GE VERNOVA

Learning & Development
Learning Module

G500/G100 Configure Network Communications

L&D
Learning & Development

SME Source Markham

Learning Module Objective

At the completion of this module you will be able to identify and recite all concepts presented.

If you are viewing this as part of a structured training program *PLEASE* complete the associated assessment test. You are required to score above 80%.

Here's What is Covered in this Module

1. Network Communication Overview
2. Types of Network Connections
3. Add a Network Connection
4. Modify/Delete a Network Connection
5. Connection Application Parameters
6. Connection Security - Modbus TCP/SSH Tunnel
7. Secure Connection Relay
8. VPN Server
9. Syslog Client

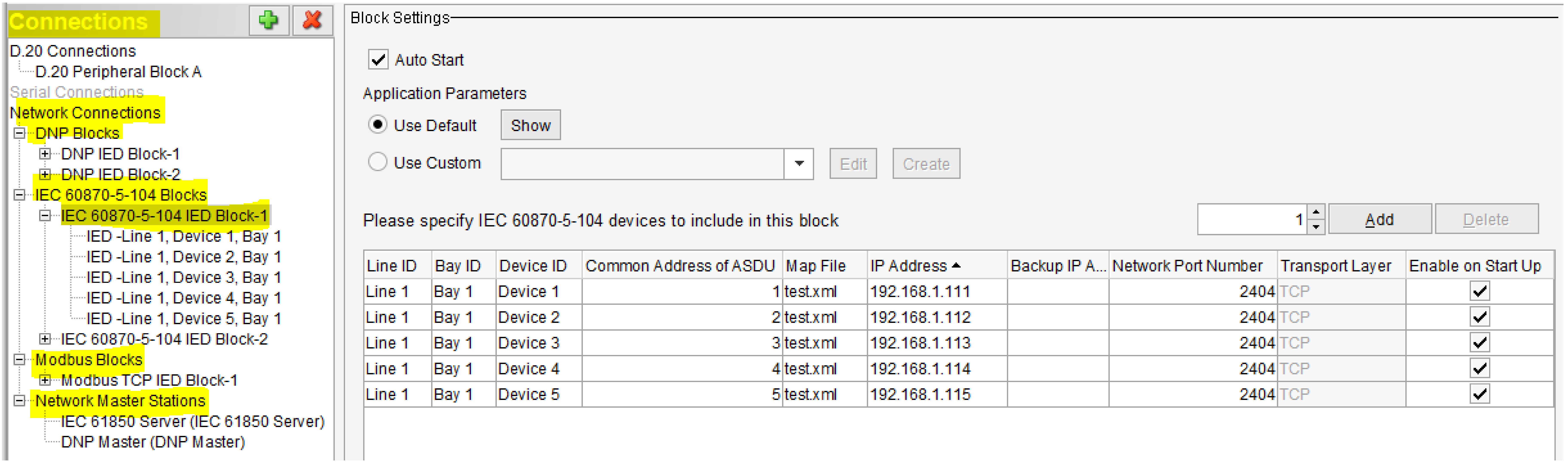
Network Communications Overview

Network connections to the MCP (G500/G100) are shown as sub-items under the **Network Connections** heading of the **Connections** pane. To improve the efficiency of communications, the MCP supports network capable device and master connections using “Blocks” that can process communications concurrently.

Network Blocks

Network blocks appear under the **Network Connections** heading of the **Connections** tab as <**Protocol Name> Blocks**.

- Each network block is an instance of a designated protocol (client or server application).
- Each network block can be configured for the number of device (client) or master station (server) connections and instance-specific protocol settings that are used for the network communications.



Connections

- D.20 Connections
  - D.20 Peripheral Block A
- Serial Connections
- Network Connections
  - DNP Blocks
    - DNP IED Block-1
    - DNP IED Block-2
  - IEC 60870-5-104 Blocks
    - IEC 60870-5-104 IED Block-1
      - IED -Line 1, Device 1, Bay 1
      - IED -Line 1, Device 2, Bay 1
      - IED -Line 1, Device 3, Bay 1
      - IED -Line 1, Device 4, Bay 1
      - IED -Line 1, Device 5, Bay 1
    - IEC 60870-5-104 IED Block-2
  - Modbus Blocks
    - Modbus TCP IED Block-1
  - Network Master Stations
    - IEC 61850 Server (IEC 61850 Server)
    - DNP Master (DNP Master)

Block Settings

☑ Auto Start

Application Parameters

● Use Default [Show]

○ Use Custom [Edit] [Create]

Please specify IEC 60870-5-104 devices to include in this block 1 [Add] [Delete]

Line ID	Bay ID	Device ID	Common Address of ASDU	Map File	IP Address ▲	Backup IP A...	Network Port Number	Transport Layer	Enable on Start Up
Line 1	Bay 1	Device 1	1	test.xml	192.168.1.111		2404	TCP	✓
Line 1	Bay 1	Device 2	2	test.xml	192.168.1.112		2404	TCP	✓
Line 1	Bay 1	Device 3	3	test.xml	192.168.1.113		2404	TCP	✓
Line 1	Bay 1	Device 4	4	test.xml	192.168.1.114		2404	TCP	✓
Line 1	Bay 1	Device 5	5	test.xml	192.168.1.115		2404	TCP	✓

Each additional block/instance uses additional system resources increasing system throughput.

Type of Network Connections

Each network connection can be configured for either:

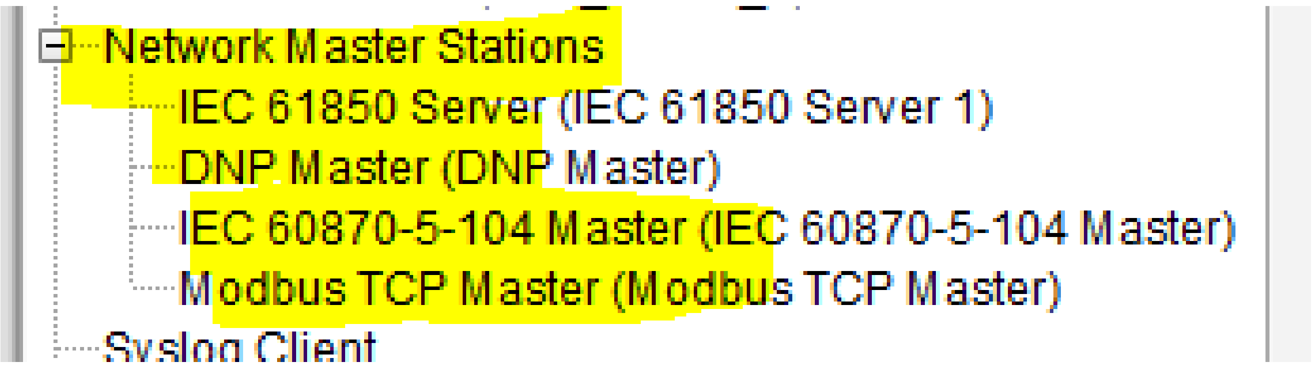
- Master station (server) communications using a selected protocol.
- IEDs (client) communications using a selected protocol.

Network Devices

- Network capable devices can be connected to one or more data collection blocks and polled according to the instance-specific protocol settings.

Master Stations

- The MCP can support communications to multiple (up to **eight**) master stations.
- A single Master block defines the master station connections. A master station represents a single instance of a server application.
- Each configured master station application is shown as an entry under the **Network Master Stations** option on the **Connections** tab.



```
⊟ Network Master Stations
    IEC 61850 Server (IEC 61850 Server 1)
    DNP Master (DNP Master)
    IEC 60870-5-104 Master (IEC 60870-5-104 Master)
    Modbus TCP Master (Modbus TCP Master)
  Syslog Client
```

Network connections can be configured using the following protocols / functions:

IED Block:

- DNP3 IED Block
- IEC 60870-5-104 IED Block
- Modbus TCP IED Block
- SNMP Block
- IEC61850 Client (View-Only)

Master Stations:

- DNP3 Master
- IEC 60870-5-104 Master
- Modbus TCP Master
- IEC61850 Server

Others:

- Secure Connection Relay
- VPN Server
- Syslog Client

The data presented to each master station may be identical or unique as defined by a server map.

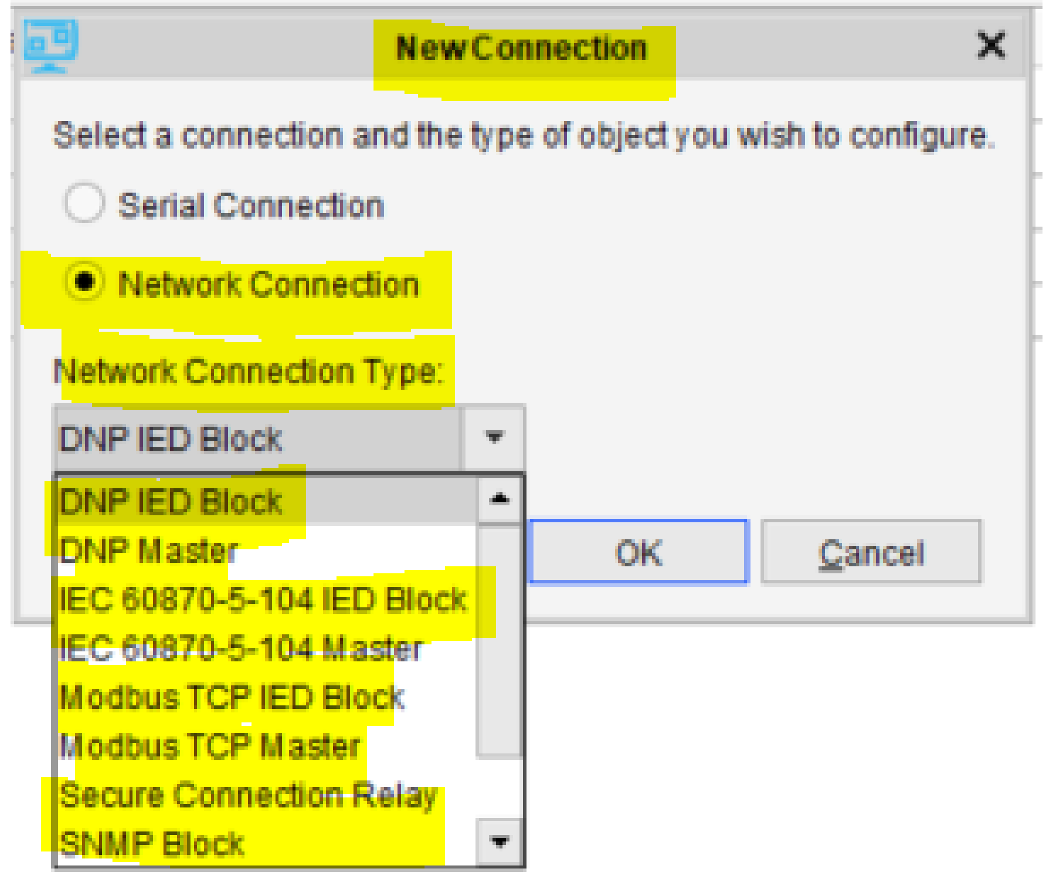
IEC61850 Client are available for viewing only and cannot be edited under the **Connections** Tab. To change the IEC61850 Client configuration, you must use the IEC61850 Loader tool and re-load the configuration into the MCP. Refer to the IEC61850 Loader online help for more information.

Add a Network Connection

You can manage the network connections on the MCP on the **Connections** tab on the Configuration page. Each network connection can be configured for device (client) or master station (server) communications using a selected protocol. A map file **MUST** be available in the MCP before a protocol type can be added.

To Add a Network Connection:

1. On the **Connections** tab, click Add Connection (**+**) button.
2. On the **New Connection** window, select **Network Connection** and select the **Network Connection Type** from the list.
3. Select whether the application automatically starts (Auto-Start) when the configuration is loaded and when the MCP reboots.
4. Modify the settings for the new connection. Double-click a cell to modify a value.
5. The fields under **Configuration Parameters** are specific to the connection type.
6. Click **Save Configuration** to save your changes.



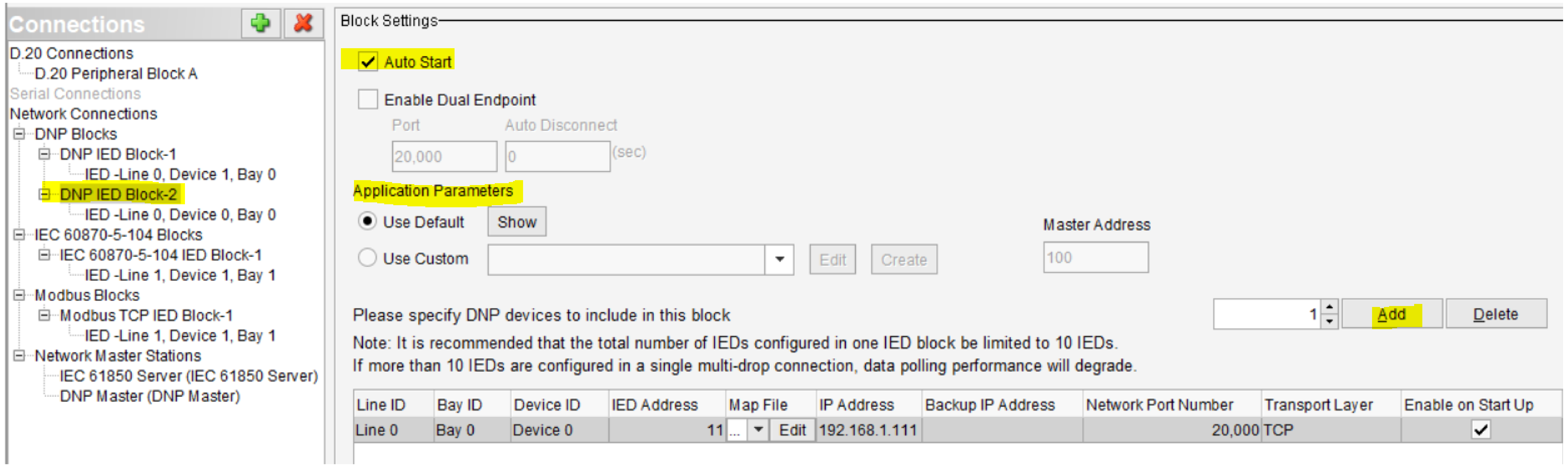
New Connection

Select a connection and the type of object you wish to configure.

○ Serial Connection

● Network Connection

Network Connection Type: DNP IED Block



☑ Auto Start

□ Enable Dual Endpoint

Port 20,000 Auto Disconnect 0 (sec)

Application Parameters

● Use Default Show

○ Use Custom Edit Create

Master Address 100

Please specify DNP devices to include in this block 1 Add Delete

Note: It is recommended that the total number of IEDs configured in one IED block be limited to 10 IEDs.
If more than 10 IEDs are configured in a single multi-drop connection, data polling performance will degrade.

Line ID	Bay ID	Device ID	IED Address	Map File	IP Address	Backup IP Address	Network Port Number	Transport Layer	Enable on Start Up
Line 0	Bay 0	Device 0	11	... Edit	192.168.1.111		20,000	TCP	✓

The MCP includes several default map files. If you require a custom map, create it first before setting up the network connection.

Modify / Delete a Network Connection

To Modify a Network Connection:

1. Select the connection in the **Connections** pane.
2. Double-click or select a configuration parameter field
3. Enter a new value in the parameter field.
4. Click **Save Configuration** to save your changes.

Changing a Map file

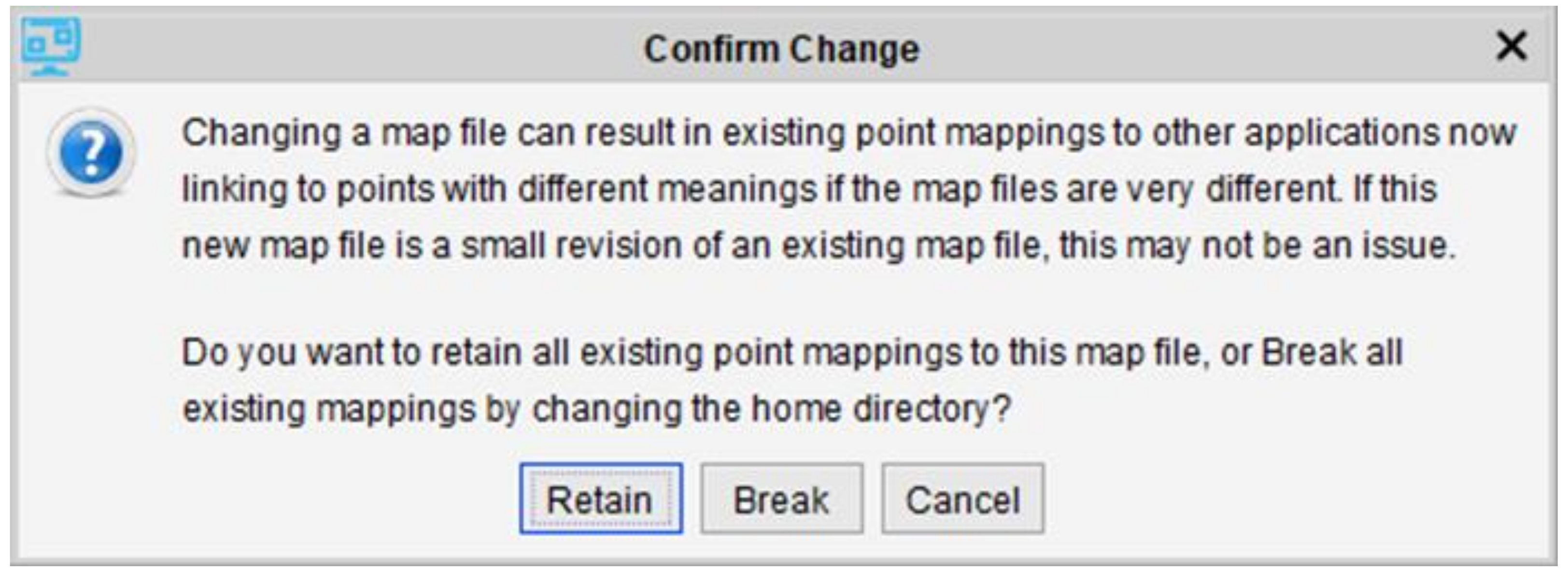
If you select a different map file for an existing IED connection in the dropdown list, or when you save it as a different filename when opened from within the Connections > Map File Edit button, you will be prompted with the following dialog:

- **Retain:**

  Apply the new map file with home directory and point mappings unchanged
- **Break:**

  Apply the new map file with home directory changed and existing point mappings invalidated
- **Cancel:**

  Abandon the change and revert to what was selected before

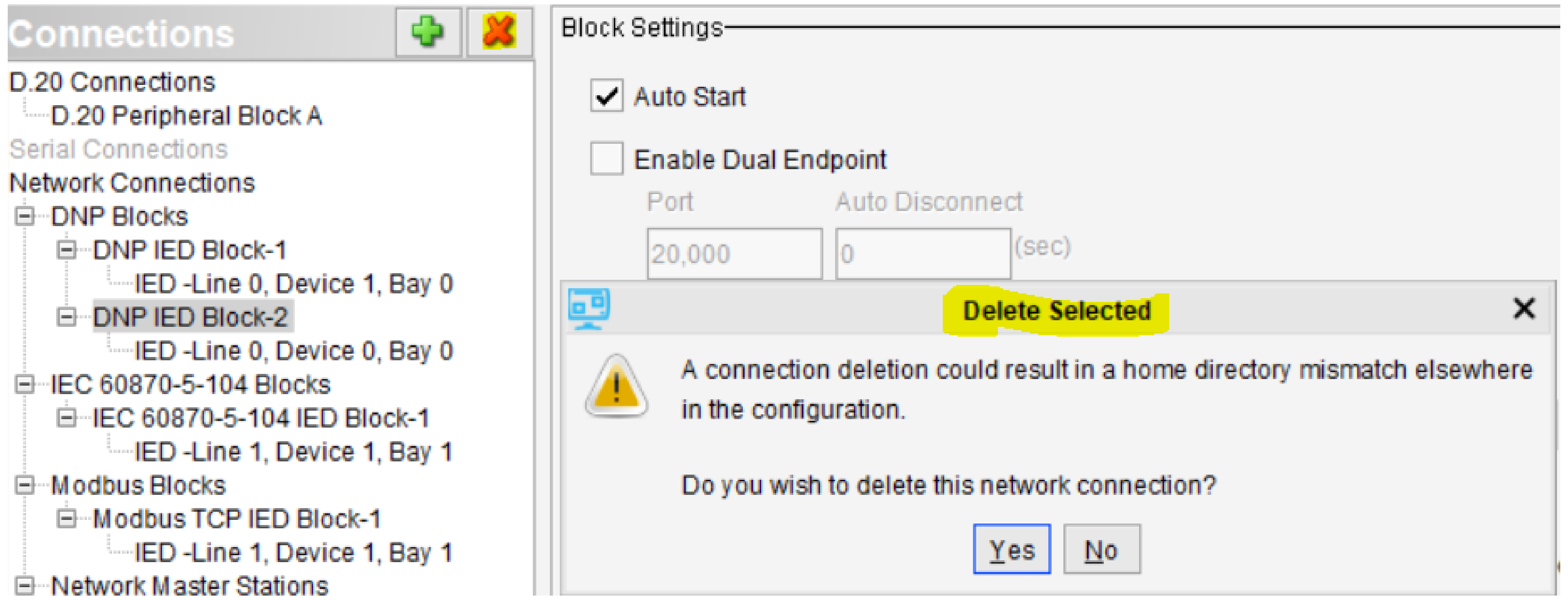


Changing a map file can result in existing point mappings to other applications now linking to points with different meanings if the map files are very different. If this new map file is a small revision of an existing map file, this may not be an issue.

Do you want to retain all existing point mappings to this map file, or Break all existing mappings by changing the home directory?

To Delete a Network Connection:

1. Select the connection/block you wish to delete in the **Connections** pane.
2. Click Delete Connection (**X**) button.
3. Click **Yes** to confirm deletion.
   Result: The item is removed from the connections/blocks list.
4. Click **Save Configuration** to save your changes.



☑ Auto Start

□ Enable Dual Endpoint

Port: 20,000

Auto Disconnect: 0 (sec)

A connection deletion could result in a home directory mismatch elsewhere in the configuration.

Do you wish to delete this network connection?

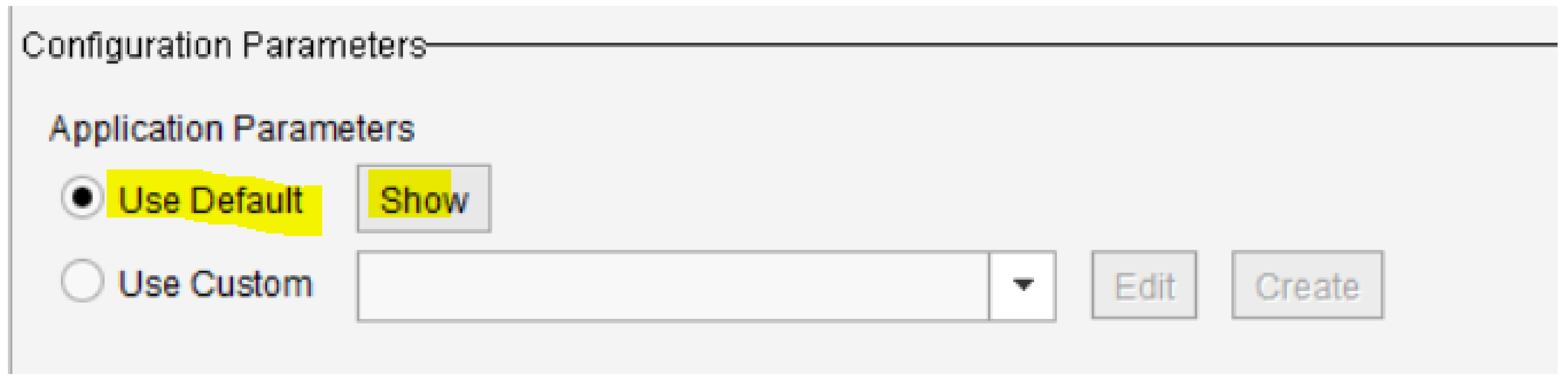
Deleting a Network Connection will also delete configured devices. In Addition, it could result in a home directory mismatch elsewhere in the configuration.

Connection Application Parameters

The **Application Parameters** window allows you to view and modify the protocol settings for a specific client or server connection. Application parameters are available on the **Connections** tab on the **Configuration** page. The settings shown vary based on the connection type and protocol selected.

To View Default Application Parameters:

1. Under **Application Parameters**, select **Use Default** and then click **Show**.
   Result: The Application Parameters window opens.



Configuration Parameters

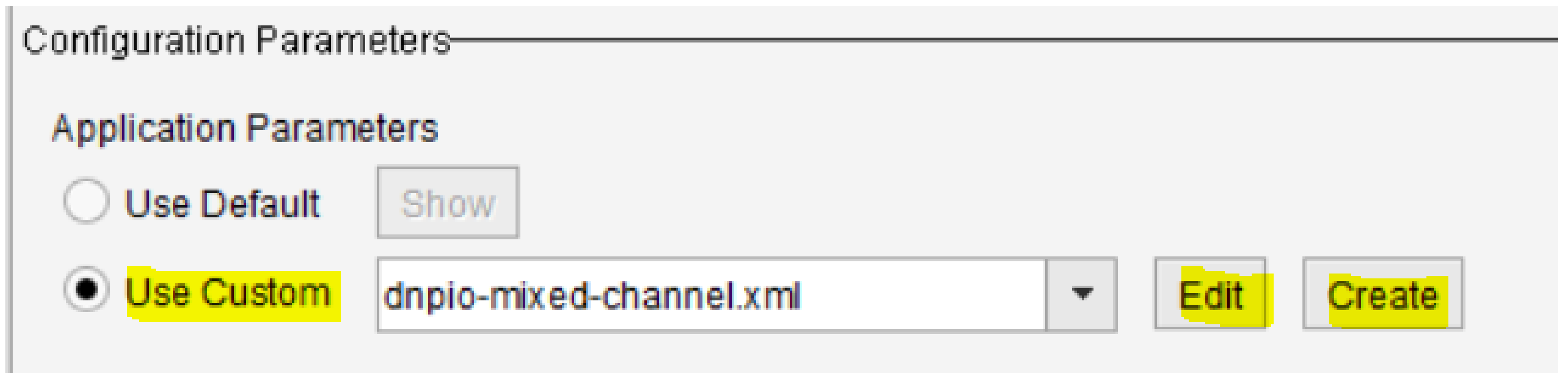
Application Parameters

● Use Default　Show

○ Use Custom　▾　Edit　Create

To Create a Custom Application Parameters Profile:

1. Under **Application Parameters**, select **Use Custom** and click **Create**. The **Application Parameters** window opens.
2. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list.
3. When you are done, click **Save**. On the **Save As** window, enter a filename and click **Save**.
4. Click **Save Configuration** to save your changes.



Configuration Parameters

Application Parameters

○ Use Default　Show

● Use Custom　dnpio-mixed-channel.xml ▾　Edit　Create

To Modify Application Parameters:

1. Under **Application Parameters**, select **Use Custom** and select the profile name from the drop-down list and then click **Edit**.
2. if this profile is created and has not been committed yet, the **Choose Version** popup appears. Select the version:
   - **COMMITTED**: The most recently committed version.
   - **UNCOMMITTED**: The version created, but not committed yet.
3. The **Application Parameters** window opens.
4. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list.
5. When you are done, click **Save**. On the **Save As** window, enter a filename and click **Save**.
6. Click **Save Configuration** to save your changes.

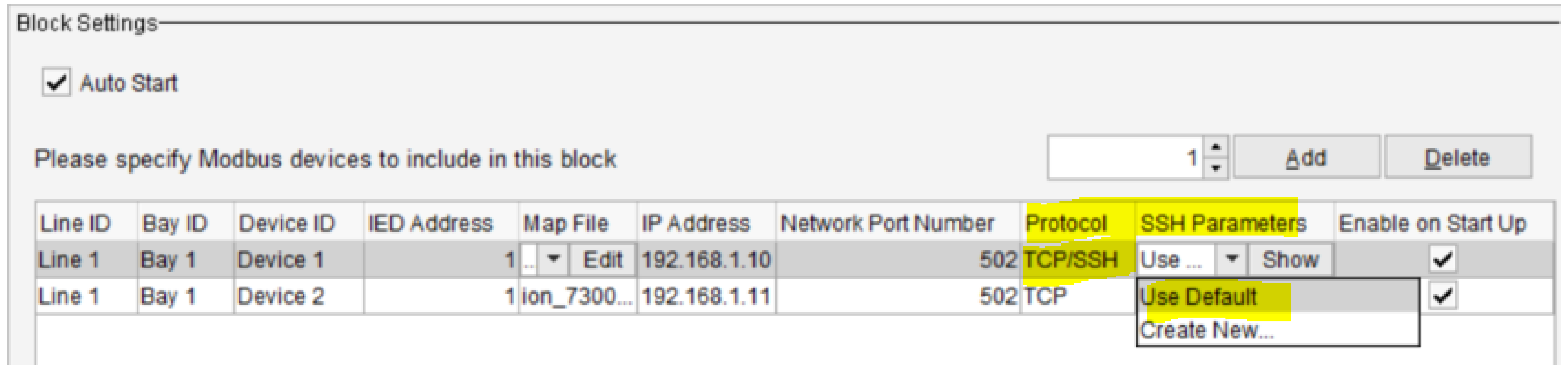
More advanced parameters may be available on the Advanced sub-tab on the Application Parameters window.

Connection Security – Modbus TCP/SSH Tunnel

The MCP supports Modbus TCP/SSH protocol to establish a secure SSH connection with the UR IEDs that support SSHv2 protocol through Machine-to-Machine (M2M) access role. This can be configured by selecting Protocol as TCP/SSH while adding the device.

The following SSH Parameters are used:

- SSH Server Port (Default: 22)
- M2M User Name (Default: m2m_user)
- SSH Key Rotation Period (Default: 1 day)



Block Settings

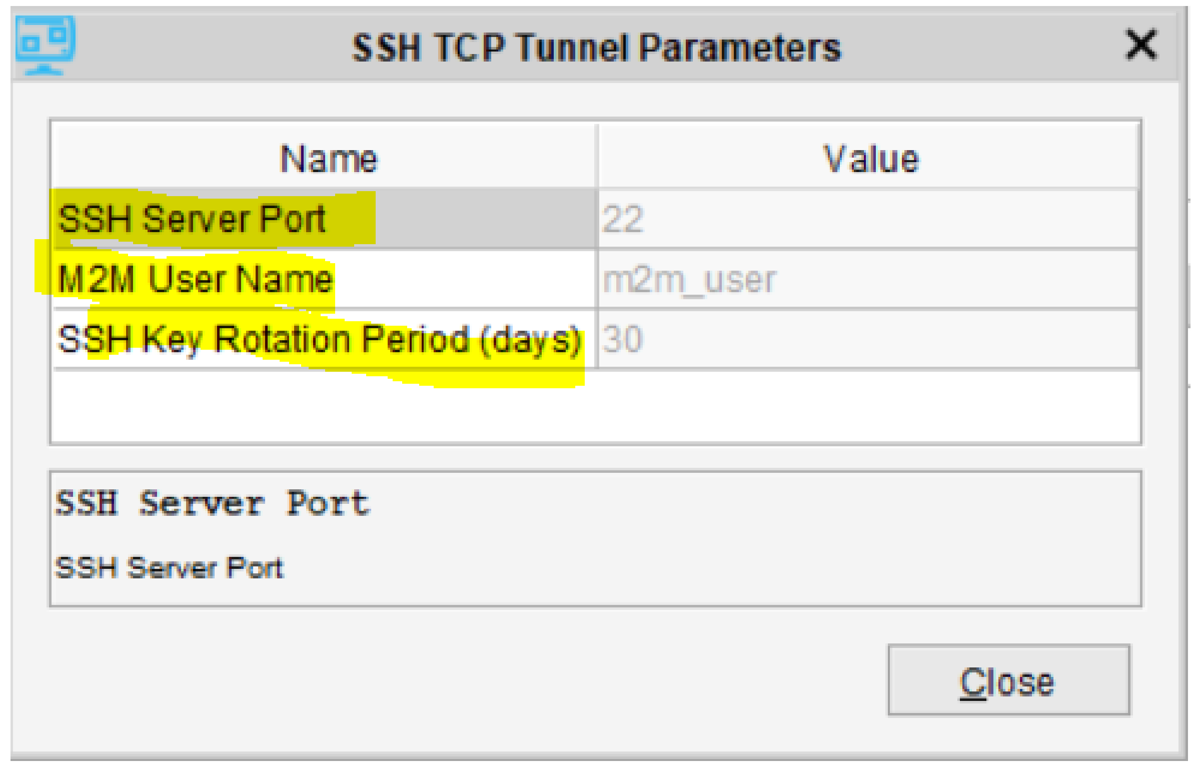
☑ Auto Start

Please specify Modbus devices to include in this block

Line ID	Bay ID	Device ID	IED Address	Map File	IP Address	Network Port Number	Protocol	SSH Parameters	Enable on Start Up
Line 1	Bay 1	Device 1	1	.. ▾ Edit	192.168.1.10	502	TCP/SSH	Use ... ▾ Show	✓
Line 1	Bay 1	Device 2	1	ion_7300...	192.168.1.11	502	TCP	Use Default Create New...	✓

To View Default SSH Parameters:

1. On **SSH Parameters** field, select **Use Default** and then click **Show**.
   Result: The default SSH Parameters window opens.



SSH TCP Tunnel Parameters

Name	Value
SSH Server Port	22
M2M User Name	m2m_user
SSH Key Rotation Period (days)	30

SSH Server Port

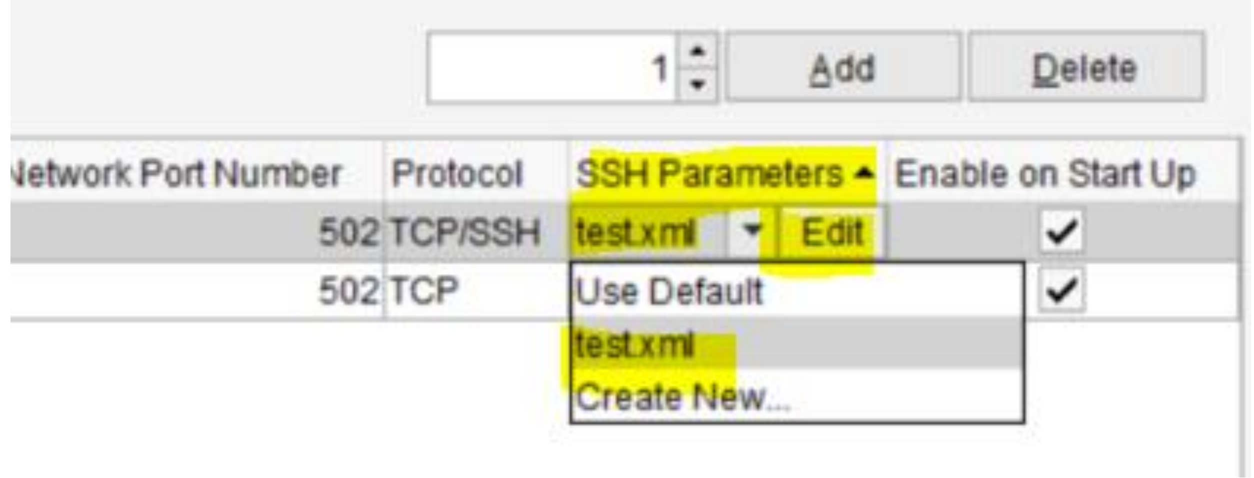
SSH Server Port

To Create a New SSH Parameters Profile:

1. On **SSH Parameters** field**,** select **Create New**. The **SSH Parameters** window opens.
2. To modify a parameter, double-click the associated value and enter a new value.
3. When you are done, click **Save**.
4. On the **Save As** window, enter a filename and click **Save**.

To Modify a SSH Parameters Profile:

1. On **SSH Parameters** field, select the profile you want to modify from the drop-down list and then click **Edit**. The **SSH Parameters** window opens.
2. To modify a parameter, double-click the associated value and enter a new value.
3. When you are done, click **Save**.
4. On the **Save As** window, enter a filename and click **Save**.



Network Port Number	Protocol	SSH Parameters	Enable on Start Up
502	TCP/SSH	test.xml ▾ Edit	✓
502	TCP	Use Default test.xml Create New...	✓

The MCP provides an option in the IED communication summary on Runtime HMI for copying the MCP's public key into an UR IED.

The MCP also provides an option for rotating the MCP's public key into the UR IED on an on-demand basis.

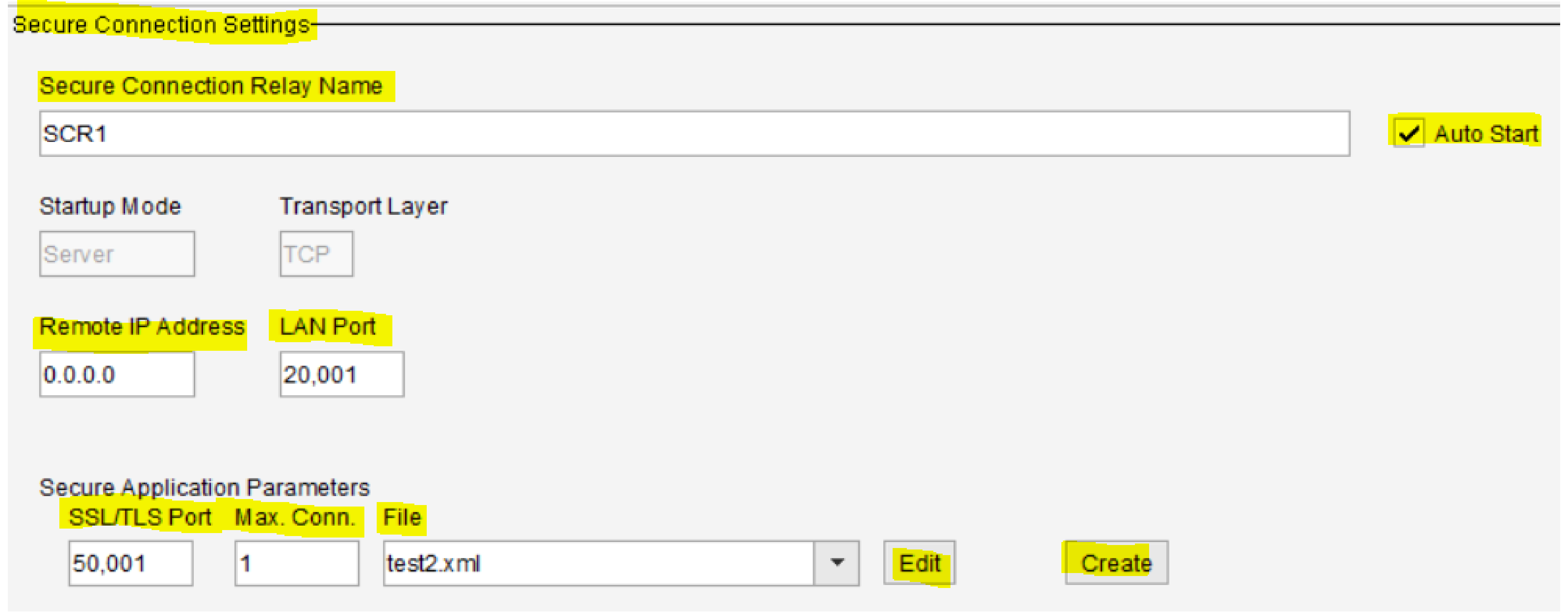
Secure Connection Relay

A secure connection relay is used to apply security features to any existing ethernet connection. A secure SSL/TLS connection is established to connect an external client device to the MCP to access a protected service in the substation.

The following Secure Connection Settings are used:

- Secure Connection Relay Name
- Auto Start (Default: Enabled)
- Remote IP Address (Default: 0.0.0.0)
- LAN Port (Default: 20001)
- SSL/TLS Port (Default: 50000 + x)
- Max. Conn. (Default: 1)
- File

  Select the **Secure Application Parameters** profile defining this connection. After a profile is created, it can be saved and reused on other connections



Secure Connection Settings

Secure Connection Relay Name: SCR1 ☑ Auto Start

Startup Mode: Server

Transport Layer: TCP

Remote IP Address: 0.0.0.0

LAN Port: 20,001

Secure Application Parameters

SSL/TLS Port	Max. Conn.	File
50,001	1	test2.xml

Parameters

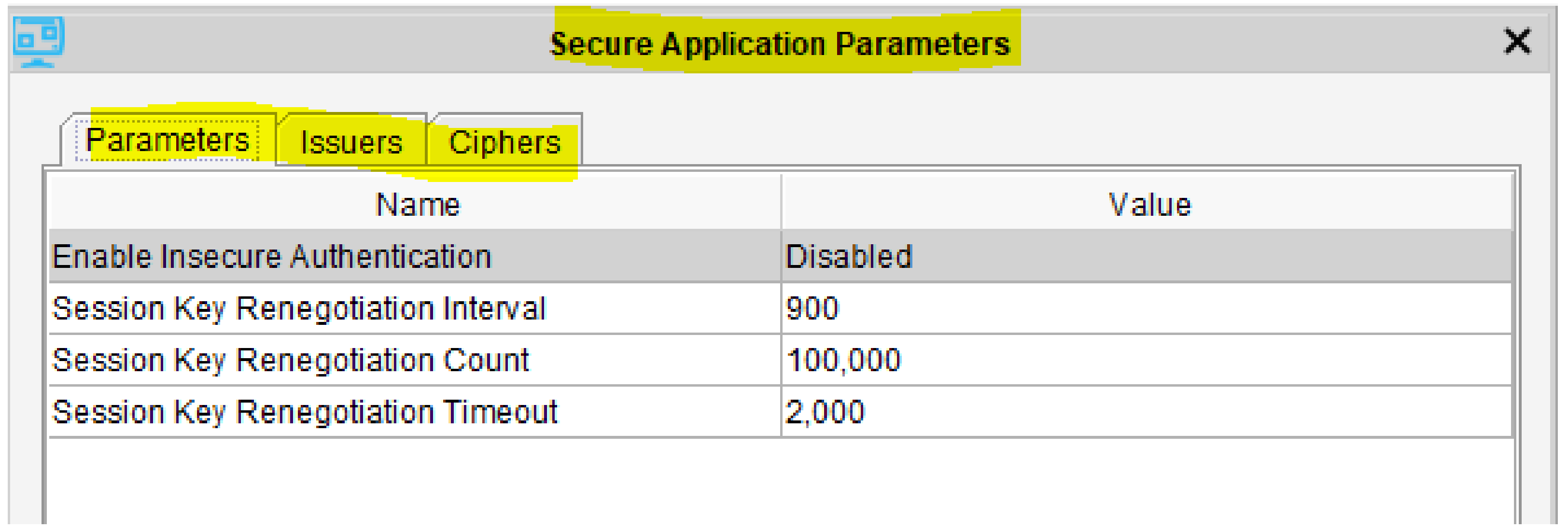
- □ Enable insecure authentication (Default: Disabled)
- □ Session key renegotiation interval (Default: 900s)
- □ Session key renegotiation count (Default: 100,000 Bytes)
- □ Session key renegotiation timeout (Default: 2,000 ms)

Issuers

- □ Peer / Issuer
- □ Enable Peer identity validation (Default: Enabled)

Ciphers

- □ Cipher name
- □ Permit null encryption (Default: Disabled)
- □ Secure protocol (Default: TLS1.0)



Secure Application Parameters

Name	Value
Enable Insecure Authentication	Disabled
Session Key Renegotiation Interval	900
Session Key Renegotiation Count	100,000
Session Key Renegotiation Timeout	2,000

A client device could be a PC with Tactical Software Serial/IP or Stunnel, SCADA master that supports SSL/TLS and mutual authentication using certificates.

A protected device could be a master server application on the MCP, or any other device connected to the MCP in the substation.

It is strongly recommended that the users employ SSL/TLS tunnels to protect the following services:

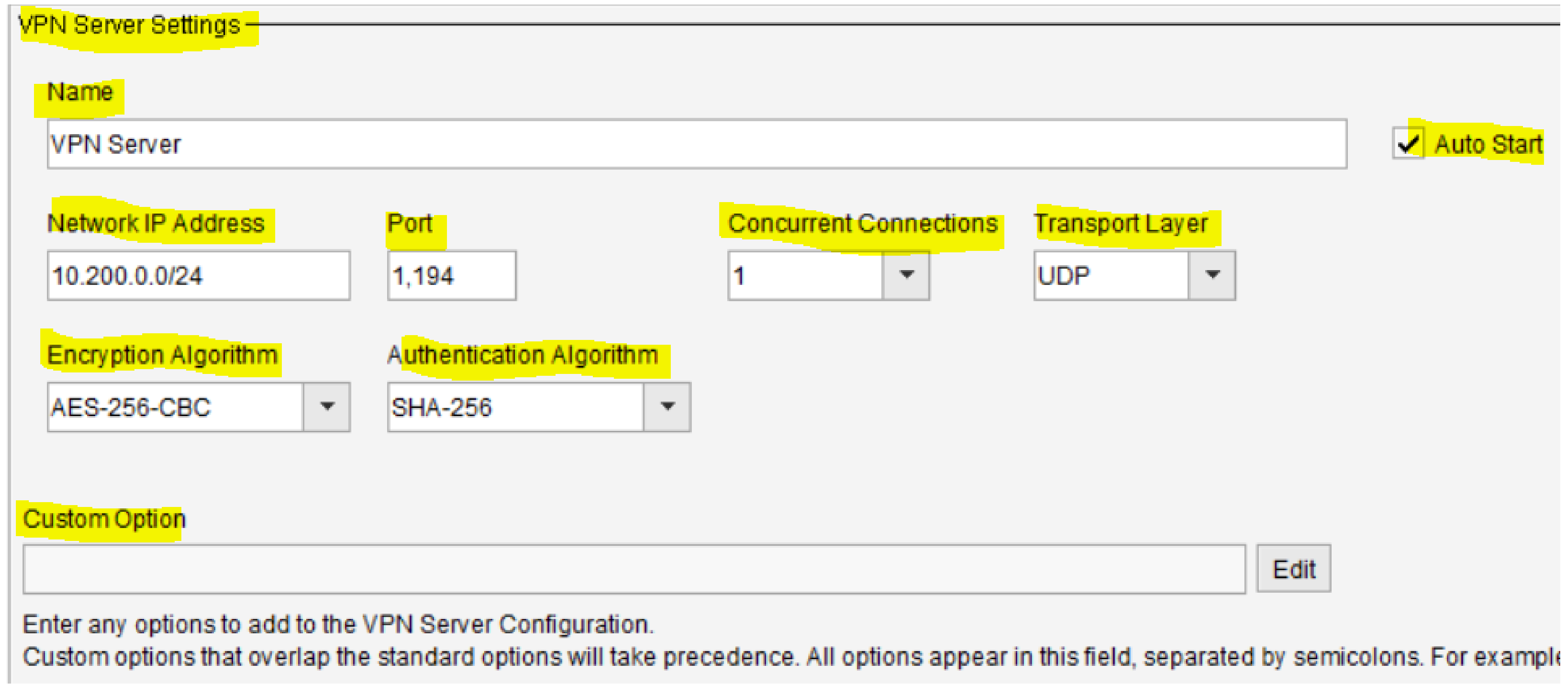
- DNP3 Master
- IEC 60870-5-104 Master
- Modbus TCP Master

The user assumes all responsibility for associated security risks when enabling unsecured services onto an unprotected network.

VPN Server

A VPN (Virtual Private Network) channel is available between the MCP and an OpenVPN client running on a remote computer. This VPN channel allows access to the protected services in the substation. The following settings are used when configuring a **VPN Server**:

- Name (Default: VPN Server)
- Auto Start (Default: Enabled)
- Network IP Address (Default: 10.200.0.0/24)
- Port (Default: 1194)
- Concurrent Connections (Default: 1)
- Transport Layer (Default: UDP)
- Encryption Algorithm (Default: AES-256-CBC)
- Authentication Algorithm (Default: SHA-256)
- Custom Option



Name: VPN Server

☑ Auto Start

Network IP Address: 10.200.0.0/24

Port: 1,194

Concurrent Connections: 1

Transport Layer: UDP

Encryption Algorithm: AES-256-CBC

Authentication Algorithm: SHA-256

Custom Option:

Enter any options to add to the VPN Server Configuration.
Custom options that overlap the standard options will take precedence. All options appear in this field, separated by semicolons. For example

Enter any options to be added to the VPN Server Configuration. Custom options that overlap the standard options take precedence. All options appear in this field, separated by semicolons. For example: reneg-sec 900; keepalive 90

To Edit This Field:

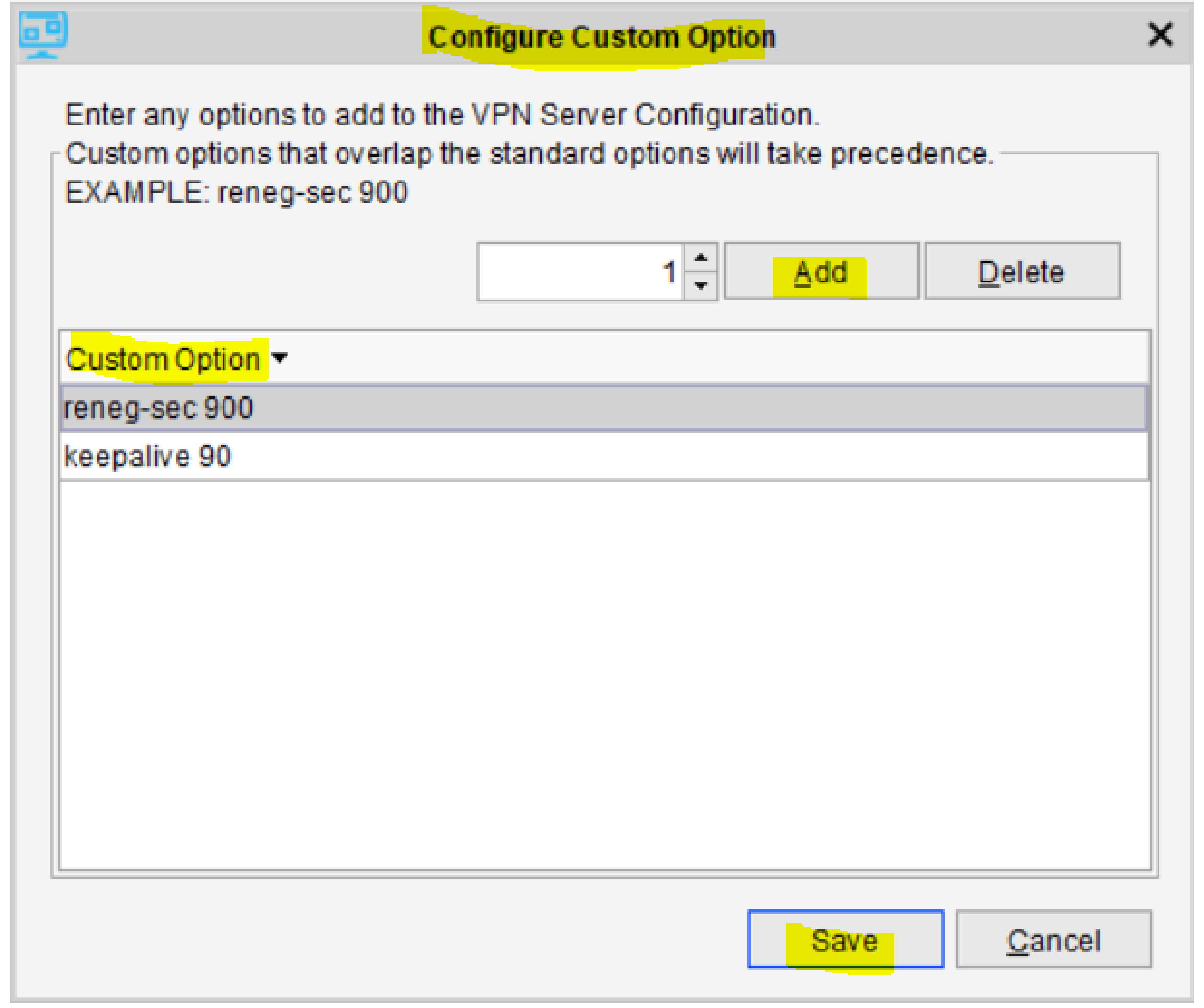
1. Click the **Edit** button.

   Result: The **Configure Custom Option** window appears.

2. Click the **Add** button.

   Result: A line appears as a **Custom Option**.

3. Enter the text.
4. Click **Save**.



Enter any options to add to the VPN Server Configuration.
Custom options that overlap the standard options will take precedence.
EXAMPLE: reneg-sec 900

1

Custom Option
reneg-sec 900
keepalive 90

Refer to the Integration of MCP with OpenVPN Client - Configuration Guide (SWM0103) for the detailed procedures used to:

Implement a simple Certification Authority using Open-Source tool - XCA

Install certificates on the MCP and Windows PC running OpenVPN client

Configure VPN Server and VPN Client configuration on the MCP

Configure OpenVPN client to communicate to the MCP over Virtual Private Network

Custom Options are advanced options and take precedence over the standard options. The standard options are secure by default. Implementing custom options can impact the security strength (e.g., using weak ciphers such as DES*, RC2-*, and BF-*). The customer assumes risk of weakened security when implementing custom options. Consult the online OpenVPN literature for guidance.

Syslog Client

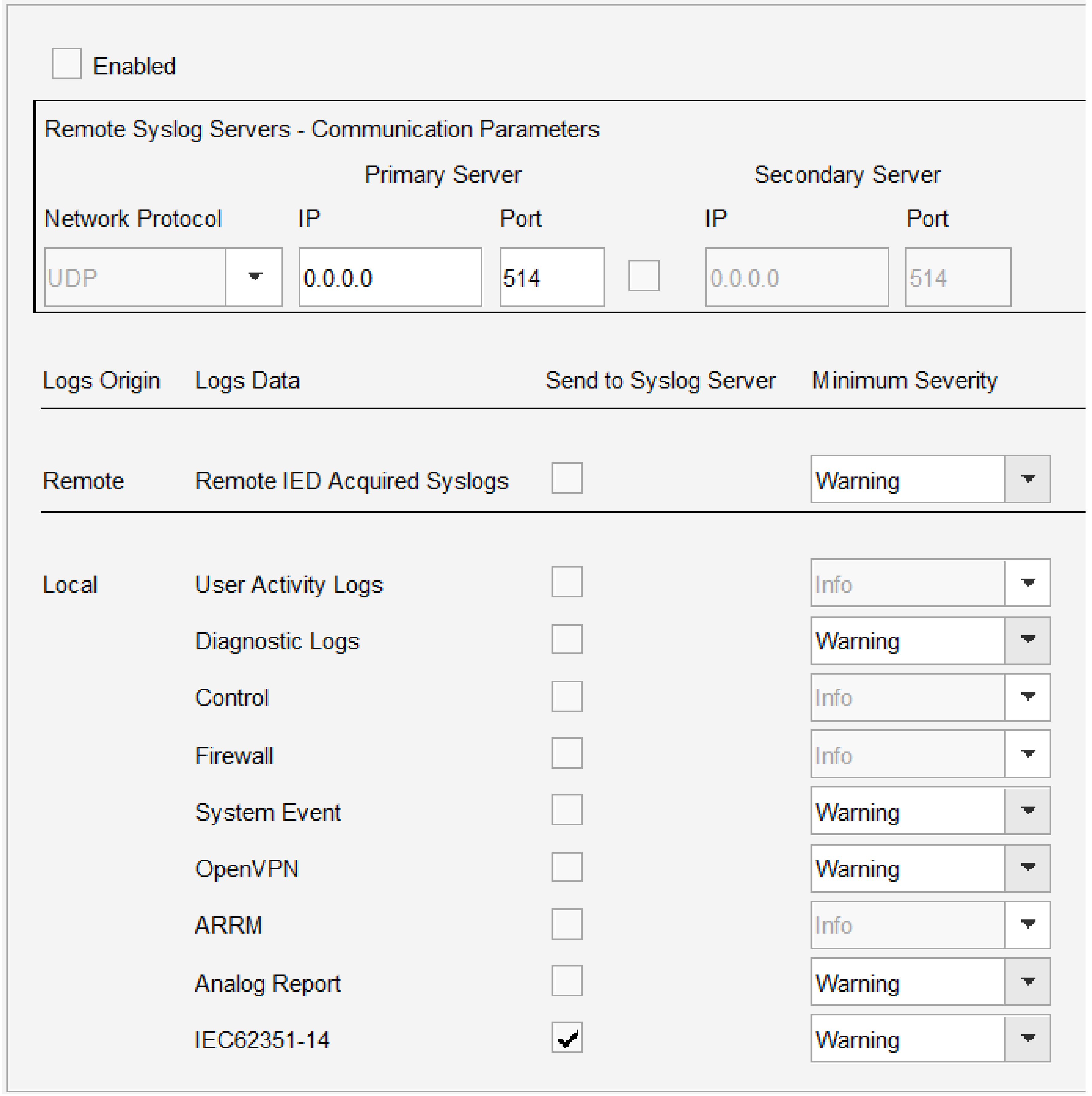
When the **Syslog Client** application is configured, it enables the MCP to transfer the internally generated security events, application log events & locally buffered remote IED syslogs to remote syslog server over **UDP**.

While configuring Syslog Client, these **Remote Syslog Servers – Communication Parameters** are available:

- Enabled
- Network Protocol
- Primary Server IP
- Primary Server Port
- Secondary Server Enabled
- Secondary Server IP
- Secondary Server Port

There are two categories of logs supported: **Remote Logs** and **Local Logs**. For each supported type of Logs, you can select whether to **Send to Syslog Server** and set the **Minimum Severity** individually:

- Remote IED Acquired Syslogs (Default Min. Severity: Warning)
- User Activity Logs (Min. Severity Always as Info)
- Diagnostic Logs (Default Min. Severity: Warning)
- Control Logs (Min. Severity Always as Info)
- Firewall Logs (Min. Severity Always as Info)
- System Events (Default Min. Severity: Warning)
- OpenVPN Logs (Default Min. Severity: Warning)
- ARRM Logs (Min. Severity Always as Info)
- Analog Report Logs (Default Min. Severity: Warning)
- IEC62351-14 Security Events (Default Min. Severity: Warning)



☐ Enabled

Remote Syslog Servers - Communication Parameters

	Primary Server			Secondary Server	
Network Protocol	IP	Port		IP	Port
UDP	0.0.0.0	514	☐	0.0.0.0	514

Logs Origin	Logs Data	Send to Syslog Server	Minimum Severity
Remote	Remote IED Acquired Syslogs	☐	Warning
Local	User Activity Logs	☐	Info
	Diagnostic Logs	☐	Warning
	Control	☐	Info
	Firewall	☐	Info
	System Event	☐	Warning
	OpenVPN	☐	Warning
	ARRM	☐	Info
	Analog Report	☐	Warning
	IEC62351-14	☑	Warning

Type of Minimum Severity:

- Alarm (Highest)
- Error
- Warning
- Notice
- Info (Lowest)

The Remote Syslog Server shall be accessible via **Predix EdgeManager IP**. To configure the Edge Manager IP, refer to the **EdgeManager Connectivity Configuration** detailed under the Configure Network Interfaces topic of the MCP Settings .

Analog Report Logs are not available after and including MCP V2.60.

GE VERNOVA

Learning & Development

Thank You

Technical Support by Location

Protection & Control or Automation
North America, Latin America
✉ GA.SupportNAM@ge.com
☎ North America: 1-800-547-8629
☎ International: 1-877-605-6777

Europe
✉ GA.SupportERCIS@ge.com
☎ +34 94 485 8817

Monitoring & Diagnostics Worldwide
✉ contact.center@ge.com
☎ +44 (0) 1785 250 070

Industrial Communications Worldwide
☎ North America: 1-800-474-0964
☎ International: 1-585-242-8311

Learning & Development By Location

Protection & Control or Automation
North America, Latin America
✉ training.multilin@ge.com

Europe
✉ GA.SupportERCIS@ge.com

Montpellier, France
✉ Grid-sam-training@ge.com
☎ +33 4 67 54 21 50

Monitoring & Diagnostics Worldwide
✉ Trainingevents.ManD@ge.com

Industrial Communications Worldwide
✉ training.mds@ge.com

GE Grid Solutions Website

http://www.gegridsolutions.com
http://www.gegridsolutions.com/Resources

Follow Us On Social Media

You Tube https://www.youtube.com/user/GEGridAutomationLD

Connect on LinkedIn
https://www.linkedin.com/company/gegridsolutions/

Need help fast? Reach out with this link today!

https://www.gegridsolutions.com/contact.htm

Contact Us

Copyrights

Copyrights 2024

GE VERNOVA