DNP Client Ethernet Driver

Table of Contents

DNP Client Ethernet Driver

Help version 1.206

CONTENTS

Overview

The DNP Client Ethernet Driver provides a reliable way to connect DNP server Ethernet devices to OPC Client applications; including HMI, SCADA, Historian, MES, ERP, and countless custom applications.

Setup

In the DNP3 protocol, a channel describes a physical communications path between two endpoints. A DNP3 session describes a specific communication between a DNP client node and a DNP server node. In the DNP Client Ethernet Driver, the OPC server channel represents the DNP3 channel and OPC server devices represent individual DNP3 sessions.

Communication Protocol

Distributed Network Protocol 3.0 (DNP3) via TCP or UDP

Supported Devices

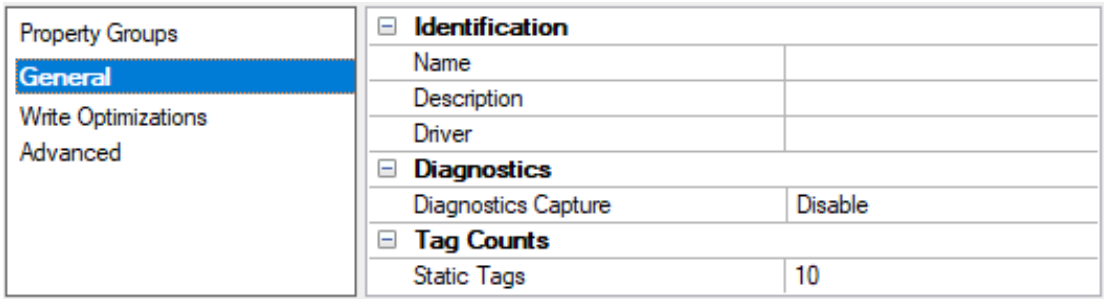
Any DNP3 server device

Channel and Device Limits

The maximum number of channels supported by this driver is 1024. The maximum number of devices supported by this driver is 1024 per channel.

Channel Properties — General

This server supports the use of multiple simultaneous communications drivers. Each protocol or driver used in a server project is called a channel. A server project may consist of many channels with the same communications driver or with unique communications drivers. A channel acts as the basic building block of an OPC link. This group is used to specify general channel properties, such as the identification attributes and operating mode.



Identification

Name: Specify the user-defined identity of this channel. In each server project, each channel name must be unique. Although names can be up to 256 characters, some client applications have a limited display window when browsing the OPC server's tag space. The channel name is part of the OPC browser information. The property is required for creating a channel.

For information on reserved characters, refer to "How To... Properly Name a Channel, Device, Tag, and Tag Group" in the server help.

Description: Specify user-defined information about this channel.

Many of these properties, including Description, have an associated system tag.

Driver: Specify the protocol / driver for this channel. Specify the device driver that was selected during channel creation. It is a disabled setting in the channel properties. The property is required for creating a channel.

Note: With the server's online full-time operation, these properties can be changed at any time. This includes changing the channel name to prevent clients from registering data with the server. If a client has already acquired an item from the server before the channel name is changed, the items are unaffected. If, after the channel name has been changed, the client application releases the item and attempts to re-acquire using the old channel name, the item is not accepted. Changes to the properties should not be made once a large client application has been developed. Utilize proper user role and privilege management to prevent operators from changing properties or accessing server features.

Diagnostics

Diagnostics Capture: When enabled, this option makes the channel's diagnostic information available to OPC applications. Because the server's diagnostic features require a minimal amount of overhead processing, it is recommended that they be utilized when needed and disabled when not. The default is disabled.

Note: This property is not available if the driver does not support diagnostics.

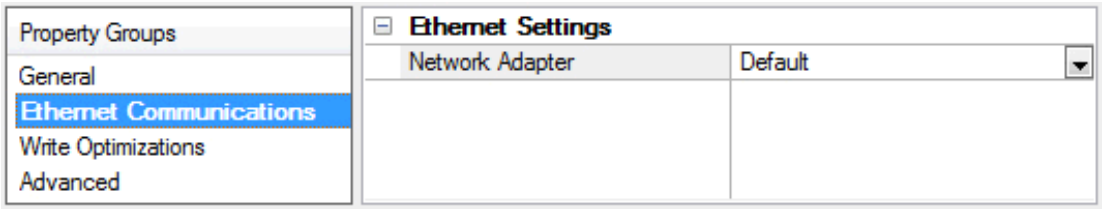
For more information, refer to "Communication Diagnostics" and "Statistics Tags" in the server help.

Tag Counts

Static Tags: Provides the total number of defined static tags at this level (device or channel). This information can be helpful in troubleshooting and load balancing.

Channel Properties — Ethernet Communications

Ethernet Communication can be used to communicate with devices.

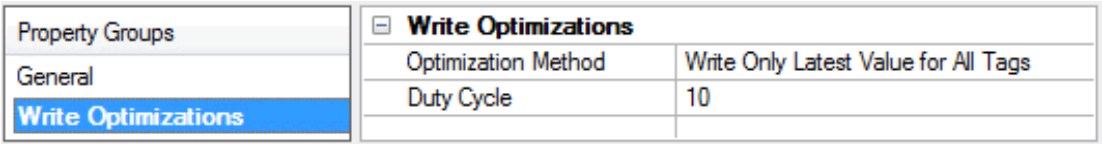


Ethernet Settings

Network Adapter: Specify the network adapter to bind. When left blank or Default is selected, the operating system selects the default adapter.

Channel Properties — Write Optimizations

The server must ensure that the data written from the client application gets to the device on time. Given this goal, the server provides optimization properties to meet specific needs or improve application responsiveness.



Write Optimizations

Optimization Method: Controls how write data is passed to the underlying communications driver. The options are:

- **Write All Values for All Tags**: This option forces the server to attempt to write every value to the controller. In this mode, the server continues to gather write requests and add them to the server's internal write queue. The server processes the write queue and attempts to empty it by writing data to the device as quickly as possible. This mode ensures that everything written from the client applications is sent to the target device. This mode should be selected if the write operation order or the write item's content must uniquely be seen at the target device.
- **Write Only Latest Value for Non-Boolean Tags**: Many consecutive writes to the same value can accumulate in the write queue due to the time required to actually send the data to the device. If the server updates a write value that has already been placed in the write queue, far fewer writes are needed to reach the same final output value. In this way, no extra writes accumulate in the server's queue. When the user stops moving the slide switch, the value in the device is at the correct value at virtually the same time. As the mode states, any value that is not a Boolean value is updated in the server's internal write queue and sent to the device at the next possible opportunity. This can greatly improve the application performance.
  Note: This option does not attempt to optimize writes to Boolean values. It allows users to optimize the operation of HMI data without causing problems with Boolean operations, such as a momentary push button.
- **Write Only Latest Value for All Tags**: This option takes the theory behind the second optimization mode and applies it to all tags. It is especially useful if the application only needs to send the latest

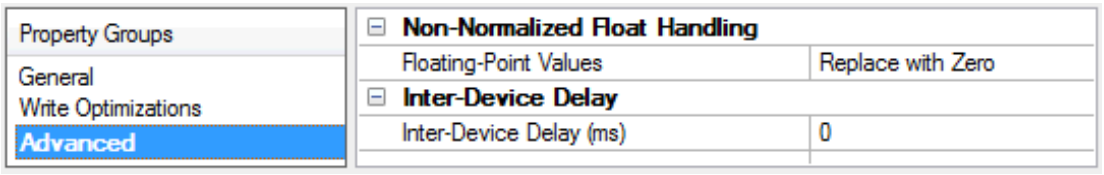
value to the device. This mode optimizes all writes by updating the tags currently in the write queue before they are sent. This is the default mode.

Duty Cycle: is used to control the ratio of write to read operations. The ratio is always based on one read for every one to ten writes. The duty cycle is set to ten by default, meaning that ten writes occur for each read operation. Although the application is performing a large number of continuous writes, it must be ensured that read data is still given time to process. A setting of one results in one read operation for every write operation. If there are no write operations to perform, reads are processed continuously. This allows optimization for applications with continuous writes versus a more balanced back and forth data flow.

Note: It is recommended that the application be characterized for compatibility with the write optimization enhancements before being used in a production environment.

Channel Properties — Advanced

This group is used to specify advanced channel properties. Not all drivers support all properties; so the Advanced group does not appear for those devices.



Non-Normalized Float Handling: A non-normalized value is defined as Infinity, Not-a-Number (NaN), or as a Denormalized Number. The default is Replace with Zero. Drivers that have native float handling may default to Unmodified. Non-normalized float handling allows users to specify how a driver handles non-normalized IEEE-754 floating point data. Descriptions of the options are as follows:

- **Replace with Zero**: This option allows a driver to replace non-normalized IEEE-754 floating point values with zero before being transferred to clients.
- **Unmodified**: This option allows a driver to transfer IEEE-754 denormalized, normalized, non-number, and infinity values to clients without any conversion or changes.

Note: This property is disabled if the driver does not support floating-point values or if it only supports the option that is displayed. According to the channel's float normalization setting, only real-time driver tags (such as values and arrays) are subject to float normalization. For example, EFM data is not affected by this setting.

For more information on the floating-point values, refer to "How To ... Work with Non-Normalized Floating-Point Values" in the server help.

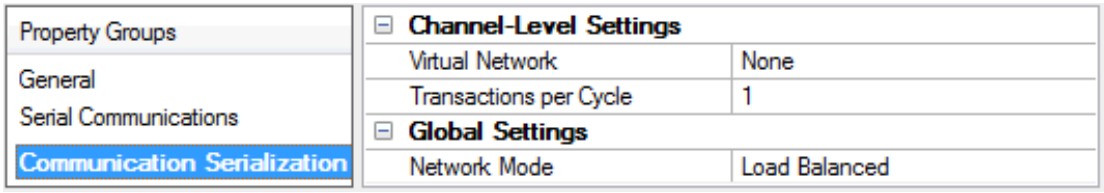
Inter-Device Delay: Specify the amount of time the communications channel waits to send new requests to the next device after data is received from the current device on the same channel. Zero (0) disables the delay.

Note: This property is not available for all drivers, models, and dependent settings.

Channel Properties — Communication Serialization

The server's multi-threading architecture allows channels to communicate with devices in parallel. Although this is efficient, communication can be serialized in cases with physical network restrictions (such as Ethernet radios). Communication serialization limits communication to one channel at a time within a virtual network.

The term "virtual network" describes a collection of channels and associated devices that use the same pipeline for communications. For example, the pipeline of an Ethernet radio is the client radio. All channels using the same client radio associate with the same virtual network. Channels are allowed to communicate each in turn, in a "round-robin" manner. By default, a channel can process one transaction before handing communications off to another channel. A transaction can include one or more tags. If the controlling channel contains a device that is not responding to a request, the channel cannot release control until the transaction times out. This results in data update delays for the other channels in the virtual network.



Channel-Level Settings

Virtual Network: Specify the channel's mode of communication serialization. Options include None and Network 1 - Network 500. The default is None. Descriptions of the options are as follows:

- **None**: This option disables communication serialization for the channel.
- **Network 1 - Network 500**: This option specifies the virtual network to which the channel is assigned.

Transactions per Cycle: Specify the number of single blocked/non-blocked read/write transactions that can occur on the channel. When a channel is given the opportunity to communicate, this is the number of transactions attempted. The valid range is 1 to 99. The default is 1.

Global Settings

Network Mode: This property is used to control how channel communication is delegated. In **Load Balanced** mode, each channel is given the opportunity to communicate in turn, one at a time. In **Priority** mode, channels are given the opportunity to communicate according to the following rules (highest to lowest priority):

1. Channels with pending writes have the highest priority.
2. Channels with pending explicit reads (through internal plug-ins or external client interfaces) are prioritized based on the read's priority.
3. Scanned reads and other periodic events (driver specific).

The default is Load Balanced and affects *all* virtual networks and channels.

Devices that rely on unsolicited responses should not be placed in a virtual network. In situations where communications must be serialized, it is recommended that Auto-Demotion be enabled.

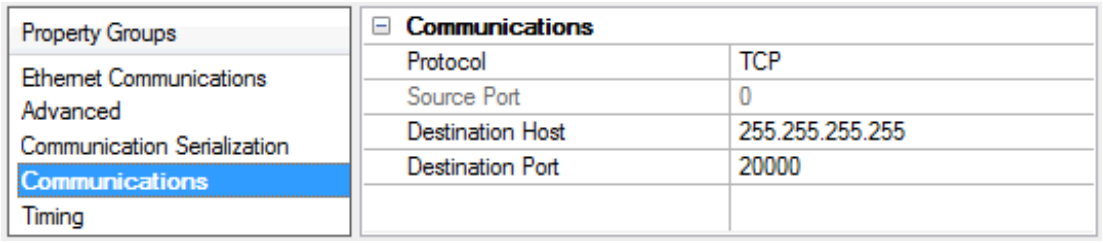
Due to differences in the way that drivers read and write data (such as in single, blocked, or non-blocked transactions); the application's Transactions per cycle property may need to be adjusted. When doing so, consider the following factors:

- How many tags must be read from each channel?
- How often is data written to each channel?
- Is the channel using a serial or Ethernet driver?

- Does the driver read tags in separate requests, or are multiple tags read in a block?
- Have the device's Timing properties (such as Request timeout and Fail after *x* successive timeouts) been optimized for the virtual network's communication medium?

Channel Properties — Communications

The Communications group is used to specify the protocol settings for communication with the DNP outstation.



Protocol: Specify the communication protocol. Options include TCP and UDP. The default setting is TCP.

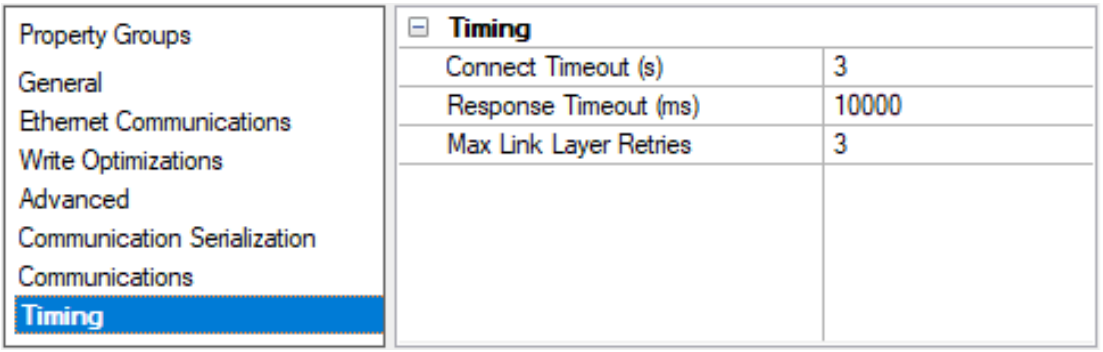
Source Port: Specify the Source Port. The default setting is 0.
Note: When the selected protocol is TCP, this parameter is disabled. When the selected protocol is UDP, setting the Source Port to 0 causes an implicit bind using a unique source port assigned by the system.

Destination Host: Specify the Destination Host. The default setting is 255.255.255.255.

Destination Port: Specify the Destination Port. The valid range is 1 to 65535. The default setting is 20000.

Channel Properties — Timing

The Timing group is independent of any OPC timeout values and only affects the DNP communications with DNP server units. It is used to specify the length of time the driver waits until a connect or response timeout occurs.



Connect Timeout (s) This property specifies how long the device waits for a connection request to complete before timing out. The valid range is 1 to 30 seconds. The default setting is 3 seconds.

Response Timeout (ms): This property specifies how long the device waits for a response to a request before timing out. The valid range is 100 to 3600000 milliseconds. The default setting is 10000 milliseconds.

Max Link Layer Retries: This property specifies how many times the server sends a link layer status request when the device is not responding. When the limit is reached, the connection closes and a DNR error is posted. The valid range is from 0 to 255. The default setting is 3 retries.

For more information on performance, refer to ***Timing and Other Considerations****.*

Timing and Other Considerations

Suggested Time Settings

Since the DNP3 protocol keeps communications at a minimum, the following suggested settings help the server and driver operate efficiently.

1. Only one transaction can be handled on the communications channel at a time. In situations where multiple devices share a single communications channel, the driver must move from one device to the next as quickly as possible to gather information at an effective rate. As more devices are added (or more information is requested from a device), the overall update rate begins to suffer.
   An unresponsive device blocks the other devices on that channel from receiving service while the Channel Response Timeout elapses. The explicit requests to the devices slow down and the event poll intervals are affected once one or more devices fail to respond.

2. The entire send and receive transaction for a device must complete within the device Request Timeout. If the send is successful, the response must be received within the Channel Response Timeout. The device Request Timeout should be greater than or equal to the Channel Response Timeout.

3. Timeouts should be set to accommodate the responsiveness of a particular DNP server device: they should not be set too low. For example, if the device Request Timeout and/or Channel Response Timeout were set to zero, the driver would be perpetually timed out and all effective communication would cease. Under these circumstances, users would likely receive Event Log error messages such as "Device <device name> is not responding". To determine the best settings for the Channel Response Timeout and the device Request Timeout, consider the following example:

   There is one communications channel for 10 devices, and 9 of them are offline. Each device waits the duration of the Channel Response Timeout (default setting 10 seconds), which blocks the other devices. To keep the tenth device from failing due to the device Request Timeout (default setting 30 seconds), the device Request Timeout must be longer than it takes all of the offline devices to timeout one at a time. In this situation, a device Request Timeout of 100 seconds should allow the tenth device to successfully complete its send and receive transaction after the nine devices timed out.

4. If the channel response timeout is longer than a device's poll interval, a delay may occur in event polling. For example, a device that shares a channel with other devices is not responding. If any device on that channel has a poll interval set at a shorter rate than the channel response timeout, the poll interval rate for that device is not met. Event polling occurs as soon as the timeout has elapsed and the device is serviced. Once the device begins communicating again, the event poll interval returns to its defined rate.

5. Object group 50 is the DNP server's clock. Since it cannot be received in event polls or through unsolicited messages, the DNP Client Ethernet Driver must explicitly request a read. Furthermore, because it is a time datum, the driver requests a read every time the tag is pulled for an update. On a default instantiation, that is every 200 ms. To avoid congesting the communications link, create a separate OPC group for the object group 50 time tag and set that group's update rate to 1000 ms or slower. For more information on all objects, refer to **Object Definitions**.

Tip: There are a variety of communication serialization tags that can be used to debug timing issues involving a serialization network.
For more information, refer to "Communication Serialization Tags" in the server help documentation.

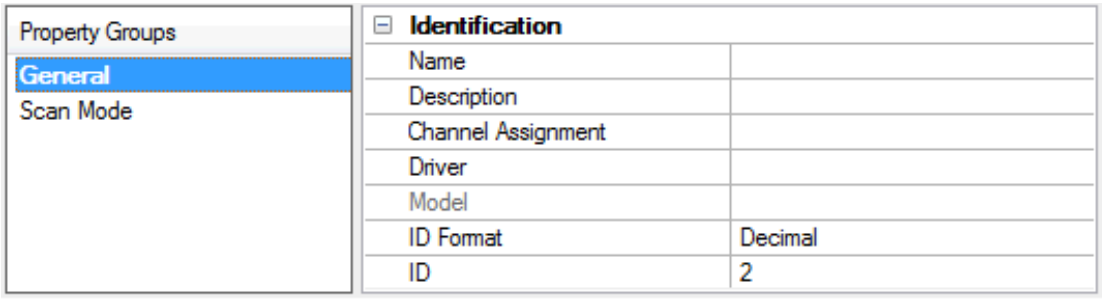
Effects of DNP Devices Going Offline

When a device goes offline, it may disrupt the DNP communications for all devices using the same channel. This is because DNP is a synchronous protocol; meaning, it requires an acknowledgment, timeout, or confirmed failure for the current command before the next command in the queue may be transmitted. The driver often queues multiple commands within a typical DNP timeout period. The DNP stack must dispose of these commands in the order they are received. Outstanding commands for still-responsive DNP server devices can be blocked until the command queue empties. For more examples of offline scenarios, refer to "Suggested Time Settings" above.

Devices that have gone offline cause a delay in the shutdown of the OPC server while the server waits for timeouts to expire.

Device Properties — General

A device represents a single target on a communications channel. If the driver supports multiple controllers, users must enter a device ID for each controller.



Identification

Name: Specify the name of the device. It is a logical user-defined name that can be up to 256 characters long and may be used on multiple channels.

Note: Although descriptive names are generally a good idea, some OPC client applications may have a limited display window when browsing the OPC server's tag space. The device name and channel name become part of the browse tree information as well. Within an OPC client, the combination of channel name and device name would appear as "ChannelName.DeviceName".
For more information, refer to "How To... Properly Name a Channel, Device, Tag, and Tag Group" in server help.

Description: Specify the user-defined information about this device.
Many of these properties, including Description, have an associated system tag.

Channel Assignment: Specify the user-defined name of the channel to which this device currently belongs.

Driver: Selected protocol driver for this device.

Model: Specify the type of device that is associated with this ID. The contents of the drop-down menu depend on the type of communications driver being used. Models that are not supported by a driver are

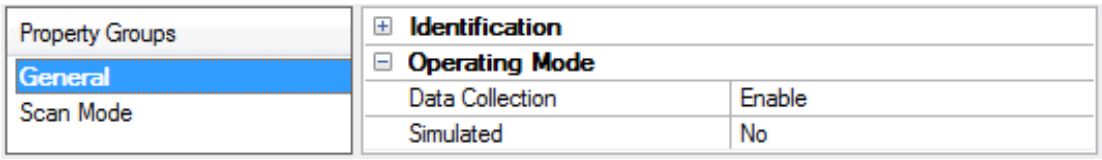
disabled. If the communications driver supports multiple device models, the model selection can only be changed when there are no client applications connected to the device.

Note: If the communication driver supports multiple models, users should try to match the model selection to the physical device. If the device is not represented in the drop-down menu, select a model that conforms closest to the target device. Some drivers support a model selection called "Open," which allows users to communicate without knowing the specific details of the target device. For more information, refer to the driver help documentation.

ID: Specify the device's driver-specific station or node. The type of ID entered depends on the communications driver being used. For many communication drivers, the ID is a numeric value. Drivers that support a Numeric ID provide users with the option to enter a numeric value whose format can be changed to suit the needs of the application or the characteristics of the selected communications driver. The format is set by the driver by default. Options include Decimal, Octal, and Hexadecimal.

Note: If the driver is Ethernet-based or supports an unconventional station or node name, the device's TCP/IP address may be used as the device ID. TCP/IP addresses consist of four values that are separated by periods, with each value in the range of 0 to 255. Some device IDs are string based. There may be additional properties to configure within the ID field, depending on the driver.

Operating Mode



Data Collection: This property controls the device's active state. Although device communications are enabled by default, this property can be used to disable a physical device. Communications are not attempted when a device is disabled. From a client standpoint, the data is marked as invalid and write operations are not accepted. This property can be changed at any time through this property or the device system tags.

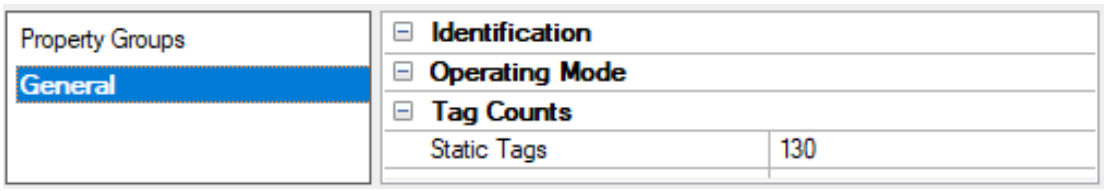
Simulated: Place the device into or out of Simulation Mode. In this mode, the driver does not attempt to communicate with the physical device, but the server continues to return valid OPC data. Simulated stops physical communications with the device, but allows OPC data to be returned to the OPC client as valid data. While in Simulation Mode, the server treats all device data as reflective: whatever is written to the simulated device is read back and each OPC item is treated individually. The data is not saved if the server removes the item (such as when the server is reinitialized). The default is No.

Notes:

1. This System tag (_Simulated) is read only and cannot be written to for runtime protection. The System tag allows this property to be monitored from the client.
2. When a device is simulated, updates may not appear faster than one (1) second client.

Simulation Mode is for test and simulation purposes only. It should never be used in a production environment.

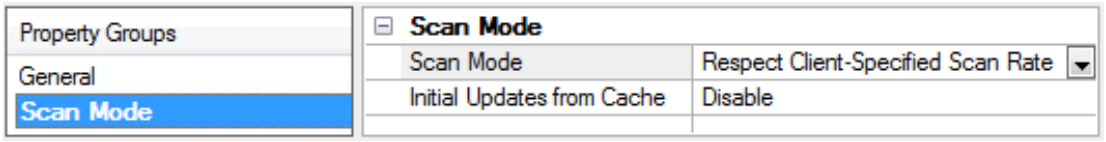
Tag Counts



Static Tags: Provides the total number of defined static tags at this level (device or channel). This information can be helpful in troubleshooting and load balancing.

Device Properties — Scan Mode

The Scan Mode specifies the subscribed-client requested scan rate for tags that require device communications. Synchronous and asynchronous device reads and writes are processed as soon as possible; unaffected by the Scan Mode properties.



Scan Mode: Specify how tags in the device are scanned for updates sent to subscribing clients. Descriptions of the options are:

- **Respect Client-Specified Scan Rate**: This mode uses the scan rate requested by the client.
- **Request Data No Faster than Scan Rate**: This mode specifies the value set as the maximum scan rate. The valid range is 10 to 99999990 milliseconds. The default is 1000 milliseconds.
  Note: When the server has an active client and items for the device and the scan rate value is increased, the changes take effect immediately. When the scan rate value is decreased, the changes do not take effect until all client applications have been disconnected.
- **Request All Data at Scan Rate**: This mode forces tags to be scanned at the specified rate for subscribed clients. The valid range is 10 to 99999990 milliseconds. The default is 1000 milliseconds.
- **Do Not Scan, Demand Poll Only**: This mode does not periodically poll tags that belong to the device nor perform a read to get an item's initial value once it becomes active. It is the OPC client's responsibility to poll for updates, either by writing to the _DemandPoll tag or by issuing explicit device reads for individual items. *For more information, refer to "Device Demand Poll" in server help*.
- **Respect Tag-Specified Scan Rate**: This mode forces static tags to be scanned at the rate specified in their static configuration tag properties. Dynamic tags are scanned at the client-specified scan rate.

Initial Updates from Cache: When enabled, this option allows the server to provide the first updates for newly activated tag references from stored (cached) data. Cache updates can only be provided when the new item reference shares the same address, scan rate, data type, client access, and scaling properties. A device read is used for the initial update for the first client reference only. The default is disabled; any time a client activates a tag reference the server attempts to read the initial value from the device.

Device Properties — Tag Generation

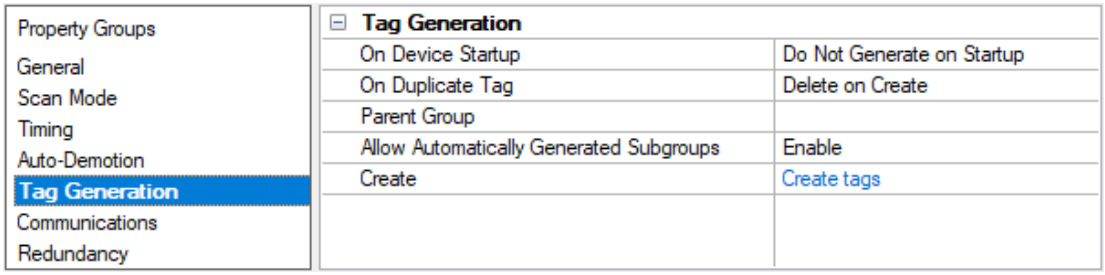
The automatic tag database generation features make setting up an application a plug-and-play operation. Select communications drivers can be configured to automatically build a list of tags that correspond to device-specific data. These automatically generated tags (which depend on the nature of the supporting driver) can be browsed from the clients.

Not all devices and drivers support full automatic tag database generation and not all support the same data types. Consult the data types descriptions or the supported data type lists for each driver for specifics.

If the target device supports its own local tag database, the driver reads the device's tag information and uses the data to generate tags within the server. If the device does not natively support named tags, the driver creates a list of tags based on driver-specific information. An example of these two conditions is as follows:

1. If a data acquisition system supports its own local tag database, the communications driver uses the tag names found in the device to build the server's tags.
2. If an Ethernet I/O system supports detection of its own available I/O module types, the communications driver automatically generates tags in the server that are based on the types of I/O modules plugged into the Ethernet I/O rack.

Note: Automatic tag database generation's mode of operation is completely configurable. *For more information, refer to the property descriptions below.*



On Property Change: If the device supports automatic tag generation when certain properties change, the **On Property Change** option is shown. It is set to **Yes** by default, but it can be set to **No** to control over when tag generation is performed. In this case, the **Create tags** action must be manually invoked to perform tag generation.

On Device Startup: Specify when OPC tags are automatically generated. Descriptions of the options are as follows:

- **Do Not Generate on Startup**: This option prevents the driver from adding any OPC tags to the tag space of the server. This is the default setting.
- **Always Generate on Startup**: This option causes the driver to evaluate the device for tag information. It also adds tags to the tag space of the server every time the server is launched.
- **Generate on First Startup**: This option causes the driver to evaluate the target device for tag information the first time the project is run. It also adds any OPC tags to the server tag space as needed.

Note: When the option to automatically generate OPC tags is selected, any tags that are added to the server's tag space must be saved with the project. Users can configure the project to automatically save from the **Tools** | **Options** menu.

On Duplicate Tag: When automatic tag database generation is enabled, the server needs to know what to do with the tags that it may have previously added or with tags that have been added or modified after the communications driver since their original creation. This setting controls how the server handles OPC tags that were automatically generated and currently exist in the project. It also prevents automatically generated tags from accumulating in the server.

For example, if a user changes the I/O modules in the rack with the server configured to **Always Generate on Startup**, new tags would be added to the server every time the communications driver detected a new I/O module. If the old tags were not removed, many unused tags could accumulate in the server's tag space. The options are:

- **Delete on Create**: This option deletes any tags that were previously added to the tag space before any new tags are added. This is the default setting.
- **Overwrite as Necessary**: This option instructs the server to only remove the tags that the communications driver is replacing with new tags. Any tags that are not being overwritten remain in the server's tag space.
- **Do not Overwrite**: This option prevents the server from removing any tags that were previously generated or already existed in the server. The communications driver can only add tags that are completely new.
- **Do not Overwrite, Log Error**: This option has the same effect as the prior option, and also posts an error message to the server's Event Log when a tag overwrite would have occurred.

Note: Removing OPC tags affects tags that have been automatically generated by the communications driver as well as any tags that have been added using names that match generated tags. Users should avoid adding tags to the server using names that may match tags that are automatically generated by the driver.

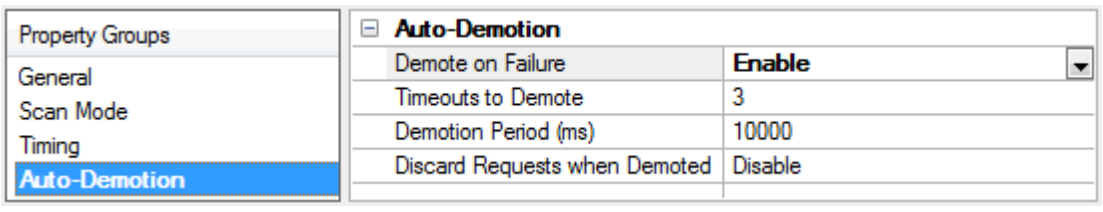
Parent Group: This property keeps automatically generated tags from mixing with tags that have been entered manually by specifying a group to be used for automatically generated tags. The name of the group can be up to 256 characters. This parent group provides a root branch to which all automatically generated tags are added.

Allow Automatically Generated Subgroups: This property controls whether the server automatically creates subgroups for the automatically generated tags. This is the default setting. If disabled, the server generates the device's tags in a flat list without any grouping. In the server project, the resulting tags are named with the address value. For example, the tag names are not retained during the generation process.
Note: If, as the server is generating tags, a tag is assigned the same name as an existing tag, the system automatically increments to the next highest number so that the tag name is not duplicated. For example, if the generation process creates a tag named "AI22" that already exists, it creates the tag as "AI23" instead.

Create: Initiates the creation of automatically generated OPC tags. If the device's configuration has been modified, **Create tags** forces the driver to reevaluate the device for possible tag changes. Its ability to be accessed from the System tags allows a client application to initiate tag database creation.
Note: **Create tags** is disabled if the Configuration edits a project offline.

Device Properties — Auto-Demotion

The Auto-Demotion properties can temporarily place a device off-scan in the event that a device is not responding. By placing a non-responsive device offline for a specific time period, the driver can continue to optimize its communications with other devices on the same channel. After the time period has been reached, the driver re-attempts to communicate with the non-responsive device. If the device is responsive, the device is placed on-scan; otherwise, it restarts its off-scan time period.



Demote on Failure: When enabled, the device is automatically taken off-scan until it is responding again.
Tip: Determine when a device is off-scan by monitoring its demoted state using the _AutoDemoted system tag.

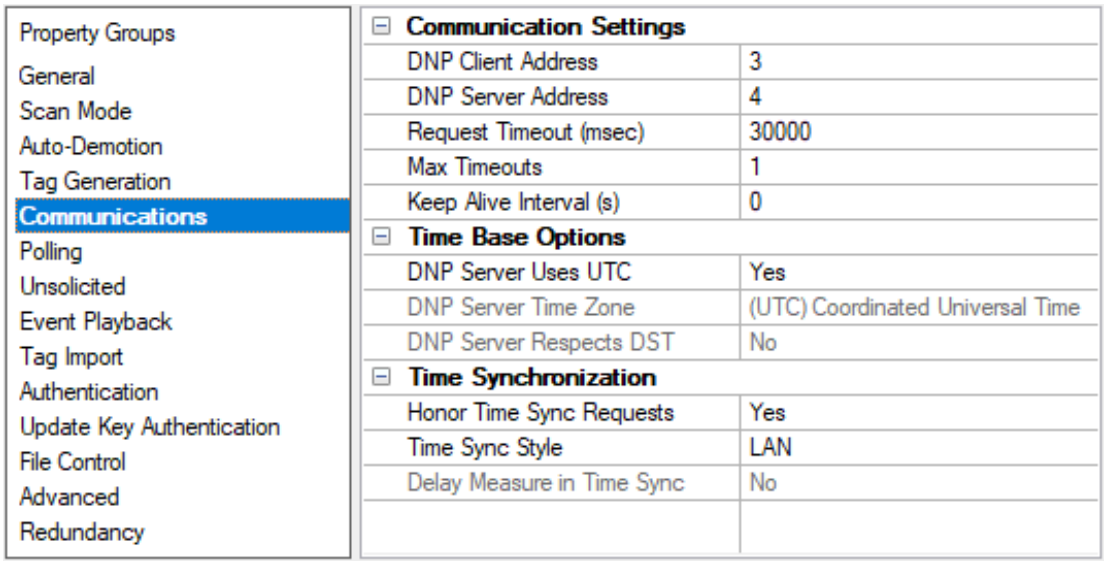
Timeouts to Demote: Specify how many successive cycles of request timeouts and retries occur before the device is placed off-scan. The valid range is 1 to 30 successive failures. The default is 3.

Demotion Period: Indicate how long the device should be placed off-scan when the timeouts value is reached. During this period, no read requests are sent to the device and all data associated with the read requests are set to bad quality. When this period expires, the driver places the device on-scan and allows for another attempt at communications. The valid range is 100 to 3600000 milliseconds. The default is 10000 milliseconds.

Discard Requests when Demoted: Select whether or not write requests should be attempted during the off-scan period. Disable to always send write requests regardless of the demotion period. Enable to discard writes; the server automatically fails any write request received from a client and does not post a message to the Event Log.

Device Properties — Communications

The Communication Settings section is used to specify the DNP client and server 16-bit addresses, the request timeout, and the keep-alive interval.



Communication Settings

- **DNP Client Address:** This property specifies the address of the DNP client (this device) to which the DNP server devices communicate. The address must be unique and can range from 0 to 65519. Some addresses are reserved. The default setting is 3.
- **DNP Server Address:** This property specifies the address to the DNP server (remote device). The valid range is 0 to 65519. The default setting is 4.
- **Request Timeout (ms):** This property specifies the amount of time in which a command must be completed once it is transmitted. The valid range is 100 to 3600000 milliseconds. The default setting is 30000 milliseconds.
  For more information on performance, refer to ***Timing and Other Considerations****.*

- **Max. Timeouts:** This property specifies the maximum number of successive timeouts that can occur with the same request before the device is considered to be in error. A timeout occurs when the entire request and response do not complete within the device Request Timeout, or when the request successfully transmits but the response is not received within the Channel Response Timeout. Due to incremented sequence numbers, the regenerated request is not identical to the original request. Requests to and responses from other devices on the same channel may occur between retries. The valid range is 1 to 10 timeouts. The default setting is 1 timeout.
  Note: If a large response is being received when the timeout expires, it is NOT considered a timeout because there is no problem with communications. Only if the device truly stops responding does a timeout occur. For more information on such a message, refer to **Unable to receive response from device**.
- **Keep-Alive Interval (sec):** This property specifies when to transmit a keep-alive status request to the DNP server. The valid range is 0 to 86400 seconds. The default setting is 0 seconds (which indicates that a keep-alive status request message are not sent).
  Important: The status request is only transmitted if the entire Keep-Alive Interval elapses without any communication from the DNP server. The keep-alive timer restarts whenever a message is received from a DNP Server. If a response is not received from the keep-alive status request, the connection is called broken and the appropriate action is taken. If a keep-alive design is desired and polling for events occurs, users should set the Keep-Alive Interval longer than the Event Poll Intervals. In this situation, the received event poll response restarts the keep-alive timer: as a result, no keep-alive status request is sent. A keep-alive status request is only transmitted if polling ceases.
  Note: This parameter is disabled when the channel protocol is set to UDP.

Time Base Options

The Time Base Options section is used to specify the DNP server time base for time synchronization and event time of occurrence. Although the DNP3 specification indicates that DNP3 time corresponds to Universal Coordinated Time (UTC), these parameters allow users to specify that the DNP server use a different time base. The driver uses these parameters both when synching the device time and when converting the device's event time of occurrence to UTC time.

- **DNP Server Uses UTC:** This property specifies the time base of the DNP server to be used during time synchronization and event time of occurrences. When Yes is selected, Universal Coordinated Time is used. The default setting is Yes.
  Caution: Because the majority of DNP servers follow the DNP3 specification and use UTC as their time base, it is not recommended that users change this setting unless it is known that the device does not follow the DNP3 specification.
- **DNP Server Time Zone:** This property specifies the time zone to be used to set the time in the DNP server. This option is only available when the UTC parameter is set to No. The default setting is (UTC) Coordinated Universal Time, which is set according to the DNP3 specification.
- **DNP Server Respects DST:** This property specifies whether the time that is set in the DNP server respects Daylight Saving Time. When No is selected, Daylight Saving Time is ignored. This option is only available when the UTC parameter is set to No. The default setting is No because UTC does not use Daylight Saving Time.

Time Synchronization

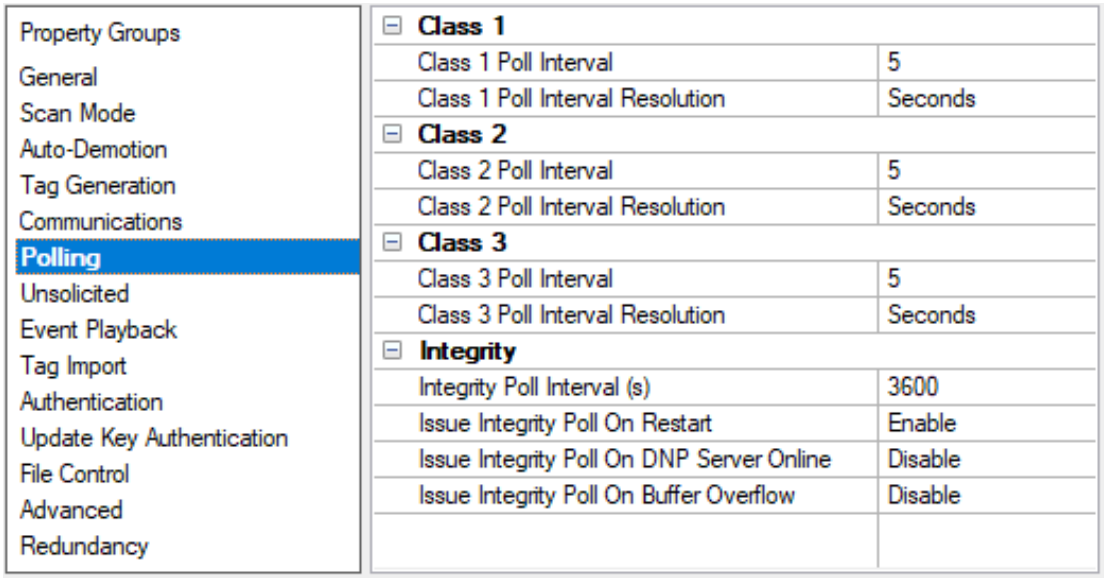
The Time Synchronization section is used to specify the device's time synchronization style and delays. Until time synchronization has occurred, it is possible for the reported DNP server's time information to be inaccurate.

- **Honor Time Sync Requests**: When set to No, the driver does not respect time synchronization requests from the device. The request is acknowledged, but no time synchronization occurs. The

default setting is Yes.

- **Time Sync Style:** This property specifies the DNP client's style of time synchronization when a synchronization request is received from the DNP server. Options include Serial and LAN. In Serial, the DNP client makes a delay measurement using function code 23 over the link and then writes a lag-corrected value using object group 50 - Variation 1. In LAN, the DNP client first sends a request with function code 24 to tell the DNP server to record the current time. Then, the DNP client writes the current time using object group 50 - Variation 3. The default setting is LAN. This option is only available when Honor Time Sync Requests is set to Yes.
- **Delay Measure in Time Sync:** When enabled, this property specifies that the delay measure function code 23 is used in time synchronization. This option is only available when Honor Time Sync Requests is set to Yes and Time Sync Style is Serial. The default setting is No.

Device Properties — Polling



Class *n*

Class *n* Poll Interval: Specify the frequency with which each event class is polled for data changes. To turn off the event poll for a given class, enter zero (0). The default setting is 5 seconds. The valid ranges are:

- Milliseconds: 0, 10 – 99999
- Seconds: 0 - 86400
- Minutes: 0 – 1440
- Hours: 0 - 24

Class *n* Poll Interval Resolution: Select the units for the poll interval from the drop-down list to the right. Choices are milliseconds, seconds, minutes, and hours.

Integrity

The Integrity properties control when a complete data retrieval is requested from the DNP server device using classes 0, 1, 2, and 3 data requests.

Integrity Poll Interval: This property specifies the frequency with which a complete data retrieval is requested from the DNP server device. To turn off integrity polling, enter zero (0). The valid range is 0 to 2592000 seconds (30 days). The default setting is 3600 seconds.

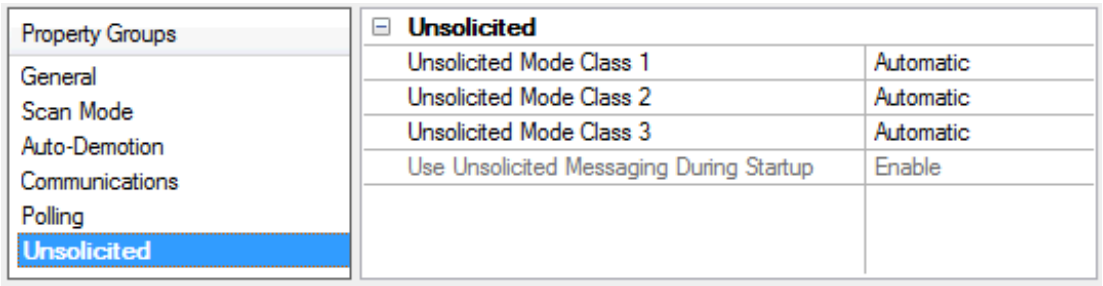
Issue Integrity Poll on Restart: This property specifies whether integrity polls occur on Restart. The default setting is enable.

Issue Integrity Poll on DNP Server Online: This property specifies whether integrity polls occur whenever the DNP server comes online. The default setting is disable.

Issue Integrity Poll on Buffer Overflow: This property specifies whether integrity polls occur whenever the DNP server indicates it has an event buffer overflow. The default setting is disable.

Device Properties — Unsolicited

The Unsolicited group is used to specify whether the DNP server sends class 1, 2, and 3 unsolicited data updates.



Unsolicited Mode Class *n*: Specify whether unsolicited messaging is allowed. Options include **Automatic**, **Enable**, and **Disable**. **Automatic** takes no action and is at the DNP server's discretion. **Enable** permits the reporting of data updates for the selected classes. **Disable** turns off unsolicited messaging. The default setting is **Automatic**.

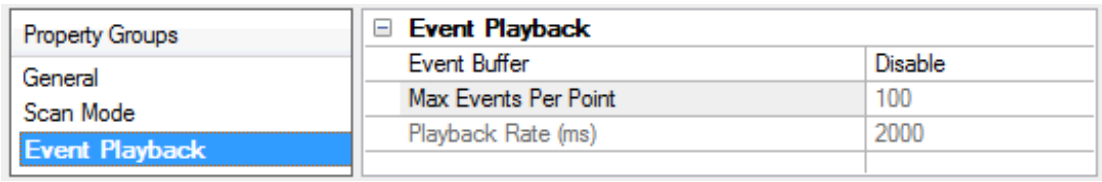
Use Unsolicited Messaging During Startup: Enable to allow unsolicited messaging during startup. This can only be disabled when one or more classes have **Enable** selected and no class has been set to **Automatic**. This setting applies to all event classes. The default setting is **Enable**.

Device Properties — Event Playback

The Event Playback group specifies when to retain a set number of updates and deliver them to clients. DNP server devices may be configured to retain event reports until contacted by a DNP client. The DNP server typically delivers event reports in bulk when responding to an integrity poll, event poll, or via unsolicited messages. The driver retains only the most recent update for a given I/O point and discards most or all of the historical stream by default.

- Event Playback continues if the device goes into an error state. If the device is still in an error state when playback for the tag completes, the tag quality is bad.

- Playback may be disrupted periodically by TCP connection attempts. It stops if auto-demotion is enabled and the device is demoted.



Event Buffer: When enabled, this option allows event reports from the remote DNP device to be buffered and played back for OPC client collection. The default setting is disabled.

Note: The OPC client may display intermittent buffered values if the DNP server sends buffered data while Event Playback is turned off.

Max Events Per Point: This property specifies the maximum events to be collected per point. The valid range is 1 to 10000. The default setting is 100.

Note: More than the specified Max Events Per Point can be played back if the DNP Client Ethernet Driver is in the middle of processing buffered data from the DNP server and more events arrive (or if Max Events Per Point is exceeded during the playback).

Playback Rate (ms): This property specifies the rate at which event reports are played back. The valid range is 50 to 10000. The default setting is 2000 milliseconds.

Effects of Playback on Clients

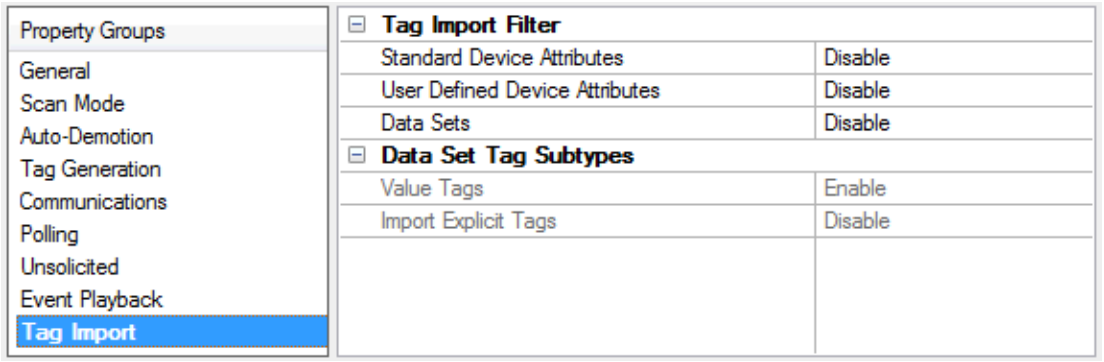
1. To assure retrieval of all buffered events, the client must have an update rate that is at least twice as fast as the Playback Rate. If the client's update rate is slower, it effectively overrides the Playback Rate.
2. Event Playback introduces latency to the tags for those affected objects. After the initial burst of events is played out of the buffer, incoming updates are only reported at the Playback Rate. New updates may have a time period of 2000 milliseconds between arriving and reporting to clients (at the default settings).

Notes:

1. Buffering should only be used when preservation of the event stream is more important than timely delivery of point updates. If a tag's event buffer fills up, new reports displace the oldest reports in the queue.
2. Enabling the OPC DA setting "Return initial updates for items in a single callback" may result in loss of buffered data when using drivers that support Event Playback for unsolicited device protocols. The compliance setting should be disabled if loss of buffered data is a concern. Consult the OPC Compliance Options in the server help.

Device Properties — Tag Import

The Tag Import group is used to specify options for importing tags from the DNP device.



Tag Import Filter

- **Standard Device Attributes:** When enabled, the driver creates tags for standardized object group 0 device Attributes defined by DNP3 at set index 0. The default setting is disabled.
- **User Defined Device Attributes:** When enabled, the driver creates tags for object group 0 device Attributes indexes 1 and above. The default setting is disabled.
- **Data Sets:** When enabled, the driver creates tags for object group 87 - Data Sets. The default setting is disabled.
  Note: The DNP Client Ethernet Driver does not create tags for data sets with more than 32 elements.

Important: The driver creates all tag groups through communication with the device after it determine that tags are available in the target device. For accurate tag import, the communication settings must be correct.

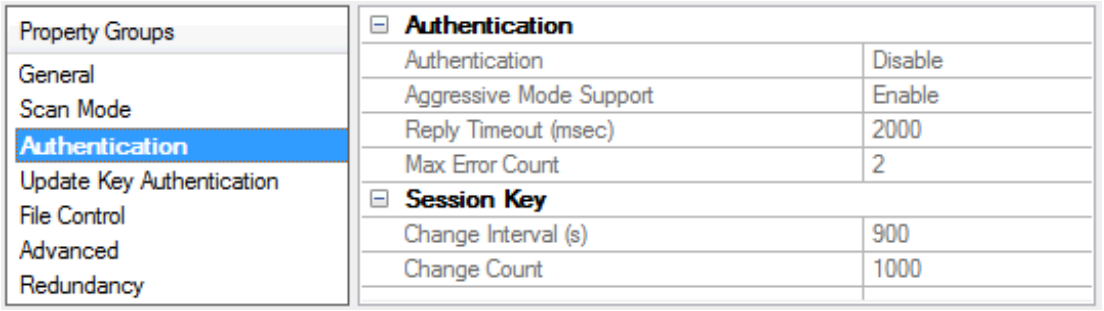
Data Set Tag Subtypes

- **Value Tags** These properties specify the sub-type of the Data Set tags. They are only available when data sets are selected for import. The default is enabled.
- **Import Explicit Tags:** These properties specify the sub-type of the Data Set tags. They are only available when data sets are selected for import. The default is disabled.

For more information on sub-types, refer to Address Descriptions.

Device Properties — Authentication

The Authentication group is used to configure the device's authentication settings.



Authentication

Authentication: When enabled, this property enables authentication. If the device requires authentication, the DNP client needs to configure it as well. The default setting is disabled.

Note: A tag import is performed when this property changes. This ensures that the authentication object internal statistics tags are automatically generated when authentication is enabled. These tags are pre-defined and may be imported without communication with the device. When authentication is disabled, a tag import is performed to remove the authentication object internal Statistics tags. When a tag import is in progress, the properties on this page is disabled. *For more information, refer to* ***Tag Import***.

Aggressive Mode Support: Enable, to reduce traffic by not requiring a critical request "challenge and reply" after at least one "challenge and reply" was successful during the session key change interval. The default setting is enabled.

Reply Timeout (ms): This property specifies how long the device waits for an authentication reply. The valid range is 0 to 300000 milliseconds. The default setting is 2000 milliseconds.

Max. Error Count: This property specifies the number of error messages sent before error message transmission is disabled. It is also used to limit the number of authentication attempts when there is no reply from the DNP server. With proper timeout settings, the maximum number of authentication retries per response timeout are Max. Error Count + 2. The valid range is 0 to 10. The default setting is 2.

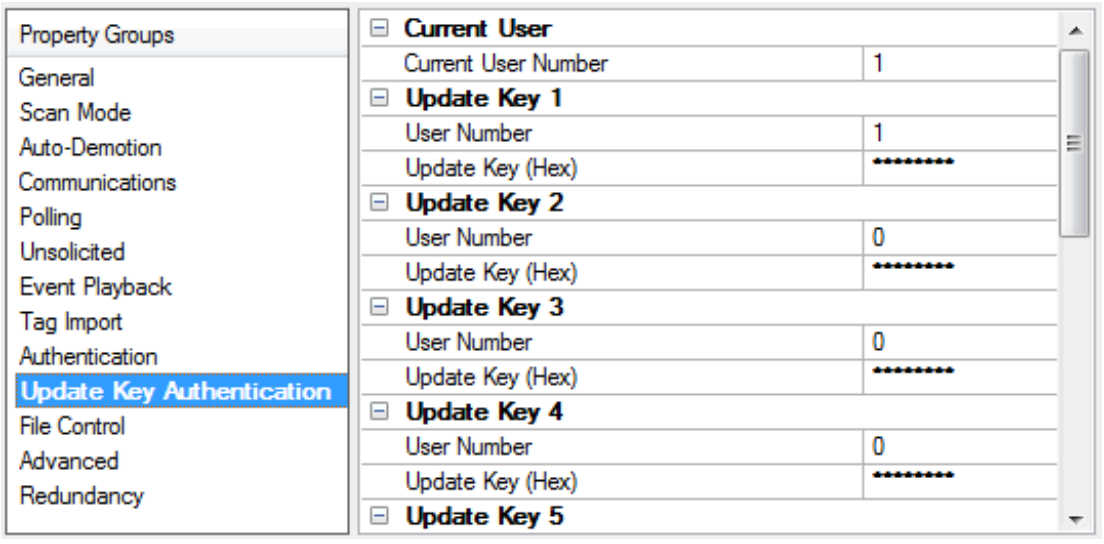
Session Key

Change Interval (s): This property specifies the session key change timeout to be used by the DNP client to determine when to change session keys. When a value of 0 is entered, Session Key Change Count is used instead. The valid range is 0 to 7200 seconds. The default setting is 900 seconds.

Change Count: This property specifies the number of transmitted authentication messages at which the DNP client changes session keys. The messages may have been transmitted in either direction. The valid range is 0 to 65535. The default setting is 1000.
Note: The DNP Client Ethernet Driver automatically matches the HMAC algorithm as configured in the DNP server.

Device Properties — Update Key Authentication

The Update Key Authentication group is used to configure the device's authentication settings.



Current User

Current User Number: Specify how many users can retrieve the Update Key during authentication. The default setting is 1.

Update Key *n*

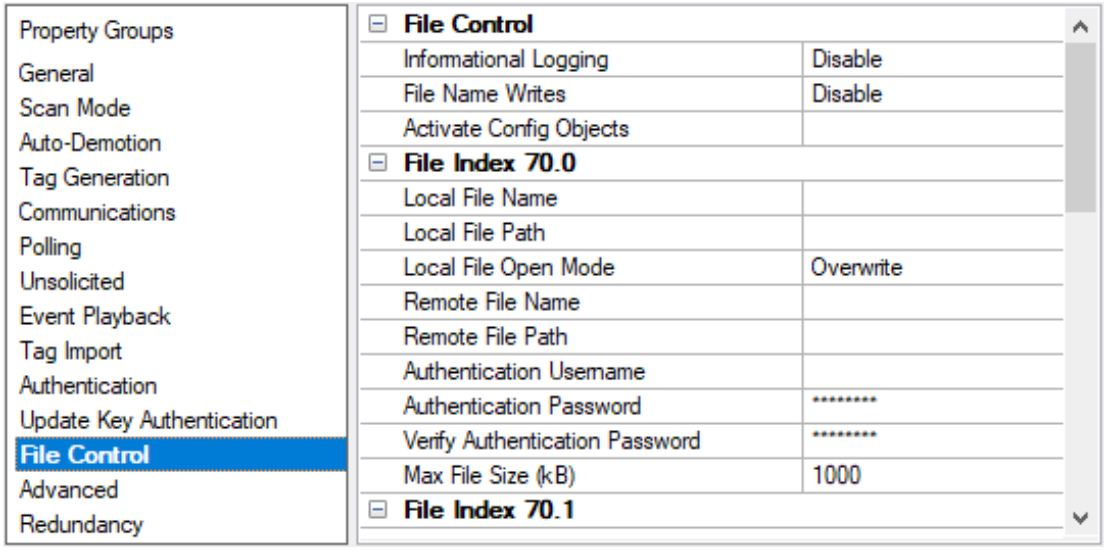
This section displays an array of 10 users, each with a unique 16 hexadecimal byte Update Key. The same User Number-Update Key combination must be configured in the device.

User Number: This property modifies the current User Number. The valid range for User Number is 0 to 65535. The default setting for the first row of User Numbers is 1. All others are 0.

Update Key: Modify the existing Update Key in this field. Update Keys can be entered either as 32 characters (such as "493B56AF89120C0429767DB301C63CA8") or as 16 sets of 2 characters that are separated by spaces (such as "49 3B 56 AF 89 12 0C 04 29 76 7D B3 01 C6 3C A8").
Tip: Copy and paste functionality works properly for these fields using the Windows clipboard .

Device Properties — File Control

The File Control feature set is intended to be used as a mechanism for transferring log and configuration files between DNP clients and servers. The DNP Client Ethernet Driver supports the transfer of files to and from a DNP client. In the File Control group of device properties, change settings by clicking in the right column to access a drop-down menu of the available options.



File Control

Informational Logging: When enabled, this parameter logs informational messages to the Event Log during file transfers. When disabled, informational logging is turned off. In both cases, error messages are always logged to the Event Log. The default setting is disabled.

File Name Writes: When enabled, the file name tags are created with read / write access. When disabled, the file name tags are created with read-only access. The default setting is disabled.
Note: When the applied setting changes from disabled to enabled, a message is invoked warning the user that writes to the file name tags changes the device properties.

Activate Config Objects: Specify a comma-delimited string that contains a list of the objects to be used in the Activate Configuration Request. All 70.index objects listed in the string must have the remote file name

and path defined in the File Index section for that index. All 110.index objects listed must have a tag defined for that data point. For example, the format of this list would be 70.0, 70.1, 110.5. The maximum number of characters allowed for this string is 256.

File Index 70.*n*

The following local and remote path and file settings, file authentication, and maximum size are for the DNP client local file index *n*.

Local File Name: Specify the name of the file located on the DNP client. It can include the entire path, part of the path, or only the file name. If a local path is defined, the local file identifier is defined by either *<local path>\<local file name>* or *<local path>/<local file name>*. The file name property is exposed to the client in a tag. If the **File Name Writes** property is enabled, the client can change the file name as needed by writing to the tag. The maximum number of characters for the file identifier is 256.

Local File Path: Specify the local path of the file. When users double-click in the right column of this property, a file path browser is invoked. If the **Local File Name** property contains the entire file identifier, the path property should remain empty. For security, the path property is not exposed to the client in a tag. A non-empty path precedes a backslash (or forward slash) and the local file name to identify the local file. The maximum number of characters for the file identifier is 256.
Note: The Local File Path and Name must form a valid UNC path (which cannot contain the characters | ?'* :<>). For security purposes, the parent directory (denoted by '..') is not permitted. Furthermore, the current user must have Read/Write privileges to the Local File Identifier.

Local File Open Mode: When **Overwrite** is selected, the local file is overwritten during file transfers. When **Append** is selected, the incoming file data is appended to an existing file. The default setting is Overwrite.

Remote File Name: This is the definition of the DNP server remote file. The Remote File Identifier is restricted in length to 256 characters. Because the server cannot verify that the file name and path are valid, users must make sure to specify the path correctly to avoid unintended file transfers. For example, users that set the Remote File Identifier to a folder / directory on the DNP server may find that the transfer completes successfully, but that the file cannot be used by the DNP client. **Remote File Name:** Specify the name of the file located on the DNP server. This entry can include the entire path, part of the path, or only the file name. If a remote path is defined, then the remote file identifier is defined by either *<remote path>\<remote file name>* or *<remote path>/<remote file name>*. The file name property is exposed to the client in a tag. If the **File Name Writes** property is enabled, then the client can change the file name as needed by writing to the tag. The maximum number of characters for the file identifier is 256.

Remote File Path: Specify the path of the file located on the DNP server. If the **Remote File Name** property contains the entire file identifier, the path property should remain empty. For security, the path property is not exposed to the client in a tag. A non-empty path precedes a backslash (or forward slash) and the remote file name to identify the remote file. The maximum number of characters for the file identifier is 256.

Authentication Username: Specify the username required by the device to authenticate the file. The maximum number of characters is 32.

Authentication Password: Specify the password required by the device to authenticate the file. The encrypted password is case-sensitive and is not displayed. The maximum number of characters is 32.

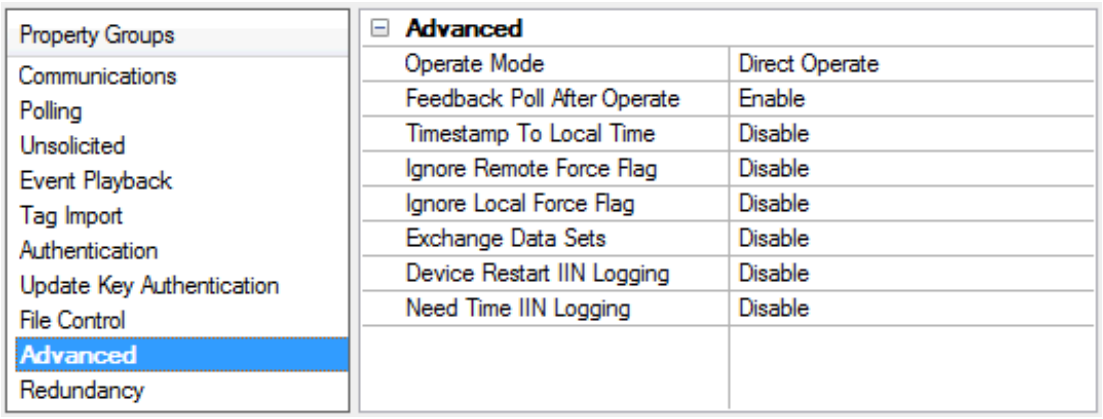
Verify Authentication Password: This property verifies the password entered in the parameter above. The encrypted verification password is case-sensitive and is not displayed. The maximum number of characters is 32.

Max File Size (kB): Specify the maximum file size in kilobytes that are allowed in file transfers. The valid range is 100 to 65535 kilobytes. The default setting is 1000 kilobytes.

Tip: When property changes are made and applied, a tag import is performed. At that time, a tag group titled "File Control" is created automatically. Four tags for each of the 0-9 file indexes that have non-empty file names or path names are also created. The format of the tags is *70.<index>.Upload, 70.<index>.Download, 70.<index>.LocalFileName*, and *70.<index>.RemoteFileName*. These tags are pre-defined, and may be imported without communication with the device. When a tag import is in progress, the properties on this page are disabled. *For more information, refer to* ***Tag Import***.

Device Properties — Advanced

The Advanced group is used to specify the operate mode, whether to perform a feedback poll after a write, how to display the DNP .Timestamp, whether to exchange data sets on restart, and whether to log informational messages to the Event Log when device Restart or Need Time IIN bits are set.



Operate Mode: This property determines whether the writable I/O points (object group 10 - Binary Outputs and object group 40 - Analog Outputs) use the Direct Operate or Select then Operate sequence. The default selection is Direct Operate.

Note: Individual tags' write behavior can override this setting by writing a Boolean True to the output's corresponding .DO or .SO sub-type tags. *For more information, refer to* ***DNP DO and SO sub-types***.

Feedback Poll After Operate: When enabled, this property enables a feedback poll to occur after an operate. The default setting is enabled.

Timestamp to Local Time: When enabled, this property converts the UTC timestamp to local time. It is displayed in .Timestamp tags. The default setting is disabled.

Ignore Remote Force Flag: If the DNP Remote Force flag is set and this property is disabled, the quality of the corresponding .Value and .Explicit tags is bad. If the DNP Remote Force flag is set at the DNP server end and this property is enabled, the quality of the corresponding .Value and .Explicit tags remain good. The default setting is disabled.

Ignore Local Force Flag: If the DNP Local Force flag is set and this property is disabled, the quality of the corresponding .Value and .Explicit tags are bad. If the DNP Local Force flag is set at the DNP server end and this parameter is enabled, the quality of the corresponding .Value and .Explicit tags remain good. The default setting is disabled.

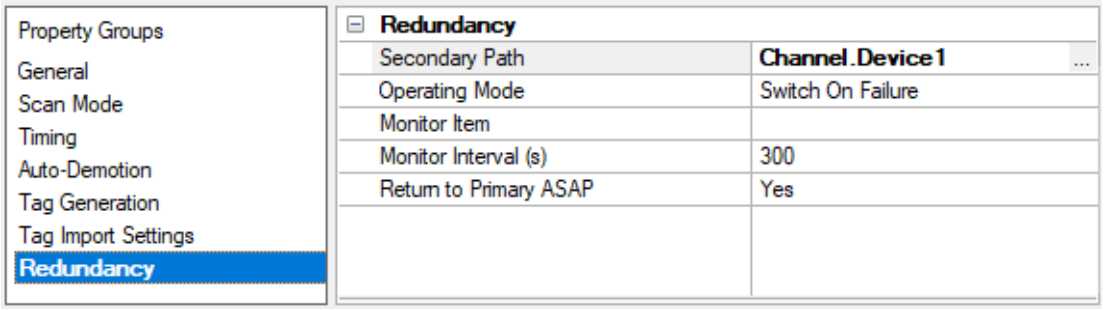
Exchange Data Sets: When enabled, this property ensures that the data set prototypes and descriptors are exchanged with the DNP server whenever the DNP client or server restarts. When disabled, the initial exchange of data sets does not take place. If a Data Set tag needs to be updated, the data set prototype and descriptors must be exchanged before requesting the update. If the DNP client restarts and does not exchange data sets, any data set events that occurred before the DNP client restarted are lost: the DNP client has no information about the data sets. The default setting is disabled.

Device Restart IIN Logging: When enabled, this property logs informational messages to the Event Log when a response from the DNP server has the device restart IIN 1.7 bit set. When disabled, informational logging is turned off. The default setting is disabled.

Need Time IIN Logging: When enabled, this property logs informational messages to the Event Log when a response from the DNP server has the Need Time IIN 1.4 bit set. When disabled, informational logging is turned off. The default setting is disabled.

For more information on DNP flag bytes, refer to "DNP Object Flag Definitions" located in object group 1, 3, 10, 20, 21, 30, and 40.

Device Properties — Redundancy



Redundancy is available with the Media-Level Redundancy Plug-In.

Consult the website, a sales representative, or the user manual for more information.

Data Types Description

Data Type	Description
Boolean	Single bit
Word	Unsigned 16-bit value bit 0 is the low bit bit 15 is the high bit
Short	Signed 16-bit value bit 0 is the low bit bit 14 is the high bit bit 15 is the sign bit
DWord	Unsigned 32-bit value bit 0 is the low bit bit 31 is the high bit
Long	Signed 32-bit value bit 0 is the low bit bit 30 is the high bit bit 31 is the sign bit
Float	32-bit floating-point value
Double	64-bit floating-point value
String	Null-terminated ASCII string

Address Descriptions

Tag Addressing

Tag addressing is of the form *OBJ.VAR.IDX.SUB (ObjectGroup.Variation.Index.Sub-Type)*, where:

- **OBJ:** The data object group.
- **VAR:** The variation requested for the tag equates to data type. Strings do not have a variation component.

  Note: The variation is only applicable to .Value and .Explicit sub-types. For .Value tags, no request is sent to the DNP server. All variations defined for .Value tags in the DNP client display the value in the DNP server's default event variation. For .Explicit tags, the variation is used in the request to the DNP server. If the request is for variation 0, the DNP server returns the value in its default static variation. All other variations for .Explicit tags are specifically requested from the DNP server.
- **IDX:** The specific data object in a given group. For example, IDX 4 is the 5th binary input. Indexes start with 0 for each object group with multiple points. Some objects, such as Objects 50 and 60, do not have an index component.
- **SUB:** The specific attribute of the point.

See Also: *Other Object Groups*

Sub-Types

Certain object group variations in the DNP3 protocol return multiple data items. For example, object group 20.1 asks for an analog input point's 32-bit value as well as a Flag byte. Many event object group variations also return the time of occurrence: because the OPC interface does not handle complex data types, the value, flags, and timestamp data are not available in a single tag. The OPC server must retrieve the various parts of the combined report in separate tags.

- For the .SUB value attribute, the data type is designated by the variation (.VAR). If the variation is .0, the .SUB value attribute has the same data type as the default variation.
- For the .SUB flags attributes contained within the flags attribute, the data type is always Boolean. They are unaffected by the variation.
- For the .SUB flags attribute, the data type is always byte. It is unaffected by the variation.
- The .SUB timestamp attribute is always Date. It is unaffected by the variation.

Sub-Type	Description
Value	The current value of the point. The data type returned from the DNP server depends on the default event variation and the default static variation configured in the DNP server for the point. The data type exposed to the client depends on the variation part of the tag address.
Explicit	The current value of the point. The data type varies as determined by the selected variation. Reading a tag with the Explicit sub-type causes the driver to initiate a DNP Read transaction. DNP is usually used in a report-by-exception model, where the DNP server device responds to an Event Poll with the point data that has changed since the last report. Some DNP server devices may have I/O points that are not configured to answer to Event or Integrity polls. These points require special handling via the .Explicit sub-type. The .Explicit sub-type triggers a DNP read transaction for every tag update, which may cause traffic on the DNP bus. Tags using the .Explicit sub-type must use a suitable update rate. Rates of 1000 ms or longer are recommended, as is limiting the use of .Explicit tags to only

Sub-Type	Description
	where required. It is the user's responsibility to configure .Explicit tags appropriately. **Note**: To reduce traffic, Explicit reads of the same object group and variation are blocked together to be read 64 at a time. If any tag in the block fails, the whole block fails.
Timestamp	The date and time of the last update received from the DNP server (if an event has occurred and the time of occurrence was returned). A successful write to a .Value or .Explicit tag causes its corresponding .Timestamp tag quality to be bad. The timestamp of the .Timestamp tag is then the timestamp of the update from the write. The next time a DNP timestamp is received, the quality of the .Timestamp tag changes to good and its timestamp displays the DNP timestamp. **Note**: The timestamp of the .Value item is only updated if its value has changed since the last update. To find the current DNP timestamp value for the point, use the DNP .Timestamp tag.
Online	Boolean: True if the DNP server is online.
Restart	Boolean: True if the DNP server has been restarted.
Lost	Boolean: True if communications with this point were lost.
RemoteForce	Boolean: True if the point value is forced to its current state at a device other than the end device.
LocalForce	Boolean: True if the point value is forced to its current state at the end device. **Note**: Local force is not yet implemented.
Chatter	Boolean: True if the DNP server's chatter filter is activated and applying correction.
Reference Check	Boolean: True if the reference signal used to digitize the analog input is not stable and the resulting digitized value may not be correct.
Over-range	Boolean: True if the digitized signal or calculation has exceeded its range. The actual value field can be ignored as its value is not defined.
DO*	Boolean: True if a writable point is set to Direct Operate mode. Writing to a tag of this sub-type overrides the global Operate Mode setting. *For more information, refer to* ***Operate Mode****.*
SO*	Boolean: True if a writable point is set to Select then Operate mode. Writing to a tag of this sub-type overrides the global Operate Mode setting. *For more information, refer to* ***Operate Mode***.
Flags	The full set of transaction flags (0 through 7) for the specified DNP point.
Operate	This limited functionality is only retained to support older projects. New projects should use the enhanced Operate commands shown below.* * The user specifies a crafted value to write. The .Operate sub-type is implemented as a DWord, but currently only the lowest 8 bits are significant. Bits 0-3 form a command number. Allowable values are currently 0-4. Values outside

Sub-Type	Description
	this range result in a failed write. The commands are as follows: 0 - No operation 1 - Pulse on 2 - Pulse off 3 - Latch on (same as writing a 1 to 10.x.x.Value) 4 - Latch off (same as writing a 0 to 10.x.x.Value. Bit 4 is the Queue command modifier. Bit 5 is the Clear command modifier. Bits 6 & 7 form a Trip-Close command pair. Allowable values are currently 0-2. Values outside this range result in a failed write. Bit 6 is the Paired Close command modifier. Bit 7 is the Paired Trip command modifier. The allowable commands are as follows: 0 - Nul 1 - Close 2 - Trip
OperateWithParams	This subtype can be used to send a command to a Control Relay Output Block (CROB) and set each of the CROB values in a single write. The variation of the tag does not matter. Writing to this tag causes an Object Group 12 control operation on a binary output. The CROB control code is built from the string value written to the tag. It is a comma-separated list where the values are in the following order: OnTime, OffTime, OpType, TripCloseCode, Clear, FeedbackDelay. Values left out default to 0.
Enhanced Operate Controls	These expanded Operate sub-types allow a user to completely control commands sent to a Control Relay Output Block.**
Operate.OpType	This Byte contains the specific operation type to perform. The commands are as follows: 0 - No operation 1 - Pulse on 2 - Pulse off 3 - Latch on (same as writing a 1 to 10.x.x.Value) 4 - Latch off (same as writing a 0 to 10.x.x.Value)
Operate.TripCloseCode	This Byte contains the Trip-Close code to apply to the operation. The commands are as follows: 0 - No operation 1 - Close 2 - Trip
Operate.Clear	This Boolean adds the 'Clear' attribute to the command.
Operate.OnTime	This DWord specifies the on-time in milliseconds for the command.

Sub-Type	Description
Operate.OffTime	This DWord specifies the off-time in milliseconds for the command.
Operate.FeedbackDelay	This DWord specifies the time in milliseconds before a feedback poll is performed after the command completes.
Operate.Set	After all of the parameters above have been written, writing True to this Boolean initiates the command.

* Direct Operate (DO) and Select-then-Operate (SO) sub-types apply only to object groups 10 and 40. DO and SO are not allowed for other object groups.
** ***See Also:*** *Object 10 - Binary Outputs*.

Object Group 0 - Device Attributes

These tags are only read explicitly once after start. If the device does not support object group 0 (or the specific variation), the tag quality is bad; as such, explicit reads of this tag do not resume until the DNP client or server restarts.

Attributes

The default data type is shown in **bold**.

OBJ.VAR.IDX Attributes*	.SUB Attribute	Data Type	Access
0.{1-253}.{0-65535}	Value	Byte, Char, Double, **DWord**, Float, Long, Short, String**, Word	Read/Write

* The IDX attribute indicates the particular set of device attributes that are defined in the device. The set of standardized device attributes defined by DNP3 are accessible at set index 0; indexes 1 and above are available for vendor-specific attributes.

** Device attribute strings have a maximum length of 210 characters.

Note: Flags do not apply.

Variations

Variations for object group 0 do not equate to a specific data type. A variation is a specific element for a set of device attributes. If the tag is configured by the user, the variation's data type must match the data type that is configured in the DNP server.

Although the DNP protocol allows requests for object group 0, variations 254 and 255, the DNP Client Ethernet Driver does not allow tags to be created with those variations. The responses to each of those requests may be too large for a tag value.

Number	Description
254	This attribute is used as shorthand to request that a device return all of its attributes in a single response.
255	This special attribute is used to retrieve a list of all the device attribute variation numbers (in addition to their properties) that are supported by the device at a specified index.

Note: Tags with other device attribute variations can both be manually created and automatically generated through the Tag Import settings in device Properties. During tag import, the driver issues requests for group 0 Variation 254 and group 0 Variation 255 to gather information from the device and to create only those device attribute tags as defined in the responses. For more information, refer to **Tag Import**.

Examples

Tag Address	Definition	Description
0.211.0.Value	Displays the standard DNP device Attribute Number of Analog Outputs.	If a value for this tag has not been received from the device, an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. If the response to the initial request indicates that the device does not support the variation 211 of set 0, then no other request is issued and tag quality is bad. The user must configure the tag's data type to match the data type as configured by the DNP server.
0.250.0.Value	Displays the standard DNP device Attribute Manufacturer's product name and model.	If a value for this tag has not been received from the device, an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. If the response to the initial request indicates that the device does not support variation 250 of set 0, no other request is issued and the tag quality is bad. The user must configure the tag's data type to match the data type as configured by the DNP server.
0.211.1.Value	Displays the custom device attribute set 1 variation 211 value.	If a value for this tag has not been received from the device, an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. If the response to the initial request indicates that the device does not support variation 211 of set 1, then no other request is issued and the tag quality is bad. The user must configure the tag's data type to match the data type as configured by the DNP server.

Object Group 1- Binary Inputs

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 1 - Binary Input State is reflected in object group 2 - Binary Input Change Event. *For more information, refer to **Other Object Groups**.*

Attributes

The default data type is shown in **bold**.

OBJ.VAR.IDX Attributes	.SUB Attribute	Data Type	Access
1.{0,1,2}.{0-65535}	Chatter, LocalForce, Lost, Online, RemoteForce, Restart	Boolean	Read Only
1.{0,1,2}.{0-65535}	Flags	Byte	Read Only
1.{0,1,2).{0-65535}	TimeStamp	Date	Read Only
1.0.{0-65535}	Value, Explicit	Boolean	Read Only
1.1.{0-65535}	Value, Explicit	**Boolean**	Read Only
1.2.{0-65535}	Value, Explicit	Byte	Read Only

Variations

Number	Description
0	Variation determined by DNP server device
1	Packed format
2	With Flags

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online and State. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force
- 4: Local Force
- 5: Chatter
- 6: Reserved
- 7: State - Status of input

Examples

Tag Address	Definition	Description
1.0.0.Value*	Value of point 0 as a Boolean	This tag is updated from the data store that is populated via responses to integrity and event polls. An explicit request is not sent to the device. Although the DNP server could return variation 1 or 2 (depending on its object group 2 default event variation), this tag displays the state of the binary input point 0 without the flags.
1.0.5.Explicit	Value of point 5 as a Boolean	An explicit request is sent to the device to get the value for this tag. Other object 1 variation 0 Explicit tags are blocked with this tag in one request. Although the DNP server could return variation 1 or 2 (depending on its default static variation), this tag displays the

Tag Address	Definition	Description
		state of the binary input point 5 without the flags.
1.1.10.Explicit	Value of point 10 as a Boolean	An explicit request is sent to the device to get the value for this tag. Other object 1 variation 1 explicit tags are blocked with this tag in one request. Although the DNP server may have returned the response with other points in a packed format, this tag only displays the 0 or 1, depending on the state of point 10.
1.1.10.Value*	Value of point 10 as a Boolean	This tag is updated from the data store that is populated via responses to integrity and event polls. An explicit request is not sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server. The DNP server uses object 2 default event variation.
1.2.10.Explicit	Value of point 10 as a byte	An explicit request is sent to the device to get the value for this tag. Other object 1 variation 2 explicit tags are blocked with this tag in one request. This tag displays the status of the point as a byte where bits 0-6 are the flags and bit 7 is the state of the digital input point 10.
1.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned)	This tag is updated from the data store that is populated via responses to integrity and event polls. An explicit request is not sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the device sends an event with the time. The object group 2 default event variation on the device needs to be 2 or 3 for it to return the event time of occurrence.
1.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary input point 9. An explicit request is not sent to the device. The value of this tag displays the latest flags byte received for point 9 (regardless of the variation in the tag address).
1.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary input point 3. An explicit request is not sent to the device. The value of this tag displays the state of bit 2 from the flag byte received for point 3 (regardless of the variation in the tag address).

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to* ***Communications***.

Object Group 3 - Double Bit Inputs

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 3 - double-bit input state is reflected in object group 4 - Double Bit Input Change Event. For more information, refer to **Other Object Groups**.

Attributes

The default data type is shown in **bold**.

OBJ.VAR.IDX Attributes	.SUB Attribute	Data Type	Access
3.{0,1,2}.{0-65535}	Chatter, LocalForce, Lost, Online, RemoteForce, Restart	Boolean	Read Only
3.{0,1,2}.{0-65535}	Flags	Byte	Read Only
3.{0,1,2}.{0-65535}	TimeStamp	Date	Read Only
3.0.{0-65535}	Value, Explicit	Byte	Read Only
3.1.{0-65535}	Value, Explicit	**Byte**	Read Only
3.2.{0-65535}	Value, Explicit	Byte*	Read Only

* The extra bits are used to provide Flags.

Variations

Number	Description	Bits
0	Variation determined by DNP server device	N/A
1	Packed format	Bits 0 and 1: 0 is Intermediate, 1 is OFF, 2 is ON, 3 is Indeterminate.
2	With flags	Bits 6 and 7: 0 is Intermediate, 1 is OFF, 2 is ON, 3 is Indeterminate.

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online and State. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force
- 4: Local Force
- 5: Chatter
- 6: State - Status of input
- 7: State - Status of input

Examples

Tag Address	Definition	Description
3.0.0.Value*	Value of point 0	This tag is updated from the data store that is populated via

Tag Address	Definition	Description
	as a byte	responses to integrity and event polls. No explicit request is sent to the device. Although the DNP server could return variation 1 or 2 (depending on its object group 4 default event variation), this tag displays the state of the double-bit binary input point 0 without the flags.
3.0.5.Explicit	Value of point 5 as a byte	An explicit request is sent to the device to get the value for this tag. Other object 3 variation 0 Explicit tags are blocked with this tag in one request. Although the DNP server could return variation 1 or 2 (depending on its default static variation), this tag displays the state of the double-bit binary input point 5 without the flags.
3.1.10.Explicit	Value of point 10 as a byte	An explicit request is sent to the device to get the value for this tag. Other object 3 variation 1 Explicit tags are blocked with this tag in one request. Although the DNP server returned the response in a packed format, possibly with other points, this tag only shows 0 (intermediate), 1 (Off), 2 (On), or 3 (indeterminate); depending on the state of point 10.
3.1.10.Value*	Value of point 10 as a byte	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server (which uses its object 4 default event variation).
3.2.10.Explicit	Value of point 10 as a byte	An explicit request is sent to the device to get the value for this tag. Other object 3 variation 2 Explicit tags are blocked with this tag in one request. This tag displays the status of the point as a byte where bits 0-5 are the flags and bits 6 & 7 are the state of the digital input point 10.
3.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned).	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the device sends an event with the time. The object group 4 default event variation on the device needs to be 2 or 3 for it to return the event time of occurrence.
3.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary input point 9. No explicit request is sent to the device. The value of this tag displays the latest flag byte received for point 9 regardless of the variation in the tag address.
3.0.3.Lost*	Latest state of the bit 2 of the Flag Byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary input point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2 from the flag byte received for point 3 regardless of the variation in the tag address.

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to Communications.*

Object Group 10 - Binary Outputs

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 10 - Binary Output State is reflected in object group 11 - Binary Output Change Event, object group 12 - Control Relay Output Block, and object group 13 - Binary Output Command Event. For more information, refer to **Other Object Groups**.

See Also: **Object Group 12 - Binary Output Commands**

Attributes

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
10.{0,1,2}.{0-65535}	LocalForce, Lost, Online, RemoteForce, Restart	Boolean	Read Only
10.{0,1,2}.{0-65535}	DO, SO	Boolean	Read/Write
10.{0,1,2}.{0-65535}	Operate.Set, Operate.Clear	Boolean	Read/Write
10.{0,1,2}.{0-65535}	OperateWithParams*	String	Write Only
10.{0,1,2}.{0-65535}	Operate.OpType, Operate.TripCloseCode	Byte	Read/Write
10.{0,1,2}.{0-65535}	Operate.OnTime, Operate.OffTime, Operate.FeedbackDelay	DWord	Read/Write
10.{0,1,2}.{0-65535}	Flags	Byte	Read Only
10.{0,1,2}.{0-65535}	TimeStamp	Date	Read Only
10.0.{0-65535}	Value, Explicit	Boolean	Read/Write
10.1.{0-65535}	Value, Explicit	**Boolean**	Read/Write
10.2.{0-65535}	Value, Explicit	Byte*	Read Only

* The extra bits are used to provide Flags.

Variations

Number	Description
0	Variation determined by DNP server device
1	Packed format
2	Status with Flags

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online and State. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost

- 3: Remote Force
- 4: Local Force
- 5: Reserved
- 6: Reserved
- 7: State - Status of input.

Binary Output Examples

Tag Address	Definition	Description
10.0.0.Value*	Value of point 0 as a Boolean	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit requests are sent to the device. Although the DNP server could return variation 1 or 2 (depending on its object group 11 default event variation), this tag displays the state of the binary output point 0 without the flags.
10.0.5.Explicit	Value of point 5 as a Boolean	An explicit request is sent to the device to get the value for this tag. Other object 10 variation 0 Explicit tags are blocked with this tag in one request. Although the DNP server could return variation 1 or 2 (depending on its default static variation), this tag displays the state of the binary output point 5 without the flags.
10.1.10.Explicit	Value of point 10 as a Boolean	An explicit request is sent to the device to get the value for this tag. Other object 10 variation 1 Explicit tags are blocked with this tag in one request. Although the DNP server may return the response with other points in a packed format, this tag only shows the 0 or 1 (depending on the state of point 10).
10.1.10.Value*	Value of point 10 as a Boolean	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The variation of 1 in the tag address sets the data type of the tag. It does not define the data type returned by the DNP server, which uses its object group 11 default event variation.
10.2.10.Explicit	Value of point 10 as a byte	An explicit request is sent to the device to get the value for this tag. Other object 10 variation 2 Explicit tags are blocked with this tag in one request. This tag displays the status of the point as a byte, where bits 0-6 are the flags and bit 7 is the state of the digital output point 10.
10.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned)	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the device sends an event with the time. The object group 11 default event variation on the device needs to be 2 for it to return the event time of occurrence.
10.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary output point 9. No explicit request is sent to the device. The value of this tag displays the latest flags' byte received for point 9 (regardless of the variation in the tag address).

Tag Address	Definition	Description
10.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for binary output point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2 from the flag byte received for point 3 (regardless of the variation in the tag address).
10.0.2.DO*	Boolean value indicating if operations on binary output point 2 should be Direct Operate or Select then Operate	Writing to this tag does not cause an explicit write to the device. It also does not change the overall device property for Operate Mode: it only changes it for Binary Output point 2. The variation of the tag does not matter. The value of this tag is used when an operation is performed on binary output point 2 either using the Operate sub-type commands or a synchronous / asynchronous write to a 10.x.2.Value or 10.x.2.Explicit tag.
10.0.2.SO*	Boolean value indicating if operations on binary output point 2 should be Direct Operate or Select then Operate	Writing to this tag does not cause an explicit write to the device. It also does not change the overall device property for Operate Mode: it only changes it for Binary Output point 2. The variation of the tag does not matter. The value of this tag is used when an operation is performed on binary output point 2 either using the Operate sub-type commands or a synchronous / asynchronous write to a 10.x.2.Value or 10.x.2.Explicit tag.

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to Communications*.

Object Group 12 - Binary Output Commands

Control Relay Output Block Operate Command Examples

To perform digital control operations (such as electro-mechanical relays) at binary output points using object group 12, variation 1, use tags addressed with object group 10. An operation on an object group 10 tag issues the CROB command using object group 12, variation 1. Depending on the Feedback Poll after Operate device property, another request may be sent after the actual operate request to obtain the latest value of all binary output points. If the operate is successful but the feedback poll fails, the device reports status code 4.

See Also: **Unable to write to address <address> on device <device>. Control-Related Status Code <status code>.**

The following example discusses how to issue a Select then Operate request for Binary Output point 10 that closes the point one time for 250 milliseconds.

1. To start, click **Device Properties** | **Advanced**. Then, set the **Operate Mode** to **Select Then Operate**.

   Note: If the device's Operate Mode is Direct Operate, create a tag with the address "10.0.10.SO". Then, write "1" to that tag.

2. Next, create a tag with the address "10.0.10.Operate.Optype". Then, write "1" to that tag. This sets the **Operation Type Field** of the **Control Code** to **Pulse On**.
3. Next, create a tag with the address "10.0.10.Operate.Tripclosecode". Then, write "1" to that tag. This sets the **Trip-Close Code Field** of the **Control Code** to **Close**.
4. Next, create a tag with the address "10.0.10.Operate.Ontime". Then, write "250" to that tag. This sets the duration (in milliseconds) in which the output drive remains active.
5. Next, create a tag with the address "10.0.10.Operate.Set". Then, write "1" to that tag. This triggers the DNP client to send the object group 12, variation 1 request that performs the digital control operation.

Tip: The above example can also be accomplished by creating and writing to a single tag. To do so, follow step 1 above, then:
Create a tag with the address "10.0.10.OperateWithParams" and write "250,0,1,1,0,0" to that tag. This triggers the DNP client to send the Object Group 12, variation 1 request with a CROB that has the values desired. The string that is written is a comma-separated list where the values are: OnTime, OffTime, OpType, TripCloseCode, Clear, FeedbackDelay.

See Also: *Object Group 10 - Binary Outputs*

Note: The Channel Diagnostics should display the three transactions. The DNP client sends a request using function code 0x03 to select the output point. The DNP server responds by echoing the request if everything is okay. The DNP client then sends the operate request using function code 0x04. The DNP server responds by echoing the request if everything is okay. The DNP client then sends the feedback poll and the DNP server responds with the current static value for all binary outputs.

Tag Address	Definition	Description
10.0.2.Operate.Clear	Value of the CROB control code bit 5	This Boolean tag displays a 0 or 1, depending on the last update from the client. The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used in building the CROB control code to be written to the object group 12 point 2 with the Operate.Set tag.
10.0.2.Operate.OpType	Value of the CROB control code bits 0-3.	This byte tag displays the operation type, depending on the last update from the client. Operation types are as follows: Nul (0) Pulse_On (1) Pulse_Off (2) Latch_On (3) Latch_Off (4) The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used in building the CROB control code that is written to the object group 12 point 2 with the Operate.Set tag.
10.0.2.Operate.TripCloseCode	Value of the CROB control code	This byte tag displays the Trip-Close field, depending on the last update from the client. Trip-close fields are as follows:

Tag Address	Definition	Description
	bits 6 & 7	Nul (0) Paired_Close (1) Paired_Trip (2) The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used in building the CROB control code to be written to the object group 12 point 2 with the Operate.Set tag.
10.0.2.Operate.OnTime	Value in milliseconds that the operation on the binary output point 2 remains active	This DWord tag displays the on time last updated from the client. The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used in an object group 12 control operation on binary output point 2 when the Operate.Set tag is toggled to 1.
10.0.2.Operate.OffTime	Value in milliseconds that the operation on the binary output point 2 remains non-active	This DWord tag displays the off time last updated from the client. The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used in an object group 12 control operation on binary output point 2 when the Operate.Set tag is toggled to 1.
10.0.2.Operate.FeedbackDelay	Value in milliseconds to delay after receiving the response before issuing feedback poll	This DWord tag displays the feedback delay last updated from the client. The variation of the tag does not matter. Writing to this tag does not cause an explicit write to the device. It is used to delay before issuing a feedback poll after receiving a response to an object group 12 control operation on binary output point 2.
10.0.2.Operate.Set	Always displays a Boolean value of 0 with good quality	The variation of the tag does not matter. Writing a 1 to this tag causes an object group 12 control operation on binary output point 2. The CROB control code is built from the values of the Operate.Clear, Operate.OpType, and Operate.TripCloseCode tags. The values of the Operate.OnTime, Operate.OffTime, and Operate.FeedbackDelay tags are used in the operation as well.
10.0.2.OperateWithParams	Always displays an empty string or the last written value with good quality	The variation of the tag does not matter. Writing to this tag causes an object group 12 control operation on binary output point 2. The CROB control code is built from the string value written to the tag. It is a comma-separated list where the values are in the following order: OnTime, OffTime, OpType, TripCloseCode, Clear, FeedbackDelay. Values left out default to 0.

Object Group 20 - Counters

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 20 - Counter value is reflected in object group 22 - Counter Event Change. *For more information, refer to* ***Other Object Groups****.*

Attributes

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
20.{0,1,2,5,6}.{0-65535}	LocalForce, Lost, Online, RemoteForce, Restart	Boolean	Read Only
20.{0,1,2,5,6}.{0-65535}	Flags	Byte	Read Only
20.{0,1,2,5,6}.{0-65535}	TimeStamp	Date	Read Only
20.0.{0-65535}	Value, Explicit	DWord	Read Only
20.1.{0-65535}	Value, Explicit	DWord	Read Only
20.2.{0-65535}	Value, Explicit	Word	Read Only
20.5.{0-65535}	Value, Explicit	**DWord**	Read Only
20.6.{0-65535}	Value, Explicit	Word	Read Only

Variations

Number	Description
0	Variation determined by DNP server device
1	32-bit with Flag
2	16-bit with Flag
5	32-bit without Flag
6	16-bit without Flag

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force

- 4: Local Force
- 5: Rollover
- 6: Discontinuity
- 7: Reserved

Examples

Tag Address	Definition	Description
20.0.0.Value*	Value of point 0 as a DWord	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The DNP server could return variation 1, 2, 5, or 6; depending on its object group 22 default event variation. These all fit in a DWord.
20.0.5.Explicit	Value of point 5 as a DWord	An explicit request is sent to the device to get the value for this tag. Other object 20 variation 0 explicit tags are blocked with this tag in one request. The DNP server could return variation 1, 2, 5, or 6; depending on its default static variation. These all fit in a DWord.
20.1.10.Explicit	Value of point 10 as a DWord	An explicit request is sent to the device to get the value for this tag. Other object 20 variation 1 Explicit tags are blocked with this tag in one request.
20.1.10.Value*	Value of point 10 as a DWord	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit requests are sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server. The DNP server uses its object group 22 default event variation.
20.2.10.Explicit	Value of point 10 as a Word	An explicit request is sent to the device to get the value for this tag. Other object 20 variation 2 Explicit tags are blocked with this tag in one request.
20.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned)	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. They have bad quality until the device sends an event with the time. The object group 22 default event variation on the device needs to be 5 or 6 for it to return the event time of occurrence.
20.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for counter point 9. No explicit request is sent to the device. The value of this tag displays the latest flags' byte received for point 9 (regardless of the variation in the tag address).
20.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for counter point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2

		from the flags byte received for point 3 (regardless of the variation in the tag address).

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP server local time in which the event occurred within the DNP server. *For more information, refer to* ***Communications***.

Object Group 21 - Frozen Counters

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 21 - Frozen Counter value is reflected in object group 23 - Frozen Counter Event Change. *For more information, refer to* ***Other Object Groups***.

Attributes

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
21.{0,1,2,5,6,9,10}.{0-65535}	LocalForce, Lost, Online, RemoteForce, Restart	Boolean	Read Only
21.{0,1,2,5,6,9,10}.{0-65535}	Flags	Byte	Read Only
21.{0,1,2,5,6,9,10}.{0-65535}	TimeStamp	Date	Read Only
21.0.{0-65535}	Value, Explicit	DWord	Read Only
21.1.{0-65535}	Value, Explicit	DWord	Read Only
21.2.{0-65535}	Value, Explicit	Word	Read Only
21.5.{0-65535}	Value, Explicit	DWord	Read Only
21.6.{0-65535}	Value, Explicit	Word	Read Only
21.9.{0-65535}	Value, Explicit	**DWord**	Read Only
21.10.{0-65535}	Value, Explicit	Word	Read Only

Variations

Number	Description
0	Variation determined by DNP server device
1	32-bit with Flag
2	16-bit with Flag

Number	Description
5	32-bit with Flag and Time
6	16-bit with Flag and Time
9	32-bit without Flag
10	16-bit without Flag

DNP Object Flag Definitions
If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force
- 4: Local Force
- 5: Rollover
- 6: Discontinuity
- 7: Reserved

Examples

Tag Address	Definition	Description
21.0.0.Value*	Value of point 0 as a DWord	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The DNP server could return variation 1, 2, 5, 6, 9, or 10; depending on its object group 23 default event variation. These all fit in a DWord.
21.0.5.Explicit	Value of point 5 as a DWord	An explicit request is sent to the device to get the value for this tag. Other object 21 variation 0 Explicit tags are blocked with this tag in one request. The DNP server could return variation 1, 2, 5, 6, 9, or 10; depending on its default static variation. These all fit in a DWord.
21.1.10.Explicit	Value of point 10 as a DWord	An explicit request is sent to the device to get the value for this tag. Other object 21 variation 1 Explicit tags are blocked with this tag in one request.
21.1.10.Value*	Value of point 10 as a DWord	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server. The DNP server uses its object group 23 default event variation.
21.2.10.Explicit	Value of point 10 as a Word	An explicit request is sent to the device to get the value for this tag. Other object 21 variation 2 Explicit tags are blocked with this tag in one request.
21.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the

Tag Address	Definition	Description
	occurred and the time of occurrence was returned)	device sends an event with the time. The object group 23 default event variation on the device needs to be 5 or 6 for it to return the event time of occurrence.
21.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for frozen counter point 9. No explicit request is sent to the device. The value of this tag displays the latest flags' byte received for point 9 (regardless of the variation in the tag address).
21.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for frozen counter point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2 from the flags byte received for point 3 (regardless of the variation in the tag address).

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to Communications.*

Object Group 30 - Analog Inputs

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: object group 30 - Analog Input value is reflected in object group 32 - Analog Input Change Event. For more information, refer to **Other Object Groups**.

Attributes

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
30.{0,1,2,3,4,5,6}.{0-65535}	LocalForce, Lost, Online, RemoteForce, Restart, OverRange, ReferenceCheck	Boolean	Read Only
30.{0,1,2,3,4,5,6}.{0-65535}	Flags	Byte	Read Only
30.{0,1,2,3,4,5,6}.{0-65535}	TimeStamp	Date	Read Only
30.0.{0-65535}	Value, Explicit	Double	Read Only
30.1.{0-65535}	Value, Explicit	Long	Read Only
30.2.{0-65535}	Value, Explicit	Short	Read Only
30.3.{0-65535}	Value, Explicit	Long	Read Only

OBJ.VAR.IDX Attributes	.SUB Attribute	Data Type	Access
30.4.{0-65535}	Value, Explicit	Short	Read Only
30.5.{0-65535}	Value, Explicit	Float	Read Only
30.6.{0-65535}	Value, Explicit	**Double**	Read Only

Variations

Number	Description
0	Variation determined by DNP server device
1	32-bit with Flag
2	16-bit with Flag
3	32-bit without Flag
4	16-bit without Flag
5	32-bit floating-point with Flag
6	64-bit floating-point with Flag

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force
- 4: Local Force
- 5: Overrange
- 6: Reference Check
- 7: Reserved

Examples

Tag Address	Definition	Description
30.0.0.Value*	Value of point 0 as a Double	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The DNP server could return variation 1, 2, 3, 4, 5, or 6; depending on its object group 32 default event variation. These fit in a Double.
30.0.5.Explicit	Value of point 5 as a Double	An explicit request is sent to the device to get the value for this tag. Other object 30 variation 0 Explicit tags are blocked with this tag in one request. The DNP server could return variation 1, 2, 3, 4, 5, or 6; depending on its default static variation. These fit in a Double.
30.1.10.Explicit	Value of point 10 as a Long	An explicit request is sent to the device to get the value for this tag. Other object 30 variation 1 Explicit tags are blocked with this tag in one request.

Tag Address	Definition	Description
30.1.10.Value*	Value of point 10 as a Long	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server. The DNP server uses its object group 32 default event variation. If the DNP server is returning a floating-point value using object group 32 variations 5, 6, 7, or 8, this tag only displays the integer part of the value of the point.
30.2.10.Explicit	Value of point 10 as a Short	An explicit request is sent to the device to get the value for this tag. Other object 30 variation 2 Explicit tags are blocked with this tag in one request.
30.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned)	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the device sends an event with the time. The object group 32 default event variation on the device needs to be 3, 4, 7, or 8 for it to return the event time of occurrence.
30.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for analog input point 9. No explicit request is sent to the device. The value of this tag displays the latest flags' byte received for point 9 (regardless of the variation in the tag address).
30.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for analog input point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2 from the flags byte received for point 3 (regardless of the variation in the tag address).

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to* ***Communications***.

Object Group 34 - Analog Inputs Deadband

These tags are only read explicitly once after start. Explicit reads of the same object group and Variation are blocked together: A block that contains a failed tag continues to be read until the tag's quality changes to good or is removed.

Attributes

The default data type is shown in **bold**.

OBJ.VAR.IDX Attributes	.SUB Attribute	Data Type	Access
34.0.{0-65535}	Value, Explicit	DWord	Read/Write
34.1.{0-65535}	Value, Explicit	Word	Read/Write

OBJ.VAR.IDX Attributes	.SUB Attribute	Data Type	Access
34.2.{0-65535}	Value, Explicit	**DWord**	Read/Write
34.3.{0-65535}	Value, Explicit	Float	Read/Write

Variations

Number	Description
0	Variation determined by DNP server device*
1	Deadband 16-bit
2	Deadband 32-bit
3	Deadband 32-bit floating-point

* Variation 0 is used to request the default variation.

Examples

Tag Address	Definition	Description
34.0.0.Value	Deadband Value of analog input point 0 as a DWord	If a value for this tag has not been received from the device, then an explicit request is sent. The DNP server could return variation 1, 2, or 3; depending on its object 34 default variation. These all fit in a DWord. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 34 variation 0 Explicit and Value tags are blocked with this tag in one request.
34.0.5.Explicit	Deadband value of analog input point 5 as a DWord	If a value for this tag has not been received from the device, then an explicit request is sent. The DNP server could return variation 1, 2, or 3; depending on its object 34 default variation. These all fit in a DWord. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 34 variation 0 Explicit and Value tags are blocked with this tag in one request.
34.1.10.Explicit	Deadband value of analog input point 10 as a Word	If a value for this tag has not been received from the device, then an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 34 variation 1 Explicit and Value tags are blocked with this tag in one request.
34.1.10.Value	Deadband value of analog input point 10 as a Word	If a value for this tag has not been received from the device, then an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 34 variation 2 Explicit and Value tags are blocked with this tag in one request.
34.2.10.Explicit	Deadband value of analog input point 10 as a	If a value for this tag has not been received from the device, then an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 34 variation 2 Explicit and Value tags are blocked with this tag in one request.

Tag Address	Definition	Description
	DWord	

Object Group 40 - Analog Outputs

The status for each point in an object group is retained on each transaction; all flags are reported in their sub-type tags. The corresponding event object may also return Time of Occurrence.

Note: Object group 40 - Analog Output value is reflected in object group 41 - Analog Output Write, object group 42 - Analog Output Change Event, and object group 43 - Analog Output Command Event. For more information, refer to **Other Object Groups**.

See Also: **Object Group 41 - Analog Output Commands**

Attributes

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
40.{0,1,2,3,4}.{0-65535}	LocalForce, Lost, Online, RemoteForce, Restart, Over-Range, ReferenceCheck	Boolean	Read Only
40.{0,1,2,3,4}.{0-65535}	DO, SO	Boolean	Read/Write
40.{0,1,2,3,4}.{0-65535}	Flags	Byte	Read Only
40.{0,1,2,3,4}.{0-65535}	Timestamp	Date	Read Only
40.0.{0-65535}	Value, Explicit	Double	Read/Write
40.1.{0-65535}	Value, Explicit	Long	Read/Write
40.2.{0-65535}	Value, Explicit	Short	Read/Write
40.3.{0-65535}	Value, Explicit	Float	Read/Write
40.4.{0-65535}	Value, Explicit	**Double**	Read/Write

Variations

Variation	Description
0	Status - Variation determined by DNP server device*
1	Status 32-bit with flag
2	Status 16-bit with flag
3	Status 32-bit floating-point with flag
4	Status 64-bit floating-point with flag

* Variation 0 is used to request the default variation.

DNP Object Flag Definitions

If the device returns an exception bit set, the quality of the .Value or .Explicit tag is bad. The following available bits are exception bits, excluding Online. Descriptions are as follows:

- 0: Online
- 1: Restart
- 2: Communications Lost
- 3: Remote Force
- 4: Local Force
- 5: Overrange
- 6: Reference Check
- 7: Reserved

Examples

Tag Address	Definition	Description
40.0.0.Value*	Value of point 0 as a Double	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The DNP server could return variation 1, 2, 3, 4, 5, 6, 7, or 8; depending on its object group 42 default event variation. These all fit in a Double.
40.0.5.Explicit	Value of point 5 as a Double	An explicit request is sent to the device to get the value for this tag. Other object 40 variation 0 Explicit tags are blocked with this tag in one request. The DNP server could return variation 1, 2, 3, or 4; depending on its default static variation. These all fit in a Double.
40.1.10.Explicit	Value of point 10 as a Long	An explicit request is sent to the device to get the value for this tag. Other object 40 variation 1 Explicit tags are blocked with this tag in one request.
40.1.10.Value*	Value of point 10 as a Long	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. The variation of 1 in the tag address sets the data type of the tag, but does not define the data type returned by the DNP server. The DNP server uses its object group 42 default event variation. If the DNP server is returning a floating-point value using object group 42 variations 5, 6, 7, or 8, this tag only displays the integer part of the value of the point.
40.2.10.Explicit	Value of point 10 as a Short	An explicit request is sent to the device to get the value for this tag. Other object 40 variation 2 Explicit tags are blocked with this tag in one request.
40.0.8.Timestamp*	Event Time of Occurrence of point 8 (if an event has occurred and the time of occurrence was returned)	This tag is updated from the data store that is populated via responses to integrity and event polls. No explicit request is sent to the device. This tag shows a timestamp of 1999-11-30T00:00:00 or 1899-12-30T00:00:00. It has bad quality until the device sends an event with the time. The object group 42 default event variation on the device needs to be 3, 4, 7, or 8 for it to return the event time of occurrence.
40.0.9.Flags*	Latest Flag byte for point 9	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for analog output point 9. No explicit request is sent to the device. The value of this tag displays the latest flag byte received for point 9 (regardless of the variation in the tag address).

Tag Address	Definition	Description
40.0.3.Lost*	Latest state of bit 2 of the Flag byte for point 3	This tag is updated from the data store that is populated via responses to integrity and event polls or an explicit request for analog output point 3. No explicit request is sent to the device. The value of this tag displays the state of bit 2 from the flag byte received for point 3 (regardless of the variation in the tag address).
40.0.2.DO*	Boolean value indicating if operations on analog output point 2 should be Direct Operate or Select then Operate	Writing to this tag does not cause an explicit write to the device. It also does not change the overall device property for Operate Mode. It only changes it for Analog Output point 2. The variation of the tag does not matter. The value of this tag is used when an operation is performed on analog output point 2 using a synchronous or asynchronous write to a 40.x.2.Value or 40.x.2.Explicit tag.
40.0.2.SO*	Boolean value indicating if operations on analog output point 2 should be Direct Operate or Select then Operate	Writing to this tag does not cause an explicit write to the device. It also does not change the overall device property for Operate Mode. It only changes it for Analog Output point 2. The variation of the tag does not matter. The value of this tag is used when an operation is performed on analog output point 2 using a synchronous or asynchronous write to a 40.x.2.Value or 40.x.2.Explicit tag.

* If an event time of occurrence is received with the event, then the tag's OPC timestamp should display the DNP client local time in which the event occurred within the DNP server. *For more information, refer to* ***Communications****.*

Object Group 41 - Analog Output Commands

Issuing an Analog Output Command

To issue an analog output command, execute a synchronous or an asynchronous write to a 40.x.x.Value or a 40.x.x.Explicit tag. Depending on the Feedback Poll after Operate device property, another request may be sent after the actual operate request to obtain the latest value of all analog output points. If the operate is successful but the feedback poll fails, the device reports status code 4. *For more information, refer to* ***Advanced****.*

- ***Unable to write to address <address> on device <device>. Control-Related Status Code <status code>***

Function Codes

The function code used in the write request depends on the setting of the overall device property for Operate Mode and/or any 40.x.x.DO or 40x.x.SO tags. The Select then Operate option sends two requests - the first with the select function code (3) followed by a request with the operate function code (4). The Direct Operate option sends one request with the direct operate function code (5). *For more information on the Operate Mode device property, refer to* ***Advanced****.*

- *For more information on the DO and SO sub-type, refer to* ***Object Group 40 - Analog Outputs****.*

Object Group 50 - Time and Date

Object group 50 is the DNP server clock. Since it cannot be read through unsolicited replies, the DNP Client Ethernet Driver must explicitly request a read. The driver requests a read every time the tag is pulled for an update because it's a time datum. On a default instantiation, this occurs every 200 ms. To avoid congesting the communications link, create a separate OPC group for the object group 50 time tag. Set the group update rate to 1000 ms or slower.

Note: Object group 50 - Time and Date is reflected in object group 51 - Time and Date Common Time of Occurrence (CTO). *For more information, refer to* ***Other Object Groups***.

Attributes

The default data type is shown in **bold**.

OBJ.VAR Attributes	.SUB Attribute	Data Type	Access
50.0	Value, Explicit	Date	Read Only
50.1	Value, Explicit	**Date**	Read Only

Note: Flags do not apply.

Variations

Number	Description
0	Time and Data Absolute time*
1	Time and Date Absolute time

* Allowed, but same as 50.1.

Examples

Tag Address	Definition	Description
50.0.Value	Date and time saved in the DNP server	An explicit request for object 50 variation 1 is sent to the device to get the value for this tag. The update rate should not be set too often since it causes traffic every time the tag needs to be updated.
50.1.Value	Date and time saved in the DNP server	An explicit request for object 50 variation 1 is sent to the device to get the value for this tag. The update rate should not be set too often since it causes traffic every time the tag needs to be updated.
50.0.Explicit	Date and time saved in the DNP server	An explicit request for object 50 variation 1 is sent to the device to get the value for this tag. The update rate should not be too set often since it causes traffic every time the tag needs to be updated.
50.1.Explicit	Date and time saved in the DNP server	An explicit request for object 50 variation 1 is sent to the device to get the value for this tag. The update rate should not be set too often since it causes traffic every time the tag needs to be updated.

Object Group 60 - Class Poll Data Request

When a Boolean True is written to these tags, object group 60 variations 1-4 initiate class 0-3 reads (respectively). Object group 60 tags can be used to 'manually' poll when the recommended event and integrity class polling intervals cannot be used. This approach is not recommended, however, because care must be taken to keep the requests in proper order. An integrity poll polls class 1, 2, 3, and 0 in that order, in one request, and without time lapses in between.

When using the object group 60 tags to poll for events, users should poll the event classes (variations 2, 3, and 4) before polling for class 0 static data (variation 1). This ensures that event data is received in the correct order and that the latest value is received after preceding events. Although a class object group 60.1 request can be issued immediately after any of the event class object group 60.2, 3, or 4 requests, these are still separate requests. Users risk losing any events that occurred between the last class 1, 2, or 3 request and the class 0 request. A read of these tags always returns a Boolean False with good quality.

Attributes

These tags trigger commands on the DNP server device when a True value is written. They read back as zero or False.

OBJVAR Attributes	.SUB Attribute	Data Type	Access
60.{1}	Value, Explicit	Boolean	Read/Write
60.{2}	Value, Explicit	Boolean	Read/Write
60.{3}	Value, Explicit	Boolean	Read/Write
60.{4}	Value, Explicit	Boolean	Read/Write

Note: Flags do not apply.

Variations

Number	Description
1	Initiates a poll of DNP Class 0 data
2	Initiates a poll of DNP Class 1 data
3	Initiates a poll of DNP Class 2 data
4	Initiates a poll of DNP Class 3 data

Examples

Tag Address	Definition	Description
60.1.Value	Always displays a Boolean value of 0 with good quality	Writing a 1 to this tag initiates a request for Class 0 data. The sub-type can be value or explicit.
60.2.Value	Always displays a Boolean value of 0 with good quality	Writing a 1 to this tag initiates a request for Class 1 data. The sub-type can be value or explicit.
60.3.Explicit	Always displays a Boolean value of 0 with good quality	Writing a 1 to this tag initiates a request for Class 2 data. The sub-type can be value or explicit.
60.4.Explicit	Always displays a Boolean value of 0 with good quality	Writing a 1 to this tag initiates a request for Class 3 data. The sub-type can be value or explicit.

Object Group 70 - File Identifiers

Attributes

OBJIDX Attributes	.SUB Attributes	Data Type	Access
70.0-9	Download, Upload	Boolean	Read/Write
70.0-9	LocalFileName, RemoteFileName	String	Read/Write

Note: Flags do not apply.

Examples

Tag Address	Definition	Description
70.0.Upload	Displays the current status of a file transfer upload for the file settings configured for index 0. 0: No file transfer upload in progress 1: Upload in progress	Writing a 1 to this tag causes a file transfer of the remote file on the DNP server to the local file on the DNP client. The file identifiers are built from the path and the file name properties. If the path does not already end in a backslash or forward slash, one is added before the file name. The tag displays a 1 until the transfer completes (at which time the tag displays a 0). If an upload is in progress, writing a 0 to this tag causes the file transfer to be terminated.
70.5.Download	Displays the current status of a file transfer download for the file settings configured for index 5. 0: No file transfer download in progress 1: Download in progress	Writing a 1 to this tag causes a file transfer of the local file on the DNP client to the remote file on the DNP server. The file identifiers are built from the path and the file name properties. If the path does not already end in a backslash or forward slash, one is added before the file name. The tag displays a 1 until the transfer completes (at which time the tag displays a 0). If a download is in progress, writing a 0 to this tag causes the file transfer to be terminated.
70.6.LocalFileName	Displays the currently configured local file name from the device property File Control tab for	This tag is Read Only unless the device Property for File Name Writes is set to Yes. If the tag has Read / Write access, writing to this tag updates the corresponding File Control device property. The contents of the local file name property is appended to the local path to build the file identifier. A backslash or forward slash separates the path from the file name.

Tag Address	Definition	Description
	index 6.	
70.8.RemoteFileName	Displays the currently configured remote file name from the device property File Control tab for index 8.	This tag is Read Only unless the device Property for File Name Writes is set to Yes. If the tag has Read / Write access, writing to this tag updates the corresponding File Control device property. The contents of the remote file name property is appended to the remote path to build the file identifier. A backslash or forward slash separates the path from the file name.

Object Group 80 - Internal Indications

Attributes

The default data type is shown in **bold**.

OBJVAR Attributes	.SUB Attribute	Data Type	Access
80.{0}	Value, Explicit	Word	Read Only
80.{1}	Value, Explicit	**Word**	Read Only

Note: Flags do not apply.

Variations

Number	Description
0	Internal Indications packed format*
1	Internal Indications packed format

* Allowed, but same as 80.1.

IIN Definitions

Object group 80 returns the DNP Internal Indication bits (IIN) as an unsigned short integer. The data is refreshed with each response from the DNP server, and therefore represents the latest IIN report.

Internal Indication	Bit Mask	Reason
DNPDEFS_IIN_RESTART	0x8000	DNP server has been restarted
DNPDEFS_IIN_TROUBLE	0x4000	DNP server is reporting trouble
DNPDEFS_IIN_LOCAL	0x2000	DNP server is running in local mode
DNPDEFS_IIN_NEED_TIME	0x1000	DNP server requires time synchronization
DNPDEFS_IIN_CLASS_3	0x0800	DNP server has Class 3 data available
DNPDEFS_IIN_CLASS_2	0x0400	DNP server has Class 2 data available
DNPDEFS_IIN_CLASS_1	0X0200	DNP server has Class 1 data available
DNPDEFS_IIN_ALL_STATIONS	0x0100	The message was directed to the DNP broadcast address
DNPDEFS_IIN_BAD_CONFIG	0x0020	DNP server is misconfigured

Internal Indication	Bit Mask	Reason
DNPDEFS_IIN_ALREADY_EXECUTING	0x0010	DNP server has received a duplicate request
DNPDEFS_IIN_BUFFER_OVFL	0x0008	DNP server has lost one or more event reports
DNPDEFS_IIN_OUT_OF_RANGE	0x0004	Command received references a non-existent I/O point
DNPDEFS_IIN_OBJECT_UNKNOWN	0x0002	Command received references an unknown object
DNPDEFS_IIN_BAD_FUNCTION	0x0001	Command received is not supported

Examples

Tag Address	Definition	Description
80.0.Value	Latest Value of the two IIN bytes as a Word	The DNP server's response to every request includes two internal indication bytes. The bits of these bytes have special meanings as defined by the DNP spec. This tag displays the IIN bytes received in the last response from the device. This is read from the data store and does not send an explicit request. The sub-type can be value or explicit; the variation can be 0 or 1. It makes no difference.
80.1.Explicit	Latest Value of the two IIN bytes as a Word	The DNP server's response to every request includes two internal indication bytes. The bits of these bytes have special meanings as defined by the DNP spec. This tag displays the IIN bytes received in the last response from the device. This is read from the data store and does not send an explicit request. The sub-type can be value or explicit; the variation can be 0 or 1. It makes no difference.

Object Group 87 - Data Sets

.Value tags are populated by the data received from unsolicited events or integrity and event class polling. .Explicit tags cause a device read: because tags for one set are blocked together, there is only one device read for the entire data set.

Notes:

1. At this time, data sets can only be defined in the DNP server. Users who manually create tags must define the correct data types. The DNP client obtains the description of the data sets from the DNP server to automatically define tags.

2. Object group 88 - Data Set - Snapshot data is reflected in object group 87 - Data Sets - Present value tags. *For more information, refer to* ***Other Object Groups****.*

Attributes

Variations for object group 87 do not equate to specific data types. Users must configure the tag with the same data type that is configured in the DNP server for the specific data set element. Descriptions of the attributes are as follows:

- **VAR:** This attribute indicates the particular element of the data set.
- **IDX:** This attribute indicates the particular data set that is defined in the device.

The default data type is shown in **bold**.

OBJVAR.IDX Attributes	.SUB Attribute	Data Type	Access
87.{0-1}.{0-65535}	Value, Explicit	Byte, Char, Date, Double, **DWord**, Float, Long, Short, String, Word	Read Only
87.{2-32}.{0-65535}	Value, Explicit	Byte, Char, Date, Double, **DWord**, Float, Long, Short, String, Word	Read/Write
87.{0}.{0-65535}	Set	**Boolean**	Read/Write

Variations

DNP Object Flag Definitions

To get a data point's flags, the DNP server's definition of the data set must include an element specifically for DNP flags.

Examples

Tag Address	Definition	Description
87.5.1.Explicit	Displays the fifth element of data set 1	The .Explicit sub-type indicates that a request to the device for all elements of data set 1 occurs every time the tag needs to be updated.
87.7.2.Value	Displays the seventh element of data set 2	The .Value sub-type indicates the tags for data set 2 is only updated from the data store that is populated through unsolicited messages or integrity and event polls.
87.0.2.Set	Always displays a Boolean value of 0 with good quality	Writing a 1 to this tag causes an object group 87 write operation on data set 2. The write only takes place if there is data pending to be written due to a previous write to other .Value or .Explicit tags of this data set.

Object Group 110 - Octet String Object

These tags are only read explicitly once after start. Explicit reads of the same object group and Variation are blocked together: A block that contains a failed tag continues to be read until the tag's quality changes to good or is removed.

Notes:

1. Object group 110 - Octet String value is reflected in object group 111 - Octet String Event Change. *For more information, refer to* ***Other Object Groups***.
2. Zero-length string tags return bad quality.

Attributes

The default data type is shown in **bold**.

OBJIDX Attributes	.SUB Attribute	Data Type	Access
110.{0-65535}	Value, Explicit - takes up to 255 characters	**String**	Read/Write

Note: Flags do not apply.

Variations

Number	Description
String Length	Octet String

Examples

Tag Address	Definition	Description
110.0.Value	Value of point 0 as a String	If a value for this tag has not been received from the device, then an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 110 explicit and value tags are blocked with this tag in one request. The sub-type can be Value or Explicit: it makes no difference.
110.5.Explicit	Value of point 5 as a String	If a value for this tag has not been received from the device, then an explicit request is sent. Once the point has been initialized, the tag receives its updates from the data store. A second explicit request is only issued if the DNP server or client restarts. Other object 110 explicit and value tags are blocked with this tag in one request. The sub-type can be value or explicit: it makes no difference.

Object Group 120 - Authentication Object

The authentication object tags are internal statistics for DNP authentication.

Attributes

The default data type is shown in **bold**.

OBJVAR Attributes	.SUB Attribute	Description	Data Type	Access
120.KeyStatRQTX	Value Reset	Key status requests sent to outstation.	**DWord** **Bool**	Read Only Read/Write
120.KeyStatRQRX	Value Reset	Key status responses received from out-station.	**DWord** **Bool**	Read Only Read/Write

OBJVAR Attributes	.SUB Attribute	Description	Data Type	Access
120.KeyStatRQRX_NoInit	Value Reset	Key status request responded with an uninitialized failure.	**DWord Bool**	Read Only Read/Write
120.KeyStatRQRX_CommFail	Value Reset	Key status request responded with a communications failure.	**DWord Bool**	Read Only Read/Write
120.KeyStatRQRX_AuthFail	Value Reset	Key status request responded with an authentication failure.	**DWord Bool**	Read Only Read/Write
120.KeyChangeTX	Value Reset	Key change requests sent to the outstation.	**DWord Bool**	Read Only Read/Write
120.AggrModeRQTX	Value Reset	Aggressive mode requests sent to the outstation.	**DWord Bool**	Read Only Read/Write
120.AggrModeResponseRX	Value Reset	Aggressive mode responses from the outstation	**DWord Bool**	Read Only Read/Write
120.AggrModeResponseRX_Failed	Value Reset	Aggressive mode request responded with a failure.	**DWord Bool**	Read Only Read/Write
120.ChallRQTX	Value Reset	Challenge requests sent to the outstation.	**DWord Bool**	Read Only Read/Write
120.ChallRQRX	Value Reset	Challenge requests received from the outstation.	**DWord Bool**	Read Only Read/Write
120.CriticalChallRQTX	Value Reset	Critical challenge requests sent to the outstation.	**DWord Bool**	Read Only Read/Write
120.CriticalChallRQRX	Value Reset	Critical challenge requests received from the outstation.	**DWord Bool**	Read Only Read/Write
120.ChallReplyTX	Value Reset	Challenge responses sent to the outstation.	**DWord Bool**	Read Only Read/Write
120.ChallReplyRX	Value Reset	Challenge responses received from the outstation.	**DWord Bool**	Read Only Read/Write
120.ChallReplyRX_Failed	Value Reset	Challenge responses with a failure.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_Invalid	Value Reset	Invalid errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_UnexpectedReply	Value Reset	Unexpected reply errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_NoReply	Value Reset	No reply errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_ AggrModeNotSupported	Value Reset	Aggressive mode not supported errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_HMACAlgNotSupported	Value Reset	HMAC algorithm not supported errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_KeyWrapAlgNotSupported	Value Reset	Key wrap algorithm not supported errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_UserAccessDenied	Value Reset	User access denied errors sent to outstation.	**DWord Bool**	Read Only Read/Write
120.ErrorTX_	Value	Key change denied errors sent to out-	**DWord**	Read Only

OBJVAR Attributes	.SUB Attribute	Description	Data Type	Access
KeyChangeDenied	Reset	station.	**Bool**	Read/Write
120.ErrorTX_InvalidSign	Value Reset	Invalid signature errors sent to out-station.	**DWord** **Bool**	Read Only Read/Write
120.ErrorTX_InvalidCert	Value Reset	Invalid certificate errors sent to out-station.	**DWord** **Bool**	Read Only Read/Write
120.ErrorTX_UnknownUser	Value Reset	Unknown user errors sent to outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorTX_VendorSpecific	Value Reset	Vendor-specific errors sent to outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_Invalid	Value Reset	Invalid errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_Unex-pectedReply	Value Reset	Unexpected reply errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_NoReply	Value Reset	No reply errors received from out-station.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_ AggrModeNotSupported	Value Reset	Aggressive mode not supported errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_HMACAl-gNotSupported	Value Reset	HMAC algorithm not supported errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_KeyWrapAl-gNotSupported	Value Reset	Key wrap algorithm not supported errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_User-AccessDenied	Value Reset	User access denied errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_ KeyChangeDenied	Value Reset	Key change denied errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_InvalidSign	Value Reset	Invalid signature errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_InvalidCert	Value Reset	Invalid certificate errors received from outstation.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_UnknownUser	Value Reset	Unknown user errors received from out-station.	**DWord** **Bool**	Read Only Read/Write
120.ErrorRX_VendorSpecific	Value Reset	Vendor-specific errors received from outstation.	**DWord** **Bool**	Read Only Read/Write

Examples

Tag Address	Definition	Description
120.KeyStatRQTX.Value	Value of the KeyStatRQTX authentication statistic	The number of key status requests sent to the outstation since startup or last reset.
120.KeyStatRQTX.Reset	Reset the KeyStatRQTX authentication statistic	The KeyStatRQTX statistic is cleared with a write value of 1.

Other Object Groups

Certain objects are not used in the driver due to the fact that their values are reflected in other objects.

Object	Name	Reflected in Object	Name
2	Binary Input Change Event	1	Binary Input State
4	Double Bit Input Change Event	3	Double Bit Input State
11	Binary Output Change Event	10	Binary Output State
12	Control Relay Output Block	10	Binary Output State
13	Binary Output Command Event	10	Binary Output State
22	Counter Event Change	20	Counter Value
23	Frozen Counter Event Change	21	Frozen Counter Value
32	Analog Input Change Event	30	Analog Input Value
41	Analog Output Write	40	Analog Output Value
42	Analog Output Change Event	40	Analog Output Value
43	Analog Output Command Event	40	Analog Output Value
51	Time and Date Common Time of Occurrence (CTO)	50	Time and Date
88	Data Set - Snapshot	87	Data Set - Present Value
111	Octet String Event Change	110	Octet String Value

Internal Tags

Tag	Description	Data Type	Access
_AuthCurrentUserNumber	This tag allows the authentication Current User Number device property to be changed from a client application. Valid values range from 0 to 65535.	Word	Read/Write
_ChannelResponseTimeout	This tag allows the Request Timeout channel property to be changed from a client application. Valid values range from 100 to 3600000.	DWord	Read/Write
_DestinationHost	This tag allows the Destination Host channel property to be changed from a client application. The Host address must be formatted correctly.	String	Read/Write
_DestinationPort	This tag allows the Destination Port channel property to be changed from a client application. Valid values range from 1 to 65535.	Word	Read/Write
_DeviceRequestQueueDepth	This tag indicates the current depth of the queue used for storing device requests. It is useful for diagnostic purposes for issues such as tag update delays. Although a zero or steady value is expected, a non-zero value is not a problem unless it continues to grow and causes a delay in tag updates. For example, if the project has a device defined with 100 blocks of .Explicit tags and the _DeviceRequestQueueDepth tag value is 100, then something is blocking the tags from being updated on time.	DWord	Read Only
_DeviceRequestTimeout	This tag allows the Request Timeout device property to be changed from a client application. Valid values range from 0 to 3600000.	DWord	Read/Write
_EventClass1PollInterval*	This tag allows the Event Class Poll 1 Interval device property to be changed from a client application. Valid values range from 0 to 86400 seconds.	DWord	Read/Write
_EventClass2PollInterval*	This tag allows the Event Class Poll 2 Interval device property to be changed from a client application. Valid values range from 0 to 86400 seconds.	DWord	Read/Write
_EventClass3PollInterval*	This tag allows the Event Class 3 Poll Interval device property to be changed from a client application. Valid values range from 0 to 86400 seconds.	DWord	Read/Write
_IntegrityPollInterval	This tag allows the Integrity Poll device property to be changed from a client application. Valid values range from 0 to 2592000.	DWord	Read/Write
_DNPClient	This tag allows the DNP client address device property to be changed from a client application. Valid values range from 0 to 65519.	DWord	Read/Write
_Protocol	This tag allows the Ethernet Protocol channel property to be changed from a client application. Valid values range from 0 to 1. A value of 0 indicates TCP/IP; a	Byte	Read/Write

Tag	Description	Data Type	Access
	value of 1 indicates UDP.		
_DNPServerAddress	This tag allows the DNP server address device property to be changed from a client application. Valid values range from 0 to 65519.	DWord	Read/Write
_SourcePort	This tag allows the Source Port channel property to be changed from a client application. Valid values range from 0 to 65535.	Word	Read/Write
_TimeSyncStyle	This tag allows the Time Synchronization Style device property to be changed from a client application. Valid values range from 0 to 1. A value of 0 indicates the Serial Time Sync Style; a value of 1 indicates the LAN Time Sync Style.	Byte	Read/Write

* Any write to this tag changes the units to seconds. There is currently no mechanism to change the units to milliseconds, minutes, or hours from an internal tag.

Special Tags

Tag	Description
ActivateConfig	When a Boolean True is written to this tag, an Activate Configuration Request is sent to the DNP server device. The tag is read back as zero or false and always has good quality.*
Coldrestart	When a Boolean True is written to this tag, a cold restart is sent to the DNP server device. The tag is read back as zero or false.
Unsolreceived	When Unsolicited Messaging is enabled for the device in the OPC server, the tag increments by 1 every time an unsolicited message is received from the DNP server. **Note**: This tag is read / write, so it can be reset to any value by the operator.
Warmrestart	When a Boolean True is written to this tag, a warm restart is sent to the DNP server device. The tag is read back as zero or false.

* The objects included in the request are defined in the Activate Config Objects parameter located in **Device Properties** | **File Control**. *For more information, refer to* ***File Control***.

Device Profile

For more information on a specific section of the device profile, select a link from the list below.

For a copy of the device profile template, refer to DNP.org.

Device Properties — Identification

Component	Description	Current Value	Methods
Device Function	Clients send DNP requests.	Client	N/A
Device Name	This is the model and name of the device, which should be sufficient to distinguish it from any other device from the same organization.	DNP Client Ethernet	N/A
Hardware Version	N/A	- Windows 7 - Windows Server 2008 - Windows Vista Business / Ultimate - Windows Server 2003 SP2 - Windows XP SP2 - Windows Server 2019 - Windows Server 2016 - Windows 8 and 10 - Windows 10 IoT Enterprise - Windows Server 2012 and 2012 R2	N/A
Software Version	N/A	v.5	N/A
Device Profile Document Version	The version of the device profile Document is indicated by a whole number incremented with each new release.	4	N/A
Supported WITS Major Version	The major version of the WITS Standard implemented by the device.	1	N/A
Supported WITS Minor Version	The minor version of the WITS Standard implemented by the device.	0	N/A

Component	Description	Current Value	Methods
DNP Levels Supported for Requests	The DNP3 level to which the device conforms fully. Requests can be indicated independently.	3	N/A
DNP Levels Supported for Responses	The DNP3 level to which the device conforms fully. Responses can be indicated independently.	3	N/A
Supported Function Blocks	N/A	Object 0 - Attribute objects, Data Sets, File Transfer, Secure authentication, and Function Code 31 - Activate Configuration.	N/A
Notable Additions	This brief description intends to identify the most obvious features that the device supports, in addition to the highest supported level of DNP. The complete list of features is described in the Implementation Table.	- Enabling and disabling unsolicited responses on an individual class basis. - Double-bit Input objects. - Variations with time for Frozen Counters, Frozen Counter Events, and Analog Input Events. - Floating-point variations for both Analog Inputs and Analog Outputs. - Analog Input Reporting Deadband. - Event objects for Binary and Analog Outputs. - Device Attribute objects including the Standard DNP set 0 and User-defined sets. - Data Set objects. - Authentication. - File Control. - Activate Configuration.	*For more information, refer to* ***Address Descriptions***.
Methods to Set Configurable Parameters	N/A	N/A	Methods include .opf and .xml project files.*

* In addition to custom Channel Properties and Device Properties dialogs.

IP Networking

Component	Description	Current Value	Methods
IP Type of End Point	N/A	TCP Initiating UDP Data-	N/A

Component	Description	Current Value	Methods
		gram	
IP Address	N/A	Configurable IP Address	N/A
IP Accepts TCP Connections or UDP Datagrams from:	N/A	Allows all TCP connections	N/A
IP addresses from which TCP Connections or UDP Datagrams are Accepted	N/A	*.*.*.*	N/A
IP TCP Listen Port Number	N/A	Not supported	N/A
IP TCP Listen Port Number of Remote Device	N/A	20000	Property is located on device Communications Property page. The destination port ranges from 1 to 65535.
IP TCP Keep-Alive Timer	N/A	N/A	N/A
IP Local UDP Port	N/A	Let the system choose	Property is located on Channel Communications Property page. The source port ranges from 0 to 65535.
IP Destination UDP Port for DNP3 Requests	N/A	20000	Property is located on device Communications Property page. The destination port ranges from 1 to 65535.
IP Multiple Outstation Connections - Client (Master)	N/A	Supports multiple	N/A
IP Time Synchronization Support	N/A	DNP3 LAN procedure (function code 24)	Property is located on device Communications Property page.

Link Layer

Component	Description	Current Value	Methods
Data Link Address	This indicates if the link address is configurable over the entire valid range of 0 to 65519.	Ranges from 0 to 65519.	DNP server address property is located on device Communications Property page.
Sends Confirmed User Data Frames	This is a list of conditions under which the device transmits the following confirmed link layer services: TEST_LINK_STATES RESET_LINK_STATES CONFIRMED_USER_DATA	Never	N/A
Data Link Layer Confirmation Timeout	This timeout applies to any secondary data link message that requires a confirmation or response (such as link reset, link status, user data, and so forth).	2 seconds	N/A

Component	Description	Current Value	Methods
Maximum Data Link Retries	This is the number of times that the device retransmits a frame that requests Link Layer confirmation.	3 retries	N/A
Maximum Number of Octets Transmitted in a Data Link Frame	This number includes the checksum. With a length field of 255, the maximum size would be 292.	292	N/A
Maximum Number of Octets that can be Received in a Data Link Frame	This number includes the checksum. With a length field of 255, the maximum size would be 292. The device must be able to receive 292 octets to be compliant.	292	N/A

* Data link addresses 0xFFF0 through 0xFFFF are reserved for broadcast or other special purposes.

Application Layer

Component	Description	Current Value	Methods
Maximum Number of Octets Transmitted in an Application Layer Fragment other than File Transfer	This size does not include any transport or frame octets. DNP clients must provide a setting less than or equal to 249.	249	N/A
Maximum Number of Octets Transmitted in an Application Layer Fragment Containing File Transfer	N/A	N/A	N/A
Maximum Number of Octets that can be Received in an Application Layer Fragment	This size does not include any transport or frame octets. DNP clients must provide a setting greater than or equal to 2048.	2048	N/A
Timeout waiting for Complete Application Layer Fragment	Timeout if all frames of a message fragment are not received in the specified time. It is measured from the time that the first frame of a fragment is received until the last frame is received.	N/A	N/A
Maximum Number of objects Allowed in a Single Control Request for CROB (g12)	N/A	N/A	N/A
Maximum Number of objects Allowed in a Single Control Request for Analog Outputs (g41)	N/A	N/A	N/A

Component	Description	Current Value	Methods
Maximum Number of objects Allowed in a Single Control Request for Data Sets (g85, 86, 87)	N/A	N/A	N/A
Supports Mixing object groups* in the Same Control Request	N/A	N/A	N/A

* AOBs, cROBs, and Data Sets.

DNP Clients (Masters) Only

Component	Description	Current Value	Methods
Timeout Waiting for Complete Application Layer Response	Timeout on DNP client if all fragments of a response message are not received in the specified time.	10000 ms	Property is located on the Channel Communications Property page. Supported response timeouts are 100 to 3600000.
Maximum Application Layer Retries for Request Messages	This is the number of times a DNP client retransmits an application layer request message if a response is not received. This parameter must never cause a DNP client to retransmit control or time sync messages.	0	Max. Timeouts property is located on the Device Communications Property page. Supported timeouts are 1 to 10 (0 to 9 retries).
Incremental Timeout Waiting for First or Next Fragment of an Application Layer Response	N/A	None	N/A

Security Parameters

Component	Description	Current Value	Methods
DNP3 Device Support for Secure Authentication	Indicates whether the device supports secure authentication (and, if so, what version).	Version 2	Authentication can be enabled on the Authentication tab in device properties. The User Number and Update Key tag properties can be configured in the User Numbers/Update Key tab in device properties.
Maximum Number of Users	The device must support details for each user.	10	The maximum number of users cannot be con-

Component	Description	Current Value	Methods
	Users are identified by a 16-bit user number. Indicates the actual limit to the number of simultaneous users that can be supported.		figured, but the User Number and Update Keys can be configured in device properties.
Security Message Response Timeout	The authentication of critical messages may involve additional message exchanges (challenges and responses), which can require an extension to the normal DNP3 message response timeout. This timeout specifies an additional amount of time to be used when extra security transactions are involved.	2000 milliseconds	The Reply Timeout property is located on the Authentication tab in device properties. The valid range is 0 to 300000 milliseconds.
Aggressive Mode of Operation (Receive)	DNP3 devices have the option to accept "aggressive" mode requests, where challenge data used for authentication is appended to a critical message instead of being solicited through a separate message exchange.	Yes. Accepts aggressive mode requests.	The Enable Aggressive Mode Support property is located on the Authentication tab in device properties.
Aggressive Mode of Operation (Issue)	DNP3 devices must support the issuing of "aggressive" mode of operation, where challenge data used for authentication is appended to a critical message instead of being solicited through a separate message exchange.	Yes. Issues aggressive mode requests.	When authentication is enabled, Aggressive Mode Support is enabled by default.
Session Key Change Interval	To defend against a compromising attack, the session key is changed at regular intervals. To accommodate systems with infrequent communications, this change interval can be disabled to use just the Session	900 seconds	This property is located on the Authentication tab in device properties. The valid range is 0 to 7200 seconds. 0 disables the interval and use the Session Key Change Message Count instead.

Component	Description	Current Value	Methods
	Key Change Message Count instead.		
Session Key Change Message Count	In addition to changing at regular intervals, the session key is also changed after a specified number of messages have been exchanged.	1000	The Session Key Change Count property is located on the Authentication tab in device properties. The valid range is 0 to 65535.
Maximum Error Count	To assist in countering denial of service attacks, the DNP3 device stops replying with error codes after a number of successive authentication failures. Setting the error count to zero inhibits all error messages.	2	This property is located on the Authentication tab in device properties. The valid range is 0 to 10.
MAC Algorithm Requested in Challenge Exchange	Part of the authentication message is hashed using an MAC algorithm. The output of the MAC algorithm is truncated.	Supports the following: HMAC-SHA-1: Truncated to the left-most 4 octets HMAC-SHA-1: Truncated to the left-most 8 octets HMAC-SHA-1: Truncated to the left-most 10 octets HMAC-SHA-256: Truncated to the left-most 8 octets HMAC-SHA-256: Truncated to the left-most 16 octets	N/A
Key-wrap Algorithm to Encrypt Session Keys	When a session key is updated, it is encrypted using AES-128. Other algorithms are optional.	Supports AES-128	Not configurable

Implementation Tables

The following implementation tables identify which object groups and variations, function codes, and qualifiers are supported by the DNP client in both requests and responses. The Request columns identify all requests that may be sent by the DNP client or all requests that must be parsed by a DNP server. The

Response columns identify all responses that must be parsed by the DNP client or all responses that may be sent by a DNP server.

Note: Both the Request Function Code and the Response Function Code are in decimal.

Code	Description
1	Read
2	Write
3	Select
4	Operate
5	Direct operate
6	Direct operate, no acknowledgment
20	Enable unsolicited responses
21	Disable unsolicited responses
25	Open file
26	Close file
27	Delete file
28	Get file information
29	Authenticate file
30	Cancel file transfer
31	Activate configuration
32	Authentication request
129	Response
130	Unsolicited response
131	Authentication response

Note: Both the Request Qualifier Code and the Response Qualifier Code are in hexadecimal.

Code	Description
00	8-bit start-stop
01	16-bit start-stop
06	No range, or all
07	8-bit limited quantity
08	16-bit limited quantity
17	8-bit index
18	16-bit index
5B	Free format

Object Group 0 - Device Attributes

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1-253	Standard Set 0 and User Defined Sets	1 2	00, 06 00	129 N/A	00, 17 N/A
254	Non-specific all attributes request	1	00, 06	129	00, 17
255	List of attribute variations	1	00, 06	129	00, 5B

Object Group 1 - Binary Inputs

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	Packed format	1	00, 01, 06	129	00, 01
2	With flags	1	00, 01, 06	129	00, 01

Object Group 2 - Binary Input Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	Without time	N/A	N/A	129, 130	17, 28
2	With absolute time	N/A	N/A	129, 130	17, 28
3	With relative time	N/A	N/A	129, 130	17, 28

Object Group 3 - Double-Bit Inputs

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	Packed format	1	00, 01, 06	129	00, 01
2	With flags	1	00, 01, 06	129	00, 01

Object Group 4 - Double-Bit Binary Input Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	Without time	N/A	N/A	129, 130	17, 28
2	With absolute time	N/A	N/A	129, 130	17, 28

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
3	With relative time	N/A	N/A	129, 130	17, 28

Object Group 10 - Binary Outputs

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	Packed format	1	00, 01, 06	129	00, 01
2	Output status with flags	1	00, 01, 06	129	00, 01

Object Group 11 - Binary Output Events

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	Status without time	N/A	N/A	129, 130	17, 28
2	Status with time	N/A	N/A	129, 130	17, 28

Object Group 12 -Binary Command

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Control Relay Output Block (CROB)	3, 4, 5, 6	17, 28	129	Echo of request

Object Group 20 - Counters

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	32-bit with flag	1	00, 01, 06	129	00, 01
2	16-bit with flag	1	00, 01, 06	129	00, 01
5	32-bit without flag	1	00, 01, 06	129	00, 01
6	16-bit without flag	1	00, 01, 06	129	00, 01

Object Group 21 - Frozen Counters

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	32-bit with flag	1	00, 01, 06	129	00, 01
2	16-bit with flag	1	00, 01, 06	129	00, 01
5	32-bit with flag and time	1	00, 01, 06	129	00, 01
6	16-bit with flag and time	1	00, 01, 06	129	00, 01
9	32-bit without flag	1	00, 01, 06	129	00, 01
10	16-bit without flag	1	00, 01, 06	129	00, 01

Object Group 22 - Counter Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	32-bit with flag	N/A	N/A	129, 130	17, 28
2	16-bit with flag	N/A	N/A	129, 130	17, 28
5	32-bit with flag and time	N/A	N/A	129, 130	17, 28
6	16-bit with flag and time	N/A	N/A	129, 130	17, 28

Object Group 23 - Frozen Counter Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	32-bit with flag	N/A	N/A	129, 130	17, 28
2	16-bit with flag	N/A	N/A	129, 130	17, 28
5	32-bit with flag and time	N/A	N/A	129, 130	17, 28
6	16-bit with flag and time	N/A	N/A	129, 130	17, 28

Object Group 30 - Analog Input

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	32-bit with flag	1	00, 01, 06	129	00, 01
2	16-bit with flag	1	00, 01, 06	129	00, 01
3	32-bit without flag	1	00, 01, 06	129	00, 01
4	16-bit without flag	1	00, 01, 06	129	00, 01
5	Single-precision floating-point with flag	1	00, 01, 06	129	00, 01

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
6	Double-precision floating-point with flag	1	00, 01, 06	129	00, 01

Object Group 32 - Analog Input Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	32-bit without time	N/A	N/A	129, 130	17, 28
2	16-bit without time	N/A	N/A	129, 130	17, 28
3	32-bit with time	N/A	N/A	129, 130	17, 28
4	16-bit with time	N/A	N/A	129, 130	17, 28
5	Single-precision floating-point without time	N/A	N/A	129, 130	17, 28
6	Double-precision floating-point without time	N/A	N/A	129, 130	17, 28
7	Single-precision floating-point with time	N/A	N/A	129, 130	17, 28
8	Double-precision floating-point with time	N/A	N/A	129, 130	17, 28

Object Group 34 - Analog Inputs Deadband

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	16-bit	1 2	00, 01, 06 00, 01	129 N/A	00, 01 N/A
2	32-bit	1 2	00, 01, 06 00, 01	129 N/A	00, 01 N/A
3	Single-precision floating-point	1 2	00, 01, 06 00, 01	129 N/A	00, 01 N/A

Object Group 40 - Analog Outputs

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	1	00, 01, 06	N/A	N/A
1	32-bit with flag	1	00, 01, 06	129	00, 01
2	16-bit with flag	1	00, 01, 06	129	00, 01

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
3	Single-precision floating-point with flag	1	00, 01, 06	129	00, 01
4	Double-precision floating-point with flag	1	00, 01, 06	129	00, 01

Object Group 41 - Analog Output Status

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	32-bit	3, 4, 5, 6	17, 28	129	Echo of request
2	16-bit	3, 4, 5, 6	17, 28	129	Echo of request
3	Single-precision floating-point	3, 4, 5, 6	17, 28	129	Echo of request
4	Double-precision floating-point	3, 4, 5, 6	17, 28	129	Echo of request

Object Group 42 - Analog Output Event

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
0	Any variation	N/A	N/A	N/A	N/A
1	32-bit without time	N/A	N/A	129, 130	17, 28
2	16-bit without time	N/A	N/A	129, 130	17, 28
3	32-bit with time	N/A	N/A	129, 130	17, 28
4	16-bit with time	N/A	N/A	129, 130	17, 28
5	Single-precision floating point without time	N/A	N/A	129, 130	17, 28
6	Double-precision floating-point without time	N/A	N/A	129, 130	17, 28
7	Single-precision floating-point with time	N/A	N/A	129, 130	17, 28
8	Double-precision floating-point with time	N/A	N/A	129, 130	17, 28

Object Group 50 - Time and Date

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Absolute time	1 2	07 07	129 N/A	07 N/A
3	Absolute time at last recorded time	2	07	N/A	N/A

Object Group 51 - Time and Date CTO

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Absolute time, synchronized	N/A	N/A	129, 130	07
2	Absolute time, unsynchronized	N/A	N/A	129, 130	07

Object Group 52 - Time Delay

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Coarse	N/A	N/A	129	07
2	Fine	N/A	N/A	129	07

Object Group 60 - Class Poll Data Request

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Code	Response Qualifier Codes
1	Class 0 data	1	06	N/A	N/A
2	Class 1 data	1 20 21	06, 07, 08 06 06	N/A N/A N/A	N/A N/A N/A
3	Class 2 data	1 20 21	06, 07, 08 06 06	N/A N/A N/A	N/A N/A N/A
4	Class 3 data	1 20 21	06, 07, 08 06 06	N/A N/A N/A	N/A N/A N/A

Object Group 70 - File Identifiers

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
2	Authentication	29	5B	129	5B
3	File command	25, 27	5B	N/A	N/A
4	File command status	26, 30 N/A	5B N/A	129 130	5B 5B
5	File transport	1, 2 N/A	5B N/A	129 130	5B 5B
6	File transport status	1 N/A	5B N/A	129 130	5B 5B
7	File descriptor	28 N/A	5B N/A	129 130	5B 5B
8	File specification string	31	5B	N/A	N/A

Object Group 80 - Internal Indications

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Packed format	1	00, 01	129	00, 01

Object Group 85 - Data Set Prototype

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	With UUID	1	06	129	5B

Object Group 86 - Data Set Descriptor

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Data Set contents	1	06	129	5B

Object Group 87 - Data Set Present Value

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Present Value	1 2	00, 01, 06 00, 01	129 N/A	5B N/A

Object Group 88 - Data Set Snapshot

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Data Set Snapshot	N/A	N/A	129, 130	5B

Object Group 110 - Octet String Object

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	String	1	00, 01, 06	129	00, 01

Object Group 120 - Authentication Object

Variation	Description	Request Function Code	Request Qualifier Codes	Response Function Codes	Response Qualifier Codes
1	Challenge	32	5B	131	5B
2	Reply	32	5B	131	5B
3	Aggressive Mode Request	1, 2, 3, 4, 5, 6, 20, 21	07	N/A	N/A
4	Session Key Status Request	32	07	N/A	N/A
5	Session Key Status	N/A	N/A	131	5B
6	Session Key Change	32	5B	N/A	N/A
7	Error	32	5B	131	5B
9	HMAC	32	5B	N/A	N/A

Error Descriptions

The following categories of messages that may be generated. Click on the link for a list of messages.

Address Validation Messages

The following messages may be generated. Click on the link for a description of the message.

Address <address> is not valid on device <channel> <device>.

Error Type:
Warning

Possible Cause:
A scan tag with an invalid address was sent to the driver for initialization.

Solution:
Correct the address in the invalid tag.

Address <address> is out of range for the specified device or register.

Error Type:
Warning

Possible Cause:
A tag address that has been specified statically references a location that is beyond the range of supported locations for the device.

Solution:
Verify that the address is correct; if it is not, re-enter the address in the client application.

Data type <type> is not valid for device address <address>.

Error Type:

Warning

Possible Cause:
A tag address that has been specified statically has been assigned an invalid data type.

Solution:
Modify the requested data type in the client application.

Device address <address> contains a syntax error.

Error Type:
Warning

Possible Cause:
A tag address that has been specified statically contains one or more invalid characters.

Solution:
Re-enter the address in the client application.

Device address <address> is read only.

Error Type:
Warning

Possible Cause:
A tag address that has been specified statically has a requested access mode that is not compatible with what the device supports for that address.

Solution:
Change the access mode in the client application.

Authentication Error Messages

The following messages may be generated. Click on the link for a description of the message.

Secure authentication failure on device <channel.device>. Device does not support the function code (IIN2.0).
Secure authentication failure on device <channel.device>. Key status request communications failure. Session keys are not valid.
Secure authentication failure on device <channel.device>. Key status request non-authentic. Session keys are not valid.
Secure authentication failure on device <channel.device>. Aggressive mode response indicates improper authentication.
Secure authentication failure on device <channel.device>. Challenge reply indicates improper authentication.
Secure authentication failure on device <channel.device>. User= <user number>, AssocID= <association ID>, sequence= <sequence number>. RX error code= <error code>-<error description>.

Secure authentication failure on device <channel.device>. User= <user number>, AssocID= <association ID>, sequence= <sequence number>. TX error code= <error code>-<error description>.
Secure authentication failure on device <device>. Key status request response status code: <status code>.

Secure authentication failure on device <channel.device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:
The device is not configured to support authentication.

Solution:
Either disabled the "Authentication" property in device properties or enable authentication on the device.

Secure authentication failure on device <channel.device>. Key Status Request communications failure. Session keys are not valid.

Error Type:
Warning

Possible Cause:
1. The DNP client and server are not configured to match.
2. Either the DNP client or server restarted and the other is expecting a different session key.

Solution:
1. Ensure that the User Number / Update Key pairs on the DNP client match those in the device.
2. Correct any invalid settings (such as KeyWrap Algorithm). Then, wait for the DNP client to issue the key change request.

Secure authentication failure on device <channel.device>. Key Status Request non-authentic. Session Keys are not valid.

Error Type:
Warning

Possible Cause:
The Update Keys do not match or there is another issue with encryption configuration.

Solution:
Correct the invalid Update Key for the current User Number.

Secure authentication failure on device <channel.device>. Aggressive Mode Response indicates improper authentication.

Error Type:
Warning

Possible Cause:
The Update Keys do not match or there is another issue with encryption configuration.

Solution:
Correct the invalid Update Key for the current User Number.

Secure authentication failure on device <channel.device>. Challenge Reply indicates improper authentication.

Error Type:
Warning

Possible Cause:
The Update Keys do not match or there is another issue with encryption configuration.

Solution:
Correct the invalid Update Key for the current User Number.

Note:
The DNP server rejected the critical request.

Secure authentication failure on device <channel.device>. User= <User Number>, AssocID= <Association ID>, Sequence= <Sequence Number>. RX Error Code= <error code>-<error description>.

Error Type:
Warning

Possible Cause:
An error occurred when receiving a message.

Solution:

1. To determine the solution, refer to the code's error description.

Code Number	Description
1	Invalid Information
2	Unexpected Reply
3	No Reply
4	Aggressive Mode Not Supported
5	HMAC Algorithm Not Supported
6	Key Wrap Algorithm Not Supported
7	User Access Denied
8	Key Change Request Denied
9	Invalid Signature
10	Invalid Certification
11	Unknown User
128..255	Vendor Specific

2. When a User Number is provided, it can be used to confirm that the User Number and Update Key match in the DNP client and server.
3. When an Association ID is provided, it can be used to uniquely identify the association between the DNP client and server on which the error occurred. This ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers (or identifiers on the DNP client and server).
4. When a Sequence Number is provided, it can be used to determine which request (such as a Challenge or Key Change) had the authentication failure.

Secure authentication failure on device <channel.device>. User= <User Number>, AssocID= <Association ID>, Sequence= <Sequence Number>. TX Error Code= <error code>-<error description>.

Error Type:

Warning

Possible Cause:

An error occurred when transmitting a message.

Solution:

1. To determine the solution, refer to the code's error description.

Code Number	Description
1	Invalid Information
2	Unexpected Reply
3	No Reply
4	Aggressive Mode Not Supported
5	HMAC Algorithm Not Supported
6	Key Wrap Algorithm Not Supported
7	User Access Denied
8	Key Change Request Denied
9	Invalid Signature
10	Invalid Certification
11	Unknown User
128..255	Vendor Specific

2. When a User Number is provided, it can be used to confirm that the User Number and Update Key match in the DNP client and server.
3. When an Association ID is provided, it can be used to uniquely identify the association between DNP client and server on which the error occurred. This ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers (or identifiers on the DNP client and server).
4. When a Sequence Number is provided, it can be used to determine which request (such as a Challenge or Key Change) had the authentication failure.

Secure authentication failure on device <device>. Key Status Request response status code: <status code>.

Error Type:

Warning

Possible Cause:

An invalid status code was returned in the Key Status Request response from the DNP server.

Solution:

The status code returned in the error message describes the status of the two Session Keys as known by the DNP server. If the status code is 0 ("not used") or 5-255 ("reserved for future use"), determine why the DNP server is responding with an unsupported status code in the object group 120 variation 5 response.

Automatic Tag Database Generation Error Messages

The following messages may be generated. Click on the link for a description of the message.

Unable to add data set <data set index> on device <device name>. Data set has <number of elements> elements. The maximum number of elements allowed is <max. elements>.
Unable to generate a tag database for device <device>. Channel is not open.

Unable to add data set <data set index> on device <device name>. Data set has <number of elements> elements. The maximum number of elements allowed is <max. elements>.

Error Type:
Informational

Possible Cause:
The data set at the specified index has more than the maximum number of elements allowed.

Solution:
Reduce the data set's number of elements.

Unable to generate a tag database for device <device>. Channel is not open.

Error Type:
Warning

Possible Cause:
The driver was unable to initialize the communication stack.

Solution:
Reinitialize the driver by right-clicking on the Administration menu and then selecting Reinitialize. If the problem persists, restart the DNP client.

Unable to generate a tag database for device <device>. Session is not open.

Error Type:
Warning

Possible Cause:
The driver was unable to initialize the communication stack.

Solution:
Reinitialize the driver by right-clicking on the Administration menu and then selecting Reinitialize. If the problem persists, restart the DNP client.

Unable to generate a tag database for device <driver>. The device is not responding.

Error Type:
Warning

Possible Cause:

1. The Ethernet connection between the device and the Host PC is broken.
2. The communication parameters for the Ethernet connection are incorrect.
3. The named device may have been assigned an incorrect Network ID.
4. A device on the channel is unresponsive, due to improper timing settings or a broken communications link.
5. There are multiple channels using DNS host names that resolve to the same IP address.

Solution:

1. Verify the cabling between the DNP client and server device.
2. Verify that the specified communications parameters match those of the device.
3. Verify that the Network ID given to the named device matches that of the actual device.
4. Locate the unresponsive device and then correct the timing settings or fix the broken communications link.
5. Ensure that all channels are using a unique destination host.

Unable to read device attribute set <set number>. No tags added on device <device>.

Error Type:

Warning

Possible Cause:

The device attribute set specified does not exist in the device.

Solution:

Disable "Standard Device Attributes" and/or "User-Defined Device Attributes" in the Tag Import group.

Device Status Messages

The following messages may be generated. Click on the link for a description of the message.

<item description> on device <device> has been auto-demoted.
<item description> on device <device> has been auto-promoted to determine if it can be completed.
Added <tag count> data set tag(s).
Data set write of value <value to be written> pending on tag address <address> on device <device>.
Device <device> does not support the LAN time sync style record current time function code 24 .
Device <device> does not support the LAN time sync style write to object group 50, variation 3.
Device <device> indicated an event buffer overflow (IIN 2.3).
Device <device> indicated it restarted (IIN 1.7).

<Item description> on device <device> has been auto-demoted.

Error Type:

Warning

Possible Cause:

The device continues to set an IIN bit, which requires the DNP client to do something (such as time synchronization or clear the device restart bit); however, the device is rejecting the DNP client's attempts to do so. This is possibly due to an issue with the authentication settings. When a number of successive cycles of request timeouts and retries have occurred, the DNP client stops trying for a period of time.

Solution:

Confirm that the authentication settings specified in the DNP client match those specified in the DNP server.

<Item description> on device <device> has been auto-promoted to determine if it can be completed.

Error Type:

Warning

Possible Cause:
A request that was previously demoted has been promoted so that the DNP client can try to resend the request.

Solution:
If the request is successful, nothing needs to be done. If the item continues to be demoted, ensure that the authentication settings are correct.

Added <tag count> data set tag(s).

Error Type:
Informational

Possible Cause:
If the added tag count for Data Set tags is 0, possible causes may be as follows:

1. There are no data sets defined in the DNP server.
2. The DNP server has a mismatched configuration; that is, it may be reporting that it has more prototypes or descriptors than actually have elements defined. When the DNP client requests the prototype or descriptor definition, the DNP server then responds with a property error because it doesn't have definitions for all of them.

Solution:
1. Either define the data set descriptors in the DNP server or disabled the Data Set property in Tag Import.
2. Correct the DNP server so that it reports the actual number of prototypes and descriptors that have elements defined.

Data Set write of value <value to be written> pending on tag address <address> on device <device>.

Error Type:
Informational

Possible Cause:
A write occurred to a tag that references a data set element. The value is not displayed in the tag value, but is pending a write to the data set.

Solution:
The data set write is complete when a data set tag with the sub-type .Set has a Boolean True written to it.

Device <device> does not support the LAN Time Sync Style Record Current Time Function Code 24.

Error Type:
Warning

Possible Cause:

The device does not support function code 24 - LAN (which is the specified time synchronization method).

Solution:
In **Device Properties** | **Communications**, change the time synchronization setting to Serial.

Note:
Time synchronization is successful despite the error message. To prevent the error message from occurring, change the setting as described above.

Device <device> does not support the LAN Time Sync Style write to object group 50, variation 3.

Error Type:
Warning

Possible Cause:
The device does not support a write to object group 50, variation 3, which is used in the second part of the LAN time synchronization method.

Solution:
To prevent the error message from occurring, open **Device Properties** and then select the **Communications** tab. In **Time Sync Style**, select **Serial**.

Note:
Time synchronization is successful despite the error message.

Device <device> indicated an event buffer overflow (IIN 2.3).

Error Type:
Warning

Possible Cause:
A response from the device included IIN bytes along with the bit set, indicating that an event buffer overflow condition exists. At least one unconfirmed event was lost because the event buffers did not have enough room to store the information.

Solution:
1. If many events occur between event polls (and the bit is being set by the DNP server) decrease the event poll interval to keep the buffer size small.
2. To avoid logging unnecessary events, adjust the analog point deadband.

See Also:
Event Playback

Device <device> indicated it restarted (IIN 1.7).

Error Type:
Informational

Possible Cause:
A response from the device included IIN bytes along with the bit set. This indicates that the device restarted.

Solution:
N/A

Device <device> initialization completed.

Error Type:
Informational

Possible Cause:

1. The DNP client has successfully communicated with the device, and the following requests have successfully completed (if configured):
    - Integrity poll on restart.
    - Data set change on startup.
    - Enable unsolicited messages.
    - Disable unsolicited messages.
2. When this message repeats frequently in the Event Log, it indicates that the DNP client is repeatedly restarting. This may occur when channel serialization is in use, and the DNP client receives a request from the DNP server when it does not have the channel token. As such, the DNP server does not receive a response in the specified time and closes the socket.

Solution:

1. N/A
2. Determine why the DNP client is restarting, and then correct the setup. If it is because the DNP server is sending a request (such as a Link Status request, a Keep Alive request, or an unsolicited message) while channel serialization is in use, then the DNP server should be reconfigured to disable the requests or to increase the timeout (so it does not close the socket).

Device <device> requested time synchronization (IIN 1.4).

Error Type:
Informational

Possible Cause:
A response from the device included IIN bytes along with the bit set. This indicates that the device requires time synchronization from the DNP client.

Solution:
N/A

Device <device> is restarting.

Error Type:

Information

Possible Cause:
The client wrote a "1" to a Warmrestart or Coldrestart tag.

Solution:
N/A

Device <device name> is not responding.

Error Type:
Serious

Possible Cause:

1. The Ethernet connection between the device and the Host PC is broken.
2. The communications parameters for the Ethernet connection are incorrect.
3. The named device may have been assigned an incorrect network ID.
4. A device on the channel is unresponsive, due to improper timing settings or a broken communications link.
5. There are multiple channels using DNS host names that resolve to the same IP address.
6. The response from the device took longer to receive than the amount of time specified in the "Request Timeout" device setting.

Solution:

1. Verify the cabling between the DNP client and server device.
2. Verify that the specified communications parameters match those of the device.
3. Verify that the network ID given to the named device matches that of the actual device.
4. Locate the unresponsive device and then correct the timing settings or fix the broken communications link.
5. Ensure that all channels are using a unique Destination Host.
6. Increase the Request Timeout setting so that the entire response can be handled.

See Also:
Timing and Other Considerations
Communications

Failed to resolve destination host <host name> on channel <channel name>.

Error Type:
Fatal

Possible Cause:

The channel has been configured to use a DNS host name instead of an IP address. The server cannot resolve the host name to an IP address.

Solution:
Ensure that the outstation device is online and registered with the domain.

The Keep-Alive Interval with UDP Protocol on device <device> was overridden.

Error Type:
Warning

Possible Cause:
The XML project file contains a value for the Keep-Alive Interval that is not 0, and the channel protocol is set to UDP.

Solution:
Change the Keep-Alive Interval in the XML project to 0. Alternatively, change the channel protocol to TCP.

Reached max. events per point for object group <object group> point <data index> on device <device>.

Error Type:
Warning

Possible Cause:
At least one unconfirmed event was lost because the event buffers did not have enough room to store the information.

Reasons:
1. The value specified for the Max. Events Per Point parameter is too small to receive all of the events without discarding data.
2. The event poll intervals are too large.
3. The DNP server is logging unnecessary events (such as changes in a floating value).

Solution:
1. Determine the buffer size allowed in the DNP server, and then set the max. events per point parameter to the same value (or larger). This driver allows 10000 events per point. The default setting is 100.
2. If many events occur between event polls (and the max. events per point is reached) decrease the event poll interval to keep the buffer size small.
3. To avoid logging unnecessary events, adjust the analog point deadband.

See Also:
Event Playback

Request failed on device <device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:
The device returned IIN bytes in the response with the "Function code not supported" bit set. This indicates that the device does not support the function code sent by the DNP client in the request.

Solution:
In Channel Diagnostics, check the TX entry that has a similar timestamp as the error in the Event Log to determine which function code the device is not supporting. The solution depends on the function code.

Note:
For example, if the device should support the "Enable unsolicited responses" (0x14) function code or the "Disable unsolicited responses" (0x15) function code, correct the configuration in the device. If the device should not accept the function codes 0x14 or 0x15, change the Class 1, 2, and 3 Unsolicited Mode in device properties to Automatic. For more information on specific function code error messages, refer to **Error Descriptions**.

Request to enable unsolicited messaging failed on device <device>.

Error Type:
Warning

Possible Cause:
The device rejected a request to enable unsolicited messages on start.

1. The device may not be configured to allow the DNP client to modify its unsolicited settings.
2. There is an issue with the authentication settings.

Solution:
1. Check how unsolicited or spontaneous messaging is configured in the device. If it does not allow the DNP client to configure unsolicited settings, change the unsolicited modes for each class to Automatic in the DNP client's Unsolicited group in device properties.
2. Confirm that the authentication settings specified in the DNP client match those specified in the DNP server.

Unable to bind to local address (IP: xxx.xxx.xxx.xxx, Source Port: x).

Error Type:
Serious

Possible Cause:

1. More than one channel has been configured to use the same network adapter and source port.
2. Another application is running on the system that has already acquired the indicated network adapter and source port for exclusive use.

Solution:

1. Select a different local IP address or source port for one of the repeating channels. The computer may also need to be multi-homed.
2. Close the other application.

Unable to read point(s) <OBJ.VAR.IDX> on device <device>. Failed to initialize communication stack.

Error Type:
Fatal

Possible Cause:
The driver was unable to initialize the communication stack.

Solution:
Reinitialize the driver by right-clicking on the Administration menu and selecting **Reinitialize**. If the problem persists, restart the DNP client.

Unable to read point(s) <OBJ.VAR.IDX> on device <device>. Internal Error occurred.

Error Type:
Fatal

Possible Cause:
An internal error occurred within the driver.

Solution:
The driver may recover on its own. If the problem persists, restart the DNP client.

Unable to read point(s) <OBJ.VAR.IDX – OBJ.VAR.IDX> on device <device>. Failed to initialize communication stack.

Error Type:
Fatal

Possible Cause:
The driver was unable to initialize the communication stack.

Solution:
Reinitialize the driver by right-clicking on the Administration menu and selecting **Reinitialize**. If the problem persists, restart the DNP client.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Internal error occurred.

Error Type:
Fatal

Possible Cause:
An internal error occurred within the driver.

Solution:
The driver may recover on its own. If the problem persists, restart the DNP client.

Unable to read tag <tag address> on device <device>. Device indicates one or more exception conditions (DNP flags byte=<hexadecimal byte> - <DNP flag exception list).

Error Type:
Warning

Possible Cause:
The device returned the data point DNP flag byte with either the Online bit cleared or with one or more of the exception bits set.

Solution:
For a list of flag bits that are specific to the object group, refer to the "DNP Object Flag Definitions" subtopic located in the object group's address descriptions. For more information on a particular exception and how to clear it, refer to the device's documentation.

Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Error Type:
Warning

Possible Cause:

1. The response timeout is too short to allow the DNP server's integrity or event poll response to complete in time. The DNP server may be returning a large number of points, but the timeout elapsed before the data could be received.
2. There is an issue with the authentication settings.
3. The data set exchange objects 213 and 215 are unknown to the device during initialization, causing it to be unable to complete.
4. The connection between the device and the host PC was interrupted while receiving the response.

Solution:

1. If the DNP server has been configured to return a large number of points (such as during a class 0 poll) change the channel's Response Timeout to a value that allow the response to complete successfully.
2. Confirm that the authentication settings in the DNP client match those in the DNP server.
3. If data sets are not in use, disable the Exchange Data Sets property in the Advanced tab of device properties.
4. Verify the cabling between the DNP client and server device.

Notes:

1. The channel's response timeout should be as accurate as possible, because it is also the time that the driver waits before reporting that the device is not responding.
2. The device request timeout should be greater than the channel response timeout.

See Also:

Timing and Other Considerations
Communications

Unable to write to address <address> on device <device>. Failed to initialize communication stack.

Error Type:

Fatal

Possible Cause:

The driver was unable to initialize the communication stack.

Solution:

Reinitialize the driver by right-clicking on the Administration menu and selecting **Reinitialize**. If the problem persists, restart the DNP client.

Unable to write to address <address> on device <device>. Internal error occurred.

Error Type:

Fatal

Possible Cause:

An internal error occurred within the driver.

Solution:

The driver may recover on its own. If the problem persists, restart the DNP client.

Write complete to data set <index> on device <device>.

Error Type:

Informational

Possible Cause:
A Data Set tag with the sub-type .Set had a Boolean True written to it while pending writes existed.

Solution:
The pending data set writes have been sent to the device, although they may not have been successful.

Note:
This message indicates that the write completed and the pending data has been cleared.

Driver Messages
The following messages may be generated. Click on the link for a description of the message.

Winsock initialization failed (OS error = n).
Winsock shut down failed (OS error = n).
Winsock V1.1 or higher must be installed to use the driver.

Winsock initialization failed (OS Error = n).
Error Type:
Fatal

OS Error Code	Indication	Possible Solution
10091	Indicates that the underlying network subsystem is not ready for network communication.	Wait a few seconds and restart the driver.
10067	Limit on the number of tasks supported by the Windows Sockets implementation has been reached.	Close one or more applications that may be using Winsock and restart the driver.

Winsock shutdown failed (OS Error = n).
Error Type:
Fatal

OS Error Code	Possible Solution
10036	The network subsystem is still busy with unfinished processing. Wait a few seconds and restart the driver.
10050	The network subsystem has failed. For more information, contact the network administrator.
10093	The network subsystem was not initialized before the shutdown was attempted. Wait a few seconds and try again.

Winsock V1.1 or higher must be installed to use the driver.
Error Type:

Fatal

Possible Cause:

The version number of the Winsock DLL found on the system is less than 1.1.

Solution:

Upgrade Winsock to version 1.1 or higher.

DNP-Specific Messages

The following messages may be generated. Click on the link for a description of the message.

Read Errors
Write Errors

Read Errors

The following error/warning messages may be generated. Click on the link for a description of the message.

The returned value for tag address <tag address> in device <device name> has a length of zero. The tag value cannot be set.
The returned value of <date returned value> for tag address <address> in device <device> is invalid for the <data type> tag.
The returned value of <returned numeric value> for tag address <address> in device <device> is invalid for the <data type> tag data type.
The returned value of <returned numeric value> for tag address <address> in device <device> is out of range for the <data type> tag data type.
The returned value of <returned string value> for tag address <address> in device <device> is invalid for the <data type> tag data type.
Unable to read point(s) <OBJVAR.IDX> on device <device>. An abnormal condition exists in the device (IIN1.6).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device detected corrupt configuration (IIN2.5).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device does not support the function code (IIN2.0).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device reports that some output points are in local mode (IIN1.5).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Device reports that the operation is already executing (IIN2.4).
Unable to read point(s) <OBJVAR.IDX> on device <device>. Session shutting down or duplicate request.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Unrecognized object returned in response.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. An abnormal condition exists in the device (IIN1.6).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device detected corrupt configuration (IIN2.5).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support the function code (IIN2.0).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device reports that the operation is already executing (IIN2.4).

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Session shutting down or duplicate request.

Unable to read point(s) <OBJVAR.IDX - OBJVAR.IDX> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Unrecognized object returned in response.

Unable to read set <set index> of object group <object group> on device <device>. An abnormal condition exists in the device (IIN1.6).

Unable to read set <set index> of object group <object group> on device <device>. Device detected corrupt configuration (IIN2.5).

Unable to read set <set index> of object group <object group> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Unable to read set <set index> of object group <object group> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Unable to read set <set index> of object group <object group> on device <device>. Device does not support the function code (IIN2.0).

Unable to read set <set index> of object group <object group> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Unable to read set <set index> of object group <object group> on device <device>. Device reports that the operation is already executing (IIN2.4).

Unable to read set <set index> of object group <object group> on device <device>. Session shutting down or duplicate request.

Unable to read set <set index> of object group <object group> on device <device>. Unrecognized object returned in response.

Unable to read tag address <address> on device <device>. Element Index <variation> is not defined in data set <index>.
Unable to read tag address <address> on device <device>. No definition for Data Set <index>.
Unable to read tag address <address> on device <device>. Response missing data.

The returned value for tag address <tag address> in device <device name> has a length of zero. The tag value cannot be set.

Error Type:
Warning

Possible Cause:
The tag has addressed an element that has been defined in the DNP server with a data length of zero.

Solution:
Increase the data length to an appropriate value for the data type.

The returned value of <date returned value> for tag address <address> in device <device> is invalid for the <data type> tag data type.

Error Type:
Warning

Possible Cause:
The device has configured the device attribute variation or data set element as a Date value, but the tag's data type is not Date.

Solution:
Change the tag's data type to Date.

The returned value of <returned numeric value> for tag address <address> in device <device> is invalid for the <data type> tag data type.

Error Type:
Warning

Possible Cause:
The device has configured the device attribute variation or data set element as a numeric value, but the tag's data type is String.

Solution:
Change the tag's data type to the appropriate numeric type.

The returned value of <returned numeric value> for tag address <address> in device <device> is out of range for the <data type> tag data type.

Error Type:
Warning

Possible Cause:
The device has configured the device attribute variation or data set element as a data type that is out of range for the data type of the tag.

Solution:
Change the tag's data type to match the data type configured in the DNP server.

The returned value of <returned string value> for tag address <address> in device <device> is invalid for the <data type> tag data type.

Error Type:
Warning

Possible Cause:
The device has configured the device attribute variation or data set element as a string, but the tag's data type is numeric.

Solution:
Change the tag's data type to string.

Unable to read point(s) <OBJVAR.IDX> on device <device>. An abnormal condition exists in the device (IIN1.6).

Error Type:
Warning

Possible Cause:
An abnormal condition has occurred that is specific to the device.

Solution:
Resolve any hardware issues found in the DNP server.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Device detected corrupt configuration (IIN2.5).

Error Type:
Warning

Possible Cause:
The device has detected that its configuration is corrupt.

Solution:
Reconfigure the DNP server.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Error Type:
Warning

Possible Cause:

1. The device does not support a point in the specified range.
2. The device does not understand the parameters sent in the request.

Solution:
Change the point(s) to one supported by the DNP server.

Unable to read point(s) <OBJ.VAR.IDX> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Error Type:
Warning

Possible Cause:
The device does not support the requested operation for the objects in the request.

Solution:
Verify that the DNP server supports the requested operation.

Unable to read point(s) <OBJ.VAR.IDX> on device <device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:
The device does not support the function code.

Solution:
None.

Note:
For more information, refer to the device's documentation.

Unable to read point(s) <OBJ.VAR.IDX> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Error Type:
Warning

Possible Cause:
Some output points are in local mode.

Solution:
Correct the mode in the DNP server's configuration.

Note:
For more information, refer to the device's documentation.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Device reports that the operation is already executing (IIN2.4).

Error Type:
Warning

Possible Cause:
The specified point is being acted upon by another client.

Solution:

1. Stop the other client from acting upon the points.
2. Delay the operation of the points.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Session shutting down or duplicate request.

Error Type:
Warning

Possible Cause:
The client disconnected while a transaction was in progress.

Solution:
Confirm that the connection between the DNP client and server is okay.

Unable to read point(s) <OBJVAR.IDX> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Error Type:
Warning

Possible Cause:

1. The response timeout is too short to allow the read to complete in time. The DNP server may have returned a large number of points in the response, but the timeout elapsed before the data was received.
2. There is an issue with the authentication settings.

Solution:

1. If the DNP server is returning a large number of points in the response, change the channel's Response Timeout to a value that allows the response to complete successfully.
2. Confirm that the authentication settings in the DNP client match those in the DNP server.

Notes:

1. The channel's response timeout should be as accurate as possible, because it is also the time that the driver waits before reporting that the device is not responding.
2. The device's request timeout should be greater than the channel's response timeout.

See Also:
Timing and Other Considerations
Communications

Unable to read point(s) <OBJVAR.IDX> on device <device>. Unrecognized object returned in response.

Error Type:
Warning

Possible Cause:
The response from the DNP server contains something that is unrecognized. This does not include function codes or objects, which have their own error messages. For more information, refer to the list below.

1. The qualifier may be incorrect or unsupported.
2. The length of the response may not match the length that was expected.
3. For object group 87 - data sets reads, this error may mean that more elements are in the data set than are allowed.

Solution:
1. Review the channel diagnostics to find which qualifier is being used in the response from the DNP server. Then, check the object's implementation table to see if that qualifier is supported. If it is not, determine whether the DNP server can be configured to use a supported qualifier for the object or function code.
2. Review the channel diagnostics to find if the length reported in the response matches the number of bytes actually sent from the DNP server or if the checksum was calculated correctly. Then, determine whether a faulty connection is causing the missing bytes and correct as necessary.
3. If the tag is a data set tag of object group 87 and the data set has more than 32 elements, reduce the number of elements in the data set on the DNP server.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. An abnormal condition exists in the device (IIN1.6).

Error Type:
Warning

Possible Cause:
An abnormal condition has occurred that is specific to the device.

Solution:
Resolve any hardware issues found in the DNP server.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device detected corrupt configuration (IIN2.5).

Error Type:
Warning

Possible Cause:
The device has detected that its configuration is corrupt.

Solution:
Reconfigure the DNP server.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Error Type:
Warning

Possible Cause:

1. The device does not support a point in the specified range.
2. The device does not understand the parameters sent in the request.

Solution:
Change the points to ones supported by the DNP server.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Error Type:
Warning

Possible Cause:
The device does not support the requested operation for the objects in the request.

Solution:
Verify that the DNP server supports the requested operation.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:
The device does not support the function code.

Solution:
None.

Note:
For more information, refer to the device's documentation.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Error Type:
Warning

Possible Cause:
Some output points are in local mode.

Solution:
Correct the mode in the DNP server's configuration.

Note:
For more information, refer to the device's documentation.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Device reports that the operation is already executing (IIN2.4).

Error Type:
Warning

Possible Cause:
The specified points are being acted upon by another client.

Solution:

1. Stop the other client from acting upon the points.
2. Delay the operation of the points.

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Session shutting down or duplicate request.

Error Type:
Warning

Possible Cause:
The client disconnected while a transaction was in progress.

Solution:
Confirm that the connection between the DNP client and server is okay.

Unable to read point(s) <OBJVAR.IDX - OBJVAR.IDX> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Error Type:
Warning

Possible Cause:
1. The Response Timeout is too short to allow the read to complete in time. The DNP server may have returned a large number of points in the response, but the timeout elapsed before the data was received.
2. There is an issue with the authentication settings.

Solution:
1. If the DNP server is returning a large number of points in the response, change the channel's response timeout to a value that allows the response to complete successfully.
2. Confirm that the authentication settings in the DNP client match those in the DNP server.

Notes:
1. The channel's response timeout should be as accurate as possible, because it is also the time that the driver waits before reporting that the device is not responding.
2. The device's request timeout should be greater than the channel's response timeout.

See Also:
Timing and Other Considerations
Communications

Unable to read point(s) <OBJVAR.IDX – OBJVAR.IDX> on device <device>. Unrecognized object returned in response.

Error Type:
Warning

Possible Cause:
The DNP server does not support the read request.

Solution:
Change the request to one supported by the DNP server.

Unable to read set <set index> of object group <object group> on device <device>. An abnormal condition exists in the device (IIN1.6).

Error Type:
Warning

Possible Cause:
An abnormal condition has occurred that is specific to the device.

Solution:
Resolve any hardware issues found in the DNP server.

Unable to read set <set index> of object group <object group> on device <device>. Device detected corrupt configuration (IIN2.5).

Error Type:
Warning

Possible Cause:
The device has detected that its configuration is corrupt.

Solution:
Reconfigure the DNP server.

Unable to read set <set index> of object group <object group> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Error Type:
Warning

Possible Cause:

1. The device does not support a point in the specified range.
2. The device does not understand the parameters sent in the request.

Solution:
Change the points to one supported by the DNP server.

Unable to read set <set index> of object group <object group> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Error Type:
Warning

Possible Cause:
The device does not support the requested operation for the objects in the request.

Solution:
Verify that the DNP server supports the requested operation.

Unable to read set <set index> of object group <object group> on device <device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:

The device does not support the function code.

Solution:
None.

Note:
For more information, refer to the device's documentation.

Unable to read set <set index> of object group <object group> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Error Type:
Warning

Possible Cause:
Some output points are in local mode.

Solution:
Correct the mode in the DNP server's configuration.

Note:
For more information, refer to the device's documentation.

Unable to read set <set index> of object group <object group> on device <device>. Device reports that the operation is already executing (IIN2.4).

Error Type:
Warning

Possible Cause:
The specified point is being acted upon by another client.

Solution:

1. Stop the other client from acting upon the points.
2. Delay the operation of the points.

Unable to read set <set index> of object group <object group> on device <device>. Session shutting down or duplicate request.

Error Type:
Warning

Possible Cause:
The client disconnected while a transaction was in progress.

Solution:
Confirm that the connection between the DNP client and server is okay.

Unable to read set <set index> of object group <object group> on device <device>. Unrecognized object returned in response.

Error Type:
Warning

Possible Cause:
The response from the DNP server contains something that is unrecognized. This does not include function codes or objects, which have their own error messages. For more information, refer to the list below.

1. The qualifier may be incorrect or unsupported.
2. The length of the response may not match the length that was expected.
3. For object group 87 - Data Sets reads, this error may mean that more elements are in the data set than are allowed.

Solution:

1. Review the channel diagnostics to find which qualifier is being used in the response from the DNP server. Then, check the object's implementation table to see if that qualifier is supported. If it is not, determine whether the DNP server can be configured to use a supported qualifier for the object or function code.
2. Review the channel diagnostics to find if the length reported in the response matches the number of bytes actually sent from the DNP server, or if the checksum was calculated correctly. Then, determine whether a faulty connection is causing the missing bytes and correct as necessary.
3. If the tag is a data set tag of object group 87 and the data set has more than 32 elements, reduce the number of elements in the data set on the DNP server.

Unable to read tag address <address> on device <device>. Element index <variation> is not defined in data set <index>.

Error Type:
Warning

Possible Cause:
The DNP server does not define this element index within the data set.

Solution:

1. If the element index should be defined, correct the data set in the DNP server.
2. If the element index is invalid, correct the tag address in the project.

Unable to read tag address <address> on device <device>. No definition for data set <index>.

Error Type:
Warning

Possible Cause:

1. A data set definition does not exist for the data set index of the .Value tag being read.
2. A data set exchange took place between the DNP client and server. A new data set was then added in the DNP server unknown to the DNP client.

Solution:

1. Create the data set in the DNP server.
2. Initiate a data set exchange. To do so, click **Device Properties** | **Tag Import** and select **Import Tags**. Alternatively, restart the DNP client.

Unable to read tag address <address> on device <device>. Response missing data.

Error Type:
Warning

Possible Cause:
Although the response from the DNP server indicated success, data for one or more points in the requested range was not included in the response.

Solution:
Confirm that the points are enabled in the DNP server.

Note:
For example, if the tag references object group 87 - data sets, confirm that all data set elements are configured in the DNP server with the correct data type and length and that the data set characteristics are correctly configured.

Write Errors

The following error/warning messages may be generated. Click on the link for a description of the message.

Unable to write to address <address> on device <device>. Activate configuration-related status code <status code> - <description>.
Unable to write to address <address> on device <device>. An abnormal condition exists in the device (IIN1.6).
Unable to write to address <address> on device <device>. Channel response timeout must be between <min channel response timeout> and <max. channel response timeout>.
Unable to write to address <address> on device <device>. Control-related status code <status code>
Unable to write to address <address> on device <device>. Destination <destination host>:<destination port> already in use on channel <channel>.
Unable to write to address <address> on device <device>. Destination port must be between <min. source port> and <max. source port>.

Unable to write to address <address> on device <device>. Device detected corrupt configuration (IIN2.5).
Unable to write to address <address> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).
Unable to write to address <address> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).
Unable to write to address <address> on device <device>. Device does not support the function code (IIN2.0).
Unable to write to address <address> on device <device>. Device reports that some output points are in local mode (IIN1.5).
Unable to write to address <address> on device <device>. Device reports that the operation is already executing (IIN2.4).
Unable to write to address <address> on device <device>. Device request timeout must be between <min value> and <max. value>.
Unable to write to address <address> on device <device>. Element index <variation> is not defined in data set <index>.
Unable to write to address <address> on device <device>. Event poll interval must be between <min. value> and <max. value>.
Unable to write to address <address> on device <device>. File name writes have been disabled.
Unable to write to address <address> on device <device>. Integrity poll interval must be between <min. value> and <max. value>.
Unable to write to address <address> on device <device>. DNP client address <DNP address> already in use as DNP server address on device <device>.
Unable to write to address <address> on device <device>. DNP client address must be between <min DNP address> and <max. DNP address>.
Unable to write to address <address> on device <device>. DNP client and server address cannot be the same.
Unable to write to address <address> on device <device>. No definition for data set <index>.
Unable to write to address <address> on device <device>. Protocol must be between <min protocol> and <max. protocol>.
Unable to write to address <address> on device <device>. Select operate response invalid.
Unable to write to address <address> on device <device>. Session shutting down or duplicate request.
Unable to write to address <address> on device <device>. DNP server address <DNP address> already in use on device <device>.
Unable to write to address <address> on device <device>. DNP server address must be between <min DNP address> and <max. DNP address>.
Unable to write to address <address> on device <device>. Source port must be between <min source port> and <max. source port>.
Unable to write to address <address> on device <device>. Tag <data type> data type is incompatible with the data set element <data type> data type.

Unable to write to address <address> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.
Unable to write to address <address> on device <device>. Unrecognized object returned in Response.
Unable to write to address <address> on device <device>. Unsupported operation type.
Unable to write to address <address> on device <device>. Unsupported trip-close code.
Unable to write to address <address> on device <device>. Write value specified is invalid or incomplete.

Unable to write to address <address> on device <device>. Activate configuration-related status code <status code> - <description>.

Error Type:
Warning

Possible Cause:
The Activate Configuration Request that was sent to the DNP server contained an invalid object or specification string.

Solution:
For information on a specific status code, refer to the table below.

Status Code	Description
0	No errors were detected in the corresponding request object. No errors were detected in the configuration data referenced by the corresponding request object.
1	An error was detected in the request object. For example, the DNP server was unable to locate a file referenced by a g70 file specification string, or the DNP server does not have a name referenced by a g110 octet string.
2	An error was detected in the configuration data referenced by the corresponding request data.
3	An error occurred that is not listed above.
4	The Activate Config object was not checked for errors.

Unable to write to address <address> on device <device>. An abnormal condition exists in the device (IIN1.6).

Error Type:
Warning

Possible Cause:
An abnormal condition has occurred that is specific to the device.

Solution:
Resolve any hardware issues found in the DNP server.

Unable to write to address <address> on device <device>. Channel response timeout must be between <min channel response timeout> and <max. channel response timeout>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the channel response timeout range of 100 to 3600000 milliseconds.

Unable to write to address <address> on device <device>. Control-related status code <status code>.

Error Type:
Warning

Possible Cause:

1. The value written to the .Operate sub-type was not understood by the DNP server.
2. If the operate was successful but the feedback poll failed, the device reports status code 4.

Solution:
For information on a specific code number, refer to the table below.

Code Number	Identifier Name	Description
0	Success	Request accepted, initiated, or queued.
1	Timeout	Request not accepted because the operate message was received after the arm timer timed out. The arm timer was started when the select operation for the same point was received.
2	No_Select	Request not accepted because no previous matching select request exists. An operate message was sent to activate an output that was not previously armed with a matching select message.
3	Format_ Error	Request not accepted because there were formatting errors in the control request (either select, operate, or direct operate).
4	Not_Sup-ported	1. Request not accepted because a control operation is not supported for this point. 2. The device does not understand the feedback poll request for the latest value of all objects of an object group.
5	Already_Act-ive	Request not accepted because the control queue is full (or the point is already active).
6	Hardware_ Error	Request not accepted because of control hardware problems.
7	Local	Request not accepted because the Local/Remote switch is in the Local position.

Code Number	Identifier Name	Description
8	Too_Many_Objs	Request not accepted because too many objects appeared in the same request.
9	Not_Authorized	Request not accepted because of insufficient authorization.
10	Automation_Inhibit	Request not accepted because it was prevented or inhibited by a local automation process.
11	Processing_Limited	Request not accepted because the device cannot process any more activities than are presently in progress.
12	Out_Of_Range	Request not accepted because the value is outside the acceptable range permitted for this point.
13 to 125	Reserved	Reserved for future use.
126	Non_Participating	Sent in request messages indicating that the outstation neither issues nor performs the control operation.
127	Undefined	Request not accepted due to an undefined reason.

Unable to write to address <address> on device <device>. Destination <destination host >:<destination port> already in use on channel <channel>.

Error Type:
Warning

Possible Cause:
The destination host and the destination port specified are already in use.

Solution:
Make sure that each channel in the server project has a unique destination host and destination port combination.

Unable to write to address <address> on device <device>. Destination port must be between <min. source port> and <max. source port>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the Destination Port range of 1 to 65535.

Unable to write to address <address> on device <device>. Device detected corrupt configuration (IIN2.5).

Error Type:
Warning

Possible Cause:
The device has detected that its configuration is corrupt.

Solution:
Reconfigure the DNP server.

Unable to write to address <address> on device <device>. Device does not support a point in the range or other parameter error (IIN2.2).

Error Type:
Warning

Possible Cause:

1. The device does not support a point in the specified range.
2. The device does not understand the parameters sent in the request.

Solution:
Change the tag address to one supported by the DNP server.

Unable to write to address <address> on device <device>. Device does not support requested operation for objects in the request (IIN2.1).

Error Type:
Warning

Possible Cause:
The device does not support the requested operation for the objects in the request.

Solution:
Verify that the DNP server supports the requested operation.

Unable to write to address <address> on device <device>. Device does not support the function code (IIN2.0).

Error Type:
Warning

Possible Cause:
The device does not support the function code.

Solution:
None.

Note:
For more information, refer to the device's documentation.

Unable to write to address <address> on device <device>. Device reports that some output points are in local mode (IIN1.5).

Error Type:
Warning

Possible Cause:
Some output points are in local mode.

Solution:
Correct the mode in the DNP server's configuration.

Note:
For more information, refer to the device's documentation.

Unable to write to address <address> on device <device>. Device reports that the operation is already executing (IIN2.4).

Error Type:
Warning

Possible Cause:
The specified address is being acted upon by another client.

Solution:

1. Stop the other client from acting upon the address.
2. Delay the operation of the address.

Unable to write to address <address> on device <device>. Device Request Timeout must be between <min. value> and <max. value>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the device request timeout range of 0 to 3600000 seconds.

Unable to write to address <address> on device <device>. Element index <variation> is not defined in data set <index>.

Error Type:
Warning

Possible Cause:
The DNP server does not define this element index within the data set.

Solution:

1. If the element index should be defined, correct the data set in the DNP server.
2. If the element index is invalid, correct the tag address in the project.

Unable to write to address <address> on device <device>. Event poll interval must be between <min. value> and <max. value>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the Event Poll Interval range of 0 to 86400 seconds.

Unable to write to address <address> on device <device>. File name writes have been disabled.

Error Type:
Warning

Possible Cause:
An attempt to modify the value of a 70.<index>.LocalFileName tag or 70.<index>.RemoteFileName tag failed because the File Name Writes property was disabled in File Control (located in device properties).

Solution:
Enable the File Name Writes property.

See Also:
File Control

Unable to write to address <address> on device <device>. Integrity poll interval must be between <min. value> and <max. value>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the Integrity Poll Interval range of 0 to 2592000 seconds.

Unable to write to address <address> on device <device>. DNP client address <DNP client address> already in use as DNP server address on device <device>.

Error Type:
Warning

Possible Cause:
The DNP client address is already in use as a DNP server address on another device.

Solution:
Specify a DNP client address that is unique among all DNP server addresses in the channel.

Unable to write to address <address> on device <device>. DNP client address must be between <min. DNP> and <max. DNP address>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the DNP client address range of 0 to 65519.

Unable to write to address <address> on device <device>. DNP client and DNP server address cannot be the same.

Error Type:
Warning

Possible Cause:
The DNP client and server address are the same.

Solution:
Specify unique values for the DNP client address and the DNP server address.

Unable to write to address <address> on device <device>. No definition for data set <index>.

Error Type:
Warning

Possible Cause:

1. A data set definition does not exist for the data set index of the write tag.
2. A data set exchange took place between the DNP client and server. A new data set was then added in the DNP server unknown to the DNP client.

Solution:

1. Create the data set in the DNP server.
2. Initiate a data set exchange. To do so, click **Device Properties** | **Tag Import** and then select **Import Tags**. Alternatively, restart the DNP client.

Unable to write to address <address> on device <device>. Protocol must be between <min. protocol> and <max. protocol>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value that is allowed.

Note:
The Protocol value is an enumerated type: a value of 0 corresponds to TCP/IP, and a value of 1 corresponds to UDP. No other values are allowed.

Unable to write to address <address> on device <device>. Select Operate response invalid.

Error Type:
Warning

Possible Cause:
The device did not return an acceptable response to a Select then Operate request.

Solution:
Verify that the DNP server is configured to operate on the point.

Unable to write to address <address> on device <device>. Session shutting down or duplicate request.

Error Type:
Warning

Possible Cause:
The client disconnected while a transaction was in progress.

Solution:
Confirm that the connection between the DNP client and server is okay.

Unable to write to address <address> on device <device>. DNP server address <DNP address> already in use on device <device>.

Error Type:

Warning

Possible Cause:
The DNP server address is already in use as a DNP client address or address on another device in the channel.

Solution:
Specify a DNP server address that is unique among all DNP client addresses and DNP server addresses in the channel.

Unable to write to address <address> on device <device>. DNP server address must be between <min. DNP address> and <max. DNP address>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the DNP server address range of 0 to 65519.

Unable to write to address <address> on device <device>. Source port must be between <min source port> and <max. source port>.

Error Type:
Warning

Possible Cause:
The value is out of range.

Solution:
Specify a value within the Source Port range of 0 to 65535.

Unable to write to address <address> on device <device>. Tag <data type> data type is incompatible with the data set element <data type> data type.

Error Type:
Warning

Possible Cause:

1. The value being written is incompatible with the definition of the data set for that element.
2. The value being written is less than the minimum value or greater than the maximum value that is allowed for the data type. This error may also be caused by a value of ±Infinity to ±NaN.

Solution:

1. Correct the tag's data type so that it matches the data type defined for the element in the data set.
2. Write a value that is within the valid range allowed for the data type.

Unable to write to address <address> on device <device>. Unable to receive response from device <device> within timeout. Either the request or response could not be completed or the response is invalid.

Error Type:
Warning

Possible Cause:
1. The Response Timeout is too short to allow the write to complete in time. The DNP server may have returned a large number of points in the feedback poll, but the timeout elapsed before the data was received.
2. There is an issue with the authentication settings.

Solution:
1. If the DNP server is returning a large number of points in the feedback poll, change the channel's Response Timeout to a value that allows the response to complete successfully.
2. Confirm that the authentication settings in the DNP client match those in the DNP server.

Notes:
1. The channel's Response Timeout should be as accurate as possible, because it is also the time that the driver waits before reporting that the device is not responding.
2. The device's Request Timeout should be greater than the channel's Response Timeout.

See Also:
Timing and Other Considerations
Communications

Unable to write to address <address> on device <device>. Unrecognized object returned in response.

Error Type:
Warning

Possible Cause:
The DNP server does not support the value being written to the object group.

Solution:
Change the value to one supported by the DNP server.

Unable to write to address <address> on device <device>. Unsupported Operation Type.

Error Type:
Fatal

Possible Cause:
An invalid DNP operation code was specified when writing to the .Operate.OpType tag.

Solution:
Correct the .Operate.OpType tags value.

Unable to write to address <address> on device <device>. Unsupported Trip-Close Code.

Error Type:
Fatal

Possible Cause:
An invalid DNP Trip-Close code was specified when writing to the .Operate.TripCloseCode tag.

Solution:
Correct the .Operate.TripCloseCode tag's value.

Unable to write to address <address> on device <device>. Write value specified is invalid or incomplete.

Error Type:
Warning

Possible Cause:

1. An invalid value was written to the Operate.Set, Operate, object group 60, Warmrestart, Coldrestart, ActivateConfig, or data set .Set tag.
2. An attempt to write a data set occurred when there was no pending data to be written.
3. An attempt to write a large data set caused the request message to surpass the maximum fragment size.
4. An attempt to send an Activate Configuration Request failed due to a syntax error.
5. An attempt to send an Activate Configuration Request failed due to a remote file identifier not defined at the 70.index.
6. An attempt to send an Activate Configuration Request failed due to a string not defined at 110.index.
7. An attempt to initiate a file transfer failed because a file transfer is already in progress on that device.

Solution:

1. Correct the value written to the Operate.Set, Operate, object group 60, Warmrestart, Coldrestart, or data set .Set tag.
2. Before writing a True to the data set .Set tag, write data to one or more elements of a data set.
3. Reduce the number of bytes being written to the data set.
4. Correct the Activate Config Objects string to a valid format: object.index, object.index, object.index, and so forth.
5. Fix the Activate Config Objects string file object 70.index if it is incorrect. If it is correct, then define the remote file and path at that index.
6. Fix the Activate Config Objects string object 110.index if it is incorrect. If it is correct, then create a tag with the address to that string index.
7. Wait for the file transfer in progress to complete before attempting another on the device.

Note:
The default maximum DNP client transmit fragment size is 2048 bytes.

File Control Messages

The following messages may be generated. Click on the link for a description of the message.

File Transfer failure on device <device> for file index <index>. Device returned file-related status code <status code> - <description>.
File Transfer failure on device <device> for file index <index>. File size of <size> kilobytes is greater than maximum file size of <maximum size> kilobytes.
File Transfer failure on device <device> for file index <index>. File transfer stopped by user.
File Transfer failure on device <device> for file index <index>. File transfer stopped due to communications issue.
File Transfer failure on device <device> for file index <index>. Local file <file name> is empty.
File Transfer failure on device <device> for file index <index>. Local file open failure. <local file open failure>.
File Transfer failure on device <device> for file index <index>. Session shutting down or duplicate request.
Invalid local file for file index 70.<file index>, general error.
Invalid local file for file index 70.<file index>, verify the specified path is write-enabled.
Invalid local file path for file index 70.<file index>.
Invalid local file syntax for file index 70.<file index>.

File Transfer failure on device <device> for file index <index>. Device returned File-Related Status Code <status code> - <description>.

Error Type:
Warning

Possible Cause:

The DNP server is reporting that an error occurred during a file transfer request from the DNP client.

Solution:

For information on a specific code number, refer to the table below.

Code Number	Identifier Name	Description
0	Success	The requested operation was successful.
1	Permission_ Denied	Permission was denied due to improper authentication key, user name, or password.
2	Invalid_ Mode	An unsupported or unknown operation mode was requested.
3	File_Not_ Found	The requested file does not exist. The path may be incorrect.
4	File_Locked	The requested file is already in use by another user.
5	Too_Many_ Open	File could not be opened because the number of simultaneously opened files would be exceeded.
6	Invalid_ Handle	There is no file opened with the handle in the request.
7	Write_ Block_Size	The outstation is unable to negotiate a suitable write block size.
8	Comm_Lost	Communications were lost or cannot be established with the end device where the file resides.
9	Cannot_ Cancel	A cancel request was unsuccessful because the DNP server is unable or not programmed to cancel, or the DNP server knows that cancelling the file would make it unusable.
10-15	Reserved	Reserved for future use.
16	Not_ Opened	File handle does not reference an opened file.
17	Handle_ Expired	File closed due to inactivity timeout. This code is sent in a file transport status event object (g70v6) when the timeout occurs.
18	Buffer_Over-run	Too much file data was received for the DNP server to process.
19	Fatal	An error happened in the file processing that prevents any further activity with this file.
20	Block_Seq	The block number did not have the expected sequence number.
21-254	Reserved	Reserved for future use.
255	Undefined	Some other error not listed above occurred.

File Transfer failure on device <device> for file index <index>. File size of <size> kilobytes is greater than maximum file size of <maximum size> kilobytes.

Error Type:

Warning

Possible Cause:
The file to be copied has a file size that exceeds the configured maximum file size for this file index.

Solution:
If the file size is expected, increase the maximum file size configured for that file index. If the file should not reach that size, determine the reason for its growth.

File Transfer failure on device <device> for file index <index>. File transfer stopped by user.

Error Type:
Warning

Possible Cause:
During a file transfer, the user wrote a 0 to the upload or download tag of the file index to stop the transfer.

Solution:
None.

File Transfer failure on device <device> for file index <index>. File transfer stopped due to communications issue.

Error Type:
Warning

Possible Cause:
The Ethernet connection between the device and the Host PC disconnected during a file transfer.

Solution:
Verify the cabling between the DNP client and server device.

File Transfer failure on device <device> for file index <index>. Local file <file name> is empty.

Error Type:
Warning

Possible Cause:
The file that is to be downloaded to the DNP server is empty.

Solution:
Determine why the file is empty. Then, correct it and re-attempt to download the file to the DNP server.

File Transfer failure on device <device> for file index <index>. Local file open failure. <local file open failure>.

Error Type:
Warning

Possible Cause:

1. File was not found.
2. Invalid or incorrect path.
3. Too many open files.
4. Access denied.
5. Disk is full.
6. An unspecified error occurred.

Solution:

1. If the Append option is desired, confirm that the file name and path are configured correctly. Otherwise, change the local file's Open Mode to Overwrite to create a new local file.
2. If the local path is invalid, correct it for the file index in File Control (located in device properties). If the path is incorrect (and the server_runtime is running as a service), then configure the server_runtime service with a non-system user account with the correct permissions.
3. The number of open files exceeds the maximum allowed. Determine what is causing the files to remain open.
4. The file could not be accessed. Correct the file's access rights.
5. The local disk is full. Free up some disk space.
6. Determine the problem with the file or path name.

File Transfer failure on device <device> for file index <index>. Session shutting down or duplicate request.

Error Type:
Warning

Possible Cause:
The device disconnected while a transaction was in progress.

Solution:
Confirm that the connection between the DNP client and server is okay.

Invalid local file for file index 70.<file index>, general error.

Error Type:
Warning

Possible Cause:
The specified Local File Identifier is invalid. The error is unspecified.

Solution:

1. Specify a new local file path and/or name with read/write privileges.
2. If this is a network drive, verify that both the current user and the user associated with the service have read/write privileges.

Invalid Local File for File Index 70.<file index>, verify the specified path is write-enabled.

Error Type:
Warning

Possible Cause:
The current user does not have Read/Write privileges to the specified Local File Identifier.

Solution:
Verify that the current user (or the user associated with the service) has Read/Write privileges to the specified file and folders.

Invalid Local File path for File Index 70.<file index>.

Error Type:
Warning

Possible Cause:
The Local File Identifier (which consists of the Local File Path and Name) does not include a valid path to the file.

Solution:
Verify the file name's directory/folder hierarchy. The specified file is created at runtime (excluding its path) if it does not already exist.

Invalid Local File syntax for File Index 70.<file index>.

Error Type:
Warning

Possible Cause:

1. The Local File Identifier (which consists of the Local File Path and Name) contains one or more invalid characters (such as | ?'* :<>).
2. The Local File Identifier contains the parent directory (denoted by '..'), which is not permitted for security purposes.

Solution:

1. Verify that the specified Local File Identifier does not contain invalid characters.
2. Verify that the specified Local File Identifier does not contain the parent directory.

Index

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W