule. Available settings will change depending on what **Mode** is selected.

Click **CREATE** to save your changes and add the new rule.

Create Index - 1-to-1

If **1-to-1** is selected for the **Mode**, these settings will appear. 1-to-1 NAT maps one public IP address to one private IP address.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of this rule.	1 to 512	N/A
Mode	Specify which NAT mode to use for this rule. • **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. • **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. • **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. • **Advanced**: Allows you to set up an advanced NAT rule. • **Twin IP Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advanced / Twin IP Mapping	1-to-1
Auto Create Source NAT	Enable or disable the Auto Create Source NAT feature. If this is disabled, 1-to-1 NAT will only perform DNAT.	Enabled / Disabled	Disabled
NAT Loopback	Enable or disable NAT Loopback. NAT loopback allows devices on a private network to access a server or service hosted on the same network using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled
VRRP Binding	Select which VRRP index this rule should use, or disable VRRP binding. Virtual Router Redundancy Protocol (VRRP) Binding is a feature that allows the 1-to-1 NAT rule to be bound to a VRRP index. VRRP Binding is only supported in 1-to-1 NAT. If a VRRP index is selected, the 1-to-1 NAT rule is only valid when the system is the master. If no VRRP index is selected, the 1-to-1 NAT rule will be valid regardless of whether the system is the master or backup.	Disabled / VRRP Index No.	Disabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN

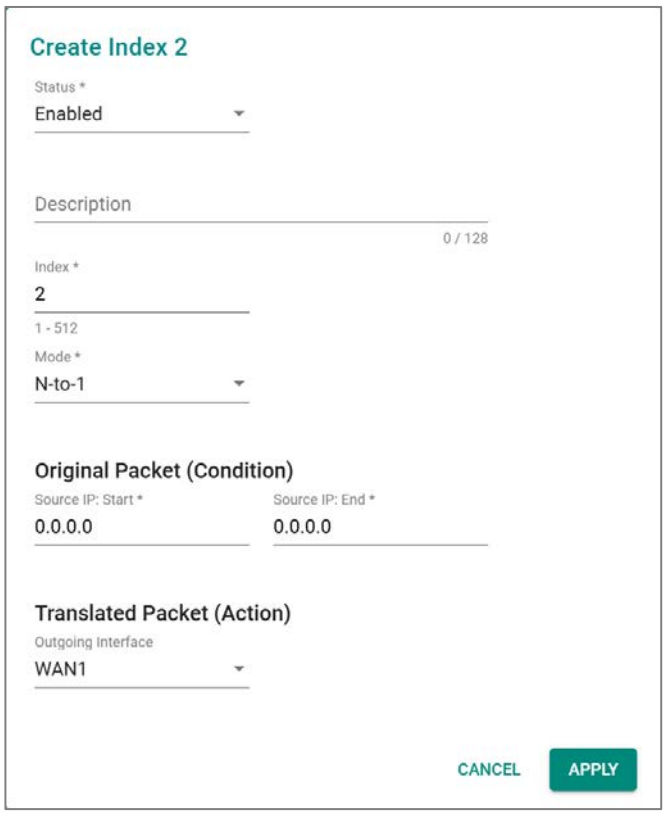
UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify which destination IP addresses will be handled for incoming packets. • **Single**: This rule will apply to a single destination IP for incoming packets. • **Range**: This rule will apply to a range of destination IPs for incoming packets. **Note** With the Range option, you can establish several 1-to-1 NAT mappings within a designated IP address range. Make sure that the Range values for Original Packet (Condition) settings align precisely with the Range values in the Translated Packet (Action) settings for accurate destination IP mapping.	Single / Range	Single
Destination IP **(If Destination IP Mapping Type is Single)**	Specify the destination IP this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify how to handle the destination IP address translation for the internal network. • **Single**: Packets will be translated to a single IP address. • **Range**: Packets will be translated to a range of IP addresses. **Note** With the Range option, you can establish several 1-to-1 NAT mappings within a designated IP address range. Make sure that the Range values for Original Packet (Condition) settings align precisely with the Range values in the Translated Packet (Action) settings for accurate destination IP mapping.	Single / Range	Single
Destination IP **(If Destination IP Mapping Type is Single)**	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range to translate to on the internal network.	Valid IP address	0.0.0.0

Create Index - N-to-1

If **N-to-1** is selected for the **Mode**, these settings will appear. N-to-1 NAT maps multiple private IP addresses to one public IP address.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A
Mode	Specify which NAT mode to use for this rule**.** • **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. • **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. • **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. • **Advanced**: Allows you to set up an advanced NAT rule. • **Twin IP Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advanced / Twin IP Mapping	1-to-1

Original Packet (Condition)

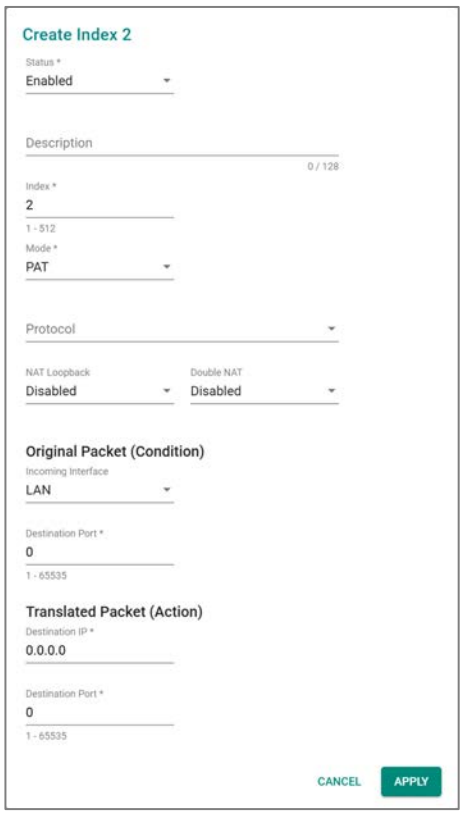
UI Setting	Description	Valid Range	Default Value
Source IP: Start	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source IP: End	Specify the starting IP address of the source IP range this rule will apply to.	Valid IP address	0.0.0.0

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the interface for the NAT rule. **Note** The Outgoing Interface cannot be set to Any, as N-1 NAT requires a specific outgoing interface to be designated.	Drop-down list of interfaces	WAN

Create Index - PAT

If **PAT** is selected for the **Mode**, these settings will appear. Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A
Mode	Specify which NAT mode to use for this rule**.** • **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. • **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. • **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. • **Advanced**: Allows you to set up an advanced NAT rule. • **Twin IP Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advanced / Twin IP Mapping	1-to-1
Protocol	Select which protocols this rule will include.	ICMP / TCP / UDP	N/A

UI Setting	Description	Valid Range	Default Value
NAT Loopback	Enable or disable NAT Loopback. NAT loopback allows devices on a private network to access a server or service hosted on the same network using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
Destination Port	Specify the destination port this rule will apply to.	1 to 65535	Any

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Destination IP	Specify the destination IP to translate to on the internal network.	Valid IP address	0.0.0.0
Destination Port	Specify the port number to translate to on the internal network.	1 to 65535	0

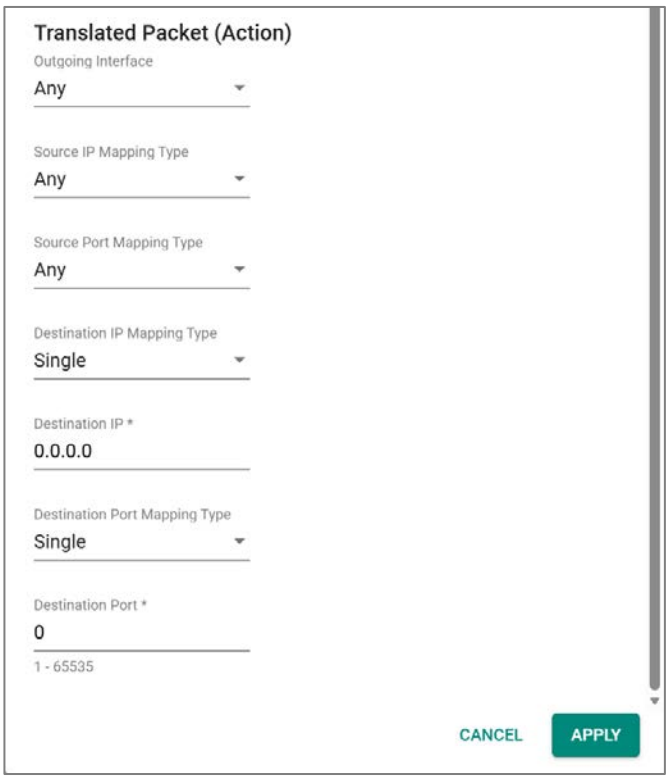
Create Index - Advanced

If **Advanced** is selected for the **Mode**, these settings will appear. This mode allows you to set up an advanced NAT rule, which can provide you with more flexibility for NAT configuration.

Note

Please keep these in mind before setting up an advanced NAT rule:

- When using a Range, please ensure that the corresponding Range values are consistent.
- Advance Mode only allows for a single range to be entered and does not support configuring multiple ranges in the same rule.
- Port settings can only be configured when the Protocol includes either TCP or UDP.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 512	N/A
Mode	Specify which NAT mode to use for this rule**.** • **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. • **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. • **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. • **Advanced**: Allows you to set up an advanced NAT rule. • **Twin IP Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advanced / Twin IP Mapping	1-to-1
Protocol	Select which protocols this rule will include.	ICMP / TCP / UDP	N/A

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
Source IP Mapping Type	Specify which source IP addresses will be handled for incoming packets. • **Any**: This rule will apply to all source IPs. • **Single**: This rule will apply to a single source IP for incoming packets. • **Range**: This rule will apply to a range of source IPs for incoming packets. • **Subnet**: This rule will apply to a source IP and subnet mask.	Any / Single / Range / Subnet	Any
Source IP **(If Source IP Mapping Type is Single or Subnet)**	Specify the source IP this rule will apply to.	Valid IP address	0.0.0.0
Subnet Mask **(If Source IP Mapping Type is Subnet)**	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)
Source IP: Start **(If Source IP Mapping Type is Range)**	Specify the start of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source IP: End **(If Source IP Mapping Type is Range)**	Specify the end of the source IP range this rule will apply to.	Valid IP address	0.0.0.0
Source Port Mapping Type	Specify which source ports will be handled for incoming packets. • **Any**: This rule will apply to all source ports. • **Single**: This rule will apply to a single source port for incoming packets. • **Range**: This rule will apply to a range of source ports for incoming packets.	Any / Single / Range	Any

UI Setting	Description	Valid Range	Default Value
Source Port **(If Source Port Mapping Type is Single)**	Specify the source port this rule will apply to.	1 to 65535	N/A
Source Port: Start **(If Source Port Mapping Type is Range)**	Specify the start of the source port range this rule will apply to.	1 to 65535	N/A
Source Port: End **(If Source Port Mapping Type is Range)**	Specify the end of the source port range this rule will apply to.	1 to 65535	N/A
Destination IP Mapping Type	Specify which destination IP addresses will be handled for incoming packets. • **Any**: This rule will apply to all destination IPs. • **Single**: This rule will apply to a single destination IP for incoming packets. • **Range**: This rule will apply to a range of destination IPs for incoming packets. • **Subnet**: This rule will apply to a destination IP and subnet mask.	Any / Single / Range / Subnet	Any
Destination IP **(If Destination IP Mapping Type is Single or Subnet)**	Specify the destination IP this rule will apply to. **Note** If your host is directly connected to the device or connected through a L2 switch, and the original destination IP is in the hosts' subnet but different from the incoming interface IP, you may add the original destination IP as a secondary IP for the incoming interface so the device can receive and use NAT for traffic from the host. Refer to Secondary IP for more information.	Valid IP address	0.0.0.0
Subnet Mask **(If Destination IP Mapping Type is Subnet)**	Specify the subnet this rule will apply to.	Valid subnet	24 (255.255.255.0)

UI Setting	Description	Valid Range	Default Value
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination Port Mapping Type	Specify which destination ports will be handled for incoming packets. • **Any**: This rule will apply to all destination ports. • **Single**: This rule will apply to a single destination port for incoming packets. • **Range**: This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
Destination Port **(If Destination Port Mapping Type is Single)**	Specify the destination port this rule will apply to.	1 to 65535	N/A
Destination Port: Start **(If Destination Port Mapping Type is Range)**	Specify the start of the destination port range this rule will apply to.	1 to 65535	N/A
Destination IP: End **(If Destination Port Mapping Type is Range)**	Specify the end of the destination port range this rule will apply to.	1 to 65535	N/A

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the interface for the NAT rule. **Note** If a Translated Destination IP is used, the Outgoing Interface cannot be configured.	Drop-down list of interfaces	Any
Source IP Mapping Type	Specify how to handle source IP translation for the internal network. • **Any**: This rule will translate to all source IPs. • **Single**: This rule will translate to a single source IP. • **Range**: This rule will translate to a range of source IPs. • **Subnet**: This rule will translate to a source IP and subnet mask. • **Dynamic**: This rule will translate to the IP of an outgoing interface.	Any / Single / Range / Subnet / Dynamic	Any
Source IP **(If Source IP Mapping Type is Single or Subnet)**	Specify the source IP this rule will translate to. **Note** If Source IP Mapping Type is Single, if the destination host for the desired traffic is directly connected to the device or connected through a L2 switch, and the translated source IP is in the hosts' subnet but different from the outgoing interface IP, you may add the translated source IP as a secondary IP for the outgoing interface so the device can receive and use NAT for traffic going to the destination host. Refer to Secondary IP for more information.	Valid IP address	0.0.0.0
Subnet Mask **(If Source IP Mapping Type is Subnet)**	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)
Source IP: Start **(If Source IP Mapping Type is Range)**	Specify the start of the source IP range this rule will translate to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Source IP: End **(If Source IP Mapping Type is Range)**	Specify the end of the source IP range this rule will translate to.	Valid IP address	0.0.0.0
Source Port Mapping Type	Specify how to handle source port translation for the internal network. • **Any**: This rule will translate to all source ports. • **Single**: This rule will translate to a single source port. • **Range**: This rule will translate to a range of source ports.	Any / Single / Range	Any
Source Port **(If Source Port Mapping Type is Single)**	Specify the source port this rule will translate to. **Note** If the Translated Source IP Mapping Type is set to Dynamic, the Translated Source Port cannot be set.	1 to 65535	N/A
Source Port: Start **(If Source Port Mapping Type is Range)**	Specify the start of the source port range this rule will translate to.	1 to 65535	N/A
Source Port: End **(If Source Port Mapping Type is Range)**	Specify the end of the source port range this rule will translate to.	1 to 65535	N/A
Destination IP Mapping Type	Specify how to handle destination IP address translation for the internal network. • **Any**: This rule will translate to all destination IPs. • **Single**: This rule will translate to a single destination IP. • **Range**: This rule will translate to a range of destination IPs. • **Subnet**: This rule will translate to a destination IP and subnet mask.	Any / Single / Range / Subnet	Any

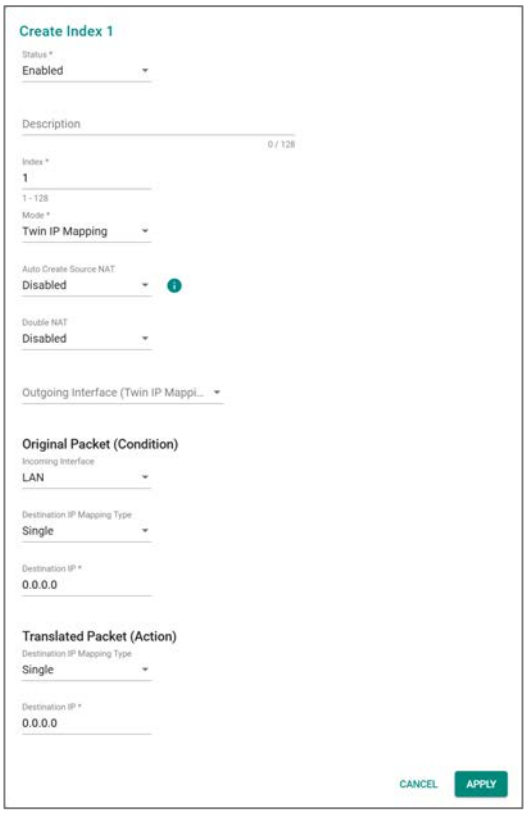
UI Setting	Description	Valid Range	Default Value
Destination IP **(If Destination IP Mapping Type is Single or Subnet)**	Specify the destination IP this rule will translate to.	Valid IP address	0.0.0.0
Subnet Mask **(If Destination IP Mapping Type is Subnet)**	Specify the subnet this rule will translate to.	Valid subnet	24 (255.255.255.0)
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0
Destination Port Mapping Type	Specify how to handle destination port translation for the internal network. • **Any**: This rule will apply to all destination ports. • **Single**: This rule will apply to a single destination port for incoming packets. • **Range**: This rule will apply to a range of destination ports for incoming packets.	Any / Single / Range	Any
Destination Port **(If Destination Port Mapping Type is Single)**	Specify the destination port this rule will translate to.	1 to 65535	N/A
Destination Port: Start **(If Destination Port Mapping Type is Range)**	Specify the start of the destination port range this rule will translate to.	1 to 65535	N/A
Destination Port: End **(If Destination Port Mapping Type is Range)**	Specify the end of the destination port range this rule will translate to.	1 to 65535	N/A

Create Index - Twin IP Mapping

If **Twin IP Mapping** is selected for the **Mode**, these settings will appear. This mode allows you to configure NAT with a duplicated LAN IP to provide flexibility for configuring duplicated LAN IP conversion.

Limitations

- Currently, Twin IP Mapping mode is only supported by the NAT-108 Series.
- Twin IP Mapping mode does not support transitioning between duplicate-IP devices.
- Twin IP Mapping mode supports a maximum of 4 duplicate-IP interfaces.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this rule.	Enabled / Disabled	Enabled
Description	Specify a name for this rule.	1 to 128 characters	N/A
Index	Specify the index of this rule.	1 to 128	N/A

UI Setting	Description	Valid Range	Default Value
Mode	Specify which NAT mode to use for this rule. • **1-to-1**: 1-to-1 NAT maps one public IP address to one private IP address. • **N-to-1**: N-to-1 NAT maps multiple private IP addresses to one public IP address. • **PAT**: Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers. • **Advanced**: Allows you to set up an advanced NAT rule. • **Twin IP Mapping**: Allows you to set up a NAT rule with a duplicated LAN IP.	1-to-1 / N-to-1 / PAT / Advanced / Twin IP Mapping	1-to-1
Auto Create Source NAT	Enable or disable the auto create source NAT feature. If this is disabled, 1-to-1 NAT will only perform Destination NAT (DNAT) translation.	Enabled / Disabled	Disabled
NAT Loopback	Enable or disable NAT loopback. NAT loopback allows devices on a private network to access a server or service hosted on the same network by using the public IP address of the network.	Enabled / Disabled	Disabled
Double NAT	Enable or disable Double NAT. Double NAT lets you use 1-to-1 rules to facilitate two-way communication.	Enabled / Disabled	Disabled

Original Packet (Condition)

UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the interface to use for this rule.	Drop-down list of interfaces	LAN
Destination IP Mapping Type	Specify which destination IP addresses will be handled for incoming packets. • **Single**: This rule will apply to a single destination IP for incoming packets. • **Range**: This rule will apply to a range of destination IPs for incoming packets.	Single / Range	Single

UI Setting	Description	Valid Range	Default Value
Destination IP **(If Destination IP Mapping Type is Single)**	Specify the destination IP this rule will apply to. **Note** If your host is directly connected to the device or connected through a L2 switch, and the original destination IP is in the hosts' subnet but different from the incoming interface IP, you may add the original destination IP as a secondary IP for the incoming interface so the device can receive and use NAT for traffic from the host. Refer to Secondary IP for more information.	Valid IP address	0.0.0.0
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will apply to.	Valid IP address	0.0.0.0

Translated Packet (Action)

UI Setting	Description	Valid Range	Default Value
Destination IP Mapping Type	Specify how to handle destination IP address translation for the internal network. • **Single**: This rule will translate to a single destination IP. • **Range**: This rule will translate to a range of destination IPs.	Single / Range	Single
Destination IP **(If Destination IP Mapping Type is Single)**	Specify the destination IP this rule will translate to.	Valid IP address	0.0.0.0
Destination IP: Start **(If Destination IP Mapping Type is Range)**	Specify the start of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination IP: End **(If Destination IP Mapping Type is Range)**	Specify the end of the destination IP range this rule will translate to.	Valid IP address	0.0.0.0

Edit Index

Menu Path: NAT > NAT Setting

Clicking the **Edit ( )** icon for an entry on the **NAT > NAT Setting** page will open a dialog box that lets you edit the entry.

Click **APPLY** to save your changes.

For a complete list of settings, refer to Create NAT Rule.

Delete Index

Menu Path: NAT > NAT Setting

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

ALG Settings

Menu Path: NAT > ALG Settings

This page lets you configure the Application Layer Gateway (ALG) feature, which helps Session Initiation Protocol (SIP) traffic (used for VoIP) function correctly, especially when a device is behind a Network Address Translation (NAT) firewall.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Enable SIP ALG	Enable or disable SIP ALG.	Disabled / Enabled	Disabled

PN-DCP Forwarding

Menu Path: NAT > PN-DCP Forwarding

This page lets you manage the PN-DCP forwarding function, which allows PROFINET discovery packets to pass through the device and provides address forwarding services, enabling PROFINET communication devices to discover each other and successfully establish connections.

Limitations

You can create up to 1 forwarding interface pair.

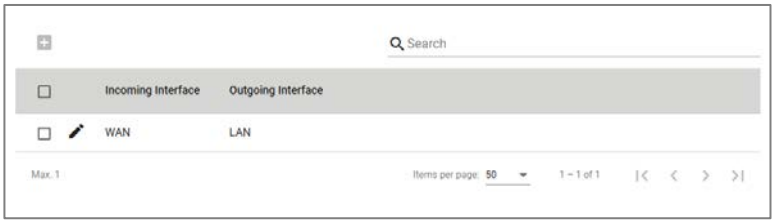
Limitations

You can create up to 20 translated IP entries.

PN-DCP Forwarding Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable PN-DCP forwarding.	Enabled / Disabled	Disabled

PN-DCP Forwarding List



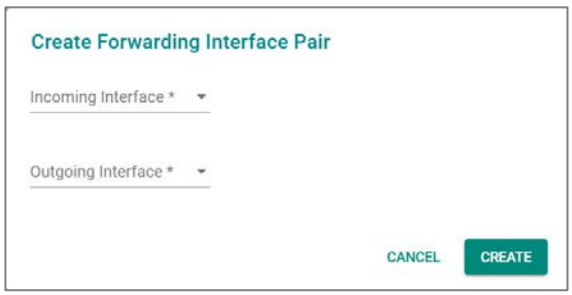
UI Setting	Description
Incoming Interface	Shows the incoming interface used by the policy.
Outgoing Interface	Shows the outgoing interface used by the policy.

Create Forwarding Interface Pair

Menu Path: NAT > PN-DCP Forwarding

Clicking the **Add (⊕)** icon in the Forwarding Interface Pair List on the **NAT > PN-DCP Forwarding** page will open this dialog box. This dialog lets you create a new PN-DCP Forwarding Interface Pair.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

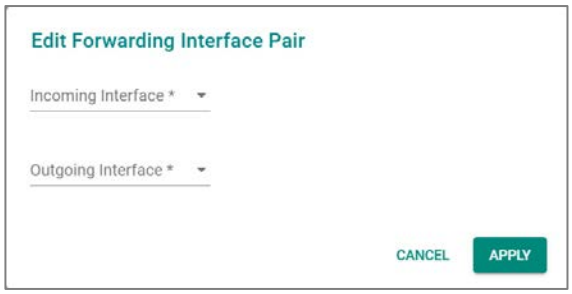
UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

Edit Forwarding Interface Pair

Menu Path: NAT > PN-DCP Forwarding

Clicking the **Edit ( )** icon for an entry in the Forwarding Interface Pair List on the **NAT > PN-DCP Forwarding** page will open this dialog box. This dialog lets you edit an existing entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

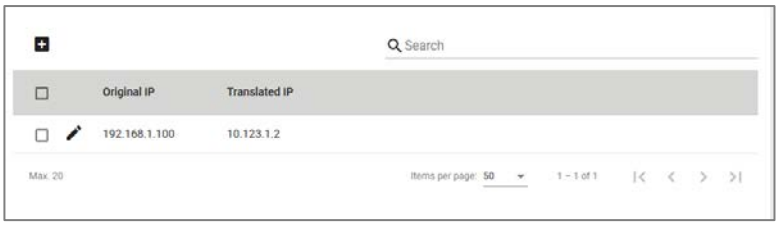
UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

Delete Forwarding Interface Pair

Menu Path: NAT > PN-DCP Forwarding

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Translated IP List



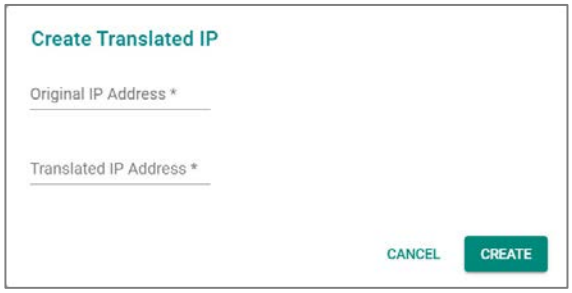
UI Setting	Description
Original IP	Shows the original IP this rule will apply to.
Translated IP	Shows the translated IP to use for the outgoing interface.

Create Translated IP

Menu Path: NAT > PN-DCP Forwarding

Clicking the **Add ( )** icon in the Translated IP List on the **NAT > PN-DCP Forwarding** page will open this dialog box. This dialog lets you create a new translated IP entry.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Original IP Address	Specify the original IP this rule will apply to.	Valid IP address	N/A
Translated IP Address	Specify the translated IP to translate to the outgoing interface.	Valid IP address	N/A

Edit Translated IP

Menu Path: NAT > PN-DCP Forwarding

Clicking the **Edit ( )** icon for an entry in the Translated IP List on the **NAT > PN-DCP Forwarding** page will open this dialog box. This dialog lets you edit an existing entry.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Original IP Address	Specify the original IP this rule will apply to.	Valid IP address	N/A
Translated IP Address	Specify the translated IP to translate to the outgoing interface.	Valid IP address	N/A

Delete Translated IP

Menu Path: NAT > PN-DCP Forwarding

You can delete an entry in the Translated IP List by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Object Management

Menu Path: Object Management

This page lets you use object-based firewall management to help protect your network on a granular level. You can create, modify, and edit the objects you need based on your security requirements. These objects are used when creating Layer 3-7 policies for the device's firewall.

In addition, objects allow for more efficient firewall rule management. A single object can be assigned to multiple rules and changes to the object will apply to all associated rules, removing the need to update individual policies one by one.

This page includes the following tabs:

- Object Member
- Object Member Grouping
- Interface Grouping

Object Management - User Privileges

Privileges to Object Management settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Object Management	R/W	R/W	R

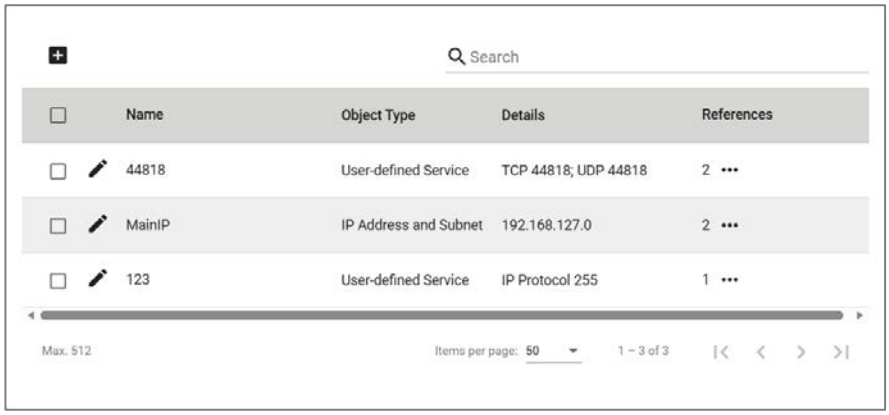
Object Member

Menu Path: Object Management - Object Member

This page lets you create and manage objects that can be used when configuring other features.

Limitations

You can create up to 512 objects.



UI Setting	Description
Name	Shows the name of the object.
Type	Shows the type of the object.
Details	Shows the settings for the object. These settings will vary depending on the object's **Type**.
References	Shows the number of times this object is referenced in other settings or object groupings. You can select the **More (•••)** icon for an object to show where the object is referenced.

Create Object

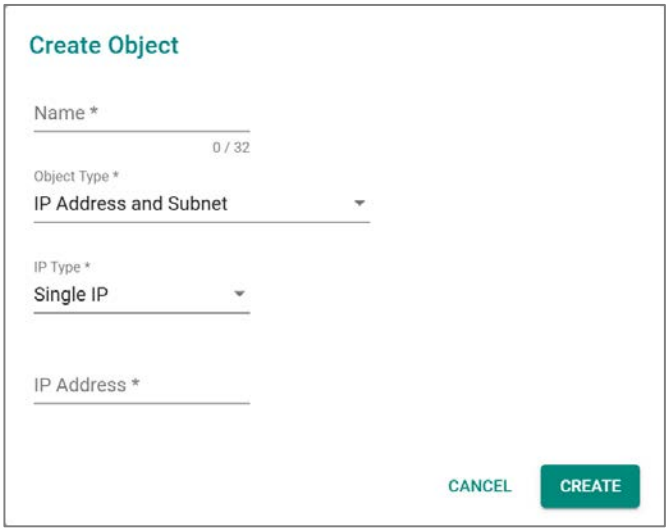
Menu Path: Object Management - Object Member

Clicking the **Add (⊞)** icon on the **Object Management - Object Member** page will open this dialog box. This dialog lets you create a new object. Available settings will vary depending on which **Object Type** is selected.

Click **CREATE** to save your changes and add the new object.

Create Object - IP Address and Subnet

If **IP Address and Subnet** is selected for the **Object Type**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Type	Select the type of IP address to use for the object.	Single IP / IP Range / Subnet	Single IP
IP Address **(If IP Type is Single)**	Specify the IP address to use for the object.	Valid IP Address	N/A
IP Address: Start **(If IP Type is IP Range)**	Specify the start of the IP range to use for the object.	Valid IP Address	N/A

UI Setting	Description	Valid Range	Default Value
IP Address: End **(If IP Type is IP Range)**	Specify the end of the IP range to use for the object.	Valid IP Address	N/A
Subnet **(If IP Type is Subnet)**	Specify the IP address of the subnet to use for the object.	Valid IP Address	N/A
Subnet Mask **(If IP Type is Subnet)**	Select the subnet mask to use for the object.	Drop-down list of subnet masks	N/A

Create Object - Network Service

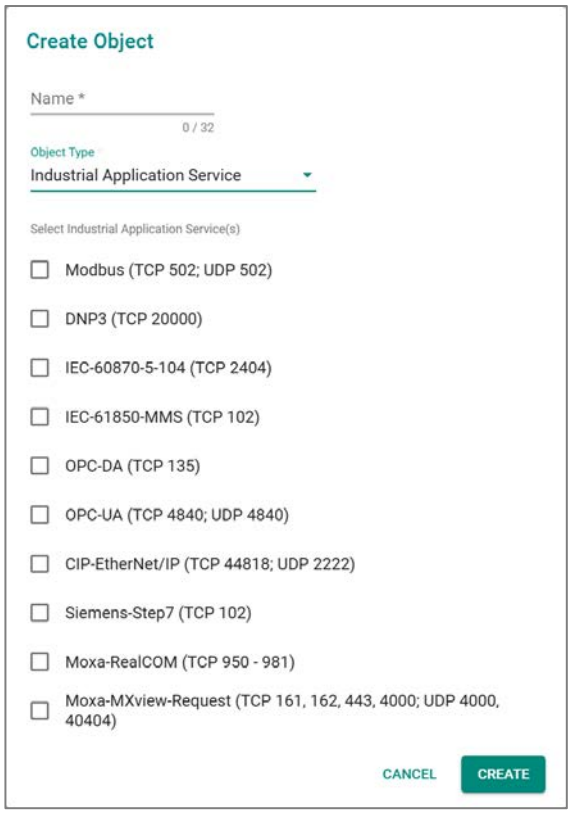
If **Network Service** is selected for the **Object Type**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A

UI Setting	Description	Valid Range	Default Value
Select Network Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options. • **Remote-Access**: This category includes protocols used for remote access to a device. • **Remote-Desktop**: This category includes protocols used by various remote desktop services. • **Email**: This category includes protocols used for sending and receiving emails. • **File-Transfer**: This category includes protocols used for different methods of file transfer. • **Web-Access**: This category includes protocols used by web browsers. • **Network-Service**: This category includes protocols used by various network services. • **Authentication**: This category includes protocols used by authentication services. • **VOIP-and-Streaming**: This category includes protocols used for VOIP calling and streaming video. • **SQL-Server**: This category includes protocols used for SQL servers. **Note** FTP data ports are dynamically identified and filtered based on real-time traffic.	• **Remote-Access**: WINS (TCP 1512; UDP 1512) / TELNET (TCP 23) / SSH (TCP 22) • **Remote-Desktop**: PC-Anywhere (TCP 5631; UDP 5632) / Chrome-Remote-Desktop (UDP 5222) / AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) / Teamviewer (TCP 5938) / RDP (TCP 3389) / VNC (TCP 5900) / X-WINDOW (TCP 6000 - 6063) • **Email**: IMAP (TCP 143) / IMAPS (TCP 993) / POP3 (TCP 110) / POP3S (TCP 995) / SMTP (TCP 25) / SMTPS (TCP 465) • **File-Transfer**: FTP (TCP 21) / FTPS (TCP 990) / Simple-FTP (TCP 115; UDP 115) / TFTP (UDP 69) / NFS (TCP 111, 2049; UDP 111, 2049) / SAMBA (TCP 139) / AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) / SMB (TCP 445) / Secure-FTP (TCP22) • **Web-Access**: HTTP (TCP 80) / HTTPS (TCP 443) • **Network-Service**: BGP (TCP 179) / DHCP (UDP 67) / DHCP6 (UDP 546) / DNS (TCP 53; UDP 53) / NTP (TCP 123; UDP 123) / ICMP-PING (ICMP Type Any Code Any) / OSPF (IP Protocol 89) / RIP (TCP 520) / SNMP (TCP 161 - 162; UDP 161 - 162) / SYSLOG-TCP (TCP 514) / SYSLOG-UDP (UDP 514) • **Authentication**: LDAP (TCP 389; UDP 389) / LDAPS (TCP 636; UDP 636) / RADIUS (UDP 1812 - 1813) / TACACS+ (TCP 49; UDP 49) • **VOIP-and-Streaming**: SIP (TCP 5060; UDP 5060) / RSTP (TCP 554, 7070, 8554; UDP 554) • **SQL-Server**: MS-SQL (TCP 1433 - 1434) / MYSQL (TCP 3306)	N/A

Create Object - Indust1rial Application Service

If **Industrial Application Service** is selected for the **Object Type**, these settings will appear.

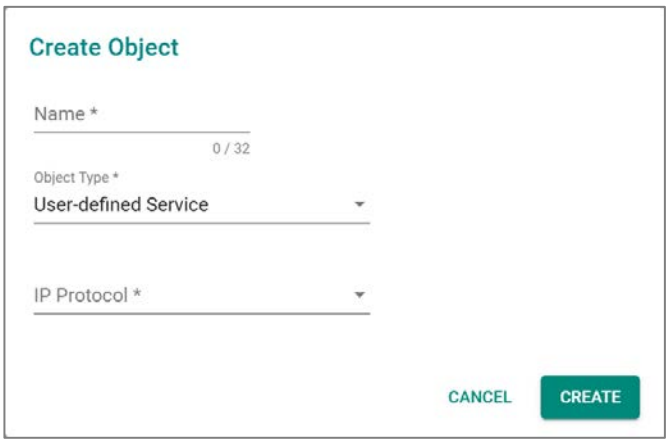


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A

UI Setting	Description	Valid Range	Default Value
Select Industrial Application Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Modbus (TCP 502; UDP 502) DNP3 (TCP 20000) IEC-60870-5-104 (TCP 2404) IEC-61850-MMS (TCP 102) OPC-DA (TCP 135) OPC-UA (TCP 4840; UDP 4840) CIP-EtherNet/IP (TCP 44818; UDP 2222) Siemens-Step7 (TCP 102) Moxa-RealCOM (TCP 950 - 981) Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)	N/A

Create Object - User-defined Service

If **User-defined Service** is selected for the **Object Type**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Protocol	Select the IP protocols to use for the object.	TCP / UDP / TCP and UDP / ICMP Custom IP Protocol	N/A
Service Port Type **(If IP Protocol is TCP, UDP, or TCP and UDP)**	Select how to define ports for the object. • **Any**: All ports will be included. • **Single TCP and UDP Port**: Specify a single port to include. • **TCP and UDP Port Range**: Specify a range of ports to include.	Any / Single TCP and UDP Port / TCP and UDP Port Range	
Port **(If Service Port Type is Single TCP and UDP Port)**	Specify a port to include.	1 to 65535	N/A
Port: Start **(If Service Port Type is TCP and UDP Port Range)**	Specify the start of the port range to use for the object.	1 to 65535	N/A
Port: End **(If Service Port Type is TCP and UDP Port Range)**	Specify the end of the port range to use for the object.	1 to 65535	N/A
ICMP Type (Decimal) **(If IP Protocol is ICMP)**	Specify the ICMP type in decimal form to use for the object. Leave this blank to allow all ICMP types to be included.	Blank, 0 to 255	N/A

UI Setting	Description	Valid Range	Default Value
ICMP Code (Decimal) **(If IP Protocol is ICMP)**	Specify the ICMP code in decimal form to use for the object. Leave this blank to allow all ICMP codes to be included.	Blank, 0 to 255	N/A
IP Protocol (Decimal) **(If IP Protocol is Custom IP Protocol)**	Specify the IP protocol in decimal form to use for the object.	0 to 255	N/A

Edit Object

Menu Path: Object Management - Object Member

Clicking the **Edit ( )** icon for an object on the **Object Management - Object Member** page will open this dialog box. This dialog lets you edit an existing object. Available settings will vary depending on which **Object Type** is selected.

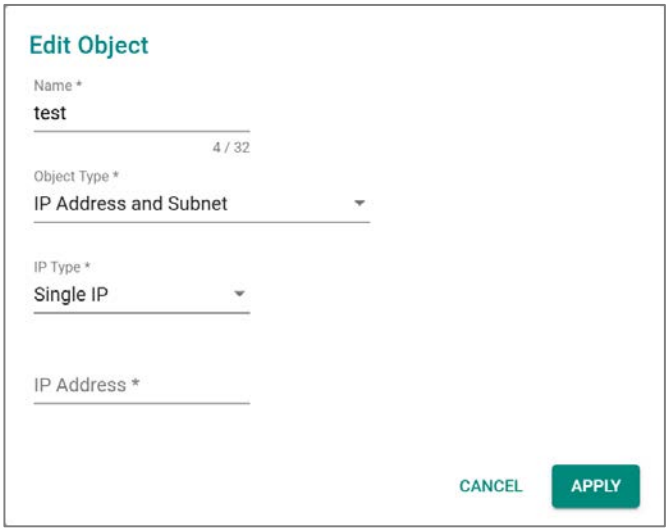
Click **APPLY** to save your changes.

Note

When editing an object, you cannot change its Object Type.

Edit Object - IP Address and Subnet

If **IP Address and Subnet** is selected for the **Object Type**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Type	Select the type of IP address to use for the object.	Single IP / IP Range / Subnet	Single IP
IP Address **(If IP Type is Single)**	Specify the IP address to use for the object.	Valid IP Address	N/A
IP Address: Start **(If IP Type is IP Range)**	Specify the start of the IP range to use for the object.	Valid IP Address	N/A

UI Setting	Description	Valid Range	Default Value
IP Address: End **(If IP Type is IP Range)**	Specify the end of the IP range to use for the object.	Valid IP Address	N/A
Subnet **(If IP Type is Subnet)**	Specify the IP address of the subnet to use for the object.	Valid IP Address	N/A
Subnet Mask **(If IP Type is Subnet)**	Select the subnet mask to use for the object.	Drop-down list of subnet masks	N/A

Edit Object - Network Service

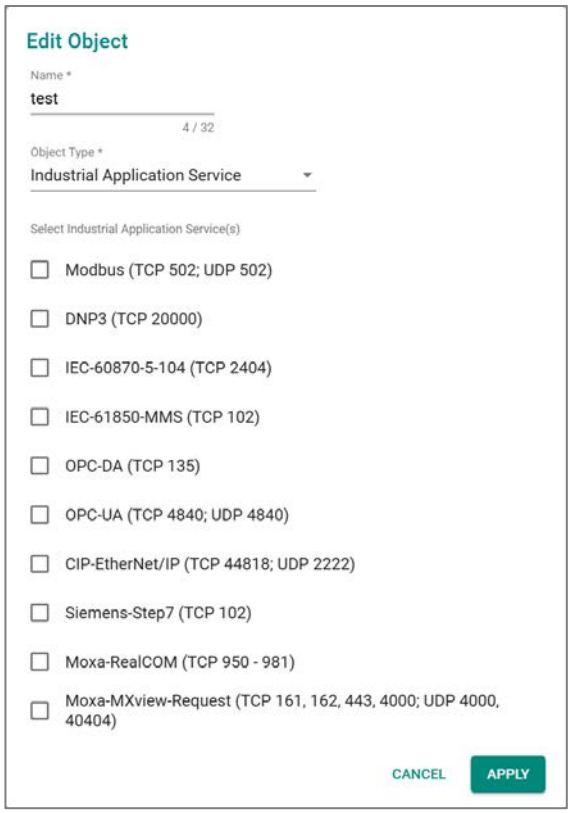
If **Network Service** is selected for the **Object Type**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A

UI Setting	Description	Valid Range	Default Value
Select Network Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options. • **Remote-Access**: This category includes protocols used for remote access to a device. • **Remote-Desktop**: This category includes protocols used by various remote desktop services. • **Email**: This category includes protocols used for sending and receiving emails. • **File-Transfer**: This category includes protocols used for different methods of file transfer. • **Web-Access**: This category includes protocols used by web browsers. • **Network-Service**: This category includes protocols used by various network services. • **Authentication**: This category includes protocols used by authentication services. • **VOIP-and-Streaming**: This category includes protocols used for VOIP calling and streaming video. • **SQL-Server**: This category includes protocols used for SQL servers. **Note** FTP data ports are dynamically identified and filtered based on real-time traffic.	• **Remote-Access**: WINS (TCP 1512; UDP 1512) / TELNET (TCP 23) / SSH (TCP 22) • **Remote-Desktop**: PC-Anywhere (TCP 5631; UDP 5632) / Chrome-Remote-Desktop (UDP 5222) / AnyDesk (TCP 6568, 7070; UDP 50001 - 50003) / Teamviewer (TCP 5938) / RDP (TCP 3389) / VNC (TCP 5900) / X-WINDOW (TCP 6000 - 6063) • **Email**: IMAP (TCP 143) / IMAPS (TCP 993) / POP3 (TCP 110) / POP3S (TCP 995) / SMTP (TCP 25) / SMTPS (TCP 465) • **File-Transfer**: FTP (TCP 21) / FTPS (TCP 990) / Simple-FTP (TCP 115; UDP 115) / TFTP (UDP 69) / NFS (TCP 111, 2049; UDP 111, 2049) / SAMBA (TCP 139) / AFS3 (TCP 7000 - 7009; UDP 7000 - 7009) / SMB (TCP 445) / Secure-FTP (TCP22) • **Web-Access**: HTTP (TCP 80) / HTTPS (TCP 443) • **Network-Service**: BGP (TCP 179) / DHCP (UDP 67) / DHCP6 (UDP 546) / DNS (TCP 53; UDP 53) / NTP (TCP 123; UDP 123) / ICMP-PING (ICMP Type Any Code Any) / OSPF (IP Protocol 89) / RIP (TCP 520) / SNMP (TCP 161 - 162; UDP 161 - 162) / SYSLOG-TCP (TCP 514) / SYSLOG-UDP (UDP 514) • **Authentication**: LDAP (TCP 389; UDP 389) / LDAPS (TCP 636; UDP 636) / RADIUS (UDP 1812 - 1813) / TACACS+ (TCP 49; UDP 49) • **VOIP-and-Streaming**: SIP (TCP 5060; UDP 5060) / RSTP (TCP 554, 7070, 8554; UDP 554) • **SQL-Server**: MS-SQL (TCP 1433 - 1434) / MYSQL (TCP 3306)	N/A

Edit Object - Industrial Application Service

If **Industrial Application Service** is selected for the **Object Type**, these settings will appear.

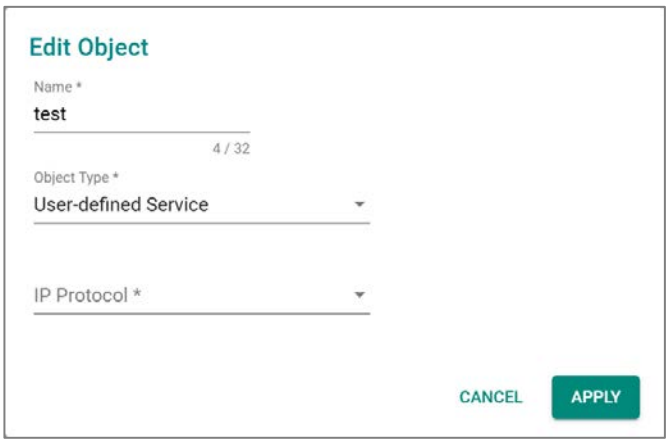


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A

UI Setting	Description	Valid Range	Default Value
Select Industrial Application Service(s)	Select a category of network services, or individual services to use for the object. You can select multiple options.	Modbus (TCP 502; UDP 502) DNP3 (TCP 20000) IEC-60870-5-104 (TCP 2404) IEC-61850-MMS (TCP 102) OPC-DA (TCP 135) OPC-UA (TCP 4840; UDP 4840) CIP-EtherNet/IP (TCP 44818; UDP 2222) Siemens-Step7 (TCP 102) Moxa-RealCOM (TCP 950 - 981) Moxa-MXview-Request (TCP 161, 162, 443, 4000; UDP 4000, 40404)	N/A

Edit Object - User-defined Service

If **User-defined Service** is selected for the **Object Type**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select a type for the object. • **IP Address and Subnet**: You can specify an IP address, a range of IP addresses, or a subnet. • **Network Service**: You can select from a list of protocol and port combinations used for common network services. • **Industrial Application Service**: You can select from a list of protocol and port combinations used for industrial communications and applications. • **User-defined Service**: You can specify your own protocol and port combination.	IP Address and Subnet / Network Service / Industrial Application Service / User-defined Service	N/A
IP Protocol	Select the IP protocols to use for the object.	TCP / UDP / TCP and UDP / ICMP Custom IP Protocol	N/A
Service Port Type **(If IP Protocol is TCP, UDP, or TCP and UDP)**	Select how to define ports for the object. • **Any**: All ports will be included. • **Single TCP and UDP Port**: Specify a single port to include. • **TCP and UDP Port Range**: Specify a range of ports to include.	Any / Single TCP and UDP Port / TCP and UDP Port Range	
Port **(If Service Port Type is Single TCP and UDP Port)**	Specify a port to include.	1 to 65535	N/A
Port: Start **(If Service Port Type is TCP and UDP Port Range)**	Specify the start of the port range to use for the object.	1 to 65535	N/A
Port: End **(If Service Port Type is TCP and UDP Port Range)**	Specify the end of the port range to use for the object.	1 to 65535	N/A
ICMP Type (Decimal) **(If IP Protocol is ICMP)**	Specify the ICMP type in decimal form to use for the object. Leave this blank to allow all ICMP types to be included.	Blank, 0 to 255	N/A

UI Setting	Description	Valid Range	Default Value
ICMP Code (Decimal) **(If IP Protocol is ICMP)**	Specify the ICMP code in decimal form to use for the object. Leave this blank to allow all ICMP codes to be included.	Blank, 0 to 255	N/A
IP Protocol (Decimal) **(If IP Protocol is Custom IP Protocol)**	Specify the IP protocol in decimal form to use for the object.	0 to 255	N/A

Delete Object

Menu Path: Object Management - Object Member

You can delete an object by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Note

You cannot delete an object if it is referenced in other settings or object groupings. You will need to remove the object from those settings or groupings before deleting the object.

You can select the More ( ) icon for an object to show where the object is referenced.

Object Member Grouping

Menu Path: Object Management - Object Member Grouping

This page lets you group different kinds of objects. These groups can be used when configuring other features so settings can apply to multiple objects.

Limitations

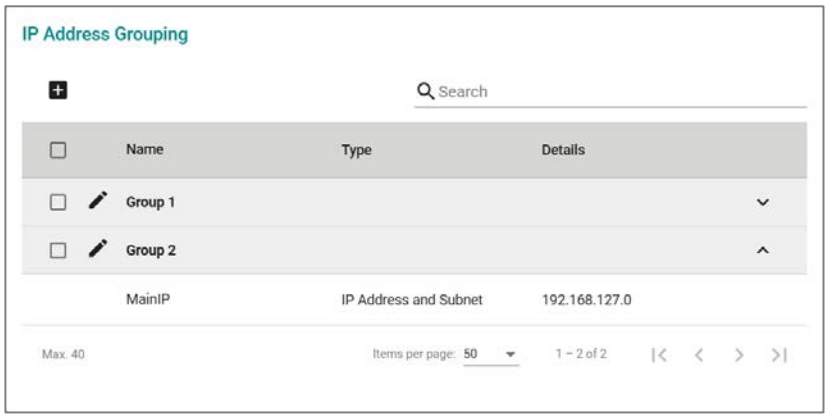
You can create up to 40 IP address groups.

Limitations

You can create up to 40 user-defined service groups.

IP Address Grouping

- Select the **Expand (⌄)** icon for a group to view the items in the group.
- Select the **Collapse (⌃)** icon for a group to hide the items in the group.



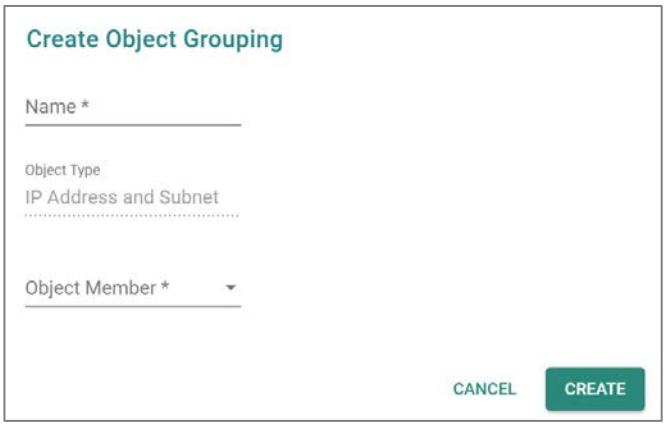
UI Setting	Description
Name	Shows the name of the IP address group.
Type	Shows the object type for items in the group. All items in these groups are **IP Address and Subnet** objects.
Details	Shows the IP addresses or address ranges for the object.

IP Address Grouping - Create Object Grouping

Menu Path: Object Management - Object Member Grouping

Clicking the **Add (⊞)** icon for the **IP Address Grouping** table on the **Object Management - Object Member Grouping** page will open this dialog box. This dialog lets you create a new IP address grouping.

Click **CREATE** to save your changes and add the new grouping.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object grouping.	1 to 32 characters	N/A
Object Type (View-only)	Shows the object type used by the grouping. This is fixed to **IP Address and Subnet**.	IP Address and Subnet	IP Address and Subnet
Object Member	Select objects to include in the grouping.	Drop-down list of IP Address and Subnet objects	N/A

IP Address Grouping - Edit Object Grouping

Menu Path: Object Management - Object Member Grouping

Clicking the **Edit ( )** icon for an entry in the **IP Address Grouping** table on the **Object Management - Object Member Grouping** page will open this dialog box. This dialog lets you edit an existing IP address grouping.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object grouping.	1 to 32 characters	N/A
Object Type **(View-only)**	Shows the object type used by the grouping. This is fixed to **IP Address and Subnet**.	IP Address and Subnet	IP Address and Subnet
Object Member	Select objects to include in the grouping.	Drop-down list of IP Address and Subnet objects	N/A

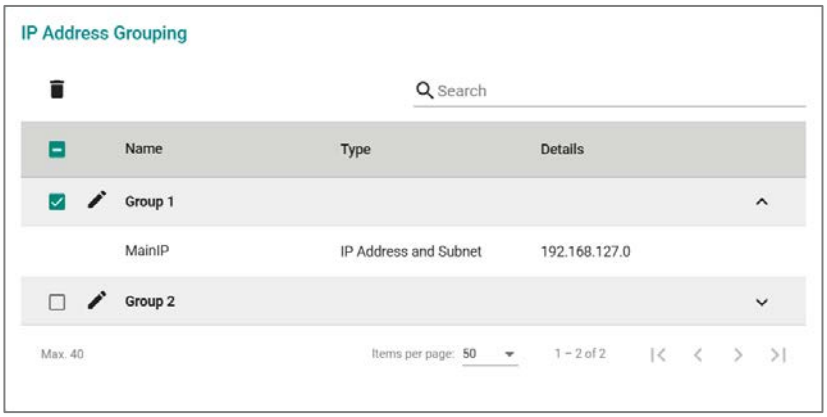
IP Address Grouping - Delete Object Grouping

Menu Path: Object Management - Object Member Grouping

You can delete an object by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

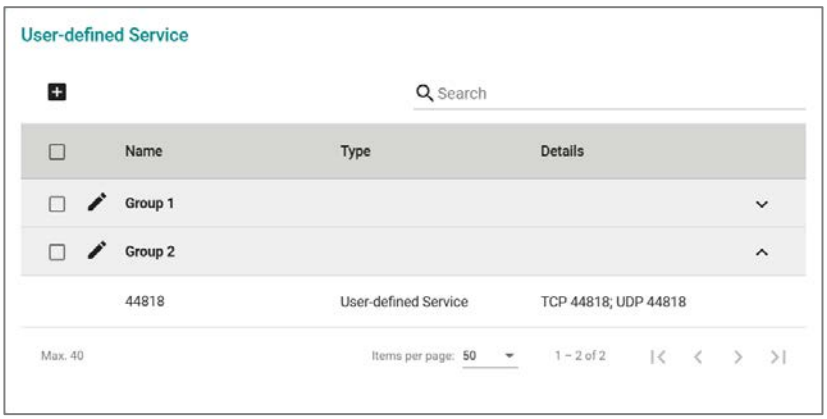
Note

Deleting an object grouping will only delete the grouping itself; it will not delete the objects the grouping references.



User-defined Service

- Select the **Expand (⌄)** icon for a group to view the items in the group.
- Select the **Collapse (⌃)** icon for a group to hide the items in the group.



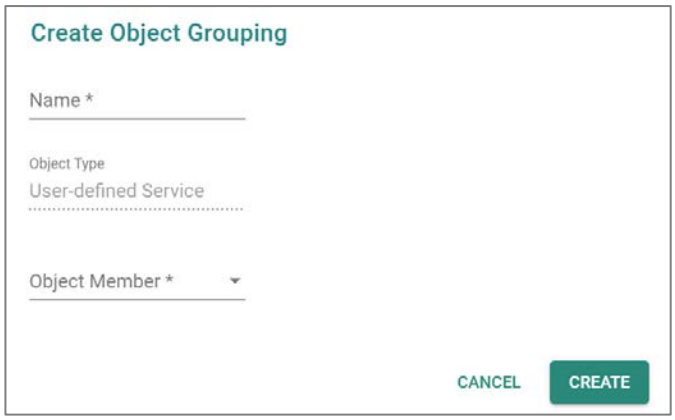
UI Setting	Description
Name	Shows the name of the user-defined service group.
Type	Shows the object type for items in the group. All items in these groups are **User-defined Service** objects.
Details	Shows the configured protocol and port for the object.

User-defined Service - Create Object Grouping

Menu Path: Object Management - Object Member Grouping

Clicking the **Add (⊕)** icon for the **User-defined Service** table on the **Object Management - Object Member Grouping** page will open this dialog box. This dialog lets you create a new user-defined service grouping.

Click **CREATE** to save your changes and add the new grouping.



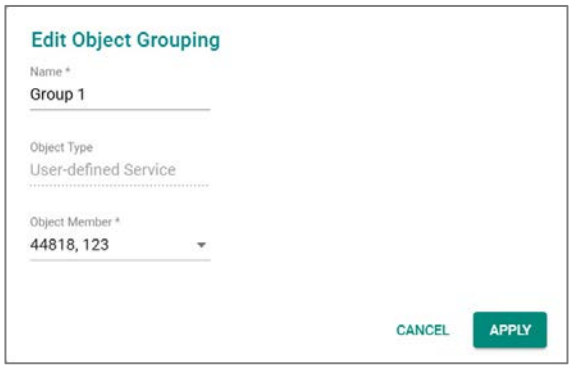
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object group.	1 to 32 characters	N/A
Object Type (View-only)	Shows the object type used by the grouping. This is fixed to **User-defined Service**.	User-defined Service	User-defined Service
Object Member	Select objects to include in the grouping.	Drop-down list of User-defined Service objects	N/A

User-defined Service - Edit Object Grouping

Menu Path: Object Management - Object Member Grouping

Clicking the **Edit (✎)** icon for an entry in the **User-defined Service** table on the **Object Management - Object Member Grouping** page will open this dialog box. This dialog lets you edit an existing user-defined service grouping.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object group.	1 to 32 characters	N/A
Object Type **(View-only)**	Shows the object type used by the grouping. This is fixed to **User-defined Service**.	User-defined Service	User-defined Service
Object Member	Select objects to include in the grouping.	Drop-down list of User-defined Service objects	N/A

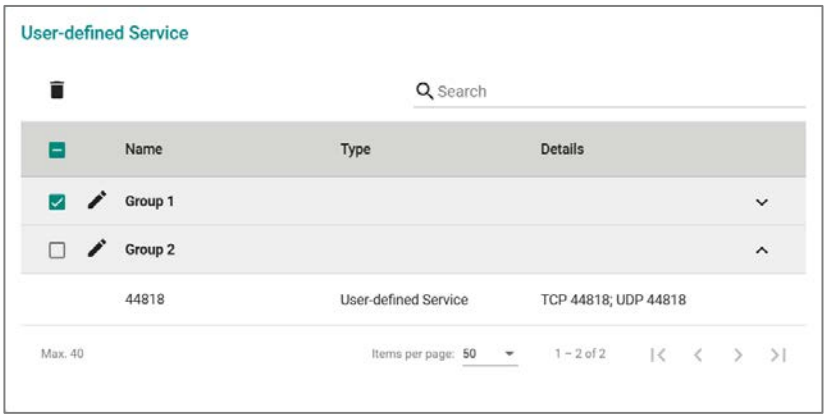
User-defined Service - Delete Object Grouping

Menu Path: Object Management - Object Member Grouping

You can delete a grouping by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Note

Deleting an object grouping will only delete the grouping itself; it will not delete the objects the grouping references.



Interface Grouping

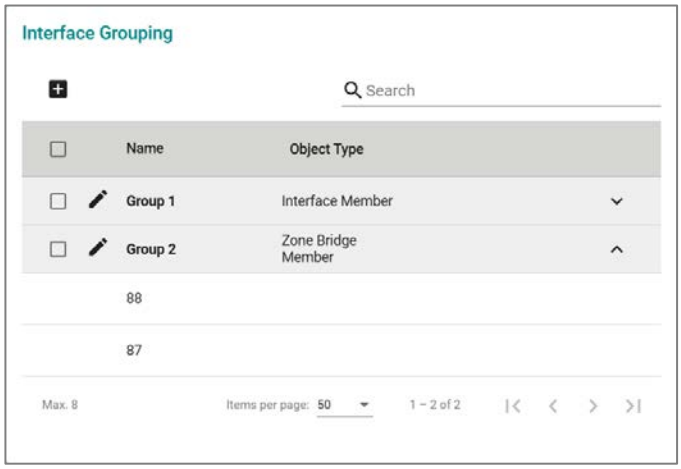
Menu Path: Object Management - Interface Grouping

This page lets you group interface objects. These groups can be used when configuring other features so settings can apply to multiple interfaces.

Limitations

You can create up to 8 interface groups.

- Select the **Expand (⌄)** icon for a group to view the items in the group.
- Select the **Collapse (⌃)** icon for a group to hide the items in the group.



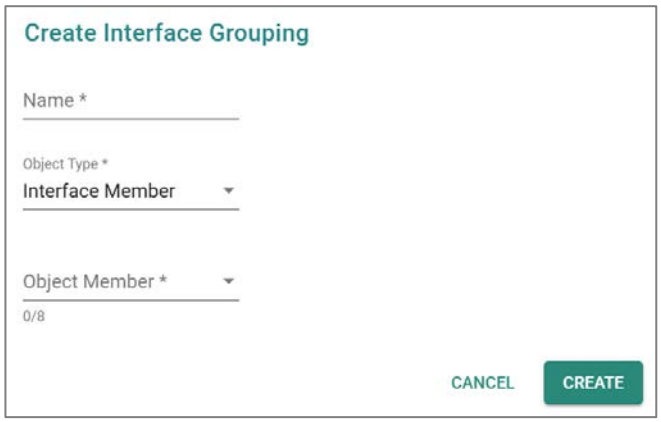
UI Setting	Description
Name	Shows the name of the interface group.
Object Type	Shows the object type for items in the group.

Create Interface Grouping

Menu Path: Object Management - Interface Grouping

Clicking the **Add (⊕)** icon on the **Object Management - Interface Grouping** page will open this dialog box. This dialog lets you create a new interface grouping.

Click **CREATE** to save your changes and add the new grouping.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface group.	1 to 32 characters	N/A
Object Type	Select an object type for the grouping. • **Interface Member**: Select physical interfaces to include in the interface group. • **Port Bridge Member**: Select bridge ports to include in the interface group. • **Zone Bridge Member**: Select zone bridge interfaces to include in the interface group.	Interface Member / Port Bridge Member / Zone Bridge Member	Interface Member

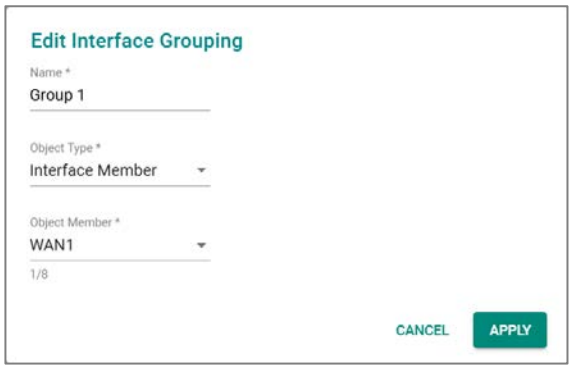
UI Setting	Description	Valid Range	Default Value
Object Member	Select one or more interfaces to include in the group. The available interfaces depend on the selected Object Type.	Drop-down list of interfaces, ports, or zones • If **Object Type** is **Interface Member:** Up to 8 objects can be selected • If **Object Type** is **Port Bridge Member:** The maximum number depends on the number of ports supported by the device. • If **Object Type** is **Zone Bridge Member:** Up to 32 objects can be selected	N/A

Edit Interface Grouping

Menu Path: Object Management - Interface Grouping

Clicking the **Edit ( )** icon for an entry on the **Object Management - Interface Grouping** page will open this dialog box. This dialog lets you edit an existing interface grouping.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the interface group.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Object Type	Select an object type for the grouping. • **Interface Member**: Select physical interfaces to include in the interface group. • **Port Bridge Member**: Select bridge ports to include in the interface group. • **Zone Bridge Member**: Select zone bridge interfaces to include in the interface group.	Interface Member / Port Bridge Member / Zone Bridge Member	Interface Member
Object Member	Select one or more interfaces to include in the group. The available interfaces depend on the selected Object Type.	Drop-down list of interfaces, ports, or zones • If **Object Type** is **Interface Member:** Up to 8 objects can be selected • If **Object Type** is **Port Bridge Member:** The maximum number depends on the number of ports supported by the device. • If **Object Type** is **Zone Bridge Member:** Up to 32 objects can be selected	N/A

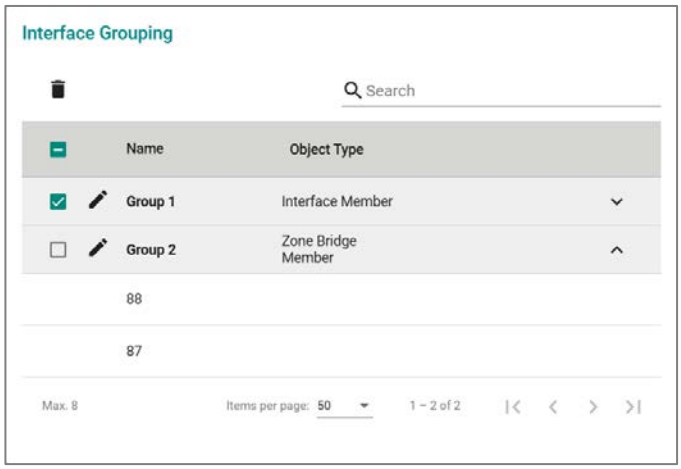
Delete Interface Grouping

Menu Path: Object Management - Interface Grouping

You can delete a grouping by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Note

Deleting an object grouping will only delete the grouping itself; it will not delete the objects the grouping references.


Interface Grouping
Search
Name
Object Type
Group 1
Interface Member
Group 2
Zone Bridge Member
88
87
Max. 8
Items per page: 50
1 – 2 of 2

Firewall

Menu Path: Firewall

The Firewall settings area lets you configure settings related to your device's firewall.

This settings area includes these sections:

- Layer 2 Policy
- Layer 3 Policy
- Layer 3-7 Policy
- Malformed Packets
- Session Control
- DoS Policy
- Soft Lockdown Mode
- Device Lockdown
- Advanced Protection

Network Configuration - User Privileges

Privileges to Firewall settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Layer 2 Policy	R/W	R/W	R
Layer 3 Policy	R/W	R/W	R
Layer 3-7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Soft Lockdown Mode	R/W	R/W	R

Settings	Admin	Supervisor	User
Device Lockdown	R/W	R/W	R
Advanced Protection			
Dashboard	R/W	R/W	-
Configuration	R/W	R/W	-
Protocol Filter Policy	R/W	R/W	-
ADP	R/W	R/W	-
IPS	R/W	R/W	-
Domain Protection	R/W	R/W	-

Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

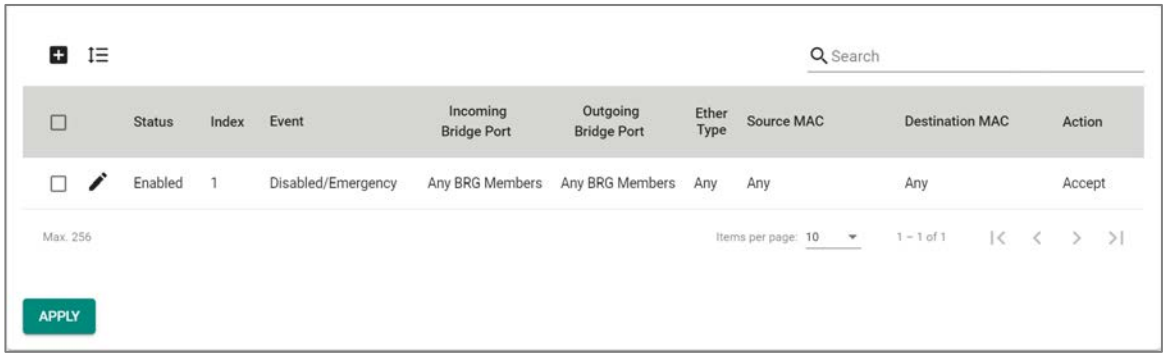
This page lets you configure advanced Layer 2 policies for your device's firewall. Layer 2 firewall policies can filter packets from bridge ports and have a higher priority than Layer 3 policies.

Note

Packets are checked by using the policy with the lowest index number first. If the packet matches the policy, the defined action will be taken and the remaining rules will not be run for the packet. If the packet does not match the policy, the next policy will be used.

Limitations

You can create up to 256 Layer 2 policies.



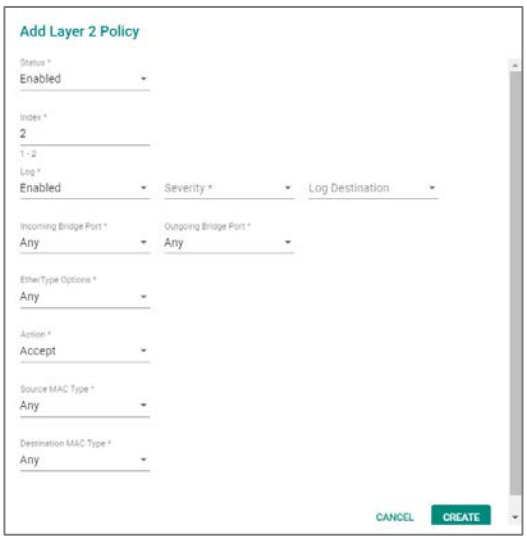
UI Setting	Description
Status	Shows whether the policy is enabled or disabled.
Index	Shows the index of the policy. The index determines the order for processing policies.
Event	Shows whether logging is enabled or disabled for the event and the severity assigned to the event.
Incoming Bridge Port	Shows the incoming bridge port for the policy.
Outgoing Bridge Port	Shows the outgoing bridge port for the policy.
Ether Type	Shows the EtherType that the policy applies to.
Source MAC	Shows the source MAC the policy applies to.
Destination MAC	Shows the destination MAC the policy applies to.
Action	Shows the action that will be taken for applicable traffic.

Add Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

Clicking the **Add (⊞)** icon on the **Firewall > Layer 2 Policy** page will open this dialog box. This dialog lets you create a new policy.

Click **CREATE** to save your changes and add the new policy.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Index	Specify the index number for the policy. The index determines the order for processing policies; rules are processed from lowest index to highest. **Note** If you enter an index number used by an existing rule, the existing rule and all rules with a higher index will have their index number automatically incremented by 1 to accomodate the new rule.	1 to last used index plus 1	Last used index plus 1
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send logs for this event. You can select multiple options. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • Trap: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Syslog: Event logs will be sent to a syslog server. Refer to Syslog for more information.	Local Storage / Trap / Syslog	N/A
Incoming Bridge Port	Select the incoming bridge port for this policy.	Any	Any
Outgoing Bridge Port	Select the outgoing bridge port for this policy.	Any	Any
EtherType Options	Select the Layer 2 EtherType protocol that this policy should apply to. You can select a type from the drop-down list, or you can select Manual to specify one manually. Refer to EtherTypes for Layer 2 for more information about common EtherTypes.	Any / Manual / IPv4 / X25 / ARP / Frame Relay ARP / G8BPQ AX.25 Ethernet Packet / DEC Assigned proto / DEC DNA Dump/Load / DEC DNA Remote Console / DEC DNA Routing / DEC LAT / DEC Diagnostics / DEC Customer use / DEC Systems Comms Arch / Trans Ether Bridging / Raw Frame Relay / Appletalk AARP / Appletalk / 802.1Q Virtual LAN tagged frame / Novell IPX / NetBEUI / IP version 6 / PPP / MultiProtocol over ATM / PPPoE discovery messages / PPPoE session messages / Frame-based ATM Transport over Ethernet / Loopback	Any
Manual **(if EtherType Options is anything other than Any)**	If **EtherType Options** is set to **Manual**, enter the EtherType value in hexadecimal this policy should apply to. If **EtherType Options** is set to a predefined **EtherType**, its value will be shown here and cannot be changed.	Valid EtherType hex code	N/A, EtherType value for the selected EtherType

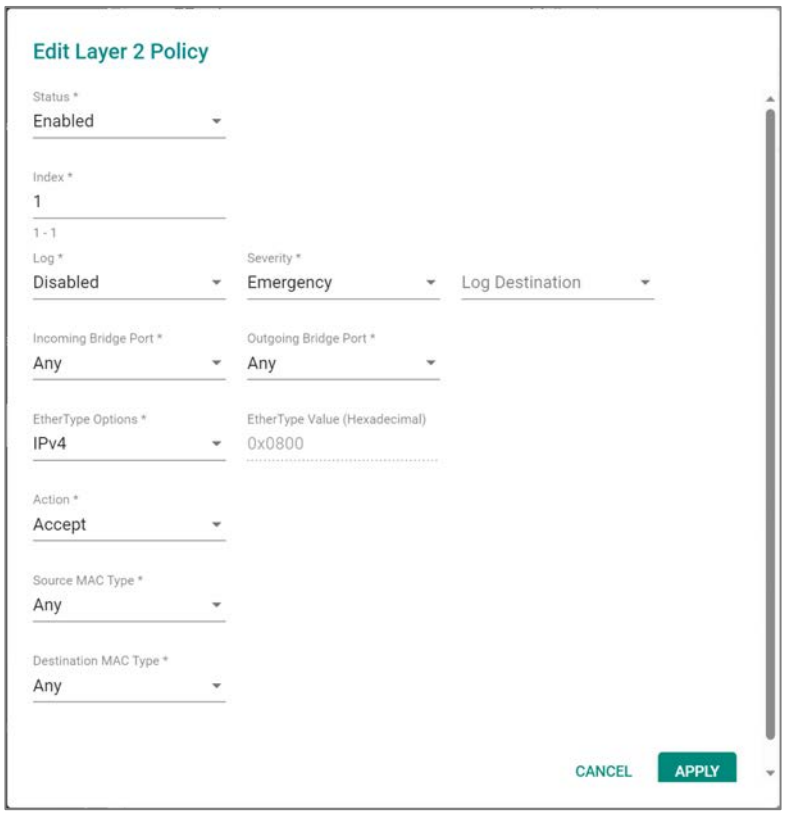
UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Source MAC Type	Select which source MAC addresses to check with this policy. • **Any**: The firewall will check packets coming from all source MAC addresses. • **Single**: The firewall will only check packets coming from a specified source MAC address.	Any / Single	Any
Destination MAC Type	Select which destination MAC addresses to check with this policy. • **Any**: The firewall will check packets going to all destination MAC addresses. • **Single**: The firewall will only check packets going to a specific destination MAC address.	Any / Single	Any

Edit Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

Clicking the **Edit ( )** icon for a policy on the **Firewall > Layer 2 Policy** page will open this dialog box. This dialog lets you modify an existing policy.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Index	Specify the index number for the policy. The index determines the order for processing policies; rules are processed from lowest index to highest. **Note** If you enter an index number used by an existing rule, the existing rule and all rules with a higher index will have their index number automatically incremented by 1 to accomodate the new rule.	1 to last used index plus 1	Last used index plus 1
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send logs for this event. You can select multiple options. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • Trap: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Syslog: Event logs will be sent to a syslog server. Refer to Syslog for more information.	Local Storage / Trap / Syslog	N/A
Incoming Bridge Port	Select the incoming bridge port for this policy.	Any	Any
Outgoing Bridge Port	Select the outgoing bridge port for this policy.	Any	Any
EtherType Options	Select the Layer 2 EtherType protocol that this policy should apply to. You can select a type from the drop-down list, or you can select Manual to specify one manually. Refer to EtherTypes for Layer 2 for more information about common EtherTypes.	Any / Manual / IPv4 / X25 / ARP / Frame Relay ARP / G8BPQ AX.25 Ethernet Packet / DEC Assigned proto / DEC DNA Dump/Load / DEC DNA Remote Console / DEC DNA Routing / DEC LAT / DEC Diagnostics / DEC Customer use / DEC Systems Comms Arch / Trans Ether Bridging / Raw Frame Relay / Appletalk AARP / Appletalk / 802.1Q Virtual LAN tagged frame / Novell IPX / NetBEUI / IP version 6 / PPP / MultiProtocol over ATM / PPPoE discovery messages / PPPoE session messages / Frame-based ATM Transport over Ethernet / Loopback	Any
Manual **(if EtherType Options is anything other than Any)**	If **EtherType Options** is set to **Manual**, enter the EtherType value in hexadecimal this policy should apply to. If **EtherType Options** is set to a predefined **EtherType**, its value will be shown here and cannot be changed.	Valid EtherType hex code	N/A, EtherType value for the selected EtherType

UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Source MAC Type	Select which source MAC addresses to check with this policy. • **Any**: The firewall will check packets coming from all source MAC addresses. • **Single**: The firewall will only check packets coming from a specified source MAC address.	Any / Single	Any
Destination MAC Type	Select which destination MAC addresses to check with this policy. • **Any**: The firewall will check packets going to all destination MAC addresses. • **Single**: The firewall will only check packets going to a specific destination MAC address.	Any / Single	Any

Delete Layer 2 Policy

Menu Path: Firewall > Layer 2 Policy

You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon. The index numbers for the remaining policies will be updated automatically.

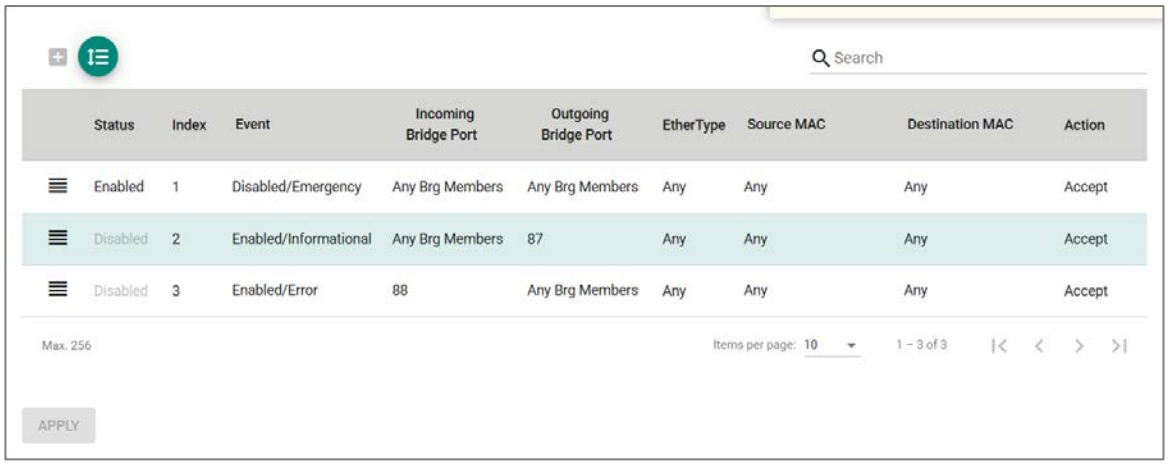
Reorder Layer 2 Policies

Menu Path: Firewall > Layer 2 Policy

You can reorder entries by clicking the **Reorder Priorities ( )** icon, moving entries into the order you want, then clicking the **Reorder Priorities ( )** icon again. Policies will

have their index numbers automatically updated to match the order you specify. Reordering policies affects the order used to process the policies; policies are processed from lowest index to highest.

Click **APPLY** to save your changes.



Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

This page lets you configure Layer 3 policies to secure and control network traffic. Click **APPLY** to save your changes.

> **Note**
> Availability of this feature may vary depending on your product model and version.

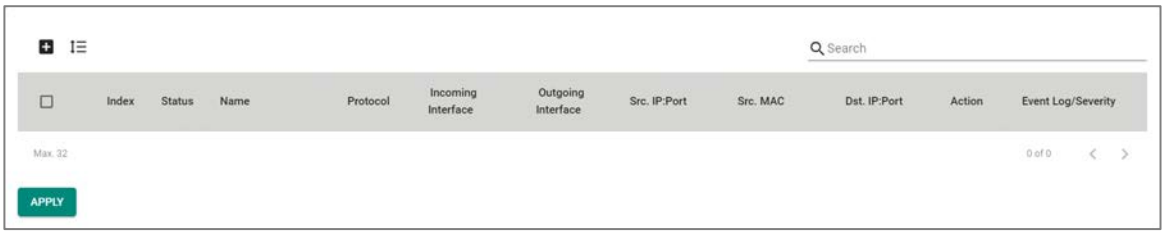
Limitations

You can create up to 32 Layer 3 policies.

Layer 3 Policy Settings

UI Setting	Description	Valid Range	Default Value
Firewall Event Log	Enable or disable logging of Layer 3 firewall events.	Enabled / Disabled	Disabled

Layer 3 Policy List



UI Setting	Description
Index	Shows the index of the policy. Policies with a lower index will be processed before policies with a higher index.
Status	Shows whether the policy is enabled.
Name	Shows the name of the policy.
Protocol	Shows the protocol used by the policy.
Incoming Interface	Shows the incoming interface used by the policy.
Outgoing Interface	Shows the outgoing interface used by the policy.

UI Setting	Description
Src. IP:Port	Shows the source IP address and port used by the policy.
Src. MAC	Shows the source MAC address and port used by the policy.
Dst. IP:Port	Shows the destination IP address and port used by the policy.
Action	Shows the action the firewall should take for traffic that matches this policy.
Event Log/Severity	Shows the event log destination and severity level for events from this policy.

Create Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

Clicking the **Add (⊞)** icon on the **Firewall > Layer 3 Policy** page will open this dialog box. This dialog lets you create a new Layer 3 policy.

Click **CREATE** to save your changes and add the new policy.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. Policies with a lower index will be processed before policies with a higher index.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 64 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send logs for this event. You can select multiple options. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
Automation Profile	Select a profile to use for this policy. Each profile will automatically set some of the source and destination settings based on the selected protocol.	All / TCP / UDP / ICMP / EtherNet/IP I/O (TCP) / EtherNet/IP I/O (UDP) / EtherNet/IP messaging (TCP) / EtherNet IP messaging (UDP) / FF Annunciation (TCP) / FF Annunciation (UDP) / FF Fieldbus Message Specification (TCP) / FF Fieldbus Message Specification (UDP) / FF System Management (TCP) / FF System Management (UDP) / FF LAN Redundancy Port (TCP) / FF LAN Redundancy Port (UDP) / LonWorks (TCP) / LonWorks (UDP) / LonWorks2 (TCP) / LonWorks2 (UDP) / Modbus TCP/IP (TCP) / Modbus TCP/IP (UDP) / PROFINET RT Unicast (TCP) / PROFINET RT Unicast (UDP) / PROFINET RT Multicast (TCP) / PROFINET RT Multicast (UDP) / PROFINET Context Manager (TCP) / PROFINET Context Manager (UDP) / IEC 60870-5-104 process control over IP (TCP) / IEC 60870-5-104 process control over IP (UDP) / IPsec NAT-Traversal (TCP) / IPsec NAT-Traversal (UDP) / DNP3 (TCP) / DNP3 (UDP) / FTP-data (TCP) / FTP-data (UDP) / FTP-control (TCP) / FTP-control (UDP) / SSH (TCP) / SSH (UDP) / Telnet (TCP) / Telnet (UDP) / HTTP (TCP) / HTTP (UDP) / IPsec (TCP) / IPsec (UDP) / L2TP (TCP) / L2TP (UDP) / PPTP (TCP) / PPTP (UDP) / RADIUS (TCP) / RADIUS (UDP) / RADIUS Accounting (TCP) / RADIUS Accounting (UDP) / EtherCAT (TCP) / EtherCAT (UDP)	All

UI Setting	Description	Valid Range	Default Value
Filter Mode	Select the filter mode to use for packet filtering. • **IP Address Filter**: The policy will filter packets based on IP addresses.	IP Address Filter	IP Address Filter
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	ACCEPT
Source IP Address	Select which source IP addresses this policy will apply to. • **All:** The firewall policy will check all source IP addresses in the packet. • **Single:** The firewall policy will check for a single specified source IP address in the packet. • **Range:** The firewall policy will check for any source IP addresses in the packet that are within a specified range.	All / Single / Range	All
Source IP: Start **(If Source IP Address is Single or Range)**	Specify the source IP address or the beginning of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0
Source IP: End **(If Source IP Address is Range)**	Specify the end of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Source Port **(If Automation Profile is TCP or UDP)**	Select which source ports this policy will apply to. • **All:** The firewall policy will check all source ports in the packet. • **Single:** The firewall policy will check for a single specified source port in the packet. • **Range:** The firewall policy will check for any source ports in the packet that are within a specified range.	If **Automation Profile** is **TCP** or **UDP**: All / Single / Range For all other **Automation Profile** options: All	All
Source Port: Start **(If Source Port is Single or Range)**	Specify the source port or the start of the source port range this policy will apply to.	1 to 65535	N/A
Source Port: End **(If Source Port is Range)**	Specify the end of the source port range this policy will apply to.	1 to 65535	N/A
Destination IP Address	Select which destination IP addresses this policy will apply to. • **All:** The firewall policy will check all destination IP addresses in the packet. • **Single:** The firewall policy will check for a single specified destination IP address in the packet. • **Range:** The firewall policy will check for any destination IP addresses in the packet that are within a specified range.	All / Single / Range	All

UI Setting	Description	Valid Range	Default Value
Destination IP: Start **(If Destination IP Address is Single or Range)**	Specify the destination IP address or the beginning of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Address is Range)**	Specify the end of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0
Destination Port	Select which destination ports this policy will apply to. • **All:** The firewall policy will check all destination ports in the packet. • **Single:** The firewall policy will check for a single specified destination port in the packet. • **Range:** The firewall policy will check for any destination ports in the packet that are within a specified range.	If **Automation Profile** is **All** or **ICMP:** All If **Automation Profile** is **TCP** or **UDP:** All / Single / Range For all other **Automation Profile** options: Single	If **Automation Profile** is **All, TCP, UDP,** or **ICMP:** All For all other **Automation Profile** options: Single
Destination Port: Start **(If Destination Port is Single or Range)**	Specify the destination port or the start of the destination port range this policy will apply to. Most of the **Automation Profile** options will fill in this setting with the default port used for that service. Refer to Ethernet Protocol Default Ports for more information.	1 to 65535	N/A
Destination Port: End **(If Destination Port is Range)**	Specify the end of the destination port range this policy will apply to.	1 to 65535	N/A

Edit Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

Clicking the **Edit ( )** icon for an entry on the **Firewall > Layer 3 Policy** page will open this dialog box. This dialog lets you edit an existing Layer 3 policy.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. Policies with a lower index will be processed before policies with a higher index.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 64 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send logs for this event. You can select multiple options. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any
Outgoing Interface	Select the outgoing interface for this policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Automation Profile	Select a profile to use for this policy. Each profile will automatically set some of the source and destination settings based on the selected protocol.	All / TCP / UDP / ICMP / EtherNet/IP I/O (TCP) / EtherNet/IP I/O (UDP) / EtherNet/IP messaging (TCP) / EtherNet IP messaging (UDP) / FF Annunciation (TCP) / FF Annunciation (UDP) / FF Fieldbus Message Specification (TCP) / FF Fieldbus Message Specification (UDP) / FF System Management (TCP) / FF System Management (UDP) / FF LAN Redundancy Port (TCP) / FF LAN Redundancy Port (UDP) / LonWorks (TCP) / LonWorks (UDP) / LonWorks2 (TCP) / LonWorks2 (UDP) / Modbus TCP/IP (TCP) / Modbus TCP/IP (UDP) / PROFINET RT Unicast (TCP) / PROFINET RT Unicast (UDP) / PROFINET RT Multicast (TCP) / PROFINET RT Multicast (UDP) / PROFINET Context Manager (TCP) / PROFINET Context Manager (UDP) / IEC 60870-5-104 process control over IP (TCP) / IEC 60870-5-104 process control over IP (UDP) / IPsec NAT-Traversal (TCP) / IPsec NAT-Traversal (UDP) / DNP3 (TCP) / DNP3 (UDP) / FTP-data (TCP) / FTP-data (UDP) / FTP-control (TCP) / FTP-control (UDP) / SSH (TCP) / SSH (UDP) / Telnet (TCP) / Telnet (UDP) / HTTP (TCP) / HTTP (UDP) / IPsec (TCP) / IPsec (UDP) / L2TP (TCP) / L2TP (UDP) / PPTP (TCP) / PPTP (UDP) / RADIUS (TCP) / RADIUS (UDP) / RADIUS Accounting (TCP) / RADIUS Accounting (UDP) / EtherCAT (TCP) / EtherCAT (UDP)	All
Filter Mode	Select the filter mode to use for packet filtering. • **IP Address Filter**: The policy will filter packets based on IP addresses.	IP Address Filter	IP Address Filter
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	ACCEPT

UI Setting	Description	Valid Range	Default Value
Source IP Address	Select which source IP addresses this policy will apply to. • **All:** The firewall policy will check all source IP addresses in the packet. • **Single:** The firewall policy will check for a single specified source IP address in the packet. • **Range:** The firewall policy will check for any source IP addresses in the packet that are within a specified range.	All / Single / Range	All
Source IP: Start **(If Source IP Address is Single or Range)**	Specify the source IP address or the beginning of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0
Source IP: End **(If Source IP Address is Range)**	Specify the end of the source IP address range this policy will apply to.	Valid IP address	0.0.0.0
Source Port **(If Automation Profile is TCP or UDP)**	Select which source ports this policy will apply to. • **All:** The firewall policy will check all source ports in the packet. • **Single:** The firewall policy will check for a single specified source port in the packet. • **Range:** The firewall policy will check for any source ports in the packet that are within a specified range.	If **Automation Profile** is **TCP** or **UDP**: All / Single / Range For all other **Automation Profile** options: All	All

UI Setting	Description	Valid Range	Default Value
Source Port: Start **(If Source Port is Single or Range)**	Specify the source port or the start of the source port range this policy will apply to.	1 to 65535	N/A
Source Port: End **(If Source Port is Range)**	Specify the end of the source port range this policy will apply to.	1 to 65535	N/A
Destination IP Address	Select which destination IP addresses this policy will apply to. • **All:** The firewall policy will check all destination IP addresses in the packet. • **Single:** The firewall policy will check for a single specified destination IP address in the packet. • **Range:** The firewall policy will check for any destination IP addresses in the packet that are within a specified range.	All / Single / Range	All
Destination IP: Start **(If Destination IP Address is Single or Range)**	Specify the destination IP address or the beginning of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0
Destination IP: End **(If Destination IP Address is Range)**	Specify the end of the destination IP address range this policy will apply to.	Valid IP address	0.0.0.0

UI Setting	Description	Valid Range	Default Value
Destination Port	Select which destination ports this policy will apply to. • **All:** The firewall policy will check all destination ports in the packet. • **Single:** The firewall policy will check for a single specified destination port in the packet. • **Range:** The firewall policy will check for any destination ports in the packet that are within a specified range.	If **Automation Profile** is **All** or **ICMP:** All If **Automation Profile** is **TCP** or **UDP:** All / Single / Range For all other **Automation Profile** options: Single	If **Automation Profile** is **All, TCP, UDP,** or **ICMP:** All For all other **Automation Profile** options: Single
Destination Port: Start **(If Destination Port is Single or Range)**	Specify the destination port or the start of the destination port range this policy will apply to. Most of the **Automation Profile** options will fill in this setting with the default port used for that service. Refer to Ethernet Protocol Default Ports for more information.	1 to 65535	N/A
Destination Port: End **(If Destination Port is Range)**	Specify the end of the destination port range this policy will apply to.	1 to 65535	N/A

Delete Layer 3 Policy

Menu Path: Firewall > Layer 3 Policy

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

This page lets you configure Layer 3-7 policies to secure and control network traffic.

Click **APPLY** to save your changes.

Note

Packets are checked by using the policy with the lowest index number first. If the packet matches the policy, the defined action will be taken and the remaining rules will not be run for the packet. If the packet does not match the policy, the next policy will be used.

Limitations

- EDF, EDR, and OnCell Series: You can create up to 1025 Layer 3-7 policies.
- TN Series: You can create up to 2049 Layer 3-7 policies.

Layer 3-7 Policy Settings

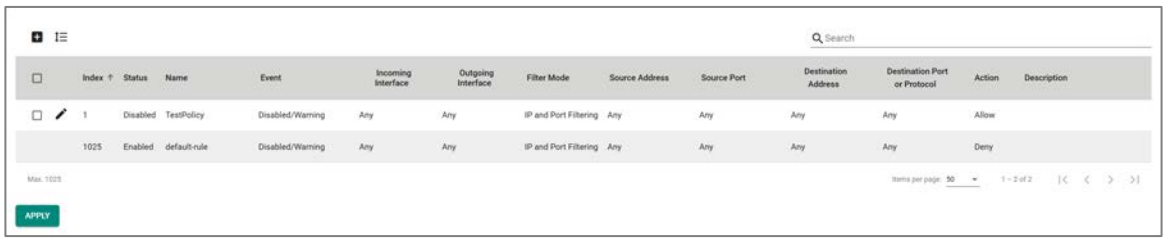
Global Policy Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Layer 3-7 policy settings.	Enabled / Disabled	Disabled
Default Action	Select what the default action should be for traffic that doesn't match any of the configured firewall rules. • **Allow All**: Allow all network traffic that does not match any rule. • **Deny All**: Block all network traffic that does not match any rule.	Allow All / Deny All	Deny All

Global Policy Event Settings

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable global policy event logging. This will allow event logging for actions taken due to the global policy.	Enabled / Disabled	Enabled
Default Action Log	Enable or disable default action log.	Enabled / Disabled	Disabled
Default Action Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Default Action Log Destination	Select the default action log destination.	Syslog / Trap / Local Storage	N/A

Layer 3-7 Policy List



UI Setting	Description
Index	Shows the index of the policy. The index determines the order for processing policies.
Status	Shows whether the policy is enabled or disabled.
Name	Shows the name of the policy.
Event	Shows whether logging is enabled or disabled for the event and the severity assigned to the event.
Incoming Interface	Shows the incoming interface for the policy.
Outgoing Interface	Shows the outgoing interface for the policy.
Filter Mode	Shows the filter mode used for the policy.

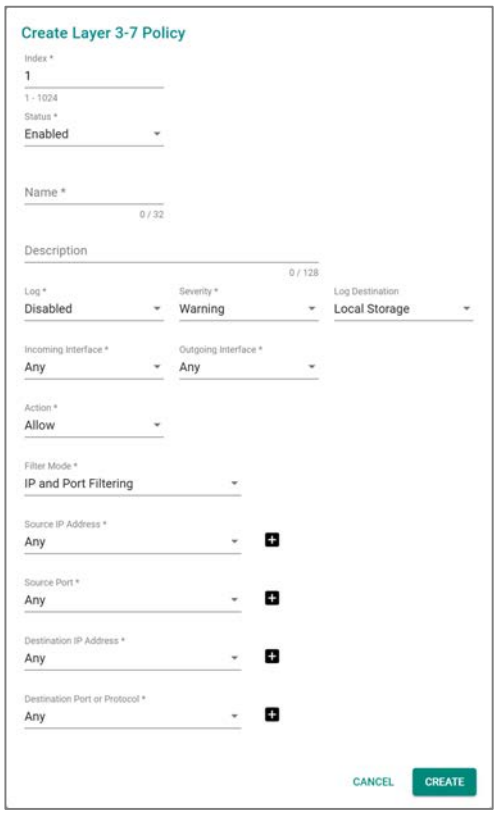
UI Setting	Description
Source Address	Shows the source IP addresses the policy applies to.
Source Port	Shows the source ports the policy applies to.
Destination Address	Shows the destination IP addresses the policy applies to.
Destination Port or Protocol	Shows the destination ports or protocols the policy applies to.
Action	Shows the action that will be taken for applicable traffic.
Description	Shows the description of the policy.

Create Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

Clicking the **Add (⊞)** icon on the **Firewall > Layer 3-7 Policy** page will open this dialog box. This dialog lets you create a new policy.

Click **CREATE** to save your changes and add the new policy.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Description	Specify a description for the policy.	0 to 128 characters	N/A
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** The incoming and outgoing interfaces can not be the same. This restriction does not apply to bridge interfaces.	Any / Drop-down list of interfaces	Any
Outgoing Interface	Select the outgoing interface for this policy. **Note** The incoming and outgoing interfaces can not be the same. This restriction does not apply to bridge interfaces.	Any / Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Filter Mode	Select the filter mode to use for packet filtering. • **IP and Port Filtering**: The policy will filter based on IP address and port. • **IP and Source MAC Binding**: The policy will filter based on IP address and will also check the source MAC address. • **Source MAC Filtering**: The policy will filter based on source MAC address.	IP and Port Filtering / IP and Source MAC Binding / Source MAC Filtering	IP and Port Filtering
Source IP Address **(If Filter Mode is IP and Port Filtering or IP and Source MAC Binding)**	Select the source IP addresses this policy will apply to. Select **Any** to check traffic from all source IP addresses, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any
Source Port **(If Filter Mode is IP and Port Filtering)**	Select the source ports this policy will apply to. Select **Any** to check traffic from all source ports, or select a pre-defined object. You can also click the Add ( ) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	Any
Source MAC Address **(If Filter Mode is IP and Source MAC Binding or Source MAC Filtering)**	Specify the source MAC address this policy will apply to.	Valid MAC address	N/A
Destination IP Address **(If Filter Mode is IP and Port Filtering)**	Select the destination IP addresses this policy will apply to. Select **Any** to check all traffic going to any destination IP address, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any

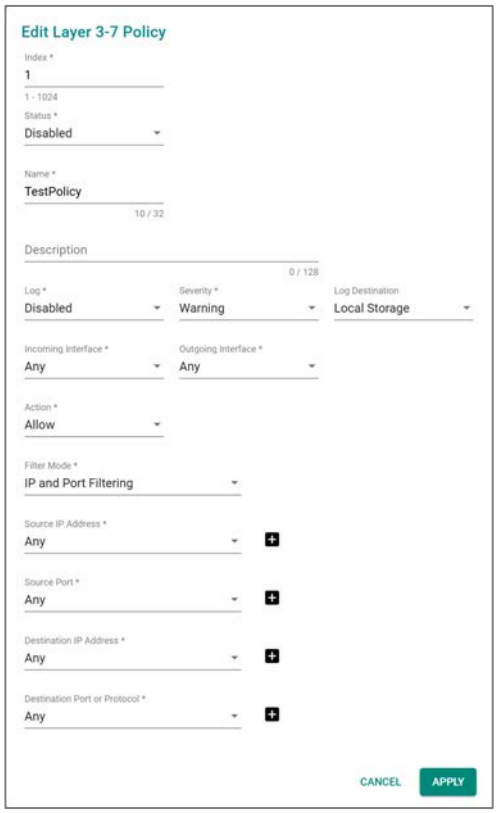
UI Setting	Description	Valid Range	Default Value
Destination Port or Protocol **(If Filter Mode is IP and Port Filtering)**	Select the destination ports or protocl this policy will apply to. Select **Any** to check all traffic going to any destination port or protocol, or select a pre-defined service or object. You can also click the Add ( ) icon to create a new Network Service, Industrial Application Service, or User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of Network Service, Industrial Application Service, and port-based User-defined Service objects	Any

Edit Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

Clicking the **Edit ( )** icon for a policy on the **Firewall > Layer 3-7 Policy** page will open this dialog box. This dialog lets you modify an existing policy.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 1024	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Description	Specify a description for the policy.	0 to 128 characters	N/A
Log	Enable or disable firewall event logging for this policy.	Enabled / Disabled	Enabled
Severity	Select the severity level to assign events for this policy. Refer to Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A
Incoming Interface	Select the incoming interface for this policy. **Note** The incoming and outgoing interfaces can not be the same. This restriction does not apply to bridge interfaces.	Any / Drop-down list of interfaces	Any
Outgoing Interface	Select the outgoing interface for this policy. **Note** The incoming and outgoing interfaces can not be the same. This restriction does not apply to bridge interfaces.	Any / Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Action	Select the action the firewall should take for traffic that matches this policy. • **Accept**: The firewall will accept packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Accept / Drop	Accept
Filter Mode	Select the filter mode to use for packet filtering. • **IP and Port Filtering**: The policy will filter based on IP address and port. • **IP and Source MAC Binding**: The policy will filter based on IP address and will also check the source MAC address. • **Source MAC Filtering**: The policy will filter based on source MAC address.	IP and Port Filtering / IP and Source MAC Binding / Source MAC Filtering	IP and Port Filtering
Source IP Address **(If Filter Mode is IP and Port Filtering or IP and Source MAC Binding)**	Select the source IP addresses this policy will apply to. Select **Any** to check traffic from all source IP addresses, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any
Source Port **(If Filter Mode is IP and Port Filtering)**	Select the source ports this policy will apply to. Select **Any** to check traffic from all source ports, or select a pre-defined object. You can also click the Add ( ) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	Any
Source MAC Address **(If Filter Mode is IP and Source MAC Binding or Source MAC Filtering)**	Specify the source MAC address this policy will apply to.	Valid MAC address	N/A
Destination IP Address **(If Filter Mode is IP and Port Filtering)**	Select the destination IP addresses this policy will apply to. Select **Any** to check all traffic going to any destination IP address, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	Any

UI Setting	Description	Valid Range	Default Value
Destination Port or Protocol **(If Filter Mode is IP and Port Filtering)**	Select the destination ports or protocl this policy will apply to. Select **Any** to check all traffic going to any destination port or protocol, or select a pre-defined service or object. You can also click the Add ( ) icon to create a new Network Service, Industrial Application Service, or User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of Network Service, Industrial Application Service, and port-based User-defined Service objects	Any

Delete Layer 3-7 Policy

Menu Path: Firewall > Layer 3-7 Policy

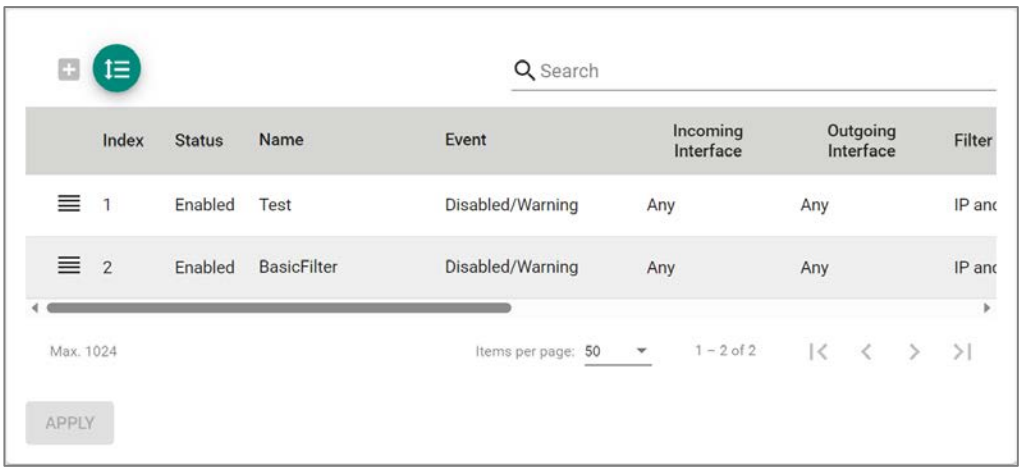
You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon. The index numbers for the remaining policies will be updated automatically.

Reorder Layer 3-7 Policies

Menu Path: Firewall > Layer 3-7 Policy

You can reorder entries by clicking the **Reorder Priorities ( )** icon, moving entries into the order you want, then clicking the **Reorder Priorities ( )** icon again. Policies will have their index numbers automatically updated to match the order you specify. Reordering policies affects the order used to process the policies; policies are processed from lowest index to highest.

Click **APPLY** to save your changes.



Malformed Packets

Menu Path: Firewall > Malformed Packets

This page lets you configure the Malformed Packets feature, which enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable recording an event when malformed packets are dropped.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • Syslog: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A

Session Control

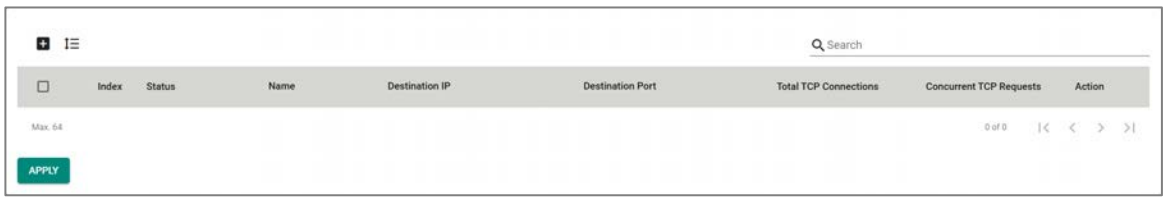
Menu Path: Firewall > Session Control

This page lets you configure session control policies to help protect backend hosts or services and avoid system abnormalities.

Click **APPLY** to save your changes.

> **Note**
>
> If a TCP connection is successfully established, but no data is sent, the connection will be released after 8 seconds. If the interval between the last data transmission for the connection exceeds 300 seconds, the connection will also be released.

> **Limitations**
>
> You can create up to 64 session control policies.



UI Setting	Description
Index	Shows the index of the policy. The index determines the order for processing policies.
Status	Shows whether the policy is enabled or disabled.
Name	Shows the name of the policy.
Destination IP	Shows the destination IP addresses the policy applies to.
Destination Port	Shows the destination ports the policy applies to.
Total TCP Connections	Shows the total number of TCP connections this policy allows.
Concurrent TCP Connections	Shows the number of concurrent TCP connections this policy allows.

UI Setting	Description
Action	Shows the action that will be taken for applicable traffic.

Create Session Control Policy

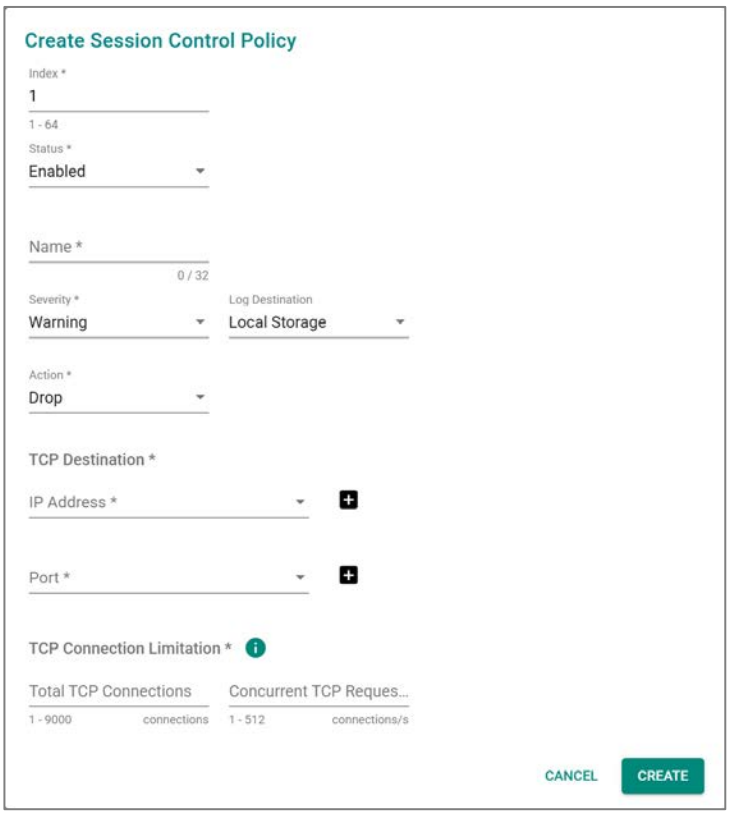
Menu Path: Firewall > Session Control

Clicking the **Add (⊕)** icon on the **Firewall > Session Control** page will open this dialog box. This dialog lets you create a new policy.

Click **CREATE** to save your changes and add the new policy.

> **Note**
> IP Address and Port cannot both be set to Any.

> **Note**
> At least one TCP Connection Limitation must be defined.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A
Action	Select the action the firewall should take for traffic that matches this policy. • **Monitor**: The firewall will monitor packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Monitor / Drop	Drop
IP Address	Select the IP addresses this policy will apply to. Select **Any** to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	N/A
Port	Select the ports this policy will apply to. Select **Any** to check traffic from all ports, or select a pre-defined object. You can also click the Add ( ) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	N/A
Total TCP Connections	Specify the total allowed number of TCP connections.	1 to 9000	N/A
Concurrent TCP Requests	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

Edit Session Control Policy

Menu Path: Firewall > Session Control

Clicking the **Edit ( )** icon for an policy on the **Firewall > Session Control** page will open this dialog box. This dialog lets you modify an existing policy.

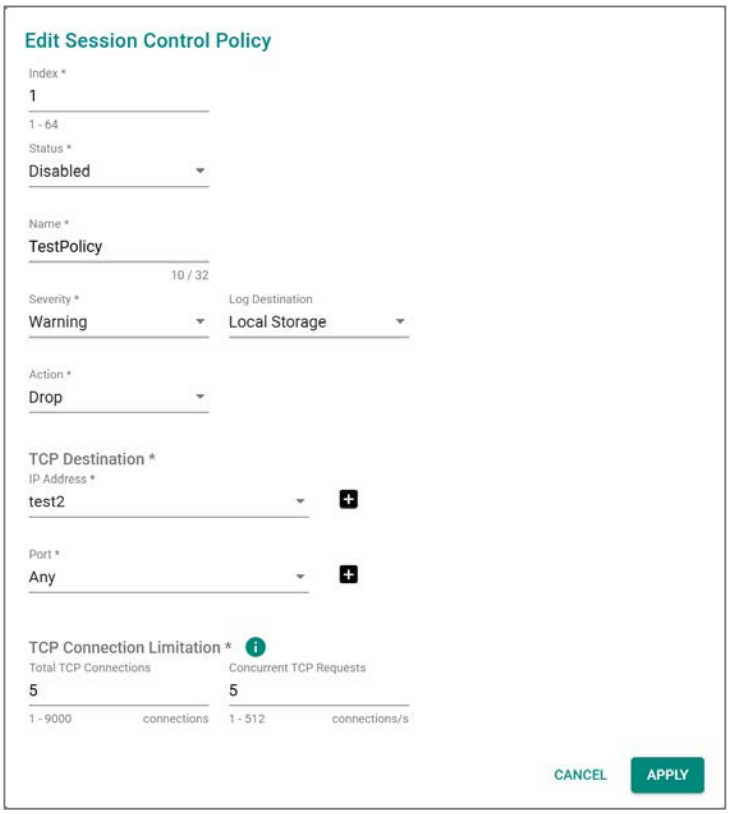
Click **APPLY** to save your changes.

Note

IP Address and Port cannot both be set to Any.

Note

At least one TCP Connection Limitation must be defined.



UI Setting	Description	Valid Range	Default Value
Index	Specify the index number for the policy. The index determines the order for processing policies.	1 to 64	Last used index plus 1
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	N/A
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A
Action	Select the action the firewall should take for traffic that matches this policy. • **Monitor**: The firewall will monitor packets that match the policy. • **Drop**: The firewall will drop packets that match the policy.	Monitor / Drop	Drop
IP Address	Select the IP addresses this policy will apply to. Select **Any** to check traffic from all IP addresses, or select a pre-defined object. You can also click the Add ( ) icon to create a new IP Address and Subnet object. Refer to Create Object for more information.	Any / Drop-down list of IP Address and Subnet objects	N/A
Port	Select the ports this policy will apply to. Select **Any** to check traffic from all ports, or select a pre-defined object. You can also click the Add ( ) icon to create a new User-defined Service object. Refer to Create Object for more information.	Any / Drop-down list of port-based User-defined Service objects	N/A
Total TCP Connections	Specify the total allowed number of TCP connections.	1 to 9000	N/A
Concurrent TCP Requests	Specify the total allowed number of concurrent TCP requests.	1 to 512	N/A

Delete Session Control Policy

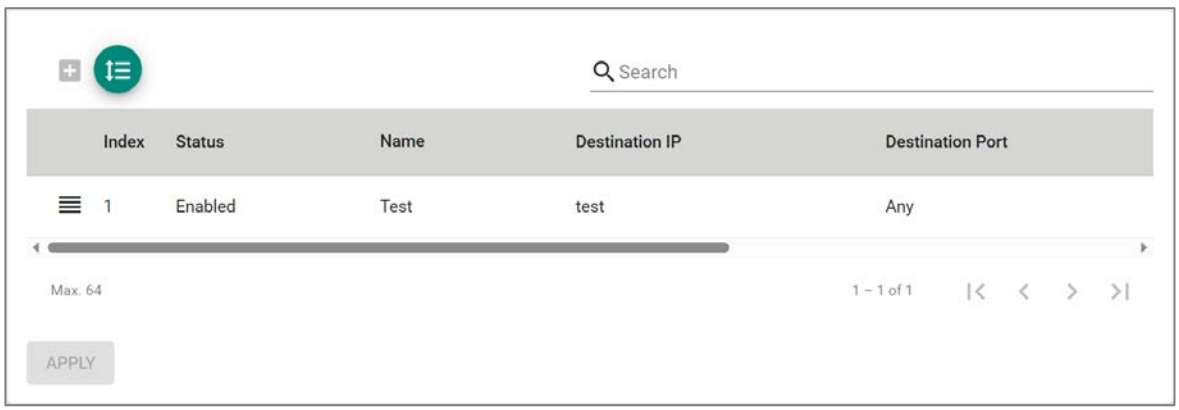
Menu Path: Firewall > Session Control

You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon. The index numbers for the remaining policies will be updated automatically.

Reorder Session Control Policies

Menu Path: Firewall > Session Control

You can reorder policies by clicking the **Reorder Priorities ( )** icon, moving the entries into the order you want, then clicking the **Reorder Priorities ( )** icon again. Reordering policies affects the order used to process the policies. Policies will have their index numbers automatically updated to match the order you specify. Reordering policies affects the order used to process the policies; policies are processed from lowest index to highest.



DoS Policy

Menu Path: Firewall > DoS Policy

This page lets you configure Denial of Service (DoS) protection features. You can configure different DoS functions for detecting abnormal packet formats or traffic flows, allowing your device to drop packets when it detects an abnormal packet format or identifies unusual traffic conditions.

This page includes these tabs:

- Global
- Device Policy

DoS Policy - Global

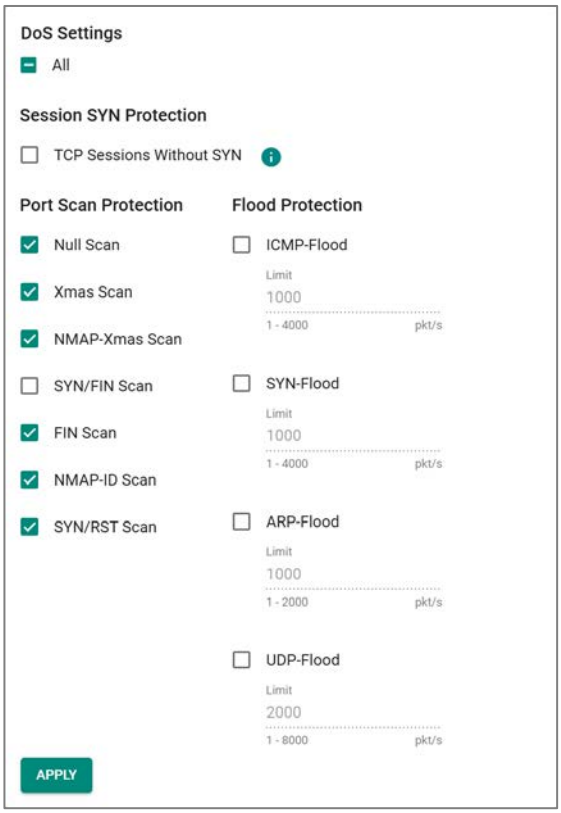
Menu Path: Firewall > DoS Policy - Global

This page lets you configure the device's global DoS policies.

DoS Log Settings

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable DoS event logs.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign to DoS-related events. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A

DoS Settings



UI Setting	Description	Valid Range	Default Value
DoS Settings	Toggle all DoS protection methods on or off.	All	N/A
Session SYN Protection	Enable or disable session SYN protection methods. • **TCP Sessions Without SYN**: When enabled, this function will verify the SYN state within the TCP flag when establishing TCP sessions. If the SYN tag is missing in the initial packet, the system will drop the packet and block the connection. Running TCP sessions will be re-established to perform the check. **⚠ Warning** When NAT is enabled for asymmetric network architectures, it is strongly advised to keep TC Sessions Without SYN disabled to avoid unexpected disconnections.	TCP Sessions Without SYN	Checked for all methods

UI Setting	Description	Valid Range	Default Value
Port Scan Protection	Enable or disable port-scan protection methods.	Null Scan / Xmas Scan / NMAP-Xmas Scan / SYN/FIN Scan / FIN Scan / NMAP-ID Scan / SYN/RST Scan	Enabled for all methods
Flood Protection	Enable or disable flood protection methods. When enabling a protection method, specify the limit in packets/second that will trigger the corresponding flood protection. **Note** If Accept All LAN Port Connections is enabled in Trusted Access, Flood Protection will be disabled. Refer to Trusted Access for more information. **Note** For Flood Protection, each interface has an independent limit which does not affect the limits of other interfaces.	ICMP-Flood: 1 to 4000 SYN-Flood: 1 to 4000 ARP-Flood: 1 to 2000 UDP-Flood: 1 to 8000	Enabled with Limit set to 1000 for ICMP-Flood, SYN-Flood, ARP-Flood Disabled with Limit set to 0 for UDP-Flood

Device Policy

Menu Path: Firewall > DoS Policy - Device Policy

This page lets you configure device policies that lets you apply flood protection mechanisms for specific destination IP addresses.

Limitations

You can create up to 64 device policies.

Device Policy Log Settings

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable logging of device policy events.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog:** Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap:** Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A

Device Policy List

UI Setting	Description
Index	Shows the index of the policy. The index determines the order for processing policies.
Name	Shows the name of the policy.

UI Setting	Description
Enforcement	Shows whether the policy is enabled or disabled.
Type	Shows the type of flood protection the policy uses.
Destination IP	Shows the destination IP addresses the policy applies to.
Destination Port	Shows the destination ports the policy applies to.
Limit	Shows the limit in packets per second that must be exceeded to trigger an event for the policy.
Action	Shows the action that will be taken for applicable traffic when an event is triggered for the policy.
Hit Counter	Shows the number of times the policy has been triggered since the last boot.

Add Device Policy

Menu Path: Firewall > DoS Policy - Device Policy

Clicking the **Add (⊞)** icon on the **Firewall > DoS Policy - Device Policy** page will open this dialog box. This dialog lets you create a new device policy.

Click **CREATE** to save your changes and add the new policy.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of the policy. The index determines the order for processing policies.	1 to Current number of device policies + 1, up to 64	Current number of device policies + 1
Enforcement	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Type	Select the type of flood protection the policy will use. • **ICMP-Flood**: A type of cyberattack that overloads a target network with Internet Control Message Protocol (ICMP) echo requests. • **SYN-Flood**: A form of denial-of-service attack against systems that provide services over the Transmission Control Protocol (TCP). • **UDP-Flood**: A volumetric denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.	ICMP-Flood / SYN-Flood / UDP-Flood	ICMP-Flood

UI Setting	Description	Valid Range	Default Value
Destination IP	Specify the destination IP address this policy will apply to. When selecting IP Address, enter the IP address to use.	Any / IP Address (Valid IP address)	Any
Destination Port **(If Type is SYN-Flood or UDP-Flood)**	Specify the destination IP port this policy will apply to. When selecting Port Number, enter the port number to use.	Any / Port Number (1 to 65535)	Any
Limit	Specify the limit in packets per second that must be exceeded to trigger an event for the policy.	**ICMP-Flood and SYN-Flood**: 1 to 4000 **UDP-Flood**: 1 to 8000	**ICMP-Flood and SYN-Flood**: 1000 **UDP-Flood**: 2000
Action	Select the action the firewall should take for traffic that matches this policy. • **Drop**: The firewall will drop packets that match the policy. • **Monitor:** The firewall will allow packets that match the policy, but will log the event.	Drop / Monitor	Drop

Edit Device Policy

Menu Path: Firewall > DoS Policy - Device Policy

Clicking the **Edit ( )** icon for a policy on the **Firewall > DoS Policy - Device Policy** page will open this dialog box. This dialog lets you edit the policy.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of the policy. The index determines the order for processing policies.	1 to Current number of device policies + 1, up to 64	Current number of device policies + 1
Enforcement	Enable or disable the policy.	Enabled / Disabled	Enabled
Name	Specify a name for the policy.	1 to 32 characters	N/A
Type	Select the type of flood protection the policy will use. • **ICMP-Flood**: A type of cyberattack that overloads a target network with Internet Control Message Protocol (ICMP) echo requests. • **SYN-Flood**: A form of denial-of-service attack against systems that provide services over the Transmission Control Protocol (TCP). • **UDP-Flood**: A volumetric denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.	ICMP-Flood / SYN-Flood / UDP-Flood	ICMP-Flood

UI Setting	Description	Valid Range	Default Value
Destination IP	Specify the destination IP address this policy will apply to. When selecting IP Address, enter the IP address to use.	Any / IP Address (Valid IP address)	Any
Destination Port **(If Type is SYN-Flood or UDP-Flood)**	Specify the destination IP port this policy will apply to. When selecting Port Number, enter the port number to use.	Any / Port Number (1 to 65535)	Any
Limit	Specify the limit in packets per second that must be exceeded to trigger an event for the policy.	**ICMP-Flood and SYN-Flood**: 1 to 4000 **UDP-Flood**: 1 to 8000	**ICMP-Flood and SYN-Flood**: 1000 **UDP-Flood**: 2000
Action	Select the action the firewall should take for traffic that matches this policy. • **Drop**: The firewall will drop packets that match the policy. • **Monitor:** The firewall will allow packets that match the policy, but will log the event.	Drop / Monitor	Drop

Delete Device Policy

Menu Path: Firewall > DoS Policy - Device Policy

You can delete a policy by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Soft Lockdown Mode

Menu Path: Firewall > Soft Lockdown Mode

This page lets you configure Soft Lockdown Mode for your device. For more information on how this feature works, refer to Soft Lockdown.

Note

Soft Lockdown Mode is a feature designed for railway applications and is only supported by the TN-4900 Series.

Soft Lockdown Status

UI Setting	Description
Status	Shows the status of Soft Lockdown Mode.

Soft Lockdown Mode Settings

Note

In addition to the criteria defined in these settings, the device will enter Soft Lockdown Mode if any enabled critical service is no longer alive.

All enabled critical services must be alive to leave Soft Lockdown Mode.

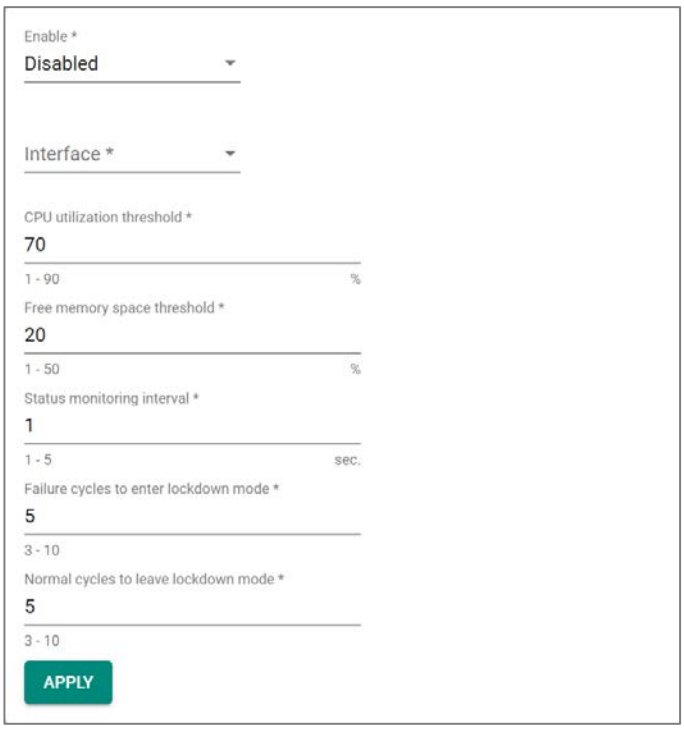
Note

The critical services that apply to Soft Lockdown Mode are as follows:

- DHCP Server (refer to DHCP Server)
- DHCP Relay Agent (refer to DHCP Relay Agent)
- SNMP Server (refer to SNMP)
- Turbo Ring V2 (refer to Turbo Ring V2)

Note

If Soft Lockdown Mode and DHCP Server are both enabled, make sure at least one LAN interface's IP is within the DHCP server pool and at least one physical port is assigned to this LAN interface.



UI Setting	Description	Valid Range	Default Value
Enable	Enable/Disable use of the Soft Lockdown Mode feature.	Enabled / Disabled	Disable
Interface	Specify which interface Soft Lockdown Mode will apply to. When in Soft Lockdown Mode, all traffic on this interface (both ingress and egress) will be blocked.	Drop-down list of interfaces	N/A
CPU utilization threshold	Specify the maximum CPU utilization % allowed. If the CPU utilization % goes over this threshold, a failure will be triggered for the current cycle.	1 to 90	70
Free memory space threshold	Specify the minimum free memory % allowed. If the free memory % goes below this threshold, a failure will be triggered for the current cycle.	1 to 50	20
Status monitoring interval	Specify a cycle time in seconds to monitor CPU and memory usage for failure detection.	1 to 5	1

UI Setting	Description	Valid Range	Default Value
Failure cycles to enter lockdown mode	Specify the number of consecutive cycles with failures allowed before entering soft lockdown mode.	3 to 10	5
Normal cycles to leave lockdown mode	Specify the required number of normal consecutive cycles without failures before leaving soft lockdown mode.	3 to 10	5

Device Lockdown

Menu Path: Firewall > Device Lockdown

This page lets you configure Device Lockdown to secure and control network traffic.

Device Lockdown offers a straightforward method to automatically configure firewall whitelisting. Users are not required to know the device's IP or MAC address to set up firewall rules. The Learning function enables the device to gather device information from network traffic to establish whitelisting rules. Additionally, users can customize the learning table according to their needs.

> **Note**
> Device Lockdown is specifically designed for and is only available for NAT Series devices.

This page includes these tabs:

- Settings
- Learning Table

Device Lockdown - Settings

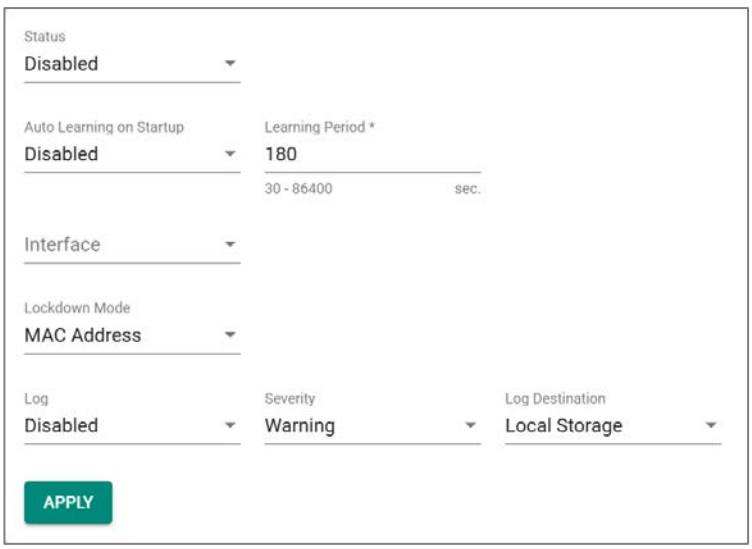
Menu Path: Firewall > Device Lockdown - Settings

This page lets you manage the Device Lockdown feature.

Learning Status

UI Setting	Description
Learning Status	Shows the learning status for the Device Lockdown feature. • **START LEARNING:** Learn whitelist information from ARP tables through network traffic. **Note** When the Learning Status process is in progress, Device Lockdown cannot be enabled until the process is complete. • **STOP LEARNING:** Stop the current learning process.

Device Lockdown Settings



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable device lockdown. **Note** When Status is enabled, the Learning Table can't be manually configured. Please disable Status to make modifications.	Enabled / Disabled	Disabled
Auto Learning on Startup	Enable or disable auto learning on startup.	Enabled / Disabled	Disabled
Learning Period	Specify the duration in seconds auto learning will be enabled for.	30 to 86400	180
Interface	Select which interfaces to lock down. Multiple interfaces can be selected.	Drop-down list of interfaces	N/A
Lockdown Mode	Select the firewall filtering criteria.	MAC Address / MAC + IP Access	MAC Address
Log	Enable or disable device lockdown event logs.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	Local Storage

Device Lockdown - Learning Table

Menu Path: Firewall > Device Lockdown - Learning Table

This page lets you view and manage the current learning table used for the Device Lockdown feature.

Limitations

You can create up to 128 learning list entries.

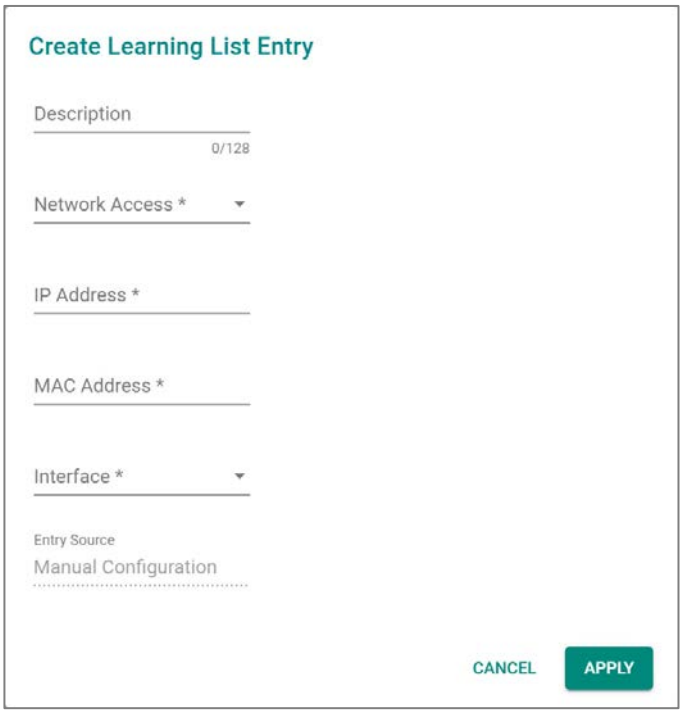
UI Setting	Description
Description	Shows the description used to identify the learning table rule.
Network Access	Shows the network access rule to apply to the specified IP address or MAC address. • **Allow**: Grants access to the specified IP address or MAC address. • **Block:** Denies access to the specified IP address or MAC address.
IP Address	Shows the IP address the rule applies to. **Any** means it applies to all IP addresses.
MAC Address	Shows the MAC address the rule applies to. **Any** means it applies to all MAC addresses.
Interface	Shows the interface that the rule applies to.
Entry Source	Shows the source of the rule. • **Manual Configuration**: The rule was manually created by a user. • **Auto Learning**: The rule was created through the learning feature. Refer to Learning Status for more information.

Create Learning List Entry

Menu Path: Firewall > Device Lockdown - Learning Table

Clicking the **Add (+)** icon on the **Firewall > Device Lockdown - Learning Table** page will open this dialog box. This dialog lets you manually create a new learning list entry.

Click **CREATE** to save your changes and add the new entry.



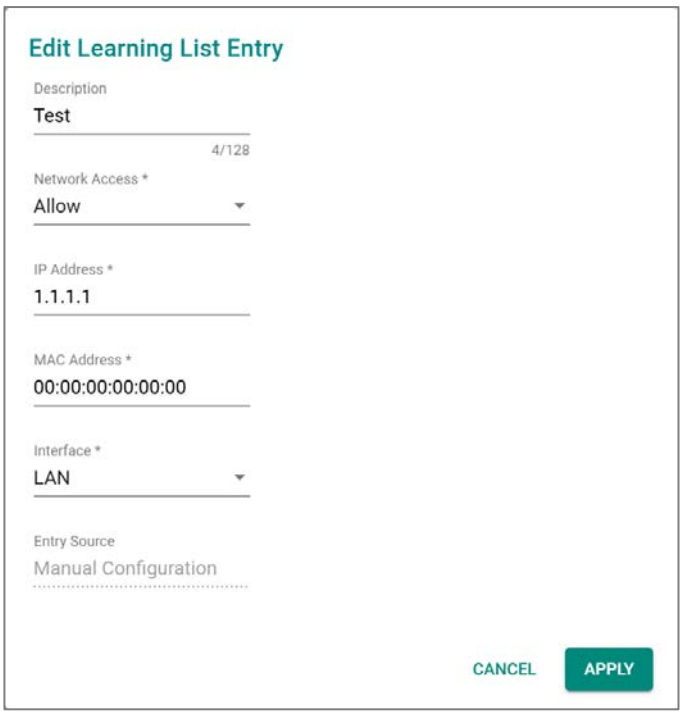
UI Setting	Description	Valid Range	Default Value
Description	Specify a description to help identify the entry.	Up to 128 characters	N/A
Network Access	Specify the network access rule to apply for this entry. • **Allow**: Grants access to the specified IP address or MAC address. • **Block:** Denies access to the specified IP address or MAC address.	Allow / Block	N/A
IP Address	Specify the IP address the rule applies to.	Valid IP address	N/A
MAC Address	Specify the MAC address the rule applies to.	Valid MAC address	N/A
Interface	Specify the interface the rule applies to.	Drop-down list of interfaces	N/A
Entry Source (View only)	Shows how the entry was created.	Manual Configuration / Auto Learning	Manual Configuration

Edit Learning List Entry

Menu Path: Firewall > Device Lockdown - Learning Table

Clicking the **Edit ( )** icon for an entry on the **Firewall > Device Lockdown - Learning Table** page will open this dialog box. This dialog lets you edit an existing learning list entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Description	Specify a description to help identify the entry.	Up to 128 characters	N/A
Network Access	Specify the network access rule to apply for this entry. • **Allow**: Grants access to the specified IP address or MAC address. • **Block:** Denies access to the specified IP address or MAC address.	Allow / Block	N/A
IP Address	Specify the IP address the rule applies to.	Valid IP address	N/A
MAC Address	Specify the MAC address the rule applies to.	Valid MAC address	N/A

UI Setting	Description	Valid Range	Default Value
Interface	Specify the interface the rule applies to.	Drop-down list of interfaces	N/A
Entry Source (View only)	Shows how the entry was created.	Manual Configuration / Auto Learning	Manual Configuration

Delete Learning List Entry

Menu Path: Firewall > Device Lockdown - Learning Table

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Advanced Protection

Menu Path: Firewall > Advanced Protection

This section lets you monitor and configure your device's advanced firewall features.

This section includes these pages:

- Dashboard
- Configuration
- Protocol Filter Policy
- ADP
- IPS
- Domain Protection

Dashboard

Menu Path: Firewall > Advanced Protection > Dashboard

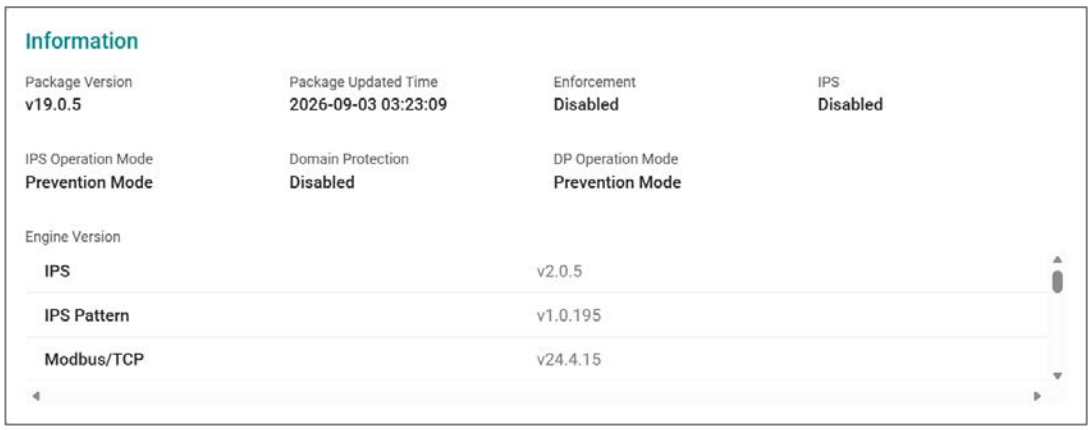
This page lets you see an overview of your firewall's advanced protection activity with real-time event counters.

Note

Please note that available status displays may vary depending on the product and model, and whether an IPS license is installed or not.

Information

This display shows the versions of the installed firewall engines and security packages currently installed on the device, as well as whether various functions are enabled.



UI Setting	Description
Package Version	Shows the version of the current Network Security Package installed on the device.
Package Updated Time	Shows when the current Network Security Package was installed.
Enforcement	Shows whether DPI protocol filtering is enabled.
IPS	Shows whether IPS is enabled.
IPS Operation Mode	Shows which operation mode IPS is using.
Domain Protection	Shows whether domain protection is enabled.
DP Operation Mode	Shows the domain protection operation mode being used.

UI Setting	Description
Engine Version	Shows the versions of the different engines being used. **Note** Starting from v9.0 of the Network Security Package, when the IPS license expires, existing IPS patterns can still be used for IPS protection. However, the IPS patterns will not be updated and will remain at their current versions when you update the Network Security Package.

Intrusion Prevention System (IPS)

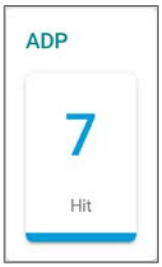
This display shows the current number of Intrusion Prevention System (IPS) events. Clicking on an item will take you to a filtered view of the IPS event log. Refer to Firewall Log for more information.

Domain Protection

This display shows the current number of Domain Protection events. Clicking on it will take you to the Domain Protection event log. Refer to Firewall Log for more information.

ADP

This display shows the current number of Anomaly Detection and Prevention (ADP) events. Clicking on an item will take you to the ADP event log. Refer to Firewall Log for more information.



Enforcement

This display shows the current number of industrial protocol events. Clicking on an item will take you to a filtered view of the Protocol Filter Policy event log. Refer to Firewall Log for more information.

Configuration

Menu Path: Firewall > Advanced Protection > Configuration

This page lets you configure your application firewall's advanced protection settings.

This page includes these tabs:

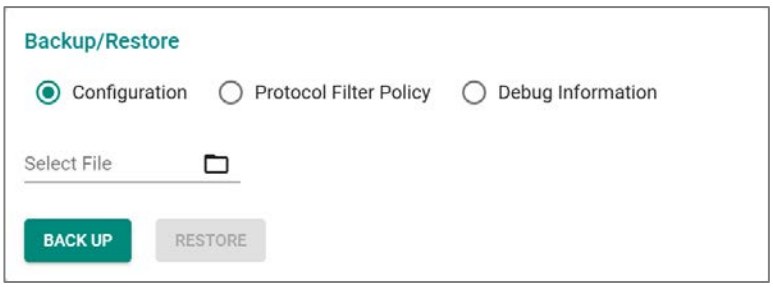
- Global Settings
- Protocol Filter Object
- Protocol Filter Profile

Configuration - Global Settings

Menu Path: Firewall > Advanced Protection > Configuration - Global Settings

This page lets you configure global settings for your application firewall's advanced protection features. You can also back up and restore your advanced protection settings on this page.

Backup/Restore

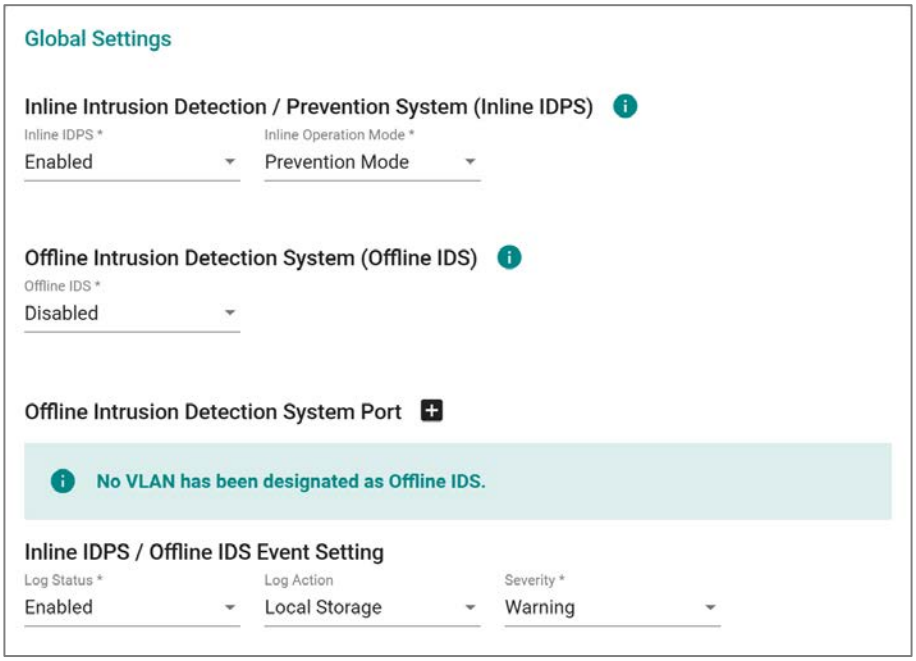


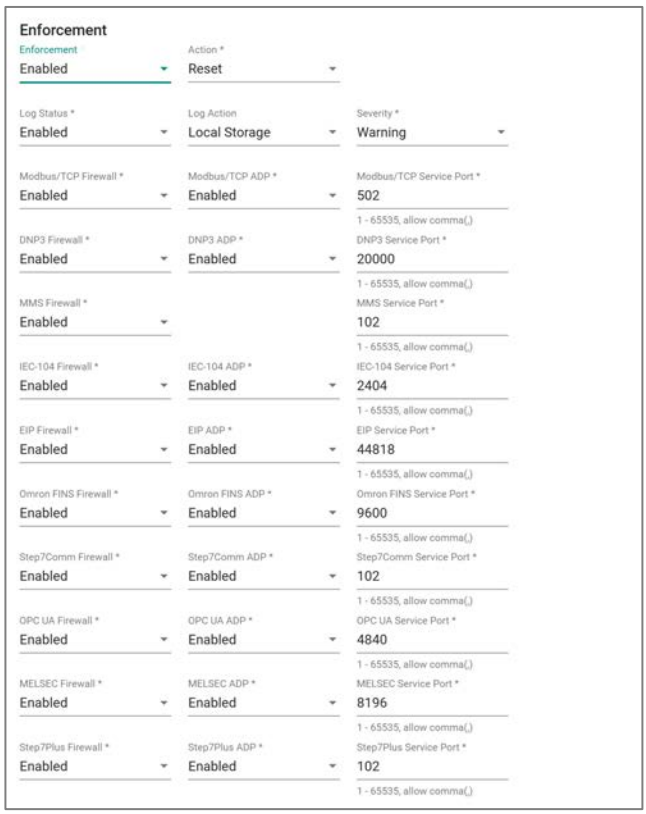
UI Setting	Description	Valid Range	Default Value
Backup/Restore	Select which settings you want to back up or restore. If you want to back up your settings, click **BACK UP**. • **Configuration**: Back up/restore all settings on the Configuration page. • **Protocol Filter Policy**: Back up/restore all policies on the Protocol Filter Policy page. • **Debug Information**: Back up debug information for your firewall's advanced protection features.	Configuration / Protocol Filter Policy / Debug Information	Configuration
Select File **(If Backup/Restore is Configuration or Protocol Filter Policy)**	If you want to restore settings, click this field and select the settings file from your local computer, then click **RESTORE**.	N/A	N/A

Global Settings

Note

Available settings will vary depending on your product model and whether an active IPS license is installed.





Inline Intrusion Detection / Prevention System (Inline IDPS)

UI Setting	Description	Valid Range	Default Value
Inline IDPS	Enable or disable the inline intrusion detection/prevention system (inline IDPS).	Enabled / Disabled	Enabled
Inline Operation Mode	Select an inline operation mode to use for the device. • **Prevention Mode**: Detects and blocks malicious traffic for real-time protection. • **Detection Mode**: Inspects traffic and logs potential threats without blocking. This can be useful for PoC or commissioning stages.	Prevention Mode / Detection Mode	Prevention Mode

Offline Intrusion Detection System (Offline IDS)

UI Setting	Description	Valid Range	Default Value
Offline IDS	Enables or disables the offline intrusion detection system (offline IDS). When enabled, the device will inspect traffic from a mirrored port or RSPAN without affecting live operations.	Enabled / Disabled	Disabled

Offline Intrusion Detection System Port

- Select the **Add (⊞)** icon to add a port for offline IDS analysis.
- Select the **Delete (⊞)** icon for a port to remove it from offline IDS analysis.

Limitations

You can add up to 6 ports for offline IDS.

Note

For EDR-G9010, EDR-8010, TN-4900 Series

- VLAN configuration is required for the offline IDS port to analyze incoming RSPAN traffic.
- The RSPAN switch port must also be configured with the same VLAN tag as the ofline IDS port.

For EDR-G9004, EDF-G1002-BP Series

- VLAN configuration is not required, as these models analyze traffic without VLAN tagging.
- Port Limitations:
  - EDR-G9004 only supports the WAN 2 port for offline IDS.
  - EDF-G1002-BP only supports the management port for offline IDS.

UI Setting	Description	Valid Range	Default Value
Port	Select a port for offline IDS traffic analysis.	Drop-down list of ports	N/A
VLAN	Specify a VLAN tag for the offline IDS port. The VLAN must match the setting on the switch providing port mirroring or RSPAN.	1 to 4094	Automatically assigns an unused VLAN starting from 1003

Inline IDPS / Offline IDS Event Setting

UI Setting	Description	Valid Range	Default Value
Log Status	Enable or disable inline IDPS and offline IDS event logging.	Enabled / Disabled	Disabled
Log Action	Specify where to send inline IDPS and offline IDS event logs. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	Local Storage
Severity	Select the severity level to assign to inline IDPS and offline IDS events. Refer to the Severity Level List for more information.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

Domain Protection

UI Setting	Description	Valid Range	Default Value
DP	Enable or disable domain protection.	Enabled / Disabled	Disabled
DP Operation Mode	Select an operation mode for domain protection. • **Prevention Mode**: The device will block traffic based on your domain protection settings. Refer to Domain Protection for more information. • **Detection Mode**: The device will not block traffic, and will only generate events based on your domain protection settings.	Prevention Mode / Detection Mode	Prevention Mode
Log Status	Enable or disable domain protection event logging.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Log Action	Specify where to send domain protection event logs. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	Local Storage
Severity	Select the severity level to assign to domain protection events. Refer to the Severity Level List for more information.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

Enforcement

UI Setting	Description	Valid Range	Default Value
Enforcement	Enable or disable DPI protocol filtering.	Enabled / Disabled	Enabled
Action	Select the default action of the protocol filter when enforcement is enabled. **Note** The Event Log (Firewall Log) will display Policy ID '99999' when this default action is activated. • **Accept**: The firewall will accept packets when no defined Protocol Filter Policy matches. With this setting, no logs are recorded. • **Monitor**: The firewall will accept packets when no defined Protocol Filter Policy matches. With this setting, each packet of an identified application protocol will have a corresponding Event Log entry. • **Reset**: The firewall will drop packets when no defined Protocol Filter Policy matches. With this setting, only the first packet of an identified application protocol will be recorded in Event Log.	Accept / Monitor / Reset	Reset

UI Setting	Description	Valid Range	Default Value
Log Status	Enable or disable enforcement event logging.	Enabled / Disabled	Disabled
Log Action	Specify where to send enforcement event logs. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	Local Storage
Severity	Select the severity level to assign to enforcement events. Refer to the Severity Level List for more information.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning
Modbus/TCP Firewall	Enable or disable the Modbus/TCP protocol filter engine.	Enabled / Disabled	Enabled
Modbus/TCP ADP	Enable or disable ADP for Modbus/TCP traffic.	Enabled / Disabled	Enabled
Modbus/TCP Service Port	Specify the service port for Modbus/TCP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	502
DNP3 Firewall	Enable or disable the DNP3 protocol filter engine.	Enabled / Disabled	Enabled
DNP3 ADP	Enable or disable ADP for DNP3 traffic.	Enabled / Disabled	Enabled
DNP3 Service Port	Specify the service port for DNP3 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	20000
MMS Firewall	Enable or disable the MMS protocol filter engine.	Enabled / Disabled	Enabled
MMS Service Port	Specify the service port for MMS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
IEC-104 Firewall	Enable or disable the IEC-104 protocol filter engine.	Enabled / Disabled	Enabled
IEC-104 ADP	Enable or disable ADP for IEC-104 traffic.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
IEC-104 Service Port	Specify the service port for IEC-104 traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	2404
EIP Firewall	Enable or disable the EIP protocol filter engine.	Enabled / Disabled	Enabled
EIP ADP	Enable or disable ADP for EIP traffic.	Enabled / Disabled	Enabled
EIP Service Port	Specify the service port for EIP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	44818
Omron FINS Firewall	Enable or disable the Omron FINS protocol filter engine.	Enabled / Disabled	Enabled
Omron FINS ADP	Enable or disable ADP for Omron FINS traffic.	Enabled / Disabled	Enabled
Omron FINS Service Port	Specify the service port for Omron FINS traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	9600
Step7Comm Firewall	Enable or disable the Step7Comm protocol filter engine.	Enabled / Disabled	Enabled
Step7Comm ADP	Enable or disable ADP for Step7Comm traffic.	Enabled / Disabled	Enabled
Step7Comm Service Port	Specify the service port for Step7Comm traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102
TRDP Firewall	Enable or disable the TRDP protocol filter engine.	Enabled / Disabled	Enabled
TRDP Service Port	Specify the service port for TRDP traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	17224, 17225
OPC UA Firewall	Enable or disable the OPC UA protocol filter engine.	Enabled / Disabled	Enabled
OPC UA ADP	Enable or disable ADP for OPC UA traffic.	Enabled / Disabled	Enabled
OPC UA Service Port	Specify the service port for OPC UA traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	4840
MELSEC Firewall	Enable or disable the MELSEC protocol filter engine.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
MELSEC ADP	Enable or disable ADP for MELSEC traffic.	Enabled / Disabled	Enabled
MELSEC Service Port	Specify the service port for MELSEC traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	8196
Step7Plus Firewall	Enable or disable the Step7Plus protocol filter engine.	Enabled / Disabled	Enabled
Step7Plus ADP	Enable or disable ADP for Step7Plus traffic.	Enabled / Disabled	Enabled
Step7Plus Service Port	Specify the service port for Step7Plus traffic. You can specify multiple ports by separating them with a comma.	1 to 65535	102

Troubleshooting

UI Setting	Description	Valid Range	Default Value
Debug Logging	Enable or disable debug logging for troubleshooting.	Enabled / Disabled	Disabled

Protocol Filter Object

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

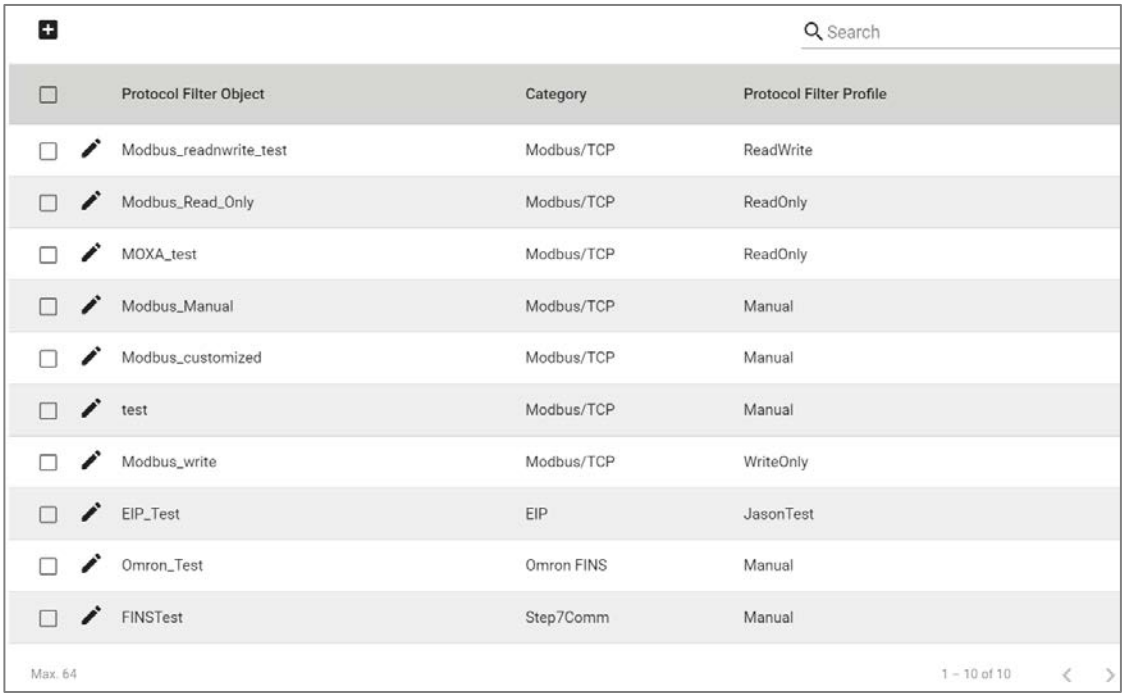
This page lets you create and manage protocol filter objects, which can simplify creation and maintenance of protocol filter policies.

Note

Available protocols may vary across different product models and versions.

Limitations

You can create up to 64 protocol filter objects.



UI Setting	Description
Protocol Filter Object	Shows the name of the object
Category	Shows the protocol category of the object.
Protocol Filter Profile	Shows which protocol filter profile the object uses.

Protocol Filter Object - Create Object

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

Clicking the **Add (⊞)** icon on the **Firewall > Advanced Protection > Configuration - Protocol Filter Object** page will open this dialog box. This dialog lets you create a protocol filter object. Click **CREATE** to save your changes and add the new object.

Create Object - Modbus/TCP

If **Modbus/TCP** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A

UI Setting	Description	Valid Range	Default Value
Slave ID	Specify the Modbus slave ID. Leave this field blank to represent any ID. **Note** The Slave ID is used to identify Modbus devices. This ID can be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.	0 to 255 / 0x00 to 0xFF	Any
Protocol Filter Profile	Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. • **Read Only**: Use a set of commonly used function codes associated with read-only access. • **Write Only**: Use a set of commonly used function codes associated with write-only access. • **Read/Write**: Use a set of commonly used function codes associated with read/write access. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Read Only / Write Only / Read/Write / Drop-down list of related protocol filter profiles / Manual	N/A
Function Code	Shows which function codes will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which function codes to use for this object. You can select multiple options.	Drop-down list of function codes	Depends on the selected **Protocol Filter Profile**
PLC Address Base 1 **(If only one Function Code is selected)**	Select whether the PLC's starting address should start from 0x00 or 0x01. This should be set based on your PLCs to ensure DPI filters the correct addresses and values. • **Enabled**: The PLC's starting address starts at 0x01. • **Disabled**: The PLC's starting address starts at 0x00.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Filter Type **(If only one Function Code is selected)**	Select the filter type to use. • **None**: Filter traffic by specified function codes. • **Address Range**: Filter traffic by specified PLC register addresses. • **Data Value**: Filter the traffic by specified data values in the registers.	None / Address Range / Data Value	None
Address Range **(If Filter Type is Address Range)**	Define the address range to use for the filter. You can enter the address range in decimal or hexadecimal format.	0 to 65535 / 0x0000 to 0xFFFF	N/A
Start Address **(If Filter Type is Data Value)**	Specify the starting address for the PLC register address. You can enter the addresss in decimal or hexadecimal format.	0 to 65535 / 0x0000 to 0xFFFF	N/A
Value **(If Filter Type is Data Value)**	Specify a data value to filter for. You can enter up to 16 bits (2 bytes) of binary data for the data value.	0 to 1111111111111111 (binary data)	N/A

Create Object - DNP3

If **DNP3** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
Source Address	Shows the source address to check for in DNP3 packets, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the source address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**
Destination Address	Shows the destination address to check for in DNP3 packets, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**
Application Function Code	Shows which function code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which function code to use for this object.	Drop-down list of function codes	Depends on the selected **Protocol Filter Profile**
Group	Shows the group to use to classify types within a message, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function code to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Variation	Shows the variation to use for encoding formats, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the variation to use for this object.	0 to 255 or 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**

Create Object - MMS

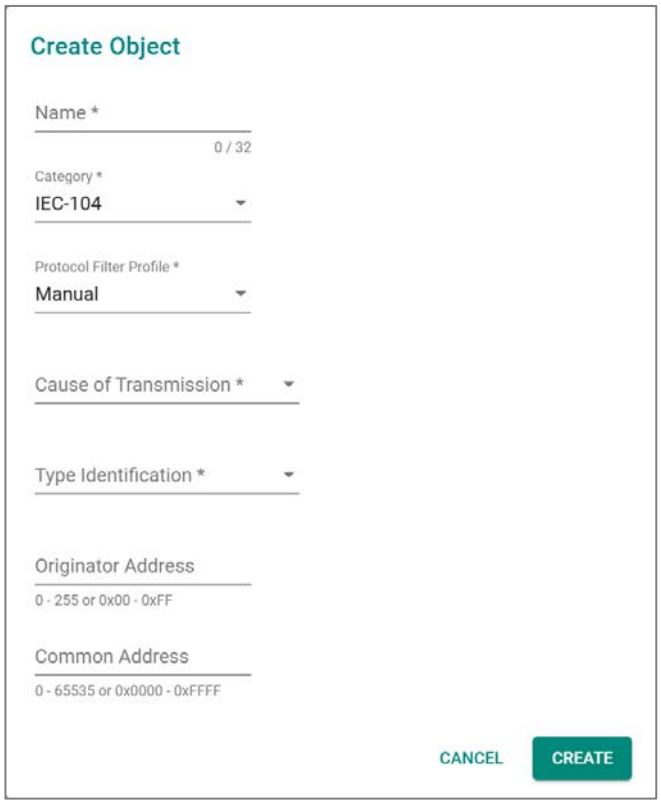
If **MMS** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A
Device	Specify a device name for the object.	1 to 255 characters	N/A

UI Setting	Description	Valid Range	Default Value
Item ID	Specify an item ID for the object.	1 to 255 characters	N/A
Command Type	Shows which MMS command type will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the command type to use for the object. Refer to MMS Command Types for an overview of all command types.	Drop-down list of MMS command types	Depends on the selected **Protocol Filter Profile**
Service	Shows which service will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the service to use for the object.	Any / Confirmed Request / Confirmed Response / Unconfirmed	Depends on the selected **Protocol Filter Profile**
Service Operation	Shows which service operations will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the service operations to use for the object. You can select multiple options. Refer to MMS Service Operation List for an overview of all service operations.	Drop-down list of service operations	Depends on the selected **Protocol Filter Profile**
MMS Data Type	Specify which MMS data types to use for the object. You can select multiple options. For each service operation, specify the values to use. You can specify multiple values by separating them with a comma.	Drop-down list of MMS data types 0 to 65535	N/A

Create Object - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Identify Service / Read Service / Write Service / Report Service / File Operation Service / Journal Service / Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
Cause of Transmission	Shows which IEC-104 cause of transmission code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the cause to use for the object. Refer to the IEC-104 Cause of Transmission List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 cause of transmission codes	Depends on the selected **Protocol Filter Profile**
Type Identification	Shows which IEC-104 type identification code will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select the type to use for the object. Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 type identification codes	Depends on the selected **Protocol Filter Profile**
Originator Address	Shows which originator address will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the address to use for the object.	0 to 255 / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Common Address	Shows which common address will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the address to use for the object.	0 to 65535 / 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**

Create Object - EIP-CIP (EDF/EDR/NAT/TN Series)

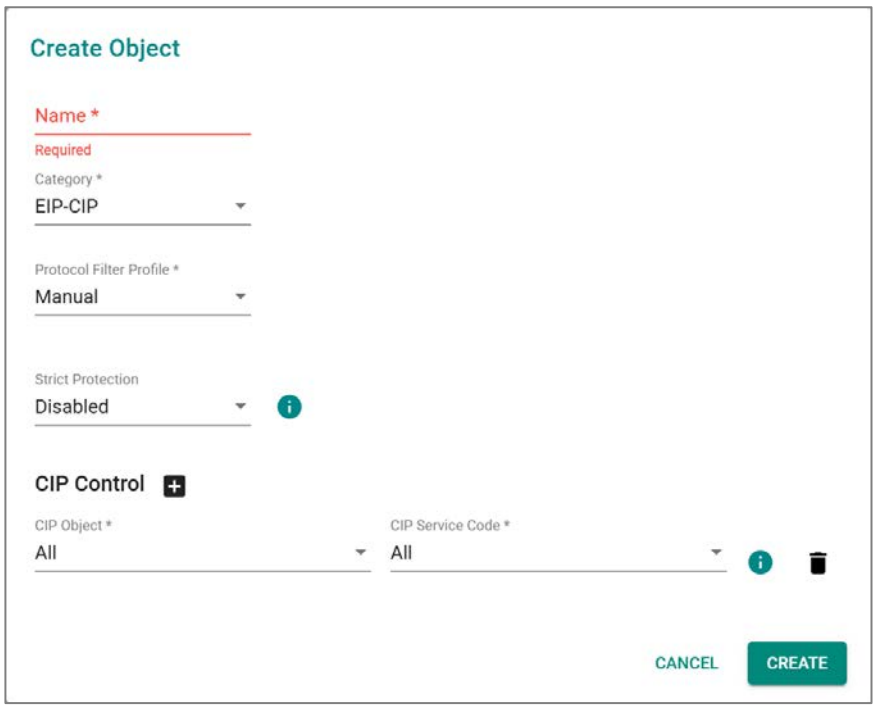
If **EIP-CIP** is selected for the **Category**, these settings will appear.

Select the **Add (⊕)** icon to add a CIP control.

Select the **Delete (🗑)** icon to delete the corresponding CIP control.

Limitations

You can add up to 8 CIP controls to an EIP-CIP protocol filter entry.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A

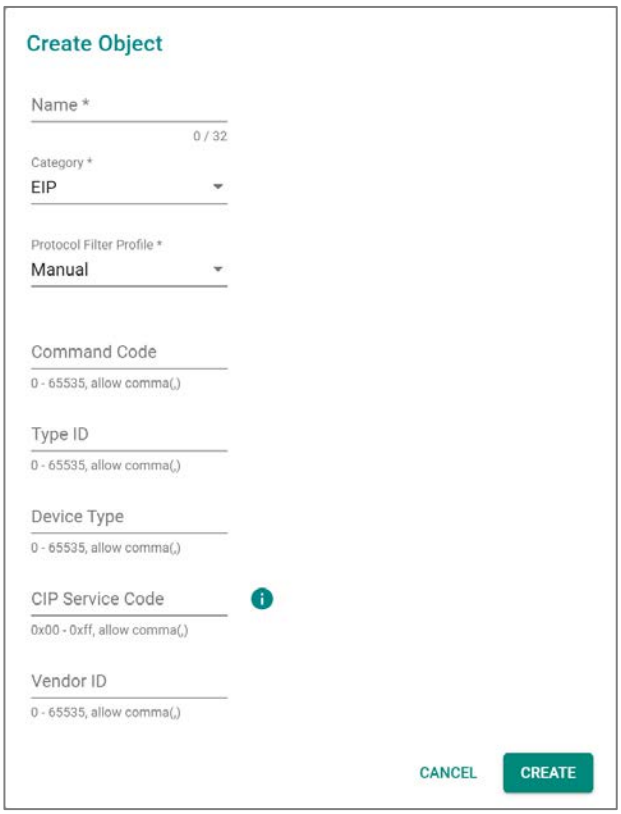
UI Setting	Description	Valid Range	Default Value
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
Strict Protection	Enable or disable Strict Protection, which controls how CIP Multiple Service Packets (0x0A) are handled. • **Enabled:** A Multiple Service Packet is allowed only when all included sub-services are read operations. If any sub-service contains a write operation, the entire packet is blocked. • **Disabled:** The additional check on all sub-services in a Multiple Service Packet is not applied.	Enabled / Disabled	Disabled

CIP Control

UI Setting	Description	Valid Range	Default Value
CIP Object	Shows the CIP objects that will be used for the CIP control, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the CIP objects to use for this object. Multiple values can be entered by separating them with commas. Refer to CIP Object List for an overview of the different CIP objects.	All / Drop-down list of CIP objects / 0x00 to 0xff	All
CIP Service Code	Shows the CIP service codes that will be used for the CIP control, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the CIP service codes to use for this object. Multiple values can be entered by separating them with commas.	All / Drop-down list of CIP service codes based on the selected **CIP Object** / 0x00 to 0xff	All

Create Object - EIP (OnCell Series)

If **EIP** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
Command Code	Shows the EIP command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Type ID	Shows the type IDs that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the type IDs to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Device Type	Shows the device types that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the device types to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
CIP Service Code	Shows the CIP service codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the CIP service codes to use for this object. Multiple values can be entered by separating them with commas.	0x00 to 0xff	Depends on the selected **Protocol Filter Profile**
Vendor ID	Specify the vendor IDs to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Object - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
TCP Command	Shows the TCP command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	Depends on the selected **Protocol Filter Profile**
Command Code	Shows the command codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the command codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Error Code	Shows the error codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the error codes to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	Depends on the selected **Protocol Filter Profile**
Client Node Address	Specify the client node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
Server Node Address	Specify the server node addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A
File Position	Specify the file positions to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
File Position Begin Address	Specify the file position begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

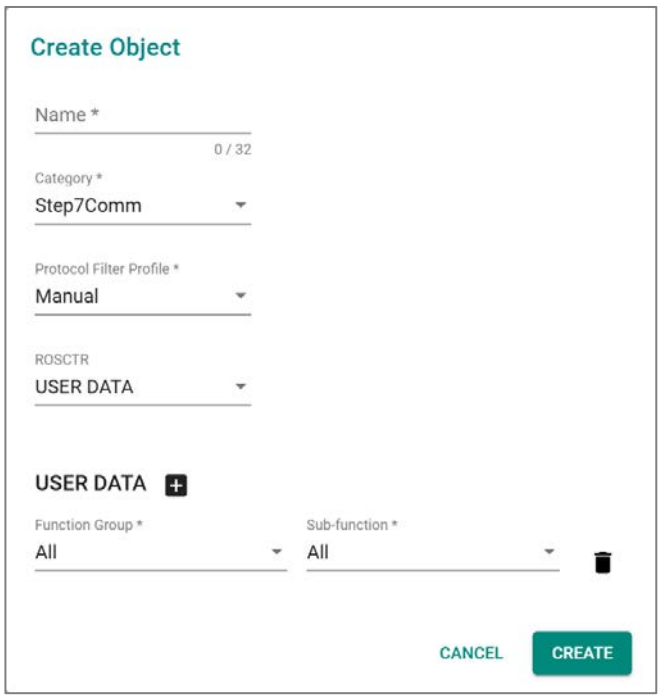
UI Setting	Description	Valid Range	Default Value
Begin Address	Specify the begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Record Begin Address	Specify the record begin addresses to use for this object. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Object - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.

Limitations

When ROSCTR is USER DATA, you can add up to 8 USER DATA entries.

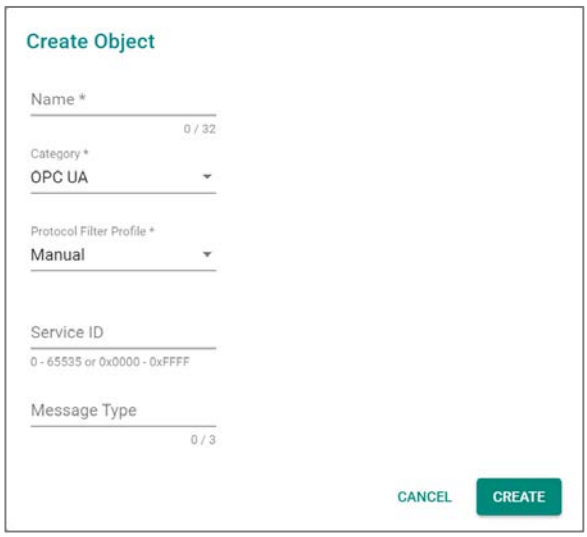


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
ROSCTR	Shows the ROSCTR control that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the ROSCTR control to use for this object. When **ROSCTR** is **USER DATA**, select the **Add ( )** icon to add a USER DATA entry.	ANY / JOB (Function) / USER DATA	Depends on the selected **Protocol Filter Profile**
Function **(If ROSCTR is JOB (Function))**	Select the function codes that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function codes to use for this object. You can specify multiple values by separating them with a comma.	All / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**

UI Setting	Description	Valid Range	Default Value
Function Group **(If ROSCTR is USER DATA)**	Select the function group that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the function groups to use for this object. You can specify multiple values by separating them with a comma.	All / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**
Sub-function **(If ROSCTR is USER DATA)**	Select the sub-function groups that will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, specify the sub-function codes to use for this object. You can specify multiple values by separating them with a comma.	All / 0x00 to 0xFF	Depends on the selected **Protocol Filter Profile**

Create Object - OPC UA

If **OCP UA** is selected for the **Category**, these settings will appear.



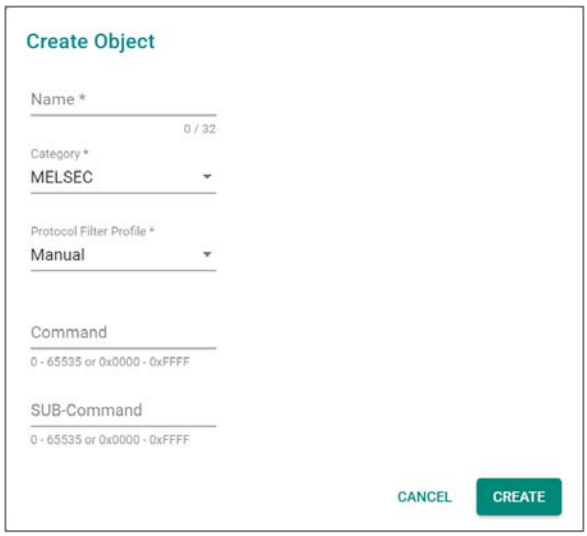
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a protocol filter profile based on the OPC UA operations you want to allow. The preset profiles are preconfigured with the required OPC UA service IDs and message types, so you do not need to configure them manually. • **OPCUA_DiscoverAndExplore:** Allow OPC UA clients to discover servers and browse the server address space, such as viewing available nodes and information. • **OPCUA_Response:** Allow OPC UA response messages from the server. • **OPCUA_DataReadOnly:** OPC UA clients can only read data values and cannot write or modify data. • **OPCUA_DataSubscriptOnly:** OPC UA clients can only subscribe to and monitor data changes and cannot write or modify data. • **Manual:** Manually configure the OPC UA service IDs and message types for the object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	OPCUA_DataSubscriptOnly / OPCUA_DataReadOnly / OPCUA_Response / OPCUA_DiscoverAndExplore / Drop-down list of related protocol filter profiles / Manual	N/A
Service ID	Shows the service IDs that will be used for this object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the service IDs to use for this object in decimal or hexadecimal format. Multiple values can be entered by separating them with commas.	0 to 65535, 0x0000 to 0xFFFF	Depends on the selected **Protocol Filter Profile**

UI Setting	Description	Valid Range	Default Value
Message Type	Shows the message type that will be used for this object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the message type to use for this object. **Note** Some defined message types are: • HEL: Hello message • ACK: Acknowledge message • ERR: Error message • RHE: ReverseHello message	0 to 3 characters	Depends on the selected **Protocol Filter Profile**

Create Object - MELSEC

If **MELSEC** is selected for the **Category**, these settings will appear.

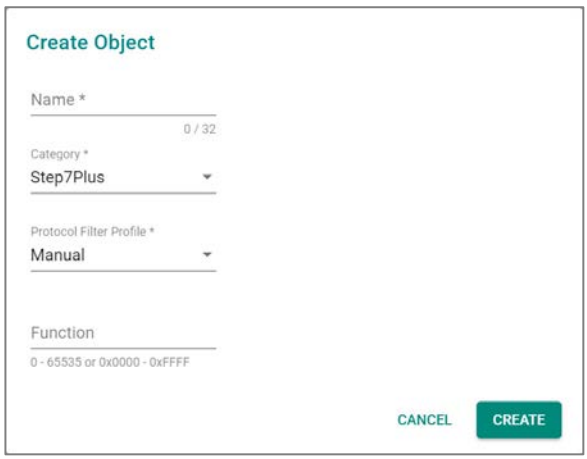


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
Command	Specify a command for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A
SUB-Command	Specify a sub-command for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A

Create Object - Step7Plus

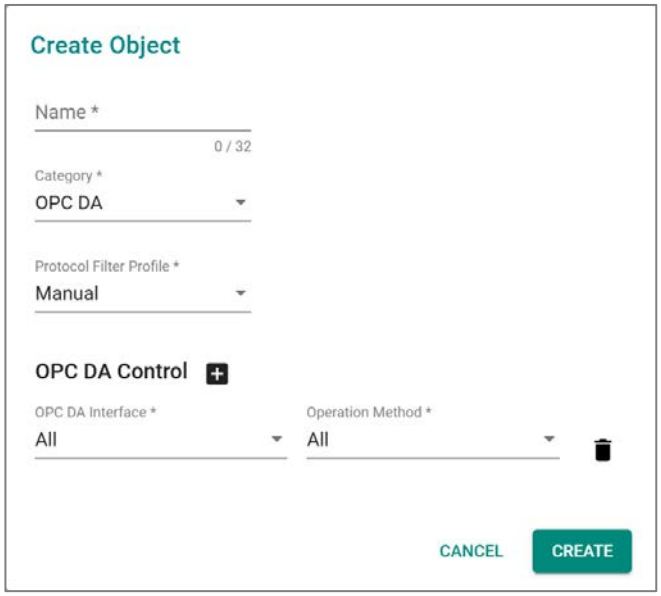
If **Step7Plus** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	1 to 64 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Protocol Filter Profile	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A
Function	Specify a Step7Plus function code for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A

Create Object - OPC DA

If **OPC DA** is selected for the **Category**, these settings will appear.

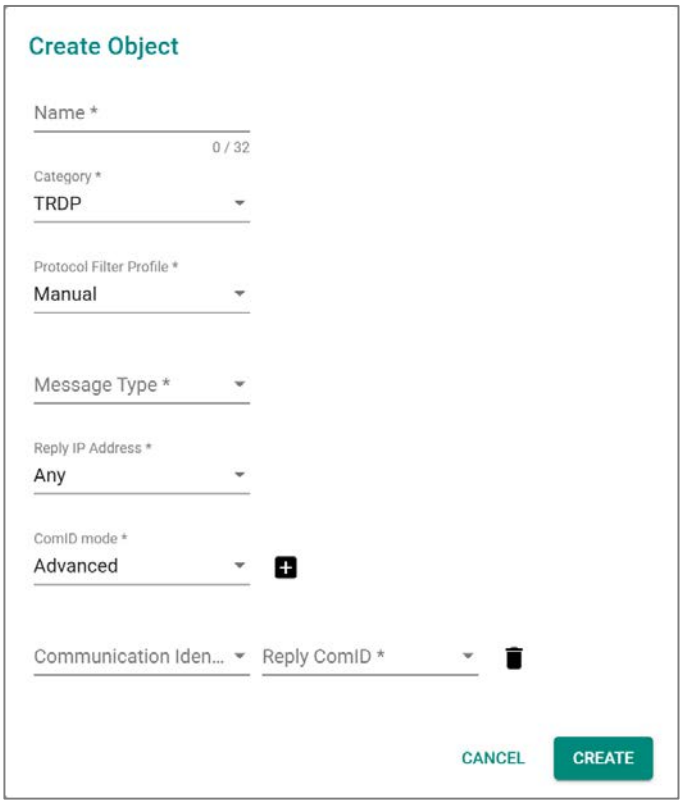


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Category	Select a protocol for this object.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A

UI Setting	Description	Valid Range	Default Value
Protocol Filter Profile	Select a preset protocol filter profile or **Manual** to define the OPC DA operations for this object. The preset profiles contain predefined combinations of OPC DA interfaces and operation methods, so you do not need to configure each operation individually. • **OPCDA_DataReadWrite:** Allow OPC DA clients to read and write process data. • **OPCDA_DataReadOnly:** Allow OPC DA clients to read process data without writing or modifying data values. • **OPCDA_ConfigReadOnly:** Allow OPC DA clients to view configuration-related information without modifying the configuration. • **OPCDA_ConfigReadWrite:** Allow OPC DA clients to view and modify configuration-related information. • **Manual:** Manually configure the OPC DA interfaces and operation methods for the object.	OPCDA_DataReadWrite / OPCDA_DataReadOnly / OPCDA_ConfigReadOnly / OPCDA_ConfigReadWrite / Manual	N/A
OPC DA Interface	Shows the OPC DA interfaces included in the selected **Protocol Filter Profile**. If **Protocol Filter Profile** is **Manual**, select the OPC DA interface to use for this object. Select **All** to include all supported OPC DA interfaces. Select the **Add (+)** button to add an OPC DA control entry. **Limitations** You can add up to 13 OPC DA control entries to an OPC DA protocol filter entry.	All / Drop-down list of supported OPC DA interfaces	Depends on the selected Protocol Filter Profile
Operation Method	Shows the operation methods included for the corresponding **OPC DA Interface** in the selected **Protocol Filter Profile**. If **Protocol Filter Profile** is **Manual**, select the operation methods to use for the selected OPC DA interface. Select **All** to include all operation methods supported by that interface. To select specific methods, deselect **All** before selecting the methods to use. Multiple methods can be selected.	All / Available operation methods for the selected OPC DA interface	Depends on the selected Protocol Filter Profile

Create Object - TRDP (TN Series)

If **TRDP** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the object.	1 to 32 characters	N/A
Category	Select a protocol for this object. **Note** Available settings will vary depending on your product model.	• **TN Series**: TRDP	N/A
Protocol Filter Profile	Select a preset protocol filter profile or a user-configured protocol filter profile to use for this protocol filter object. • **Manual**: Manually enter the settings for this object. Refer to TRDP Protocol Filter Profiles for more information on TRDP presets. Refer to Protocol Filter Profile for more information on creating protocol filter profiles.	Drop-down list of related protocol filter profiles / Manual	N/A

UI Setting	Description	Valid Range	Default Value
Message Type	Shows which message types will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which message types to use for this object. You can select multiple options. Refer to TRDP Message Types for more information.	Drop-down list of message types	Depends on the selected **Protocol Filter Profile**
Reply IP Address	Specify the reply IP address type to use.	Any / Single / Range / Subnet	Any
IP Address **(If Single is selected for Reply IP Address)**	Specify the IP address to use for the protocol filter object.	Valid IP Address	N/A
IP Address: From * **(If Range is selected for Reply IP Address)**	Specify the start of the IP range to use for the protocol filter object.	Valid IP Address	N/A
IP Address: To * **(If Range is selected for Reply IP Address)**	Specify the end of the IP range to use for the protocol filter object.	Valid IP Address	N/A
Subnet **(If Subnet is selected for Reply IP Address)**	Specify the IP address of the subnet to use for the protocol filter object.	Valid IP Address	N/A
Subnet Mask **(If Subnet is selected for Reply IP Address)**	Select the subnet mask to use for the protocol filter object.	Drop-down list of subnet masks	N/A

UI Setting	Description	Valid Range	Default Value
ComID Mode	Select whether to use **Basic** or **Advanced** ComID mode. • **Basic**: Only a communication identifier needs to be specified. • **Advanced**: You can specify multiple sets of communication identifiers and reply ComIDs. Select the **Add ( )** icon to add additional sets of information.	Basic / Advanced	Basic
Communication Identifier	Shows which communication identifiers will be used for the object, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, select which communication identifiers to use for this object. You can select multiple options. The last option in the list lets you add your own communication identifiers. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	Depends on the selected **Protocol Filter Profile**
Reply ComID **(If ComID Mode is selected for Advanced)**	Select which Reply ComID to use for this object. You can select multiple options. The last option in the list lets you add your own communication identifier. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	N/A

Edit Protocol Filter Object

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

Clicking the **Edit ( )** icon for an entry on the **Firewall > Advanced Protection > Configuration - Protocol Filter Object** page will open a dialog box that lets you edit the entry.

Click **APPLY** to save your changes.

For a complete list of settings, refer to Create Protocol Filter Object.

Delete Protocol Filter Object

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Object

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Protocol Filter Profile

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

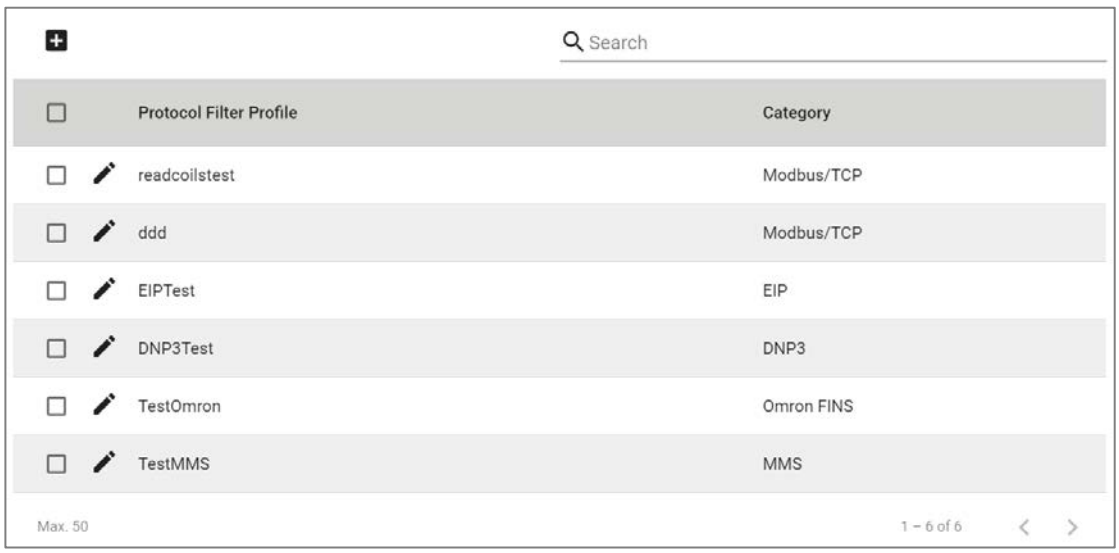
This page lets you create and manage protocol filter profiles to simplify maintaining protocol-related settings. Protocol filter profiles can be used when creating protocol filter objects, and a single profile can be used in multiple protocol filter objects.

Note

Available protocols may vary across different product models and versions.

Limitations

You can create up to 50 protocol filter profiles.



UI Setting	Description
Protocol Filter Profile	Shows the name of the profile.
Category	Shows the protocol category of the profile.

Create Protocol Filter Profile

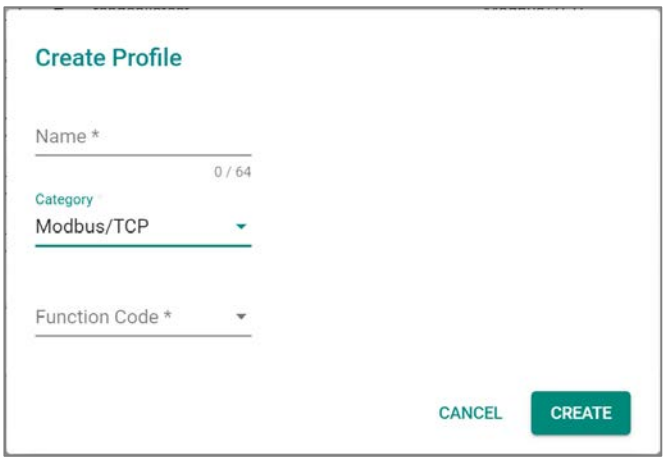
Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

Clicking the **Add (⊕)** icon on the **Firewall > Advanced Protection > Configuration - Protocol Filter Profile** page will open this dialog box. This dialog lets you create a protocol filter profile.

Click **CREATE** to save your changes and add the new profile.

Create Profile - Modbus/TCP

If **Modbus/TCP** is selected for the **Category**, these settings will appear.

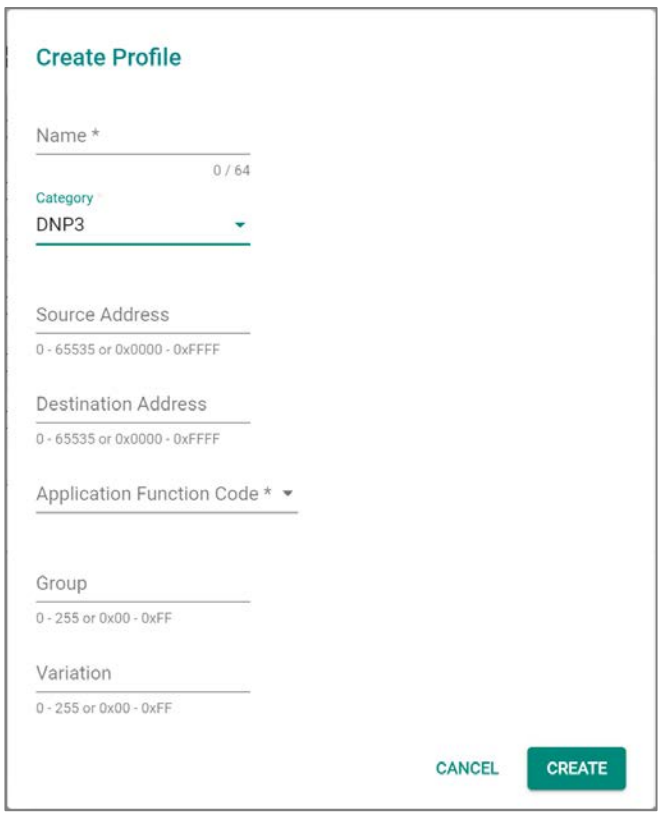


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Function Code	Select which function codes to use for this profile. You can select multiple options.	Drop-down list of function codes	N/A

Create Profile - DNP3

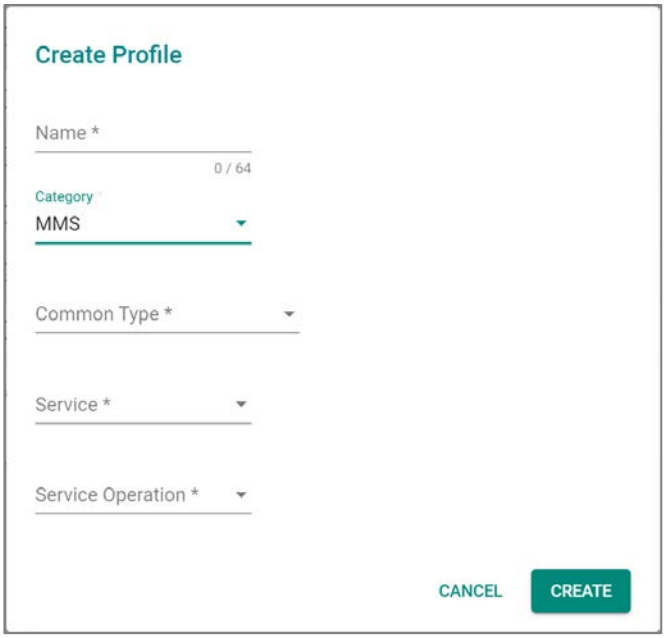
If **DNP3** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Source Address	Specify the source address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A
Destination Address	Specify the destination address to check for in DNP3 packets.	0 to 65535 / 0x0000 to 0xFFFF	N/A
Application Function Code	Select which function code to use for this profile.	Drop-down list of function codes	N/A
Group	Specify the function code to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A
Variation	Specify the variation to use for this profile.	0 to 255 or 0x00 to 0xFF	N/A

Create Profile - MMS

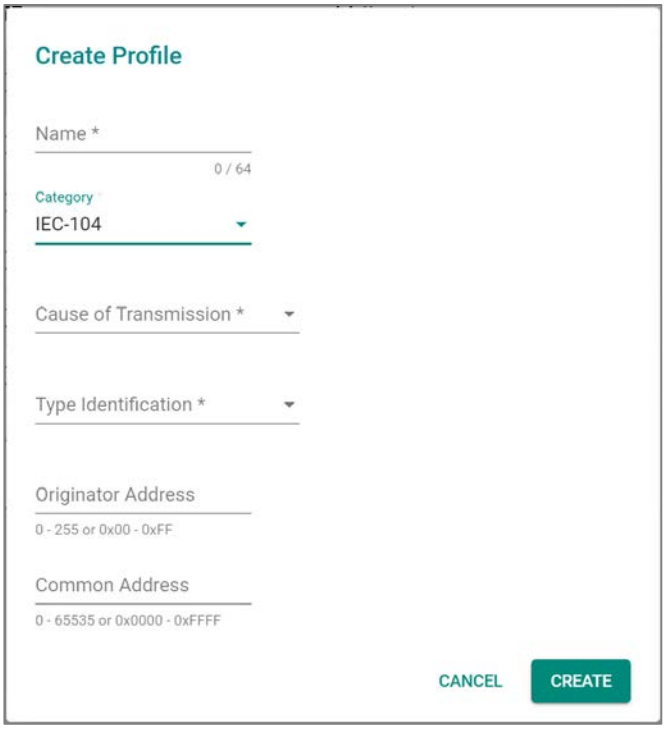
If **MMS** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Command Type	Select the command type to use for the profile. Refer to **MMS Command Types** for an overview of all command types.	Drop-down list of MMS command types	N/A
Service	Select the service to use for the profile.	Any / Confirmed Request / Confirmed Response / Unconfirmed	N/A
Service Operation	Select the service operations to use for the profile. You can select multiple options. Refer to **MMS Service Operation List** for an overview of all service operations.	Drop-down list of service operations	N/A

Create Profile - IEC-104

If **IEC-104** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Cause of Transmission	Select the IEC-104 cause of transmission code to use for the profile. Refer to the IEC-104 Cause of Transmission List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 cause of transmission codes	N/A

UI Setting	Description	Valid Range	Default Value
Type Identification	Select the IEC-104 type identification code to use for the profile. Refer to the IEC-104 Type Identification List for an overview of the different codes and corresponding descriptions.	Drop-down list of IEC-104 type identification codes	N/A
Originator Address	Specify the originator address to use for the profile.	0 to 255 / 0x00 to 0xFF	N/A
Common Address	Specify the common address to use for the profile.	0 to 65535 / 0x0000 to 0xFFFF	N/A

Create Profile - EIP-CIP (EDF/EDR/NAT/TN Series)

If **EIP** is selected for the **Category**, these settings will appear.

Select the **Add (⊞)** icon to add a CIP control.

Select the **Delete (🗑)** icon to delete the corresponding CIP control.

Limitations

You can add up to 8 CIP controls to an EIP-CIP protocol filter entry.

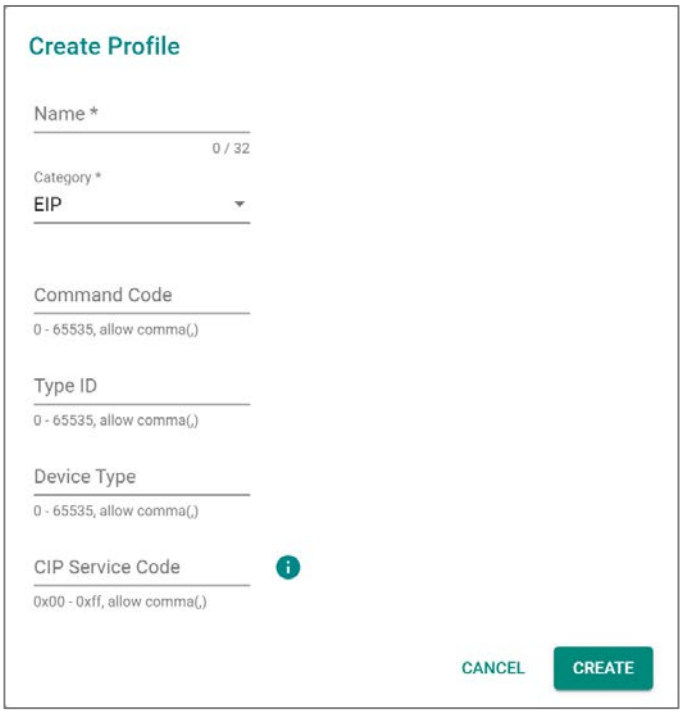
UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Strict Protection	Enable or disable Strict Protection, which controls how CIP Multiple Service Packets (0x0A) are handled. • **Enabled:** A Multiple Service Packet is allowed only when all included sub-services are read operations. If any sub-service contains a write operation, the entire packet is blocked. • **Disabled:** The additional check on all sub-services in a Multiple Service Packet is not applied.	Enabled / Disabled	Disabled

CIP Control

UI Setting	Description	Valid Range	Default Value
CIP Object	Shows the CIP objects that will be used for the CIP control, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the CIP objects to use for this object. Multiple values can be entered by separating them with commas. Refer to CIP Object List for an overview of the different CIP objects.	All / Drop-down list of CIP objects / 0x00 to 0xff	All
CIP Service Code	Shows the CIP service codes that will be used for the CIP control, based on the selected **Protocol Filter Profile**. If **Manual** is selected for the **Protocol Filter Profile**, manually specify the CIP service codes to use for this object. Multiple values can be entered by separating them with commas.	All / Drop-down list of CIP service codes based on the selected **CIP Object** / 0x00 to 0xff	All

Create Profile - EIP (OnCell Series)

If **EIP** is selected for the **Category**, these settings will appear.

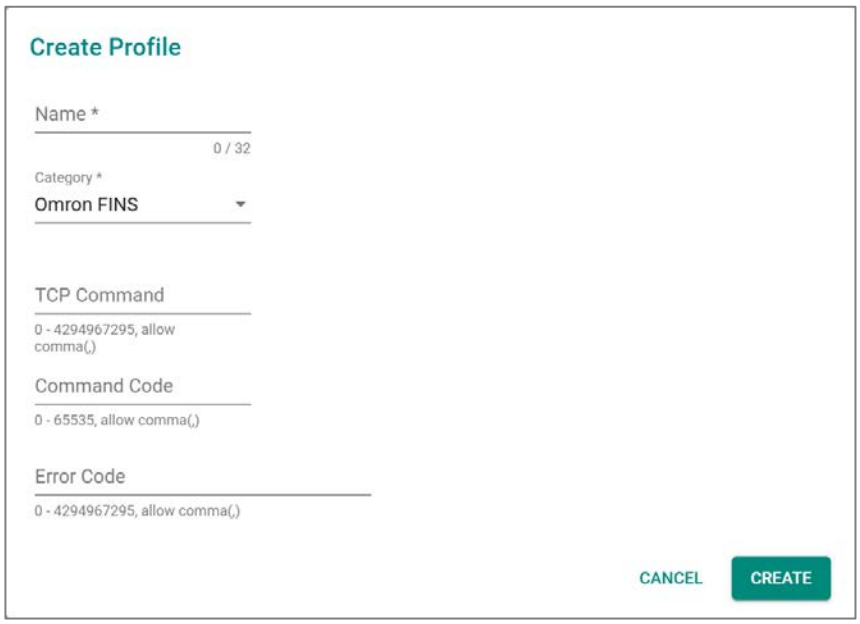


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Command Code	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Type ID	Specify the type IDs to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Device Type	Specify the device types to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

UI Setting	Description	Valid Range	Default Value
CIP Service Code	Specify the CIP service codes that will be used for the profile. Multiple values can be entered by separating them with commas.	0x00 to 0xff	N/A

Create Profile - Omron FINS

If **Omron FINS** is selected for the **Category**, these settings will appear.

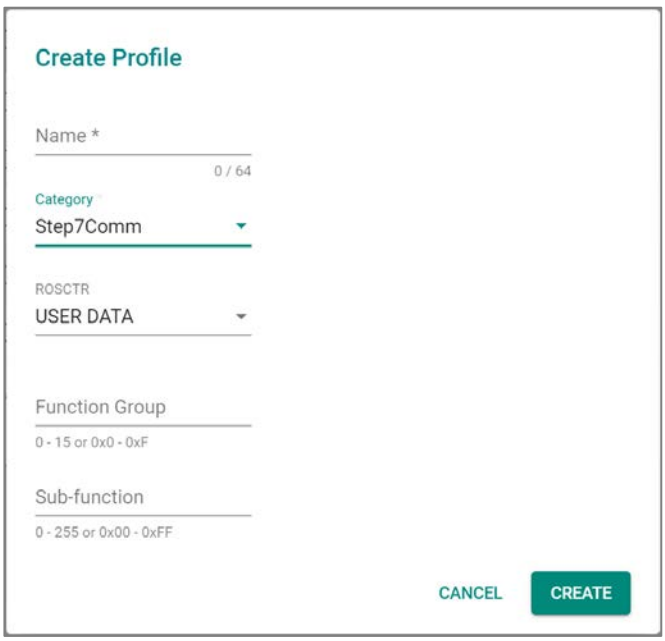


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
TCP Command	Specify the TCP command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 4294967295	N/A

UI Setting	Description	Valid Range	Default Value
Command Code	Specify the command codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A
Error Code	Specify the error codes to use for this profile. You can specify multiple values by separating them with a comma.	0 to 65535	N/A

Create Profile - Step7Comm

If **Step7Comm** is selected for the **Category**, these settings will appear.

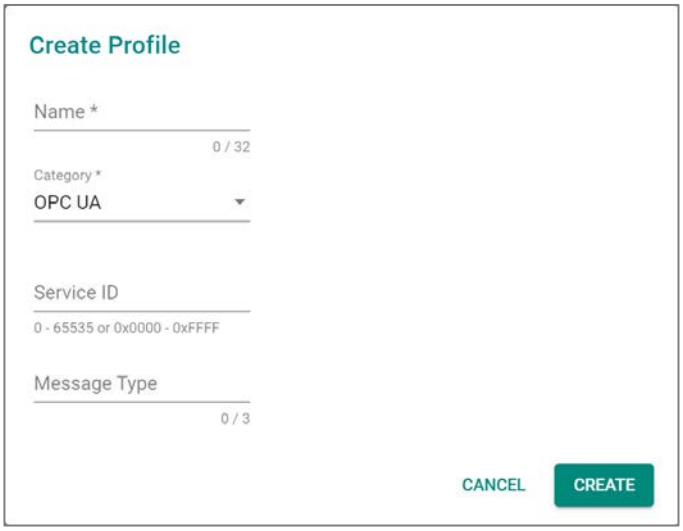


UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
ROSCTR	Specify the ROSCTR control to use for this profile.	ANY / JOB / USER DATA	N/A
Function **(If ROSCTR is JOB)**	Specify the function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A
Function Group **(If ROSCTR is USER DATA)**	Specify the function group to use for this profile.	0 to 15 / 0x0 to 0xF	N/A
Sub-function **(If ROSCTR is USER DATA)**	Specify the sub-function code to use for this profile.	0 to 255 / 0x00 to 0xFF	N/A

Create Profile - OPC UA

If **OPC UA** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 32 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Service ID	Specify an OPC UA Service ID for this profile.	0 to 4294967295 or 0x00000000 to 0xFFFFFFFF	N/A
Message Type	Specify the message type.	0 to 3 characters	N/A

Create Profile - MELSEC

If **MELSEC** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 32 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Command	Specify a command for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A
SUB-Command	Specify a sub-command for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A

Create Profile - Step7Plus

If **Step7Plus** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 32 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF/EDR/NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
Function	Specify a Step7Plus function code for this profile.	0 to 65535 or 0x0000 to 0xFFFF	N/A

Create Profile - OPC DA

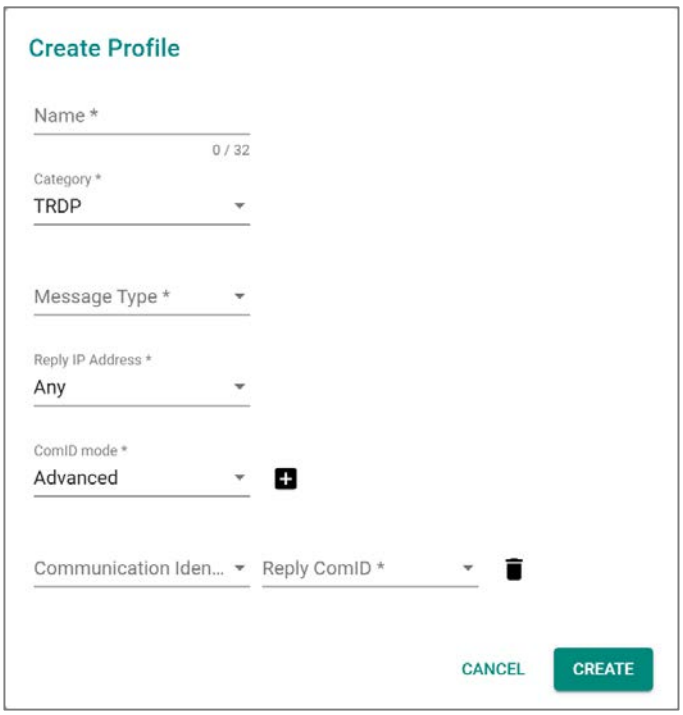
If **OPC DA** is selected for the **Category**, these settings will appear.

UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 32 characters	N/A
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **EDF / EDR / NAT Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP-CIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus / OPC DA • **OnCell Series**: Modbus/TCP / DNP3 / MMS / IEC-104 / EIP / Omron FINS / Step7Comm / OPC UA / MELSEC / Step7Plus	N/A
OPC DA Interface	Shows the OPC DA interfaces included in the selected **Protocol Filter Profile**. Select **All** to include all supported OPC DA interfaces. Select the **Add (+)** button to add an OPC DA control entry. **Limitations** You can add up to 13 OPC DA control entries to an OPC DA protocol filter entry.	All / Drop-down list of supported OPC DA interfaces	N/A

UI Setting	Description	Valid Range	Default Value
Operation Method	Shows the operation methods included for the corresponding **OPC DA Interface** in the selected **Protocol Filter Profile**. Select **All** to include all operation methods supported by that interface. To select specific methods, deselect **All** before selecting the methods to use. Multiple methods can be selected.	All / Available operation methods for the selected OPC DA interface	N/A

Create Profile - TRDP (TN Series)

If **TRDP** is selected for the **Category**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the profile.	1 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Category	Select a protocol for this profile. **Note** Available settings will vary depending on your product model.	• **TN Series**: TRDP	N/A
Message Type	Select which message types to use for this profile. You can select multiple options. Refer to TRDP Message Types for more information.	Drop-down list of message types	N/A
Reply IP Address	Default is Any which specifies all IP addresses.	Any / Single / Range / Subnet	Any
IP Address **(If Single is Reply IP Address)**	Specify the IP address to use for the protocol filter object.	Valid IP Address	N/A
IP Address: From * **(If Range is Reply IP Address)**	Specify the start of the IP range to use for the protocol filter object.	Valid IP Address	N/A
IP Address: To * **(If Range is Reply IP Address)**	Specify the end of the IP range to use for the protocol filter object.	Valid IP Address	N/A
Subnet **(If Subnet is Reply IP Address)**	Specify the IP address of the subnet to use for the protocol filter object.	Valid IP Address	N/A
Subnet Mask **(If Subnet is Reply IP Address)**	Select the subnet mask to use for the protocol filter object.	Drop-down list of subnet masks	N/A
ComID Mode	Select whether to use **Basic** or **Advanced** ComID mode. • **Basic**: Only a communication identifier needs to be specified. • **Advanced**: You can specify multiple sets of communication identifiers and reply ComIDs. Select the **Add ( )** icon to add additional sets of information.	Basic / Advanced	Basic

UI Setting	Description	Valid Range	Default Value
Communication Identifier	Select which communication identifiers to use for this profile. You can select multiple options. The last option in the list lets you add your own communication identifier. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	N/A
Reply ComID **(If ComID Mode is Advanced)**	Select which Reply ComID to use for this profile. You can select multiple options. The last option in the list lets you add your own communication identifier. You can specify multiple values by separating them with a comma. Refer to IEC 61375-2-3 Communication Identifiers for more information.	Drop-down list of communication identifiers 1 to 4294967295	N/A

Edit Protocol Filter Profile

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

Clicking the **Edit ( )** icon for an entry on the **Firewall > Advanced Protection > Configuration - Protocol Filter Profile** page will open a dialog box that lets you edit the entry.

Click **APPLY** to save your changes.

For a complete list of settings, refer to Create Protocol Filter Profile.

Delete Protocol Filter Profile

Menu Path: Firewall > Advanced Protection > Configuration - Protocol Filter Profile

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Protocol Filter Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

This page lets you manage your application firewall's protocol filtering policies, which allow you to inspect industrial protocol packets. This allows you to control protocol traffic

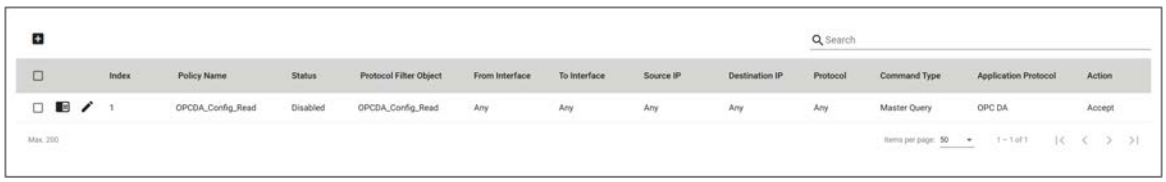
based on the configured protocol filter policies and Anomaly Detection and Protection (ADP) settings. Refer to ADP for more information.

Note

Before creating protocol filter policies, you will need to set up protocol filter objects to define what application protocols your policies will apply to. Refer to Protocol Filter Object for more information.

Limitations

You can create up to 200 protocol filter policies.



UI Setting	Description
Index	Shows the index of the policy.
Policy Name	Shows the name of the policy.
Status	Shows whether the policy is enabled or disabled.
Protocol Filter Object	Shows the protocol filter object used for the policy.
From Interface	Shows the From Interface for the policy.
To Interface	Shows the To Interface for the policy.
Source IP	Shows the source IP addresses for the policy.
Destination IP	Shows the destination IP addresses for the policy.
Protocol	Shows the protocols for the policy.
Command Type	Shows the packet transmission direction for this policy.
Application Protocol	Shows the industrial protocol for this policy.

UI Setting	Description
Action	Shows the action the firewall will take for packets that match the policy.

Add Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

Clicking the **Add (⊕)** icon on the **Firewall > Advanced Protection > Protocol Filter Policy** page will open this dialog box. This dialog lets you create a new protocol filter policy.

Click **CREATE** to save your changes and add the new policy.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of the policy.	1 to 200	1
Policy Name	Specify a name for the policy.	1 to 64 characters	N/A

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Disabled
From Interface	Select the From Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any
To Interface	Select the To Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any
Source IP	Select how the policy will check the packet's source IP address. • **Any:** The policy will check all source IP addresses in the packet. • **Single**: The policy will only check for the specified source IP address in the packet. • **Range**: The policy will check all source IP addresses in the packet within the specified IP range. • **Subnet:** The policy will check for source IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
Destination IP	To decide how the policy will check the packet's destination IP address. • **Any:** The policy will check all destination IP addresses in the packet. • **Single**: The policy will only check for the specified destination IP address in the packet. • **Range**: The policy will check all destination IP addresses in the packet within the specified IP range. • **Subnet:** The policy will check for destination IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
Protocol	Select the protocol for this policy.	Any / TCP / UDP	Any

UI Setting	Description	Valid Range	Default Value
Command Type	Select the packet transmission direction for this policy.	Master Query / Slave Response	Master Query
Application Protocol	Select the protocol filter object to use to define the application protocol for this policy. Refer to Protocol Filter Object for more information.	Custom object	N/A
Action	Select the action to take for packets that match the policy. • **Accept**: The firewall will accept packets that match the policy. • **Monitor**: The firewall will monitor packets that match the policy. With this setting, each packet of an identified application protocol will have a corresponding Event Log entry. • **Reset**: The firewall will drop packets that match the policy, and the session will be disconnected. With this setting, only the first packet of an identified application protocol will be recorded in Event Log.	Accept / Monitor / Reset	Accept

Edit Protocol Filter Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

Clicking the **Edit ( )** icon for an entry on the **Firewall > Advanced Protection > Protocol Filter Policy** page will open this dialog box. This dialog lets you edit the entry.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Index	Specify the index of the policy.	1 to 200	1
Policy Name	Specify a name for the policy.	1 to 64 characters	N/A
Status	Enable or disable the policy.	Enabled / Disabled	Disabled
From Interface	Select the From Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any

UI Setting	Description	Valid Range	Default Value
To Interface	Select the To Interface for the policy. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Any / Drop-down of interfaces	Any
Source IP	Select how the policy will check the packet's source IP address. • **Any:** The policy will check all source IP addresses in the packet. • **Single**: The policy will only check for the specified source IP address in the packet. • **Range**: The policy will check all source IP addresses in the packet within the specified IP range. • **Subnet:** The policy will check for source IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
Destination IP	To decide how the policy will check the packet's destination IP address. • **Any:** The policy will check all destination IP addresses in the packet. • **Single**: The policy will only check for the specified destination IP address in the packet. • **Range**: The policy will check all destination IP addresses in the packet within the specified IP range. • **Subnet:** The policy will check for destination IP addresses in the packet that are within the specified subnet mask.	Any / Single / Range / Subnet	Any
Protocol	Select the protocol for this policy.	Any / TCP / UDP	Any
Command Type	Select the packet transmission direction for this policy.	Master Query / Slave Response	Master Query
Application Protocol	Select the protocol filter object to use to define the application protocol for this policy. Refer to Protocol Filter Object for more information.	Custom object	N/A

UI Setting	Description	Valid Range	Default Value
Action	Select the action to take for packets that match the policy. • **Accept**: The firewall will accept packets that match the policy. • **Monitor**: The firewall will monitor packets that match the policy. With this setting, each packet of an identified application protocol will have a corresponding Event Log entry. • **Reset**: The firewall will drop packets that match the policy, and the session will be disconnected. With this setting, only the first packet of an identified application protocol will be recorded in Event Log.	Accept / Monitor / Reset	Accept

Delete Protocol Filter Policy

Menu Path: Firewall > Advanced Protection > Protocol Filter Policy

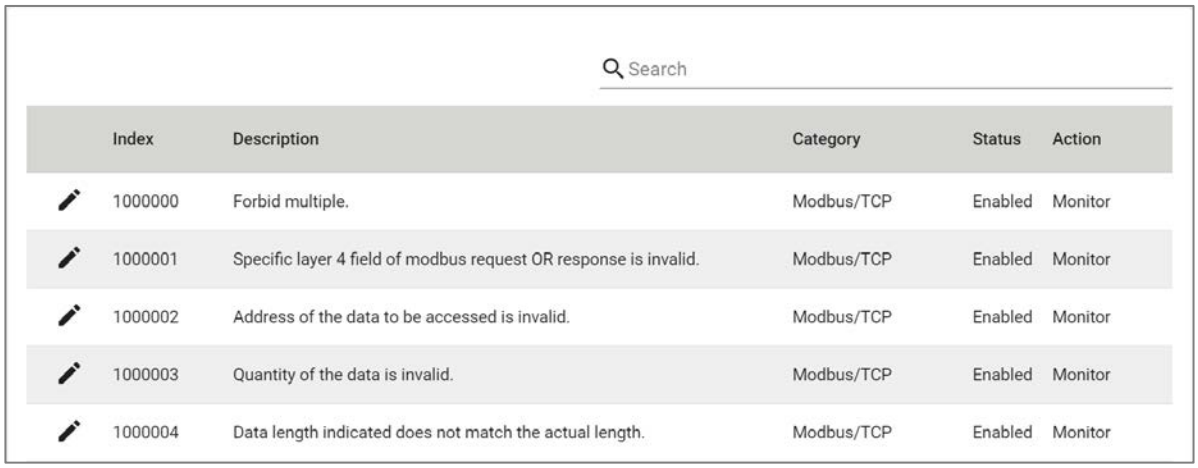
You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

ADP

Menu Path: Firewall > Advanced Protection > ADP

This page lets you configure your device's Anomaly Detection and Protection (ADP) parameters.

> **Note**
> Availability of this feature may vary depending on your product model and version.



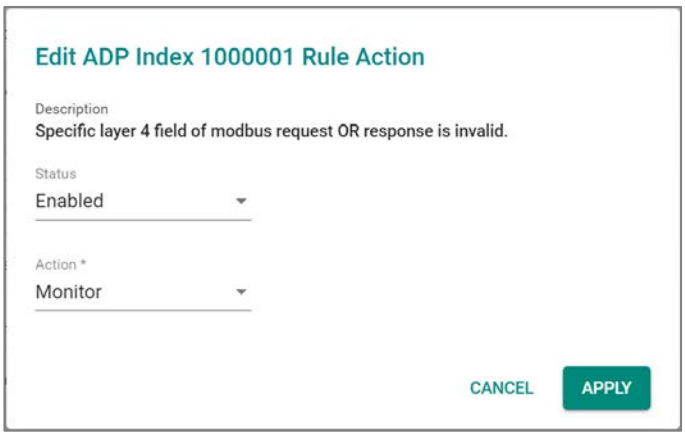
UI Setting	Description
Index	Shows the index of the ADP rule.
Description	Shows a description of the condition that will trigger the ADP rule.
Category	Shows the category of the ADP rule.
Status	Shows whether the ADP rule is enabled or disabled.
Action	Shows the action the application firewall will take when the ADP rule is matched.

Edit ADP Rule Action

Menu Path: Firewall > Advanced Protection > ADP

Clicking the **Edit ( )** icon for a rule on the **Firewall > Advanced Protection > ADP** page will open this dialog box. This dialog lets you modify an ADP rule.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Description (View-only)	Shows a description of the condition that will trigger the ADP rule.	N/A	N/A
Status	Enable or disable the ADP rule.	Enabled / Disabled	Enabled
Action	Select the action to take for packets that match the rule. • **Accept**: The firewall will accept packets that match the rule. • **Monitor**: The firewall will monitor packets that match the rule and an event log will be recorded in Event Log - Firewall Log. • **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

IPS

Menu Path: Firewall > Advanced Protection > IPS

This page lets you configure the Intrusion Prevention System (IPS) feature, which helps protect against cyberthreats by performing pattern-based detection and blocking known attacks.

Note

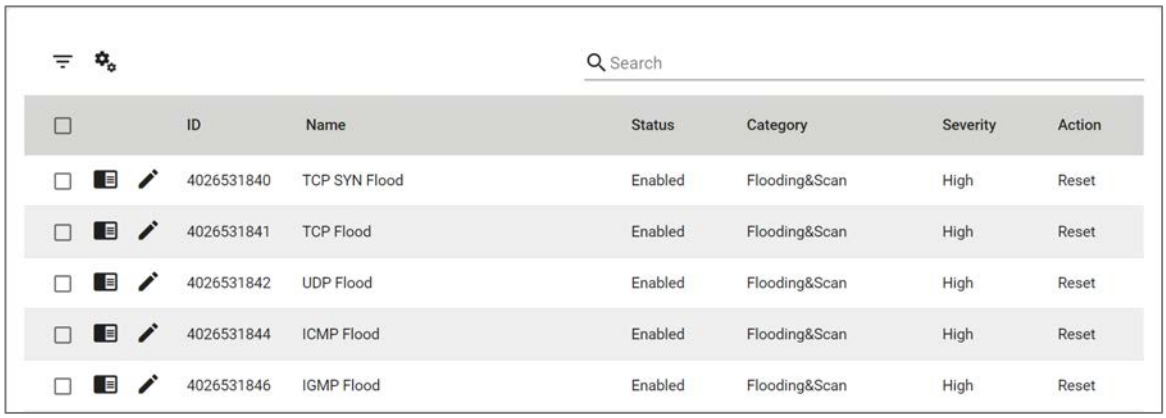
Availability of this feature may vary depending on your product model and version.

Note

A separate IPS license is required to enable IPS functionality on the device.

Note

Starting from v9.0 of the Network Security Package, when the IPS license expires, existing IPS patterns can still be used for IPS protection. However, the IPS patterns will not be updated and will remain at their current versions when you update the Network Security Package.



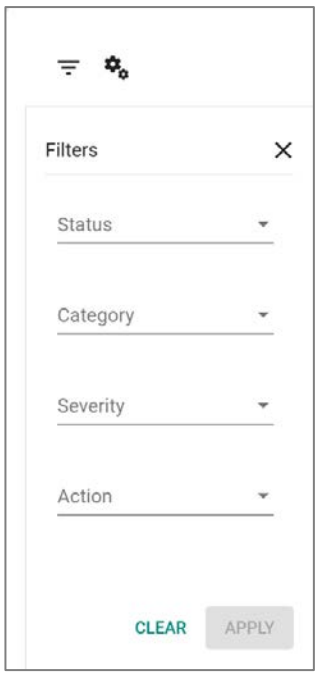
UI Setting	Description
ID	Shows the ID of the rule.
Name	Shows the name of the rule.
Status	Shows whether the rule is enabled or disabled.
Category	Shows the category of the rule.
Severity	Shows the severity assigned to the rule.
Action	Shows the action that will be taken when the rule is triggered.

Filter IPS Rules

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Filter ( )** icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you filter the IPS Rule List according to various criteria.

Click **APPLY** to apply the filter, or click **CLEAR** to reset all filter criteria.



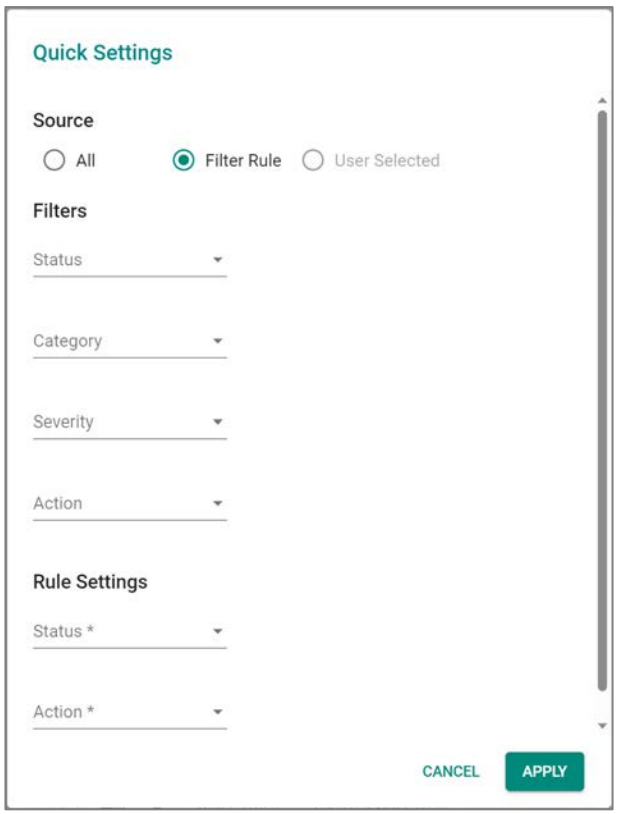
UI Setting	Description	Valid Range	Default Value
Status	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
Category	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
Severity	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
Action	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

Quick Settings

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Settings ( )** icon on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you quickly configure many rules at the same time.

Click **APPLY** to save your changes.



Source

UI Setting	Description	Valid Range	Default Value
Source	Select which rules to modify with the **Rule Settings** you specify. • **All**: Modify all rules. This option will not be available if you selected rules in the IPS Rule List before opening this dialog. • **Filter Rule**: Only modify rules that match the filter criteria you specify. This option will not be available if you selected rules in the IPS Rule List before opening this dialog. • **User Selected**: Only modify the rules that you have selected using their checkboxes. This option is only available if you select rules in the IPS Rule List before opening this dialog.	All / Filter Rule / User Selected	All

Filters

(If **Source** is **Filter Rule**)

UI Setting	Description	Valid Range	Default Value
Status	Filter for enabled or disabled rules.	Enabled / Disabled	N/A
Category	Filter for a specific rule category.	File vulnerabilities / Buffer Overflow / DoS attacks / Exploits / Malware traffic / Reconnaissance / Web threats / Flooding & Scan / Protocol Attack Protection / IP Spoofing	N/A
Severity	Filter for a specific severity level.	Information / Low / Medium / High / Critical	N/A
Action	Filter for a specific rule action.	Accept / Monitor / Reset	N/A

Rule Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the IPS rule.	Enabled / Disabled	Enabled

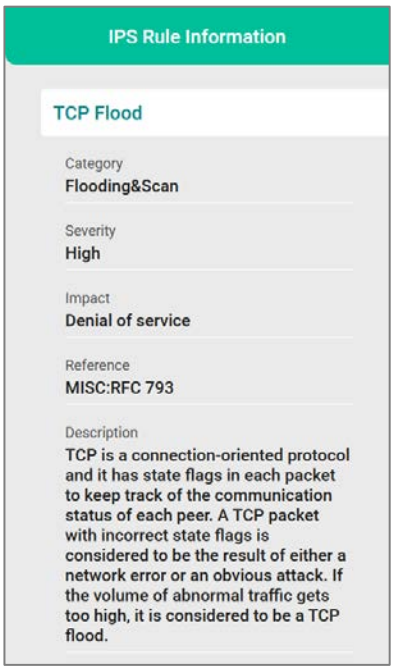
UI Setting	Description	Valid Range	Default Value
Action	Select the action to take for packets that match the rule. • **Accept**: The firewall will accept packets that match the rule. • **Monitor**: The firewall will monitor packets that match the rule. • **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

Detailed Information

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Detailed Information ( )** icon for a rule on the **Firewall > Advanced Protection > IPS** page will toggle display of a panel with detailed information about the rule.

IPS Rule Information



UI Setting	Description
Category	Shows the category of the attack.

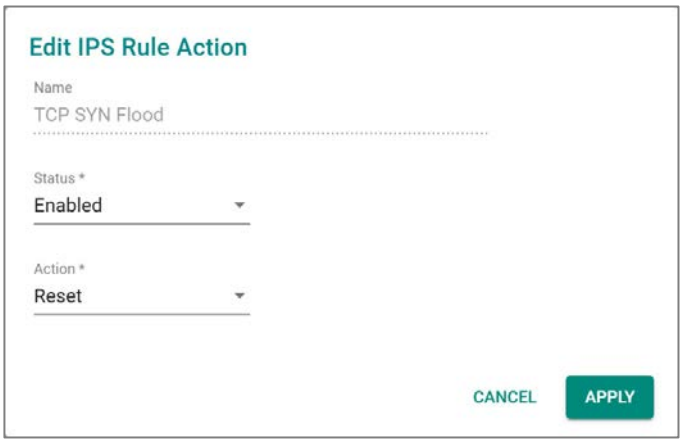
UI Setting	Description
Severity	Shows the severity assigned to the attack.
Impact	Shows the impact of the attack.
Reference	Shows the reference ID for more information about the attack, if available.
Description	Shows a description of the attack.

Edit IPS Rule Action

Menu Path: Firewall > Advanced Protection > IPS

Clicking the **Edit ( )** icon for a rule on the **Firewall > Advanced Protection > IPS** page will open this dialog box. This dialog lets you modify an IPS rule.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name (View-only)	Shows the name of the IPS rule.	N/A	N/A
Status	Enable or disable the IPS rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Action	Select the action to take for packets that match the rule. • **Accept**: The firewall will accept packets that match the rule. • **Monitor**: The firewall will monitor packets that match the rule. • **Reset**: The firewall will drop packets that match the rule, and the session will be disconnected.	Accept / Monitor / Reset	Monitor

Domain Protection

Menu Path: Firewall > Advanced Protection > Domain Protection

Use this page to configure domain protection by adding domain keywords to a denylist or allowlist to control URL access.

Note

This page lets you configure domain protection, but does not enable it.

To enable domain protection, refer to Global Settings for more information.

Limitations

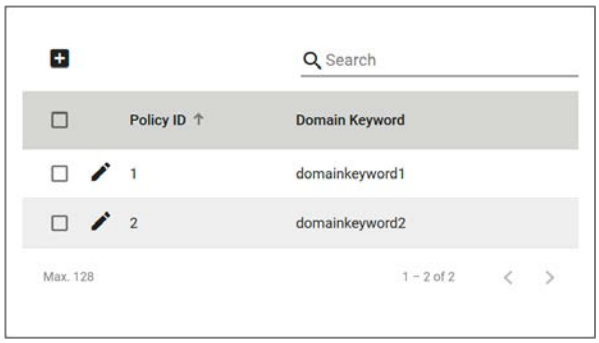
You can create up to 128 domain protection policies.

Protection Method

Global Settings

UI Setting	Description	Valid Range	Default Value
Protection Method	Specify which domain protection method to use. • **Denylist:** The device will block access to URLs that contain a keyword from the Domain Protection Policy List. Access to all other URLs will be allowed. • **Allowlist:** The device will only allow access to URLs that contain a keyword from the Domain Protection Policy List. Access to all other URLs will be blocked.	Denylist / Allowlist	Denylist

Domain Protection Policy List



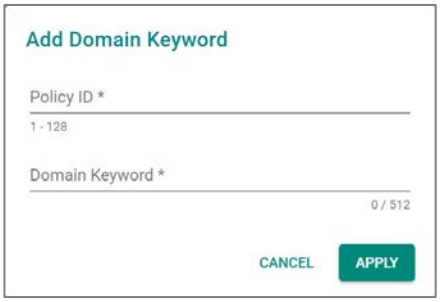
UI Setting	Description
Policy ID	Shows the ID of the policy.
Domain Keyword	Shows the domain keyword for the policy. • If the **Protection Method** is **Denylist,** access to URLs with this keyword in the domain will be blocked. • If the **Protection Method** is **Allowlist,** access to URLs with this keyword in the domain will be allowed.

Add Domain Keyword

Menu Path: Firewall > Advanced Protection > Domain Protection

Clicking the **Add (⊞)** icon on the **Firewall > Advanced Protection > Domain Protection** page will open this dialog box. This dialog lets you create a new domain keyword to use for Domain Protection.

Click **CREATE** to save your changes and add the new keyword.



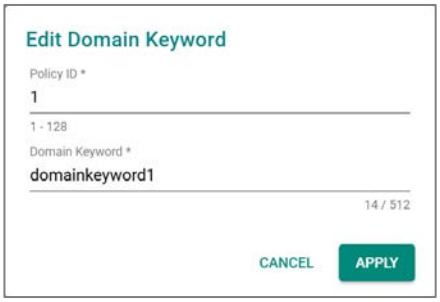
UI Setting	Description	Valid Range	Default Value
Policy ID	Specify an ID to help identify the policy.	1 to 128	N/A
Domain Keyword	Specify the domain keyword to use for this domain protection policy. **Note** Any URL request with the keyword in the domain of the address will be identified as a match. If the keyword is in the address, but not in the domain, it will not be counted as a match. For example, if "test" is the domain keyword: • test.website.com will be a match • www.test.com will be a match • www.website.com/test will not be a match	1 to 512 characters	N/A

Edit Domain Keyword

Menu Path: Firewall > Advanced Protection > Domain Protection

Clicking the **Edit ( )** icon for an entry on the **Firewall > Advanced Protection > Domain Protection** page will open this dialog box. This dialog lets you edit an existing entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Policy ID	Specify an ID to help identify the policy.	1 to 128	N/A
Domain Keyword	Specify the domain keyword to use for this domain protection policy. **Note** Any URL request with the keyword in the domain of the address will be identified as a match. If the keyword is in the address, but not in the domain, it will not be counted as a match. For example, if "test" is the domain keyword: • test.website.com will be a match • www.test.com will be a match • www.website.com/test will not be a match	1 to 512 characters	N/A

VPN

Menu Path: VPN

The VPN settings area lets you configure settings related to your device's VPN functionality.

This settings area includes these sections:

- IPSec
- OpenVPN Client
- L2TP Server

VPN - User Privileges

Privileges to VPN settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
IPSec	R/W	R/W	R
OpenVPN Client	R/W	R/W	-
L2TP Server	R/W	R/W	R

IPSec

Menu Path: VPN > IPSec

This page lets you set up IPSec VPN tunnels for your device.

This page includes these tabs:

- General
- IPSec Connections
- IPSec Status

IPSec - General

Menu Path: VPN > IPSec - General

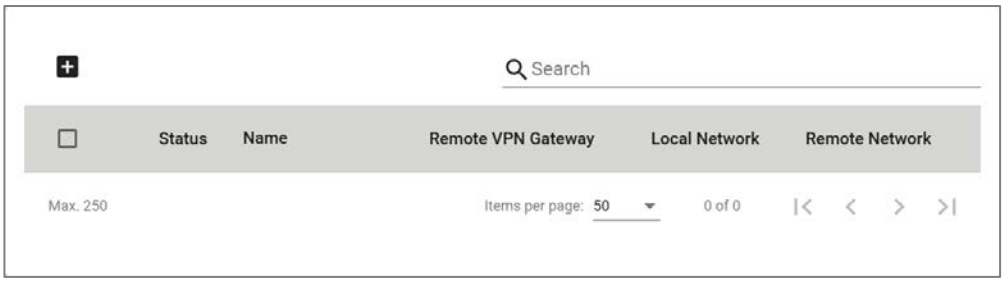
This page lets you configure global settings that affect all IPsec tunnels.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable all IPSec VPN services.	Enabled / Disabled	Disabled
IPSec NAT-T	Enable or disable IPSec NAT-T (NAT-Traversal). This option should be enabled if there is an external industrial secure router located between VPN tunnels.	Enabled / Disabled	Disabled
VPN Event Log	Enable or disable VPN event logging. Refer to Event Log for more information.	Enabled / Disabled	Disabled
Log Destination **(If VPN Event Log is Enabled)**	Specify where to send logs for this event. You can select multiple options. • **Local Storage**: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information.	Local Storage / Syslog / Trap	N/A

IPSec Connections

Menu Path: VPN > IPSec - IPSec Connections

This page lets you create and edit IPSec VPN tunnels for your device.



UI Setting	Description
Status	Shows whether the tunnel is enabled or disabled.
Name	Shows the name of the tunnel.
Remote VPN Gateway	Shows the IP address or domain name of the remote VPN gateway for the tunnel.
Local Network	Shows the tunnel's local network IP address.
Remote Network	Shows the tunnel's remote network IP address.

Create IPSec Connection

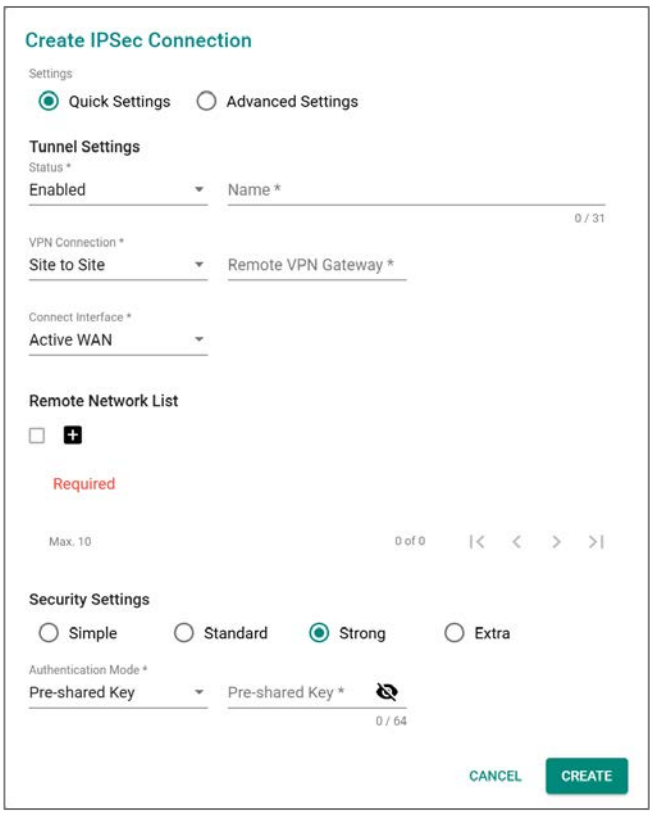
Menu Path: VPN > IPSec - IPSec Settings

Clicking the **Add (⊞)** icon on the **VPN > IPSec - IPSec Settings** page will open this dialog box. This dialog lets you create a new IPSec connection.

Click **CREATE** to save your changes and add the new connection.

Create IPSec Connection - Quick Settings

If **Quick Settings** is selected, these settings will appear.



Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled
Name	Enter a name for this tunnel. **Note** Names must start with a character that is not a number.	1 to 31 characters	N/A
VPN Connection	Select the type of VPN connection to use for this rule. • **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. • **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
Remote VPN Gateway	If **VPN Connection** is **Site to Site**, specify an IP address or domain name (FQDN) for the remote VPN gateway.	Valid IP address or domain name (FQDN)	N/A

UI Setting	Description	Valid Range	Default Value
Connect Interface	Specify a LAN or WAN interface to bind to the IPSec point-to-point tunnel.	Drop-down list of interfaces	TN-4900 Series: WAN Other models: Active WAN

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

Security Settings

<table>
<tr><th>UI Setting</th><th>Description</th><th>Valid Range</th><th>Default Value</th></tr>
<tr><td>Security Strength</td><td>Select the security strength for the tunnel. Different settings will change the Encryption Algorithm and Hash Algorithm used, which can be viewed in Advanced Settings.

Note
When creating an IPsec connection, it is highly recommended to use similar levels of algorithms between IPsec devices.

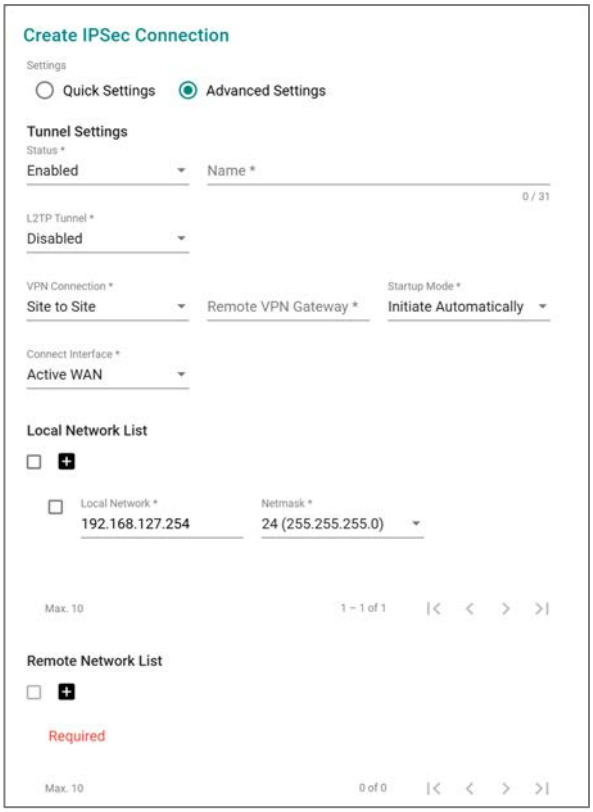
The different security levels use the following settings:

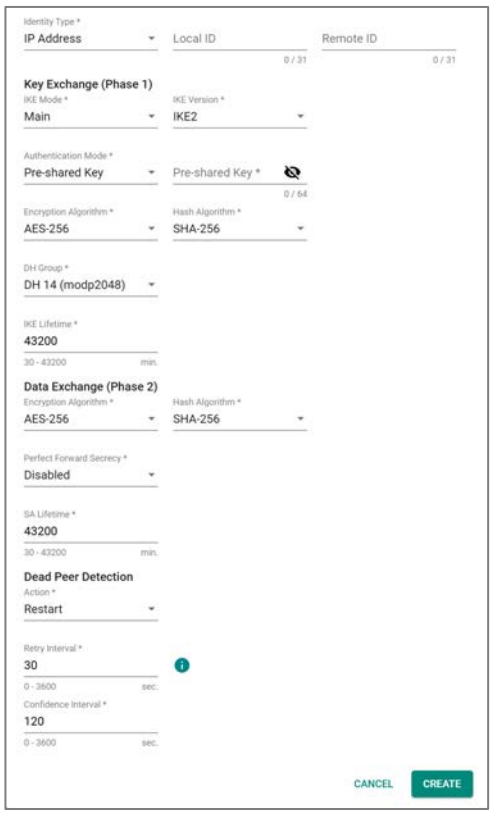
Key Exchange 1
<table><tr><th>Type</th><th>Simple</th><th>Standard</th><th>Strong</th><th>Extra</th></tr><tr><td>Encryption Algorithm</td><td>DES</td><td>3DES</td><td>AES-256</td><td>AES-256-GCM</td></tr><tr><td>Hash Algorithm</td><td>MD5</td><td>SHA-1</td><td>SHA-256</td><td>N/A</td></tr><tr><td>PRF</td><td>N/A</td><td>N/A</td><td>N/A</td><td>PRFSHA512</td></tr><tr><td>DH Group</td><td>DH1</td><td>DH2</td><td>DH14</td><td>DH31</td></tr></table>
Key Exchange 2
<table><tr><th>Type</th><th>Simple</th><th>Standard</th><th>Strong</th><th>Extra</th></tr><tr><td>Encryption Algorithm</td><td>DES</td><td>3DES</td><td>AES-256</td><td>AES-256-GCM</td></tr><tr><td>Hash</td><td>MD5</td><td>SHA-1</td><td>SHA-256</td><td>N/A</td></tr><tr><td>PRF</td><td>N/A</td><td>N/A</td><td>N/A</td><td>prfsha512</td></tr></table></td><td>Simple / Standard / Strong / Extra</td><td>Strong</td></tr>
</table>

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select X.509 or X.509 With CA. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. • **X.509**: The local and remote systems will authenticate the VPN connection using local certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. • **X.509 With CA**: The local and remote systems will authenticate the VPN connection using a local certificate imported in advance by the user on the **Certificate Management > Local Certificate** page, and a CA certificate (for the CA that issued the local certificate) imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key **(If Authentication Mode is Pre-shared Key)**	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	1 to 64 characters	N/A
Local **(If Authentication Mode is X.509 or X.509 With CA)**	Select the certificate to use for local authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A
Remote **(If Authentication Mode is X.509)**	Select the certificate to use for remote authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A

Create IPSec Connection - Advanced Settings

If **Advanced Settings** is selected, these settings will appear.





Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled
Name	Enter a name for this tunnel. **Note** Names must start with a character that is not a number.	1 to 31 characters	N/A
L2TP Tunnel	Enable or disable L2TP over IPSec.	Enabled / Disabled	Disabled
VPN Connection	Select the type of VPN connection to use for this rule. • **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. • **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site

UI Setting	Description	Valid Range	Default Value
Remote VPN Gateway	If **VPN Connection** is **Site to Site**, specify an IP address or domain name (FQDN) for the remote VPN gateway.	Valid IP address or domain name (FQDN)	N/A
Startup Mode	Select a startup mode for the tunnel. • **Initiate Automatically:** The VPN tunnel will actively initiate the connection with the remote VPN gateway to ensure the tunnel is always ready. • **Wait for Connection**: The VPN tunnel will wait for the remote VPN gateway to initiate the connection. • **Route Mode**: The VPN tunnel will only initiate a connection when routing packets are generated, and relies on traffic to trigger the tunnel.	Initiate Automatically / Wait for Connection / Route Mode	Initiate Automatically
Connect Interface	Specify a LAN or WAN interface to bind to the IPSec point-to-point tunnel.	Drop-down list of interfaces	TN-4900 Series: WAN Other models: Active WAN

Local Network List

You can configure multiple local networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 local networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Local Network	Specify the IP address and subnet mask of the local VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the local network.	Drop-down list of netmasks	24 (255.255.255.0)

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

Identity

UI Setting	Description	Valid Range	Default Value
Identity Type	Select an ID type to use to identify VPN tunnel connections. • **IP Address**: Use an IP address. • **FQDN**: Use a Fully Qualified Domain Name (FQDN). • **Key ID**: Use a user-defined key ID string. • **Auto(with Cisco)**: Use this when establishing connections to Cisco systems.	IP Address / FQDN / Key ID / Auto(with Cisco)	IP Address
Local ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the local ID for identifying the VPN tunnel connection. The Local ID must be identical to the Remote ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A
Remote ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the remote ID for identifying the VPN tunnel connection. The Remote ID must be identical to the Local ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A

Key Exchange (Phase 1)

UI Setting	Description	Valid Range	Default Value
IKE Mode	Select the IKE mode to use for authentication. • **Main**: Both the remote and local VPN gateway will negotiate which encryption/hash algorithm and DH groups can be used for this VPN tunnel. Both VPN gateways must use the same algorithm to communicate. • **Aggressive**: The remote and local VPN gateways will not negotiate the algorithm and will only use the user-defined configuration.	Main / Aggressive	Main
IKE Version	Select which version of IKE to use. **Note** When using IKEv1 with Main mode in a site-to-any configuration, using multiple pre-shared keys (PSKs) may cause VPN connection failures. In such cases, IKEv2 is the recommended option for proper compatibility and establishing reliable tunnels. • **IKE1**: Use IKE Version 1 protocol. • **IKE2**: Use IKE Version 2 protocol.	IKE1 / IKE2	IKE2

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select X.509 or X.509 With CA. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. • **X.509**: The local and remote systems will authenticate the VPN connection using local certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. • **X.509 With CA**: The local and remote systems will authenticate the VPN connection using a local certificate imported in advance by the user on the **Certificate Management > Local Certificate** page, and a CA certificate (for the CA that issued the local certificate) imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key **(If Authentication Mode is Pre-shared Key)**	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	1 to 64 characters	N/A
Local **(If Authentication Mode is X.509 or X.509 With CA)**	Select the certificate to use for local authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A

UI Setting	Description	Valid Range	Default Value
Remote **(If Authentication Mode is X.509)**	Select the certificate to use for remote authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A
Encryption Algorithm	Select the encryption algorithm to use for key exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
Hash Algorithm **(If Encryption Algorithm is not AES-256-GCM)**	Select the hash algorithm to use for key exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
PRF **(If Encryption Algorithm is AES-256-GCM)**	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
DH Group	Select the Diffie-Hellman group. This is the key exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14(modp2048)
IKE Lifetime	Specify the lifetime (in minutes) for IKE SA.	30 to 43200	43200

Data Exchange (Phase 2)

UI Setting	Description	Valid Range	Default Value
Encryption Algorithm	Select the encryption algorithm to use for data exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256

UI Setting	Description	Valid Range	Default Value
Hash Algorithm **(If Encryption Algorithm is not AES-256-GCM)**	Select the hash algorithm to use for data exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
PRF **(If Encryption Algorithm is AES-256-GCM)**	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
Perfect Forward Secrecy	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Enabled / Disabled	Disabled
DH Group **(If Perfect Forward Secrecy is Enabled)**	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14 (modp2048)
SA Lifetime	Specify the lifetime (in minutes) for Phase 2 IKE SA.	30 to 43200	43200

Dead Peer Detection

UI Setting	Description	Valid Range	Default Value
Action	Specify the action the system should take when a dead peer is detected. • **Hold**: Maintain the VPN tunnel. • **Restart**: Reconnect the VPN tunnel. • **Clear**: Clear the VPN tunnel. • **Disabled**: Disable Dead Peer Detection.	Hold / Restart / Clear / Disabled	Restart
Retry Interval	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	0 to 3600	30

UI Setting	Description	Valid Range	Default Value
Confidence Interval	Specify the interval (in seconds) at which the system will check to see if the connection is alive or not.	0 to 3600	120

Edit IPSec Connection

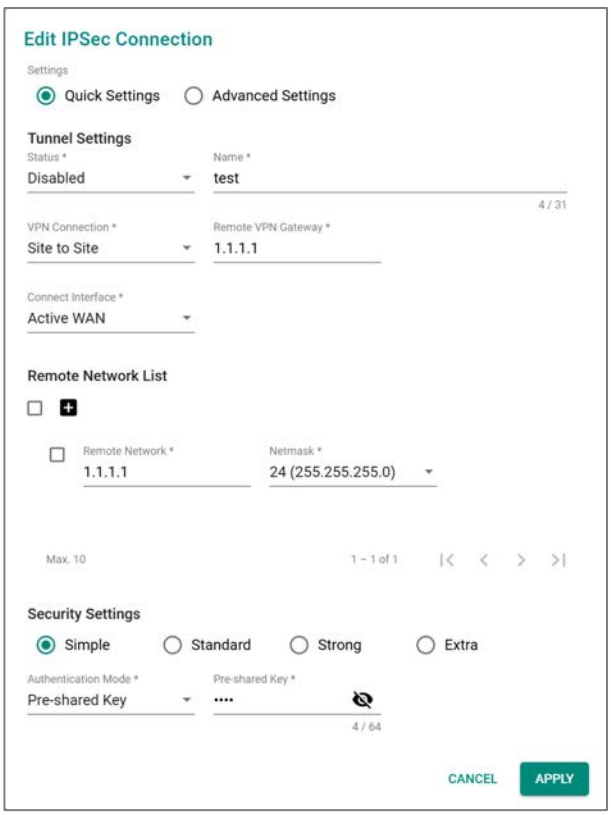
Menu Path: VPN > IPSec - IPSec Settings

Clicking the **Edit ( )** icon for an entry on the **VPN > IPSec - IPSec Settings** page will open this dialog box. This dialog lets you edit an existing IPSec connection.

Click **APPLY** to save your changes.

Edit IPSec Connection - Quick Settings

If **Quick Settings** is selected, these settings will appear.



Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled
Name	Enter a name for this tunnel. **Note** Names must start with a character that is not a number.	1 to 31 characters	N/A
VPN Connection	Select the type of VPN connection to use for this rule. • **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. • **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site
Remote VPN Gateway	If **VPN Connection** is **Site to Site**, specify an IP address or domain name (FQDN) for the remote VPN gateway.	Valid IP address or domain name (FQDN)	N/A
Connect Interface	Specify a LAN or WAN interface to bind to the IPSec point-to-point tunnel.	Drop-down list of interfaces	TN-4900 Series: WAN Other models: Active WAN

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

Security Settings

UI Setting	Description	Valid Range	Default Value
Security Strength	Select the security strength for the tunnel. Different settings will change the **Encryption Algorithm** and **Hash Algorithm** used, which can be viewed in **Advanced Settings**. **Note** When creating an IPsec connection, it is highly recommended to use similar levels of algorithms between IPsec devices. The different security levels use the following settings: **Key Exchange 1** **Key Exchange 2**	Simple / Standard / Strong / Extra	Strong

Key Exchange 1

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash Algorithm	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	PRFSHA512
DH Group	DH1	DH2	DH14	DH31

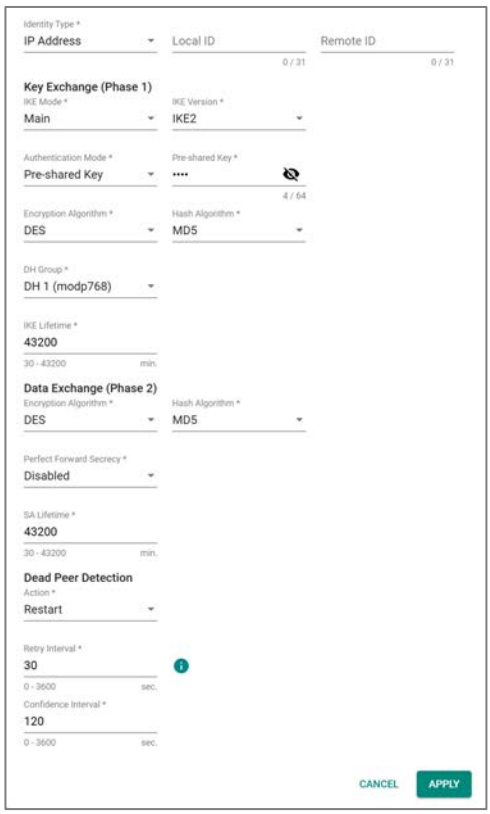
Key Exchange 2

Type	Simple	Standard	Strong	Extra
Encryption Algorithm	DES	3DES	AES-256	AES-256-GCM
Hash	MD5	SHA-1	SHA-256	N/A
PRF	N/A	N/A	N/A	prfsha512

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select X.509 or X.509 With CA. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. • **X.509**: The local and remote systems will authenticate the VPN connection using local certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. • **X.509 With CA**: The local and remote systems will authenticate the VPN connection using a local certificate imported in advance by the user on the **Certificate Management > Local Certificate** page, and a CA certificate (for the CA that issued the local certificate) imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key **(If Authentication Mode is Pre-shared Key)**	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	1 to 64 characters	N/A
Local **(If Authentication Mode is X.509 or X.509 With CA)**	Select the certificate to use for local authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A
Remote **(If Authentication Mode is X.509)**	Select the certificate to use for remote authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A

Edit IPSec Connection - Advanced Settings

If **Advanced Settings** is selected, these settings will appear.



Tunnel Settings

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the tunnel.	Enabled / Disabled	Enabled
Name	Enter a name for this tunnel. **Note** Names must start with a character that is not a number.	1 to 31 characters	N/A
L2TP Tunnel	Enable or disable L2TP over IPSec.	Enabled / Disabled	Disabled
VPN Connection	Select the type of VPN connection to use for this rule. • **Site to Site**: The VPN tunnel for the Local and Remote subnets is fixed. • **Site to Site(Any)**: The VPN tunnel for the Remote subnet area is dynamic and is fixed for the Local subnet.	Site to Site / Site to Site(Any)	Site to Site

UI Setting	Description	Valid Range	Default Value
Remote VPN Gateway	If **VPN Connection** is **Site to Site**, specify an IP address or domain name (FQDN) for the remote VPN gateway.	Valid IP address or domain name (FQDN)	N/A
Startup Mode	Select a startup mode for the tunnel. • **Initiate Automatically:** The VPN tunnel will actively initiate the connection with the remote VPN gateway to ensure the tunnel is always ready. • **Wait for Connection**: The VPN tunnel will wait for the remote VPN gateway to initiate the connection. • **Route Mode**: The VPN tunnel will only initiate a connection when routing packets are generated, and relies on traffic to trigger the tunnel.	Initiate Automatically / Wait for Connection / Route Mode	Initiate Automatically
Connect Interface	Specify a LAN or WAN interface to bind to the IPSec point-to-point tunnel.	Drop-down list of interfaces	TN-4900 Series: WAN Other models: Active WAN

Local Network List

You can configure multiple local networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 local networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Local Network	Specify the IP address and subnet mask of the local VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the local network.	Drop-down list of netmasks	24 (255.255.255.0)

Remote Network List

You can configure multiple remote networks for the tunnel. Click the add icon ( ) to add a new entry. Select an entry and click the delete icon ( ) to delete it.

Limitations

You can add up to 10 remote networks for an IPSec VPN tunnel.

UI Setting	Description	Valid Range	Default Value
Remote Network	Specify the IP address and subnet mask of the remote VPN network.	Valid IP address	N/A
Netmask	Select a netmask to use for the remote network.	Drop-down list of netmasks	24 (255.255.255.0)

Identity

UI Setting	Description	Valid Range	Default Value
Identity Type	Select an ID type to use to identify VPN tunnel connections. • **IP Address**: Use an IP address. • **FQDN**: Use a Fully Qualified Domain Name (FQDN). • **Key ID**: Use a user-defined key ID string. • **Auto(with Cisco)**: Use this when establishing connections to Cisco systems.	IP Address / FQDN / Key ID / Auto(with Cisco)	IP Address
Local ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the local ID for identifying the VPN tunnel connection. The Local ID must be identical to the Remote ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A
Remote ID **(If Identity Type is IP Address, FQDN, or Key ID)**	Specify the remote ID for identifying the VPN tunnel connection. The Remote ID must be identical to the Local ID of the connected VPN gateway in order to successfully establish the VPN tunnel connection.	1 to 31 characters	N/A

Key Exchange (Phase 1)

UI Setting	Description	Valid Range	Default Value
IKE Mode	Select the IKE mode to use for authentication. • **Main**: Both the remote and local VPN gateway will negotiate which encryption/hash algorithm and DH groups can be used for this VPN tunnel. Both VPN gateways must use the same algorithm to communicate. • **Aggressive**: The remote and local VPN gateways will not negotiate the algorithm and will only use the user-defined configuration.	Main / Aggressive	Main
IKE Version	Select which version of IKE to use. **Note** When using IKEv1 with Main mode in a site-to-any configuration, using multiple pre-shared keys (PSKs) may cause VPN connection failures. In such cases, IKEv2 is the recommended option for proper compatibility and establishing reliable tunnels. • **IKE1**: Use IKE Version 1 protocol. • **IKE2**: Use IKE Version 2 protocol.	IKE1 / IKE2	IKE2

UI Setting	Description	Valid Range	Default Value
Authentication Mode	Select the authentication mode to use for the tunnel. **Note** You must have certificates already imported to select X.509 or X.509 With CA. Refer to Certificate Management for more information. **Pre-Shared Key**: Pre-Shared Key is a user-defined authentication string used by two systems to establish an IPsec VPN connection. • **X.509**: The local and remote systems will authenticate the VPN connection using local certificates imported in advance by the user on the **Certificate Management > Local Certificate** page. • **X.509 With CA**: The local and remote systems will authenticate the VPN connection using a local certificate imported in advance by the user on the **Certificate Management > Local Certificate** page, and a CA certificate (for the CA that issued the local certificate) imported on the **Certificate Management > Trusted CA Certificate** page.	Pre-Shared Key / X.509 / X.509 With CA	Pre-Shared Key
Pre-Shared Key **(If Authentication Mode is Pre-shared Key)**	Specify a pre-shared key to use to authenticate the IPSec VPN connection.	1 to 64 characters	N/A
Local **(If Authentication Mode is X.509 or X.509 With CA)**	Select the certificate to use for local authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A

UI Setting	Description	Valid Range	Default Value
Remote **(If Authentication Mode is X.509)**	Select the certificate to use for remote authentication. **Note** You must import a certificate before you can select it from the drop-down box. Refer to Local Certificate for more information.	Drop-down list of certificates	N/A
Encryption Algorithm	Select the encryption algorithm to use for key exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256
Hash Algorithm **(If Encryption Algorithm is not AES-256-GCM)**	Select the hash algorithm to use for key exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
PRF **(If Encryption Algorithm is AES-256-GCM)**	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
DH Group	Select the Diffie-Hellman group. This is the key exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14(modp2048)
IKE Lifetime	Specify the lifetime (in minutes) for IKE SA.	30 to 43200	43200

Data Exchange (Phase 2)

UI Setting	Description	Valid Range	Default Value
Encryption Algorithm	Select the encryption algorithm to use for data exchange.	DES / 3DES / AES-128 / AES-192 / AES-256 / AES-256-GCM	AES-256

UI Setting	Description	Valid Range	Default Value
Hash Algorithm **(If Encryption Algorithm is not AES-256-GCM)**	Select the hash algorithm to use for data exchange.	MD5 / SHA-1 / SHA-256 / SHA-512	SHA-256
PRF **(If Encryption Algorithm is AES-256-GCM)**	Select the PRF algorithm for AES-256-GCM.	PRFSHA256 / PRFSHA384 / PRFSHA512	PRFSHA256
Perfect Forward Secrecy	Enable or disable Perfect Forward Secrecy. When enabled, different security keys are used for different IPsec phases in order to enhance security.	Enabled / Disabled	Disabled
DH Group **(If Perfect Forward Secrecy is Enabled)**	Select the Diffie-Hellman group. This is the Key Exchange group between the remote and VPN gateways.	DH 1(modp768) / DH 2(modp1024) / DH 5(modp1536) / DH 14(modp2048) /DH15 (modp3072) / DH16 (modp4096) / DH17 (modp6144) / DH18 (modp8192) / DH22 (modp1024s160) / DH23 (modp2048s224) / DH24 (modp2048s256) / DH31 (curve25519)	DH 14 (modp2048)
SA Lifetime	Specify the lifetime (in minutes) for Phase 2 IKE SA.	30 to 43200	43200

Dead Peer Detection

UI Setting	Description	Valid Range	Default Value
Action	Specify the action the system should take when a dead peer is detected. • **Hold**: Maintain the VPN tunnel. • **Restart**: Reconnect the VPN tunnel. • **Clear**: Clear the VPN tunnel. • **Disabled**: Disable Dead Peer Detection.	Hold / Restart / Clear / Disabled	Restart
Retry Interval	Specify the interval (in seconds) at which Dead Peer Detection messages are sent.	0 to 3600	30

UI Setting	Description	Valid Range	Default Value
Confidence Interval	Specify the interval (in seconds) at which the system will check to see if the connection is alive or not.	0 to 3600	120

Delete IPSec Connection

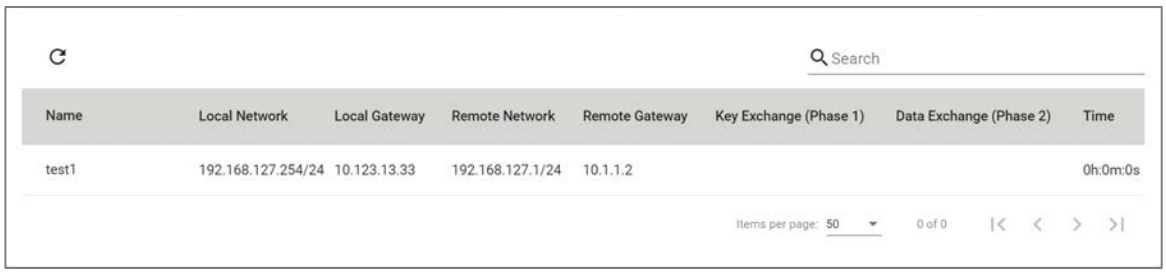
Menu Path: VPN > IPSec - IPSec Settings

You can delete tunnels by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

IPSec Status

Menu Path: VPN > IPSec - IPSec Status

This page lets you see the status of your IPSec VPN tunnels.



UI Setting	Description
Name	Shows the name of the tunnel.
Local Network	Shows the local network address for the tunnel.
Local Gateway	Shows the local gateway address for the tunnel.
Remote Network	Shows the remote network address for the tunnel.
Remote Gateway	Shows the remote gateway address for the tunnel.
Key Exchange (Phase 1)	Shows the status of key exchange phase.
Data Exchange (Phase 2)	Shows the status of the data exchange phase.
Time	Shows how long the connection has been up.

OpenVPN Client

Menu Path: VPN > OpenVPN Client

This page lets you manage the OpenVPN Client feature of your device.

> **Note**
>
> Availability of this feature may vary depending on your product model and version.

> **Note**
>
> For models with WAN redundancy, such as the EDR-G9004, running the OpenVPN client under WAN redundancy mode currently only supports failover, not failback. This means the device will not automatically switch back to the primary connection once it is restored.

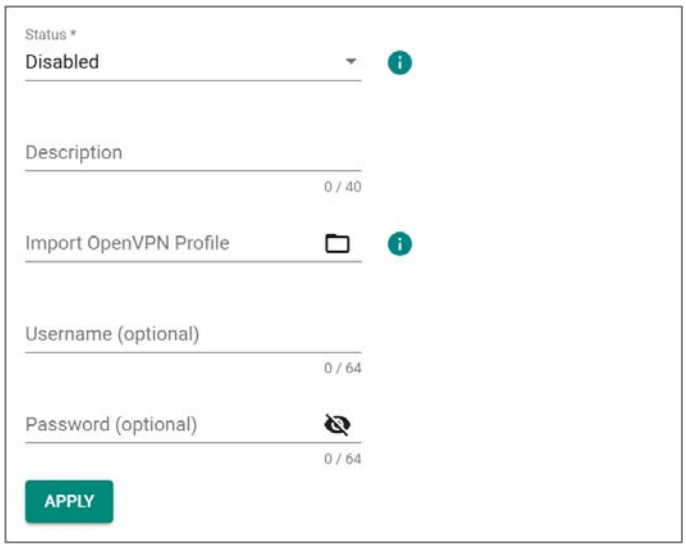
This page includes these tabs:

- Settings
- Status

OpenVPN Client - Settings

Menu Path: VPN > OpenVPN Client - Settings

This page lets you manage your OpenVPN Client settings.

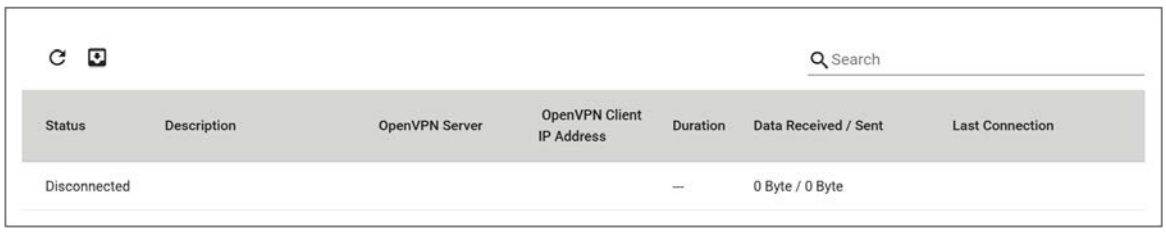


UI Setting	Description	Valid Range	Default Value
Status	Enable or Disable OpenVPN Client. **Note** IPsec and OpenVPN cannot be enabled simultaneously.	Enabled / Disabled	Disabled
Description	Specify the description for the OpenVPN Client connection.	0 to 40 characters	N/A
Import OpenVPN Profile	Import the .ovpn file for OpenVPN Client setup. **Note** Importing OpenVPN profiles is not supported in the CLI interface.	.ovpn files	N/A
Username (optional)	Specify the username.	0 to 64 characters	N/A
Password (optional)	Specify the password.	0 to 64 characters	N/A

OpenVPN Client - Status

Menu Path: VPN > OpenVPN Client - Status

This page lets you view the status of your OpenVPN Client connection.



UI Setting	Description
Status	Shows the status of the connection.
Description	Shows the description of the connection.
OpenVPN Server	Shows the OpenVPN Server IP Address.

UI Setting	Description
OpenVPN Client IP Address	Shows the OpenVPN Client IP Address.
Duration	Shows the duration of OpenVPN connection.
Data Received / Sent	Shows the number of bytes received/sent through the OpenVPN tunnel.
Last Connection	Shows when the device was last connected to the OpenVPN server.

L2TP Server

Menu Path: VPN > L2TP Server

This page lets you configure the L2TP server function of your device. L2TP is a popular choice for VPN applications with remote roaming users since an L2TP client is built into the Microsoft Windows operating system. Since L2TP does not provide any encryption, it is usually combined with IPsec to provide data encryption.

This page includes these tabs:

- Server Setting (WAN)
- User Name Settings

Server Setting (WAN)

Menu Path: VPN > L2TP Server - Server Setting (WAN)

This page lets you enable and configure the L2TP server function of your device.

Limitations

You can configure an L2TP WAN server for each WAN interface of the device.

Note

WAN server settings will only be editable if a WAN for the corresponding WAN ID has been configured. Refer to WAN/WAN1 for more information.

UI Setting	Description	Valid Range	Default Value
L2TP Server Mode	Enable or disable the L2TP server.	Enabled / Disabled	Disabled
Local IP	Specify the IP address of the local subnet.	Valid IP address	0.0.0.0
Offered IP: Start	Specify the starting IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0
Offered IP: End	Specify the ending IP address of the offered IP range used for L2TP clients.	Valid IP address	0.0.0.0

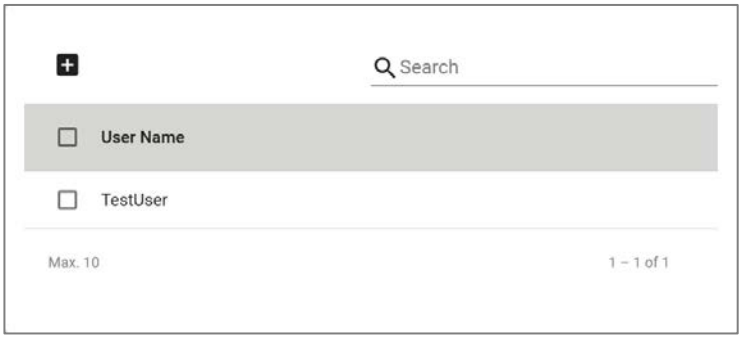
User Name Settings

Menu Path: VPN > L2TP Server - User Name Settings

This page lets you manage users that can connect to your device's L2TP server.

Limitations

You can add up to 10 users for the L2TP Server.



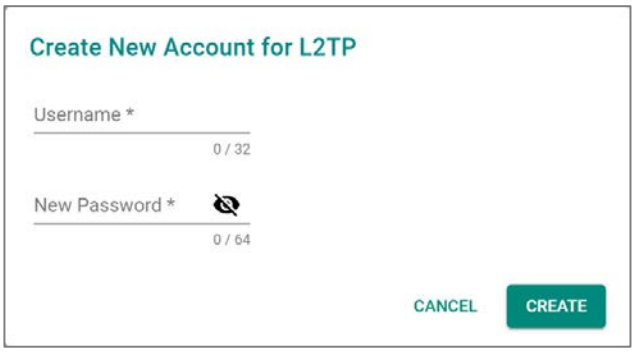
UI Setting	Description
User Name	Shows the name of the user account.

Create New Account for L2TP

Menu Path: VPN > L2TP Server - User Name Settings

Clicking the **Add (⊞)** icon on the **VPN > L2TP Server - User Name Settings** page will open this dialog box. This dialog lets you create a new user account for the device's L2TP server.

Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Username	Enter a username for the L2TP account.	1 to 32 characters	N/A
New Password	Enter a password for the L2TP account.	1 to 64 characters	N/A

Delete Account for L2TP

Menu Path: VPN > L2TP Server - User Name Settings

You can delete an account by using the checkboxes to select the accounts you want to delete, then clicking the **Delete ( )** icon.

Certificate Management

Menu Path: Certificate Management

The Certificate Management settings area lets you manage X.509 digital certificates for your device. These certificates are commonly used for IPsec, OpenVPN, and HTTPS authentication. Alternatively, you can import certificates from other CAs.

Certificates are a time-based form of authentication. Before processing certificates, please ensure that your device is synced with the local device. For more information about syncing device time, please refer to Time.

This section includes these pages:

- Local Certificate
- Trusted CA Certificate
- Certificate Signing Request

> ⚠ **Warning**
>
> For security reasons, if the device is deployed without a CA server environment, we strongly recommend using short lifetime certificates (e.g., 24 hours) to ensure system security.

> ⚠ **Warning**
>
> Because the device's default signature certificates are manufactured without third-party signatures, there is a potential risk of man-in-the-middle attacks that impersonate services, with the client-side being unable to verify.
>
> Therefore, we recommend that upon activating the device, you use the Local Certificate feature to add or update the certificate to one that belongs to your company and that is issued by a recognized certification authority in order to ensure the security and trustworthiness of your network communications.

Certificate Management - User Privileges

Privileges to Certificate Management settings are granted to the different authority levels as follows. Refer to User Accounts for more information.

Settings	Admin	Supervisor	User
Local Certificate	R/W	R/W	-

Settings	Admin	Supervisor	User
Trusted CA Certificate	R/W	-	-
Certificate Signing Request	R/W	-	-

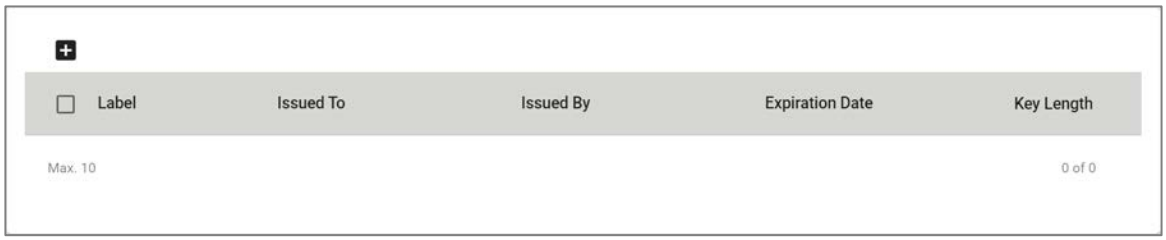
Local Certificate

Menu Path: Certificate Management > Local Certificate

This page lets you import and manage X.509 digital certificates.

Limitations

You can import up to 10 local certificates.



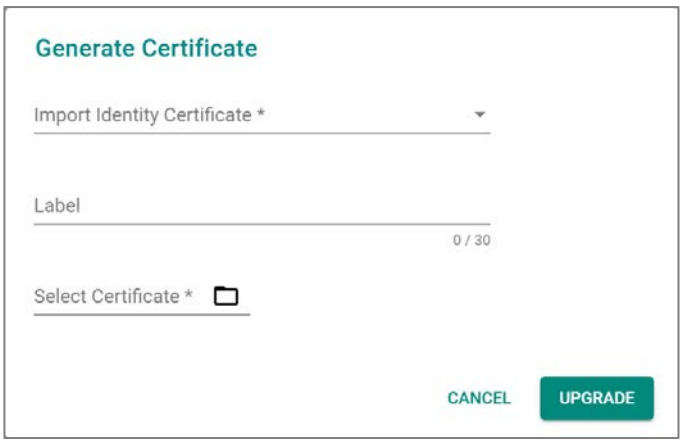
UI Setting	Description
Label	Shows the label identifying the certificate.
Issued To	Shows who the certificate was issued to.
Issued By	Shows who the certificate was issued by.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

Generate Certificate

Menu Path: Certificate Management > Local Certificate

Clicking the **Add (⊕)** icon on the **Certificate Management > Local Certificate** page will open this dialog box. This dialog lets you import a certificate from your local computer.

Click **UPGRADE** to save your changes and add the new certificate.



UI Setting	Description	Valid Range	Default Value
Import Identity Certificate	Select the type of certificate to import. • **Certificate**: Used for certificates with a .crt file extension. • **Certificate From CSR**: Used for certificates issued by another CA. • **Certificate From PKCS#12**: Used for certificates with a .p12 file extension. **Note** Before importing a certificate issued by another CA, you should import its related trusted CA certificate first on the Trusted CA Certificate page. Otherwise, your device may not recognize the certificate and reject the connection.	Certificate / Certificate From CSR / Certificate From PKCS#12	N/A
Label	Enter a label to help identify the certificate. If this is empty, the file name of the certificate will be used.	1 to 30 characters	N/A

UI Setting	Description	Valid Range	Default Value
CSR Common Name **(if Import Identity Certificate is Certificate From CSR)**	Select the CSR common name for the certificate. **Note** CSRs must be created in advance on the CSR Generate page to select them here.	Drop-down list of CSR names	N/A
Import Password **(if Import Identity Certificate is Certificate From PKCS#12)**	Enter the password for the certificate.	0 to 32 characters	N/A
Select Certificate	Click this field and select the certificate file from your computer.	Select a file from your computer	N/A

Delete Certificate

Menu Path: Certificate Management > Local Certificate

You can delete certificates by using the checkboxes to select the certificates you want to delete, then clicking the **Delete ( )** icon.

Note

You cannot delete a certificate if it is currently in use. If you would like to delete the item, you can go to SSL and change the certificate source to Auto Generate then unlock the certificate you'd like to change.

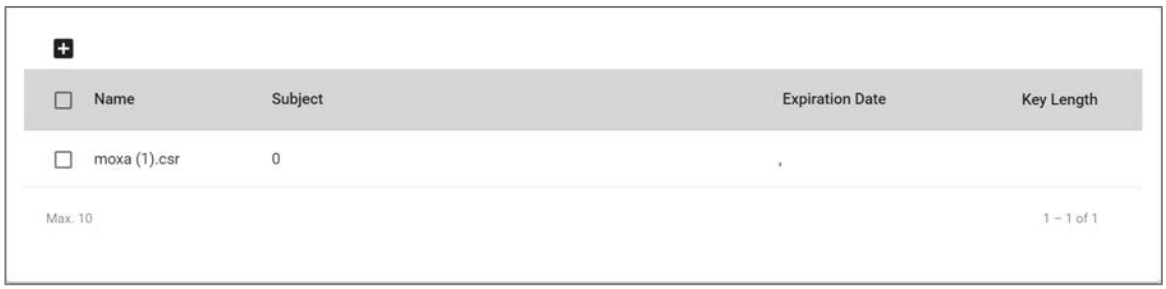
Trusted CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

This page lets you import and manage trusted CA certificates.

Limitations

You can import up to 10 trusted CA certificates.



UI Setting	Description
Name	Shows the name of the certificate file.
Subject	Shows the subject from the certificate.
Expiration Date	Shows the expiration date of the certificate.
Key Length	Shows the key length of the certificate.

Generate CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

Clicking the **Add (⊕)** icon on the **Certificate Management > Trusted CA Certificate** page will open this dialog box. This dialog lets you import a CA certificate from your local computer.

Click **UPGRADE** to save your changes and add the new certificate.

UI Setting	Description	Valid Range	Default Value
Select Certificate	Click this field and select the certificate file from your computer.	Select a file from your computer	N/A

Delete CA Certificate

Menu Path: Certificate Management > Trusted CA Certificate

You can delete certificates by using the checkboxes to select the certificates you want to delete, then clicking the **Delete ( )** icon.

Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request

This page lets you generate and manage key pairs and certificate signing requests (CSRs). Certificate signing requests are needed to apply for and import a digital identity certificate from a CA.

To get a certificate from a CA for connection purposes, you will need to:

1. Generate a key pair
2. Generate a CSR

This page includes these tabs:

- Key Pair Generate
- CSR Generate

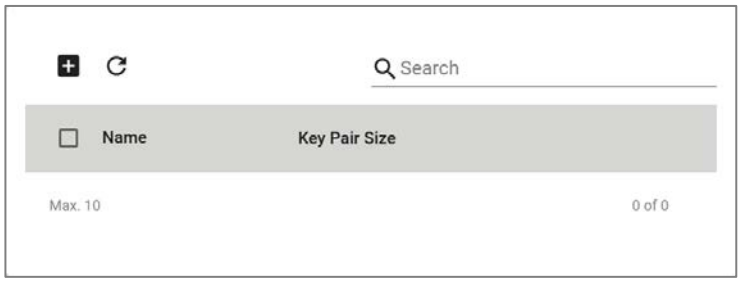
Key Pair Generate

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

This page lets you generate and manage key pairs, which are used to generate CSRs.

Limitations

You can generate up to 10 key pairs.



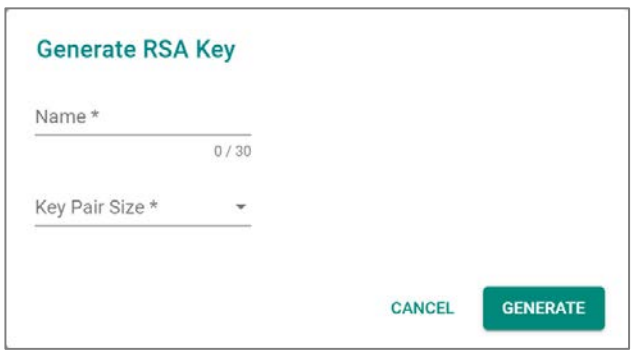
UI Setting	Description
Name	Shows the name of the RSA key.
Key Pair Size	Shows the size used for the key pair.

Generate RSA Key

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

Clicking the **Add (⊞)** icon on the **Certificate Management > Certificate Signing Request - Key Pair Generate** page will open this dialog box. This dialog lets you generate a new key pair to use when generating a CSR.

Click **GENERATE** to save your changes and add the new key pair.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the RSA key.	1 to 30 characters	N/A
Key Pair Size	Select the key pair size to use.	1024 Bit / 2048 Bit / 3072 Bit / 4096 Bit	N/A

Delete RSA Key

Menu Path: Certificate Management > Certificate Signing Request - Key Pair Generate

You can delete key pairs by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

CSR Generate

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

This page lets you generate and manage CSRs.

Limitations

You can generate up to 10 CSRs.

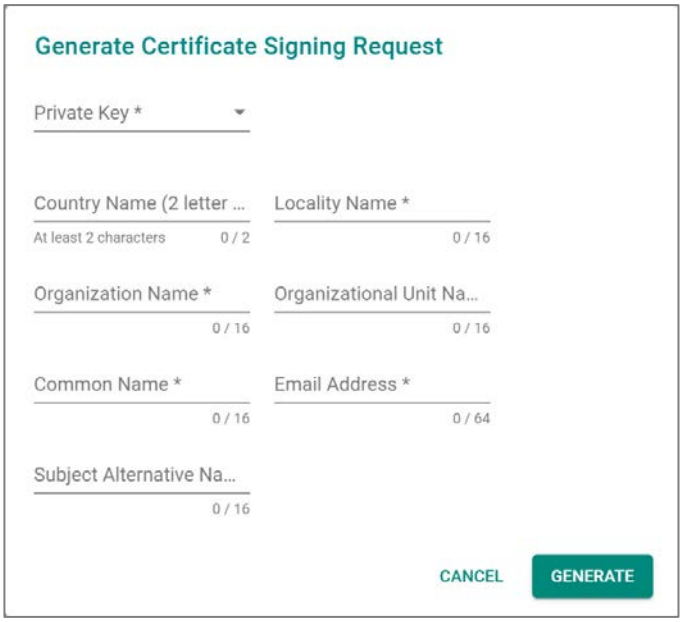
UI Setting	Description
Name	Shows the name of the CSR.
Subject	Shows the subject of the CSR.
Key Length	Shows the key length used by the CSR.

Generate Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

Clicking the **Add (⊕)** icon on the **Certificate Management > Certificate Signing Request - CSR Generate** page will open this dialog box. This dialog lets you generate a new CSR.

Click **CREATE** to save your changes and add the new CSR.



UI Setting	Description	Valid Range	Default Value
Private Key	Select the key pair to use. To generate and manage key pairs, refer to Key Pair Generate.	Drop-down list of key pairs	N/A
Country Name (2 letter code)	Specify the 2-letter country code for the CSR.	2 characters	N/A
Locality Name	Specify the locality name for the CSR.	1 to 16 characters	N/A
Organization Name	Specify the organization name for the CSR.	1 to 16 characters	N/A
Organization Unit Name	Specify the organization unit name for the CSR.	1 to 16 characters	N/A

UI Setting	Description	Valid Range	Default Value
Common Name	Specify the common name for the CSR.	1 to 16 characters	N/A
Email Address	Specify the email address for the CSR.	1 to 64 characters	N/A
Subject Alternative Name	Specify the subject alternative name for the CSR.	1 to 16 characters	N/A

Delete Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

You can delete CSRs by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Export Certificate Signing Request

Menu Path: Certificate Management > Certificate Signing Request - CSR Generate

You can export a CSR by using the checkboxes to select the entry you want to export, then clicking the **Export ( )** icon.

> **Note**
>
> The export icon will only be available when a single entry is selected; it will not be available if multiple entries are selected.

Security

Menu Path: Security

The Security settings area lets you configure security settings to help you secure your device and your network.

This settings area includes these sections:

- Device Security
- Network Security
- Authentication
- MXview Alert Notification

Security - User Privileges

Privileges to Security settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R/W	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-

Settings	Admin	Supervisor	User
LDAP	R/W	-	-
2-Factor Authentication	R/W	-	-
RADIUS Server	R/W	-	-
MXview Alert Notification	R/W	R/W	R

Device Security

Menu Path: Security > Device Security

This section lets you configure security settings to protect your device.

This section includes these pages:

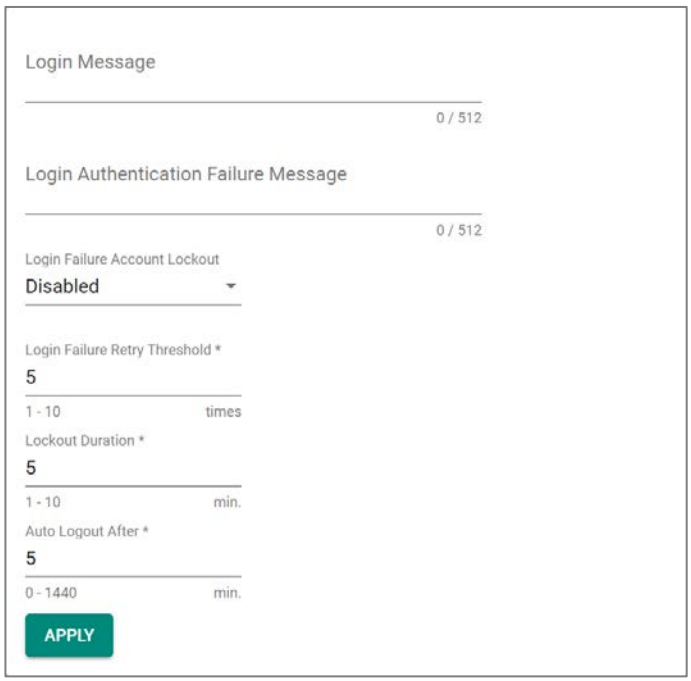
- Login Policy
- Trusted Access
- SSH & SSL

Login Policy

Menu Path: Security > Device Security > Login Policy

This page lets you configure the login policies for your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Login Message	Specify the welcome message to display when users log in to the device. **⚠ Warning** The Login Message should not include login-related information.	0 to 512 characters	N/A
Login Authentication Failure Message	Specify the message to display if the user fails to log in. **⚠ Warning** The Login Authentication Failure Message should not include information about passwords or other sensitive information.	0 to 512 characters	N/A
Login Failure Account Lockout	Enable or disable the lockout function, which will temporarily prevent users from logging in for the **Lockout Duration** after the **Login Failure Retry Threshold** is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled
Login Failure Retry Threshold	Specify the number of login retry attempts before the user is locked out for the **Lockout Duration**.	1 to 10	5

UI Setting	Description	Valid Range	Default Value
Lockout Duration	Specify the lockout duration (in minutes) during which a locked-out user will be unable to log in.	1 to 10	5
Auto Logout After	Specify the amount of time a user can be idle before they will be automatically logged out from the device.	1 to 1440	5

Trusted Access

Menu Path: Security > Device Security > Trusted Access

This page lets you limit access to the device to trusted IP addresses you specify. You can also limit access to the device to LAN connections only.

Limitations

- EDF, EDR, NAT, and TN Series: You can create up to 32 allowlist policies.
- OnCell Series: You can create up to 10 trusted IP entries.

Trusted Access Settings (EDF/EDR/NAT/TN)

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable Trusted Access event logging.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign to Trusted Access events. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

UI Setting	Description	Valid Range	Default Value
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A

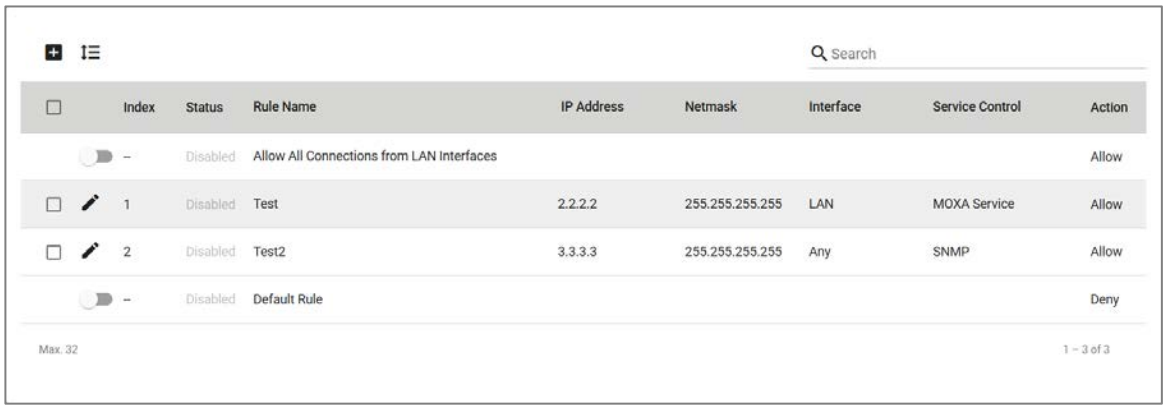
Trusted Access Rule List (EDF/EDR/NAT/TN)

There are two default rules that can be enabled or disabled by using their toggle buttons:

- **Allow All Connections from LAN Interfaces**: When enabled, all connections from LAN interfaces will be allowed.
- **Default Rule**: When enabled, all connections will be denied unless allowed by another policy.

Caution

Ensure there is a rule that allows access to the host PC you are using to access the device's Web UI before enabling the Default Rule. Enabling the Default Rule without a rule to allow your host PC to connect will cause you to lose access to the device.



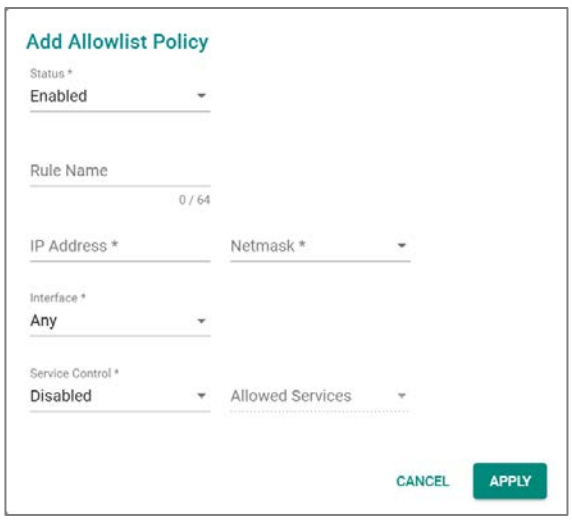
UI Setting	Description
Index	Shows the index of the rule. Rules will be checked from lowest index to highest, and only the first matching rule will be used.
Status	Shows whether the rule is enabled or disabled.
Rule Name	Shows the name of the rule.
IP Address	Shows the IP address the rule applies to.
Netmask	Shows the netmask the rule applies to.
Interface	Shows the interface the rule applies to.
Service Control	Shows which services the rule applies to.
Action	Shows which action will be taken for traffic matching the rule.

Add Allowlist Policy

Menu Path: Security > Device Security > Trusted Access

Clicking the **Add (⊕)** icon on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you add an allowlist policy.

Click **APPLY** to save your changes and add the new entry.



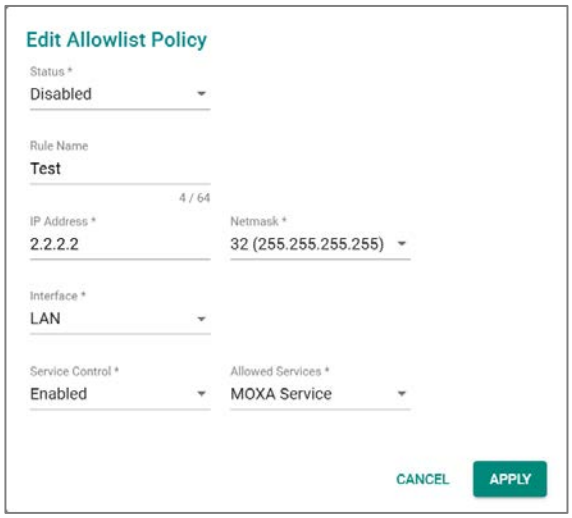
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Rule Name	Specify a name to identify the policy.	1 to 64 characters	N/A
IP Address	Specify the IP address the policy will apply to.	Valid IP address	N/A
Netmask	Select a netmask the policy will apply to.	Drop-down list of netmasks	N/A
Interface	Select which interface the policy will apply to. **Any** will apply the rule to all interfaces.	Any / Drop-down list of interfaces	Any
Service Control	Enable or disable service control for the rule. • **Enabled**: The rule will allow specific traffic as specified by **Allowed Services**. • **Disabled**: The rule will allow all traffic.	Enabled / Disabled	Disabled
Allowed Services	Select which services the rule will apply to. Services allow the rule to apply to specific protocols and ports only. You can select multiple services. • **Web (HTTP/HTTPS)**: TCP 80, 443 • **CLI (SSH/Telnet)**: TCP 22, 23 • **SNMP**: TCP 161 - 162, UDP 161 - 162 • **MOXA Service**: TCP 443, UDP 40404	Web (HTTP/HTTPS) / CLI (SSH/Telnet) / SNMP / MOXA Service	N/A

Edit Allowlist Policy

Menu Path: Security > Device Security > Trusted Access

Clicking the **Edit ( )** icon for an entry on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you edit an existing allowlist policy.

Click **APPLY** to save your changes.

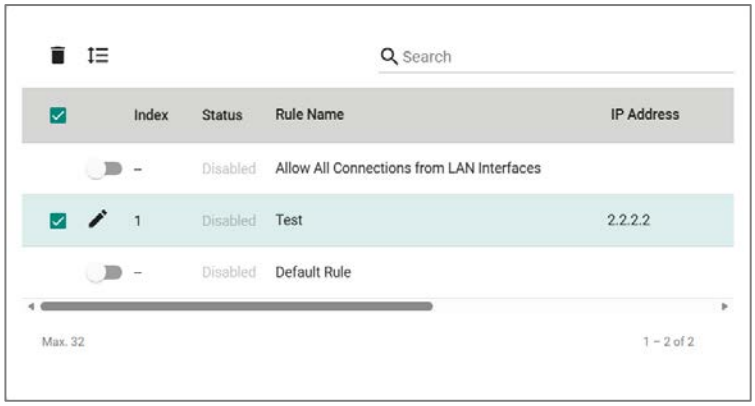


UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the policy.	Enabled / Disabled	Enabled
Rule Name	Specify a name to identify the policy.	1 to 64 characters	N/A
IP Address	Specify the IP address the policy will apply to.	Valid IP address	N/A
Netmask	Select a netmask the policy will apply to.	Drop-down list of netmasks	N/A
Interface	Select which interface the policy will apply to. **Any** will apply the rule to all interfaces.	Any / Drop-down list of interfaces	Any
Service Control	Enable or disable service control for the rule. • **Enabled**: The rule will allow specific traffic as specified by **Allowed Services**. • **Disabled**: The rule will allow all traffic.	Enabled / Disabled	Disabled
Allowed Services	Select which services the rule will apply to. Services allow the rule to apply to specific protocols and ports only. You can select multiple services. • **Web (HTTP/HTTPS)**: TCP 80, 443 • **CLI (SSH/Telnet)**: TCP 22, 23 • **SNMP**: TCP 161 - 162, UDP 161 - 162 • **MOXA Service**: TCP 443, UDP 40404	Web (HTTP/HTTPS) / CLI (SSH/Telnet) / SNMP / MOXA Service	N/A

Delete Allowlist Rule

Menu Path: Security > Device Security > Trusted Access

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Trusted Access Settings (OnCell)

> **Warning**
>
> Depending on the features you enable, you may lose access to your device if the computer you are using to configure the device is not in the Trusted IP List or connected through a LAN connection.

> **Note**
>
> Trusted Access is restricted to the user interface, which includes the Web UI, CLI interface, and Moxa commands from software such as MXconfig and MXview.
>
> Both the DNS Server and NTP Server are only accessible through LAN, VLAN, and Bridge interfaces. In other words, DNS clients and NTP clients cannot access the DNS or NTP service via WAN interfaces on the device.

UI Setting	Description	Valid Range	Default Value
Trusted IP List	Enable or disable the Trusted IP List. • **Enabled:** Only IP addresses in the Trusted IP List can access the device. • **Disabled:** Any IP address can access the device.	Enabled / Disabled	Enabled
Accept All LAN Port Connections	Enable or disable accepting all connections from LAN connections. • **Enabled:** The device can only be accessed through a LAN connection. • **Disabled:** The device can be accessed through any connection.	Enabled / Disabled	Enabled
Log	Enable or disable Trusted Access event logging.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign to Trusted Access events. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	N/A

Trusted IP List

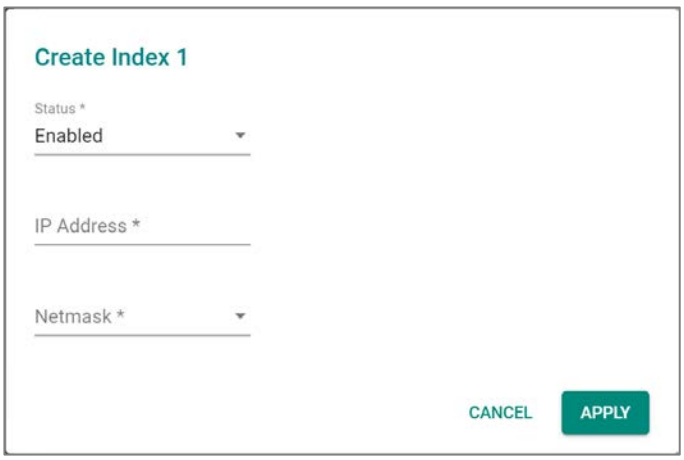
UI Setting	Description
Index	Shows the index of the Trusted IP entry.
Status	Shows whether the Trusted IP entry is enabled or disabled.
IP Address	Shows the IP address of the Trusted IP entry.
Netmask	Shows the netmask of the Trusted IP entry.

Trusted Access - Create Index

Menu Path: Security > Device Security > Trusted Access

Clicking the **Add (⊕)** icon on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you add a trusted IP entry.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the Trusted IP entry.	Enabled / Disabled	Enabled
IP Address	Specify the IP address of the trusted host(s).	Valid IP address	N/A
Netmask	Select a netmask for the trusted host(s).	Drop-down list of netmasks	N/A

SSH & SSL

Menu Path: Security > Device Security > SSH & SSL

This page lets you manage your SSH key and SSL certificate.

This page includes these tabs:

- SSH
- SSL

SSH

Menu Path: Security > Device Security > SSH & SSL - SSH

This page lets you manage your device's SSH key.

This shows you when the current SSH key was created.

Click **REGENERATE** to generate a new SSH key for your device.

> ⚠ **Warning**
>
> Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.

SSL

Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate.

Click **APPLY** to save your changes.

SSL Settings

UI Setting	Description	Valid Range	Default Value
Certificate Source	Select the source for your device's SSL certificate. • **Auto Generate**: Your device will generate a certificate automatically. • **Local Certificate Database**: Your device will use an imported certificate from the Local Certificate database. You will only be able to select certificates from a CSR or PKCS#12 certificates. Refer to Certificate Management for more information.	Auto Generate / Local Certificate Database	Auto Generate
Certificate File **(If Certificate Source is Local Certificate Database)**	Select the imported certificate file to use.	Drop-down list of applicable imported certificates	N/A
Created on **(View-only)**	Shows when the current certificate was created.	N/A	N/A
Expiration Date **(View-only)**	Shows when the current certificate will expire.	N/A	N/A

Network Security

Menu Path: Security > Network Security

This section lets you manage your device's network security features.

This section includes these pages:

- IEEE 802.1X

IEEE 802.1X

Menu Path: Security > Network Security > IEEE 802.1X

This page lets you manage your device's IEEE 802.1X authentication feature.

This page includes these tabs:

- General
- IEEE 802.1X Status
- Remote RADIUS
- Local Database (New)
- Local Database (Legacy)

> **Note**
>
> We recommend that users enable 802.1X as it provides enhanced network security and better access control.

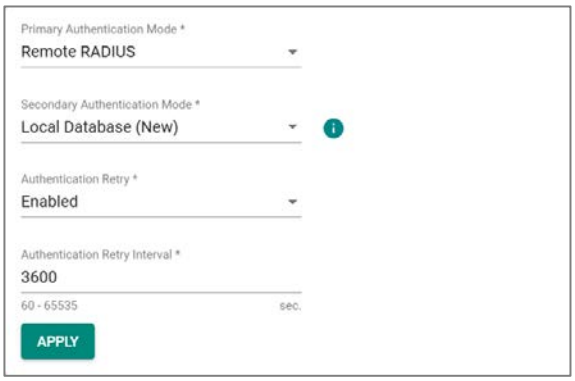
IEEE 802.1X - General

Menu Path: Security > Network Security > IEEE 802.1X - General

This page lets you configure your device's IEEE 802.1X settings.

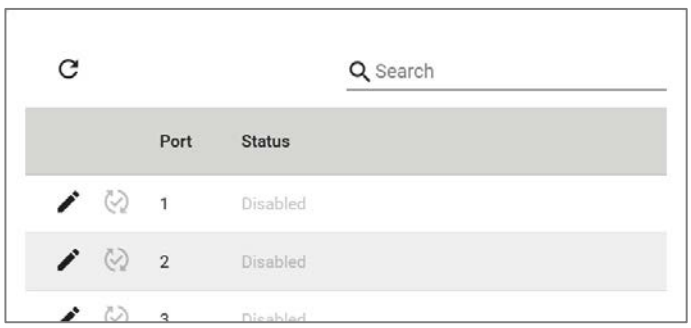
Click **APPLY** to save your changes.

IEEE 802.1X Settings



UI Setting	Description	Valid Range	Default Value
Primary Authentication Mode	Select the primary method of authentication to use. • **Remote RADIUS**: Use a remote RADIUS server for authentication. • **Local Database (Legacy)**: Use the local database for authentication. • **Local Database (New)**: Use the local RADIUS server for authentication.	Remote RADIUS / Local Database (Legacy) / Local Database (New)	Local Database (Legacy)
Secondary Authentication Mode	Select the secondary method of authentication to use. This will be used if the remote RADIUS server is unavailable. • **None**: No secondary authentication will be used. • **Local Database (Legacy)**: Use the local database for authentication. • **Local Database (New)**: Use the local RADIUS server for authentication.	If **Primary Authentication Mode** is **Remote RADIUS**: None / Local Database (Legacy) / Local Database (New) If **Primary Authentication Mode** is **Local Database (Legacy)** or **Local Database (New)**: None	None
Authentication Retry	Enable or disable reauthentication.	Enabled / Disabled	Enabled
Authentication Retry Interval	Specify the authentication retry interval in seconds.	60 to 65535	3600

IEEE 802.1X Port List



UI Setting	Description
Port	Shows which port the entry is for.

UI Setting	Description
Status	Shows whether IEEE 802.1X port access control is enabled or disabled for the port.

IEEE 802.1X - Port Settings

Menu Path: Security > Network Security > IEEE 802.1X - General

Clicking the **Edit ( )** icon for a port on the **Security > Network Security > IEEE 802.1X - General** page will open this dialog box. This dialog lets you edit a port's IEEE 802.1X settings.

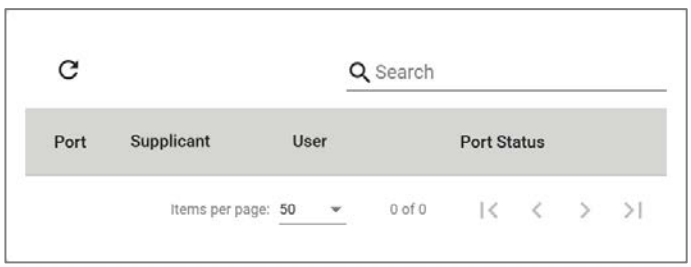
Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable IEEE 802.1X port access control for this port.	Enabled / Disabled	Disabled

IEEE 802.1X Status

Menu Path: Security > Network Security > IEEE 802.1X - IEEE 802.1X Status

This page lets you see the IEEE 802.1X status of your ports.



UI Setting	Description
Port	Shows which port the entry is for.
Supplicant	Shows the MAC address of the device requesting access.
User	Shows the user's name.
Port Status	Shows the status of the 802.1X port. • **INITIALIZE**: The device is rebooting, the supplicant is sending an EAPoL start packet, or the port link is down. • **CONNECTING**: Communication is being established with a supplicant. • **DISCONNECTED**: This state is entered from the CONNECTING state, the AUTHENTICATED state, and the ABORTING state if an explicit logoff request is received from the supplicant, and from the CONNECTING state if the number of allowed reauthentication attempts has been exceeded. • **AUTHENTICATING**:The supplicant is being authenticated. • **AUTHENTICATED**: The supplicant was successfully authenticated. • **ABORTING**: The authentication procedure is being prematurely aborted due to receipt of a reauthentication request, an EAPOL-Start frame, an EAPOL-Logoff frame, or an authTimeout. • **HELD**: Authentication of the supplicant was unsuccessful.

Remote RADIUS

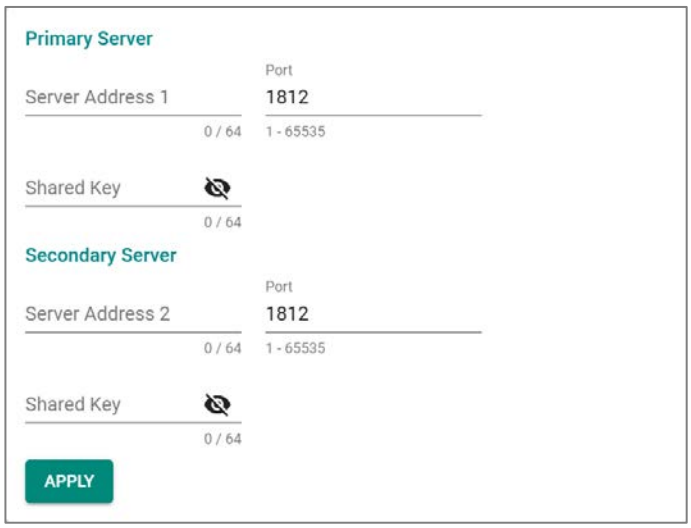
Menu Path: Security > Network Security > Remote RADIUS

This page lets you specify a remote RADIUS server to use for IEEE 802.1X authentication.

Click **APPLY** to save your changes.

Note

The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.



UI Setting	Description	Valid Range	Default Value
Server Address 1	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name up to 64 characters	N/A
UDP Port	Specify the port number for the primary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the primary RADIUS server.	0 to 64 characters	N/A
Server Address 2	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name up to 64 characters	N/A
UDP Port	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the secondary RADIUS server.	0 to 64 characters	N/A

Local Database (New)

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (New)

This page lets you set up a local RADIUS server and create local RADIUS user accounts to use for IEEE 802.1X authentication.

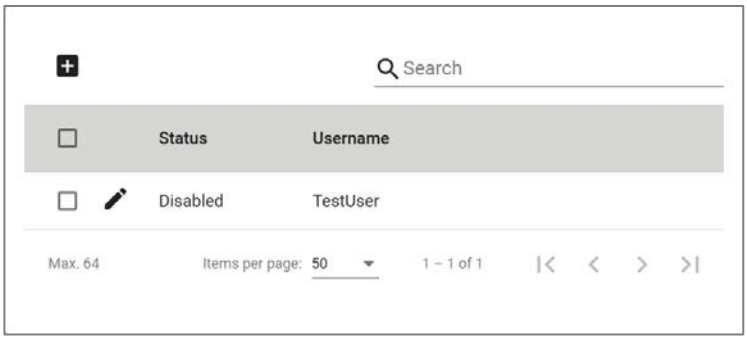
Limitations

You can create up to 64 users for the IEEE 802.1X Local Database (New).

Local Database (New) Settings

UI Setting	Description	Valid Range	Default Value
RADIUS Server	Enable or disable the local RADIUS server for IEEE 802.1X authentication.	Enabled / Disabled	Disabled
Authentication Method	Select the authentication method for the RADIUS server. • **Auto**: The authentication method will be automatically determined. • **PEAP-MSCHAPv2**: Uses credentials provided by the user for authentication. • **EAP-TLS**: Uses client and server certificate-based authentication.	Auto / PEAP-MSCHAPv2 / EAP-TLS	Auto
Certificate	Select the local certificate to use for authentication. Certificates must be installed before you can select them. Refer to Local Certificate for more information.	None / Drop-down list of installed certificates	None
Trusted CA Certificate	Select the trusted CA certificate to use for authentication. Certificates must be installed before you can select them. Refer to Trusted CA Certificate for more information.	None / Drop-down list of installed CA certificates	None

Local Database (New) User List



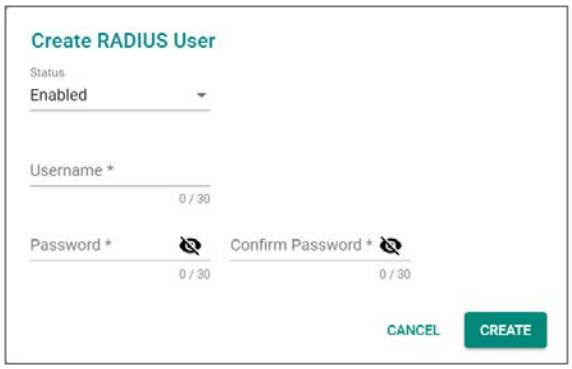
UI Setting	Description
Status	Shows whether the account is enabled or disabled.
Username	Shows the username of the account.

Local Database (New) - Create RADIUS User

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (New)

Clicking the **Add (⊞)** icon on the **Security > Network Security > IEEE 802.1X - Local Database (New)** page will open this dialog box. This dialog lets you create a new local RADIUS user account for IEEE 802.1X authentication.

Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the local RADIUS user.	Enabled / Disabled	Enable
Username	Specify the username for this user.	1 to 30 characters	N/A

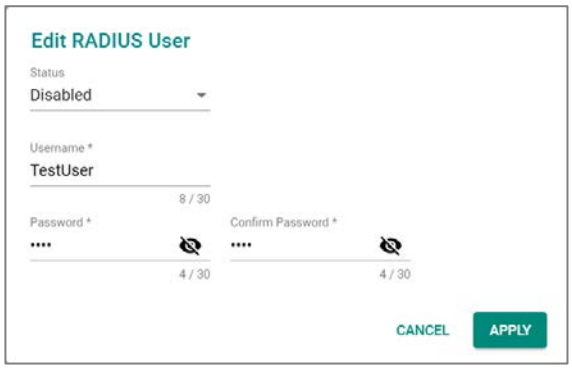
UI Setting	Description	Valid Range	Default Value
Password	Specify the password for this user.	1 to 30 characters	N/A
Password	Re-enter the password for this user.	1 to 30 characters	N/A

Local Database (New) - Edit RADIUS User

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (New)

Clicking the **Edit ( )** icon for an entry on the **Security > Network Security > IEEE 802.1X - Local Database (New)** page will open this dialog box. This dialog lets you edit an existing local RADIUS user account.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the local RADIUS user.	Enabled / Disabled	Enable
Username	Specify the username for this user.	1 to 30 characters	N/A
Password	Specify the password for this user.	1 to 30 characters	N/A
Password	Re-enter the password for this user.	1 to 30 characters	N/A

Local Database (New) - Delete RADIUS User

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (New)

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Local Database (Legacy)

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (Legacy)

This page lets you create local database user accounts to use with IEEE 802.1X authentication.

Limitations

You can create up to 32 users for the IEEE 802.1X Local Database (Legacy).

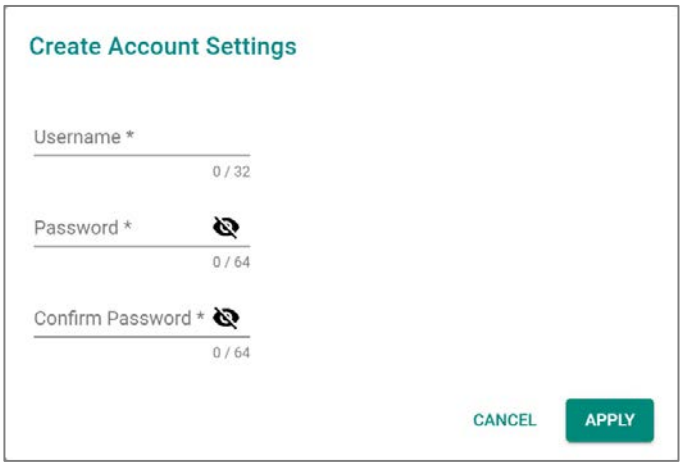
UI Setting	Description
Username	Shows the username of the account.

Local Database (Legacy) - Create Account Settings

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (Legacy)

Clicking the **Add (+)** icon on the **Security > Network Security > IEEE 802.1X - Local Database (Legacy)** page will open this dialog box. This dialog lets you create a new local database user account for IEEE 802.1X authentication.

Click **CREATE** to save your changes and add the new account.

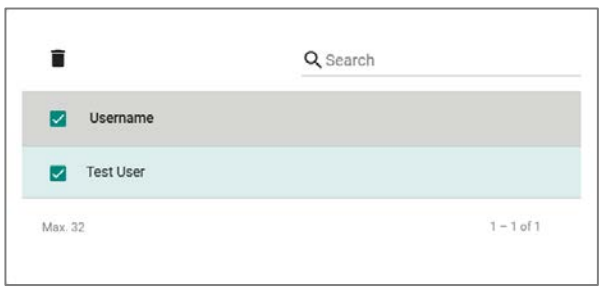


UI Setting	Description	Valid Range	Default Value
Username	Specify the username for this account.	1 to 32 characters	N/A
Password	Specify the password for this user account.	1 to 64 characters	N/A
Confirm Password	Re-enter the password for this user account.	1 to 64 characters	N/A

Local Database (Legacy) - Delete Account Settings

Menu Path: Security > Network Security > IEEE 802.1X - Local Database (Legacy)

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Authentication

Menu Path: Security > Authentication

This section lets you manage login authentication for your device.

This section includes these pages:

- Login Authentication
- RADIUS
- TACACS+
- LDAP
- 2-Factor Authentication

Login Authentication

Menu Path: Security > Authentication > Login Authentication

This page lets you configure your device's login authentication settings.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
Authentication Protocol	Select the method of authentication to use. • **Local:** Use the local database for authentication. • **RADIUS**: Use a RADIUS server for authentication. • **TACACS+**: Use a TACACS+ Server for authentication. • **RADIUS, Local**: Use a RADIUS server for authentication first. If it fails, the device will use the local database for authentication. • **TACACS+, Local**: Use a TACACS+ server for authentication first. If it fails, the device wil use the local database for authentication. • **LDAP**: Use an LDAP server for authentication. • **LDAP, Local**: Use an LDAP server for authentication first. If it fails, the device wil use the local database for authentication. **⚠ Warning** If you configure the device to use a remote server such as RADIUS or TACACS+ but don't use a local database as a backup, you will unable to log in through network services (HTTP/HTTPS/Telnet/SSH) if the device is unable to connect to the remote server for authentication. In such an event, the only way to access the device would be through the console port.	Local / RADIUS / TACACS+ / RADIUS, Local / TACACS+, Local / LDAP / LDAP, Local	Local

RADIUS

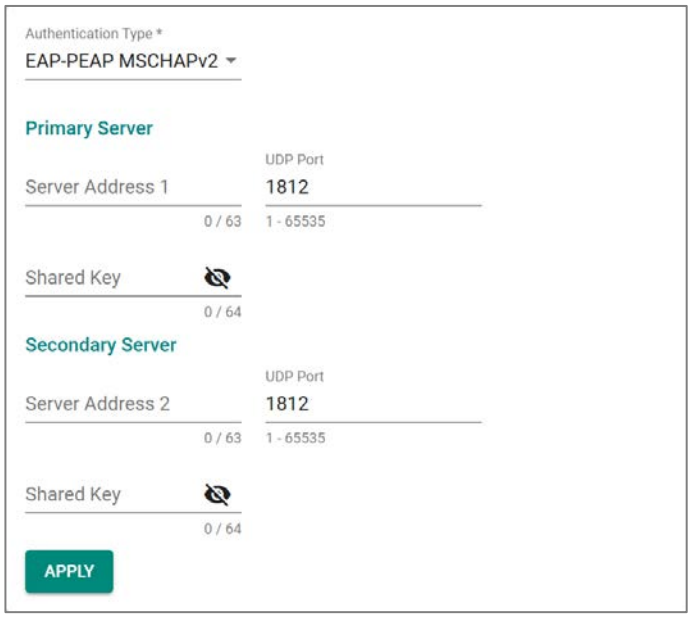
Menu Path: Security > Authentication > RADIUS

This page lets you specify a RADIUS server to use for login authentication.

Click **APPLY** to save your changes.

✎ Note

The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.



UI Setting	Description	Valid Range	Default Value
Authentication Type	Select the authentication method to use for the RADIUS servers.	PAP / CHAP / EAP-PEAP MSCHAPv2	EAP-PEAP MSCHAPv2
Server Address 1	Specify the IP address or domain name for the primary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the primary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the primary RADIUS server.	0 to 64 characters	N/A
Server Address 2	Specify the IP address or domain name for the secondary RADIUS server.	Valid IP address or domain name	N/A
UDP Port	Specify the port number for the secondary RADIUS server.	1 to 65535	1812
Shared Key	Specify the shared key for the secondary RADIUS server.	0 to 64 characters	N/A

TACACS+

Menu Path: Security > Authentication > TACACS+

This page lets you set up TACACS+ protocol to authenticate remote users.

UI Setting	Description	Valid Range	Default Value
Server IP Address 1	Specify the IPv4 address of the primary TACACS+ server to use. Setting the address to 0.0.0.0 will disable use of a primary TACACS+ server. **Note** When authenticating a remote user, the device will try to authenticate them using the primary server specified by Server IP Address 1. If the device fails to connect to the primary server, it will try to authenticate by using the secondary server specified by Server IP Address 2.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port to use for authentication requests to the primary TACACS+ server.	1 to 65535	49
Share Key	Specify the shared encryption key for the primary TACACS+ server.	1 to 64 characters	N/A
Auth Type	Specify which authentication type the primary TACACS+ server uses.	PAP / CHAP / ASCII	CHAP
Timeout	Specify the amount of time in seconds a client will wait for a response from the primary TACACS+ server before re-transmitting the request.	5 to 120	5

UI Setting	Description	Valid Range	Default Value
Retry	Specify the number of times the device will try to contact the primary TACACS+ server.	0 to 5	1
Server IP Address 2	Specify the IPv4 address of the secondary TACACS+ server to use. Setting the address to 0.0.0.0 will disable use of a secondary TACACS+ server.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port to use for authentication requests to the secondary TACACS+ server.	1 to 65535	49
Share Key	Specify the shared encryption key for the secondary TACACS+ server.	1 to 64 characters	N/A
Auth Type	Specify which authentication typethe secondary TACACS+ server uses.	PAP / CHAP / ASCII	CHAP
Timeout	Specify the amount of time in seconds a client will wait for a response from the secondary TACACS+ server before re-transmitting the request.	5 to 120	5
Retry	Specify the number of times the device will try to contact the secondary TACACS+ server.	0 to 5	1

LDAP

Menu Path: Security > Authentication > LDAP

This page lets you manage LDAP authentication for your device. LDAP (Lightweight Directory Access Protocol) is an open protocol used to access and manage directory information services. You can use it for authentication and user management in systems like OpenLDAP, Active Directory, and similar directory-based services.

This page includes these tabs:

- General
- Role Mapping
- Test

LDAP - General

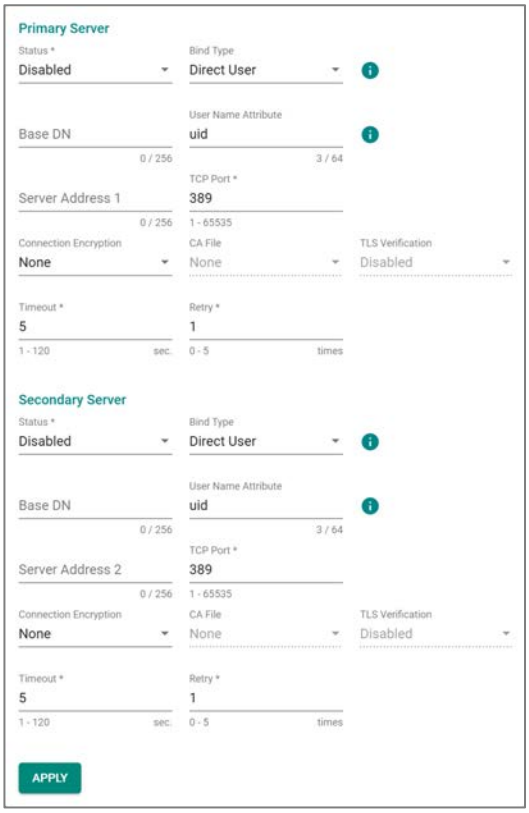
Menu Path: Security > Authentication > LDAP - General

This page lets you specify LDAP servers for your device to use.

Limitations

You can add up to 2 LDAP servers.

You can set up a primary and a secondary LDAP server for your device. If the device cannot connect to the primary LDAP server, the secondary server will be used.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the LDAP server.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Bind Type	Select the authentication process to use with the LDAP server. • **UPN**: A UPN (User Principal Name) is used for authentication based on an email address. UPN is only supported for Windows AD. • **Two-phase**: An authentication process that binds with a predetermined service account, then rebinds using user credentials for secure account verification. • **Direct User**: An authentication where users log in directly by using preset criteria.	UPN / Two-phase / Direct User	Direct User
Base DN	Specify the base distinguished name (DN) of the LDAP server. This acts as the starting point for LDAP searches, and is typically the root of the directory tree.	0 to 256 characters	N/A
Default Domain **(If Bind Type is UPN)**	Specify the default domain of the LDAP server.	0 to 256 characters	N/A
Bind DN **(If Bind Type is Two-phase)**	Specify the bind distinguished name (DN) of the LDAP server. This is the user on the LDAP server permitted to search the LDAP directory.	0 to 256 characters	N/A
Bind Passsword **(If Bind Type is Two-phase)**	Specify the password for the bind DN for the LDAP server.	0 to 128 characters	N/A
User Name Attribute **(If Bind Type is Two-Phase or Direct User)**	Specify the user name attribute used to identify users for the LDAP server.	0 to 64 characters	uid
Server Address	Specify the IP address of the LDAP server.	Valid IP address	N/A
TCP Port	Specify the TCP port of the LDAP server.	1 to 65535	389
Connection Encryption	Select the encryption method to use to connect to the LDAP server.	None / SSL/TLS / STARTTLS	None
CA File	Select which CA file to use for the LDAP server. If **Connection Encryption** is **None**, this will be fixed to **None**.	None / Drop-down list of installed CA files	None
TLS Verification	Enable or disable TLS verification when connecting to the LDAP server. If **Connection Encryption** is **None**, this will be fixed to **Disabled**.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Timeout	Specify the amount of time in seconds the device will wait for a response from the LDAP server before determining a connection timeout has occurred.	1 to 120	5
Retry	Specify the number of times the device will try to connect to the LDAP server if a timeout occurs. After reaching the retry limit, the device will try to connect to the other server.	0 to 5	1

Role Mapping

Menu Path: Security > Authentication > LDAP - Role Mapping

This page lets you manage LDAP role mappings for your device. Role mappings allow you to assign an authority level to users based on their LDAP attributes.

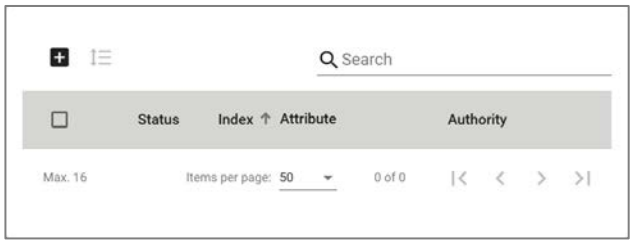
Limitations

You can create up to 16 LDAP role mappings.

Role Mapping Settings

UI Setting	Description	Valid Range	Default Value
Matching Policy	Select the policy to determine which role mapping entry to use for a user. • **First Hit**: The first matching role mapping entry will be used. Role mapping entries will be checked from lowest index to highest. • **Highest Privilege**: The matching role mapping entry that grants the highest authority level will be used.	First Hit / Highest Privilege	First Hit

Role Mapping List



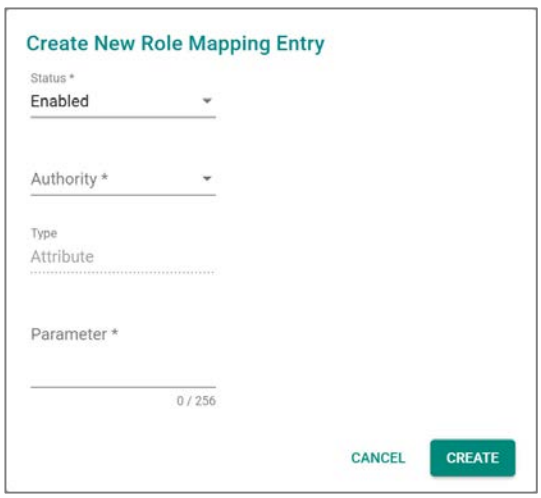
UI Setting	Description
Status	Shows whether the role mapping entry is enabled or disabled.
Index	Shows the index of the role mapping entry. Role mapping entries will be checked from lowest index to highest.
Attribute	Shows the user attributes of the role mapping entry that must be matched to assign the corresponding authority level.
Authority	Shows the authority level to assign to a matching user.

Create New Role Mapping Entry

Menu Path: Security > Authentication > LDAP - Role Mapping

Clicking the **Add (⊞)** icon on the **Security > Authentication > LDAP - Role Mapping** page will open this dialog box. This dialog lets you create a new role mapping entry.

Click **CREATE** to save your changes and add the new entry.



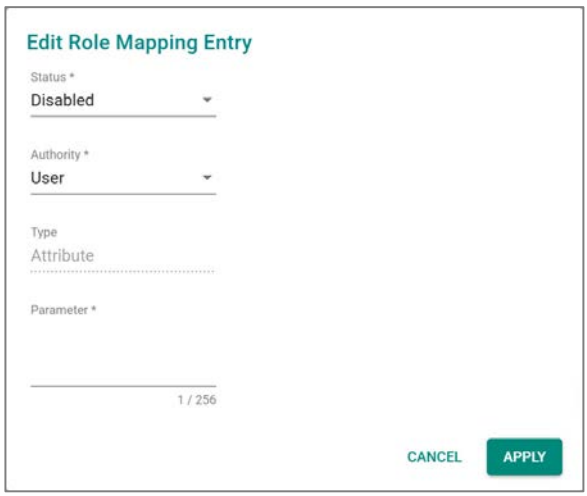
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the role mapping entry.	Enabled / Disabled	Enabled
Authority	Select the authority level to assign to matching users.	Admin / Supervisor / User	N/A
Type	Shows how to determine whether a user is a match. This is fixed to **Attribute**. • **Attribute**: User attributes will be checked to determine a match.	Attribute	Attribute
Parameter	Specify the parameter values that users must match for the role mapping entry.	1 to 256 characters	N/A

Edit Role Mapping Entry

Menu Path: Security > Authentication > LDAP - Role Mapping

Clicking the **Edit ( )** icon for an entry on the **Security > Authentication > LDAP - Role Mapping** page will open this dialog box. This dialog lets you edit an existing role mapping entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the role mapping entry.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Authority	Select the authority level to assign to matching users.	Admin / Supervisor / User	N/A
Type	Shows how to determine whether a user is a match. This is fixed to **Attribute**. • **Attribute**: User attributes will be checked to determine a match.	Attribute	Attribute
Parameter	Specify the parameter values that users must match for the role mapping entry.	1 to 256 characters	N/A

Delete a Role Mapping Entry

Menu Path: Security > Authentication > LDAP - Role Mapping

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

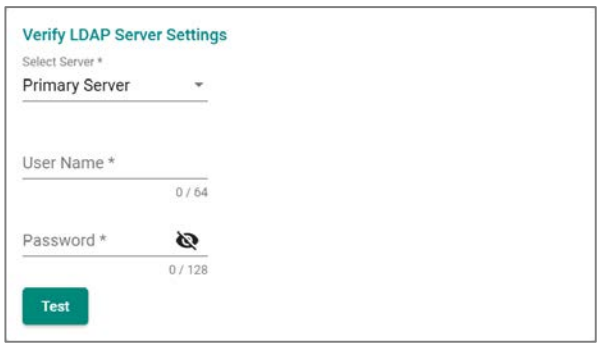
LDAP - Test

Menu Path: Security > Authentication > LDAP - Test

This page lets you test and verify your LDAP server settings.

Verify LDAP Server Settings

After entering the required information, select **Test** to run a connection test.



UI Setting	Description	Valid Range	Default Value
Select Server	Select the LDAP server to test.	Primary Server / Secondary Server	Primary Server
User Name	Specify the user name to test.	1 to 64 characters	N/A
Password	Specify the password to test.	1 to 128 characters	N/A

2-Factor Authentication

Menu Path: Security > Authentication > 2-Factor Authentication

This page lets you manage 2-factor authentication for your device. 2-factor authentication is a way to improve the security of logins to your device.

This page includes these tabs:

- Settings
- TOTP

2-Factor Authentication - Settings

Menu Path: Security > Authentication > 2-Factor Authentication - Settings

This page lets you configure the main 2-factor authentication settings.

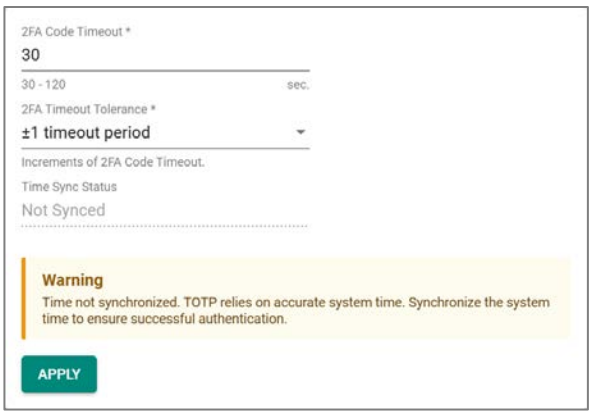
UI Setting	Description	Valid Range	Default Value
2-Factor Authentication	Enable or disable 2-factor authentication for the device.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Algorithm	Select which encryption algorithm to use for 2-factor authentication. Important Update the algorithm used in 2FA authenticator applications when changing the 2FA algorithm of the device. Changing the 2FA algorithm will change how 2FA codes are generated.	SHA1 / SHA256 / SHA512	SHA1
Services Using 2FA	Select which services/protocols will use 2-factor authentication. You can select multiple services.	HTTP / HTTPS / Telnet / SSH	N/A

TOTP

Menu Path: Security > Authentication > 2-Factor Authentication - TOTP

This page lets you configure TOTP (Time-based One-Time Password) settings for 2-factor authentication. TOTP uses a constantly changing 6-digit code that updates at least every 30 seconds and is generated entirely offline on your device or emailed to you, depending on your settings.



UI Setting	Description	Valid Range	Default Value
2FA Code Timeout	Specify the amount of time in seconds in between 2FA code changes.	30 to 120	30

UI Setting	Description	Valid Range	Default Value
2FA Timeout Tolerance	Specify the number of timeout periods to allow for 2FA. • **±1 timeout period**: The current and the most recently timed out 2FA codes will be accepted. • **No tolerance**: Only the current 2FA code will be accepted.	±1 timeout period / No tolerance	±1 timeout period
Time Sync Status	Shows the current status of time syncing.	N/A	N/A

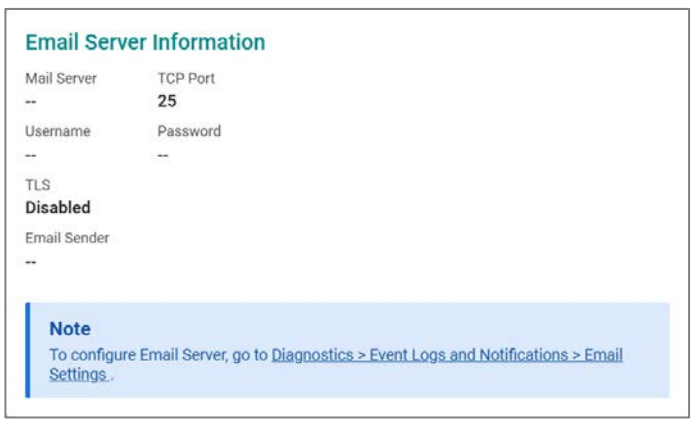
2-Factor Authentication - Email

Menu Path: Security > Authentication > 2-Factor Authentication - Email

This page lets you view details of the email server used to send one-time 2FA codes.

Note

The email server information cannot be edited here. Refer to Email Settings for more information.



UI Setting	Description
Mail Server	Shows the address of the email server to use to send one-time 2FA codes to users that have email 2FA enabled. Refer to User Accounts for more information.
TCP Port	Shows the TCP port of the email server.
Username	Shows the username used to log in to the email server.

UI Setting	Description
Password	Shows the password used to log in to the email server.
TLS	Shows whether TLS (Transport Layer Security) is enabled for encrypted email transmission.
Email Sender	Shows the sender email address for emails sent.

RADIUS Server

Menu Path: Security > RADIUS

This page lets you manage your device's RADIUS Server feature.

This page includes these tabs:

- General
- RADIUS Client List
- Authentication User List

RADIUS Server - General

Security > RADIUS Server - General

This page lets you configure RADIUS Server settings on your device.

RADIUS Server - General

UI Setting	Description	Valid Range	Default Value
Radius Server	Enable or disable RADIUS Server feature.	Enabled / Disabled	Disabled
Authentication Port	Specify the port number for authentication.	1 to 65535 **Note** Port 18120 is prohibited as reserved for internal use.	1812

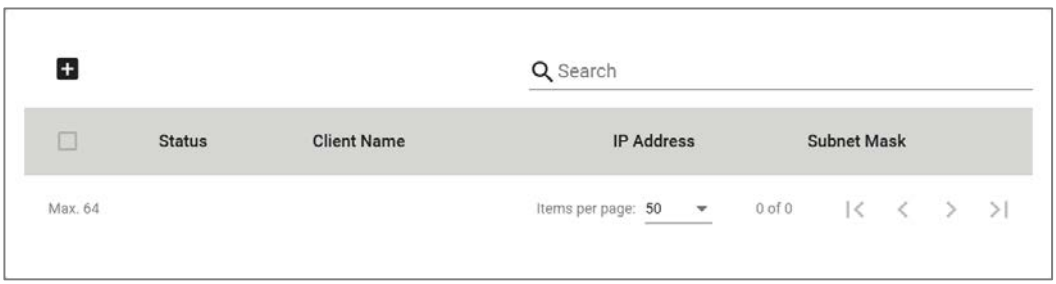
RADIUS Client List

Menu Path: Security > RADIUS Server - RADIUS Client List

This page lets you manage RADIUS clients for your device.

Limitations

You can create up to 64 RADIUS client entries.



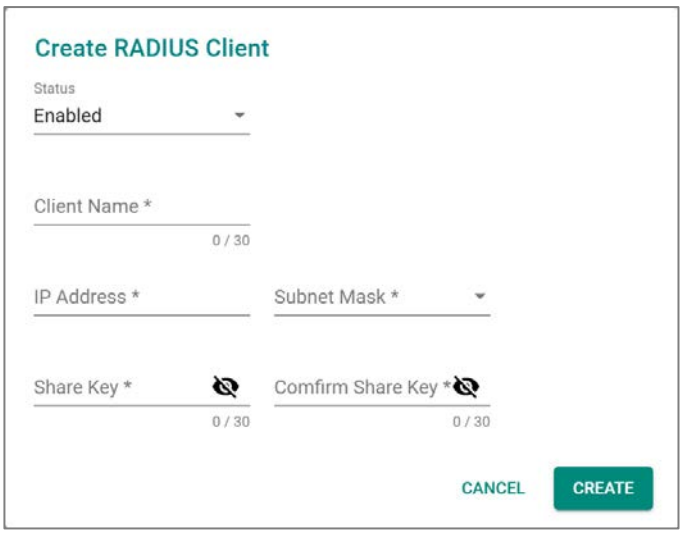
UI Setting	Description
Status	Shows the status of the RADIUS client.
Client Name	Shows the name of the RADIUS client.
IP Address	Shows the IP address setting of the RADIUS client.
Subnet Mask	Shows the subnet mask setting of the RADIUS client.

Create RADIUS Client

Menu Path: Security > RADIUS Server - RADIUS Client List

Clicking the **Add (⊕)** icon on the **Security > RADIUS Server - RADIUS Client List** page will open this dialog box. This dialog lets you create new RADIUS client entries for your device.

Click **CREATE** to save your changes.



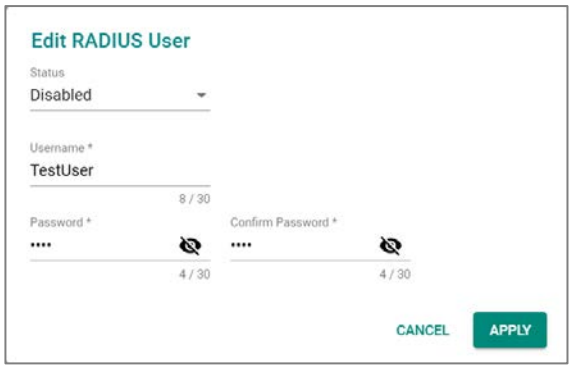
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this RADIUS client.	Enabled / Disabled	N/A
Name	Enter a name for this RADIUS client	1 to 30 characters	N/A
IP Address	Specify an IP address for the RADIUS client.	Valid IP address	N/A
Subnet Mask	Select a subnet mask for the RADIUS client.	Drop-down list of subnet masks	N/A
Share Key	Specify a share key of the RADIUS client for authentication.	1 to 30 characters	N/A
Confirm Share Key	Enter the share key again to confirm.	1 to 30 characters	N/A

Edit RADIUS Client

Menu Path: Security > RADIUS Server - RADIUS Client List

Clicking the **Edit ( )** icon on the **Security > RADIUS Server - RADIUS Client List** page will open this dialog box. This dialog lets you edit an existing RADIUS client entry for your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this RADIUS client.	Enabled / Disabled	N/A
Name	Enter a name for this RADIUS client	1 to 30 characters	N/A
IP Address	Specify an IP address for the RADIUS client.	Valid IP address	N/A
Subnet Mask	Select a subnet mask for the RADIUS client.	Drop-down list of subnet masks	N/A
Share Key	Specify a share key of the RADIUS client for authentication.	1 to 30 characters	N/A
Confirm Share Key	Enter the share key again to confirm.	1 to 30 characters	N/A

Delete RADIUS Client

Menu Path: Security > RADIUS Server - RADIUS Client List

You can delete RADIUS clients by using the checkboxes to select the clients you want to delete, then clicking the **Delete ( )** icon.

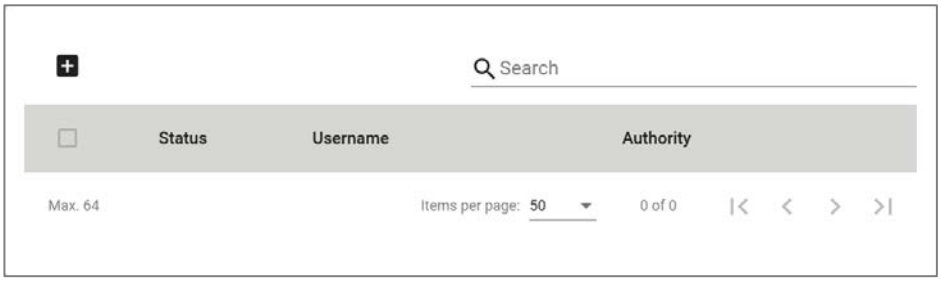
RADIUS User List

Menu Path: Security > RADIUS Server - RADIUS User List

This page lets you configure users for RADIUS server authentication.

Limitations

You can create up to 64 RADIUS authentication users.



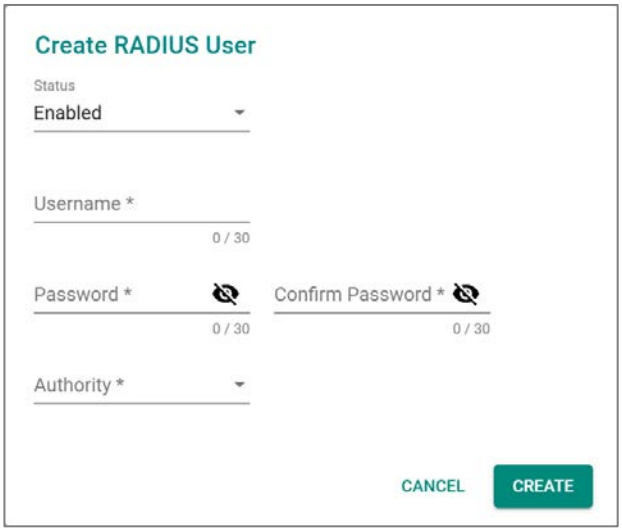
UI Setting	Description
Status	Shows the status of the authentication user.
Username	Shows the name of the authentication user.
Authority	Shows the authority level of the authentication user.

Create Authentication User

Menu Path: Security > RADIUS Server - Authentication User List

Clicking the **Add (⊞)** icon on the **Security > RADIUS Server - Authentication User List** page will open this dialog box. This dialog lets you create new authentication users for your device.

Click **CREATE** to save your changes.



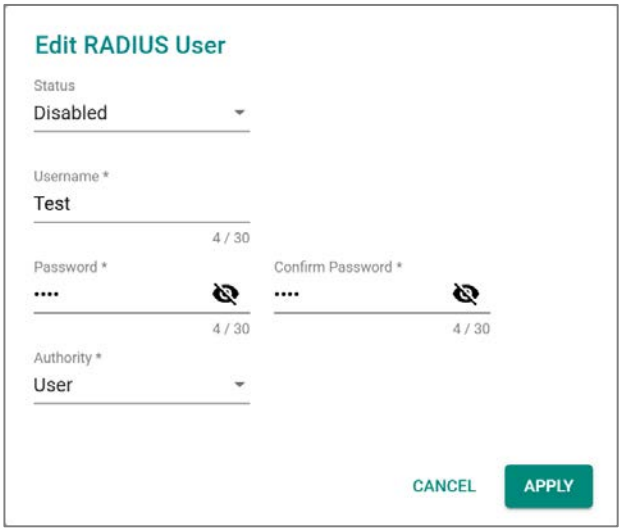
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this authentication user.	Enabled / Disabled	Enabled
Username	Enter a username for the authentication user.	1 to 30 characters	N/A
Password	Enter a password for the authentication user.	1 to 30 characters	N/A
Confirm Password	Enter the password again to confirm.	1 to 30 characters	N/A
Authority	Select the authority level of the authentication user.	Admin / User	N/A

Edit Authentication User

Menu Path: Security > RADIUS Server - Authentication User List

Clicking the **Edit ( )** icon on the **Security > RADIUS Server - Authentication User List** page will open this dialog box. This dialog lets you edit an existing authentication user for your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable this authentication user.	Enabled / Disabled	Enabled
Username	Enter a username for the authentication user.	1 to 30 characters	N/A
Password	Enter a password for the authentication user.	1 to 30 characters	N/A
Confirm Password	Enter the password again to confirm.	1 to 30 characters	N/A
Authority	Select the authority level of the authentication user.	Admin / User	N/A

Delete Authentication User

Menu Path: Security > RADIUS Server - Authentication User List

You can delete authentication users by using the checkboxes to select the users you want to delete, then clicking the **Delete ( )** icon.

MXview Alert Notification

Menu Path: Security > MXview Alert Notification

This page lets you configure device notifications for MXview.

This page includes these tabs:

- Security Notification Setting
- Security Status

Security Notification Setting

Menu Path: Security > MXview Alert Notification - Security Notification Setting

This page lets you configure your MXview security alert notification settings.

> **Note**
>
> Notifications are handled by the SNMP Trap function, which should be configured in advance. Refer to SNMP Trap/Inform for more information.
>
> In MXview, go to Preferences > Server > SNMP Trap Server and make sure the matching SNMP version is selected.

UI Setting	Description	Valid Range	Default Value
Firewall Event Notification	Enable or disable notifications for Firewall events. **Note** After enabling this, you will need to enable logging and select Trap as the log destination for each firewall policy and feature you want notifications for.	Enabled / Disabled	Disabled

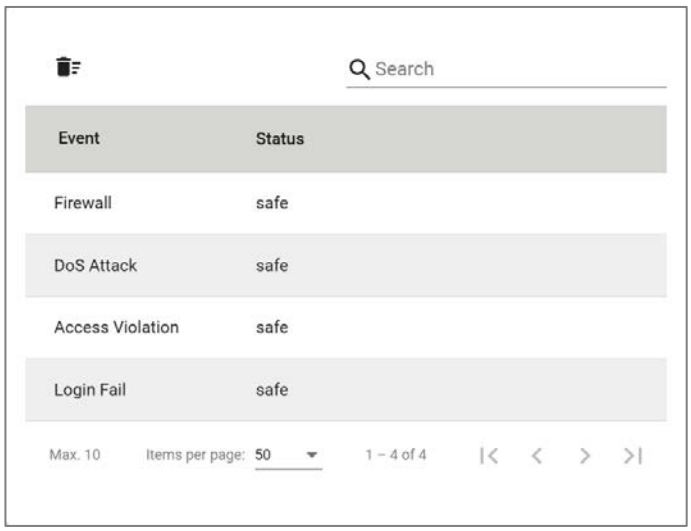
UI Setting	Description	Valid Range	Default Value
DoS Attack Event Notification	Enable or disable notifications for DoS attack events. **Note** After enabling this, you will need to go to DoS Policy to enable logging and select Trap as the log destination to receive notifications.	Enabled / Disabled	Disabled
Access Violation Event Notification	Enable or disable notifications for Access Violation events. **Note** After enabling this, you will need to go to Trusted Access to enable logging and select Trap as the log destination to receive notifications.	Enabled / Disabled	Disabled
Login Fail Event Notification	Enable or disable notifications for Login Fail events. **Note** After enabling this, you will need to go to Event Notifications to enable logging and select Trap as the log destination to receive notifications.	Enabled / Disabled	Disabled

Security Status

Menu Path: Security > MXview Alert Notification - Security Status

This page lets you see the status of all MXview security event types.

Clicking the **Reset ( )** icon will clear the status of all events to default (**safe**).



UI Setting	Description
Event	Shows the name of the event type. Event types shown will vary depending on the device model. **Note** The status of Device Lockdown can not be accessed in MXview One.
Status	Shows the current status of the event type. • **safe**: No event of this type has been detected. • **attacked**: An event of this type was detected.

Diagnostics

Menu Path: Diagnostics

The Diagnostics settings area lets you keep track of system and network performance, check event logs, and check the status of the port connectors.

This settings area includes these sections:

- System Status
- Network Status
- Event Logs and Notifications
- Tools
- Asset Recognition

Diagnostics - User Privileges

Privileges to Diagnostics settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
System Status			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Connection Management	R/W	R/W	R
Duplicate IP Detection	R/W	R/W	R
Event Log and Notifications			

Settings	Admin	Supervisor	User
Event Log	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R	R
SNMP Trap / Inform	R/W	-	-
Email Settings	R/W	R	R
SMS Settings	R/W	R	R
Tools			
Diagnostic Support	R/W	R/W	R
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R
Netflow	R/W	R/W	R
Asset Recognition	R/W	R/W	-

System Status

Menu Path: Diagnostics > System Status

This section lets you check on various system statuses.

This section includes these pages:

- Utilization
- Fiber Check

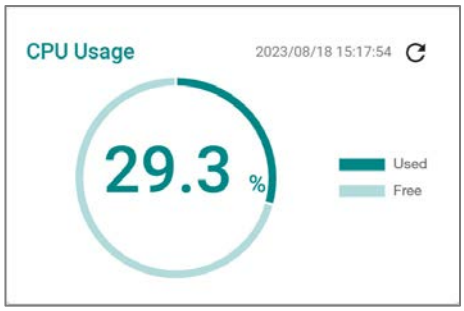
Utilization

Menu Path: Diagnostics > System Status > Utilization

This page lets you monitor current and historical system resource utilization.

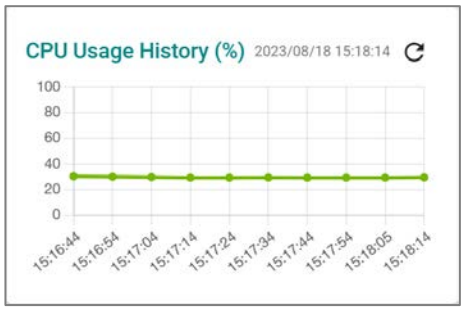
CPU Usage

This shows the current CPU usage of your device.



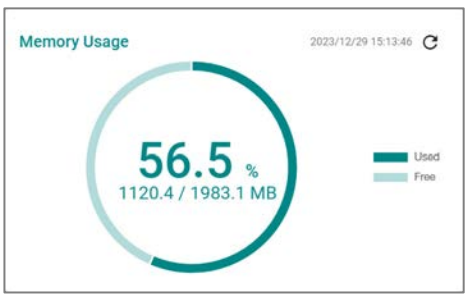
CPU Usage History

This shows the CPU usage of your device over time.



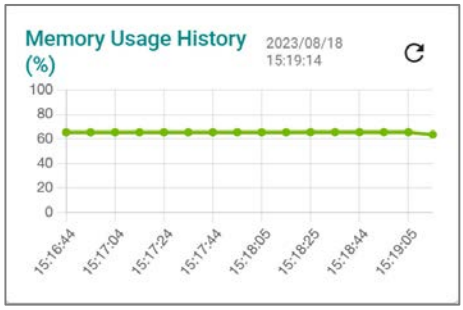
Memory Usage

This shows your device's current memory usage.



Memory Usage History

This shows your device's memory usage over time.



Fiber Check

Menu Path: Diagnostics > System Status > Fiber Check

This page lets you diagnose the link status of the device's fiber connectors, including SFP and fixed type (multi-mode SC/ST and single-mode SC) connectors. It lets you monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly.

You can enable trap, email warning, and/or relay warning functions to receive an alarm or relay if one of the fiber ports exceeds the temperature or power threshold for that port. Refer to Event Logs and Notifications for more information.

This page includes these tabs:

- Status
- Threshold Settings

Fiber Check - Status

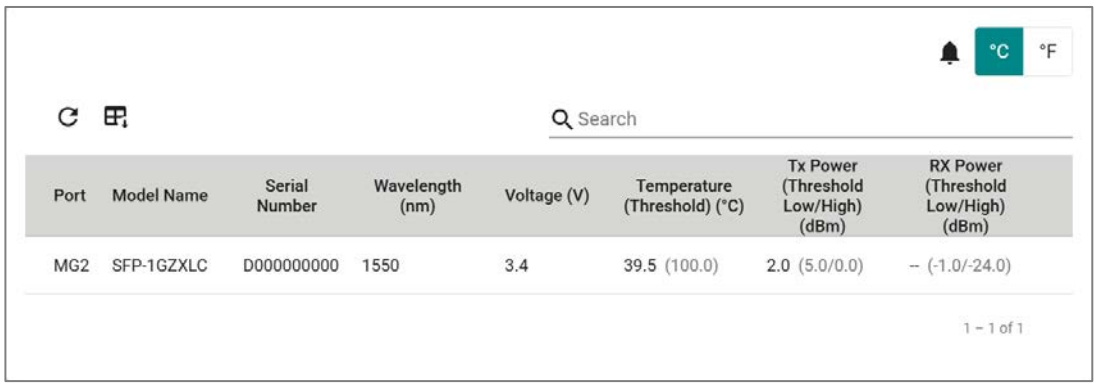
Menu Path: Diagnostics > System Status > Fiber Check - Status

This page lets you manage and view the status of your device's fiber ports.

Fiber Check Settings

UI Setting	Description	Valid Range	Default Value
Fiber Check	Enable or disable the fiber check feature.	Enabled / Disabled	Disabled

Fiber Check Status List



UI Setting	Description
Port	Shows the port the entry is for.
Model Name	Shows the model name of the port.
Serial Number	Shows the serial number of the port.
Wavelength (nm)	Shows the wavelength in nm of the port.
Voltage (V)	Shows the voltage in V of the port.
Temperature (Threshold)	Shows the current temperature of the port, and the low and high temperature thresholds in parentheses ( ). You can change between C and F temperatures by using the buttons at the top of the table.
Tx Power (Threshold Low/High) (dBm)	Shows the current Tx power in dBm of the port, and the low and high thresholds for Tx power in parentheses ( ).
Rx Power (Threshold Low/High) (dBm)	Shows the current Rx power in dBm of the port, and the low and high thresholds for Rx power in parentheses ( ).

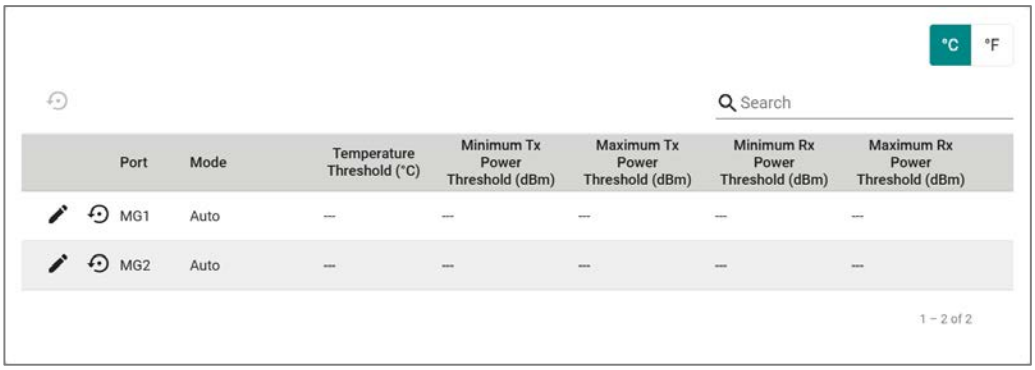
Fiber Check - Threshold Settings

Menu Path: Diagnostics > System Status > Fiber Check - Threshold Settings

This page lets you configure fiber check threshold parameters for sending event notifications.

Select the **Reset ( )** icon for a port to reset its thresholds to the defaults.

Select the **Reset ( )** icon for the table to reset all port thresholds to their defaults.



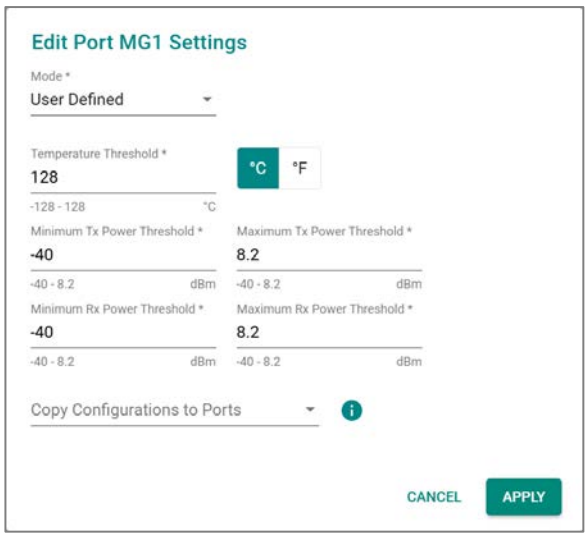
UI Setting	Description
Port	Shows the port the entry is for.
Mode	Shows whether the port is using Auto or User Defined threshold settings.
Temperature Threshold (°C)	Shows the temperature threshold for the port. An event will be triggered if the temperature goes above this threshold. You can change between °C and °F temperatures by using the buttons at the top of the table.
Minimum Tx Power Threshold (dBm)	Shows the low threshold for Tx power in dBm. An event will be triggered if Tx power goes below this threshold.
Maximum Tx Power Threshold (dBm)	Shows the high threshold for Tx power in dBm. An event will be triggered if Tx power goes above this threshold.
Minimum Rx Power Threshold (dBm)	Shows the low threshold for Rx power in dBm. An event will be triggered if Rx power goes below this threshold.
Maximum Rx Power Threshold (dBm)	Shows the high threshold for Rx power in dBm. An event will be triggered if Rx power goes above this threshold.

Fiber Check - Threshold Settings - Edit Port Settings

Menu Path: Diagnostics > System Status > Fiber Check - Threshold Settings

Clicking the **Edit ( )** icon for a port on the **Diagnostics > System Status > Fiber Check - Threshold Settings** page will open this dialog box. This dialog lets you edit the threshold settings for the port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Mode	Specify how fiber check threshold values should be set. • **Auto:** Threshold values will be automatically specified. Refer to Fiber Check Threshold Values for Auto Mode for more information. • **User Defined**: Threshold values are manually specified.	Auto / User Defined	Auto
Temperature Threshold	Specify the temperature threshold for the port. An event will be triggered if the temperature goes above this threshold. You can change between °C and °F temperatures by using the drop-down menu to the right.	°C: -128 to 128 °F: -198.4 to 262.4	°C: 128 °F: 262.4
Minimum Tx Power Threshold	Specify the low threshold for Tx power in dBm. An event will be triggered if Tx power goes below this threshold.	-40 to 8.2	-40

UI Setting	Description	Valid Range	Default Value
Maximum Tx Power Threshold	Specify the high threshold for Tx power in dBm. An event will be triggered if Tx power goes above this threshold.	-40 to 8.2	8.2
Minimum Rx Power Threshold	Specify the low threshold for Rx power in dBm. An event will be triggered if Rx power goes below this threshold.	-40 to 8.2	-40
Maximum Rx Power Threshold	Specify the high threshold for Rx power in dBm. An event will be triggered if Rx power goes above this threshold.	-40 to 8.2	8.2
Copy Configurations to Ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	Drop-down list of ports

Network Status

Menu Path: Diagnostics > Network Status

This section lets you check on the status of your device's network connections.

This section includes these pages:

- Network Statistics
- LLDP
- ARP Table
- Connection Management
- Duplicate IP Detection

Network Statistics

Menu Path: Diagnostics > Network Status > Network Statistics

This page lets you see the real-time packet and bandwidth status for your device.

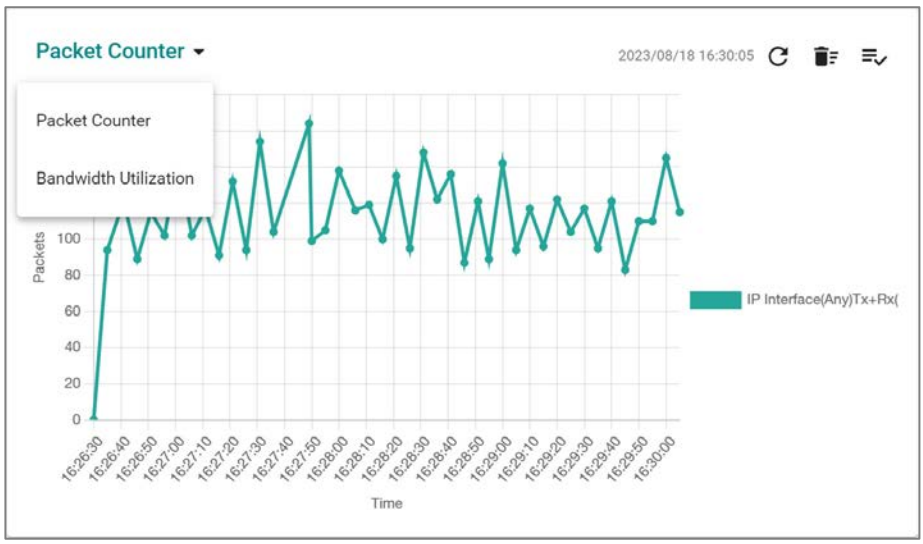
Network Status Display

This display lets you switch between **Packet Counter** and **Bandwidth Utilization** views by clicking on the drop-down menu.

- **Packet Counter**: This view shows how many packets are being handled over time. This view updates every 5 seconds.
- **Bandwidth Utilization**: This view shows bandwidth utilization over time. This view updates every 3 seconds.

Note

The default line shows activity for all IP interfaces for both Tx and Rx activity. You can add additional lines by clicking the Display Settings button.



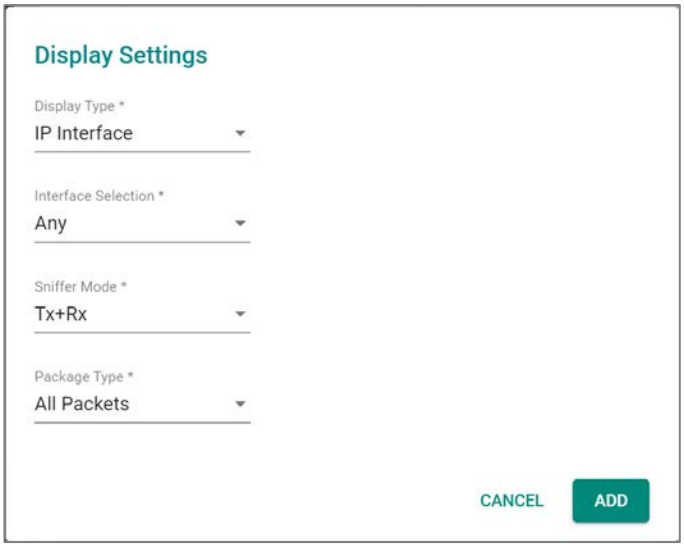
UI Setting	Description
Refresh ( )	Updates statistics immediately without waiting for the refresh interval.
Reset Statistics Graph ( )	Clears the display and resets display settings back to defaults.
Display Settings ( )	Opens **Display Settings**, which allows you to add lines based on user-defined criteria.

Display Settings

Menu Path: Diagnostics > Network Status > Network Statistics

Clicking the **Display Settings ( )** icon on the **Diagnostics > Network Status > Network Statistics** page will open this dialog box. This dialog lets you define additional interfaces or ports to monitor.

Click **ADD** to save your changes and add the new line.

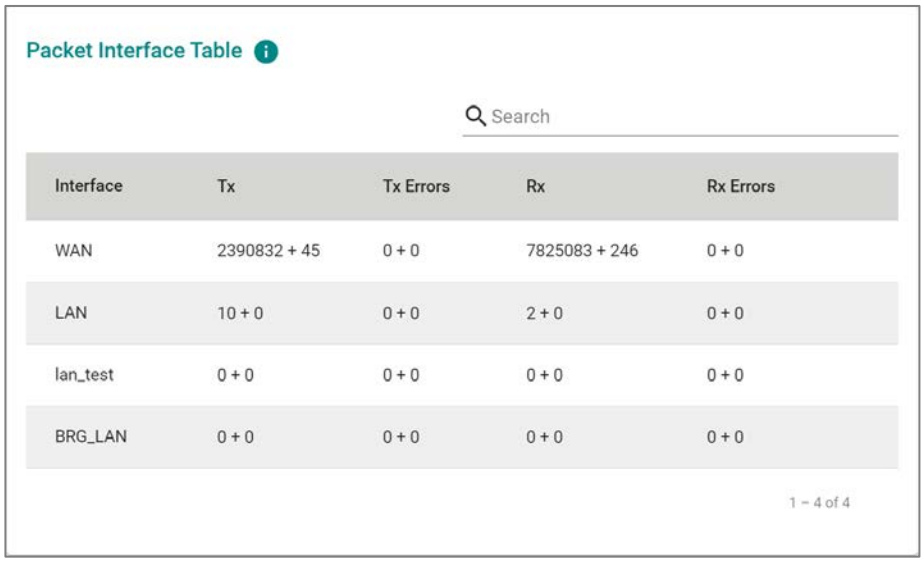


UI Setting	Description	Valid Range	Default Value
Display Type	Select whether to monitor an IP interface or a port. • **Port**: Monitor traffic for a specific port. • **IP Interface**: Monitor traffic for a specific network interface.	Port / IP Interface	IP Interface
Interface Selection **(If Display Type is IP Interface)**	Select which interface to monitor. **Note** Available interfaces will vary depending on your product model and configuration. Refer to Network Interfaces for more information about managing your device's interfaces.	Drop-down list of interfaces	Any

UI Setting	Description	Valid Range	Default Value
Port Selection (If Display Type is Port)	Select which port to monitor. **Note** Available ports will vary depending on your product model.	Drop-down list of ports	All ports
Sniffer Mode	Select which type of traffic to monitor. • **Tx+Rx**: Monitor both transmit and receive traffic. • **Tx**: Only monitor transmit traffic. • **Rx**: Only monitor receive traffic.	Tx+Rx / Tx / Rx	Tx+Rx
Package Type	Select which packet type to monitor. • **All Packets**: Monitor all packet types. • **Unicast**: Only monitor unicast packets. • **Broadcast**: Only monitor broadcast packets. • **Multicast**: Only monitor multicast packets. • **Error Packets**: Only monitor error packets. **Note** If Display Type is IP Interface, only All Packets and Error Packets will be available.	All Packets / Unicast / Broadcast, Multicast / Error Packets	All Packets

Packet Interface Table

This table shows how many packets are being handled by each interface. Values are shown as *Total Packets + Packets in the past 5 seconds*.



LLDP Settings

Menu Path: Diagnostics > Network Status > LLDP

This page lets you configure Link Layer Discovery Protocol (LLDP) settings.

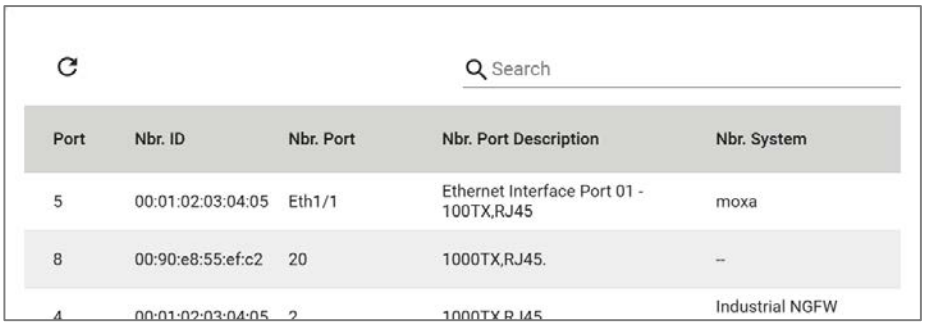
LLDP Settings

UI Setting	Description	Valid Range	Default Value
LLDP	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled
Transmit Interval	Specify the interval in seconds at which LLDP messages are sent.	5 to 32768	30

LLDP Ring Port Bypass Settings

UI Setting	Description	Valid Range	Default Value
LLDP Ring Port Bypass	Enable or disable LLDP Ring Port Bypass.	Enabled / Disabled	Disabled

LLDP Status List



UI Setting	Description
Port	Shows the number of the port that connects to the neighbor device.
Nbr. ID	Shows the unique ID (typically the MAC address) that identifies the neighbor device.
Nbr. Port	Shows the port number of the connected neighbor device's interface that is used to connect to this device.
Nbr. Port Description	Shows the port description of the connected neighbor device's interface that is used to connect to this device.
Nbr. System	Shows the hostname of the neighbor device.

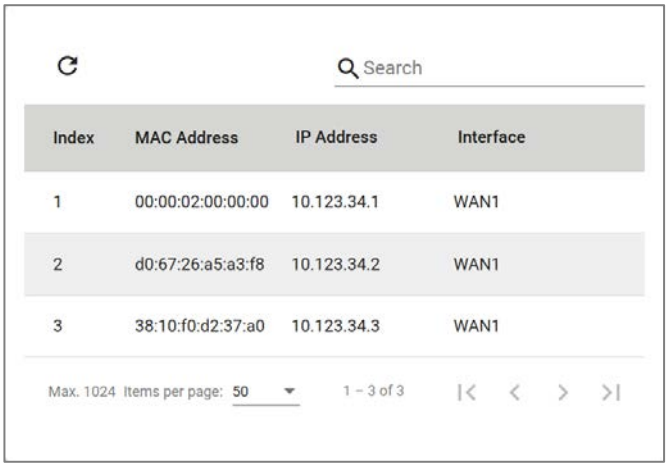
ARP Table

Menu Path: Diagnostics > Network Status > ARP Table

This page lets you see the device's Address Resolution Protocol (ARP) table.

Limitations

The ARP table can show up to 1024 entries.



UI Setting	Description
Index	Shows the index of the device entry.
MAC Address	Shows the MAC address of the device.
IP Address	Shows the IP address used for the device.
Interface	Shows the interface the device is connecting through.

Connection Management

Menu Path: Diagnostics > Network Status > Connection Management

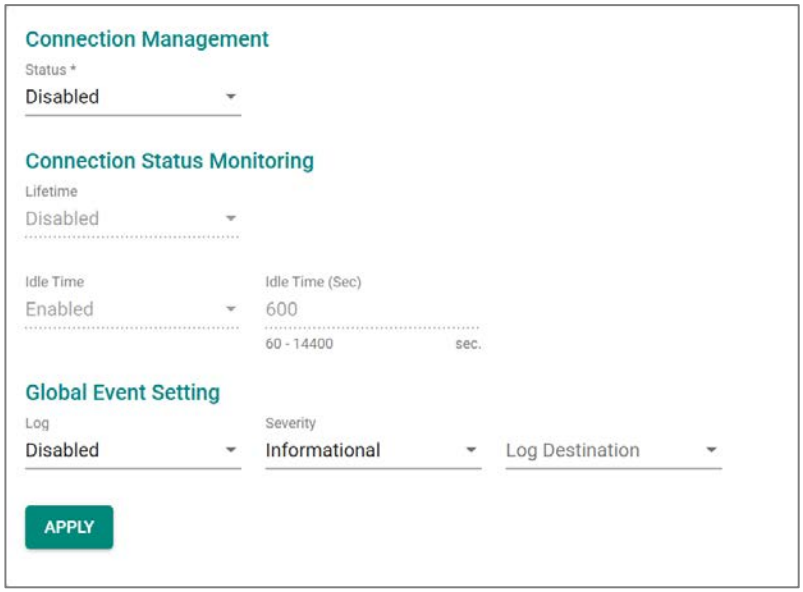
This page lets you configure the Connection Management feature of your device.

Click **APPLY** to save your changes.

Connection Management Settings

Note

New connections cannot be made if the Total TCP Connection limit is reached for an applicable session control policy, or if the device limit of 10000 connections is reached. Refer to Session Control for more information about session control policies.



Connection Management

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable connection management.	Enabled / Disabled	Disabled

Connection Status Monitoring

UI Setting	Description	Valid Range	Default Value
Lifetime	Enable or disable connection management through connection lifetime monitoring. Disabling this means that connections will have an infinite lifetime and will not be deleted.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Lifetime (Sec) **(If Lifetime is Enabled)**	Specify the maximum lifetime of a connection in seconds before it will be deleted.	300 to 14400	N/A
Idle Time	Enable or disable connection management through connection idle time monitoring.	Enabled / Disabled	Enabled
Idle Time (Sec) **(If Idle Time is Enabled)**	Specify the maximum idle time of a connection in seconds before deleting the connection. Longer idle times allow connections to stay open without relying on clients to send keep-alive messages.	60 to 14400	600

Global Event Setting

UI Setting	Description	Valid Range	Default Value
Log	Enable or disable logging of connection management events.	Enabled / Disabled	Disabled
Severity	Select the severity level to assign events for this policy. Refer to the Severity Level List for more information about severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	
Log Destination	Specify where to send logs for this event. You can select multiple options. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • Local Storage: Event logs will be stored on local storage and will show up in the device's Event Log. Refer to Event Log for more information.	Syslog / Trap / Local Storage	None

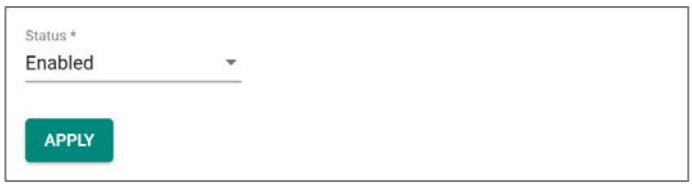
Connection Table

UI Setting	Description
ID	Shows the ID of the connection the entry is for.
Incoming Interface	Shows the incoming interface for the connection.
Outgoing Interface	Shows the outgoing interface for the connection.
Source IP	Shows the source IP address for the connection.
Source Port	Shows the source port for the connection.
Destination IP	Shows the destination IP address for the connection.
Destination Port	Shows the destination port for the connection.
IP Protocol	Shows whether the connection uses TCP, UDP, ICMP, or an unknown protocol.
Packets	Shows how many packets have been transferred for the connection.
Lifetime	Shows how long the connection has been up.
Remaining Time	Shows how much time is remaining for the connection before it is deleted.
Lifetime Management	If Connection Management is enabled, clicking **EXTEND** will reset the remaining time for the connection to the specified **Lifetime (sec)** value. Refer to Connection Management Settings for more information.
Idle Timeout	Shows the allowable idle time for the connection.

Duplicate IP Detection

Menu Path: Diagnostics > Network Status > Duplicate IP Detection

This page lets you enable Duplicate IP Detection, which triggers a system event if duplicate IPs are detected on an interface.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the Duplicate IP Detection function. When enabled, the device monitors ARP traffic on all LAN/Bridge interfaces and triggers a system event whenever it sees the same IP address associated with two different MAC addresses on the same interface. Refer to Event Notifications - System for more information.	Enabled / Disabled	Enabled

Event Logs and Notifications

Menu Path: Diagnostics > Event Logs and Notifications

This section lets you set up and view your device's event logs and notifications.

This section includes these pages:

- Event Log
- Event Notifications
- Syslog
- SNMP Trap/Inform
- Email Settings
- SMS Settings

Event Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log

This page lets you browse and export your device's various event logs to PDF, JSON, or Excel files.

> **Note**
>
> Browser extensions such as ad blockers may interfere with file exports.
>
> If you encounter this issue, we strongly recommend using a recommended browser and disabling any plug-ins. Refer to Using a Web Browser to Configure the Industrial Secure Router for more information.

This page includes these tabs:

- System Log
- Firewall Log
- VPN Log
- Network Log
- Asset Recognition
- Settings and Backup

> **Note**
>
> The timestamp on event logs will automatically synchronize with the NTP/SNTP server and applies to all new event logs. Refer to System > Time > NTP/SNTP Server for more details.

System Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - System Log

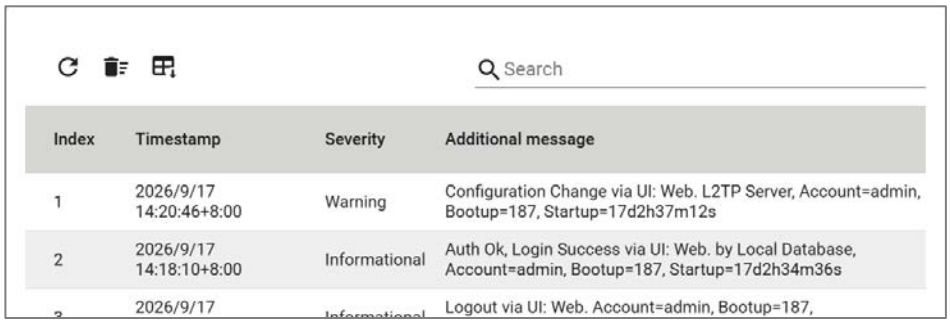
This page lets you view your device's system-related event logs.

Limitations

The system log can record up to 1000 events.

Actions

- Click the **Refresh icon ( )** to refresh the logs.
- Click the **Clear System Log icon ( )** to delete all logs.
- Click the **Export icon ( )** to export all logs to a file.



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Additional message	Shows additional information about the event, based on the type of event. The username of the account will also be recorded for the following events: **Login Success, Login Fail**, **Configuration Change**, **User Logout**.

Firewall Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Firewall Log

This page lets you view your device's firewall-related event logs.

Limitations

Each firewall log can record up to 1000 events.

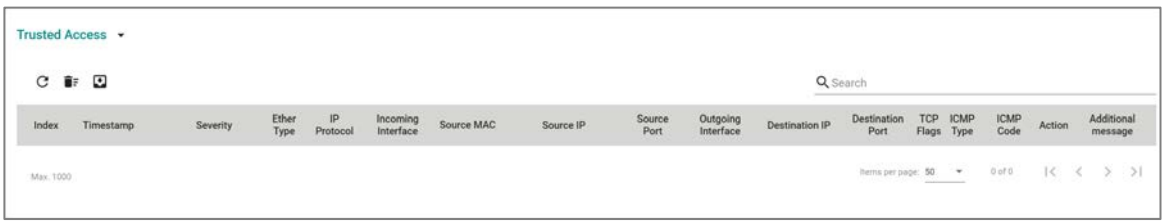
You can switch between different firewall logs by clicking on the drop-down menu.

- Trusted Access
- Malformed Packets
- DoS Policy
- Layer 3-7 Policy
- Protocol Filter Policy
- ADP
- IPS
- Session Control
- Layer 2 Policy
- Ping Response
- Domain Protection
- Device Lockdown

Actions

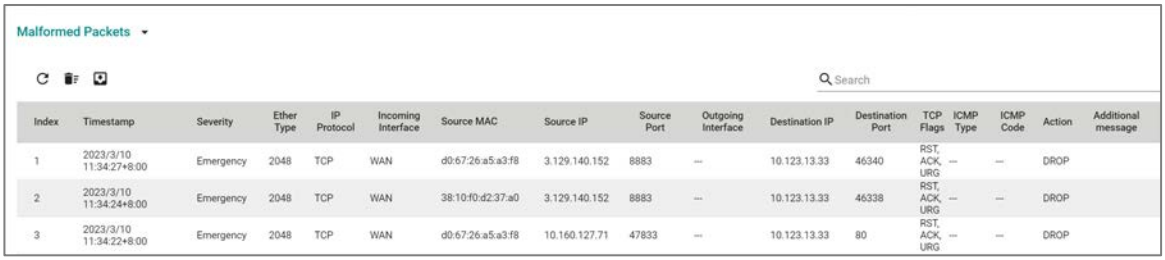
- Click the **Refresh icon ( )** to refresh the logs.
- Click the **Clear System Log icon ( )** to delete all logs.
- Click the **Export icon ( )** to export all logs to a file.

Trusted Access



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

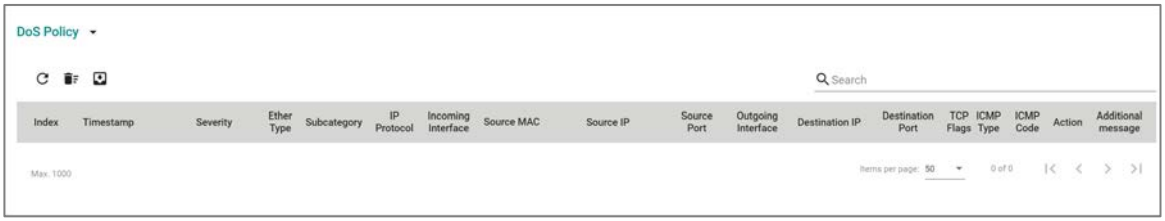
Malformed Packets



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.

UI Setting	Description
Action	Shows the action taken by the firewall for this event: • Aceept • Drop
Additional message	Shows additional information about the event, based on the type of event.

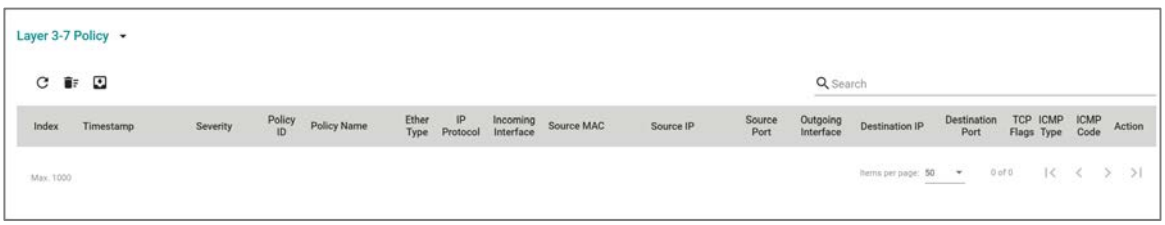
DoS Policy



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
Subcategory	Shows the subcategory that applies to this event: • Null Scan • Xmas Scan • NMAP-Xmas Scan • SYN/FIN Scan • FIN Scan • NMAP-ID Scan • SYN/RST Scan • NEW-TCP-Without-SYN Scan • ICMP-Death • SYN-Flood • ARP-Flood • UDP-Flood

UI Setting	Description
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

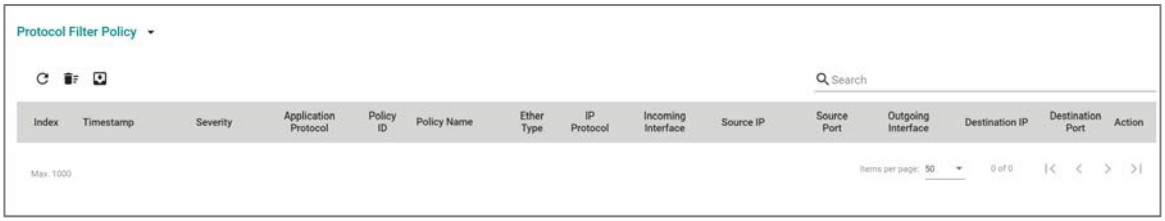
Layer 3-7 Policy



UI Setting	Description
Index	Shows the index of the event.

UI Setting	Description
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event: • Allow • Deny

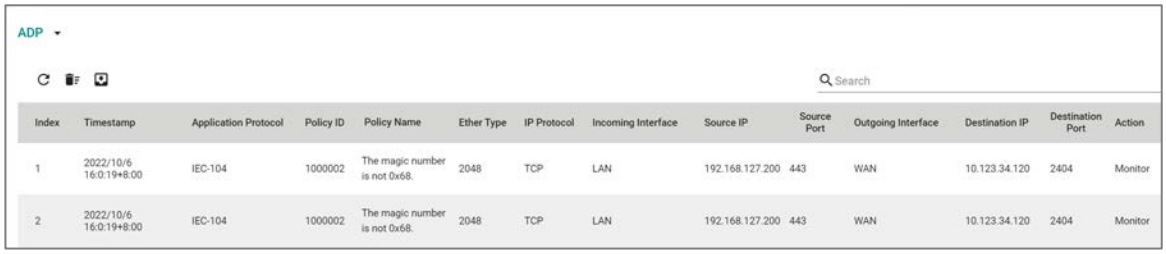
Protocol Filter Policy



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Application Protocol	Shows which application this event is related to.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherTypes for this traffic.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags for this traffic.

UI Setting	Description
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.

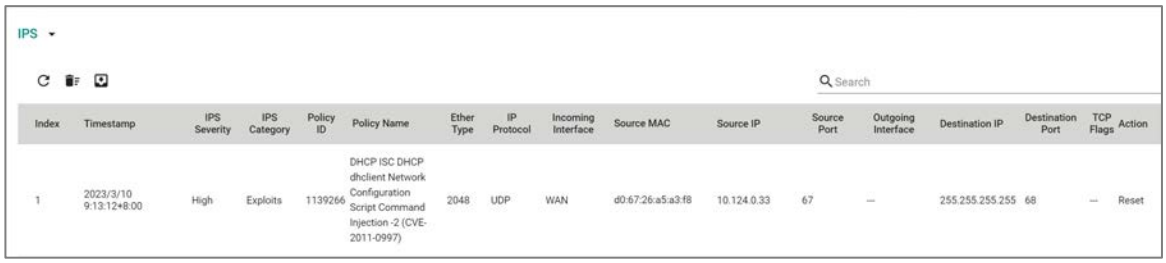
ADP



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Application Protocol	Shows the application protocol that applies to this event.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
Subcategory	Shows the subcategory that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.

UI Setting	Description
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
Action	Shows the action taken by the firewall for this event: • **Accept**: The traffic will be allowed to pass through. • **Reset**: The traffic will not be allowed to pass through. • **Monitor**: The traffic will be allowed to pass through, but a log entry will be created for it.

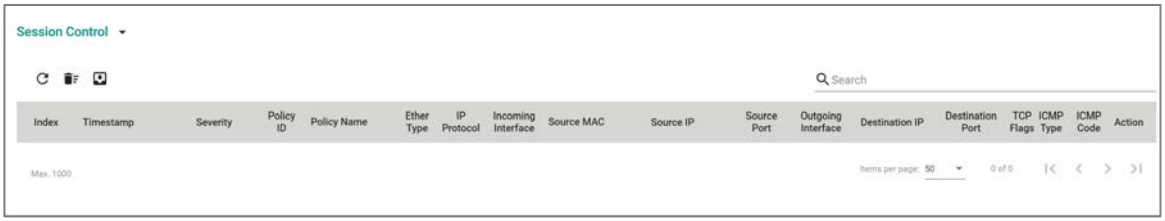
IPS



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
IPS Severity	Shows the IPS severity of the event: • Information • Low • Medium • High • Critical

UI Setting	Description
IPS Category	Shows the IPS category of the event: • File vulnerabilities • Buffer overflow • DoS attacks • Exploits • Malware traffic • Reconnaissance • Web threats • Flooding & scan • Protocol attack protection • IP spoofing
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
Action	Shows the action taken by the firewall for this event.

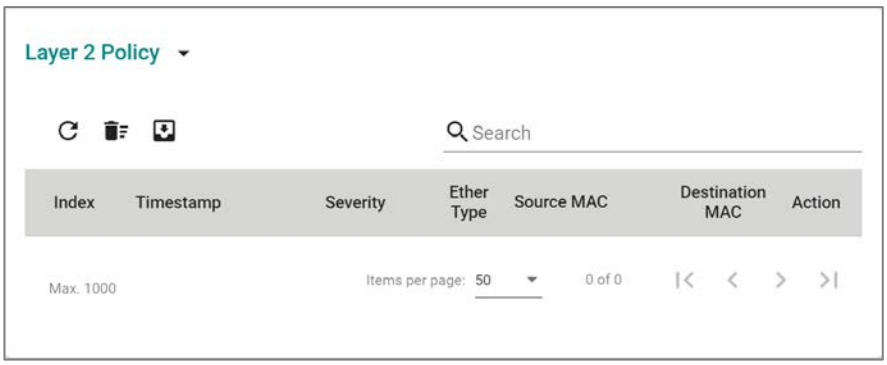
Session Control



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Policy Name	Shows the name of the firewall policy that applies to this event.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.

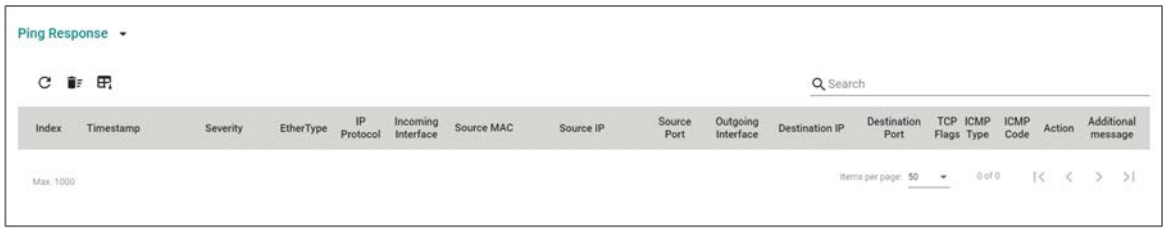
UI Setting	Description
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.

Layer 2 Policy



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
Source MAC	Shows the source MAC address for this traffic.
Destination MAC	Shows the destination MAC address for this traffic.
Action	Shows the action taken by the firewall for this event: • Allow • Deny

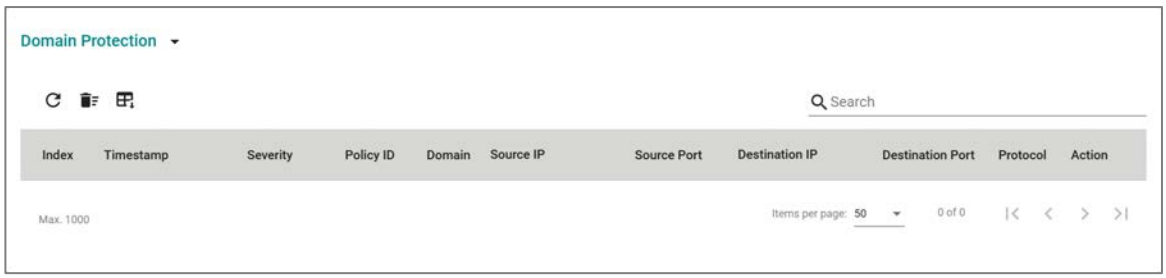
Ping Response



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.

UI Setting	Description
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

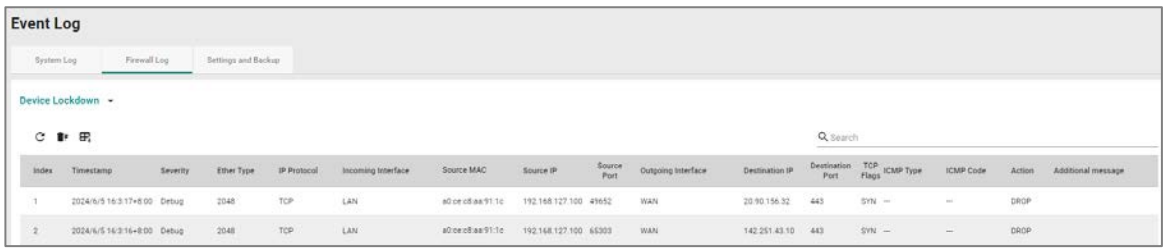
Domain Protection



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Policy ID	Shows the ID of the firewall policy that applies to this event.
Domain	Shows the domain of this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
Protocol	Shows the IP protocol for this traffic.
Action	Shows the action taken by the firewall for this event.

Device Lockdown

> **Note**
>
> Device Lockdown is specifically designed for and will only be available on the NAT series.



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Ether Type	Shows the EtherType that applies to this event.
IP Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for this traffic.
Source MAC	Shows the source MAC address for this traffic.
Source IP	Shows the source IP address for this traffic.
Source Port	Shows the source port for this traffic.
Outgoing Interface	Shows the destination interface for this traffic.
Destination IP	Shows the destination IP address for this traffic.
Destination Port	Shows the destination port for this traffic.
TCP Flags	Shows the TCP flags that apply to this event.

UI Setting	Description
ICMP Type	Shows the ICMP type that applies to this event.
ICMP Code	Shows the ICMP code that applies to this event.
Action	Shows the action taken by the firewall for this event.
Additional Message	Shows the additional message for this event.

VPN Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - VPN Log

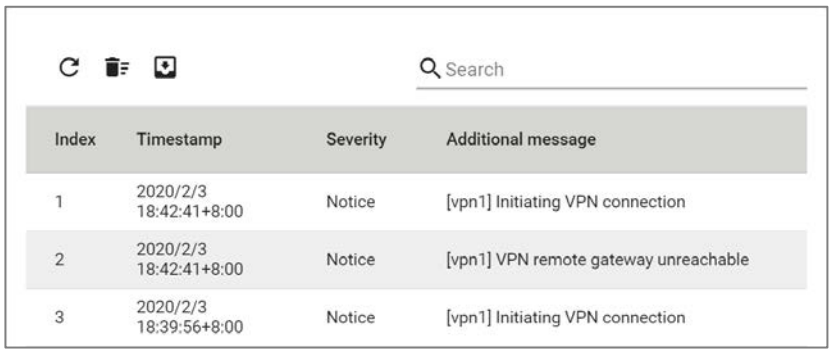
This page lets you view your device's VPN-related event logs.

Limitations

The VPN log can record up to 1000 events.

Actions

- Click the **Refresh icon ( )** to refresh the logs.
- Click the **Clear System Log icon ( )** to delete all logs.
- Click the **Export icon ( )** to export all logs to a file.



UI Setting	Description
Index	Shows the index of the event.

UI Setting	Description
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event.
Additional message	Shows additional information about the event, based on the type of event.

Network Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Network Log

This page lets you view your device's network-related event logs.

Limitations

Each network log can record up to 1000 events.

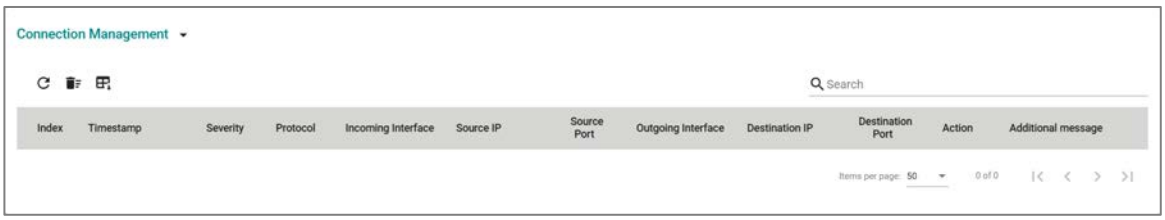
You can switch between different network logs by clicking on the drop-down menu.

- Connection Management
- RX Discard
- Neighbor MAC Change

Actions

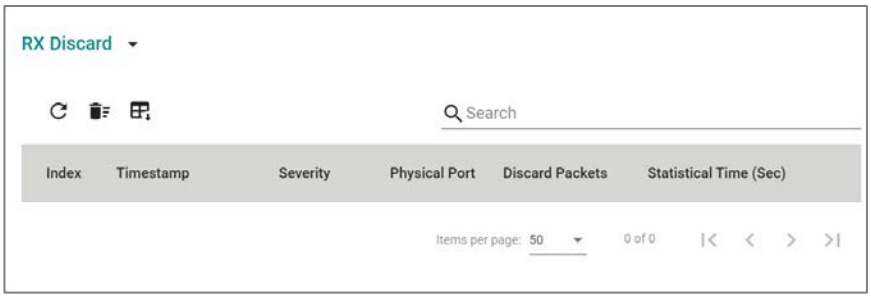
- Click the **Refresh icon ( )** to refresh the logs.
- Click the **Clear System Log icon ( )** to delete all logs.
- Click the **Export icon ( )** to export all logs to a file.

Network Log - Connection Management



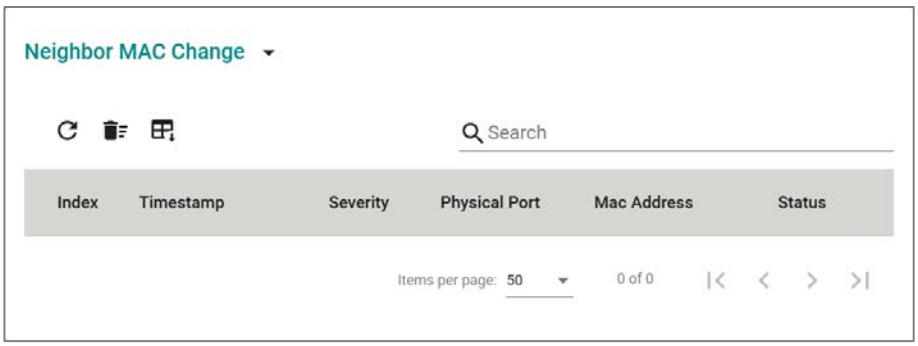
UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Protocol	Shows the IP protocol for this traffic.
Incoming Interface	Shows the incoming interface for the connection.
Source IP	Shows the source IP address for the connection.
Source Port	Shows the source port for the connection.
Outgoing Interface	Shows the outgoing interface for the connection.
Destination IP	Shows the destination IP address for the connection.
Destination Port	Shows the destination port for the connection.
Action	Shows the action taken by the firewall for this event.
Additional message	Shows additional information about the event, based on the type of event.

Network Log - RX Discard



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Physical Port	Shows which port has discarded RX packets.
Discard Packets	Shows how many RX packets were discarded. **Note** The Discard Packets count will reset after the device is rebooted.
Statistical Time (Sec)	Shows the interval in seconds between RX discard packet checks.

Network Log - Neighbor MAC Change



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Severity	Shows the severity categorization of the event: Refer to the Severity Level List for more information.
Physical Port	Shows the physical port the neghbor device is connected to.
MAC Address	Shows the new MAC address of the neighbor device.
Status	Shows the status of the neighbor MAC change event.

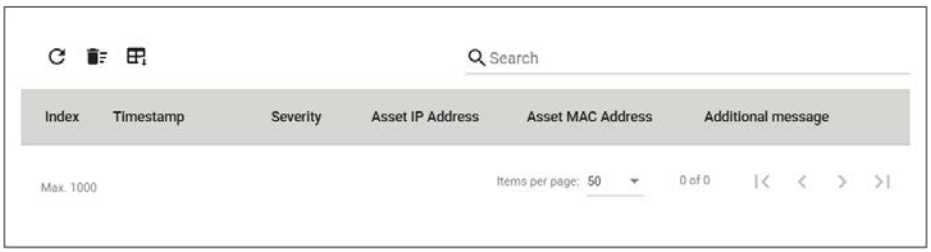
Asset Recognition Log

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Asset Recognition Log

This page lets you view your device's asset-recognition-related event logs.

Limitations

The asset recognition log can record up to 1000 events.



UI Setting	Description
Index	Shows the index of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.

UI Setting	Description
Severity	Shows the severity categorization of the event. Refer to the Severity Level List for more information.
Asset IP Address	Shows the IP address of the asset.
Asset MAC Address	Shows the MAC address of the asset.
Additional message	Shows additional information about the event, based on the type of event.

Settings and Backup

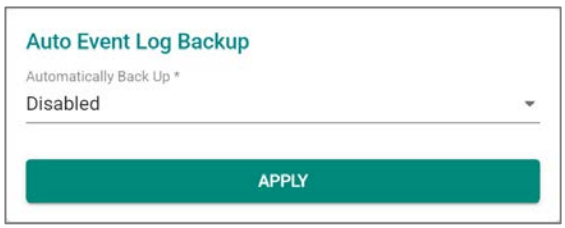
Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup

This page lets you clear all the logs or enable automatic event log backups. You can also set up capacity warnings and oversize actions that trigger when log storage has exceeded the specified storage threshold.

Clear All Logs

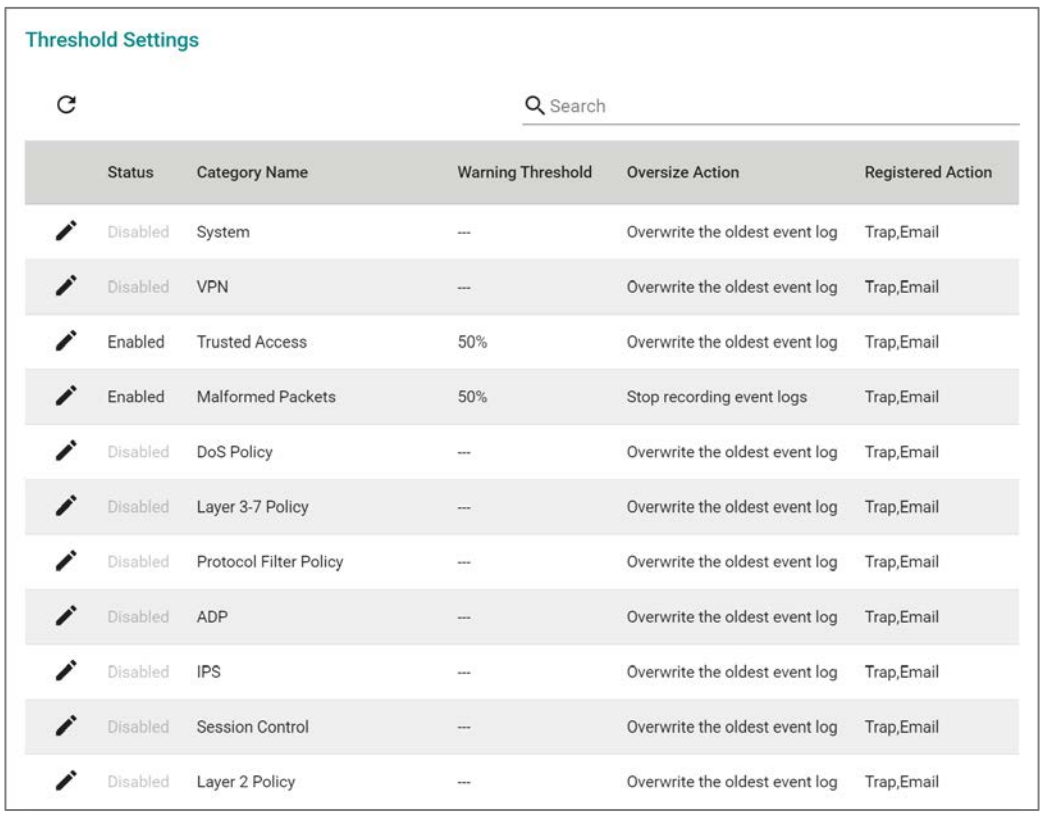
Click the **CLEAR** button to clear all event logs.

Auto Event Log Backup



UI Setting	Description	Valid Range	Default Value
Automatically Restore	Enable or disable automatic event log backups.	**Enabled / Disabled**	Disabled

Threshold Settings



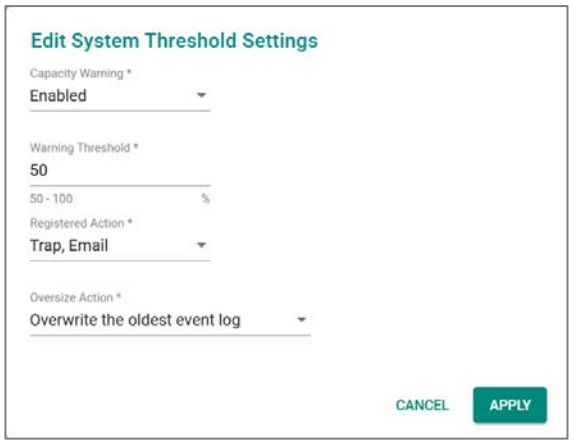
UI Setting	Description
Status	Shows whether threshold settings are enabled for the category.
Category Name	Shows which event log the threshold settings apply to.
Warning Threshold	Shows the threshold percentage that must be reached to trigger a warning sent through the **Registered Action** methods.
Oversize Action	Shows what action will be taken when log storage is full for the selected category.
Registered Action	Shows how threshold warnings will be sent.

Edit Threshold Settings

Menu Path: Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Log - Settings and Backup** page will open this dialog box. This dialog lets you edit the threshold settings the selected event log category.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Capacity Warning	Enable or disable capacity warnings for the selected event log category.	Enabled / Disabled	Disabled
Warning Threshold **(If Capacity Warning is Enabled)**	Specify the percentage threshold of how full the log must be before sending a capacity warning for the selected event log category.	50 to 100	50
Registered Action **(If Capacity Warning is Enabled)**	Select how the warning is sent. You can select multiple options. • **Trap**: A trap warning will be sent. • **Email**: A warning email will be sent.	Trap / Email	Trap, Email

UI Setting	Description	Valid Range	Default Value
Oversize Action	Select the oversize action to take when event log storage is full for the selected category. • **Overwrite the oldest event log**: The oldest events will be deleted when new events are created. • **Stop recording event logs**: No new events will be recorded.	Overwrite the oldest event log / Stop recording event logs	Overwrite the oldest event log

Event Notifications

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications

This page lets you configure notifications for various kinds of events.

This page includes these tabs:

- System
- Firewall
- Port
- CPU Usage
- Port Usage
- RX Discard
- Relay Warning

Event Notifications - System

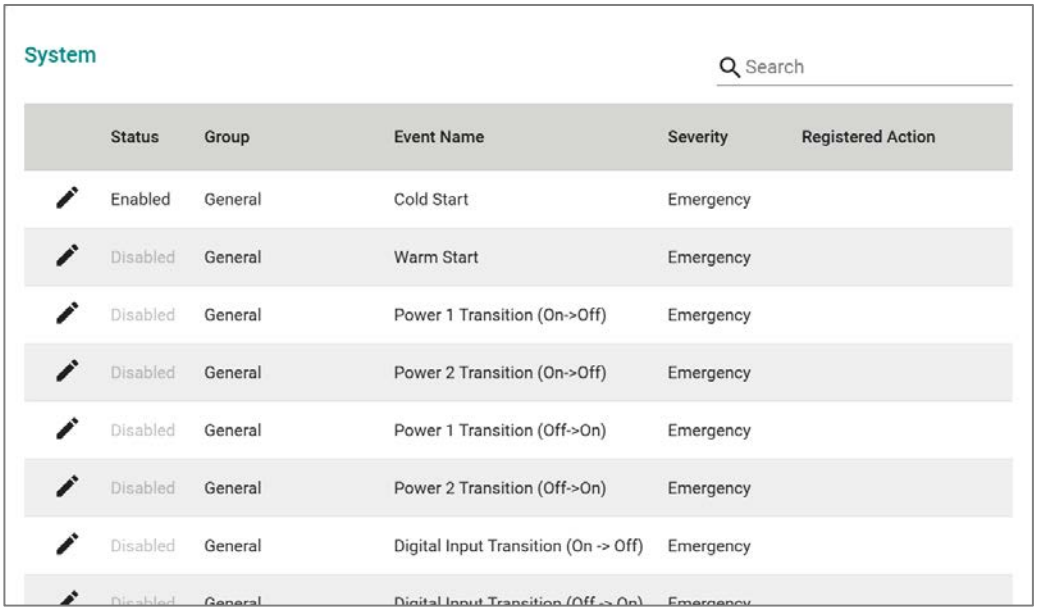
Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System

This page lets you configure notification settings for various system events related to the overall functions of the device. Each event can be configured independently with different warning methods and severity classifications.

You can switch between different system notification settings by clicking on the drop-down menu.

- System
- License

System Notification List



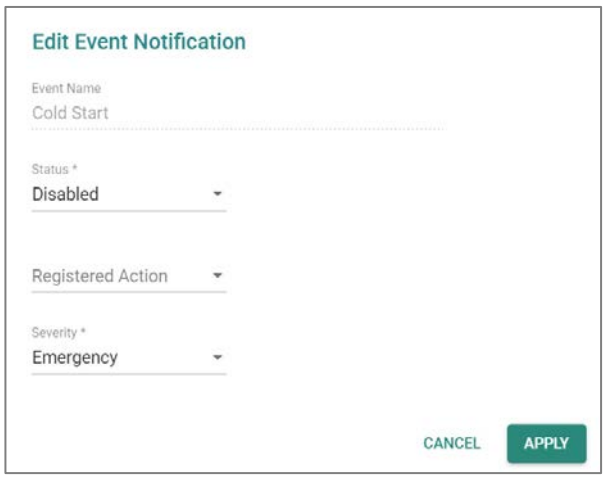
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Group	Shows which group this event belongs to.
Event Name	Shows the name of the event. Refer to the System Event List for more details.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - System - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System

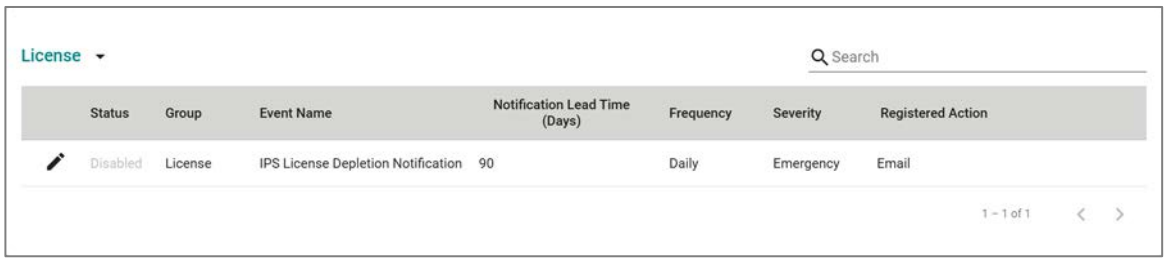
Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System** page will open this dialog box. This dialog lets you change the notification settings for the selected event.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event. Refer to the System Event List for more information.	(Fixed)	(Fixed)
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Registered Action	Specify what actions to take for this event. You can select multiple options. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Email**: A notification will be sent to the email server defined in the Email Settings section. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Relay:** A notification will be sent through the relay interface, if the device has one, when the event is triggered. The device's STATE LED will also be triggered accordingly. **Note** The types of actions available may vary depending on the event type and the device model.	Trap / Email / Syslog / Relay	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

License Notification List



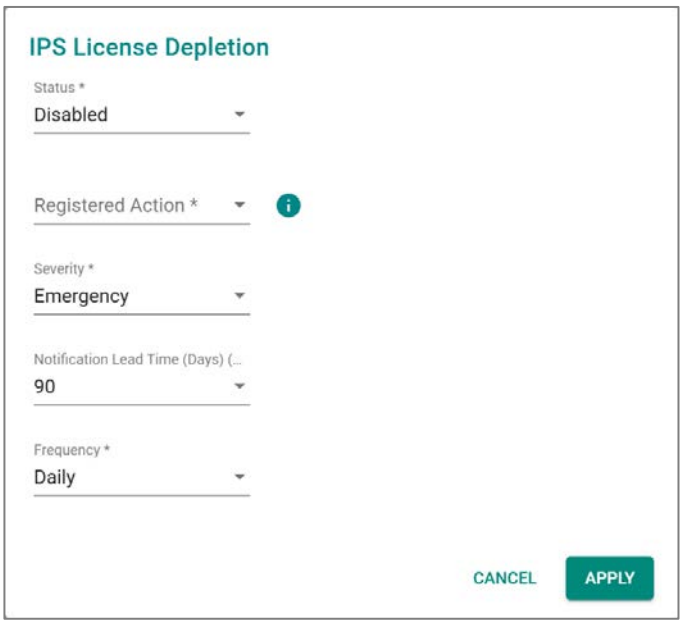
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Group	Shows which group this event belongs to.
Event Name	Shows the name of the event. Refer to the System Event List for more details.
Notification Lead Time (Days)	Shows the number of days before the expected depletion of the IPS license to send notifications.
Frequency	Shows how frequently notifications will be sent.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - System - License - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System - License

Clicking the **Edit ( )** icon for an License entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System - License** page will open this dialog box. This dialog lets you change the notification settings for the selected event.

Click **APPLY** to save your changes.



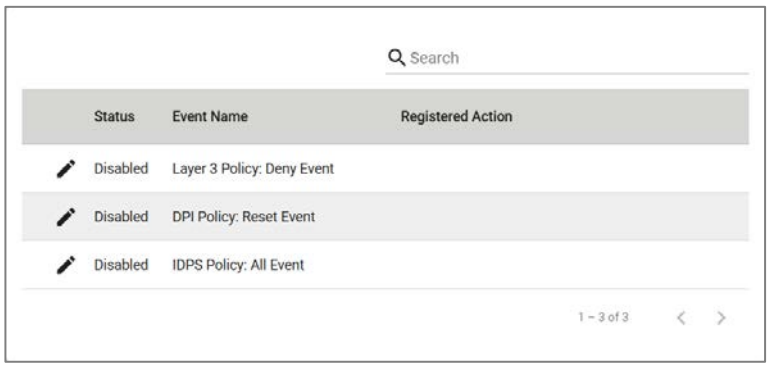
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Registered Action	Specify what actions to take for this event. You can select multiple options. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Email**: A notification will be sent to the email server defined in the Email Settings section. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. **Note** The types of actions available may vary depending on the event type and the device model.	Trap / Email / Syslog	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency
Notification Lead Time (Days)	Select the number of days before the expected depletion of the IPS license to send a notification.	30 / 60 / 90 / 180	90

UI Setting	Description	Valid Range	Default Value
Frequency	Specify how frequently the device will check for IPS license depletion and recalculate the IPS depletion rate.	Daily / Weekly / Monthly	Daily

Event Notifications - Firewall

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Firewall

This page lets you configure notification settings based on the device's firewall.



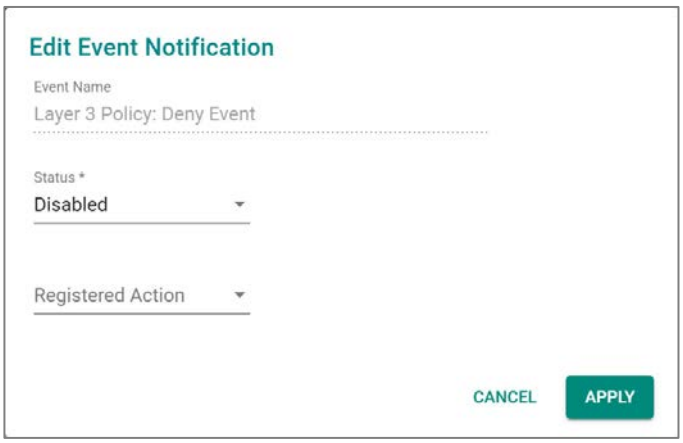
UI Setting	Description
Status	Indicates whether event notifications are enabled for the event.
Event Name	Shows the name of the firewall event.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - Firewall - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Firewall

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - Firewall** page will open this dialog box. This dialog lets you change the notification settings for the event.

Click **APPLY** to save your changes.



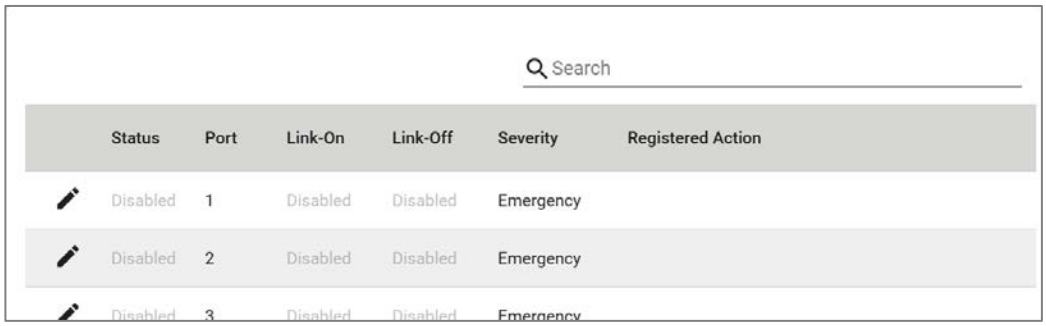
UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event.	N/A	N/A
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Registered Action	Select what actions to take for this event. You can select multiple options. • Relay: A notification will be sent through the relay interface, if the device has one, when the event is triggered. The device's STATE LED will also be triggered accordingly.	Relay	N/A

Event Notifications - Port

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port

This page lets you configure notification settings for various events related to your device's physical port status. Each port can be configured independently with different warning methods and severity classifications.

When a port event is triggered, the FAULT LED/STATE LED on your device will also light up if your device has one.



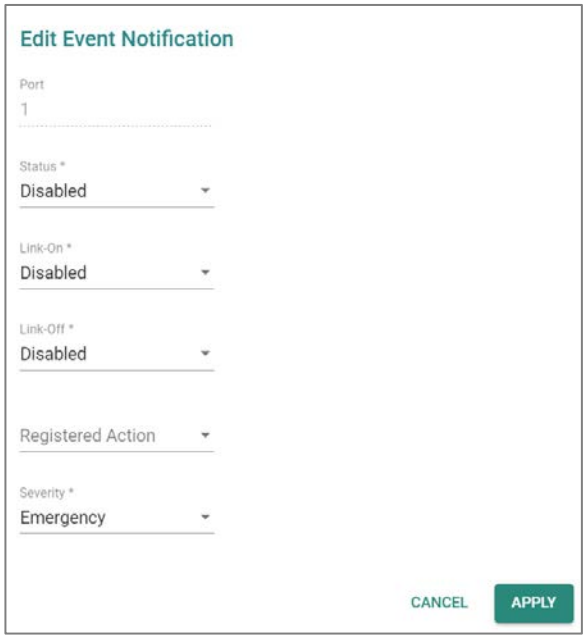
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Port	Shows which group this event belongs to.
Link-On	Shows whether notifications for Link-On events are enabled or disabled.
Link-Off	Shows whether notifications for Link-Off events are enabled or disabled.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - Port - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - Port** page will open this dialog box. This dialog lets you change the notification settings for the selected port.

Click **APPLY** to save your changes.



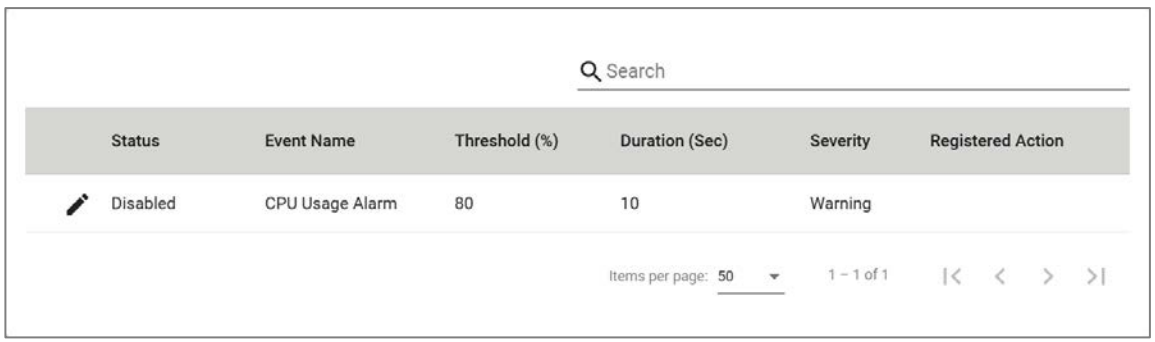
UI Setting	Description	Valid Range	Default Value
Port **(View-only)**	Shows which physical port the event notifications are for. **Note** Available ports will vary depending on your product and model.	N/A	N/A
Status	Enable or disable notifications for this port.	Enabled / Disabled	Disabled
Link-On	Enable or disable notifications for Link-On events. If enabled, an event will be triggered when a device connects to the port.	Enabled / Disabled	Disabled
Link-Off	Enable or disable notifications for Link-Off events. If enabled, an event will be triggered when the port is disconnected from a device, such as when a cable is unplugged or the connected device is shut down.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Registered Action	Select what actions to take for this event. You can select multiple options. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Email**: A notification will be sent to the email server defined in the Email Settings section. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Relay:** A notification will be sent through the relay interface, if the device has one, when the event is triggered. The device's STATE LED will also be triggered accordingly. **Note** The types of actions available may vary depending on the event type and the device model.	Trap / Email / Syslog / Relay	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Emergency

Event Notifications - CPU Usage

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage

This page lets you configure notification settings based on CPU usage.



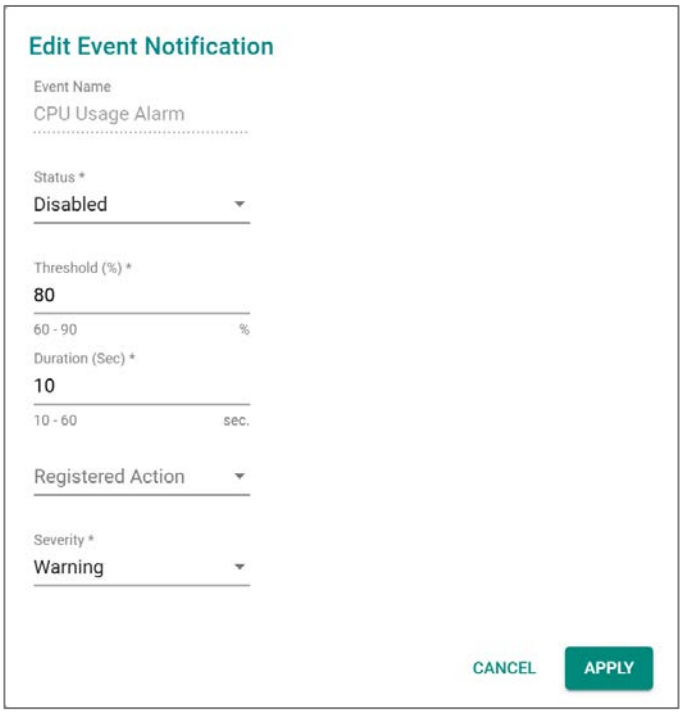
UI Setting	Description
Status	Shows whether event notifications are enabled for this kind of event.
Event Name	Shows which group this event belongs to.
Threshold(%)	Shows the CPU usage threshold percentage that must be exceeded for event notifications.
Duration(Sec)	Shows the amount of time in seconds CPU usage must exceed the threshold to trigger a notification.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - CPU Usage - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - CPU Usage** page will open this dialog box. This dialog lets you change the notification settings for CPU usage.

Click **APPLY** to save your changes.



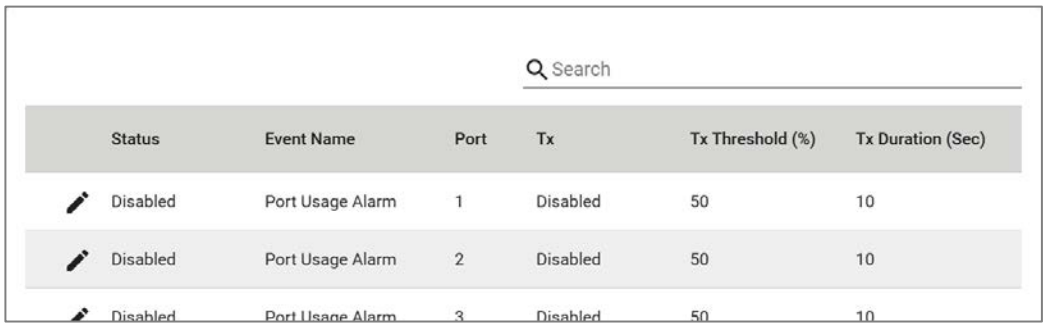
UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event.	N/A	N/A
Status	Enable or disable notifications for this event.	Enabled / Disabled	Disabled
Threshold(%)	Specify the CPU usage threshold percentage that must be exceeded for to trigger the event.	60 to 90	80
Duration(Sec)	Specify the amount of time in seconds CPU usage must exceed the threshold to trigger the event.	10 to 60	10

UI Setting	Description	Valid Range	Default Value
Registered Action	Select what actions to take for this event. You can select multiple options. • **Email**: A notification will be sent to the email server defined in the Email Settings section. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. **Note** The actions available may vary depending on the event type and the device model.	Email / Syslog	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

Event Notifications - Port Usage

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage

This page lets you configure notification settings based on port usage. Each port can be configured independently with different warning methods and severity classifications.



UI Settings	Description
Status	Shows whether event notifications are enabled for this kind of event.

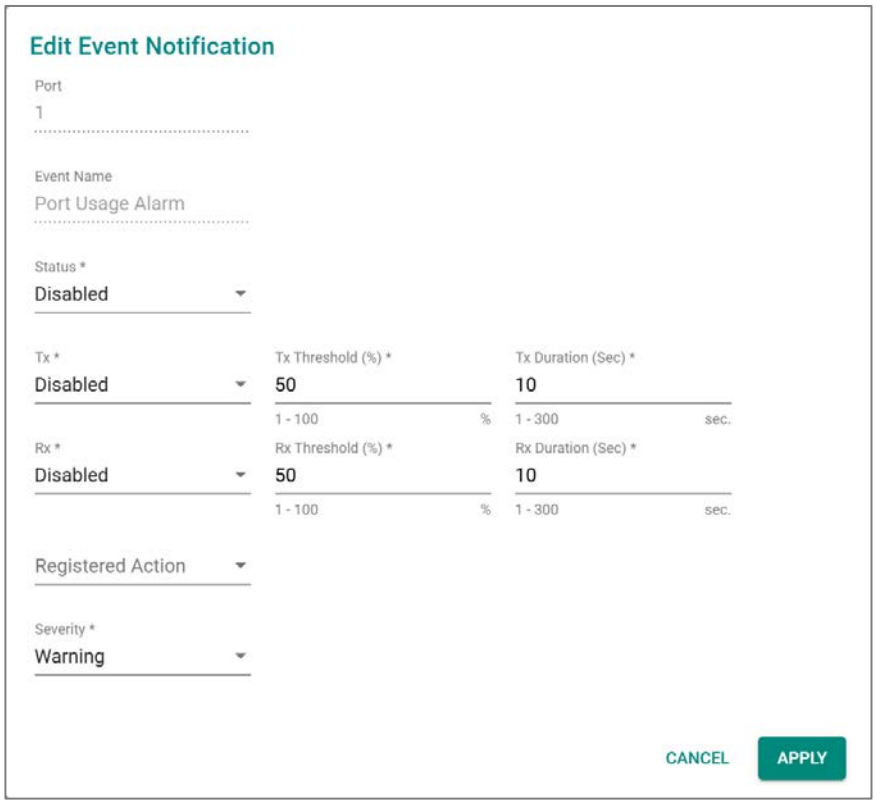
UI Settings	Description
Port	Shows which port this event belongs to. **Note** Available ports will vary depending on your product and model.
Tx	Shows whether Tx traffic is being monitored for event notifications.
Tx Threshold(%)	Shows the Tx threshold percentage that must be exceeded for event notifications.
Tx Duration	Shows the amount of time in seconds Tx traffic must exceed the Tx threshold to trigger a notification.
Rx	Shows whether Rx traffic is being monitored for event notifications.
Rx Threshold(%)	Shows the set Rx threshold percentage that must be exceeded for event notifications.
Rx Duration(Sec)	Shows the amount of time in seconds Rx traffic must exceed the Rx threshold to trigger a notification.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows how notifications will be sent for this kind of event.

Event Notifications - Port Usage - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - Port Usage** page will open this dialog box. This dialog lets you change the notification settings for the selected port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port (View-only)	Shows which physical port the event notifications are for. **Note** Available ports will vary depending on your product and model.	N/A	N/A
Event Name (View-only)	Shows the name of the event.	N/A	N/A
Tx	Enable or disable Tx monitoring for event notifications.	Enabled / Disabled	Disabled
Tx Threshold(%)	Specify the Tx threshold percentage that must be exceeded to trigger an event.	1 to 100	50
Tx Duration	Specify the amount of time in seconds Tx traffic must exceed the Tx threshold to trigger an event.	1 to 300	10
Rx	Enable or disable Rx monitoring for event notifications.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Rx Threshold(%)	Specify the Rx threshold percentage that must be exceeded to trigger an event.	1 to 100	50
Rx Duration(Sec)	Specify the amount of time in seconds Rx traffic must exceed the Rx threshold to trigger an event.	1 to 300	10
Registered Action	Select what actions to take for this event. You can select multiple options. • **Email**: A notification will be sent to the email server defined in the Email Settings section. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • SNMP Trap: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. **Note** The types of actions available may vary depending on the event type and the device model.	Email / Syslog / SNMP Trap	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Warning

Event Notifications - RX Discard

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - RX Discard

This page lets you configure notifications for RX discard events for each port. Each event can be configured independently with different warning methods and severity classifications.

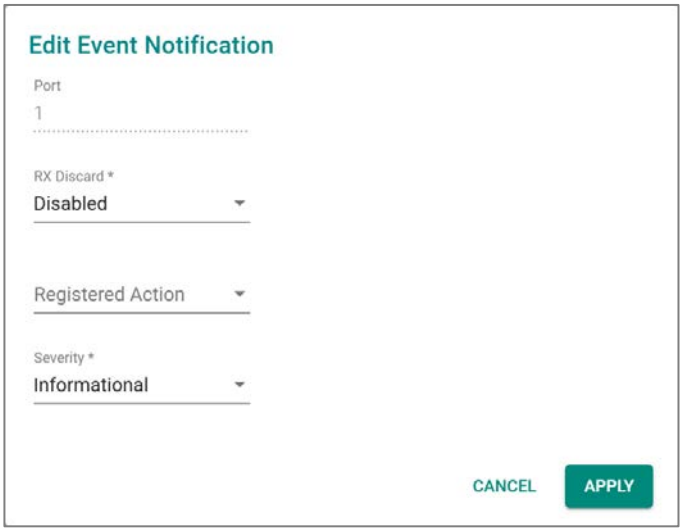
UI Setting	Description
Port	Shows the port the entry is for.
RX Discard	Shows whether RX discard event notifications are enabled for the port.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows the actions that will be triggered when the event occurs.

Event Notifications - RX Discard - Edit Event Notification

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - RX Discard

Clicking the **Edit ( )** icon for a port on the **Diagnostics > Event Logs and Notifications > Event Notifications - System** page will open this dialog box. This dialog lets you change RX discard event notification settings for the selected port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Port	Shows the port you are editing RX discard notification settings for.	N/A	N/A
RX Discard	Enable or disable RX discard event notifications for this port.	Enabled / Disabled	Disabled
Registered Action	Select what actions to take for this event. You can select multiple options. • **Trap**: Event notifications will be sent to a trap server. Refer to SNMP Trap/Inform for more information. • **Syslog**: Event logs will be sent to a syslog server. Refer to Syslog for more information. • **Local Storage**: Event logs will be saved to the device's Network Log. Refer to Network Log - RX Discard for more information. **Note** The types of actions available may vary depending on the event type and the device model.	Trap / Syslog / Local Storage	N/A
Severity	Select the severity to assign for this event. Refer to the Severity Level List for more information about the different severity levels.	Emergency / Alert / Critical / Error / Warning / Notice / Informational / Debug	Informational

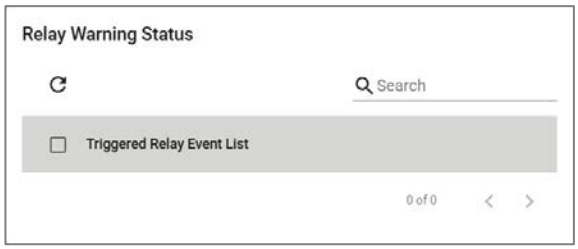
Event Notifications - Relay Warning

Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Relay Warning

This page lets you configure relay warning notifications.

Relay Event Operation

UI Setting	Description	Valid Range	Default Value
Status	Enable or disable relay event notifications.	Enabled / Disabled	Enabled



UI Setting	Description
Triggered Relay Event List	Shows events that have triggered the relay output.

Syslog

Menu Path: Diagnostics > Event Logs and Notifications > Syslog

This page lets you configure your device to connect to syslog servers to store event logs. When an event occurs, an event notification can be sent as a syslog UDP packet to the specified Syslog servers. Each syslog server can be enabled individually.

Administrators can manually import self-signed certificates for syslog client services. However, they should check the root certificate and validity of the signature before

importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When the device sends an imported certificate to the syslog server, the syslog server will attempt to verify the certificate by searching the approved certificate pool on the server to identify the imported certificate.

Note

To centralize data collection and potentially use it for forensic purposes in the future, we recommend that users deploy a syslog server in their environment and enable the syslog functionality on their devices to send logs to the remote server for storage. Additionally, we strongly recommend that these logs be properly stored on a syslog server for at least one year.

It is advised that the syslog server administrator utilize software or design automated processes for syslog management (including protection, collection, etc.).

For syslog management, it is essential to establish SOPs or any automated protection mechanisms to prevent authorized users from inadvertently deleting logs stored on the syslog server.

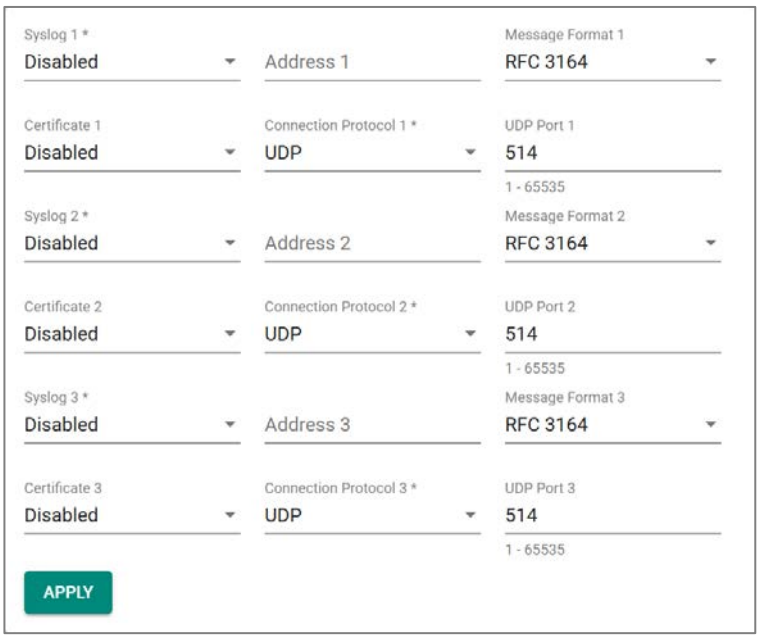
Note

In order to ensure the security of your network, we recommend the following:

- The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
- The lifetime of certificates generated for syslog client services should be short and in accordance with the organization's security procedures and requirements.
- For security reasons, it is recommended to send event logs to a centralized syslog server for continuous network event monitoring.

Limitations

You can connect to up to 3 syslog servers.



UI Setting	Description	Valid Range	Default Value
Syslog	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled
Address	Enter the IP address of the specified syslog server.	Valid IP address	N/A
Message Format	Select the message format for the specified syslog server.	RFC 3164 / RFC 5424	RFC 3164
Certificate	Select a syslog server certificate to use for the specified server, or disable use of certificates.	Drop-down list of certificates / Disabled	Disabled
Connection Protocol	Select the connection protocol of the specified syslog server.	UDP / TCP	If Certificate is disabled: UDP If a Certificate is selected: TCP
UDP Port	Specify the UDP port of the specified syslog server.	1 to 65535	514

SNMP Trap/Inform

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform

This page lets you configure the SNMP Trap/Inform notification feature.

This page includes these tabs:

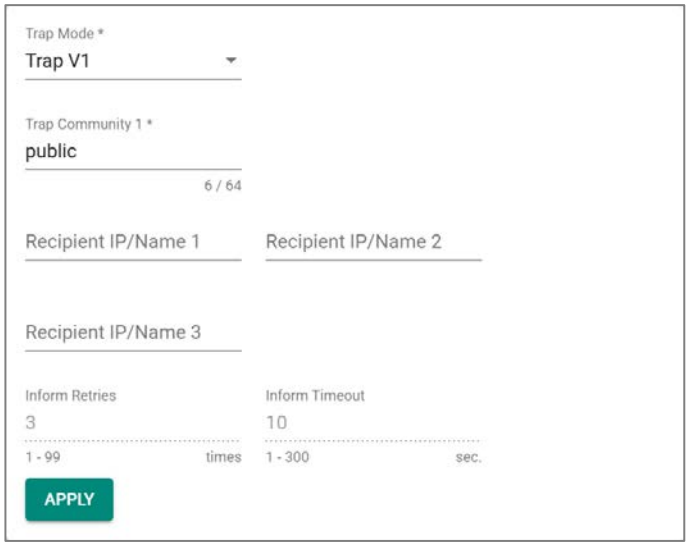
- General
- SNMP Account

SNMP Trap / Inform - General

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - General

This page lets you configure the SNMP Trap/Inform settings of your device.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Trap Mode	Select a mode to use for SNMP notifications. Trap notifications are sent without requesting an acknowledgement from the recipient. Inform notifications will request an acknowledgement from the recipient, and will retry sending the notification if the acknowledgement is not received. • **Trap V1**: Use Trap V1 for SNMP notifications. • **Trap V2**: Use Trap V2 for SNMP notifications. • **Inform V2**: Use Inform V2 for SNMP notifications. • **Trap V3**: Use Trap V3 for SNMP notifications. • **Inform V3**: Use Inform V3 for SNMP notifications.	Trap V1 / Trap V2 / Inform V2 / Trap V3 / Inform V3	Trap V1

UI Setting	Description	Valid Range	Default Value
Trap Community 1	Specify the community string that will be used for authentication.	1 to 64 characters	public
Recipient IP/Name 1/2/3	Specify the name of the recipient trap server that will receive notifications.	Recipient IP or name	N/A
Inform Retries **(If Trap Mode is Inform V2 or Inform V3)**	Specify the number of times to retry sending an inform notification.	1 to 99	3
Inform Timeout **(If Trap Mode is Inform V2 or Inform V3)**	Specify the amount of time to wait (in seconds) to wait for an acknowledgement before trying to resend an inform notification.	1 to 300	10

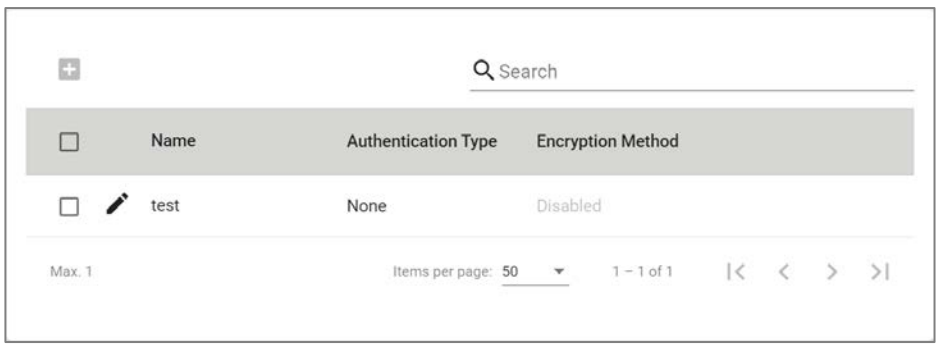
SNMP Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Account

This section lets you configure an SNMP trap account for your device.

Limitations

You can configure up to 1 SNMP trap account.



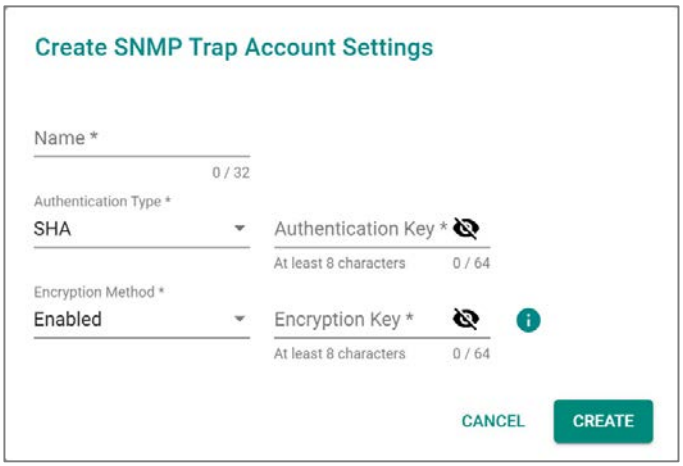
UI Setting	Description
Name	Shows the name of the SNMP trap account.
Authentication Type	Shows which authentication method is used for the account.
Encryption Method	Shows which encryption method is used for the account.

Create SNMP Trap Account Settings

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Account

Clicking the **Add (⊕)** icon on the **Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Account** page will open this dialog box. This dialog lets you add an SNMP trap account for your device.

Click **CREATE** to save your changes and add the new account.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 32 characters	N/A

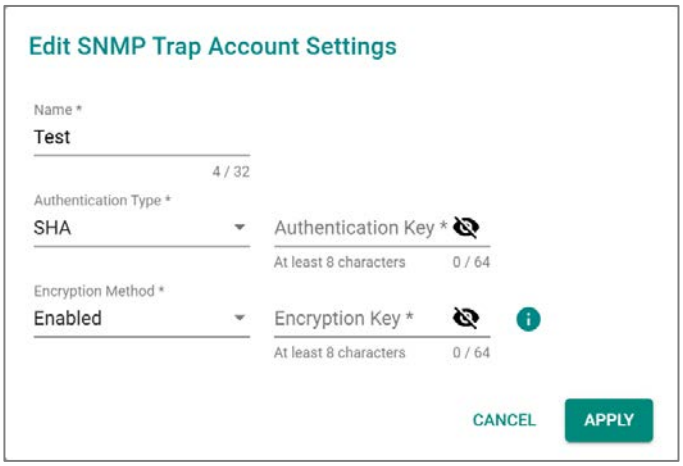
UI Setting	Description	Valid Range	Default Value
Authentication Type	Select which authentication method to use for the account. • **None**: No authentication will be used. • **MD5**: Use MD5 authentication. • **SHA**: Use SHA authentication. • **SHA-256**: Use SHA-256 authentication. • **SHA-512**: Use SHA-512 authentication.	None / MD5 / SHA	None
Authentication Key **(If Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Enable or disable AES encryption for the account.	Enabled / Disabled	Disabled
Encryption Key **(If Encryption Method is Enabled)**	Specify an encryption password for the account.	8 to 64 characters	N/A

Edit SNMP Trap Account Settings

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Account

Clicking the **Edit ( )** icon for an entry on the **Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Account** page will open this dialog box. This dialog lets you modify an existing SNMP trap account.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
Name	Specify a name for the account.	1 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account. • **None**: No authentication will be used. • **MD5**: Use MD5 authentication. • **SHA**: Use SHA authentication. • **SHA-256**: Use SHA-256 authentication. • **SHA-512**: Use SHA-512 authentication.	None / MD5 / SHA	None
Authentication Key **(If Authentication Type is MD5 or SHA)**	Specify an authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Enable or disable AES encryption for the account.	Enabled / Disabled	Disabled
Encryption Key **(If Encryption Method is Enabled)**	Specify an encryption password for the account.	8 to 64 characters	N/A

Delete SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Account

You can delete an account by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Email Settings

Menu Path: Diagnostics > Event Logs and Notifications > Email Settings

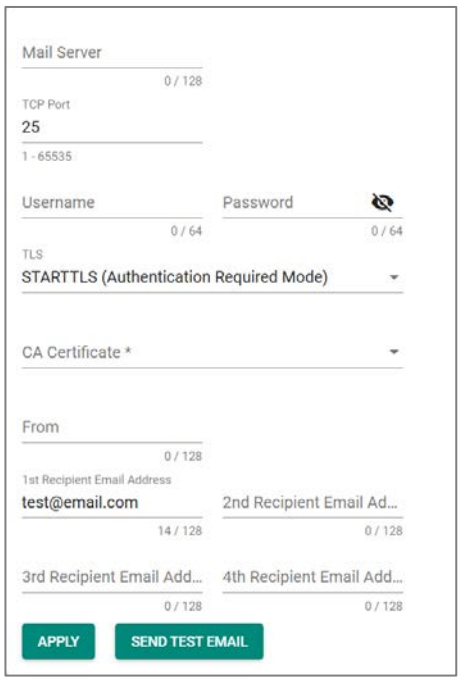
This page lets you configure your device's email notification settings. You can specify which mail server and account to use, and which email addresses to send email notifications to.

This server will also be used to send one-time 2FA codes to users that have email 2FA enabled. Refer to 2-Factor Authentication and User Accounts for more information.

Click **APPLY** to save your changes.

Click **SEND TEST MAIL** to send a test email using the current settings and recipients.

> **Note**
>
> Auto warning email messages will be sent through an authentication-protected SMTP server that supports CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication.
>
> We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.



UI Setting	Description	Valid Range	Default Value
Mail Server	Specify the address of the email server. You can enter a domain name or IP address.	1 to 128 characters	N/A
TCP Port	Specify the TCP port of the email server.	1 to 65535	25
Username	Specify the username used to log in to the email server.	0 to 64 characters	N/A
Password	Specify the password used to log in to the email server.	0 to 64 characters	N/A
TLS	Specify whether to enable TLS (Transport Layer Security) for encrypted email transmission.	Disabled / STARTTLS (No Authentication Mode) / STARTTLS (Authentication Required Mode)	Disabled
CA Certificate **(If TLS is STARTTLS (Authentication Required Mode))**	Select the CA certificate to use for STARTTLS. Refer to Trusted CA Certificate for more information.	List of installed CA certificates	N/A
From	Specify the sender email address to use for email notifications.	0 to 128 characters	N/A

UI Setting	Description	Valid Range	Default Value
Recipient Email Address	Enter an email address to send email notifications to. You can set up to 4 email addresses to receive email notifications.	0 to 128 characters	N/A

SMS Settings

Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings

This page lets you configure your device's SMS notification settings. You can specify which phone number to send SMS notifications to.

Note

Availability of this feature may vary depending on your product model and version.

Note

Ensure your SIM card plan supports sending SMS messages before using this feature. If SMS service is unavailable on the SIM card, it may cause unexpected cellular communication errors. If this occurs, disable all SMS functions and restart the device to recover normal operation.

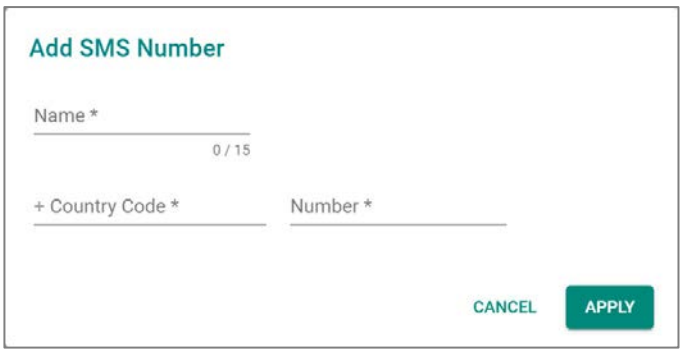
UI Setting	Description
Name	Shows the SMS recipient's name.
Country Code	Shows the SMS recipient number's country code.
Number	Shows the SMS recipient's phone number.

Add SMS Number

Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings

Clicking the **Add (⊕)** icon on the **Diagnostics > Event Logs and Notifications > SMS Settings** page will open this dialog box. This dialog lets you add an SMS recipient for your device notification.

Click **CREATE** to save your changes and add the new SMS recipient.



UI Setting	Description	Valid Range	Default Value
Name	Enter the SMS recipient's name.	1 to 15 characters	N/A
Country Code	Enter the SMS recipient number's country code.	1 to 4 digits	N/A
Number	Enter the SMS recipient's phone number.	1 to 15 digits	N/A

Edit SMS Settings

Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings

Clicking the **Edit (✎)** icon for an entry on the **Diagnostics > Event Logs and Notifications > SMS Settings** page will open this dialog box. This dialog lets you modify an existing SMS recipient.

Click **APPLY** to save your changes.

Edit SMS Number

UI Setting	Description	Valid Range	Default Value
Name	Enter the SMS recipient's name.	1 to 15 characters	N/A
Country Code	Enter the SMS recipient number's country code.	1 to 4 digits	N/A
Number	Enter the SMS recipient's phone number.	1 to 15 digits	N/A

Delete SMS Number

Menu Path: Diagnostics > Event Logs and Notifications > SMS Settings

You can delete SMS recipients by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Tools

Menu Path: Diagnostics > Tools

This section lets you use various tools to check for network issues.

This section includes these pages:

- Diagnostic Support
- Port Mirroring
- Ping
- NetFlow

Diagnostic Support

Menu Path: Diagnostics > Tools > Diagnostic Support

This page lets you generate files and import files for troubleshooting.

This page includes these tabs:

- Tech Support File
- Diagnostic Logging Profile
- Cellular Debugging
- Module Firmware
- MRC

> **Note**
> Please note that settings and available options may vary depending on the product model.

Tech Support File

Menu Path: Diagnostics > Tools > Diagnostic Support - Tech Support File

This page lets you generate a tech support file that includes device information such as system logs, system status, and configurations. This file can be provided to Moxa technical support to assist troubleshooting.

Click the **GENERATE** button to generate and save a tech support file to your local host. You can specify a password to encrypt the file.

UI Setting	Description	Valid Range	Default Value
File Encryption Password	Specify a password to use for tech support file encryption.	1 to 64 characters	N/A

Cellular Debugging

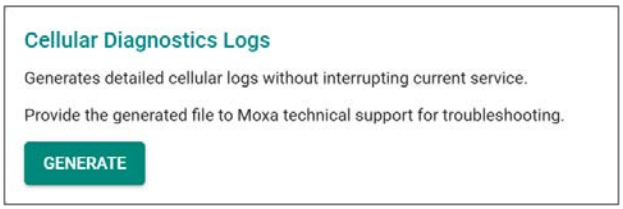
Menu Path: Diagnostics > Tools > Diagnostic Support - Cellular Debugging

This page lets you download detailed cellular logs and run cellular module diagnostics for troubleshooting.

Cellular Diagnostics Logs

Click the **GENERATE** button to generate and save a cellular diagnostic logs file to your local host.

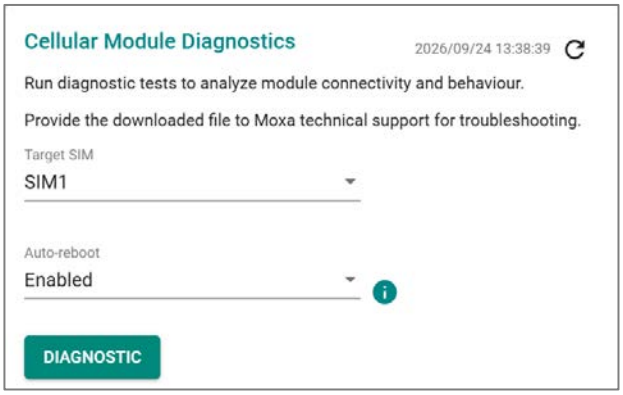
> **Note**
>
> Cellular diagnostic logs are retained for approximately 7 days. To prevent data from being overwritten, please download all relevant logs as soon as possible after an event occurs.



Cellular Module Diagnostics

Click the **DIAGNOSTIC** button to run the cellular module diagnostics test. Diagnostics will take about 10 minutes to complete.

> **Note**
>
> Performing Cellular Module Diagnostics will suspend active transmissions, including Cellular, SMS, GNSS, and WAN Redundancy, and will also suspend related system logs and notifications.
>
> A new connection will be established via the command line during the diagnostic process. If successful, data transmission may resume concurrently. However, a system reboot will be required after the diagnostic process to fully restore all functions.



UI Setting	Description	Valid Range	Default Value
Target SIM	Select the SIM card to perform diagnostics on.	SIM1 / SIM2	SIM1
Auto-reboot	Enable or disable auto-reboot after testing is complete to restore all functions. • **Enable**: The device will automatically reboot after the test to restore all functions. **Diagnostic Status** will display 'Test Complete' after reboot. • **Disable**: A manual reboot will be required after diagnostic tests are completed to restore all functions.	Enabled / Disabled	Enabled

Diagnostic Status

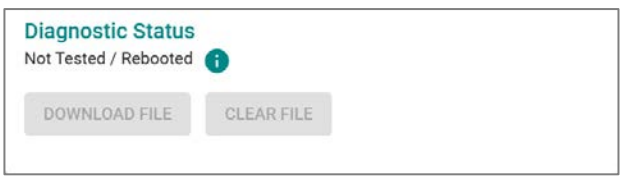
Click the **Refresh ( )** button to update the status of the cellular module diagnostic test.

Click **DOWNLOAD FILE** to save the results of a completed diagnostics test to your local device.

Click **CLEAR FILE** to remove the diagnostics test results from the device.

Note

Due to the large size of diagnostic result files, it is highly recommended to clear them after downloading them. This will free up device memory and prevent excessive storage consumption.



UI Setting	Description
Diagnostic Status	Shows the current status of cellular module diagnostics testing. • **Not Tested / Rebooted**: The device has not been tested yet, or testing was completed and the device has been rebooted. • **Testing**: Testing is in progress. Changing any settings during testing may affect the results. • **Test Complete**: Test complete. A reboot is required to restore full system functionality.

Module Firmware

Menu Path: Diagnostics > Tools > Diagnostic Support - Module Firmware

This page lets you upgrade the firmware of the cellular module using a firmware file provided by Moxa Technical Support.

UI Setting	Description	Valid Range	Default Value
Select File	Select the firmware upgrade file from your local host, then click **UPGRADE** to upgrade the module's firmware.	N/A	N/A

Diagnostic Logging Profile

Menu Path: Diagnostics > Tools > Diagnostic Support - Diagnostic Logging Profile

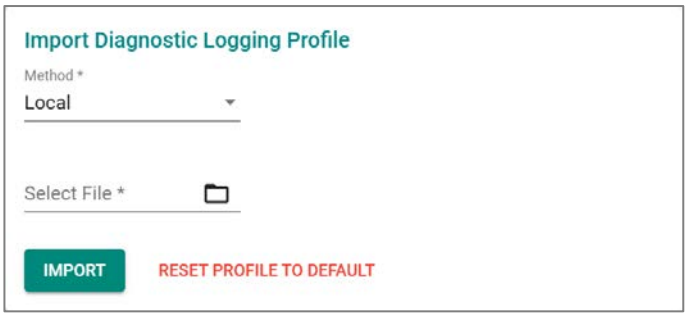
This page lets you import a diagnostic logging profile provided by Moxa Technical Support to collect detailed diagnostic logs for specific system agents.

The collected diagnostic logs are included in generated Tech Support files, and can be provided to Moxa Technical Support to assist troubleshooting. Refer to Tech Support File for more information on generating a Tech Support file.

Import Diagnostic Logging Profile - Local

If you select **Local** as your **Method**, these settings will appear.

Specify the required settings, then select **IMPORT** to import the diagnostic logging profile.



UI Setting	Description	Valid Range	Default Value
Method	Select the method used to import the diagnostic logging profile.	Local / TFTP / USB / SCP / SFTP	Local
Select File	Select the diagnostic logging profile file from your local host.	N/A	N/A

Import Diagnostic Logging Profile - TFTP

If you select **TFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **IMPORT** to import the diagnostic logging profile.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

UI Setting	Description	Valid Range	Default Value
Method	Select the method used to import the diagnostic logging profile.	Local / TFTP / USB / SCP / SFTP	Local
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address	N/A
File Name	Specify the file name of the diagnostic logging profile file to import, including its full path on the server. Example: /path_to_profile_file/profile_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 63 characters, including file extension File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

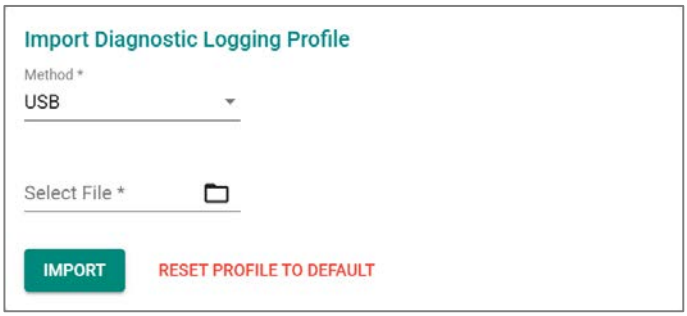
Import Diagnostic Logging Profile - USB

If you select **USB** as your **Method**, these settings will appear.

Specify the required settings, then select **IMPORT** to import the diagnostic logging profile.

Note

To use this feature, USB Function must be enabled in Hardware Interface.

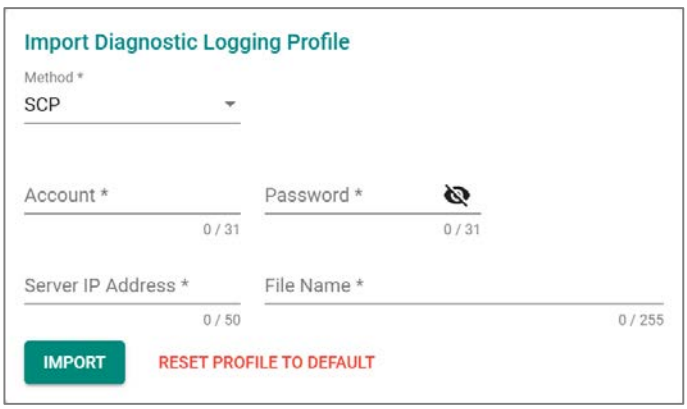


UI Setting	Description	Valid Range	Default Value
Method	Select the method used to import the diagnostic logging profile.	Local / TFTP / USB / SCP / SFTP	Local
Select File	Select the diagnostic logging profile file to use from the ABC-02 device inserted into the USB port.	Select a file from the ABC-02 device	N/A

Import Diagnostic Logging Profile - SCP

If you select **SCP** as your **Method**, these settings will appear.

Specify the required settings, then select **IMPORT** to import the diagnostic logging profile.



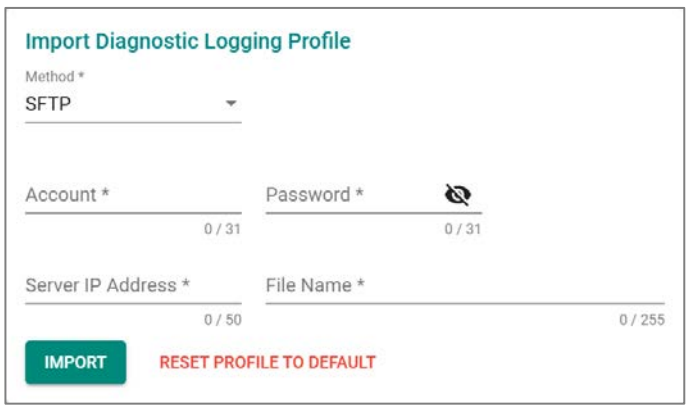
UI Setting	Description	Valid Range	Default Value
Method	Select the method used to import the diagnostic logging profile.	Local / TFTP / USB / SCP / SFTP	Local
Account	Enter the account name to use to connect to the SCP server.	1 to 31 characters	N/A

UI Setting	Description	Valid Range	Default Value
Password	Enter the account password to use to connect to the SCP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SCP server where the diagnostic logging profile file is stored.	Valid IP address up to 50 characters	N/A
File Name	Specify the file name of the diagnostic logging profile file to restore from, including its full path on the server. Example: `/path_to_profile_file/profile_file.conf` **Note** If a path is not specified, the default folder for the server will be used.	Up to 255 characters File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

Import Diagnostic Logging Profile - SFTP

If you select **SFTP** as your **Method**, these settings will appear.

Specify the required settings, then select **IMPORT** to import the diagnostic logging profile.



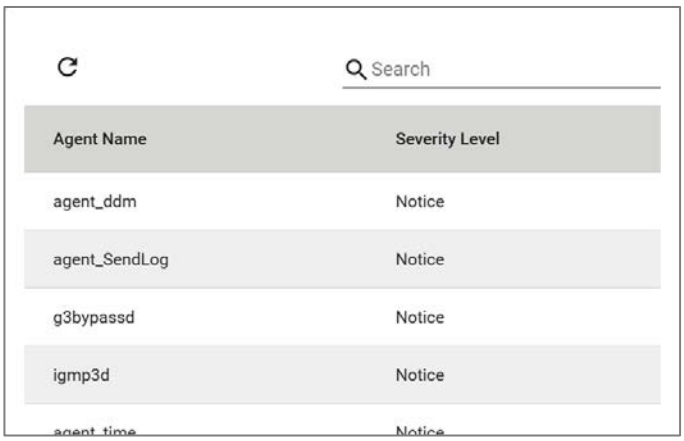
UI Setting	Description	Valid Range	Default Value
Method	Select the method used to import the diagnostic logging profile.	Local / TFTP / USB / SCP / SFTP	Local
Account	Enter the account name to use to connect to the SFTP server.	1 to 31 characters	N/A

UI Setting	Description	Valid Range	Default Value
Password	Enter the account password to use to connect to the SFTP server.	1 to 31 characters	N/A
Server IP Address	Specify the IP address of the SFTP server where the diagnostic logging profile file is stored.	Valid IP address up to 50 characters	N/A
File Name	Specify the file name of the diagnostic logging profile file to restore from, including its full path on the server. Example: `/path_to_profile_file/profile_file.conf` **Note** If a path is not specified, the default folder for the server will be used.	Up to 255 characters File name can only contain the characters A-Z, a-z, 0-9, and special characters -._()	N/A

Agent List

This list shows the agents and severity levels that will be included in generated Technical Support files. Refer to Tech Support File for information on generating a Technical Support file.

This list is updated by importing a diagnostic logging profile provided by Moxa Technical Support.



UI Setting	Description
Agent Name	Shows the name of the software agent responsible for related device functions.

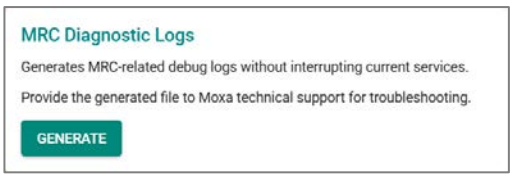
UI Setting	Description
Severity Level	Shows the severity level configured for the agent.

MRC

Menu Path: Diagnostics > Tools > Diagnostic Support - MRC

This page lets you generate a MRC-related debug log file. This file can be provided to Moxa technical support to assist troubleshooting.

Click the **GENERATE** button to generate and save an MRC debug log file to your local host.



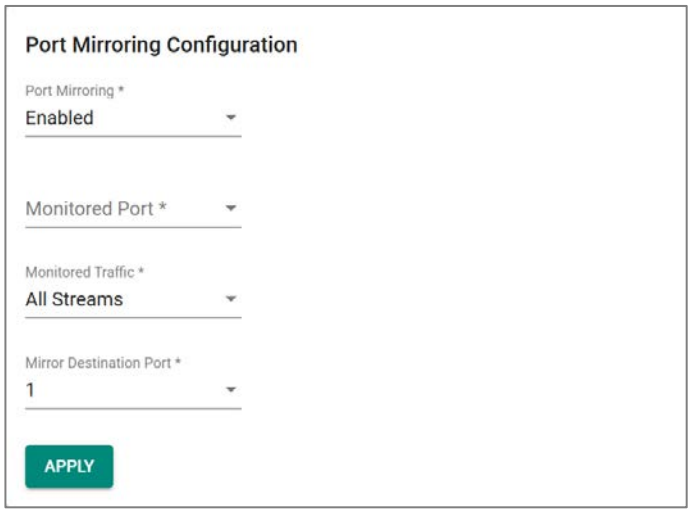
Port Mirroring

Menu Path: Diagnostics > Tools > Port Mirroring

This page lets you configure the port mirror function, which can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation.

Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

> **Note**
>
> For security reasons, it is recommended to use port mirroring to send traffic to an intrusion detection system (IDS) for analysis.



UI Setting	Description	Valid Range	Default Value
Port Mirroring	Enable or disable the port mirror function.	Enabled / Disabled	Disabled
Monitored Port **(If Port Mirroring is Enabled)**	Select the ports you want to monitor for network activity. Multiple ports can be selected.	Drop-down list of ports	N/A
Monitored Traffic **(If Port Mirroring is Enabled)**	Select the type of traffic that will be monitored. • **Ingress Stream**: Select this option to monitor only those data packets coming into the Moxa industrial secure router's port. • **Egress Stream**: Select this option to monitor only those data packets being sent out through the Moxa industrial secure router's port. • **All Streams**: Select this option to monitor data packets both coming into and being sent out through the Moxa industrial secure router's port.	Ingress Stream / Egress Stream / All Streams	All Streams
Mirror Destination Port **(If Port Mirroring is Enabled)**	Select the port that will be used to mirror the activity of the monitored ports. **Note** The mirror destination port cannot be one of the monitored ports.	Drop-down list of ports	1

Ping

Menu Path: Diagnostics > Tools > Ping

This page lets you use the ping function, which is useful for troubleshooting network problems.

The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the device itself. In this way, you can use your device to send ping commands out through its ports.

UI Setting	Description	Valid Range	Default Value
IP Address/Domain Name	Specify the IP address or domain name you want to ping, then click the **PING** button. The ping result will be displayed below.	Valid IP address or domain name up to 50 characters	N/A
Source Interface	Select the specified interface to ping from.	Not Specified, Drop-down list of interfaces	Not Specified

NetFlow

Menu Path: Diagnostics > Tools > NetFlow

This page lets you create and edit NetFlows for your device.

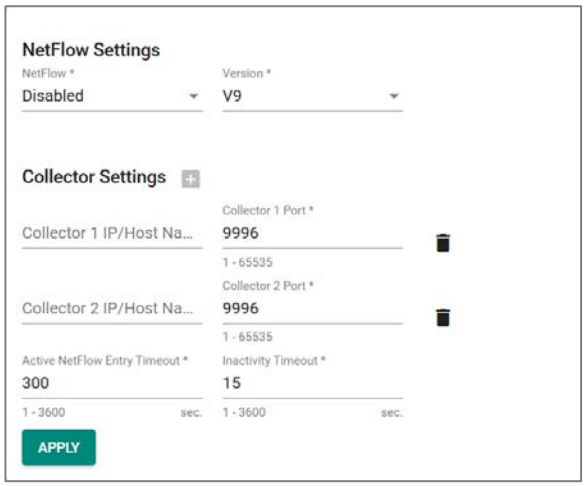
Limitations

You can create up to 4 NetFlow entries.

Limitations

You can add up to 2 NetFlow collectors.

NetFlow Settings



NetFlow Settings

UI Setting	Description	Valid Range	Default Value
NetFlow	Enable or disable NetFlow.	Enabled / Disabled	Disabled
Version	Specify which version of NetFlow to use.	V5 / V9 / IPFIX	V9

Collector Settings

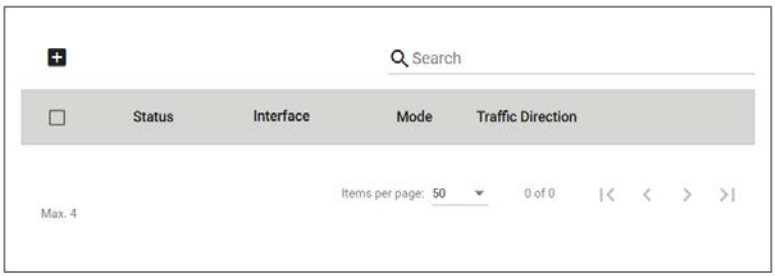
Click the **Add (+)** icon to add a collector.

Click the **Delete (🗑)** icon for a collector to delete it.

UI Setting	Description	Valid Range	Default Value
Collector IP / Host Name	Specify the collector IP or host name.	Valid IP address or host name	N/A
Collector Port	Specify the collector port number.	1 to 65535	9996

UI Setting	Description	Valid Range	Default Value
Active NetFlow Entry Timeout	Specify the active NetFlow entry timeout in seconds. This is the maximum duration a flow can remain "active" in the router's flow cache.	1 to 3600	300
Inactivitiy Timeout	Specify the inactivity timeout in seconds. This is the maximum duration a flow can remain "inactive" without new packet matches.	1 to 3600	15

NetFlow List



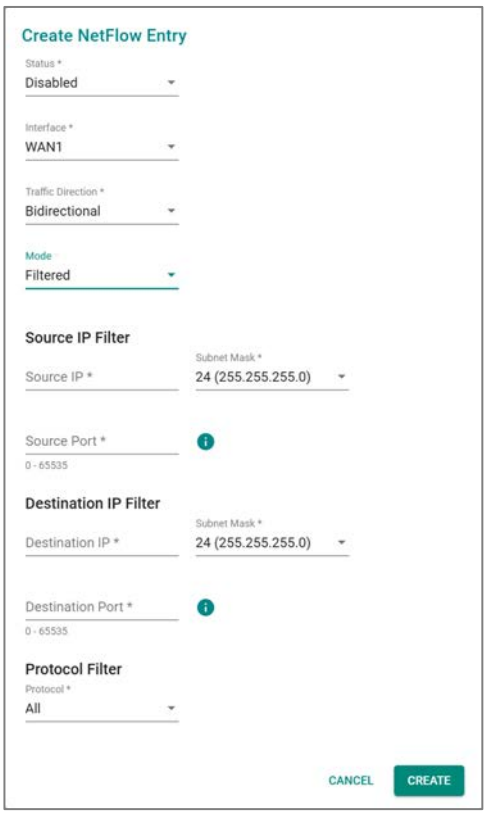
UI Setting	Description
Status	Shows whether the entry is enabled or disabled.
Interface	Shows the interface for the NetFlow entry.
Mode	Shows the mode for the NetFlow entry.
Traffic Direction	Shows the traffic direction for the NetFlow entry.

Create NetFlow Entry

Menu Path: Diagnostics > Tools > NetFlow

Clicking the **Add (⊞)** icon for the NetFlow List on the **Diagnostics > Tools > NetFlow** page will open this dialog box. This dialog lets you create a new NetFlow entry.

Click **CREATE** to save your changes and add the new NetFlow entry.



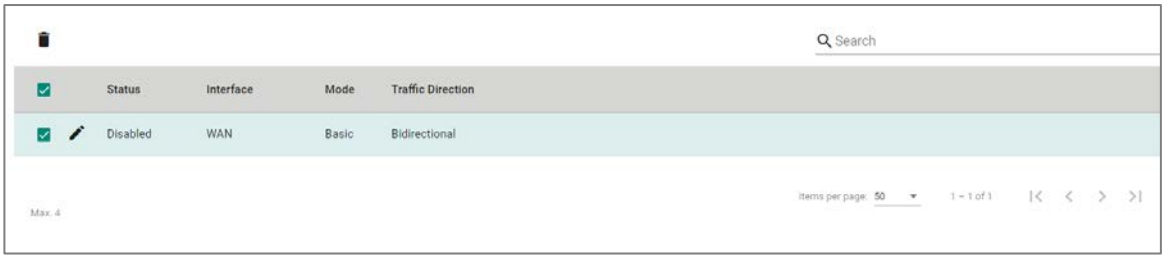
UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the NetFlow entry.	Enabled / Disabled	Disabled
Interface	Specify the interface for the NetFlow entry.	Drop-down list of interfaces	WAN
Traffic Direction	Select the traffic direction for the NetFlow entry.	Bidirectional / Ingress / Egress	Bidirectional
Mode	Select the mode for the NetFlow entry. • **Basic:** This mode enables you to configure a NetFlow entry for your device. • **Filtered:** This mode allows you to filter traffic by IP address or specific protocol.	Basic / Filtered	Basic

UI Setting	Description	Valid Range	Default Value
Sampling Rate **(If Mode is Basic)**	Specify the sampling rate of the NetFlow entry. 0 disables use of the sampling rate, which is the same as setting it to 1. **Note** A lower number indicates more frequent sampling, with 1 representing sampling every packet, thus providing full visibility and accuracy. However, more intensive sampling may adversely affect performance.	0 to 65535	N/A
Source IP **(If Mode is Filtered)**	Specify the source IP.	Valid IP address	N/A
Subnet Mask **(If Mode is Filtered)**	Select the subnet mask for the source IP.	Drop-down list of subnet masks	N/A
Source Port **(If Mode is Filtered)**	Specify the port for the source IP. Setting this to 0 means all ports will be allowed.	0 to 65535	N/A
Destination IP **(If Mode is Filtered)**	Specify the destination IP.	Valid IP address	N/A
Subnet Mask **(If Mode is Filtered)**	Select the subnet mask for the destination IP.	Drop-down list of subnet masks	N/A
Destination Port **(If Mode is Filtered)**	Specify the port for the destination IP. Setting this to 0 means all ports will be allowed.	0 to 65535	N/A
Protocol **(If Mode is Filtered)**	Select the protocol to filter.	All / TCP / UDP	N/A

Delete NetFlow

Menu Path: Diagnostics > Tools > NetFlow

You can delete a NetFlow by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.



Asset Recognition

Menu Path: Diagnostics > Asset Recognition

This page lets you enable the asset recognition feature to detect assets in the same subnet.

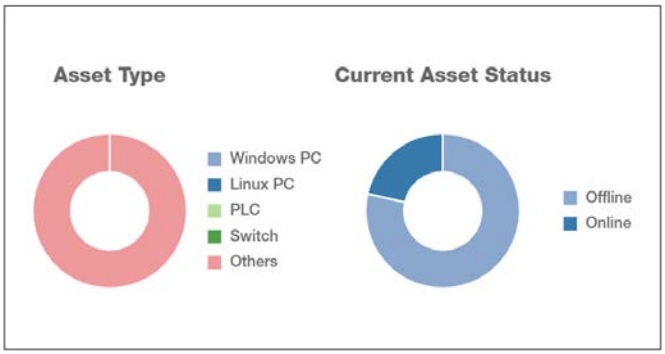
Asset Recognition - Global Settings

UI Setting	Description	Valid Range	Default Value
Asset Recognition	Enable or disable asset recognition.	Enabled / Disabled	Disabled
Detected Cycle	Specify the interval for the system to scan for and recognize new devices.	30 sec / 40 sec / 50 sec / 1 min / 2 min	1 min

UI Setting	Description	Valid Range	Default Value
Offline Record Time	Specify the maximum amount of time a recognized device will remain listed after losing network connectivity.	24 hours / 36 hours / 48 hours / 60 hours / 72 hours	72 hours

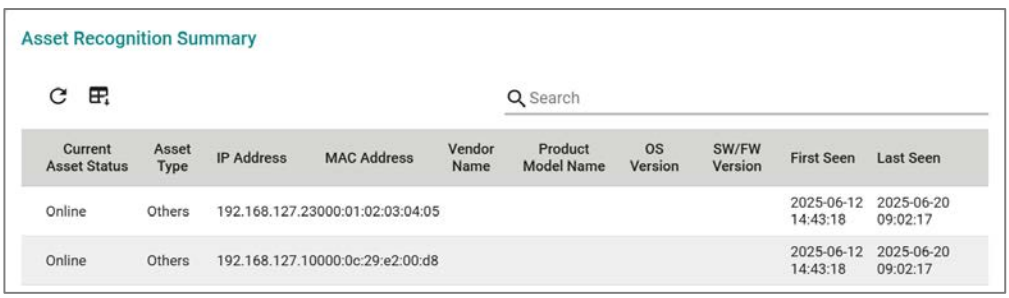
Asset Type and Current Asset Status

These charts provide an overview of all discovered assets, grouped by device type and current status. Hover over an area on a chart to display a pop-up that shows how many devices are in that category.



UI Setting	Description
Asset Type	Shows an overview of Windows PCs, Linux PCs, PLCs, switches, and any other discovered assets exposing RFC 1213 (MIB-II) data.
Current Asset status	Shows an overview of the current offline/online status of assets.

Asset Recognition Summary



UI Setting	Description
Current Asset Status	Indicates whether the asset is currently online or offline.
Asset Type	Shows whether the asset was detected as a Windows PC, Linux PC, Switch, PLC, or Other.
IP Address	Shows the IP address assigned to the asset.
MAC Address	Shows the MAC address of the asset.
Vendor Name	Shows the manufacturer of the asset, as reported via SNMP or other discovery methods.
Product Model Name	Shows the model identifier of the asset, as reported via SNMP or other discovery methods.
OS Version	Shows the operating system version of the asset, as reported via SNMP or other discovery methods.
SW/FW Version	Shows the software or firmware version of the asset, as reported via SNMP or other discovery methods.
First Seen	Shows when the asset was first detected by the system.
Last Seen	Shows when the asset was last seen by the system.

Industrial Application

Menu Path: Industrial Application

This menu settings area lets you configure settings related to specific industrial applications.

This settings area includes these sections:

- IEC 61375

> **Note**
> Availability of this feature may vary depending on your product model and version.

Industrial Application - User Privileges

Privileges to Industrial Application settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
IEC 61375			
Ethernet Train Backbone	R/W	R/W	R
Communication Profile	R/W	R/W	R
Operational Status	R/W	R/W	R

IEC 61375 Setting

Menu Path: Industrial Application > IEC 61375

This section lets you configure IEC 61375 settings related to Ethernet Train Backbone Nodes (ETBN).

The IEC 61375 section includes these pages:

- Ethernet Train Backbone

- Communication Profile
- Operational Status

> **⚠ Warning**
>
> Do not connect ETBNs through ETB ports before the ETBN has been configured.
>
> If Turbo Ring V2 and ETBN are enabled at the same time, Turbo Ring V2 must be configured before ETBN for Turbo Ring V2 to work normally.

Ethernet Train Backbone

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone

This page lets you configure Ethernet Train Backbone settings for your device.

This page includes these tabs:

- TTDP Settings
- Local ETBN Status
- ETB Status
- TCN Multicast Table

TTDP Settings

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

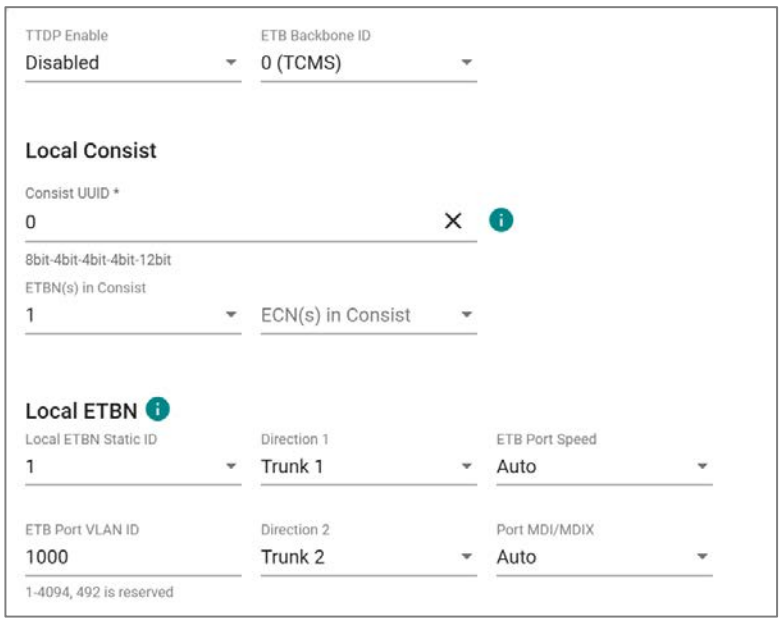
This page lets you set up Train Topology Discovery Protocol (TTDP) for your router. Click **APPLY** to save your changes.

> **⚠ Warning**
>
> Enabling TTDP will overwrite settings for Port Trunk, VLAN, Interface, QoS, VRRP, and Turbo Ring V2.

Note

We recommend setting ETB ports to MDI mode, and using crossover cables for the interconnection of ETBNs.

TTDP Settings



UI Setting	Description	Valid Range	Default Value
TTDP Enable	Enable or Disable TTDP.	Enabled / Disabled	Disabled
ETB Backbone ID	Specify an ETB backbone ID to use.	0 (TCMS) / 1 (Multimedia) / 2 (Not specialized) / 3 (Not specialized)	0 (TCMS)

Local Consist

UI Setting	Description	Valid Range	Default Value
Consist UUID	Shows the UUID of the local consist. Consists with the same UUID will be considered to be the same consist. Therefore, the consist UUIDs for different consists should be unique. You can manually assign a consist UUID, or you can generate a random one by clicking on the **X** button to erase the existing UUID, then clicking the **Refresh ( ) icon** to generate a random UUID.	Valid 8bit-4bit-4bit-4bit-12bit UUID	0
ETBN(s) in Consist	Specify the number of ETBNs in this consist.	1 to 32	1
ECN(s) in Consist	Specify the number of ECNs in this consist.	1 to 32	N/A

Local ETBN

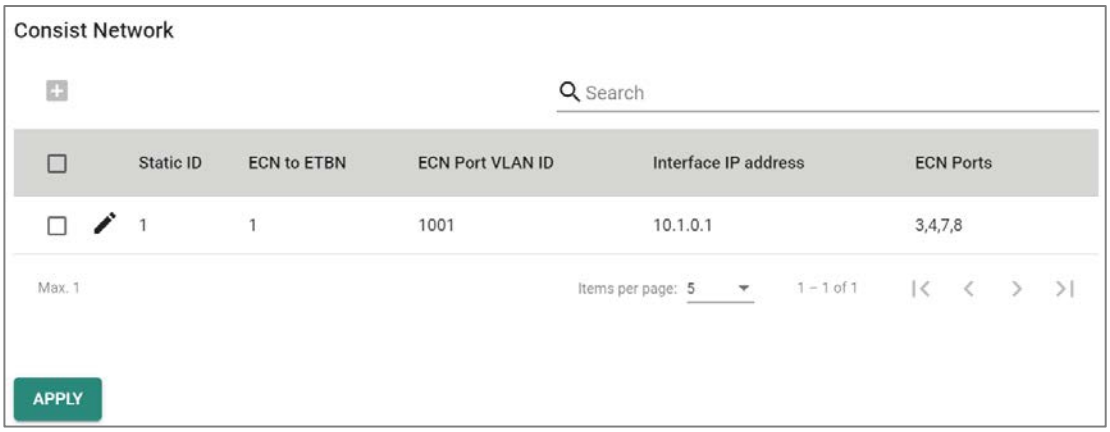
UI Setting	Description	Valid Range	Default Value
Local ETBN Static ID	Specify the static ID of this ETBN within the consist.	Drop-down list of ETBN Static IDs (available options depend on the **ETBN(s) in Consist** setting in **TTDP Settings**)	1
Direction 1	Specify the consist direction for Direction 1. The default setting is ports 1 and 2 will point towards direction 1, and ports 5 and 6 will point towards direction 2.	Trunk 1 / Trunk 2	Trunk 1
ETB Port Speed	Specify the ETB port speed to use. When set to **Auto**, the port will use its default speed. For example, a 1G port set to **Auto** will use 1G for its port speed.	Auto / 1G / 100M	Auto
ETB Port VLAN ID	Specify the VLAN ID for the ETB ports. We recommend using the same VLAN ID for all ETBNs on each train.	1 to 4094, 492 is reserved	1000

UI Setting	Description	Valid Range	Default Value
Direction 2	Specify the consist direction for Direction 2. The default setting is ports 1 and 2 will be point towards direction 1, and ports 5 and 6 will point to direction 2.	Trunk 1 / Trunk 2	Trunk 2
Port MDI/MDIX	Specify the ETB port interface type.	Auto / MDI / MDIX	Auto

Consist Network

Limitations

You can create up to 32 ECN entries, depending on what the ECN(s) in Consist setting is set to. Refer to TTDP Settings for more information.



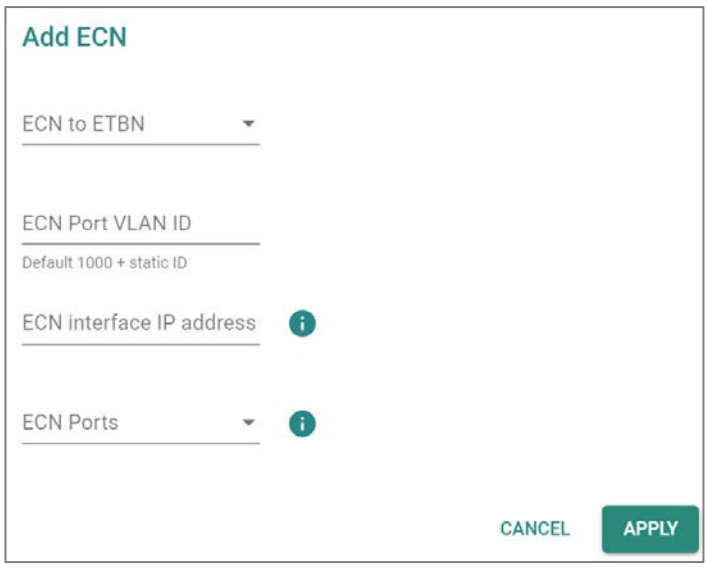
UI Setting	Description
Static ID	Shows the static ID of this ETBN within the consist.
ECN to ETBN	Shows which ETBN in the consist will be connected to by the ECN.
ECN Port VLAN ID	Shows the VLAN ID of the ECN Port.
Interface IP address	Shows the interface IP address for the ECN.
ECN Ports	Shows the ports which the selected ECN will connect to.

Add ECN

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

Clicking the **Add (⊕)** icon on the **Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings** page will open this dialog box. This dialog lets you create a new ECN entry.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
ECN to ETBN	Specify which ETBN in the consist will be connected by the ECN.	Drop-down list of ETBN Static IDs (depends on the **ETBN(s) in Consist** setting in TTDP Settings)	N/A
ECN port VLAN ID	Specify the VLAN ID of the ECN port. Specifying a VLAN ID is required if the selected ECN is connected to this ETBN. **Note** We recommend setting the ECN Port VLAN ID value to 1000 + (Local ETBN Static ID) for cases where each ETBN corresponds to its own ECN.	Valid VLAN ID	N/A

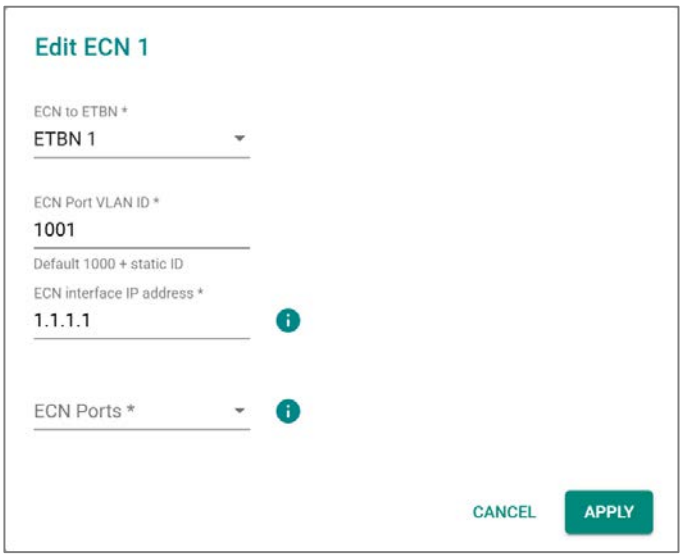
UI Setting	Description	Valid Range	Default Value
ECN interface IP address	Set the interface IP address for the ECN.	Valid IP address	N/A
ECN Ports	Specify which ports the selected ECN will connect to. Specifying ports is required if the selected ECN is connected to this ETBN. Available ports will vary depending on the product model. The port used by the ETBN cannot be selected.	Drop-down list of ports	N/A

Edit ECN

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

Clicking the **Edit ( )** icon for an entry on the **Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings** page will open this dialog box. This dialog lets you edit an existing ECN entry.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
ECN to ETBN	Specify which ETBN in the consist will be connected by the ECN.	Drop-down list of ETBN Static IDs (depends on the **ETBN(s) in Consist** setting in TTDP Settings)	N/A
ECN port VLAN ID	Specify the VLAN ID of the ECN port. Specifying a VLAN ID is required if the selected ECN is connected to this ETBN. **Note** We recommend setting the ECN Port VLAN ID value to 1000 + (Local ETBN Static ID) for cases where each ETBN corresponds to its own ECN.	Valid VLAN ID	N/A
ECN interface IP address	Set the interface IP address for the ECN.	Valid IP address	N/A
ECN Ports	Specify which ports the selected ECN will connect to. Specifying ports is required if the selected ECN is connected to this ETBN. Available ports will vary depending on the product model. The port used by the ETBN cannot be selected.	Drop-down list of ports	N/A

Delete ECN

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TTDP Settings

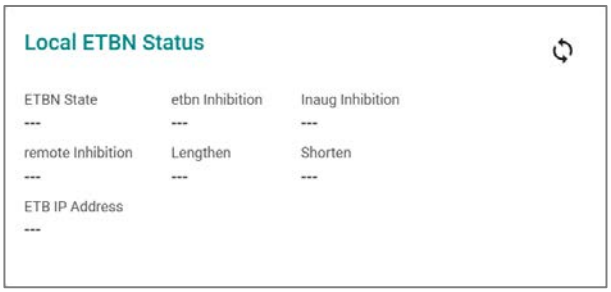
You can delete an ECN entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete ( )** icon.

Local ETBN Status

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - Local ETBN Status

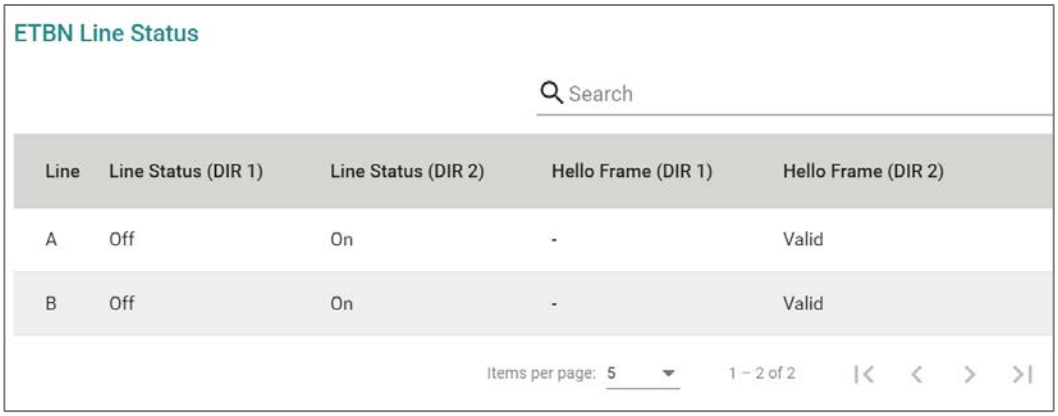
This page lets you see the status of your local ETBN.

Local ETBN Status



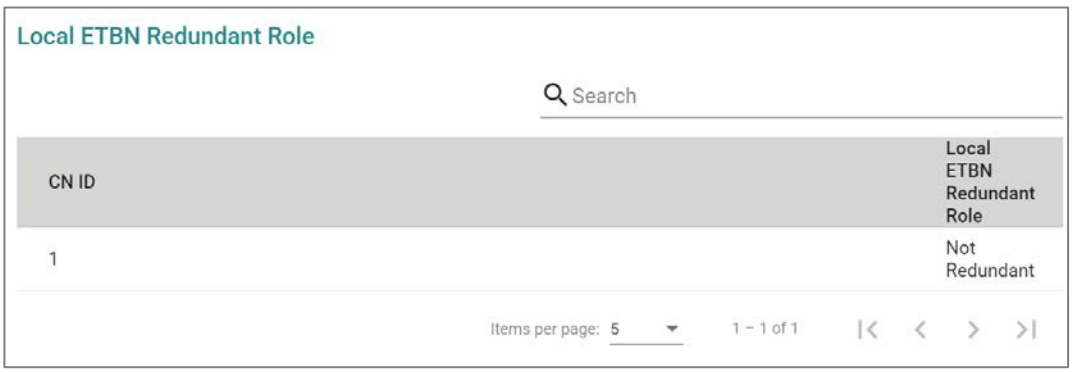
UI Setting	Description
ETBN State	Shows the inauguration status of the ETBN state machine.
etbn Inhibition	Shows information about any inhibition requests from this node.
inaug Inhibition	Shows flags that are the result of the **etbnInhibition** field of topology frames received from all other ETBNs and the CN local value. During power-up, **inaugInhibition** is meaningless until the ETBN reaches the **INAUGURATED** state at least once. The value at startup is set to **False** to allow for the first inauguration.
remote Inhibition	This shows whether the remote composition is allowed to inaugurate (only set by end nodes) when lengthening takes place. The initial value should be set as **UNDEFINED**, which means it shall not be taken into account.
Lengthen	Shows the lengthen status due to a lengthening by an inaugurated composition (can be set by any node), such as the appearance of a new consist. Set to **TRUE** if a node detects a new node with a consist UUID different from those contained in the Train Network Directory.
Shorten	Shows the shorten status due to a shortening, which is the loss of at least one consist at the end of a train (can be set by any node). Set to **TRUE** if a node detects at least one consist is lost at the end of the train according to the Train Network Directory. It resets to **FALSE** (“stable”) by default if the consist appears again or the Train Network Directory is updated.
ETB IP Address	Shows the IP address of the ETB.

ETBN Line Status



UI Setting	Description
Line	Shows which ETBN line (A or B) the entry is for.
Line Status (DIR 1)	Shows the link status of the line for Direction 1 of the ETBN line.
Line Status (DIR 2)	Shows the link status of the line for Direction 2 of the ETBN line.
Hello Frame (DIR 1)	Shows whether the neighbor Ethernet port in Direction 1 for the ETBN is up, and will send Hello Frames.
Hello Frame (DIR 2)	Shows whether the neighbor Ethernet port in Direction 2 for the ETBN is up, and will send Hello Frames.

Local ETBN Redundant Role



UI Setting	Description
CN ID	Shows the ID of the consist node, which is statically defined.
Local ETBN Redundant Role	Shows which CN is connected to the Local ETBN and whether the CN has ETBN redundancy.

ETB Status

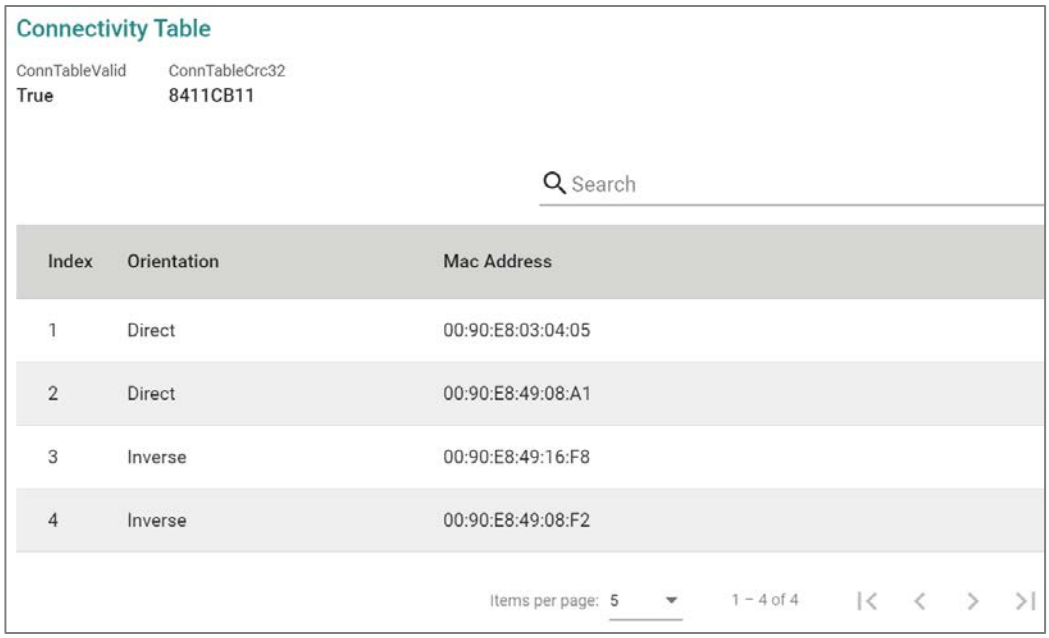
Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - ETB Status

This page lets you see the status of your ETB.

ETB Status

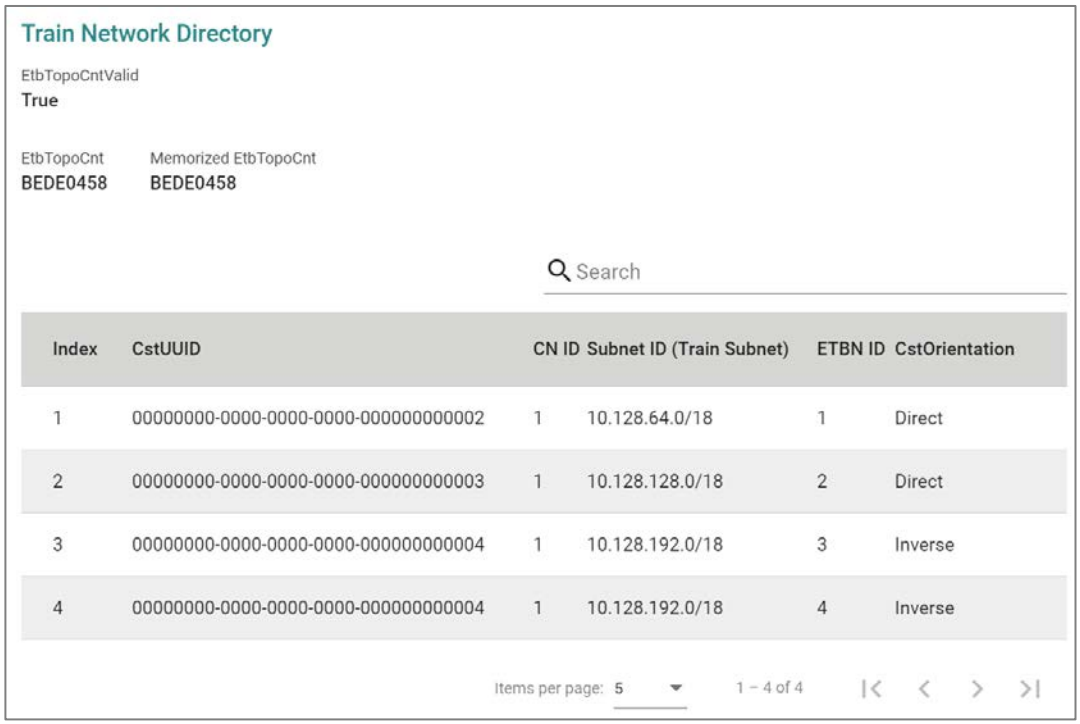
UI Setting	Description
remote Inhibition	This shows whether the remote composition is allowed to inaugurate (only set by end nodes) when lengthening takes place. The initial value should be set as **UNDEFINED**, which means it shall not be taken into account.
Lengthen	Shows the lengthen status due to a lengthening by an inaugurated composition (can be set by any node), such as the appearance of a new consist. Set to **TRUE** if a node detects a new node with a consist UUID different from those contained in the Train Network Directory.
Shorten	Shows the shorten statud due to a shortening, which is the loss of at least one consist at the end of a train (can be set by any node). Set to **TRUE** if a node detects at least one consist is lost at the end of the train according to the Train Network Directory. It resets to **FALSE** (“stable”) by default if the consist appears again or the Train Network Directory is updated.

Connectivity Table



UI Setting	Description
ConnTableValid	Shows whether the Physical Topology is shared by all ETBNs (same connectivity table CRC is used for all ETBNs).
ConnTableCrc32	Shows the CRC32 value of the internal Connectivity Table.
Index	Shows the Index number of a node. The number of entries will vary between models and depending on how many ports have been set up.
Orientation	Shows information about the orientation of the node with respect to the ETB reference direction.
MAC address	Shows the MAC address of the node.

Train Network Directory

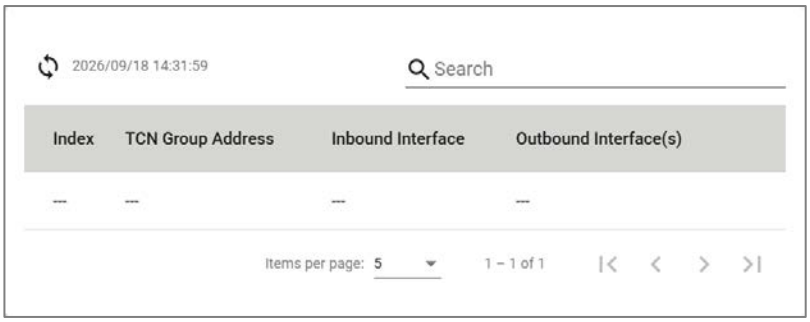


UI Setting	Description
EtbTopoCntValid	Shows whether the Logical Topology is shared by all ETBNs (same Train Network Directory CRC is used for all ETBNs).
etbTopoCnt	Shows the CRC32 checksum of the internal Train Network Directory.
Memorized etbTopoCnt	While the ETB node is in state INAUGURATED, etbTopoCnt field in TTDP TOPOLOGY frame is fixed to the memorized CRC of the Train Network Directory. The Mermorized etbTopoCnt and etbTopoCnt may be different when “inaugInhibition” is inhibited
Index	Shows the Index number of a CN.
CstUUID	Shows the Consist Universal Unique ID (refer to IETF RFC 4122) of the CN.
CN Id	Shows the ID of the CN, which is statically defined.
Subnet Id	Shows the subnet ID of the CN on the ETB.
Train Subnet	Shows the Train Subnet IP of the CN.
ETBN Id	Shows the ID of the ETBN on the ETB.
CstOrientation	Shows the orientation of the consist in relation to the direction of the train.

TCN Multicast Table

Menu Path: Industrial Application > IEC 61375 > Ethernet Train Backbone - TCN Multicast Table

This page lets you see the status of your TCN multicast entries.



UI Setting	Description
Index	Shows the index of the TCN entry.
TCN Group Address	Shows the group address for the TCN.
Inbound Interface	Shows the ETBN inbound interface of the TCN.
Outbound Interface(s)	Shows the ETBN outbound interface of the TCN.

Communication Profile

Menu Path: Industrial Application > IEC 61375 > Communication Profile

This section lets you set up communication profiles for your device.

This section includes these pages:

- ECSP Settings
- SDTv2 Settings
- ECSP Status
- SDTv2 Status

ECSP Settings

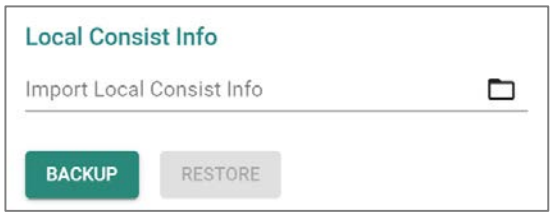
Menu Path: Industrial Application > IEC 61375 > Communication Profile - ECSP Settings

This page lets you back up or restore the local consist info file and the TRDP configuration file.

Local Consist Info

Click **BACKUP** to back up the current local consist info file to your local host. To restore, select a local consist info file from your local host, then click **RESTORE**.

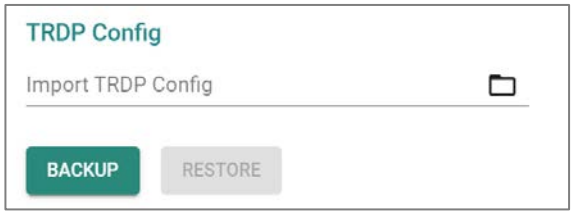
> **Note**
> You cannot back up the local consist info file if one hasn't been previously loaded onto your router.



UI Setting	Description	Valid Range	Default Value
Import Local Consist Info	Select a local consist info file to restore from by clicking on the **Folder ( ) icon**, selecting the file to restore from, then clicking **RESTORE**. Refer to Structure and Syntax of Consist Info Configuration Files for more information.	Local file	N/A

TRDP Config

Click **BACKUP** to back up the current TRDP configuration to your local host. To restore, select a TRDP configuration file from your local host, then click **RESTORE**.

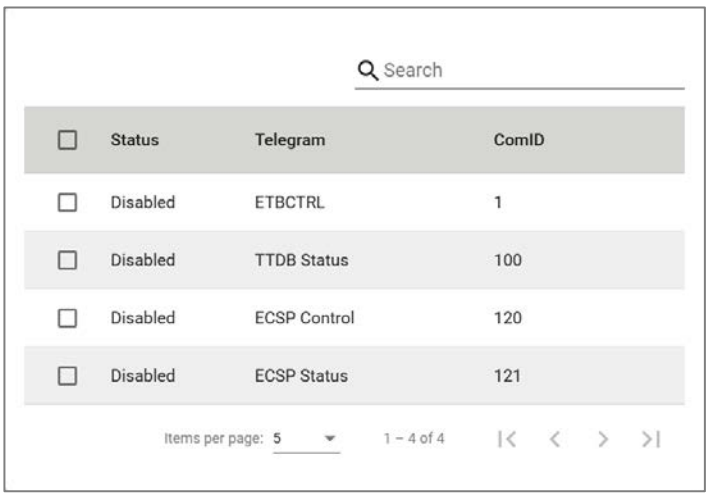


UI Setting	Description	Valid Range	Default Value
Import TRDP Config	Select a local TRDP configuration file to restore from by clicking on the **Folder (🗀) icon**, selecting the file to restore from, then clicking **RESTORE**.	Local file	N/A

SDTv2 Settings

Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTv2 Settings

This page lets you enable or disable Safe Data Transmission protocol (SDTv2) telegrams.



UI Setting	Description
Status	Shows whether the telegram is enabled.
Telegram	Shows the name of the telegram.
ComID	Shows the ComID of the telegram.

Edit Status

Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTv2 Settings

Clicking the **Edit ( )** icon after selecting entries on the **Industrial Application > IEC 61375 > Communication Profile - SDTv2 Settings** page will open this dialog box. This dialog lets you enable or disable the selected entries.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
TTDP Enable	Enable or disable the selected telegrams.	Enabled / Disabled	Enabled

ECSP Status

Menu Path: Industrial Application > IEC 61375 > Communication Profile - ECSP Status

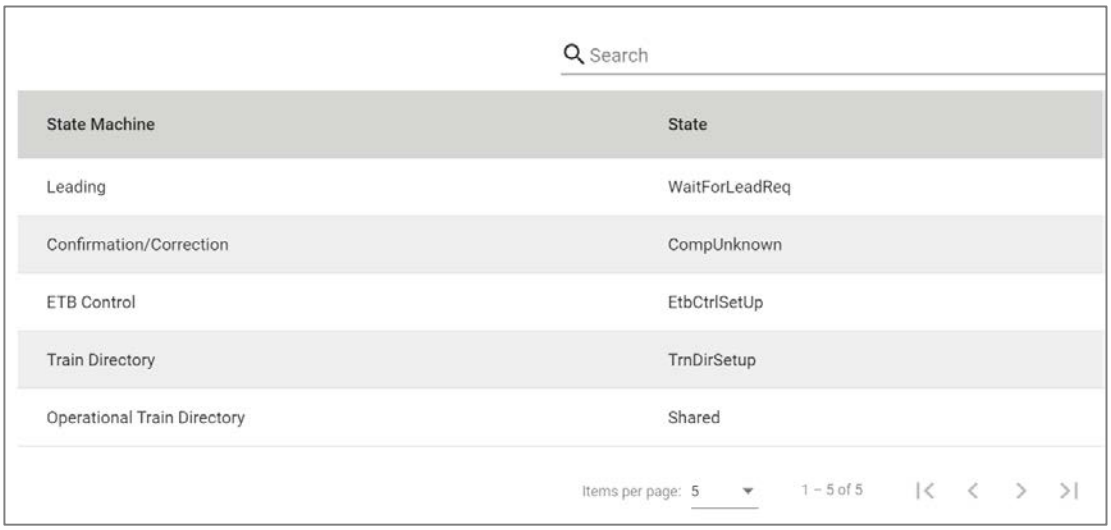
This page lets you see the current status of the ECSP and the state machines.

ECSP Status

UI Setting	Description
ETB Control Service	Shows whether the ETB Control Service Provider (ECSP) is providing ETB Control Service or not, which may be impacted by the VRRP role. **Active**: • Local ECSP (ETBN) is VRRP master, and has found an ECSC • Local ECSP (ETBN) has no redundancy **Not Active**: • Local ECSP (ETBN) is the VRRP backup
ECSC Status	Shows whether an ETB Control Service Client (ECSC) is communicating with the ECSP. • **Online**: The ECSP received a ECSP Control Telegram from an ECSC and is currently connected. • **Offline**: An ECSC previously connected to the ECSP, but is not currently connected. • **NotExist**: The ECSP has not connected to an ECSC yet.

State Machine List

The State Machine List includes the 5 state machines that have been defined in IEC 61375-2-3.



UI Settings	Description
State Machines	Shows the name of the state machine.

UI Settings	Description
State	Shows the current state of the state machine. • **Leading** Init / WaitForLeadReq / WaitForAccept / WaitForLead / WaitForLed / IsLeading / IsLed • **Confirmation / Correction** Init / CompClear / CompUnknown / CompSet / CompStored / CompReset • **ETB Control** Init / WaitForEtbCtrl / EtbCtrlSetUp • **Train Directory** Init / WaitForEtbInaug / WaitForCstInfo / TrnDirSetup • **Operational Train Directory** Init / Invalid / Valid / Shared

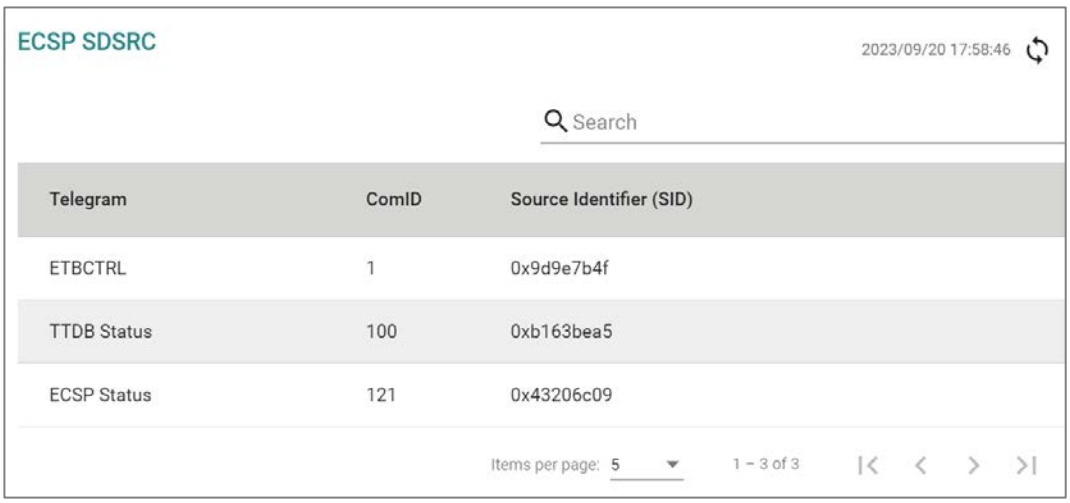
SDTv2 Status

Menu Path: Industrial Application > IEC 61375 > Communication Profile - SDTv2 Status

This page lets you see the SDSRC and SDSINK information for SDTv2 telegrams.

ECSP SDSRC

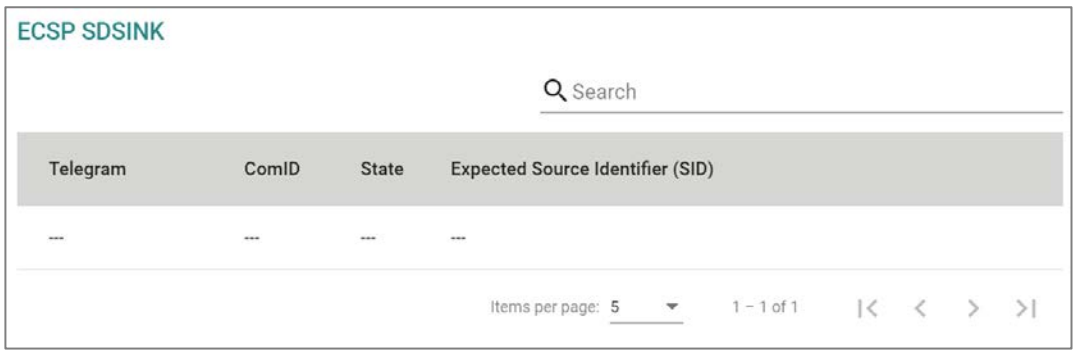
This table shows the Safe Data Source (SDSRC) used for sending vital data packets (VDPs) in SDTv2 telegrams to a Safe Data Sink (SDSINK).



UI Setting	Description
Telegram	Shows the name of the telegram.
ComID	Shows the ComID for the telegram.
Source Identifier (SID)	Shows the SID for the telegram, which is an unsigned32 value computed as an SC-32 signature of the data structure.

ECSP SDSINK

This table shows the Safe Data Sink (SDSINK) used to receive vital data packets (VDPs) in SDTv2 telegrams from a Safe Data Source (SDSRC).



UI Setting	Description
Telegram	Shows the name of the telegram.
ComID	Shows the ComID for the telegram.
State	Shows the state of the telegram. • **RegularCommunication**: In this state, transmitted VDPs cannot be considered to be safe. • **State SafeCommunication**: In this state, transmitted VDPs can be considered to be safe.
Expected Source Identifier (SID)	Shows the SID of the expected SDSRC to receive VDPs from. This information is retrieved from the Train Topology Database (TTDB).

Operational Status

Menu Path: Industrial Application > IEC 61375 > Operational Status

This page lets you know the Status of your IEC 61375 related operational settings.

This page includes these tabs:

- Consist Info
- Train Directory
- Operational Train Directory
- TCN-URI Table

Consist Info

Menu Path: Industrial Application > IEC 61375 > Operational Status - Consist Info

This page lets you see information about the current consist.

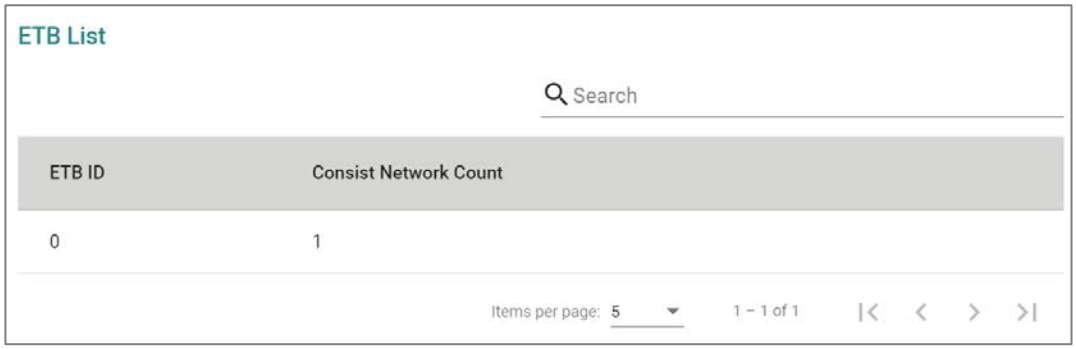
> **Note**
> Consist information can only be viewed through the Web UI and cannot be viewed through the CLI interface.

Consist Info

UI Setting	Description
Consist Class	Shows the CSTINFO class of the consist.
Consist Type	Shows the type of the consist.

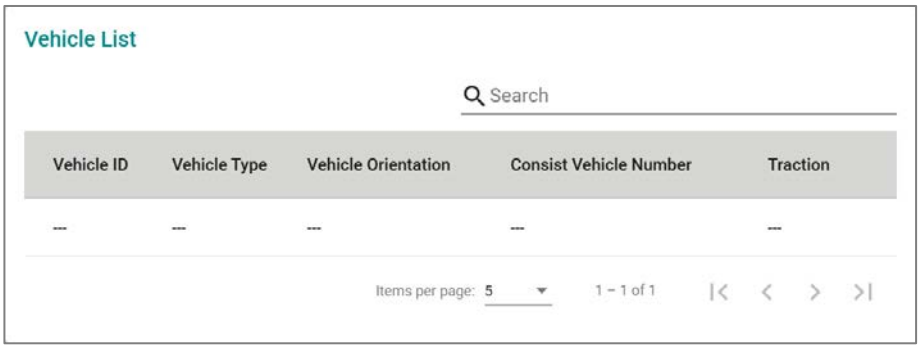
UI Setting	Description
Consist ID	Shows the ID of the consist.
Consist Owner	Shows the owner of the consist.
Consist UUID	Shows the UUID of the consist.

ETB List



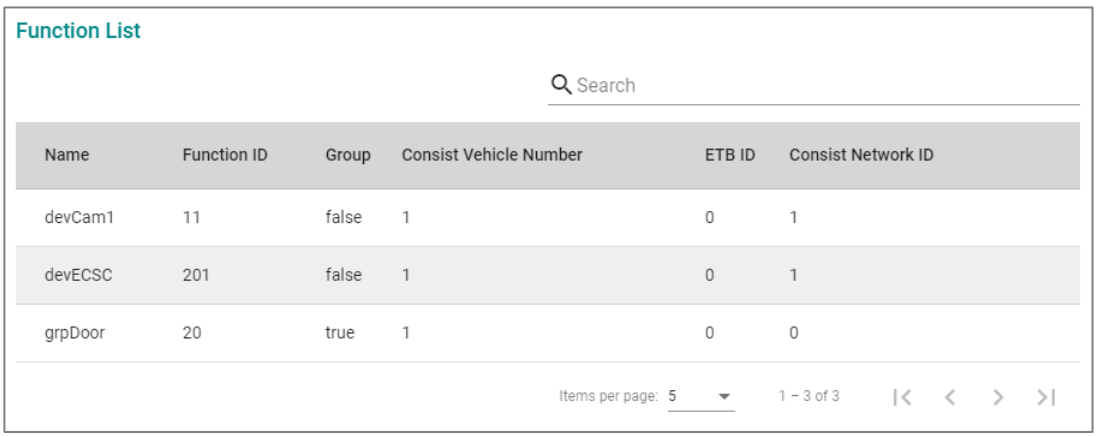
UI Setting	Description
ETB ID	Shows the ID of the ETB. • **0**: ETB0 (operational network) • **1**: ETB1 (multimedia network) • **2**: ETB2 (other network) • **3**: ETB3 (other network)
Consist Network Count	Shows how many CNs are in the consists connected to the ETB.

Vehicle List



UI Setting	Description
Vehicle ID	Shows the ID of the vehicle.
Vehicle type	Shows the type of the vehicle.
Vehicle Orientation	Shows the orientation of the vehicle. • **same**: Indicates that vehicle has the same direction with respect to the consist direction. • **inverse**: Indicates that the vehicle is in the opposite direction with respect to the consist direction.
Consist Vehicle Number	Shows the index of the vehicle within the consist.
Traction	Shows whether the vehicle has traction.

Function List



UI Setting	Description
Name	Shows the name of the device/functional group.
Function ID	Shows the ID of the device/functional group.
Group	Shows whether this is a functional group.
Consist Vehicle Number	Shows the index of the vehicle Sequence number of the vehicle within the consist the device/functional group belongs to.
ETB ID	Shows the ID of the ETB the device/functional group is on. • **0**: ETB0 (operational network) • **1**: ETB1 (multimedia network) • **2**: ETB2 (other network) • **3**: ETB3 (other network)
Consist Network ID	Shows the ID of the consist network the device/functional group is in.

Train Directory

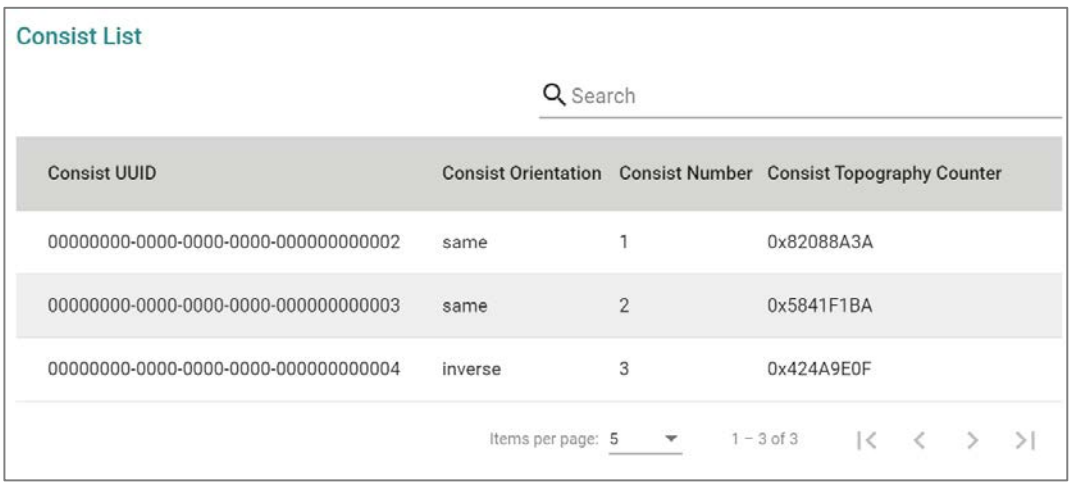
Menu Path: Industrial Application > IEC 61375 > Operational Status - Train Directory

This page shows information about the train and the consists in it.

Train Directory

UI Setting	Description
ETB ID	Shows the ID of the ETB. • **0**: ETB0 (operational network) • **1**: ETB1 (multimedia network) • **2**: ETB2 (other network) • **3**: ETB3 (other network)
Train Topography Counter	Shows a counter used to check whether all the ECSPs in the train have the same train direction during ECSP negotiation.

Consist List



UI Setting	Description
Consist UUID	Shows the UUID of the consist.
Consist Orientation	Shows the orientation of the consist. • **same**: Indicates that consist has the same direction with respect to the train direction. • **inverse**: Indicates that the consist is in the opposite direction with respect to the train direction.
Consist Number	Shows the index of the consist within the train.
Consist Topology Counter	Shows the consist topography counter provided with the CSTINFO.

Operational Train Directory

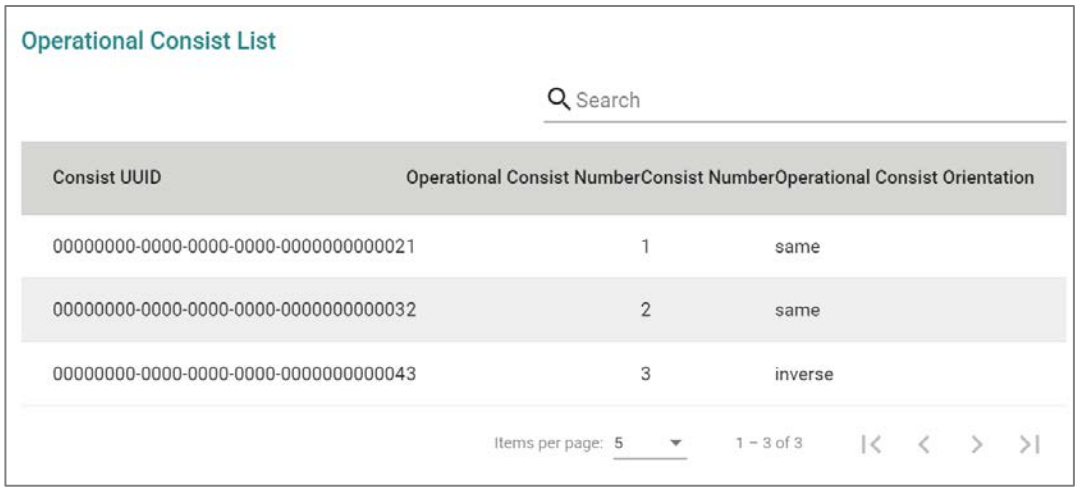
Menu Path: Industrial Application > IEC 61375 > Operational Status - Operational Train Directory

This page shows information about the operational train, consists, and vehicles.

Operational Train Directory

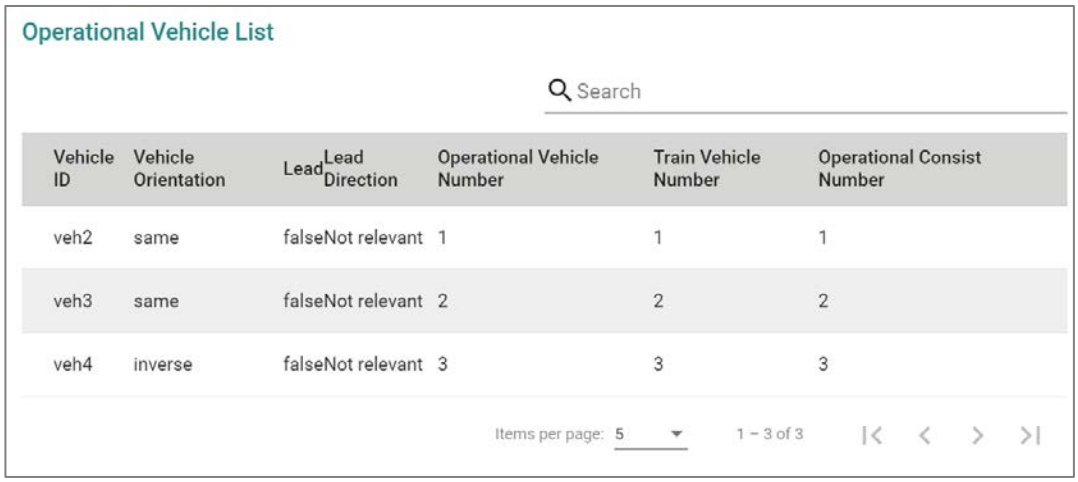
UI Setting	Description
ETB ID	Shows the ID of the ETB. • **0**: ETB0 (operational network) • **1**: ETB1 (multimedia network) • **2**: ETB2 (other network) • **3**: ETB3 (other network)
Operational Train Orientation	Shows the orientation of the vehicle. • **same**: Indicates that operational train has the same direction with respect to the train direction. • **inverse**: Indicates that the operational train is in the opposite direction with respect to the train direction. • **unknown**: The direction of the operational train is unknown.
Operational Train Topography Counter	Shows the computed operational train topography counter, which is automatically configured.

Operational Consist List



UI Setting	Description
Consist UUID	Shows the UUID of the operational consist.
Operational Consist Number	Shows the index of the operational consist, which is automatically configured.
Consist Number	Shows the index of the consist that the operational consist is in.
Operational Consist Orientation	Shows the orientation of the operational consist. • **same**: Indicates that the operational consist has the same direction with respect to the train direction. • **inverse**: Indicates that the operational consist is in the opposite direction with respect to the train direction. • **unknown**: The direction of the operational consist is unknown.

Operational Vehicle List

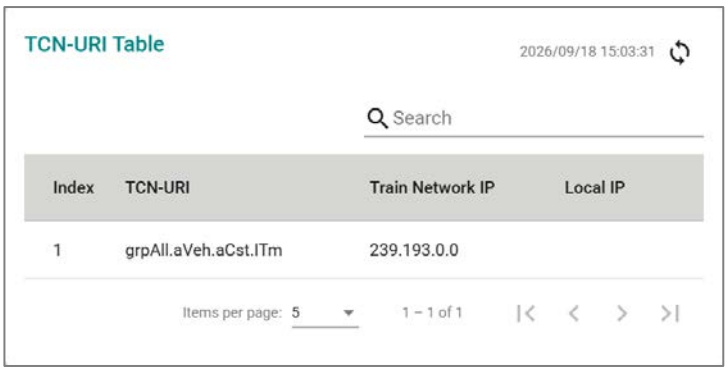


UI Setting	Description
Vehicle ID	Shows the ID of the operational vehicle.
Vehicle Orientation	Shows the orientation of the operational vehicle. • **same**: Indicates that the operational vehicle has the same direction with respect to the operational train direction. • **inverse**: Indicates that the operational vehicle is in the opposite direction with respect to the operational train direction. • **unknown**: The direction of the operational vehicle is unknown.
Lead	Shows whether the operational vehicle is leading.
Lead Direction	Shows the direction used for the operational vehicle.
Operational Vehicle Number	Shows the index of the operational vehicle in the operational train.
Train Vehicle Number	Shows the index of the vehicle that the operational vehicle belongs to.
Operational Consist Number	Shows the index of the operational consist the operational vehicle belongs to.

TCN-URI Table

Menu Path: Industrial Application > IEC 61375 > Operational Status - TCN-URI Table

This page lets you see the mappings between Train Communication Network Uniform Resource Indentifiers (TCN-URIs) and IP addresses.



UI Setting	Description
Index	Shows the index number of the TCN-URI.
TCN-URI	Shows the Train Communication Network Uniform Resource Indentifier (TCN-URI) of a component on the train.
Train Network IP	Shows the train network IP used for the TCN-URI.
Local IP	Shows the local IP used for the TCN-URI.

Chapter 4

Other Features

Firmware Image Recovery Overview

Firmware Image Recovery refers to the use of multiple copies of firmware within a device to increase reliability and reduce the risk of system failure due to firmware corruption or errors.

In many electronic devices, firmware is stored in non-volatile memory such as flash memory, and any corruption or errors in the firmware can result in the device malfunctioning or becoming unusable. To mitigate this risk, firmware recovery involves storing multiple copies of the firmware within the device, and using a mechanism to switch to a backup copy of the firmware in case the primary copy becomes corrupted or fails.

Overall, Firmware Image Recovery is a useful technique for increasing the reliability and availability of electronic devices, particularly those used in critical applications where system failure can have serious consequences.

Methodology

This device supports a “Dual-image” firmware mechanism to minimize the possibility of system failure, such as in the following situations:

1. When the user encounters an accident when upgrading the device firmware, such as a power outage, which may cause firmware corruption.
2. When the memory encounters lifespan issues or damage from external factors, parts of partitions may become corrupted.

This mechanism involves storing two copies of the firmware in separate memory partitions within the device, and using a boot loader to select the active copy at runtime. If a situation occurs, the firmware can still roll back to the previous version to boot the device.

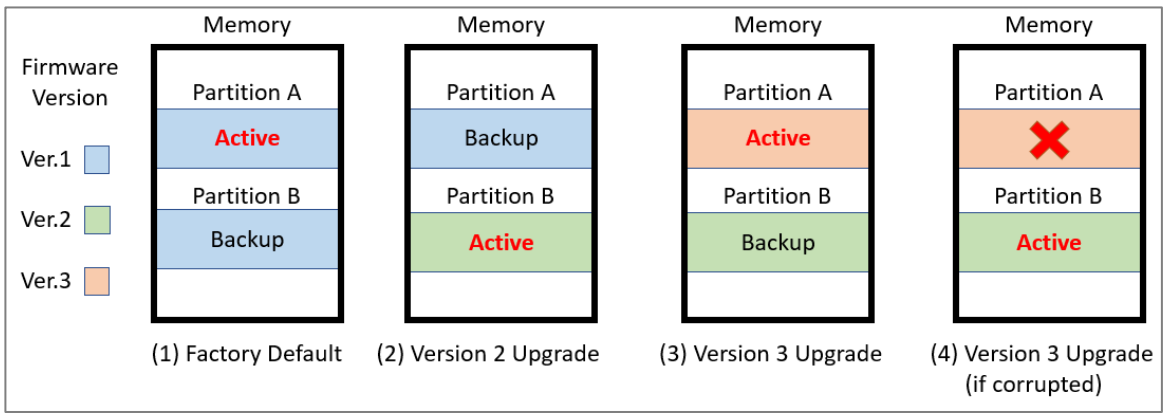
⚠ Warning

Firmware Image Recovery will not be able to help if the bootloader sector or the entire memory is corrupted.

How Dual-imaging Works

Here is an overview of how the Dual-image function works.

1. When the product leaves the factory, it will keep two identical copies of the firmware version 1 in separate memory partitions A and B within the device. Partition A will be selected as the active copy by default.
2. When the user upgrades the firmware version 2, Partition B will be overwritten to store the new image as well as be selected as the active copy at the same time. Partition A will keep a previous version 1 as a backup.
3. When the user upgrades the firmware version 3, Partition A will be overwritten to store the new image as well as be selected as the active copy at the same time. Partition B will keep a previous version 2 as a backup.
4. Based on (3), if the user encounters an accident when upgrading the firmware version 3 and Partition A is corrupted, the bootloader will choose backup Partition B as the active one to continue to boot the system and the system will record a “Boot Failed, Fallback to Previous Firmware” event into the system logs.



Note

- Resetting the device to factory default settings only restores user configurations, and will not restore the firmware image in both partitions.
- This mechanism is done automatically by the system and is not user-configurable.

Soft Lockdown

> **Note**
>
> Soft Lockdown Mode is a feature designed for railway applications and is only supported by the TN-4900 Series.

Moxa routers can act as firewalls to help provide protection from external attacks that try to gain access and control over the network. On the other hand, while protecting the network, it is also important to prevent potential malfunctions that may occur and avoid unexpected network operation failures.

To handle this, Soft Lockdown Mode is a monitoring and protection mechanism that monitors important indicators and enters Soft Lockdown Mode once user-defined failure criteria are reached to ensure that device operation remains stable. For details about Soft Lockdown Mode settings, refer to Soft Lockdown Mode.

Soft Lockdown Criteria

The criteria for entering and leaving Soft Lockdown Mode are defined by the following:

- **Performance Thresholds**: If the CPU utilization % exceeds a user-defined threshold, or the amount of free memory % goes below a user-defined threshold, a failure will be detected for the current cycle.
- **Monitoring Interval**: This defines how long a single monitoring cycle will be.
- **Number of Cycles to Enter Soft Lockdown Mode**: This defines how many consecutive cycles with failures are required to enter Soft Lockdown Mode.
- **Number of Cycles to Leave Soft Lockdown Mode**: This defines how many consecutive cycles without failures are required to leave Soft Lockdown Mode.
- **Critical Services**: If any of the following critical services are enabled, the device continually check to see whether the services are alive. The device will enter Soft Lockdown Mode if any enabled critical service is no longer alive, and all enabled critical services must be alive to leave Soft Lockdown Mode.

Note

The critical services that apply to Soft Lockdown Mode are as follows:

- DHCP Server (refer to DHCP Server)
- DHCP Relay Agent (refer to DHCP Relay Agent)
- SNMP Server (refer to SNMP)
- Turbo Ring V2 (refer to Turbo Ring V2)

Warning

When the device is operating normally, its CPU and memory usage can vary due to various factors. Apart from potential attacks, the number of devices connected to the router and application settings can also lead to increased demands on CPU and memory.

It is important to carefully assess the usage and configuration of this feature to avoid triggering Soft Lockdown Mode due to normal usage to avoid impacting regular operations.

Entering Soft Lockdown Mode

The device will enter Soft Lockdown Mode when any of the following occur:

- The number of consecutive cycles with failures reaches the defined **Number of Cycles to Enter Soft Lockdown Mode**
- Any of the enabled **Critical Services** are no longer alive

When in Soft Lockdown Mode

In Soft Lockdown Mode, the device will do the following:

- Block all traffic (both ingress and egress) on the interface specified for Soft Lockdown Mode
- Log the event and the reason for the event in the system log

⚠ Warning

When Soft Lockdown Mode is enabled, the port settings and VLAN settings should not be modified in order to prevent a mismatch for the Soft Lockdown Mode interface settings.

Leaving Soft Lockdown Mode

The device will leave Soft Lockdown Mode under any of the following conditions:

- The number of normal consecutive cycles without failures reaches the defined **Number of Cycles to Leave Soft Lockdown Mode** AND all enabled **Critical Services** are alive.
- The device is restarted. After restarting, the device will enter normal operation and will only enter Soft Lockdown Mode if the criteria are fulfilled.

When leaving Soft Lockdown Mode, the device will do the following:

- Resume all traffic (both ingress and egress) on the interfaces where firewall rules are applied
- Log the event in the system log

Serial Operation Modes

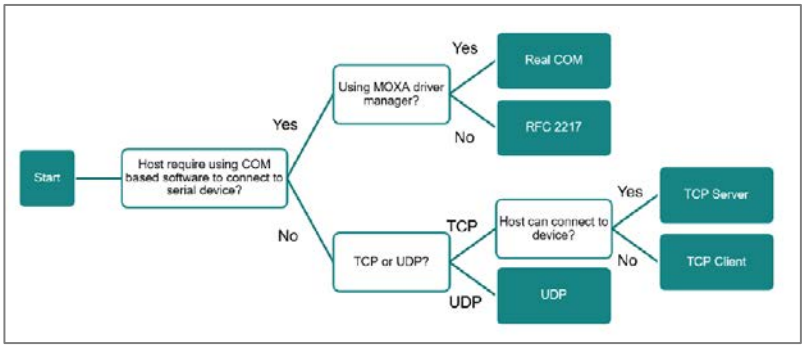
This device enables traditional serial (RS-232/422/485) devices to transmit data over a cellular network and allows you to access, manage, and configure remote facilities and equipment over the cellular network from anywhere in the world. The operation mode determines how the device's serial port will interact with the network. Which operation mode to select will depend on your specific application.

Traditional SCADA and data collection systems rely on the serial port to collect data from various types of instruments. Some software is required to connect the serial device to the COM port on the host computer. The Real COM and RFC 2217 modes allow you to expand a virtual COM port for a host computer on demand. As long as your host computer supports the TCP/IP protocol, SCADA and data collection systems will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

The main difference between Real COM and RFC 2217 mode is that Real COM mode requires MOXA Windows Driver Manager to be installed on the host. The RFC 2217 mode allows third party drivers that support the RFC 2217 standard to perform virtual COM mapping to the serial port on the industrial secure router.

Some applications do not require the serial device to be physically connected connect to a COM port, but only need to establish a connection to receive data from the serial device. In that case, you can use TCP or UDP mode to establish the connection. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer faster delivery.

TCP Server mode allows the host to request a connection to the industrial secure router. In TCP Client mode, the industrial secure router actively establishes a connection to a host computer for serial data transmission. If the industrial secure router is using a cellular connection and is difficult to access via fixed IP or VPN, you should select TCP Client mode and directly connect to the host.

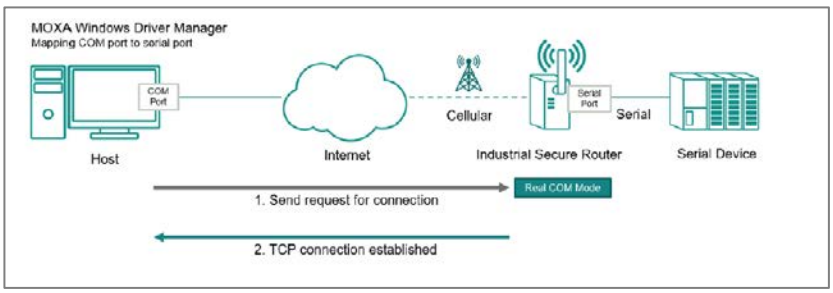


Operation Mode - Real COM

In Real COM mode, the bundled drivers can establish a transparent connection between a host and a serial device by mapping the serial port on the industrial secure router to a local COM port on the host computer.

One of the major benefits of using Real COM mode is that it allows you to use software that was written for strictly serial communication applications. The Moxa driver manager intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card to the Internet. At the other end of the connection, the industrial secure router accepts the IP frame from the cellular network, unpacks the TCP/IP packet, and then transparently sends the data through the serial port to the attached serial device. This operation mode supports up to 2 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.

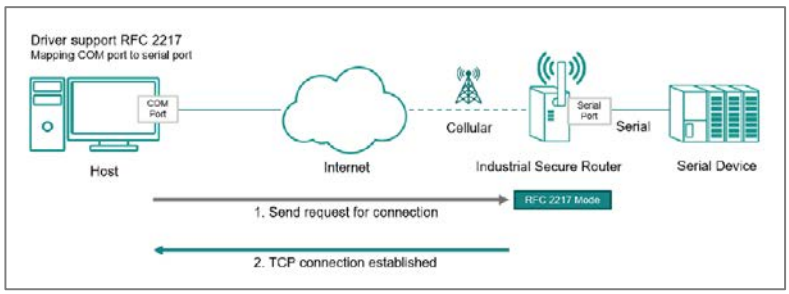
Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.



Operation Mode - RFC 2217

Similar to Real COM mode, RFC-2217 mode also uses a driver to establish a transparent connection between a host computer and a serial device by mapping the serial port on the Industrial Secure Router to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement virtual COM mapping to serial port on the Industrial Secure Router.

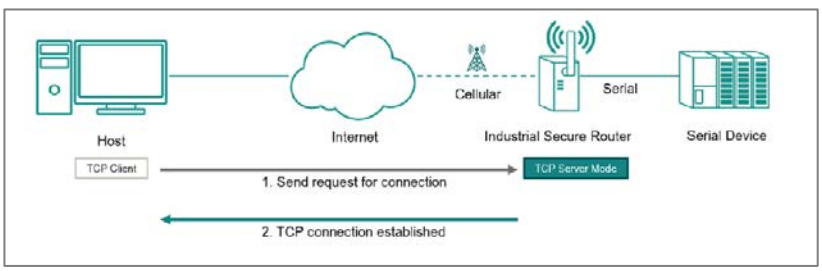
Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.

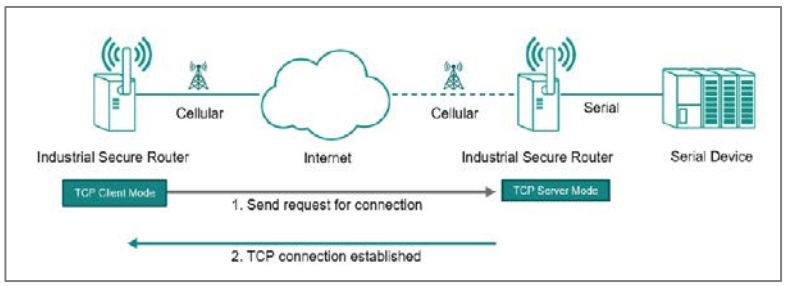


Operation Mode - TCP Server

In TCP Server mode, the serial port on the Industrial Secure Router is assigned a unique IP/port combination on a TCP/IP network. The host computer initiates contact with the Industrial Secure Router, establishes the connection, and receives data from the serial device. This operation mode supports up to 2 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.

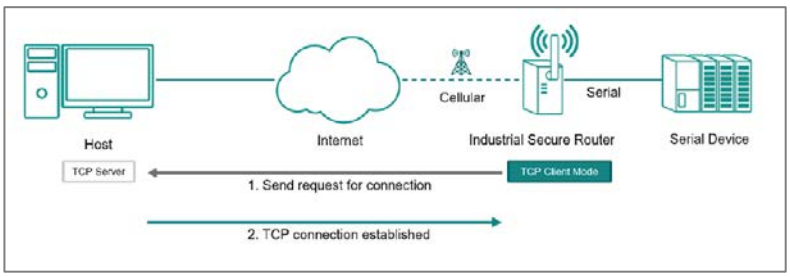
Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.





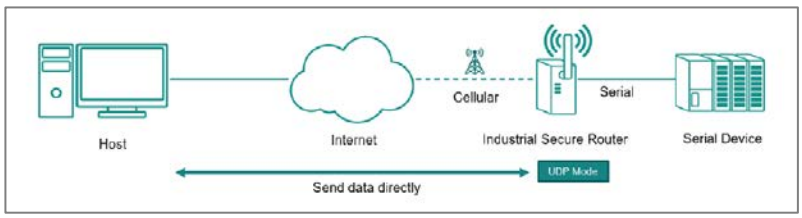
Operation Mode - TCP Client

In TCP Client Mode, the Industrial Secure Router can actively establish a TCP connection with a predetermined host computer when serial data arrives. After the data has been transferred, the Industrial Secure Router can disconnect automatically from the host computer by using the TCP alive check time or inactivity time settings.



Operation Mode - UDP

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can unicast to one host or multicast to multiple hosts and the serial device can receive data from one or multiple host computers. These traits make UDP mode especially well-suited for message display applications.



Chapter 5

Device Applications

Device Applications Overview

This section goes over different device applications to help you better understand the applications themselves, and to show you how the device can help you implement those applications.

The following applications are covered:

- Network Segmentation
- Redundancy
- Routing
- OpenVPN Client
- NetFlow
- Loopback Interfaces

Network Segmentation

About Network Segmentation

Network Segmentation creates isolated virtual networks.

Segmenting a network reduces congestion and improves network performance by removing unnecessary traffic in a particular segment. For instance, segregating the passenger Wi-Fi network from the TCMS network in a train communication system ensures that the TCMS devices are not impacted by guest traffic. Such an approach helps to mitigate congestion and enhance the overall efficiency of the network.

There are two types of network segments:

- Layer-2 segments use numbered, virtual LAN segments (VLANs) to create isolated networks.
- Layer-3 segments use unique IP prefixes to create subnets.

Layer-2 Segments

A layer-2 segment is essentially a single broadcast domain. All devices connected to the segment will receive any broadcast traffic sent within it. Layer-2 segmentation uses numbered VLANs to create isolated logical segment, which allows for the separation of traffic between different VLANs.

Layer-3 Segments

In an IP network, a layer-3 segment is referred to as a subnetwork or subnet and includes all nodes that share the same network prefix as defined by their IP addresses and network mask. A router is needed to facilitate communication between layer-3 subnets. Hosts on the same subnet can communicate directly using the layer-2 segment that connects them.

VLANs in Depth

A VLAN, or Virtual Local Area Network, is a logical grouping of devices on a network.

This technology allows network administrators to divide a large network into smaller, more manageable segments without the need for additional physical hardware. Devices within a VLAN can be located anywhere on the network but communicate as though they are on the same physical segment. This facilitates traffic management, as administrators can ensure traffic is directed only to devices within the same VLAN by assigning a VLAN tag to each Ethernet frame. Consequently, VLANs provide a means to segment a network beyond the constraints of physical connections, a limitation inherent in traditional network design. VLANs can be utilized to segment your network into various groups, such as:

- **Departmental groups**—One VLAN for the R&D department, another for Office Automation, etc.
- **Hierarchical groups**—One VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—One VLAN for email users and another for multimedia users.

VLAN Standards and Implementation

The functioning of VLANs is guided by IEEE 802.1Q, often referred to as Dot1q. This standard outlines the protocol for VLAN tagging on Ethernet frames within an IEEE 802.3 Ethernet network. During the transmission of data between switches, VLAN tags identify the VLAN ownership of frames. Networking equipment reads these tags and ensures that tagged frames are delivered to devices within that VLAN, maintaining the network's logical segmentation.

A VLAN tag is a specific piece of data embedded in the header of an Ethernet frame. It comprises a 4-byte field carrying key information, such as the VLAN ID (VID) and priority level. The VID is a numerical identifier that uniquely links the frame to a specific VLAN. The priority field within the tag plays a critical role in prioritizing certain types of traffic within a VLAN. This structure contributes to effective network traffic management by giving precedence to certain data when necessary.

Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

VLANs help control traffic

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs simplify device relocation

In traditional networks, administrators spend significant time managing moves and changes, requiring manual updates of host addresses when users switch sub-networks. In contrast, VLANs simplify this process. For example, when relocating a host from Port 1 to Port 6 in a different network section, simply assign Port 6 to the relevant VLAN (e.g., VLAN R&D A). This enables seamless communication between VLANs, eliminating the need for re-cabling.

VLANs provide extra security

Devices within each VLAN can only communicate with other devices on the same VLAN. If VLAN R&D B needs to communicate with VLAN OA(Office Automation) A, the traffic must pass through a routing device or Layer 3 switch.

Important

Network segmentation is not a substitute for network security. While network segmentation can provide a degree of isolation that contributes to the overall security environment, the primary benefit of VLANs is improved performance by ensuring minimal crosstalk between unrelated systems. Network segmentation should be complimented with network security procedures.

Scenario: Layer 2 Segmentation of 3 Factories

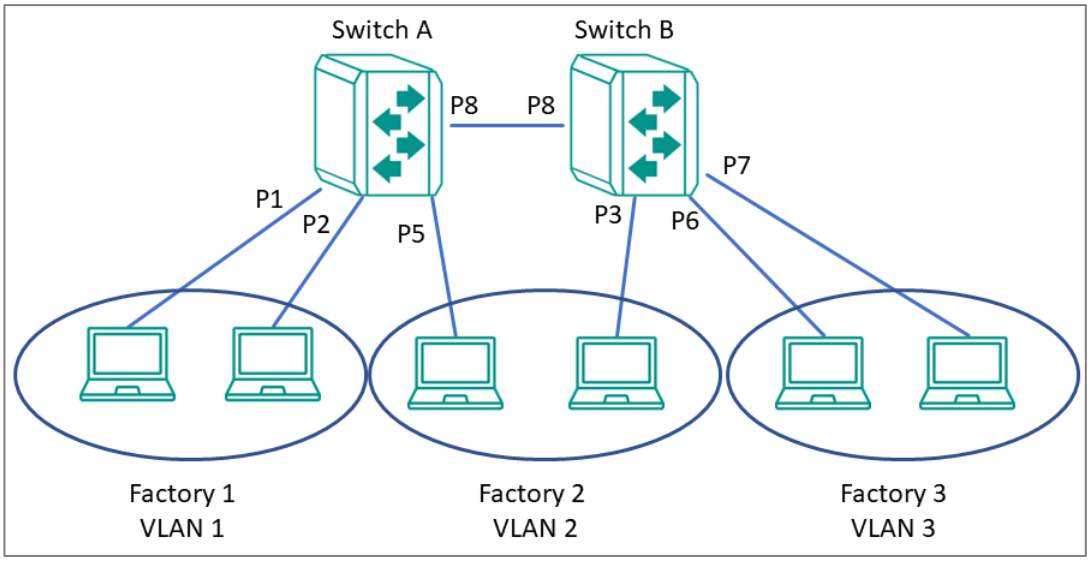
Short Description: A manufacturer uses layer 2 segmentation to manage traffic between three different factories, each with many devices.

Two switches are used to connect the all of the devices together on the same network, but devices from any factory may be connected to either switch. To simplify management and ensure smooth operations, we can configure the switches to make sure that each factory is on its own VLAN.

Each VLAN can be enlarged using simple switches to connect any number of devices in the factory

For our example scenario, we will simplify to two devices connected to each switch. Traffic VLANs are usually assigned to ports, so it's important to note which port we'll be using for each device. The switches are connected each other using port 8, and will allow VLANs to be split between the two switches as necessary, without causing interference or performance drops on the others.
We need a topology that:

- Allows devices on the same VLAN to communicate with each other
- Ensure devices on different VLANs cannot communicate with each other



This diagram outlines how we might create a network meeting these requirements. Each factory is on its own VLAN, and that Factory 2's VLAN is split between two switches. With VLAN segmentation and a Trunk connecting the two switches, Factory 2's VLAN will have comparable performance to VLANs within the same switch. Because of VLAN isolation, administrators can manage and prioritize traffic to ensure that packets do not leave their corresponding VLAN.

Important

Be careful when configuring VLANs on a remote switch. Modifications to the configuration could affect connectivity. For example, if the management VLAN of the switch is VLAN 1 and you are connected to ports that do not belong to VLAN 1, you may be disconnected from the switch during configuration.

Example: Creating VLANs for Layer 2 Segmentation of 3 Factories

Create VLANs in preparation for assigning them to ports.

Before you begin: Make sure you have an environment configured in line with our scenario. This includes:

- 3 routers in a ring topology with backbone connected on ports 7 and 8
- 2 gateways for each router (Service A and Service B), connected at ports 1 and 2, respectively
- Administrator credentials to all three routers

To create VLANs for this example, do the following:

1. Sign in to Switch A using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To add a VLAN ID, click on the **Settings** tab, and then click the **Add ( )** button.
   Result: The **Create VLAN** screen appears.
4. Specify the VLAN to create in the VID, and then click Create. For Factory 1, we will create VLAN 1.
   Result: The VLAN will appear on the VLAN table at the top of the page.
5. Repeat this process to create VLANs 2 and 3 for the factories, and then create VLAN 1000 for the link between switches.

Results: We created VLANs for each factory (VIDs 1, 2, 3) and the VLAN for communication between switches (VID 1000).

What to do next: After you have created all 4 VLANs on Switch A, repeat this process on Switch B. Once Switch B is configured, you can continue on to assigning VLANs to ports.

Example: Assigning VLANs to Ports on Switch A

VLANs must be assigned to ports on Switch A to route traffic correctly.

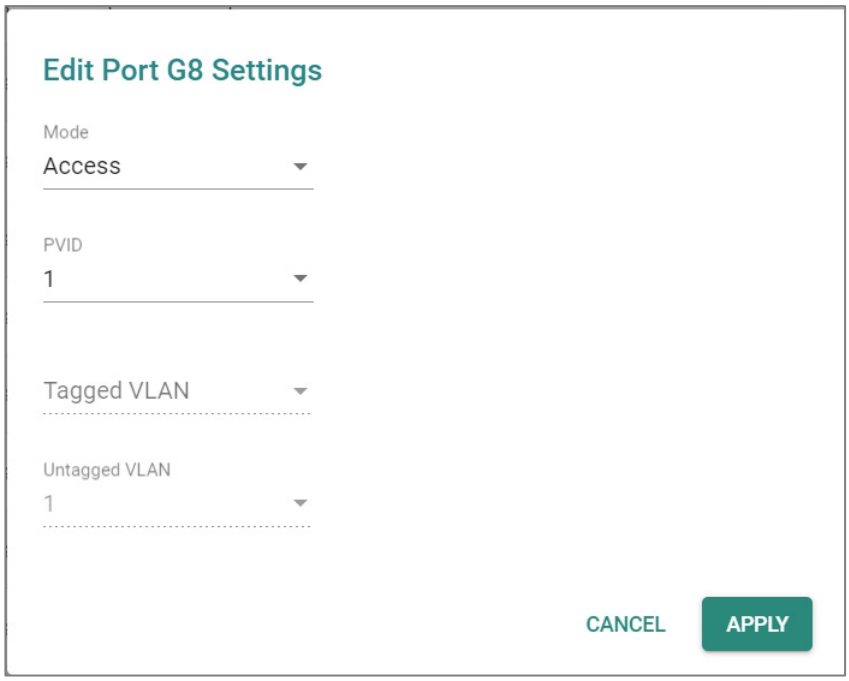
Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Switch A using administrator credentials.

2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

   Since we're assigning factory 1 to ports 1 and 2, start with **Port 1**. If you are repeating this step, you can substitute **Port 1** with information from the table at the end of this procedure.

   Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

   To assign the chosen port to Factory 1, specify **Mode Access** and **PVID** as 1.

Tutorial Info:

Access mode is used when connecting single devices without tags. These are usually end-user devices that belong to a single VLAN, and do not need to communicate with devices in other VLANs.

Trunk mode allows a port to carry traffic for multiple VLANs over a single physical connection. This is useful for linking switches together that may have many different VLANs.

Hybrid mode is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

Note: The port VID (PVID) setting will apply a VLAN tag only for untagged traffic coming through that port. If traffic going through the port has already been tagged with a VLAN ID, the PVID setting will not change the existing tag.

Result: The **Port Table** will show the new port configuration.

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
2	• **PVID**: 1 • **Mode**: **Access Mode**
5	• **PVID**: 2 • **Mode**: **Access Mode**
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 1, 2, 3

Results: Ports on Switch A have been assigned VIDs and modes, ensuring that untagged traffic on ports 1 and 2 will automatically be tagged as VLAN 1. Traffic on port 5 will be automatically tagged as VLAN 2. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

What to do next: Assign VLANs to Ports on Switch B.

> Important
>
> The Port settings on each switch will be slightly different. Make sure each switch is configured correctly by following the instructions for Switch B.

Example: Assigning VLANs to Ports on Switch B

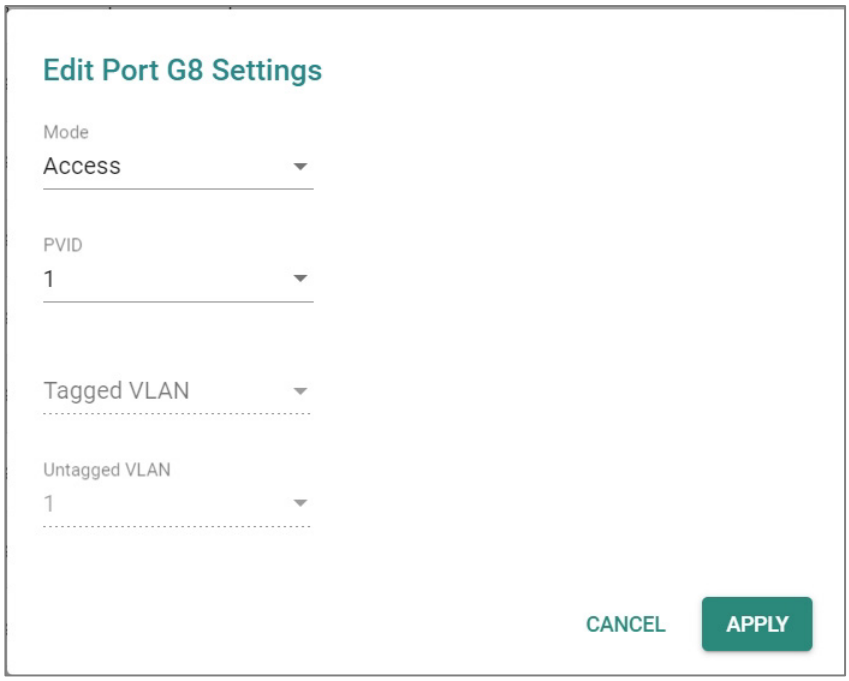
VLANs must be assigned to ports on Switch B to route traffic correctly.

Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Switch A using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

Since we're assigning factory 2 to port 3, start with **Port 3**. If you are repeating this step, you can substitute **Port 3** with information from the table at the end of this procedure.

Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

   To assign the chosen port to Factory 3, specify **Mode Access** and **PVID** as 2.

Tutorial Info:

Access mode is used when connecting single devices without tags. These are usually end-user devices that belong to a single VLAN, and do not need to communicate with devices in other VLANs.

Trunk mode allows a port to carry traffic for multiple VLANs over a single physical connection. This is useful for linking switches together that may have many different VLANs.

Hybrid mode is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

Note: The port VID (PVID) setting will apply a VLAN tag only for untagged traffic coming through that port. If traffic going through the port has already been tagged with a VLAN ID, the PVID setting will not change the existing tag.

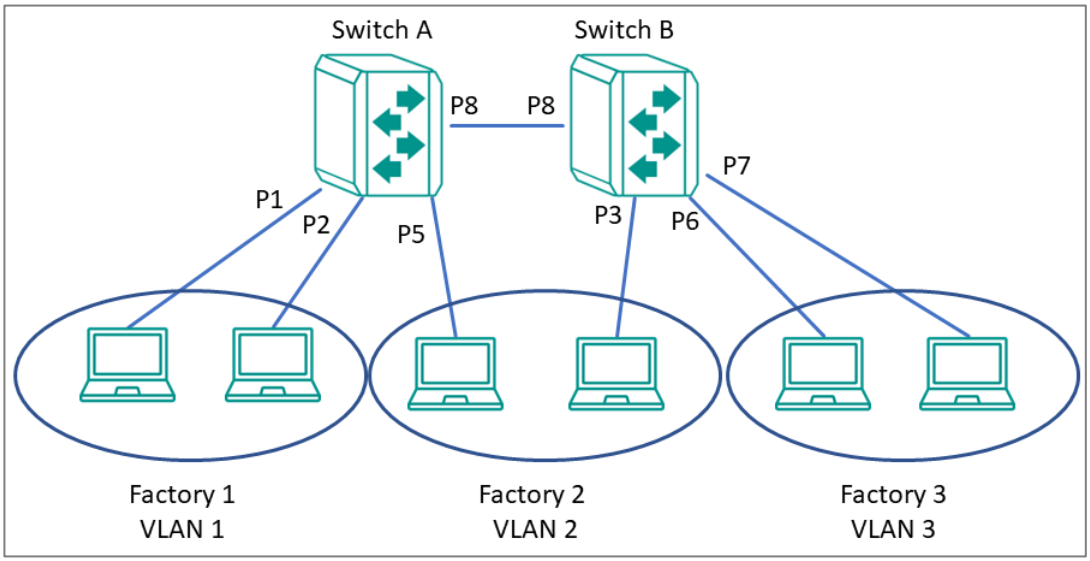
Result: The **Port Table** will show the new port configuration.

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
6	• **PVID**: 1 • **Mode**: **Access Mode**
7	• **PVID**: 2 • **Mode**: **Access Mode**
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 1, 2, 3

Results: Ports on Switch B have been assigned VIDs and modes, ensuring that untagged traffic on ports 6 and 7 will automatically be tagged as VLAN 3. Traffic on port 3 will be automatically tagged as VLAN 2. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

When combined with the previous settings, we complete the network segmentation. Traffic on VLANs 1-3 will remain isolated, and VLAN 1000 will allow traffic between switches while retaining VLAN tagging.



Scenario: Layer 3 Segmentation of Two Services

Short Description: A manufacturer uses layer 3 segmentation to manage traffic between three different factories, each with many devices.

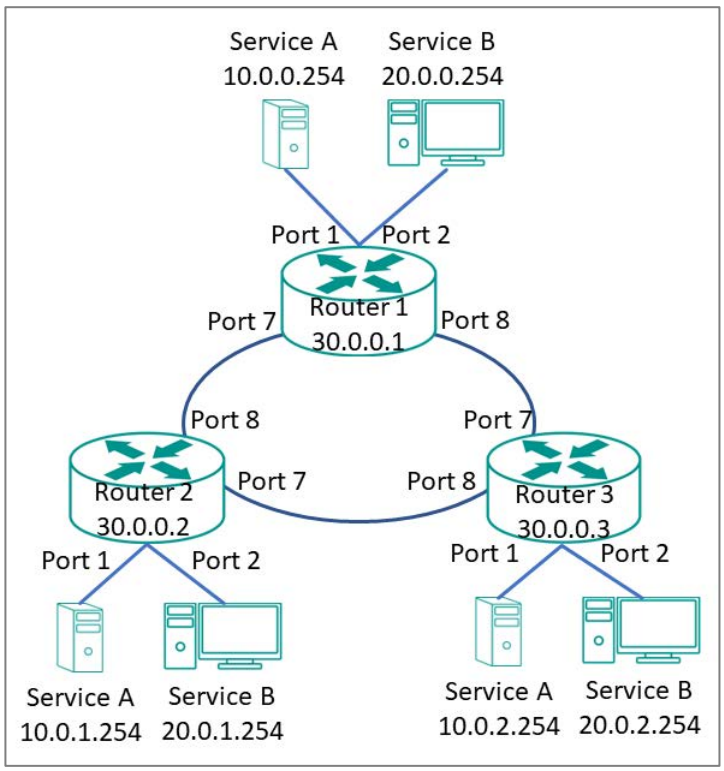
Three routers are used to connect the all of the devices together on the same network, but devices from any factory may be connected to either switch. Each factory has devices running Service A and Service B. Devices need to connect to the corresponding service in other factories, while being isolated from the different services in their own factories.

Each VLAN can be enlarged using simple switches to connect any number of devices in the factory.

For our example scenario, we will simplify to two devices (one for each service) connected to each router. These devices will serve as gateways for additional devices connected to their corresponding service. We can assign separate subnets to each port (an interface), so it's important to note which port we'll be using for each device.

We need a topology that:

- Allows devices on the same subnet to communicate with each other
- Ensure devices on different subnet cannot communicate with each other



This diagram outlines how we might create a network meeting these requirements. Each service is on its own subnet. Routers are connected in a ring topology, also on its own subnet. Because of subnet isolation, administrators can manage and prioritize traffic to ensure that packets do not leave their corresponding subnet.

To deploy this topology we need to do the following:

- Configure VLANs for each interface and bind them to ports
- Configure IP ranges for each interface and assign them to ports

In our example, we are segmenting by Service, rather than by area.

Example: Creating VLANs for Layer 3 Segmentation

Create VLANs in preparation for assigning them to ports.
Before you begin: Make sure you have an environment configured in line with our scenario. This includes:

- 3 routers in a ring topology with backbone connected on ports 7 and 8
- 2 gateways for each router (Service A and Service B), connected at ports 1 and 2, respectively
- Administrator credentials to all three routers

To create VLANs for this example, do the following:

1. Sign in to Switch A using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To add a VLAN ID, click on the **Settings** tab, and then click the ***[Add]*** button.

   Result: The **Create VLAN** screen appears.
4. Specify the VLAN to create in the **VID**, and then click **Create**. For Service A, we will create VLAN 10.
   Result: The VLAN will appear on the VLAN table at the top of the page.
5. Repeat this process to create VLAN 20 for Service B, and then create VLAN 1000 for the link between switches.

Results: We created VLANs for each Service (VIDs 10 and 20) and the VLAN for backbone between different sites (VID 1000).

What to do next: After you have created all 3 VLANs on Router 1, repeat this process on Routers 2 and 3. The configuration options will be the same. Once VLANs have been configured on all routers, you can move on to assigning VLANs to ports.

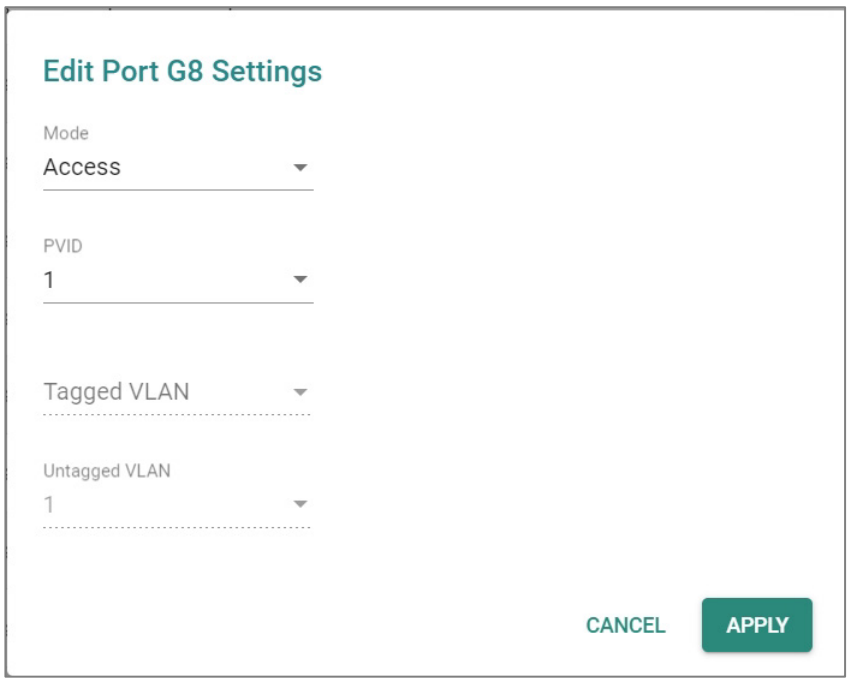
Example: Assigning VLANs to Ports for Layer 3 Segmentation

VLANs must be assigned to ports on each router to route traffic correctly.

Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to Router 1 using administrator credentials.
2. Go to **Network Configuration→Layer 2 Switching→VLAN**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and the click the corresponding ***[Edit]*** button.

   Since we're assigning Service A to port 1, start with **Port 1**. If you are repeating this step, you can substitute **Port 1** with information from the table at the end of this procedure.
   Result: The **Edit Port Settings** panel appears.



4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.
   To assign the chosen port to Service A, specify **Mode Access** and **PVID** as 10.

Tutorial Info:

Access mode is used when connecting single devices without tags. These are usually end-user devices that belong to a single VLAN, and do not need to communicate with devices in other VLANs.

Trunk mode allows a port to carry traffic for multiple VLANs over a single physical connection. This is useful for linking switches together that may have many different VLANs.

Hybrid mode is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

Note: The port VID (PVID) setting will apply a VLAN tag only for untagged traffic coming through that port. If traffic going through the port has already been tagged with a VLAN ID, the PVID setting will not change the existing tag.

Result: The **Port Table** will show the new port configuration.

5. To add the remaining ports, repeat this procedure with the following substitutions and settings:

Port	Settings
2	• **PVID**: 10 • **Mode**: **Access Mode**
5	• **PVID**: 20 • **Mode**: **Access Mode**
7	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 10, 20
8	• **PVID**: 1000 • **Mode**: **Trunk Mode** • **Tagged VLAN**: 10, 20

Results: Ports on Router 1 have been assigned VIDs and modes, ensuring that untagged traffic on Port 1 will automatically be tagged as VLAN 10. Traffic on port 2 will be automatically tagged as VLAN 20. Port 8 has been configured as a Trunk that will allow traffic to move between switches while retaining the tags.

Example: Assigning IPs to Router Interfaces

IP subnets must be assigned to interfaces to ensure traffic from corresponding VLANs is segmented correctly.

To assign IPs to router interfaces:

1. Sign in to Router 1 using administrator credentials.
2. Go to **Network Configuration→Network Interfaces→LAN**, and then press ***[Add]***.
   Result: The **Create LAN Interface Entry** screen appears.
3. To add the interface for Service A, specify all of the following, and then click **Create**:

Field	Setting
Name	Service A
VLAN ID	10
IP Address	10.0.1.254
Netmask	**8 (255.0.0.0)**

   Result: The LAN interface will appear on the Network Interface list.
4. To add the interface for Service B, specify all of the following, and then click **Create**:

Field	Setting
Name	Service B
VLAN ID	20
IP Address	20.0.1.254
Netmask	**8 (255.0.0.0)**

   Result: The LAN interface will appear on the Network Interface list.
5. To add the interface for the backbone connection, specify all of the following, and then click **Create**:

Field	Setting
Name	Backbone
VLAN ID	1000
IP Address	30.0.0.1
Netmask	**8 (255.0.0.0)**

Result: The LAN interface will appear on the Network Interface list.

Results: Interfaces have been configured on Router 1 to allow effective network segmentation. Now you need to configure the additional networks.

What to do next: Repeat this task with the following adjustments:

Router	Item	Value
Router 2	Service A	10.0.2.254
	Service B	20.0.2.254
	Backbone	30.0.0.2
Router 3	Service A	10.0.3.254
	Service B	20.0.3.254
	Backbone	30.0.0.3

Once all routers have been configured with the correct IP interfaces, you can configure a routing solution. Once that's done, your network will be ready to use.

Example: Configuring Static Routing for Layer 3 Segmentation

For complex environments, routing must be configured.

This example uses simple static routing to route traffic across the network. A production network may chose a dynamic routing option instead.

To configure dynamic routing for the Layer 3 example:

1. Sign in to Switch A using administrator credentials.
2. Go to **Routing→Unicast Route→Static Routes**, and then click the **Add (⊕)** icon.

Result: The **Create new static route** panel appears.

3. Specify all of the following:

Item	Value
Name	Serivce A Router 2
Status	**Enable**
Destination Address	**10.0.1.254** Refers to Production Service A on Router 2.
Subnet Mask	**8 (255.0.0.0)** Refers to the subnet mask of the destination address.
Next Hop	30.0.0.2 Refers to the Router 2 Interface as the next hop on the network.
Metric	1

4. Click **Create**.

Result: The new static routing entry should appear in the routing table.

5. Repeat this process for Service B. Specify all of the following:

Item	Value
Name	**Service B Router 2**
Status	**Enable**
Destination Address	**20.0.1.254** Refers to Production Service A on Router 2.
Subnet Mask	**8 (255.0.0.0)** Refers to the subnet mask of the destination address.

Item	Value
Next Hop	30.0.0.2 Refers to the Router 2 Interface as the next hop on the network.
Metric	**1**

6. Once this step is complete, repeat the process on Routers 2 and 3. The information for each router should appear as follows:

Item	Service A Router 1	Service B Router 1	Service A Router 2	Service B Router 2	Service A Router 3	Service B Router 3
Appears On	Routers 2/3	Routers 2/3	Routers 1/3	Routers 1/3	Routers 1/2	Routers 1/2
Name	Service A Router 1	Service B Router 1	Service A Router 2	Service B Router 2	Service A Router 3	Service B Router 3
Status	**Enable**	**Enable**	**Enable**	**Enable**	**Enable**	**Enable**
Destination Address	10.0.0.254	20.0.0.254	10.0.1.254	20.0.1.254	10.0.2.254	20.0.2.254
Subnet Mask	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**	**8 (255.0.0.0)**
Next Hop	30.0.0.1	30.0.0.1	30.0.0.2	30.0.0.2	30.0.0.3	30.0.0.3
Metric	1	1	1	1	1	1

Results: Once the routing configuration is completed, the Example Layer 3 Segmented Network will be ready to use. This will ensure that packets for each service will be isolated from the other, while still be efficiently guided around the network.

About Redundancy

Redundancy in industrial networks refers to averting the impact of unexpected shutdowns. If a service becomes unavailable, it can cause interruptions to productivity and services, resulting in potentially significant losses for businesses. Therefore, it is crucial to establish a redundancy protocol to quickly recover from any abnormalities and maintain productivity.

What kinds of redundancy protocols are there?

Moxa network devices support a variety of network redundancy protocols for both OSI Layer 2 and Layer 3.

- Layer 2: Moxa devices have redundancy protocol support for RSTP, MSTP, Turbo Ring v2, Turbo Chain, Ring Coupling, and Dual Homing for pathway redundancy. These mechanisms establish alternative paths that can be used to reach a destination if the primary connection fails.
- Layer 3: Moxa devices use Virtual Router Redundancy Protocol (VRRP) to ensure that the default gateway function can switch to a backup device in case the primary device fails. This ensures that routing functions remain available even if the primary device goes offline.

By implementing redundancy mechanisms at both Layer 2 and Layer 3, you can help ensure that your networks are reliable and available, even in the event of a failure or outage.

About Layer 2 Redundancy Protocols

Selecting the appropriate Layer 2 redundancy protocol for your network depends on several factors, including:

- The topology and size of your network
- The applications and services you are running
- Your availability and performance requirements

Suggestions for protocol selection will be mentioned in later chapters. Here's a brief summary of each protocol to help you make an informed decision.

Category		RSTP	Turbo Ring v2	Turbo Chain
Specification needs	Diameter	40 pcs	**V** 250 nodes per ring	**V** 250 nodes per chain
	Recovery Time		**V** Fast Ethernet: 20 ms Gigabit Ethernet: 50 ms	**V** Fast Ethernet: 20 ms Gigabit Ethernet: 50 ms
	Link Health Check (Packet Detection Mechanism)	**V** 2 sec/1 RSTP BPDU (default)	**O** Gigabit Ethernet: 10 ms/LHC pkt.	**O** Gigabit Ethernet: 10 ms/LHC pkt.
Application needs	Multi-Vendor Support	**V** Public Standard	Moxa proprietary	Moxa proprietary
	Easy-Deployment	Mesh	**V** Ring Topology	**V** Chain Topology
	Flexible Scalability		**O** Turbo Ring + Ring Coupling	**V** Directly connected to existing network without any changes.
Supported Models		Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series, TN series.	Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series, TN series.	Managed switch: EDS series, IKS series, ICS series, TN series, PT series, RKS series, MDS series. Router: EDR series.

V: Most appropriate

O: Partially applicable

About Scenarios for Turbo Chain and Turbo Ring

Large Semiconductor Network

A semiconductor factory plans to construct a new facility to increase chip production capacity for future electric vehicles. They require a large automated network (100+ switches) with redundant mechanisms to prevent unexpected downtime that could impact production lines. Additionally, their network must balance traffic across multiple links to prevent congestion and improve overall performance.

Analysis

1. This is a new project with no existing infrastructure.
2. A redundancy protocol is required and must support a network with at least 100 switches.
3. Link aggregation is needed to increase total throughput beyond what a single connection can sustain.

Solution: Turbo Ring v2

Turbo Ring v2 is suitable in situations where extremely fast failover times are required, such as in mission-critical industrial control systems. Turbo Ring v2 facilitates easy ring topology deployment. With Moxa Turbo Ring technology, networks can recover within 20 ms (Fast Ethernet/fiber) or 50ms (gigabit copper) on a network with up to 250 nodes.

Legacy Rapid Transit Network

A Phase II Metro project needs to build 15 new metro stations in an existing transit system, each requiring networking infrastructure. This project not only establishes its own system with a redundant topology but also ensures compatibility with the Phase I system. The Phase I system comprises a mesh topology with RSTP protocol, consisting of over 30 switches, with cabling that is outdated and no longer replaceable. Nevertheless, Phase II must be interconnected with Phase I without any modifications to the latter.

Analysis

1. This is a rebuilt project and it should be interconnected with RSTP topology.
2. Redundancy protocol is required and support 100+ switches network.

Solution: Turbo Chain

Turbo Chain is most suitable for this situation. One of the key advantages of Turbo Chain is its simplicity and ease of deployment. It can be directly interconnected to RSTP topology with any change on RSTP network.

Note:

The following two alternative solutions would also work in this scenario:

1. Turbo Ring v2 with Ring coupling to RSTP is also a alternate solution. This would depend on network physical deployment.
2. RSTP could be used to expand an existing RSTP network.

Inter-Consist Rail Network

A well-known railway vehicle manufacturer needs to plan a new on-board network, planning a ring network via Turbo Ring for multiple vehicles to form a consist. The consists also need to be interconnected with each other when connected as a train, and a redundant backup mechanism should be provided between consists.

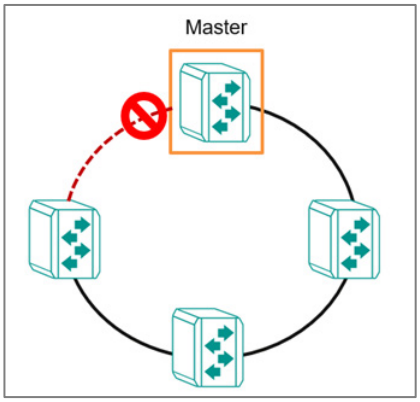
Solution: Ring Coupling

Connection between Turbo Ring networks can be connected with ring coupling. This will allow consists with their own rings to be dynamically uncoupled and recoupled without reconfiguration.

About Turbo Ring v2

Turbo Ring v2 is a high-performance, redundant network topology developed by Moxa for configuring network devices in redundant loops.

In the event of a link failure, the network can automatically reconfigure itself to maintain uninterrupted communication. Recovery times are within 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet on a network of up to 250 nodes.



Turbo Ring v2 allows connected network devices to elect a "master" switch, which blocks packets from traveling through any of the network's redundant loops and manages the network. If a section breaks, the protocol adjusts the ring so that the disconnected parts of the network establish contact. This enables continuous network operations, even when there is a fault in the network.

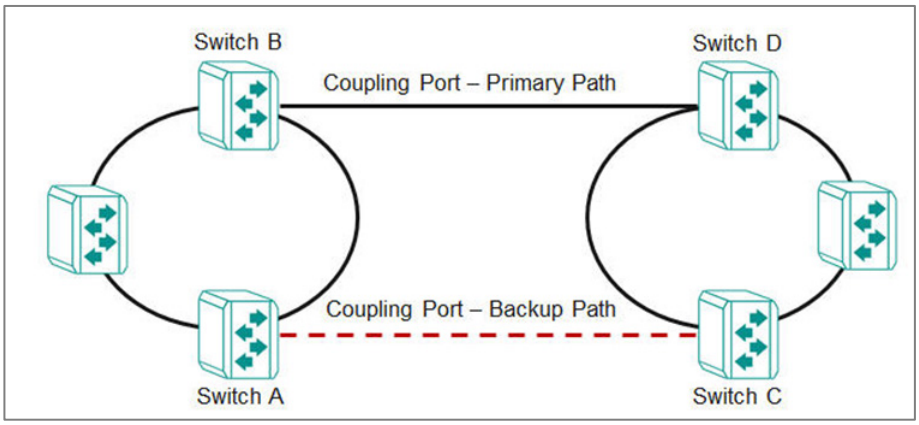
Furthermore, the election mechanism is redundant. If the "master" device itself fails, the network devices detect the failure and automatically elect another. The process occurs quickly, ensuring no interruption.

Turbo Ring v2 supports a backup segment connected to the redundant port (secondary port) on the ring "master". In this case, the backup path is easily identifiable for troubleshooting and replacement.

About Ring Coupling

Ring Coupling refers to the practice of coupling two rings together.

This may be useful when creating a large redundant ring is inconvenient or impractical, such as for devices in remote areas. Smaller redundant rings can be coupled together for inter-ring communication while still maintaining redundancy of constituent rings and couplings.



Ring coupling uses extra ports on each pair of coupled switches. In this example, that means:

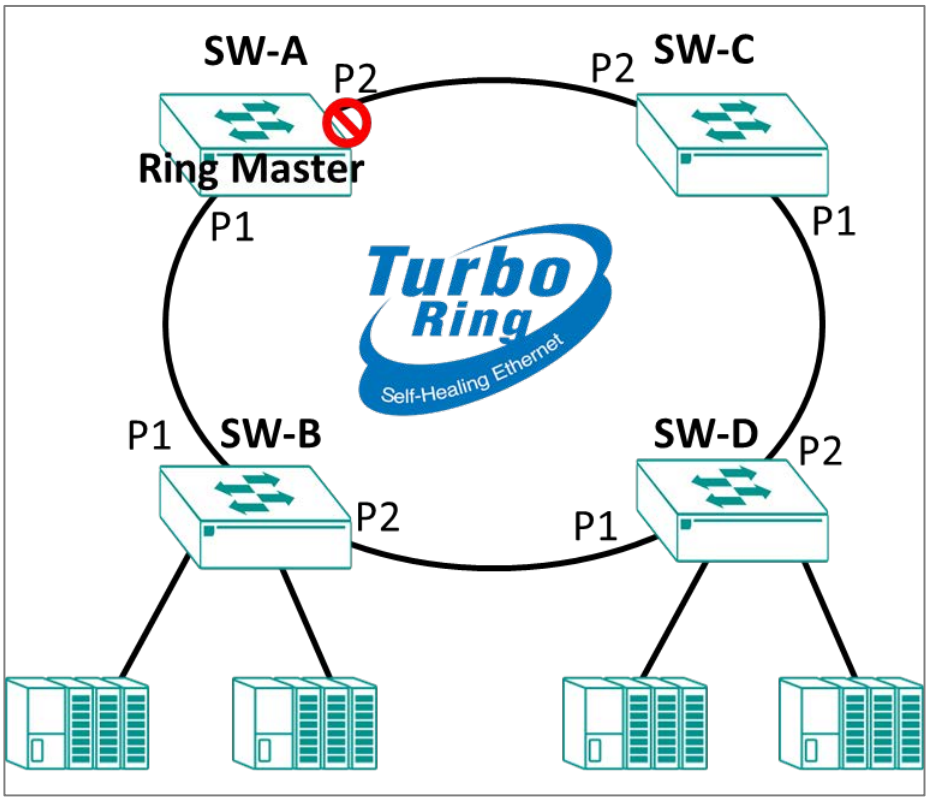
- The (Primary) coupling port on Switch B monitors the main path and connects directly to the port on Switch D.
- The (Backup) coupling port on Switch A monitors the main path and connects directly to the port on Switch C.

> **Note**
> Only one coupling (primary + backup) per ring pair.

Scenario: Using Turbo Ring in a Manufacturing Plant

In this scenario, we describe a factory using a simple ring topology.

A manufacturing plant has a complex network of machines and devices that communicate with each other to keep the production line running smoothly. To ensure that the network remains stable and reliable, the plant needs to use Turbo Ring v2 to create a fault-tolerant network by forming a ring topology.



Set up Turbo Ring v2 to connect multiple networks of machines and devices to create a fault-tolerant network and achieve continuous operations.

Ensure that switches are installed and powered. Wait to connect them until the end. To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.
   See the subsequent sections for details about how to configure each device.
2. Connect the network devices in a ring topology, using ports 1 and 2 for ring segments.

If the master network device fails, the other devices in the ring will automatically detect the problem and initiate a new election process to select a new master switch, ensuring that there is no significant interruption in communication.

Example: Configuring the Master for Turbo Ring v2 in a Manufacturing Plant

Configure the device labeled SW-A for Turbo Ring v2 in our factory example.

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click ***[Add]***.

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Enabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Repeat this step on devices SW-B, SW-C, and SW-D, but with the **Master** setting set to **Disabled**. This process is outlined in the subsequent section.

Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click ***[Edit]***.

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Disabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

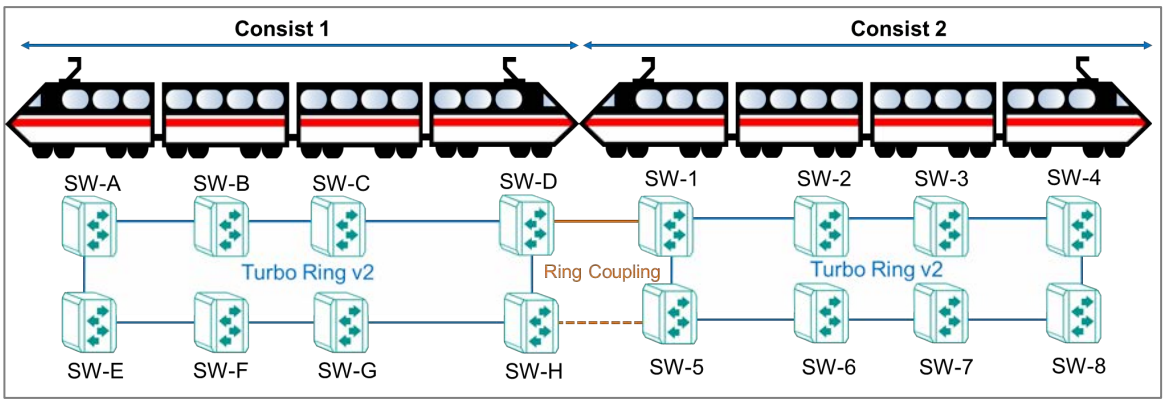
Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

Scenario: Using Turbo Ring in an On-board Train Application

In this scenario, we describe setting up Turbo Ring v2 with ring coupling between train consists.

A railway vehicle manufacturer needs to plan a new on-board network with redundancy and flexible inter-consist communication. The customer plans a ring network with Turbo Ring v2 between multiple vehicles to form one ring per consist. Multiple consists will then use ring coupling for inter-consist communication.



This structure allows for easy administration as consists are coupled and uncoupled.

To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.
   See the subsequent sections for details about how to configure each device.
2. Connect the network devices SW-A through SW-H in a ring topology, using ports 1 and 2 for segments of the ring. Do the same for SW-1 through SW-8. Do not connect the ring coupling yet.
3. Configure the Primary Coupling Path path on SW-D.
   See the subsequent sections for details about how to configure ring coupling.
4. Configure the Backup Ring Coupling on SW-H.
   See the subsequent sections for details about how to configure ring coupling.

Once all devices have been configured, you can connect the ring ports and coupling ports.

Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports and as ring ports.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click ***[Edit]***.

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Disabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1** and **2** as ring ports.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click ***[Edit]***.

   The Ring 1 Settings screen appears.
5. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Disabled**
Ring Port 1	**1**
Ring Port 2	**2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.

Example: Configuring the Primary Ring Coupling Between Consists

Both network devices that make up the ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.
- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-D as the primary ring coupler:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Under Ring Coupling Settings, click ***[Edit]***.

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Status	**Enabled**
Coupling Mode	**Primary Path**
Coupling Port	**5**

5. Click **Apply** to save your changes.

The device has been configured as a primary ring coupling.

Connect the ring coupling ports. Once both devices are connected, you can move on to configuring the backup coupling.

Example: Configuring the Backup Ring Coupling Between Consists

Both network devices that make up the backup ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.

- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-H as the backup coupler:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **General**.
3. Under Ring Coupling Settings, click ***[Edit]***.

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Status	**Enabled**
Coupling Mode	**Backup Path**
Coupling Port	**5**

5. Click **Apply** to save your changes.

The device has been configured as a backup ring coupling.

Once the device has been configured, connect the ring coupling ports. Your coupling configuration will be complete.

About RSTP

Rapid Spanning Tree Protocol (RSTP) is an IEEE 802.1w network protocol that enhances the speed and stability of the Spanning Tree Protocol (STP).

RSTP promotes high availability and a "loop-free" topology, similar to STP, but more quickly within Ethernet networks. It provides faster convergence and is backward compatible with STP. While STP takes 30-50 seconds to converge, RSTP can achieve sub-second convergence.

For applications that require redundancy, but require use of only open-standard protocols and no proprietary protocols, RSTP is a good choice.

How RSTP Works

Based on the original concept of the STP mode, the RSTP tree also grows from root to leaf to build a loop-free topology. This means that RSTP ensures that there is only a single active path between any two devices on an active connection. The remaining disabled connections serve as backup paths in case an active connection fails.

If you are new to STP, please refer to the IEEE 802.1D standard. As an enhancement of STP, RSTP speeds up network convergence. Rapid Spanning Tree Protocol (RSTP) includes additional information in the Bridge Protocol Data Units (BPDUs) that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connect through point-to-point links allow a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally, rather than network-wide. This allows RSTP to carry out automatic configuration and restore a links faster than STP. Additionally, as RSTP is a widely used protocol, Moxa equipment supports connections with switches from various vendors which support RSTP to form a redundant network architecture.

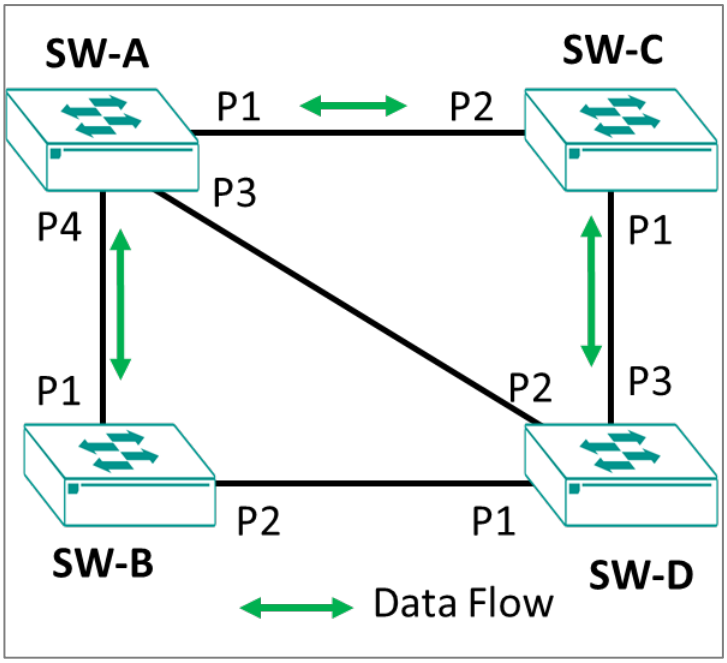
When RSTP is enabled on a network, the spanning tree algorithm automatically determines the configuration of the spanning tree. RSTP's algorithm follows these general procedures:

1. **Determining the root bridge:** The switch with the lowest bridge priority is considered the root bridge through priority competition. In case of a tie, a tiebreaker based on the MAC address is used to determine the root bridge. Specifically, the switch with the lowest MAC address is considered the root bridge. All other switches are automatically designated as non-root switches.
2. **Selecting the root port for non-root switches:** The root port is selected as the best path to the root bridge based on the root cost, which is typically determined by the bandwidth of the link. Each non-root switch has only one root port.
3. **Assigning designated ports:**Each connection (segment) must have a port assigned as the designated port for forwarding traffic. The designated port is the one that sends the best BPDU on its segment.

4. **Remaining ports in blocking state:**All remaining ports, including alternate ports or backup ports, are in a blocking state. These ports do not transmit data to other switches or learn MAC addresses.

Scenario: RSTP on 4 Network Devices

In this scenario, we configure 4 network devices with RSTP.



SW-A will serve as the RSTP root. SW-B, C, and D will be connected to all other devices, but use the green arrow paths as their primary data path.

Ports are configured as follows:

	Device SW-A	Device SW-B	Device SW-C	Device SW-D
Connects to SW-A	N/A	P1	P2	P2
Connects to SW-B	P4	N/A	N/A	P1
Connects to SW-C	P1	N/A	N/A	P3
Connects to SW-D	P3	P2	P1	N/A

Example: Configuring SW-A for RSTP

Here's how to configure SW-A as the root device for RSTP in our example.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Set **Bridge Priority** to **28672** to ensure that SW-A will always be set as the root.
5. Click **Apply** to save changes.
6. Locate **Port 1** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.
7. Set **Status** to **Enabled**.
8. Click **Apply** to save changes.

   The port settings will be reflected in the table.
9. Locate **Port 3** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.
10. Click **Apply** to save changes.

    The port settings will be reflected in the table.
11. Locate **Port 4** on the list, and then click ***[Edit]***.

    The Edit Port Settings screen appears.
12. Click **Apply** to save changes.

    The port settings will be reflected in the table.

SW-A is now configured for RSTP.

Continue to configure SW-B.

Example: Configuring SW-B and SW-C for RSTP

Here's how to configure SW-B and SW-C for RSTP in our example.

1. Sign in to the device with administrator credentials.

2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Click **Apply** to save changes.
5. Locate **Port 1** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.
6. Set **Status** to **Enabled**.
7. Click **Apply** to save changes.

   The port settings will be reflected in the table.
8. Locate **Port 2** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.
9. Click **Apply** to save changes.

   The port settings will be reflected in the table.

SW-B is now configured for RSTP.

Repeat this procedure on SW-C, and then proceed to configure SW-D.

Example: Configuring SW-D for RSTP

Here's how to configure SW-D for RSTP in our example.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Set **Status** to **Enabled**.
4. Click **Apply** to save changes.
5. Locate **Port 1** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.
6. Set **Status** to **Enabled**.
7. Click **Apply** to save changes.

   The port settings will be reflected in the table.

8. Locate **Port 2** on the list, and then click ***[Edit]***.

   The Edit Port Settings screen appears.

9. Set **Status** to **Enabled**.

10. Click **Apply** to save changes.

    The port settings will be reflected in the table.

11. Locate **Port 3** on the list, and then click ***[Edit]***.

    The Edit Port Settings screen appears.

12. Set Path Cost to `150000`

    This will ensure that this path will be preferred over the other two ports.

13. Click **Apply** to save changes.

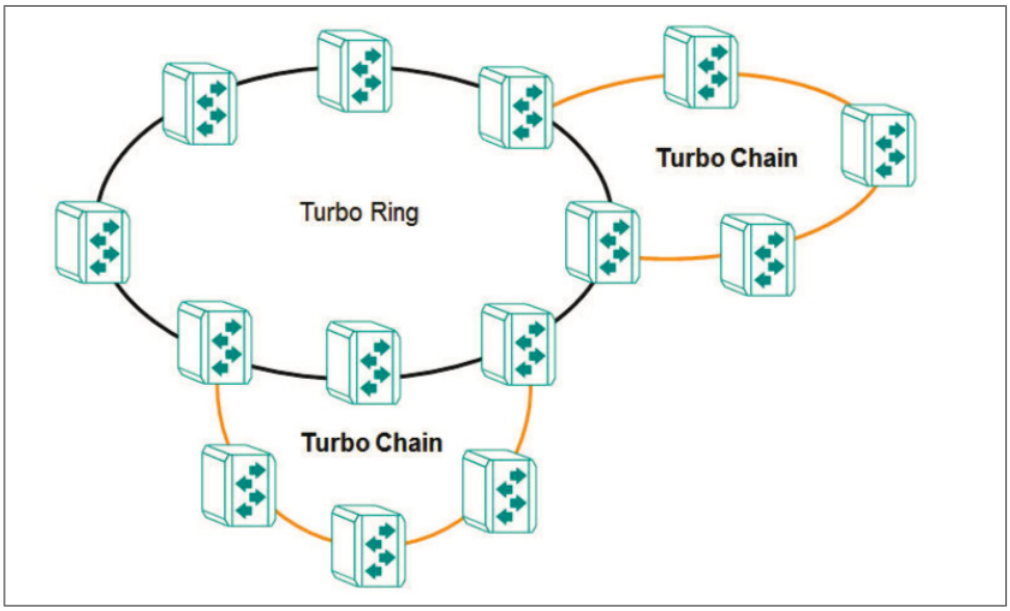
    The port settings will be reflected in the table.

SW-D is now configured for RSTP. Now that all network devices are configured, in the event that one link is severed, data will automatically flow over backup paths.

About Turbo Chain

Turbo Chain allows flexible expansion on top of an existing topology

This allows for flexible, cost-effective expansions. This allows you to grow existing networks without replacement the main ring while still maintaining reliability and redundancy.

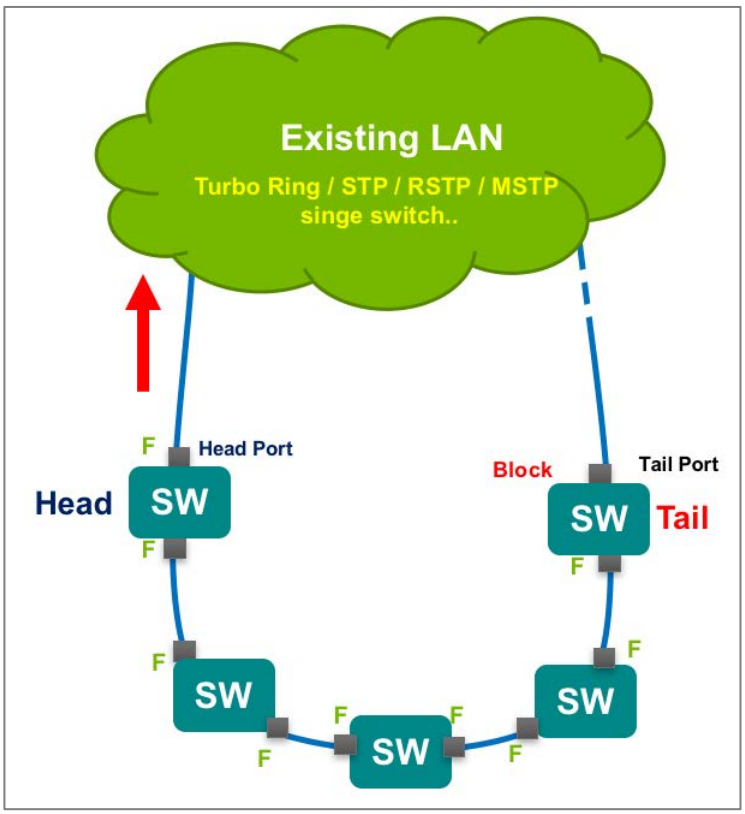


Turbo Chain is a proprietary redundancy technology developed by Moxa, designed for use in widely distributed networks. It enables Ethernet switches to be connected in a daisy-chain configuration, where each switch serves as a backup path for connected devices. Turbo Chain supports system recovery times of under 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet in member port link environments.

Turbo Chain is suitable for industrial networks with complex topologies, particularly those utilizing multi-ring architectures. It allows the creation of flexible and scalable topologies with rapid media recovery.

In a typical Turbo Chain setup, each Ethernet switch is connected to two others in a daisy-chain configuration. The switches are categorized into three types: Head, Tail, and Member switches. The Head switch connects the chain to the external network, while the Tail switch provides redundancy. If the Head port is disconnected, the Tail port immediately assumes the role of data transfer, ensuring continuous communication.

This technology ensures that in the event of a link or switch failure, Turbo Chain quickly reroutes traffic to an available backup path, minimizing network downtime and maintaining uninterrupted communication.



Turbo Chain is often used in industrial automation, transportation, and surveillance applications where network reliability is critical. It is compatible with other Moxa networking technologies, such as Turbo Ring, and other Redundancy protocols like STP/RSTP, MSTP etc, to provide further redundancy and resilience for industrial networks.

To sum up, here are some of the features of Turbo Chain technology:

1. **Topology**: Turbo Chain uses a daisy-chain topology to connect Ethernet switches in a loop-free configuration.
2. **Redundancy**: Turbo Chain provides a backup path on the tail switch to ensure network availability and reduce downtime in the event of a switch or link failure.
3. **Fast failover**: Turbo Chain has a fast failover mechanism that can detect and activate backup paths in a matter of milliseconds (< 20 ms) to ensure uninterrupted communication between devices.
4. **Compatibility**: Turbo Chain is compatible with other redundancy technologies, such as Turbo Ring and RSTP, to provide even greater redundancy and resilience for industrial networks.

Example: Configuring Turbo Chain

In this example, we will configure network devices for Turbo Chain.

- Determine which devices will be the head, tail, and members of the chain. The head and tail must connect to the main LAN.
- Do not connect any of the chain devices until configuration of all devices is complete.
- Do not use any of the chain ports until configuration is completed. Do not use these ports for administration, as applying the chain configuration to these ports will disconnect you from the web GUI.

You can configure the head, tail, and member devices in any order as long as you do not connect them until after all devices are configured. Choose a device to configure and do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Chain**, and then click **Settings**.
3. Set **Turbo Chain** to **Enabled**.
4. For **Chain Role**, specify one of the following:
    - **Head** - specify only one head of the chain. This will be the primary connection to the rest of the network.
    - **Tail** - specify only one tail of the chain. This device will be the backup connection to the rest of the network.
    - **Member** - specify one or more member devices. Member devices make up the "links" between the head and the tail of the chain. Make sure that there are no loops in the chain.
5. Specify the following Ports based on the **Chain Role**:

Head Chain Role Option	Port Value
Head Port	**1**
Member Port	**2**

Member Chain Role Option	
Member Port 1	**1**
Member Port 2	**2**

Tail Chain Role Option	
Tail Port	**1**
Member Port	**2**

6. Click **Apply** to save changes.
7. Repeat this procedure to configure all devices in the chain. Once all devices have been configured, connect the devices in the chain.

Once all devices are configured and connected, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

About VRRP

The Virtual Router Redundancy Protocol (VRRP) is a layer 3 redundancy protocol enabling multiple routers to collaborate as a group and share a virtual IP address.

The main purpose of VRRP is to provide redundancy for the default gateway utilized by hosts on a LAN or VLAN.

In a VRRP setup, a single router is designated as the "master" while the other routers are "backup" routers. The master router is responsible for forwarding packets sent to the virtual IP address. Additionally, backup routers supervise the master router and take over its tasks in case of failure. This enables automatic failover and redundancy, guaranteeing network connectivity—even in the event of a router failure.

Benefits of VRRP

1. **Increased Network Reliability**: VRRP enables multiple routers to work together in a group, sharing a virtual IP address. This provides redundancy for the default

gateway, ensuring that network connectivity is maintained even if one of the routers fails. This increases the overall reliability of the network and helps prevent downtime.

2. **Automatic Failover**: VRRP facilitates automatic failover, where backup routers take over the tasks of the master router in case of a failure. This ensures that there is no disruption to network services and users can continue to access resources without any interruption.
3. **Easy Network Management**: VRRP simplifies network management by allowing multiple routers to work together as a group, sharing a virtual IP address. This eliminates the need for complex routing protocols and reduces the risk of misconfiguration.

About VRRP States

With VRRP, routers are assigned different roles and states to ensure seamless failover and improved network availability.

The three primary states of VRRP are:

1. **Init State**: This is the initial state when a VRRP router starts up. The router initializes its VRRP configuration and has not yet determined whether it should become a Master or a Backup router. The router remains in the Init state until it starts receiving VRRP advertisements from other routers in the same VRRP group or until it begins sending advertisements itself.
2. **Master State**: In this state, the router is responsible for forwarding packets sent to the virtual IP address and acts as the default gateway for the devices in the network. The router with the highest priority (or lowest IP address in case of a tie) becomes the Master router. The Master router periodically sends VRRP advertisements to the other routers in the VRRP group to maintain its role. If the Master router fails, one of the Backup routers will take over the role based on priority.
3. **Backup State**: Routers in the Backup state are waiting to take over the Master role if the current Master router fails. Backup routers listen for VRRP advertisements from the Master router and update their timers accordingly. If a Backup router stops receiving VRRP advertisements from the Master router for a certain period (typically three times the advertisement interval), it assumes that

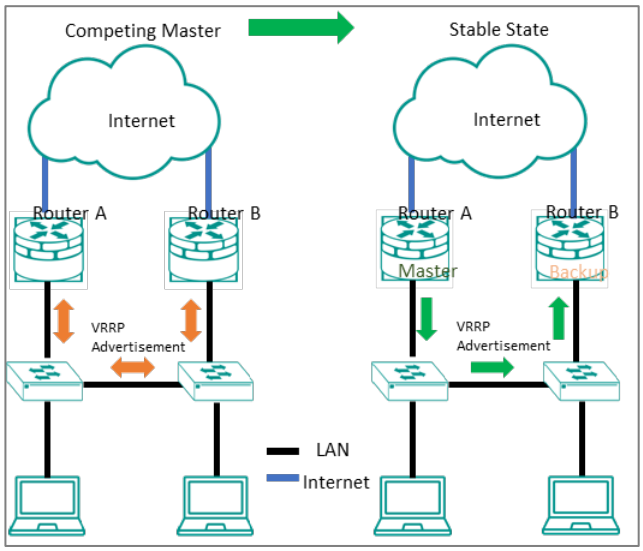
the Master router has failed and attempts to transition to the Master state based on its priority.

The VRRP states ensure that the network has a functioning default gateway at all times, providing redundancy and improving network availability in case of router failure. By implementing VRRP, network administrators can achieve increased network reliability, automatic failover, and easier network management.

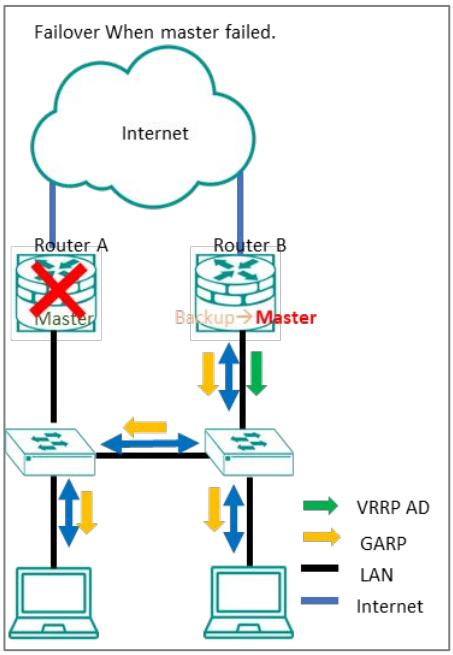
VRRP in Depth

VRRP group routers select a master router based on priority, with the highest priority being the master.

To accomplish this, Each router in the group announces its priority, and the master router regularly sends out VRRP advertisements to the other routers to update its status.



The virtual IP address is linked with the VRRP group, and the master router forwards network packets using the virtual IP address as the source address. The backup routers stay inactive, listening to the VRRP messages from the master and ready to take over if the master fails. The Master Router sends advertisement packets to the backup routers to inform them that it is still operational. The advertisement interval is manually configured, with a default value of 1 second. If the master router fails, the Backup Router is unable to receive advertisement packets from the Master. Once the advertisement down timer expires, backup router will realize that the Master is experiencing issues or has powered down and one of the backup routers with a higher priority takes over as the new master, ensuring there is no disruption in network connectivity.



VRRP can also be set up to use preemption, which allows a higher-priority router to take over as the master even if the current master router is still functional. This can be useful when the higher-priority router is available again after a period of downtime.

In summary, VRRP is a valuable protocol that provides redundancy in network environments where high availability is critical. It enables multiple routers to act as a single virtual router, ensuring network traffic continues to flow in the event of a router failure.

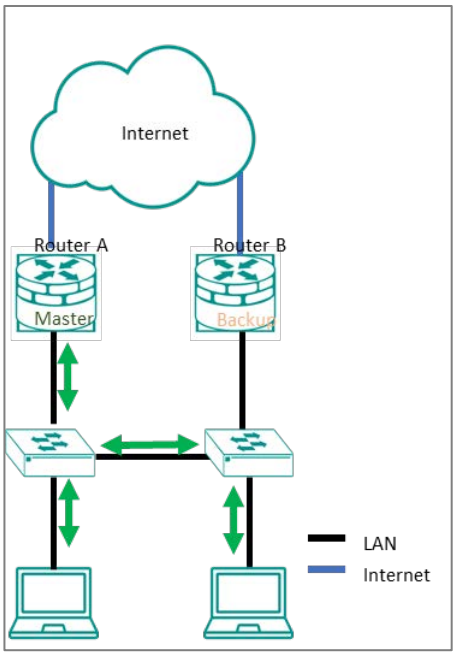
Scenario: VRRP on Two Routers

In this scenario, we'll configure two routers connected to the same LAN (Local Area Network).We will configure VRRP to ensure that if one of the routers fails, the other router will continue to forward traffic to the LAN.

For example, suppose Router A (LAN interface IP: 192.168.127.1) is initially configured as the master and Router B (LAN interface IP: 192.168.127.2) as the backup in the VRRP group. Router A is responsible for forwarding packets to the LAN. The master should keep tracking the interface by ping the device (IP 192.168.127.100) in order to make sure of the LAN communication.

If Router A were to fail by ping lost or any link down event, Router B would detect this and assume the role of the master. It would then begin forwarding packets to the LAN,

ensuring that there is no disruption in network connectivity. Once Router A becomes available, it can take over as the master, and Router B reverts to its backup role.



Example: Configuring VRRP on Router A

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Router A: 192.168.127.1
- Router B: 192.168.127.2

To configure Router A, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
3. On the lower table of the screen, click ***[Add]***.

   The Create Virtual Router screen appears.
4. Configure the following, and then click **Create**.

Option	Value
Interface	LAN1

Option	Value
Virtual IP	192.168.127.3
Priority	200
Preemption	**Enabled**
Target IP	192.168.127.100

The **Virtual Router** settings appear in the list.

5. Under the Virtual Router list, click **Apply**.
6. At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Router A is now configured for VRRP.

Continue to configure Router B.

Example: Configuring VRRP on Router B

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Router A: 192.168.127.1
- Router B: 192.168.127.2

To configure Router B, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
3. On the lower table of the screen, click ***[Add]***.

The Create Virtual Router screen appears.

4. Configure the following, and then click **Create**.

Option	Value
Interface	LAN1
Virtual IP	192.168.127.3

Option	Value
Priority	100
Preemption	**Enabled**
Target IP	192.168.127.100

The **Virtual Router** settings appear in the list.

5. Under the Virtual Router list, click **Apply**.
6. At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Both routers are now configured for VRRP. In the event of a failure of one router, the other can take over using the same virtual IP address, ensuring continued function without reconfiguration.

Routing

About Routing

IP routing is the process of forwarding Internet Protocol (IP) traffic between different networks using one or more intermediate devices.

When one device wants to send a packet to another on a different network, it forwards the packet to its default gateway—usually a router. The router examines the destination IP address and determines the next "hop" along the path to the destination. This process continues with subsequent routers until the packet reaches its destination. Each router along the path checks its own routing table to determine the best path for the packet. Routing tables contain information about network topology and a list of networks and associated routes. Each route correlates information by destination IP or IP range, and includes information such as the next-hop router and the cost of sending packets along that route.

Static routing and **dynamic routing** are two methods of populating the routing table with information about how to reach different networks.

Static routing is manually-configured. Network administrators configure the routing table on each router. This method is simple to configure and allows packets to take predictable paths as long as network topology does not change.

Dynamic routing protocols automatically update the routing table on each router. This method is more flexible and scalable, making it suitable for larger and more complex networks.

In addition to how routes are configured, packets can be routed between a single sender and single recipient (**unicast**), or from one sender to multiple devices at a time (**multicast**).

Unicast delivery is used to send packets from one sender to one recipient, as is typically the case with most network traffic. When a device sends a packet with an unicast destination address, the router looks up the destination address in its routing table and forwards the packet to the next hop on the path to the destination.

Multicast delivery, on the other hand, is used to send packets from one sender to many recipients. With multicast, a single packet is sent out to a group of devices on the

network that have expressed interest in receiving packets for that group. This is useful for applications such as video streaming, where the same content needs to be sent to multiple devices simultaneously. Dynamic multicast routing protocols, such as Protocol Independent Multicast (**PIM**), are used to ensure that multicast packets are delivered only to devices that have expressed interest in receiving them.

Routing and Packet Delivery

	Unicast	Multicast
Static	Manual Configuration	Manual Configuration
Dynamic	• **RIP** • **OSPF**	**PIM**

Note

The TN-4908 series currently only supports static multicast routes in multicast stream routing.

About Static Routing

A static route is a manually configured network path used to deliver network traffic to a specific destination network or host. Unlike dynamic routes established by routing protocols, static routes are created and managed by a network administrator. They are typically used in small networks or situations where there is a limited number of destinations that need to be reached.

Among these static routes, a special type known as the default route, or 'gateway of last resort', plays a critical role. This default route, often designated as 0.0.0.0/0, represents a catch-all path. When a device doesn't have a specific route for a packet's destination IP address, it will utilize the default route, sending the data along this path. This ensures that all data, regardless of its destination, has a route to follow.

While both default and static routes are manually configured, they serve different purposes. Static routes are used for specific, predefined network paths, while the default route is a catch-all, used when no other path is available for a specific data packet. This allows for increased control over network traffic while ensuring that data can reach otherwise unspecified networks, typically including the public Internet.

Static routes, including default routes, offer several advantages, including:

- More control over network traffic, allowing administrators to direct traffic along specific paths.
- Less overhead and resource usage, as static routes don't require routers to exchange routing information.
- Faster convergence, since there are no routing updates to process.

However, static routes also have some disadvantages:

- May be time-consuming and prone to human error, as administrators must manually configure and update routes.
- Unable to adapt to network changes automatically, requiring manual intervention to update routing tables when network topology changes.
- May not scale well in large networks with numerous destinations and frequent changes.

In summary, static routing is a method for unicast communication in which network paths are manually configured by network administrators. While they offer more control over network traffic and can improve performance in some cases, static routes can be time-consuming to manage and may not be well-suited for large, dynamic networks.

About Multicast Routing

Multicast routing is an efficient method for transmitting network traffic to a group of devices simultaneously. This approach helps conserve network resources, improve performance, and reduce congestion by sending only one copy of a message to all interested devices in the group.

A **Static Multicast Route** is a manually configured network path used to deliver multicast traffic to a specific group of devices on a network. It is a type of multicast route that is manually created and configured by a network administrator, rather than dynamically established by a multicast routing protocol. Static multicast routes are typically used in small networks where the multicast group membership is known and does not change frequently. They can also be used in situations where the multicast traffic needs to be routed through a specific path in the network, or when multicast traffic needs to be constrained to a specific set of network interfaces.

Note

While enabling the static multicast routing, it is crucial to regularly review and adjust your configurations in response to any alterations in the network topology or multicast group memberships.

About Selecting a Routing Protocol

Short Description: There are several factors to consider when selecting a routing protocol.

1. **Network Size**: In a small network with only a few L3 devices with two or three interfaces, static routing is often the simplest and most efficient option. Dynamic routing, on the other hand, is more suitable for multiple Layer 3 interfaces with many devices and complex interconnections.
2. **Topology Stability**: If the network topology is relatively stable and changes infrequently, static routing can be a reliable and predictable choice. In contrast, dynamic routing protocols like **RIP** and **OSPF** are designed to adapt to changes in the network, making them better suited for networks that are constantly changing.
3. **Operational Cost**: Static routing requires manual configuration of each router, which can be time-consuming and error-prone in large networks. Dynamic routing protocols can automate this process, making it easier to manage and scale the network.
4. **Number of Receivers**: Unicast is a one-to-one communication method, while multicast is a one-to-many communication method. Unicast is typically used for sending data to a specific recipient, while multicast is used for delivering data to multiple recipients who have expressed interest in receiving data for a specific multicast group.

Note

Dynamic routing can be vulnerable to attacks that manipulate routing information.

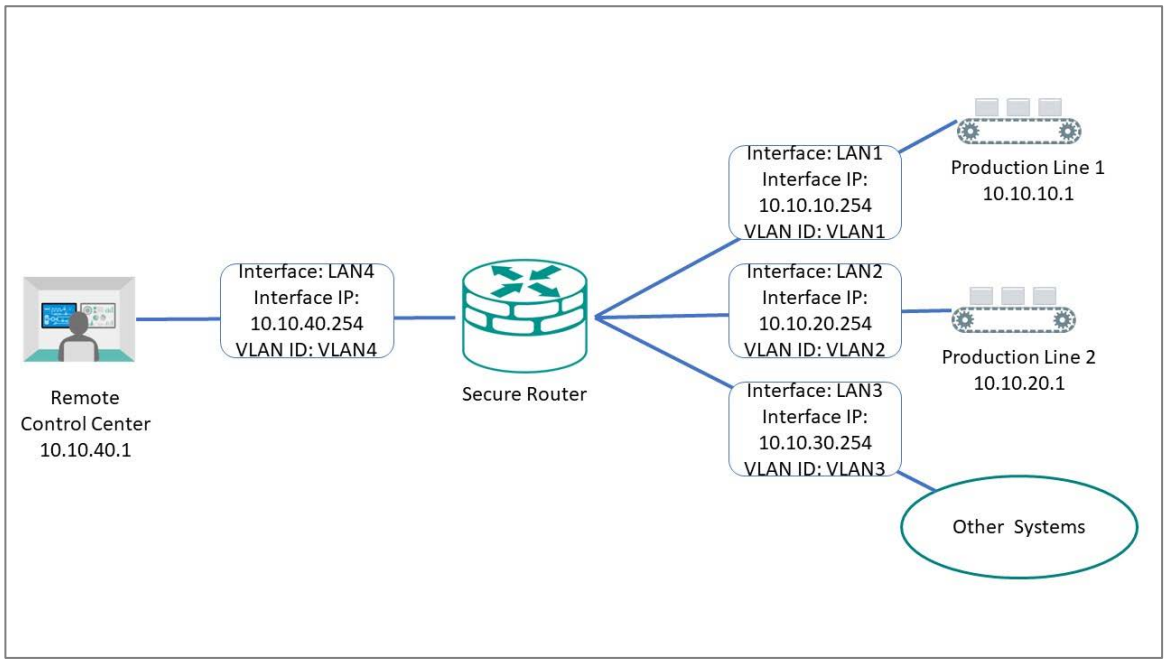
A combination of both static and dynamic routing may also be appropriate in some cases, such as when you have a core network that uses static routes and branch networks that use dynamic routing protocols.

Example: Adding a Static Unicast Route for Factory Automation

A factory operator wants to create static routes between two production lines to coordinate handoffs in a multistage manufacturing process. Static routes allow packets to traverse different subnets, and will ensure efficient routing of packets between the two production lines, as well as to the central control center. This also improves performance by reducing network congestion, ensuring that packets will not be retransmitted to other devices or other subnets.

Before you begin: Make sure you have correctly configured:

- Each device with an IP address.
- VLANs for each subnet. Refer to VLAN for more information.
- VLAN assignment to an Interface. Refer to Network Interfaces for more information.



To create a static route to Production Line 1, do the following:

1. Go to **Routing→Unicast Route→Static Routes**, and then click ***[Add]***.

   Result: The **Create new static route** panel appears.

2. Specify all of the following:

Item	Value
Name	Specify a name for the route. Names must not exceed 10 characters. Names are for user reference only and do not affect functionality.
Status	**Enable**
Destination Address	`10.10.10.1` Refers to Production Line 1.
Subnet Mask	**24(255.255.255.0)** Refers to the subnet mask of the destination address.
Next Hop	`10.10.10.254` Refers to the Secure Router LAN1 Interface as the next hop on the network.
Metric	1 Indicates the preference or priority of a particular route, with lower values having higher priority. When multiple static routes are available (or both static and dynamic routing protocols are available), the router uses the **Metric** value to determine the best route to use. For static routes, a value of 1 is recommended.

Note

The Destination Address and Subnet Mask identify which traffic forwards to the next hop. For multi-hop entries, the Subnet Mask will correspond to the Destination Address and not the Next Hop.

3. Click **Create**.

Result: The new static routing entry should appear in the routing table.

Results:

Packets meeting the destination criteria will be routed to the appropriate interface and applicable subnet, and will not be propagated further.

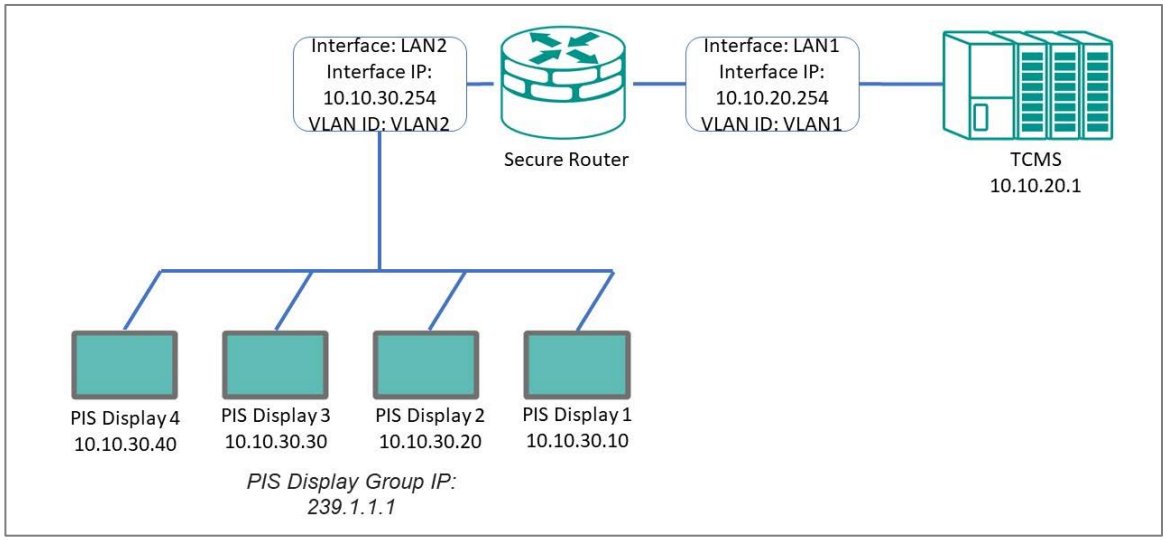
What to do next: Repeat this procedure to add Production Line 2 (`10.10.20.1`), the Remote Control Center (`10.10.40.1`), and Other Systems (`10.10.30.1`) to the Static Routing Table.

Example: Adding Static Multicast Route for Passenger Speed Display

A train operator wants to display current train speed on the PIS (Passenger Information System), requiring the TCMS (Train Control Management System) to share speed information with the PIS. There are multiple displays in multiple cars throughout the train. Multicast static routing allows the TCMS to send a single packet to multiple displays across the train, minimizing traffic congestion and processing overhead. The reduction in the total number of packets on the network can make it easier to manage quality of service and allocate network resources effectively.

Before you begin: Make sure you have correctly configured:

- Each device with an IP address.
- Each display device to join the multicast group (`239.1.1.1` in this example). Consult your PIS system documentation for details.
- VLANs for each subnet. Refer to VLAN for more information.
- VLAN assignment to an Interface. Refer to Network Interfaces for more information.
- IGMP Snooping as Enabled on the VLAN for the PIS displays. Refer to VLAN Settings - Edit VLAN Settings for more information.



To create a static multicast route for the PIS Display Group, do the following:

1. Go to **Routing→Multicast Route→Multicast Route Settings**, make sure **Mode** is set to **Static Multicast Route**, and then click **Apply**.
2. Go to **Routing→Multicast Route→Static Multicast Route**, and then click ***[Add]***.

   Result: The **Create Static Multicast Route** panel appears.
3. Specify all of the following:

Item	Value
Status	**Enable**
Group Address	`239.1.1.1` Refers to the group IP used by the PIS displays. Packets sent to this address will be sent to all devices configured to listen on this IP which also share the other parameters specified in this section.
Source Address Type	Choose **Specify Source**, and then specify `10.10.20.1` This refers to the Control Unit, ensuring that other potential devices on this interface and VLAN do not generate unnecessary packets and traffic.
Inbound Interface	**LAN1** Refers to the interface connecting the TCMS to the Secure Router. Since the TCMS provides the speed data for the displays.

Item	Value
Outbound Interface	**LAN2** Refers to the interface connecting the PIS screens to the Secure Router.

4. Click **Create**.

Result: The new static routing entry appears in the routing table.

Results:

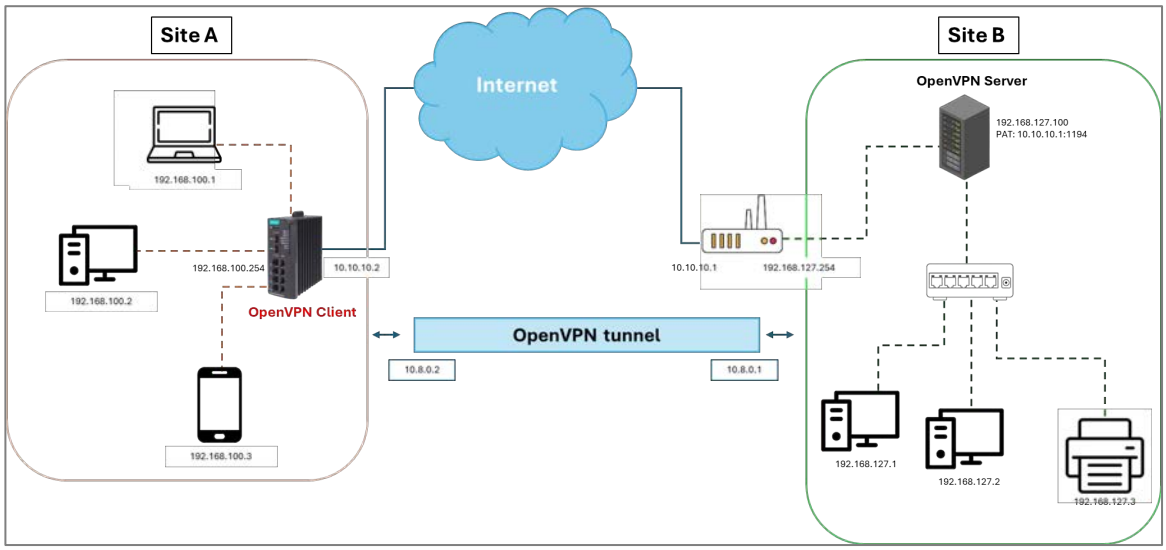
Multicast packets from the TCMS meeting the specified criteria will be sent to PIS screens, allowing them to display speed data without generating duplicate or extra packets that might reduce network performance.

About OpenVPN Client

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections. It can establish a safe and encrypted tunnel between devices and a VPN server, ensuring the internet traffic remains private and secure. OpenVPN can also traverse network address translators (NAT) and firewalls, making it a versatile and powerful solution for secure communication over the Internet.

Scenario: Using a Site-to-Site OpenVPN Tunnel

Our scenario has two locations, Site A and Site B, which need to securely share resources.



Site A has multiple devices that need access to the resources at Site B. Configuring OpenVPN on each device at Site A is complex and time-consuming. To simplify the setup, the user decides to use the router at Site A as an OpenVPN client, facilitating connections from all devices at site A to site B as though they were on the local network.

Configuring the Router as an OpenVPN Client

Configuring the router as client allows all traffic from devices at Site A to be tunneled over the Internet to Site B as though they were on the same network.

Before you begin: Make sure that you have an OpenVPN Profile (.ovpn file) from the VPN server. Additionally, the router at site B must be configured with PAT (Port Address Translation) to forward OpenVPN packets to the OpenVPN server at IP address 192.168.127.100.

> **Note**
> Applying the OpenVPN client will disable the IPSec VPN, which may result in VPN connection loss.

1. Sign in to the device with administrator credentials.
2. Go to **VPN** > **OpenVPN Client** > **Settings**.
3. Configure all of the following:

Option	Value
Status	**Enabled**
Description	Optionally enter a description of up to 40 characters.
Import OpenVPN Profile	Import an OpenVPN profile from the local file system.
Username	Enter a username if required by the OpenVPN server.
Password	Enter a password if required by the OpenVPN server.

4. Click **Apply** to save your settings.

Results: After the OpenVPN connection is established, the connection will be visible under **VPN** > **OpenVPN Client** > **Status**. Additionally, the routing information for the VPN will be visible in the routing table under **Routing** > **Unicast Route** > **Routing Table**.

What to do next: If the OpenVPN server cannot identify IPs from site A, it may be necessary to add a NAT rule on the OpenVPN client.

Example: Configuring NAT to Translate over OpenVPN

For OpenVPN servers that are unable to identify IP addresses from site A, you can add a NAT rule on the OpenVPN client router.

1. Sign into the device with administrator credentials.

2. To configure the inbound rule, go to **NAT**, and then click ***[Add]***.

3. Configure all of the following:

Option	Value
Status	**Enabled**
Description	Optional: Enter your description here
Index	Specify an index (ID) for the route.
Mode	**Advance**
Protocol	**ICMP, TCP, UDP**
Incoming Interface (Original Packet)	**LAN**
Source IP Mapping Type (Original Packet)	**Subnet Mask**
Source IP (Original Packet)	192.168.100.0
Subnet Mask (Original Packet)	**24 (255.255.255.0)**
Source Port mapping Type (Original Packet)	**Any**
Destination IP Mapping Type (Original Packet)	**Any**
Destination Port Mapping Type (Original Packet)	**Any**
Outgoing Interface (Translated Packet)	**Any**
Source IP Mapping Type (Translated Packet)	**Single**
Source IP (Translated Packet)	10.8.0.2
Source Port Mapping Type (Translated Packet)	**Any**
Destination IP Mapping Type (Translated Packet)	**Any**
Destination Port Mapping Type (Translated Packet)	**Any**

4. Click **Apply**.

The NAT rule will appear on the list.

The router will now ensure that packets between the local network and the OpenVPN tunnel are translated to the tunnel IP address to facilitate transmission on the remote server.

About NetFlow

NetFlow collects detailed information about the traffic passing through a network interface.

It provides network administrators with valuable insights into traffic flow within the network, allowing them to monitor and analyze network traffic effectively. This capability is crucial for performance monitoring, capacity planning, troubleshooting, and security analysis.

NetFlow In Depth

Netflow architecture generally contains three main components.

NetFlow Exporter

NetFlow exporters are devices that collect and export traffic data, typically a router. The exporter gathers data from the network interface, aggregates packet headers, and sends this information via UDP to the NetFlow collector for analysis.

> **Note**
>
> The exporter identifies the flows by at least one of the following features: IP Source, IP Destination, Source Port, Destination Port, Class of Service, Layer 3 Protocol Type, and Interface.

NetFlow Collector

NetFlow collectors are servers or appliances that receive the aggregated flows transmitted by NetFlow exporters, storing and preprocessing the flow data for the NetFlow analyzer.

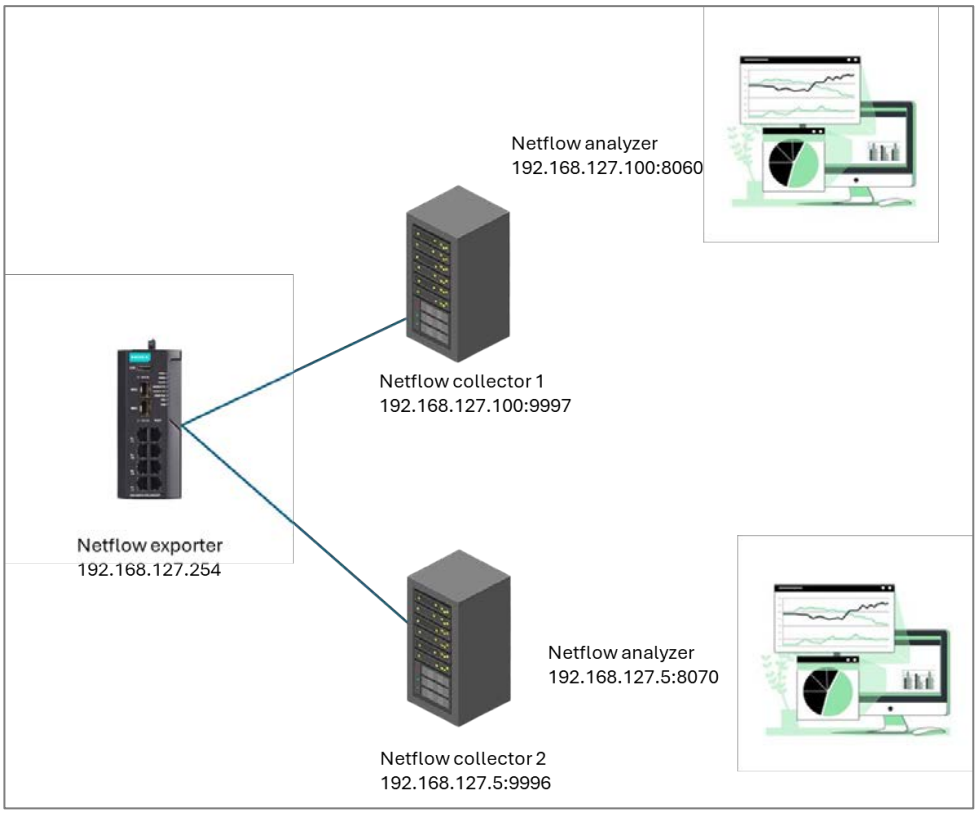
NetFlow Analyzer

NetFlow analyzers are software tools designed to analyze flow data records stored by NetFlow collectors, transforming them into visual reports to aid network administrators in understanding and optimizing network performance.

Scenario: Using NetFlow to Collect LAN Interface Data

See how NetFlow can be used to monitor an enterprise network.

In a large enterprise network, network administrators need to monitor network traffic in real time to ensure stable performance and quickly identify potential security threats. The diagram provided is a simplified example to illustrate the basic concept of NetFlow monitoring and analysis. The system consists of three main components: a NetFlow Exporter, two NetFlow Collectors for redundancy, and a NetFlow Analyzer.

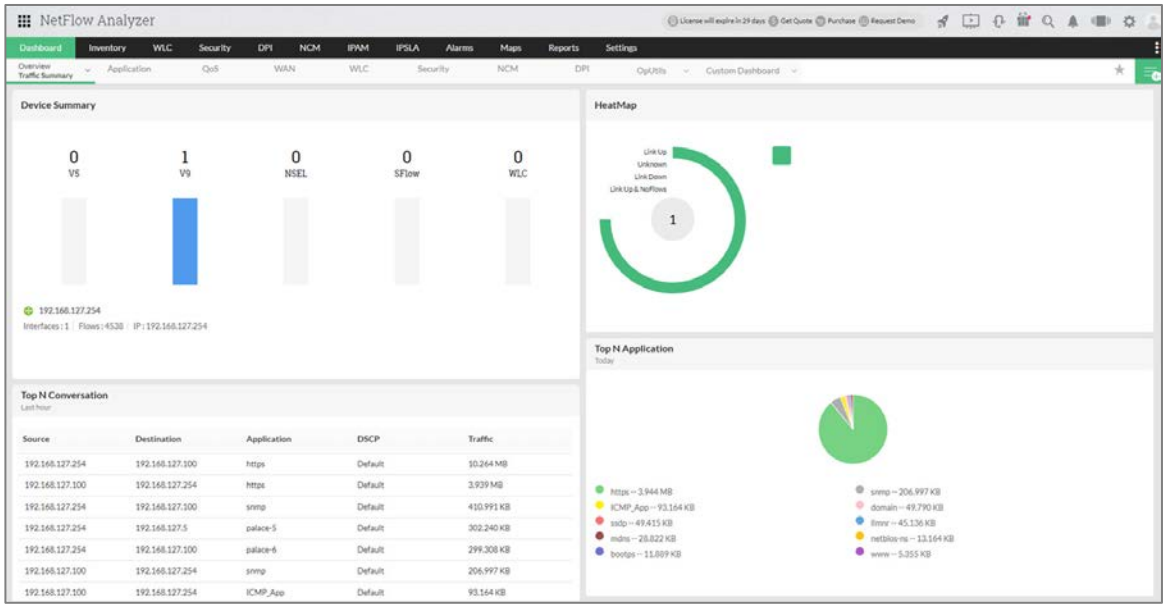


- Netflow Exporter: The router collects network traffic data from the interfaces, and sends it to two Netflow collector servers.
- 2 NetFlow Collectors (Middle Servers)

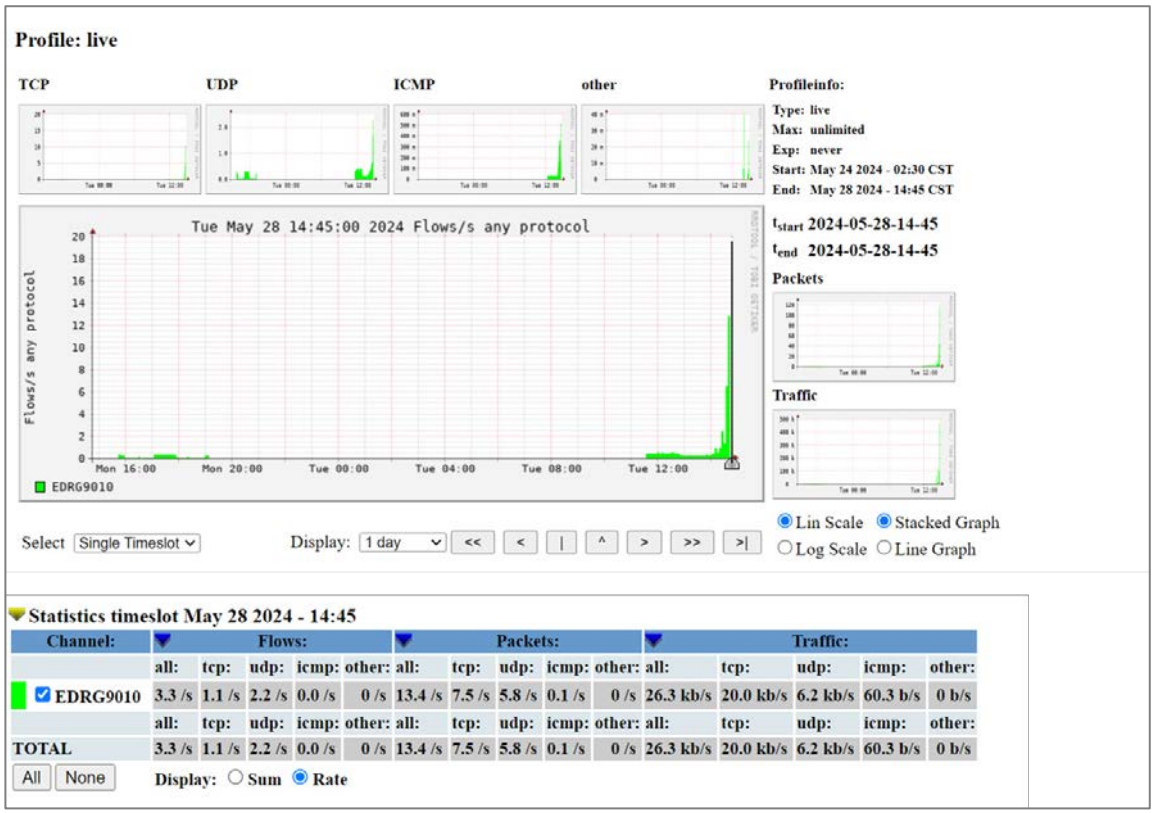
Flows will be sent to both collectors simultaneously. If one collector fails, the other will continue to operate, providing a degree of redundancy.

- NetFlow Analyzers (Software Based):

- One NetFlow collector running **NetFlow Analyzer on Windows OS**



- One NetFlow collector running **NfSen on Linux**



After collection, the data is sent to an analyzer. The analyzer processes this data and transforms it into visual reports, making it easier to understand and analyze network traffic patterns.

Example: Configuring the Router as a NetFlow Exporter

To be effective in a NetFlow topology, the device must be configured as a NetFlow Exporter with the correct settings for collectors.

1. Sign in to the device using administrator credentials.
2. Go to **Diagnostics** > **Tools** > **NetFlow**.
3. To create Collector entires, next to **Collector Settings**, click ***[Add]*** twice.
4. Under **NetFlow Settings**, configure all of the following:

Option	Value
NetFlow	**Enabled**
Version	**V9**Selected the correspond NetFlow version for your NetFlow collector.
Collector 1 IP/Host Name	192.168.127.100
Collector 1 Port	9997
Collector 2 IP/Host	192.168.127.5
Collector 2 Port	9996
Active NetFlow Entry Timeout	1
Inactivity Timeout	1

5. Click **Apply** to apply these settings.
6. Above the table on the bottom half of the page, click ***[Add]***.

The Create NetFlow Entry screen appears.

7. Specify all of the following:

Option	Value
Status	**Enabled**
Interface	**LAN** Select the network interface to be monitor by NetFlow. In this scenario, "LAN" interface (192.168.127.254/24) is selected.
Traffic Direction	**Bidirectional**
Mode	**Basic** **Basic** mode collects all data from the interface. **Filter** mode collects specific data flow according to source IP, source port, destination IP, destination port, and Protocol (TCP, UDP).
Sampling Rate	1 This parameter defines the sampling rate of NetFlow data. When the user inputs a parameter, the system will automatically sample 1 packet from the specified number of packets as the sampling rate. For example, if the parameter is set to 100, it means that 1 packet will be randomly selected from every 100 packets as the sampling rate. The range of the sampling rate is 0~65535, the default value is 0, which means the sampling function is inactive, the result is sames as sampling every packet (sampling rate = 1).

Consider the following guidelines for setting the sampling rate for a production environment:

- Low Traffic Volume: 1 per 100-500 packets
- Medium Traffic Volume: 1 per 1,000-2,000 packets
- High Traffic Volume: 1 per 2,000-4,000 packets

8. Click **Create** to save changes.

About Loopback Interfaces

Loopback interfaces are dummy IP interfaces to allow otherwise identical subnets to communicate without address conflicts or wasted ports.

Imagine a scenario where you need to enable NAT (Network Address Translation) to traverse a VPN (Virtual Private Network). Currently, the setup requires using a Secondary IP, which needs to be bound to a physical interface. This method, although functional, consumes a physical interface and requires additional configuration. Instead, consider using a virtual interface. A virtual interface is a software-based representation of a network interface that doesn't correspond to a physical port. By using virtual interfaces, you can achieve the same objectives without consuming physical hardware resources.

Scenario: Connecting Two Subnets

In this network topology, two routers need to establish a VPN tunnel, but their underlying LANs use the same subnet (192.168.127.0/24). This setup typically encounters difficulties because VPN tunnels cannot usually be established between two identical subnets.

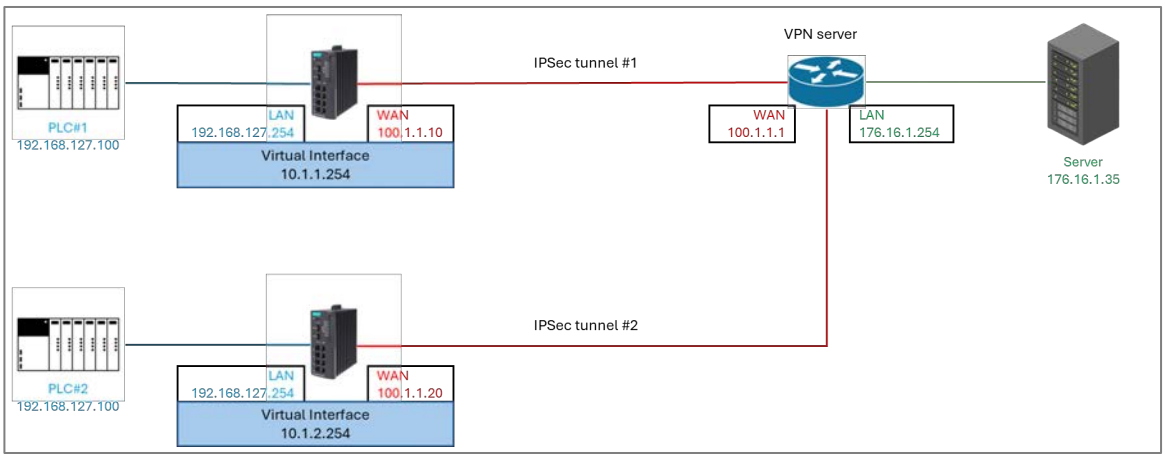
A common solution to this problem is configuring a **secondary IP** address on a physical interface. However, this approach requires binding the secondary IP to an additional physical interface. If the user does not need or cannot use additional physical interfaces, this method becomes impractical.

To solve this problem, we utilized the **loopback interface** feature. Each router is configured with a loopback interface, each with a unique IP address(10.1.1.254 and 10.1.2.254). This way, the two routers can establish VPN tunnels with their respective loopback interfaces without wasting physical ports.

This configuration allows VPN tunnels to be established between two identical LAN subnets (192.168.127.0/24) by using loopback interfaces to isolate and forward internal traffic. loopback interfaces provide an additional IP layer for the routers, allowing VPN connections to operate normally without changing the internal LAN subnet. This way, PLC#1 and PLC#2 under the LAN can communicate with the remote server (176.16.1.30) through NAT, enabling cross-subnet data exchange.

Using loopback interfaces not only solves the VPN connection issue, but also avoids the need for additional physical interfaces, making it an efficient and flexible solution.

Sample Topology



In this topology, PLC #1 and #2 both need to communicate with the server over a VPN connection. However, since they have identical local IP addresses and local subnets, their simultaneous connection would ordinarily result in IP address conflicts and routing problems. With loopback interfaces configured with unique IP addresses, this can be avoided using the loopback interface as a medium for Network Address Translation.

- The VPN tunnel is established between the 176.16.1.0/24 subnet on the server side and the 10.1.1.254/24 and 10.1.2.254/24 loopback interfaces on the routers.
- Internal LAN addresses (192.168.127.0/24) are translated via NAT to communicate through the loopback interfaces. Specifically, PLC#1 at 192.168.127.100 will be translated to 10.1.1.254, and PLC#2 will be translated to 10.1.2.254.
- PLC#1 and PLC#2 use NAT to have their traffic directed through the loopback interface, enabling seamless communication with the server at 176.16.1.254.

By utilizing loopback interfaces and NAT, the architecture ensures that even with identical LAN subnets, VPN connectivity and inter-subnet communication are maintained without the need for additional physical interfaces.

Setup

To configure this setup, you will need:

- Loopback Interface configuration on both routers (see subsequent section)
- NAT configuration to translate the NAT (see subsequent section)

- IPSec tunnels between the VPN server(WAN IP: 100.1.1.1), Router 1 (WAN IP: 100.1.1.254), and Router 2 (WAN IP: 100.1.2.254) using the loopback interfaces as endpoints.

Example: Configuring a Loopback Interface for IPSec Tunnel #1

Virtual interfaces need to be defined before they can be translated.

1. Sign into the device with administrator credentials.
2. Go to **Network Configuration** > **Network Interfaces** > **Virtual Interface**.
3. Under Loopback Interface, click ***[Add]***.

   The Create Loopback Interface Entry screen appears.
4. Configure all of the following:

Option	Value
Name	Specify a name. For our example, we will use VPNLoopback.
Status	**Enabled**
ID	1
IP Address	10.1.1.254
Netmask	**24 (255.255.255.0)**

5. Click **Apply**.

   The loopback interface appears in the list.

Repeat this procedure on the other router to configure a loopback interface for IPSec tunnel #2 with the following differences:

- **IP Address**: 10.1.2.254

Example: Configuring NAT to Translate to the Loopback Interface

For the Virtual Interface to be effective, NAT must be configured to correctly translate packets using the interface. Two rules must be configured on each router: an inbound rule and an outbound rule.

1. Sign into the device with administrator credentials.
2. To configure the inbound rule, go to **NAT**, and then click ***[Add]***.
3. Configure all of the following:

Option	Value
Status	**Enabled**
Description	Optional: Enter your description here
Index	Specify an index (ID) for the route.
Mode	**Advance**
Protocol	**ICMP, TCP, UDP**
Incoming Interface (Original Packet)	**WAN**
Source IP Mapping Type (Original Packet)	**Any**
Source Port mapping Type (Original Packet	**Any**
Destination IP Mapping Type (Original Packet)	**Single**
Destination IP (Original Packet)	10.1.1.254
Destination Port Mapping Type (Original Packet)	**Any**
Outgoing Interface (Translated Packet)	**Any**
Source IP Mapping Type (Translated Packet)	**Any**
Destination IP Mapping Type (Translated Packet)	**Single**

Option	Value
Destination IP (Translated Packet)	192.168.127.100 This matches the PLC on our LAN.
Destination Port Mapping Type (Translated Packet)	**Any**

4. Click **Apply**.

5. To configure the outbound rule, go to **NAT**, and then click ***[Add]***.

6. Configure all of the following:

Option	Value
Status	**Enabled**
Description	Optional: Enter your description here
Index	Specify an index (ID) for the route.
Mode	**Advance**
Protocol	**ICMP, TCP, UDP**
Incoming Interface (Original Packet)	**WAN**
Source IP Mapping Type (Original Packet)	**Any**
Source Port mapping Type (Original Packet	**Any**
Destination IP Mapping Type (Original Packet)	**Single**
Destination IP (Original Packet)	192.168.127.100 This matches the PLC on our LAN.
Destination Port Mapping Type (Original Packet)	**Any**
Outgoing Interface (Translated Packet)	**Any**
Source IP Mapping Type (Translated Packet)	**Any**
Destination IP Mapping Type (Translated Packet)	**Single**

Option	Value
Destination IP (Translated Packet)	10.1.1.254
Destination Port Mapping Type (Translated Packet)	**Any**

7. Click **Apply**.

Repeat this procedure on the other router to configure NAT binding for IPSec Tunnel #2 and corresponding virtual interface, with the following differences:

- Inbound rule:
    - **Destination IP** (Original Packet) : 10.1.2.254
- Outbound rule:
    - **Destination IP** (Translated Packet) : 10.1.2.254

About NAT

Network Address Translation (NAT) is a networking technique that allows multiple devices on a private network to share a single public IP address for accessing external networks, such as the internet.NAT is widely used to conserve IPv4 addresses, improve security, and provide flexibility in network design.

NAT in Depth

NAT has two main mechanisms:

1. **IP Address Translation:**
    - NAT operates on a router or gateway, translating private IP addresses (e.g., 192.168.x.x, 10.x.x.x) to a single public IP address for outbound traffic.
    - Inbound traffic addressed to the public IP is translated back to the corresponding private IP.
2. **Mapping Mechanism**:
    - NAT maintains a **translation table** that maps private IP addresses and ports to public IP addresses and ports.
    - When an internal device initiates a connection, NAT creates an entry in this table to track the session.

Types of NAT

1. **NAT 1-1**:
    - A one-to-one mapping between private and public IP addresses.
    - Commonly used for devices that require a consistent public IP, such as web servers.
2. **NAT N-1**:
    - Maps private IP addresses to a pool of public IP addresses on a first-come, first-served basis.

- Useful when there are fewer public IPs than private devices.

3. **Port Forwarding**:
    - Maps multiple private IP addresses to a single public IP by using different port numbers.
    - This is the most common NAT implementation in residential and small-business networks.

NAT Advantages

1. **Conservation of IPv4 Addresses**:
    - Reduces the need for unique public IPs for each device in a private network.
2. **Improved Security**:
    - Hides internal network structure, making it harder for attackers to directly access private devices.
3. **Simplified IP Management**:
    - Allows the use of private IPs internally, avoiding conflicts with public IP address space.
4. **Flexibility in Addressing**:
    - Facilitates network merging or renumbering without requiring changes to the internal IP schema.

Scenario: NAT for Renewable Power Generators

A renewable energy company specializes in manufacturing tidal power generators. Each generator comes pre-installed with a set of monitoring and control devices (e.g., sensors, PLCs, and communication modules) that have identical configurations, including static IP addresses, to simplify the manufacturing process. For instance, every generator's internal devices use the same private IP scheme (e.g., 192.168.100.x).

When these generators are deployed at a tidal power farm, they are connected to a shared local network. However:

This system has the following risks:

1. IP Address Conflicts:
    - The identical IP configurations of the internal devices create conflicts when multiple generators are connected to the same network.
2. High Manual Configuration Effort:
    - Manually reconfiguring each generator's devices to assign unique IPs would be time-consuming and prone to error, especially when dealing with dozens or hundreds of generators.
3. Centralized Monitoring:
    - The company’s energy management system relies on an Endpoint Detection and Response (EDR) platform to monitor and manage the networked devices. The EDR must differentiate devices across generators without altering their default configurations.

In this scenario, NAT 1-to-1 mapping can be deployed at each generator.

This approach allows the company to map the internal, identical IP ranges of each generator to unique IP ranges or subnets on the shared local network, without altering the original configurations.

See the following sections for guidelines for configuring this scenario.

Example: Configuring 1-to-1 NAT for Device Management

You can add manual network address translation to accommodate fixed IPs on devices.

Make sure that IP interfaces have been assigned.

1. Sign in to the device with administrator credentials.
2. Go to **NAT**, and then click ***[Add]***.

   The Create Index screen appears.
3. Configuring the First Device on Generator 1.
4. To add the inbound NAT rule for the first generator, specify all of the following, and then click **Apply**:

Option	Value
Mode	**1-to-1**
Original Packet (Condition) - Incoming Interface	**WAN**
Original Packet (Condition) - Destination IP	`10.10.0.1`
Translated Packet (Action) - Destination IP	`192.168.100.1`

The Index appears on the table.

5. Click ***[Add]***.
6. To add the outbound NAT rule for the first generator, specify all of the following, and then click **Apply**:

Option	Value
Mode	**1-to-1**
Original Packet (Condition) - Incoming Interface	**LAN**
Original Packet (Condition) - Destination IP	`192.168.100.1`
Translated Packet (Action) - Destination IP	`10.10.0.1`

The Index appears on the table.

The network device will translate between 10.10.0.1 on WAN and 192.168.100.1 without the needing to adjust the settings of the sender or the recipient, or even having them be aware that they have cross a network boundary.

To configure additional devices in this scenario, repeat the above procedure with the following differences:

Options	Generator 1				Generator 2					
	Device 2		Device 3		Device 1		Device 2		Device 3	
	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule	Inbound Rule	Outbound Rule
Original Packet (Condition) - Incoming Interface	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN	WAN	LAN
Original Packet (Condition) - Destination IP	10.10.0.2	192.168.100.2	10.10.0.3	192.168.100.3	10.10.0.4	192.168.100.1	10.10.0.5	192.168.100.2	10.10.0.6	192.168.100.3
Translated Packet (Action) - Destination IP	192.168.100.2	10.10.0.2	192.168.100.3	10.10.0.3	192.168.100.1	10.10.0.4	192.168.100.2	10.10.0.5	192.168.100.3	10.10.0.6

Scenario: Isolated Product Network with Limited Internet Access (NAT N-to-1)

Note

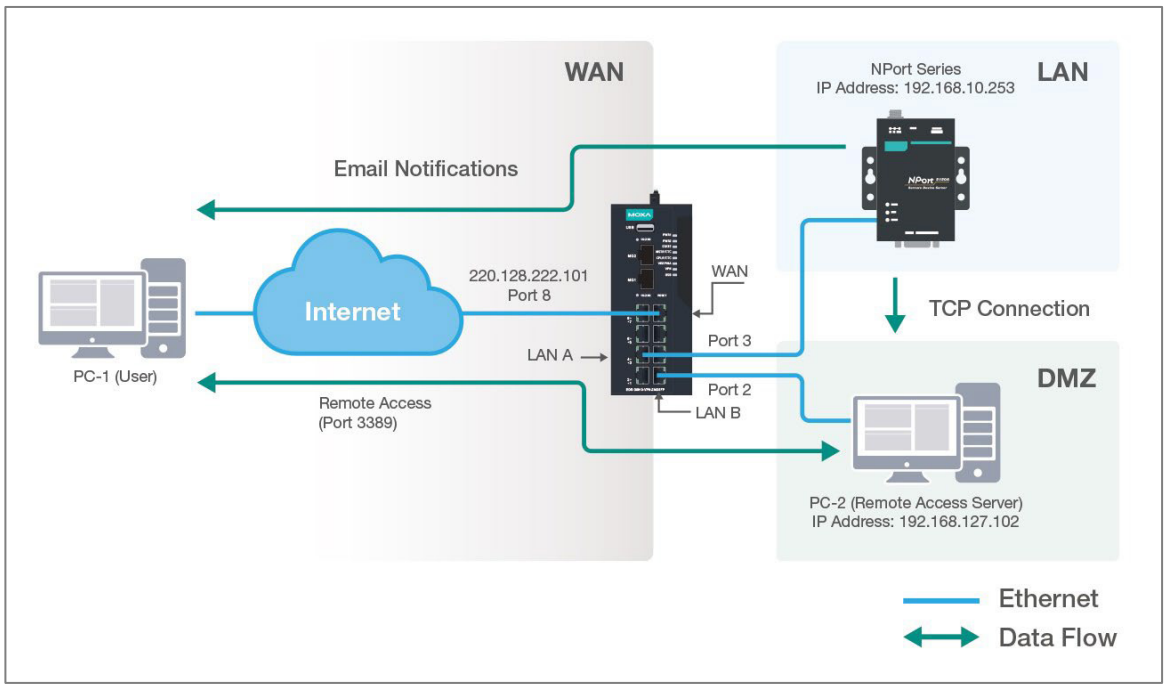
Warning: This is not a security tutorial. While Moxa firewalls can block incoming connections from the internet, internet-connected computers with outbound-only internet access are still vulnerable to high-level compromises that could allow lateral movement within a network. For example, a desktop could become infected with malware through a fishing email, which then sends an outgoing connection request to a command-and-control server, allowing unauthorized remote access.

The security of this example is contingent on the security and access control of all internet-connected computers in the example. The example provided is should be viewed as a tutorial on NAT and DMZ concepts, which can be used in tandem with comprehensive security measures for network protection. NAT and DMZ are tools in a security toolkit, and are not a replacement for or guarantee of comprehensive network security. Secure your devices. Develop, implement, and maintain a comprehensive, multi-layered security strategy.

A DMZ (demilitarized zone) is a region located between an organization's internal trusted network and the external untrusted network. The primary purpose of a DMZ is to provide an additional layer of security while allowing certain network services and resources to be visible to the external world.

A factory has the following networking needs:

- An production network (LAN). This network will contain production equipment that must be protected, but PCs must be able to access the Internet.
- A DMZ network with a single computer serving as a remote access server for connections from the internet, which has network access to the production equipment. Security is contingent on the security of the remote access server.
- A WAN network (Internet Connection).



The this architecture can be created using a series of N-to-1 NAT/PAT rules and Firewall rules on a MOXA router.

The following steps will outline how to configure this scenario. For details on each step, see subsequent sections. Your actual setup will vary depending on local conditions.

1. Configure network interfaces **WAN** (**WAN1** for dual-WAN devices), **LAN**, and **DMZ**.
2. Configure firewall rules to enforce traffic flows.
    a. Create an allowlist paradigm by configuring **Global Policy Default Action** to **Deny All**
    b. Add Layer 3 firewall rules for directional access between each interface:
        - WAN-to-DMZ
        - DMZ-to-WAN
        - LAN-to-DMZ
        - LAN-to-WAN
3. Configure NAT rules to route data between interfaces. This is done after creating firewall rules to ensure no unfiltered traffic gets through.
4. Create the following rules

a. **N-to-1** based on an IP range for directional **WAN** (**WAN1** for dual-WAN devices) access for **LAN**.

b. **PAT** to allow port-specific, directional access from **WAN** and **DMZ** to accommodate the remote desktop protocol.

No port other than 3389 will be forwarded to minimize the potential attack surface.

c. **N-to-1** based on an IP range for directional **WAN** (**WAN1** for dual-WAN devices) access for **DMZ**.

See subsequent sections for detailed configuration instructions.

Example: Configuring Interfaces for DMZ

Interfaces must be defined so they can be referenced for Firewall and NAT rules.

1. Sign in to the device with administrator credentials.
2. To add interface **LAN**, go to **Network Configuration** > **Network Interfaces** > **LAN**, and then press **Add**.
3. Specify all of the following, and then click **Create**:

Field	Setting
Name	LAN
VLAN ID	10
Connection Type	**Static IP**
IP Address	192.168.10.0
Netmask	**24 (255.255.255.0)**

The LAN interface will appear on the Network Interface list.

4. To add interface **WAN**, go to **Network Configuration** > **Network Interfaces** > **WAN1** (**WAN1** for dual-WAN devices), and then press **Add**.
5. Specify all of the following, and then click **Apply**:

Field	Setting
Connection Type	**Static IP**
IP Address	220.128.222.101
Netmask	**8 (255.0.0.0)**

6. To add interface **DMZ**, go to **Network Configuration** > **Network Interfaces** > **WAN2/DMZ**, and then select **DMZ**.
7. Specify all of the following, and then click **Apply**:

Field	Setting
IP Address	192.168.127.102
Netmask	**24 (255.255.255.0)**

The interfaces will be available within the other rule-making screens.

Example: Creating Firewall Rules for DMZ

Firewall rules allow us to configure an allowlist paradigm, blocking any unexpected traffic.

Make sure that network interfaces have already been assigned and configured.

Important: This example of an allow list relies on interfaces, which may in turn rely on static IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated to avoid unpredictable or potentially insecure behavior.

1. Sign in to the device with administrator credentials.
2. Go to **Firewall** > **Layer 3-7 Policy**.
3. To configure the allowlist paradigm, under **Global Policy Settings**, set **Status** to **Enabled**, and make sure **Default Action** is set to **Deny All**, and then click **Apply**.
4. To add the WAN-to-DMZ rule, click **Add** and configure the following:

Option	Value
Name	WAN-DMZ
Action	**Allow**
Incoming Interface	**WAN** (**WAN1** for dual-WAN devices)
Outgoing Interface	**DMZ**
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

5. To add the DMZ-to-WAN rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**DMZ**
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

6. To add the LAN-to-DMZ rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**LAN**
Outgoing Interface	**DMZ**
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

7. To add the LAN-to-WAN rule, click **Add** and configure the following:

Option	Value
Name	DMZ-WAN
Action	**Allow**
Incoming Interface	**LAN**
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)
Filter Mode	**IP and Port Filtering**

Click **Create** to add the entry to the table.

8. Click **Apply** to apply newly created firewall rules.

All traffic not conforming to the above rules will be blocked by the firewall.

Add NAT rule to ensure traffic is routed correctly between different interface.

Example: Configuring NAT Rules for DMZ

NAT rules allow the device to translate packets between different interfaces and IP subnets.

1. Sign in to the device with administrator credentials.
2. Go to **NAT**, click **Add**, and then configure the following to add a NAT rule to allow **LAN** access to **WAN** (**WAN1** for dual-WAN devices):

Option	Value
Description	LAN-WAN
Mode	**N-to-1**
Source IP Start	192.168.127.1
Source IP END	192.168.127.254
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)

Click **Apply** to add the rule to the table.

3. To add a NAT rule to allow **DMZ** access to **WAN** (**WAN1** for dual-WAN devices), click **Add**, and then configure the following:

Option	Value
Description	DMZ-WAN
Mode	**N-to-1**
Source IP Start	192.168.10.1
Source IP END	192.168.255.254
Outgoing Interface	**WAN** (**WAN1** for dual-WAN devices)

Click **Apply** to add the rule to the table.

4. To add a NAT rule to allow **WAN** (**WAN1** for dual-WAN devices) traffic to the remote access server on **DMZ**, click **Add**, and then configure the following:

Option	Value
Description	Remote-Access-Server
Mode	**PAT**
Original Packet (Condition) - Incoming Interface	**WAN** (**WAN1** for dual-WAN devices)
Original Packet (Condition) - Destination Port	3389
Translated Packet (Action) - Destination IP	192.168.127.102
Translated Packet (Action) - Destination Port	3389

Click **Apply** to add the rule to the table.

5. Click **Apply** under the table to save your changes.

About L2TP

The Layer 2 Tunneling Protocol (L2TP) is a widely used tunneling protocol designed to enable virtual private networks (VPNs) and assist Internet Service Providers (ISPs) in delivering various network services.

While L2TP efficiently encapsulates data, it does not include encryption or security features on its own, making it unsuitable for transmitting sensitive information.

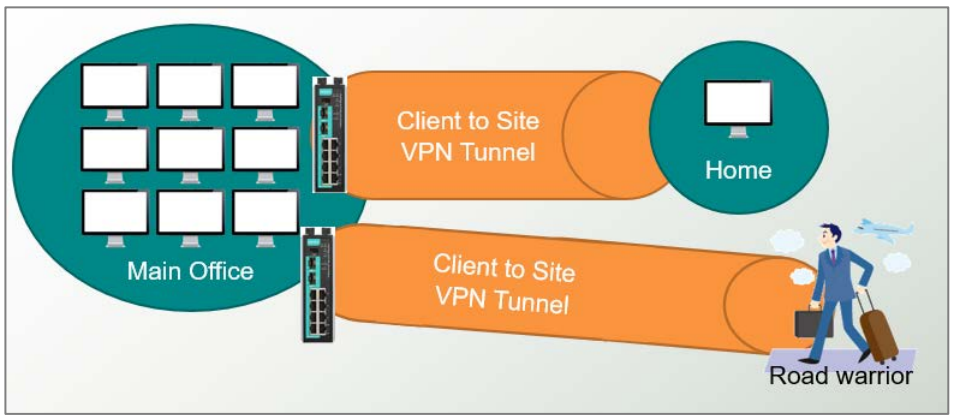
To support data confidentiality and protection, L2TP is often paired with Internet Protocol Security (IPSec). IPSec enhances L2TP by providing encryption and authentication. This combination—known as L2TP over IPSec—delivers a reliable VPN solution that merges L2TP's tunneling capabilities with IPSec's robust security.

L2TP over IPSec is ideal for remote access and client-to-site VPNs, offering an excellent balance of compatibility, scalability, and security.

Scenario: Configuring L2TP with IPSec for Corporate VPN

A company has a centralized office network (Main Office) where critical business resources, such as servers, applications, and databases, are hosted.

Remote employees, including those working from home and traveling (Road Warriors), need secure access to the internal network.



In this scenario, the Main Office VPN server uses the IP address 220.128.222.100.

The following examples outline how configure network devices to support this scenario.

Example: Configuring L2TP Server

L2TP is the tunneling protocol that encapsulates other traffic, and must be configured before IPSec can be added.

1. Sign in to the device with administrator credentials.
2. Go to **VPN** > **L2TP Server**, and then click **Server Setting (WAN)**.
3. Under L2TP Server Mode, choose **Enabled** from the drop down menu.
4. Specify all of the following:

Option	Value
Local IP	Specify the IP of the device. For our example, we will use `192.168.127.254`
Offered IP: Start	Specify the start of the IP range `192.168.127.1`
Offered IP: End	`192.168.127.100`

5. Click **Apply** to save your changes.
6. Click **User Name Settings**, and then click ***[Add]***.

   The Create New Account for L2TP screen appears.
7. Specify a **Username** and **New Password**, and then click **Create**.

   The account appears on the table.

You can now continue to configure IPSec.

Example: Configuring IPSec for L2TP Server

IPSec can be used to add a layer of security to L2TP tunnels, providing a balance of security, convenience, and compatibility.

For L2TP/IPSec connections, L2TP must be configured before IPSec can be configured.

1. Sign in to the device with administrator credentials.
2. Go to **VPN** > **IPSec**, and then click **General**.

3. Under **Status**, choose **Enabled** from the drop down menu, and then click **Apply** to save your changes.
4. Click **IPSec Settings** and then click ***[Add]***.

The Create IPSec Connection screen appears.

5. Configure all of the following:

Option	Value
Settings	**Advanced Settings**
Name	Specify a human-readable name for the connection.
L2TP Tunnel	Choose **Enabled** from the drop down menu.
Pre-shared Key	Specify a key used to encrypt traffic.

6. Click **Create**.

The connection appears in the table.

The connection is now ready to use. Configure the corresponding settings on the client to connect.

About IPSec

A site-to-site IPsec VPN (Virtual Private Network) is a secure connection between two networks over the internet.

It enables organizations to connect their remote sites, such as branch offices or data centers, allowing them to communicate securely as if they were on the same local network.

In an industrial network context, using an IPsec VPN can be particularly advantageous under the following conditions:

Remote Access to Control Systems

- **Remote Monitoring and Control**: When operators or engineers need secure access to SCADA (Supervisory Control and Data Acquisition) systems from remote locations.
- **Maintenance and Support**: If external vendors or technicians require secure access to diagnose or maintain equipment.

Interconnecting Facilities

- **Multi-Site Operations**: For organizations with multiple manufacturing plants or facilities needing secure communication between them.

Regulatory Compliance

- **Industry Standards**: Compliance with regulations such as NIST, IEC 62443, ISO 27001 and UR E26/E27, which often require secure communications and data protection.

Sensitive Data Handling

- **Intellectual Property Protection**: Protecting proprietary processes or designs from unauthorized access during transmission.
- **Confidential Operational Data**: Securing sensitive operational data, including production metrics and inventory levels.

Cybersecurity Enhancement

- **Mitigating Risks**: In environments increasingly targeted by cyber threats, such as ransomware, an IPsec VPN adds an important layer of security.
- **Segmentation**: Enhancing network segmentation to separate operational technology (OT) from IT environments securely.

Interfacing with IoT Devices

- **Secure Communication**: Ensuring secure communication between IoT devices and centralized systems, especially when data is transmitted over public networks.

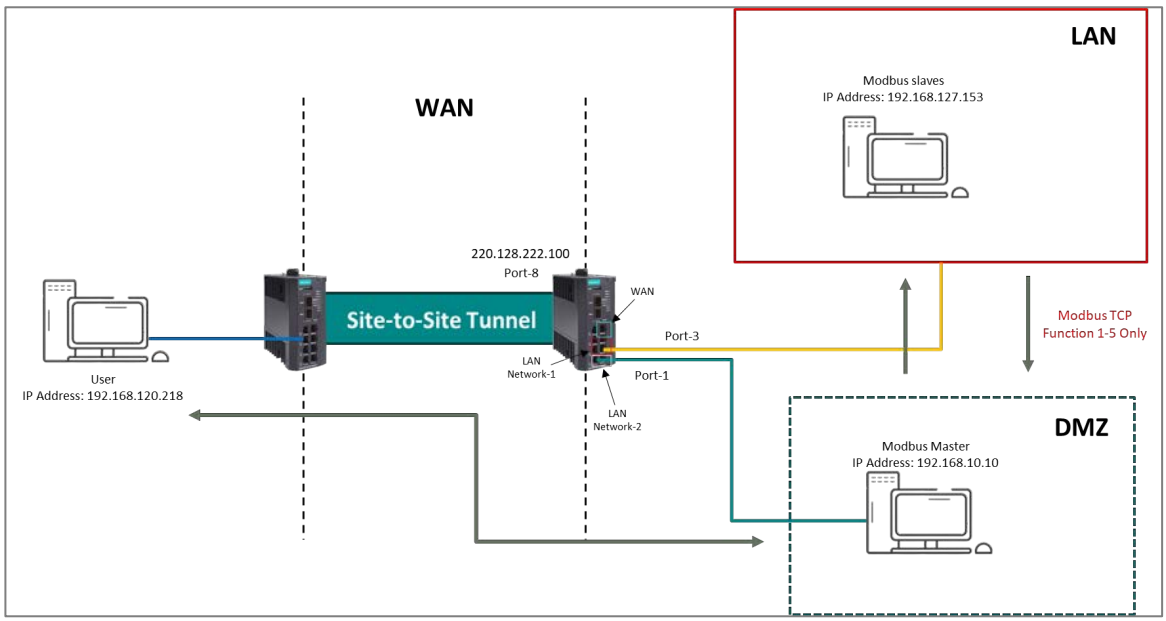
Disaster Recovery and Backup

- **Secure Backup Transfers**: Safeguarding the transfer of backup data between sites to ensure business continuity.

Scenario: Using IPSec to Configure Site-to-site VPNs

The customer operates a Modbus system and requires secure remote access to on-site equipment via the internet. To address their security concerns, the following constraints and solutions are in place:

1. **Local Area Network (LAN) Protection**:
    - Many production line devices reside within a local area network (LAN).
    - To safeguard these Modbus devices, direct access from the internet to the LAN is strictly prohibited.
2. **Network Segmentation**:
    - A separate network zone, known as a Demilitarized Zone (DMZ), has been established to isolate internet traffic from the LAN.
    - This zone serves as an intermediary to protect internal systems.
3. **Data Transmission Security**:
    - All data transmitted between the DMZ and the internet must be encrypted to ensure confidentiality and integrity.
    - The customer plans to implement a site-to-site VPN tunnel to secure data transfer between the remote location and the DMZ.
4. **Access Restrictions**:
    - To comply with the customer's custom security policy, all access from the wide area network (WAN) to both the LAN and the DMZ is explicitly denied.



Example: Configuring Field Site Device as a Server for Site-to-site VPN Access

1. Sign in to the device with administrator credentials.
2. Go to **VPN** > **IPSec**, and then click **General**.
3. Under **Status**, choose **Enabled** from the drop down menu, and then click **Apply** to save your changes.
4. Click **IPSec Settings** and then click ***[Add]***.

The Create IPSec Connection screen appears.

5. Configure all of the following:

Option	Value
Settings	**Advanced Settings**
Name	Specify a human-readable name for the connection.
VPN Connection	**Site to Site(Any)**
Local Network List	• **Local Network:** 192.168.10.254 • **Netmask**: **24 (255.255.255.0)**
Remote Network List	Click ***[Add]***, and then specify: • **Remote Network**: 192.168.120.254 • **Netmask**: **24 (255.255.255.0)**
Pre-shared Key	Specify a key used to encrypt traffic.

6. Click **Create**.

The connection appears in the table.

The connection is now ready to use. Configure the corresponding settings on the remote site to connect.

Example: Configure Remote Site Device as a Client for Site-to-site VPN Access

1. Sign in to the device with administrator credentials.

2. Go to **VPN** > **IPSec**, and then click **General**.
3. Under **Status**, choose **Enabled** from the drop down menu, and then click **Apply** to save your changes.
4. Click **IPSec Settings** and then click ***[Add]***.

The Create IPSec Connection screen appears.

5. Configure all of the following:

Option	Value
Settings	**Advanced Settings**
Name	Specify a human-readable name for the connection.
VPN Connection	**Site to Site**
Remote VPN Gateway	220.128.222.100
Startup Mode	**Initiate Automatically**
Local Network List	• **Local Network:** 192.168.10.254 • **Netmask**: **24 (255.255.255.0)**
Remote Network List	Click ***[Add]***, and then specify: • **Remote Network**: 192.168.120.254 • **Netmask**: **24 (255.255.255.0)**
Pre-shared Key	**Specify a key used to encrypt traffic.**

6. Click **Create**.

The connection appears in the table.

The connection is now ready to use. Configure the corresponding settings on the remote site to connect.

Chapter 6

Railway Applications

Overview of IEC 61375 for Rail Applications

IEC 61375 helps operators save time and money by standardizing communication throughout a train network while minimizing configuration.

Ease of Coupling / Decoupling

Adjusting the length of trains by coupling or decoupling consists is a common practice to optimize the economics of revenue-generating rail services. Reduction in complexity and network configuration makes train coupling/decoupling more efficient, reducing downtime of revenue-generating services. IEC 61375 streamlines the train inauguration process with the Train Topology Discovery Protocol (TTDP).

TTDP allows the operational train composition and ETB state to be stored in a Train Topology Database (TTDB), stored on each ETBN router after successful inauguration. Moxa ETBN Routers make this information accessible through a web UI, a command line interface, and Simple Network Management Protocol (SNMP). End Devices (EDs) can further utilize the Train Real-time Data Protocol (TRDP) to retrieve the train's operational status and consist information from the ETBN. TRDP-based control and monitoring service interfaces allow the configuration of leading train direction, as well as access to comprehensive train network details.

Simplify On-board Device Communication

Train coupling involves connecting either identical or different groups of train cars, known as consists. When using equipment compliant with the IEC 61375 standard, an operational train network configuration is automatically established. This setup ensures essential services, such as TCN-DNS and R-NAT, are configured on the ETBNs (Ethernet Train Backbone Node), regardless of whether the consists are similar or disparate.

This allows onboard EDs to seamlessly send and receive messages across consists using their respective TCN-URIs, without requiring any manual network configuration adjustments within the ECN. This reduction in manual configuration time reduces the need for downtime due to network configuration issues.

Failover Supports Redundancy

IEC 61375 encourages the implementation of redundant communication paths and redundant network components. Redundancy helps ensure that even if one communication path or network component fails, there is an alternative path or component available for data transmission. This enhances the overall reliability of the onboard communication network.

Getting to Know IEC 61375

IEC 61375 is a standard that outlines Train Communication Networks (TCNs).

Issued by the International Electrotechnical Commission, IEC 61375 defines the functional requirements and architecture for Train Communication Networks to ensure interoperability between different media types in an onboard train system. Supported media types include the Multifunction Vehicle Bus (MVB), Ethernet, and wireless, among others.

Rigorous application of the standard ensures standardized communication within and between different train components, contributing to interoperability and seamless integration of systems across the train network.
For the purpose of configuring your device for a rail environment, a basic grasp of the following standards and their terminology is helpful:

- IEC 61375-2-3 - Communication Profiles
- IEC 61375-2-5 - Ethernet Train Backbones
- IEC 61375-3-4 - Ethernet Consist Networks

The following sections provide foundational knowledge of these parts.

- **About Communication Profiles (IEC 61375-2-3)**
  Part 2-3 defines the rules of data exchange between and within consists - known as profiles.
- **About Ethernet Train Backbones (IEC 61375-2-5)**
  Part 2-5 defines the backbone for communication between consists based on Ethernet.
- **About Ethernet Consist Networks (IEC 61375-3-4)**
  Part 3-4 defines networks within consists based on Ethernet.

About Communication Profiles (IEC 61375-2-3)

Part 2-3 defines the rules of data exchange between and within consists - known as profiles.

Onboard application data such as Train Control and Monitoring System (TCMS) or Onboard Multimedia and Telematic Subsystems (OMTS) can take advantage of this

communication profile to facilitate interoperability/data exchange. Train Communication Networks (TCN) can leverage the following services:

Train Real-time Data Protocol (TRDP)

The Train Real-time Data Protocol contains two message types:

- Message Data (MD) - Request and Reply
- Process Data (PD) - Periodical Information/Monitoring

Communication Identifiers (ComIDs) are unique identifiers that distinguish between different types of TRDP participants. They are assigned to messages to define the purpose and destination within the communication network. On Moxa devices, attributes like port numbers for PD/MD are set using an XML file loaded onto the router.

Train Topology Database (TTDB)

The Train Topology Database (TTDB) contains the following four data blocks:

- Consist Info
- Train Directory
- Operational Train Directory
- Train Network Directory

Moxa routers feature a TTDB manager that reads the database and displays the current train composition. TTDB-related status can also be retrieved from the TRDP with reserved ComIDs, as well as through the web and Command-line interfaces.

ETB Control Service Provider (ECSP) and Client (ECSC)

The ETB Control Service Provider (ECSP) runs on each ETBN, and controls the ETB. They ensure efficient communication and event handling. ETBs require static consist information, uploaded in the form of an XML file on Moxa ETBN routers. Refer to Structure and Syntax of Consist Info Configuration Files for more information about XML configuration files.

The ETB Control Server Client (ECSC) is a consumer or user of the control services provided by the ECSP. Typically, it communicates with the ECSP through TRDP to access

ETB control services, enabling actions like train inauguration and setting the leading direction.

TCN Domain Name System (TCN-DNS)

Train Consist Network Domain Name system (TCN-DNS) focuses on domain name resolution and provides a way to help user to get operational train end device IP without pre-configured. It assists in mapping human-readable domain names to machine-readable IP addresses within the train communication environment. It supports multiple domain name resolutions via TRDP. After ECSP is configured correctly, the TCN-URI will be created automatically and available for query.

After the train inauguration process is completed, an operational train topology is established and end-device train network IP addresses are generated automatically. Certain activities—such as changing the train direction or inserting or removing a consist—will trigger dynamic regeneration of end-device train network IP addresses. TCN-DNS is advantageous because it doesn't require preconfiguration. It can automatically map URLs to IP addresses based on the train operational status.

TCN Uniform Resource Identifier (TCN-URI)

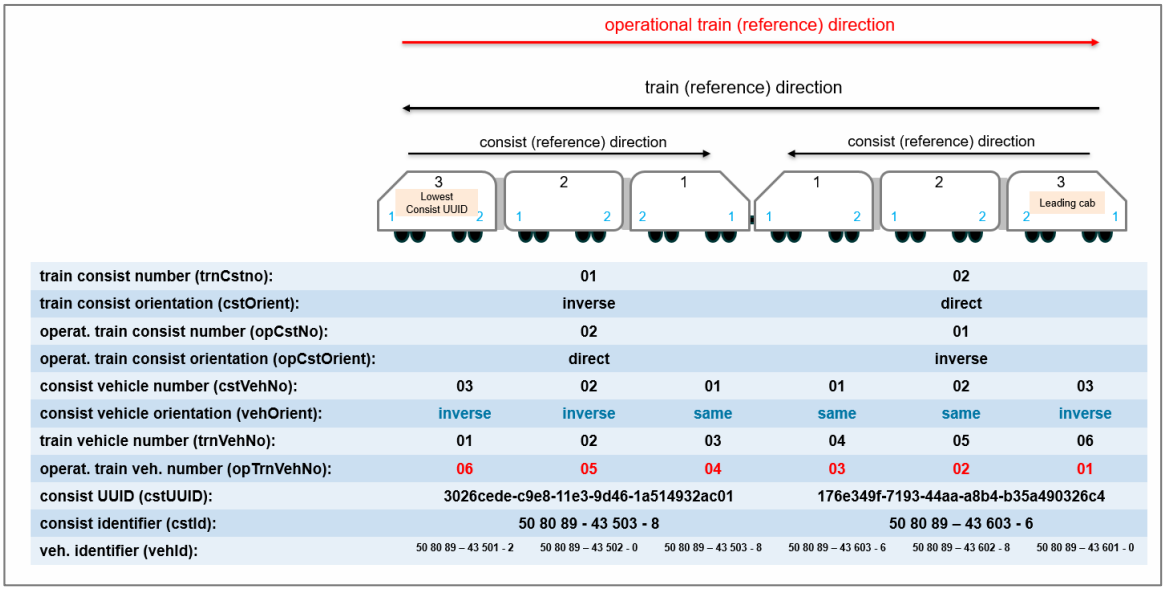
The TCN Uniform Resource Identifier (TCN-URI) defines URIs for resources within the train communication network. This can include addressing schemes, identification of specific resources, or end devices for communication within the train system. TCN-URIs can be resolved by the TCN-DNS on ETB routers.

Safe Data Transmission (SDTv2)

Safe Data Transmission (SDTv2) is a TRDP mechanism ensuring reliability and safety of data exchanged within the train communication network. SDTv2 offers features such as sink-time supervision, safety codes, and other error detection mechanisms to guarantee the integrity and accuracy of transmitted information.

IEC 61375-2-3 Terms

IEC 61375-2-3 defines terms such as directions, orientations, and numbers in a train. These concepts can be better understood through the diagram provided below.



train consist number (trnCstno):		01			02	
train consist orientation (cstOrient):		inverse			direct	
operat. train consist number (opCstNo):		02			01	
operat. train consist orientation (opCstOrient):		direct			inverse	
consist vehicle number (cstVehNo):	03	02	01	01	02	03
consist vehicle orientation (vehOrient):	inverse	inverse	same	same	same	inverse
train vehicle number (trnVehNo):	01	02	03	04	05	06
operat. train veh. number (opTrnVehNo):	06	05	04	03	02	01
consist UUID (cstUUID):	3026cede-c9e8-11e3-9d46-1a514932ac01			176e349f-7193-44aa-a8b4-b35a490326c4		
consist identifier (cstId):	50 80 89 - 43 503 - 8			50 80 89 – 43 603 - 6		
veh. identifier (vehId):	50 80 89 – 43 501 - 2	50 80 89 – 43 502 - 0	50 80 89 – 43 503 - 8	50 80 89 – 43 603 - 6	50 80 89 – 43 602 - 8	50 80 89 – 43 601 - 0

About Ethernet Train Backbones (IEC 61375-2-5)

Part 2-5 defines the backbone for communication between consists based on Ethernet. This ensures interoperability among different network architectures. This standard consists of the follow parts:

Ethernet Train Backbone Node (ETBN)

An ETBN is a pivotal element within the TCN, functioning as a network node that facilitates communication between subsystems and end devices within a train.

Train Topology Discovery Protocol (TTDP)

TTDP's primary purpose is to discover the train network topology during train inauguration. TTDP plays a crucial role in maintaining situational awareness within the train communication network, allowing devices to dynamically discover the presence of neighboring devices. This capability is vital for configuring, optimizing, and troubleshooting the network, ensuring that data is transmitted efficiently and reliably between different components within the train.

About Ethernet Consist Networks (IEC 61375-3-4)

Part 3-4 defines networks within consists based on Ethernet. This network utilizes Ethernet technology to enable communication within a train consist, allowing devices and systems within the train to exchange data.

Ethernet Device (ED)

An Ethernet Device (ED) is a networked device that operates within a train communication system.

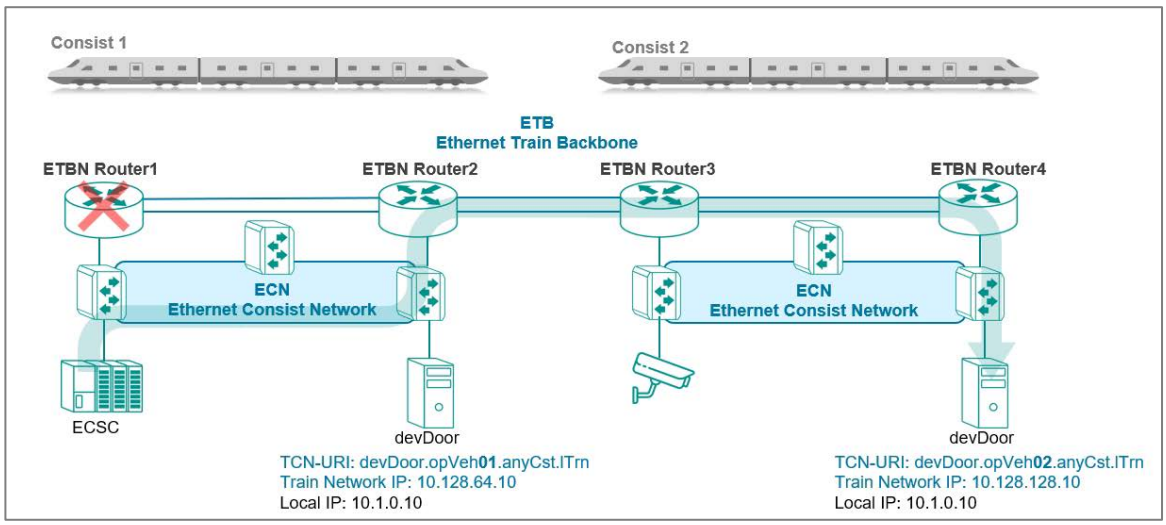
Railway-Network Address Translation (R-NAT)

Railway-Network Address Translation (R-NAT) bridges the gap between internal and external networks. Internal train networks typically use private IP addresses that are not accessible (private, non-routable) outside the train network. R-NAT can translate these addresses to allow the ETB IP address to be used by internal devices to access external network resources. This allows internal devices to communicate with external devices, such as external railway infrastructure.

Scenario: 2 Consists, Each with 2 Redundant ETBNs/ECSPs

In this scenario, we demonstrate an inter-consist network connection with two ETBN in each consist. Having two ETBN routers on each Consist offers enhanced networking reliability.

With the Virtual Router Redundancy Protocol (VRRP) and a redundant router, router failures can be bypassed. In this example with 2 redundant ETBN routers in each consist, in the event ETBN Router 1 fails, the ECSC on Consist 1 can still reach ED (devDoor) on Consist 2 with TCN-URI:devDoor.opVeh02.anyCst.lTrn. ETBN Router 1 will be bypassed, and ETBN router 2 will be used instead. Packets will be relayed to ETBN Router 3 and ETBN Router 4 in turn, before finally reaching the destination train network IP (10.128.128.10).



About Traffic Flows in ETBNs

A sample of traffic flow over an ETBN using a cross-consist camera connection.

Network Topology

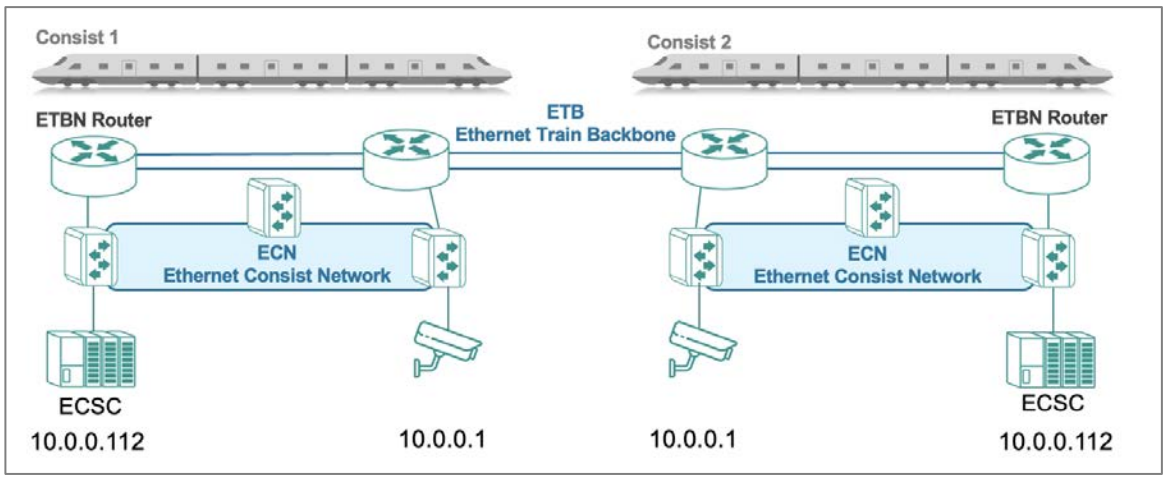
In the example topology below, there are two ETBNs in each consist, and there are two consists coupled together.

The two ETBNs in each consist will negotiate to decide which will serve as primary and backup ECSPs.

The primary ECSP will do two things:

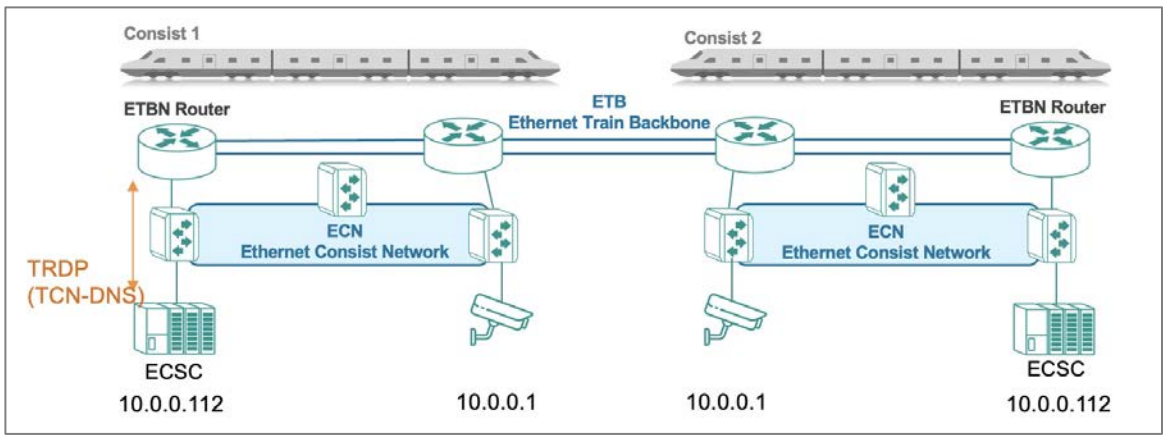
1. Act as the gateway for end device cross-subnet(consist) traffic.
2. Act as the ECSP providing ECSP functions (e.g., respond to TCN-DNS queries from other end devices.)

Let's see how the communication works when the ECSC in consist 1 wants to communicate with the camera in Consist 2.



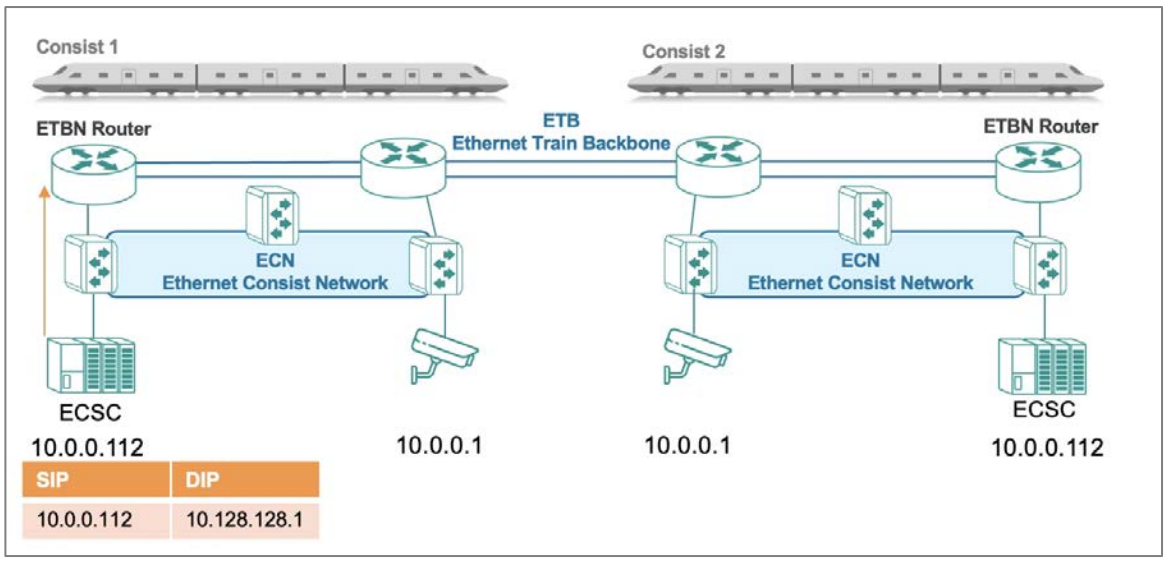
T=0 Getting Camera IP

The ECSC in Consist 1 will ask the ECSP (ETBN router) for the Camera IP in consist 2 using TRDP(TCN-DNS). In this case, the master ECSP will respond with the global IP of the camera in consist 2 (10.128.128.1).



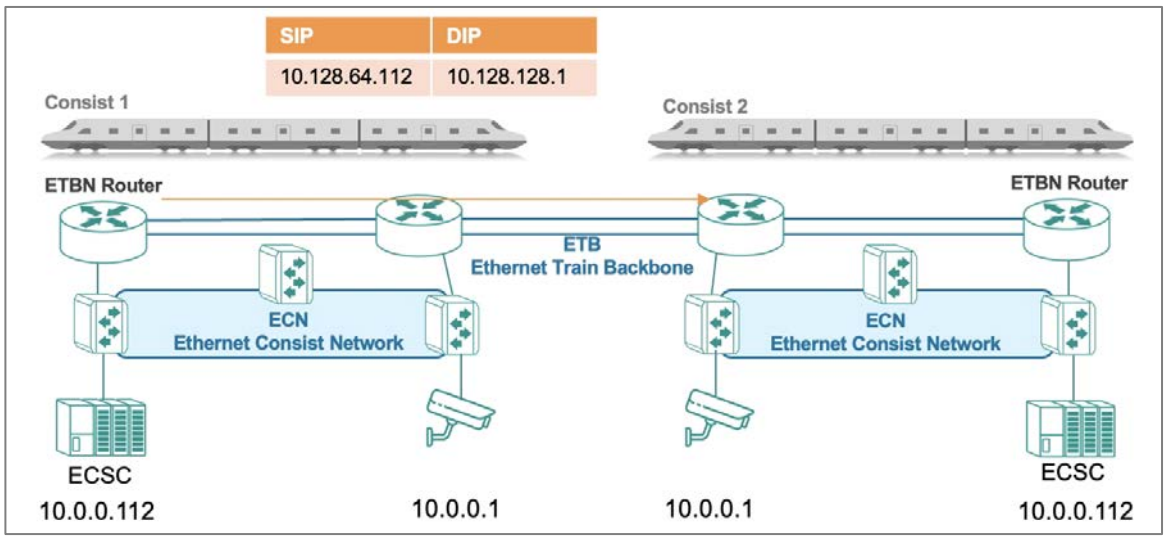
T=1 DIP/SIP

After getting the IP of the consist 2 camera, the ECSC will send out a packet with DIP=camera IP(10.128.128.1), SIP=ECSC local IP(10.0.0.112). Because this is cross-subnet communication, the ECSC will send the packet to the default gateway (10.0.63.254, which is the virtual IP provided by the two ETBNs).



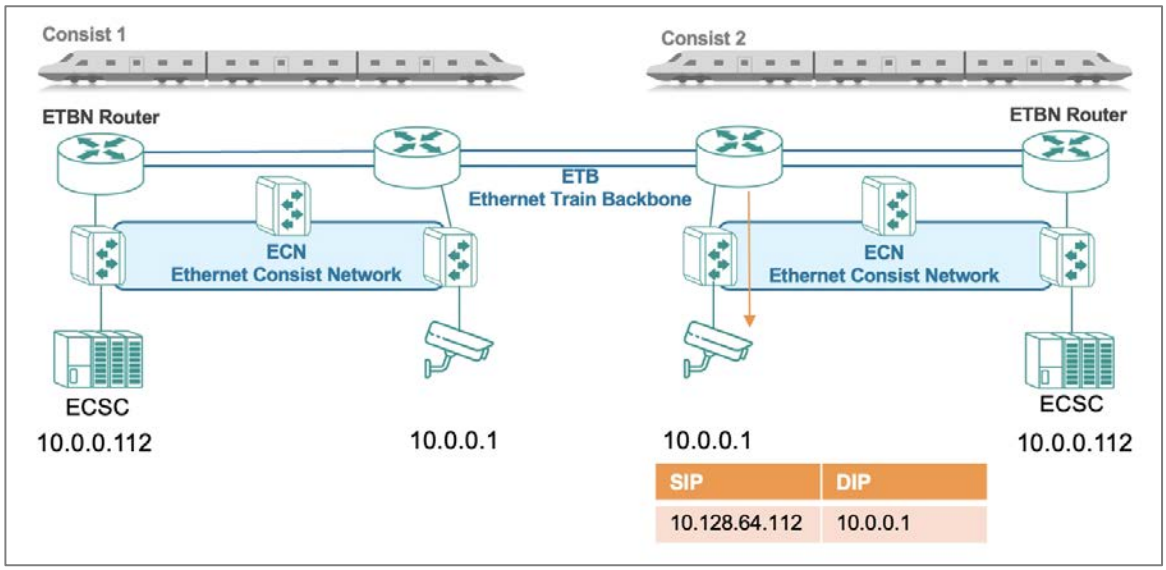
T=2 R-NAT Translation from Consist 1

After receiving the packet, the ETBN router will translate the source IP address from Consist 1 using R-NAT, and then send it to the corresponding ETBN in Consist 2. In this case, the ETBN in Consist 1 will translate the SIP of the ECSC (10.0.0.112) to the global IP (10.128.64.112).



T=3 R-NAT Translation to Consist 2

When the ETBN in Consist 2 receives the packets, it translates the destination IP address using R-NAT, and then sends them to the ECN interface. In this case, the ETBN in Consist 2 will translate the DIP of the camera (10.128.128.1) to the local IP (10.0.0.1).



Example: Configuring 2 Consists with 2 Redundant ETBN Routers Each

Redundant routers in each consist provide an extra layer of reliability.

- Make sure that hardware environment is ready to accommodate this topology and configuration.
- Make sure that you have correctly defined the XML configuration file required for Communication Profiles. While this tutorial provides a sample file, it only covers one consist. Refer to Structure and Syntax of Consist Info Configuration Files for more information about XML configuration files.

To configure hardware to match the example configuration with 2 Consists with 2 Redundant ETBN Routers, do the following:

1. Configure Consist 1:
    a. Configure TTDP on ETBN router 1.
    Refer to Example: Configuring TTDP for ETBN Router 1 on Consist 1 for detailed instructions.
    b. Configure IEC 61375 Communication Profile on ETBN router 1.
    Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.
    c. Configure TTDP on ETBN router 2.
    Refer to Example: Configuring TTDP for ETBN Router 2 on Consist 1 for detailed instructions.
    d. Configure the IEC 61375 Communication Profile on ETBN router 2.
    Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.
2. Configure Consist 2:
    a. Configure TTDP on ETBN router 1.
    Refer to Example: Configuring TTDP for ETBN Router 1 on Consist 2 for detailed instructions.

b. Configure IEC 61375 Communication Profile on ETBN router 1.
   Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

c. Configure TTDP on ETBN router 2.
   Refer to Example: Configuring TTDP for ETBN Router 2 on Consist 2 for detailed instructions.

d. Configure IEC 61375 Communication Profile on ETBN router 2.
   Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

The TTDP configuration procedure for each ETBN router is similar. The following provides a quick reference of the differences in each configuration:Table 1. Comparison of 2 Consists with 2 Redundant ETBN Routers Each

	Consist 1		Consist 2	
	ETBN Router 1	ETBN Router 2	ETBN Router 1	ETBN Router 2
Consist UUID	00000000-0000-0000-0000-000000000001		00000000-0000-0000-0000-000000000002	
Local ETBN Static ID	**1**	**2**	**1**	**2**
ECN interface IP address	**10.0.0.1**	**10.0.0.2**	**10.0.0.1**	**10.0.0.2**

Example: Configuring TTDP for ETBN Router 1 on Consist 1

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.
Consist UUID	`00000000-0000-0000-0000-000000000001` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**2** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**1** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
Direction 2	**Trunk 2**
ETB Port Speed	**Auto**
ETB Port VLAN ID	`1000` Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add** (**+**) button will be available.

6. Click **Add (⊕)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1** and **ETBN 2**
ECN Port VLAN ID	1001 • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + Local ETBN Static ID.
ECN interface IP address	10.0.0.1 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for ETBN 1 on Consist 1.

To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

After configuring ETBN router 1 on Consist 1, you must configure ETBN router 2 on Consist 1, as well as ETBNs 1 and 2 on Consist 2.
This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Example: Configuring TTDP for ETBN Router 2 on Consist 1

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.
Consist UUID	`00000000-0000-0000-0000-000000000001` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**2** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**2** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.

Option	Description
Direction 2	**Trunk 2**
ETB Port Speed	**Auto**
ETB Port VLAN ID	1000 Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add (⊕)** button will be available.

6. Click **Add (⊕)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1** and **ETBN 2**
ECN Port VLAN ID	1001 • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + **Local ETBN Static ID**.
ECN interface IP address	10.0.0.2 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.

Option	Description
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for ETBN 2 on Consist 1.

To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

After configuring ETBN router 2 on Consist 1, you must configure ETBN routers 1 and 2 on Consist 2.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Example: Configuring TTDP for ETBN Router 1 on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.

Option	Description
Consist UUID	`00000000-0000-0000-0000-000000000002` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**2** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**1** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
Direction 2	**Trunk 2**
ETB Port Speed	**Auto**
ETB Port VLAN ID	`1000` Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add (⊞)** button will be available.

6. Click **Add (⊞)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1** and **ETBN 2**
ECN Port VLAN ID	1001 • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + **Local ETBN Static ID**.
ECN interface IP address	10.0.0.1 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for ETBN 1 on Consist 1.2

To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

After configuring ETBN router 1 on Consist 2, you must configure ETBN router 2 on Consist 2.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Example: Configuring TTDP for ETBN Router 2 on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.
Consist UUID	`00000000-0000-0000-0000-000000000002` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**2** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**2** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.

Option	Description
Direction 2	**Trunk 2**
ETB Port Speed	**Auto**
ETB Port VLAN ID	1000 Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add (⊕)** button will be available.

6. Click **Add (⊕)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1** and **ETBN 2**
ECN Port VLAN ID	1001 • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + Local ETBN Static ID.
ECN interface IP address	10.0.0.2 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.

Option	Description
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for ETBN 2 on Consist 2.

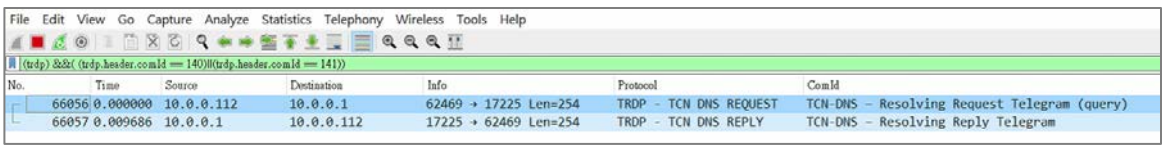
To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

This example uses 4 ETBN routers, 2 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Checking End-Device IPs

There are multiple ways to check the IP addresses of connected devices.

- Use an ECSP (ETB Control Service Provider) or TRDP application to query the end devices' IP with the TRDP protocol.



Using WireShark to check IP addresses.

- Use the web console to check by opening the web console, and then navigating to **IEC-61375→Operational Status→TCN-UI Table**.

TCN-URI Table

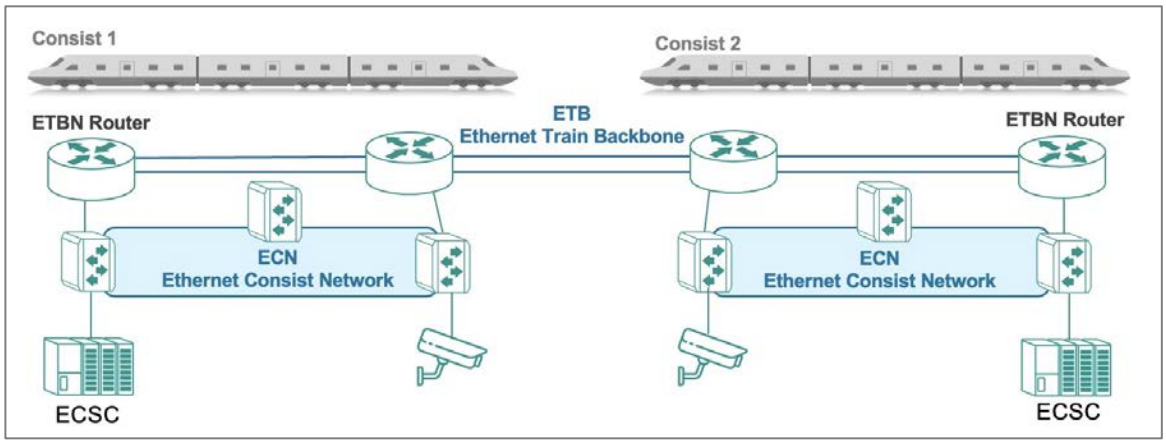
1970/01/22 11:03:03

Search

Index	TCN-URI	Train Network IP	Local IP
1	grpAll.aVeh.aCst.ITrn	239.193.0.0	
2	grpAll.aVeh.lCst.ITrn	239.194.0.0	
3	devECSC.opVeh01.anyCst.ITrn	10.128.64.112	10.0.0.112
4	devsw1.opVeh01.anyCst.ITrn	10.128.64.101	10.0.0.101
5	devsw2.opVeh01.anyCst.ITrn	10.128.64.102	10.0.0.102
6	grpDoor.aVeh.aCst.ITm	239.193.0.20	
7	grpDoor.aVeh.lCst.ITrn	239.194.0.20	
8	grpDoor.aVeh.opCst01.ITrn	239.194.1.20	
9	devECSC.opVeh02.anyCst.ITrn	10.128.128.111	10.0.0.111
10	devsw3.opVeh02.anyCst.ITrn	10.128.128.103	10.0.0.103
11	devsw4.opVeh02.anyCst.ITrn	10.128.128.104	10.0.0.104

Getting ECSP Data with a Network Analyzer

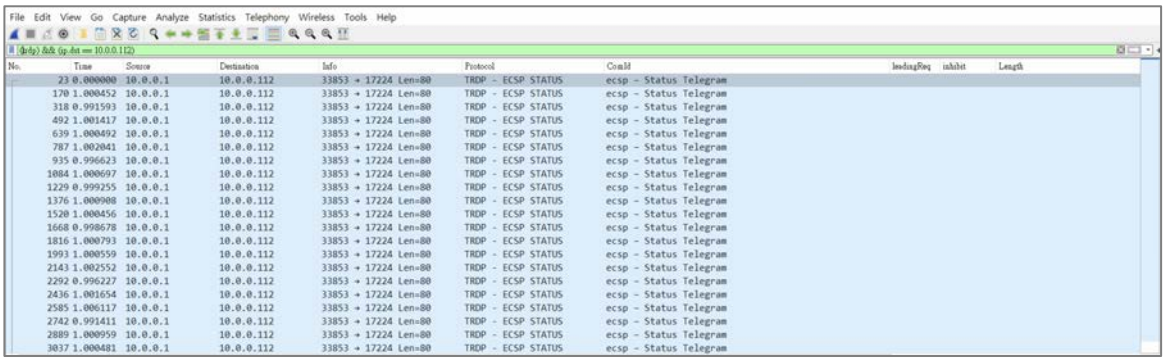
Get train orientation, topology, and set leading direction with ECSP using a Network Analyzer.



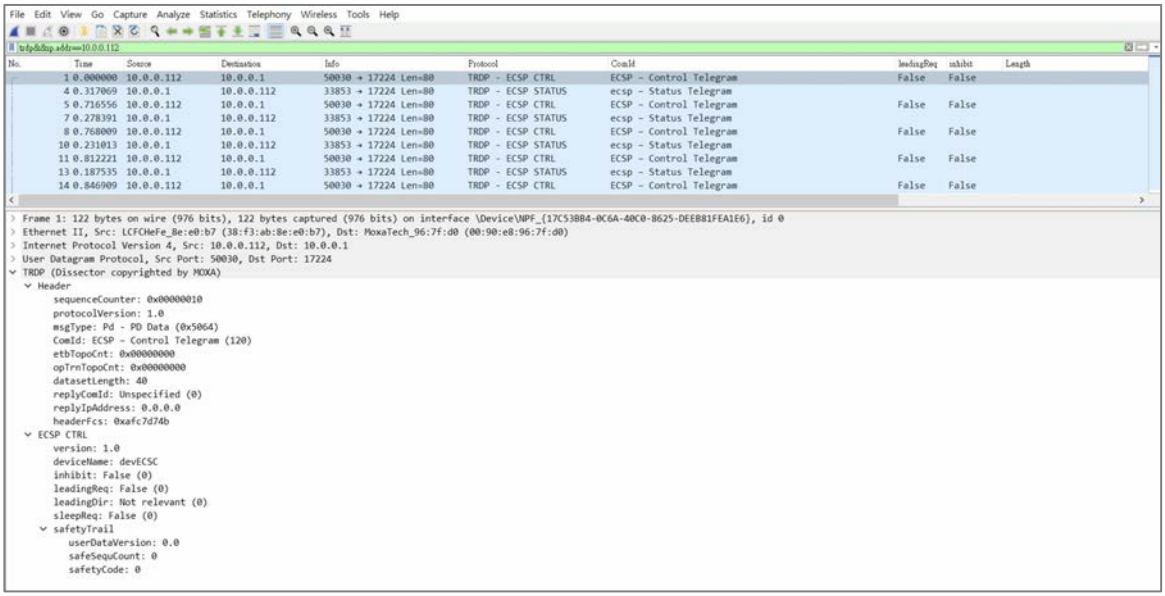
In our example with 2 consists with 2 ETBNs each, users can use ECSC or the TRDP application to query the ETB information or control the ECSP with the TRDP protocol. Here are some example uses:

- Get train topology information.
  The ECSP (10.0.0.1) periodically sends out TTDB updates on IP 239.194.0.0. Users can use the TRDP application to get TTDB information.

- Get ECSP information.
  The ECSP (10.0.0.1) periodically sends out the ECSP status to the ECSC (Ethernet Control Service Client, IP=10.0.0.112, configured the IP in the consist info XML file). Users can use the TRDP application to get ECSP status.



- Use the TRDP application as ECSC to control the ECSP.
  For example, users can change the leading direction by sending the ECSP control packet with a different value in the **leadingDir** field.



Getting ECSP Data with the Web GUI

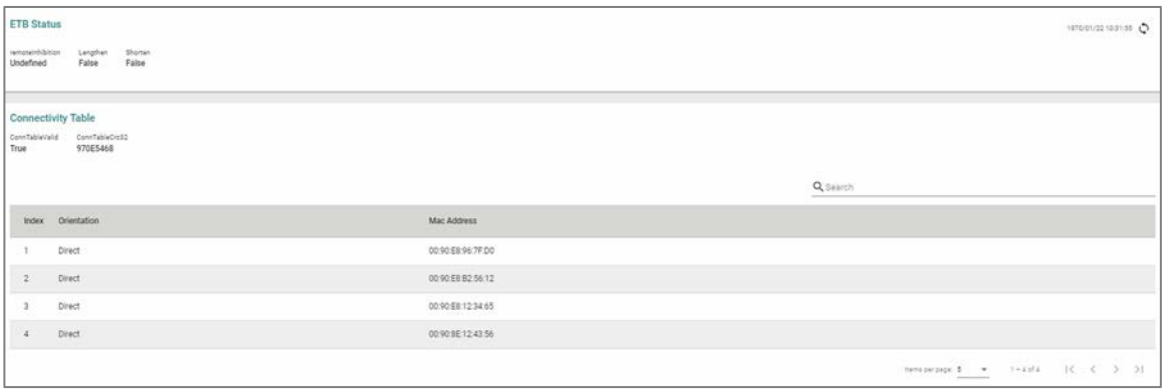
Get ETB status and Train Network Directory with ECSP using a the web GUI.

1. Using an account with **Admin** authority, log in to the network device.
2. Do any of the following:

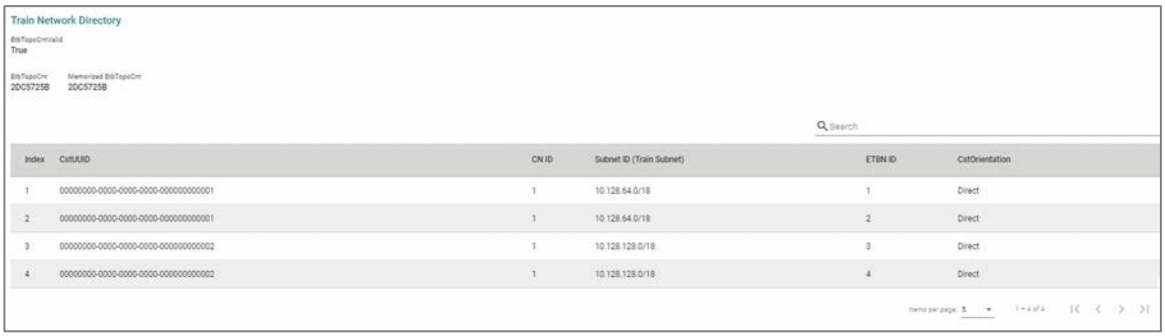
Choose from:

- To view **ETB Status**, go to **Industrial Application→IEC 61375→Ethernet Train Backbone→ETB Status**.
- To view the **Train Directory**, go to **Industrial Application→IEC 61375→Operational Status→Train Directory**.

Viewing ETB Status



Viewing Train Network Directory



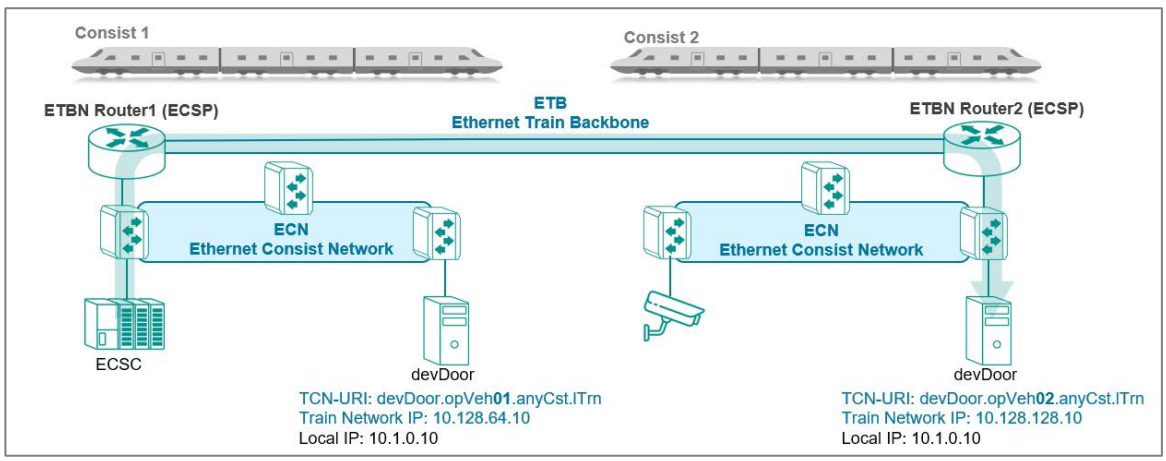
Scenario: 2 Consists, with 1 ETBN / ECSP Each

In this example, we demonstrate an inter-consist network connection with a single, non-redundant ETBN in each consist.

The ECSC on Consist 1 wants to send a command to devDoor, located on Consist 2. TCN-DNS and R-NAT make this easy, without requiring unique configuration.

While coupling two consists, as long as the inauguration is not inhibited, the train network is automatically re-established following the IEC 61375 inauguration procedure. The ETBN Router on each consist functions as a TCN-DNS server that can resolve TCN-URI requests. It also serves as a router to route the traffic to other VLAN domains.

In this example, the ECSC on Consist 1 needs to communicate with the ED (devDoor) with a TCN-URI, such as devDoor.opVeh02.anyCst.lTrn on Consist 2. Packets will be relayed to ETBN Router 1, then ETBN Router 2, before finally reaching the destination train network IP (10.128.128.10).



Example: Configuring 2 Consists with 1 ETBN / ECSP Each

Redundant routers in each consist provide an extra layer of reliability.

- Make sure that hardware environment is ready to accommodate this topology and configuration.
- Make sure that you have correctly defined the XML configuration file required for Communication Profiles. While this tutorial provides a sample file, it only covers one consist. Refer to Structure and Syntax of Consist Info Configuration Files for more information about XML configuration files.

To configure hardware to match the example configuration with 2 Consists with 1 ETBN Router each, do the following:

1. Configure Consist 1:
    a. Configure TTDP on the Consist 1 ETBN router.
    Refer to Example: Configuring TTDP for ETBN Router on Consist 1 for detailed instructions.
    b. Configure IEC 61375 Communication Profile on the Consist 1 ETBN router.
    Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.
2. Configure Consist 2:
    a. Configure TTBN on the Consist 2 ETBN router.
    Refer to Example: Configuring TTDP for ETBN Router on Consist 2 for detailed instructions.
    b. Configure IEC 61375 Communication Profile on the Consist 2 ETBN router.
    Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

The TTDP configuration procedure for each ETBN router is similar. The following provides a quick reference of the differences in each configuration:Comparison of 2 Consists with 1 ETBN/ECSP Each

	Consist 1	Consist 2
	ETBN Router 1	ETBN Router 1
Consist UUID	00000000-0000-0000-0000-000000000001	00000000-0000-0000-0000-000000000002

Example: Configuring TTDP for ETBN Router on Consist 1

Here's how to perform the GUI configuration for a 1 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.
Consist UUID	`00000000-0000-0000-0000-000000000001` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**1** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**1** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
Direction 2	**Trunk 2**

Option	Description
ETB Port Speed	**Auto**
ETB Port VLAN ID	`1000` Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add (⊕)** button will be available.

6. Click **Add (⊕)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1**
ECN Port VLAN ID	`1001` • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + **Local ETBN Static ID**.
ECN interface IP address	`10.0.0.1` Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for the ETBN router on Consist 1.

What to do next: To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

After configuring the ETBN router on Consist 1, you must configure the ETBN router on Consist 2.

This example uses 2 ETBN routers, 1 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Example: Configuring TTDP for ETBN Router on Consist 2

Here's how to perform the GUI configuration for a 2 ETBN/ECSP sample train network.

1. Using an account with Admin authority, log in to the network device.
2. Go to **Industrial Application→IEC 61375→Ethernet Train Backbone→TTDP Settings**.
3. Set **TTDP Enable** to **Enabled**.
4. Under **Local Consist**, configure all of the following:

Option	Description
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB.
Consist UUID	`00000000-0000-0000-0000-000000000002` The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.
ETBN(s) in Consist	**1** Dictated by our sample topology.
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.

5. Under **Local ETBN**, configure all of the following:

Option	Description
Local ETBN Static ID	**1** Identifies the ETBN when there are multiple ETBNs in the same consist.
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.
Direction 2	**Trunk 2**
ETB Port Speed	**Auto**
ETB Port VLAN ID	1000 Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.

Result: Once the **Local Consist** and **Local ETBN** information is filled out, the **Add (⊕)** button will be available.

6. Click **Add (⊕)** to add a Consist Network.
   The **Add ECN** screen appears.

7. In the **Add ECN** screen, configure the following:

Option	Description
ECN to ETBN	**ETBN 1**
ECN Port VLAN ID	1001 • For single ECN consists, the value should be shared by all ETBNs, and should be at least 1000. ETBNs on the same VLAN should have different IP addresses. • For multi-application consists with multiple ECNs where each ETBN handles a different ECN, the default value is 1000 + **Local ETBN Static ID**.

Option	Description
ECN interface IP address	`10.0.0.1` Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. If you are configuring multiple ETBNs on the same VLAN, they must have different IP addresses. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.

8. Click **Apply**.

Results: You have configured TTDP for the ETBN router on Consist 2.

What to do next: To finish configuring of this ETBN router, you must configure the Communication Profile by uploading an XML configuration file. Refer to Example: Configuring Communication Profiles for ETBNs/ECSPs for detailed instructions.

This example uses 2 ETBN routers, 1 on each consist. All ETBN routers in all consists must be correctly configured before the example setup is complete.

Example: Configuring Communication Profiles for ETBNs/ECSPs

ECSPs rely on static XML files that define devices within a consist.

The ETB Control Service Provider (ECSP) runs on each ETBN, and controls the ETB. They ensure efficient communication and event handling. ETBs require static consist information, uploaded in the form of an XML file on Moxa ETBN routers. These files are compiled by the user.

Before you begin: Make sure you have compiled an XML file with device information for each consist. Refer to Structure and Syntax of Consist Info Configuration Files for more information about XML configuration files.

Refer to Appendix: Sample Communication Profile Configuration File for a sample file for a single consist.

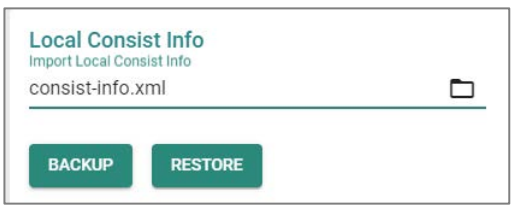
To upload a configuration file to the ETBN router:

1. Go to **Industrial Application→IEC 61375→Communication profile→TTDP Settings**.
2. Under **Local Consist Info**, click **Import Local Consist Info**.

Result: Your browser's file selection window will appear.

3. Navigate to the configuration file in your file system, and select it.

The exact button chosen will vary by operating system and browser. As of April 2024, in Microsoft Edge on Windows, the relevent button is **Open**.



Result: The chosen filename appears under **Import Local Consist Info**.

4. Click **Restore** to import the consist info.

Result: Successfully Updated appears briefly on the screen.

What to do next: You can verify that the correct consist information has been uploaded by going to **Operation Status→Consist Info→Function list** and verifying that the table correctly displays device and consist information.

Chapter 7

Security Hardening Guide

Security Hardening Guide Overview

This chapter provides an overview of security strategy, standards, and recommended best practices to improve the security landscape.

The threat landscape is constantly evolving, and no security guide can ever provide 100% protection. This chapter is constantly being expanded, and is not exhaustive.

Security Best Practices

Introduction to Defense in Depth

The Defense-in-Depth strategy is used to protect systems from various types of attacks by using multiple independent defense mechanisms.

This involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

It is crucial to understand that no single protection can guarantee complete security. That's why the Defense-in-Depth approach makes it difficult for attackers to leverage one weakness to attack the product or network as a whole. This approach requires attackers to overcome multiple obstacles undetected, increasing the difficulty level. By leveraging multiple security features and layers of protection in a product, vulnerabilities in any one layer can be mitigated.

Product Security

This section provides essential information on the installation of your product.

Physical Installation Guidelines

Physical protection of devices is vital to network security.

With physical access to devices, prospective attackers can physically bypass security mechanisms, alter network conditions, or plant additional malicious devices in networks. Follow these tips to help reduce the risk of tampering with networking devices by unauthorized personnel.

- Install switch/router in an access-controlled area. To further protect your device from potential physical attacks, it is important to important to conduct a risk analysis and implement appropriate physical security measures. Consider physical security like installation within a locked cabinet,surveillance, security guards, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.

- Install a Layer 2 switch within the security perimeter. This perimeter can be established by setting up a firewall at the border, as the switch is not designed to be directly connected to the Internet. Note that the switch should not be classified as zone or boundary equipment. Avoid connecting the device directly to the Internet, as this can leave your network vulnerable to security breaches.
- Follow the Quick Installation Guide included in the package of your device. It contains step-by-step instructions that are easy to follow and will help you set up the device quickly and efficiently.
- Examine and monitor anti-tamper labels applied to the device enclosures. These labels provide a quick and easy way for administrators to determine if the device has been tampered with.
- Deactivate any ports that are not currently in use. Fewer active ports represent fewer avenues of attack. Refer to Network Interfaces for more information.

Account Management Guidelines

Manage user accounts, set passwords, and restrict access to authorized personnel only.

- Assign the appropriate account privileges.

  Limit the number of users with admin privileges to only those who need to perform device configuration or modifications. For other users, read-only access is sufficient. Moxa devices supports both local account authentication and remote centralized mechanisms, including RADIUS and TACACS+. This allows for flexible and secure access control options.

- Implement good password practices. Good password practices include:
  - Enabling and configuring a Password Policy to ensure your password meets specified requirements.
  - Setting the minimum password length to at least eight characters.
  - Require passwords to have at least one uppercase and lowercase letter, a digit, and a special character.
  - Setting password expiration.
  - Updating passwords regularly.
  - Never sharing passwords.

Note

Based on trends in cybersecurity regulations, we recommend users increase the complexity of their passwords to the highest level to further strengthen password security.

Refer to Password Policy for more information about password policies.

Protecting Vulnerable Network Ports

Understand security risks and mitigate them by configuring network ports correctly.

- Changing port numbers for active services, including TCP port numbers for HTTP, HTTPS, Telnet, and SSH.
- Disable any ports that are not in use, as they could pose an unacceptable security risk.
- Use encrypted communication protocols wherever available. Use HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, and SNMPv3 instead of SNMPv1/v2c. Refer to Network Interfaces for more information.
- Configure automatic session locking or idle timeouts so that idle sessions cannot be hijacked.
- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications. Refer to SSH & SSL for more information.

Maintaining Communication Integrity

Ensure that information sent is accurate, complete, and secure.

Maintaining communication integrity reduces risks risk of data corruption or interception, and associated security breaches, data loss, and other negative effects on networks and their users.

- Use encryption.

Encryption uses mathematical algorithms to convert data into a secret code, making it extremely difficult for people without the correct codes to read or change the data. By using encryption, you can ensure that the data being transmitted is secure and cannot be intercepted by unauthorized users.

- Use digital signatures.

Digital signatures verify the authenticity and integrity of digital documents or messages. Using a digital signature, you can ensure that the message or document came from the expected sender and has not been altered.

- Implement access control.

Access control restricts access to only authorized users to the network and its resources. By implementing access control measures, such as firewalls or access control lists, you can prevent unauthorized access and reduce the risk of data breaches.

Communication Integrity Features

Moxa devices provide support for VPNs and secure versions of protocols to help maintain communication integrity.

VPN (Virtual Private Network)

VPN is a secure network connection allowing users to access a private network. VPNs use encryption and authentication to protect the data in transit, which makes it difficult for anyone to intercept or tamper with the data. VPNs also provide access control features to ensure only authorized users can access the network. VPNs are commonly used to securely connect remote workers to a company network securely or to allow secure access to restricted resources over the internet.

Refer to VPN for more information.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is a secure version of the regular HTTP protocol for transmitting data over the internet. HTTPS uses TLS (Transport Layer Security) encryption and digital certificates to protect the data in transit from interception, tampering, or eavesdropping.

Refer to Management Interface for more information.

SSH (Secure Shell)

SSH is a secure protocol for remote terminal login and secure file transfers. SSH uses encryption to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SSH also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SFTP (Secure File Transfer Protocol)

SFTP is a secure version of FTP (File Transfer Protocol) that uses encryption to protect the data in transit. SFTP also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SNMP v3 (Simple Network Management Protocol version 3)

SNMP v3 is a secure version of the SNMP protocol used for network management and monitoring. SNMP v3 uses encryption and authentication to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SNMP v3 also provides access control features to ensure only authorized users can access the network.

> **Note**
>
> SNMP managers should be used in accordance with their own security hardening guides and recommended security procedures.

Refer to SNMP for more information.

Device Access Control Best Practices

Device access control is an essential aspect of network security that helps protect against unauthorized access to network resources.

Unauthorized access can occur through various means, including physical access to network devices, hacking, or social engineering. Without proper access control measures

in place, networks are vulnerable to security breaches, data theft, and other malicious activities.

Device access control is particularly important for organizations that handle sensitive data, such as financial institutions, healthcare providers, and government agencies. By implementing device access control, these organizations can limit access to sensitive information and prevent security breaches. Below are some ways to ensure device access control:

- Adopt the Principle of Least Privilege. This principle involves granting users, applications, or systems the minimum level of access or permissions they need to perform their specific tasks and nothing more. Requests for additional access, such as HTTPS, SSH, or Moxa services for administration, should be carefully evaluated before being approved
- Use strong passwords. Passwords should be complex and unique for each device. Passwords should also be changed regularly to maintain security.
  Refer to Password Policy for further information.
- Implement allowlists. Allowlists are authorized devices or users allowed to access a particular network resource. Allowlists can be managed at the device, network, or application levels. Network administrators can use allowlists to ensure that only authorized devices or users can access sensitive resources. The key feature of an allowlist is that anything not on the allowlist is automatically blocked, ensuring only authorized devices, uses, or services can operate freely in a network environment.
  Refer to Trusted Access for further information.
- Implement an L3 firewall. An L3 firewall, also known as a Layer 3 firewall, is a network security device operating at the OSI model's network layer. L3 firewalls can monitor and filter traffic based on IP addresses, ports, protocols, and other network-level attributes. Using L3 firewalls, network administrators can prevent unauthorized access to the network and block potential security threats.

Note

You can block intranet hosts from all external access with isolation, such as with a DMZ, and only allow connections from specifically authorized IP addresses.

Note

To enhance device security and ensure compliance with IEC 61162-460, consider the following practices:

1. Restrict Access:
    - Only allow connections from specific, verified, and secure hosts within a controlled network.
    - Maintain an authorized list of these approved source IPs, ensuring it is documented and regularly reviewed.
2. Block Uncontrolled Networks:
    - Do not permit direct access from hosts in uncontrolled or unverified networks.
3. Example Configuration:
    - Configure trusted access to accept traffic exclusively from source IPs within the 460-network.
    - Any IP address not on this allowlist, including those from non-control networks, will be blocked.

By adhering to these guidelines, you help maintain network security and comply with IEC 61162-460 requirements.

Refer to Firewall for further information.

Configuring Allowlists in Compliance with IEC 61162-460

To enhance device security and ensure compliance with IEC 61162-460, implement the following practices:

- Restrict Access
    - Only allow connections from specific, verified, and secure hosts within a controlled network.
    - Maintain an authorized list of these approved source IPs, ensuring it is documented and regularly reviewed.
- Block Uncontrolled Networks
    - Do not permit direct access from hosts in uncontrolled or unverified networks.

By adhering to these guidelines, you help maintain network security and comply with IEC 61162-460 requirements.

Example Configuration

- Configure trusted access to accept traffic exclusively from source IPs within the 460-network.
- Any IP address not on this allowlist, including those from non-control networks, will be blocked.

About Device Integrity and Authenticity

Integrity and authenticity are vital elements of trust within a network.

Device integrity refers to the state of a device being complete, unaltered, and free from any unauthorized changes or modifications.

Authenticity refers to the assurance that the device is genuine and comes from a trusted source.

Both integrity and authenticity are critical aspects of device security. Methods to sustain these aspects include:

- Configuration Backup & Encryption
- Secure Boot

Configuration Backup and Encryption

Configuration backup and encryption protects a device's sensitive data and configuration by created an encrypted copy storing it securely. In the event of unauthorized device changes, correct configuration information can be quickly and securely restored.

The process involves creating a backup of the device's configuration and then encrypting it using a strong encryption algorithm. The encrypted backup is then stored securely to prevent unauthorized access. This process is particularly important for devices that store sensitive information, such as network equipment, servers, and other critical infrastructure. Encrypting the configuration backup ensures that the data remains protected even if the backup location is compromised.

Secure Boot

Secure Boot is a security mechanism designed to ensure that devices boot using only software that is verified as trusted. The primary function of Secure Boot is to prevent

unauthorized software from running during the boot process. It achieves this by verifying the integrity and authenticity of the bootloader and firmware.

A bootloader refers to the initial software that runs when a device is powered on. Its primary role is to load the device's operating system. Firmware is software embedded within the device that manages and controls the device's hardware functions.

Moxa hardware makes use of cryptographic modules embedded in devices to support verification processes. The device's ROM (read-only memory) contains approved bootloaders and associated digital certificates, which are used to verify the integrity of the firmware.

When the device boots, the first thing to run is the bootloader. Secure boot checks the digital signature against the certificate stored in ROM. If the signatures match, the boot process continues. If they do not match, or there is evidence of tampering, the boot process halts to prevent potential security breaches.

Securing USB Interfaces on Network Devices

- Disable USB ports when not in use.

  USB ports should be disabled by default to prevent unauthorized or accidental use.

- Limit rights to enable or configure USB ports to a minimum number of authorized users.

  Use role-based access control (RBAC) or require multi-factor authentication (MFA) to enable USB ports.

- Standardize procedures and rigorously observe them.

  Your procedures should cover:

  - When and why USB interfaces can be used
  - The type and number of USB devices permitted
  - How data on those devices must be secured. Ensure that all employees and users understand and observe these procedures

Device Resource Management and Monitoring

Moxa devices provide a number of features to help customers manage device resources efficiently and monitor security.

Device Resource Monitoring

Network device resource management is essential for network reliability and security. By monitoring use of network resources, administrators can verify that network guidelines are being followed and devices are operating efficiently and effectively.

Proactive monitoring and management of device resources such as CPU utilization, memory utilization, and network traffic allows administrators to identify potential security breaches early, and help avoid network downtime and disruption. For example, abnormal spikes in network traffic or CPU utilization could be indicative of a malware infection or a denial-of-service attack.

Examples of activities to monitor include:

- Connected ports
- CPU usage
- Memory usage

Refer to Device Summary for more information.

Event Logs

In addition to real-time monitoring and management, Moxa devices provide advanced logging options to help identify security events. Chosen event types can also generate notifications to notify administrators of unusual events where attention is needed, or to feed into larger security monitoring systems.

Moxa devices offer three kinds of logs:

- System Logs, showing details of all system-related event logs
- Firewall logs, showing details of all patterns from layers 3-7, including
    - Trusted Access
    - Malformed Packets

    - DoS Policy
    - Layer 3 – 7 Policy
    - Protocol Filter Policy
    - Anomaly Detection & Protection (ADP)
    - Intrusion Detection/Prevention System (IDS/IPS)
    - Session Control
- VPN logs, showing all VPN-related events

Refer to Event Log for more information about Event Logs.

Refer to Event Notifications for more information about Event Notifications.

Refer to SNMP for more information about SNMP configuration.

Denial of Service (DoS) Protection

In a denial-of-service (DoS) attack, the attacker attempts to overwhelm a target system with a flood of traffic or requests. The deluge of traffic causes the target system to become paralyzed, and also causes disruptions in networks and online services.

Moxa devices can prevent several types of DoS attacks by rejecting requests which ask for a particular network scan, or rejecting too many such requests in a specified period.

Refer to DoS Policy setting for more information.

Session Control

Session control refers to managing communication sessions between network objects, such as IP addresses or ports. The management process involves establishing, maintaining, and terminating sessions to ensure secure and reliable communication between various objects. Session control allows administrators to allocate device resources more efficiently by limiting the number of active sessions, and improving network security by dropping unused sessions.

Refer to Session Control for more information.

Recommended Settings for Services and Features

When prioritizing device security, the first point of assessment is often the network interfaces and services.

By deactivating unneeded interfaces and services, one can reduce potential vulnerabilities and associated security threats. Additionally, activating the appropriate security features enhances early anomaly detection and bolsters the device's defense against cyber attacks.

Common Protocols and Ports

Service Name	Default Port	Default Setting	Security Suggestions
HTTP	TCP 80	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
HTTPS	TCP 443	Enabled	
Telnet	TCP 23	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
SSH	TCP 22	Enabled	
NTP/SNTP	UDP 123	Disabled	Use SNTP to synchronize system time if possible. Enable NTP authentication if possible.
SNMP	UDP 161 UDP 162 TCP 10161 TCP 10162	Disabled	For V1 & V2c, change default community string names, i.e. public & private, to other unique names. For V3, enable SNMP admin account authentication.
Syslog	UDP 514	Disabled	Enabling Syslog is recommended to avoid missing critical logs due to limited local storage. This sends logs to an external syslog server, where they can be securely stored and retained. The syslog server is responsible for keeping these logs for a minimum period required by local regulations, ensuring critical incidents are properly documented and accessible when needed.
RADIUS	UDP 1812	Disabled	Enabling RADIUS authentication can help administrators manage password changes more efficiently.
Moxa Services	TCP 443 UDP 40404	Enabled	These 2 ports are only used by the Moxa management software. Disable it if you don't use Moxa management software.

Security-Related Functions

Function	Default Setting	Security Suggestions
Firewall	Deny All	Without precise firewall rules configuration, “Allow All” has a higher change to allow unwanted packets going into the protected network, so we highly suggest using “Deny All” instead of “Allow All”. Refer to Scenario: Airport Integrated Solutions to learn more about Allow Lists.
Password Policy	Disable	Enable password policy to comply enterprise security policies.
Login policy	Disable	Enable a login policy to heighten resistance against brute force attacks and terminating any inactive login sessions.
Malformed Packets Filtering	Disable	The "Malformed Packets Filtering" feature logs events at a user-defined severity level whenever the system discards malformed packets. Depending on the protocols active in your network, you can choose to enable this feature or leave it disabled.
DoS Policy	None	Select a DoS policy according to your network traffic to increase network robustness.
Session control	None	Configure session control policies appropriate for your traffic to improve network reliability.
802.1X over ports	Disable	Enable 802.1X port authentication to block unauthorized LAN access.
Trusted Access	Enabled	By default, the device permits all connections from the LAN attempting to access it. For enhanced security, block all LAN connections attempting to access the device. Then, use a trusted IP list to specify which trusted IPs are allowed access to the device.

Common Threats and Countermeasures

These are examples of common known threats, and suggestions for mitigation.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over HTTP data flow.	Disable HTTP, and replace HTTP transmission with HTTPS.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over Telnet data flow.	Disable Telnet, and replace HTTP transmission by SSH.
Information Disclosure	Data flowing across TFTP may be sniffed by an attacker.	Use SFTP instead of FTP.
Denial of Service	SNMP Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive SNMP requests.
Denial of Service	RADIUS Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive RADIUS requests.
Repudiation	Devices fail to synchronize a system time with a trusted NTP/SNTP server.	Enable NTP authentication to verify a connection with the trusted NTP/SNTP server.

Note

Create an incident response plan and follow it carefully. Ensure your procedures allow for user reporting and admin response to those reports. Many threats manifest themselves as irregular device behavior – such as device inability to provide basic services like routing or firewall functions, which in turn lead to interruptions or unauthorized access. Create a plan that allows admins to prepare, reboot, and monitor devices with abnormal behavior.

Recommended Operational Roles and Duties

Adhering to the principle of least privilege reduces risks by ensuring users operate at the minimum privilege required to complete their tasks.

Instead of individual allocation, privilege levels should be tied to specific job functions. For optimized device security, we recommend three distinct privilege levels, each tailored for different management needs:

Administrator

Designated for system management, this privilege level permits:

- Creation and deletion of configuration objects, files, and user accounts.
- Monitoring system status and resources.
- Modifying parameter values.

- Reviewing stored data within the device.

Administrator Responsibilities:

- Reset and periodically change the default administrator password.
- Ensure password complexity aligns with enterprise security policies.
- Manage and authorize individuals with appropriate access privileges.
- Disable non-essential interfaces or network services.
- Enable secure communication protocols to guard against data breaches.
- Regularly update firmware to address potential vulnerabilities.

Supervisor

Tailored for network experts or operators, this privilege grants:

- Monitoring of system status and resources.
- Adjusting values in configuration objects or files.
- Access to review data stored in the device.

Supervisor Responsibilities:

- Continuously monitor system status and resources to maintain device functionality.
- Routinely verify the integrity of device configuration objects and files.
- Manage trusted devices through IP and MAC allowlisting.
- Oversee and respond to system alerts to preempt device failures and security threats.

Auditor

Reserved for audit-focused personnel, this level allows:

- Monitoring of system status and resources.
- Reviewing data stored within the device.

Auditor Responsibilities:

- Regularly inspect logs to identify and assess incidents and their associated risks.

Moxa devices provide three user privilege categories: admin, supervisor, and user. We advise aligning the admin role for administrator users, the supervisor role for supervisor users, and the user role for auditor users.

Refer to:

- User Accounts

Recommended Patching and Backup Practices

Moxa's guidance on ensuring device security through regular firmware upgrades and configuration backups.

Firmware Upgrade

Moxa continuously releases firmware throughout the product lifecycle to improve features and rectify identified issues. Upon discovering a vulnerability, our approach aligns with the Moxa Product Security Incident Response Team (PSIRT) guidelines, ensuring swift and appropriate action.

Maintaining current firmware on your network devices is vital to maintain security. Using outdated firmware can expose the device to potential threats. We strongly advise periodic firmware updates. We consistently release the latest firmware and software on our official website, along with respective release notes. Check for these updates regularly.

Note

Firmware updates may cause downtime. Assess the impacts of downtime and prepare appropriately before initiating updates.

Note

Device performance may be degraded during the update process. Normal function should be restored once the update is complete and the device restarts.

Configuration Backup

For network operators and system administrators, it is essential to regularly back up device configurations. This precaution allows for quick recovery in unforeseen scenarios, such as cyber attacks.

Note

Prioritize use of secure transfer protocols – such as SFTP – for file transfers to protect the configuration maintenance process.

Refer to:

- Firmware Upgrade
- Configuration Backup and Restore

Recommendations for Vulnerability Management

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security becomes an increasingly high priority.

The Moxa Product Security Incidence Response Team (PSIRT) takes a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

To report vulnerabilities for Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

For the most up-to-date Moxa security information, please visit our security advisory page: https://www.moxa.com/en/support/product-support/security-advisory

Recommendations for Decommissioning

Recommendations for Decommissioning

To avoid any sensitive information such as account passwords or network configurations from disclosure, always delete all imported certificates and reset devices to factory default before you decommission your devices.

Note

Things to keep in mind when decommissioning or re-purposing devices:

- Device data can be cleared using the Factory Reset options. When reseting devices, make sure to confirm the operation and allow it sufficient time to complete.
- Delete all logs, and verify deletion.
- After all reset processes are complete, verify that all sensitive data has been cleared.

Using Security Features

Ensuring the security features of your network device operate effectively is vital for maintaining a secure and reliable system. During field validation, include these features—such as firewalls, encryption, and intrusion prevention—in your testing plan to confirm they function properly in real-world conditions.

This chapter outlines the available security features, how to configure them, and best practices to ensure consistent protection for your network.

Introduction to IPS

IPS (Intrusion Prevention System) is a network security technology used to detect and prevent potential threats in a network.

IPS analyzes the network traffic and identifies potential attacks, including viruses, worms, malware, and unauthorized access. Once an IPS detects a threat, it takes immediate action to block the attack and protect the security of the network and system. IPS uses signature-based and behavior analysis to identify threats and employs various techniques to protect systems, such as blocking IP addresses and protocols. It is an important component of network security architecture designed to enhance the security of networks and systems, prevent unauthorized access, and protect against data breaches.

What is the difference between IDS and IPS?

IDS (Intrusion Detection System) and IPS are network security systems that help protect against security threats and vulnerabilities.

An IDS monitors network traffic and identifies potential security threats and attacks. When it detects a security threat, it saves logs and generates an alert, which is sent to the security team for further analysis and action. An IDS is a passive security system that only monitors network traffic and does not take any action to prevent or stop an attack.

On the other hand, an IPS monitors network traffic like an IDS, but also takes active measures to prevent security threats and attacks. Additionally, an IPS can block, quarantine, or even terminate network traffic or connections deemed suspicious or

malicious. IPS systems often use a set of predefined rules or policies to identify and respond to security threats in real-time.

The main difference between IDS and IPS is that IDS only detects and notifies of potential security threats, while IPS takes action to prevent and stop the security threat. IDS is generally considered a more passive security system, whereas IPS is more proactive and can take immediate action to mitigate security risks.

IPS Applications

IPS is typically used to actively prevent and block unauthorized access or malicious activities on your network.

IPS is typically used when you want to actively prevent and block unauthorized access or malicious activities on your network. It's a proactive security solution that acts in real-time to prevent potential security threats from entering or leaving your network.

Here are some common applications of IPS:

1. **Protecting critical assets**: IPS can protect mission-critical assets or systems, such as PLCs, factory automation, ICS (Industrial Control System), from external and internal security threats.
2. **Resisting zero-day attacks**: IPS can help you detect and block unknown or zero-day attacks that have not yet been identified by traditional anti-virus or intrusion detection systems.
3. **Real-time threat detection**: IPS systems can provide real-time threat detection and prevention, reducing the risk of data breaches and other security incidents.
4. **Virtual patching**: Even devices with outdated OS can receive up-to-date protection without regular security updates and patches.

In summary, IPS should be used when you want to actively prevent and block security threats in real-time and protect critical assets or comply with specific regulations or standards.

IPS Limitations

The most notable limitation of IPS is that it relies on updated patterns—updated definitions and countermeasures of known threats—to correctly detect and act on

threats. To address this issue, Moxa provides regular updates in the form of a security package. The packages must be installed by users periodically to maintain the latest protection capabilities. The update procedure and frequency should be standardized by organizational policy.

Note

Some products may not support syslog servers. For such devices, you can design a process, script, or system to periodically retrieve the IPS/IDS logs. Alternatively, you can enable port mirroring to direct traffic to a dedicated IPS device.

As of November 2024, syslog support is planned but not yet implemented for the following products:

- EDR-8010 Series
- EDR-G9010 Series

Note

IPS is not a substitute for antivirus software or security solutions. IPS scans network packets, but does not scan devices and is not antivirus software. If an attacker finds a way to run malicious code on the device itself, IPS may not detect the infection, but may still detect the packets sent as a result of such compromise. To increase chances of detection, you can:

- Enable IPS/IDS, configure all notification features, and monitor them diligently. If characteristics of malware/malicious code are detected in outgoing packets, administrators will be notified and can respond appropriately.
- Ensure USB ports are disabled by default and closely monitor them. Attackers may attempt to load malicious code over USB ports. Establishing careful control procedures can minimize this threat. Consider restricting USB devices only to Moxa ABC-02 and regularly scanning the ABC-02 with antivirus software.

Example: Updating the Network Security Package via the Web GUI

Download the latest Network Security Package from the Moxa and install via the Web GUI.

Before you begin: Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources→Software Packages→Network Security Package for EDR-G9010 Series**

The Moxa support website is located at https://www.moxa.com/en/support.

2. Download the latest version of the Network Security Package to your computer.
3. Open the router's web interface and navigate to **System→System Management→Software Package Management→Network Security Package**.
4. Click **Source**, and then choose **Local**.
5. Click **Select Files**, and then choose a file from your local file system.
6. Click **Upgrade** to start the upgrade process.

The upgrade process will begin, and the result appears at the bottom of the interface.

What to do next:

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the web interface, go to **Firewall→Advanced Protection→Information→Package Information**, and check the version listed.

Example: Updating the Network Security Package via MXsecurity

Download the latest Network Security Package from the Moxa website and install with the MXsecurity web console.

Before you begin: Make sure you have purchased an activated an IPS license.

This task uses the Moxa EDR-G9010 series as an example product. Replace this product with your product for each step.

1. From the Moxa support website, navigate to **Resources→Software Packages→Network Security Package for EDR-G9010 Series**

The Moxa support website is located at https://www.moxa.com/en/support.

2. Download the latest version of the Network Security Package to your computer.
3. From the MXsecurity web console, go to **Device Deployment→Software Packages→Network Security Packages**.
4. Select the secure routers to update, and then click **Upgrade**.

Results: The upgrade process will begin on the selected routers, with the result displayed within seconds.

What to do next:

Confirm that the Network Security Package has been updated by checking the version information from the Package Information Screen. On the MXsecurity web console, go to **Device Deployment→Software Packages**, and check the version listed.

Example: Configuring IPS Rules via MXsecurity

Enable IPS rules and observe the generated event from the MXsecurity, the centralized cybersecurity visualization platform.

Before you begin: Make sure you have:

- a configured MXsecurity server
- an active IPS license that supports MXsecurity
- at least one Network Security Package uploaded. See Example: Updating the Network Security Package via MXsecurity for upload steps.

1. From the MXsecurity web console, go to **Management→Policy Profile**.
2. Click *[Add]*, and then configure:
    - **Profile Name**
    - **Description** (optional)
3. Select **IPS**, and then choose one of the **Package Versions** from the list.
4. Enable one or more IPS rules, then click **Apply**.

   You can choose **Select All** to enable all protection.

   Result: Your new policy profile is visible in the **Policy Profile** table.
5. To apply the profile, go to **Deployment→Policy Profile**.
6. Select the IPS profile, and then click **Apply**.

Results:

If an IPS event is triggered, you can go to **Logging→Firewall→IPS** to examine the events.

Example: Configuring IPS rules via WebGUI

Enable and configure IPS rules from device web interfaces.

Before you begin: Make sure you have:

- an active IPS license that supports device-based IPS

1. In the device UI, go to **Firewall→Advanced Protection→IPS**.
2. Identify rules to configure:

Choose from:

- Choose rules from the list
- Filter rules by clicking *[Filter]*
- Type search terms in the search box

3. Edit or enable rules by clicking *[Edit]*, then setting **Status** to **Enabled**.

You can toggle multiple rules by selecting them, and then clicking →**Quick Settings, and then setting Status to Enabled.**

Results: Selected rules will now be enabled.

What to do next: You can check the event log to verify to see actions taken by rules by going to **Diagnostics→Event Logs and Notifications→Event Log→Firewall Log.**

Introduction to Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Its primary function is to create a barrier between a private internal network and the public internet, allowing only authorized traffic to pass through and blocking unauthorized access attempts. They use various techniques to filter network traffic, including packet filtering, stateful inspection, and application filtering. Firewalls are an essential component of network security and are used by individuals, small businesses, and large enterprises to protect their networks from various types of cyber threats, such as viruses, malware, hackers, and other malicious attacks.

Stateful vs. Stateless firewalls

Firewalls can be categorized as either stateful or stateless.

Stateless firewalls, also known as packet filtering firewalls, examine individual packets of data and enforce rules based on information in the packet header, such as source and destination IP addresses or port numbers. Stateless firewalls do not keep track of the state of connections and cannot distinguish between packets belonging to different connections.

Stateful firewalls, on the other hand, keep track of the state of connections and use this information to enforce rules. They can distinguish between packets belonging to different connections and apply more complex security policies. Stateful firewalls maintain a state table that tracks information such as source and destination IP addresses, port numbers, and connection status.

Overall, stateful firewalls offer more advanced security features and are generally more effective at protecting networks from threats. However, they also require more resources and may be more complex to configure and manage. Stateless firewalls are simpler and more lightweight, but may not provide as much protection against advanced threats.

Categories of Firewall

- Policy (L2,L3~L7) : A policy in firewall function is a set of rules and criteria that are used to determine how traffic is allowed or denied on a network. Firewall policies define the actions that the firewall should take when specific traffic matches the defined criteria. Policies can be used to enact other kinds of filing, such as:
    - Physical Port Filtering: If unique VLANs are assigned to each port, and L3-7 policies are applied to each VLAN, this has the effect of applying policies to the physical port.
    - High-precision traffic control and QoS: Layer 3-7 policy can be configured to filter out unnecessary traffic, reducing bandwidth waste.
- Malformed packet: The Malformed Packets function enables the device to record event logs with a user-specified severity whenever malformed packets are dropped by the system.
- Session control: Session control in a firewall is the process of tracking and controlling the flow of network traffic between two endpoints in a network session.

Session control to help users protect backend hosts or services and avoid system abnormalities.

- DoS(Denial of Service) policy: The Industrial Secure Router provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. The Industrial Secure Router will drop packets when it either detects an abnormal packet format or identifies unusual traffic conditions.
- Protocol filter policy: The Industrial Secure Router supports industrial protocol filtering, allowing users to inspect network traffic based on specific protocols to detect anomalies and protect your network.

When to Use Firewalls

Firewalls are a fundamental component of network security and are used to protect networks from unauthorized access and cyber threats. It is a static system that filters traffic based on predefined rules, such as source/destination MAC, IP address or port.

- Prevent unauthorized access to critical assets: Firewalls are used to prevent unauthorized access to critical assets, such as a controller of a system, central monitor system.
- Safeguarding sensitive data: Firewalls are used to safeguard sensitive data such as financial information, healthcare records, and production data.
- Complying with regulations: Many industries are subject to regulations that require the use of firewalls to protect sensitive data.

In summary, firewalls are used to control traffic based on predefined rules and focus on access control. Firewalls are often used in combination with other network secure technique, like IPS (Intrusion Prevention System) to provide comprehensive protection against cyber threats.

Scenario: Airport Integrated Solutions

A network system provider is configuring a network for an airport.

Airports rely on intricate network systems to enhance efficiency, elevate safety measures, promote environmental sustainability, and reduce operational expenses.

Sub-Systems in an Airport Network:

A airport network system normally contains several sub-systems to facilitate transportation, such as:

- **Air Traffic Management System (ATMS)**: Orchestrates the safe and efficient movement of aircraft.
- **Airport Lighting Control and Monitoring System (ALCMS)**: Manages lighting information for approaches, runways, and taxiways.
- **Apron Docking Guide Systems**: Aids aircraft in safe and precise docking at the airport.
- **Apron Management System**: Supervises the activities on the airport apron area, ensuring smooth operations.

Interoperability and Security

For airports to function seamlessly, these sub-systems must intercommunicate while maintaining security against potential threats. The network should facilitate data sharing for regular flight operations while safeguarding critical systems against intrusions.

Moxa's Solution

Moxa's secure routers bolster this integration through policy-based firewalls. These policies, composed of specific rules, selectively permit or deny traffic among subsystems. For instance, designers can authorize control signals from ATMS to ALCMS, while excluding potentially disruptive traffic from other parts of the airport.

Allowlist Firewall Configuration

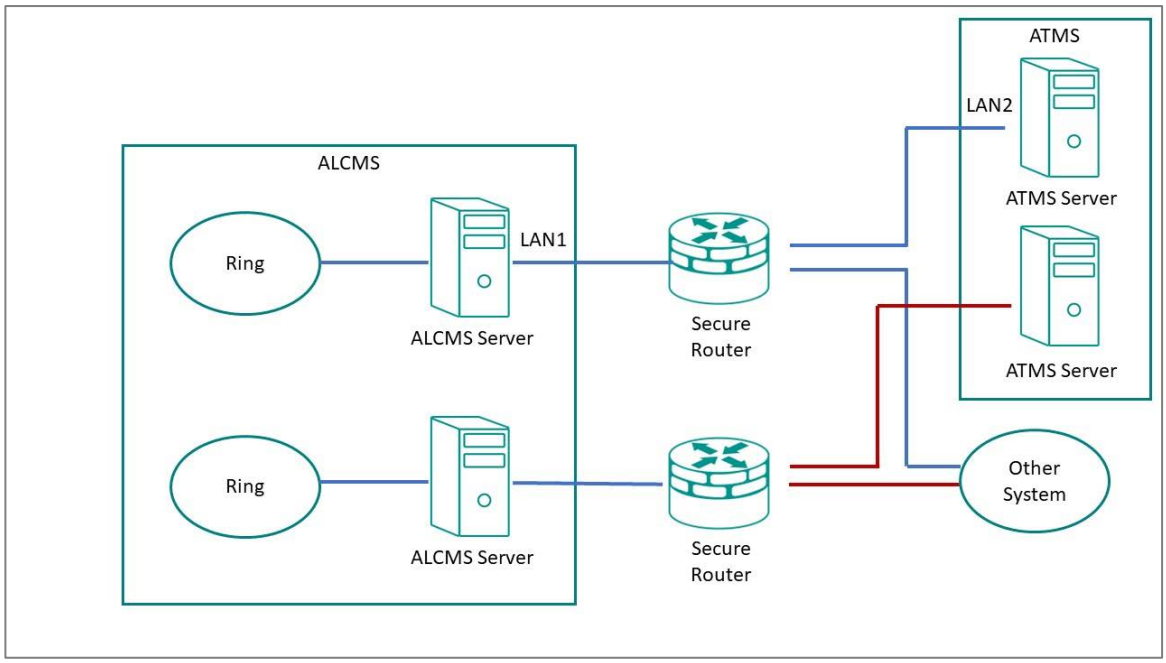
An allowlist is a network configuration that blocks all traffic except those specifically allowed.

Consider a scenario where the network designer employs dual networks for added redundancy. The firewall's rules can be fine-tuned to:

- Allow the ATMS server to communicate with the ALCMS.
- Reject all unrelated traffic and connections.

To achieve this, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.

Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, airports can achieve high levels of operational efficiency and safety.



Example: Allowing ATMS-ALCMS traffic

Create port filtering rules to allow traffic between the ATMS and ALCMS.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

> **Note**
>
> This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click ***[Add]***.

Result: The **Layer 3-7 Policy** creation panel appears.

2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	**LAN2** Refers to the ATMS server
Destination IP Address	**LAN1** Refers to the ALCMS server.

Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

Note

Layer 3-7 Policy rules represent a stateful firewall. This means that once the Source initiates traffic with Destination, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either Source or Destination may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

3. Click **Apply**.

What to do next: Add a policy rule to deny all other traffic to and from the ATMS and ALCMS. See Example: Configuring Blocked Traffic (Air)

Example: Configuring Blocked Traffic (Air)

Once you have specified "allowed" traffic, block all other traffic so that the ATMS and ALCMS systems will be effectively isolated from all other devices.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click ***[Add]***.

Result: The **Layer 3-7 Policy** creation panel appears.

2. In the **Action** field, select **Deny**.

3. In the **Filter Mode** field, select **IP and Port Filtering**.
4. Click **Apply**.
5. Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.

To reorder rules, click ***[Reorder Priorities]***

Results: Traffic between the ATMS and ALCMS systems will be permitted, but all other traffic to and from these systems will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the ATMS and ALCMS systems, effectively isolating them from this vector of attack.

What to do next:

Tip: Instead of configuring a "deny all" rule, you can configure a policy from **Global Policy Settings** to deny all traffic. To apply the policy:

1. Go to **Firewall →Layer 3-7 Policy**
2. Specify **Status** as **Enabled**.
3. Specify **Default Action** as **Deny All**.
4. Click **Apply**.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

Scenario: Railway Integrated Solutions

Short Description: A network system provider is configuring a network for a railway operator.

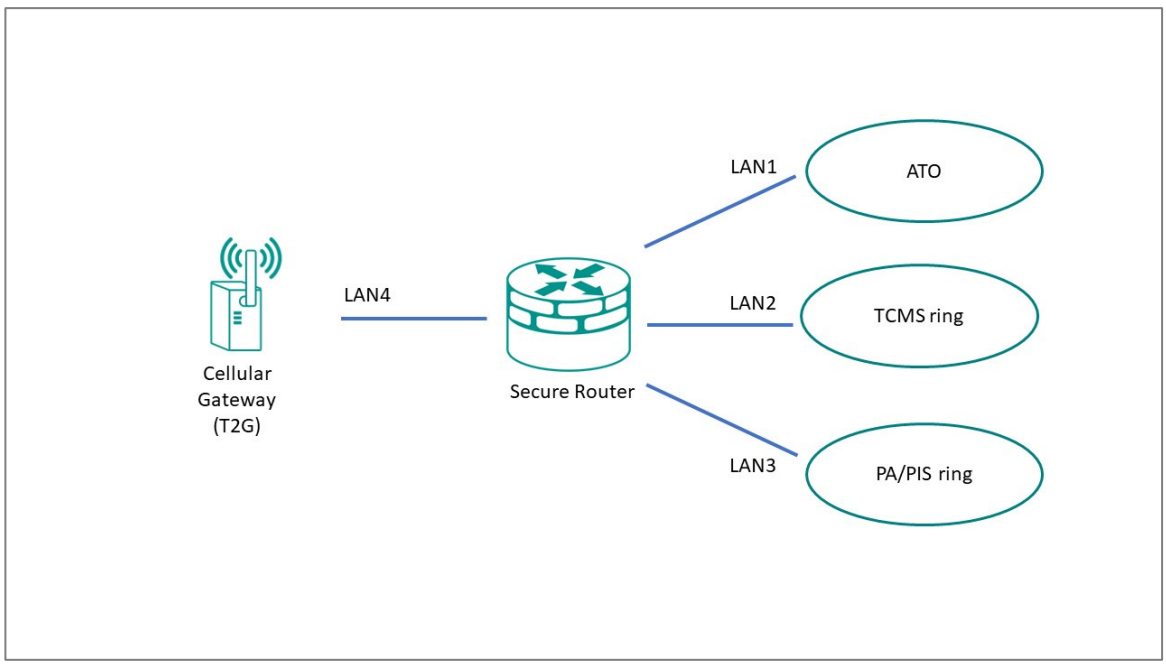
Understanding Railway Network Topology

A typical railway train network comprises multiple sub-systems working in tandem to ensure smooth operations. These sub-systems communicate crucial information, such as train speed, departure/arrival times, door status, climate control, lighting, and station updates to passengers.

Moxa's secure routers offer firewall functionality that allows seamless integration of these systems. By implementing policy-based firewall rules, these routers can permit authorized traffic and block unauthorized exchanges between the different sub-systems.

For instance, the train operating system might consist of various components:

- T2G system (usually a cellular gateway)
- ATO (Automatic Train Operation) system
- TCMS (Train Control and Management System) ring
- PA (Public Announcement system)/PIS (Public Information System) ring
- Control units for each of these systems



As an example scenario: a network designer might want configure the network such that the TCMS is the gatekeeper for all signals to the ATO, and prevent the ATO from talking to any other node on the network. We can achieve this kind of network isolation with an allowlist.

Allowlist Firewall Configuration

An allowlist is a network configuration that blocks all traffic except those specifically allowed.

To apply our example from above, the firewall's rules can be fine-tuned to:

- Allow the TCMS to access the ATO, PA/PIS, and Cellular Gateway.
- Allow the Cellular Gateway to access the TCMS and PA/PIS system.
- Reject all unrelated traffic and connections.

This configuration effectively isolates the ATO from the Cellular Gateway and PA/PIS.

To implement this configuration, set up one or more port filters to allow favorable traffic from recognized devices or ports. Then, set up a "deny all" rule to block any unspecified traffic, allowing the systems coexist securely on a shared network.

Integrating subsystems while preserving security and redundancy requires meticulous design and strategic solutions. With the right tools and approaches, operators can achieve high levels of operational efficiency and safety.

Example: Allowing TCMS traffic

Create port filtering rules to allow the TCMS to act as a gatekeeper for other devices on the network.

This procedure must be used in tandem with a correctly configured "deny all" policy to correctly implement an allowlist.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

> **Note**
> This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click ***[Add]***.

   Result: The **Layer 3-7 Policy** creation panel appears.

2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**

Item	Value
Source IP Address	LAN2 LAN2 should represent the IP address of the TCMS.
Destination IP Address	LAN1 LAN1 should represent the IP address of the ATO.

Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

Note

Layer 3-7 Policy rules represent a stateful firewall. This means that once the Source initiates traffic with Destination, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either Source or Destination may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

Tutorial Info: In this case, we will specifically create a bidirectional or "mirrored" rule for TCMS to Cellular Gateway traffic.

3. Create two more **Allow** rules.

Rule Purpose	Source IP	Destination IP
Allow TCMS to PA/PIS Traffic	LAN2	LAN3
Allow TCMS to Cellular Gateway Traffic	LAN2	LAN4

4. Click **Apply.**

Results: Rules have been created that will allow the TCMS to access all network nodes, allowing the TCMS to serve as a gatekeeper. Next, create a rule that will the allow the Cellular Gateway to access the TCMS and PA/PIS. Refer to Example: Allowing the T2G to access TCMS and PA/PIS for more information.

Example: Allowing the T2G to access TCMS and PA/PIS

Create port filtering rules to allow traffic from the Cellular Gateway to the TCMS and PA/PIS.

Before you begin: Make sure that network interfaces have already been configured with static IP addresses.

> **Note**
>
> This example of an allow list relies on fixed IP addresses. Ensure your network is configured accordingly. If the identified characteristics change, the settings will have to be updated.

1. Go to **Firewall →Layer 3-7 Policy**, and then click ***[Add]***.

   Result: The **Layer 3-7 Policy** creation panel appears.

2. Specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	LAN4 **LAN4** should represent the IP address of the Cellular Gateway.
Destination IP Address	LAN2 LAN2 should represent the IP address of the TCMS.

Tutorial Info: In this example, these settings identify the "allowed traffic" by IP address. This requires the IP address to be constant. When configuring in a production environment, make sure the characteristics you choose for your filter clearly distinguish trusted and untrusted network objects, such as IP address, protocol and port, or network interface.

> **Note**
>
> Layer 3-7 Policy rules represent a stateful firewall. This means that once the Source initiates traffic with Destination, two-way traffic will be allowed through the firewall because the firewall will remember the "state" of the connection. However, if there is a possibility that either Source or Destination may initiate the connection, it may be best to create separate "mirrored" rules to allow connections in both directions. Refer to Stateful vs. Stateless firewalls for more information.

3. To allow the Cellular Gateway to access the PA/PIS, specify all of the following:

Item	Value
Action	**Allow**
Filter Mode	**IP and Port Filtering**
Source IP Address	LAN4 LAN4 should represent the IP address of the Cellular Gateway.
Destination IP Address	LAN3 LAN3 should represent the IP address of the PA/PIS.

4. Click **Apply**.

Results: Rules have been created that will allow the Cellular Gateway to access the TCMS and PA/PIS.

What to do next: Add a policy rule to block all other traffic. Refer to Example: Configuring Blocked Traffic (Rail) for more information.

Example: Configuring Blocked Traffic (Rail)

Once you have specified "allowed" traffic, block all other traffic so that the ATO will be effectively isolated from all other devices, relying on the TCMS as a gatekeeper.

1. Go to **Firewall** →**Layer 3-7 Policy**, and then click

[Add].

Result: The **Layer 3-7 Policy** creation panel appears.

2. In the **Action** field, select **Deny**.
3. In the **Filter Mode** field, select **IP and Port Filtering**.
4. Click **Apply**.
5. Make sure that the "deny all" rule is the last rule on the list, otherwise this rule may override the allow rules.

To reorder rules, click

[Reorder Priorities]

Results: The TCMS will be able to access all network devices, and the Cellular Gateway will be able to access the TCMS and PA/PIS, but all other traffic will be blocked, effectively isolating these systems from other devices on the network. This helps make sure that even if other systems on the network are compromised, no traffic from these systems will reach the specified systems, effectively isolating them from this vector of attack.

Note

Instead of configuring a "deny all" rule, you can configure a policy from Global Policy Settings to deny all traffic. To apply the policy,

1. Go to Firewall →Layer 3-7 Policy
2. Specify Status as Enabled.
3. Specify Default Action as Deny All.
4. Click Apply.

Specific rules override generalized policies, effectively making the policy the last rule on the list.

Security Standards and Concepts

AAA

About AAA - Authentication, Authorization, and Accounting

Authentication, **A**uthorization, and **A**ccounting (AAA) is a user-based access control paradigm.

AAA coexists with other security practices. While product security and network security focus on device or process security, AAA focuses on users.

AAA comprises a set of functions for an administrator to determine which users can access a network device, which services are available to authorized users, and collect information about user activities for audits or charging purposes if required. When implemented well, AAA can provide an extra layer of security across different aspects.

Authentication

Authentication provides a method of identifying a user before access to the network device is granted, typically by having the user enter a valid username and password and/or provide a physical token or digital certificate. Additional policies such as a password complexity check or login failure lockout can also increase access security.

Authorization

After authentication is successful, a user can be authorized to use specific resources on the device or perform specific operations. For instance, a normal user with limited permissions may only view the device's system settings, whereas an administrator would have full control to view or edit all system settings.

Accounting

Accounting keeps track of user activities on the device. It monitors the resources a user consumes during network access. This can include the amount of data sent and received through an Ethernet port or the number of user login failures.

About Authentication Types

Handle authentication with the local device exclusively, or with a remote server using local accounts only as a fallback.

It is important to choose the right authentication method, or combination of authentication methods for your network environment and use case. Moxa devices offer the following authentication options.

Local Authentication

Local authentication uses the accounts and settings stored on the local network device to identify users (authentication), determine which services they can use (authorization), and track basic user activities such as amount of data transferred or number of login failures (accounting).

Remote Authentication

Remote authentication uses accounts configured on a RADIUS server - allowing AAA to be configured from a single, centralized location. However, it is important to note that local authentication is retained as a fallback mechanism to ensure the device can be configured if the RADIUS server becomes inaccessible. Additionally, Moxa products support backup RADIUS servers if the primary becomes inaccessible. Due consideration should be given to the configuration and maintenance of backup servers for redundancy.

Local vs. Remote Authentication Feature Comparison

Features	Local	Remote
Configuration location	Local device	Remote RADIUS server, local as fallback
Number of accounts	Few	Many

Features	Local	Remote
Password security requirements	Limited	Many
Allowed services*	Specified locally	Determined by server
Authority types	Admin, User, Supervisor	Admin, User
User feedback on failed login	Custom prompt	Server-defined
Setup effort	Low	High

*Allowed services are usually dependent on Authority types.

Example: Creating a Local User

Local accounts are authenticated and managed by the local device, and function even when remote RADIUS servers are unavailable.

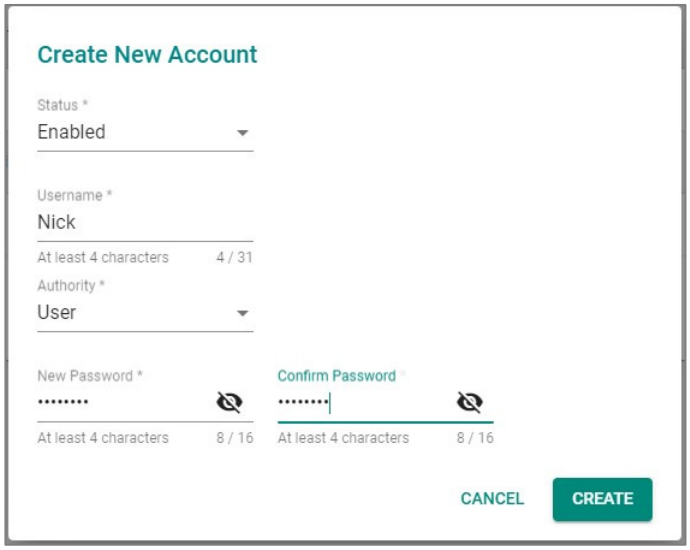
Before you begin: Make sure you have an account with **Admin** authority.

In this example, create a local user with simple **User** level authority to fill the Authentication of the AAA tripod. Once the user has been created, add additional access controls.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **System→Account Management→User Accounts**, and then click the plus icon.

   Result: The **Create New Account** panel appears.
3. Set **Status** to **Enabled**.
4. In the **Username** field, type `Nick`.
5. Set **Authority** as **User**.
6. In the **New Password** field, type `1qaz!@#$`, and then type again to confirm.
7. Click **Create**.

Results: By creating the user **Nick**, Authorization and Accounting details can now be configured.



What to do next: Now that a user account has been created, add account controls. Account controls allow setting a warning for incorrect passwords, account lockouts, and automatic logout. For details, see Example: Configuring Account Controls for Local Users.

Example: Configuring Account Controls for Local Users

Login Failure Account Lockout and Auto Logout increase the security of local accounts.

Enabling additional account controls can increase resistance to brute-force attacks as well as enable troubleshooting. This example demonstrates how to set account lockouts after failed login attempts and manage idle users.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **Security→Device Security→Login Policy**.

   Result: The **Login Policy** panel appears.
3. In the **Login Authentication Failure Message** field, type `Warning! The account will be temporarily locked if there are too many consecutive login failures.`
4. Set **Login Failure Account Lockout** to **Enabled**.
5. In the **Login Failure Retry Threshold** field, type 3.

   This is the number of failed attempts before the user account will be temporarily blocked.

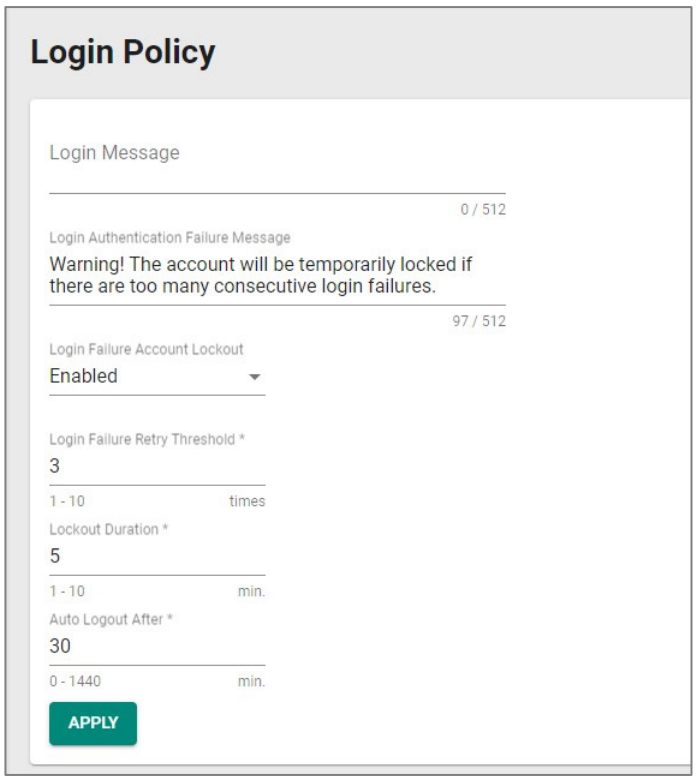
Temporary bans can help prevent password guessing and brute force attacks by preventing attackers from rapidly guessing many passwords.

6. In the **Lockout Duration** field, type `5`.

This specifies the number of minutes the account will be locked.

7. In the **Auto Lockout After** field, type `30`.

This is the amount of time in minutes before inactive accounts automatically log out.



Results: This configuration:

- Displays a warning message on failed login attempts, enabling troubleshooting
- Blocks accounts for five minutes after three unsuccessful login attempts, limiting the effectiveness of credential guessing
- Automatically logs out inactive user accounts after thirty minutes, reducing risks of unauthorized access through idle consoles

What to do next: Optionally, configure allowed access protocols. For details, see User Interface.

Example: Configuring a Remote RADIUS Server

In this example, the RADIUS server handles all Authentication, Authorization, and Accounting.

Before you begin:

- Make sure you have a working RADIUS server and corresponding configuration information. In our example, we use a server that has the following settings:
    - **PAP** authentication protocol
    - An address of 192.168.127.1
    - UDP port 1812
    - A preconfigured shared key

Remote Authentication Dial-In User Service (RADIUS) servers may make it easier to manage large numbers of users from a central location.

1. Using an account with **Admin** authority, log in to the network device.
2. Go to **Security→Authentication→Login Authentication**, and then set **Authentication Protocol** to **RADIUS, Local**.

   Tutorial Info: This setting will use the remote RADIUS server as the primary authentication source, and use local authentication as a fallback if the RADIUS server is unavailable.

> **Note**
> Enabling RADIUS authentication will not remove local accounts. Make sure local accounts have a strong, unique password. Local accounts are still required both for RADIUS server configuration as well as for local fallback if the RADIUS server is not reachable. For details, see Example: Creating a Local User.

3. Go to **Security→Authentication→RADIUS**.

   Result: The **RADIUS Server** will appear.

4. Configure all of the following:

Field	Setting
Authentication Type	**PAP**
Server Address 1	192.168.127.1

Field	Setting
UDP Port	1812
Shared Key	Enter your Shared Key here.

Tutorial Info: These configuration options are provided as an example only, and will need to match your network environment.

5. Click **Apply**.

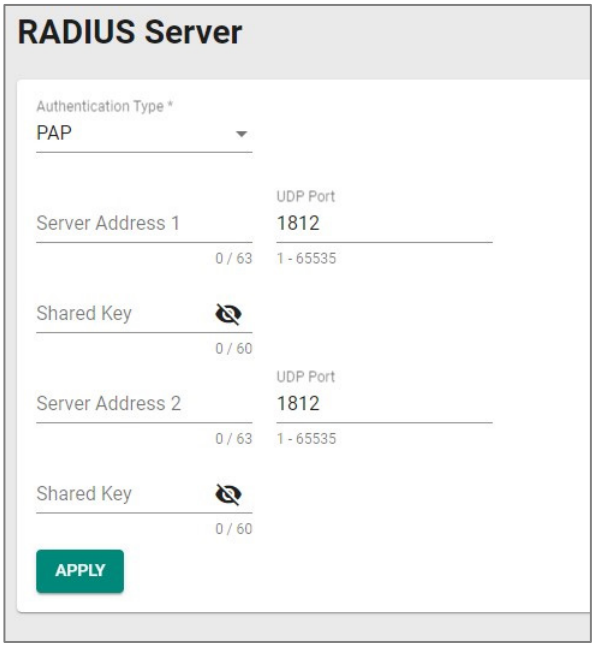
Results:

By configuring remote authentication, the network device will redirect user login requests to the RADIUS server. When logging in with remote user `Peter`, the RADIUS server will process the authentication request and determine whether to grant access to the device. If `Peter` does not match RADIUS or Local information, access will be denied.

In situations where the RADIUS server is not reachable or unavailable, users such as `Nick` (created in Example: Creating a Local User or other existing local users can still access the network device using their local passwords.

Note

If RADIUS is enabled, but unreachable, network-based logins (HTTP/HTTPS/Telnet/SSH) will not be possible, and users will be limited to logins through the console port only.

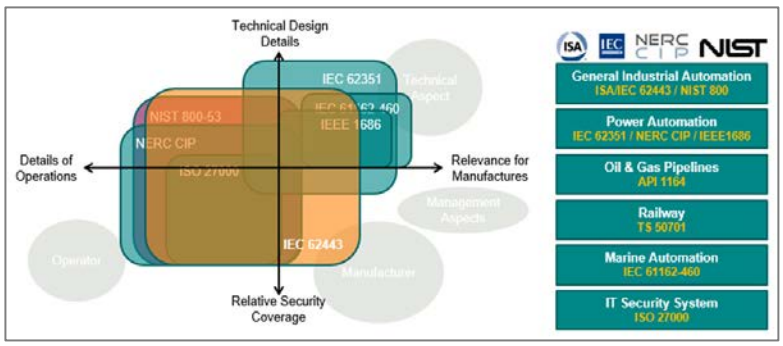


ISA / IEC 62443 Standards and Architecture

Security Reference Standards

In the field, large networks are connected through switches and routers. These devices manage all data traffic and serve as the main bridge between devices. However, if these switches and routers are compromised, the repercussions can cascade to all connected devices. To help mitigate this risk, Moxa implements the ISA/IEC 62443-4-2 standard into our network device designs.

Security Standards and Vertical Markets



Industries such as electricity, oil and gas, rail transportation, and maritime have established their own standards for security. These standards include guidelines and regulations designed to address each industry's unique concerns. Among these standards, 62443 is the most comprehensive, covering a wide range of industries and security concerns, making it an excellent choice for organizations that prioritize security in their operations.

ISA/IEC 62443 Standards and Architecture

The ISA/IEC 62443 standard is a set of guidelines and best practices designed to help organizations secure their industrial automation and control systems (IACS) against cyber threats. The framework helps assess risks to IACS and implement appropriate security measures to protect against cyber attacks and malware. The standard consists of multiple parts, with each covering different aspects of industrial cybersecurity.

Breakdown of ISA/IEC 62443

Parts of ISA/IEC 62443	Scope	Sections
ISA/IEC 62443-1	General	Part 1-1: Terminology, concepts, and models Part 1-2: Master glossary of terms and abbreviations Part 1-3: System security compliance metrics Part 1-4: IACS security life cycle and use-cases
ISA/IEC 62443-2	Process and Program requirements	Part 2-1: Establishing an industrial automation and control system security program Part 2-2: Implementation guidance for an IACS security management system Part 2-3: Patch management in the IACS environment Part 2-4: Security program requirements for IACS service providers
ISA/IEC 62443-3	Systems	Part 3-1: Security technologies for industrial automation and control systems Part 3-2: Security risk assessment and system design Part 3-3: System security requirements and security levels
ISA/IEC 62443-4	Components	Part 4-1: Secure product development lifecycle requirements Part 4-2: Technical security requirements for IACS components

Product suppliers adhere to the ISA/IEC 62443 standard to provide components for Industrial Automation and Control System (IACS) solutions. These components can be:

- Individual items
- Combined products forming a system or subsystem

Additionally, system integrators use the following sections of the ISA/IEC 62443 standard:

- IEC 62443-2-1
- IEC 62443-2-4
- IEC 62443-3-2
- IEC 62443-3-3

These standards help integrators:

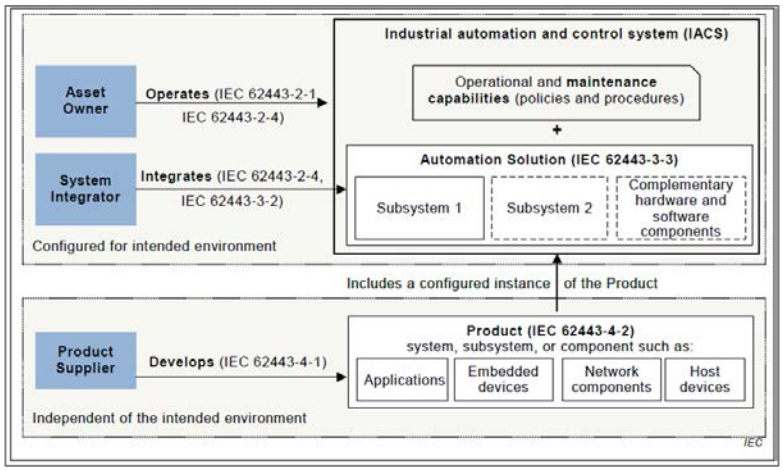
- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

Key Parts of ISA/IEC 62443 Standard

Parts of the ISA/IEC 62443 Standard	Technical Security Requirements
General **ISA/IEC 62443-1**	ISA-/IEC 62443-1-1 Foundational Requirements (FR)
System **ISA/IEC 62443-3**	ISA-/IEC 62443-3-3 System Requirements (SR)
Component **ISA/IEC 62443-4**	ISA-/IEC 62443-4-2 Component Requirements (CR)

Once the solution is ready, it's installed on-site, becoming a vital part of the IACS.

Summary of IEC 62443 Stakeholders



Establishing Foundational Requirements

ISA/IEC 62443-1-1 Foundational Requirements (FR)

FR 1	Identification and Authentication Control
FR 2	User Control
FR 3	System Integrity
FR 4	Data Confidentiality
FR 5	Restricted Data Flow
FR 6	Timely Response to Events
FR 7	Resource Availability

Once an organization settles on target security levels, foundational requirements can help further specify requirements based on the seven foundational security functions (FRs). The ISA/IEC 62443 framework includes:

- **System Requirements (SRs)**: Detailed in Part 3-3, these are guidelines for those shaping the system's overall architecture.
- **Component Requirements (CRs)**: Outlined in Part 4-2, they cater to designers focusing on individual components.

Both system and component designers reference these standards, ensuring the final product's security aligns with what the asset owner's requirements. This methodology not

only bolsters the product's defense against specific threat levels but also optimizes resource utilization among stakeholders. As a side note, every FR from Part 1-1 is paired with four distinct security levels, which trace back to standards set in Parts 3-3 and 4-2. For simplicity in cross-referencing, CRs are numerically aligned with their corresponding SRs.

Component Requirements

Part 4-2 extends the SRs from Part 3-3 by introducing CRs tailored for a variety of IACS components.

These components fall under four broad categories of SRs:

- Software Applications
- Embedded Devices
- Host Devices
- Network Devices

While a majority of Part 4-2's criteria are generic and apply uniformly across categories, there are exceptions. Unique, component-specific stipulations are clearly signposted, with exhaustive details available in dedicated clauses. For details, consult the original standards.

Requirement Enhancements

CRs may contain one or more requirement enhancements (RE). REs are additional requirements attached to CRs that add additional conditions to accommodate higher security levels.

FR 1 Applications: User Identification and Authentication

FR 1 codifies the principle that all users—humans, software processes, or devices—must first be identified and authenticated before accessing the system or assets.

Recognizing the need to verify different kinds of users, FR 1 uses the following CRs:

- **CR 1.1** focuses on human users.
- **CR 1.2** addresses software processes and devices.

Identification vs. Authentication: Consider a person's ID card. While the card identifies its owner, can someone else misuse it? Certainly. Here, the distinction between 'identifying' (matching a person to an ID card) and 'authenticating' (confirming the card holder's authenticity) becomes crucial. Each process has distinct methods and requirements.

Understanding CR and RE in Determining Security Levels: CR represents foundational requirements, whereas RE accounts for advanced needs. Together, they define the security capacity of a component. Each component's security level, according to FR, ranges from 0 (no requirements) to 4.

For instance:

- **Security Level 1**: Implementing basic identification and authentication for all human users.
- **Security Level 2**: Incorporates RE1 - uniquely identify and authenticate users, like using ID cards for employees.
- **Security Level 3**: Engages RE2 - multifactor authentication.

Multifactor Authentication Unraveled: Typically, this methodology hinges on:

1. **Knowledge**: Passwords or PINs.
2. **Possession**: Devices like smartphones or security keys.
3. **Inherence**: Biometrics such as fingerprints.

To achieve Level 3, a combination of at least two of these factors is essential.

Security Levels (SLs) and Attack Types

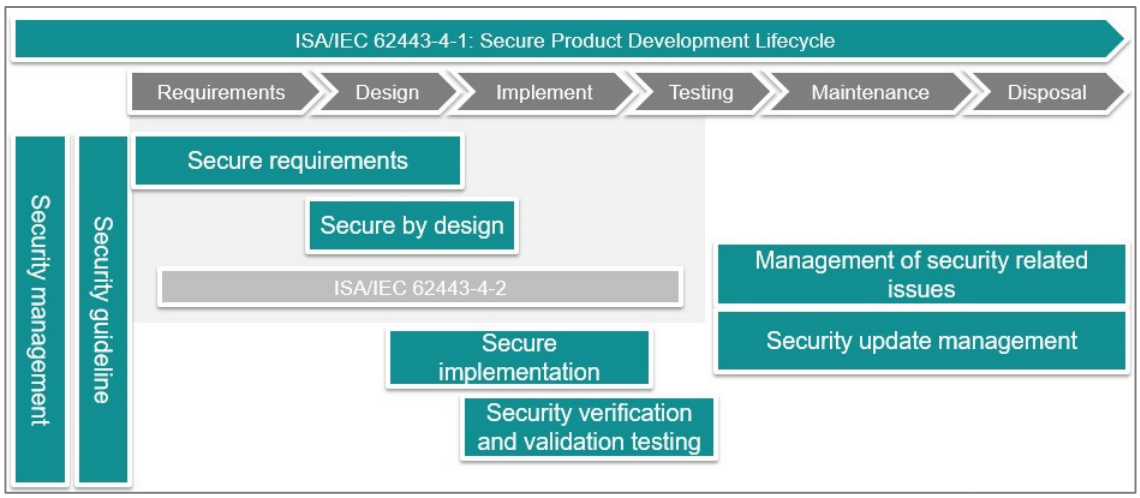
Security Level	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-1	• Ordinary user	Coincidental	N/A	N/A	N/A
SL-2	• Entry-level hacker	Intentional	Simple	Low	Low
SL-3	• Terrorist Organization • Organized crime	Intentional	Sophisticated	Moderate	Moderate
SL-4	• Nation state	Intentional	Sophisticated	Extended	High

For more information about CRs, SLs, and REs, refer to the ISA/IEC 62443 standard.

Product Lifecycle and Security

Component security plays a role throughout the product lifecycle.

Moxa's Application of ISA / IEC 62443-4-1



How Moxa applies ISA / IEC 62443-4-1

Our commitment to security includes to adhering to the ISA/IEC 62443-4-1 standard, considering security at each stage of the product's lifecycle. This includes the safeguarding of our corporate network, keys, secure design and implementation proficiencies, testing processes, and post-sales services. Our approach involves extensive training and certification of all team members associated with product design, execution, and assistance. Moreover, we offer robust support mechanisms like vulnerability handling and patch management.

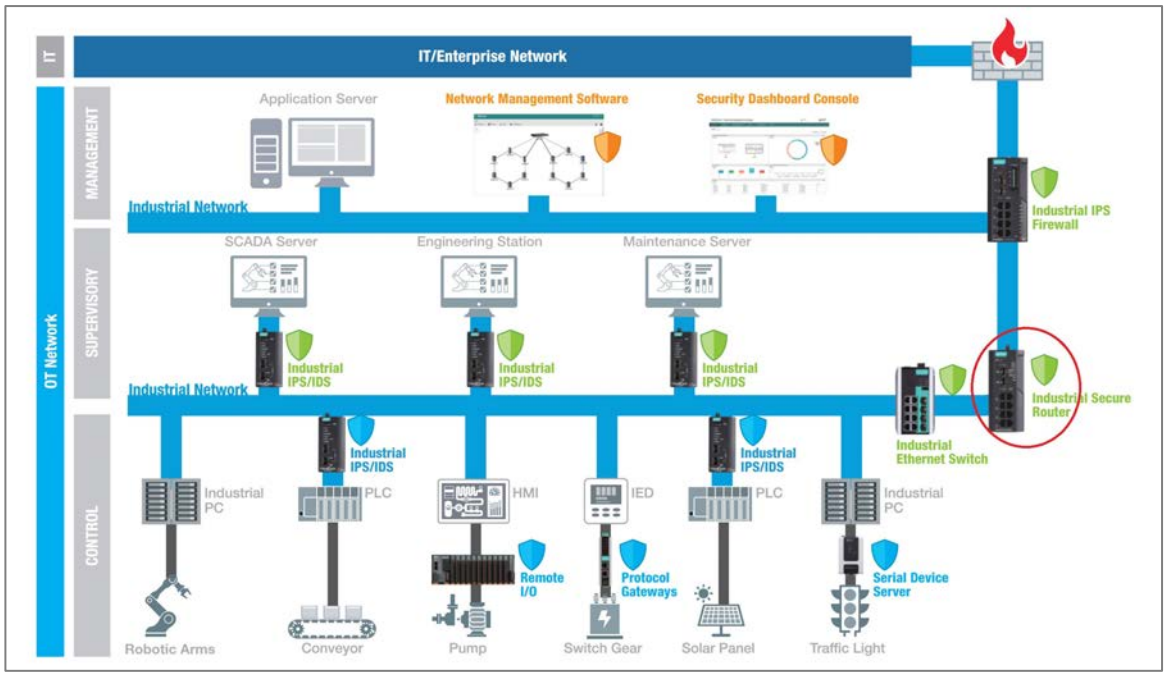
Component Security with IEC 62443-4-2

IEC 62443-4-2 serves as a guide for product suppliers, helping us decipher the specific security capability benchmarks for control system components. This standard not only clarifies which requirements should be assigned but also pinpoints those that must be integral to the components. The fusion of these component requirements with their enhancement requirements defines the component's target security level.

Product Security Context

Security context describes a product's role in a network and the security features of its environment.

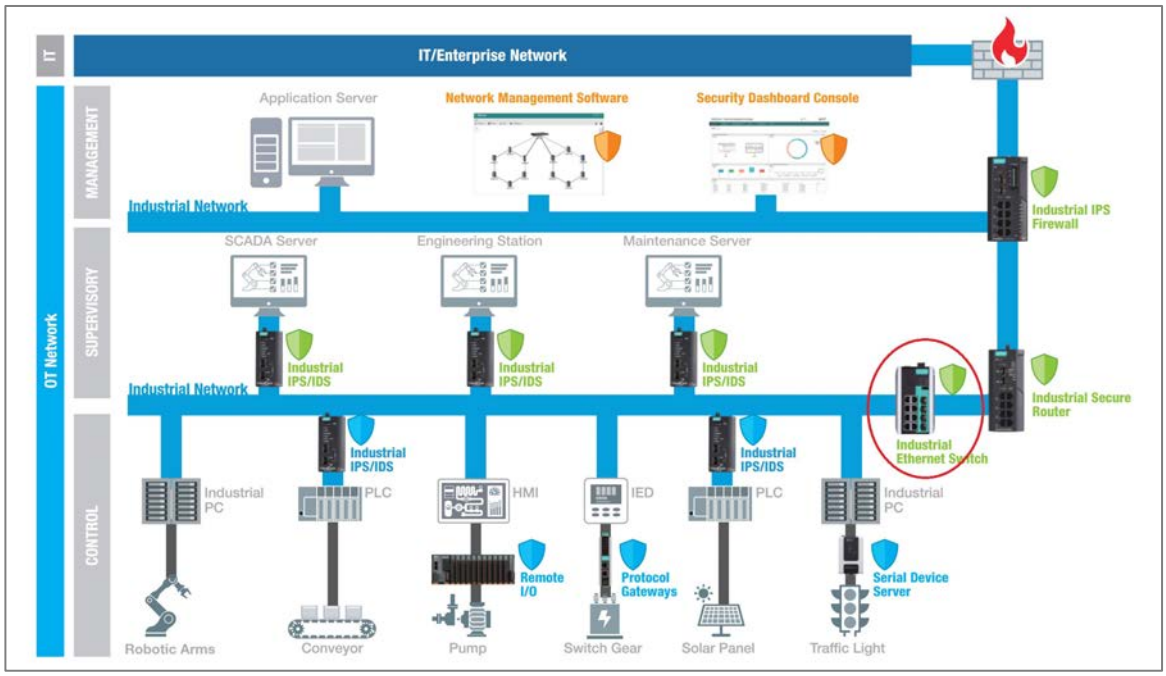
Security Context of an Industrial Secure Router



A secure router is a router with security features. Unlike a firewall—which exclusively filters and controls traffic—a secure router also monitors connections between devices. Secure routers have additional security features such as intrusion detection/prevention systems (IDS/IPS), virtual private network (VPN) support, and advanced encryption capabilities.

Secure router Intrusion Detection Systems (IDS) can be deployed behind the firewall for a defense-in-depth approach, increasing detection of attacks bypassing first-layer firewalls.

Security Context of an Industrial Ethernet Switch



Switches with enhanced security features such as access control lists (ACLs), VLAN support, and support for secure communication protocols, in conjunction with other security measures, can help create a more robust and resilient network.

ACLs and VLANs can help isolate devices on the same physical or logical network segments. This isolation adds further security to minimize or mitigate the effects of an attack.

Chapter 8

Appendix

All Settings for Example Scenario: 2 Consists with 1 ETBN/ECSP Each

All Settings for Example Scenario: 2 Consists with 2 Redundant ETBN routers

Consist	Consist 1	Consist 2
ETBN Router	ETBN Router 1	ETBN Router 1
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.	
Consist UUID	00000000-0000-0000-0000-000000000001	00000000-0000-0000-0000-000000000002
	The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.	
ETBN(s) in Consist	**1** Dictated by our sample topology.	
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.	
Local ETBN Static ID	**1** Identifies the ETBN when there are multiple ETBNs in the same consist.	
ECN interface IP address	10.0.0.1 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.	
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.	
Direction 2	**Trunk 2**	

Consist	Consist 1	Consist 2
ETB Port Speed	Auto	
ECN Port VLAN ID	1000 Defines the VLAN ID of the ETB interface. The TTDP function will generate the corresponding ETB and ECN interface.	
ECN to ETBN	**ETBN 1**	
ECN interface IP address	10.0.0.1 Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.	
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.	

All Settings for Example Scenario: 2 Consists with 2 Redundant ETBN Routers Each

All Settings for Example Scenario: 2 Consists with 2 Redundant ETBN routers

Consist	Consist 1		Consist 2	
ETBN Router	ETBN Router 1	ETBN Router 2	ETBN Router 1	ETBN Router 2
ETB Backbone ID	**0** This field identifies the type of traffic carried by the ETB, and should be the same within the same ETB. Since both ETBNs are in the same ETB, their ETB backbone IDs are the same.			
Consist UUID	00000000-0000-0000-0000-000000000001		00000000-0000-0000-0000-000000000002	
	The UUID is the same within the same consist. The example UUID is manually assigned, but they can also be randomly generated.			
ETBN(s) in Consist	**2** Dictated by our sample topology.			
ECN(s) in Consist	**1** Multi-application consists might have additional ECNs to support additional applications - such as having both TCMS and Media - but our example is limited to 1 for now.			
Local ETBN Static ID	**1**	**2**	**1**	**2**
	Identifies the ETBN when there are multiple ETBNs in the same consist.			
Direction 1	**Trunk 1** In TN-4908, port 1,2 will be set as trunk 1, and port 5,6 will be set as trunk 2. Important: The direction of all ETBNs in the same consist should be the same.			
Direction 2	**Trunk 2**			
ETB Port Speed	Auto			
ECN Port VLAN ID	1001			

Consist	Consist 1		Consist 2	
ECN interface IP address	10.0.0.1	10.0.0.2	10.0.0.1	10.0.0.2
	Defines the IP of the ECN interface. Devices in the ECN network can access the ETBN using the ECN interface IP. Use caution when setting this as the default gateway. Because this example uses redundant ETBNs, if the primary ETBN fails and the backup takes over, the gateway IP address changes. You can avoid disruptions to cross-consist communication by leveraging VRRP. Refer to Redundancy > Layer 3 Redundancy > VRRP for more information about VRRP.			
ECN Ports	**port3**, **port4**, **port7**, and **port8** The field is to define which ports on the TN-4900 are the ECN ports. These selected ports will be assigned to the ECN interface.			

CIP Object List

This is a list of CIP object classes and names.

Class ID	Name
0x01	Identity Object
0x02	Message Router Object
0x03	DeviceNet Object
0x04	Assembly Object
0x05	Connection Object
0x06	Connection Manager Object
0x07	Register Object
0x08	Discrete Input Point Object
0x09	Discrete Output Point Object
0x0a	Analog Input Point Object
0x0b	Analog Output Point Object
0x0e	Presence Sensing Object
0x0f	Parameter Object
0x10	Parameter Group Object
0x12	Group Object
0x1d	Discrete Input Group Object
0x1e	Discrete Output Group Object
0x1f	Discrete Group Object
0x20	Analog Input Group Object
0x21	Analog Output Group Object

Class ID	Name
0x22	Analog Group Object
0x23	Position Sensor Object
0x24	Position Controller Supervisor Object
0x25	Position Controller Object
0x26	Block Sequencer Object
0x27	Command Block Object
0x28	Motor Data Object
0x29	Control Supervisor Object
0x2a	AC/DC Drive Object
0x2b	Acknowledge Handler Object
0x2c	Overload Object
0x2d	Softstart Object
0x2e	Selection Object
0x30	S-Device Supervisor Object
0x31	S-Analog Sensor Object
0x32	S-Analog Actuator Object
0x33	S-Single Stage Controller Object
0x34	S-Gas Calibration Object
0x35	Trip Point Object
0x37	File Object
0x38	S-Partial Pressure Object
0x39	Safety Supervisor Object
0x3a	Safety Validator Object

Class ID	Name
0x3b	Safety Discrete Output Point Object
0x3c	Safety Discrete Output Group Object
0x3d	Safety Discrete Input Point Object
0x3e	Safety Discrete Input Group Object
0x3f	Safety Dual Channel Output Object
0x40	S-Sensor Calibration Object
0x41	Event Log Object
0x42	Motion Device Axis Object
0x43	Time Sync Object
0x44	Modbus Object
0x45	Originator Connection List Object
0x46	Modbus Serial Link Object
0x47	Device Level Ring (DLR) Object
0x48	QoS Object
0x49	Safety Analog Input Point Object
0x4a	Safety Analog Input Group Object
0x4b	Safety Dual Channel Analog Input Object
0x4c	SERCOS III Link Object
0x4d	Target Connection List Object
0x4e	Base Energy Object
0x4f	Electrical Energy Object
0x50	Non-Electrical Energy Object
0x51	Base Switch Object

Class ID	Name
0x52	SNMP Object
0x53	Power Management Object
0x54	RSTP Bridge Object
0x55	RSTP Port Object
0x56	PRP/HSR Protocol Object
0x57	PRP/HSR Nodes Table Object
0x58	Safety Feedback Object
0x59	Safety Dual Channel Feedback Object
0x5a	Safety Stop Functions Object
0x5b	Safety Limit Functions Object
0x5c	Power Curtailment Object
0x5d	CIP Security Object
0x5e	EtherNet/IP Security Object
0x5f	Certificate Management Object
0x60	Authority Object
0x61	Password Authenticator Object
0x62	Certificate Authenticator Object
0xf0	ControlNet Object
0xf1	ControlNet Keeper Object
0xf2	ControlNet Scheduling Object
0xf3	Connection Configuration Object
0xf4	Port Object
0xf5	TCP/IP Interface Object

Class ID	Name
0xf6	Ethernet Link Object
0xf7	CompoNet Link Object
0xf8	CompoNet Repeater Object
0xf9	HART Master Port Object
0xfa	I/O Aggregation Object
0x100	Protection Trip Object
0x101	Protection Alarm Object
0x102	Circuit Breaker Supervisor Object
0x103	Circuit Breaker Statistics Object
0x104	Electrical Demand Object
0x105	Electrical Statistics Object
0x106	Machine Base Data Object
0x107	HART Process Device Object
0x108	Process Device Diagnostics Object
0x109	LLDP Management Object
0x10a	LLDP Data Table Object
0x10b	IO-Link Service Parameter Objct
0x10c	IO-Link Master PHY Object
0x10d	IO-Link Device PHY Object
0x10e	Pilot Light Supervisor Object
0x10f	Select Line Link Object
0x110	In-Cabinet Actual Topologg Object
0x111	In-Cabinet Commissioning Object

Destination Ports for Layer 3 – 7 Protocol

Network Service
Remote-Access
Remote-Desktop
Email
File-Transfer
Web-Access
Network-Service
Authentication
VOIP-and-Streaming
SQL-Server

Industrial Application Service
Modbus
DNP3
IEC-60870-5-104
IEC-61850-MMS
OPC-DA
OPC-UA
CIP-EtherNet/IP
Siemens-Step7
Moxa-RealCOM

Industrial Application Service
moxa-MXview-Request

Ethernet Protocol Default Ports

This table shows the default ports used for various Ethernet protocols.

Ethernet Protocol	Port Number
DNP3 (TCP)	20000
DNP3 (UDP)	20000
Ethercat (TCP)	34980
Ethercat (UDP)	34980
EtherNet/IP I/O (TCP)	2222
EtherNet/IP I/O (UDP)	2222
EtherNet/IP messaging (TCP)	44818
EtherNet/IP messaging (UDP)	44818
FF Annunciation (TCP)	1089
FF Annunciation (UDP)	1089
FF Fieldbus Message Specification (TCP)	1090
FF Fieldbus Message Specification (UDP)	1090
FF LAN Redundancy Port (TCP)	3622
FF LAN Redundancy Port (UDP)	3622
FF System Management (TCP)	1091
FF System Management (TCP)	1091
FTP-control (TCP)	21
FTP-control (UDP)	21
FTP-data (TCP)	20
FTP-data (UDP)	20

Ethernet Protocol	Port Number
HTTP (TCP)	80
HTTP (UDP)	80
IEC 60870-5-104 process control over IP (TCP)	2404
IEC 60870-5-104 process control over IP (UDP)	2404
IPsec (TCP)	1293
IPsec (UDP)	1293
IPsec NAT-Traversal (TCP)	4500
IPsec NAT-Traversal (UDP)	4500
L2TP (TCP)	1701
L2TP (UDP)	1701
LonWorks (TCP)	2540
LonWorks (UDP)	2540
LonWorks2 (TCP)	2540
LonWorks2 (UDP)	2540
Modbus TCP/IP (TCP)	502
Modbus TCP/IP (UDP)	502
PPTP (TCP)	1723
PPTP (UDP)	1723
PROFInet Context Manager (TCP)	34964
PROFInet Context Manager (UDP)	34964
PROFInet RT Multicast (TCP)	34963
PROFInet RT Multicast (UDP)	34963
PROFInet RT Unicast (TCP)	34962

Ethernet Protocol	Port Number
PROFInet RT Unicast (UDP)	34962
RADIUS (TCP)	1812
RADIUS (UDP)	1812
RADIUS Accounting (TCP)	1813
RADIUS Accounting (UDP)	1813
SSH (TCP)	22
SSH (UDP)	22
Telnet (TCP)	23
Telnet (UDP)	23

EtherTypes for Layer 2

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

EtherType Value (Hexadecimal)	Layer 2 Protocol
0x0800	IPv4 (Internet Protocol version 4)
0x0805	X25
0x0806	ARP (Address Resolution Protocol)
0x0808	Frame Relay ARP
0x08FF	G8BPQ AX.25 Ethernet Packet
0x6000	DEC Assigned proto
0x6001	DEC DNA Dump/Load
0x6002	DEC DNA Remote Console
0x6003	DEC DNA Routing
0x6004	DEC LAT
0x6005	DEC Diagnostics
0x6006	DEC Customer use
0x6007	DEC Systems Comms Arch
0x6558	Trans Ether Bridging
0x6559	Raw Frame Relay
0x80F3	Appletalk AARP
0x809B	Appletalk
0x8100	8021Q VLAN tagged frame
0x8137	Novell IPX
0x8191	NetBEUI

EtherType Value (Hexadecimal)	Layer 2 Protocol
0x86DD	IP version 6 (Internet Protocol version 6)
0x880B	PPP
0x884C	MultiProtocol over ATM
0x8863	PPPoE discovery messages
0x8864	PPPoE session messages
0x8884	Frame-based ATM Transport over Ethernet
0x9000	Loopback

Fiber Check Threshold Values for Auto Mode

This table shows the default thresholds for temperature, Tx power, and Rx power for Moxa fiber modules.

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
FEMST	120	-20	-14	-32.0	-3.0
FEMSC	120	-20	-14	-32.0	-3.0
FESSC	120	-5.0	0.0	-34.0	-3.0
SFP-1FEMLC-T	120	-18.0	-8.0	-32.0	-3.0
SFP-1FESLC-T	120	-5.0	0.0	-34.0	-3.0
SFP-1FELLC-T	120	-5.0	0.0	-34.0	-3.0
SFP-1GSXLC-T	110	-9.5	-4.0	-18.0	0.0
SFP-1GLSXLC-T	120	-9.0	-1.0	-19.0	-1.0
SFP-1GLXLC-T	120	-9.0	-3.0	-21.0	-3.0
SFP-1GLHLC-T	120	-8.0	-3.0	-23.0	-3.0
SFP-1GLHXLC-T	120	-4.0	3.0	-24.0	-1.0
SFP-1GZXLC-T	120	0.0	5.0	-24.0	-1.0
SFP-1G10ALC-T	120	-9.0	-3.0	-21.0	-3.0

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
SFP-1G10BLC-T	120	-9.0	-3.0	-21.0	-3.0
SFP-1G20ALC-T	120	-8.0	-2.0	-23.0	-2.0
SFP-1G20BLC-T	120	-8.0	-2.0	-23.0	-2.0
SFP-1G40ALC-T	120	-3.0	2.0	-23.0	-1.0
SFP-1G40BLC-T	120	-3.0	2.0	-23.0	-1.0
SFP-1GSXLC	100	-9.5	-4.0	-18.0	0
SFP-1GLSXLC	100	-9.0	-1.0	-19.0	-1.0
SFP-1GLXLC	100	-9.0	-3.0	-21.0	-3.0
SFP-1GLHLC	100	-8.0	-3.0	-23.0	-3.0
SFP-1GLHXLC	100	-4.0	3.0	-24.0	-1.0
SFP-1GZXLC	100	0.0	5.0	-24.0	-1.0
SFP-1GEZXLC	100	0.0	5.0	-30.0	-9.0
SFP-1GEZXLC-120	100	-2.0	3.0	-33.0	-8.0
SFP-1G10ALC	100	-9.0	-3.0	-21.0	-2.0
SFP-1G10BLC	100	-9.0	-3.0	-21.0	-3.0

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
SFP-1G20ALC	100	-8.0	-2.0	-23.0	-2.0
SFP-1G20BLC	100	-8.0	-2.0	-23.0	-2.0
SFP-1G40ALC	100	-3.0	2.0	-23.0	-1.0
SFP-1G40BLC	100	-3.0	2.0	-23.0	-1.0
SFP-2.5GMLC-T	120	-7.5	-1.0	-13.5	0.0
SFP-2.5GSLC-T	120	-9.0	-3.0	-15.0	3.0
SFP-2.5GLSLC-T	120	-5.0	0.0	-16.0	0.0
SFP-2.5GSLHLC-T	120	-4.0	1.0	-19.0	1.0
SFP-10GERLC-T	110	-1.0	2.0	-15.8	-1.0
SFP-10GZRLC-T	100	0.0	4.0	-23	-7.0
SFP-10GLRLC-T	120	-8.2	0.5	-14.4	0.5
SFP-10GSRLC-T	110	-5.0	-1.0	-9.9	0.5

Glossary

1-to-1 NAT

1-to-1 NAT maps one public IP address to one private IP address.

Broadcast Forwarding

Broadcast forwarding enables users to specify the interface and UDP ports that broadcast packets will use to pass through the router, allowing devices to be queried on the network, such as Modbus devices.

CoS Mapping

CoS stands for Class of Service and refers to the differentiation and marking of different types of data during network transmission to distinguish between different types of services. CoS mapping is the process of mapping CoS levels to priority queues on the device.

Dead Interval

The dead interval is the amount of time a device will wait for a hello packet. If a hello packet is not received in this time, it will consider the other device to be dead or unavailable. By default, the dead interval is set to be four times the value of the hello interval.

Double NAT

Double NAT enables you to use 1-to-1 rules to facilitate two-way communication.

DSCP Mapping

DSCP is a field in the IP Layer 3 header that allows network administrators to classify and prioritize traffic based on the type of service being provided, ensuring that critical traffic receives priority handling and network resources are utilized efficiently. DSCP mapping is the process of mapping DSCP levels to priority queues on the device.

Hello Interval

The hello interval is the amount of time between sends of hello packets, which indicate that the device is still alive. The value of all hello intervals must be the same within a network.

Hello Packet

Hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. Hello packets are sent at a configurable interval (in seconds).

IEC 61735

IEC 61375 is an International Electrotechnical Commission standard that defines the architecture of data communication systems used in trains. The structure of the Ethernet data communication system that has been defined in the standard includes Ethernet Train Backbone (ETB) and Ethernet Consist Network (ECN) that relate to IEC 61375-2-3 Electronic Railway Equipment. It also contains information about Train Communication Networks, Communication Profiles, IEC 61375-2-5 Electronic Railway Equipment, Train Communication Networks, and Ethernet Train Backbones.

IKE

Internet Key Exchange (IKE) is a protocol used in computer networks for establishing and managing security associations and cryptographic keys in virtual private networks (VPNs) to ensure secure communication.

Link-State Advertisement Packet (LSA)

LSA packets (Link-State Advertisement) are packets that contain information about a router's links.

MTU (Maximum Transmission Unit)

The MTU (Maximum Transmission Unit) is the maximum size of a packet that can be transmitted over a network. The MTU is important because it affects the performance and efficiency of data transmission on the network.

N-to-1 NAT

N-to-1 NAT maps multiple private IP addresses to one public IP address.

NAT Loopback

NAT loopback allows devices on a private network to access a server or service hosted on the same network using the public IP address of the network.

Network Address Translation (NAT)

NAT (Network Address Translation) is method of changing an IP address during Ethernet packet transmission, which can also enhance network security. If you wan to hide an internal IP address (LAN) from the external network (WAN), NAT can translate the

internal IP address to a specific IP address, or an internal IP address range to one external IP address.

Port Address Translation (PAT)

Port Address Translation (PAT) maps multiple private IP addresses to one public IP address using different port numbers.

VRRP Binding

Virtual Router Redundancy Protocol (VRRP) Binding is a feature that allows the 1-to-1 NAT rule to be bound to a VRRP index. VRRP Binding is only supported in 1-to-1 NAT. If a VRRP index is selected, the 1-to-1 NAT rule is only valid when the system is the master. If no VRRP index is selected, the 1-to-1 NAT rule will be valid regardless of whether the system is the master or backup.

IEC 61162-460 Supplementary Declaration

Preface

IEC 61162-460 is an international standard developed by the International Electrotechnical Commission (IEC) that specifies requirements for digital interfaces used in maritime navigation and radiocommunication equipment. It serves as an extension to IEC 61162-450, focusing on enhancing safety and security within Ethernet-based shipboard networks.

The standard outlines requirements and test methods for equipment intended for use in IEC 61162-460 compliant networks. It also provides guidelines for the network's architecture and its interconnections with other networks, including provisions for redundant network configurations to ensure reliability.

By implementing IEC 61162-460, maritime systems can achieve higher safety and security standards, addressing potential external threats and improving overall network integrity. This is particularly important in modern maritime operations, where robust and secure communication networks are essential for safe navigation and effective radiocommunication.

Explanation

The configuration recommendations required for equipment to comply with IEC-61162-460 can largely refer directly to the Security Hardening Guide section. This section serves only as supplementary explanation and declaration.

Supplementary Declaration

When users configure this device, they need to additionally consider the following requirements to determine if they are necessary for the specific site. If they are, the following recommendations can be referenced:

1. It is recommended that the bandwidth allocated to each port on a 460-switch be greater than or equal to the total traffic handled by the switch.
2. When considering the configuration of trusted access, it is recommended that users restrict access to the device to specific IPs originating from the 460-network. Source IPs outside the allowlist (e.g., IPs from uncontrolled networks) will be blocked.
3. When configuring or adjusting Layer 3-7 policies, users can only access the device and configure Layer 3-7 policies through the trusted access allowlist, which specifies source IPs from the 460-network.
4. Arbitrarily replacing or modifying equipment within the 460 network may lead to cybersecurity concerns. It is recommended to first consult with the system integrator or manufacturer to assess potential risks.
5. If filtering based on each physical port is required, it is recommended to configure a VLAN interface with only one port member. Subsequently, apply the relevant rules to this interface through the Layer 3-7 policy.
6. The communication between devices or software defined within the 460-network must be managed through the EDR-G9010/EDR-8010 or by using alternative devices equipped with 460-switch and 460-forwarder functionalities to achieve control.

IEC 61375-2-3 Communication Identifiers

This is a list of IEC 61375-2-3 communication identifier ComIDs and their descriptions.

ComID	Description
0	unspecified PDU
1	ETBCTRL telegram
2	CSTINFO notification message
3	CSTINFOCTRL notification message
10	TRDP Echo
31	TRDP - statistics request command
35	TRDP - global statistics data
36	TRDP - subscription statistics data
37	TRDP - publishing statistics data
38	TRDP - redundancy statistics data
39	TRDP - join statistics data
40	TRDP- UDP listener statistics data
41	TRDP - TCP listener statistics data
80	Conformance test- control telegram
81	Conformance test - status telegram
82	Conformance test - confirmation request telegram
83	Conformance test - confirmation reply telegram
84	Conformance test - opTrnDir request telegram
85	Conformance test - opTrnDir reply telegram

ComID	Description
86	Conformance test - echo request telegram
87	Conformance test - echo reply telegram
88	Conformance test - echo notification telegram
100	TTDB - operational train directory status telegram
101	TTDB - operational train directory notification
102	TTDB - train directory information request
103	TTDB - train directory information reply
104	TTDB - consist information request
105	TTDB - consist information reply
106	TTDB - train network directory information request
107	TTDB - train network directory information reply
108	TTDB - operational train directory information request
109	TTDB - operational train directory information reply
110	TTDB - train information complete request
120	ECSP - control telegram
121	ECSP - status telegram
122	ECSP - Confirmation/Correction request
123	ECSP - Confirmation/Correction reply
130	ETBN - control request
131	ETBN - status reply
132	ETBN - train network directory request
133	ETBN - train network directory reply
140	TCN-DNS - resolving request telegram (query)

ComID	Description
141	TCN-DNS - resolving reply telegram

IEC-104 Cause of Transmission List

This is a list of IEC-104 cause of transmission codes and their descriptions.

Cause	Description
0	not used
1	periodic, cyclic
2	background interrogation
3	spontaneous
4	initialized
5	interrogation or interrogated
6	activation
7	confirmation activation
8	deactivation
9	confirmation deactivation
10	termination activation
11	feedback, caused by distant command
12	feedback, caused by local command
13	data transmission
14-19	reserved for further compatible definitions
20	interrogated by general interrogation
21	interrogated by interrogation group 1
22	interrogated by interrogation group 2
23	interrogated by interrogation group 3
24	interrogated by interrogation group 4

Cause	Description
25	interrogated by interrogation group 5
26	interrogated by interrogation group 6
27	interrogated by interrogation group 7
28	interrogated by interrogation group 8
29	interrogated by interrogation group 9
30	interrogated by interrogation group 10
31	interrogated by interrogation group 11
32	interrogated by interrogation group 12
33	interrogated by interrogation group 13
34	interrogated by interrogation group 14
35	interrogated by interrogation group 15
36	interrogated by interrogation group 16
37	interrogated by counter general interrogation
38	interrogated by interrogation counter group 1
39	interrogated by interrogation counter group 2
40	interrogated by interrogation counter group 3
41	interrogated by interrogation counter group 4
44	type-Identification unknown
45	cause unknown
46	ASDU address unknown
47	Information object address unknown

IEC-104 Type Identification List

This is a list of IEC-104 type identification codes and their descriptions.

Process information in monitor direction

Type	Description
1	Single point information
2	Single point information with time tag
3	Double point information
4	Double point information with time tag
5	Step position information
6	Step position information with time tag
7	Bit string of 32 bit
8	Bit string of 32 bit with time tag
9	Measured value, normalized value
10	Measured value, normalized value with time tag
11	Measured value, scaled value
12	Measured value, scaled value with time tag
13	Measured value, short floating-point value
14	Measured value, short floating-point value with time tag
15	Integrated totals
16	Integrated totals with time tag
17	Event of protection equipment with time tag
18	Packed start events of protection equipment with time tag

Type	Description
19	Packed output circuit information of protection equipment with time tag
20	Packed single-point information with status change detection
21	Measured value, normalized value without quality descriptor

Process telegrams with long time tag (7 octets)

Type	Description
30	Single point information with time tag CP56Time2a
31	Double point information with time tag CP56Time2a
32	Step position information with time tag CP56Time2a
33	Bit string of 32 bit with time tag CP56Time2a
34	Measured value, normalized value with time tag CP56Time2a
35	Measured value, scaled value with time tag CP56Time2a
36	Measured value, short floating-point value with time tag CP56Time2a
37	Integrated totals with time tag CP56Time2a
38	Event of protection equipment with time tag CP56Time2a
39	Packed start events of protection equipment with time tag CP56time2a
40	Packed output circuit information of protection equipment with time tag CP56Time2a

Process information in control direction

Type	Description
45	Single command

Type	Description
46	Double command
47	Regulating step command
48	Setpoint command, normalized value
49	Setpoint command, scaled value
50	Setpoint command, short floating-point value
51	Bit string 32 bit

Command telegrams with long time tag (7 octets)

Type	Description
58	Single command with time tag CP56Time2a
59	Double command with time tag CP56Time2a
60	Regulating step command with time tag CP56Time2a
61	Setpoint command, normalized value with time tag CP56Time2a
62	Setpoint command, scaled value with time tag CP56Time2a
63	Setpoint command, short floating-point value with time tag CP56Time2a
64	Bit string 32 bit with time tag CP56Time2a

System information in monitor direction

Type	Description
70	End of initializ

System information in control direction

Type	Description
100	(General-) Interrogation command
101	Counter interrogation command
102	Read command
103	Clock synchronization command
104	(IEC 101) Test command
105	Reset process command
106	(IEC 101) Delay acquisition command
107	Test command with time tag CP56Time2a

Parameter in control direction

Type	Description
110	Parameter of measured value, normalized value
111	Parameter of measured value, scaled value
112	Parameter of measured value, short floating-point value
113	Parameter activation

File transfer

Type	Description
120	File ready
121	Section ready

Type	Description
122	Call directory, select file, call file, call section
123	Last section, last segment
124	Ack file, Ack section
125	Segment
126	Directory
127	QueryLog – Request archive file

LED Behavior

This page describes the LED behaviors for different product series.

> **Note**
> Please note that some LEDs are only on models with related features.

EDF-G1002 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input PWR1.
	Off	Off	Power is not being supplied to the power PWR1.
PWR2	Amber	On	Power is being supplied to power input PWR2.
	Off	Off	Power is not being supplied to the power PWR2.
STATE	Green	On	The system passed the self-diagnosis test during boot-up and is ready to run.
		Blinking (1 Hz)	The system is ready to do a factory reset after pressing the reset button for 5 seconds.
	Red	On	The system failed the self-diagnosis test during boot-up.
	Off	Off	The system is off.
USB	Green	On	A USB device is connected.
		Blinking (1 sec off, 1 sec on)	USB data is being transmitted.
	Red	On	The USB device is malfunctioning.
	Off	Off	No USB device connected.
Bypass	Amber	On	System-halted bypass or Run-time bypass mode is enabled.
		Blinking (0.5 Hz)	Run-time bypass is enabled and operating

LED	Color	State	Description
	Off	Off	System-halted bypass or Run-time bypass mode is disabled.
HA	Green	On	Reserved.
	Amber	On	Reserved.
	Off	Off	Reserved.
10/100/1000 Mbps	Green	On	The port is active, and a link is established at 1000 Mbps.
		Blinking	Data is being transmitted at 1000 Mbps.
	Amber	On	The port is active, and a link is established at 10/100 Mbps.
		Blinking	Data is being transmitted at 10/100 Mbps.
	Off	Off	The port is inactive, or the link is down.

EDR-8010 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is not being supplied to power input P1 on the main module.
PWR2	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is not being supplied to power input P2 on the main module.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
	Red	On	The system failed the self-diagnosis test on boot-up.
MSTR/H.TC	Green	On	The EDR-8010 is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.

LED	Color	State	Description
		Off	The EDR-8010 is not set as the Master of this Turbo Ring or is set as a Member of the Turbo Chain.
CPLR / T.TC	Green	On	The EDR-8010 Series' coupling function is enabled to form a backup path, or the device is set as the Tail of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-8010 Series' coupling function is disabled, or the device is set as a Member of the Turbo Chain.
VRRP / HA	Green	On	The EDR-8010 is set as the Master of the VRRP or HA.
		Off	The EDR-8010 is not set as the Master of the VRRP or HA.
VPN	Green	On	All VPN tunnels are working normally.
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
USB	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
1G	Green	On	1G SFP link is up.
		Off	No link or the SFP link is down.
10 / 100 Mbps	Green	On	10 or 100 Mbps copper link is up.
		Off	No link or the copper link is down.

EDR-G9004 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is NOT being supplied to power input P1 on the main module.

LED	Color	State	Description
PWR2	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is NOT being supplied to power input P2 on the main module.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
	Red	On	The system failed the self-diagnosis test on boot-up.
BYPASS	Amber	On	The bypass redundancy function is enabled.
		Off	The bypass redundancy function is disabled.
WAN/DMZ	Amber	On	The WAN2/DMZ port is set to WAN mode.
	Green	On	The WAN2/DMZ port is set to DMZ mode.
		Off	The WAN2/DMZ port is disabled.
VRRP/HA	Green	On	The EDR-G9004 is set as the Master of the VRRP or HA.
		Off	The EDR-G9004 is not set as the Master of the VRRP or HA.
VPN	Green	On	All VPN tunnels are working normally.
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
USB	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
1G/2.5G	Green	On	2.5G SFP link is up.
	Amber	On	1G SFP link is up.
		Off	No link or the SFP link is down.
10/100/ 1000 Mbps	Green	On	1000 Mbps copper link is up.
	Amber	On	10/100 Mbps copper link is up.

LED	Color	State	Description
		Off	No link or the copper link is down.

EDR-G9010 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input P1 on the main module.
		Off	Power is not being supplied to power input P1 on the main module.
PWR2	Amber	On	Power is being supplied to power input P2 on the main module.
		Off	Power is not being supplied to power input P2 on the main module.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
	Red	On	The system failed the self-diagnosis test on boot-up.
MSTR / H.TC	Green	On	The EDR-G9010 is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-G9010 is not set as the Master of this Turbo Ring or is set as a Member of the Turbo Chain.
CPLR / T.TC	Green	On	The EDR-G9010 Series' coupling function is enabled to form a backup path, or the device is set as the Tail of the Turbo Chain.
		Blinking	The Turbo Ring or the Turbo Chain is down.
		Off	The EDR-G9010 Series' coupling function is disabled, or the device is set as a Member of the Turbo Chain.
VRRP / HA	Green	On	The EDR-G9010 is set as the Master of the VRRP or HA.
		Off	The EDR-G9010 is not set as the Master of the VRRP or HA.
VPN	Green	On	All VPN tunnels are working normally.

LED	Color	State	Description
	Amber	On	Only parts of the VPN tunnels are working normally.
		Off	No active VPN connections.
USB	Green	On	USB drive successfully connected.
		Blinking	USB data is being transmitted.
	Red	On	USB dongle malfunction.
1G/2.5G	Green	On	2.5G SFP link is up.
	Amber	On	1G SFP link is up.
		Off	No link or the SFP link is down.
10/100/1000 Mbps	Green	On	1000 Mbps copper link is up.
	Amber	On	10/100 Mbps copper link is up.
		Off	No link or the copper link is down.

NAT-102 Series LED Behavior

LED	Color	State	Description
PWR	Amber	On	Power is being supplied to the power input.
		Off	Power is NOT being supplied to the power.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
		Off	The system failed the self-diagnosis test on boot-up.
LEARN	Amber	Blinking	The device lockdown learning is in progress.
		Off	Learning finished.
LOCKDOWN	Green	On	The device lockdown allowlist is enabled.

LED	Color	State	Description
		Off	The device lockdown allowlist is disabled.

NAT-108 Series LED Behavior

LED	Color	State	Description
PWR	Amber	On	Power is being supplied to the power input.
		Off	Power is NOT being supplied to the power.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
		Off	The system failed the self-diagnosis test on boot-up.
LEARN	Amber	Blinking	The device lockdown learning is in progress.
		Off	Learning finished.
LOCKDOWN	Green	On	The device lockdown allowlist is enabled.
		Off	The device lockdown allowlist is disabled.

NAT-G102 Series LED Behavior

LED	Color	State	Description
PWR	Amber	On	Power is being supplied to the power input.
		Off	Power is NOT being supplied to the power.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
		Off	The system failed the self-diagnosis test on boot-up.

LED	Color	State	Description
LEARN	Amber	Blinking	The device lockdown learning is in progress.
		Off	Learning finished.
LOCKDOWN	Green	On	The device lockdown allowlist is enabled.
		Off	The device lockdown allowlist is disabled.

OnCell G4302-LTE4 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input PWR1.
	Off	Off	Power is not being supplied to the power PWR1.
PWR2	Amber	On	Power is being supplied to power input PWR2.
	Off	Off	Power is not being supplied to the power PWR2.
STATE	Green	On	The system passed the self-diagnosis test during boot-up and is ready to run.
		Blinking (1 sec off, 5 sec on)	The system is in Power Saving mode.
	Red	On	The system failed the self-diagnosis test during boot-up.
	Off	Off	The system is off.
USB	Green	On	A USB device is connected.
		Blinking (1 sec off, 1 sec on)	USB data is being transmitted.
	Red	On	The USB device is malfunctioning.
	Off	Off	No USB device connected.
SIM1	Green	On	A SIM card is installed in SIM1 and is working normally.
	Red	On	A SIM card is installed in SIM1 but is not working properly.

LED	Color	State	Description
	Off	Off	No SIM card installed.
SIM2	Green	On	A SIM card is installed in SIM2 and is working normally.
	Red	On	A SIM card is installed in SIM2 but is not working properly.
	Off	Off	No SIM card installed.
CELL	Green	On	Good cellular signal.
	Amber	On	Fair cellular signal.
	Red	On	Poor cellular signal.
	Off	Off	No cellular signal.
LTE	Green	On	4G LTE connected.
	Amber	On	UMTS/HSPA/GSM/GPRS/EDGE connected.
	Off	Off	No cellular service.
GNSS	Green	On	GNSS located successfully.
	Red	On	Less than 4 satellites located.
	Off	Off	GNSS functionality is disabled.
SERIAL	Green	On	Data is being transmitted over the serial connection.
	Off	Off	No serial connection.
VPN	Green	On	All VPN tunnels are working normally.
	Amber	On	Some VPN tunnels are not working properly.
	Red	On	Failed to establish any VPN connection.
	Off	Off	VPN functionality is disabled.
LAN/WAN	Green	On	The port is active, and a link is established at 1000 Mbps.
		Blinking	Data is being transmitted at 1000 Mbps.
	Amber	On	The port is active, and a link is established at 10/100 Mbps.

LED	Color	State	Description
		Blinking	Data is being transmitted at 10/100 Mbps.
	Off	Off	The port is inactive, or the link is down.

OnCell G4308-LTE4 Series LED Behavior

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input PWR1.
	Off	Off	Power is not being supplied to the power PWR1.
PWR2	Amber	On	Power is being supplied to power input PWR2.
	Off	Off	Power is not being supplied to the power PWR2.
STATE	Green	On	The system passed the self-diagnosis test during boot-up and is ready to run.
		Blinking (1 sec off, 5 sec on)	The system is in Power Saving mode.
	Red	On	The system failed the self-diagnosis test during boot-up.
	Off	Off	The system is off.
USB	Green	On	A USB device is connected.
		Blinking (1 sec off, 1 sec on)	USB data is being transmitted.
	Red	On	The USB device is malfunctioning.
	Off	Off	No USB device connected.
SIM1	Green	On	A SIM card is installed in SIM1 and is working normally.
	Red	On	A SIM card is installed in SIM1 but is not working properly.
	Off	Off	No SIM card installed.
SIM2	Green	On	A SIM card is installed in SIM2 and is working normally.

LED	Color	State	Description
	Red	On	A SIM card is installed in SIM2 but is not working properly.
	Off	Off	No SIM card installed.
CELL	Green	On	Good cellular signal.
	Amber	On	Fair cellular signal.
	Red	On	Poor cellular signal.
	Off	Off	No cellular signal.
LTE	Green	On	4G LTE connected.
	Amber	On	UMTS/HSPA/GSM/GPRS/EDGE connected.
	Off	Off	No cellular service.
GNSS	Green	On	GNSS located successfully.
	Red	On	Less than 4 satellites located.
	Off	Off	GNSS functionality is disabled.
SERIAL	Green	On	Data is being transmitted over the serial connection.
	Off	Off	No serial connection.
VPN	Green	On	All VPN tunnels are working normally.
	Amber	On	Some VPN tunnels are not working properly.
	Red	On	Failed to establish any VPN connection.
	Off	Off	VPN functionality is disabled.
LAN/WAN	Green	On	The port is active, and a link is established at 1000 Mbps.
		Blinking	Data is being transmitted at 1000 Mbps.
	Amber	On	The port is active, and a link is established at 10/100 Mbps.
		Blinking	Data is being transmitted at 10/100 Mbps.
	Off	Off	The port is inactive, or the link is down.

TN-4900 Series LED Behavior

System LEDs

LED	Color	State	Description
PWR1	Amber	On	Power is being supplied to power input PWR1.
		Off	Power is not being supplied to power input PWR1
PWR2	Amber	On	Power is being supplied to power input PWR2.
		Off	Power is not being supplied to power input PWR2.
FAULT	Red	On	When a user-configured event is triggered. 1. Turbo Ring is broken 2. Port link turned on or off **Note** The FAULT LED will be on during the DUT boot up state and while waiting for the system to be ready. Once the system is ready, the FAULT LED will turn off.
		Off	When the corresponding PORT alarm is enabled and a user-configured event is not triggered, or when the corresponding PORT alarm is disabled.
MSTR/ HEAD	Green	On	When the TN router is either the Master of this Turbo Ring, or the Head of this Turbo Chain.
		Blinking	When the TN router is Ring Master of this Turbo Ring and the Turbo Ring is broken, or it is the Chain Head of this Turbo Chain and the Turbo Chain is broken.
		Off	When the TN router is neither the Master of this Turbo Ring, nor the Head of this Turbo Chain.
CPLR/ TAIL	Green	On	When the TN router enables the coupling function to form a back-up path in this Turbo Ring, or it is the Tail of this Turbo Chain.
		Blinking	When Turbo Chain is down.
		Off	When the TN router disables the coupling function of Turbo Ring, or it is not the Tail of the Turbo Chain.

LED	Color	State	Description
FAULT + MSTR/HEAD + CPLR/TAIL	Rotate Blinking Sequentially		When ABC-02 is importing or exporting files.

Port LEDs

LED	Color	State	Description
FE Ports (10/100M for copper ports)	Amber	On	The port's 10 Mbps link is active.
		Blinking	Data is being transmitted at 10 Mbps.
		off	The port's 10 Mbps link is inactive.
	Green	On	The port's 100 Mbps link is active.
		Blinking	Data is being transmitted at 100 Mbps.
		off	The port's 100 Mbps link is inactive.
GB Ports (10/100/1000M, for copper ports)	Amber	On	The port's 10 or 100 Mbps link is active.
		Blinking	Data is being transmitted at 10 or 100 Mbps.
		Off	The port's 10 or 100 Mbps link is inactive.
	Green	On	The port's 1000 Mbps link is active.
		Blinking	Data is being transmitted at 1000 Mbps.
		Off	The port's 1000 Mbps link is inactive.
PoE Ports	Amber	On	Power is being supplied to a Powered Device (PD).
		Off	Power is not being supplied to a Powered Device (PD).

NAT-108 Series LED Behavior

LED	Color	State	Description
PWR	Amber	On	Power is being supplied to the power input.
		Off	Power is NOT being supplied to the power.
STATE	Green	On	The system passed the self-diagnosis test on boot-up and is ready to run.
		Blinking	Device reset is in progress, blinking once per second.
		Off	The system failed the self-diagnosis test on boot-up.
LEARN	Amber	Blinking	The device lockdown learning is in progress.
		Off	Learning finished.
LOCKDOWN	Green	On	The device lockdown allowlist is enabled.
		Off	The device lockdown allowlist is disabled.

MIB Groups

Your device comes with integrated SNMP (Simple Network Management Protocol) agent software, compliant with RFC-123 standard MIB and properties MIB. The following is a list of all the folders and related MIB files.

For comprehensive MIB information, you can use MIB browser tools. These tools provide a detailed view of the MIB tree, allowing for easier management and monitoring of network devices. Additionally, the complete MIB files can be downloaded from the product page on the Moxa website. Visit the Moxa product pages to access the latest MIB files and other related resources.

MIB Tree Structure

The MIB tree structure is designed for all Moxa router series. However, some MIB files may not be supported due to the varying support levels of each product series. Refer to the Supported Features List for detailed information about supported features.

```
--insrouter(1.3.6.1.4.1.8691.6.100)
  |
  +--swTraps(0)
  |  |
  |  +-- r-n Enumeration   varconfigChangeTrap(1)
  |  +-- r-n Enumeration   varpower1Trap(2)
  |  +-- r-n Enumeration   varpower2Trap(3)
  |  +-- r-n Enumeration   vardi1Trap(4)
  |  +-- r-n Enumeration   vardi2Trap(5)
  |  +-- r-n Enumeration   varredundancyTopologyChangedTrap(10)
  |  +-- r-n Enumeration   varturboRingCouplingPortChangedTrap(11)
  |  +-- r-n Enumeration   varturboRingMasterChangedTrap(12)
  |  +-- r-n DisplayString varVRRPStateChangeTrap(13)
  |  +-- r-n Integer32     varFiberWarningTrap(28)
  |  +-- r-n DisplayString varVPNConnectedTrap(40)
  |  +-- r-n DisplayString varVPNDisconnectedTrap(41)
  |  +-- r-n DisplayString varFirewallPolicyTrap(50)
  |  +-- r-n DisplayString varSecurityNotificationTrap(51)
  |  +-- r-n Enumeration   varLoggingCapacityTrap(52)
  |  +-- r-n DisplayString varDot1xAuthFailTrap(53)
  |  +-- r-n Enumeration   varFirmwareUpgradeTrap(54)
  |  +-- r-n DisplayString varFirewallConfigChangeTrap(55)
  |  +-- r-n DisplayString varCellularIpChange(56)
  |  +-- r-n DisplayString varCellularModuleFail(57)
  |  +-- r-n DisplayString varCellularSimDetectFail(58)
  |  +-- r-n DisplayString varCellularPinCodeFail(59)
  |  +-- r-n DisplayString varCellularSimSwitch(60)
  |  +-- r-n DisplayString varCellularModuleHighTemperature(61)
  |  +-- r-n DisplayString varCellularGuaranlinkCellularReconnect(62)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerIspReregister(63)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerCellularModuleReset(64)
  |  +-- r-n DisplayString varCellularGuaranlinkTriggerSystemReboot(65)
  |  +-- r-n DisplayString varCellularPmPowerSavingStart(66)
  |  +-- r-n DisplayString varCellularPmPowerSavingEnd(67)
  |  +-- r-n DisplayString varCellularPmSchedulingRuleExpired(68)
```

```
|  +-- r-n DisplayString varCellularSmsWrongPassword(69)
|  +-- r-n DisplayString varCellularSmsWrongCommand(70)
|  +-- r-n DisplayString varCellularSmsWrongFormat(71)
|  +-- r-n DisplayString varCellularSmsCommandDisabled(72)
|  +-- r-n DisplayString varCellularSmsTrustedNumberAuthenticationFail(73)
|  +-- r-n DisplayString varWanInterfaceChange(74)
|  +-- r-n DisplayString varWanInterfacePingFail(75)
|  +-- r-n DisplayString varSerialOpModeStateChange(76)
|  +-- r-n DisplayString varSerialDSRStateChange(77)
|  +-- r-n DisplayString varSerialDCDStateChange(78)
|  +-- r-n DisplayString varLfpOn(79)
|  +-- r-n DisplayString varLfpOff(80)
|  +-- r-n DisplayString varDeviceLockdownStateChangeTrap(81)
|  +-- r-n DisplayString varLicenseNotificationTrap(201)
|
+--swMgmt(1)
|  |
|  +--basicSetting(2)
|  |  |
|  |  +--systemSetting(1)
|  |  |  |
|  |  |  +-- rwn DisplayString sysRouterName(1)
|  |  |
|  |  +--accessibleIP(2)
|  |     |
|  |     +-- r-n Enumeration enableAccessibleIP(1)
|  |     +-- r-n Enumeration enableAccessibleLan(2)
|  |     |
|  |     +--accessibleIpTable(3)
|  |        |
|  |        +--accessibleIpEntry(1) [accessibleIpAddress]
|  |           |
|  |           +-- r-n IpAddress   accessibleIpAddress(1)
|  |           +-- r-n IpAddress   accessibleIpNetMask(2)
|  |           +-- r-n Enumeration accessibleIpState(3)
|  |
|  +--network(3)
|  |  |
|  |  +--networkSetting(1)
|  |     |
|  |     +--wanSetting(1)
|  |     |  |
|  |     |  +-- r-n Enumeration   wanConnMode(1)
|  |     |  +-- r-n Enumeration   wanConnType(2)
|  |     |  +-- r-n IpAddress     wanStaticIpAddr(3)
|  |     |  +-- r-n IpAddress     wanStaticIpMask(4)
|  |     |  +-- r-n IpAddress     wanStaticDefaultGateway(5)
|  |     |  +-- r-n DisplayString wanAdslName(6)
|  |     |  +-- r-n DisplayString wanAdslHost(7)
|  |     |  +-- r-n Enumeration   wanPptpEnable(9)
|  |     |  +-- r-n IpAddress     wanPptpAddr(10)
|  |     |  +-- r-n DisplayString wanPptpUsrName(11)
|  |     |  +-- r-n IpAddress     wanDnsServer1(13)
|  |     |  +-- r-n IpAddress     wanDnsServer2(14)
|  |     |  +-- r-n IpAddress     wanDnsServer3(15)
|  |     |  +-- r-n IpAddress     ipAddr(16)
|  |     |  +-- r-n IpAddress     ipMask(17)
|  |     |  +-- r-n IpAddress     defaultGateway(18)
|  |     |  +-- r-n Enumeration   directedBroadcast(19)
|  |     |  +-- r-n Enumeration   sourceIPOverwrite(20)
|  |     |
|  |     +--wan2Setting(2)
|  |     |  |
|  |     |  +-- r-n Enumeration   wan2ConnMode(1)
|  |     |  +-- r-n Enumeration   wan2ConnType(2)
|  |     |  +-- r-n Enumeration   wan2DmzState(3)
|  |     |  +-- r-n IpAddress     wan2StaticIpAddr(4)
|  |     |  +-- r-n IpAddress     wan2StaticIpMask(5)
|  |     |  +-- r-n IpAddress     wan2StaticDefaultGateway(6)
|  |     |  +-- r-n DisplayString wan2AdslName(7)
```

```
|  |     |  +-- r-n DisplayString wan2AdslHost(8)
|  |     |  +-- r-n Enumeration   wan2PptpEnable(10)
|  |     |  +-- r-n IpAddress     wan2PptpAddr(11)
|  |     |  +-- r-n DisplayString wan2PptpUsrName(12)
|  |     |  +-- r-n IpAddress     wan2DnsServer1(14)
|  |     |  +-- r-n IpAddress     wan2DnsServer2(15)
|  |     |  +-- r-n IpAddress     wan2DnsServer3(16)
|  |     |  +-- r-n IpAddress     wan2IpAddr(17)
|  |     |  +-- r-n IpAddress     wan2IpMask(18)
|  |     |  +-- r-n IpAddress     wan2DefaultGateway(19)
|  |     |  +-- r-n Enumeration   wan2DirectedBroadcast(20)
|  |     |  +-- r-n Enumeration   wan2SourceIPOverwrite(21)
|  |     |
|  |     +--lanSetting(3)
|  |     |  |
|  |     |  +--lanTable(1)
|  |     |     |
|  |     |     +--lanEntry(1) [lanVlanId]
|  |     |        |
|  |     |        +-- r-n Integer32     lanVlanId(1)
|  |     |        +-- r-n Enumeration   lanEnable(2)
|  |     |        +-- r-n DisplayString lanName(3)
|  |     |        +-- r-n IpAddress     lanIpAddr(4)
|  |     |        +-- r-n IpAddress     lanIpMask(5)
|  |     |        +-- r-n Enumeration   lanDirectedBroadcast(6)
|  |     |        +-- r-n Enumeration   lanSourceIPOverwrite(7)
|  |     |
|  |     +--dhcpServer(4)
|  |     |  |
|  |     |  +--dhcpSrvTable(1)
|  |     |  |  |
|  |     |  |  +--dhcpSrvEntry(1) [dhcpSvrEnable]
|  |     |  |     |
|  |     |  |     +-- r-n Enumeration dhcpSvrEnable(1)
|  |     |  |     +-- r-n Integer32   dhcpSvrLeaseTime(2)
|  |     |  |     +-- r-n IpAddress   dhcpSvrDns1(3)
|  |     |  |     +-- r-n IpAddress   dhcpSvrDns2(4)
|  |     |  |     +-- r-n IpAddress   dhcpIpRangeStart(5)
|  |     |  |     +-- r-n IpAddress   dhcpIpRangeEnd(6)
|  |     |  |     +-- r-n IpAddress   dhcpNTP(7)
|  |     |  |     +-- r-n IpAddress   dhcpDefaultGateway(8)
|  |     |  |     +-- r-n IpAddress   dhcpNetmask(9)
|  |     |  |
|  |     |  +--dhcpStaticTable(8)
|  |     |  |  |
|  |     |  |  +--dhcpStaticEntry(1) [dhcpStaticEnable]
|  |     |  |     |
|  |     |  |     +-- r-n Enumeration   dhcpStaticEnable(1)
|  |     |  |     +-- r-n DisplayString dhcpStaticName(2)
|  |     |  |     +-- r-n IpAddress     dhcpStaticIp(3)
|  |     |  |     +-- r-n MacAddress    dhcpStaticMac(4)
|  |     |  |     +-- r-n Integer32     dhcpStaticLeasetime(5)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDns1(6)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDns2(7)
|  |     |  |     +-- r-n IpAddress     dhcpStaticNtp(8)
|  |     |  |     +-- r-n IpAddress     dhcpStaticDefaultGateway(9)
|  |     |  |     +-- r-n IpAddress     dhcpStaticNetmask(10)
|  |     |  |
|  |     |  +--dhcpSvrPipTable(9)
|  |     |     |
|  |     |     +--dhcpSvrPipEntry(1) [dhcpPipEnable]
|  |     |        |
|  |     |        +-- r-n Enumeration dhcpPipEnable(1)
|  |     |        +-- r-n Integer32   dhcpPipPortNumber(2)
|  |     |        +-- r-n IpAddress   dhcpPipIp(3)
|  |     |        +-- r-n IpAddress   dhcpPipNetmask(4)
|  |     |        +-- r-n Integer32   dhcpPipLeasetime(5)
|  |     |        +-- r-n IpAddress   dhcpPipDns1(6)
|  |     |        +-- r-n IpAddress   dhcpPipDns2(7)
|  |     |        +-- r-n IpAddress   dhcpPipNtp(8)
```

```
|  |     |        +-- r-n IpAddress   dhcpPipGateway(9)
|  |     |
|  |     +--dhcpList(5)
|  |     |  |
|  |     |  +--dhcpListTable(1)
|  |     |     |
|  |     |     +--dhcpListEntry(1) [dhcpListName]
|  |     |        |
|  |     |        +-- r-n DisplayString dhcpListName(1)
|  |     |        +-- r-n DisplayString dhcpListMac(2)
|  |     |        +-- r-n IpAddress     dhcpListAddr(3)
|  |     |
|  |     +--dhcpServerMode(8)
|  |     |  |
|  |     |  +-- r-n Enumeration dhcpServerModeStatus(1)
|  |     |
|  |     +--brigdeSetting(9)
|  |     |  |
|  |     |  +-- r-n Enumeration   bridgeEnable(1)
|  |     |  +-- r-n DisplayString bridgeName(2)
|  |     |  +-- r-n IpAddress     birdgeIpAddr(3)
|  |     |  +-- r-n IpAddress     bridgeIpMask(4)
|  |     |
|  |     +--cellularSetting(10)
|  |     |  |
|  |     |  +-- rwn Enumeration cellularEnable(1)
|  |     |  +-- rwn Enumeration cellularConnectionEnable(2)
|  |     |  |
|  |     |  +--cellularSimTable(3)
|  |     |  |  |
|  |     |  |  +--cellularSimEntry(1) [cellularSimIndex]
|  |     |  |     |
|  |     |  |     +-- r-n Integer32   cellularSimIndex(1)
|  |     |  |     +-- rwn Enumeration cellularSimEnable(2)
|  |     |  |     +-- rwn Enumeration cellularSimPriority(3)
|  |     |  |
|  |     |  +--guaranlinkSetting(4)
|  |     |  |  |
|  |     |  |  +-- rwn Enumeration glinkEnable(1)
|  |     |  |  +-- rwn Enumeration glinkCheckTiming(2)
|  |     |  |
|  |     |  +--remoteSmsSetting(5)
|  |     |  |  |
|  |     |  |  +-- rwn Enumeration remoteSmsEnable(1)
|  |     |  |
|  |     |  +--gnssSetting(6)
|  |     |     |
|  |     |     +-- rwn Enumeration   gnssEnable(1)
|  |     |     +-- rwn Enumeration   gnssServerEnable(2)
|  |     |     +-- rwn Enumeration   gnssClientEnable(3)
|  |     |     +-- r-n DisplayString gnssSatelliteStatus(4)
|  |     |     +-- r-n DisplayString gnssLongitudeStatus(5)
|  |     |     +-- r-n DisplayString gnssLatitudeStatus(6)
|  |     |
|  |     +--multiWanSetting(11)
|  |        |
|  |        +--wanSettingTable(1)
|  |           |
|  |           +--wanSettingEntry(1) [wanSettingId]
|  |              |
|  |              +-- --- Integer32     wanSettingId(1)
|  |              +-- r-n DisplayString wanSettingAlias(2)
|  |              +-- r-n Enumeration   wanSettingConnMode(3)
|  |              +-- r-n Enumeration   wanSettingConnType(4)
|  |              +-- r-n IpAddress     wanSettingStaticIpAddr(5)
|  |              +-- r-n IpAddress     wanSettingStaticIpMask(6)
|  |              +-- r-n IpAddress     wanSettingStaticDefaultGateway(7)
|  |              +-- r-n DisplayString wanSettingAdslName(8)
|  |              +-- r-n DisplayString wanSettingAdslHost(9)
|  |              +-- r-n Enumeration   wanSettingPptpEnable(10)
```

```
|  |  |              +-- r-n IpAddress     wanSettingPptpAddr(11)
|  |  |              +-- r-n DisplayString wanSettingPptpUsrName(12)
|  |  |              +-- r-n IpAddress     wanSettingDnsServer1(13)
|  |  |              +-- r-n IpAddress     wanSettingDnsServer2(14)
|  |  |              +-- r-n IpAddress     wanSettingDnsServer3(15)
|  |  |              +-- r-n IpAddress     wanStatusIpAddr(16)
|  |  |              +-- r-n IpAddress     wanStatusIpMask(17)
|  |  |              +-- r-n IpAddress     wanStatusDefaultGateway(18)
|  |  |              +-- r-n Enumeration   wanSettingDirectedBroadcast(19)
|  |  |              +-- r-n Enumeration   wanSettingSourceIPOverwrite(20)
|  |  |
|  |  +--routeSetting(5)
|  |  |  |
|  |  |  +--showRoutingTable(3)
|  |  |     |
|  |  |     +--rTable(1)
|  |  |        |
|  |  |        +--rEntry(1) [rIndex]
|  |  |           |
|  |  |           +-- rwn DisplayString rType(1)
|  |  |           +-- rwn DisplayString rDestination(2)
|  |  |           +-- rwn IpAddress     rNextHop(3)
|  |  |           +-- rwn DisplayString rIfsName(4)
|  |  |           +-- rwn Integer32     rMetric(5)
|  |  |           +-- --- Integer32     rIndex(6)
|  |  |
|  |  +--natSetting(6)
|  |  |  |
|  |  |  +--natTable(1)
|  |  |     |
|  |  |     +--natEntry(1) [natIndex]
|  |  |        |
|  |  |        +-- r-n Integer32     natIndex(1)
|  |  |        +-- r-n Enumeration   natEnable(2)
|  |  |        +-- r-n DisplayString natDesc(3)
|  |  |        +-- r-n Enumeration   natMode(4)
|  |  |        +-- r-n Enumeration   natProtocolTcp(10)
|  |  |        +-- r-n Enumeration   natProtocolUdp(11)
|  |  |        +-- r-n Enumeration   natProtocolIcmp(12)
|  |  |        +-- r-n Enumeration   natNatLoopback(50)
|  |  |        +-- r-n Enumeration   natDoubleNat(51)
|  |  |        +-- r-n Integer32     natVrrpBinding(52)
|  |  |        +-- r-n DisplayString natOriIface(100)
|  |  |        +-- r-n IpAddress     natOriSrcIp1(110)
|  |  |        +-- r-n IpAddress     natOriSrcIp2(111)
|  |  |        +-- r-n IpAddress     natOriSrcMask(112)
|  |  |        +-- r-n Integer32     natOriSrcPort1(114)
|  |  |        +-- r-n Integer32     natOriSrcPort2(115)
|  |  |        +-- r-n IpAddress     natOriDstIp1(130)
|  |  |        +-- r-n IpAddress     natOriDstIp2(131)
|  |  |        +-- r-n IpAddress     natOriDstMask(132)
|  |  |        +-- r-n Integer32     natOriDstPort1(134)
|  |  |        +-- r-n Integer32     natOriDstPort2(135)
|  |  |        +-- r-n DisplayString natTransIface(150)
|  |  |        +-- r-n IpAddress     natTransSrcIp1(160)
|  |  |        +-- r-n IpAddress     natTransSrcIp2(161)
|  |  |        +-- r-n IpAddress     natTransSrcMask(162)
|  |  |        +-- r-n Enumeration   natTransSrcDyn(163)
|  |  |        +-- r-n Integer32     natTransSrcPort1(164)
|  |  |        +-- r-n Integer32     natTransSrcPort2(165)
|  |  |        +-- r-n IpAddress     natTransDstIp1(180)
|  |  |        +-- r-n IpAddress     natTransDstIp2(181)
|  |  |        +-- r-n IpAddress     natTransDstMask(182)
|  |  |        +-- r-n Integer32     natTransDstPort1(184)
|  |  |        +-- r-n Integer32     natTransDstPort2(185)
|  |  |
|  |  +--filterSetting(7)
|  |  |  |
|  |  |  +--firewallPolicy(1)
|  |  |  |  |
```

```
|  |  |  +-- r-n Enumeration firewallGlobalLogEnable(20)
|  |  |  +-- r-n Enumeration firewallGlobalMalEnable(21)
|  |  |  +-- r-n Enumeration firewallGlobalMalLevel(22)
|  |  |  +-- r-n Enumeration firewallGlobalMalFlash(23)
|  |  |  +-- r-n Enumeration firewallGlobalMalSyslog(24)
|  |  |  +-- r-n Enumeration firewallGlobalMalTrap(25)
|  |  |
|  |  +--dosSetting(2)
|  |     |
|  |     +-- r-n Enumeration dosNullScanEnable(1)
|  |     +-- r-n Enumeration dosXmasScanEnable(2)
|  |     +-- r-n Enumeration dosNmapXmasScanEnable(3)
|  |     +-- r-n Enumeration dosSynFinScanEnable(4)
|  |     +-- r-n Enumeration dosFinScanEnable(5)
|  |     +-- r-n Enumeration dosNmapIdScanEnable(6)
|  |     +-- r-n Enumeration dosSynRstScanEnable(7)
|  |     +-- r-n Enumeration dosIcmpDeathScanEnable(8)
|  |     +-- r-n Integer32   dosIcmpLimit(9)
|  |     +-- r-n Enumeration dosSynFloodScanEnable(10)
|  |     +-- r-n Integer32   dosSynLimit(11)
|  |     +-- r-n Enumeration dosArpFloodScanEnable(12)
|  |     +-- r-n Integer32   dosArpLimit(13)
|  |     +-- r-n Enumeration dosNewTCPWithoutSYNScan(14)
|  |     +-- r-n Enumeration dosUdpFloodScanEnable(15)
|  |     +-- r-n Integer32   dosUdpLimit(16)
|  |
|  +--vpnSetting(8)
|  |  |
|  |  +--vpnIpsec(1)
|  |  |  |
|  |  |  +--ipsecGlobal(1)
|  |  |  |  |
|  |  |  |  +-- r-n Enumeration ipsecGlobalState(1)
|  |  |  |  +-- r-n Enumeration ipsecGlobalNatt(2)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLog(3)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogFlash(4)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogSyslog(5)
|  |  |  |  +-- r-n Enumeration ipsecGlobalEventLogSNMPTrap(6)
|  |  |  |
|  |  |  +--ipsecSetting(2)
|  |  |  |  |
|  |  |  |  +--ipsecSettingTable(1)
|  |  |  |     |
|  |  |  |     +--ipsecSettingEntry(1) [ipsecSettingEnable]
|  |  |  |        |
|  |  |  |        +-- r-n Enumeration   ipsecSettingEnable(1)
|  |  |  |        +-- r-n IpAddress     ipsecSettingRemoteEndIp(2)
|  |  |  |        +-- r-n Enumeration   ipsecSettingL2tp(4)
|  |  |  |        +-- r-n Enumeration   ipsecSettingPfs(5)
|  |  |  |        +-- r-n DisplayString ipsecSettingName(6)
|  |  |  |        +-- r-n Enumeration   ipsecSettingSecurityLevel(7)
|  |  |  |        +-- r-n Enumeration   ipsecConnIfs(8)
|  |  |  |        +-- r-n Enumeration   ipsecStartup(9)
|  |  |  |        +-- r-n IpAddress     ipsecLocalNetwork(10)
|  |  |  |        +-- r-n IpAddress     ipsecLocalMask(11)
|  |  |  |        +-- r-n DisplayString ipsecLocalId(13)
|  |  |  |        +-- r-n IpAddress     ipsecRemoteNetwork(14)
|  |  |  |        +-- r-n IpAddress     ipsecRemoteMask(15)
|  |  |  |        +-- r-n DisplayString ipsecRemoteId(17)
|  |  |  |        +-- r-n Enumeration   ipsecAuthMode(18)
|  |  |  |        +-- r-n DisplayString ipsecPsk(19)
|  |  |  |        +-- r-n DisplayString ipsecLocalSelectPem(20)
|  |  |  |        +-- r-n DisplayString ipsecRemoteSelectPem(21)
|  |  |  |        +-- r-n Enumeration   ipsecExchange(22)
|  |  |  |        +-- r-n Enumeration   ipsecP1Encrypt(23)
|  |  |  |        +-- r-n Enumeration   ipsecP1Ah(24)
|  |  |  |        +-- r-n Enumeration   ipsecP1Dh(25)
|  |  |  |        +-- r-n Integer32     ipsecIKELifetime(27)
|  |  |  |        +-- r-n Integer32     ipsecSaLifetime(30)
|  |  |  |        +-- r-n Enumeration   ipsecP2Encrypt(31)
```

```
|  |  |  |        +-- r-n Enumeration   ipsecP2Ah(32)
|  |  |  |        +-- r-n Enumeration   ipsecDpdAction(33)
|  |  |  |        +-- r-n Integer32     ipsecDpdDelay(34)
|  |  |  |        +-- r-n Integer32     ipsecDpdTimeout(35)
|  |  |  |        +-- r-n Enumeration   ipsecIdentityType(36)
|  |  |  |        +-- r-n Enumeration   ipsecPfsDHGroup(37)
|  |  |  |        +-- r-n DisplayString ipsecLocalSubnet(38)
|  |  |  |        +-- r-n DisplayString ipsecRemoteSubnet(39)
|  |  |  |
|  |  |  +--ipsecStatus(3)
|  |  |     |
|  |  |     +--ipsecStatusTable(1)
|  |  |        |
|  |  |        +--ipsecStatusEntry(1) [ipsecStatusIndex]
|  |  |           |
|  |  |           +-- r-n DisplayString ipsecStatusName(1)
|  |  |           +-- r-n DisplayString ipsecStatusLocSubnet(2)
|  |  |           +-- r-n IpAddress     ipsecStatusLocGateway(3)
|  |  |           +-- r-n IpAddress     ipsecStatusRemGateway(4)
|  |  |           +-- r-n DisplayString ipsecStatusRemSubnet(5)
|  |  |           +-- r-n DisplayString ipsecStatusPhase1(6)
|  |  |           +-- r-n DisplayString ipsecStatusPhase2(7)
|  |  |           +-- r-n Enumeration   ipsecl2tp(8)
|  |  |           +-- --- Integer32     ipsecStatusIndex(9)
|  |  |
|  |  +--vpnL2tp(2)
|  |     |
|  |     +-- r-n Enumeration l2tpModeWan1(1)
|  |     +-- r-n IpAddress   l2tpLocalIpWan1(2)
|  |     +-- r-n IpAddress   l2tpOfferIpStartWan1(3)
|  |     +-- r-n IpAddress   l2tpOfferIpEndWan1(4)
|  |     |
|  |     +--l2tpTable(9)
|  |        |
|  |        +--l2tpEntry(1) [l2tpLoginUserName]
|  |           |
|  |           +-- r-n DisplayString l2tpLoginUserName(1)
|  |
|  +--snmpSetting(9)
|  |  |
|  |  +--snmpSetup(1)
|  |     |
|  |     +-- r-n Enumeration   snmpVersion(1)
|  |     +-- rwn Enumeration   snmpAuthType(3)
|  |     +-- rwn Integer32     snmpAccessControl1(7)
|  |     +-- rwn Integer32     snmpAccessControl2(9)
|  |     +-- rwn DisplayString trap1ServerAddr(10)
|  |     +-- rwn DisplayString trap2ServerAddr(11)
|  |     +-- rwn DisplayString trap3ServerAddr(12)
|  |     +-- rwn Enumeration   snmpInformEnable(13)
|  |     +-- rwn DisplayString snmpReadCommunity1(14)
|  |     +-- rwn DisplayString snmpReadCommunity2(15)
|  |     +-- rwn DisplayString snmpTrapCommunity(16)
|  |     +-- rwn Enumeration   snmpTrapMode(17)
|  |     +-- r-n Enumeration   snmpAdminSecurityLevel(22)
|  |     +-- r-n Enumeration   snmpUserSecurityLevel(23)
|  |
|  +--diagnosisSetting(12)
|  |  |
|  |  +--lldpSetting(2)
|  |     |
|  |     +-- rwn Enumeration lldpEnable(1)
|  |     +-- rwn Integer32   lldpInterval(2)
|  |     +-- rwn Enumeration lldpRingPortBypass(3)
|  |
|  +--monitor(13)
|  |  |
|  |  +-- r-n Enumeration power1InputStatus(7)
|  |  +-- r-n Enumeration power2InputStatus(8)
|  |  |
```

```
|  |  +--monitorFiberCheckTable(11)
|  |     |
|  |     +--monitorFiberCheckEntry(1) [portIndex]
|  |        |
|  |        +-- r-n DisplayString fiberPort(1)
|  |        +-- r-n DisplayString fiberModelName(2)
|  |        +-- r-n DisplayString fiberWaveLength(3)
|  |        +-- r-n DisplayString fiberVoltage(4)
|  |        +-- r-n DisplayString fiberTemperature(5)
|  |        +-- r-n DisplayString fiberTempWarn(6)
|  |        +-- r-n DisplayString fiberTxPower(7)
|  |        +-- r-n DisplayString fiberTxPowerWarn(8)
|  |        +-- r-n DisplayString fiberRxPower(9)
|  |        +-- r-n DisplayString fiberRxPowerWarn(10)
|  |        +-- r-n DisplayString fiberSN(13)
|  |
|  +--systemLog(14)
|  |  |
|  |  +--mxSyslog(2)
|  |     |
|  |     +-- r-n Enumeration   syslogServer1Enable(1)
|  |     +-- r-n DisplayString syslogServer1(2)
|  |     +-- r-n Integer32     syslogServer1Port(3)
|  |     +-- r-n Enumeration   syslogServer2Enable(4)
|  |     +-- r-n DisplayString syslogServer2(5)
|  |     +-- r-n Integer32     syslogServer2Port(6)
|  |     +-- r-n Enumeration   syslogServer3Enable(7)
|  |     +-- r-n DisplayString syslogServer3(8)
|  |     +-- r-n Integer32     syslogServer3Port(9)
|  |     +-- r-n DisplayString syslogServer1Cert(10)
|  |     +-- r-n DisplayString syslogServer2Cert(11)
|  |     +-- r-n DisplayString syslogServer3Cert(12)
|  |     +-- r-n Enumeration   syslogServer1MsgFormat(13)
|  |     +-- r-n Enumeration   syslogServer2MsgFormat(14)
|  |     +-- r-n Enumeration   syslogServer3MsgFormat(15)
|  |     +-- r-n Enumeration   syslogServer1ConnProto(16)
|  |     +-- r-n Enumeration   syslogServer2ConnProto(17)
|  |     +-- r-n Enumeration   syslogServer3ConnProto(18)
|  |
|  +--networkMode(15)
|  |  |
|  |  +-- r-n Enumeration networkModeSelection(1)
|  |
|  +--routingRedundancy(16)
|  |  |
|  |  +--vrrp(1)
|  |     |
|  |     +--vrrpInterfaceTable(1)
|  |     |  |
|  |     |  +--vrrpInterfaceEntry(1) [vrrpIfIndex]
|  |     |     |
|  |     |     +-- rwn DisplayString vrrpIfName(1)
|  |     |     +-- r-n IpAddress     vrrpIfAddr(2)
|  |     |     +-- rwn Enumeration   vrrpIfEnable(3)
|  |     |     +-- rwn IpAddress     vrrpIfVirtualIp(4)
|  |     |     +-- rwn Integer32     vrrpIfRouterId(5)
|  |     |     +-- rwn Integer32     vrrpIfPriority(6)
|  |     |     +-- rwn Enumeration   vrrpIfPreemption(7)
|  |     |     +-- r-n Enumeration   vrrpIfStatus(8)
|  |     |     +-- rwn DisplayString vrrpIfTrack(9)
|  |     |     +-- rwn IpAddress     vrrpPingTrackIP(10)
|  |     |     +-- rwn Integer32     vrrpPingTrackInt(11)
|  |     |     +-- rwn Integer32     vrrpPingTimeout(12)
|  |     |     +-- rwn Integer32     vrrpPingTrackSuccess(13)
|  |     |     +-- rwn Integer32     vrrpPingTrackFailure(14)
|  |     |     +-- rwn Integer32     vrrpAdvInt(15)
|  |     |     +-- rwn Integer32     vrrpPreemptDelay(16)
|  |     |     +-- --- Integer32     vrrpIfIndex(17)
|  |     |
|  |     +-- rwn Enumeration vrrpEnable(2)
```

```
|  |
|  +--portSetting(17)
|  |  |
|  |  +--portTable(1)
|  |     |
|  |     +--portEntry(1) [portIndex]
|  |        |
|  |        +-- r-n DisplayString portDesc(1)
|  |        +-- rwn Enumeration   portEnable(2)
|  |        +-- r-n Enumeration   portSpeed(3)
|  |        +-- r-n Enumeration   portMDI(4)
|  |        +-- r-n Enumeration   portFDXFlowCtrl(5)
|  |        +-- rwn DisplayString portName(6)
|  |        +-- r-n Enumeration   portType(7)
|  |        +-- r-n Integer32     portIndex(8)
|  |
|  +--portTrunking(19)
|  |  |
|  |  +--trunkSettingTable(1)
|  |  |  |
|  |  |  +--trunkSettingEntry(1) [trunkSettingIndex]
|  |  |     |
|  |  |     +-- r-n Integer32   trunkSettingIndex(1)
|  |  |     +-- r-n Enumeration trunkType(2)
|  |  |     +-- r-n PortList    trunkMemberPorts(3)
|  |  |
|  |  +--trunkTable(2)
|  |     |
|  |     +--trunkEntry(1) [trunkIndex,trunkPort]
|  |        |
|  |        +-- r-n Integer32   trunkIndex(1)
|  |        +-- r-n Integer32   trunkPort(2)
|  |        +-- r-n Enumeration trunkStatus(3)
|  |
|  +--commRedundancy(20)
|  |  |
|  |  +--spanningTree(3)
|  |  |  |
|  |  |  +-- r-n Enumeration spanningTreeRoot(1)
|  |  |  +-- r-n Enumeration spanningTreeBridgePriority(2)
|  |  |  +-- r-n Integer32   spanningTreeHelloTime(3)
|  |  |  +-- r-n Integer32   spanningTreeMaxAge(4)
|  |  |  +-- r-n Integer32   spanningTreeForwardingDelay(5)
|  |  |  |
|  |  |  +--spanningTreeTable(6)
|  |  |     |
|  |  |     +--spanningTreeEntry(1) [enableSpanningTree]
|  |  |        |
|  |  |        +-- r-n Enumeration enableSpanningTree(2)
|  |  |        +-- r-n Enumeration spanningTreePortPriority(3)
|  |  |        +-- r-n Integer32   spanningTreePortCost(4)
|  |  |        +-- r-n Enumeration spanningTreePortStatus(5)
|  |  |        +-- r-n Enumeration spanningTreePortEdge(6)
|  |  |
|  |  +-- r-n Enumeration activeProtocolOfRedundancy(4)
|  |  |
|  |  +--turboRingV2(5)
|  |  |  |
|  |  |  +--turboRingV2Ring1(1)
|  |  |  |  |
|  |  |  |  +-- r-n Integer32   ringIndexRing1(1)
|  |  |  |  +-- r-n Enumeration ringEnableRing1(2)
|  |  |  |  +-- r-n Enumeration masterSetupRing1(3)
|  |  |  |  +-- r-n Enumeration masterStatusRing1(4)
|  |  |  |  +-- r-n MacAddress  designatedMasterRing1(5)
|  |  |  |  +-- r-n Integer32   rdnt1stPortRing1(6)
|  |  |  |  +-- r-n Enumeration rdnt1stPortStatusRing1(7)
|  |  |  |  +-- r-n Integer32   rdnt2ndPortRing1(8)
|  |  |  |  +-- r-n Enumeration rdnt2ndPortStatusRing1(9)
|  |  |  |  +-- r-n Enumeration brokenStatusRing1(10)
```

```
|  |  |  |
|  |  |  +--turboRingV2Ring2(2)
|  |  |  |  |
|  |  |  |  +-- r-n Integer32   ringIndexRing2(1)
|  |  |  |  +-- r-n Enumeration ringEnableRing2(2)
|  |  |  |  +-- r-n Enumeration masterSetupRing2(3)
|  |  |  |  +-- r-n Enumeration masterStatusRing2(4)
|  |  |  |  +-- r-n MacAddress  designatedMasterRing2(5)
|  |  |  |  +-- r-n Integer32   rdnt1stPortRing2(6)
|  |  |  |  +-- r-n Enumeration rdnt1stPortStatusRing2(7)
|  |  |  |  +-- r-n Integer32   rdnt2ndPortRing2(8)
|  |  |  |  +-- r-n Enumeration rdnt2ndPortStatusRing2(9)
|  |  |  |  +-- r-n Enumeration brokenStatusRing2(10)
|  |  |  |
|  |  |  +--turboRingV2Coupling(3)
|  |  |     |
|  |  |     +-- r-n Enumeration couplingEnable(1)
|  |  |     +-- r-n Enumeration couplingMode(2)
|  |  |     +-- r-n Integer32   coupling1stPort(3)
|  |  |     +-- r-n Enumeration coupling1stPortStatus(4)
|  |  |     +-- r-n Integer32   coupling2ndPort(5)
|  |  |     +-- r-n Enumeration coupling2ndPortStatus(6)
|  |  |
|  |  +--turboChain(6)
|  |     |
|  |     +-- rwn Enumeration turboChainRole(1)
|  |     +-- rwn Integer32   turboChainPort1(2)
|  |     +-- rwn Integer32   turboChainPort2(3)
|  |     +-- r-n Enumeration turboChainPort1Status(4)
|  |     +-- r-n Enumeration turboChainPort2Status(5)
|  |
|  +--vlan(21)
|  |  |
|  |  +--vlanPortSettingTable(1)
|  |  |  |
|  |  |  +--vlanPortSettingEntry(1) [portIndex]
|  |  |     |
|  |  |     +-- r-n Enumeration   portVlanType(1)
|  |  |     +-- r-n Integer32     portDefaultVid(2)
|  |  |     +-- r-n DisplayString portFixedVid(3)
|  |  |     +-- r-n DisplayString portFixedVidUntag(5)
|  |  |
|  |  +--vlanTable(2)
|  |  |  |
|  |  |  +--vlanEntry(1) [vlanId]
|  |  |     |
|  |  |     +-- r-n Integer32 vlanId(1)
|  |  |     +-- r-n PortList  joinedAccessPorts(2)
|  |  |     +-- r-n PortList  joinedTrunkPorts(3)
|  |  |     +-- r-n PortList  joinedHybirdPorts(4)
|  |  |
|  |  +-- r-n Integer32   managementVlanId(3)
|  |  +-- r-n Enumeration vlanType(4)
|  |
|  +--swMgmtGroup(22)
|  |  |
|  |  +-- r-n Integer32     numberOfPorts(1)
|  |  +-- r-n DisplayString switchModel(2)
|  |  +-- r-n DisplayString firmwareVersion(4)
|  |
|  +--globalStatus(23)
|  |  |
|  |  +-- r-n Enumeration firewallGlobalStatus(1)
|  |  +-- r-n Enumeration natGlobalStatus(2)
|  |  +-- r-n Enumeration vpnGlobalStatus(3)
|  |  +-- r-n Enumeration securityNotificationFirewallStatus(4)
|  |  +-- r-n Enumeration securityNotificationDoSAttackStatus(5)
|  |  +-- r-n Enumeration securityNotificationAccessViolationStatus(6)
|  |  +-- r-n Enumeration securityNotificationLoginFailStatus(7)
|  |  +-- r-n Enumeration defaultPasswordChange(8)
```

```
|  |  +-- r-n Enumeration securityNotificationDeviceLockdownStatus(9)
|  |  +-- r-n Enumeration securityNotificationLayer3FilterStatus(10)
|  |
|  +--interfaceStatus(24)
|  |  |
|  |  +--interfaceStatusTable(1)
|  |  |  |
|  |  |  +--interfaceStatusEntry(1) [interfaceOverallStatus]
|  |  |     |
|  |  |     +-- r-n DisplayString interfaceOverallStatus(1)
|  |  |     +-- r-n Enumeration   interfaceOverallType(2)
|  |  |
|  |  +--cellularStatus(2)
|  |     |
|  |     +-- r-n DisplayString cellularMode(1)
|  |     +-- r-n DisplayString cellularCarrier(2)
|  |     +-- r-n DisplayString cellularRSSI(3)
|  |     +-- r-n DisplayString cellularIP(4)
|  |     +-- r-n DisplayString cellularIMEI(5)
|  |     +-- r-n DisplayString cellularIMSI(6)
|  |     +-- r-n Enumeration   cellularConnectionStatus(7)
|  |     +-- r-n DisplayString cellularSim1Status(8)
|  |     +-- r-n DisplayString cellularSim2Status(9)
|  |     +-- r-n DisplayString cellularRSRP(10)
|  |     +-- r-n DisplayString cellularRSRQ(11)
|  |     +-- r-n DisplayString cellularSINR(12)
|  |
|  +--securityNotification(25)
|  |  |
|  |  +-- r-n Enumeration eventFirewall(1)
|  |  +-- r-n Enumeration eventDoSAttack(2)
|  |  +-- r-n Enumeration eventAccessViolation(3)
|  |  +-- r-n Enumeration eventLoginFail(4)
|  |  +-- r-n Enumeration eventDeviceLockdown(5)
|  |  +-- r-n Enumeration eventLayer3Filter(6)
|  |
|  +--mtuAdjustment(28)
|  |  |
|  |  +--mtuAdjustmentTable(1)
|  |     |
|  |     +--mtuAdjustmentEntry(1) [mtuAdjustmentIndex]
|  |        |
|  |        +-- r-n DisplayString mtuAdjustmentIfName(1)
|  |        +-- rwn Integer32     mtuAdjustmentMTUsize(2)
|  |        +-- rwn Enumeration   mtuAdjustmentPRPtraffic(3)
|  |        +-- --- Integer32     mtuAdjustmentIndex(4)
|  |
|  +--poeSetting(40)
|  |  |
|  |  +--poePortTable(3)
|  |  |  |
|  |  |  +--poePortEntry(1) [poePortIndex]
|  |  |     |
|  |  |     +-- r-n Integer32     poePortIndex(1)
|  |  |     +-- rwn Enumeration   poePortEnable(2)
|  |  |     +-- rwn Integer32     powerLimit(4)
|  |  |     +-- rwn Enumeration   pdfailure(5)
|  |  |     +-- rwn DisplayString pdipaddr(6)
|  |  |     +-- rwn Integer32     pdPollingInterval(7)
|  |  |     +-- rwn Enumeration   poePortLegacyPdDetect(9)
|  |  |     +-- rwn Integer32     pdNoResponseTimeout(10)
|  |  |     +-- rwn Enumeration   pdNoResponseAction(11)
|  |  |     +-- rwn Enumeration   poePowerOutputMode(12)
|  |  |
|  |  +--poeStatusTable(6)
|  |  |  |
|  |  |  +--poeStatusEntry(1) [poePortIndex]
|  |  |     |
|  |  |     +-- r-n Enumeration poePortStatus(1)
|  |  |     +-- r-n Enumeration poePortConsumption(2)
```

```
|  |  |     +-- r-n Enumeration poePortVoltage(3)
|  |  |     +-- r-n Enumeration poePortCurrent(4)
|  |  |     +-- r-n Enumeration poePortPowerOutput(5)
|  |  |     +-- r-n Enumeration poePortClass(6)
|  |  |     +-- r-n Enumeration poePortPdFailCheck(7)
|  |  |     +-- r-n Enumeration poePortPdStatusDescription(8)
|  |  |
|  |  +--poeSystemSetting(9)
|  |     |
|  |     +-- rwn Enumeration poeSysPowerEnable(1)
|  |     +-- rwn Integer32   poeSysPowerThreshold(2)
|  |     +-- rwn Enumeration poeSysThresholdCutOff(3)
|  |     +-- r-n Integer32   poeSysAllocatedPower(4)
|  |     +-- r-n Integer32   poeSysMeasuredPower(5)
|  |     +-- rwn Integer32   poeSysPowerBudget(7)
|  |
|  +--eventlog(46)
|  |  |
|  |  +--eventlogSystem(1)
|  |  |  |
|  |  |  +--eventlogSystemTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogSystemEntry(1) [eventlogSystemIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogSystemIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogSystemTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogSystemSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogSystemEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogSystemClear(2)
|  |  |
|  |  +--eventlogVPN(2)
|  |  |  |
|  |  |  +--eventlogVPNTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogVPNEntry(1) [eventlogVPNIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogVPNIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogVPNTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogVPNSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogVPNEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogVPNClear(2)
|  |  |
|  |  +--eventlogTruseAccess(3)
|  |  |  |
|  |  |  +--eventlogTruseAccessTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogTruseAccessEntry(1) [eventlogTruseAccessIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogTruseAccessIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogTruseAccessTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogTruseAccessSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogTruseAccessEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogTruseAccessClear(2)
|  |  |
|  |  +--eventlogMalformed(4)
|  |  |  |
|  |  |  +--eventlogMalformedTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogMalformedEntry(1) [eventlogMalformedIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogMalformedIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogMalformedTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogMalformedSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogMalformedEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogMalformedClear(2)
|  |  |  |
```

```
      |  |  +--eventlogDOS(5)
      |  |  |  |
      |  |  |  +--eventlogDOSTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogDOSEntry(1) [eventlogDOSIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogDOSIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogDOSTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogDOSSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogDOSEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogDOSClear(2)
      |  |  |
      |  |  +--eventlogDevLockdown(6)
      |  |  |  |
      |  |  |  +--eventlogDevLockdownTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogDevLockdownEntry(1) [eventlogDevLockdownIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogDevLockdownIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogDevLockdownTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogDevLockdownSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogDevLockdownEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogDevLockdownClear(2)
      |  |  |
      |  |  +--eventlogL3Policy(7)
      |  |  |  |
      |  |  |  +--eventlogL3PolicyTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogL3PolicyEntry(1) [eventlogL3PolicyIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogL3PolicyIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogL3PolicyTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogL3PolicySeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogL3PolicyEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogL3PolicyClear(2)
      |  |  |
      |  |  +--eventlogProtocolFilterPolicy(8)
      |  |  |  |
      |  |  |  +--eventlogProtocolFilterPolicyTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogProtocolFilterPolicyEntry(1)
    [eventlogProtocolFilterPolicyIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogProtocolFilterPolicyIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogProtocolFilterPolicyTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogProtocolFilterPolicySeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogProtocolFilterPolicyEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogProtocolFilterPolicyClear(2)
      |  |  |
      |  |  +--eventlogADP(9)
      |  |  |  |
      |  |  |  +--eventlogADPTable(1)
      |  |  |  |  |
      |  |  |  |  +--eventlogADPEntry(1) [eventlogADPIndex]
      |  |  |  |     |
      |  |  |  |     +-- r-n Integer32     eventlogADPIndex(1)
      |  |  |  |     +-- r-n DisplayString eventlogADPTimestamp(2)
      |  |  |  |     +-- r-n Integer32     eventlogADPSeverity(3)
      |  |  |  |     +-- r-n DisplayString eventlogADPEvent(4)
      |  |  |  |
      |  |  |  +-- rwn Enumeration eventlogADPClear(2)
      |  |  |
      |  |  +--eventlogIPS(10)
      |  |  |  |
      |  |  |  +--eventlogIPSTable(1)
      |  |  |  |  |
```

```
|  |  |  |  +--eventlogIPSEntry(1) [eventlogIPSIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogIPSIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogIPSTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogIPSSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogIPSEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogIPSClear(2)
|  |  |
|  |  +--eventlogSessionControl(11)
|  |  |  |
|  |  |  +--eventlogSessionControlTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogSessionControlEntry(1) [eventlogSessionControlIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogSessionControlIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogSessionControlTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogSessionControlSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogSessionControlEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogSessionControlClear(2)
|  |  |
|  |  +--eventlogL2Filter(12)
|  |  |  |
|  |  |  +--eventlogL2FilterTable(1)
|  |  |  |  |
|  |  |  |  +--eventlogL2FilterEntry(1) [eventlogL2FilterIndex]
|  |  |  |     |
|  |  |  |     +-- r-n Integer32     eventlogL2FilterIndex(1)
|  |  |  |     +-- r-n DisplayString eventlogL2FilterTimestamp(2)
|  |  |  |     +-- r-n Integer32     eventlogL2FilterSeverity(3)
|  |  |  |     +-- r-n DisplayString eventlogL2FilterEvent(4)
|  |  |  |
|  |  |  +-- rwn Enumeration eventlogL2FilterClear(2)
|  |  |
|  |  +--eventlogPingResponse(15)
|  |     |
|  |     +--eventlogPingResponseTable(1)
|  |     |  |
|  |     |  +--eventlogPingResponseEntry(1) [eventlogPingResponseIndex]
|  |     |     |
|  |     |     +-- r-n Integer32     eventlogPingResponseIndex(1)
|  |     |     +-- r-n DisplayString eventlogPingResponseTimestamp(2)
|  |     |     +-- r-n Integer32     eventlogPingResponseSeverity(3)
|  |     |     +-- r-n DisplayString eventlogPingResponseEvent(4)
|  |     |
|  |     +-- rwn Enumeration eventlogPingResponseClear(2)
|  |
|  +-- r-n Integer32     cpuLoading5s(53)
|  +-- r-n Integer32     cpuLoading30s(54)
|  +-- r-n Integer32     cpuLoading300s(55)
|  +-- r-n Integer32     totalMemory(56)
|  +-- r-n Integer32     freeMemory(57)
|  +-- r-n Integer32     usedMemory(58)
|  +-- r-n Integer32     memoryUsage(59)
|  |
|  +--managementInterface(63)
|  |  |
|  |  +-- rwn Enumeration   httpEnable(1)
|  |  +-- rwn Integer32     httpPort(2)
|  |  +-- rwn Enumeration   sslEnable(3)
|  |  +-- rwn Integer32     sslPort(4)
|  |  +-- rwn Enumeration   telnetEnable(5)
|  |  +-- rwn Integer32     telnetPort(6)
|  |  +-- rwn Enumeration   sshEnable(7)
|  |  +-- rwn Integer32     sshPort(8)
|  |  +-- rwn Integer32     mgmtInterfaceAutoLogout(9)
|  |  +-- r-n DisplayString moxaUtilityServicePort(13)
|  |  +-- rwn Integer32     httpMaxLoginUsers(14)
|  |  +-- rwn Integer32     telnetMaxLoginUsers(15)
```

```
|  |  +-- rwn Enumeration   moxaUtilityServiceEnable(16)
|  |
|  +--pingResponse(64)
|  |  |
|  |  +--pingResponsePolicyTable(1)
|  |  |  |
|  |  |  +--pingResponsePolicyEntry(1) [pingResponsePolicyIndex]
|  |  |     |
|  |  |     +-- r-n Integer32     pingResponsePolicyIndex(1)
|  |  |     +-- r-n Enumeration   pingResponsePolicyExist(2)
|  |  |     +-- r-n Enumeration   pingResponsePolicyEnable(3)
|  |  |     +-- r-n DisplayString pingResponsePolicyIf(4)
|  |  |     +-- r-n Enumeration   pingResponsePolicyIpType(5)
|  |  |     +-- r-n IpAddress     pingResponsePolicyIp(6)
|  |  |     +-- r-n IpAddress     pingResponsePolicyMask(7)
|  |  |     +-- r-n Enumeration   pingResponsePolicyAction(8)
|  |  |
|  |  +-- rwn Enumeration pingResponseIfEnable(2)
|  |  |
|  |  +--pingResponseIfTable(3)
|  |  |  |
|  |  |  +--pingResponseIfEntry(1) [pingResponseIf]
|  |  |     |
|  |  |     +-- rwn DisplayString pingResponseIf(1)
|  |  |
|  |  +-- rwn Enumeration pingResponslLogEnable(4)
|  |  +-- rwn Enumeration pingResponslLogLevel(5)
|  |  +-- rwn Enumeration pingResponslLogFlash(6)
|  |  +-- rwn Enumeration pingResponslLogSyslog(7)
|  |  +-- rwn Enumeration pingResponslLogTrap(8)
|  |
|  +--passwordPolicy(70)
|  |  |
|  |  +-- rwn Integer32   pwdMinLength(1)
|  |  +-- rwn Enumeration pwdComplexityCheckEnable(2)
|  |  +-- rwn Enumeration pwdComplexityCheckDigitEnable(3)
|  |  +-- rwn Enumeration pwdComplexityCheckAlphabetEnable(4)
|  |  +-- rwn Enumeration pwdComplexityCheckSpecialCharEnable(5)
|  |
|  +--loginLockout(71)
|  |  |
|  |  +-- rwn Enumeration loginFailureLockoutEnable(1)
|  |  +-- rwn Integer32   loginFailureLockoutRetrys(2)
|  |  +-- rwn Integer32   loginFailureLockoutTime(3)
|  |
|  +--systemNotifyMessage(72)
|  |  |
|  |  +-- r-n DisplayString httpLoginMessage(1)
|  |  +-- r-n DisplayString httpLoginFailureMessage(2)
|  |
|  +-- r-n DisplayString serialNumber(78)
|  +-- r-n Enumeration   configEncryptEnable(79)
|  |
|  +--security(80)
|  |  |
|  |  +--portAccessControl(2)
|  |     |
|  |     +--dot1x(2)
|  |        |
|  |        +-- rwn Enumeration dataBaseOption(1)
|  |        +-- rwn Enumeration dot1xReauthEnable(5)
|  |        +-- rwn Integer32   dot1xReauthPeriod(6)
|  |        |
|  |        +--dot1xSettingTable(7)
|  |        |  |
|  |        |  +--dot1xSettingEntry(1) [portIndex]
|  |        |     |
|  |        |     +-- rwn Enumeration enableDot1X(1)
|  |        |
|  |        +--dot1xReauthTable(8)
```

```
|  |        |  |
|  |        |  +--dot1xReauthEntry(1) [dot1xReauthPortIndex]
|  |        |     |
|  |        |     +-- r-n Integer32   dot1xReauthPortIndex(1)
|  |        |     +-- rwn Enumeration dot1xReauth(2)
|  |        |
|  |        +--dot1xRadius(9)
|  |           |
|  |           +-- rwn DisplayString dot1x1stRadiusServer(2)
|  |           +-- rwn Integer32     dot1x1stRadiusPort(3)
|  |           +-- rwn DisplayString dot1x1stRadiusSharedKey(4)
|  |           +-- rwn DisplayString dot1x2ndRadiusServer(5)
|  |           +-- rwn Integer32     dot1x2ndRadiusPort(6)
|  |           +-- rwn DisplayString dot1x2ndRadiusSharedKey(7)
|  |
|  +--powerMgmtSetting(81)
|  |  |
|  |  +-- rwn Enumeration powerMgmtEnable(1)
|  |
|  +--serialSetting(82)
|  |  |
|  |  +-- rwn Enumeration serialPortIfType(1)
|  |  +-- rwn Enumeration serialPortOpMode(2)
|  |  +-- rwn Enumeration serialDataLog(3)
|  |  +-- rwn Enumeration serialPortBuffer(4)
|  |
|  +--linkFaultPassthrough(83)
|  |  |
|  |  +-- rwn Enumeration lfpState(1)
|  |  +-- rwn Integer32   lfpPort1(2)
|  |  +-- rwn Integer32   lfpPort2(3)
|  |
|  +--softLockdownModeStatus(84)
|     |
|     +-- r-n Enumeration softLockdownModeStatusStatus(1)
|     +-- r-n Enumeration softLockdownModeStatusTr2(2)
|     +-- r-n Enumeration softLockdownModeStatusDhcpSvr(3)
|     +-- r-n Enumeration softLockdownModeStatusDhcpRelayAgent(4)
|     +-- r-n Enumeration softLockdownModeStatusSnmpSvr(5)
|
+--mibNotificationsPrefix(3)
   |
   +--configChangeTrap(1) [varconfigChangeTrap]
   |
   +--power1Trap(2) [varpower1Trap]
   |
   +--power2Trap(3) [varpower2Trap]
   |
   +--di1Trap(4) [vardi1Trap]
   |
   +--di2Trap(5) [vardi2Trap]
   |
   +--redundancyTopologyChangedTrap(10) [varredundancyTopologyChangedTrap]
   |
   +--turboRingCouplingPortChangedTrap(11) [varturboRingCouplingPortChangedTrap]
   |
   +--turboRingMasterChangedTrap(12) [varturboRingMasterChangedTrap]
   |
   +--vpnConnectedTrap(40) [varVPNConnectedTrap]
   |
   +--vpnDisconnectedTrap(41) [varVPNDisconnectedTrap]
   |
   +--firewallPolicyTrap(50) [varFirewallPolicyTrap]
   |
   +--securityNotificationTrap(51) [varSecurityNotificationTrap]
   |
   +--loggingCapacityTrap(52) [varLoggingCapacityTrap]
```

MMS Command Type List

This is a list of MMS command type codes and command names.

Command Type	Command Name
1	confirmed_RequestPDU
2	confirmed_ResponsePDU
3	confirmed_ErrorPDU
4	unconfirmed_PDU
5	rejectPDU
6	cancel_RequestPDU
7	cancel_ResponsePDU
8	cancel_ErrorPDU
9	initiate_RequestPDU
10	initiate_ResponsePDU
11	initiate_ErrorPDU
12	conclude_RequestPDU
13	conclude_ResponsePDU
14	conclude_ErrorPDU

MMS Service Operation List

This is a list of MMS service operation codes and their names.

Service Operation	Service Operation Name
1	acknowledgeEventNotification
2	alterEventConditionMonitoring
3	alterEventEnrollment
4	createJournal
5	createProgramInvocation
6	defineEventAction
7	defineEventCondition
8	defineEventEnrollment
9	defineNamedType
10	defineNamedVariable
11	defineNamedVariableList
12	defineScatteredAccess
13	defineSemaphore
14	deleteDomain
15	deleteEventAction
16	deleteEventCondition
17	deleteEventEnrollment
18	deleteJournal
19	deleteNamedType
20	deleteNamedVariableList

Service Operation	Service Operation Name
21	deleteProgramInvocation
22	deleteSemaphore
23	deleteVariableAccess
24	downloadSegment
25	eventNotification
26	fileClose
27	fileDelete
28	fileDirectory
29	fileOpen
30	fileRead
31	fileRename
32	getAlarmEnrollmentSummary
33	getAlarmSummary
34	getCapabilityList
35	getDomainAttributes
36	getEventActionAttributes
37	getEventConditionAttributes
38	getEventEnrollmentAttributes
39	getNamedTypeAttributes
40	getNamedVariableListAttributes
41	getNameList
42	getProgramInvocationAttributes
43	getScatteredAccessAttributes

Service Operation	Service Operation Name
44	getVariableAccessAttributes
45	identify
46	informationReport
47	initializeJournal
48	initiateDownloadSequence
49	initiateUploadSequence
50	input
51	kill
52	loadDomainContent
53	obtainFile
54	output
55	read
56	readJournal
57	relinquishControl
58	rename
59	reportActionStatus
60	reportEventActionStatus
61	reportEventConditionStatus
62	reportEventEnrollmentStatus
63	reportJournalStatus
64	reportPoolSemaphoreStatus
65	reportSemaphoreEntryStatus
66	reportSemaphoreStatus

Service Operation	Service Operation Name
67	requestDomainDownLoad
68	requestDomainUpload
69	reset
70	resume
71	start
72	status
73	stop
74	storeDomainContent
75	takeControl
76	terminateDownloadSequence
77	terminateUploadSequence
78	triggerEvent
79	unsolicitedStatus
80	uploadSegment
81	write
82	writeJournal

PoE Configuration Suggestions

This page shows the different PoE configuration suggestions that may be given and additional information about them.

Item	Description
Disable PoE power output	A NIC or unknown PD was detected; you may want to disable PoE power output for the port.
Select Force Mode	A higher/lower resistance or higher capacitance was detected; you may want to select **Force Mode** for the port.
Select high power output	An unknown classification was detected; you may want to select High Power output.
Raise the external power supply voltage to greater than 46 VDC	When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage.
Enable PoE function for detection	The system suggests enabling the PoE function.
Select IEEE 802.3at auto mode	When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode.
Select IEEE 802.3af auto mode	When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.

Sample Local Consist Info File

The following example provides a copy-and-paste compatible Local Consist Info File for use with ETBN examples. This example assumes a single consist. Further modifications may be required for multi-consist examples.

Refer to Structure and Syntax of Local Consist Info Files for more information about XML configuration files.

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE consistinfo SYSTEM
"consistinfo.dtd"><consistinfo>    <cstId>consist1</cstId>
                  <cstOwner>Moxa</cstOwner>          <cstType>Regional
train</cstType>   <vehicleinfo tractVeh="false">
                  <cstVehNo>1</cstVehNo>
                  <vehId>vehicle1</vehId>
                  <vehOrient>same</vehOrient>
                  <vehType>Passenger vehicle</vehType>
                  <functioninfo>
                  <cnId>1</cnId>
                  <fctId>112</fctId>
                  <fctName>devECSC</fctName>
                  </functioninfo>                    <functioninfo>
                                    <cnId>1</cnId>
                  <fctId>11</fctId>
                  <fctName>devCam1</fctName>
                  </functioninfo>                    <functioninfo>
                                    <cnId>1</cnId>
                  <fctId>20</fctId>
                  <fctName>grpDoor</fctName>
                  </functioninfo>                    <functioninfo>
                                    <cnId>1</cnId>
                  <fctId>30</fctId>
                  <fctName>grpDoor1</fctName>
                  </functioninfo>   </vehicleinfo></consistinfo>
```

This page explains security practices for installing, operating, maintaining, and decommissioning the device. We strongly recommend that our customers follow these guidelines to enhance network and equipment security.

Installation

Physical Installation

1. The device MUST be installed in an access-controlled area, where only the necessary personnel have physical access to the device.
2. The device MUST be installed at the security perimeter or the boundary between different zones to provide network segmentation.
3. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
4. The device has anti-tamper labels on the enclosures. This allows an administrator to tell whether the device has been tampered with.
5. The ports that are not in use should be deactivated. Please refer to the Ports section for detailed instructions.

Acoount Management

Follow these best practices when setting up an account:

1. Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have read access privilege. The device supports both local account authentication and a remote centralized mechanism, including RADIUS.

2. Change the default password, and strengthen the account password complexity by:

   a. Enabling the “Password Policy” function.

   b. Increasing the minimum password length to at least eight characters.

   c. Defining a password policy to ensure that it contains at least an uppercase and lowercase letter, a digit, and a special character.

   d. Setting user passwords to expire after a certain period of time.

3. Enforce regulations that ensure that only a trusted host can access the device. Please refer to the Trusted Access section for detailed instructions.

Vulnerable Network Ports

1. For network security concerns, we strongly recommend that you change the port numbers, such as TCP port numbers for HTTP, HTTPS, Telnet, and SSH, for the protocols that are in use. Ports that are not in use but are still reachable pose an unacceptable security risk and should be disabled. Refer to the Management Interface section for detailed instructions.
2. In order to avoid eavesdroppers from snooping confidential information, users should adopt encryptionbased communication protocols, such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c, etc. In addition, the maximum n umber of sessions should be kept to an absolute minimum. Please refer to the Management Interface section for detailed instructions.

3. Users should generate the SSL certificate for the device before commissioning HTTPS or SSH applications. Please refer to the SSH & SSL section for detailed instructions.

Operation

In order to ensure that communications are properly protected, use a strong cryptographic algorithm for key exchange or encryption protocols for HTTPS/SSH applications. The device follows the NIST SP800- 52 and SP800-131 standards and supports TLS v1.2 and v1.3 with the following cipher suites:

TLS V1.2

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES256_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

TLS V1.3

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_AES_256_GCM_SHA384	Any	N/A	AES256 GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	Any	N/A	CHACHA20-POLY1305	SHA256
TLS_AES_128_GCM_SHA256	Any	N/A	AES128 GCM	SHA256

2. Below is a list of the recommended secure browsers that support TLS v1.2 or above:

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above
Google Chrome	v38 or above
Apple Safari	v7 or above

Reference: https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers

The device supports event logs and syslog for SIEM integration:
a. Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 1,000 entries per category. Administrators can set a warning for a pre-defined threshold. We that users regularly back up system event logs. Please refer to the Event Log section for
detailed instructions.
b. Syslog: the device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to the Syslog section for detailed instructions.

4. The device can provide information for control system inventory:
a. SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the SNMP for detailed instructions.
b. Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
c. HTTP/HTTPS: We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure the device.

5. Denial of Service protection: To avoid disruption of the normal operation of the router, administrators should configure the QoS and DoS policy functions. The device supports ingress rate limiting and egress shaper. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulted data rate per port. Please refer to the QoS section for detailed instructions. Furthermore, the device provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. Please refer to the DoS (Denial of Service) Policy section for detailed instructions.

6. Time synchronization with authentication: Time synchronization is crucial for process control. To prevent malicious attacks whereby the settings are changed without permission, authentication must be in place between the NTP server and client. The device supports NTP with a pre-shared key. Please refer to the Time section for detailed instructions.

7. Periodically regenerate the SSH and SSL certificates: Even though the device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that

users frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to the SSH & SSL section fordetailed instructions.

8. Below is the list for the protocol port numbers used for all external interfaces:

Protocol	Service Type	Port Number
TCP	SSH	22
TCP	Telnet	23
TCP	HTTP	80
TCP	HTTPS	443
UDP	DHCP	67
UDP	NTP	123
UDP	SNMP	161
UDP	Moxa Service	40404

Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
2. Frequently back up the system configurations: In order to properly protect the system configuration files from being tampered with, the device supports password encryption and signature authentication for backup files.
3. Examine event logs frequently to detect any anomalies.
4. To report vulnerabilities of Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

Decommission

To avoid any sensitive information such as your account password or certificate from being disclosed, always reset the system settings to factory default before decommissioning the device.

Severity Level List

This is a list of severity levels and descriptions, which are based on CVSS vulnerability classifications.

Syslog Severity	CEF Severity	Severity Name	Description
0	10	Emergency	System is unusable
1	8	Alert	Action must be taken immediately
2	7	Critical	Critical conditions
3	6	Error	Error conditions
4	5	Warning	Warning conditions
5	4	Notice	Normal but significant condition
6	1	Infomational	Informational messages
7	0	Debug	Debug-level messages

SMS Remote Control Commands

This table lists the SMS remote control commands of the device. Refer to Remote Control List for more information.

When sending an SMS command to the device, replace password with the **Password** specified on the SMS - General page.

Action	Command	Description
System Restart	@password@restart	The device will reboot.
Cellular Report	@password@cell.report	The device will reply with an SMS message containing the current cellular status of the device.
Cellular Start Connecting	@password@cellular.start	The device will enable the cellular data connection.
Cellular Stop Connecting	@password@cellular.stop	The device will disable the cellular data connection.
Switch SIM	@password@switchsim	The device will restart the cellular module and use the SIM card installed in the other SIM slot.
Start IPsec Tunnel	@password@ipsec.start	The device will establish an IPsec tunnel.
Stop IPsec Tunnel	@password@ipsec.stop	The device will disconnect the IPsec tunnel.
Set DO On	@password@do.on	The device will set the status of the relay output to On.
Set DO Off	@password@do.off	The device will set the status of the relay output to Off.

Status Codes

This page shows the different status codes for your device.

> **Note**
> Available settings and options will vary depending on the product model.

PoE Status Codes

Classification

Classification	Max Power (watts) by PSE Output
0	15.4
1	4
2	7
3	15.4
4	30

Device Type

Item	Description
Not Present	There are no active connections to the port.
802.3at	An IEEE 802.3at PD is connected to the port.
802.3af	An IEEE 802.3af PD is connected to the port.
NIC	A NIC is connected to the port.
Unknown	An unknown PD is connected to the port.
N/A	The PoE function is disabled.

Configuration Suggestion

Item	Description
Disable PoE power output	A NIC or unknown PD was detected; you may want to disable PoE power output for the port.
Select Force Mode	A higher/lower resistance or higher capacitance was detected; you may want to select **Force Mode** for the port.
Select high power output	An unknown classification was detected; you may want to select High Power output.
Raise the external power supply voltage to greater than 46 VDC	When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage.
Enable PoE function for detection	The system suggests enabling the PoE function.
Select IEEE 802.3at auto mode	When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode.
Select IEEE 802.3af auto mode	When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.

Structure and Syntax of Local Consist Info Files

A local consist info file uses XML syntax to represent consist information. It is composed of the physical vehicle information and the network device information within each vehicle.

The basic file structure is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<consistinfo>
    <vehicleinfo>
        <functioninfo>
        </functioninfo>
    </vehicleinfo>
</consistinfo>
```

consistinfo

The consistinfo element represents consist info. There must be only one consistinfo element per configuration file.

Attributes

There are no attributes for this element.

Child Elements

Name	Description	Valid Range
cstId	Required. Specifies a unique ID for a consist. This is different than the Consist UUID. The suggested naming convention for using a UIC for the cstId is: *"UIC" + (numerical part of UIC)* For example, the suggested cstId for *UIC 508089-43503-8* would be *UIC508089435038*.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
cstType	Optional. Specifies the type of the consist.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.

Name	Description	Valid Range
cstOwner	Optional. Specifies the owner of the consist.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
vehicleinfo	Required. List of vehicle information that belongs to the consist. Refer to vehicleinfo for more information.	The numbers of the vehicle information, ranges from 1 to 32

functioninfo

The functioninfo element represents device or functional group information in the vehicle. There can be 0 to 1024 functioninfo elements within a vehicleinfo element.

Attributes

There are no attributes for this element.

Child Elements

Name	Description	Valid Range
fctName	Required. Specifies a unique name for the device/functional group. For devices, we suggest using "dev" or "fct" as a prefix for the fctName. Examples: fctDoorCtrl, fctBrake, devHMI For functional groups, which represent multicast addresses, fctName should use "grp" as the prefix. Examples: grpDoorCtrl, grpBrake, grpETBN, grpECSC	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
cnId	Required. Specifies the static CN ID of the ECN this device/functional group connects to. Set this to 0 for functional groups.	Integer from 0 to 32
fctId	Required. Specifies the numeric ID for the device/functional group. Must be different from the Host ID of the ECN. There should be no duplicate combinations of fctId and cnId within a single consist.	Integer from 1 to 32767

vehicleinfo

The vehicleinfo element represents vehicle information in the consist. There should be 1 to 32 vehicleinfo elements within a consistinfo element.

Attributes

Name	Value	Valid Range
leading	Required. Boolean that indicates whether ECSC is attached to this vehicle.	true / false
tractVeh	Optional. Boolean that indicates whether a vehicle has traction.	true / false

Child Elements

Name	Description	Valid Range
vehId	Required. Specifies a unique ID for a vehicle. The suggested naming convention for using a UIC as for the vehId is: *"UIC" + (numerical part of UIC)* For example, suggested vehId for *UIC 508089-43501-2* would be *UIC508089435012*.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
vehType	Optional. Specifies the type of vehicle.	Valid XML element name that is 3 to 15 characters. A hyphen cannot be used as the last character.
vehOrient	Required. Specifies the vehicle orientation with respect to the consist direction. **same**: Indicates that vehicle has the same direction with respect to the consist direction. **inverse**: Indicates that the vehicle is in the opposite direction with respect to the consist direction.	same / inverse
cstVehNo	Required. Specifies the index of the vehicle within the consist. Indexing starts from consist direction 1 to direction 2. The first vehicle in consist direction 1 is assigned index 1. The second vehicle (next vehicle in direction 2 of first vehicle) has index 2, and so on.	Integer from 1 to 32

Name	Description	Valid Range
functioninfo	Required. List of devices/functional groups information within the vehicle. Refer to functioninfo for more information. Number of devices/function group information ranges from 0 to 1024	Integer from 0 to 1024

System Event List

This is a list of system events and their descriptions. Please note that some system events only apply to specific products.

Group	System Event	Description
General	Cold Start	Power was cut off and then reconnected.
General	Warm Start	The device was rebooted, such as when network parameters are changed (IP address, netmask, etc.).
General	Power 1 Transition (On->Off)	The device's power 1 is powered down.
General	Power 1 Transition (Off->On)	The device's power 1 is powered up.
General	Power 2 Transition (On->Off)	The device's power 2 is powered down.
General	Power 2 Transition (Off->On)	The device's power 2 is powered up.
General	Digital Input Transition (On->Off)	The device's input is turning off.
General	Digital Input Transition (Off->On)	The device's input is turning on.
General	Configuration Changed	A configuration setting was changed.
General	Login Failure	An incorrect password was entered.
General	Device Lockdown State Change	The device lockdown learning status has changed.
Redundancy	Ring/Chain/RSTP Topology Changed	The topology of the ring, chain, or RSTP network has changed.
Redundancy	Master Mismatch	A Turbo Ring Master mismatch occurred.
Redundancy	Coupling Topology Changed	The Coupling topology was changed.
General	Fiber Check Warning	The system detected that monitored values exceeded their safety thresholds.
Redundancy	VRRP State Change	The VRRP state was changed.

Group	System Event	Description
General	802.1X Authentication Failure	An 802.1X authentication failure occurred.
VPN	VPN Disconnected	VPN has been disconnected.
VPN	VPN Connected	VPN has been connected.
PoE	PoE PD On	Port#N PD power on.
PoE	PoE PD Off	Port#N PD power off.
PoE	Over Measured Power limitation	Over the total measured power limit.
PoE	PoE FETBad	PD Port#N MOSFET is bad.
PoE	PoE Over Temperature	The temperature of the environment exceeds the maximum operating temperature of the device.
PoE	PoE VEE Uvlo	VEE (PoE input voltage) under Voltage Lockout. The voltage of the power supply has dropped below 44V DC.
PoE	PoE PD Over Current	Current of Port#N has exceeded the safety limit.
PoE	PoE PD Check Fail	PD Port#N check failed.
PoE	Over Allocated Power limitation	The total PD power consumption exceeds the total allocated power.
General	Firmware Upgrade Success	Firmware upgrade was successful.
General	Firmware Upgrade Failure	An error occurred during the firmware upgrade.
Firewall	Layer 3 - 7 Policy Changed	A user configured firewall rule in Layer 3-7 Policy has been added, modified, or deleted.
General	Log Service Ready	Log service is ready.
Cellular	IP Change	The cellular IP address of the device has changed.
Cellular	Cellular Module Failure	The cellular module has encountered a failure and is not functioning.
Cellular	Detect SIM Failure	The system has detected a failure in the inserted SIM.
Cellular	PIN Code Failure	The device failed to validate the PIN code for the SIM card.

Group	System Event	Description
Cellular	SIM Switch	The active SIM has been switched to another SIM card.
Cellular	GuaranLink Cellular Reconnected	GuaranLink has successfully reconnected the cellular network.
Cellular	Guaranlink Triggered ISP Reregister	GuaranLink triggered re-registration with the Internet Service Provider.
Cellular	Guaranlink Triggered Cellular Module Reset	The cellular module was reset by GuaranLink due to an error condition.
Cellular	Guaranlink Triggered System Reboot	GuaranLink triggered a system reboot due to error recovery.
Power Management	Power Saving Start	The device enters the power saving mode.
Power Management	Power Saving End	The device leaves the power saving mode.
Power Management	Scheduling Rule Expired	The power saving rule has passed the set end time.
SMS	Wrong Password	The password of the remote control SMS received by the device is wrong.
SMS	Wrong Command	The command of the remote control SMS received by the device is wrong.
SMS	Wrong Format	The format of the remote control SMS received by the device is wrong.
SMS	Command Disabled	The remote control SMS received by the device is not enabled.
SMS	Trusted Number Authentication Failure	The remote control SMS received by the device is not from the Trusted Number List.
WAN Redundancy	WAN Interface Changed	The active WAN interface change to a different WAN interface.
WAN Redundancy	WAN Interface Ping Failure	The active WAN interface fails to ping the specified server.
Serial	Serial OP Mode State Changed	The serial operational mode has changed.
Serial	Serial DSR State Changed	The Data Set Ready (DSR) state of the serial port has changed.

Group	System Event	Description
Serial	Serial DCD State Changed	The Data Carrier Detect (DCD) state of the serial port has changed.
DHCP	DHCP Error Log	An error occurred in the DHCP process, and it has been logged.
IGMP Snooping	IGMP Snooping Error Log	An error occurred in IGMP snooping and has been logged.
RADIUS Server	RADIUS Server Authentication Log	An error occurred in RADIUS server authentication and has been logged.
General	Clear Relay Warning	The relay warning condition has been cleared.
General	HA Role Change	The High Availability role of the device changed.
General	Duplicate IP Detection	Detected more than one MAC address with the same IP on an interface.
NTP/SNTP Error Log	NTP/SNTP Error Log	An error occurred in NTP/SNTP synchronization and has been logged.

TRDP Message Type List

Configuration attribute requirements - msgType

This is a list of TRDP msgTypes and their descriptions.

msgType	Description
Pr	PD Request
Pp	PD Reply
Pd	PD Data
Pe	PD Data (Error)
Mn	Notification (Request without reply)
Mr	MD Request with reply
Mp	MD Reply without confirmation
Mq	MD Reply with confirmation
Mc	MD Confirm
Me	MD error

Configuration attribute requirements - msgType Profile

This is a list of TRDP msgType profiles and their descriptions.

Profile	Description
PD-PDU	A collection of “Pr, Pp, Pd, Pe”
MD-PDU	A collection of “Mn, Mr, Mp, Mq, Mc, Me”

TRDP Protocol Filter Profile List

This is a list of the different built-in protocol filter profiles for common applications and their corresponding message types and communication identifiers.

Protocol Filter Profile	Message Type	Communication Identifier (ComID)
PD-PDU	0x5072: PD Request, 0x5070: PD Reply, 0x5064: PD Data, 0x5065: PD Data (Error)	All
MD-PDU	0x4D6E: Notification (Request without reply), 0x4D72: MD Request with reply, 0x4D70: MD Reply without confirmation, -x4D71: MD Reply with confirmation, 0x4D63: MD Confirm, 0x4D65: MD error	All
Communication Framework and ETB Control Service	All	1 to 29, 50 to 79, 150 to 199
TRDP statistics data	All	30 to 41
Conformance test	All	80 to 99
TTDB	All	100 to 119
ECSP	All	120 to 129
ETBN	All	130 to 139
TCN-DNS	All	140 to 149

User Role Privileges

This page shows the privilege levels granted to the different authority levels: Admin, Supervisor, and User. Refer to User Accounts for more information on user accounts.

Privileges are indicated as follows:

- **R/W**: Read and write access granted for the relevant settings
- **R**: Read-only access granted for the relevant settings
- **-**: No access granted for the relevant settings

> **Note**
> Available settings and options will vary depending on the product model.

Options Menu

Settings	Admin	Supervisor	User
Change Language	R/W	R/W	R/W
Reboot	R/W	R/W	-
Reset to Defaults	R/W	-	-
Save Custom Default	R/W	-	-
Log Out	R/W	R/W	R/W

System

Settings	Admin	Supervisor	User
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-

Settings	Admin	Supervisor	User
Software Package Management	R/W	-	-
Configuration Backup and Restore	R/W	-	-
Account Management			
User Accounts	R/W	-	-
Password Policy	R/W	-	-
License Management	R/W	R/W	R
Management Interface			
Out of Band Management	R/W	R/W	R
User Interface	R/W	R/W	R
Ping Response	R/W	R/W	R
Hardware Interface	R/W	R/W	R
SNMP	R/W	-	-
Moxa Remote Connect	R/W	-	-
MXsecurity	R/W	R/W	-
Time			
System Time	R/W	R/W	R
NTP/SNTP Server	R/W	R/W	R
Power Management	R/W	R/W	R
SMS	R/W	R/W	R
GNSS	R/W	R/W	R
Setting Check	R/W	R/W	R

Cellular

Settings	Admin	Supervisor	User
Cellular	R/W	R/W	R

Serial

Settings	Admin	Supervisor	User
Serial Device Server	R/W	R/W	R
SCATS	R/W	R/W	R

Network Configuration

Settings	Admin	Supervisor	User
Ports			
Port Settings	R/W	R/W	R
Link Aggregation	R/W	R/W	R
Link Fault Passthrough	R/W	R/W	R
LAN Bypass Gen3	R/W	R/W	R
PoE	R/W	R/W	R
Layer 2 Switching			
VLAN	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS	R/W	R/W	R
Rate Limit	R/W	R/W	R

Settings	Admin	Supervisor	User
Multicast	R/W	R/W	R
IGMP Snooping	R/W	R/W	R
Static Multicast Table	R/W	R/W	R
Network Interfaces	R/W	R/W	R

Redundancy

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring V2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
Layer 3 Redundancy			
VRRP	R/W	R/W	R
WAN Redundancy	R/W	R/W	R

Network Service

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R
Dynamic DNS	R/W	R/W	R
DNS Server	R/W	R/W	R

Routing

Settings	Admin	Supervisor	User
Unicast Route			
Static Routes	R/W	R/W	R
RIP	R/W	R/W	R
OSPF	R/W	R/W	R
Routing Table	R	R	R
Multicast Route			
Multicast Route Settings	R/W	R/W	R
Static Multicast Route	R/W	R/W	R
Multicast Forwarding Table	R	R	R
Broadcast Forwarding	R/W	R/W	R
Directed Forwarding	R/W	R/W	R

Tunneling

Settings	Admin	Supervisor	User
VXLAN L2 Tunneling	R/W	R/W	R
GRE L3 Tunneling	R/W	R/W	R

NAT

Settings	Admin	Supervisor	User
NAT Setting	R/W	R/W	R

Settings	Admin	Supervisor	User
ALG Settings	R/W	R/W	R
PN-DCP Forwarding	R/W	R/W	R

Object Management

Settings	Admin	Supervisor	User
Object Management	R/W	R/W	R

Firewall

Settings	Admin	Supervisor	User
Layer 2 Policy	R/W	R/W	R
Layer 3 Policy	R/W	R/W	R
Layer 3-7 Policy	R/W	R/W	R
Malformed Packets	R/W	R/W	R
Session Control	R/W	R/W	R
DoS Policy	R/W	R/W	R
Soft Lockdown Mode	R/W	R/W	R
Device Lockdown	R/W	R/W	R
Advanced Protection			
Dashboard	R/W	R/W	-
Configuration	R/W	R/W	-
Protocol Filter Policy	R/W	R/W	-

Settings	Admin	Supervisor	User
ADP	R/W	R/W	-
IPS	R/W	R/W	-
Domain Protection	R/W	R/W	-

VPN

Settings	Admin	Supervisor	User
IPSec	R/W	R/W	R
OpenVPN Client	R/W	R/W	-
L2TP Server	R/W	R/W	R

Certificate Management

Settings	Admin	Supervisor	User
Local Certificate	R/W	R/W	-
Trusted CA Certificate	R/W	-	-
Certificate Signing Request	R/W	-	-

Security

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R/W	R

Settings	Admin	Supervisor	User
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-
LDAP	R/W	-	-
2-Factor Authentication	R/W	-	-
RADIUS Server	R/W	-	-
MXview Alert Notification	R/W	R/W	R

Diagnostics

Settings	Admin	Supervisor	User
System Status			
Utilization	R/W	R/W	R
Fiber Check	R/W	R/W	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Connection Management	R/W	R/W	R

Settings	Admin	Supervisor	User
Duplicate IP Detection	R/W	R/W	R
Event Log and Notifications			
Event Log	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R	R
SNMP Trap / Inform	R/W	-	-
Email Settings	R/W	R	R
SMS Settings	R/W	R	R
Tools			
Diagnostic Support	R/W	R/W	R
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R
Netflow	R/W	R/W	R
Asset Recognition	R/W	R/W	-

Industrial Application

Settings	Admin	Supervisor	User
IEC 61375			
Ethernet Train Backbone	R/W	R/W	R
Communication Profile	R/W	R/W	R
Operational Status	R/W	R/W	R

Moxa Inc.

Copyright © 2026 Moxa, Inc. All rights reserved. Reproduction without permission is prohibited. Trademarks and logos are copyrights of their respective owners.

www.moxa.com/products