

Web Configuration Guide



Contents

Introduction.....	5
Welcome	5
Web Configuration Basics	5
Accessing Web Configuration	6
Alarms	7
Reports	10
Administration	13
Help.....	14
Breadcrumbs.....	14
Administration Menu	14
Configuration Backup	15
Scheduled Backup	17
Create All .vi Files	19
Alarm Notification Properties	20
Custom Audible Alarm Notification Sounds	20
Start Database.....	21
Stop Database	22
Check Database	23
Fix Database	24
SQL Server Properties	26
Local Server List Menu.....	28
Start Server Configuration.....	29
End Server Configuration	31
Start New Log File	32
Install Devices From List	33
Update Devices From List.....	38
Add Remote	41
Copy for WebViews.....	44
Restart WebViews	45
Restart Server	46
Restart Windows.....	47
Add Note	48
Get Log File	49
Upload Files	50
Open Older Log File.....	52

Open Saved Wiretap	55
Properties	58
Remote Server List Menu	59
Connect Remote	60
Disconnect Remote	61
Delete Remote	61
Copy for WebViews.....	64
Restart Remote App	65
Restart Remote OS	66
Add Note	67
Get Updates.....	68
Get Log File	69
Upload Files	71
Download Backup.....	72
Synchronize Redundant.....	74
Properties	76
Device List Menu.....	77
Enable.....	77
Disable.....	78
Disarm	79
Re-Arm.....	81
Add User-Defined Channel.....	83
Delete	85
Rename	87
Copy for WebViews.....	88
Copy Channel Properties.....	89
Paste Channel Properties	90
Create .vi File	91
Load Driver	92
Unload Driver	94
Properties	96
Channel List Menu.....	100
Enable.....	100
Disable.....	103
Disarm / Rearm.....	105
Re-Arm.....	107

Delete	109
Rename	109
Copy for WebViews.....	110
Copy Channel Properties.....	110
Paste Channel Properties	111
Properties	112
WebViews Menu	115
New Folder.....	115
Delete	116
Cut.....	117
Copy.....	118
Paste	119
Rename	120
Create Single Page / Create Pages for Tree	121
Create Page From Template / Create Tree from Templates	123
Create Single Template / Create Templates for Tree	127
Check Files for Page	129
Check Files for Tree	130
Properties	131
WebViews Channel List Menu	132
Delete	133
Copy for WebViews.....	133

Introduction

The Foreseer Web Configuration utility is a browser-based utility used to manage your:

- Servers
- Devices
- Channels
- WebViews
- WebViews Channel Lists
- Database
- Alarms
- Reports

Welcome

Welcome to the Foreseer Web Configuration Utility Guide. You can use the Foreseer Web Configuration Utility to:

- Restart the WebViews server, the Foreseer Server, or the server machine.
- Manage Foreseer alarms.
- Run Foreseer reports.
- Start, stop, and repair the database.
- Populate and edit the WebViews tree and assign devices and channels to various WebViews pages.
- Delete Devices.
- Disable and enable Device Channels.
- Configure Channel properties.
- Add Remote Servers; including Data Acquisition Engine (DAE) appliances, and a Secondary Redundant Foreseer Server.

The following chapters outline how to access the Web Configuration Utility and how use it to configure Foreseer.

Web Configuration Basics

This section provides information on the basic functionality of the Web Configuration environment.

- Accessing Web Configuration
- Alarms
- Reports
- Breadcrumbs
- Help

Accessing Web Configuration

To access the Web Configuration Application, you must:

- Have a user account that is a member of the PXSauthAPPADMIN Windows user group.

To access the Web Configuration Application, use one of the following browsers:

- Internet Explorer 11 - 11.1451.16299.0 or later
- Safari - 12.0.3 (14606.4.5) or later
 - macOS minimum requirement – macOS 10.14 Mojave and later
- Chrome – 78.0.3904.97 or later
- Edge – 44.17763.831.0 or later

You can access the Web Configuration Utility at the following URL:

<https://machine/WebConf/>.

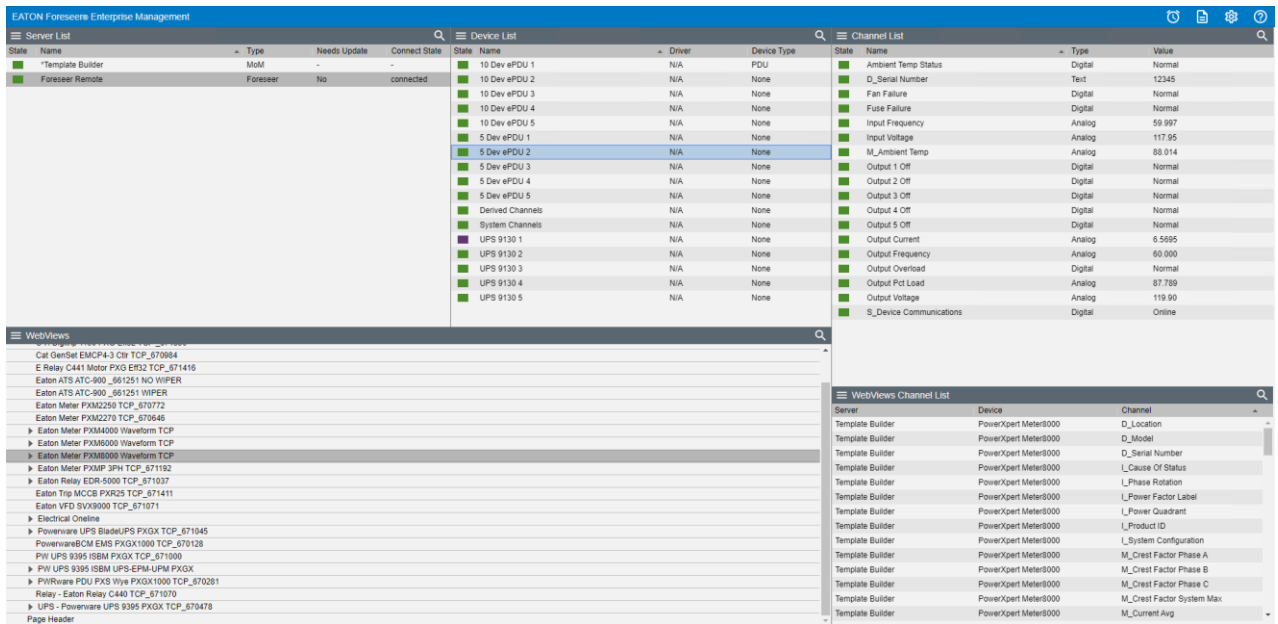
- ✔ Your browser may need to be configured to accept cookies from Foreseer. Please consult documentation for your browser or contact your organization's IT department for assistance.

Where machine is either the machine name or IP address of the machine on which Foreseer is installed. When accessing the web page, you may be challenged to provide your user ID and password.

- ✔ By default, the port for WebConfig is either 443 (HTTPS) or 80 (HTTP). By default, HTTP is not enabled.

<https://machine/webconf/>

When you access the Web Configuration Utility, you'll see something similar to the following:



Alarms

You can access the Alarm Management feature by clicking on the Alarm icon in the main header of WebConfig.



The Alarm Management features consist of the following:

- Multiple alarm selection using familiar Ctrl-click and Shift-click selection
- Optionally display Disabled and Enabled objects
- Displays a Device object when the Device is Disabled or Enabled
- When a Device object is displayed, the Device can be Enabled or Armed with one action
- Alarm list can be sorted by clicking any of the header categories in descending or ascending order
- Overall look can be changed using Themes or individual items such as background color
- Alarm Management can be displayed as a separate Window (the default) or a Dialog
- Alarm list updates can be temporarily suspended by pressing and holding the Ctrl or Shift keys
- Alarm list data columns can be sorted by simply clicking the data column heading
- Alarm list can be filtered by using the Filter icon from the toolbar.
- Select columns can be shown or hidden using the Show / Hide Columns feature from the toolbar.

The Alarm Management page displays objects that are currently in an alarm state (Critical, Caution and Acknowledged) in a list view style window. The top row of the list is column headers which can be clicked to sort the list by that category. The default sort order is descending (A to Z or 0 to 9). Clicking on the selected column toggles between descending

and ascending (Z to A or 9 to 0) sort order. When a new column is selected by clicking on the column header, it always starts with descending sort order.

State	Server	Device	Channel	Priority	Date/Time	Alarm Value	Current Value	Device Type	Location	Alarm Group
■	Foreseer Remote	UPS 9130 1	M_Ambient Temp	9999	12-04-2019 15:37:46	86.73	86.326	NONE	NONE	NONE
■	Foreseer Remote	UPS 9130 1	M_Output Current	9999	12-04-2019 15:39:52	11.62	12.874	NONE	NONE	NONE
■	Template Builder	PowerXpert Meter8000	M_Current Avg Demand	9999	12-04-2019 15:40:06	96.73	96.787	NONE	NONE	NONE
■	Template Builder	PowerXpert Meter8000	S_Discrete Input 8	9999	12-04-2019 15:40:29	Normal	Normal	NONE	NONE	NONE
■	Template Builder	PowerXpert Meter8000	M_Crest Factor Phase C	9999	12-04-2019 15:39:47	1.43	1.4482	NONE	NONE	NONE
■	Template Builder	PowerXpert Meter8000	M_Crest Factor Phase A	9999	12-04-2019 15:39:43	1.39	1.4455	NONE	NONE	NONE

In addition to active alarms, Disabled and Disarmed objects can optionally be included. To include these objects, click the Show menu and select Show Disabled (or Disarmed) to include them in the list. To return to not display them, select Hide Disabled (or Disarmed) from the menu.

Alarm Actions can be performed on selected objects from the Alarm Actions dialog box. To display the Alarm Details dialog box, select View Details from the Actions menu. A double-click will also display the dialog for a single object. With a single object selected, the top part of the dialog has a field for entering a note and the Alarm Actions buttons. The lower part displays details about the selected object. For multiple selections, the lower part is replaced with a list of the selected object names (e.g. //server-name/device-name/channel-name). The Action Buttons are:

- Acknowledge to acknowledge a Critical or Cautionary alarm.
- Re-Arm to return an acknowledged or disarmed object to the Normal state.
- Ack & Rearm to perform an Acknowledge and Rearm in one operation,
- Enable to return a disabled object to the Normal state.
- Open in WebViews to bring of the Web View that contains the alarm.

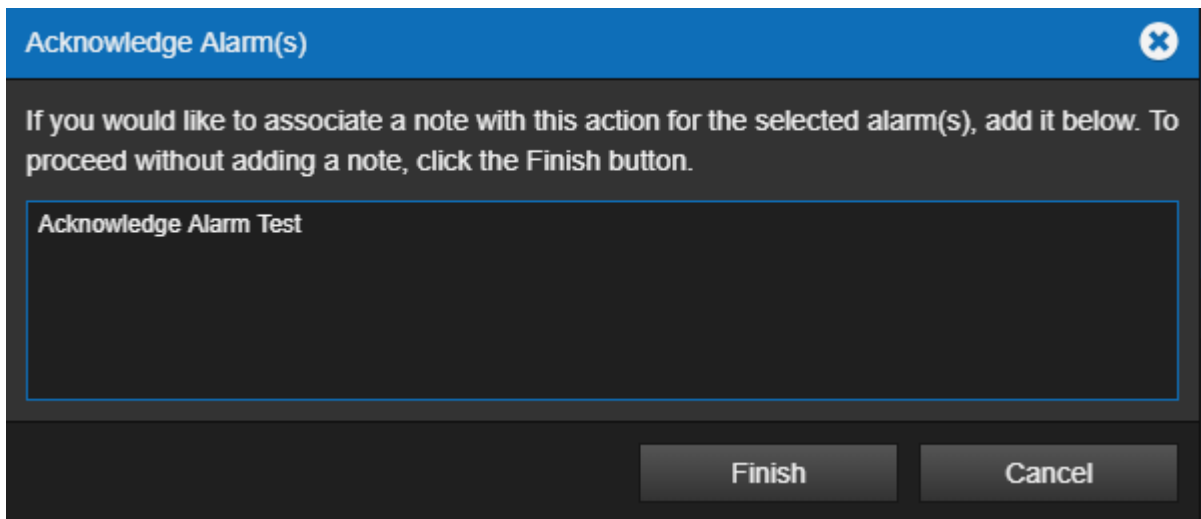
The Note field allows comments to be included about the Action. When an Action is performed, a Note is always entered into the database. The Note has two parts: the system and user parts. The system part is always entered and includes the object name, the Action name, the user name, the IP address where the action originated, and the time of the Action. The user part of the Note is the comment entered in the Note field. This part of the Note is meant for a brief (256 or less characters) comment about the reason for the Action. When multiple alarms are selected, the comment part is entered for each selected item; the object name in the system part of the Note is the only field that changes. The system part of the Note is not displayed and is always included and may not be modified.

Alarm Details
✕

Acknowledge
Re-Arm
Ack & Rearm
Enable
Open in WebViews

Channel:	M_Current Ground
Device:	PowerXpert Meter8000
Server:	Template Builder
Alarm State:	Caution
First Time:	11/19/19 11:26:41 AM
First Value:	0.00
Current Value:	0.0000
Priority:	9999
Message:	
Enter Note here...	
Notes	

Depending on the state of the object, some Actions may not be valid (e.g. an Acknowledged alarm cannot be Acknowledged). If an invalid Action is attempted, the server will reply with an Object State Conflict response. As the state of an object is dynamic, it's not always apparent if an Action is valid. An object may be acknowledgeable at the time it is selected, but it is possible that another user at a different workstation has acknowledged the alarm just before you. When multiple objects are selected and an invalid action results, a separate message will be displayed for each object that did not succeed. If this occurs, only the exceptions are displayed; all Actions that succeed do so silently. If in doubt, just review the current Alarm List or run a 1-Day Note Report to verify the Action. When running a Note Report, you may have to wait up to 15 seconds before the Action Note appears as the server buffers notes for efficiency.



Reports

Each Web Configuration page has a link to the report generator/manager.



Operators can generate and review reports about alarms, channels, system configuration, and server up time. Some Web Configuration Reports are available in two formats: standard and tab-delimited data. All reports can be exported as text files to the operator's local computer.

Reports			
Report Type	Available Reports		
Alarm History [1 Day]	10/16/19 11:37:02 [2538 bytes]		
Alarm History [30 Day]			
Alarm History [7 Day]			
Alarm History [Custom]			
Audit History			
Channel Data			
Channel	10/04/19 09:35:23 [322943 bytes]		
Driver Log File	10/04/19 09:34:17 [1244 bytes]		
Interval Data Report	10/04/19 09:38:14 [887 bytes]		
Log File	10/24/19 10:14:09 [4779 bytes]	10/23/19 11:06:42 [4392 bytes]	10/23/19 11:06:42 [4392 bytes]
Notes History [1 Day]	10/04/19 09:38:45 [390 bytes]		
Notes History [30 Day]			
Notes History [7 Day]			
Notes History [Custom]			
Previous Driver Log File			
Previous Log File			
Sequence of Events			
System Configuration	11/06/19 11:13:32 [1982 bytes]	11/06/19 11:10:33 [1939 bytes]	11/06/19 11:07:29 [3853 bytes]
System Up-Down			

To access report in the Web Configuration utility

1. Click on the Reports icon in the upper right menu.
2. Click one of the report buttons under Report Type.
3. When the report is generated, a link appears to the right of the button. Click the link to view the report in a separate browser window.

Foreseer provides the following reports:

- Alarm History (1 Day, 7 Days, or 30 Days) is a series of reports listing all alarms detected over the past day, week, month or specified time period. These three report formats consist of all alarm times, Devices and text recorded within the respective interval. If no alarms were detected during the period, that report will be blank. These are available in tabbed format.
- Alarm History (Custom) has a selection of time intervals and is similar to the other Alarm History reports except that it does not list alarms that are currently active or unacknowledged.
- Audit History (Custom) provides a history of configuration changes to the Foreseer System. This is not available as a tabbed report.
- Channel Data Report (30, 60, or 90 Day) provides minimum, maximum, and average values for each channel from the selected device over the selected time period. The default format is tab-delimited.
- Channel Report provides detailed information about each channel from each device installed in the "local" server. You can select an individual device if you wish. This report is available in tabbed format.
- Driver Log File report provides detailed information on the drivers in use by the Foreseer system.
- Interval Data Report provides users the ability to download raw historical data from the Foreseer databases in a standard CSV format.
- Log File reports all recorded events since the last Foreseer Server system reset. This report is not available in tabbed format.
- Previous Driver Log File report provides detailed information on the drivers previously in use by the Foreseer system.
- Previous Log File reports all events recorded in the previous Foreseer Server session. This report is not available in tabbed format.
- Notes History (1 Day, 7 Days, 30 Days, or Custom) reports notes logged over the last day, week, month, or specified time period. This report is available in tabbed format.
- Sequence of Events (custom) provides events logged by sequence of events recorders. This report provides a series of high-resolution (in time) events in time stamp order. The standard format is tab-delimited. For information about support for additional recording devices, contact the Power Systems Automation group at Eaton.
- System Configuration lists all configured devices, their operational parameters, and current device driver software version. The standard format is tab-delimited.
- System Up-Down reports each time the Web Server was launched and terminated. The default format is tab-delimited.

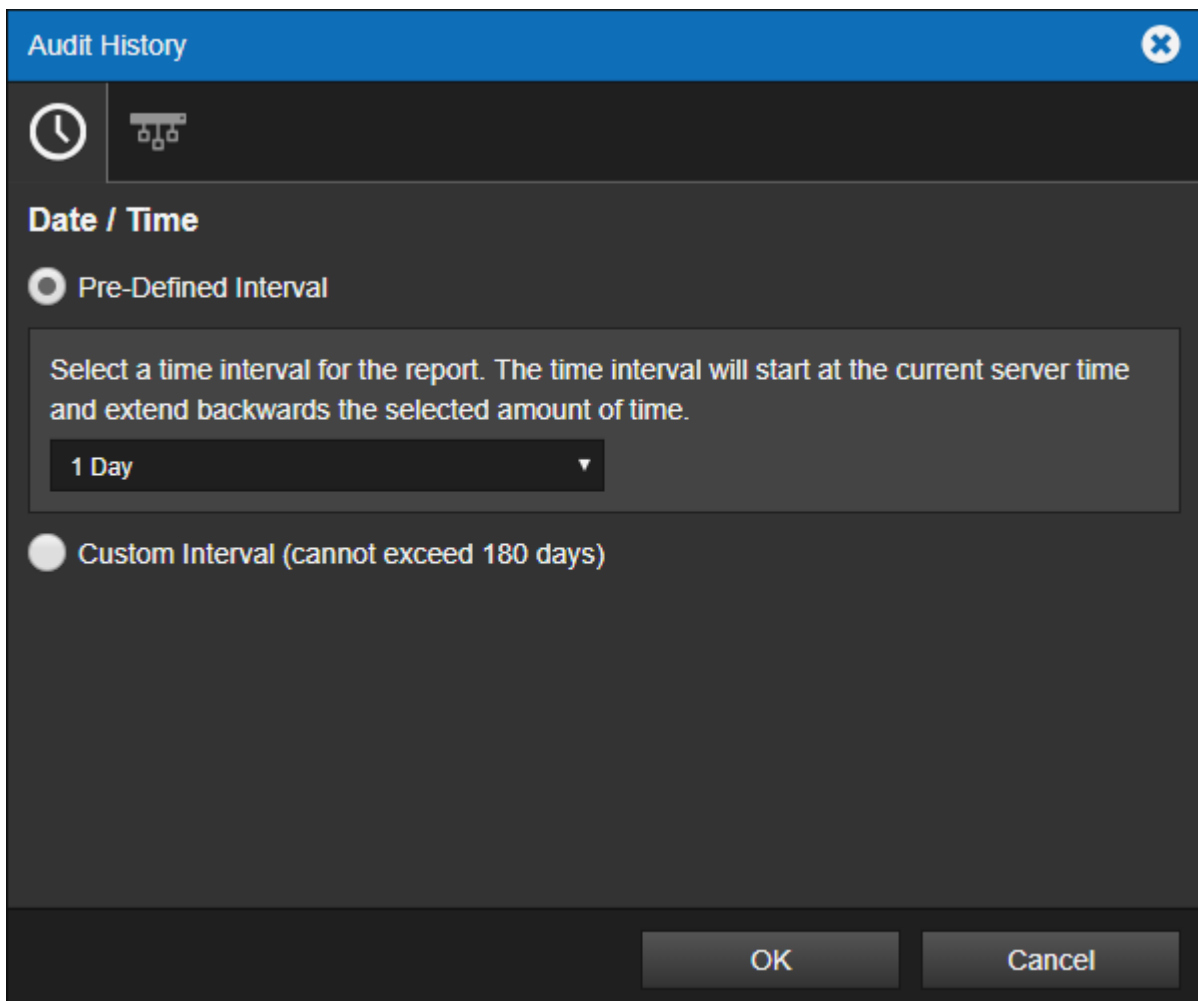
Custom Reports

Foreseer offers the ability to specify the range and content of the Custom Alarm, Audit and

Notes History Reports. Audit History reports Server, Device and Channel change information. All three report formats allow you to either set a predefined interval or enter a desired period over which the report is generated. You may also choose to include or exclude certain Devices or Channels. These output selections are presented when the chosen Custom Report is run.


To generate a Foreseer Custom Report:

1. Click the appropriate custom report button in the left pane. The appropriate Custom History dialog box is displayed divided into Date/Time and Advanced tabs. The tab contents, and the steps for specifying their parameters, are virtually identical for all three report formats



2. Indicate whether the Report will be for a Predefined Time Interval or over a Selected Time Range by clicking the corresponding button. Choosing the former requires that you select the Predefined Interval from the associated drop list. Using a Selected Time Range requires that you enter a Starting and Ending Date/Time to define the span. Any active alarms are always reported in the Alarm History Report using the Predefined Interval format, which always includes the current Server time as the Ending Time. In either case, the resulting Report Interval is calculated and shown.
3. With the reporting period defined, click on the Advanced tab to display those Custom Report parameters.

4. By default, all Devices and Channels are included in a Custom History report, although you can limit the data that is reported. Click the Include or the Exclude Device or Channel button, depending on the desired information, and the Select a Device or Channel dialog box is presented.
5. Expand the list under the appropriate Server to access its connected Devices and individual channels.
6. Highlight the desired Device(s) and/or channel(s) and click OK to add them to the Include or Exclude list. Entries can be made to both lists simultaneously. To remove an entry from either list, simply select it and press the Delete key. Deselect Include System Up/Down Notes in Report if you do not want this information in a Custom Notes History.
7. With the desired output criteria specified, click OK to run the Custom History report.
8. Click the link for the completed Report to display it.

 All active Foreseer alarms are included in the report regardless of the selected time range.

Custom Search Strings

The ability to perform specific text searches on Custom History files can be extremely useful in locating archived information about an event or piece of equipment.

To perform a custom search:

1. Click on the Include or Exclude String button in the Advanced Custom History dialog box as appropriate and a Custom Search String dialog box is displayed.
2. Enter the text string to be included or excluded in the field provided, using wild cards in most instances, and click OK to return to the Advanced Custom History dialog box. The entered string appears in the appropriate list box. You can repeat the procedure to add additional text strings to further refine your search criteria.
3. With the desired text string(s) entered, click OK to perform the specified search and a file is created containing the results.
4. Select the file from the Reports Available list and click Retrieve.
5. Save the file and the search results are displayed.

Administration

The administration icon displays the Administration sub-menu. Refer to the [Administration Menu](#) for more information. The administration icon displays the Administration sub-menu. You can enter create backups, set alarm properties as well as manage your database from this menu option.



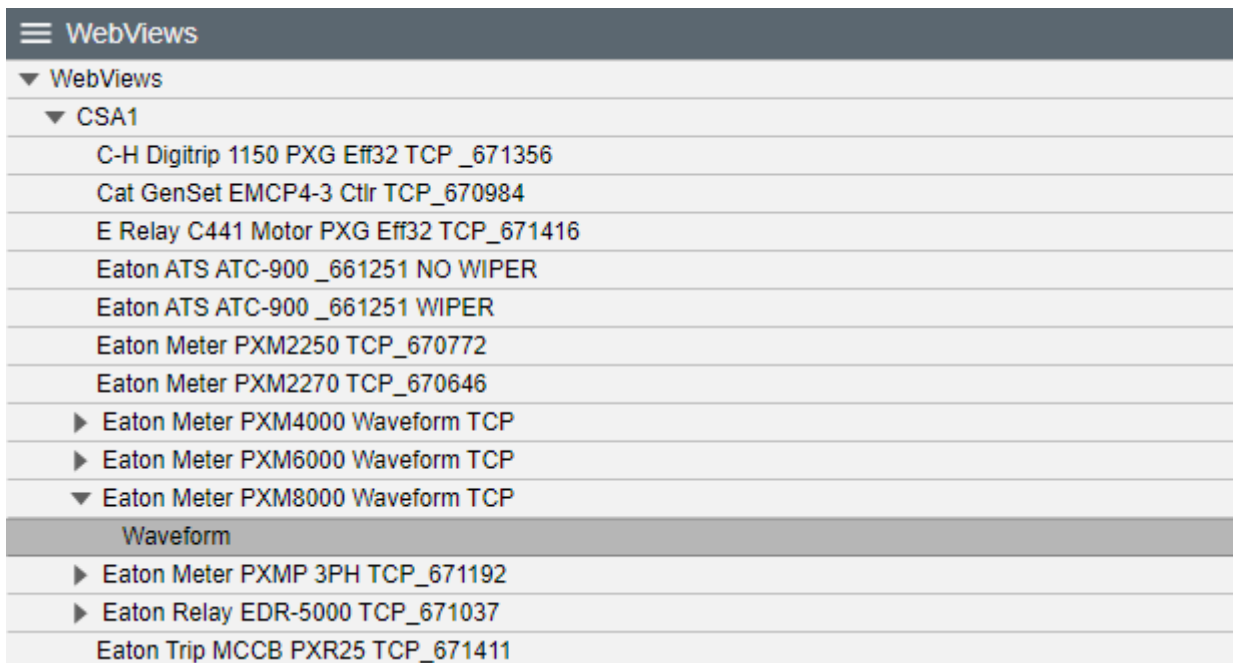
Help

Anytime you need help while using the Web Configuration Utility in Foreseer, you can select the question mark icon from the WebConfig menu.

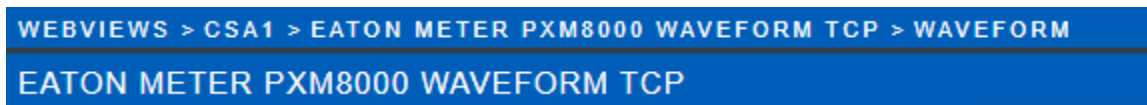


Breadcrumbs

Breadcrumbs tell operators where they are in the folder tree. WebViews pages are organized like file folders in your computer file system, which each folder representing a WebViews page. The following shows a simple structure with the "branch" of the "tree" leading from WebViews to a PXM 8000 waveform.



If an operator had navigated to the wave form page, the Breadcrumb would look like this:



In addition to providing a signpost for navigation, breadcrumbs also help operators in navigating through the system. All of the pages listed in the breadcrumb are hyperlinks, so clicking anything between WEBVIEWS and GENERATOR 1 will jump to that page.

Administration Menu

The Administration menu provides access to all of the common items used to manage your

Foreseer servers.

- Configuration Backup
- Scheduled Backup
- Create All .VI Files
- Start Database
- Stop Database
- Alarm Notification Properties
- Check Database
- Fix Database
- SQL Server Properties

Configuration Backup

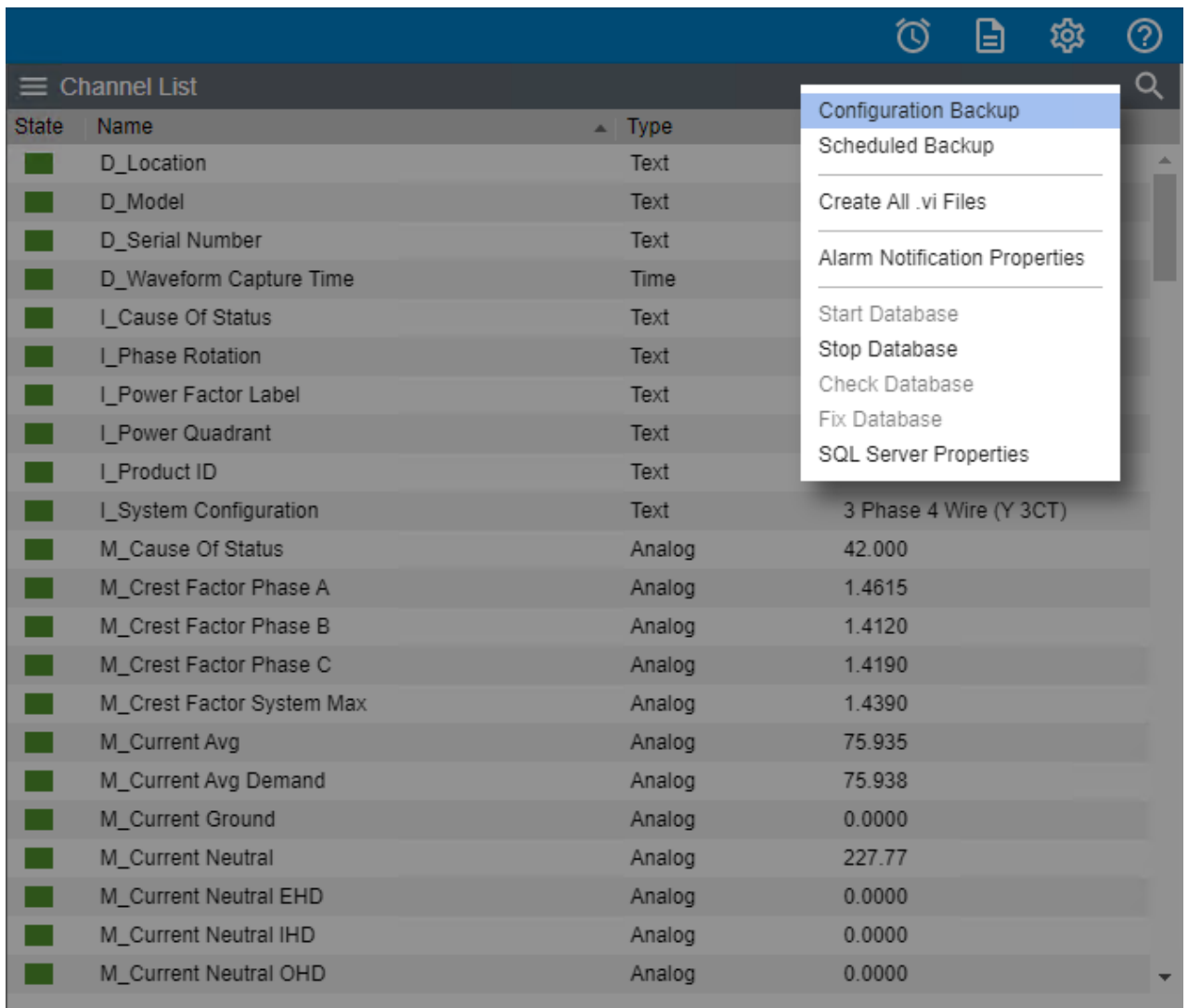
It is strongly recommended that a backup be performed after initial system configuration as well as before and after any significant modifications to ensure maximum disaster recovery capability. You must end server configuration mode before backing up the server configuration.

Significant changes are signaled via the Major Server Version System Channel.

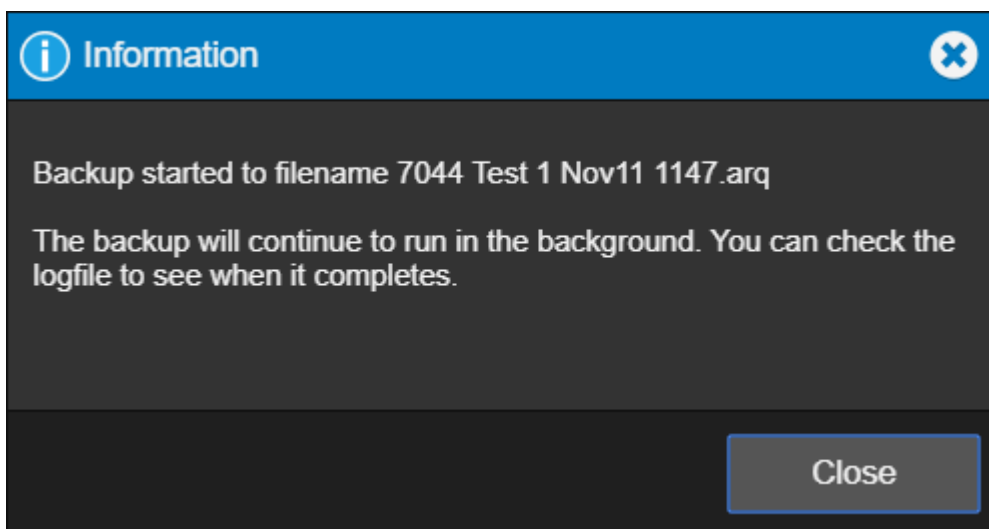
The backup archive (.ARQ) file includes the Foreseer Server configuration only, data files are not backed up in this procedure. Automatic configuration backups can be scheduled through the standalone Foreseer Configuration utility. Backups made through the Web Configuration Utility are automatically assigned a name which is a composite of the name of the server, the date, and the time (in 24-hour format).

To backup a Foreseer Server configuration:

1. Select Configuration Backup from the Configuration Menu.



- The utility reports back the name of the backup file in the Message from the web page alert box.



- The utility will report back the name of the backup file in the Message from the web page alert. In this example, the ARQ can be found in:

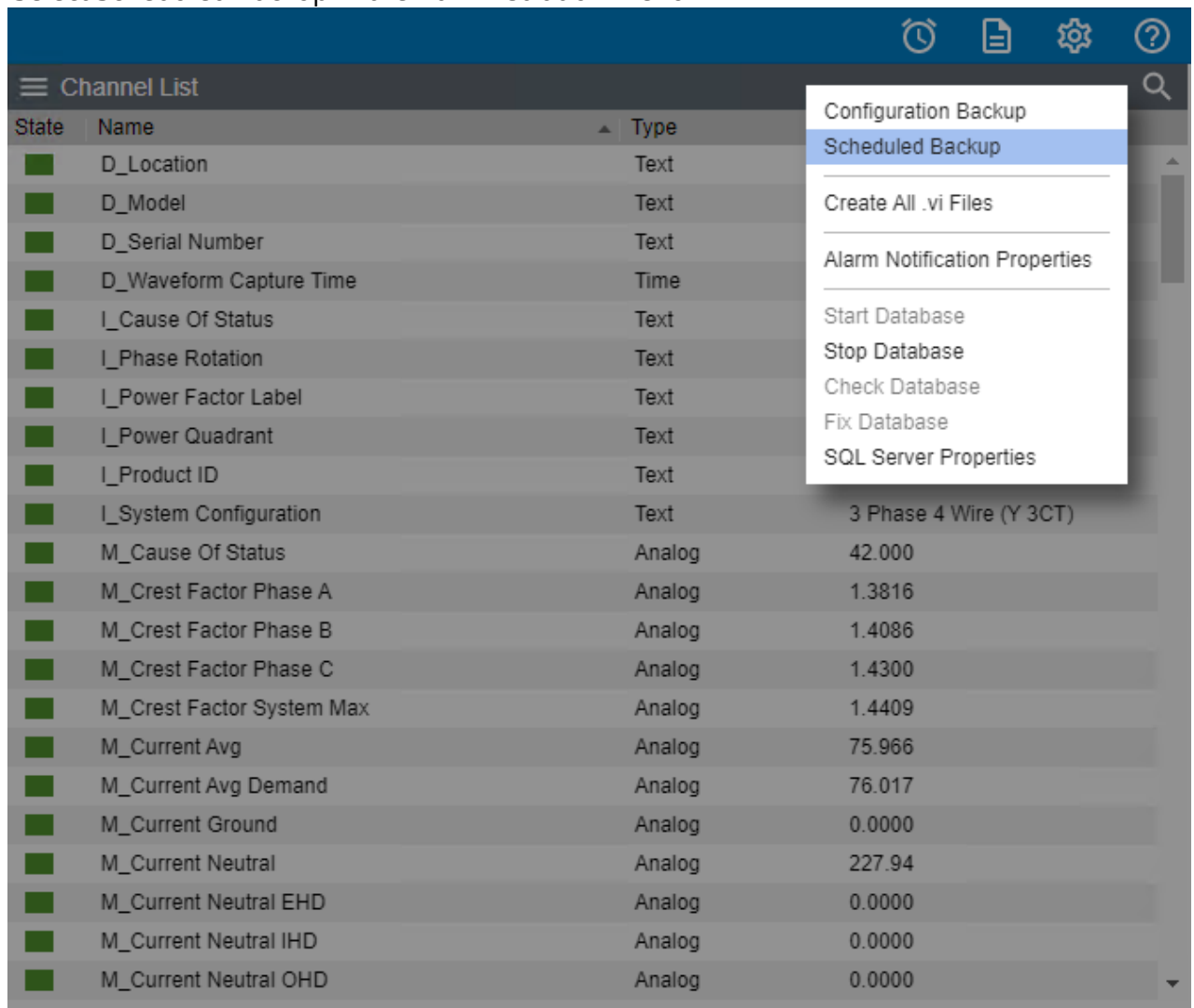
Scheduled Backup

You can schedule configuration backups automatically at specified intervals. A network drive is the recommended backup destination.

- ✓ Make certain that the user account used by Foreseer has Full Control permission for all the directories under the Foreseer installation directory. Otherwise, the backup process may fail.

To schedule regular backups:

1. Select Scheduled Backup in the Administration menu



2. The Scheduled Backup dialog is displayed.

✕
Scheduled Backup

Schedule a Configuration Backup to automatically start on the selected days at the specified time. The last "Days to Keep" backups will be retained. When the limit is reached, the oldest will be deleted when the next backup starts. The start time cannot be within 30 minutes of midnight. SQL Server backups must be scheduled separately using SQL Server Management Studio.

Backup Start Time (24 hour format)

Hour:

Minute:

Backup Days (at least one must be selected to enable backup)

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Backup Path:

Days to Keep:

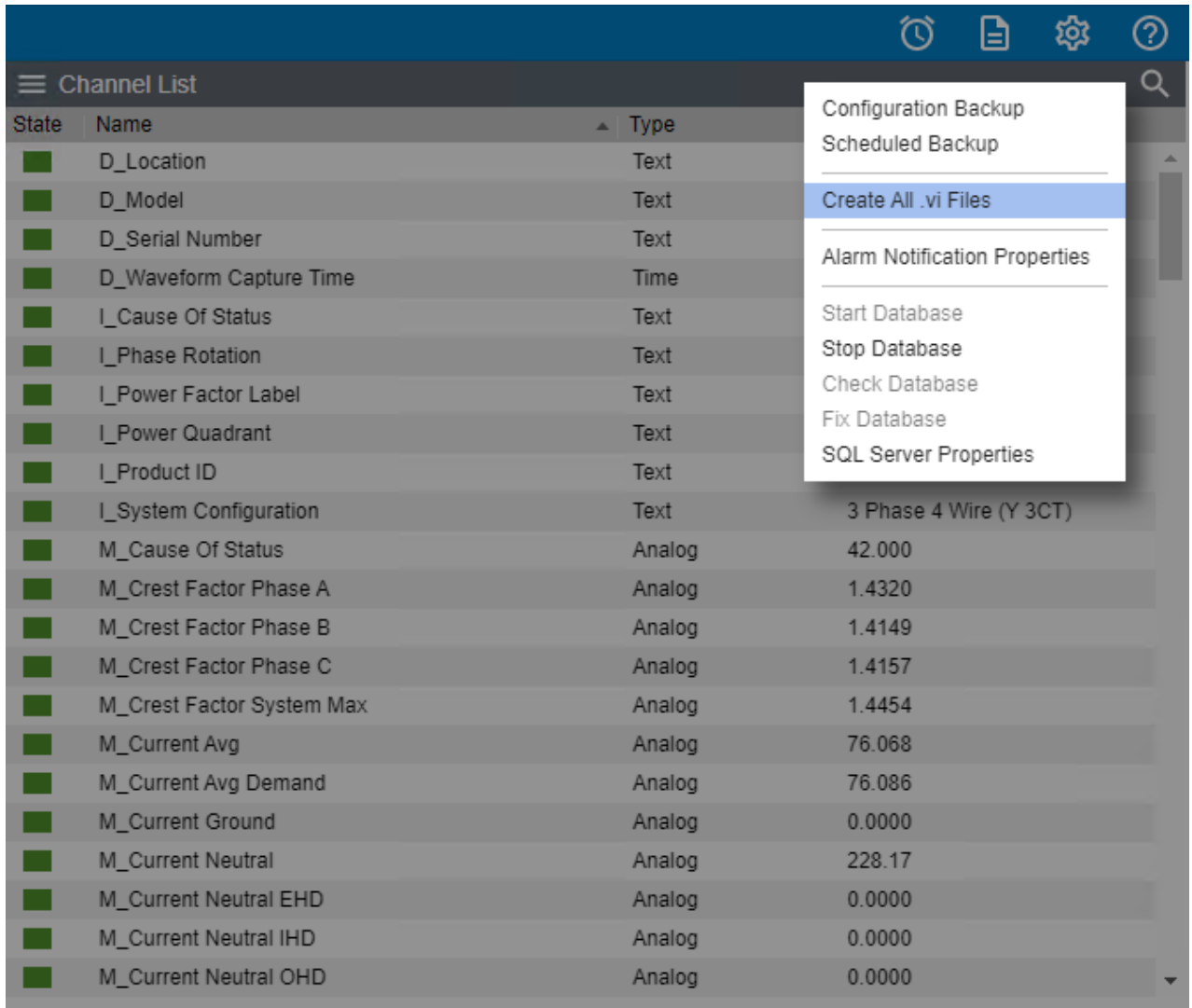
3. Specify when the backup is to be performed.
 - i. The Start Time is based on a 24- hour clock: for example, 5:00 p.m. is entered as "17:00." Note that the backup cannot occur within ten minutes of midnight and that there are restrictions based on the type of backup media. The Start Time plus the duration of the archive cannot extend through midnight if archiving to an external drive and it cannot be within the half hour preceding midnight if archiving to a remote network drive.
4. Check the Day(s) of the Week on which the backup is performed. Daily backups are strongly encouraged and recommended.
5. Enter or browse to the desired backup path.
6. You can adjust the maximum number of backups that are stored in the specified path.
7. Click OK to enable the displayed Data Backup settings. Archiving will be performed automatically at the scheduled time on the selected day(s).

Create All .vi Files

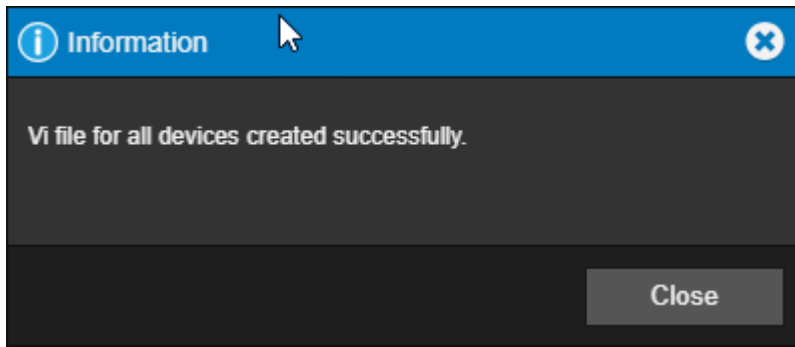
You can initiate the command to create all the .vi files for your configuration.

To Create All .vi files:

1. Select Create All .vi Files in the Administration menu

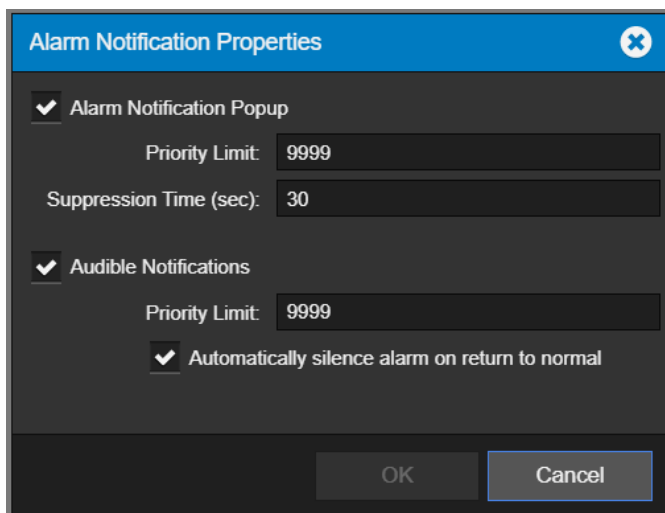


2. All of the defined .vi files in your system will be generated and named with the word Create added in the filename.
3. Upon successful completion, you will get the following dialog



Alarm Notification Properties

Alarm Notification Properties controls the behavior of the Alarm Notification pop-up dialog and audible notification when an alarm occurs during an active user session.



For the Alarm Notification Popup, you can enable (default setting) or disable the popup from appearing when an alarm occurs. You can also specify suppression time (in seconds) for displaying the popup, as well as specify the maximum alarm priority level that may trigger its appearance.

You can enable (default setting) or disable the audible notification from playing when an alarm occurs. Similar to the Alarm Notification Popup, you can specify a Priority Limit, and even toggle whether the audible notification should silence when an active alarm generates back to a normal state.

Custom Audible Alarm Notification Sounds

Audible Alarms, by default, use an alarm.mp3 file that is played when any alarm is generated in Foreseer. You may optionally add your own custom sounds into the system using either .wav or .mp3 sound files loaded into the WWW\Support\Sounds folder. These custom sounds will be used and adopted by all users of the system.


File names assigned to sound files must be in a format that links the file to a specific alarm priority. The file naming format is *Alarm_x.mp3* or *Alarm_x.wav*, where x is equal to a Foreseer Alarm Priority number ranging from 1 – 9999.

For example:

- If you want a particular sound to play when an alarm assigned with priority 1 occurs, the name of your file will be *Alarm_1.mp3* or *Alarm_1.wav*.
- If you want a particular sound to play when an alarm assigned with priority 2000 occurs, the name of your file will be *Alarm_2000.mp3* or *Alarm_2000.wav*.

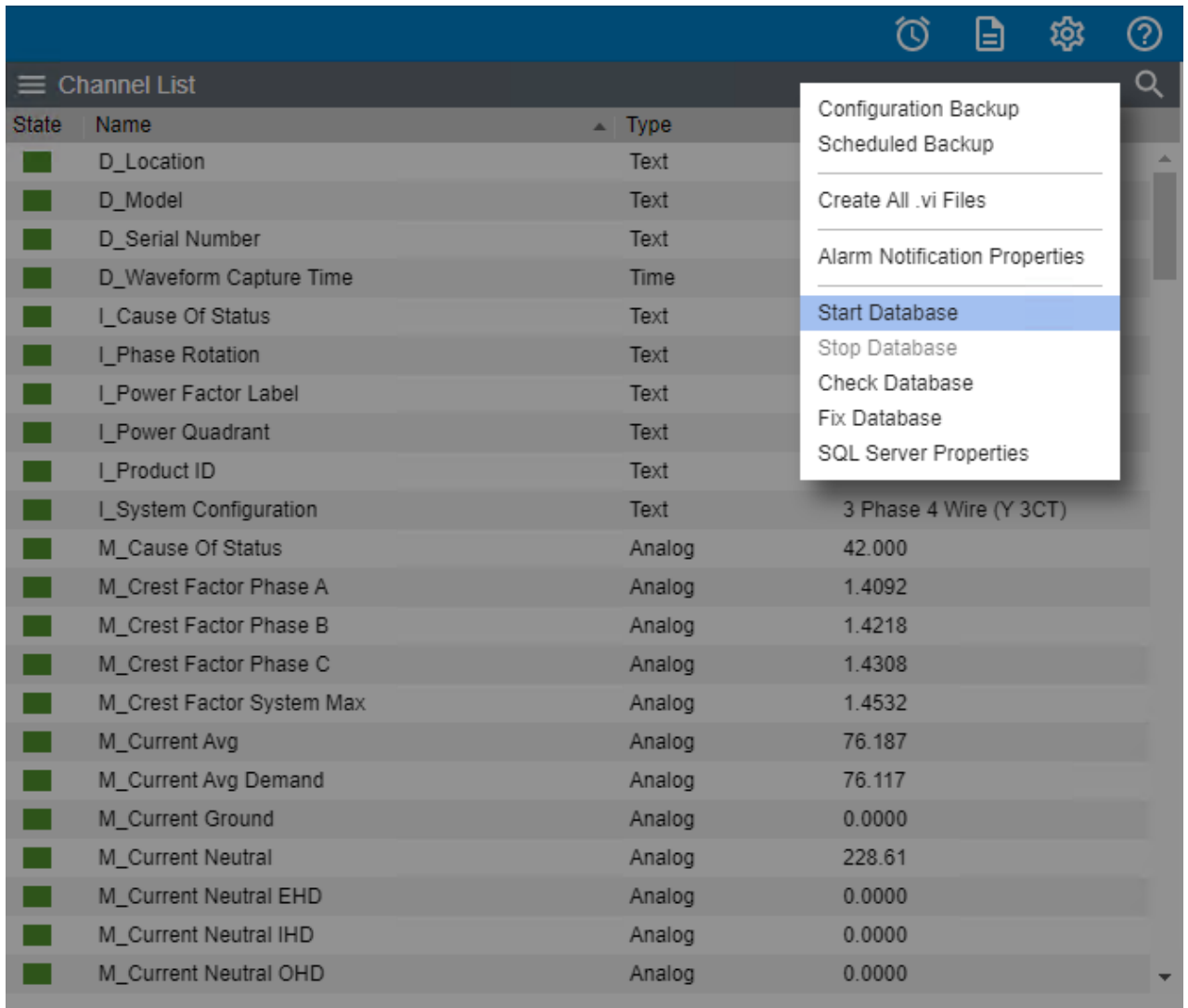
As you consider the potential to use custom sounds for different alarm priorities, make reasonable decisions on the length and content of files. For example:

- Sound files should be of a finite length and limited to sound effects.
- Bit-encoding should be of fidelity and quality for all users to understand.
- Refrain from using content that may be subject to copyright law.

 Internet Explorer 11 does not support the .wav file format.

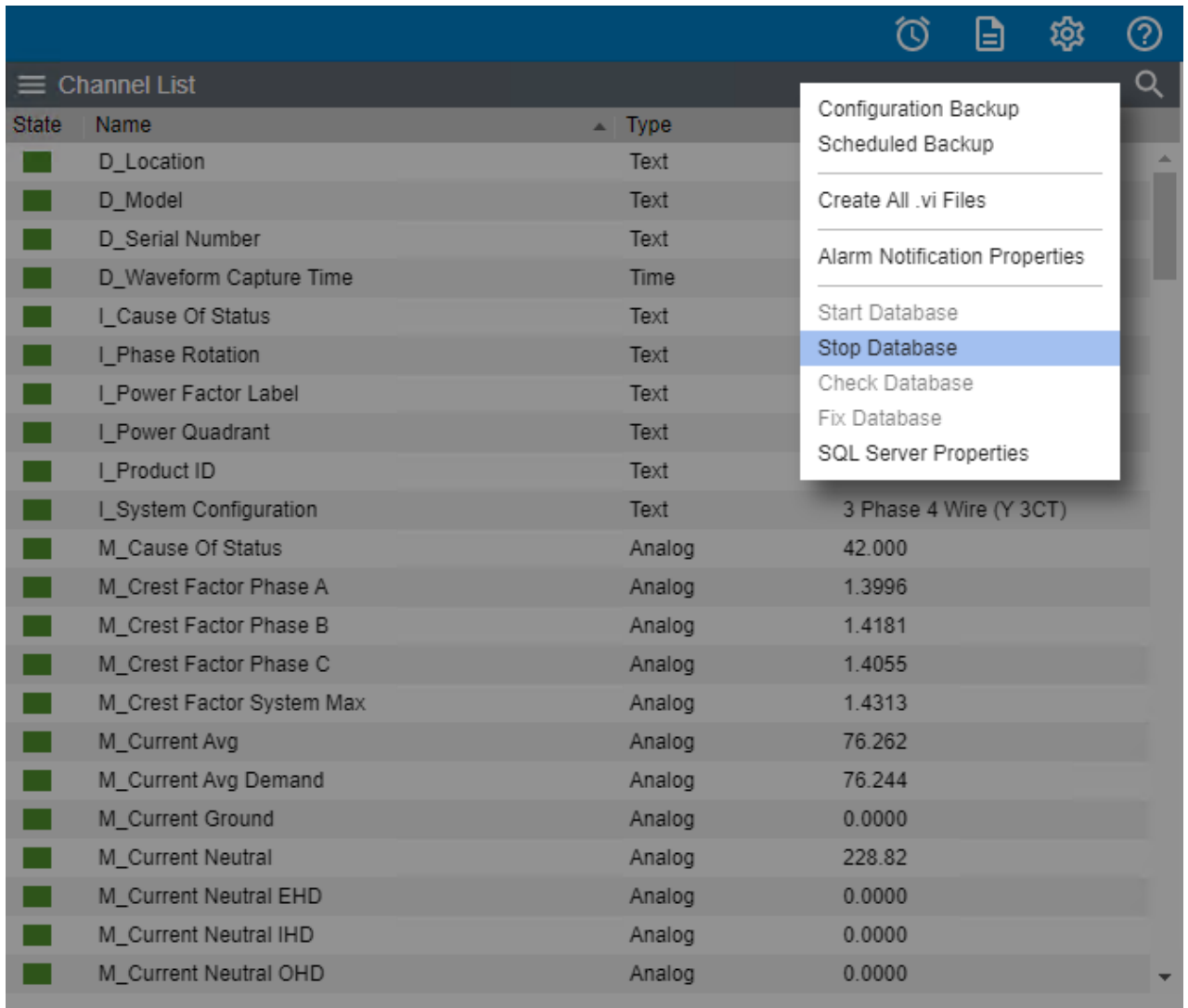
Start Database

Starts the Foreseer databases in SQL Server. You must stop the databases prior to running checking or fixing the databases.



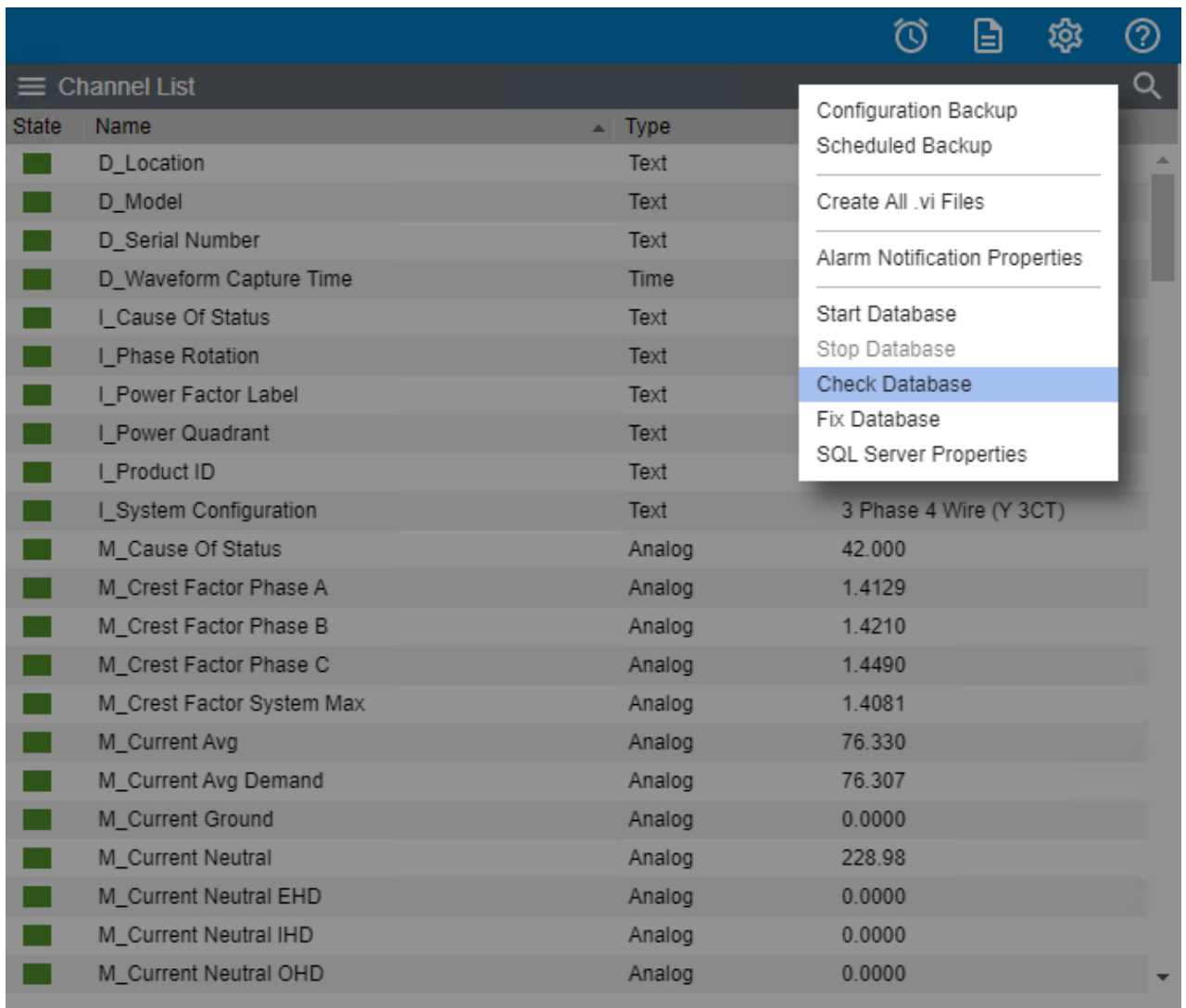
Stop Database

Stops the Foreseer databases in SQL Server. You must stop the databases prior to running checking or fixing the databases.

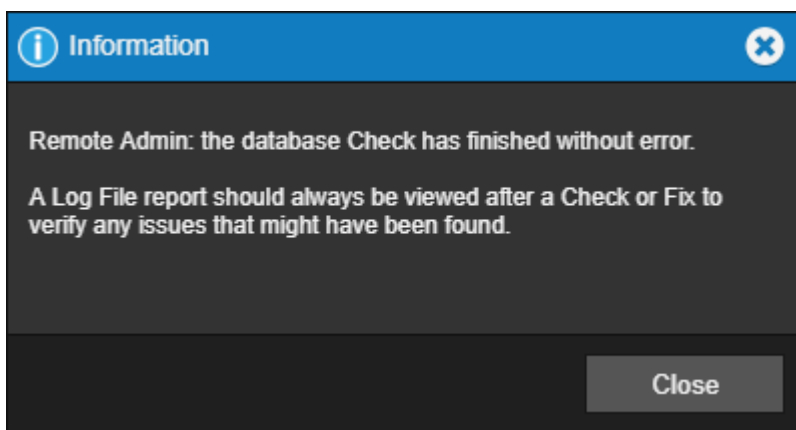


Check Database

Runs a cursory check of the Foreseer databases. This check verifies the schema, checks the channel map against the database, and verifies some of the tables.



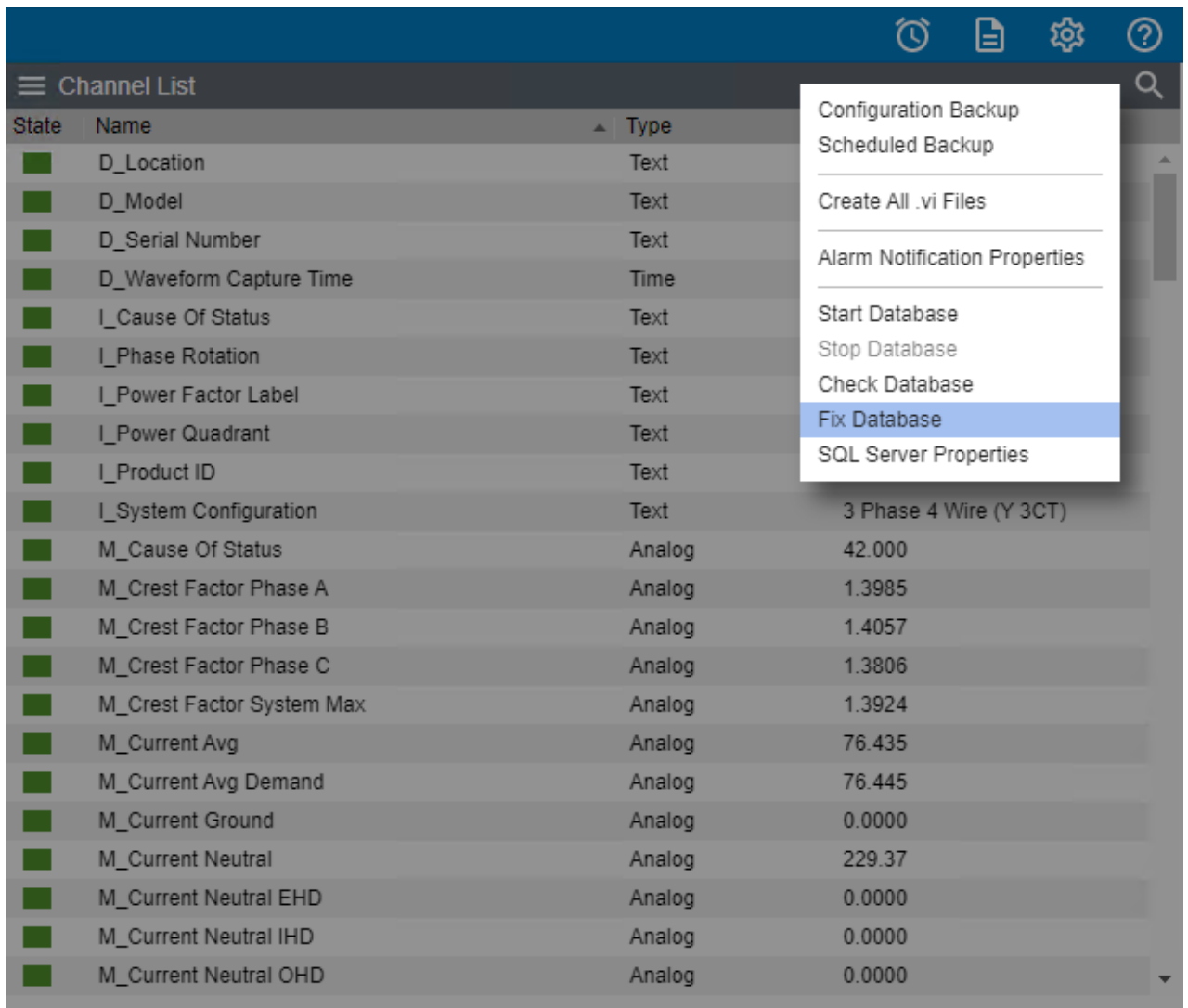
Results are written to the log, which you can review by generating a log through Reports.



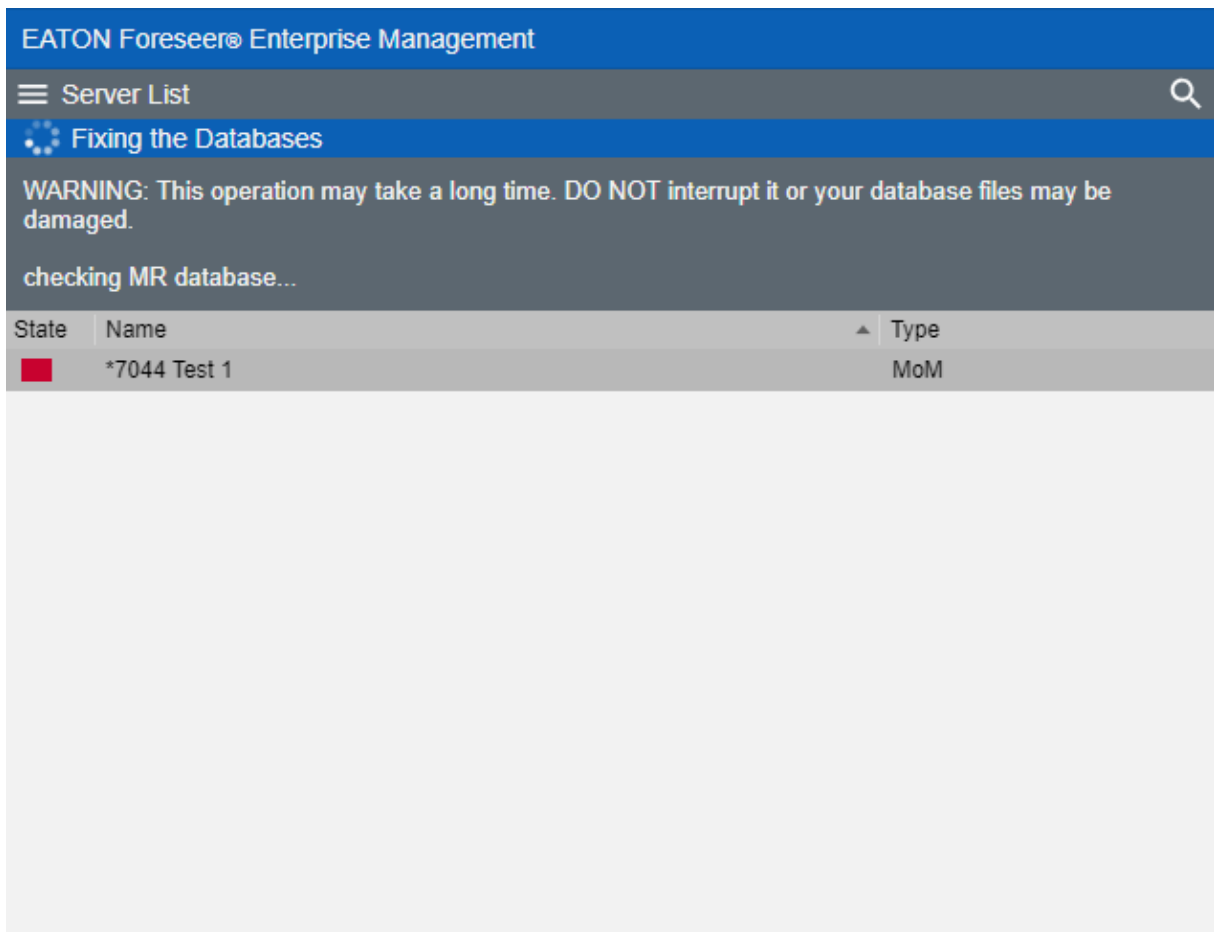
Fix Database

This is a thorough check of the Foreseer databases, including allocation and consistency checks. If problems are found, this function will attempt to fix them.

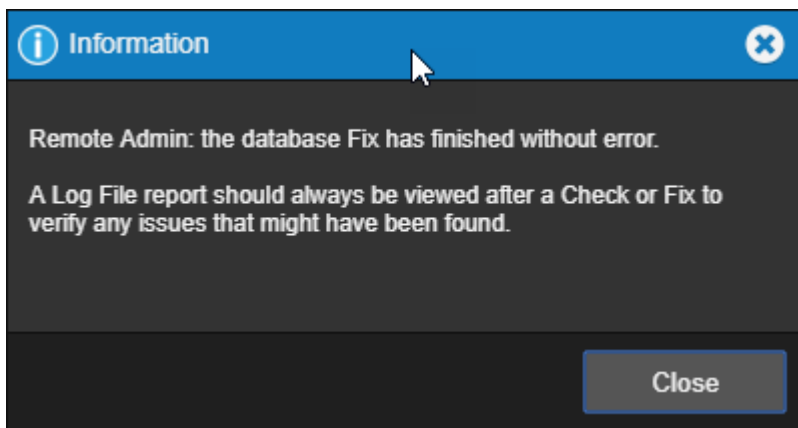
1. Select Fix Database from the Administration Menu



2. This operation may take a long time. DO NOT interrupt it or your database files may be damaged/



- Results are written to the log, which you can review by generating a log through Reports.



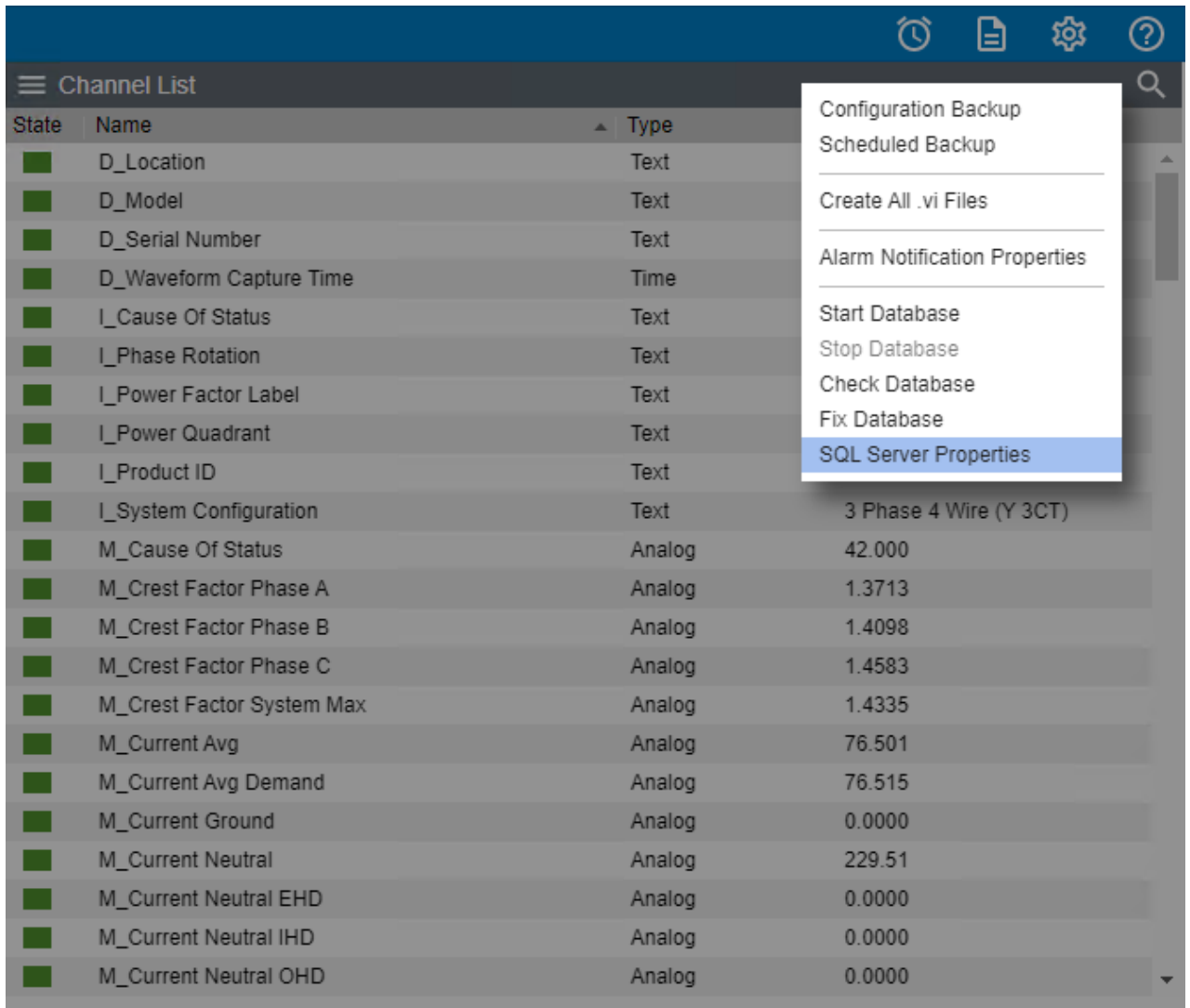
SQL Server Properties

Use this dialog box to configure access to your instance of SQL Server. Follow the instructions on the dialog box to configure the connection string.

You can choose to use either an account managed by SQL Server or a Windows account. If this isn't a new server installation, you'll need to set the account information in the Server Properties dialog box (General tab).

You can also change the location of the Data and Log files.

1. Select SQL Server Properties from the Administration Menu



2. The SQL Server Properties dialog will display.

SQL Server Setup ✕

Enter the connection string that identifies the SQL Server where the databases will be created. The format of a connection string is: SERVER_NAME\INSTANCE_NAME,TCP_PORT. If the string is left blank, it refers to the default instance on this computer.

SERVER_NAME can be a Computer Name or an IP Address. If the name identifies the local computer, a dot (period) may be used. INSTANCE_NAME identifies the instance of SQL Server if it was installed as a Named Instance.

TCP_PORT is optional and identifies a specific TCP Port for connection to SQL Server. It is typically used if the SQL Server is behind a firewall at a specific port number.

Connection String:

To use SQL Server Authentication mode, enter the Login and Password to use to connect to SQL Server. To use Windows Authentication mode, leave these entries empty.

Login:

Password:

Verify:

All databases use a single Data file in the PRIMARY filegroup and a single Log file. By default, they are located where the "master" database Data and Log files are. You may select different locations for the physical Data and Log files below. To use the defaults, leave these entries empty.

Data File Path:

Log File Path:

If a SQL Server connection fails, automatically retry the connection. A retry time of 0 will disable automatic reconnection.

Retry Time (sec):

Temporarily disable the connection retry (persists as long as checked or until the server is restarted).

Local Server List Menu

The Server List menu provides access to all of the functionality that will be required to manage your Foreseer servers.


- Start Server Configuration
- End Server Configuration
- Start New Log File
- Install Devices from List
- Update Server from List
- Add Remote
- Copy for WebViews
- Restart WebViews
- Restart Server

- Restart Windows
- Add Note
- Upload Files
- Open Older Log File
- Open Saved Wiretap
- Properties

Start Server Configuration

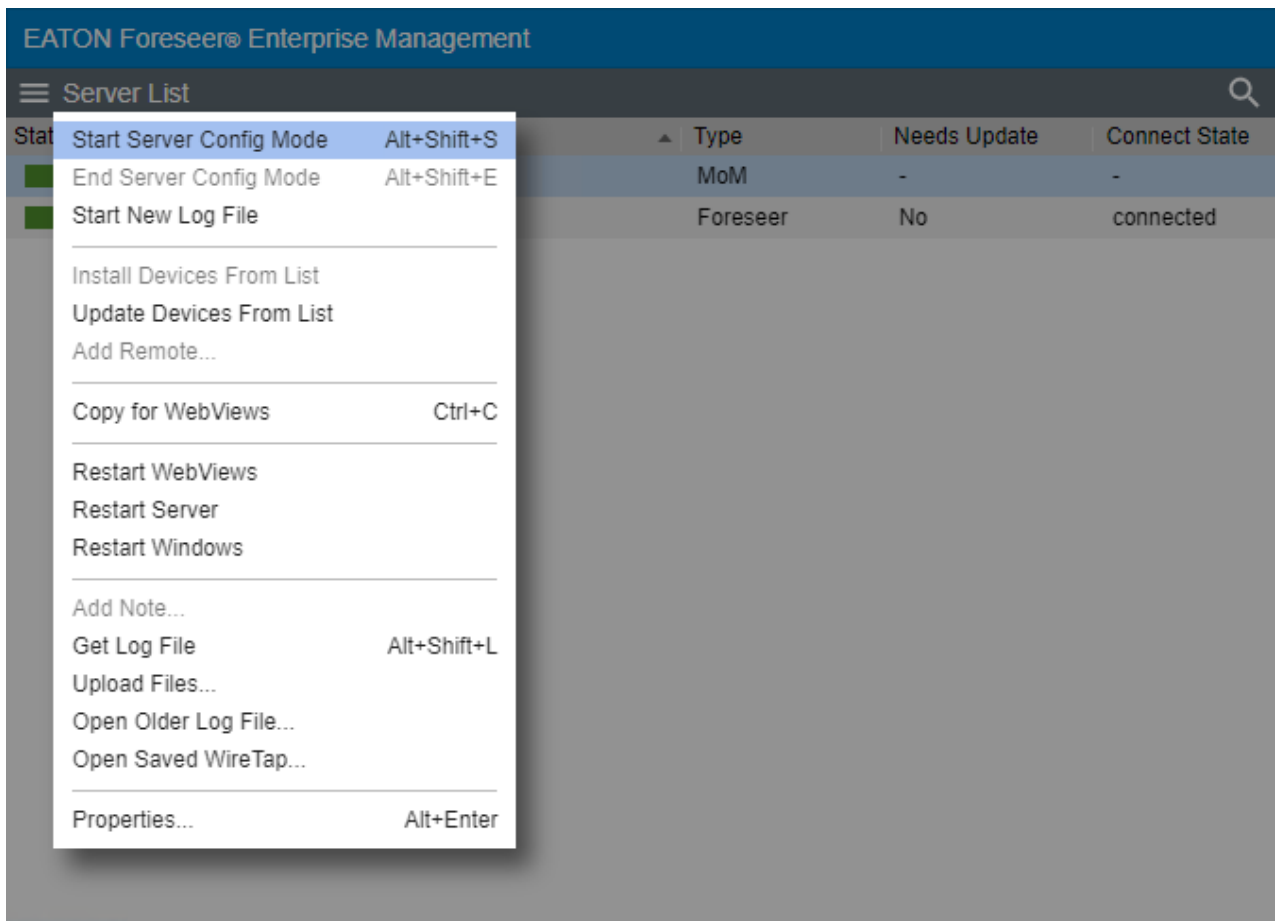
Certain configuration functions are only available when in Server Configuration mode; however, configuring backups is only available when not in Server Configuration mode. Functions that are only available in Server Configuration mode are:

- Install Devices from List
- Add Remote
- Unload Driver
- Load Driver
- Delete Device
- Rename Device
- Add User Defined Channel



 Administrative Authorization is required in initiating Server Configuration mode.

To start Server Configuration mode:


1. Select Start Server Config Mode from the Server List menu



2. A successful start of the Server Configuration Mode will be indicated by the orange Config Mode status bar in the Server List panel

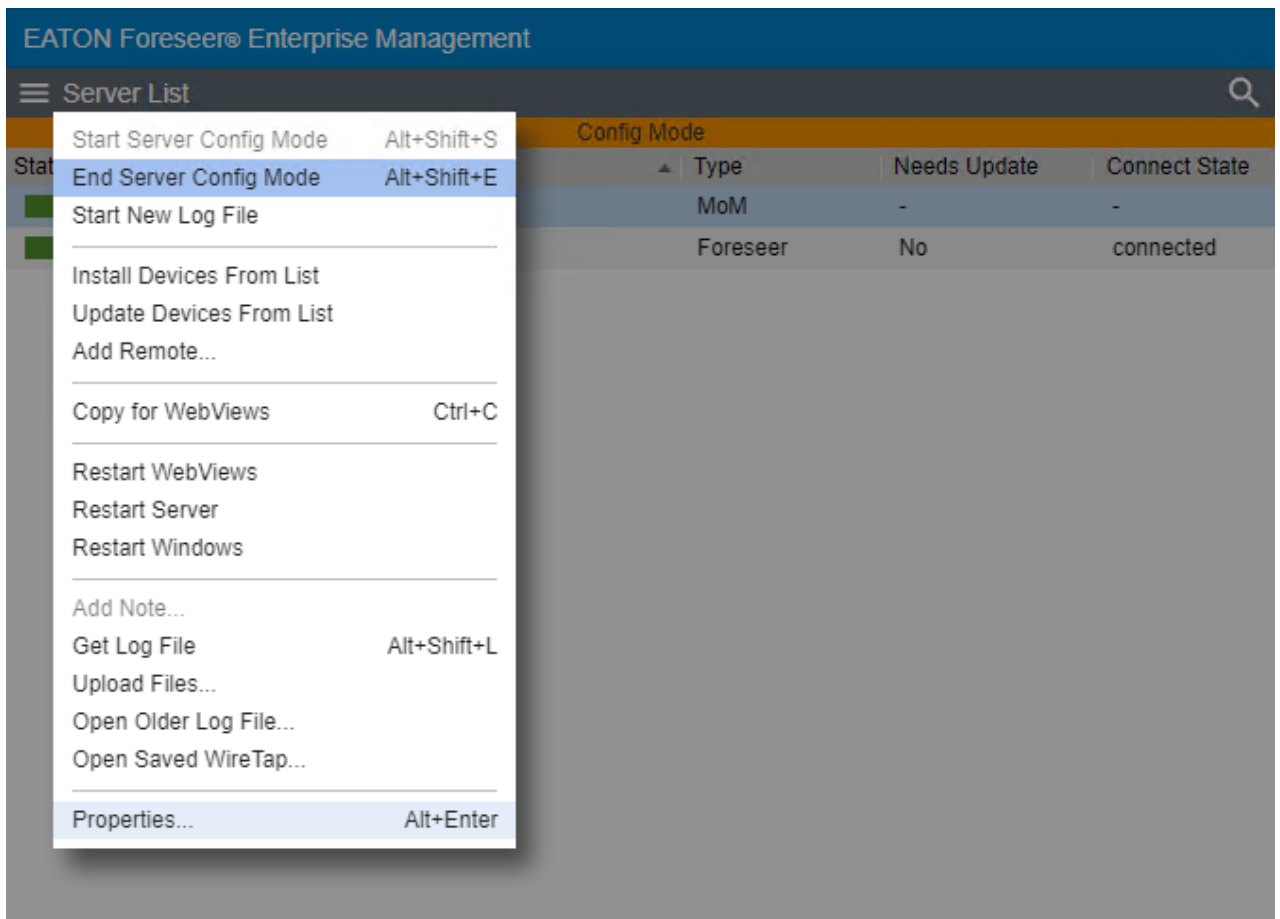
EATON Foreseer® Enterprise Management				
Server List				
Config Mode				
State	Name	Type	Needs Update	Connect State
	*Template Builder	MoM	-	-
	Foreseer Remote	Foreseer	No	connected

End Server Configuration

 Administrative Authorization is required in initiating Server Configuration mode.

To End Server Configuration mode:

1. Select End Server Config Mode from the Server List menu



Start New Log File

This command stops writing the server admin log data to the existing log file and starts a new log file that is automatically assigned a name which is a composite of the name of the prefix Log, the date, and the time (in 24-hour format). The file extension of log files is .txt. Log files reside in the

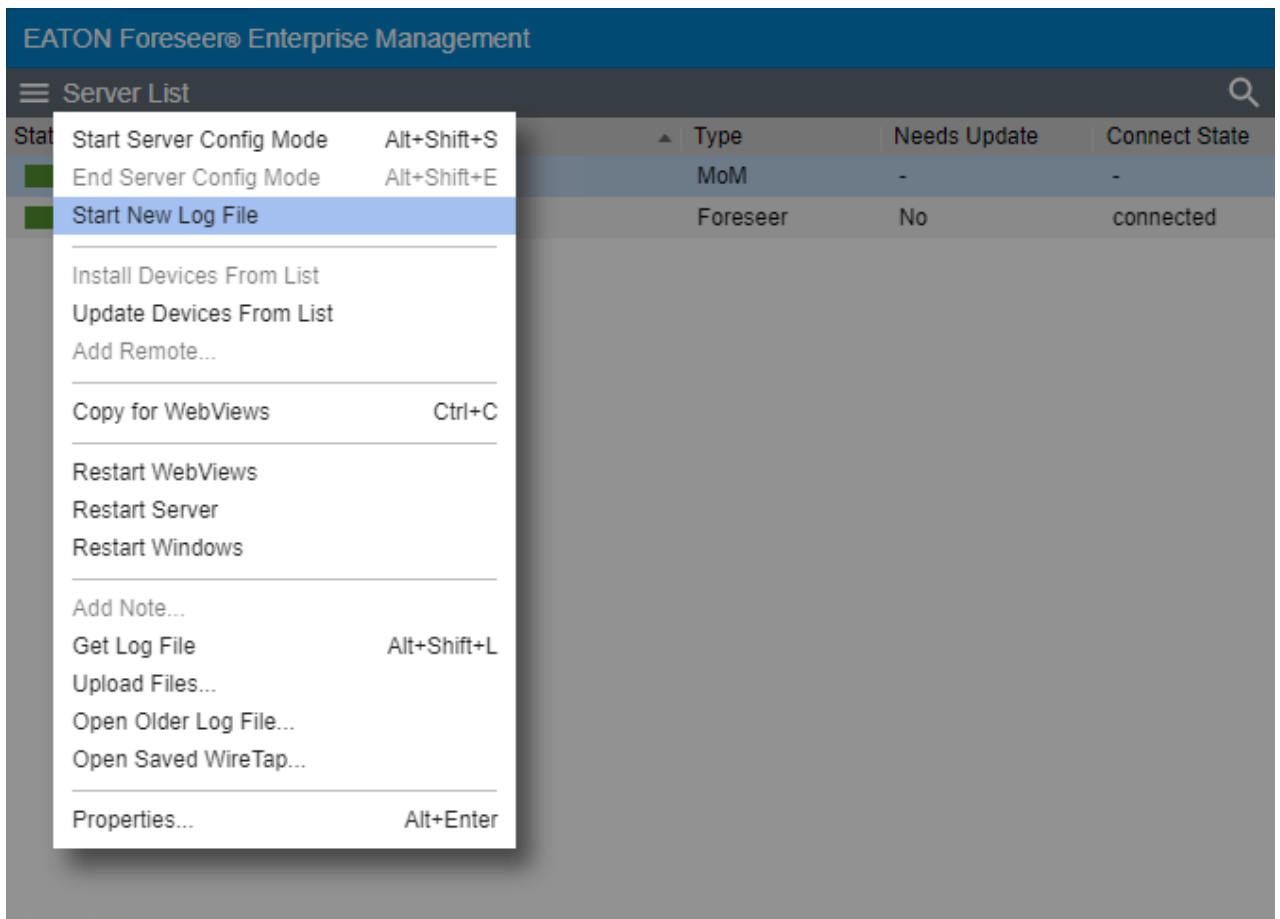
<Install Drive>:\Eaton Corporation\Foreseer\LogFiles

folder.

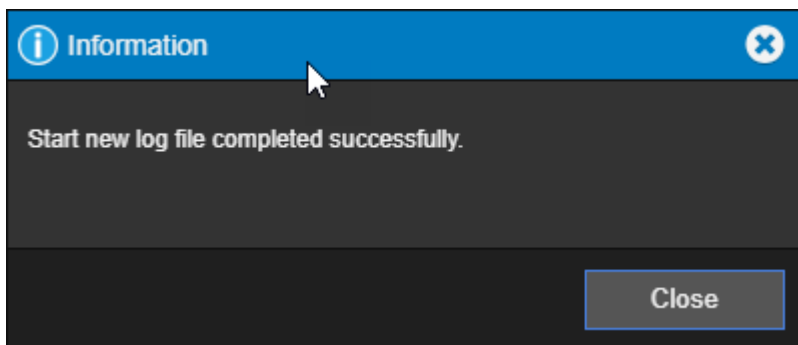
- ✔ The current LogFile.txt is located in the <Install Drive>:\Eaton Corporation\Foreseer\ directory and not in the LogFiles directory.

To start the new log file process:

1. Select Start New Log File from the Server List Menu



2. Upon completion, you will get the following success dialog



Install Devices From List

⚠ Before adding devices in any manner it is highly recommended to take a configuration backup (ARQ) so you can return to a previous point if issues are encountered.

As an alternative to loading a single device via the wizard, you can load a set of devices by predefining these in a comma-separated values (CSV) file. This "device list" file has the following format:

device_name, device_type, device_location, alarm_group_name, vi_file_name, IP_address, port_number, driver_specific_info

Where:

device_name is the name that will be used in Foreseer for the device.

device_type – a string defining the device type. You can use a pre-determine device type supported by Foreseer, or use your own custom device type string.

device_location – a string defining the location of the device.

alarm_group_name - a string defining a logical alarm grouping name.

vi_file_name is the filename of the driver file for that device. This file is stored in the install_path/Foreseer/vi folder. Note that some driver file names may have a single comma. Foreseer will handle this correctly.

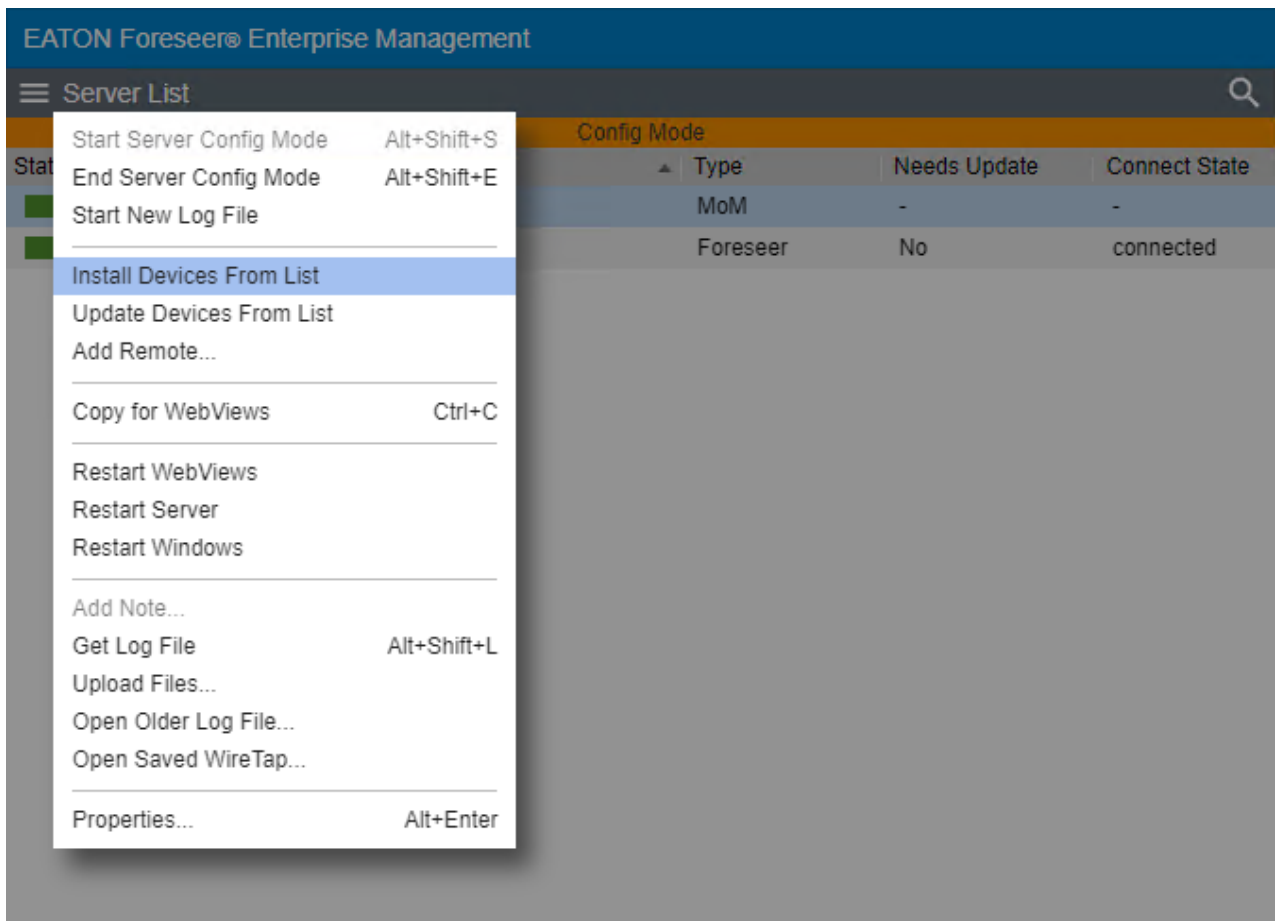
IP_address is the IP address for that device. Set this to none for the Nothing driver.

port_number is the port portion of the device address. Leave this field blank for the Nothing driver. You may also leave this field blank to use the default port for that specific device protocol, or enter a valid port number.

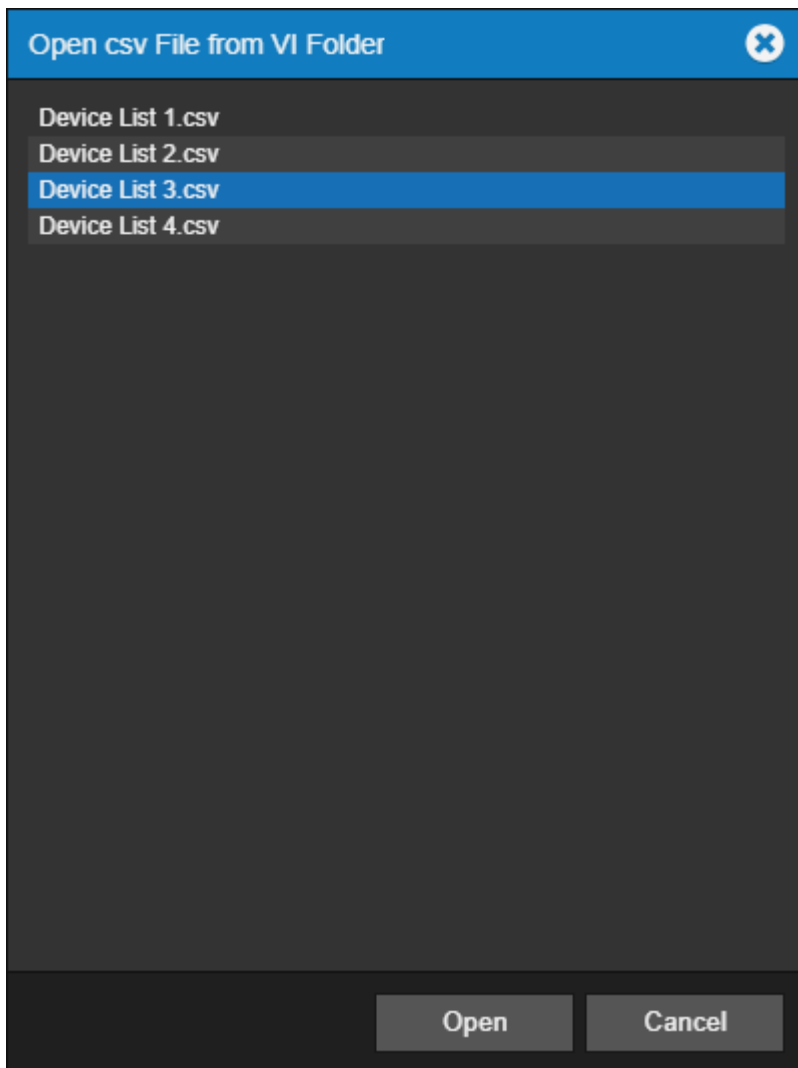
driver_specific_info is either the device ID (for Modbus) or the read community string for SNMP. Set this to none for the Nothing driver.

To add a device from list server:

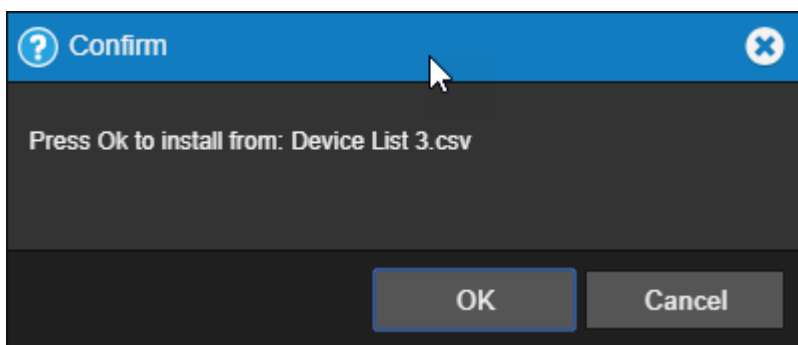
1. Select Install Device From List in the Server List menu.



2. Select Install Device From List in the Server List menu.



3. Click OK to confirm your selection.



Drivers known at this time that can be installed using the Install from List feature include:

- 6-Modbus3
- 6-SNMPManger3
- 6-PowerXpertMeter
- 6-CyberScience CyTime SER
- 6-SquareD_PM800

- 6-PowerXpertMeter2200

✔ **This feature is limited to only 15 devices at a time.**

✔ Servers that have remotes or redundant servers already added to the ARQ must follow 15 device chunks and use separate files to allow the database to update gracefully.

This is by design.

Examples:

Modbus device installs:

PX Meter 1, Meter, PA-Pittsburgh, PQ Alarms, 7-PowerXpert Meter 4000 TCP.vi,
10.22.50.30, 502, 1

PX Meter 2, Meter, PA-Pittsburgh, PQ Alarms, 7-PowerXpert Meter 150 TCP.vi,
10.22.50.50, 951, 1

SNMP device installs:

PW 5125 1, UPS, PA-Pittsburgh, UPS Alarms, 7-Powerware UPS 5125 SNMP.vi,
10.22.50.32, 161, public

PW 5125 2, UPS, PA-Pittsburgh, UPS Alarms, 7-Powerware UPS 9395 SNMP.vi,
10.22.50.75, , public

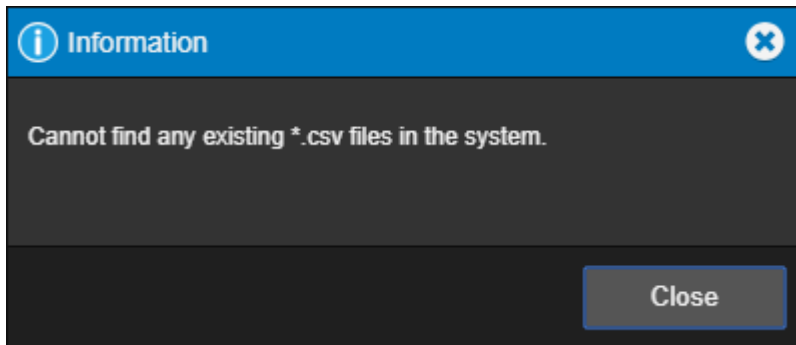
Nothing device installs:

Nothing 1, None, PA-Pittsburgh, Custom Alarms, 7-Nothing.vi, none

You can load the .csv file into Foreseer through any of the following methods:

- The Foreseer Web Configuration Utility
- The Upload Files feature of Web Configuration.
 - These files should be uploaded to the Server/Vi location.
- The Foreseer Server.
 - To load a device list file through the Foreseer Server:
 - In the Configuration menu, click Start Server Configuration.
 - In the Configuration menu, click Install Devices from List.
 - In the Select CSV File dialog box, browse to the CSV file.
 - Click Open.
 - End Server Configuration

The file will be processed and validated. If no errors are found, the devices will be added to the Foreseer system configuration. Should errors be detected in the device list file, refer to the error dialog boxes and the log report.



- ✔ After adding all of the devices to your Foreseer Server, you should run a System Configuration Report. You should maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. The System Configuration Report provides information about devices including IP address and Ports.

Update Devices From List

- ⚠ Before updating devices in any manner, especially in bulk fashion, it is highly recommended to take a configuration backup (ARQ) so you can return to a previous point if issues are encountered.

Update Devices from List provides a method to update existing Foreseer devices already installed. Specifically, this feature allows you easily populate the Device Location, Device Type, and Alarm Group Name properties of a device without needing to touch each individually through WebConfig.

After updating existing devices from list, be sure to perform a Fix Database command to commit any changes.

The Update Devices from List feature requires the use of a CSV formatted file. The Update List file has the following format:

device_name, device_type, device_location, alarm_group_name

-where-

device_name – the case sensitive name of the existing device in the Foreseer server

configuration

device_type – a string defining the device type. You can use a pre-determine device type supported by Foreseer, or use your own custom device type string.

device_location – a string defining the location of the device.

alarm_group_name - a string defining a logical alarm grouping name.

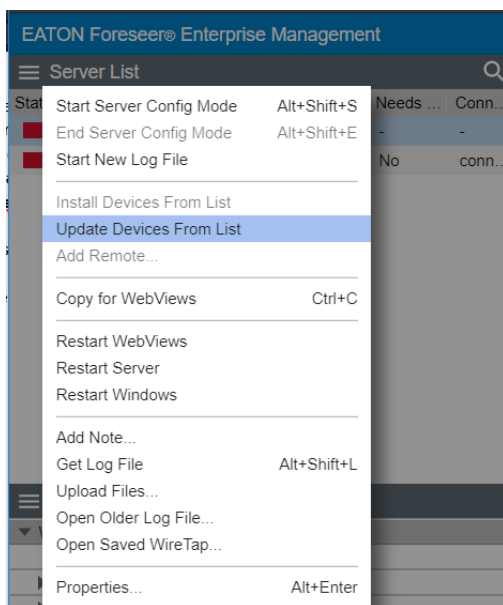
The Device Type, Device Location, and Alarm Group Name fields can be blank for situations where only one of the fields needs to be updated. The Device Name is always required in order for the Update process to find the existing device to update.

- ✓ Any CSV file that you wish to use with the Update Devices from List feature must be copied to the VI directory of your Foreseer installation.

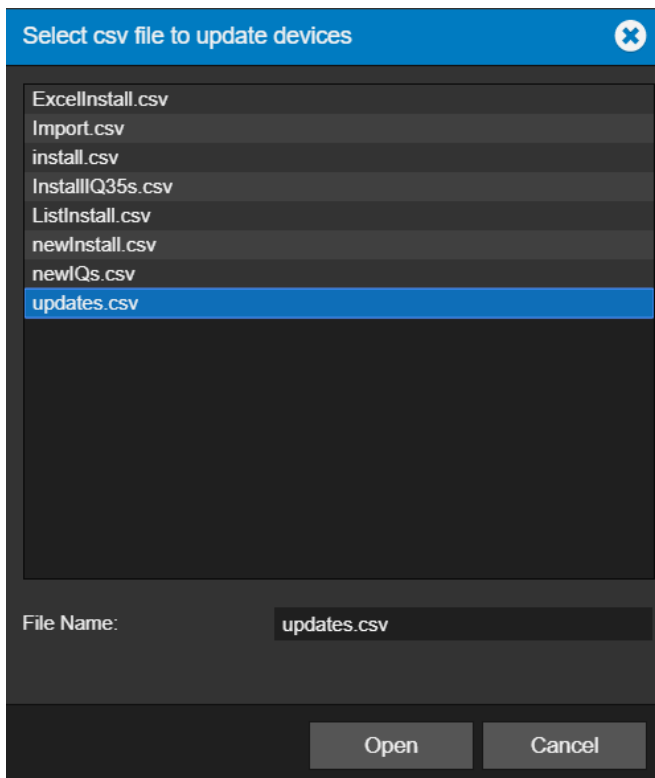
Modern cybersecurity standards prohibit .csv files from being uploaded to web servers like Foreseer using the Upload File feature. Therefore, you must make the appropriate provisions to manually copy this file into the VI directory via Windows File Explorer.

To update devices from a list, perform the following steps:

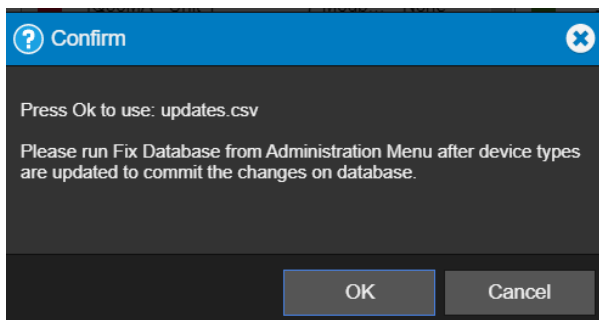
1. Select Update Device From List in the Server List menu.



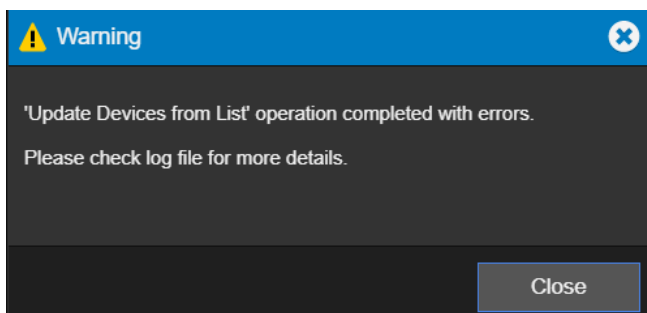
2. Select the appropriate CSV file from the list provided.



3. Click OK to confirm your selection.



If the Update from List feature experiences any issues with processing your CSV file, you may receive a message indicating as such. You can run a Log Report to troubleshoot any potential issues that may have been encountered.



- ✔ Remember to perform a Fix Database operation in order to commit these changes into your SQL Server database.

Add Remote

A local Foreseer Server can serve as host to a remote Foreseer Server (or an Outpost), expanding and enhancing system monitoring capabilities. Once defined, the Remote Server appears on the Tree View as another computer and Minor Server Version configuration elements such as Channel Properties can be modified locally. A Password provision adds another layer of security by restricting access to the Remote Server to authorized personnel.

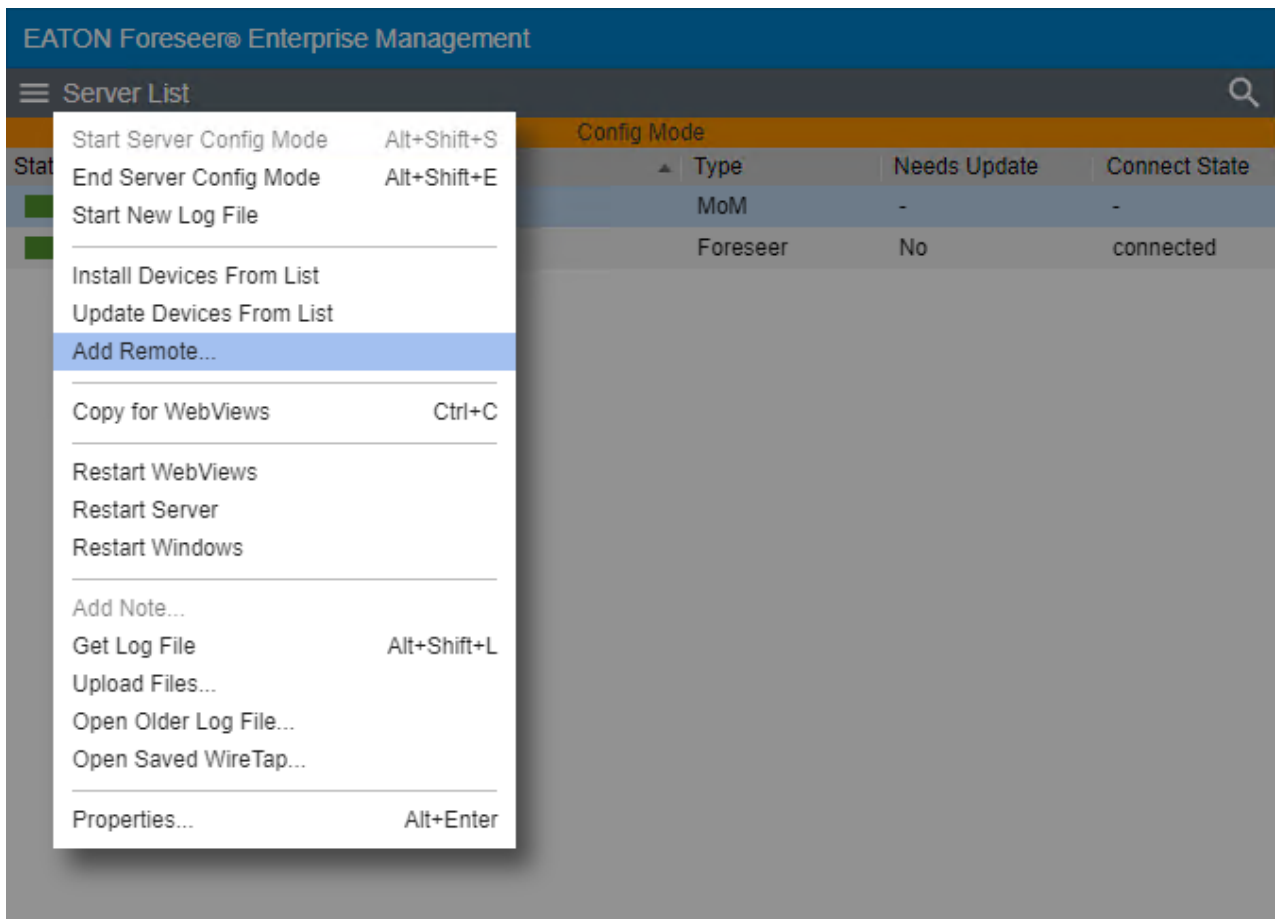
Server Config mode must be active to run this command. Activate Config mode by right-clicking server and selecting Start Server Config Mode. The **** CONFIG MODE **** message should be displayed above the tree.

- ✔ Administrative Authorization is required before proceeding with this command.

- ✔ Server Config mode must be active to run this command. Activate Config mode by right-clicking server and selecting Start Server Config Mode. The **** CONFIG MODE **** message should be displayed above the tree.

To add a remote server:

1. Select Add Remote in the Server List menu.



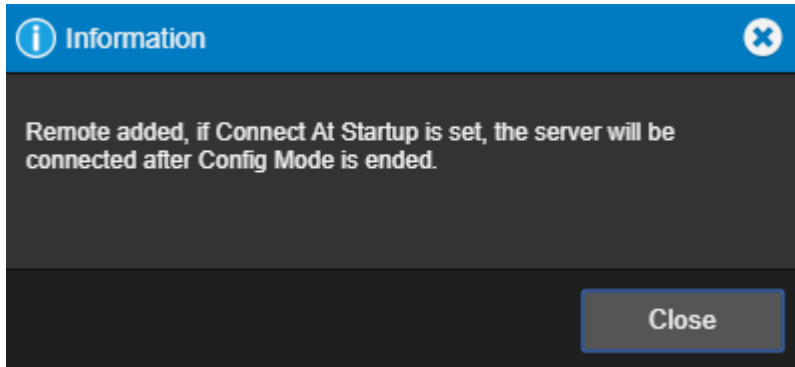
- Identify the remote server by entering its Name and Remote Address; requiring Connection Password security is optional. If a password is specified for remote server access, the password must be entered a second time in the Verify Password field. If no password is specified, it defaults to "special".

The 'Add New Remote' dialog box contains the following fields and options:

- Name: Remote - 7044 Test 1
- Remote Address: 10.130.16.16:2100
- Updates (sec): 2
- Connection Password: [Redacted]
- Verify Password: [Redacted]
- Connect to this remote at startup
- Synchronize Remote's clock on connect
- This remote is a Redundant Server
- This Remote sends waveform files

Buttons: OK, Cancel

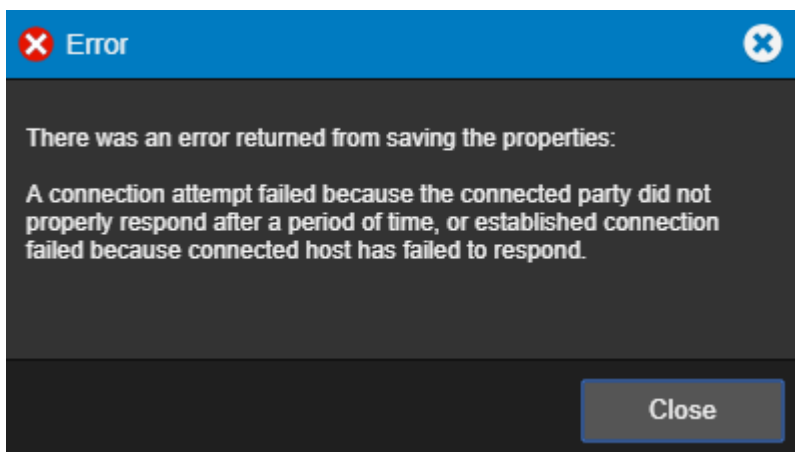
3. Either accept the 2 second default for Updates (sec) or enter a new setting.
4. Specify whether to automatically Connect to this Remote Server at startup and to synchronize the Remotes clock on connect. You can also specify whether or not this server is redundant and if it sends waveform data.
5. Click OK and the Server attempts connection with the Remote Server. Once successful, the following message will appear.

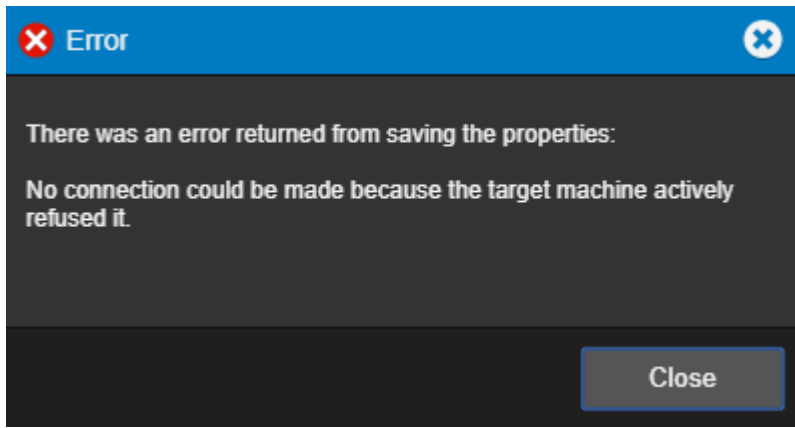


6. Once connection is established, the new Remote Server appears in the Tree View hierarchy.

A Backups folder is created containing sub-folders for each Remote Server that is added to the system. If a Remote Server configuration changes, as indicated by the Major Server Version System Channel, the Local Server will request a configuration backup. The resulting archive file is uploaded to the respective Remotes sub-folder to ensure that a current backup is available.

Possible error messages include:

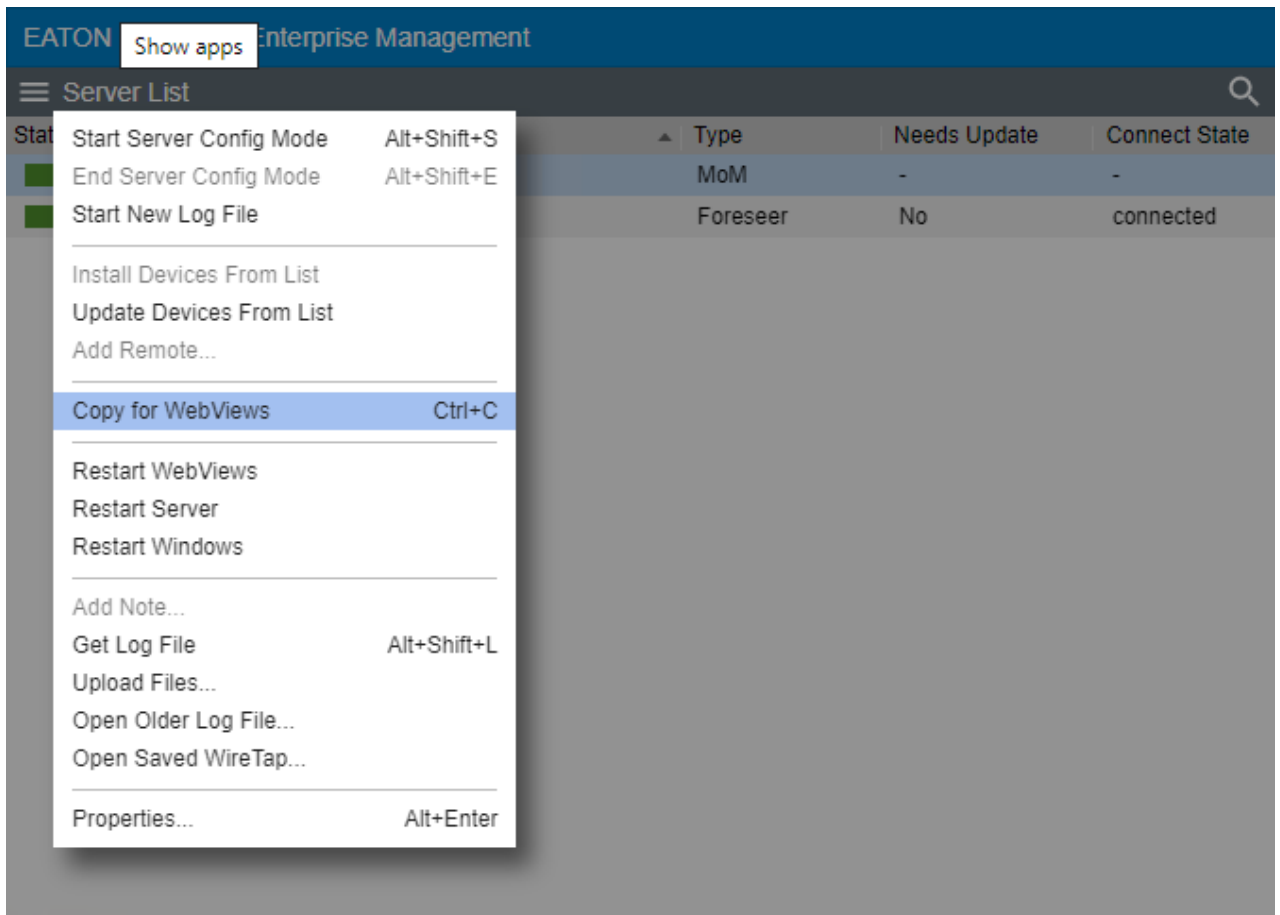


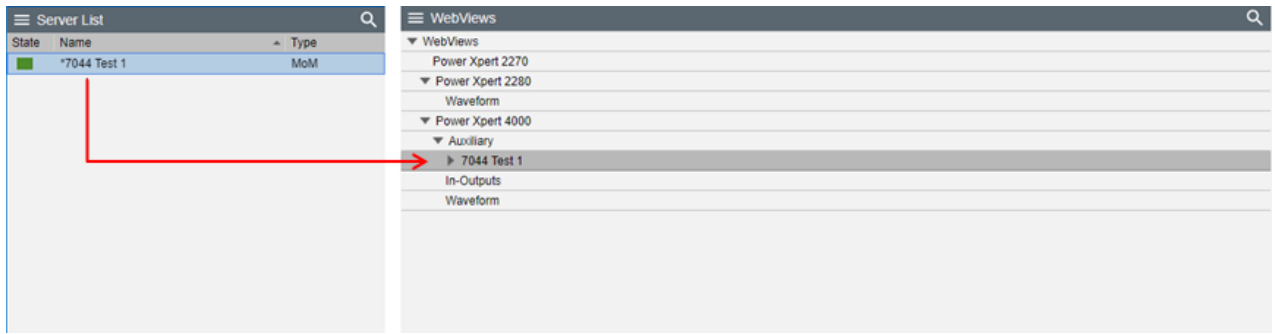


If you encounter any errors, please correct the problem identified and retry the command.

Copy for WebViews

This function copies the target and all child devices and their channels to the target folder in the WebViews tree. The server itself is given a subfolder under the target WebViews folder, and each device is given a sub folder of its own under the server folder.



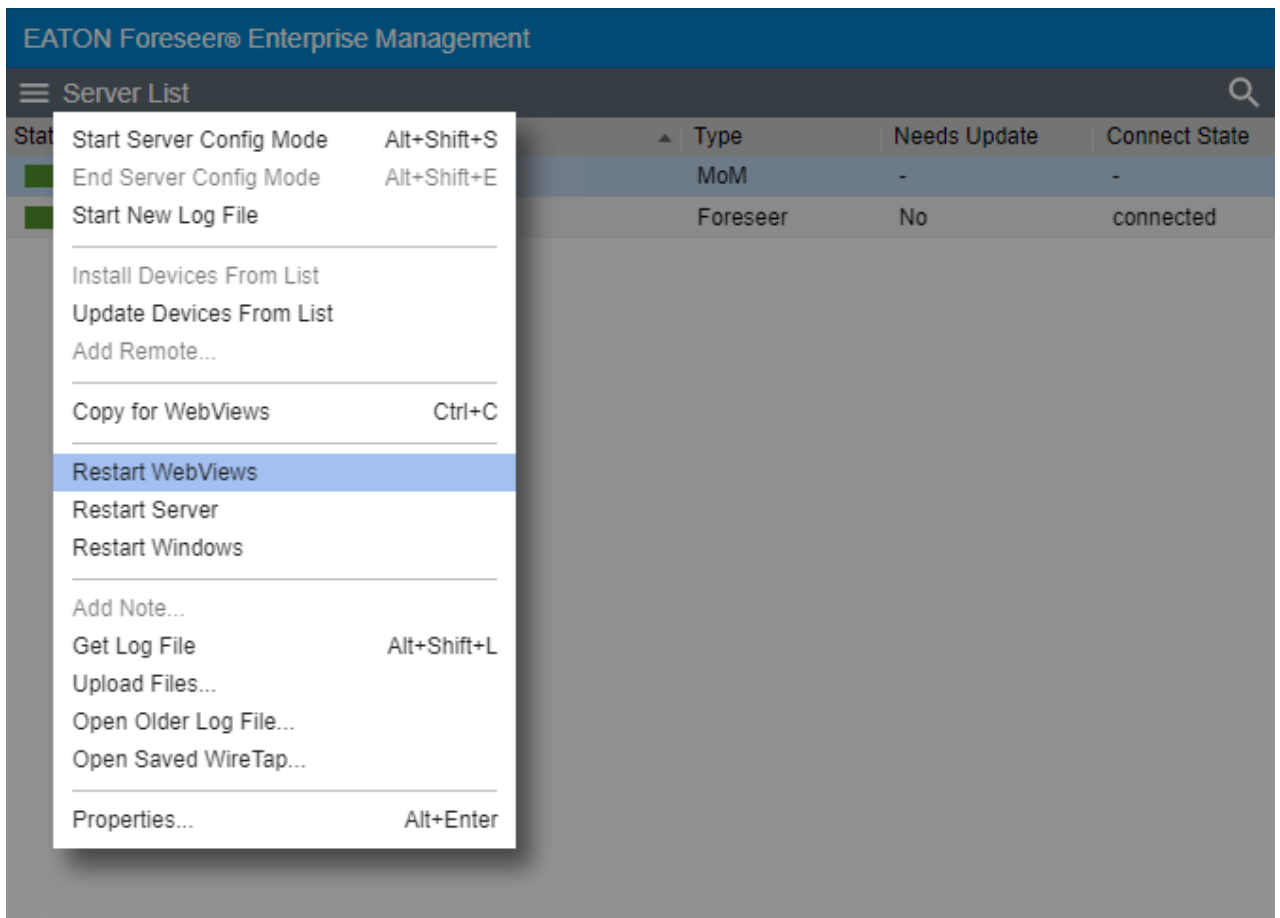


In the example shown above, “WebViews Copy”, the Local server is copied and then pasted into the Power Expert 4000 folder under WebViews. Note that the folder structure mimics the device structure under the server. Instead of copying the entire server, you can also copy individual devices and their channels to a location in the WebViews tree.

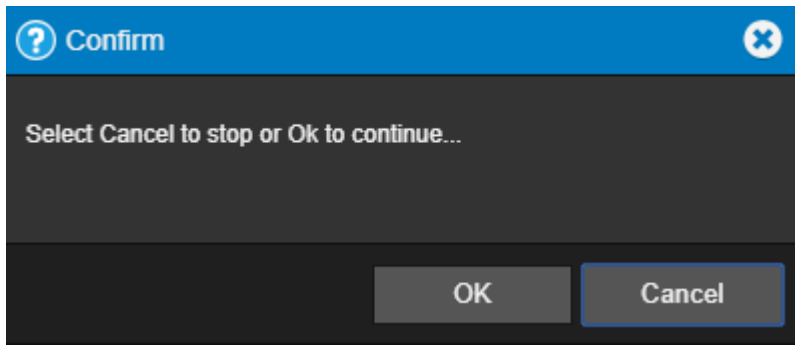
Restart WebViews

The Restart WebViews function restarts the Foreseer WebViews instance (both http and https connections will be reset). Select OK to continue this request.

1. Select Restart WebViews from the Server List menu.



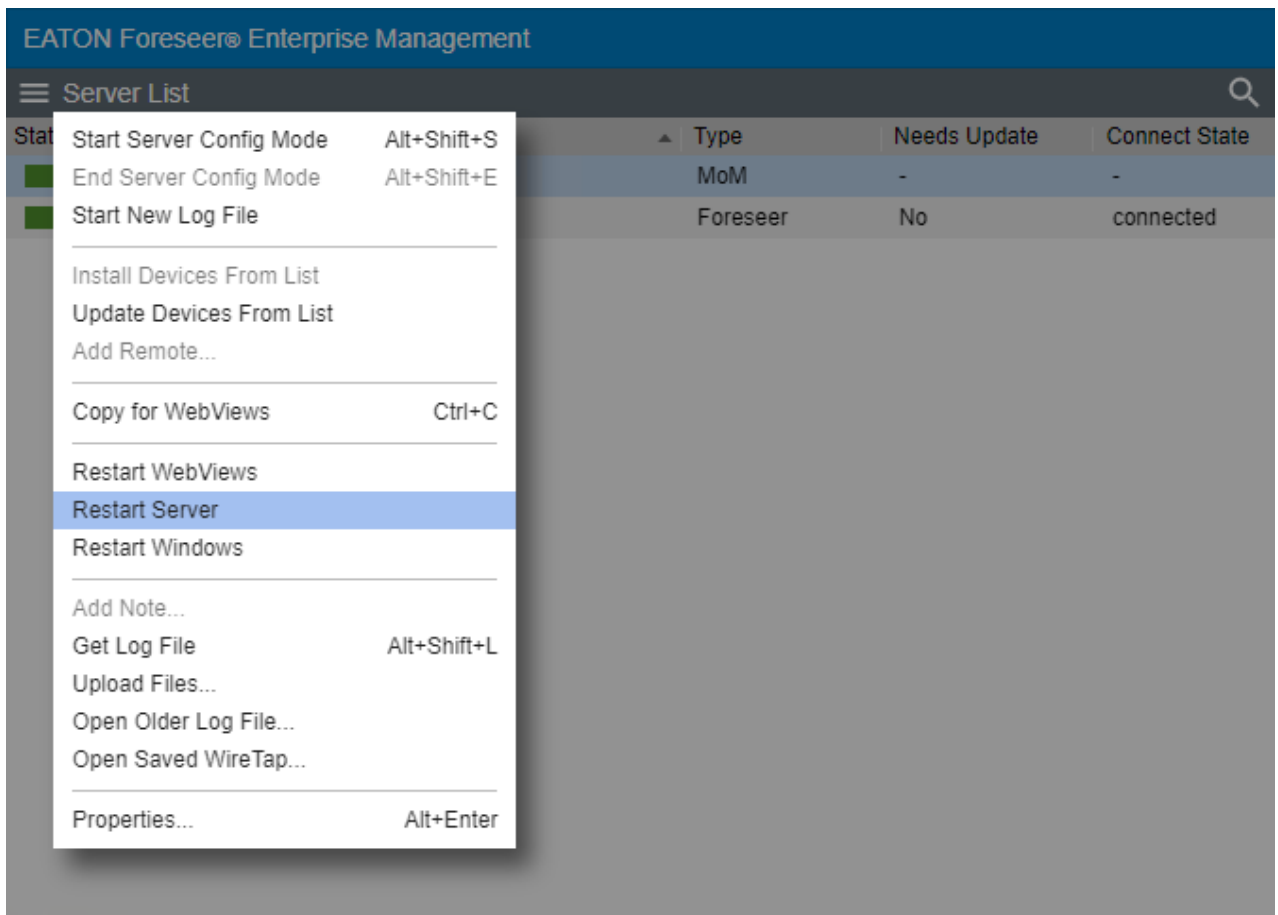
2. Select OK to continue or Cancel to stop



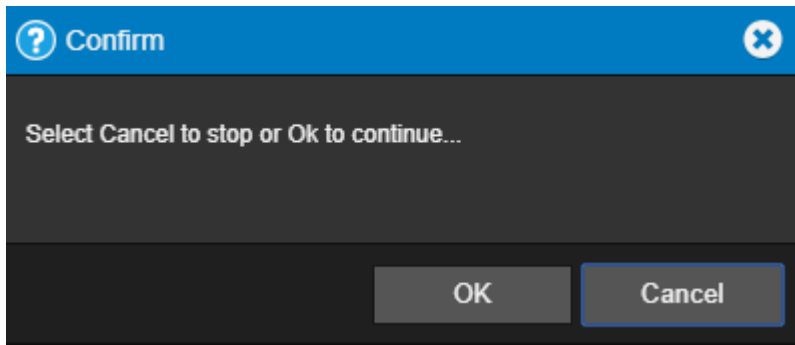
Restart Server

The Restart Server function restarts the Foreseer server. This is identical to exiting and restarting the Foreseer server from its standalone interface. Select OK to continue this request.

1. Select Restart Server from the Server List menu.



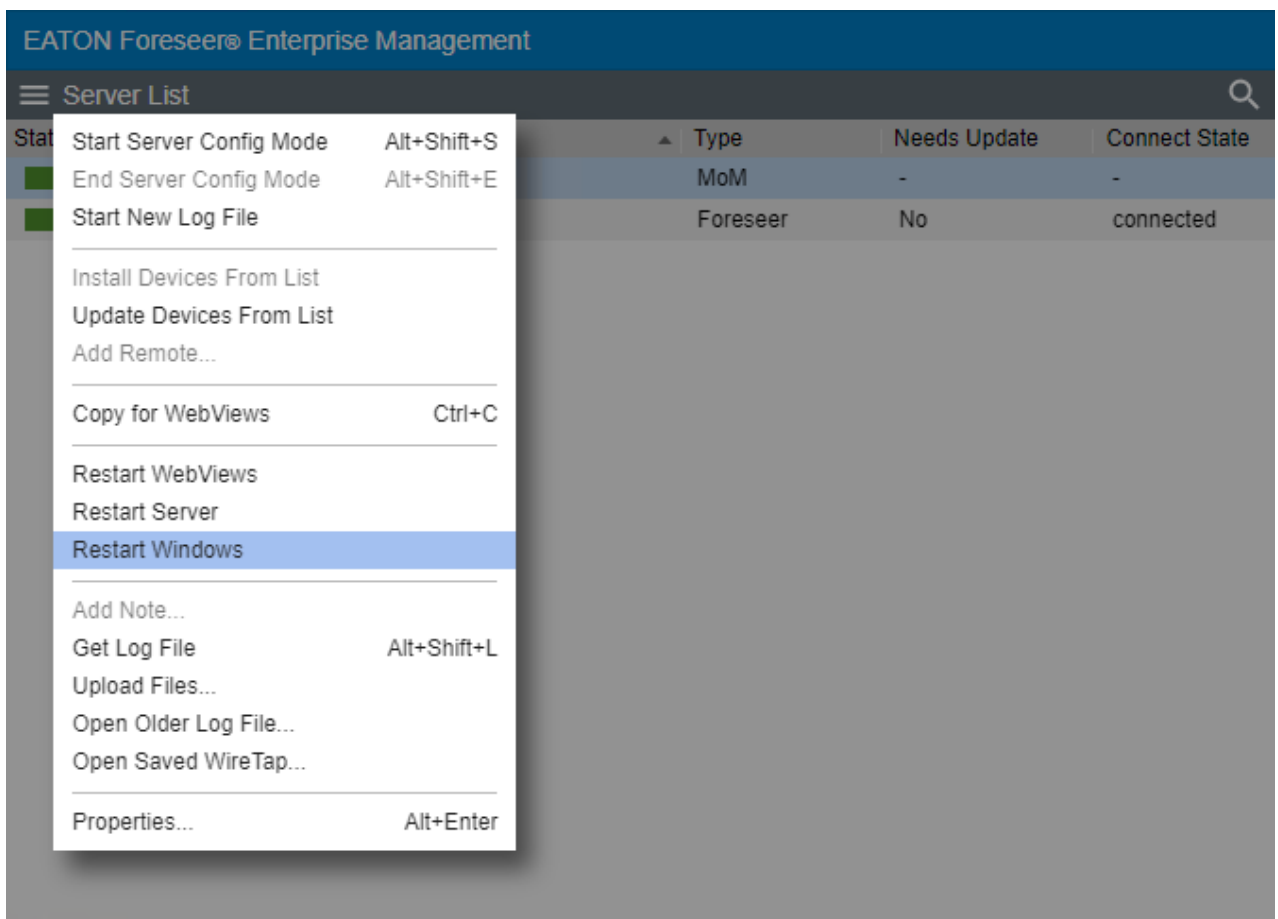
2. Select OK to continue or Cancel to stop



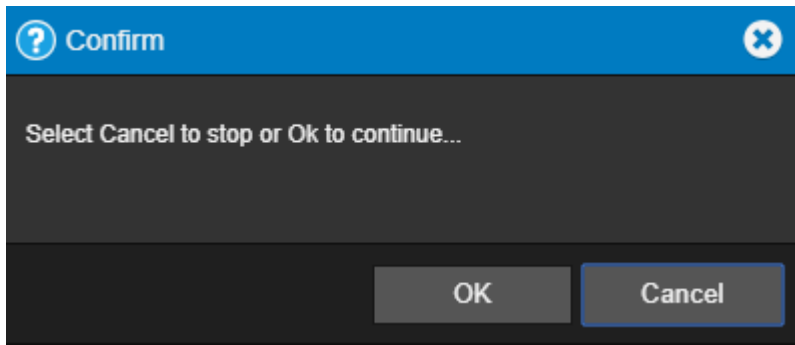
Restart Windows

The Restart Windows function restarts the server computer itself, which may have ramifications beyond just restarting the Foreseer server. Do not issue this command unless you've taken into account other software that may be running on the server. Select OK to continue this request.

1. Select Restart Server from the Server List menu.



2. Select OK to continue or Cancel to stop

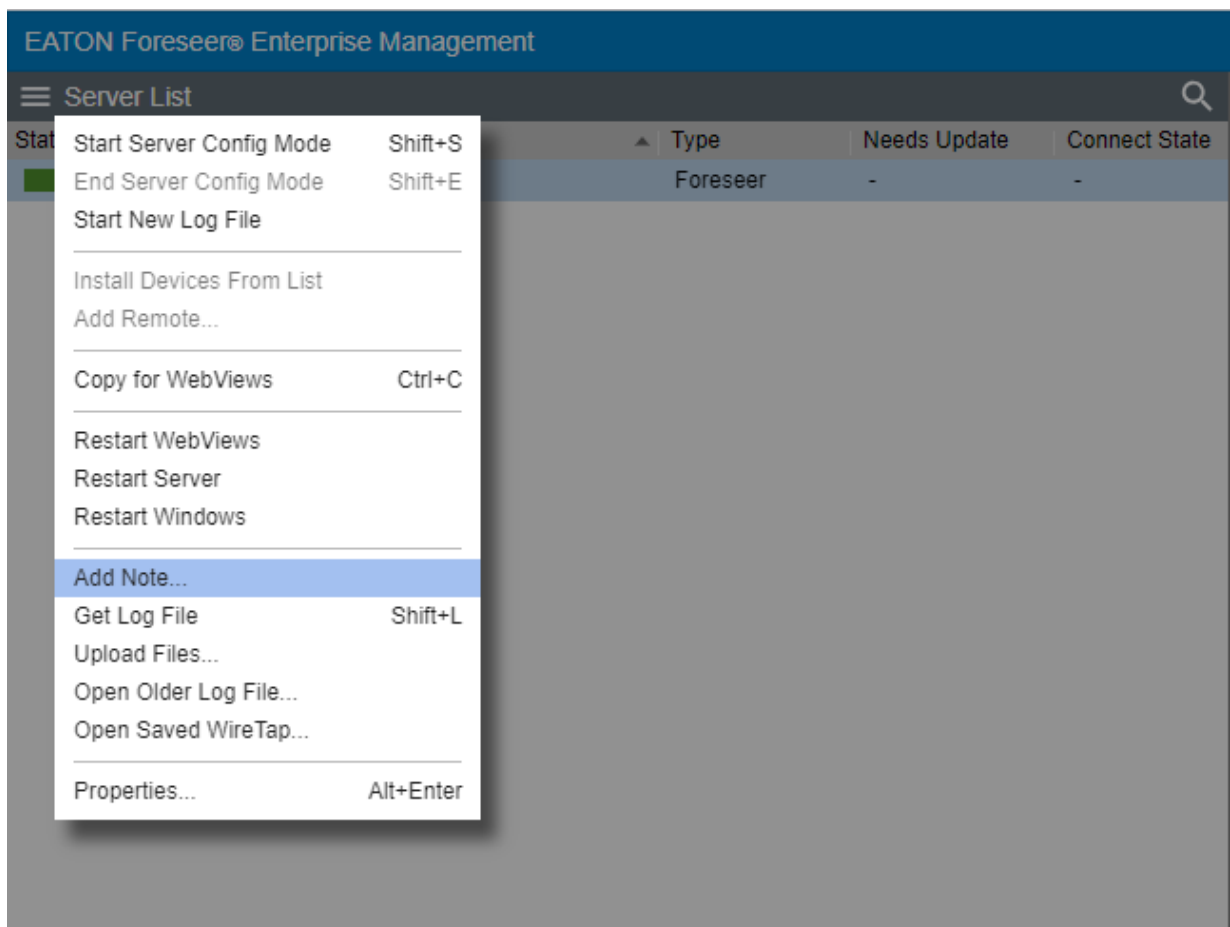


Add Note

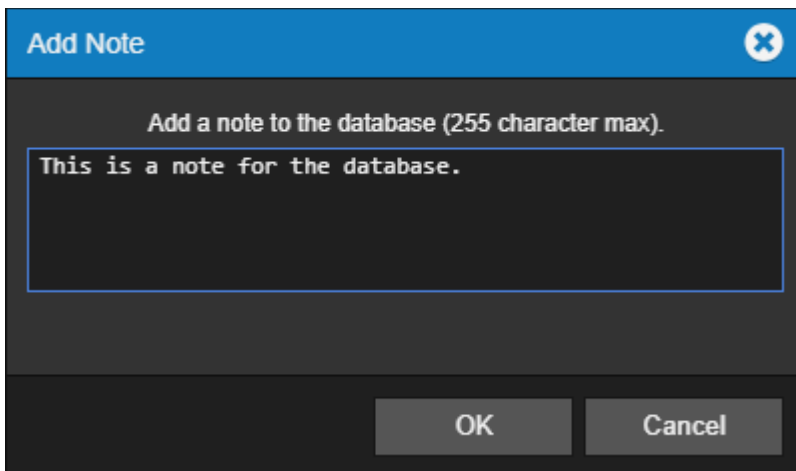
You can use the Add Notes feature to record any supplemental information relevant to a particular event when it occurs. The notes are logged into the Server's database and can be reviewed by authorized Foreseer clients or retrieved in Foreseer Reports. An unlimited number of real-time notes may be entered, but they are limited to 255 characters each. A typical use for Foreseer notes is to add information during the course of Acknowledging and/or Rearming alarms.

To create a note:

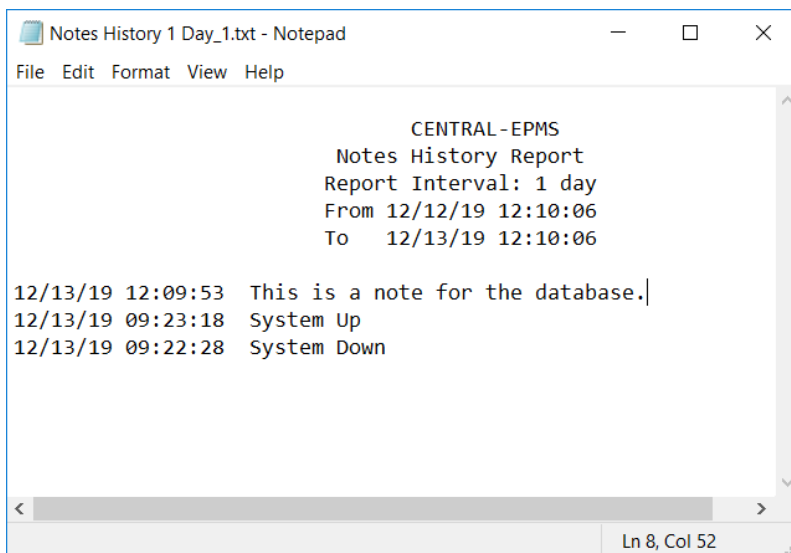
1. Select Add Note from the Server List menu



-
2. In the note editor dialog box, type a note (not exceeding 255 characters).

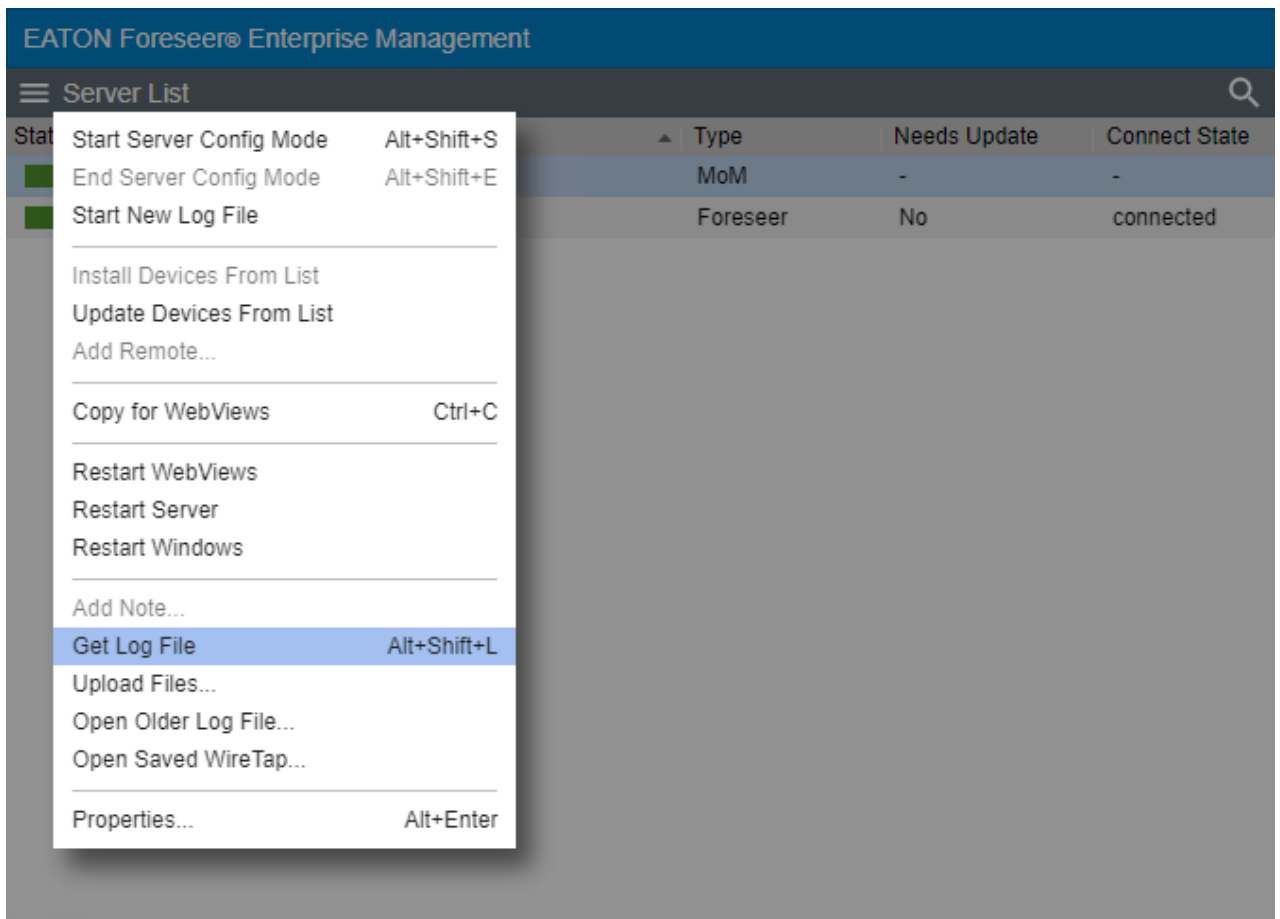


-
-
3. Select OK to continue.
4. The database note can now be reported on in the Notes History Report



Get Log File

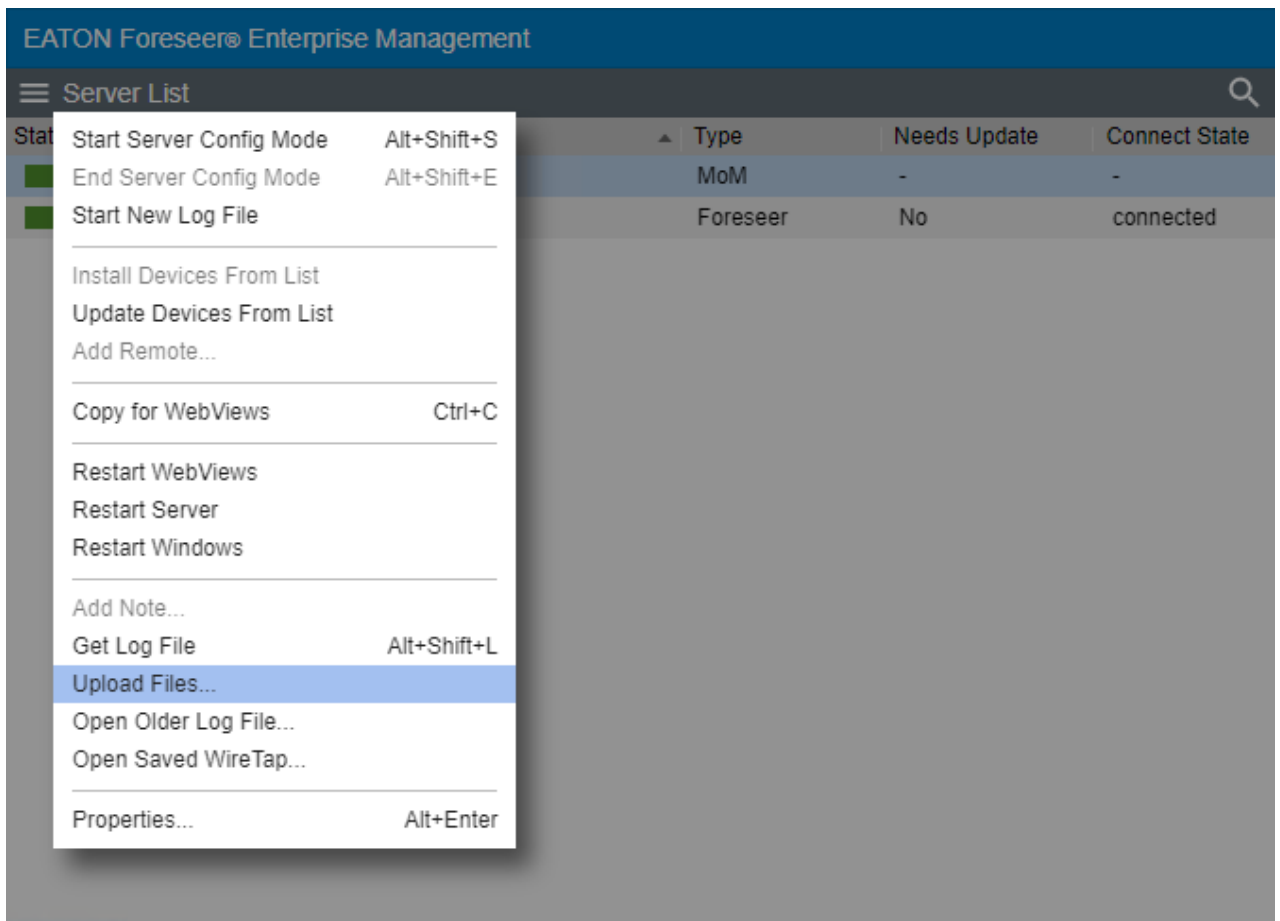
Get Log File will obtain the current Log File Report from the server.



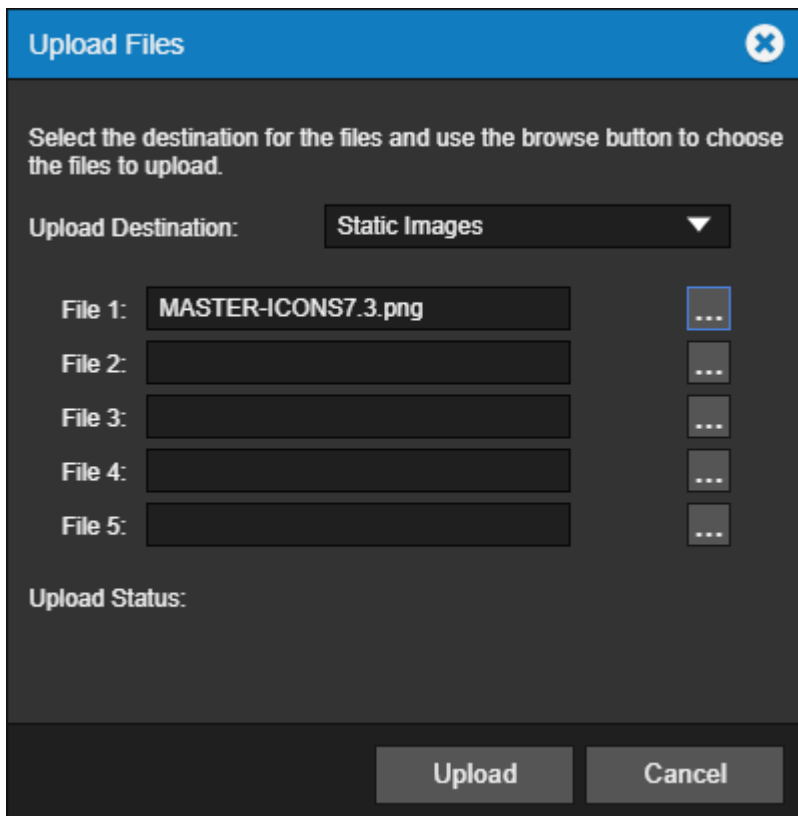
Upload Files

The Upload Files function provides a general-purpose file upload utility, useful for adding graphics, drivers, and other files to the server from a remote location. You can select up to five files to upload simultaneously, as well as selecting the target folder on the server. Target folder selections are limited to those within the Foreseer installation tree to which one would legitimately have a reason to upload files.

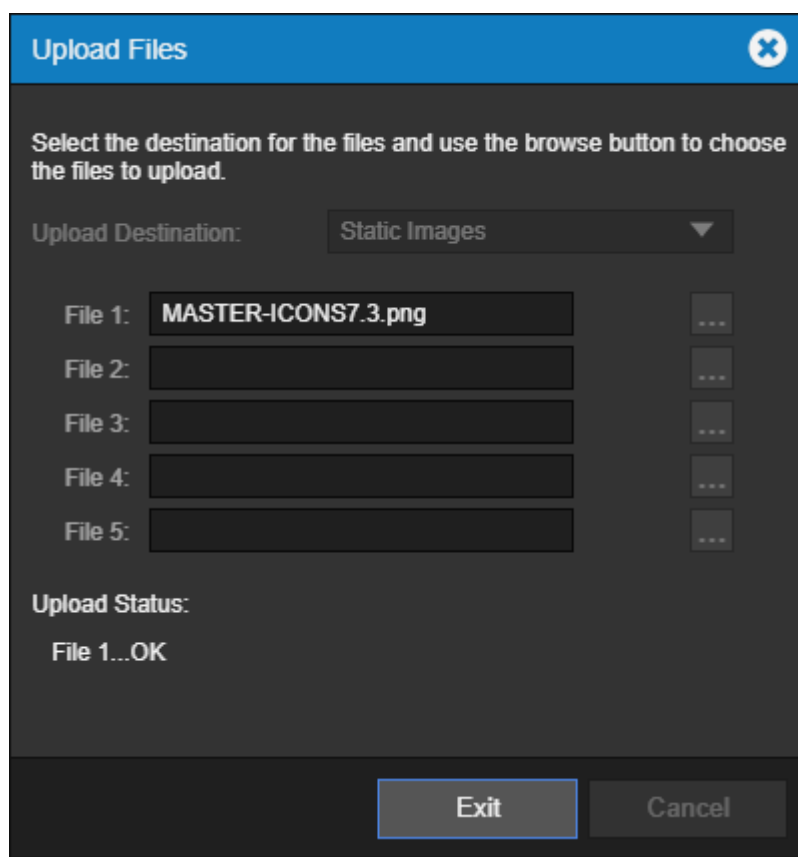
1. Select Upload Files from the Server List menu.



2. Select the destination for the files and use the browse button to choose the files to upload



3. Click Upload to continue



4. Click Exit when complete

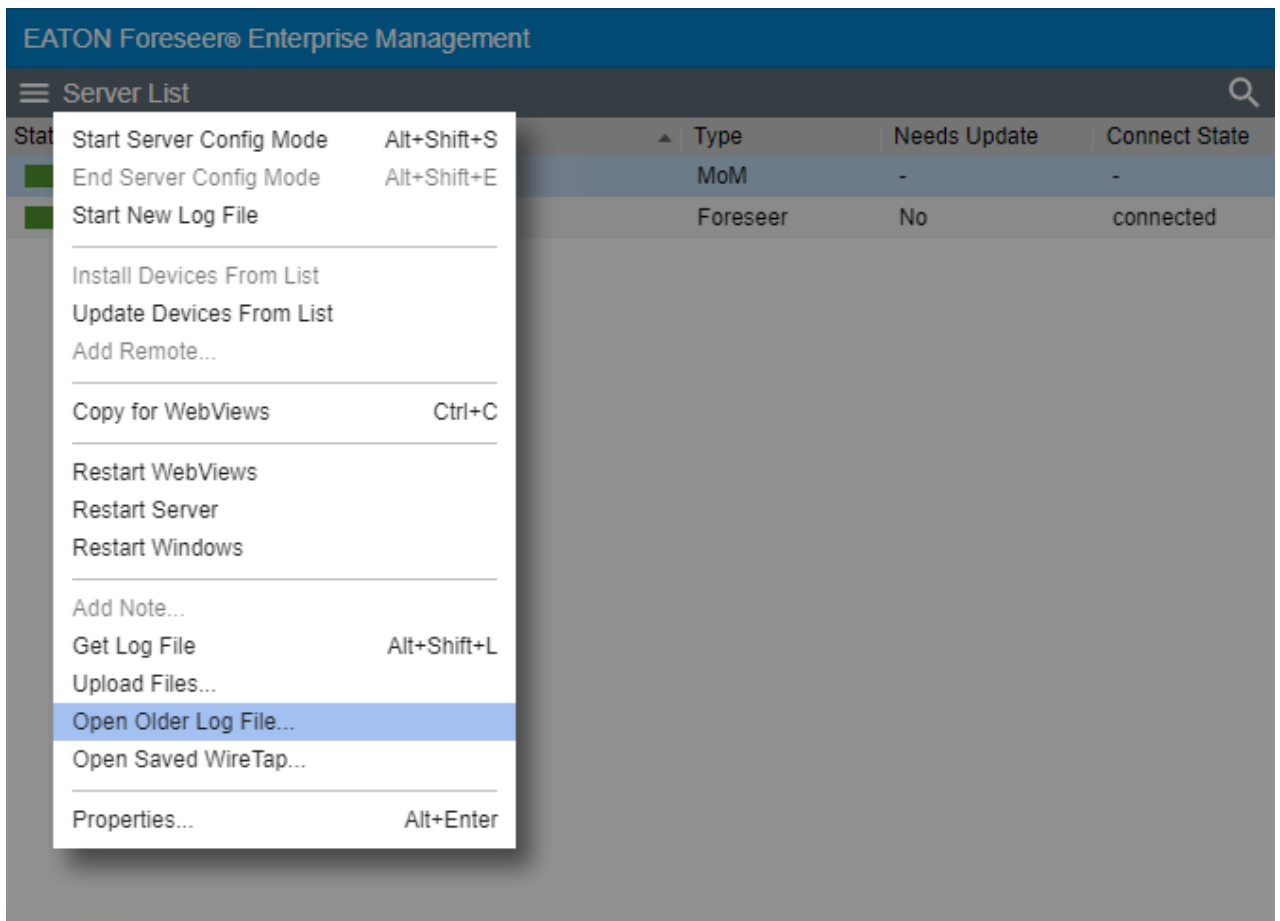
Upload destinations include:

- Update Server
- Update Vi
- Server/Vi
- WWW/Support
- Static Images
- Anime Images

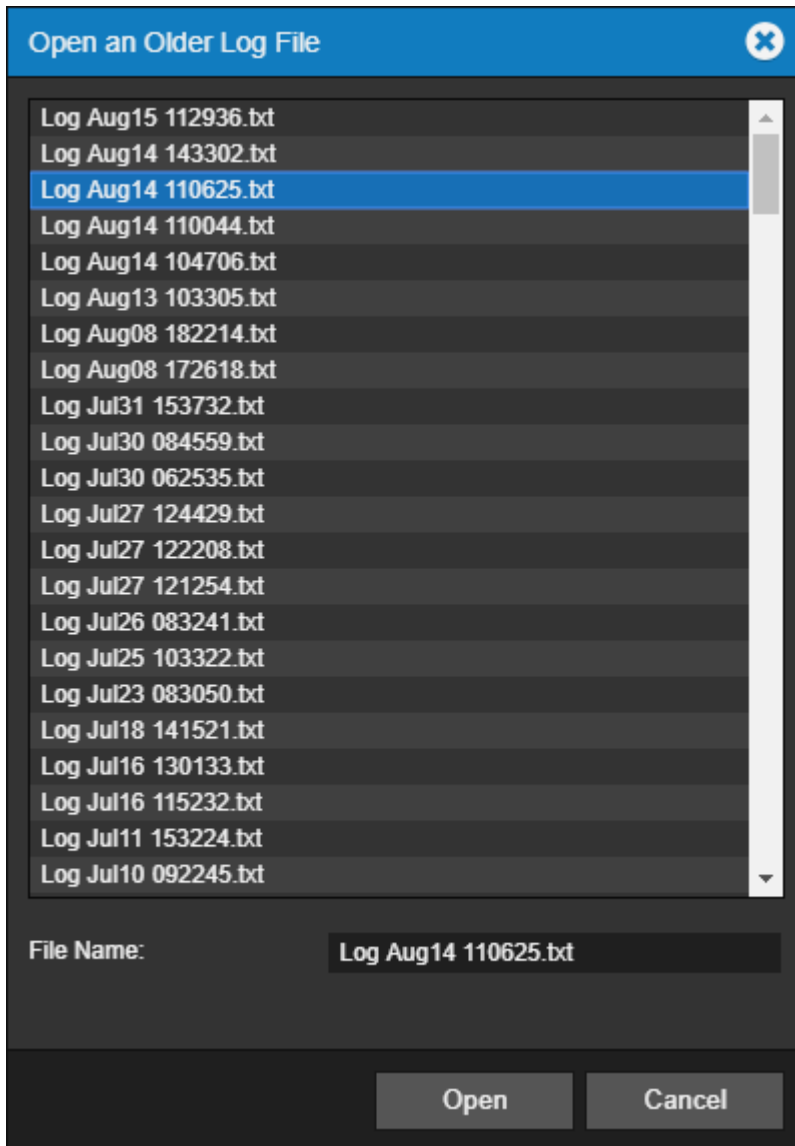
Open Older Log File

This command opens the available log data reside in the <Install Drive>:\Eaton Corporation\Foreseer\LogFiles folder.

1. Select Upload Files from the Server List menu



2. Select the file you are interested in viewing



3. View the report you selected.

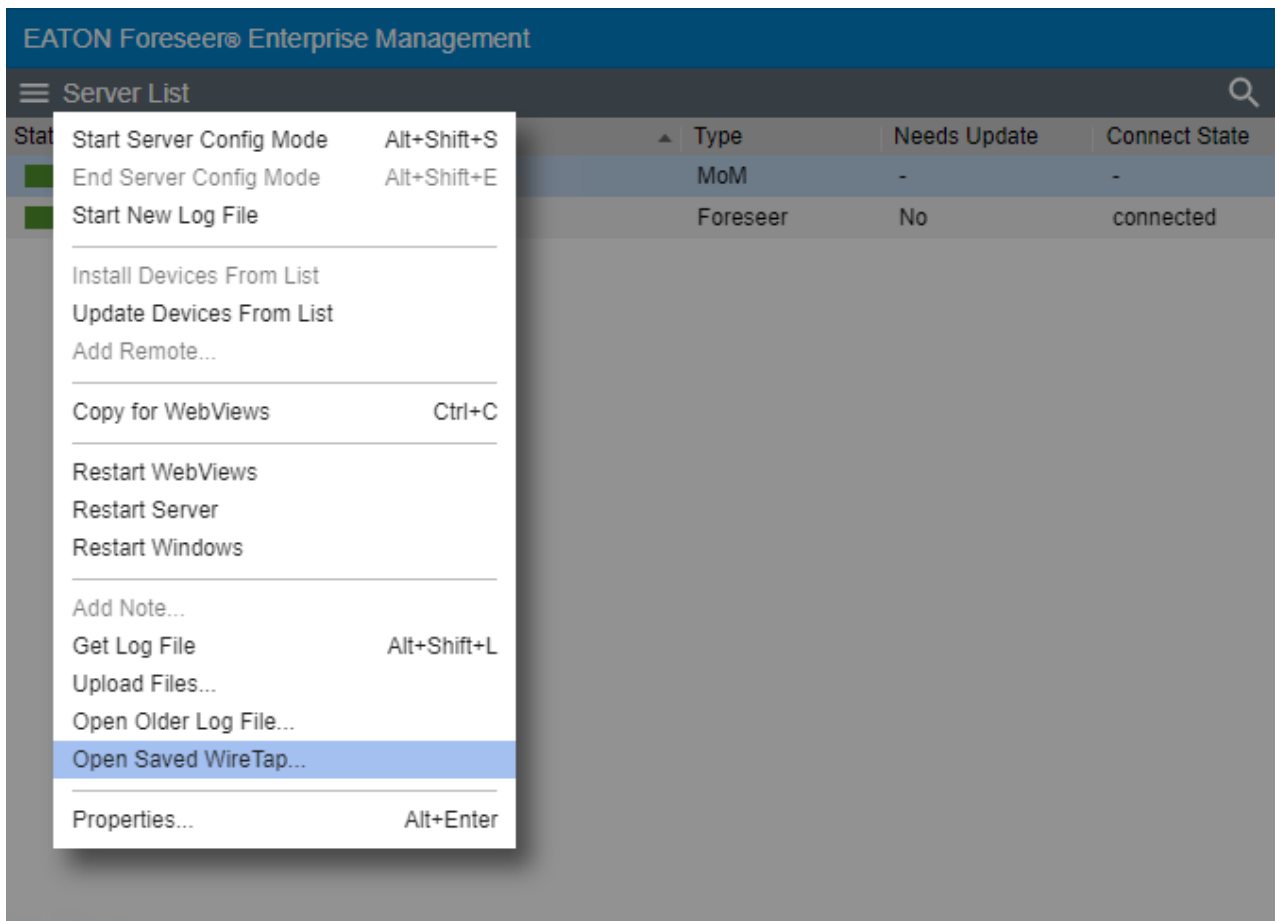
```
Log File Report
Report Time 08/14/18 10:47:06

08/14/18 10:47:06: Initializing Eaton Foreseer, Version: 7.0.54.0
08/14/18 10:47:06: Working directory: C:\Foreseer\Branches\Foreseer 7R\BUILD\x64\Release\
08/14/18 10:47:06: Running as an application
08/14/18 10:47:06: ServiceThreadProc thread started with thread id: 0xdc8
08/14/18 10:47:07: Initializing Network Interfaces...
08/14/18 10:47:07: Initializing FileSystem Objects...
08/14/18 10:47:07: Establishing Server State...
08/14/18 10:47:07:     checking the Config Restore folders
08/14/18 10:47:07:     creating server stores.
08/14/18 10:47:07:     processing existing server document.
08/14/18 10:47:07: Opening Server Document...
08/14/18 10:47:07: Reading Server Document: Version 0x070024
08/14/18 10:47:07:     Server Name: 7044 Test 1
08/14/18 10:47:07: Checking Account Impersonation...
08/14/18 10:47:07: Not using impersonation
08/14/18 10:47:07: Server Archive thread started with thread id: 0xca8
08/14/18 10:47:07: The last database session was ended without error.
08/14/18 10:47:07:     finishing network initialization.
08/14/18 10:47:07: Initializing Server Objects...
08/14/18 10:47:07: Eaton Foreseer is licensed for 25088 channels.
```

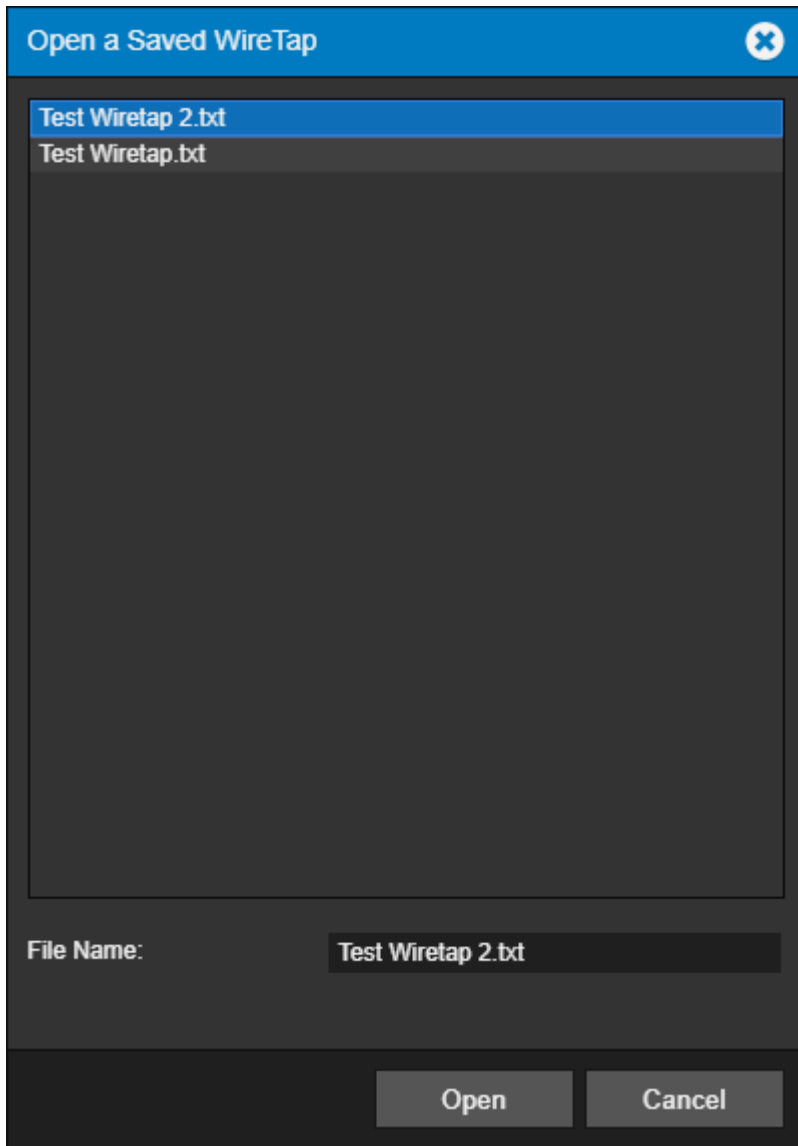
Open Saved Wiretap

This command opens the available wiretap files that reside in the <Install Drive>:\Eaton Corporation\Foreseer\WireTaps folder.

1. Select Upload Files from the Server List menu



2. Select the file you are interested in viewing



3. View the wiretap you selected.

```

Eaton Foreseer wiretap - Test Wiretap 2.txt - Google Chrome
//localhost/React/download.py?file=Test%20Wiretap%202.txt&type=wiretap

WireTap Started

WireTap File Created: 11/25/18 16:42:35
Device Name: IQ 250 1 (Unit: 1)
Communications Settings: 127.0.0.1 Port: 8001
Configuration: 7-C-H Meter IQ 250 TCP.vi, Version: r.1.1
DLL Path: C:\Foreseer\Branches\Foreseer 7R\BUILD\x64\Release\vi\7-Modbus3.dll
DLL Version: 7.1.37.12, Common Version:7.1.0

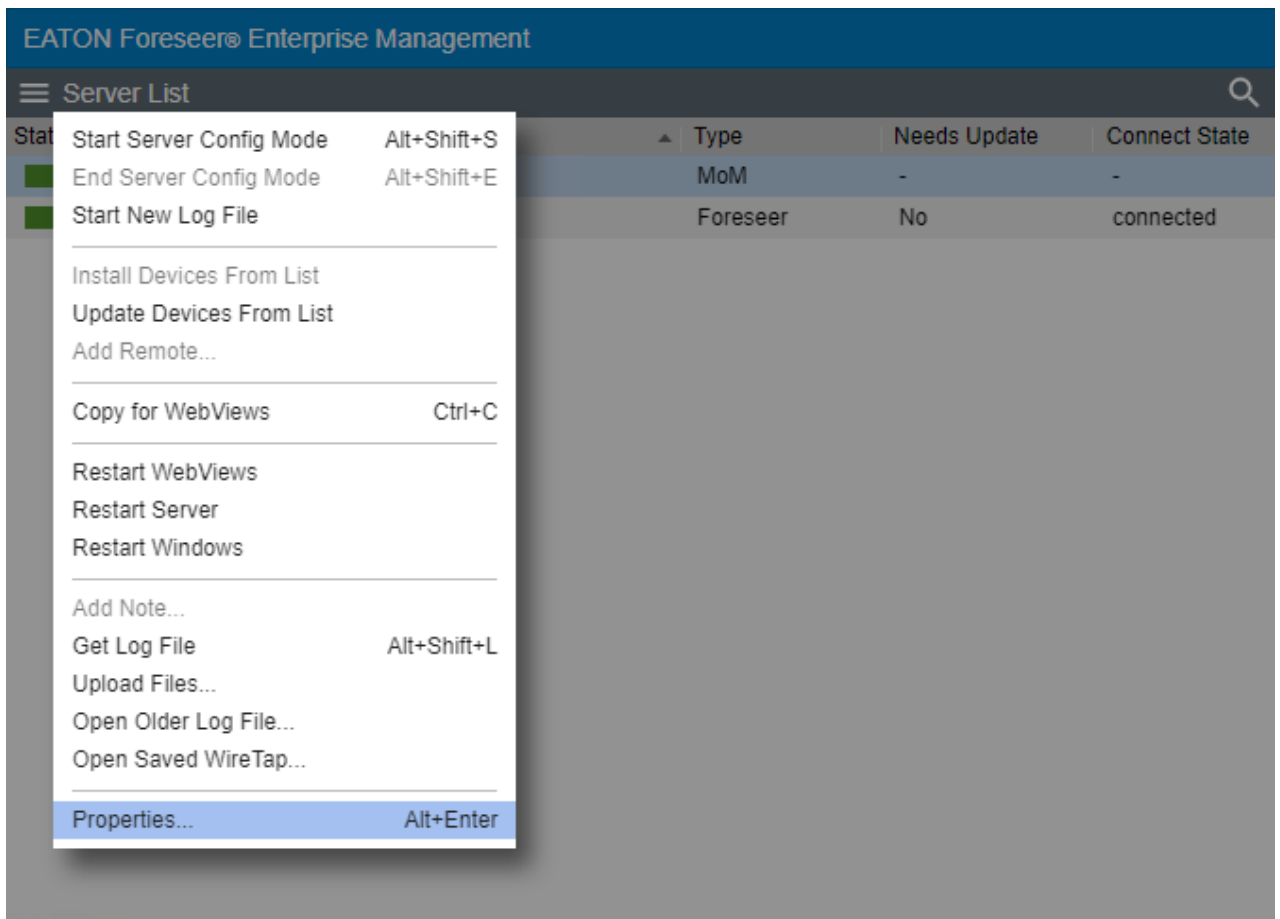
XMIT 12 bytes (16:42:35, 125 ms since last message)
 \81\AE\00\00\00\06\01\03\03\E7\00\36 [.....6]
RECV 9 bytes (16:42:35, 0 ms since last message)
 \81\AE\00\00\00\06F\01\03\6C [.....o..1]
RECV 108 bytes (16:42:35, 0 ms since last message)
 \43\8A\8F\87\43\8A\5B\37\43\8A\39\27\43\F0\AD\12\43\F1\2D\F0\43\F1\2D\33\42 [C...C.
 [7C.9'C...C.-.C.-3B]
 \BB\52\74\42\BB\3F\3C\42\BB\5D\0B\47\8A\87\3E\47\01\36\14\47\97\A6\66\3F\61 [.RtB.?
 <B.].G.>G.6.G..f?a]
 \87\CF\42\70\98\D2\43\8C\6D\B8\46\B8\F4\13\46\B9\44\FA\46\B8\2C\EE\46\2C\99
 [..Bp..C.m.F...F.D.F.,.F,.]
 \5F\46\2C\04\A0\46\2B\D4\23\46\CA\D0\B4\46\CA\BC\90\46\CA\69\EA\3F\62\AB\5C
 [_F,..F+.#F...F...F.i.?b.\]
 \3F\6D\31\89\3F\54\40\71 [?m1.?T@q]
XMIT 12 bytes (16:42:35, 62 ms since last message)

```

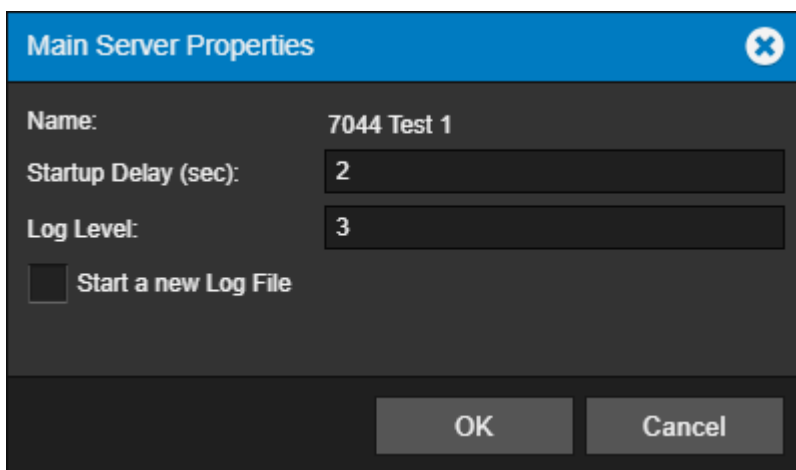
Properties

The properties dialog box provides a way to change the logging level as well as another way to start a new log file. It also reports on the server name and startup delay value.

1. Select Properties from the Server List menu



2. The Main Server Properties dialog allows you to change the Startup Delay as well as change the Log Level.
 - 1 is errors only
 - 3 is normal
 - 4 - 10 is verbose



Remote Server List Menu

The Remote Server List menu provides access to all of the functionality that will be required

to manage your Remote / Redundant Foreseer servers.

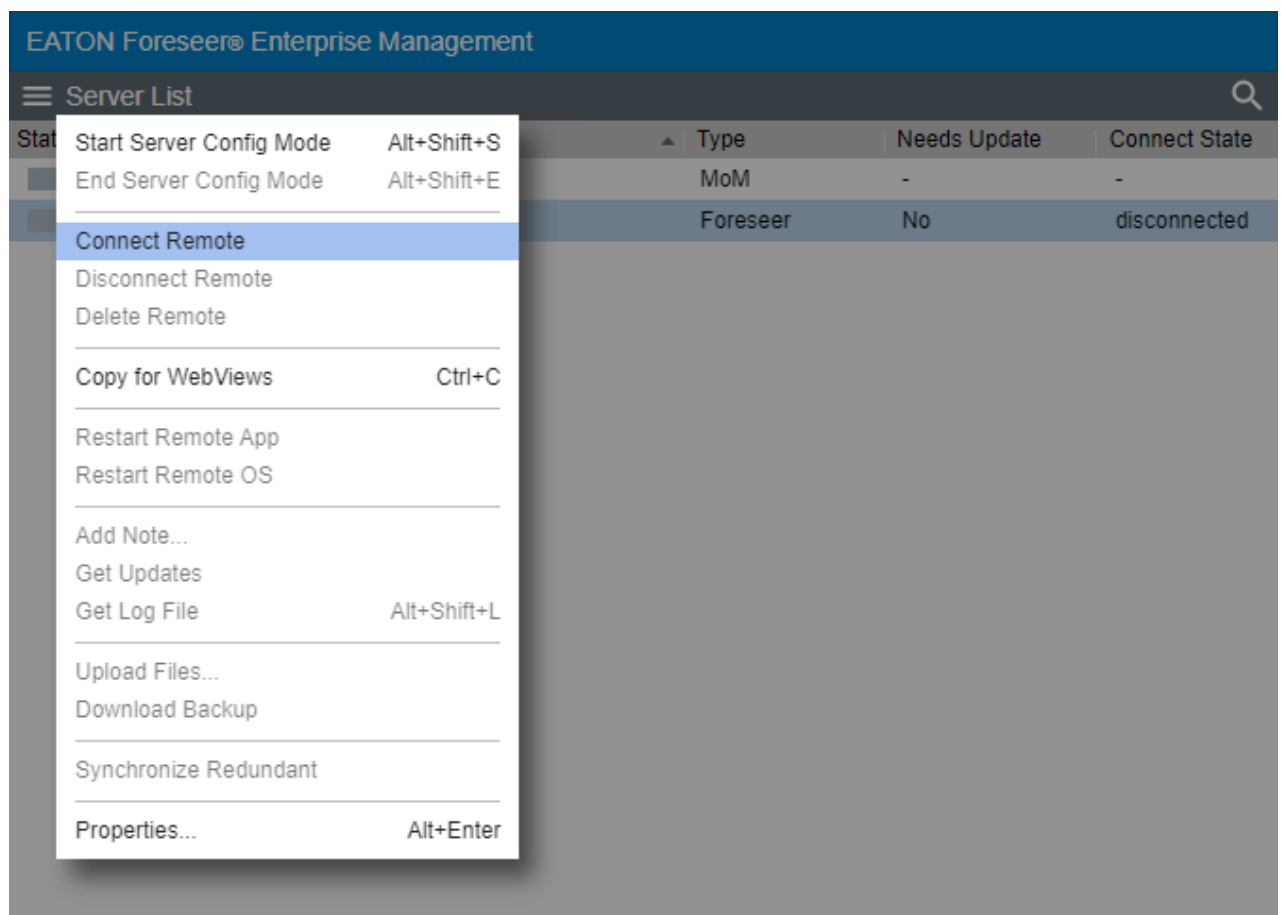
- Connect Remote
- Disconnect Remote
- Delete Remote
- Copy for WebViews
- Restart Remote App
- Restart Remote OS
- Add Note
- Get Updates
- Get Log File
- Upload Files
- Download Backup
- Synchronize Redundant
- Properties

Connect Remote

The Connect Remote function connects the Remote Foreseer server to the local server.

To connect the remote server:

1. Select Connect Remote from the Server List menu.



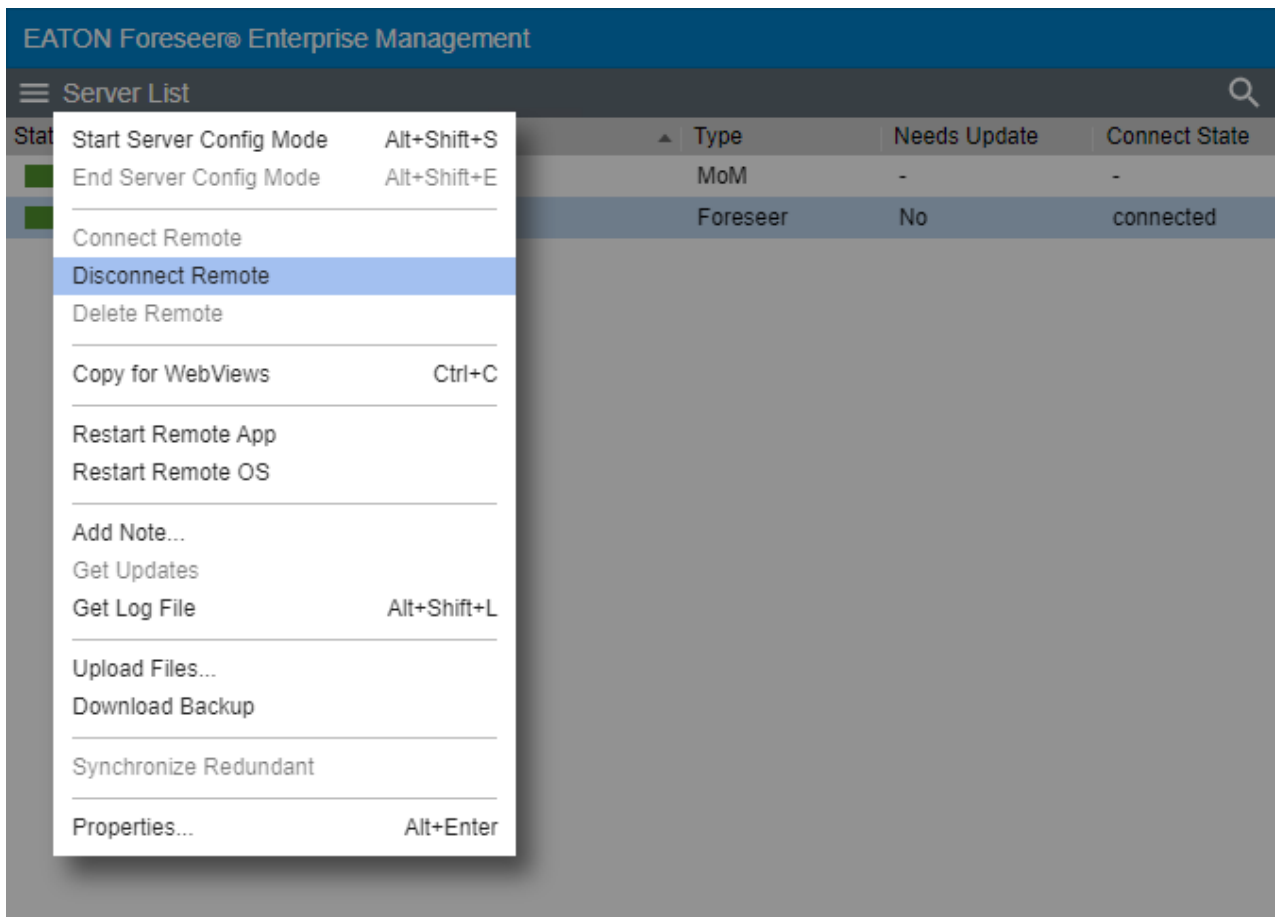
2. The remote server will now be connected to the local server

Disconnect Remote

The Disconnect Remote function disconnects the Remote Foreseer server from the local server.

To disconnect the remote server:

1. Select Disconnect Remote from the Server List menu.



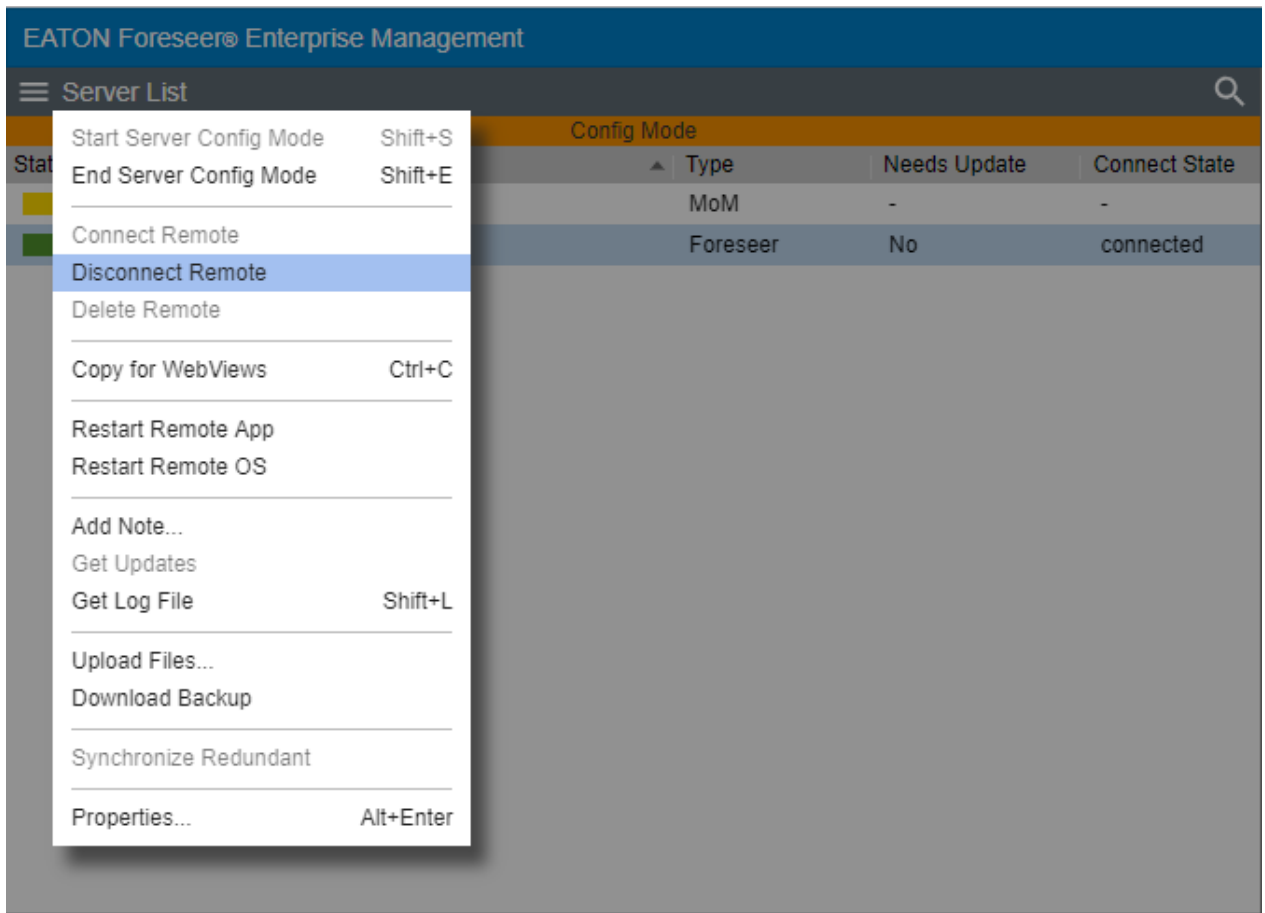
2. The remote server will now be disconnected from the local server

Delete Remote

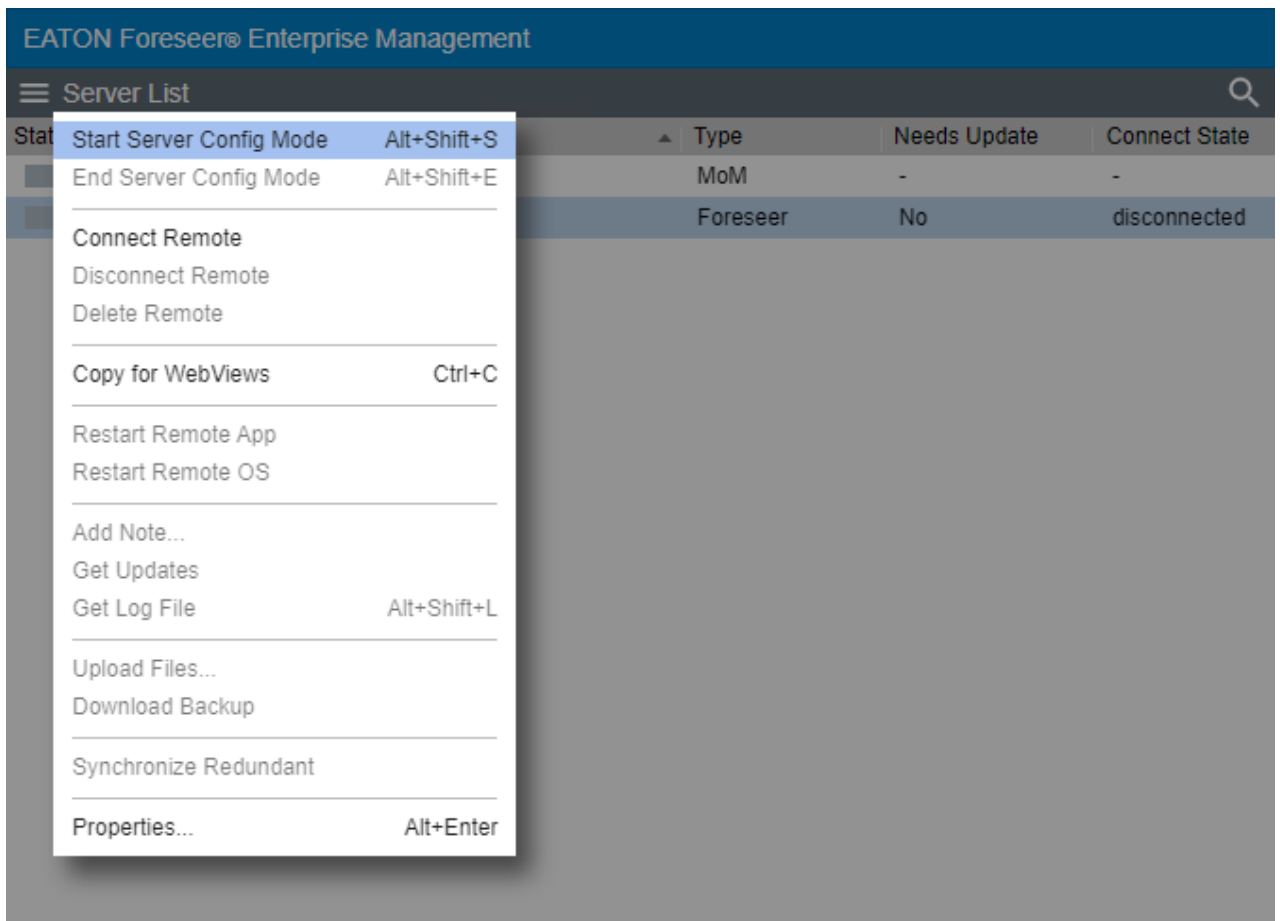
The Delete Remote function deletes the Remote Foreseer server from the local server.

To delete the remote server:

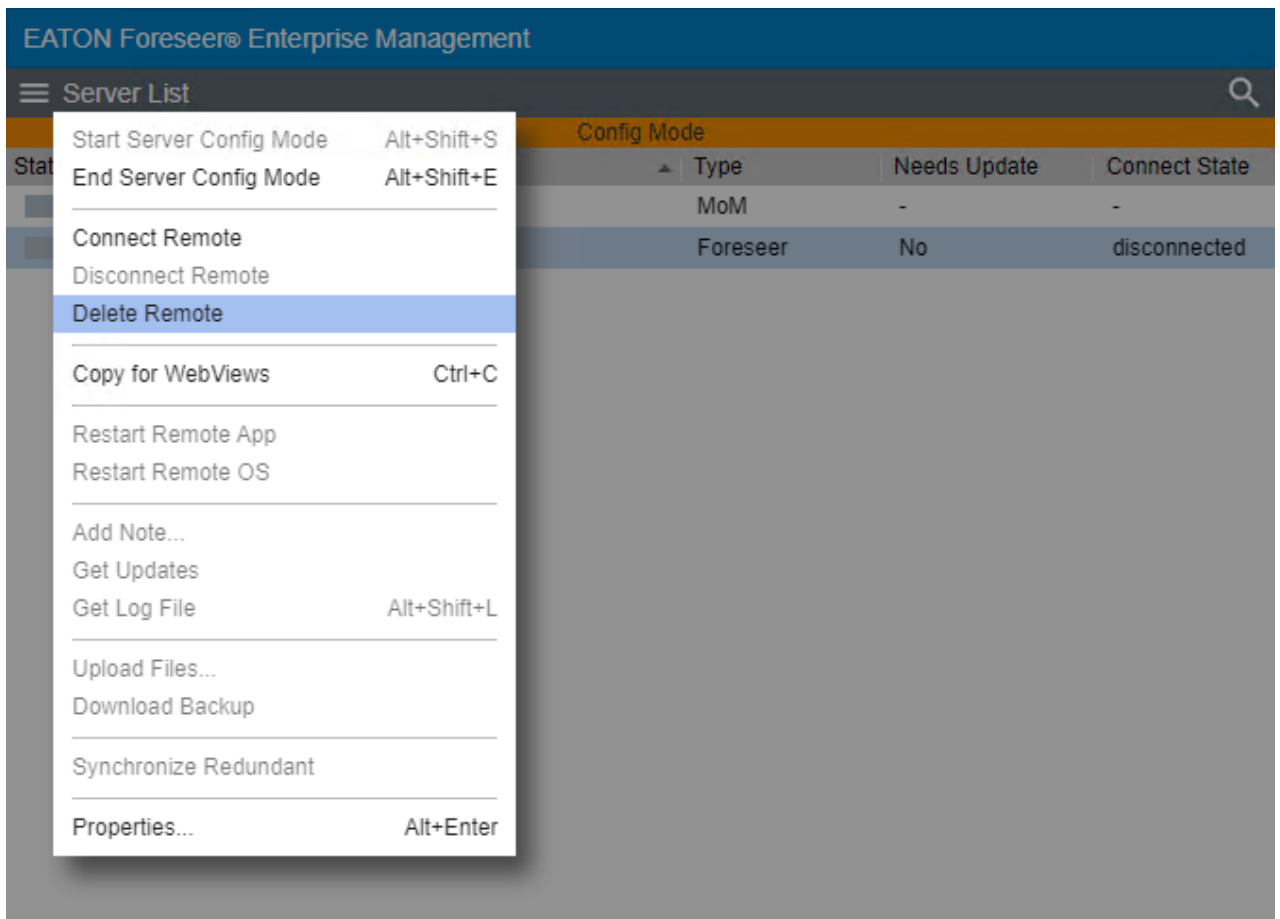
1. Select Disconnect Remote from the Server List menu.



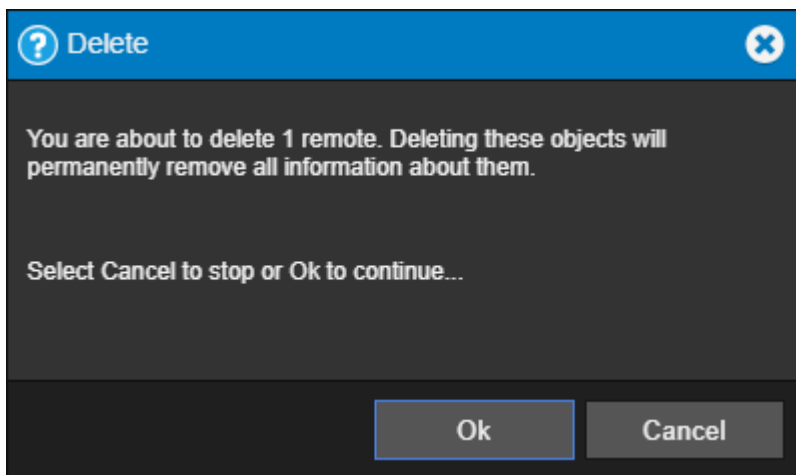
2. Select the local server and Start Server Config Mode



3. Highlight the Remote Server and Delete Remote from the Remote Server List Menu

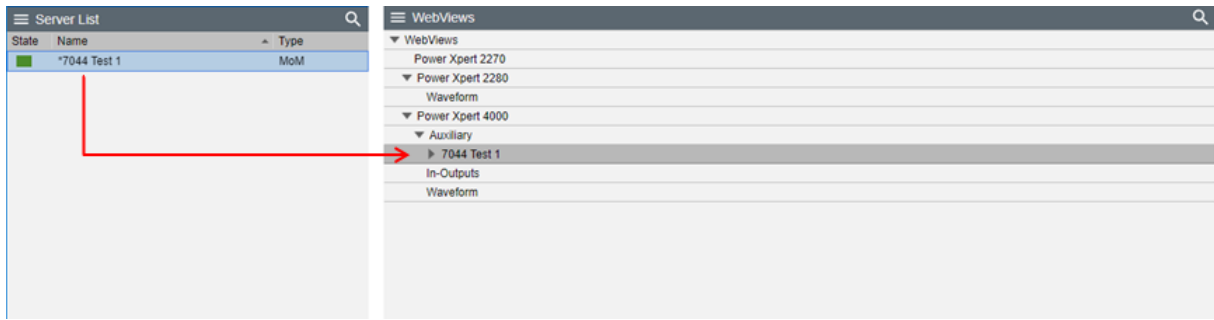


4. A confirmation dialog will appear. Click OK to continue.



Copy for WebViews

This function copies the target and all child devices and their channels to the target folder in the WebViews tree. The server itself is given a subfolder under the target WebViews folder, and each device is given a sub folder of its own under the server folder.

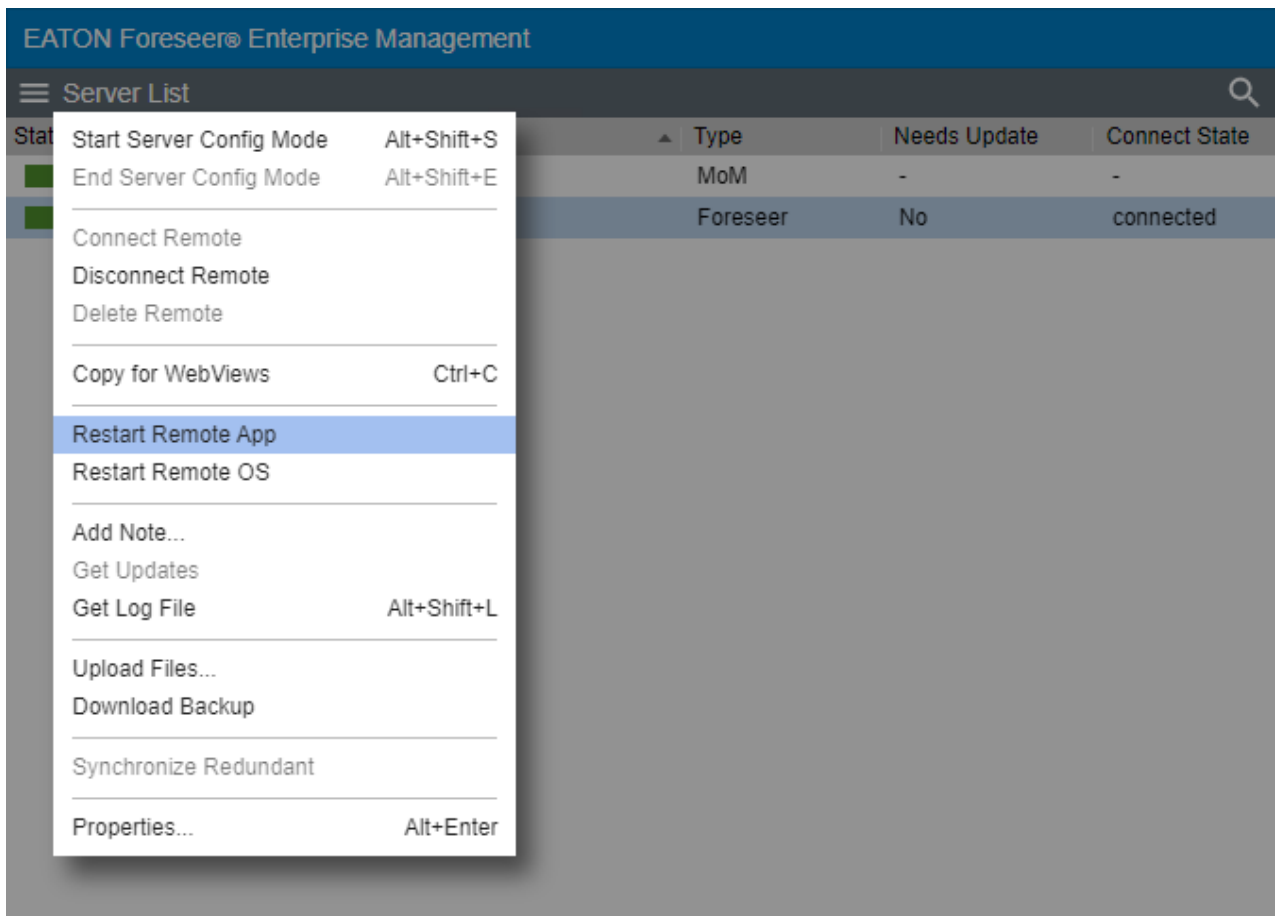


In the example shown above, “WebViews Copy”, the Local server is copied and then pasted into the Power Expert 4000 folder under WebViews. Note that the folder structure mimics the device structure under the server. Instead of copying the entire server, you can also copy individual devices and their channels to a location in the WebViews tree.

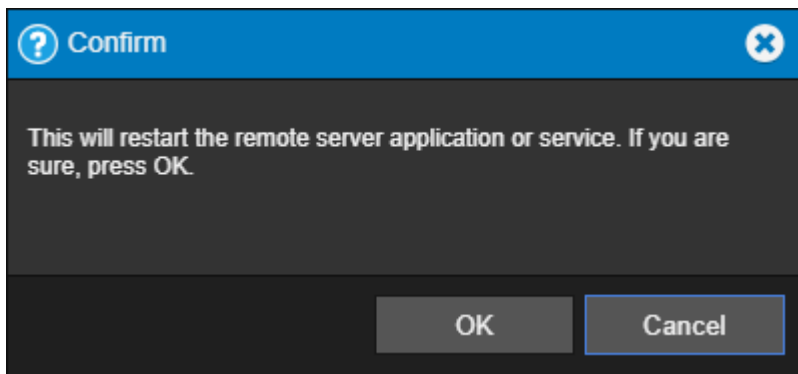
Restart Remote App

The Restart Remote App function restarts the Foreseer application instance (both http and https connections will be reset).

1. Select Restart Remote App from the Remote Server List menu.



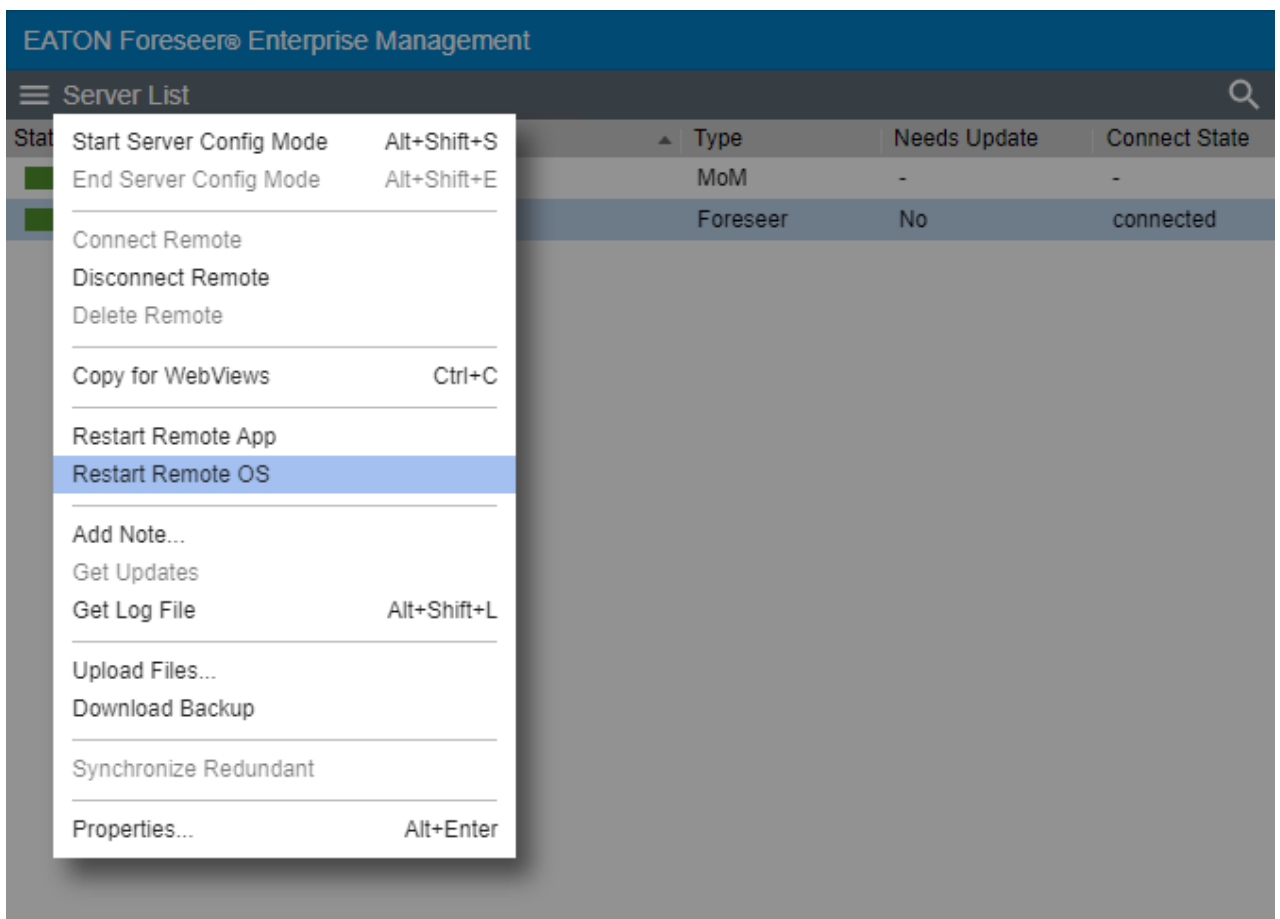
2. Select OK to continue this request.



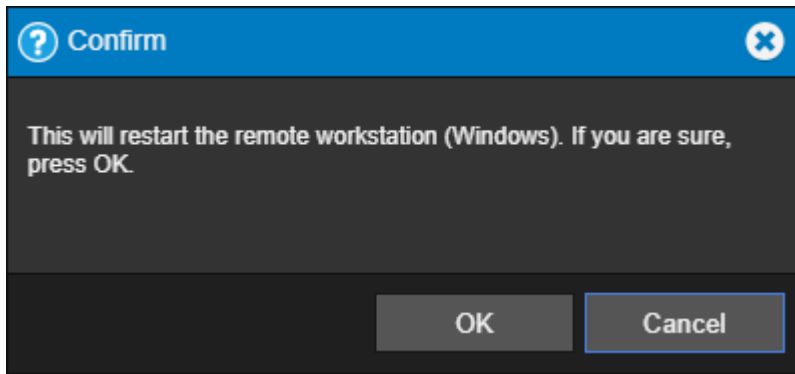
Restart Remote OS

The Restart Remote OS function restarts the remote server instance (Windows).

1. Select Restart WebViews from the Server List menu.



2. Select OK to continue this request.

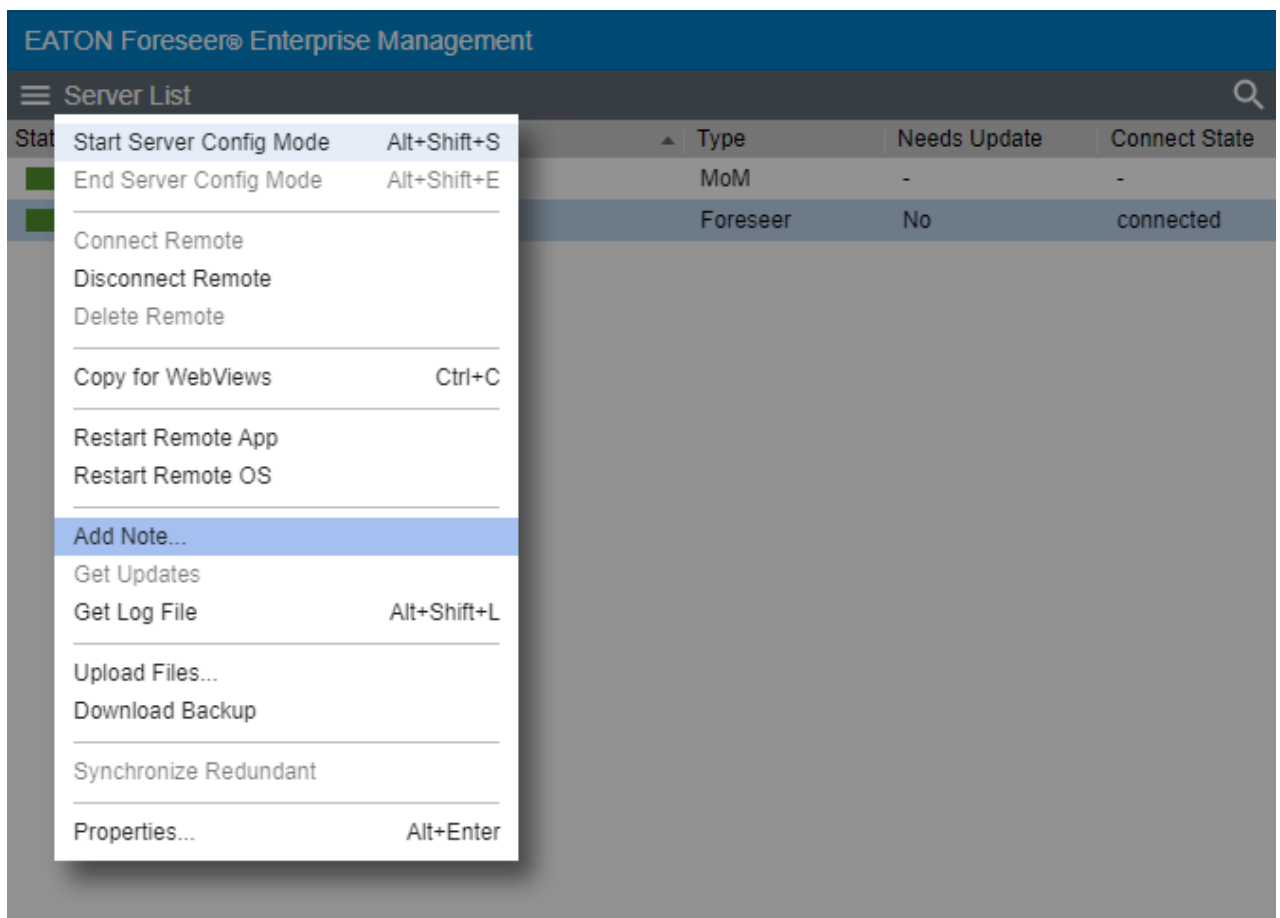


Add Note

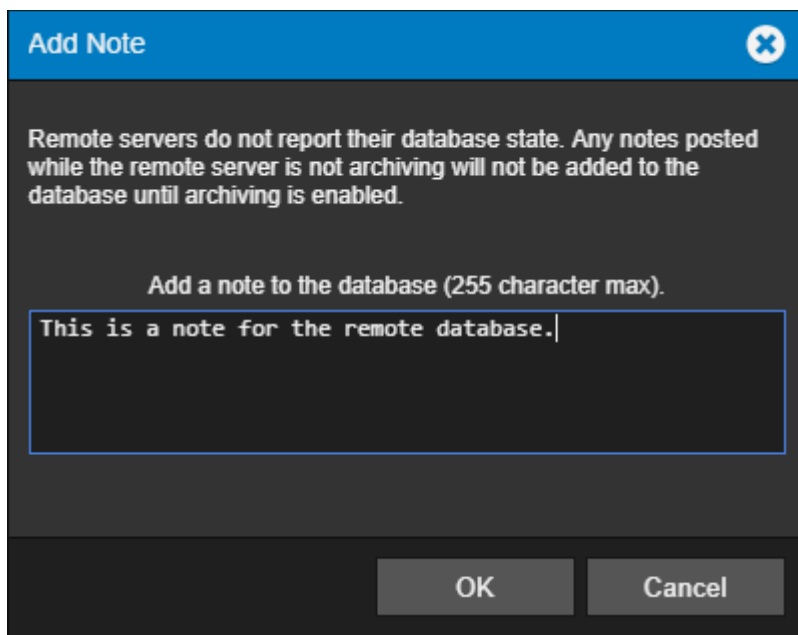
You can use the Add Notes feature to record any supplemental information relevant to a particular event when it occurs. The notes are logged into the Server's database and can be reviewed by authorized Foreseer clients or retrieved in Foreseer Reports. An unlimited number of real-time notes may be entered, but they are limited to 255 characters each. A typical use for Foreseer notes is to add information during the course of Acknowledging and/or Rearming alarms.

To create a note:

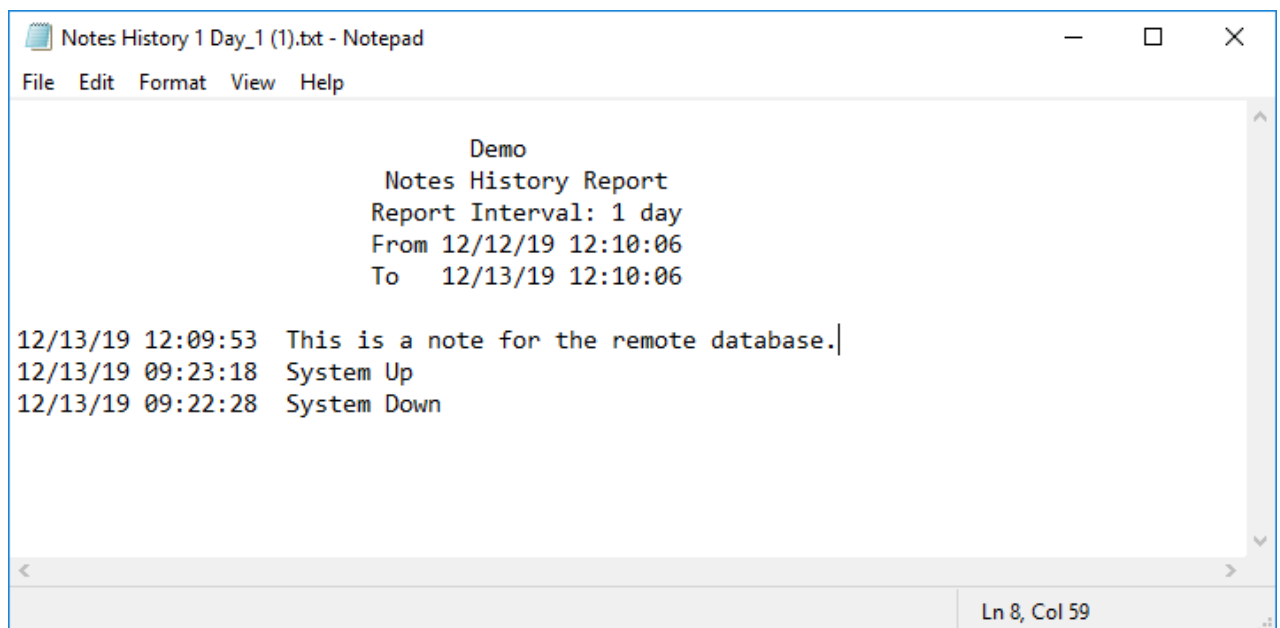
1. Select Add Note from the Server List menu



2. In the note editor dialog box, type a note (not exceeding 255 characters).



3. Select OK to continue.
4. The database note can now be reported on in the Notes History Report



Get Updates

The Restart WebViews function restarts the Foreseer WebViews instance (both http and https connections will be reset). Select OK to continue this request.

1. Start Server Config Mode Server List menu
2. Highlight the remote that needs updates
3. Select Get Update from the Server List menu

- The systems will update and notify the user that is now waiting for Server Config Mode to end

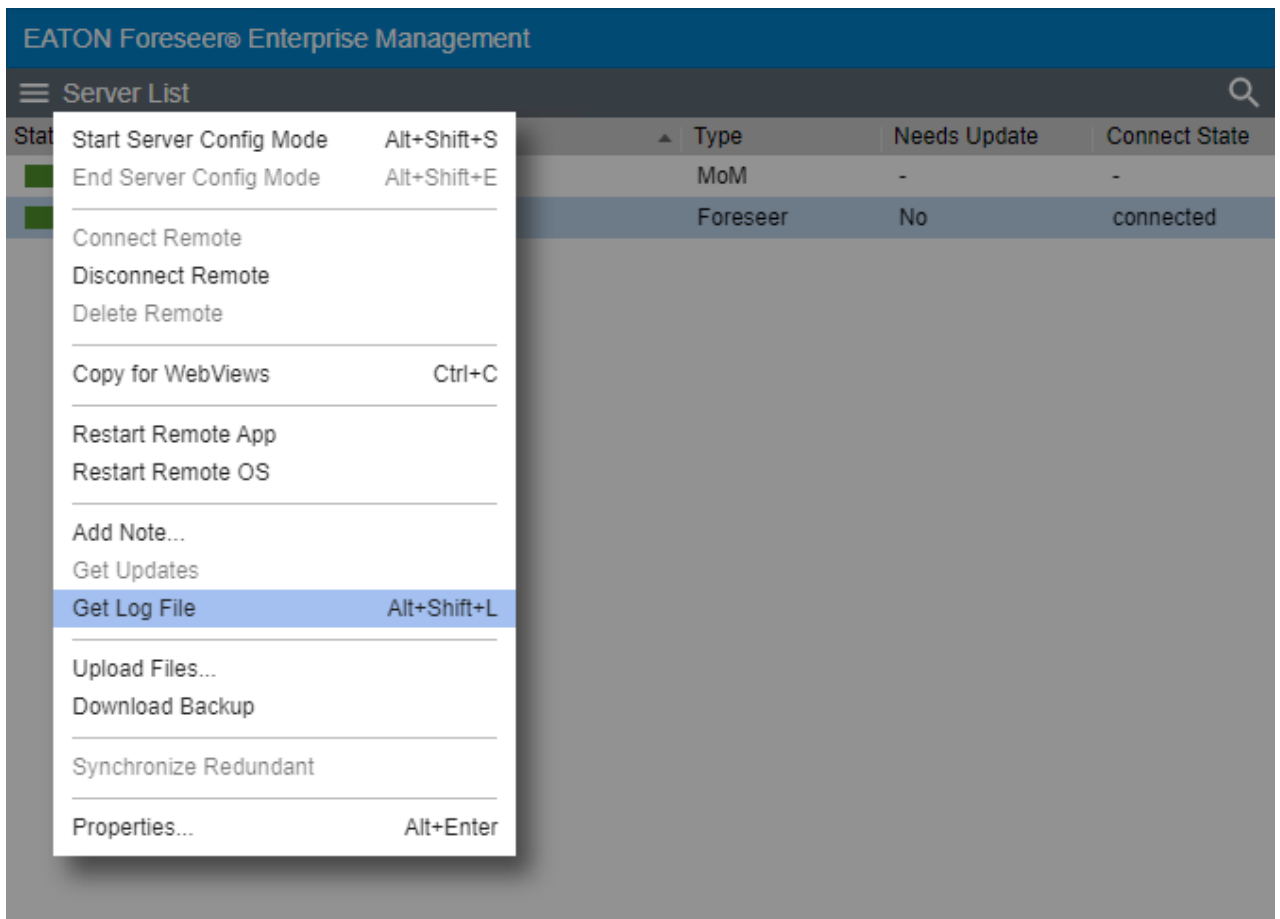
EATON Foreseer® Enterprise Management				
Server List				
Config Mode				
State	Name	Type	Needs Update	Connect State
■	*7044 Test 1	MoM	-	-
■	Remote - 7044 Test 1	Foreseer	No	wait config end...

- End Server Config mode and the system will be updated

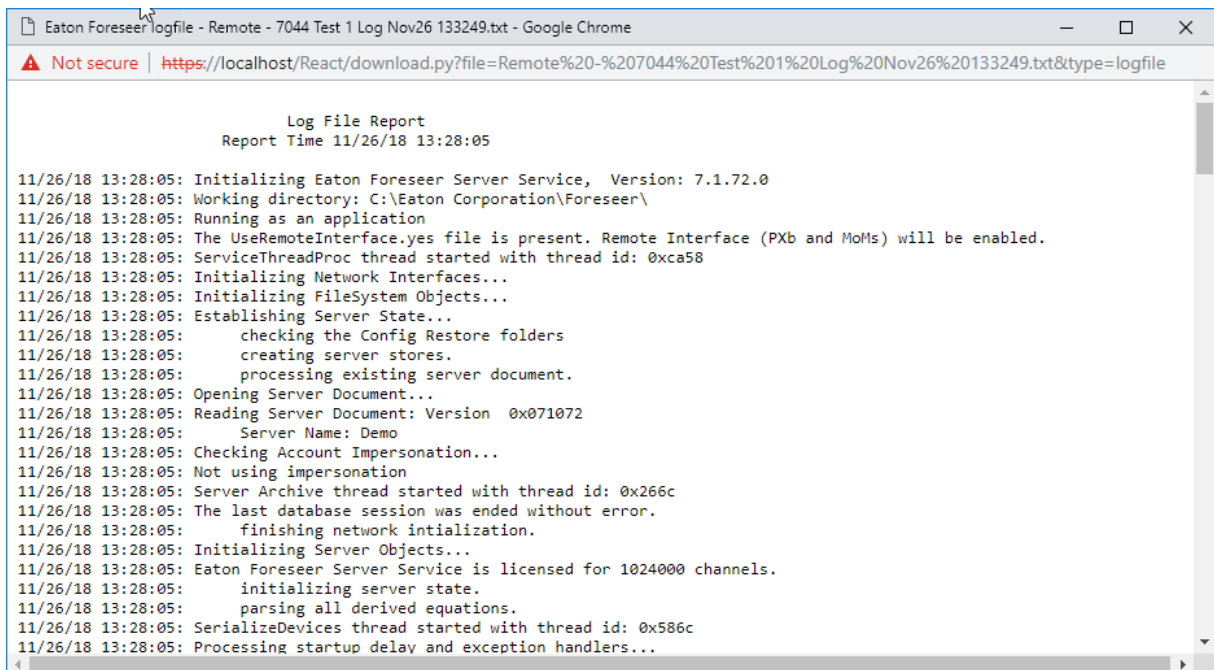
Get Log File

The Get Log File retrieves the log file from the remote Foreseer server.

- Select Get Log File from the Server List menu.



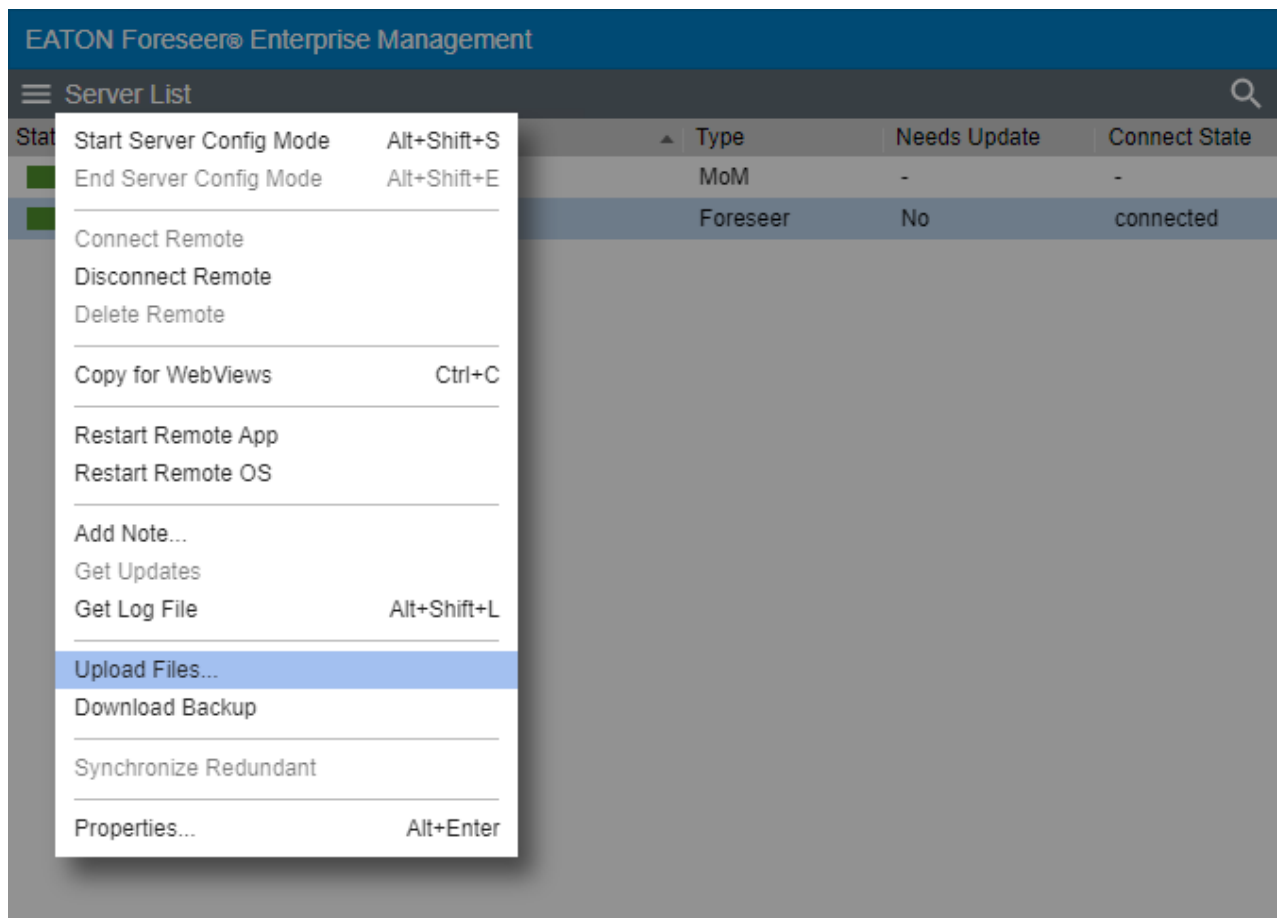
- The most recent log file will be displayed. (Make sure that pop-ups are not blocked in the browser.)



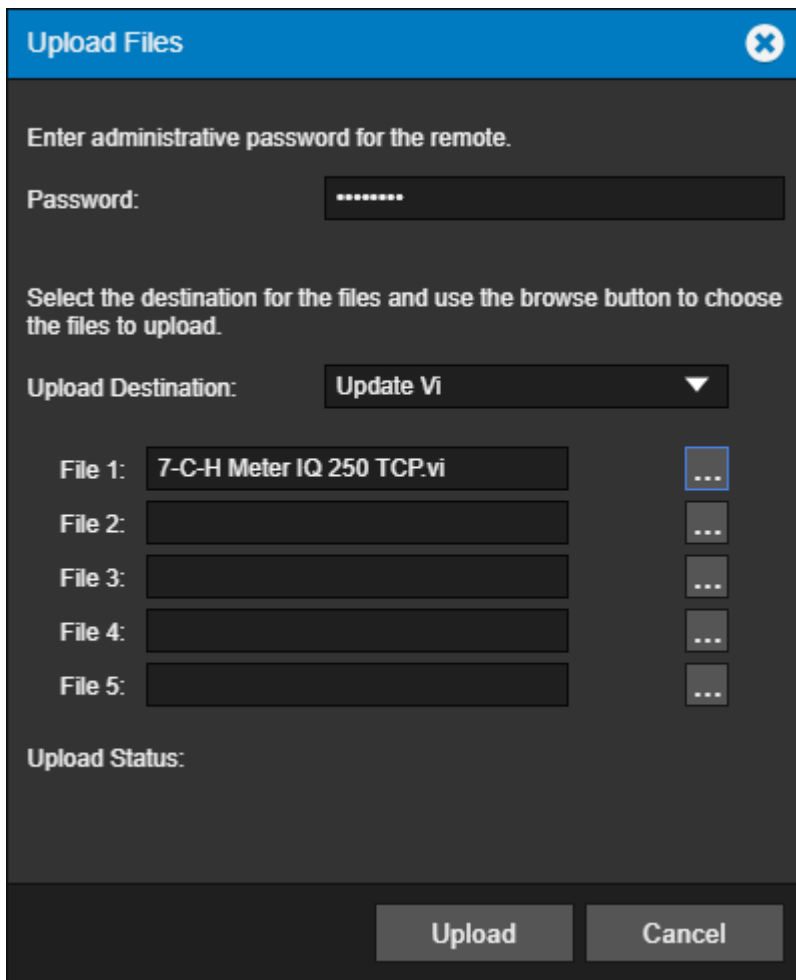
Upload Files

The Upload Files function provides a general-purpose file upload utility, useful for adding graphics, drivers, and other files to the server from a remote location. You can select up to five files to upload simultaneously, as well as selecting the target folder on the server. Target folder selections are limited to those within the Foreseer installation tree to which one would legitimately have a reason to upload files. Using this feature, you can upload common files used by Foreseer including .VI driver files, and .ARQ backups for restoration purposes.

1. Select Upload Files from the Remote Server List menu.



2. Enter the administrative password for the remote machine. Select the destination for the files and use the browse button to choose the files to upload



3. Click Upload to continue

Upload destinations include:

- Update Server
- Update Vi
- WWW/Support
- Config Restore

Download Backup

- ✓ Make certain that the user account used by Foreseer has Full Control permission for all of the directories under the Foreseer installation directory. Otherwise, the backup process may fail.

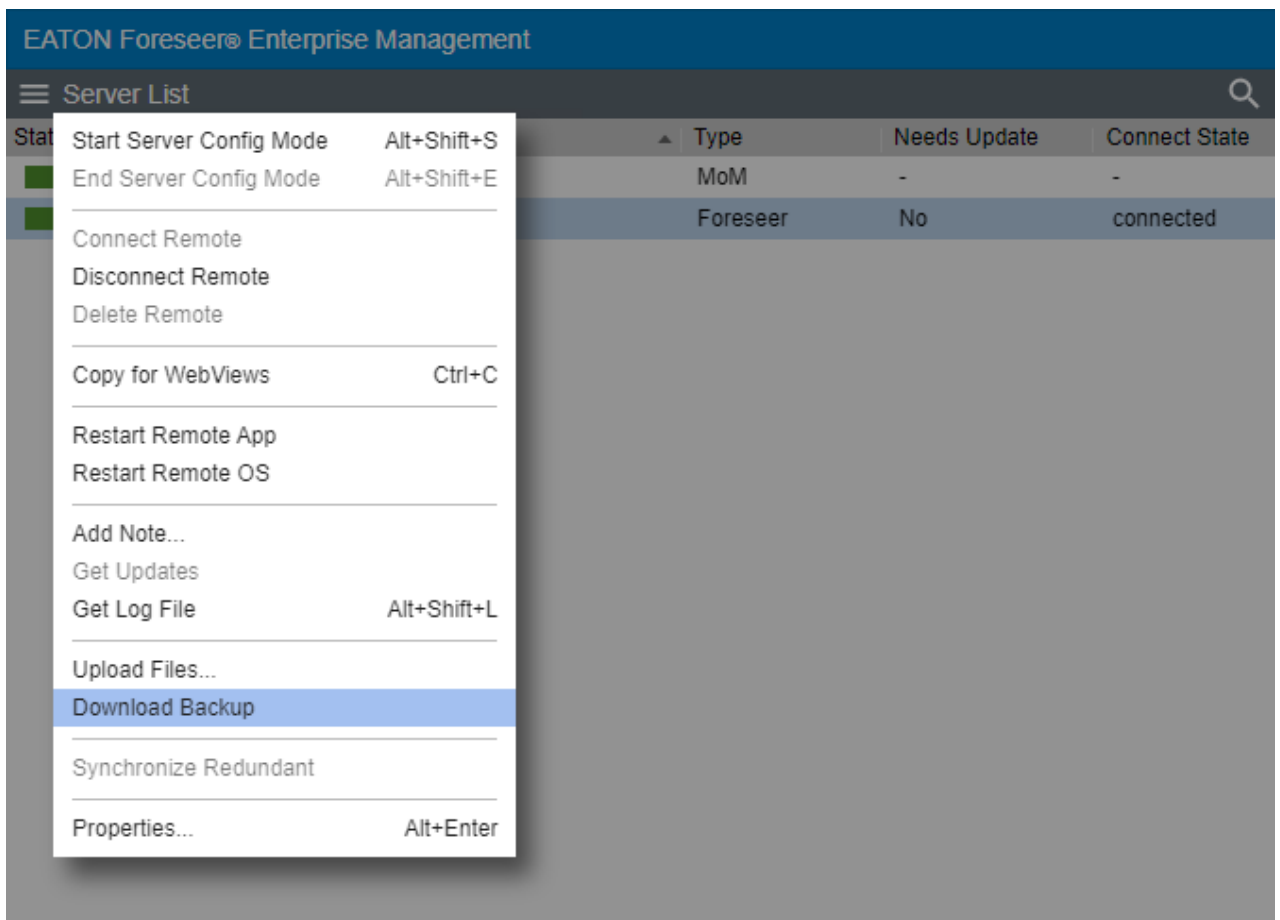
It is strongly recommended that a backup be performed after initial system configuration as well as before and after any significant modifications to ensure maximum disaster recovery capability. You must end server configuration mode before backing up the server configuration.

Significant changes are signaled via the Major Server Version System Channel.

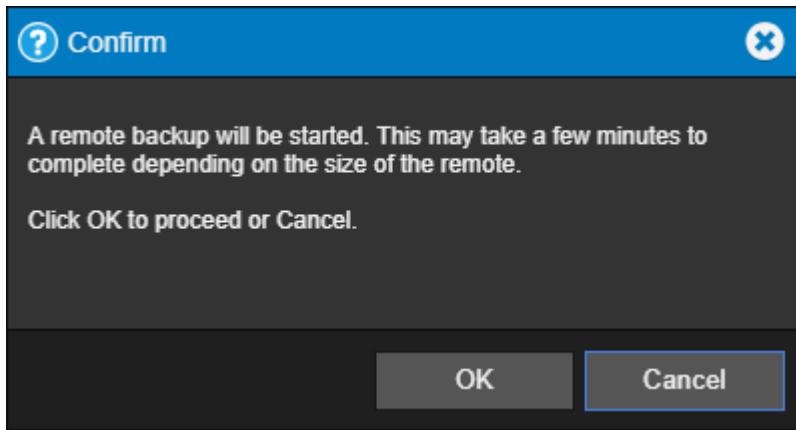
The backup archive (.ARQ) file includes the Foreseer Server configuration only, data files are not backed up in this procedure. Automatic configuration backups can be scheduled through the standalone Foreseer Configuration utility. Backups made through the Web Configuration Utility are automatically assigned a name which is a composite of the name of the server, the date, and the time (in 24-hour format).

To backup a Remote Foreseer Server configuration:

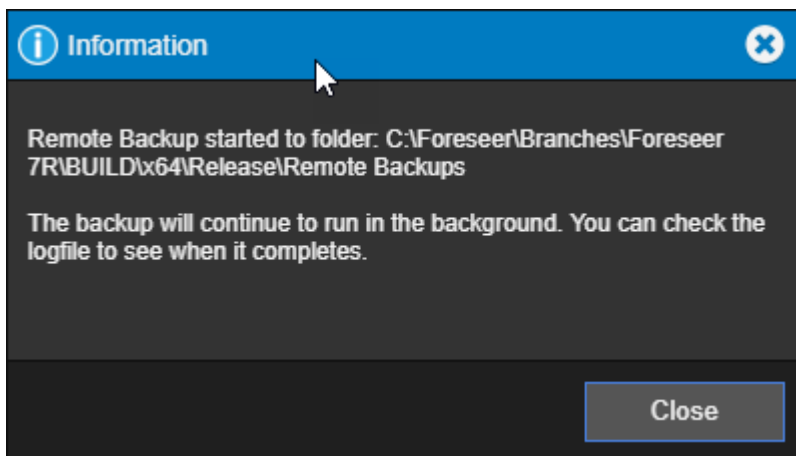
1. Select Download Backup from the Remote Server List Menu.



2. The following information dialog will appear. Click **OK** to continue.



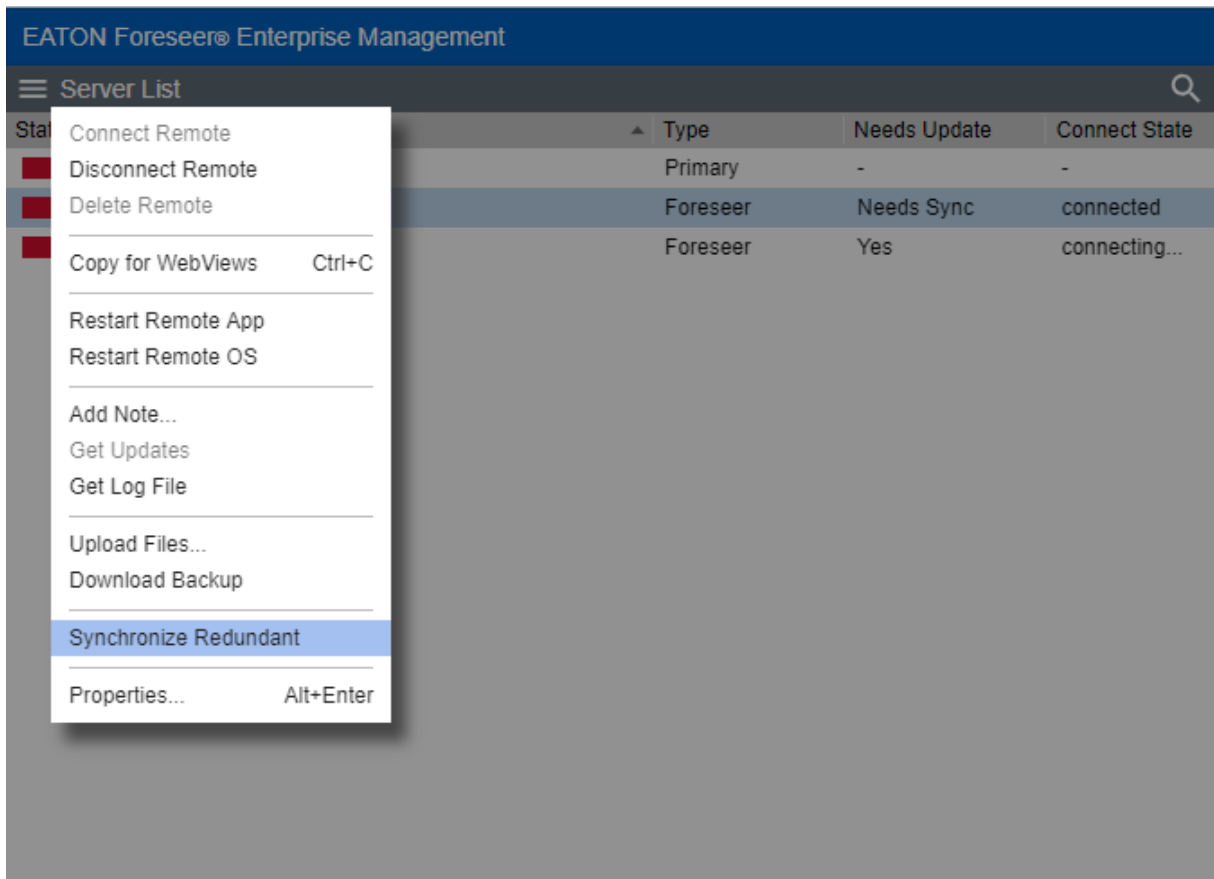
3. Another informational dialog will appear telling the user of the location of the remote backup. Click **Close** to continue



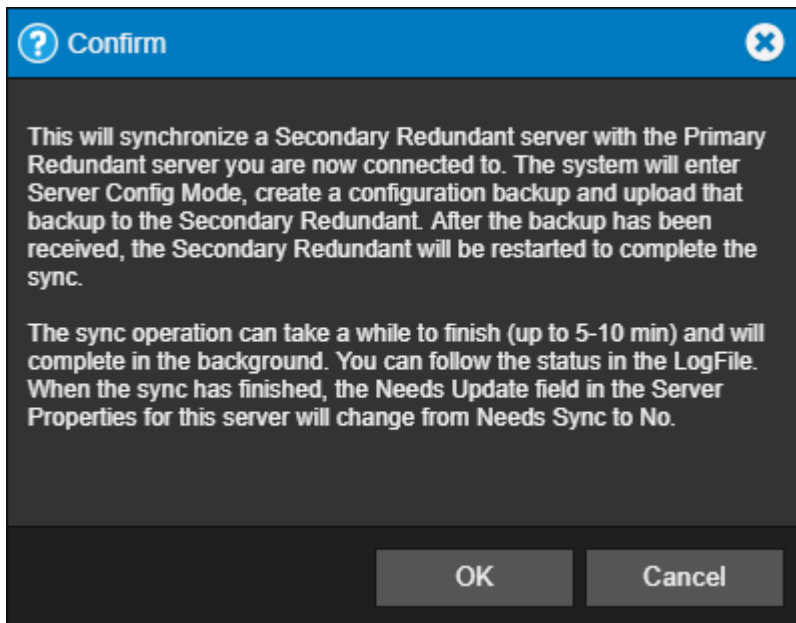
Synchronize Redundant

The Synchronize Redundant function synchronizes the Foreseer secondary redundant with the Foreseer primary server.

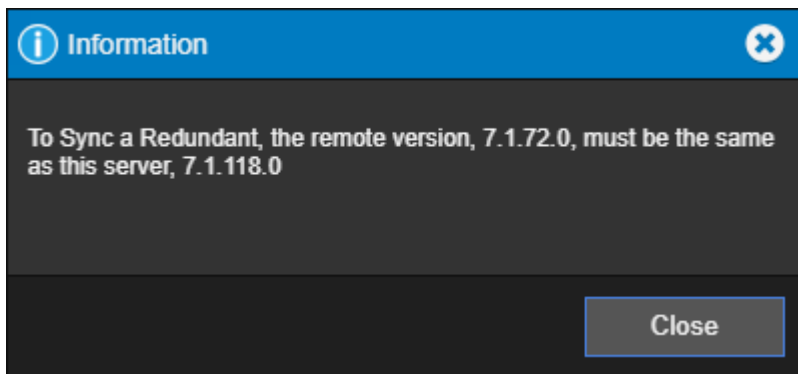
1. Highlight the redundant server that needs synchronizing.
2. Select Synchronize Redundant from the Server List menu.



3. A confirmation dialog describing the synchronization steps. Click OK to continue.



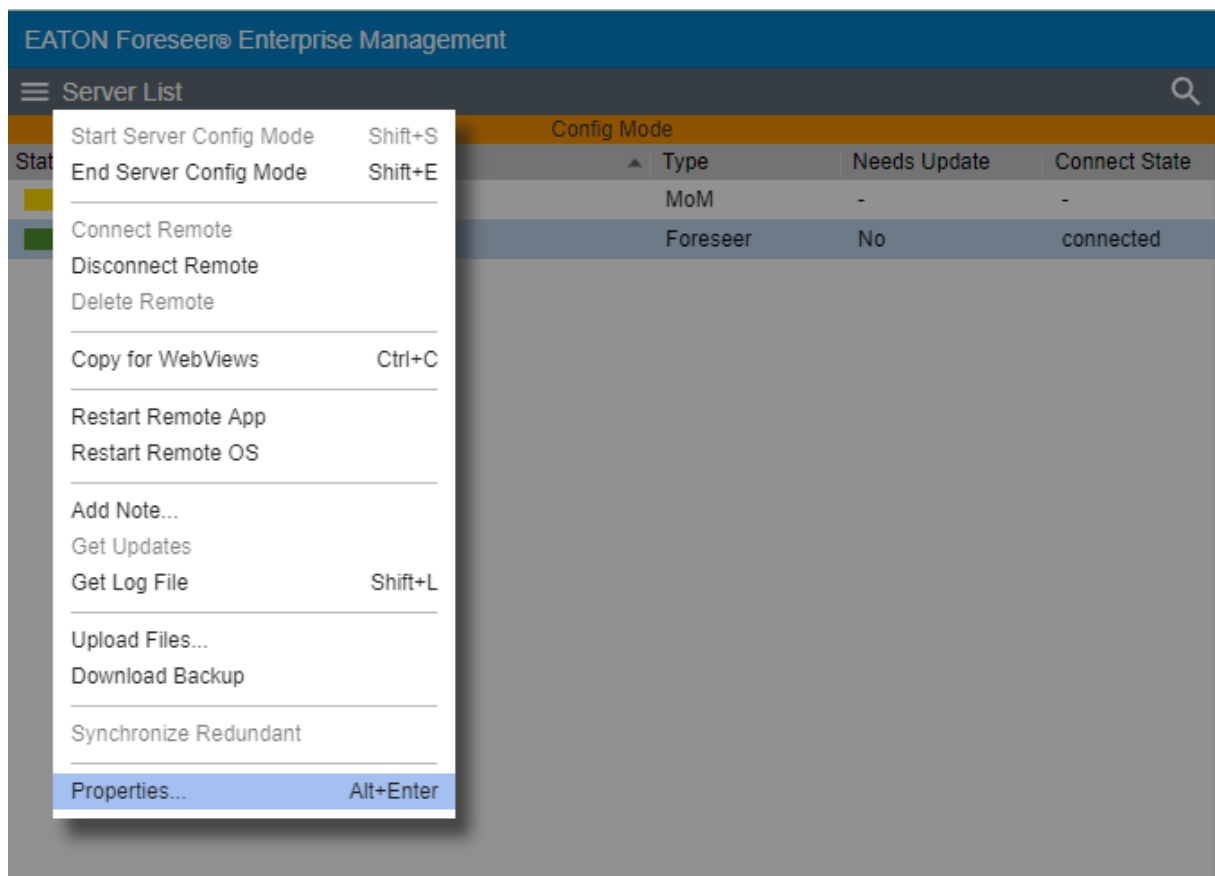
4. If the two environments are not at the same version, an information dialog will be displayed telling you about this discrepancy. The appropriate action will need to be taken to correct this issue.



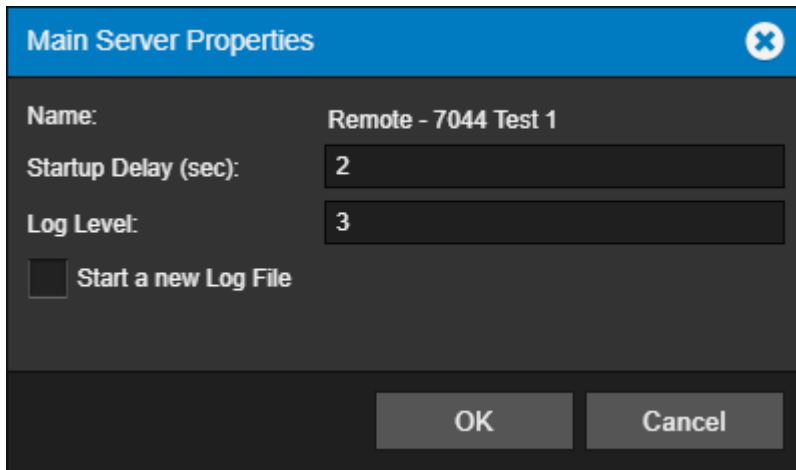
Properties

The properties dialog box provides a way to change the logging level as well as another way to start a new log file. It also reports on the server name and startup delay value.

1. Select Properties from the Remote Server List menu



2. The Main Server Properties dialog allows you to change the Startup Delay as well as change the Log Level.
 - 1 is errors only
 - 3 is normal
 - 4 - 10 is verbose




Device List Menu

The Device List menu provides access to all of the functionality that will be required to manage your Foreseer devices.

- Enable
- Disable
- Disarm
- Re-Arm
- Delete
- Rename
- Copy for WebViews
- Copy Channel Properties
- Paste Channel Properties
- Create .vi File
- Load Driver
- Unload Driver
- Properties

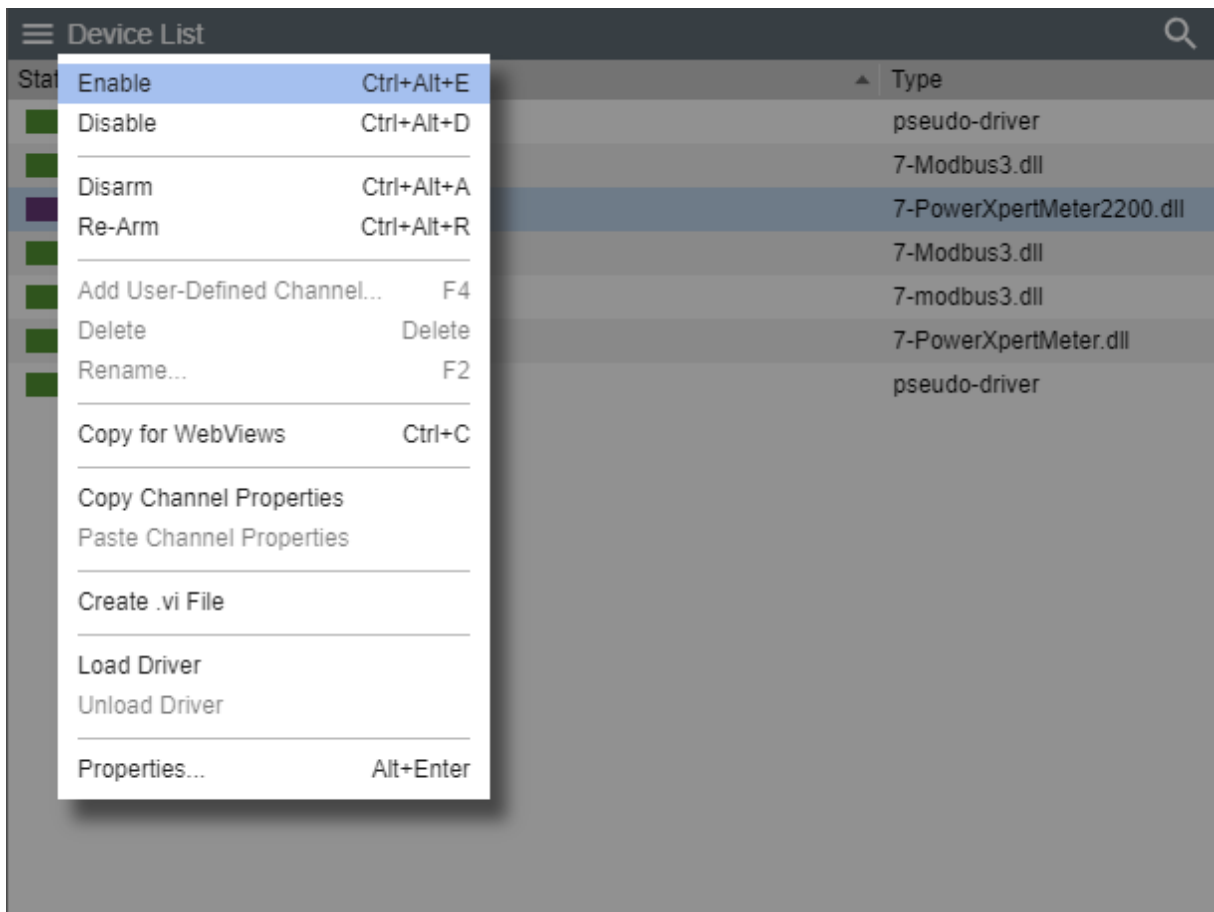
Enable

The enable function resumes all data archiving to the Foreseer Server for the selected Device.

 Administrative Authorization is required before proceeding with this command.

To Enable a device:

1. Select Enable from the Device List menu



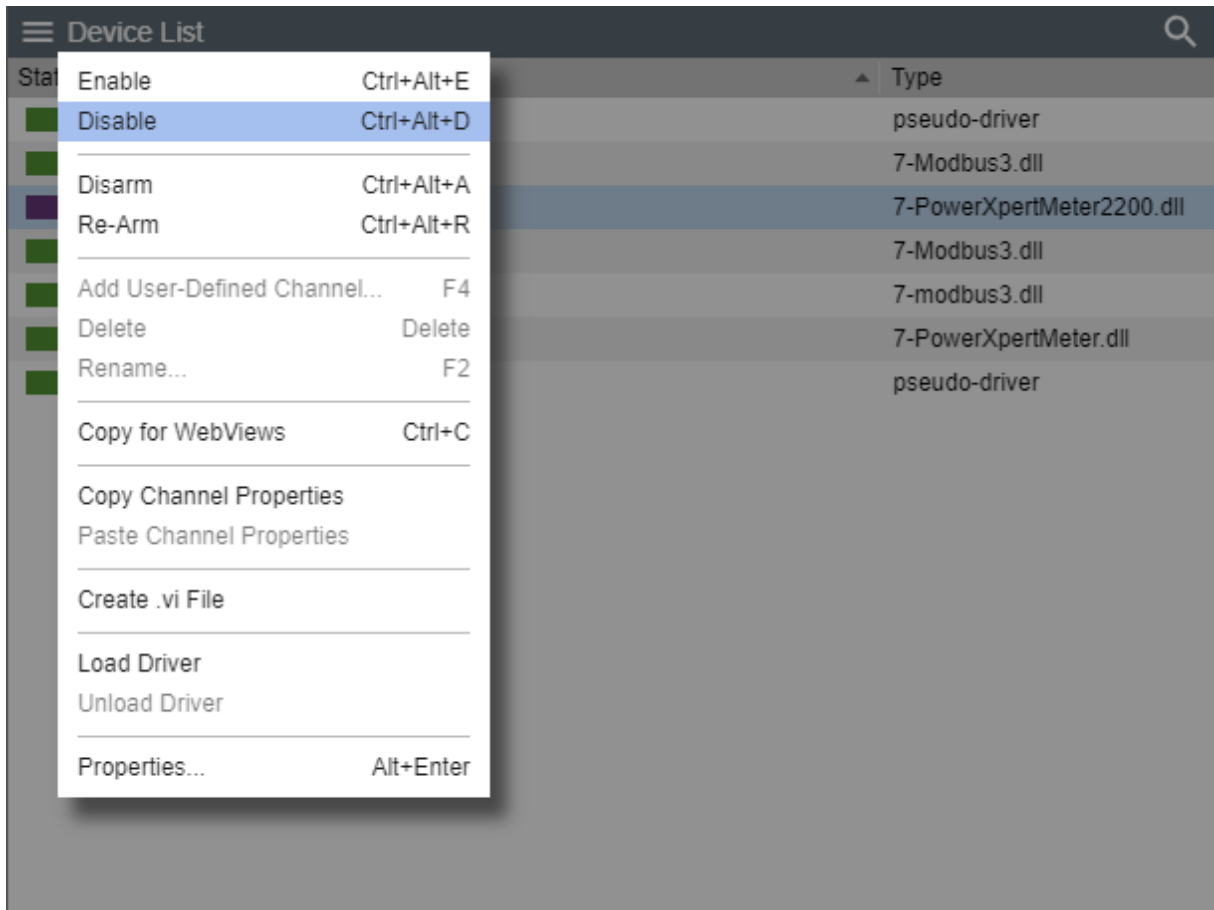
Disable

The Disable function suspends all data archiving to the Foreseer Server for the selected Device. Disabling is useful when making repairs to avoid archiving inappropriate readings and is necessary in order to [Delete](#) or [Rename](#) the Device or [Unload or Load a driver](#).

✔ Administrative Authorization is required before proceeding with this command.

To Disable a device:

1. Select Disable from the Device List menu

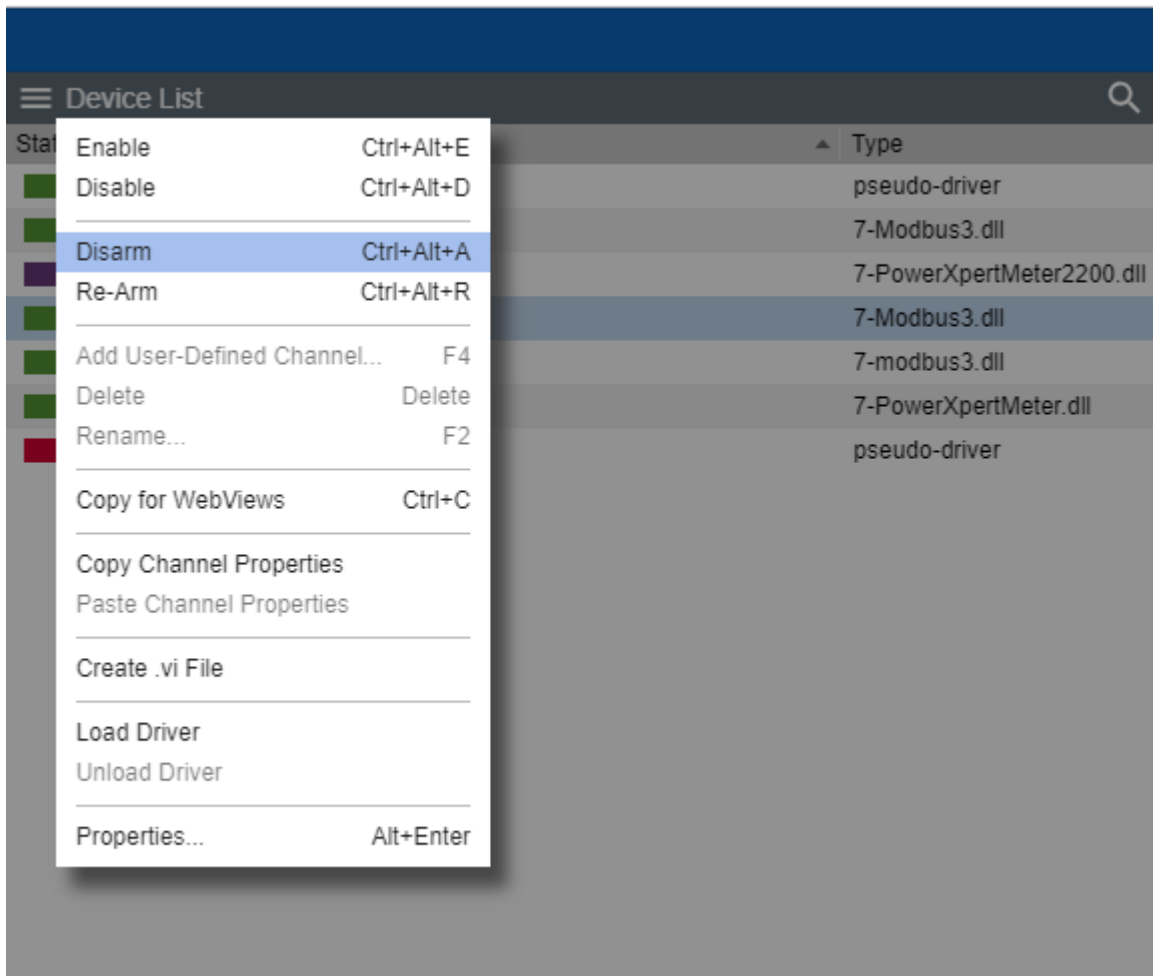


Disarm

The Disarm command stops testing the device channels' current values against the specified alarm limits for each channel, preventing alarms from being issued.

To Disarm a device:

1. Select Disarm from the Device List menu



2. The device being disarmed will turn to light-blue

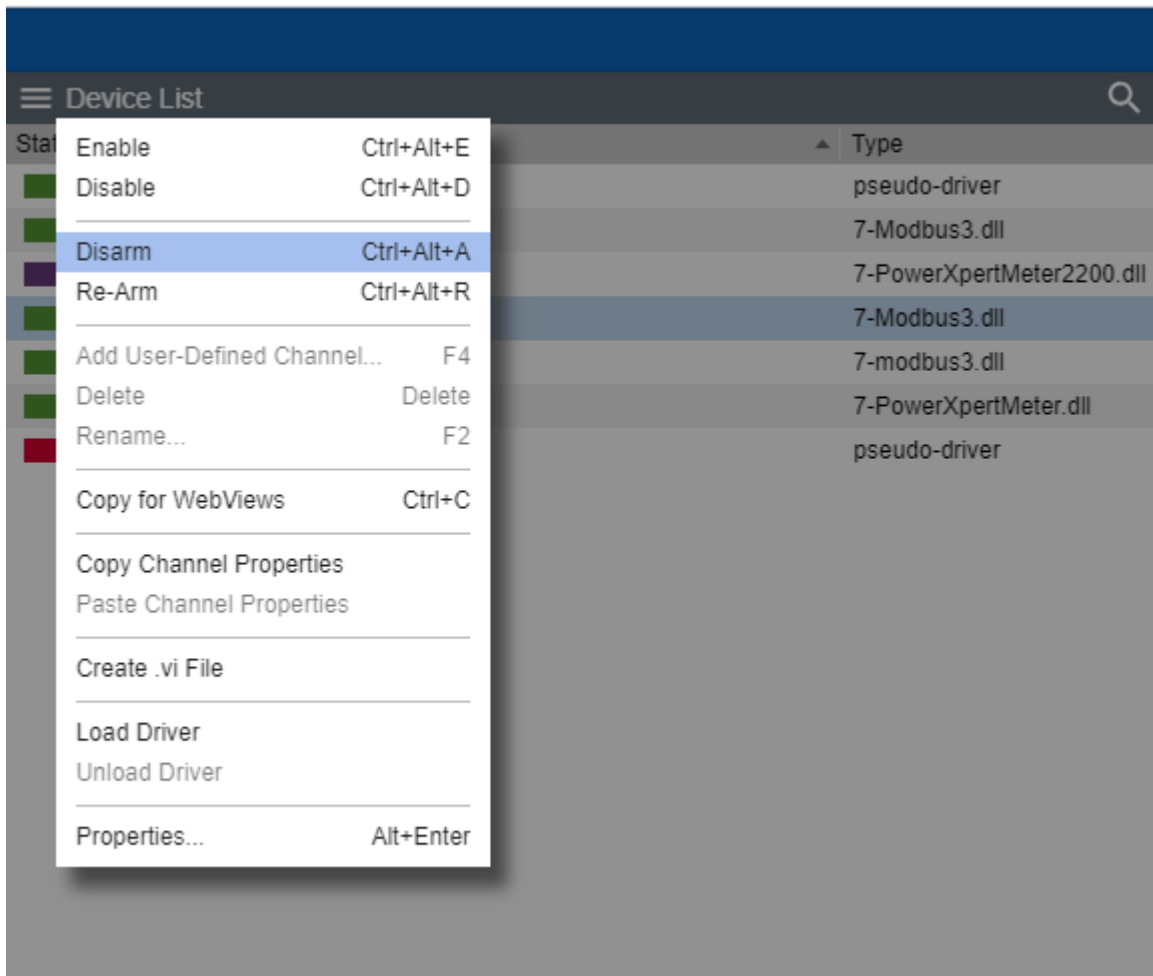
Device List			
State	Name	Type	
■	Derived Channels	pseudo-driver	
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll	
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll	
■	IQ 250 1	7-Modbus3.dll	
■	Mits 9900 Aegis 1	7-modbus3.dll	
■	PowerXpert Meter1	7-PowerXpertMeter.dll	
■	System Channels	pseudo-driver	

Re-Arm

The Rearm command resumes testing channel values against alarm limits.

To Re-Arm a device:

1. Select Re-Arm from the Device List menu



2. The device being disarmed will turn back to active if it connected and healthy.

Device List		
State	Name	Type
■	Derived Channels	pseudo-driver
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll
■	IQ 250 1	7-Modbus3.dll
■	Mits 9900 Aegis 1	7-modbus3.dll
■	PowerXpert Meter1	7-PowerXpertMeter.dll
■	System Channels	pseudo-driver

Add User-Defined Channel

The Add User-Defined Channel command creates a new Derived Channel. Derived channels are inputs in addition to the default channels installed with the Device. They may be used to compare the reported value of one channel to another to reflect an analog value, such as the difference between an input and an output voltage or indicate a digital state like the opening of a security door. These should be created or modified only under the direction of Eaton Customer Support.

✔ Administrative Authorization is required before proceeding with this command.

To Add a User Defined Channel:

1. Start Server Configuration Mode
2. If you are adding derived channels to a physical device, select the device you want to add the user defined channel to from the Device List panel. If you are not adding user defined channels to a physical device, skip to step 4.

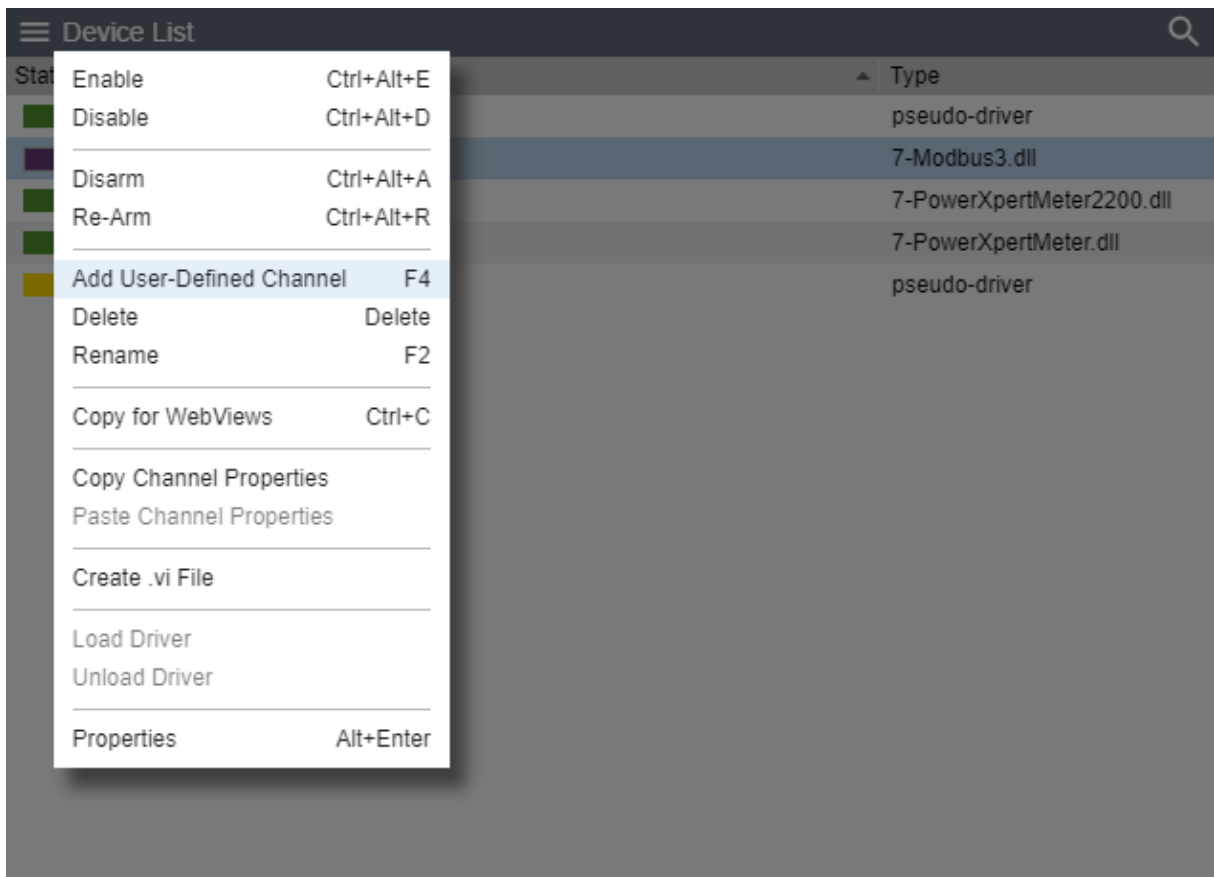
Device List		
State	Name	Type
■	Derived Channels	pseudo-driver
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll
■	PowerXpert Meter1	7-PowerXpertMeter.dll
■	System Channels	pseudo-driver

3. Select Disable from the Device List Menu

Device List		
State	Name	Type
■	Derived Channels	pseudo-driver
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll
■	PowerXpert Meter1	7-PowerXpertMeter.dll
■	System Channels	pseudo-driver

Enable	Ctrl+Alt+E
Disable	Ctrl+Alt+D
Disarm	Ctrl+Alt+A
Re-Arm	Ctrl+Alt+R
Add User-Defined Channel	F4
Delete	Delete
Rename	F2
Copy for WebViews	Ctrl+C
Copy Channel Properties	
Paste Channel Properties	
Create .vi File	
Load Driver	
Unload Driver	
Properties	Alt+Enter

4. Select Add User-Defined Channel



5. From there you will be able to add the User-Defined Channel from one of 4 options to choose from:
- Derived Analog
 - Derived Digital
 - Text
 - Date/Time

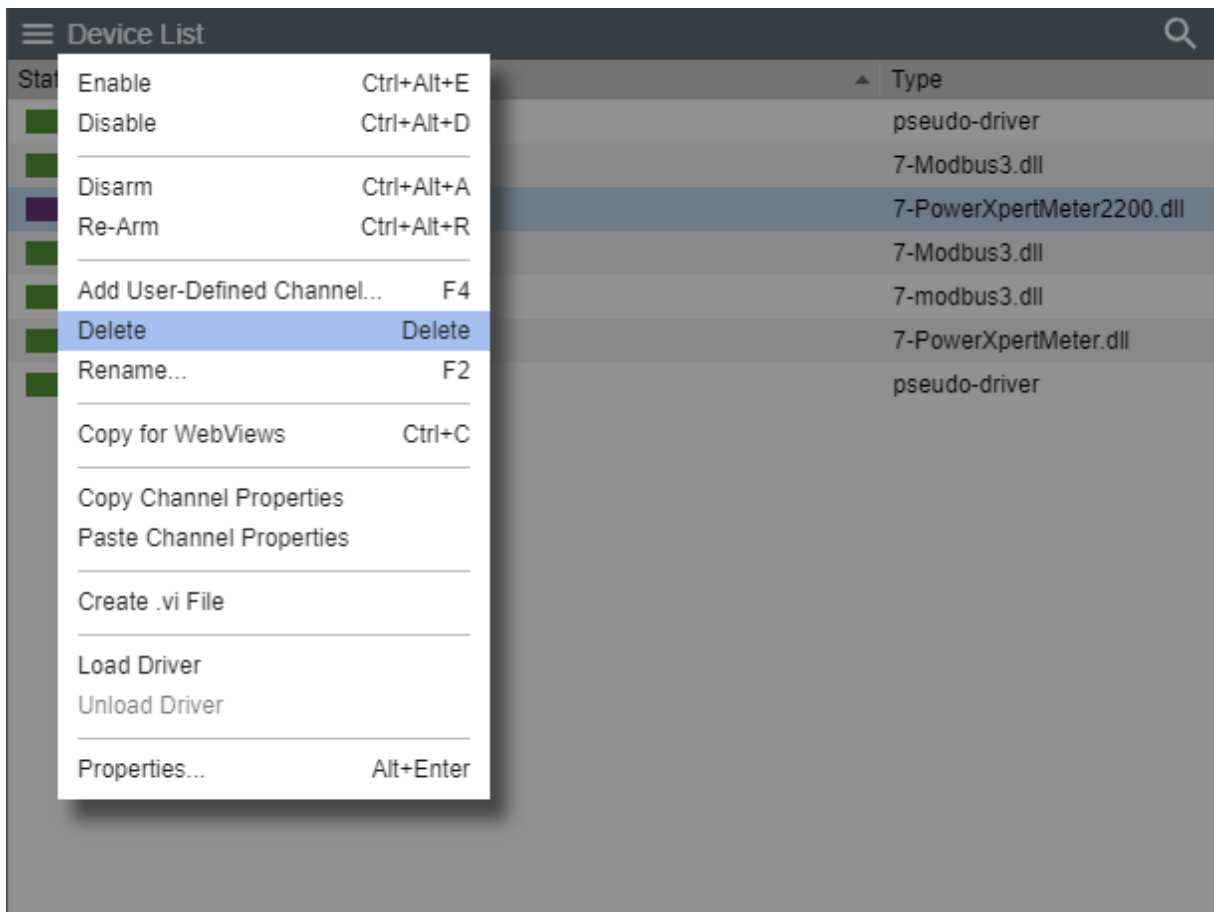
Delete

The Delete command permanently deletes the selected Device from the configuration. Once removed, its archived information is no longer available. Deleting a Device should be done with discretion as removing it can have an adverse effect on Foreseer WebViews.

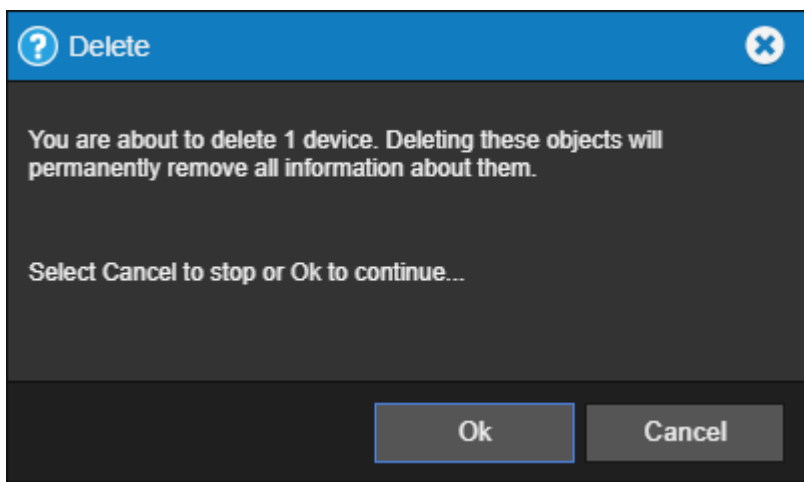
✔ Administrative Authorization is required before proceeding with this command.

To Delete a device:

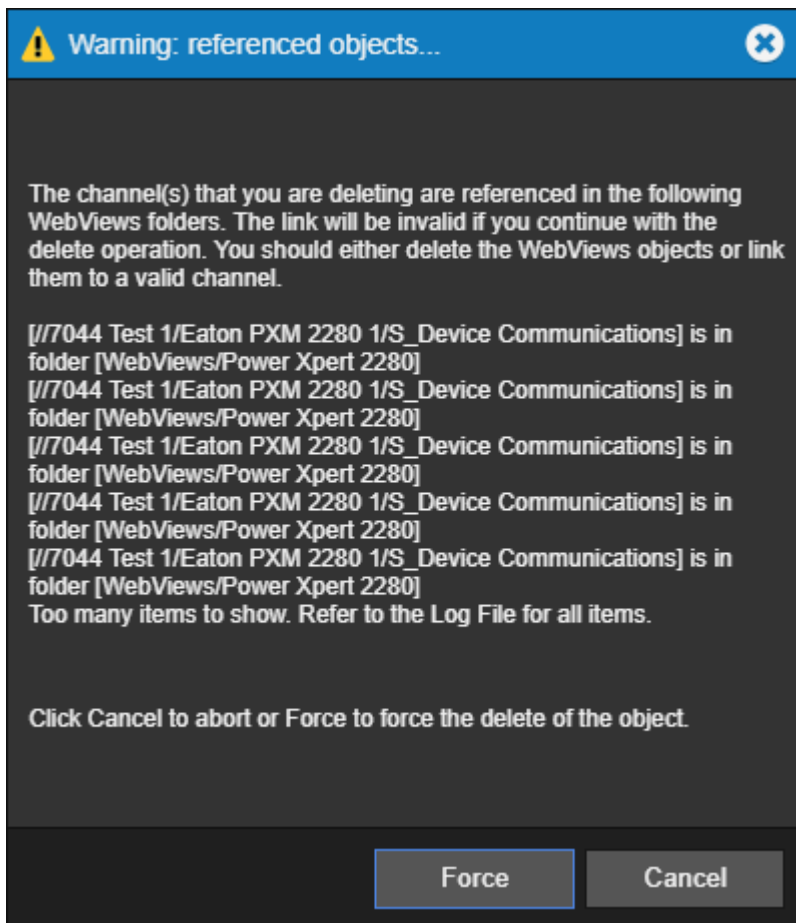
1. Select Delete a device from the Device List menu



2. Confirm that you want to delete the selected device



3. If the selected device or it's channels are connected to any WebViews folders, the following warning message will be displayed:



- ✔ If you are deleting multiple devices, the Warning: referenced objects dialog may only reference a single device in situations where one device may be referenced by multiple WebViews. If you are not comfortable with forcing this change, cancel and delete one device at a time.

4. Select Force to continue

Rename

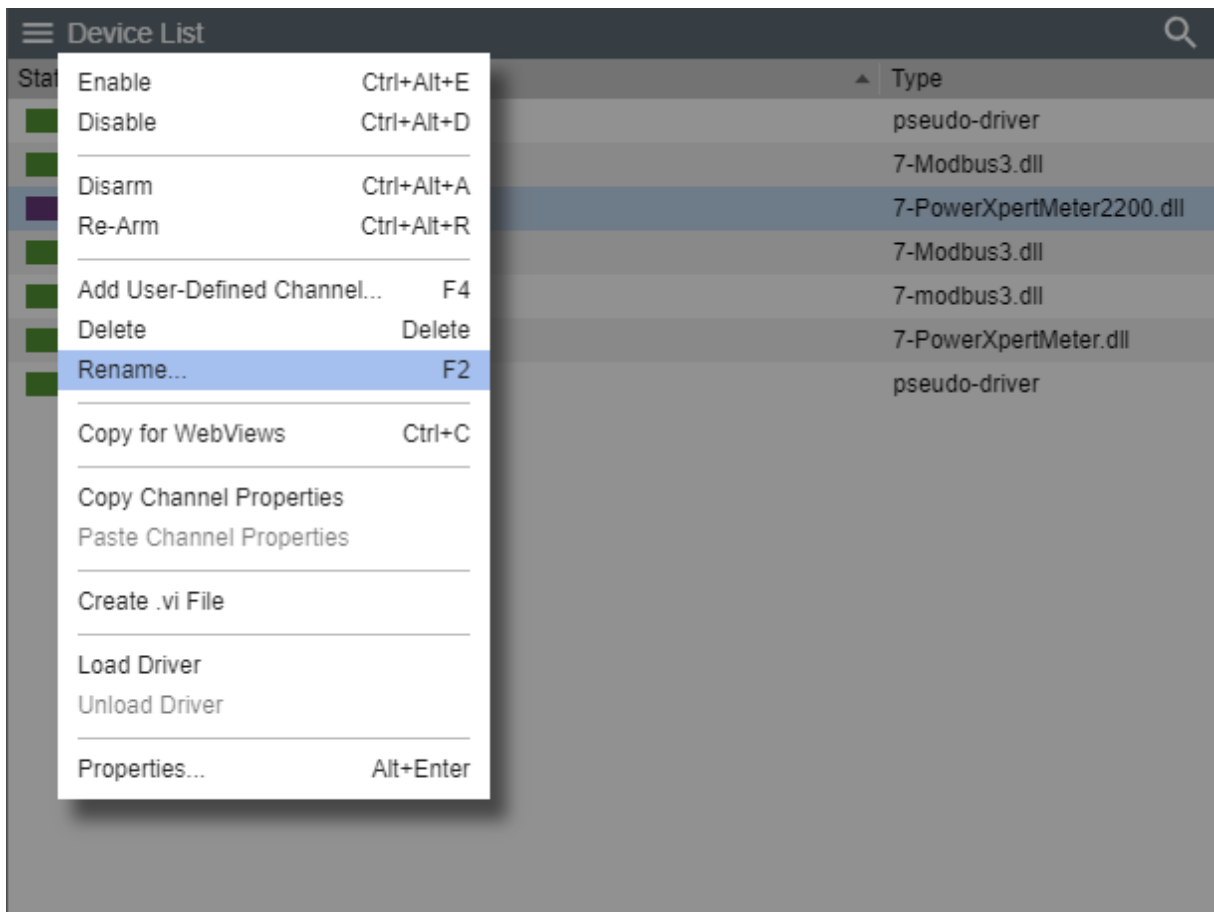
The Rename command renames the selected Device. Renaming a Device should be done with discretion as changing a name can have an adverse effect on Foreseer WebViews.

- ✔ Administrative Authorization is required before proceeding with this command.

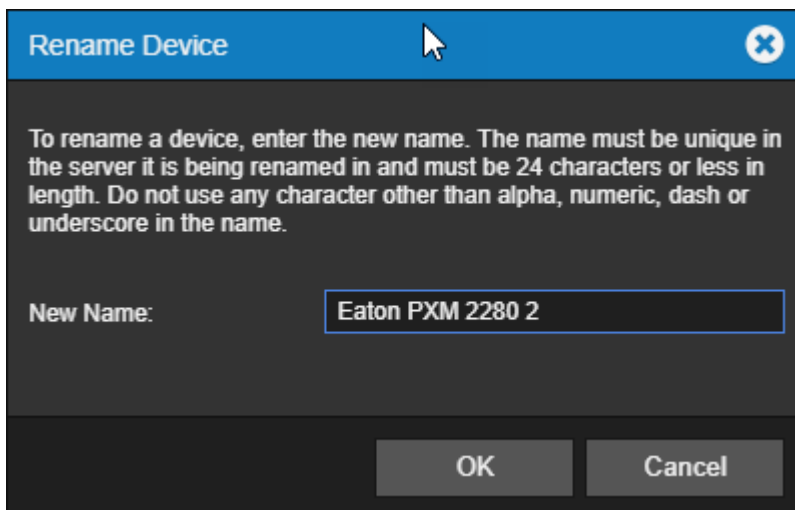
To Rename a device:

1. Start Server Configuration Mode

2. Select Rename from the Device List menu



3. Enter the new name of the device



4. Select OK to accept the new name

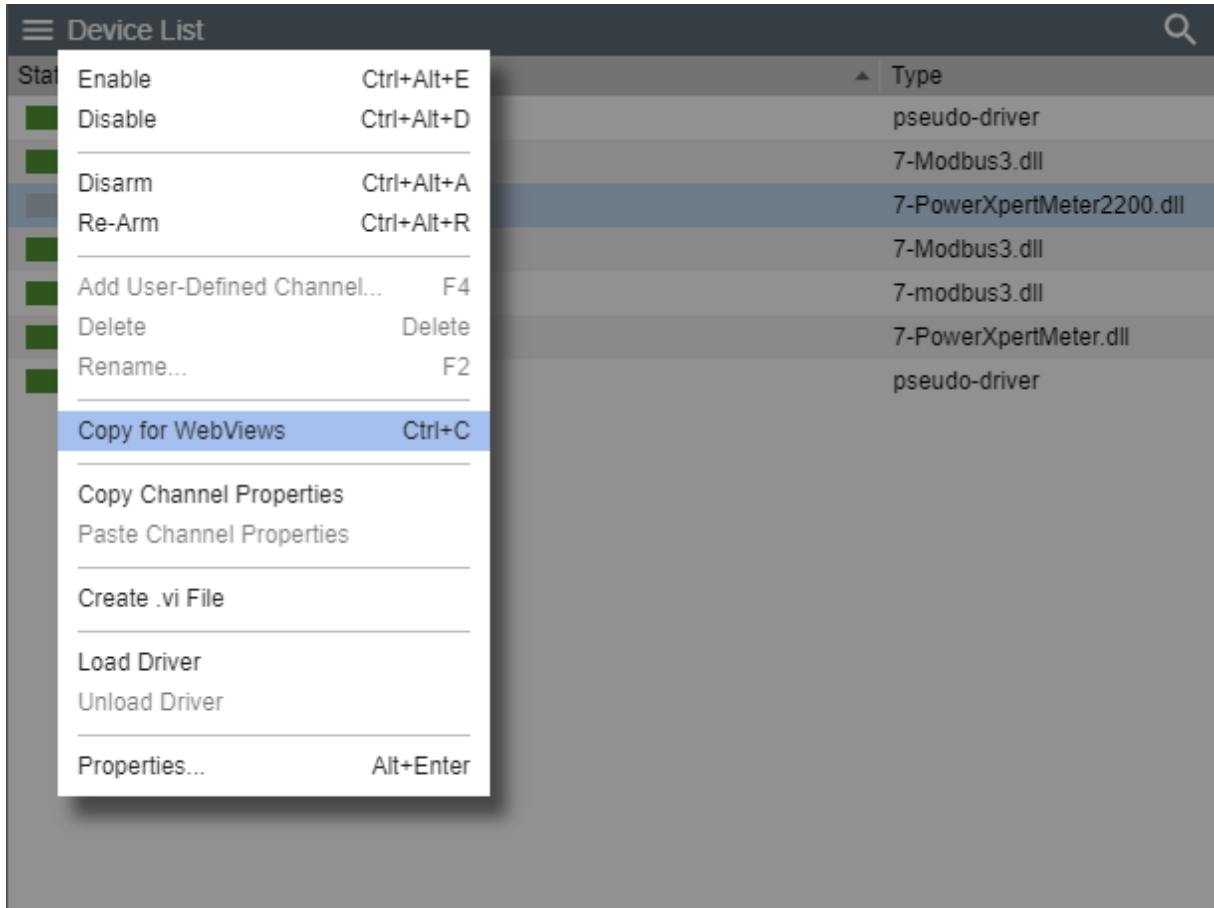
Copy for WebViews

The Copy for WebViews command copies the selected devices to the target folder in the

WebViews tree.

To make a Copy for WebViews:

1. Select Copy for WebViews from the Device List menu

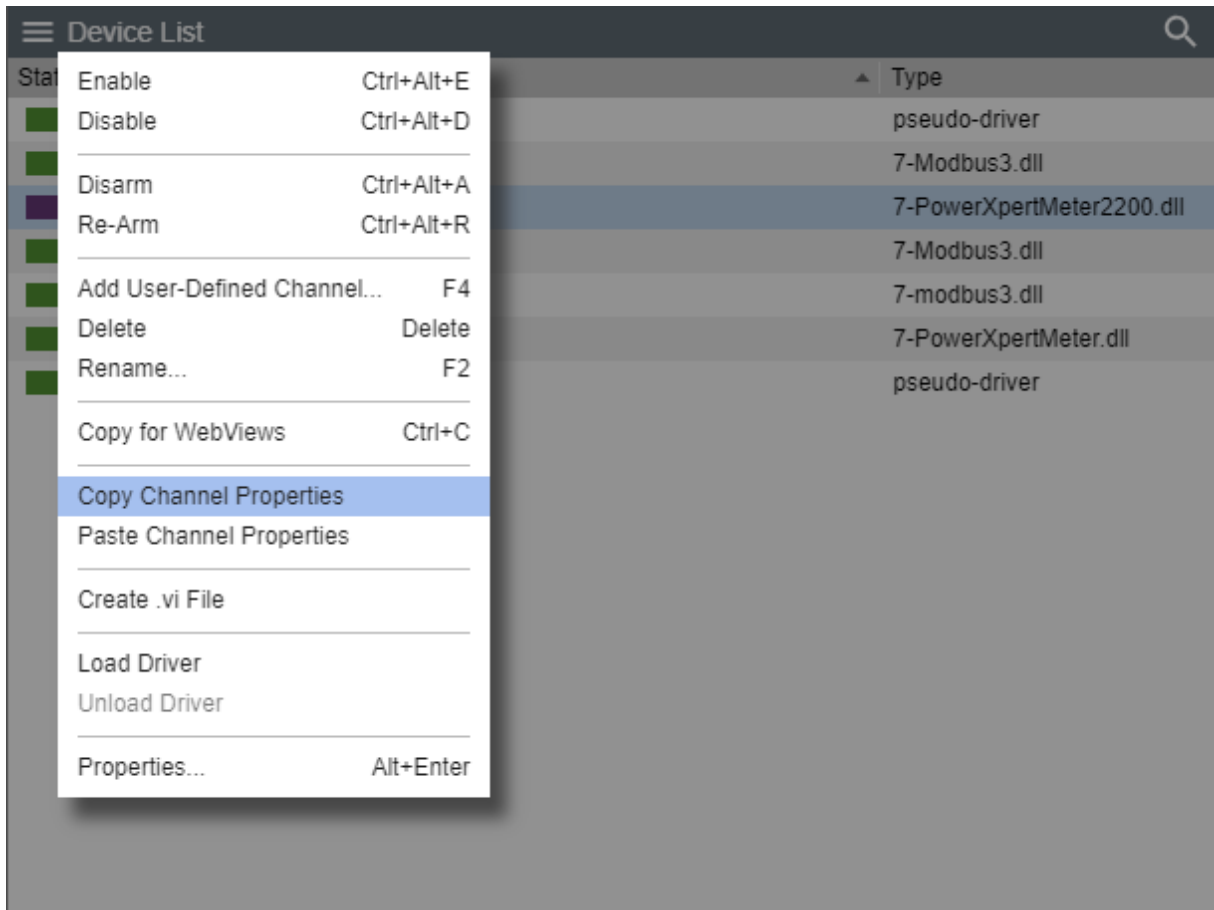


Copy Channel Properties

The Copy Channel Properties command copies all of the currently selected devices channel properties to the Windows clipboard, allowing its settings to be pasted directly into another channel as its operational parameters. This command is useful when applied to an entire device (rather than individual channels) for quickly setting up multiple devices that contain similar channels. In either case, the device being copied must be of the exact same type as the one the Properties are being pasted into.

To Copy Channel Properties:

1. Select Copy Channel Properties from the Device List menu

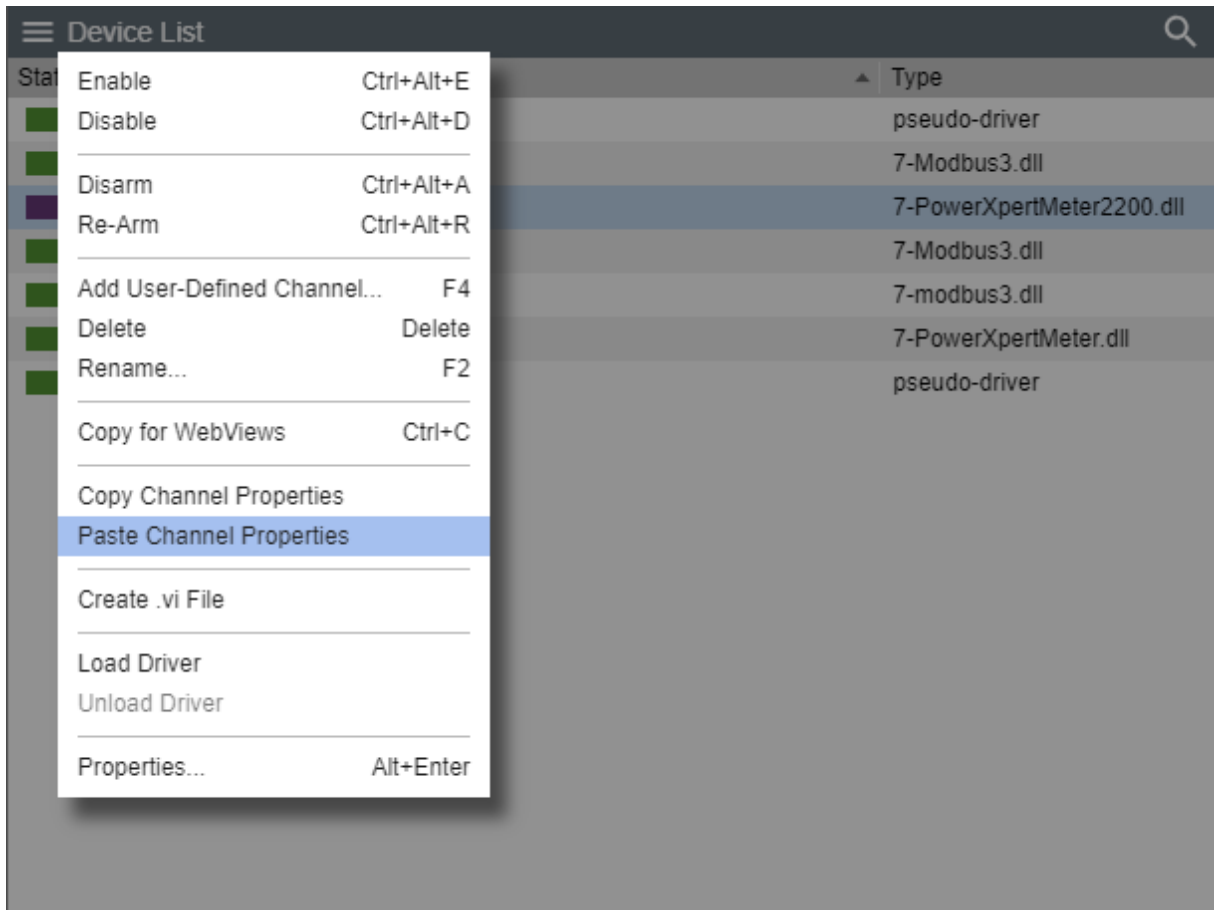


Paste Channel Properties

The Paste Channel Properties command pastes the previously copied properties into the currently selected device as its operational parameters. It also is useful when duplicating numerous channel settings on multiple devices. In either case, the device being pasted into must be of the exact same type as the one from which the properties are being copied. These settings then can be individually modified as necessary. If copying from a device, only those channels with the same name will have their properties pasted.

To Paste Channel Properties:

1. Select Paste Channel Properties from the Device List menu

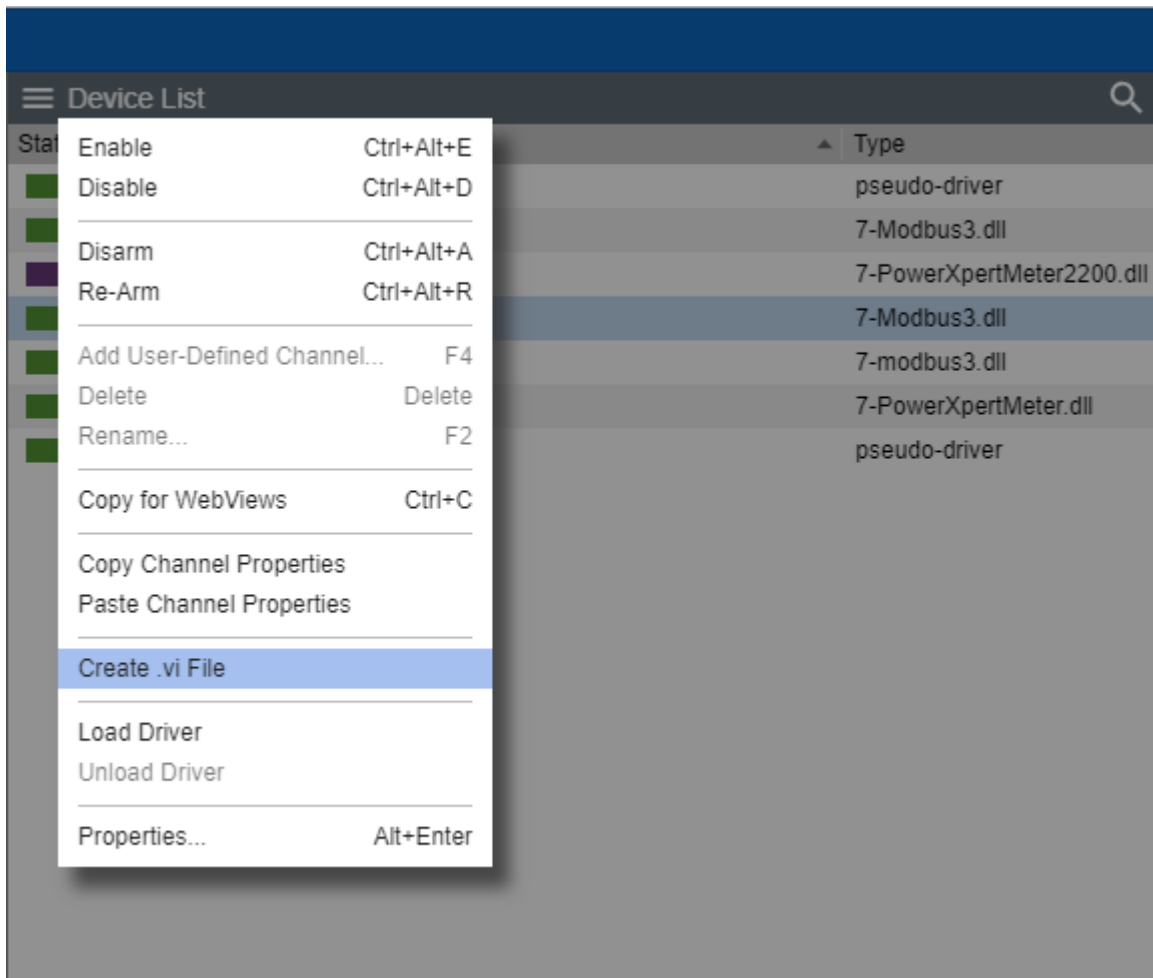


Create .vi File

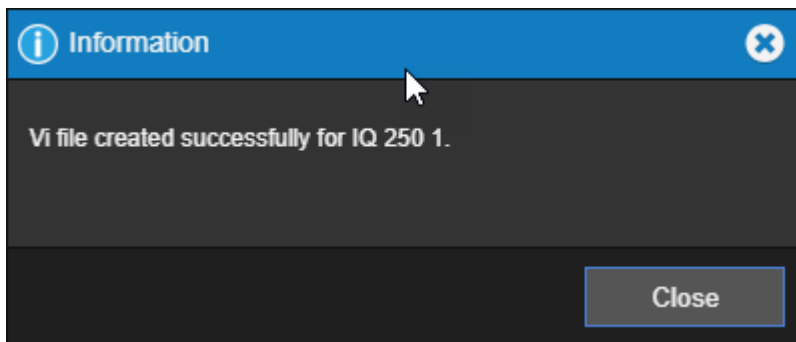
The Create .vi File command generates .VI (Device Driver) templates for all Devices on the selected Server. These device templates can then be used to define other similar Devices.

To Create .vi File:

1. Select Create .vi File from the Device List menu



2. A vi file will be created to the selected device



Load Driver

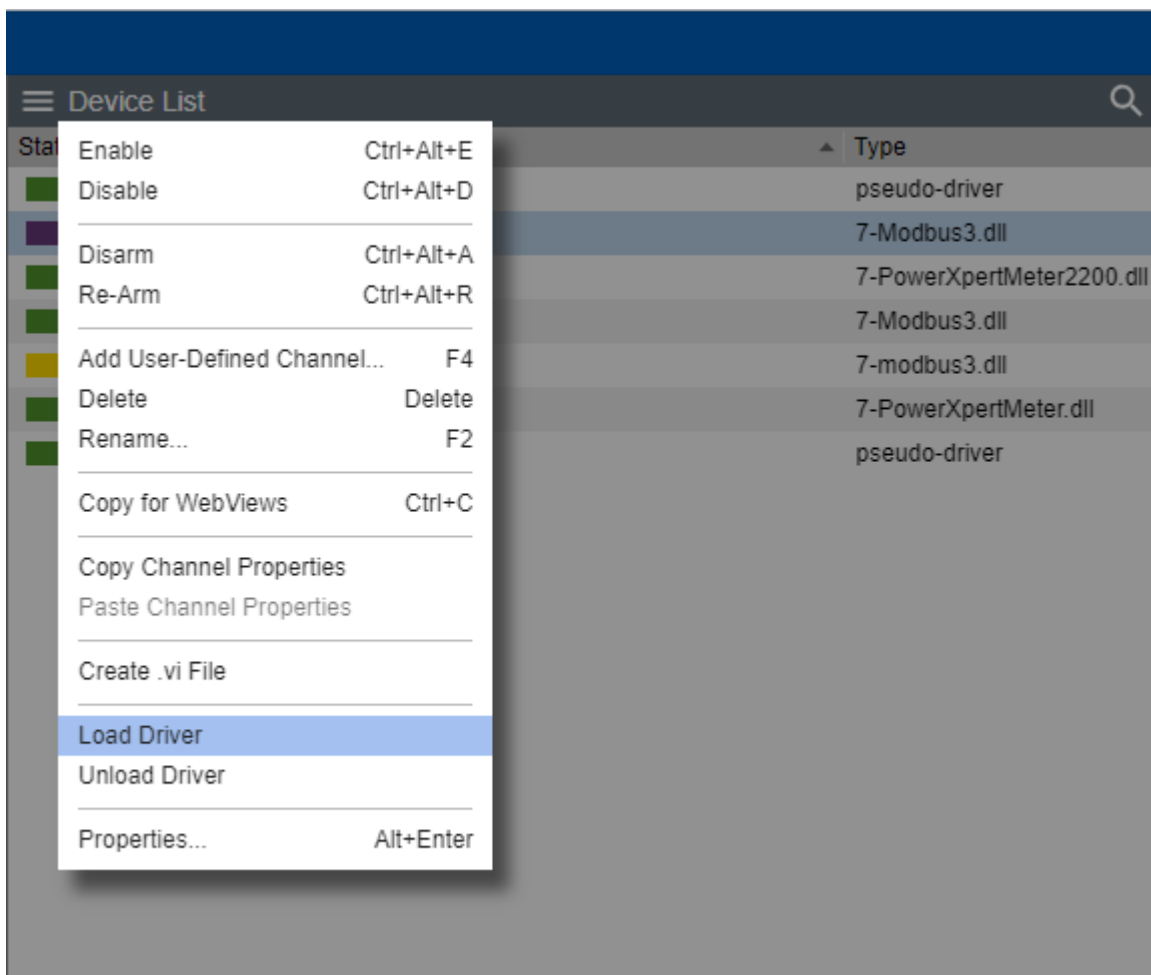
The Load Driver command are used strictly by driver developers. You can load the appropriate Device driver from the \Program Files (x86)\Eaton Corporation\Foreseer\Update VI folder.

✔ This command should only be performed at the direction of Eaton technical support.

✔ Administrative Authorization is required before proceeding with this command.

To load a driver:

1. Start Server Configuration Mode
2. Select Load Driver from the Device List menu



3. The Foreseer system will begin loading the selected driver

EATON Foreseer® Enterprise Management

Server List 🔍

Config Mode

⚙️ Loading Device Drivers

Loading driver (0 of 1): Eaton PXM 2270 Meter 1

State	Name	Type	Needs Update	Connect State
🟡	*7044 Test 1	Primary	-	-
🟢	Remote - 7044 Test 1	Foreseer	No	connected

4. End Server Config mode

Unload Driver

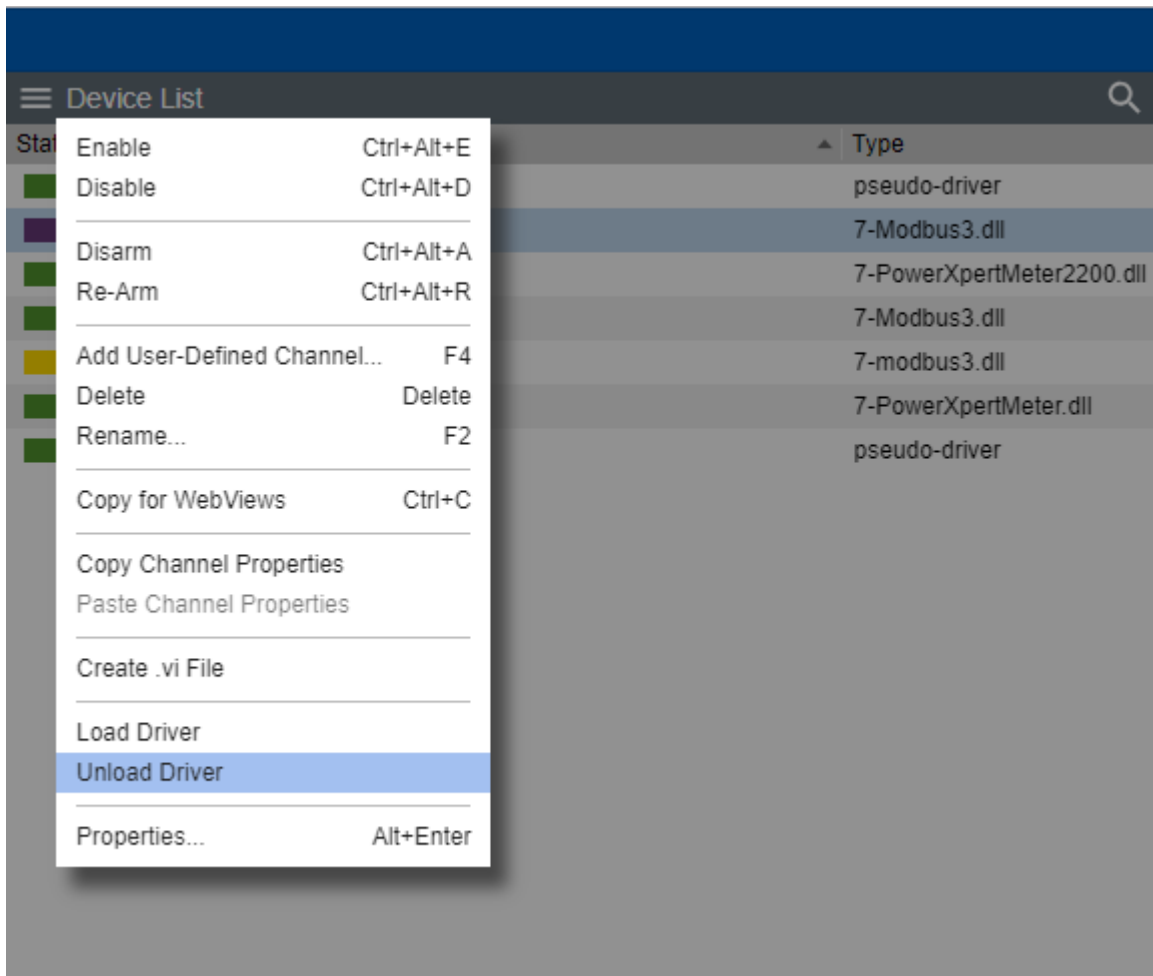
The Unload Driver commands are used strictly by driver developers. Unload clears the driver file for the selected Device. Multiple Devices of the same Type may be selected for unloading without shutting the system down.

✔️ This command should only be performed at the direction of Eaton technical support.

✔️ Administrative Authorization is required before proceeding with this command.

To Unload a driver:

1. Start Server Configuration Mode
2. Select Unload Driver from the Device List menu



3. The Foreseer system will begin unloading the selected driver

EATON Foreseer® Enterprise Management

Server List 🔍

Config Mode

Unloading Device Drivers

Unloading driver (0 of 1): Eaton PXM 2270 Meter 1

State	Name	Type	Needs Update	Connect State
🟡	*7044 Test 1	Primary	-	-
🟢	Remote - 7044 Test 1	Foreseer	No	connected

4. End Server Config mode

Properties

The Properties command furnishes operational information on the Device.

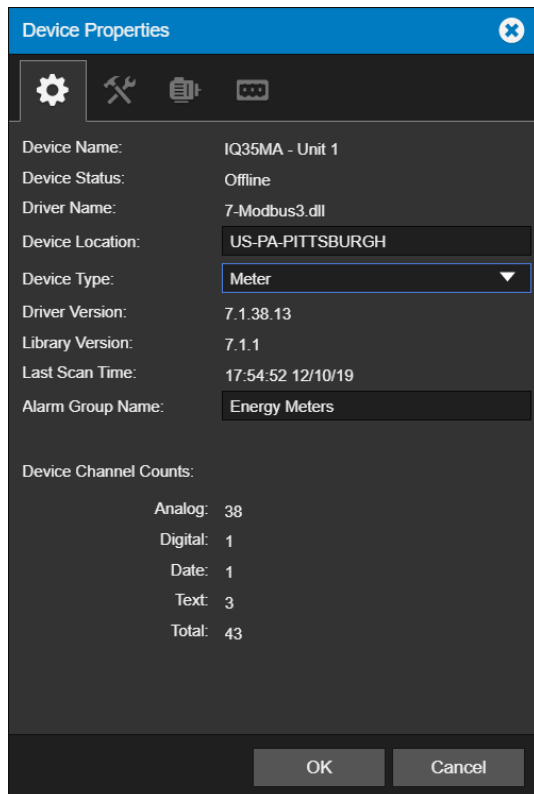
With the exception of Device Location, Device Type, and Alarm Group Name, you cannot change many of these setting without first Disabling the device.

Device Properties - General

- Device Name – reflects the name of the installed device.
- Device Status – reflects whether the device is online or offline
- Driver Name – reflects the name of the communication driver DLL used by Foreseer to “talk” to the device.
- Device Location – reflects a user string that defines the location of the device. A device location can be up to 255 characters in length and use all special characters except a comma.
- Device Type – reflects a classification category for the type or device. Assigning a device type is useful in situations where you may need to filter or sort alarms. You can select from any of the pre-canned selections or create your own custom device type designation.
- Driver Version – reflects the file version number of the communication driver DLL.
- Library Version – reflects the library version associated with the communication driver

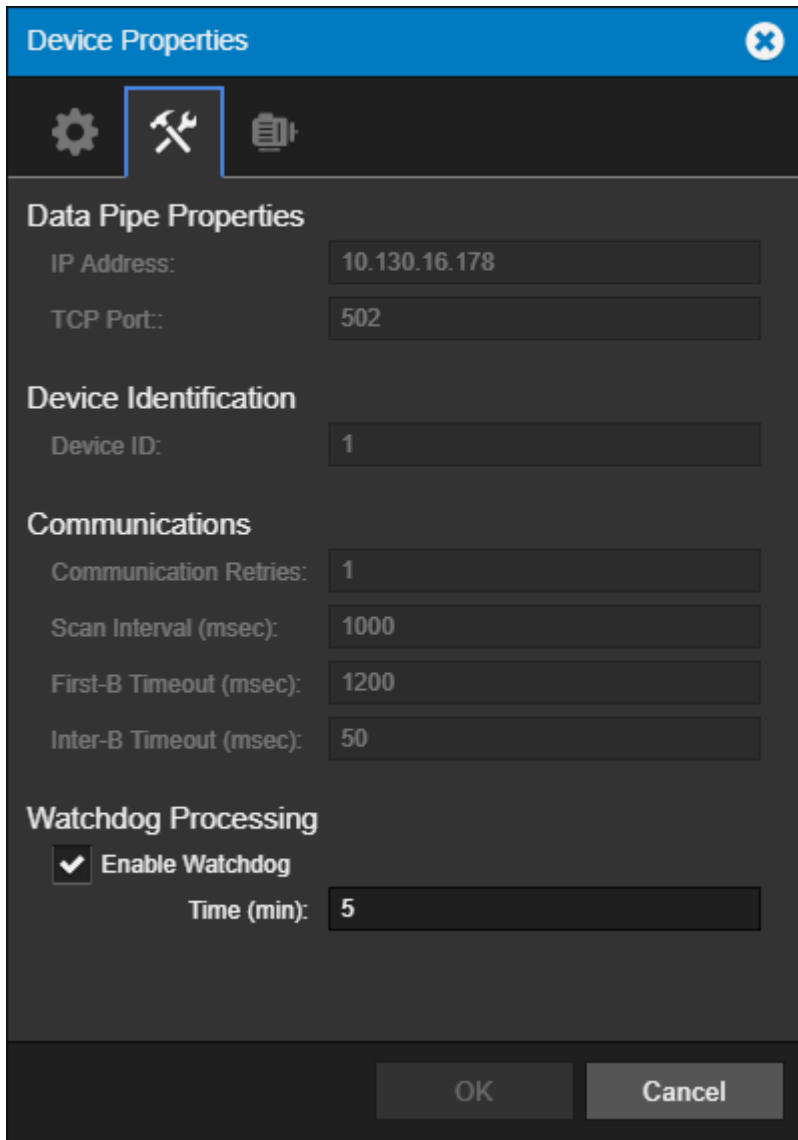
DLL.

- Last Scan Time – reflects the last successful date/time that all channels were scanned.
- Alarm Group Name – reflects a user string that defines membership of a logically assigned group. Alarm Group Names can be up to 255 characters in length and use all special characters except a comma.
- Device Channel Counts – Reflects the count of each fundamental channel type contained within the device.



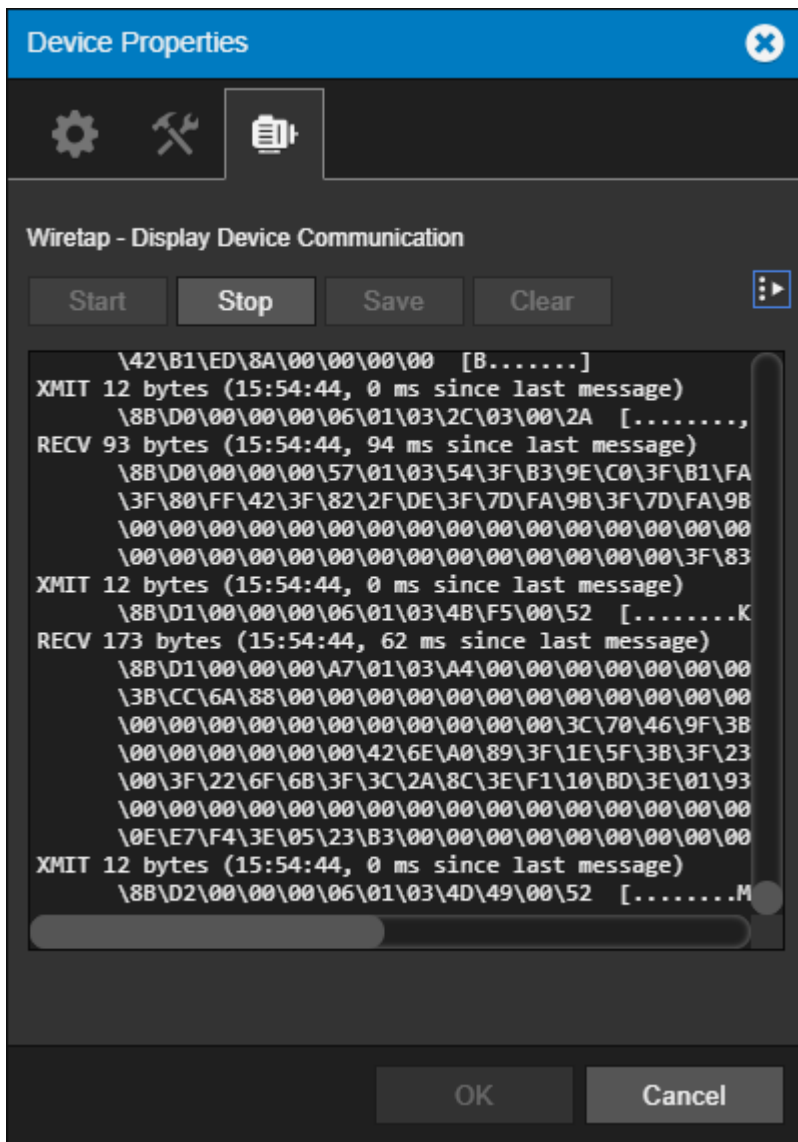
Device Properties

- Data Pipe Properties
- Device Identification
- Communications
- Watchdog Processing

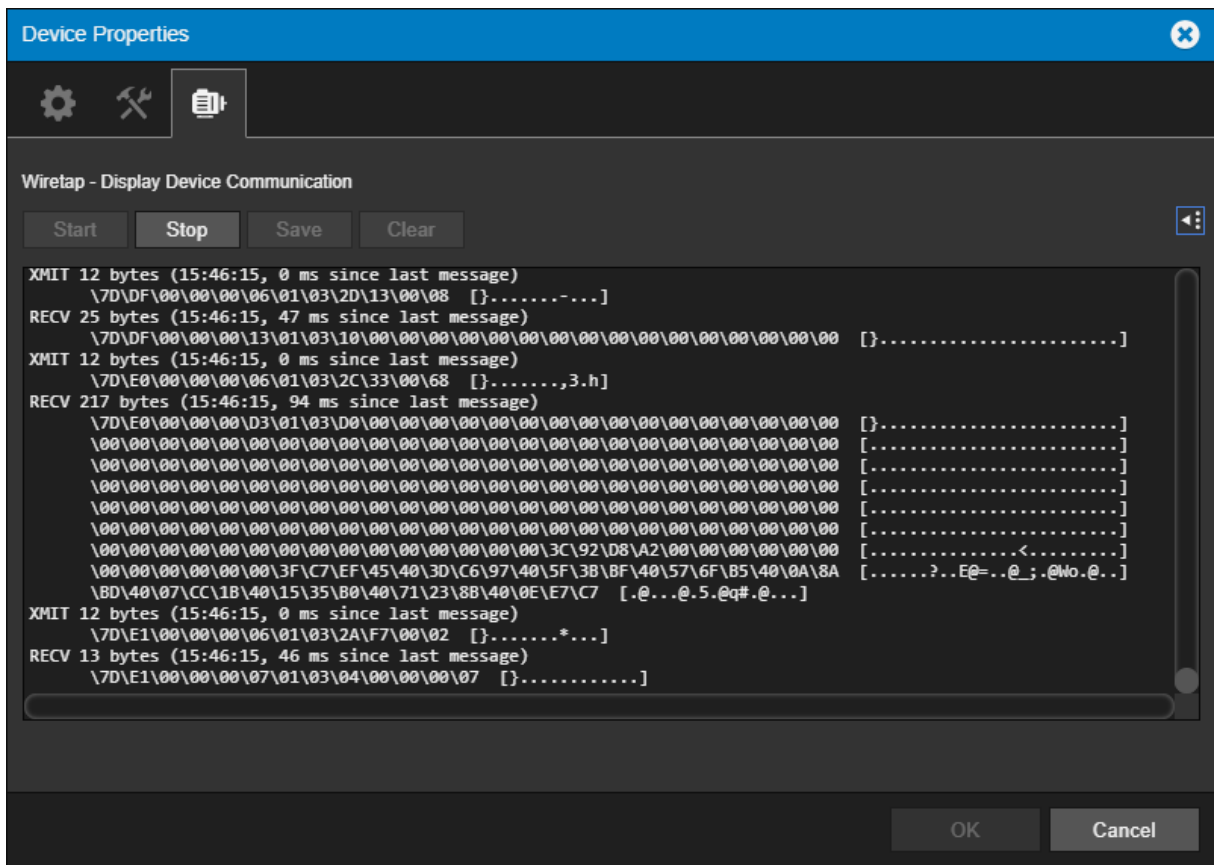


Device Properties - Wiretap

To initiate a wiretap, click the "Start" button. To stop the wiretap communication, click the "Stop" button. To see more of the display, click the arrow in the upper right corner to expand the display.



Device Properties - Wiretap (Expanded display)



Channel List Menu

The Channel List menu provides access to all of the functionality that will be required to manage your Foreseer channels.

- Enable
- Disable
- Disarm
- Re-Arm
- Delete
- Rename
- Copy for WebViews
- Copy Channel Properties
- Paste Channel Properties
- Properties

Enable

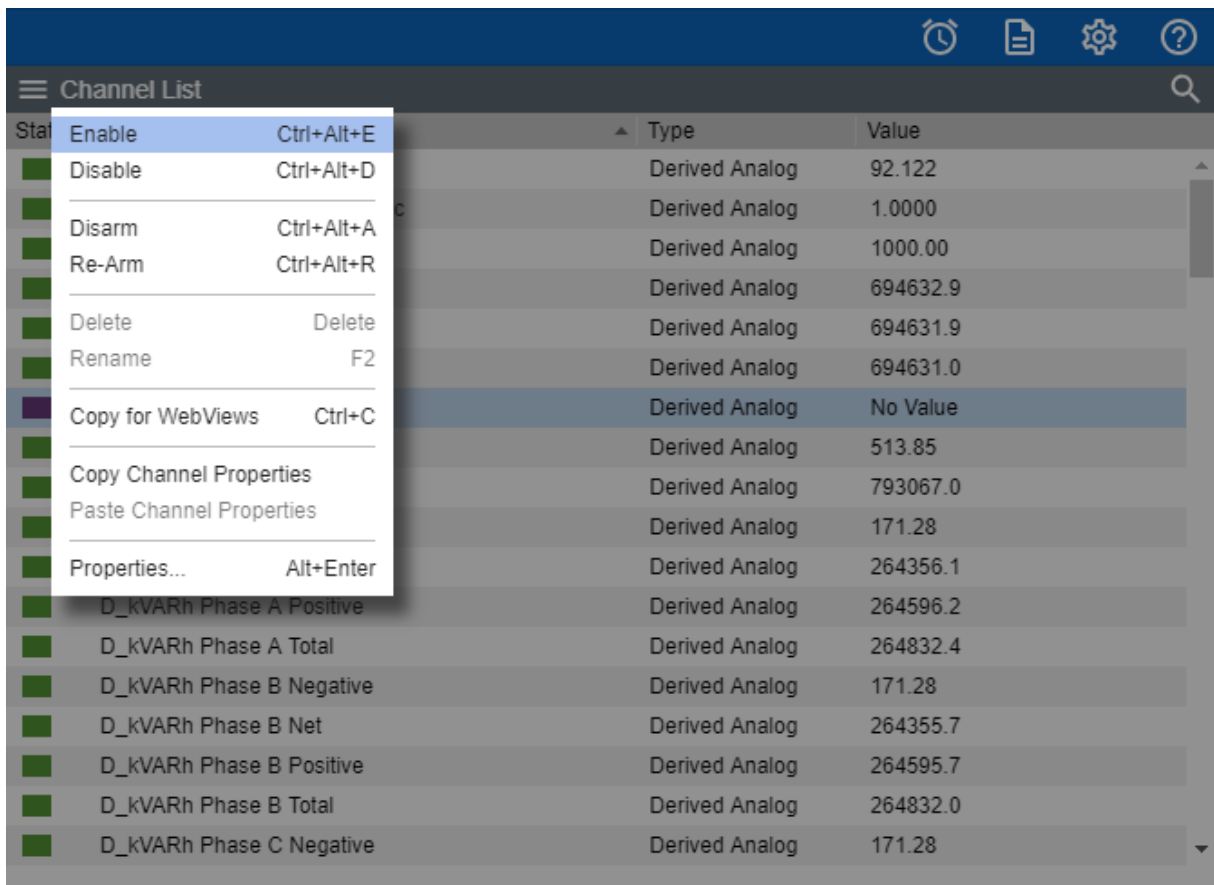
The enable command resumes data archiving for the selected Channel.

To Enable a channel:

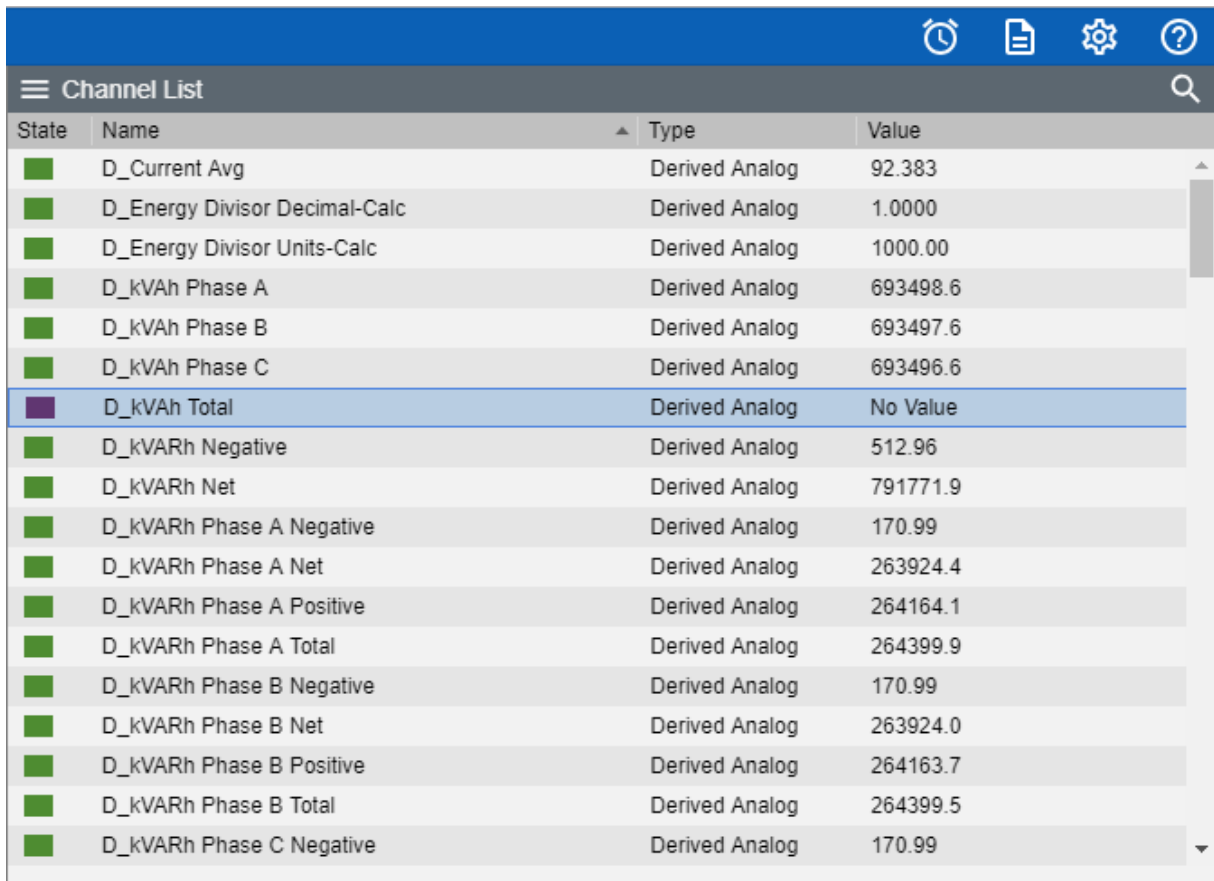
1. Select the channel you would like enabled:

State	Name	Type	Value
■	D_Current Avg	Derived Analog	92.213
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	694447.9
■	D_kVAh Phase B	Derived Analog	694446.9
■	D_kVAh Phase C	Derived Analog	694445.9
■	D_kVAh Total	Derived Analog	No Value
■	D_kVARh Negative	Derived Analog	513.70
■	D_kVARh Net	Derived Analog	792855.9
■	D_kVARh Phase A Negative	Derived Analog	171.23
■	D_kVARh Phase A Net	Derived Analog	264285.7
■	D_kVARh Phase A Positive	Derived Analog	264525.7
■	D_kVARh Phase A Total	Derived Analog	264761.9
■	D_kVARh Phase B Negative	Derived Analog	171.23
■	D_kVARh Phase B Net	Derived Analog	264285.3
■	D_kVARh Phase B Positive	Derived Analog	264525.3
■	D_kVARh Phase B Total	Derived Analog	264761.4
■	D_kVARh Phase C Negative	Derived Analog	171.23

2. Select Enable from the Channel List Menu



3. The channel will now be in a disabled state

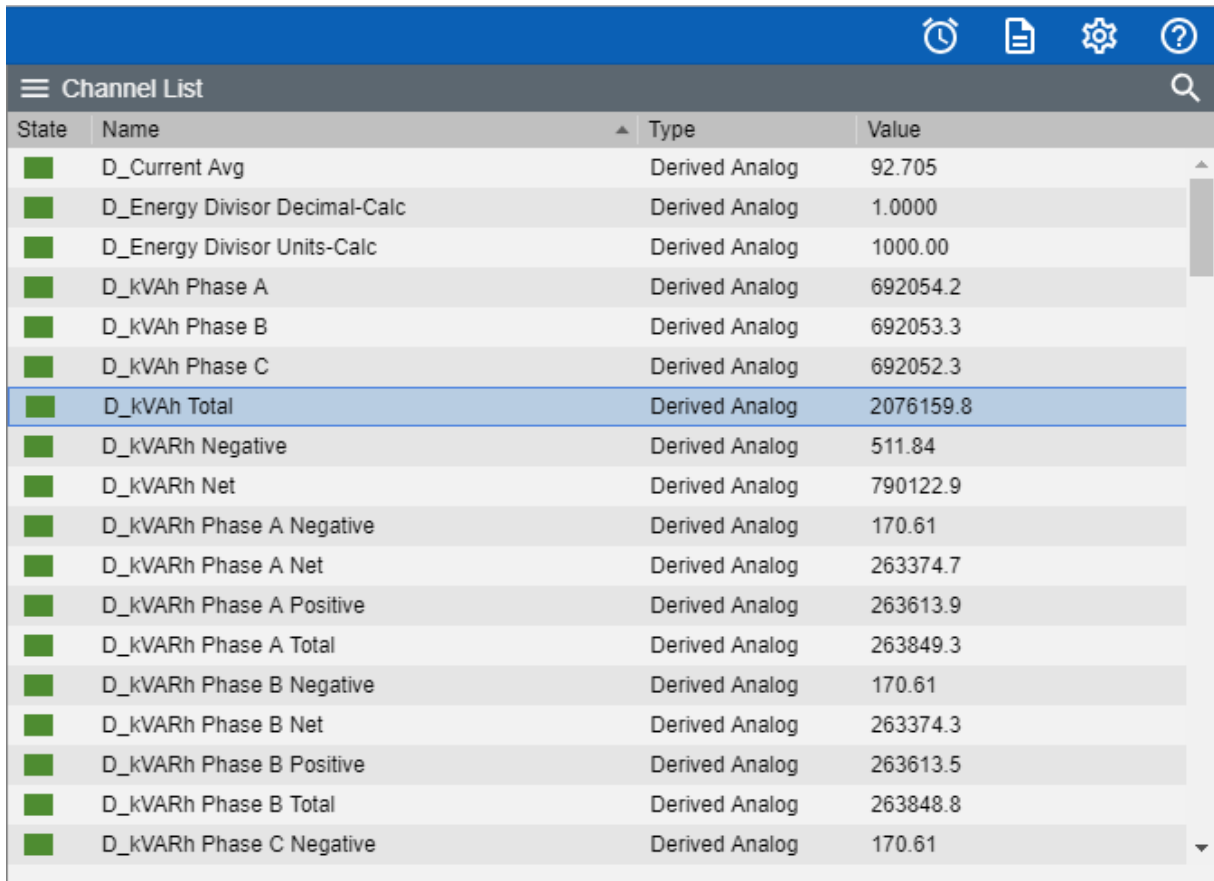


Disable

The disable command suspends all data archiving to the Foreseer Server for the selected Channel.

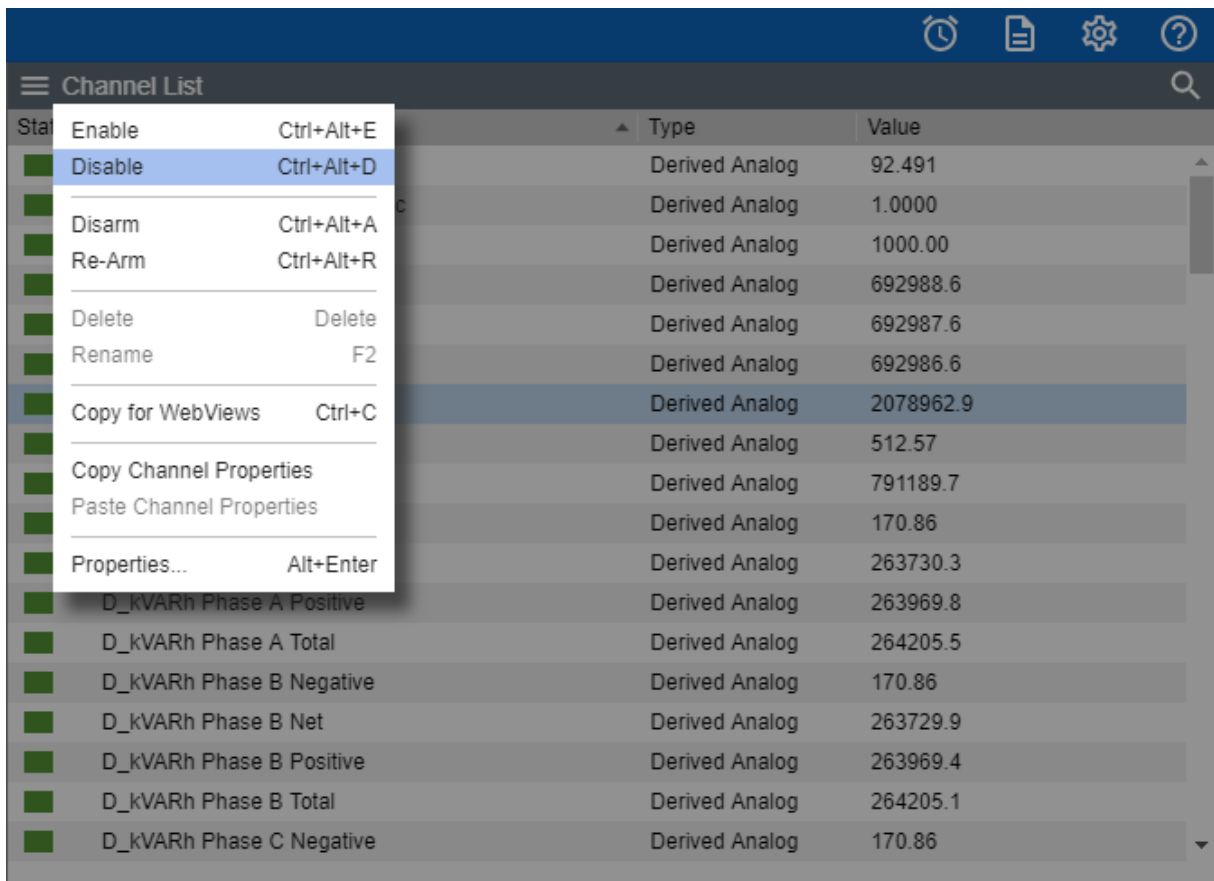
To Disable a channel:

1. Select the channel you would like disabled:

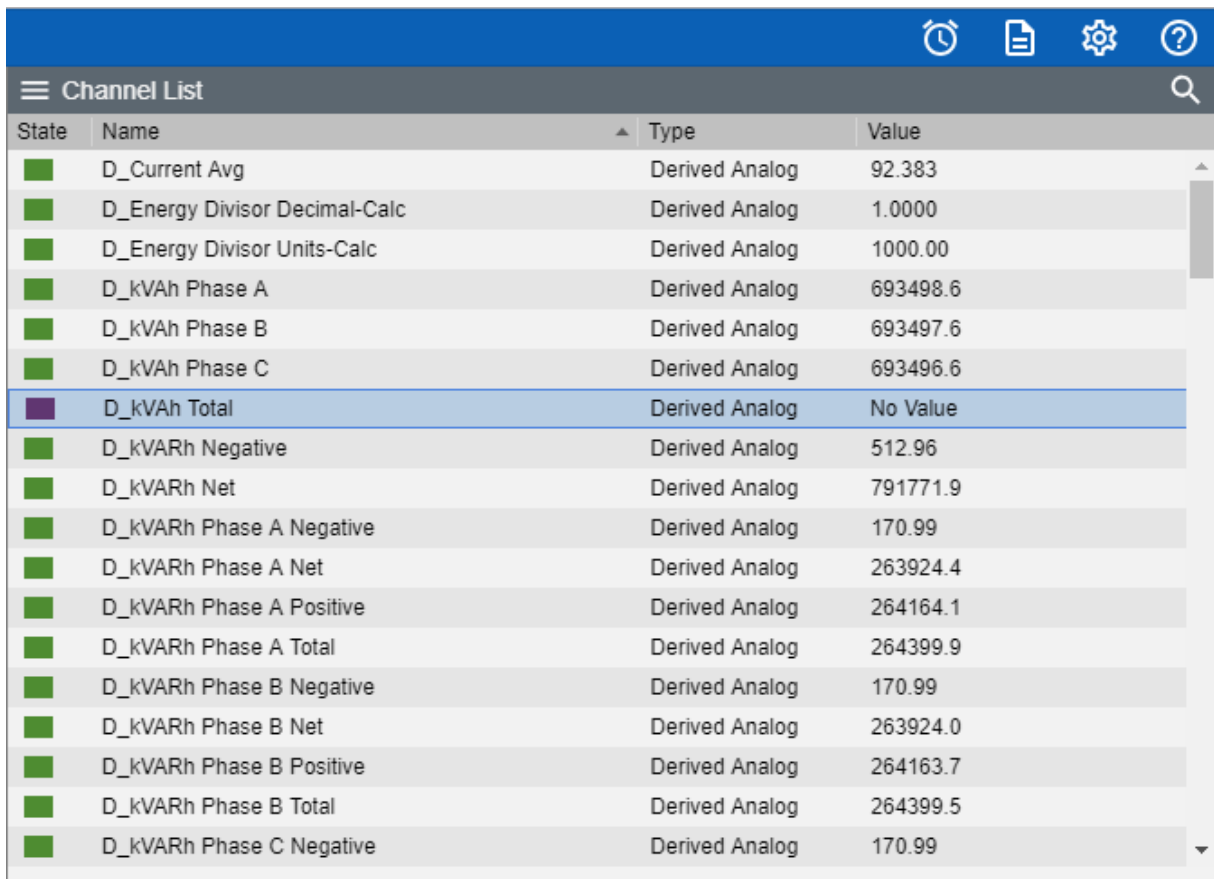


State	Name	Type	Value
■	D_Current Avg	Derived Analog	92.705
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	692054.2
■	D_kVAh Phase B	Derived Analog	692053.3
■	D_kVAh Phase C	Derived Analog	692052.3
■	D_kVAh Total	Derived Analog	2076159.8
■	D_kVARh Negative	Derived Analog	511.84
■	D_kVARh Net	Derived Analog	790122.9
■	D_kVARh Phase A Negative	Derived Analog	170.61
■	D_kVARh Phase A Net	Derived Analog	263374.7
■	D_kVARh Phase A Positive	Derived Analog	263613.9
■	D_kVARh Phase A Total	Derived Analog	263849.3
■	D_kVARh Phase B Negative	Derived Analog	170.61
■	D_kVARh Phase B Net	Derived Analog	263374.3
■	D_kVARh Phase B Positive	Derived Analog	263613.5
■	D_kVARh Phase B Total	Derived Analog	263848.8
■	D_kVARh Phase C Negative	Derived Analog	170.61

2. Select Disable from the Channel List Menu



3. The channel will now be in a disabled state

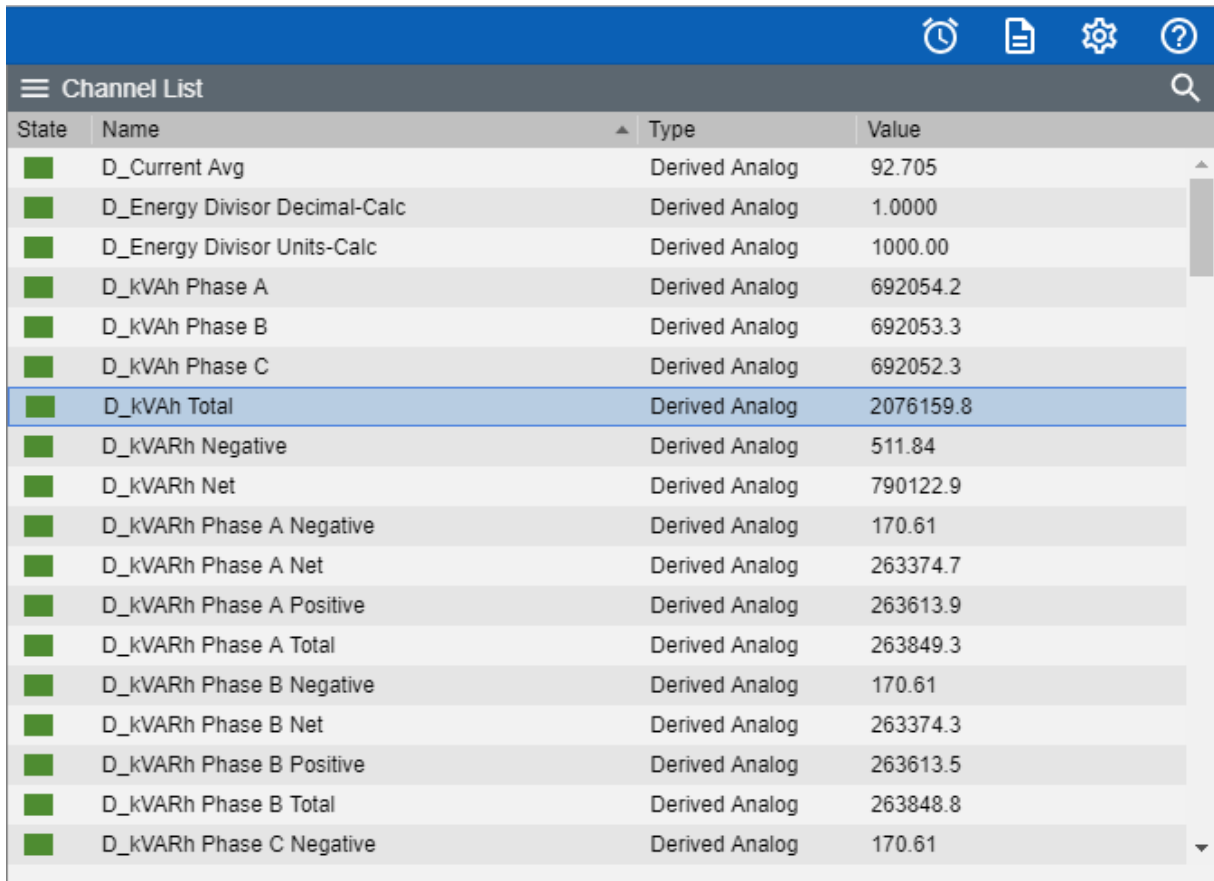


Disarm / Rearm

The Disarm command stops testing the channel's current value against the specified alarm limits, preventing an alarm from being issued.

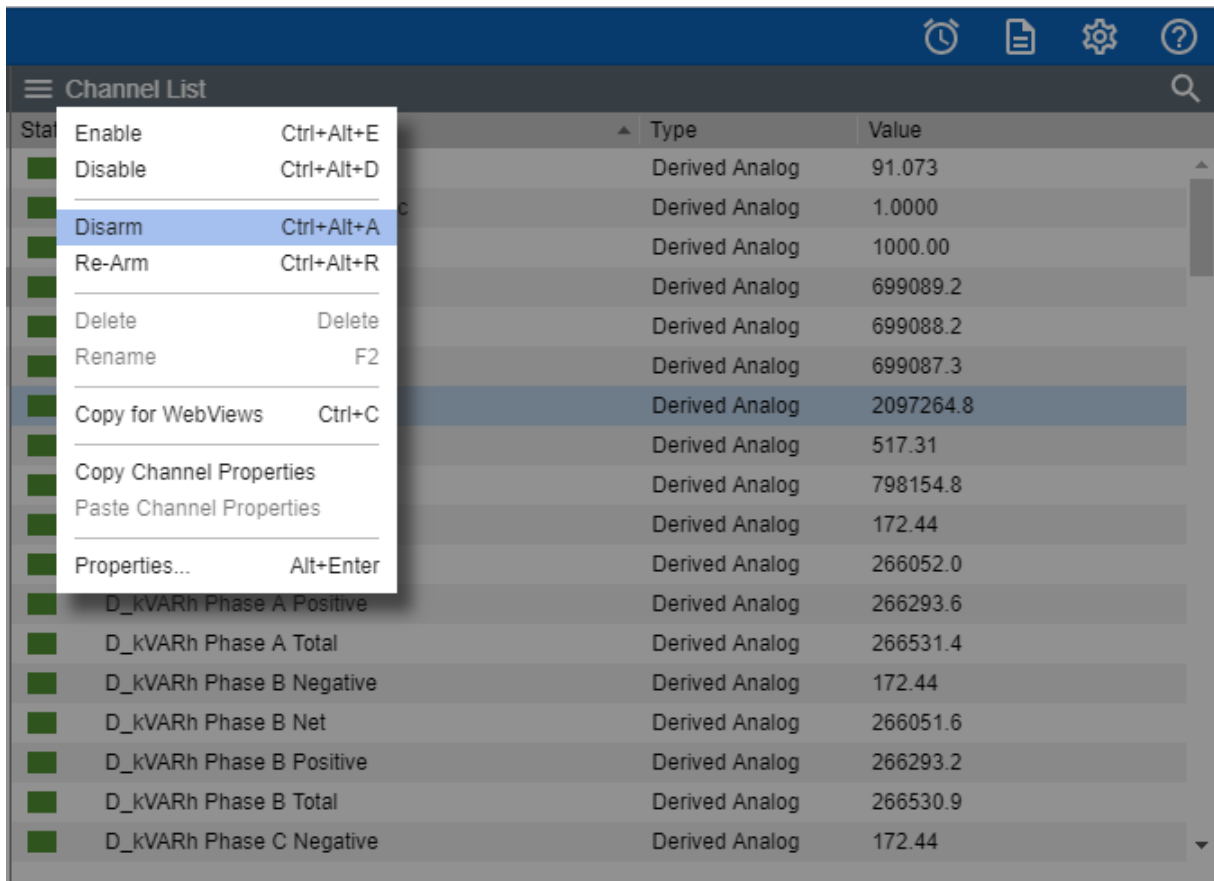
To Disarm a channel:

1. Select the channel you would like disarmed:

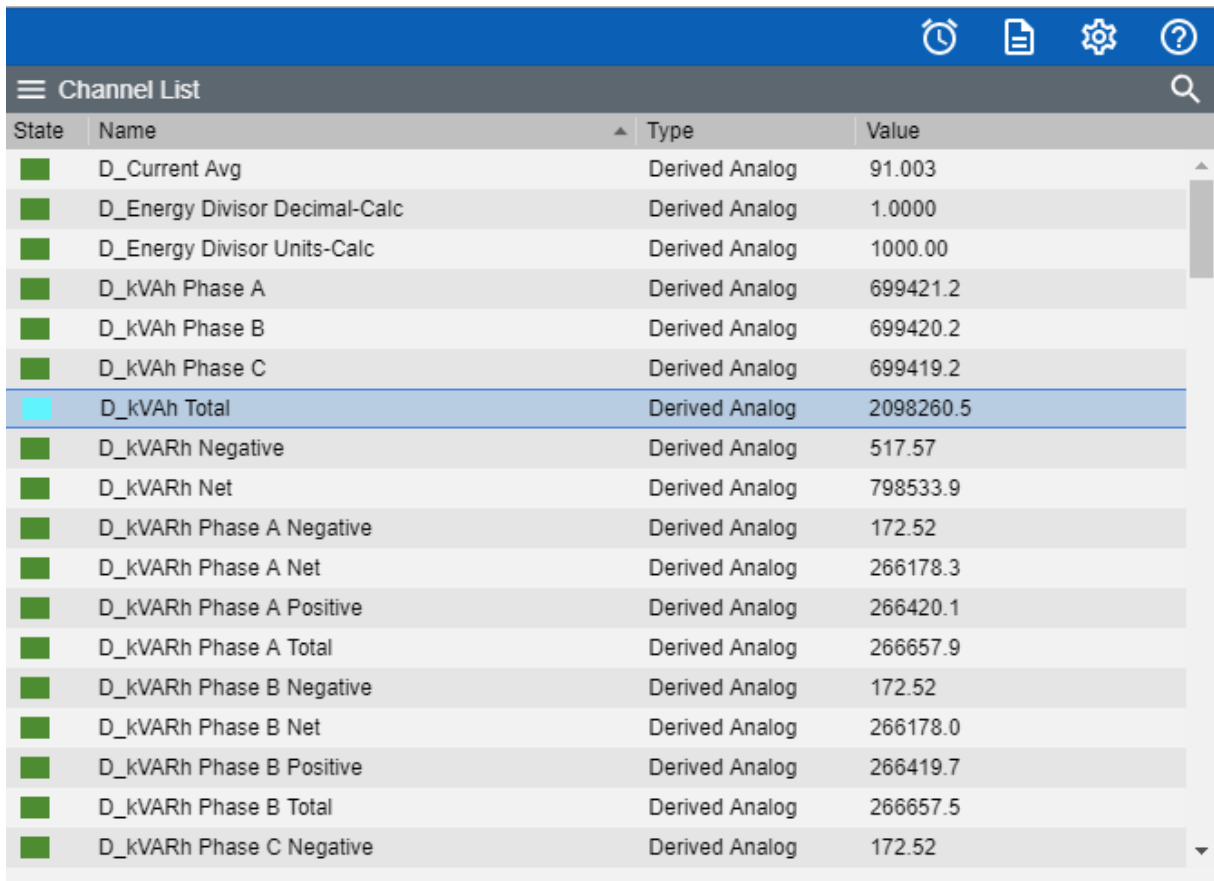


State	Name	Type	Value
■	D_Current Avg	Derived Analog	92.705
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	692054.2
■	D_kVAh Phase B	Derived Analog	692053.3
■	D_kVAh Phase C	Derived Analog	692052.3
■	D_kVAh Total	Derived Analog	2076159.8
■	D_kVARh Negative	Derived Analog	511.84
■	D_kVARh Net	Derived Analog	790122.9
■	D_kVARh Phase A Negative	Derived Analog	170.61
■	D_kVARh Phase A Net	Derived Analog	263374.7
■	D_kVARh Phase A Positive	Derived Analog	263613.9
■	D_kVARh Phase A Total	Derived Analog	263849.3
■	D_kVARh Phase B Negative	Derived Analog	170.61
■	D_kVARh Phase B Net	Derived Analog	263374.3
■	D_kVARh Phase B Positive	Derived Analog	263613.5
■	D_kVARh Phase B Total	Derived Analog	263848.8
■	D_kVARh Phase C Negative	Derived Analog	170.61

2. Select Disarm from the Channel List Menu



3. The channel will now be in a disarmed state

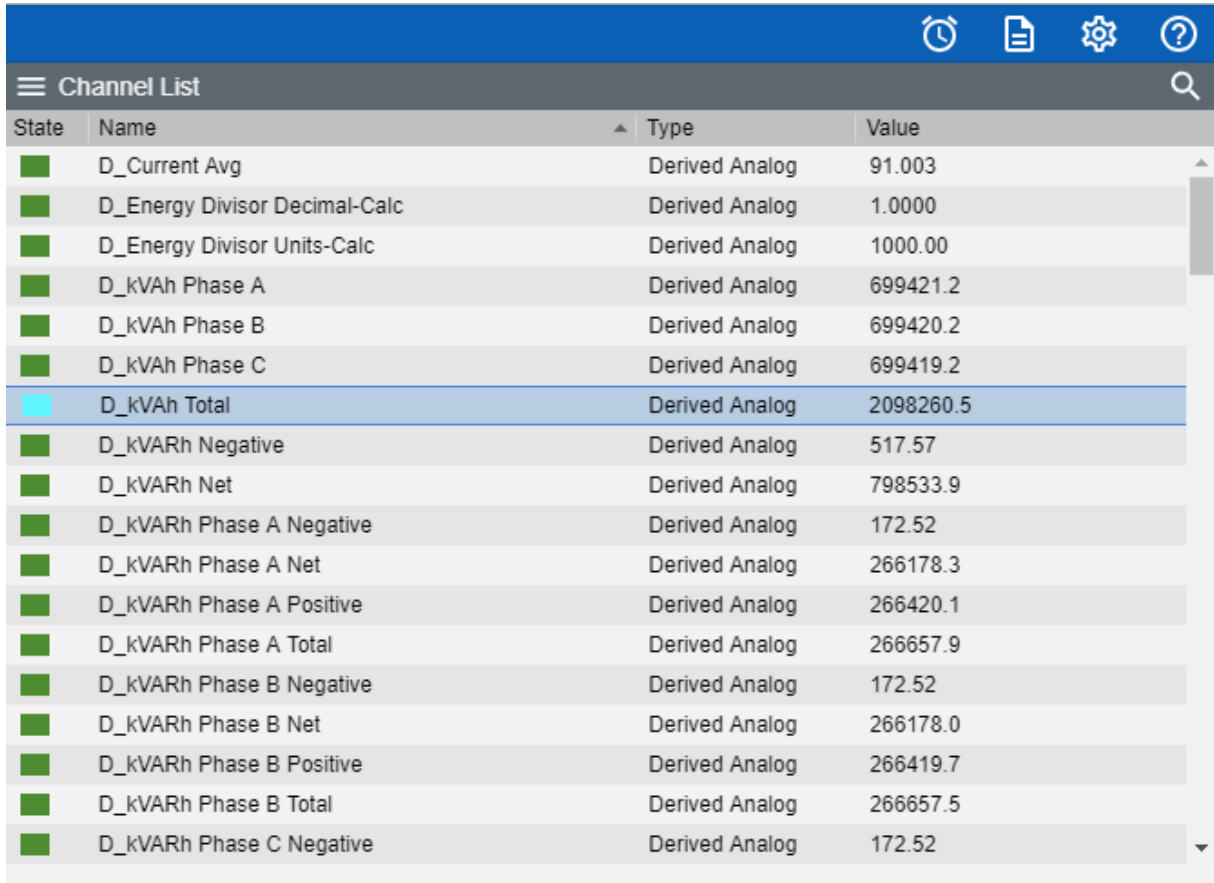


Re-Arm

The Re-Arm command resumes testing the value against alarm limits.

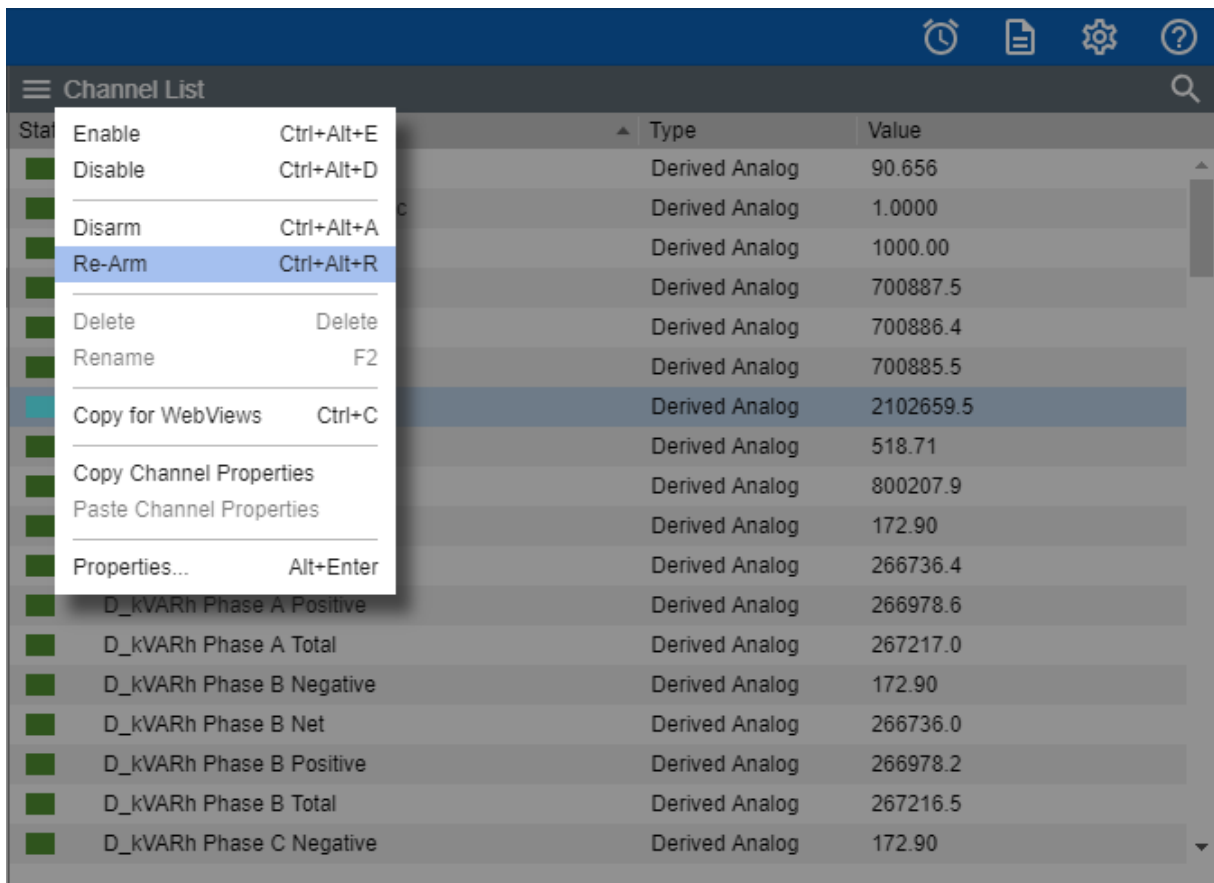
To Re-Arm a channel:

1. Select the channel you would like Re-Armed:

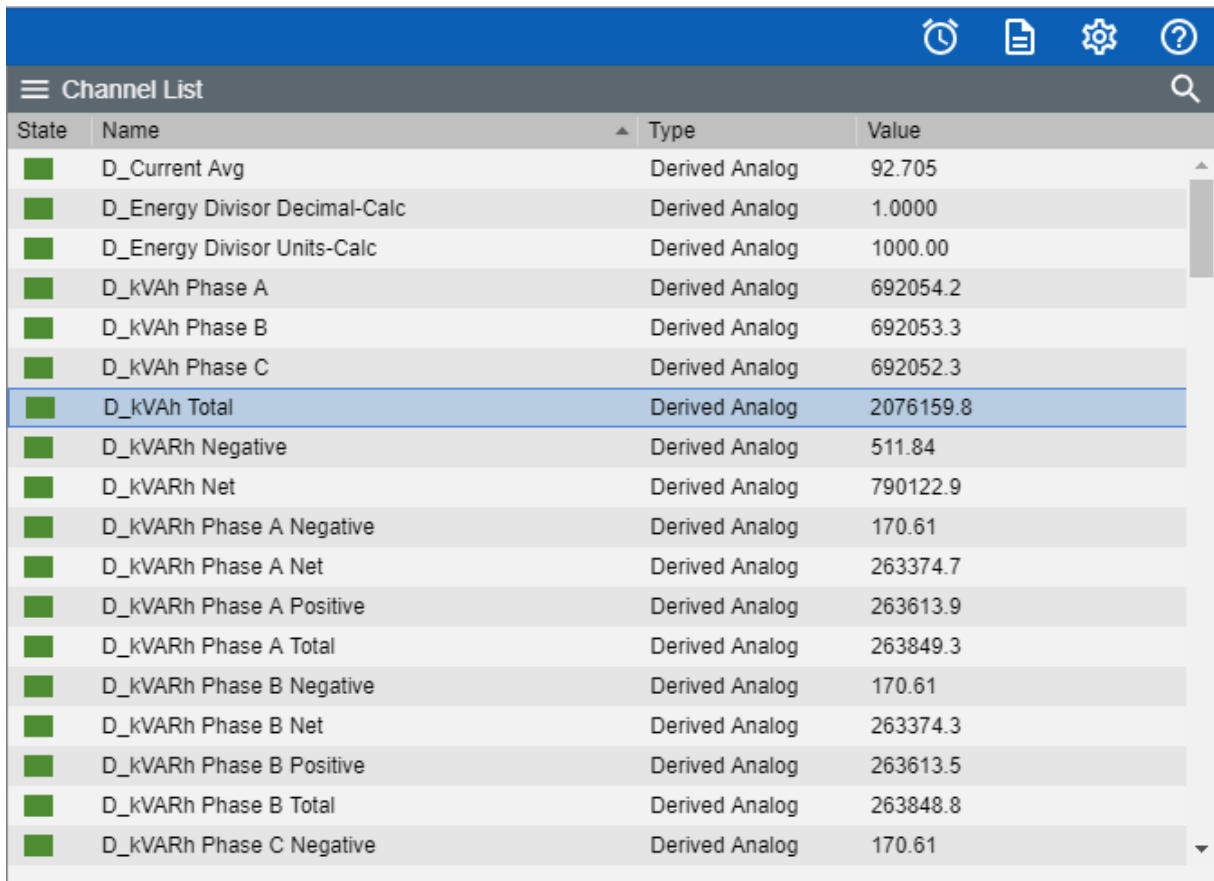


State	Name	Type	Value
■	D_Current Avg	Derived Analog	91.003
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	699421.2
■	D_kVAh Phase B	Derived Analog	699420.2
■	D_kVAh Phase C	Derived Analog	699419.2
■	D_kVAh Total	Derived Analog	2098260.5
■	D_kVARh Negative	Derived Analog	517.57
■	D_kVARh Net	Derived Analog	798533.9
■	D_kVARh Phase A Negative	Derived Analog	172.52
■	D_kVARh Phase A Net	Derived Analog	266178.3
■	D_kVARh Phase A Positive	Derived Analog	266420.1
■	D_kVARh Phase A Total	Derived Analog	266657.9
■	D_kVARh Phase B Negative	Derived Analog	172.52
■	D_kVARh Phase B Net	Derived Analog	266178.0
■	D_kVARh Phase B Positive	Derived Analog	266419.7
■	D_kVARh Phase B Total	Derived Analog	266657.5
■	D_kVARh Phase C Negative	Derived Analog	172.52

2. Select Re-Arm from the Channel List Menu



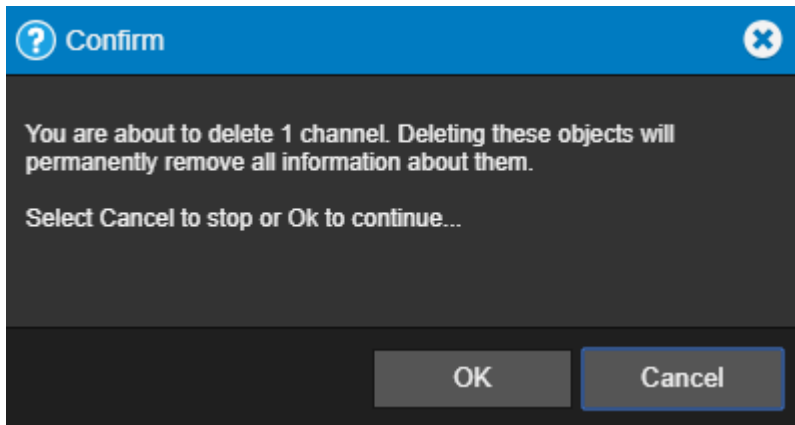
3. The channel will now be in a Re-Armed state



Delete

The Delete command permanently deletes the selected Channel from the configuration. Once removed, its archived information is no longer available.

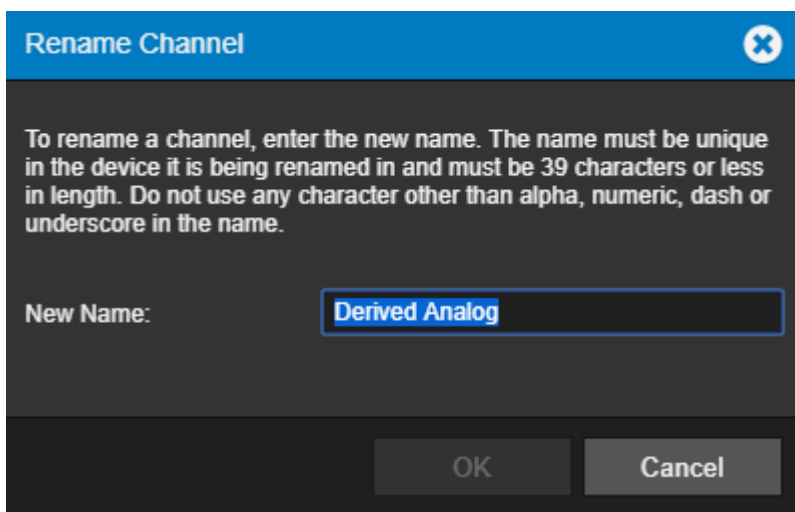
- ✔ Deleting a Channel should be done with discretion as removing it can have an adverse effect on Foreseer WebViews.



Rename

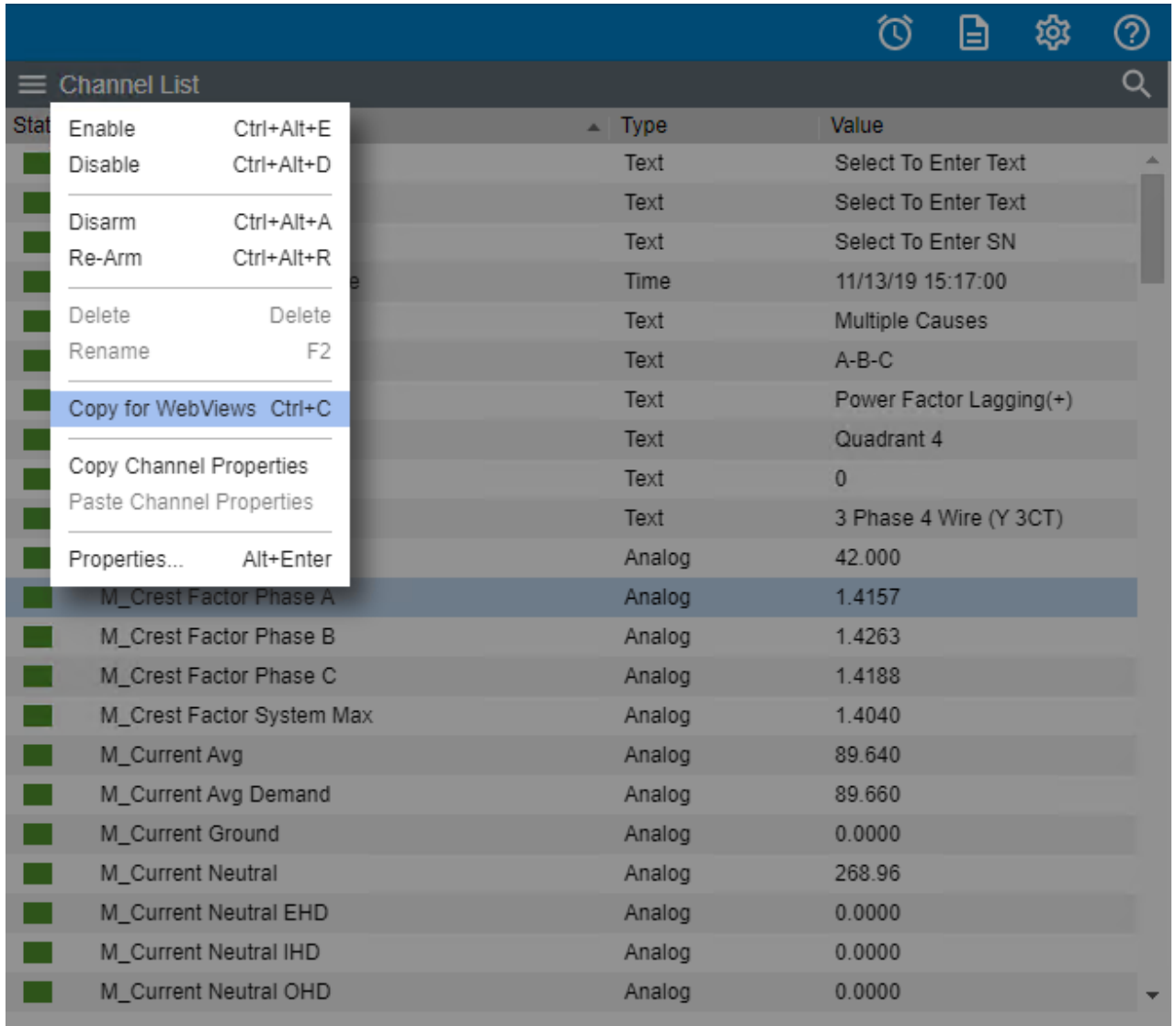
The Rename command renames the selected Channel.

- ✔ Renaming a Channel should be done with discretion as changing a name can have an adverse effect on Foreseer WebViews.



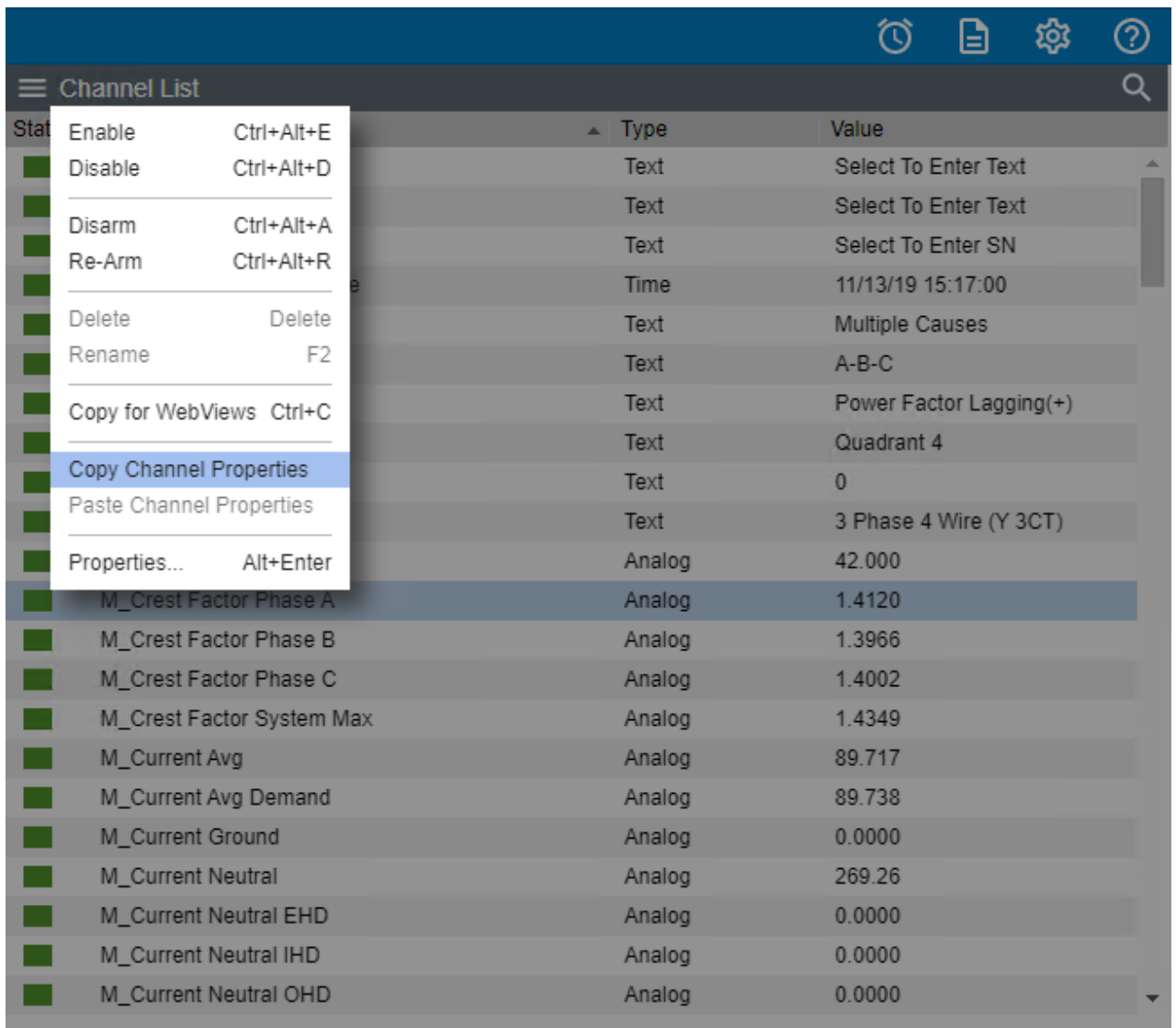
Copy for WebViews

The Copy for WebViews command copies the selected channels to the target folder in the WebViews tree.



Copy Channel Properties

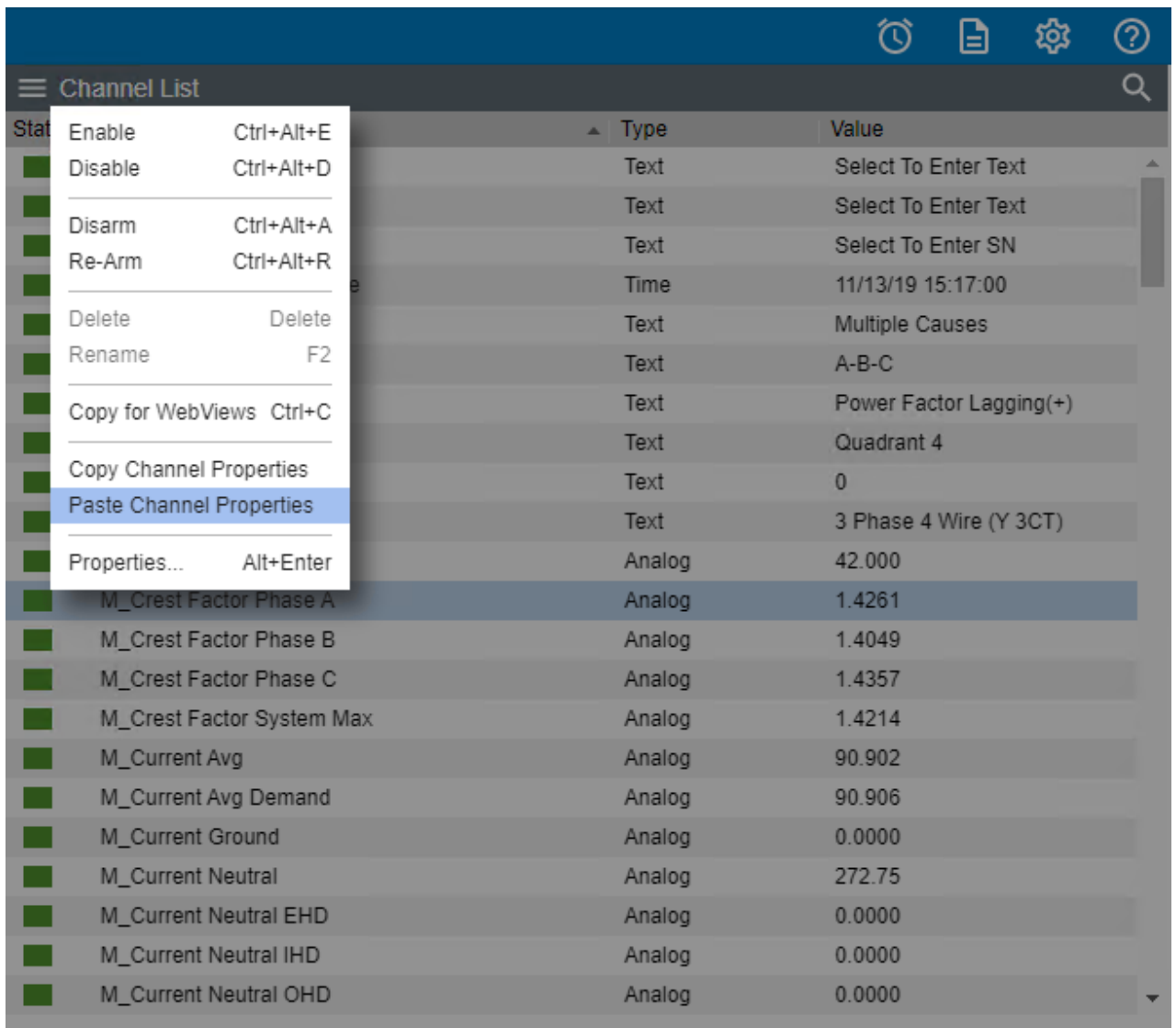
The Copy Channel Properties command copies all of the currently selected devices channel Properties to the Windows clipboard, allowing its settings to be pasted directly into another channel as its operational parameters.



- ✓ The channel being copied must be of the exact same type as the one the Properties are being pasted into.

Paste Channel Properties

The Paste Channel Properties command pastes the previously copied properties into the currently selected channel as its operational parameters. It also is useful when duplicating numerous channel settings on multiple devices. In either case, the channel or device being pasted into must be of the exact same type as the one from which the properties are being copied. These settings then can be individually modified as necessary. If copying from a device (rather than a single channel), only those channels with the same name will have their properties pasted.



Properties

- ✔ Consult with Eaton Field Engineering or Technical Support personnel before changing any channel behavior.

The Properties command furnishes operational information on the Channel. The General tab allows a channel to be Disabled or Enabled as well as providing selections that control how its data is archived on the Server.

The screenshot shows a 'Channel List' table with a context menu open over a row. The table has columns for 'Stat', 'Type', and 'Value'. The context menu includes options like 'Enable', 'Disable', 'Disarm', 'Re-Arm', 'Delete', 'Rename', 'Copy for WebViews', 'Copy Channel Properties', 'Paste Channel Properties', and 'Properties...'. The 'Properties...' option is highlighted.

Stat	Type	Value
Enable	Ctrl+Alt+E	
Disable	Ctrl+Alt+D	
Disarm	Ctrl+Alt+A	
Re-Arm	Ctrl+Alt+R	
Delete	Delete	
Rename	F2	
Copy for WebViews	Ctrl+C	
Copy Channel Properties		
Paste Channel Properties		
Properties...	Alt+Enter	
M_Crest Factor Phase A	Analog	1.4387
M_Crest Factor Phase B	Analog	1.4260
M_Crest Factor Phase C	Analog	1.3872
M_Crest Factor System Max	Analog	1.4405
M_Current Avg	Analog	91.003
M_Current Avg Demand	Analog	91.007
M_Current Ground	Analog	0.0000
M_Current Neutral	Analog	273.07
M_Current Neutral EHD	Analog	0.0000
M_Current Neutral IHD	Analog	0.0000
M_Current Neutral OHD	Analog	0.0000

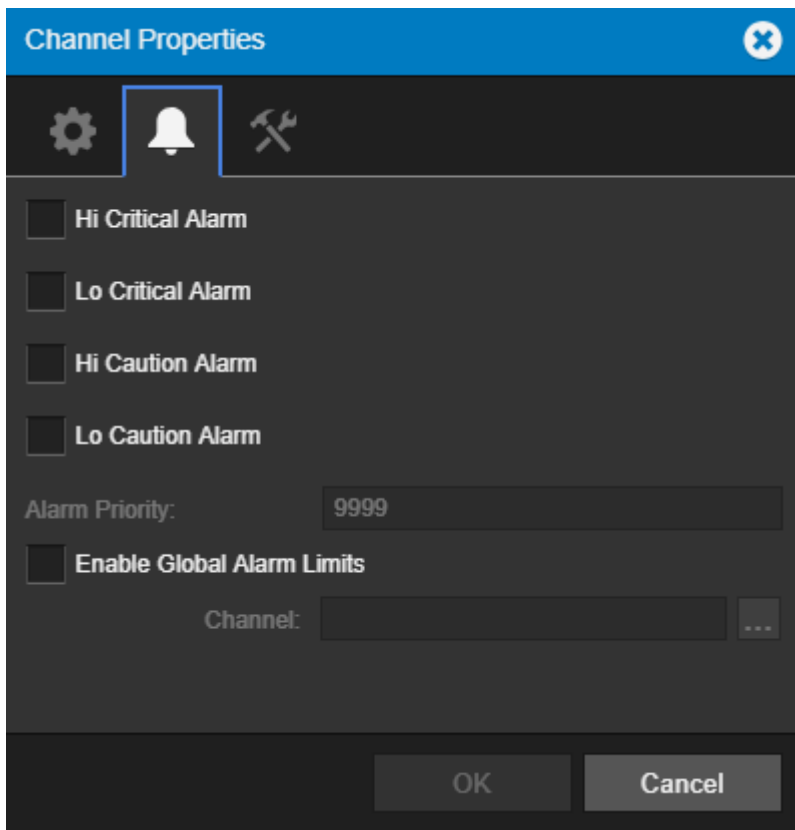
The screenshot shows the 'Channel Properties' dialog box. It has a title bar with a close button. Below the title bar are three icons: a gear (selected), a bell, and a wrench. The dialog contains the following fields:

- Name: \\7044 Test 1\Eaton PXM 2270 Meter 1\M_
- Current State: Normal
- Current Value: 232.47
- Description: Current Phase A
- Units: Amps
- Archive: Average

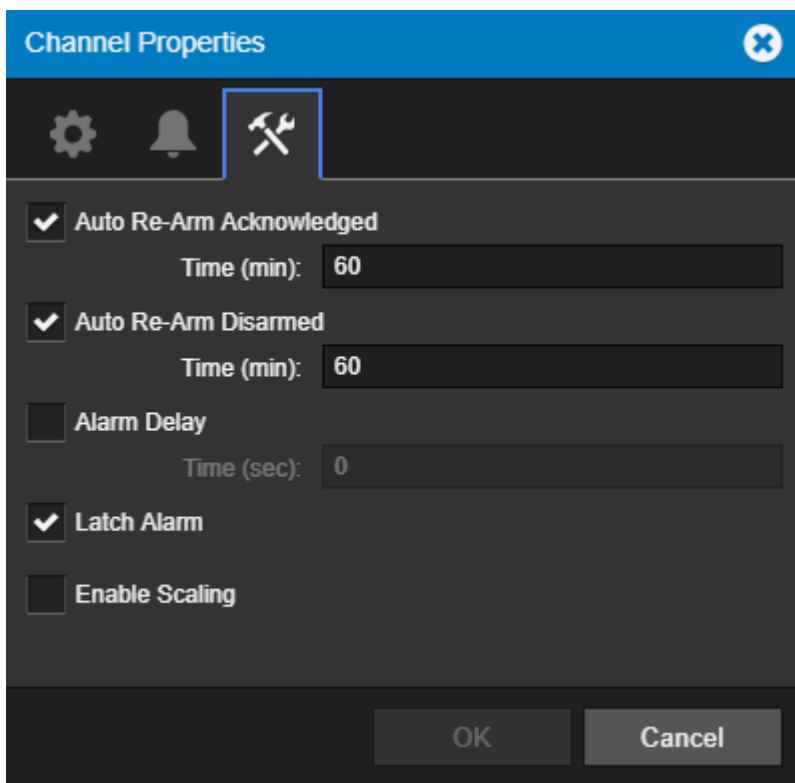
At the bottom, there are 'OK' and 'Cancel' buttons.

The Basic tab configures the Channel's alarm thresholds, associated Messages and relative

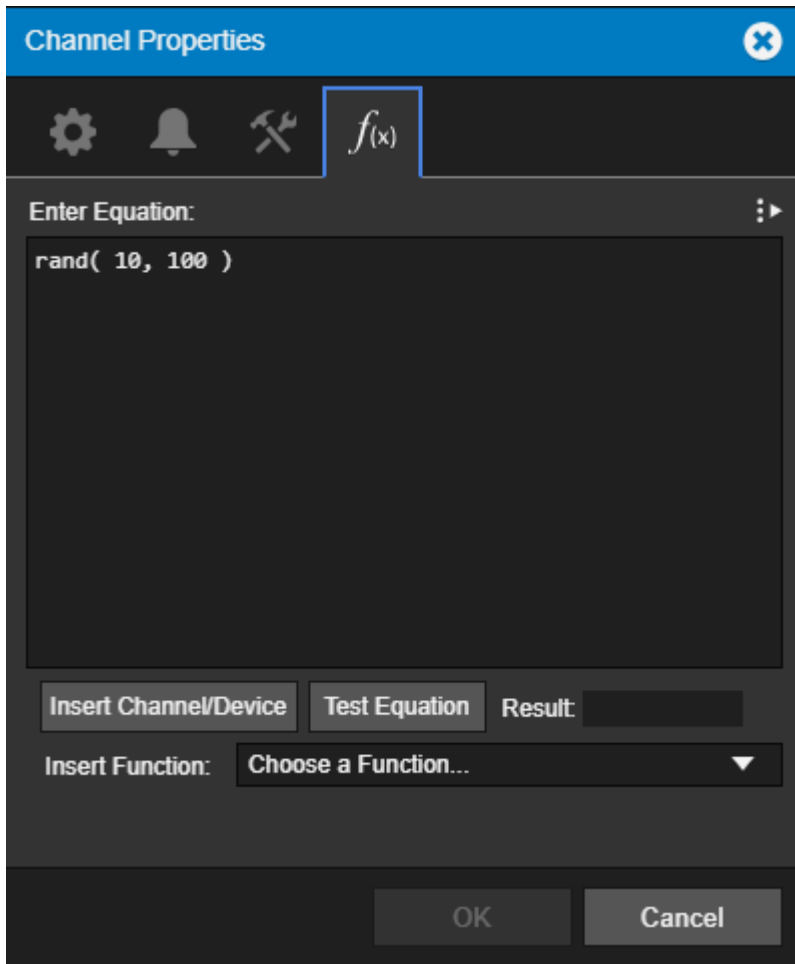
importance.



The Advanced tab configures alarm behavior as well as the scaling functions.



The User-Defined Equation tab defines the Transfer Equations for Derived Channels.



WebViews Menu

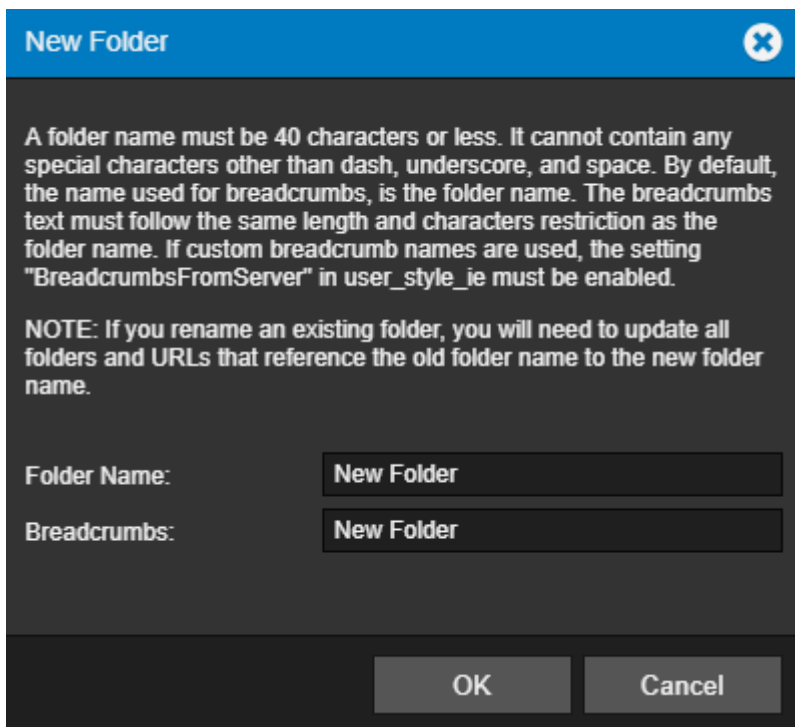
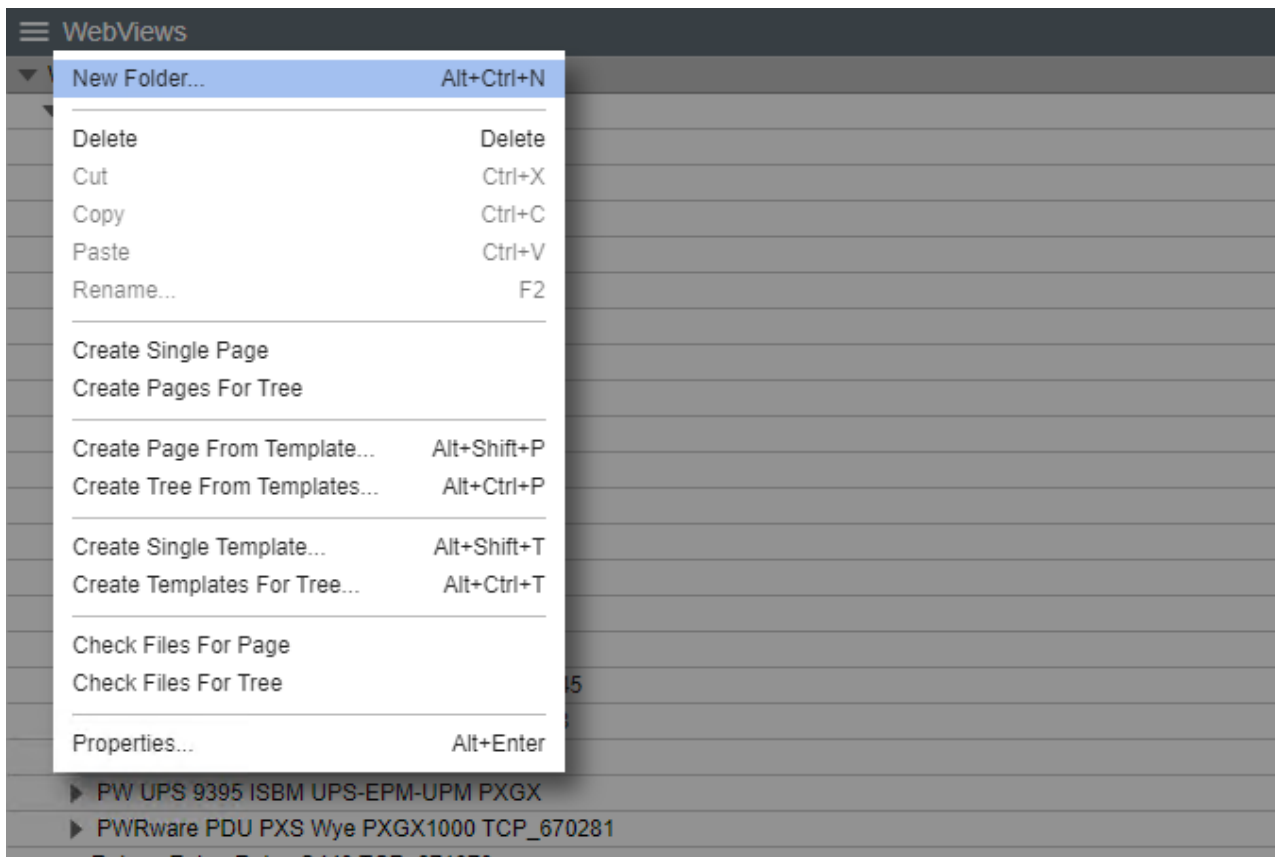
The WebViews List menu provides access to all of the functionality that will be required to manage your Foreseer WebViews files.

- New Folder
- Delete
- Cut
- Copy
- Paste
- Rename
- Create Single Page / Create Pages for Tree
- Create Page From Template / Create Tree from Templates
- Create Single Template / Create Templates for Tree
- Create Files for Page
- Create Files for Tree
- Properties

New Folder

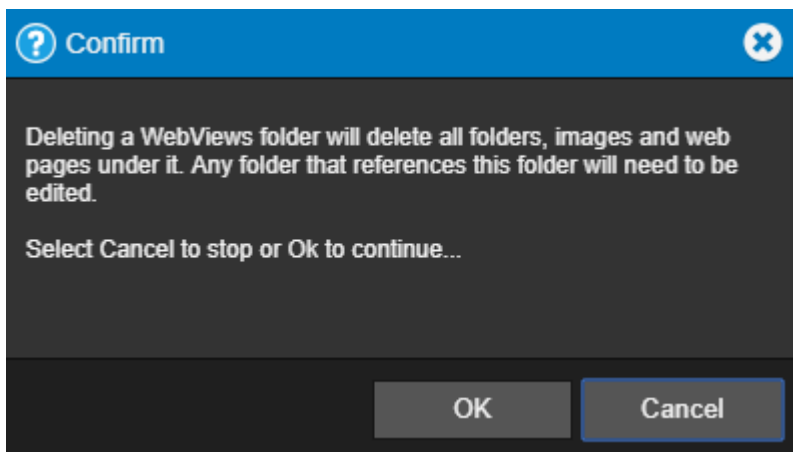
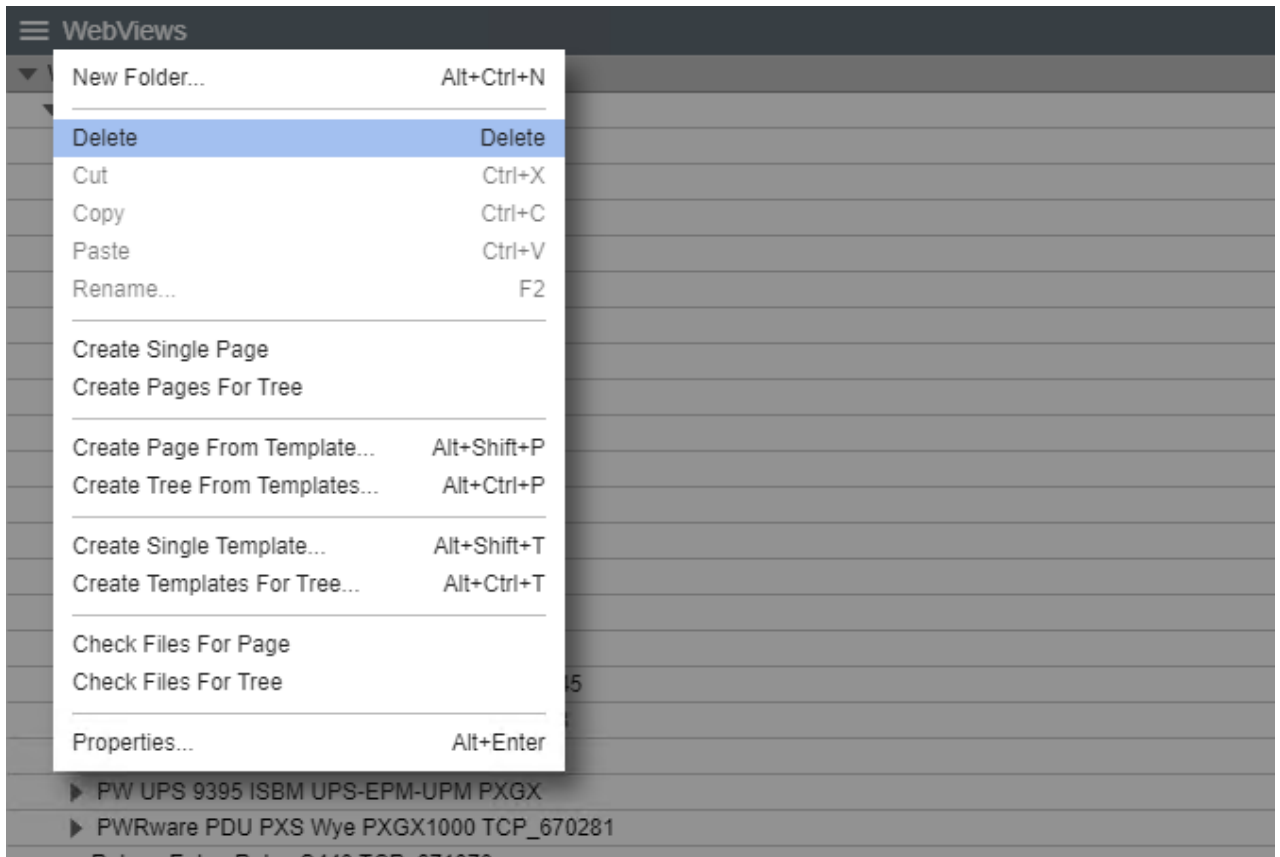
The New Folder command creates a new folder as a child of the currently selected folder.

The corresponding WebViews page is also created.



Delete

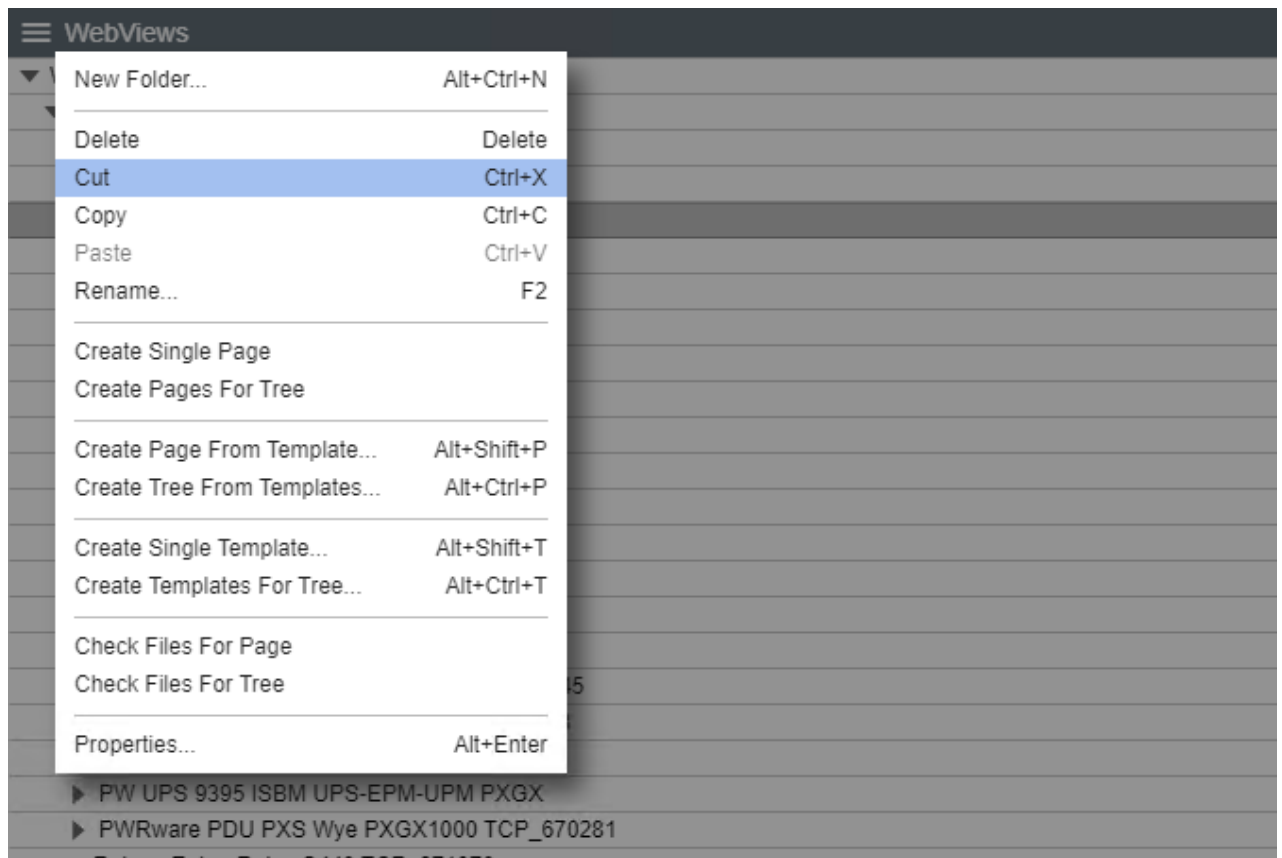
The Delete command deletes the currently selected folder and WebViews page.



- ✔ Deleting a WebViews folder will delete all folders, images, and web pages under it. Any folder that references this folder will need to be edited.

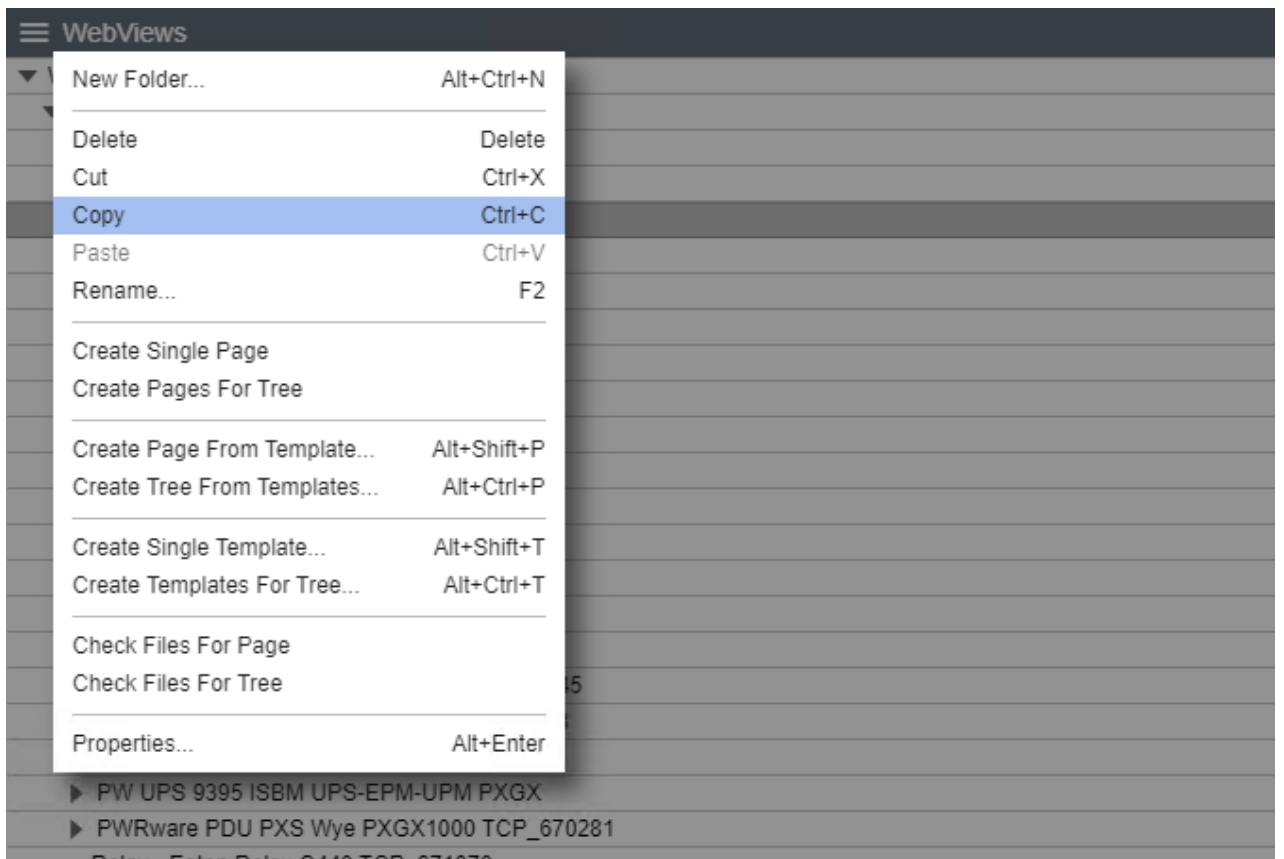
Cut

The Cut command cuts the currently selected folder (and WebViews page) so that it can be pasted to another location in the tree. There's no visual indication that the folder has been cut; however, following a Paste operation its location in the tree will change.



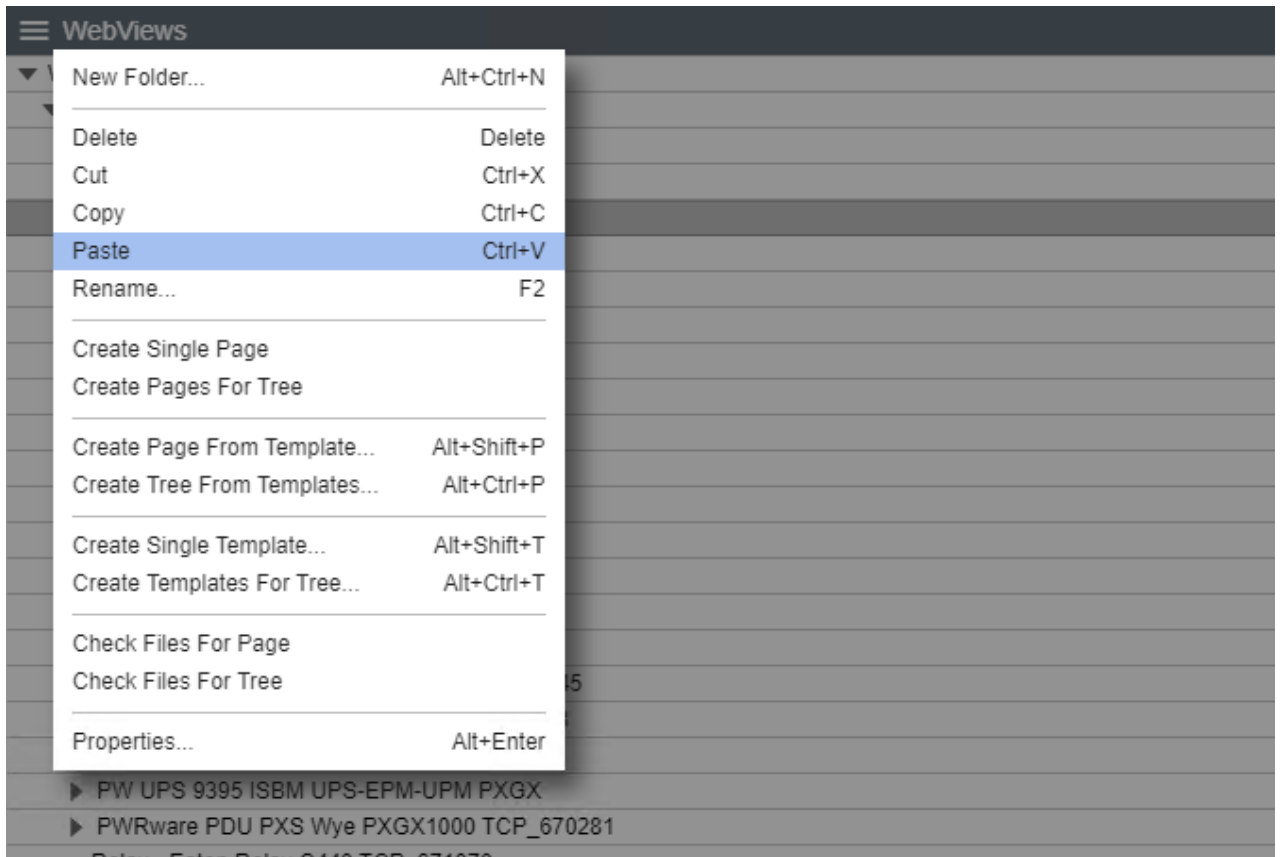
Copy

The Copy command copies the current folder and pastes the copy as a child of the selected folder.



Paste

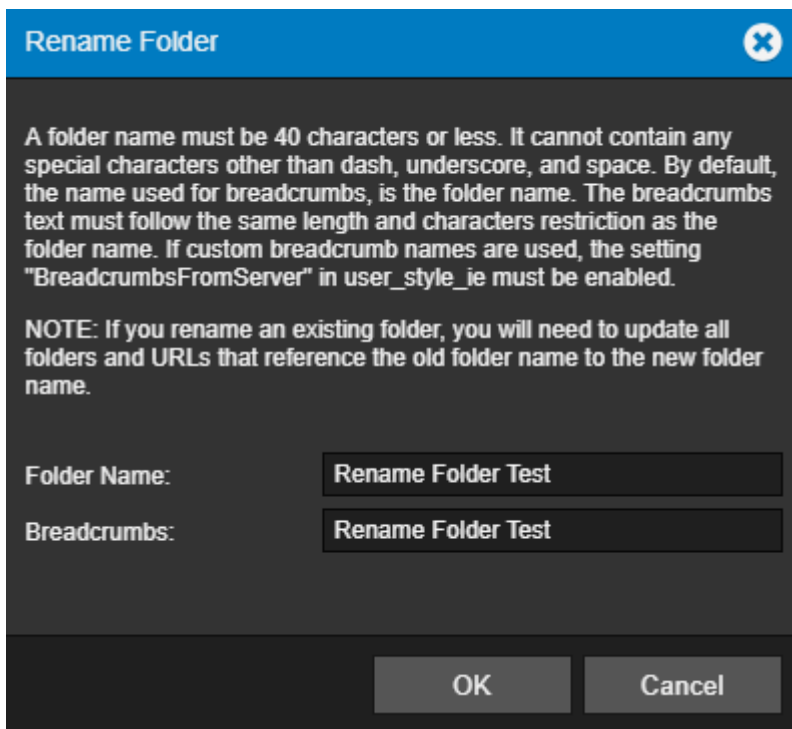
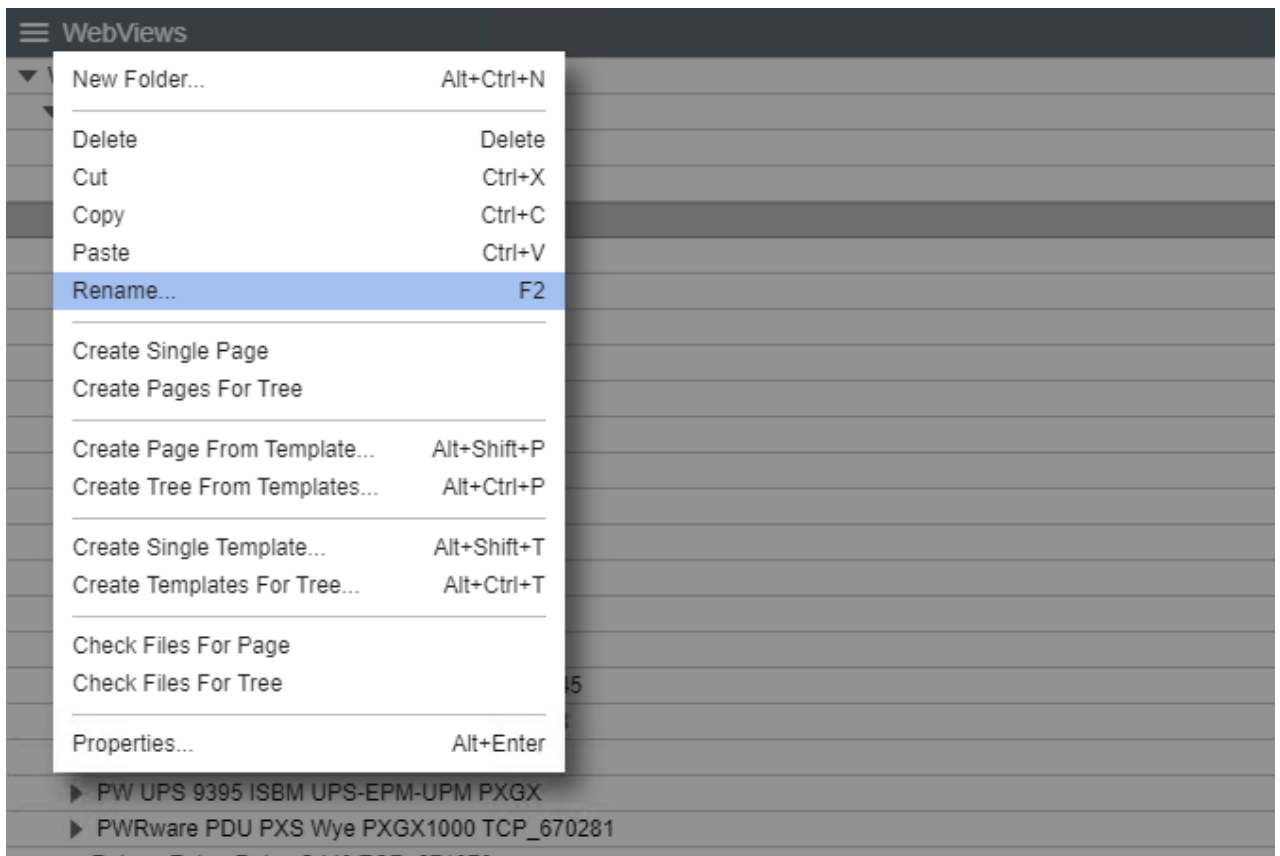
The paste command pastes the result of a Cut, Copy, or Copy Link operation as the child of the selected folder.



Rename

The Rename command renames the selected folder. If you are renaming a link, the target folder will be renamed as well. A folder name must be 40 characters or less. It cannot contain any special characters other than dash, underscore, and space. By default, the name used for breadcrumbs, is the folder name. The breadcrumbs text must follow the same length and characters restriction as the folder name. If custom breadcrumb names are used, the setting "BreadcrumbsFromServer" in user_style_ie must be enabled.

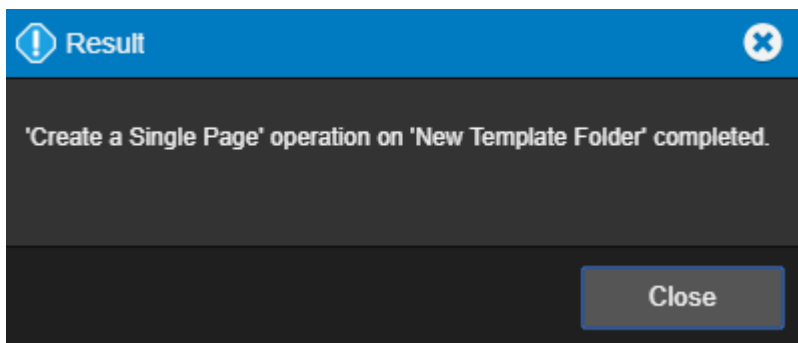
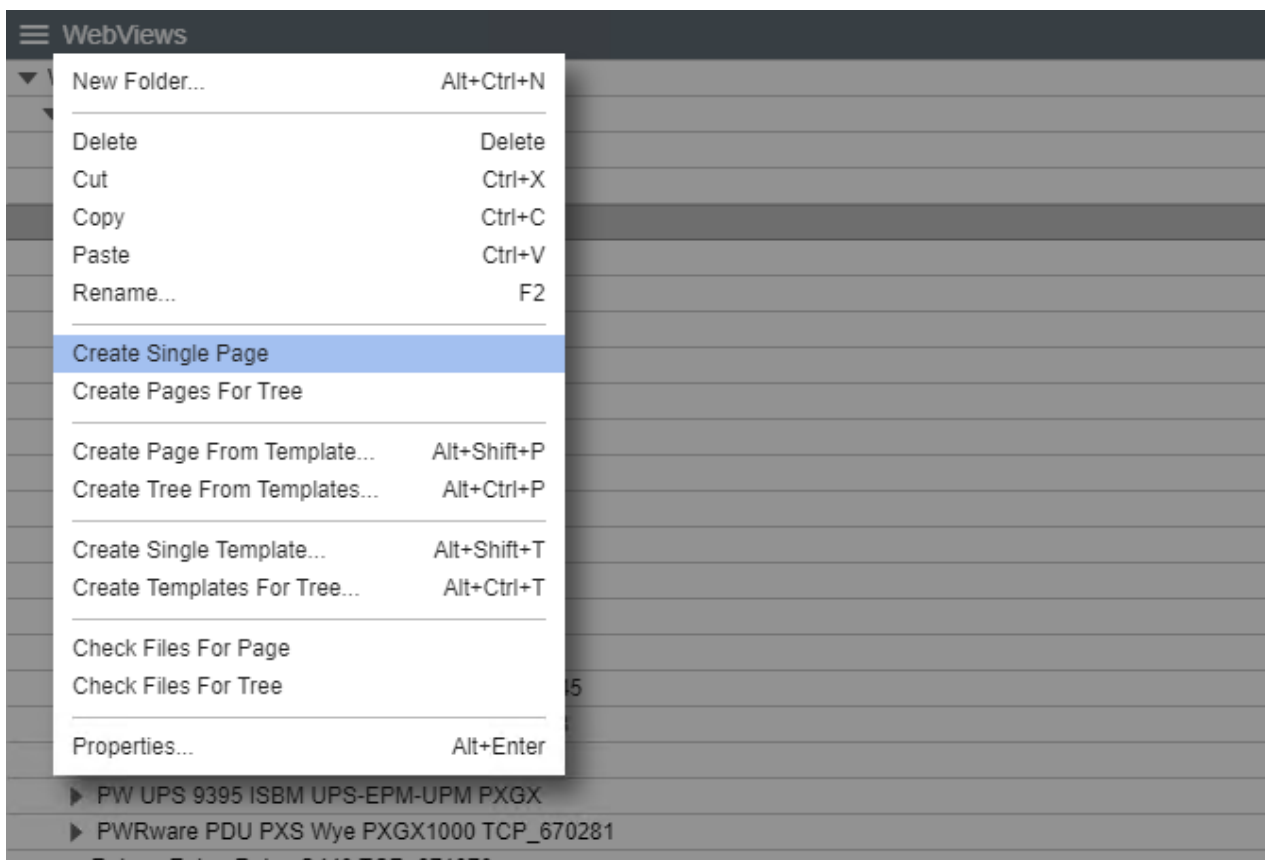
- ✔ If you rename an existing folder, you will need to update all folders and URLs that reference the old folder name to the new folder name.



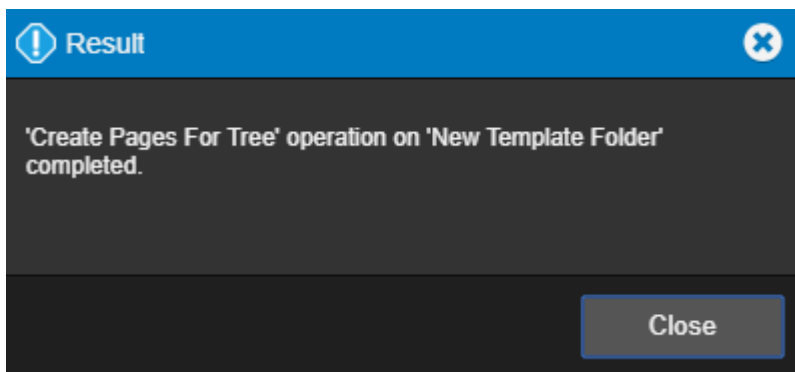
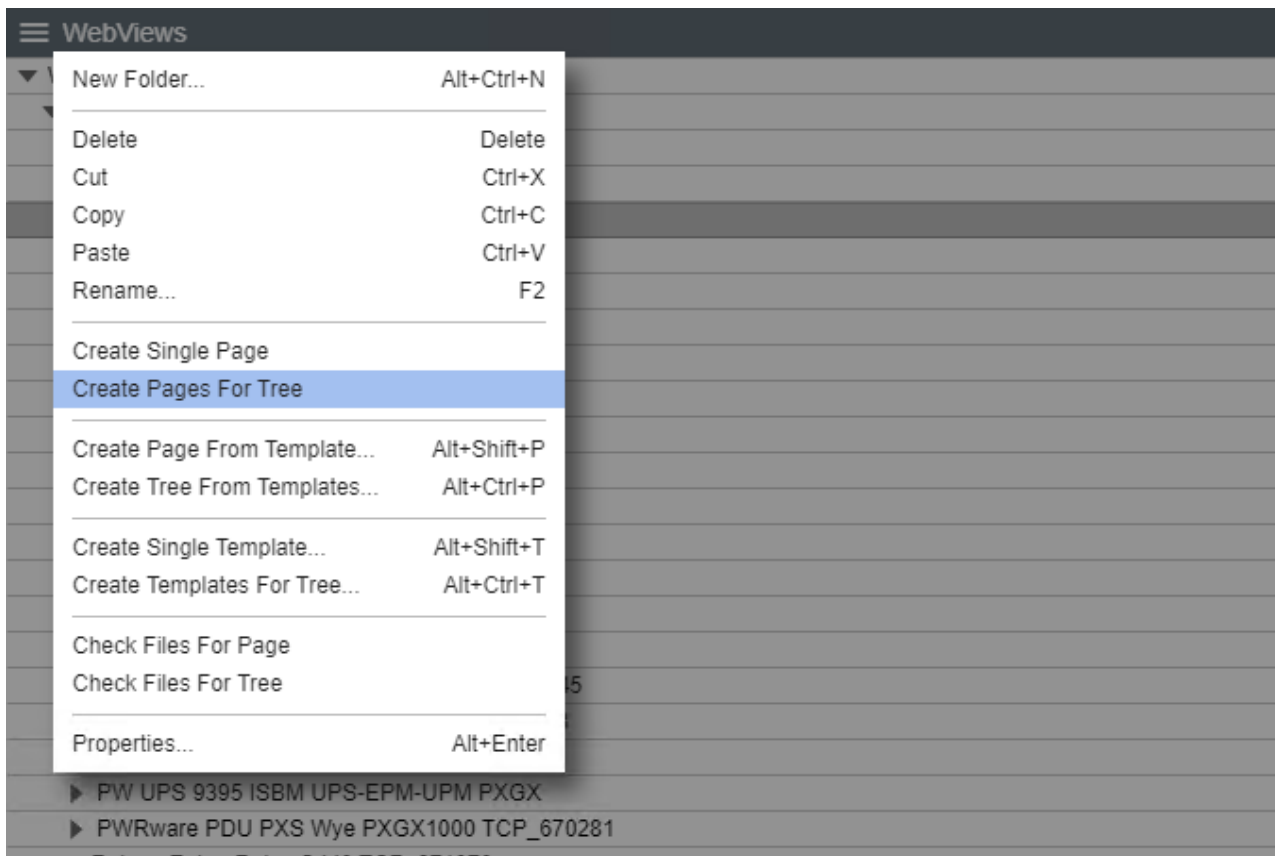
Create Single Page / Create Pages for Tree

The Create Single Page / Create Pages for Tree command recreates the WebViews page files for the selected folder in the tree. Two files, index.htm and layout.xml, are created when a WebViews Folder is created (they reside in the <Install Drive>:\Eaton

Corporation\Foreseer\WWW\WebViews folder on the server machine in a tree that mimics the structure of the WebViews tree. Should you corrupt either of these files in the course of editing (especially by editing the files directly), you can delete them and use this command to regenerate new files based on the system defaults.



The Create Pages for Tree command will recreate pages as needed for the selected folder and its children. New pages will be recreated only if either of the files for that folder are missing.

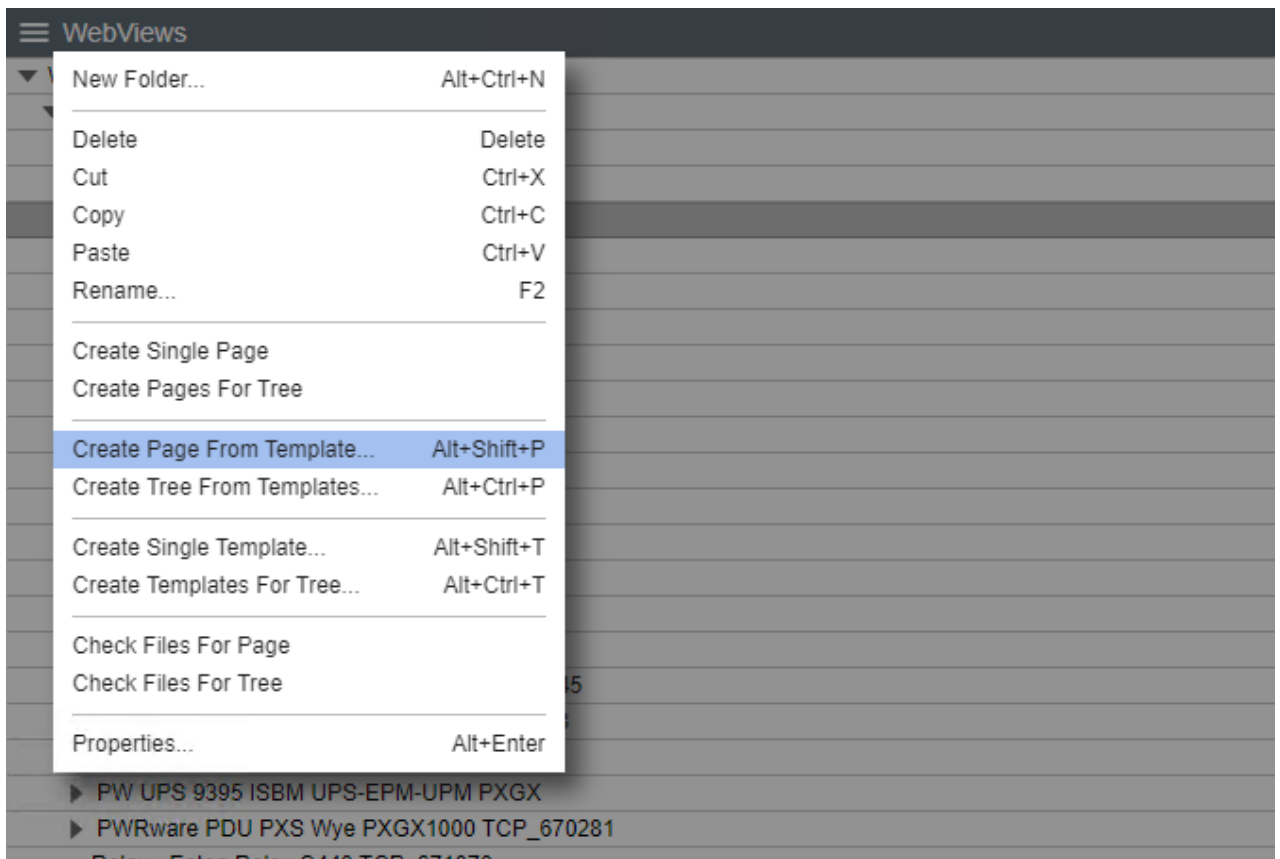


Create Page From Template / Create Tree from Templates

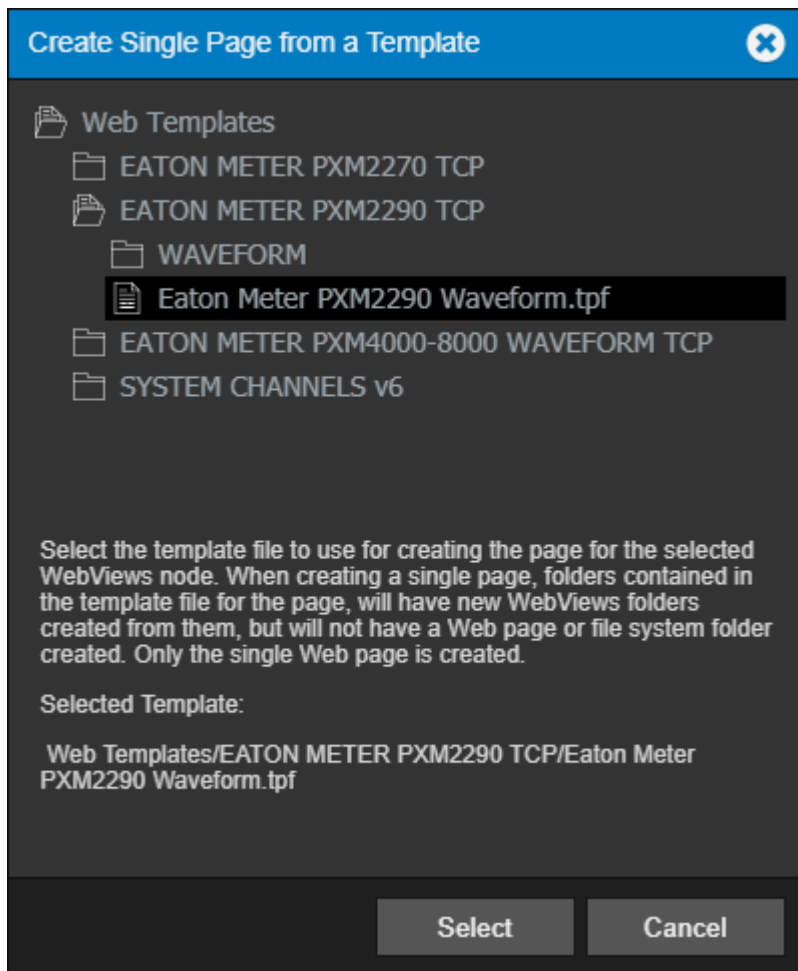
The Create Page From Template / Create Tree from Templates command creates a WebViews page or a section of the WebViews tree from the specified Template file. The page(s) can include specified Devices and their Channels.

To create a WebViews page or tree section from a template file:

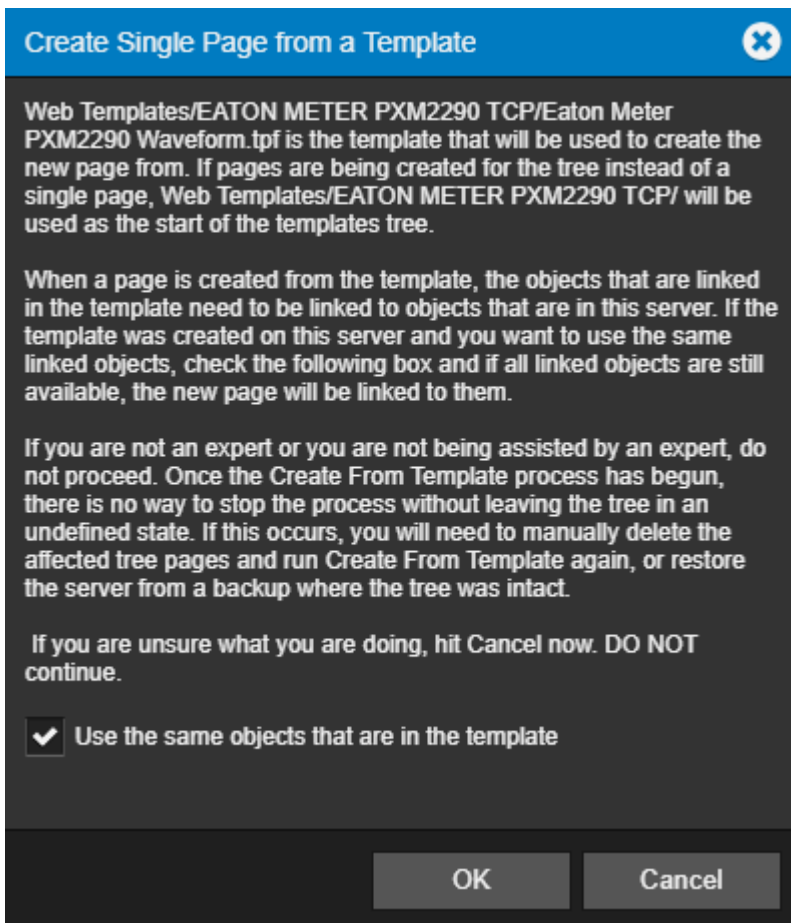
1. Highlight the location for the page in the WebViews panel and select Create Page from Template.



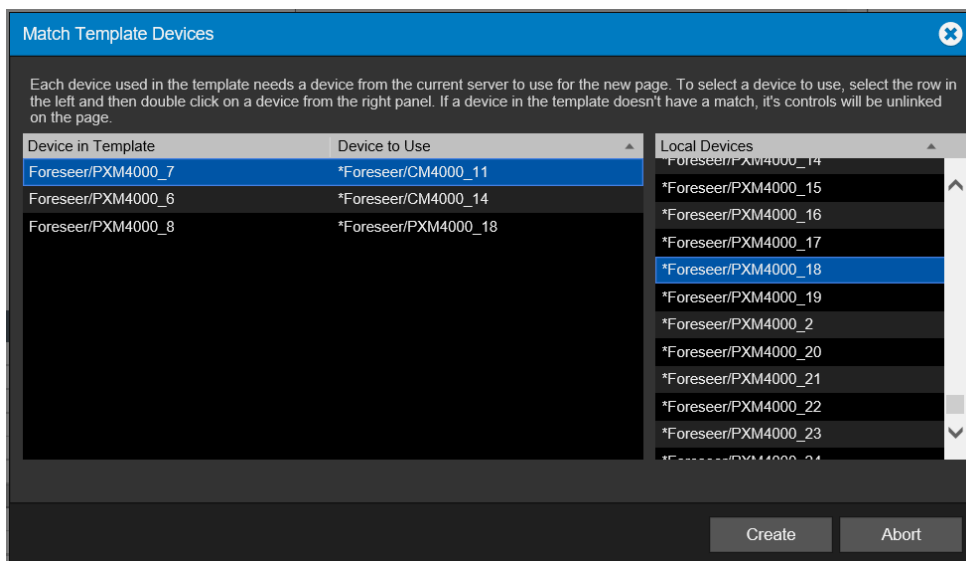
2. Select the .tpf template file to use. Template files for the currently selected folder in the templates tree are displayed. You can navigate through the tree to select files in other locations in the tree.



3. Click Select.
4. Select Use the same objects that are in the template to link to these objects automatically (if they are still available on the server). Selecting this option pre-populates the Device to Use field in the next dialog box. If you wish to select another device at that point, you still can even if this option is selected.



- In this step, you must select the device in the template and match that to an existing device in the server. The Device to Use field shows the currently selected device. You can select the server in the left pane and any device on the right pane. If you do not select a device identical to what was in the template, objects in the WebViews page will not have matching Channels and must be manually relinked.



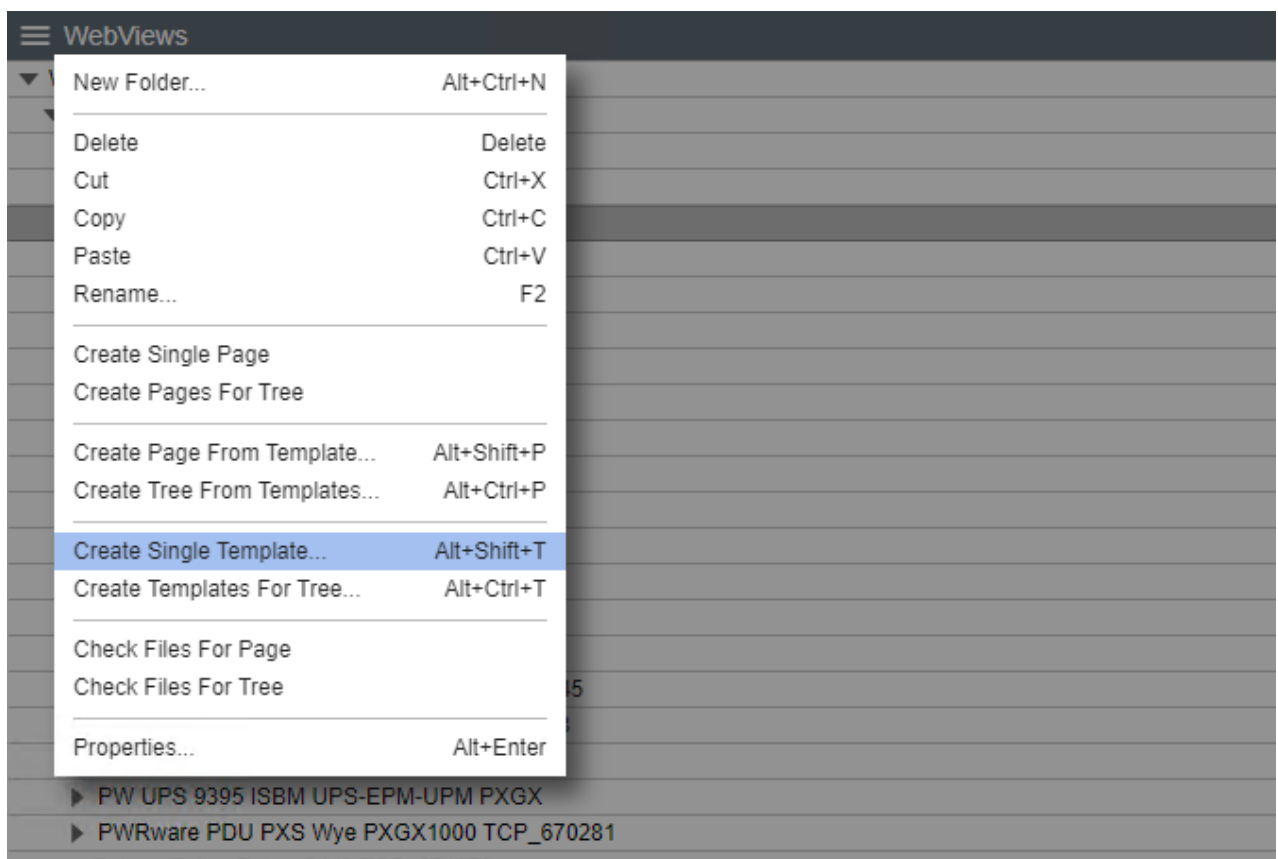
- When you've selected a device, click Create.
- The page is created and the WebViews folder should now show the set of channels from the selected device.

Create Single Template / Create Templates for Tree

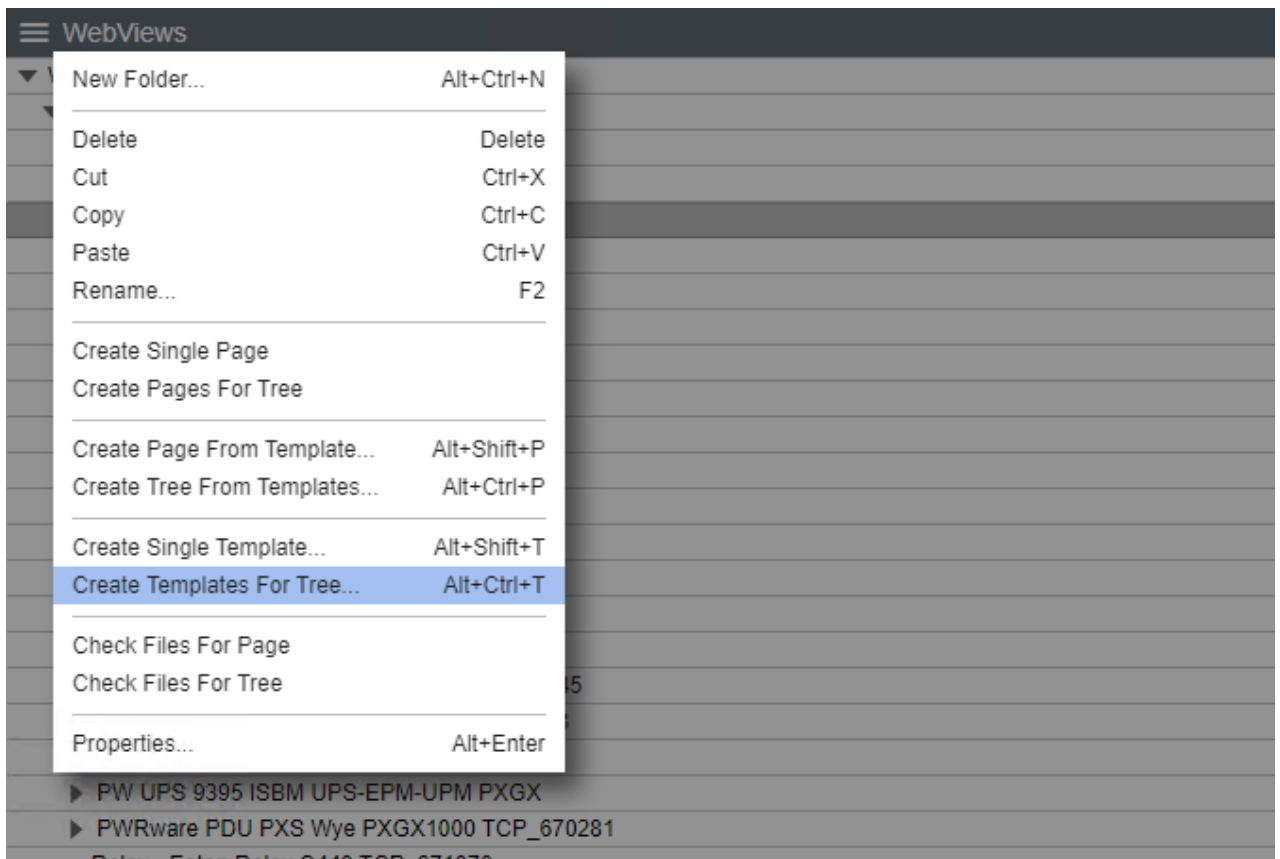
If you're using Create Single Template, the resulting template file is based on the selected WebViews page. This file will can then be used to create a copy of this WebViews page at different locations in the tree. If you're using Create Templates for Tree, the resulting template file can be used to create a copy of the selected WebViews page and all of its children. You can use this function to rapidly recreate repeating tree structures throughout the WebViews tree. For both functions, you can specify the device to use when specifying attached channels.

To create a template file:

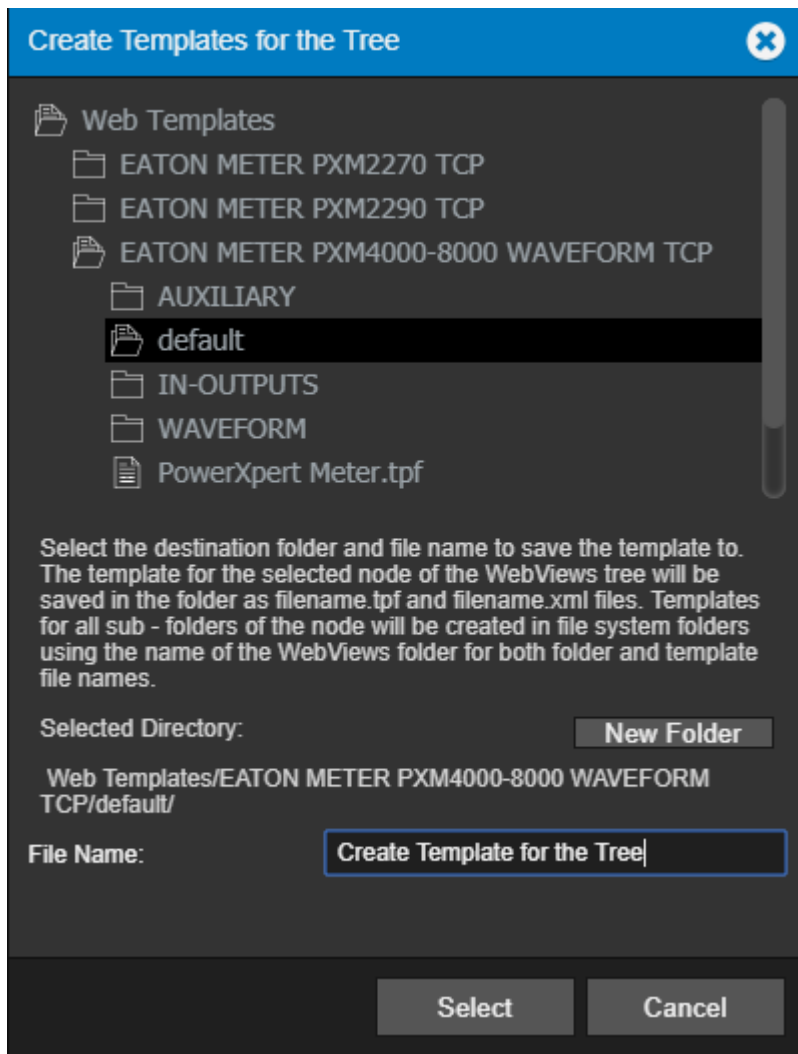
1. Highlight the location for the page in the WebViews panel and select Create Single Template.



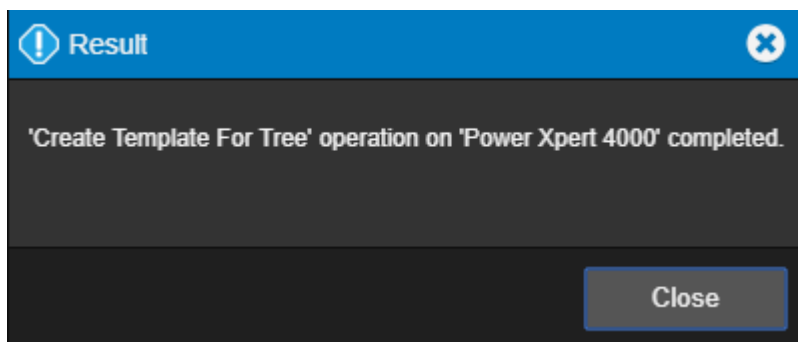
2. If you are using the Create Templates for Tree function, all of the child folders will also be included in the template file.



3. Select the .tpf template file to use. Template files for the currently selected folder in the templates tree are displayed. You can navigate through the tree to select files in other locations in the tree.

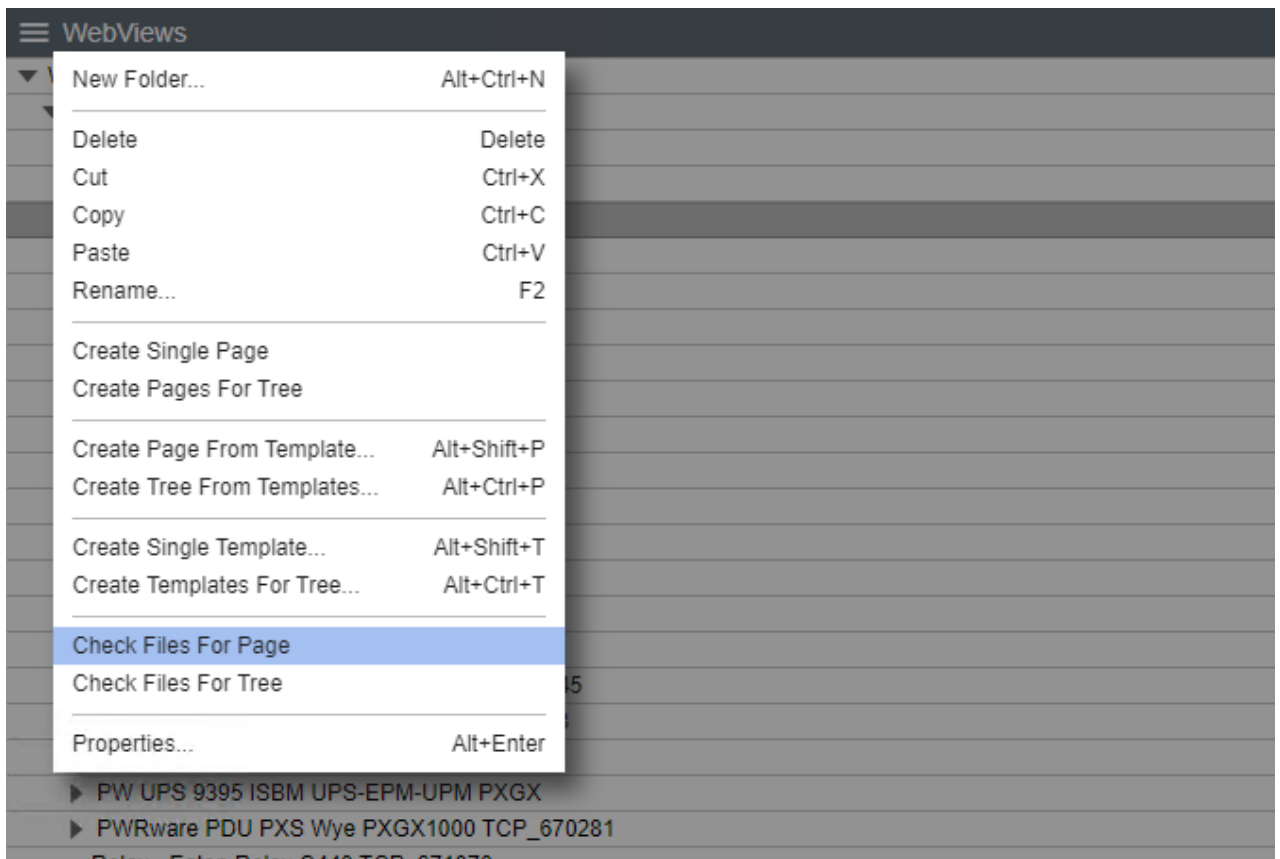


4. Click Select.



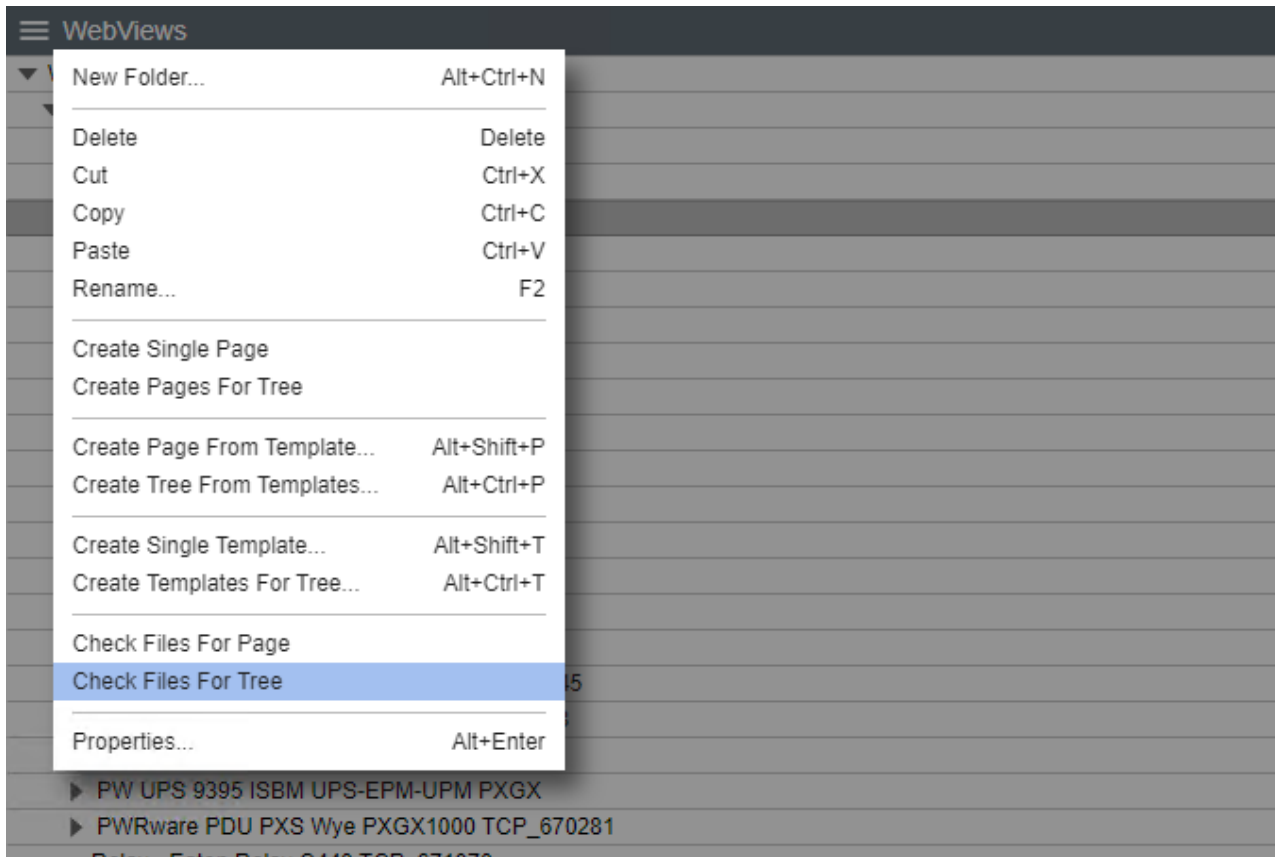
Check Files for Page

- ✔ This command is for specialized applications, and should only be used at the direction of Eaton technical support.



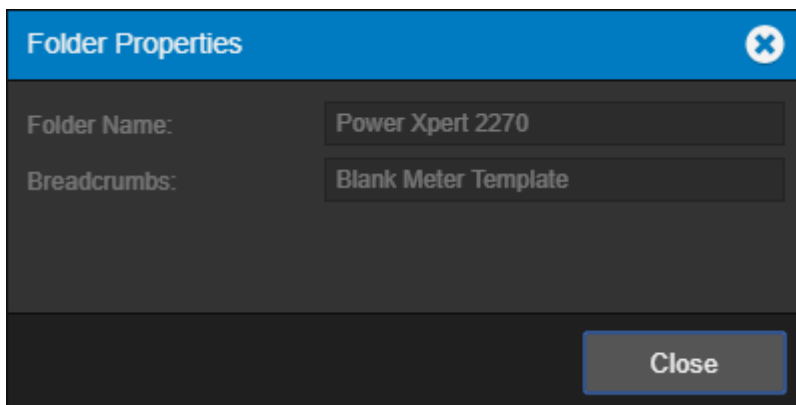
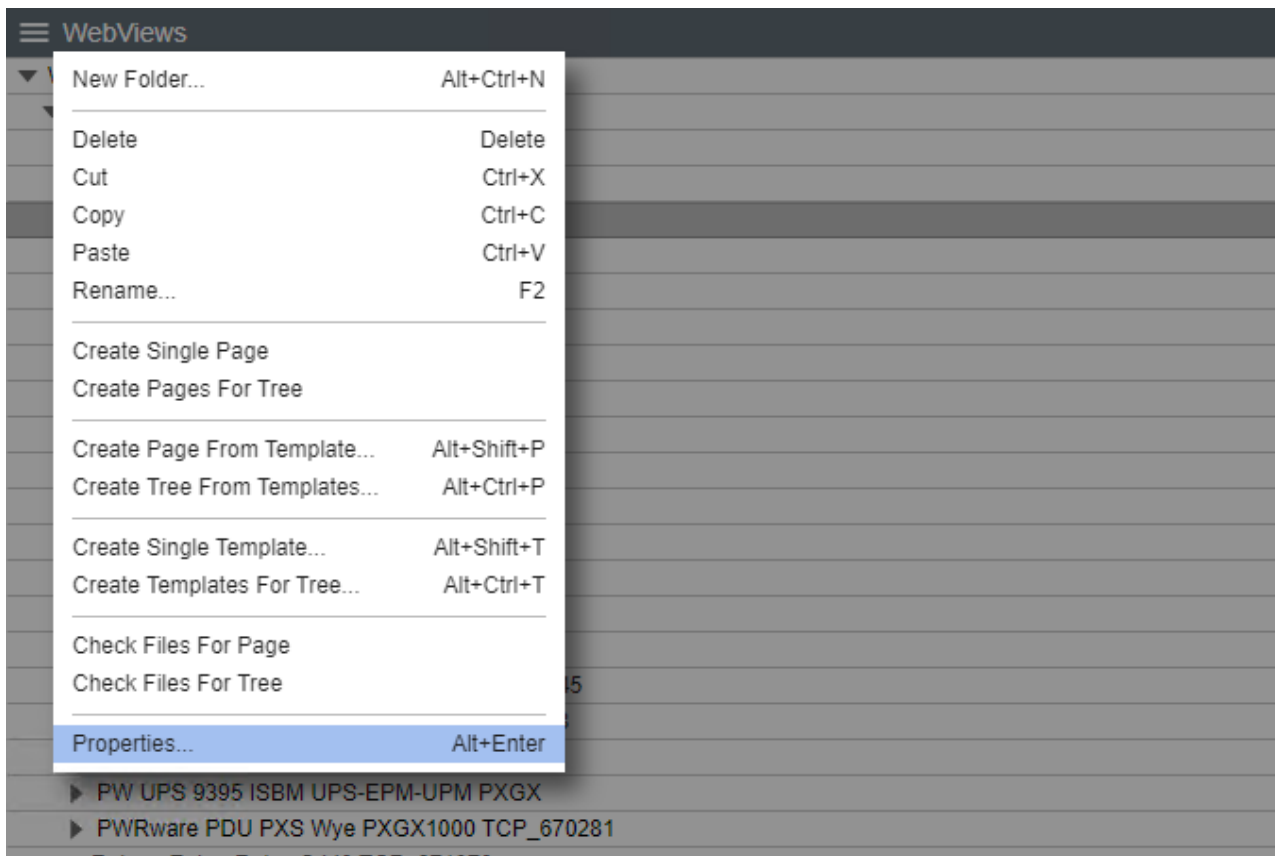
Check Files for Tree

- ✔ This command is for specialized applications, and should only be used at the direction of Eaton technical support.



Properties

The properties command furnishes general information on the WebView folder page.



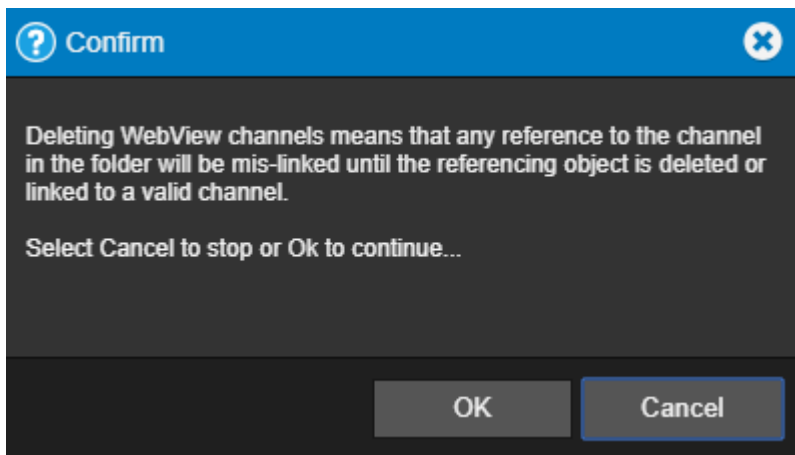
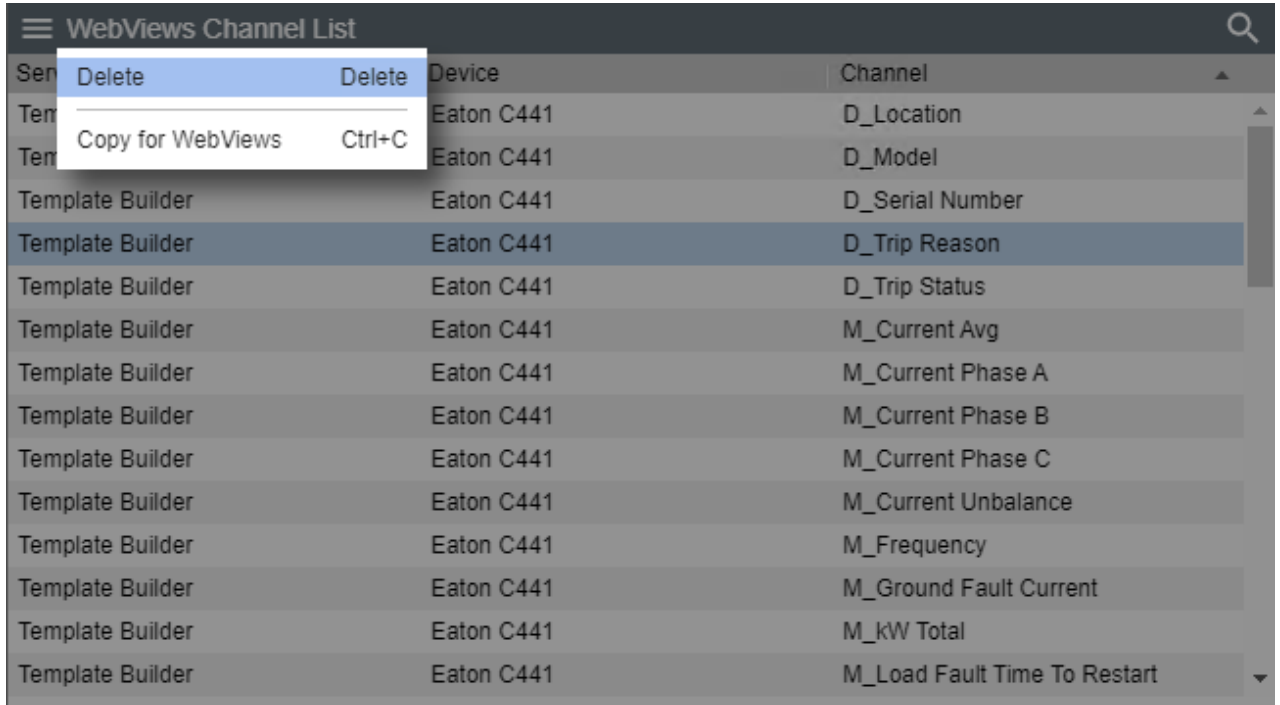
WebViews Channel List Menu

The WebViews Channel List menu provides access to all of the functionality that will be required to manage your Foreseer WebViews Channels.

- Delete
- Copy for WebViews

Delete

Deleting a WebView channel means that any reference to the channel in the folder will be mis-linked until the referencing object is deleted or linked to a valid channel.



Copy for WebViews

The Copy for WebViews command copies the selected channels to the target folder in the WebViews tree.

WebViews Channel List			Device	Channel
Sen	Delete	Delete	Eaton C441	D_Location
Tem	Copy for WebViews	Ctrl+C	Eaton C441	D_Model
Template Builder			Eaton C441	D_Serial Number
Template Builder			Eaton C441	D_Trip Reason
Template Builder			Eaton C441	D_Trip Status
Template Builder			Eaton C441	M_Current Avg
Template Builder			Eaton C441	M_Current Phase A
Template Builder			Eaton C441	M_Current Phase B
Template Builder			Eaton C441	M_Current Phase C
Template Builder			Eaton C441	M_Current Unbalance
Template Builder			Eaton C441	M_Frequency
Template Builder			Eaton C441	M_Ground Fault Current
Template Builder			Eaton C441	M_kW Total
Template Builder			Eaton C441	M_Load Fault Time To Restart

Web Configuration Guide – Foreseer 7.2.210

Publication date 12/2019

Copyright © 2019 by Eaton Corporation. All rights reserved. Specifications contained herein are subject to change without notice.

Foreseer is a registered trademark of Eaton Corporation.

EATON CORPORATION - CONFIDENTIAL AND PROPRIETARY NOTICE TO PERSONS RECEIVING THIS DOCUMENT AND/OR TECHNICAL INFORMATION THIS DOCUMENT, INCLUDING THE DRAWING AND INFORMATION CONTAINED THEREON, IS CONFIDENTIAL AND IS THE EXCLUSIVE PROPERTY OF EATON CORPORATION, AND IS MERELY ON LOAN AND SUBJECT TO RECALL BY EATON AT ANY TIME. BY TAKING POSSESSION OF THIS DOCUMENT, THE RECIPIENT ACKNOWLEDGES AND AGREES THAT THIS DOCUMENT CANNOT BE USED IN ANY MANNER ADVERSE TO THE INTERESTS OF EATON, AND THAT NO PORTION OF THIS DOCUMENT MAY BE COPIED OR OTHERWISE REPRODUCED WITHOUT THE PRIOR WRITTEN CONSENT OF EATON. IN THE CASE OF CONFLICTING CONTRACTUAL PROVISIONS, THIS NOTICE SHALL GOVERN THE STATUS OF THIS DOCUMENT.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation's ("Eaton") experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined

in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser. THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein.