

Foreseer Web Configuration Guide



Table of contents

Foreseer Web Configuration Guide	5
Introduction	5
Welcome	5
Web Configuration Basics	5
Accessing Web Configuration	6
Language Selection Dropdown	7
Alarms	7
Reports	11
Administration	15
Help	15
Breadcrumbs	16
Administration Menu	17
Configuration Backup	17
Scheduled Backup	19
Create All .vi Files	21
Alarm Notification Properties	22
Start Database	24
Stop Database	24
Check Database	25
Fix Database	26
Database Consistency Check	28
SQL Server Properties	30
Scheduled Data Deletion	34
Install Language Pack	36
Install Language Pack Process	37
Version Information	42
Update Translations	43
Download Translations	44
Upload User Defined Translations	45
Restore Translations	49
Local Server List Menu	50
Start Server Configuration	51
End Server Configuration	53
Start New Log File	53
Install Devices From List	55
Update Devices From List	59
User Defined Fields	62
Add Remote	71
Buffered Data Retrieval	75
Copy for WebViews	76
Restart WebViews	77
Restart Server	78
Restart Windows	79
Add Note	80

Get Log File	81
Upload Files	82
Open Older Log File	84
Open Saved Wiretap	87
Properties	89
Remote Server List Menu	90
Connect Remote	91
Disconnect Remote	92
Delete Remote	92
Copy for WebViews	94
Restart Remote App	95
Restart Remote OS	96
Add Note	97
Get Updates	98
Get Log File	101
Upload Files	102
Download Backup	104
Synchronize Redundant	106
Properties	108
Device List Menu	109
Enable	109
Disable	110
Disarm	111
Re-Arm	113
Add User-Defined Channel	115
Delete	118
Rename	120
Copy for WebViews	121
Copy Channel Properties	122
Paste Channel Properties	123
Create .vi File	124
Load Driver	125
Unload Driver	127
Properties	129
Text Control Points	135
Channel List Menu	138
Enable	138
Disable	141
Disarm	143
Re-Arm	145
Delete	147
Rename	147
Copy for WebViews	148
Copy Channel Properties	148
Paste Channel Properties	149
Properties	150
WebViews Menu	154
New Folder	154

Delete	155
Cut	156
Copy	157
Paste	158
Rename	159
Create Single Page / Create Pages for Tree	160
Create Page From Template / Create Tree from Templates	162
Create Single Template / Create Templates for Tree	166
Check Files for Page	168
Check Files for Tree	169
Properties	170
WebViews Channel List Menu	170
Delete	171
Copy for WebViews	171
Copyright	173

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

Welcome to the Foreseer WebConfiguration 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
- Administration
- Help

- Breadcrumbs

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.

Please check the Foreseer Release Notes for supported browser information.

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

<https://machine/WebConf/>.

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 443 (HTTPS) or 80 (HTTP). By default, HTTP is not enabled.

<https://machine/webconf/>

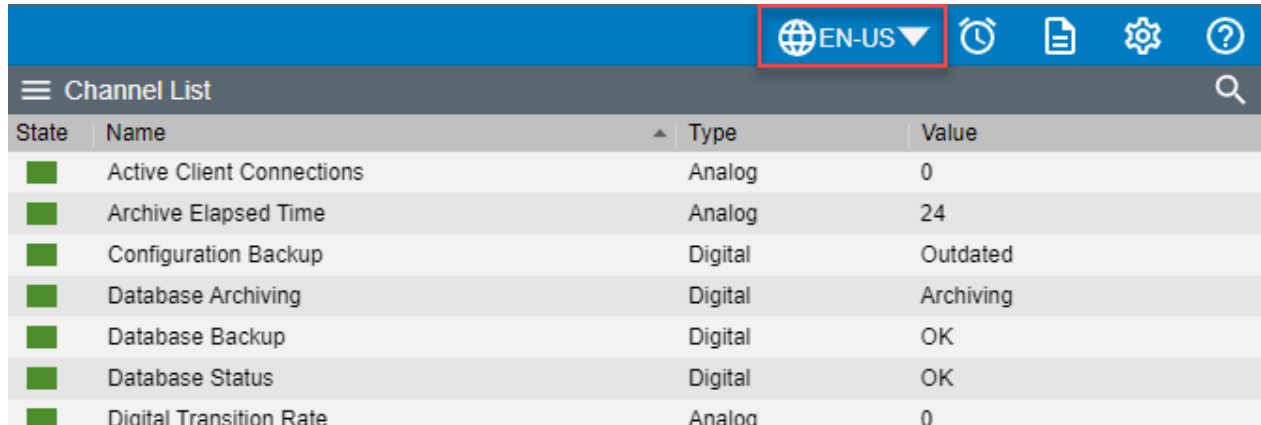
When you access the Web Configuration Utility, you'll see something similar to the following:

The screenshot displays the EATON Foreseers Enterprise Management web interface. The interface is divided into several sections:

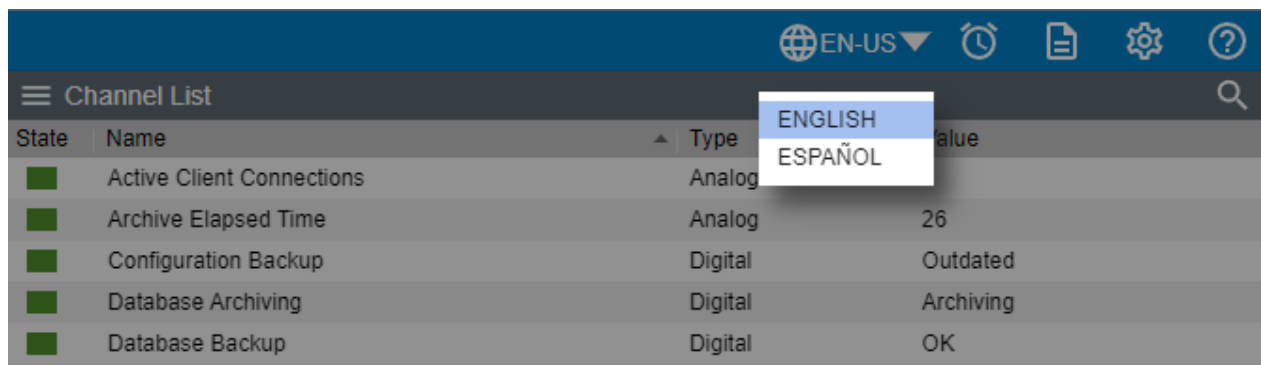
- Server List:** A table showing server status, including a 'Foreseer Remote' which is connected.
- Device List:** A table listing various devices such as ePDU units (1-5), UPS units (9130 1-5), and derived/system channels.
- Channel List:** A table listing monitoring channels like Ambient Temp Status, Input Voltage, Output 1-5, and Output Current.
- WebViews:** A list of available web views for different device types, such as 'Eaton Meter FXM2270 TCP_670846' and 'Eaton Meter FXM5000 Waveform TCP'.
- WebViews Channel List:** A table showing the mapping between servers, devices, and specific channels.

Language Selection Dropdown

Foreseer has the ability to select from multiple languages if the supporting language packs have been installed.



To access the available languages on your Foreseer system, click on the down-arrow to display a list of available languages to you.



Once you select the language of your choice, Foreseer will display all of the interface in that chosen language.

Alarms

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

State	Name	Type	Value
■	Active Client Connections	Analog	0
■	Archive Elapsed Time	Analog	24
■	Configuration Backup	Digital	Outdated
■	Database Archiving	Digital	Archiving
■	Database Backup	Digital	OK
■	Database Status	Digital	OK
■	Digital Transition Rate	Analog	0

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 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
None	Foreseer Remote	UPS 9130 1	M_Ambient Temp	9999	12-04-2019 15:37:46	86.73	86.326	NONE	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
None	Template Builder	PowerXpert Meter8000	M_Current Avrg Demand	9999	12-04-2019 15:40:06	96.73	96.787	NONE	NONE	NONE
Normal	Template Builder	PowerXpert Meter8000	S_Discrete Input 8	9999	12-04-2019 15:40:29	Normal	Normal	NONE	NONE	NONE
None	Template Builder	PowerXpert Meter8000	M_Crest Factor Phase C	9999	12-04-2019 15:39:47	1.43	1.4462	NONE	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.

- Acknowledge - acknowledges a Critical or Cautionary alarm.
- Re-Arm - returns an acknowledged or disarmed object to the Normal state.
- Ack & Rearm - performs an Acknowledge and Rearm in one operation.
- Enable - returns a disabled object to the Normal state.
- Open in WebViews - navigates you to the WebViews screen containing 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
✕

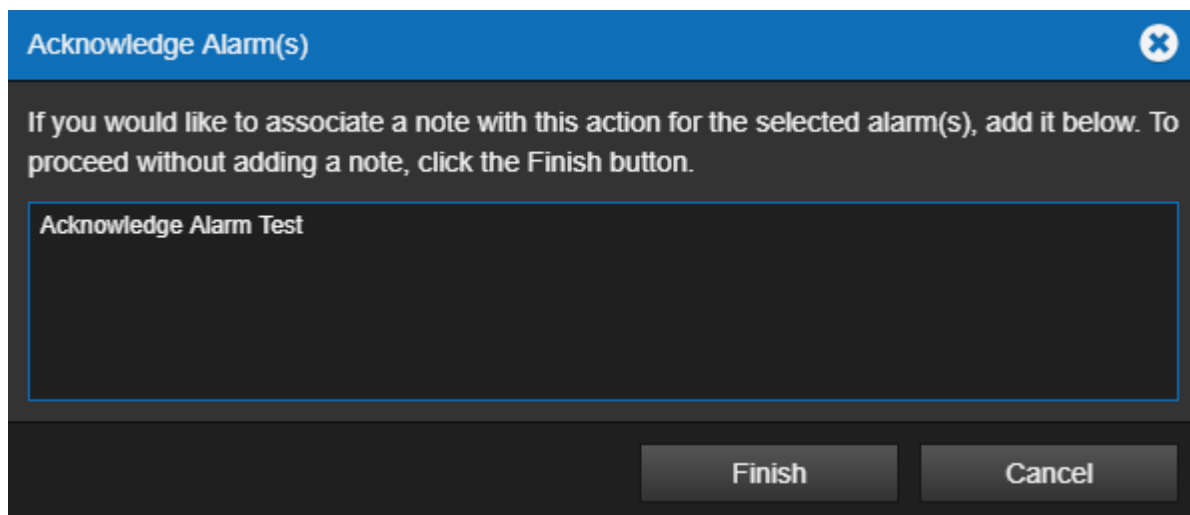
Acknowledge
Re-Arm
Ack & Rearm
Enable
Open in WebViews

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 acknowledged 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.

State	Name	Type	Value
■	Active Client Connections	Analog	0
■	Archive Elapsed Time	Analog	24
■	Configuration Backup	Digital	Outdated
■	Database Archiving	Digital	Archiving
■	Database Backup	Digital	OK
■	Database Status	Digital	OK
■	Digital Transition Rate	Analog	0

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 raw historical data from Foreseer High Resolution

databases in a standard CSV format for any Analog or Derived Analog channel.

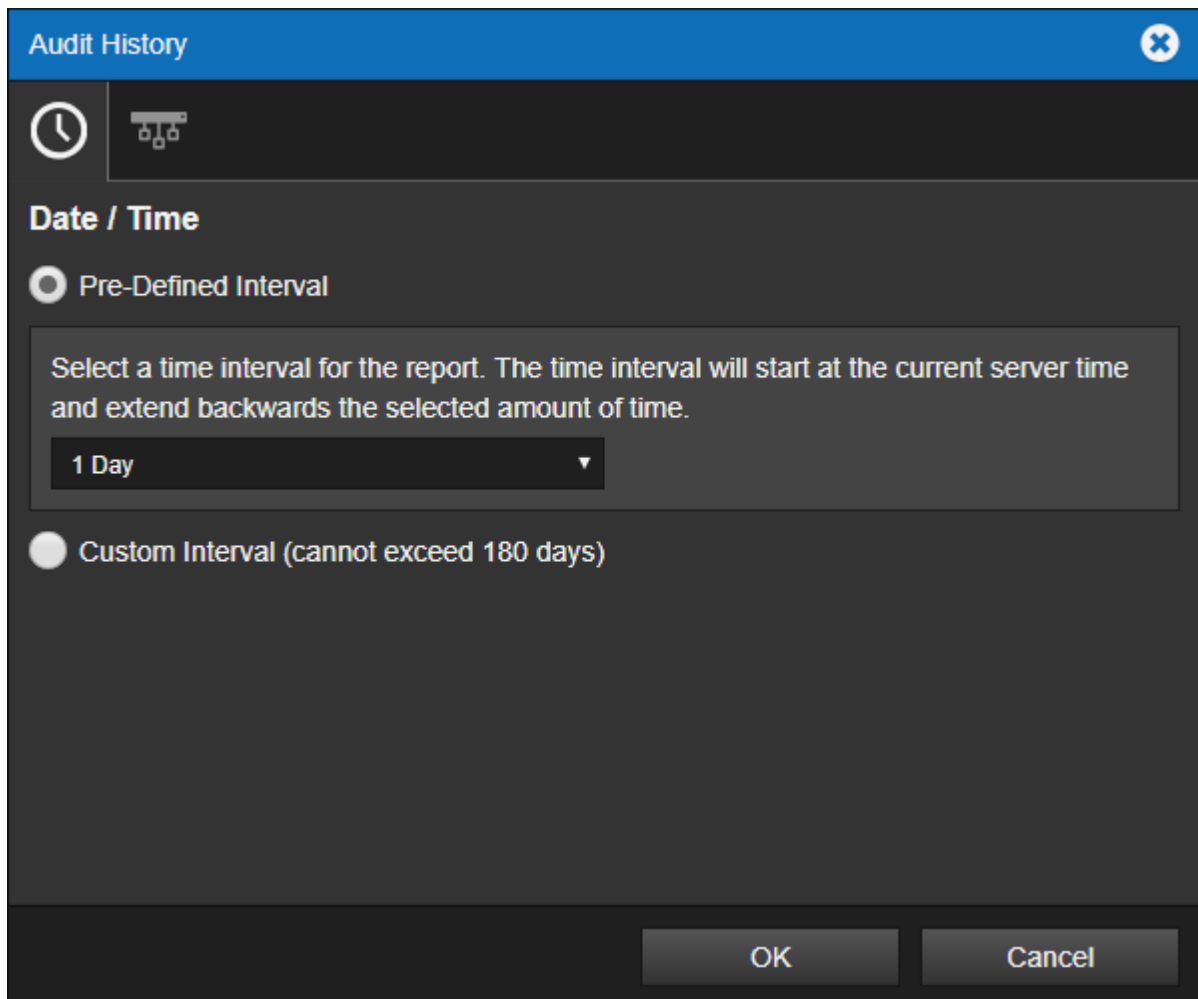
- Log File reports all recorded events since the last Foreseer Server system reset. This report is not available in tabbed format.
- Previous Driver Log File report provides detailed information on the drivers previously in use by the Foreseer system.
- Previous Log File reports all events recorded in 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

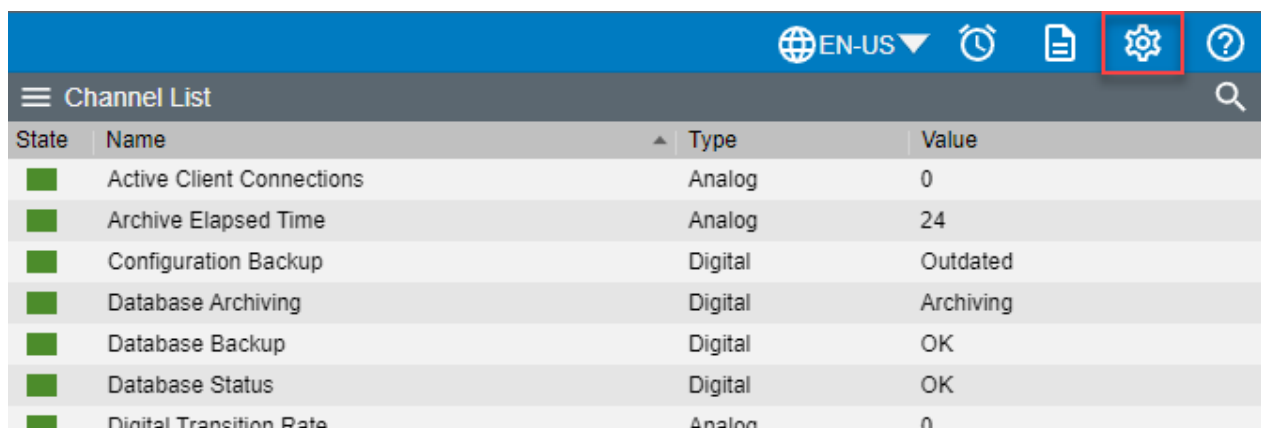
The ability to perform specific text searches on Custom History files can be extremely useful in locating archived information about an event or piece of equipment.

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



State	Name	Type	Value
■	Active Client Connections	Analog	0
■	Archive Elapsed Time	Analog	24
■	Configuration Backup	Digital	Outdated
■	Database Archiving	Digital	Archiving
■	Database Backup	Digital	OK
■	Database Status	Digital	OK
■	Digital Transition Rate	Analog	0

Help

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

State	Name	Type	Value
■	Active Client Connections	Analog	0
■	Archive Elapsed Time	Analog	24
■	Configuration Backup	Digital	Outdated
■	Database Archiving	Digital	Archiving
■	Database Backup	Digital	OK
■	Database Status	Digital	OK
■	Digital Transition Rate	Analog	0

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.

WebViews	
▼	WebViews
▼	CSA1
	C-H Digitrip 1150 PXG Eff32 TCP_671356
	Cat GenSet EMCP4-3 Ctr TCP_670984
	E Relay C441 Motor PXG Eff32 TCP_671416
	Eaton ATS ATC-900_661251 NO WIPER
	Eaton ATS ATC-900_661251 WIPER
	Eaton Meter PXM2250 TCP_670772
	Eaton Meter PXM2270 TCP_670646
▶	Eaton Meter PXM4000 Waveform TCP
▶	Eaton Meter PXM6000 Waveform TCP
▼	Eaton Meter PXM8000 Waveform TCP
	Waveform
▶	Eaton Meter PXMP 3PH TCP_671192
▶	Eaton Relay EDR-5000 TCP_671037
	Eaton Trip MCCB PXR25 TCP_671411

If an operator had navigated to the GENERATOR 1 page, the Breadcrumb would look like this:

WEBVIEWS > CSA1 > EATON METER PXM8000 WAVEFORM TCP > WAVEFORM
EATON METER PXM8000 WAVEFORM TCP

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
- Alarm Notification Properties
- Start Database
- Stop Database
- Check Database
- Fix Database
- Database Consistency Check
- SQL Server Properties
- Scheduled Data Deletion

Configuration Backup

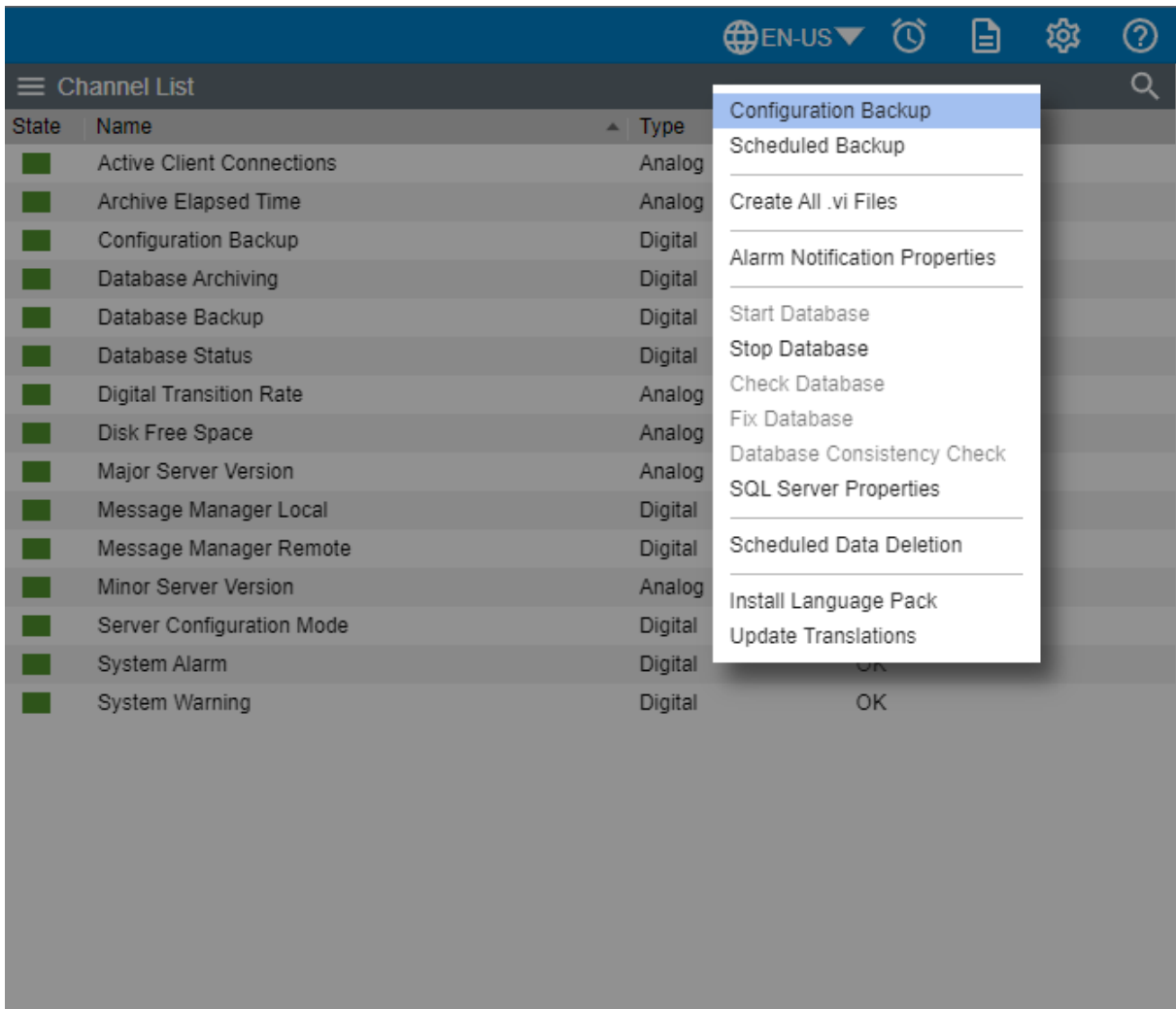
- ✔ It is strongly recommended that a backup be performed after initial system configuration as well as before and after any significant modifications to ensure maximum disaster recovery capability. You must end server configuration mode before backing up the server configuration.

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

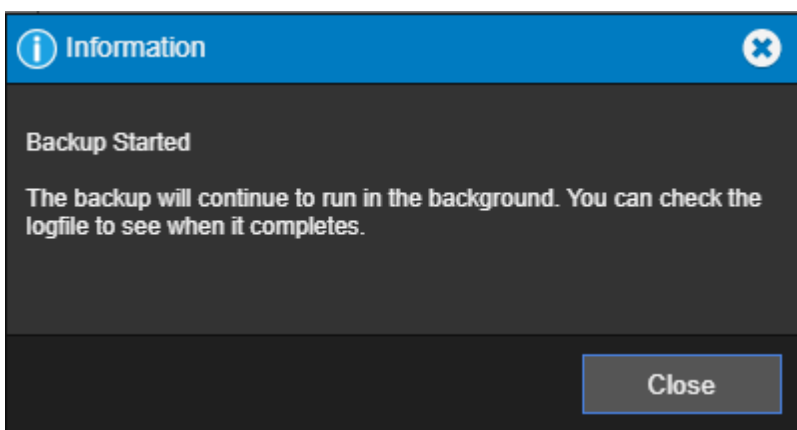
The backup archive (.ARQ) file includes the Foreseer Server configuration only, data files are not backed up in this procedure. Automatic configuration backups can be scheduled through the standalone Foreseer Configuration utility. Backups made through the Web Configuration Utility are automatically 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.



- As the dialog states, the backup will continue to run in the background. Once the backup completed, you can find the backup file in the \Restore\ directory of the Foreseer installation (typically C:\Eaton Corporation\Foreseer).

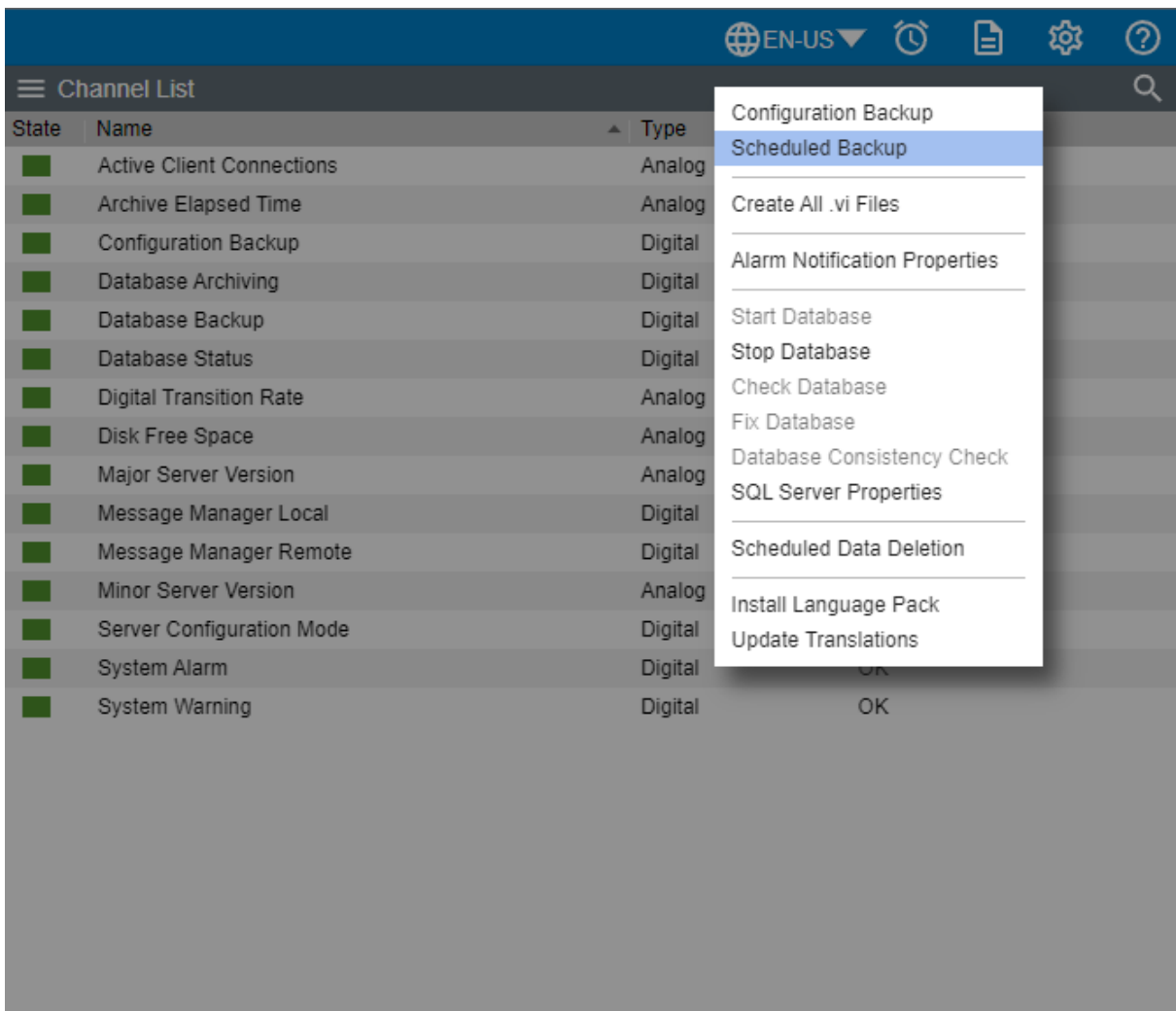
Scheduled Backup

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:

OK Cancel

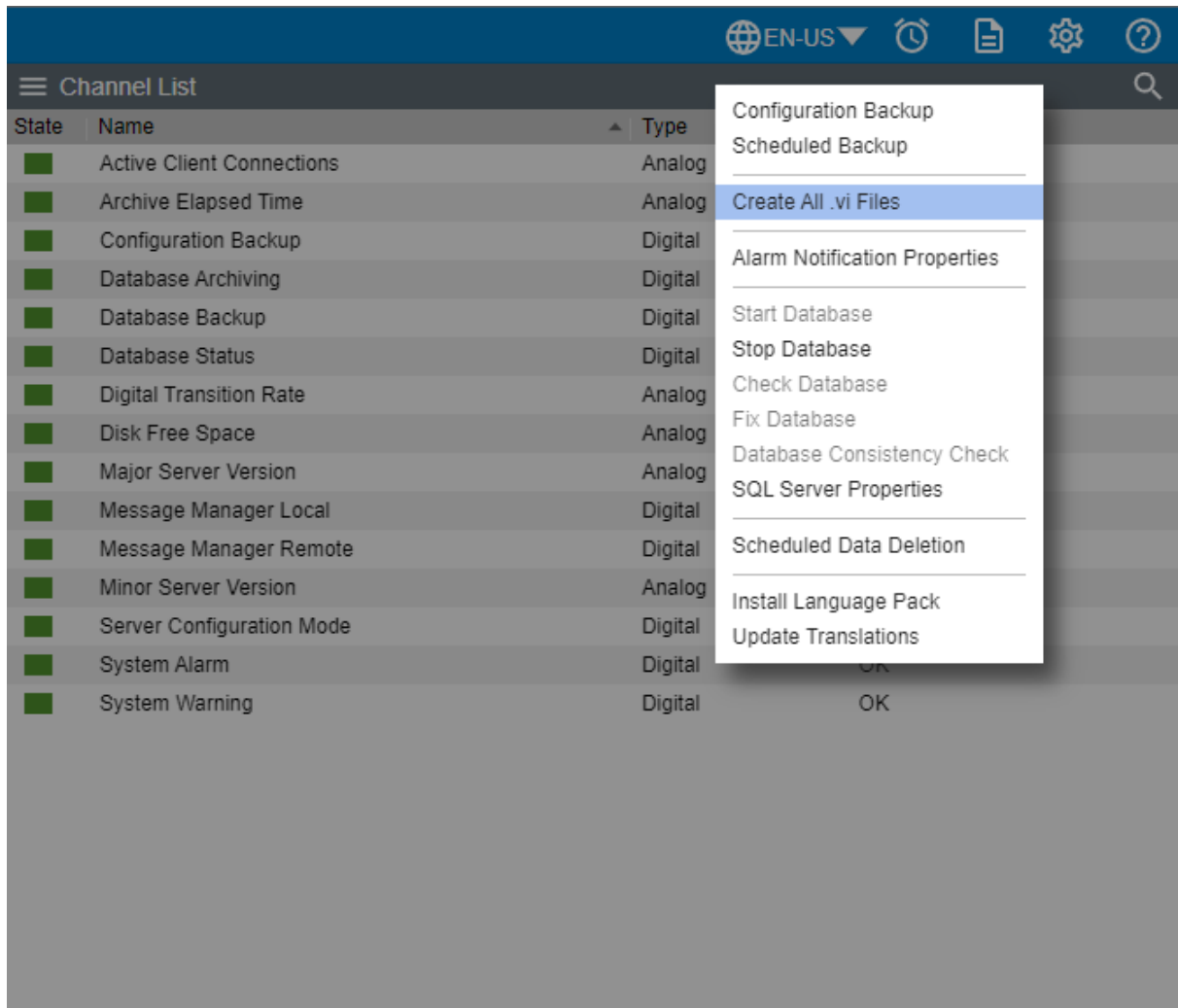
3. Specify when the backup is to be performed.
 1. The Start Time is based on a 24- hour clock: for example, 5:00 p.m. is entered as "17:00." Note that the backup cannot occur within ten minutes of midnight and that there are restrictions based on the type of backup media. The Start Time plus the duration 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

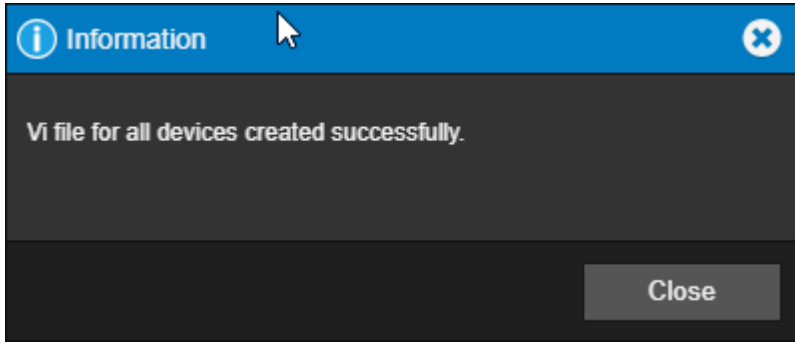
You can initiate the command to create all the .vi files for your configuration.

To Create All .vi files:

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

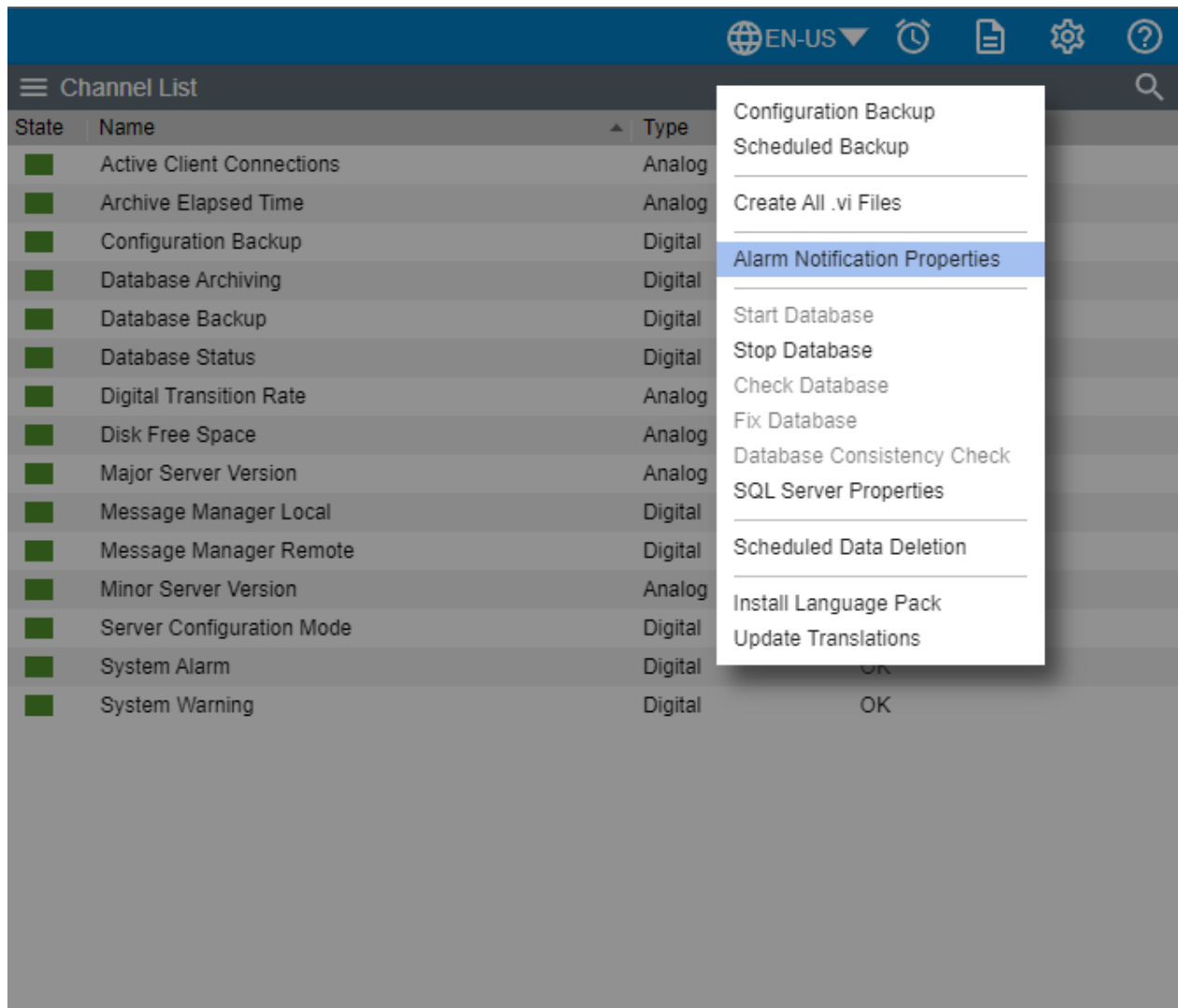


2. All of the defined .vi files in your system will be generated and named with the word Create added in the filename.
3. Upon successful completion, you will get the following dialog



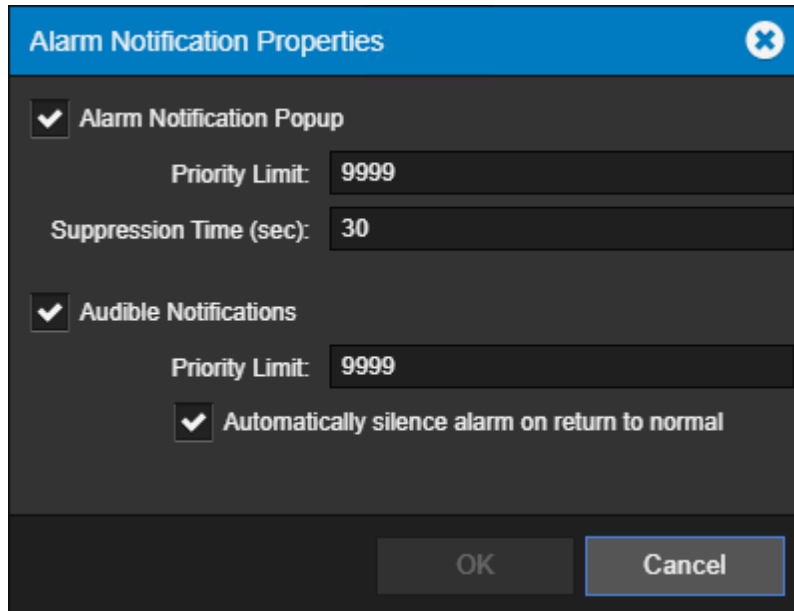
Alarm Notification Properties

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.



The screenshot shows a dialog box titled "Alarm Notification Properties". It has a blue header bar with a close button. The dialog is divided into two main sections. The first section, "Alarm Notification Popup", has a checked checkbox and two input fields: "Priority Limit" set to "9999" and "Suppression Time (sec)" set to "30". The second section, "Audible Notifications", also has a checked checkbox, a "Priority Limit" field set to "9999", and a checked checkbox labeled "Automatically silence alarm on return to normal". At the bottom of the dialog are "OK" and "Cancel" buttons.

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*.

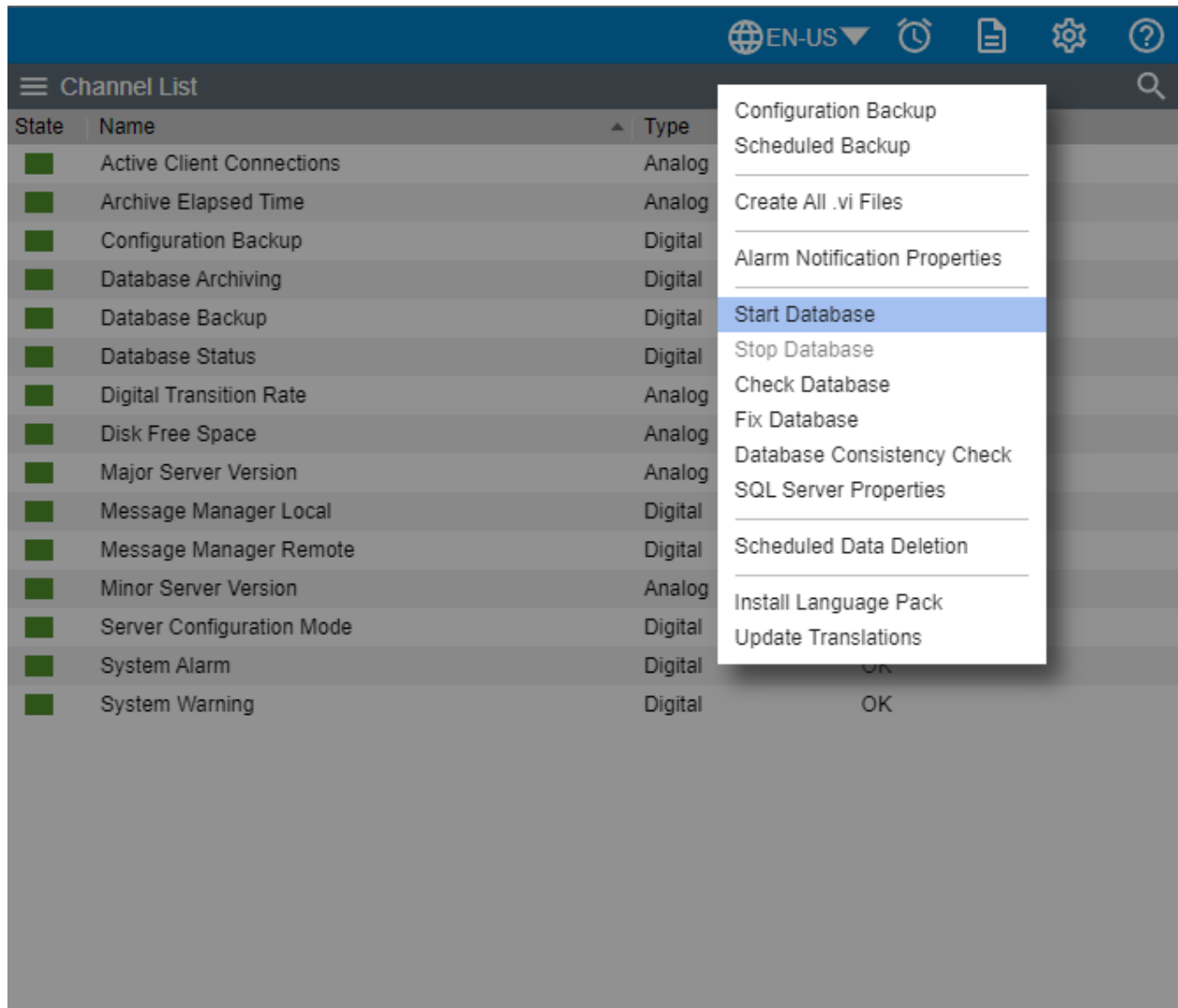
As you consider the potential to use custom sounds for different alarm priorities, make reasonable decisions on the length and content of files. For example:

- 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.

Start Database

✔ Administrative authorization is required before proceeding with this command.

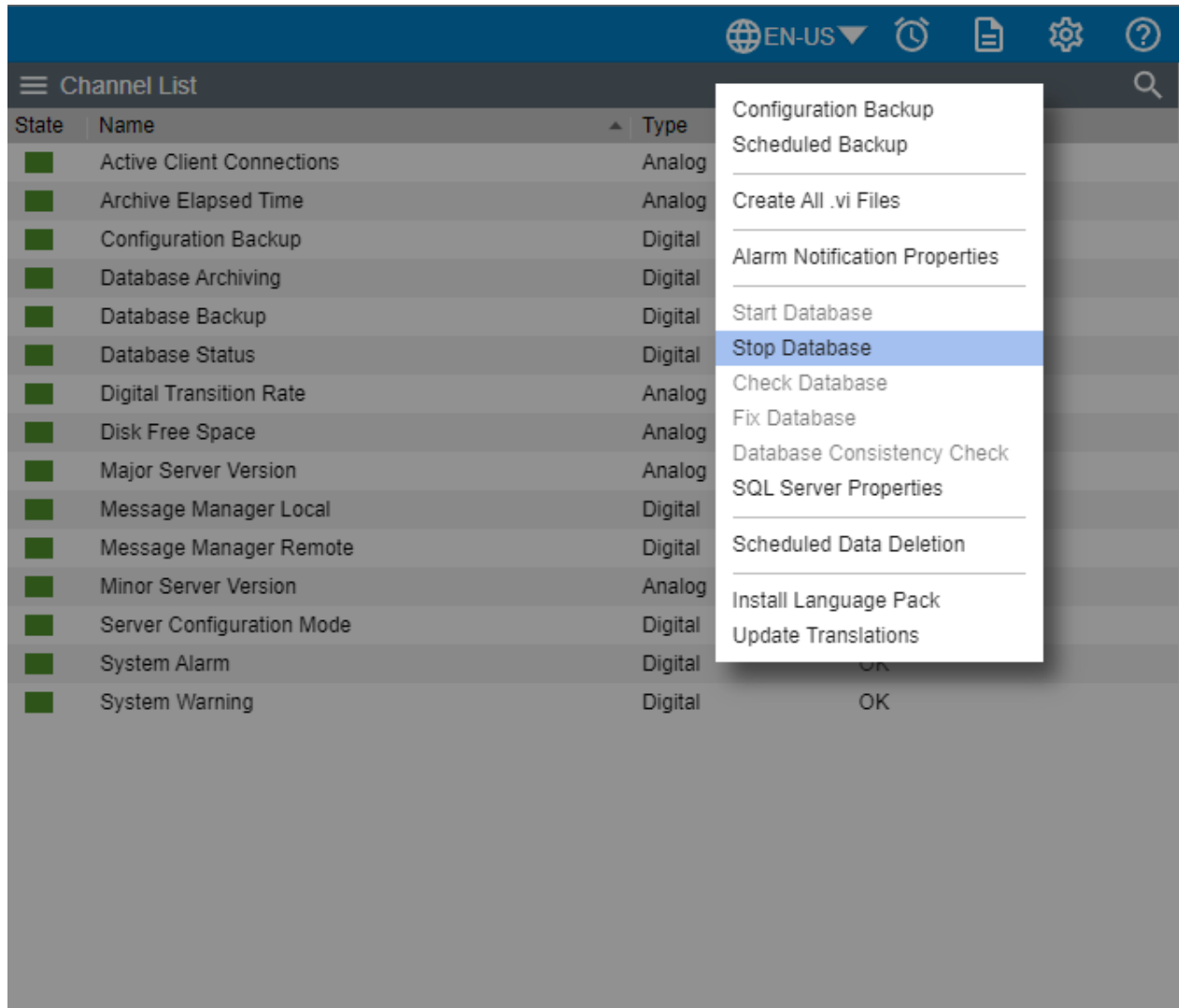
Starts the Foreseer databases in SQL Server. You must stop the databases prior to running checking or fixing the databases.



Stop Database

✔ Administrative authorization is required before proceeding with this command.

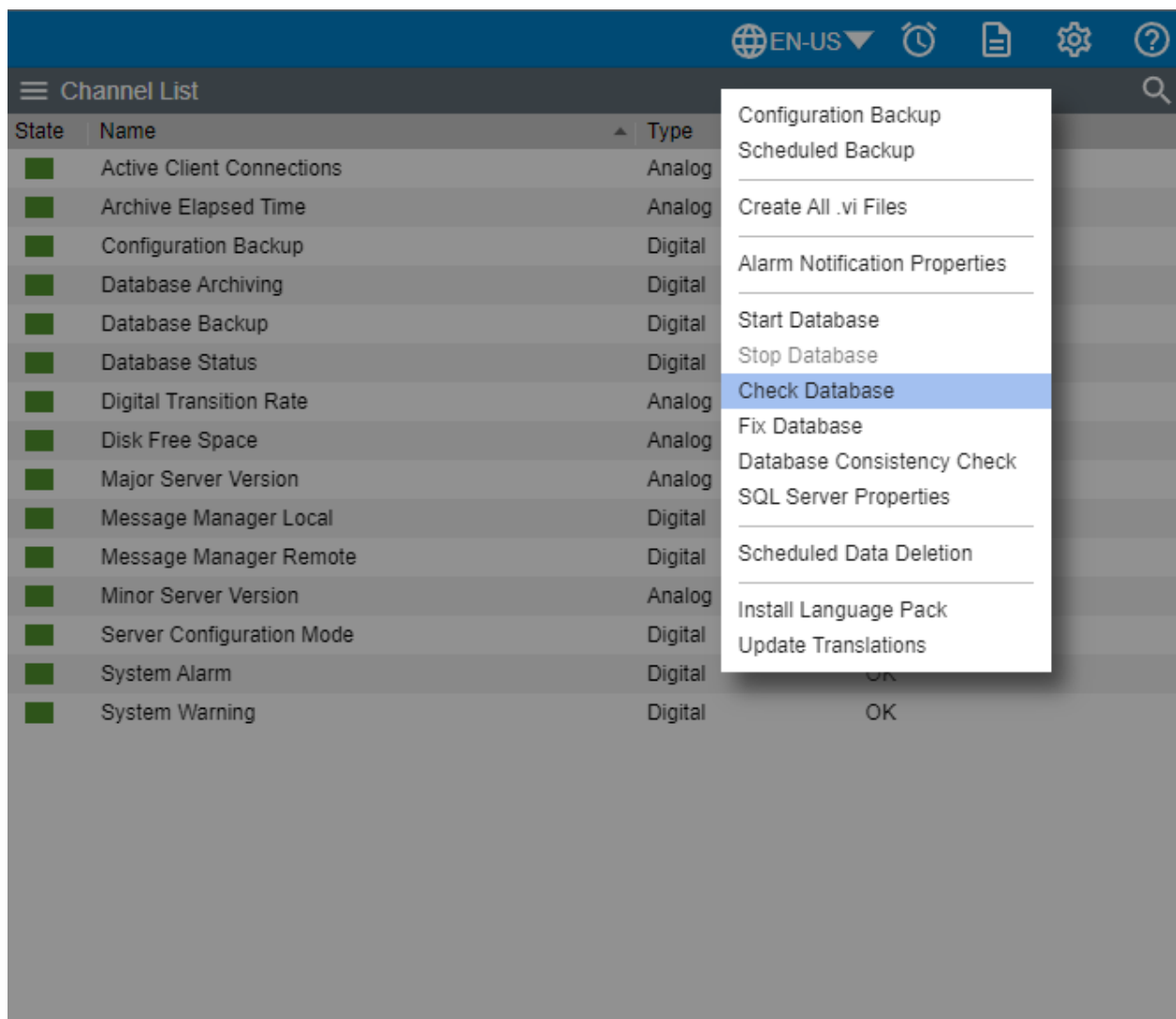
Stops the Foreseer databases in SQL Server. You must stop the databases prior to running checking or fixing the databases.



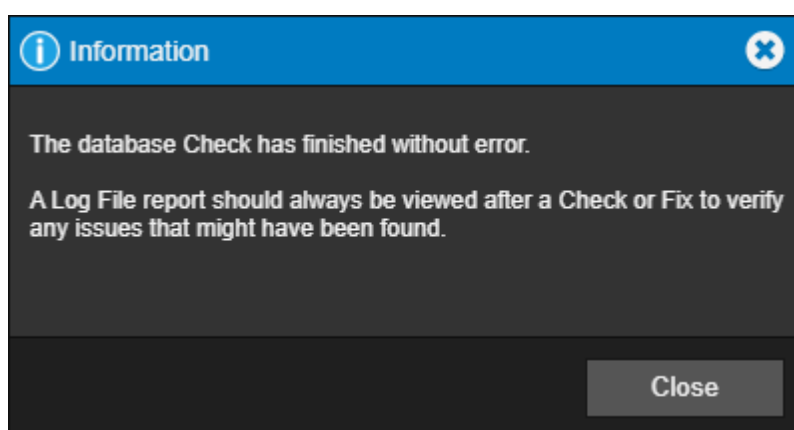
Check Database

✔ Administrative authorization is required before proceeding with this command.

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.

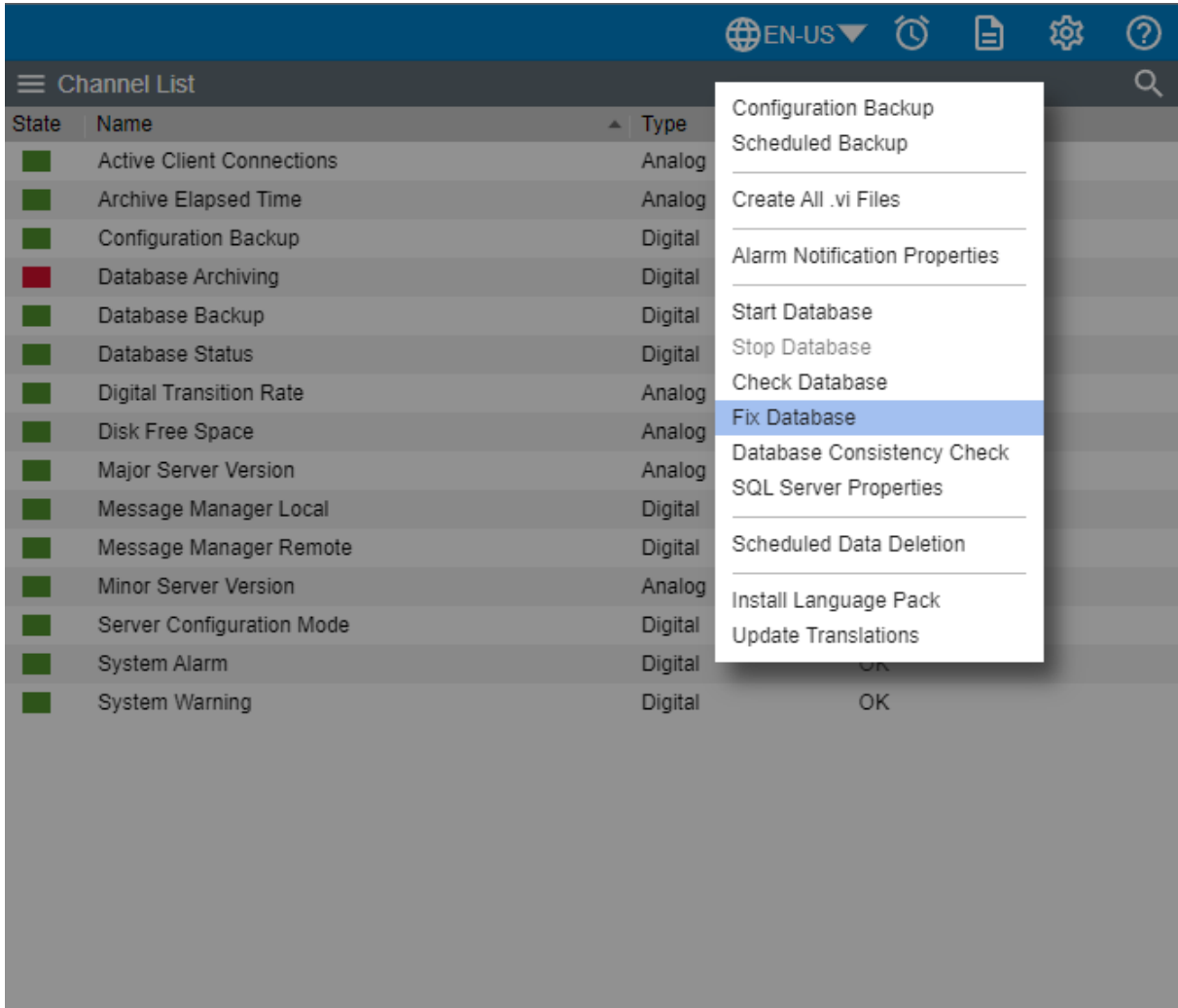


Fix Database

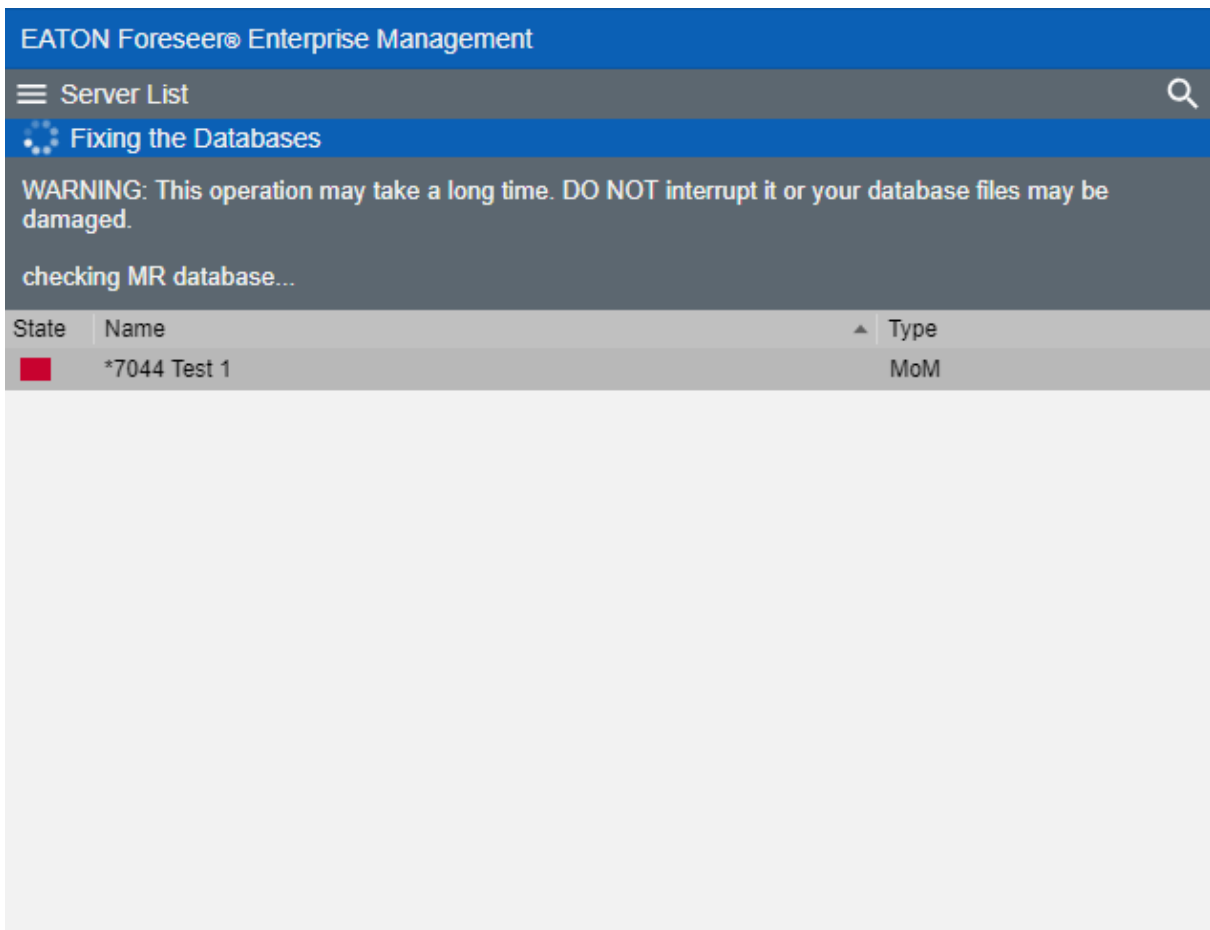
- ✔ Administrative authorization is required before proceeding with this command.

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.

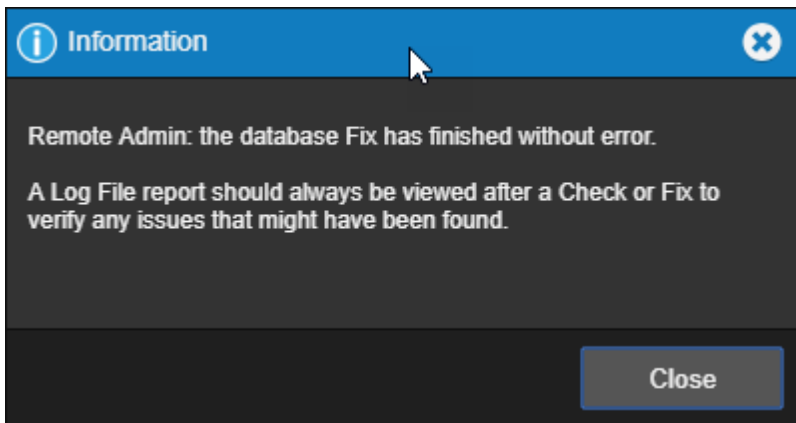
1. Select Fix Database from the Administration Menu



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.

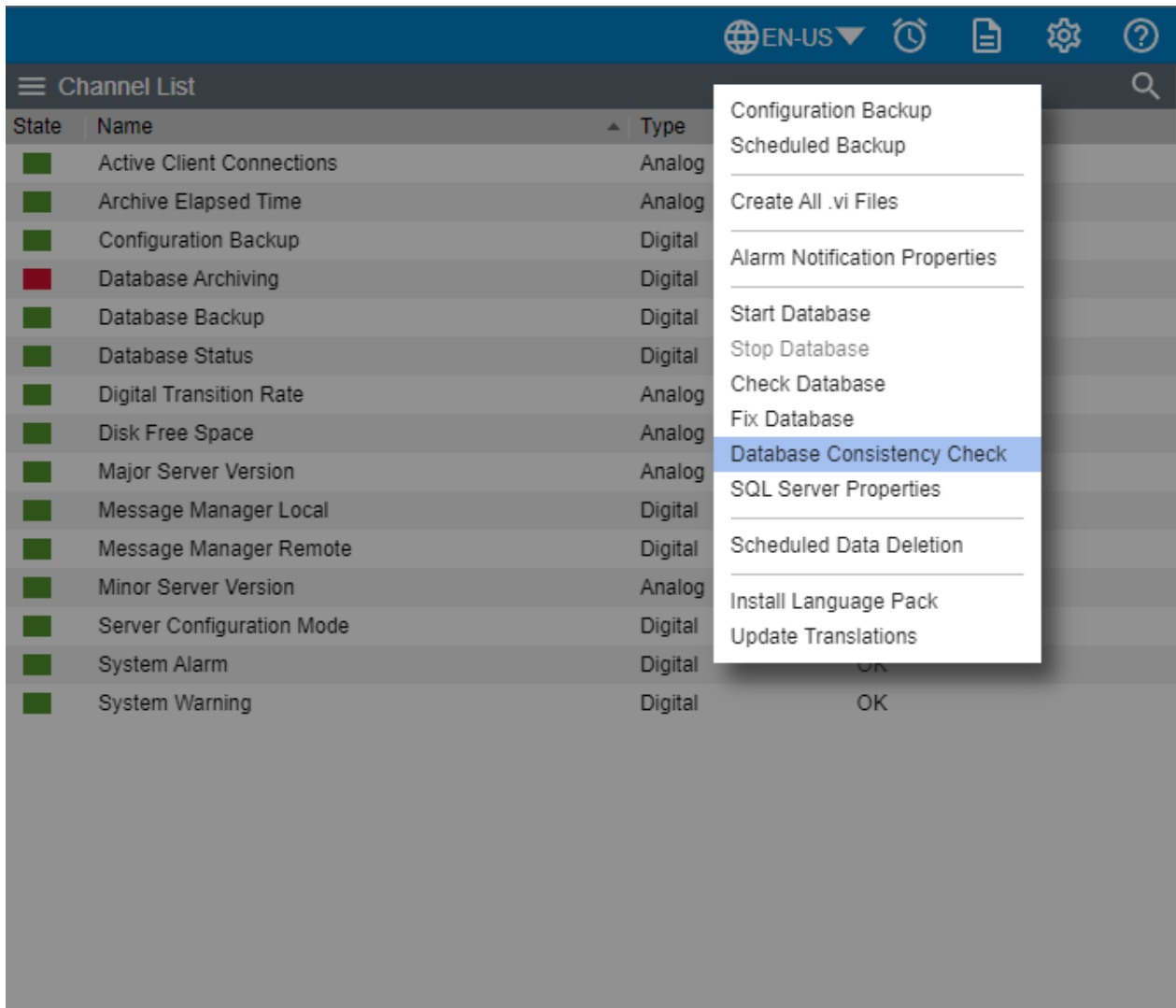


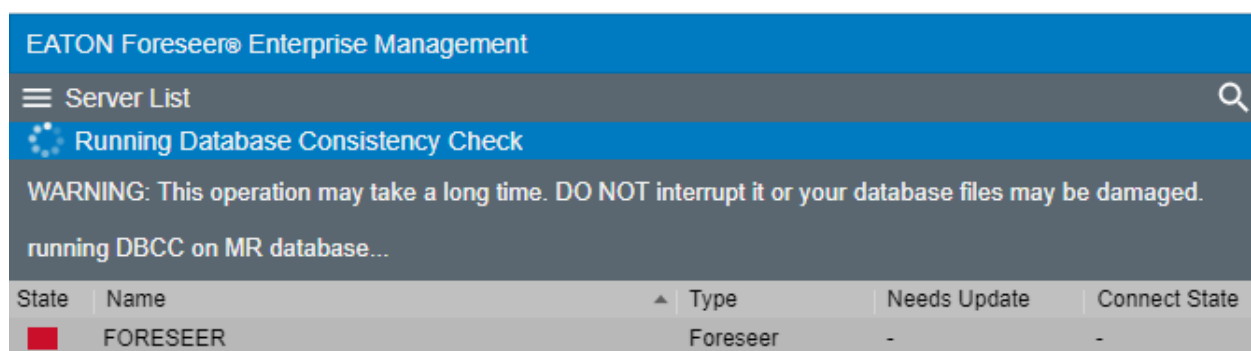
Database Consistency Check

- ✔ In order to successfully run a Database Consistency Check, the Windows service account or SQL user account used by Foreseer must contain public and db_backupOperator mapped access to the master database in order for use this command. Consult your Database Administrator for further support.

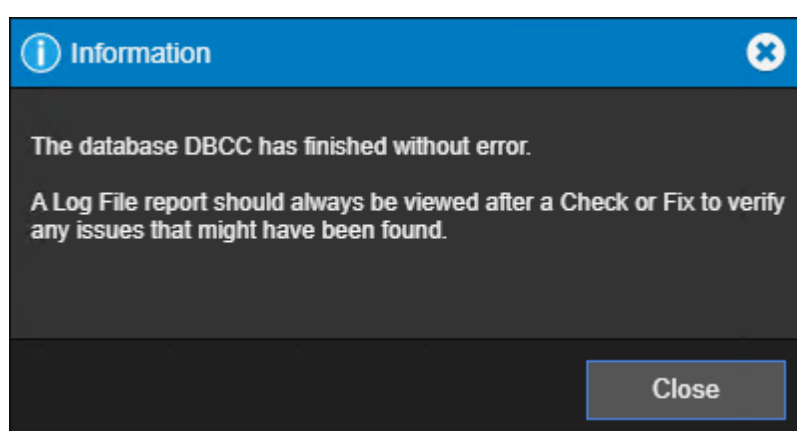
The Database Consistency Check feature is used to perform a low-level check of all active Foreseer historical databases. In prior versions, the Database Consistency Check ran anytime a Fix Database command was executed. Many times, Database Consistency Check was not necessary and could significantly increase the amount of time necessary to run Fix Database.

Beginning with Foreseer v7.3, the Database Consistency Check feature has been split from Fix Database and can be ran separately.





When you execute the Database Consistency Check (DBCC) command, the Database Engine creates a database snapshot and brings it to a transactionally consistent state. The DBCC command then runs the checks against this snapshot. After the DBCC command is completed, this snapshot is dropped.



DBCC checks the logical and physical integrity of all the objects in the specified database by performing the following operations:

- Runs DBCC CHECKALLOC on the database.
- Runs DBCC CHECKTABLE on every table and view in the database.
- Runs DBCC CHECKCATALOG on the database.
- Validates the contents of every indexed view in the database.
- Validates link-level consistency between table metadata and file system directories and files when storing VARBINARY (max) data in the file system using FILESTREAM.
- Validates the Service Broker data in the database.
- This means that the DBCC CHECKALLOC, DBCC CHECKTABLE, or DBCC CHECKCATALOG commands do not have to be run separately from DBCC CHECKDB. For more detailed information about the checks that these commands perform, see the descriptions of these commands.

SQL Server Properties

- ✓ The Windows service account of SQL user leveraged by Foreseer must be assigned the following SQL Server roles:

- public
- bulkadmin
- dbcreator

In addition to the above roles, there are times when a Database Consistency Check may need to be executed. In order to run DBCC, the account must also contain the following user mapping to the master db:

- public
- dbbackupoperator

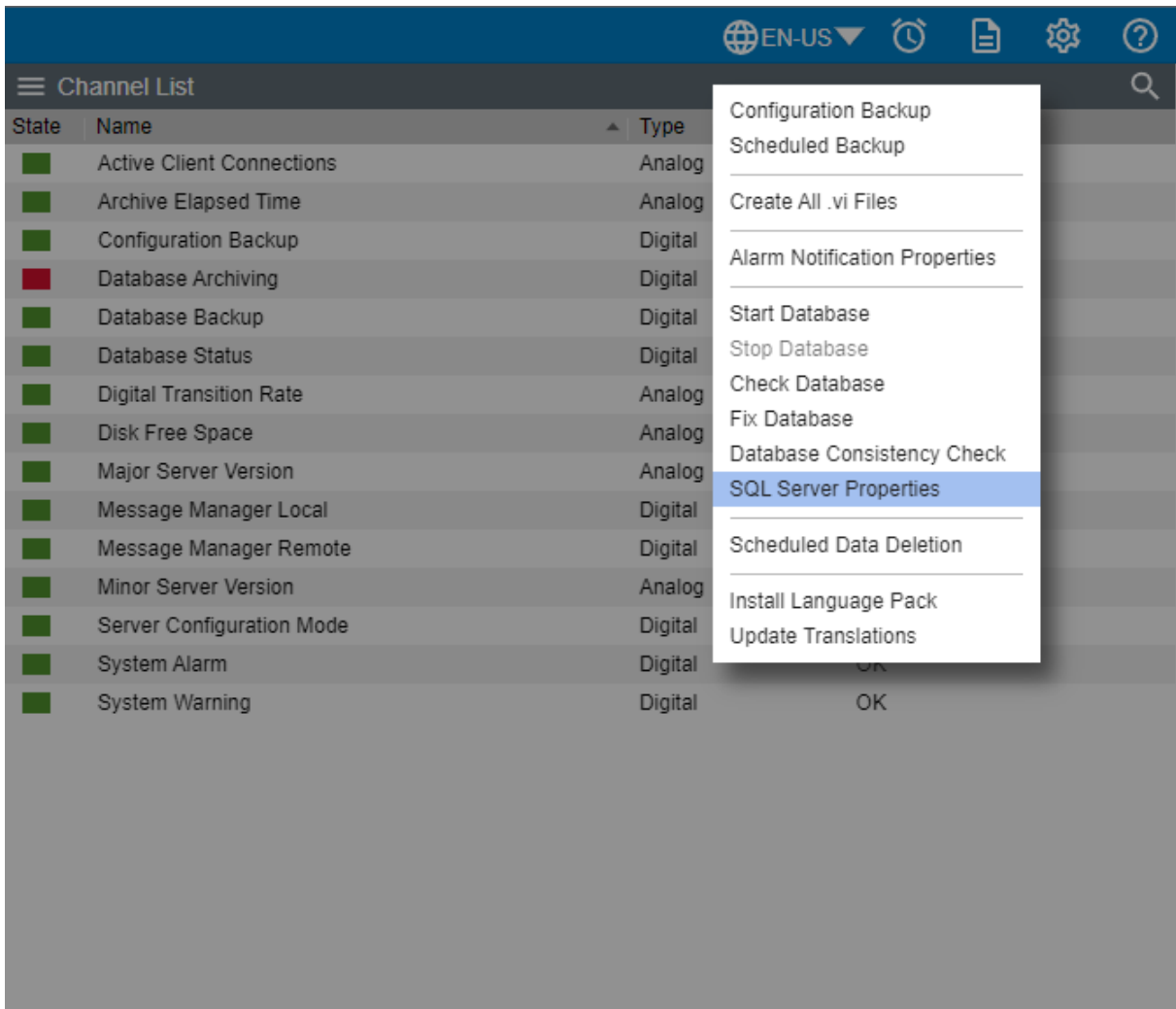
Contact your Database Administrator for assistance with provisioning of these entitlements to the account used by Foreseer.

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).

After selecting the Ok button, the informational dialog will appear

Information ✕

Changes to the SQL Server properties will not take effect until the server is restarted.

Selecting the 'Temporarily disable the connection retry' checkbox does not require a server restart.

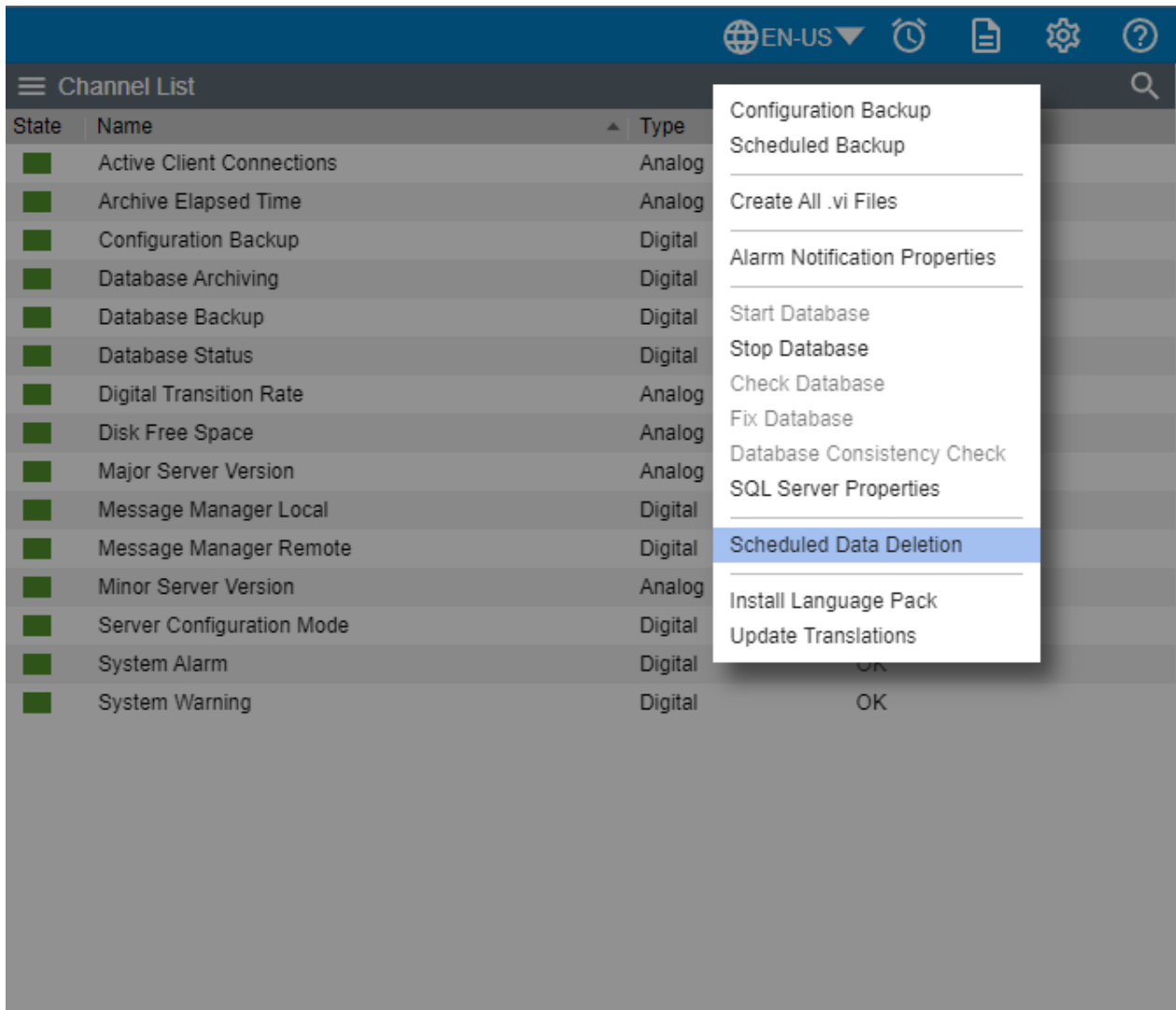
Scheduled Data Deletion

✔ Administrative authorization is required before proceeding with this command.

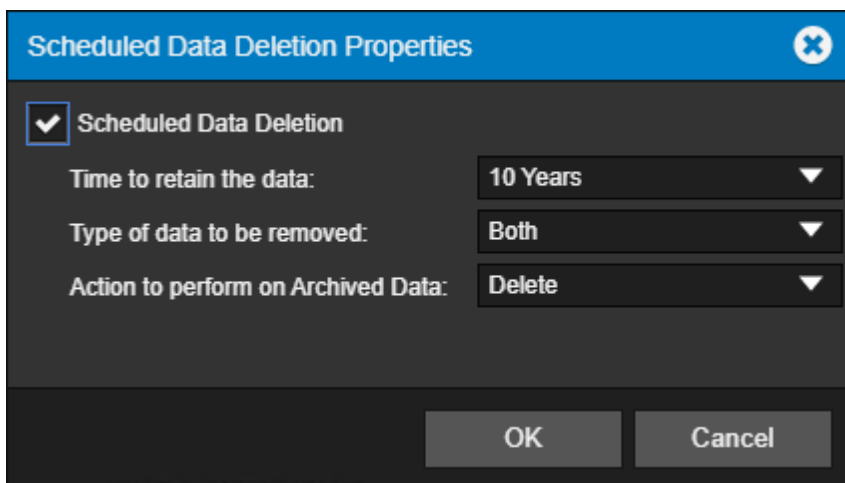
Use this dialog to control the scheduling and processing of managing your database files.

The scheduled data deletion function will process the appropriate SQL scripts to either completely remove the appropriate HR databases, MR databases, TR databases, and Async databases, or to just detach the databases but leave the files intact based on user-configured settings.

- Scripts will run on the 1st of January and July after the regular monthly database maintenance has completed and the system is actively archiving in the current month. The database files will be deleted or detached (based on configuration) over the last six months all together so that there is consistency among all the remaining databases.
- If a cycle is skipped due to the server being down, then the scripts will not run for the skipped period. The scripts will run during the next scheduled period.
- Deletions will be for entire databases only and not individual records in any database
- You can schedule deleting Waveform capture files at user-definable intervals.
 - Waveform file deletion will process on the 1st of January and July. Waveform file deletion will run irrespective of whether the database is in archiving state or not.
 - Process will run the necessary scripts to remove the appropriate .WFC files in the <Foreseer>/Captures folder.
 - Waveform deletion applies to both Foreseer Server and Foreseer Outpost
 - The Modified Date of the file will be used to determine if a file is to be deleted or retained.



The dialog will only be available to users with the appropriate administrative access in WebConfig. Dialog will include a checkbox for the user to enable/disable the feature. When the feature is disabled, all other user-configurable properties in the dialog will be unavailable for user input and “grayed out”. The default setting will be Disabled.



Time to retain the data:

- A drop-down for selecting the length of time that data is to be retained.
- Selections will be in ½ year increments starting at 1 year and ending at 10 years (1, 1.5, 2, 2.5, 3, 3.5, etc.).
- Default setting will be 10 years.

Type of data to be removed:

- A drop-down for selecting what type of data is to be removed.
- Selections will be Archived Data, Waveform Captures, and Both on Foreseer Server and only Waveform Captures on Foreseer Outpost.
 - Default setting will be Both for Foreseer Server and Waveform Captures for Foreseer Outpost.
- On Foreseer Server, if Archived Data or Both is selected, an additional drop-down property will become active to select what action to take on the databases.

Action to perform on Archived Data:

- Selections will be Delete and Detach Only
- Default will be Delete.
- This additional property will not be displayed in Foreseer Outpost.

When the necessary scripts have completed, appropriate messages will be entered into the Foreseer Log File to log the status of the data deletion routine. When scripts successfully complete, the message will indicate success of the routine and provide the number of files removed/detached.

If any of the scripts fails to run successfully, a System Warning alarm will be generated and the message in the log file will provide as much detail as possible as to why the routine was unsuccessful (unable to connect to SQL Server, sharing violation on WFC file, etc.). The Waveform Capture scripts will be considered successful if the Captures folder does not exist (no waveform devices are monitored) or no files meet the criteria for deletion.

Separate success/failure messages will be logged for the Database scripts and for the Waveform scripts.

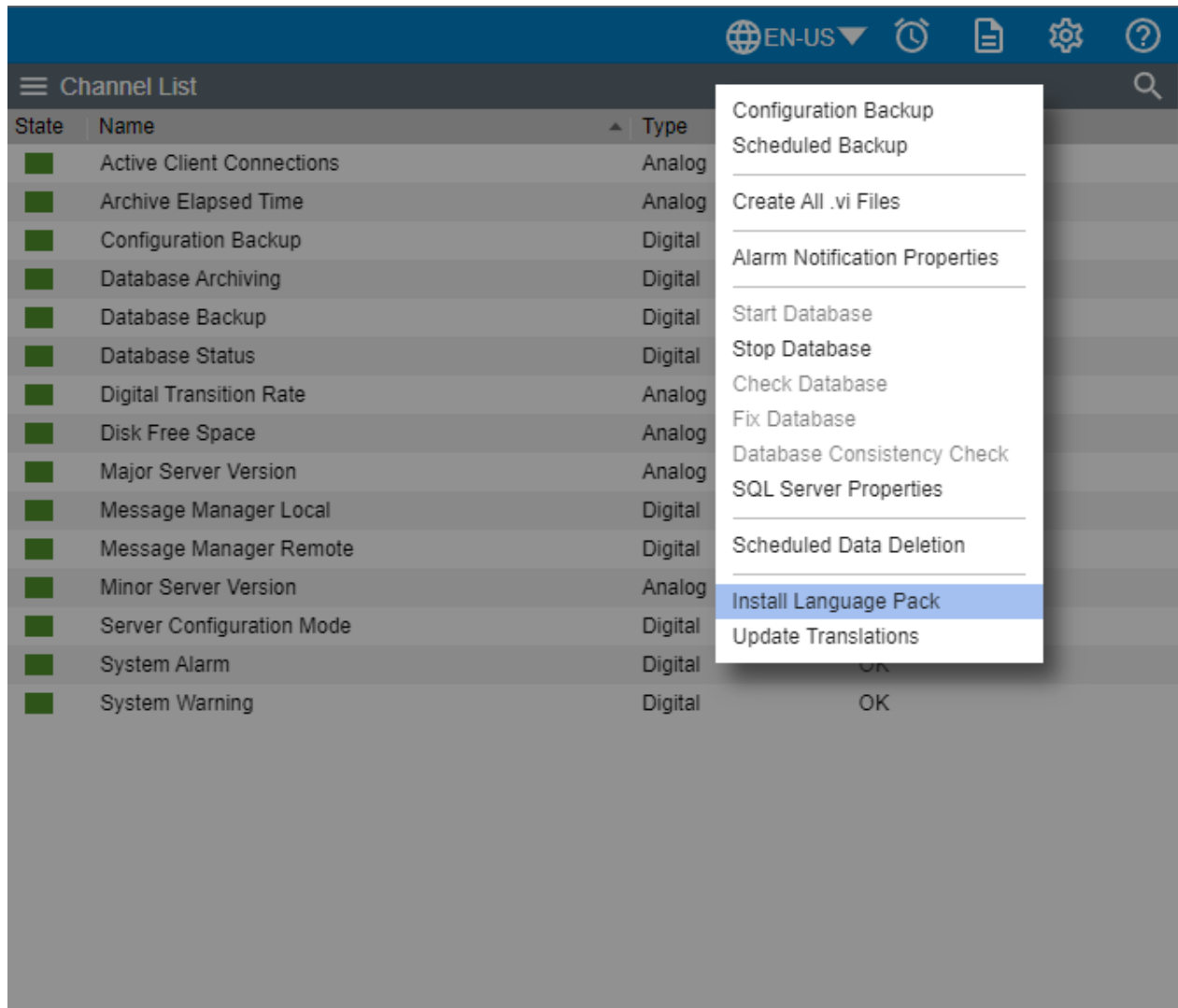
- ✓ In a Primary/Redundant server architecture, any changes made to the Scheduled Data Deletion configuration in the primary server will update the "Needs Update" column to "Needs Sync". The Scheduled Data Deletion configuration of the secondary server will be synced with that of the Primary server after a Sync operation is performed.

Install Language Pack

- ✓ Administrative authorization is required before proceeding with this command.

The Install Language Pack functionality allows you to install a new language to the Foreseer system and provide internationalization functionality to the Foreseer web environment.

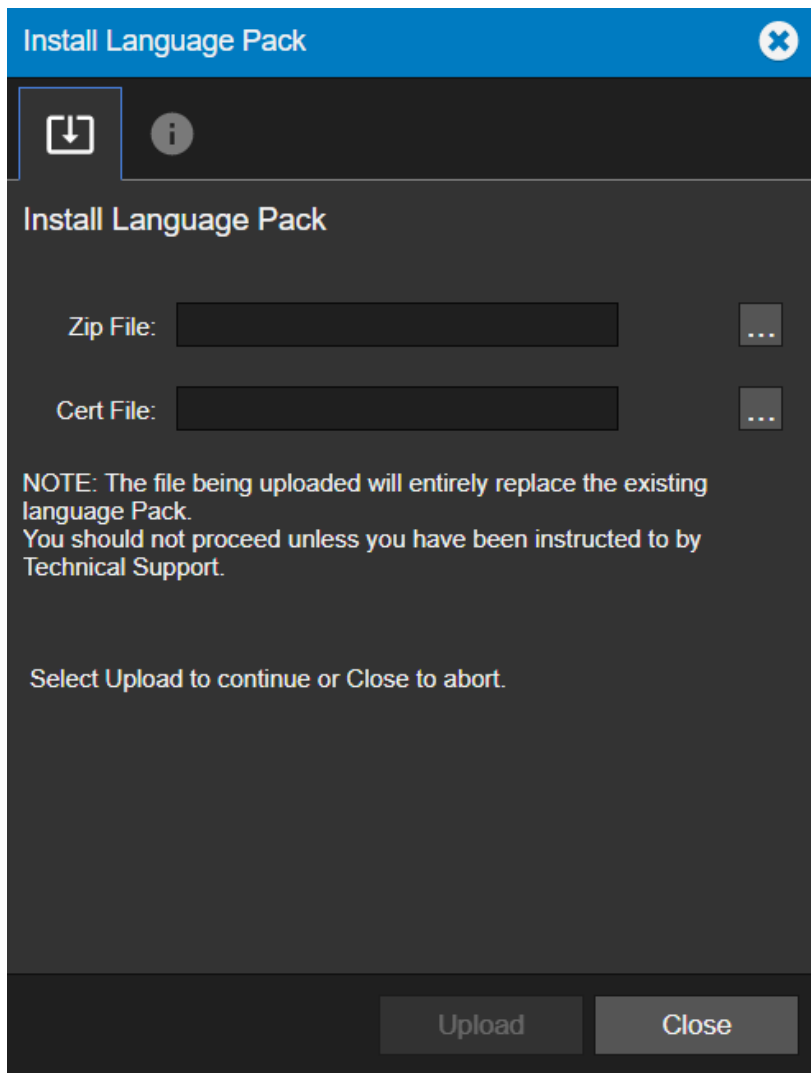
- By installing the language pack to the Foreseer environment, this will allow the use to switch between multiple languages during run-time, without having to restart the application.



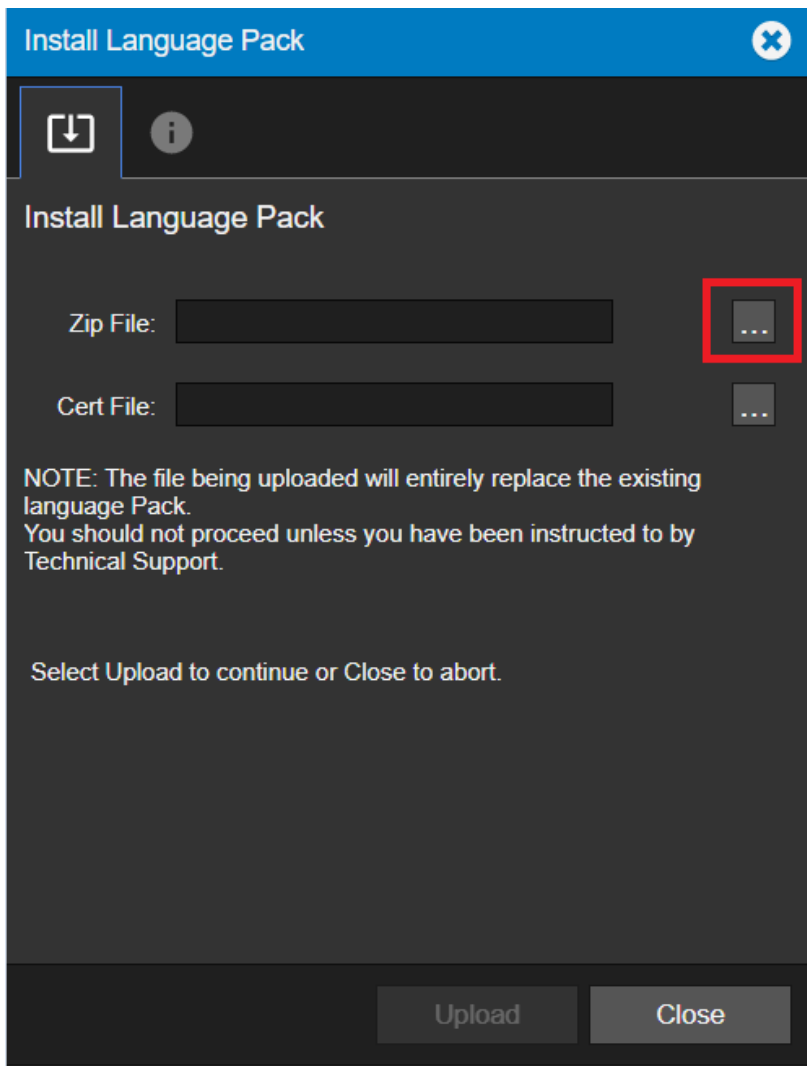
Install Language Pack Process

To install a new language pack into the Foreseer environment:

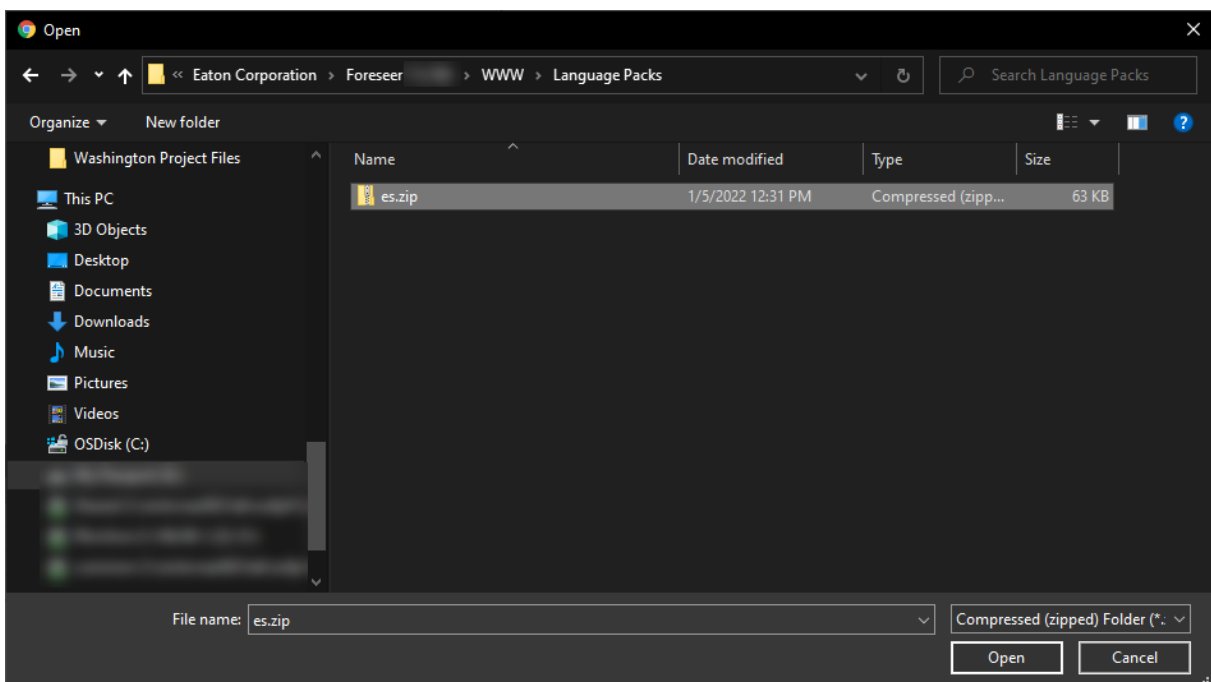
- Select the Install Language Pack to bring up the Install Language Pack dialog.



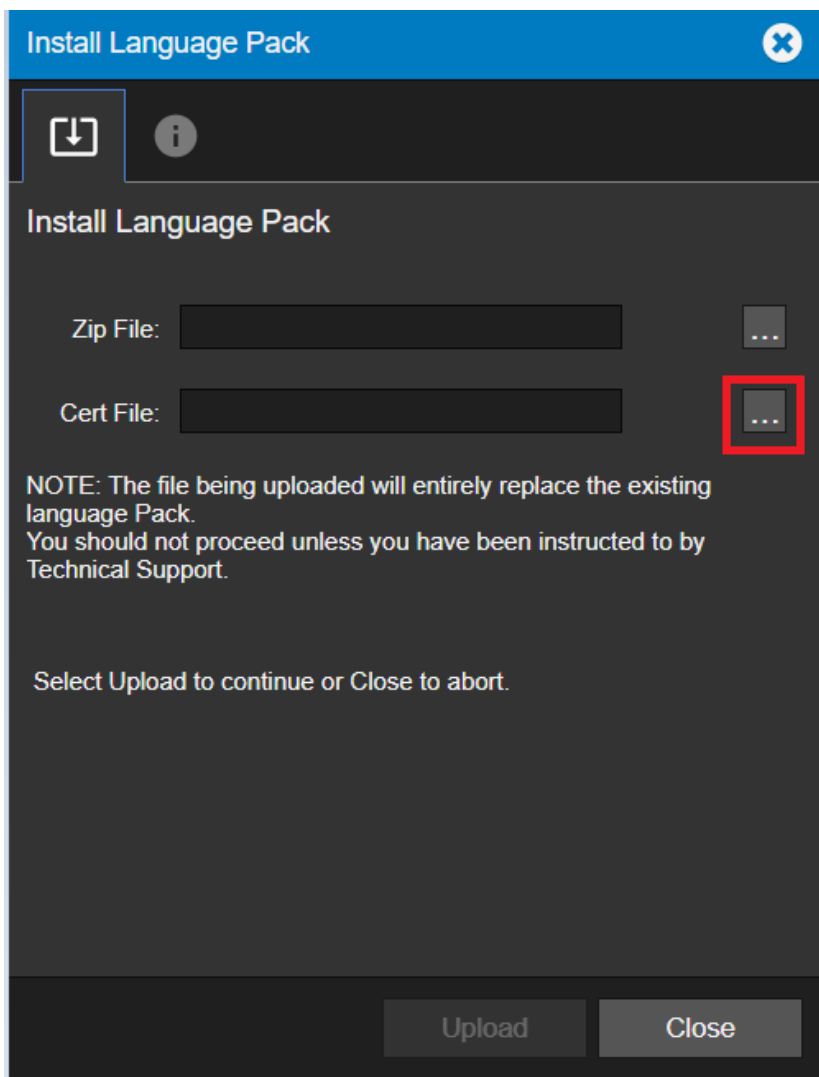
- Click the Zip File ellipse to navigate to the location where the Language Pack ZIP file is installed



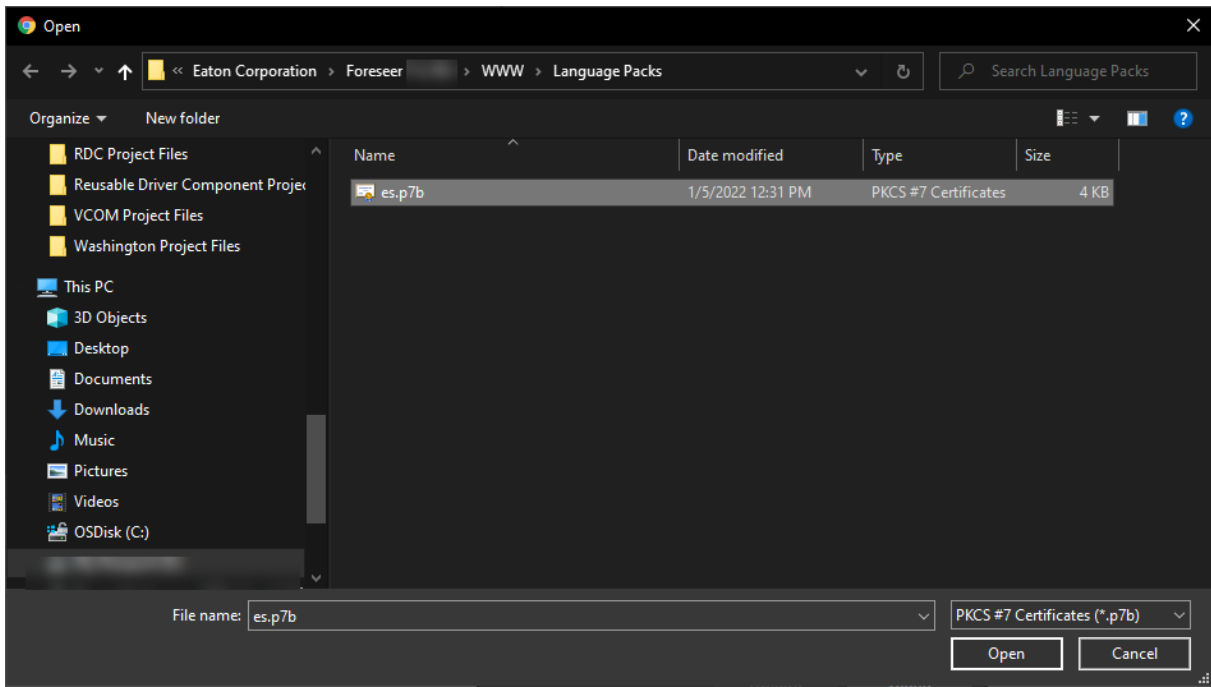
- Select the Language Pack and click Open.



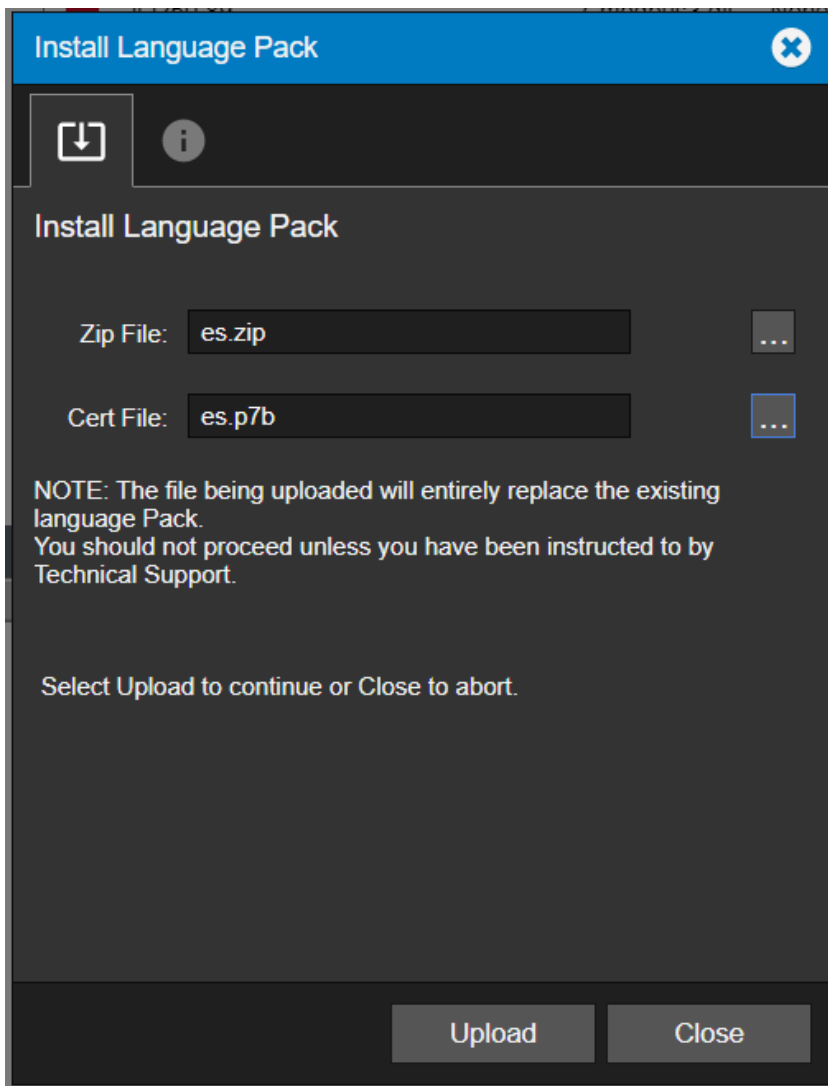
- Click the ellipse to navigate to the location where the certificate file is located.



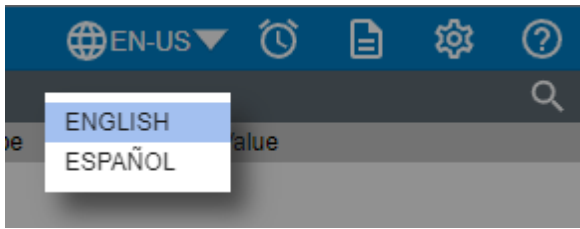
- Select the Language Pack certificate and click Open.



- Click Upload to continue the installation.



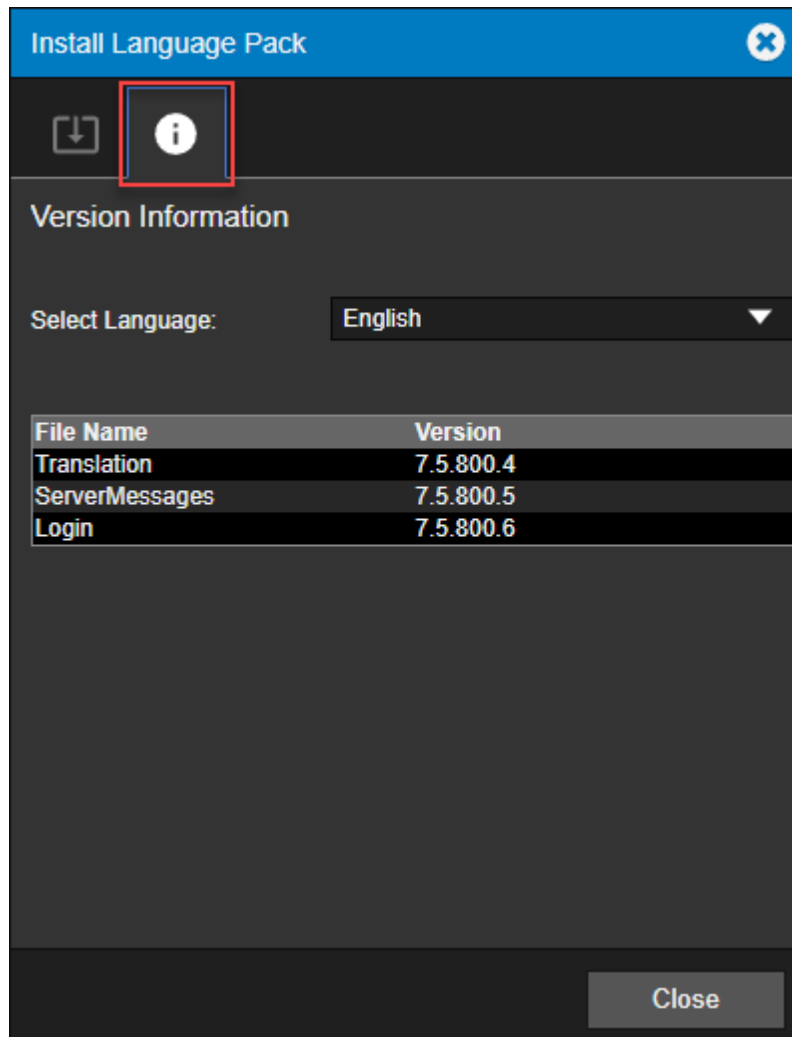
- The newly installed language is now available for selection from the menu



- Refresh the application to have the newly installed language ready for use.

Version Information

To determine the version of Foreseer Language Packs installed on your system, select the Version Information tab.



The version information for the following Language Packs will be displayed.

- Translation
- Server Messages

- Login

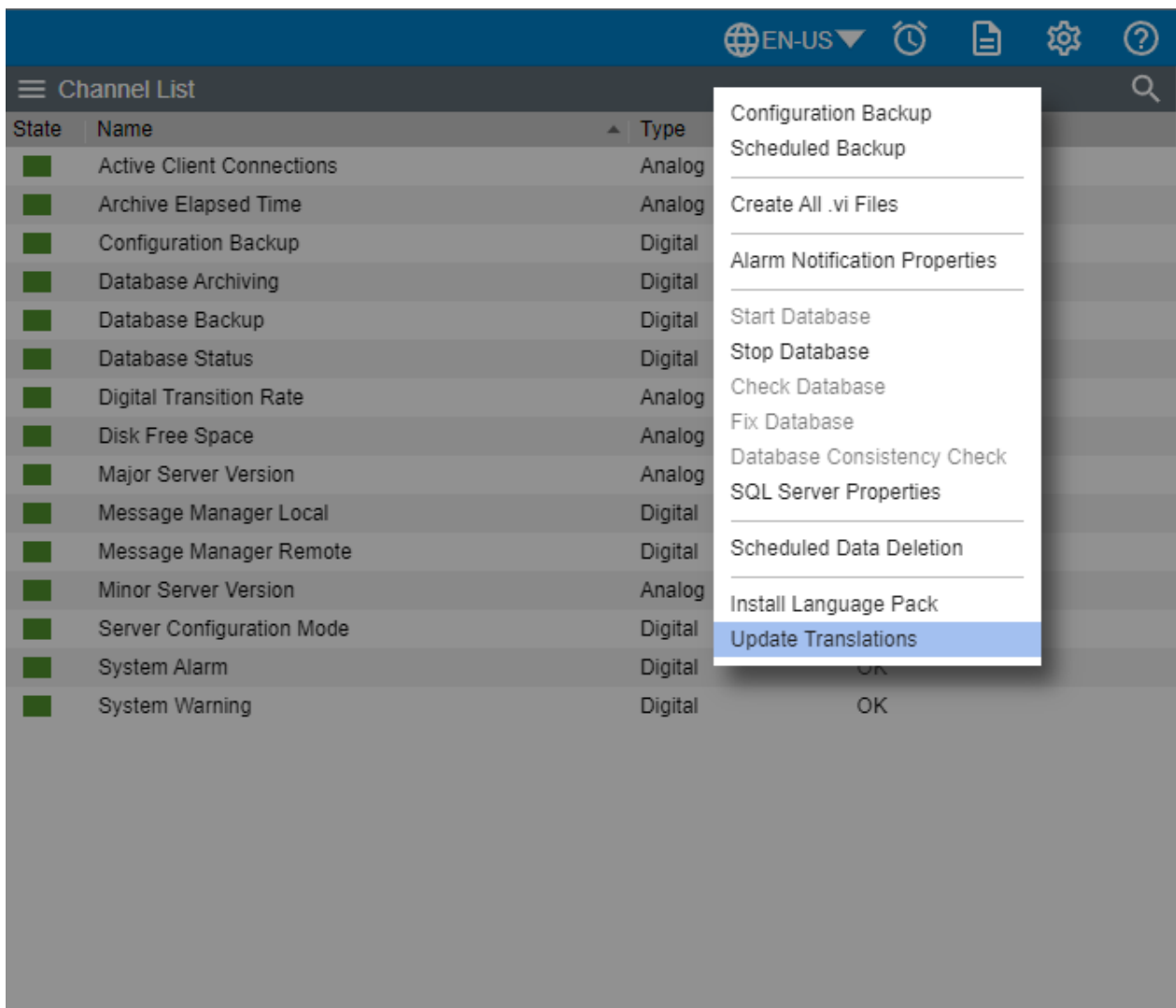
Update Translations

✔ Administrative authorization is required before proceeding with this command.

The Update Translations functionality allows you to perform a number of different operations on the Foreseer Language Pack files in support of the Internationalization of Foreseer. The functions provided are:

- Download Translations
- Upload User Defined Translations
- Restore Translations

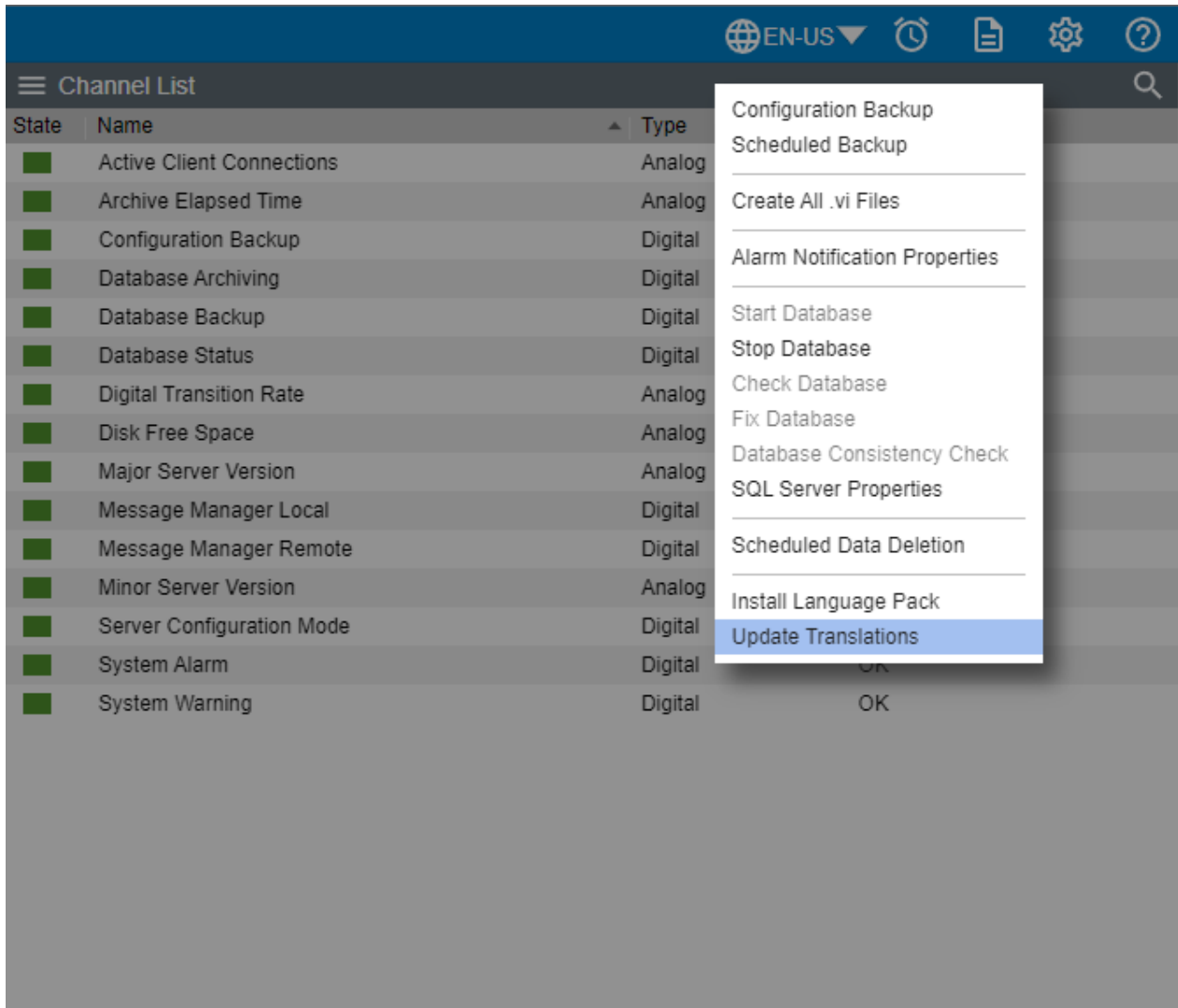
These functions are available from the Update Translations menu option.



Download Translations

✔ Administrative authorization is required before proceeding with this command.

To download the Foreseer Translations defined, select Update Translations from the Settings menu.



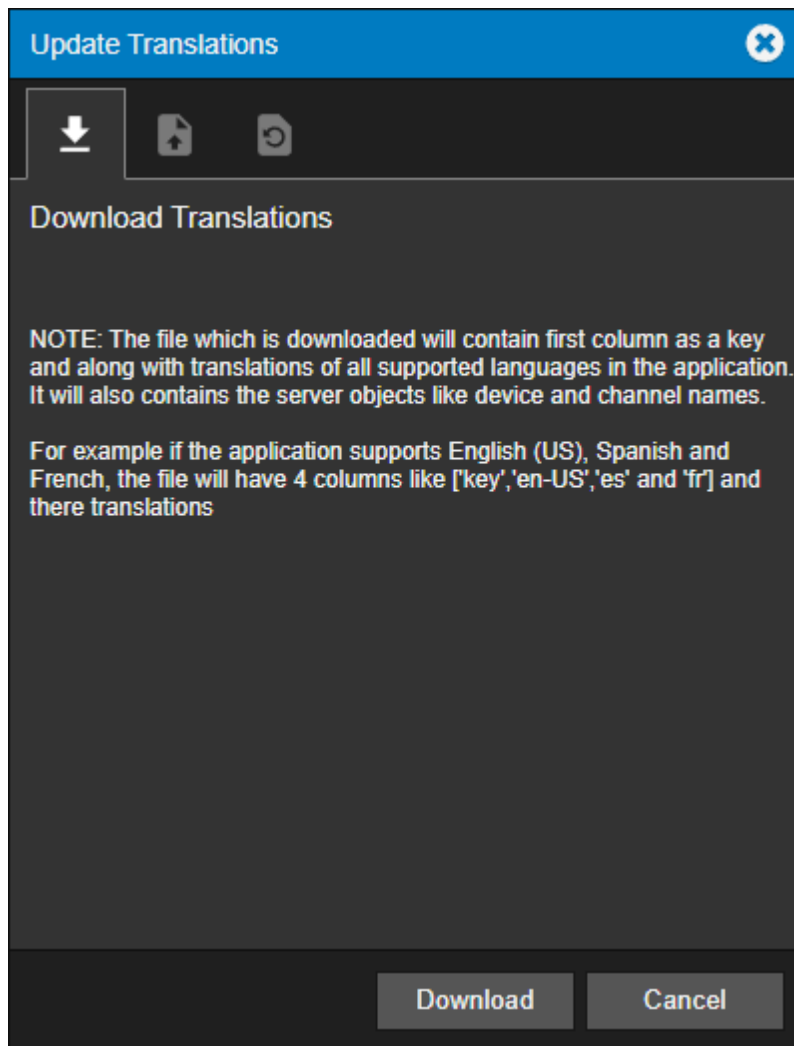
The screenshot shows the 'Channel List' table with columns for State, Name, and Type. A settings menu is open, highlighting the 'Update Translations' option.

State	Name	Type
■	Active Client Connections	Analog
■	Archive Elapsed Time	Analog
■	Configuration Backup	Digital
■	Database Archiving	Digital
■	Database Backup	Digital
■	Database Status	Digital
■	Digital Transition Rate	Analog
■	Disk Free Space	Analog
■	Major Server Version	Analog
■	Message Manager Local	Digital
■	Message Manager Remote	Digital
■	Minor Server Version	Analog
■	Server Configuration Mode	Digital
■	System Alarm	Digital
■	System Warning	Digital

- Configuration Backup
- Scheduled Backup
- Create All .vi Files
- Alarm Notification Properties
- Start Database
- Stop Database
- Check Database
- Fix Database
- Database Consistency Check
- SQL Server Properties
- Scheduled Data Deletion
- Install Language Pack
- Update Translations**

✔ The file which is downloaded will contain the first column as a key, along with the translations of all of the supported languages currently installed in the application. It will also contain the server objects like device and channel names.

From the Download Translations tab, click on Download.



The translation text file will be downloaded to your computer which will provide the user the ability to change any of the text / translations for the devices / channels defined within their Foreseer environment. This file will be in the format:

Key|English text|Translation text

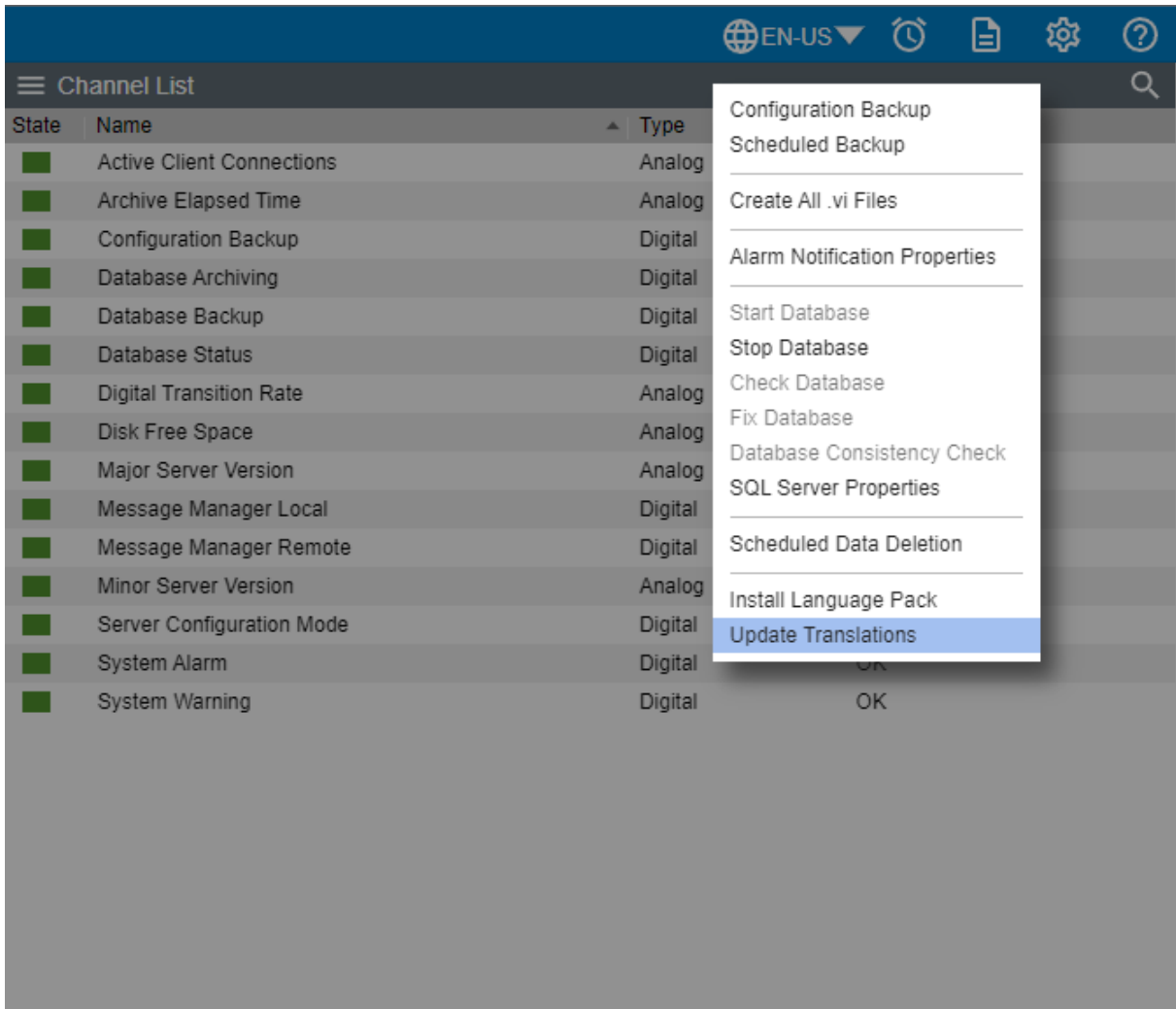
Upload User Defined Translations

✔ Administrative authorization is required before proceeding with this command.

Now that the translation text file has been modified to meet the Foreseer customer's needs, Foreseer provides a mechanism to allow these user-defined modifications to be upload into the system available for use by the application.

To upload the User Defined Foreseer Translations:

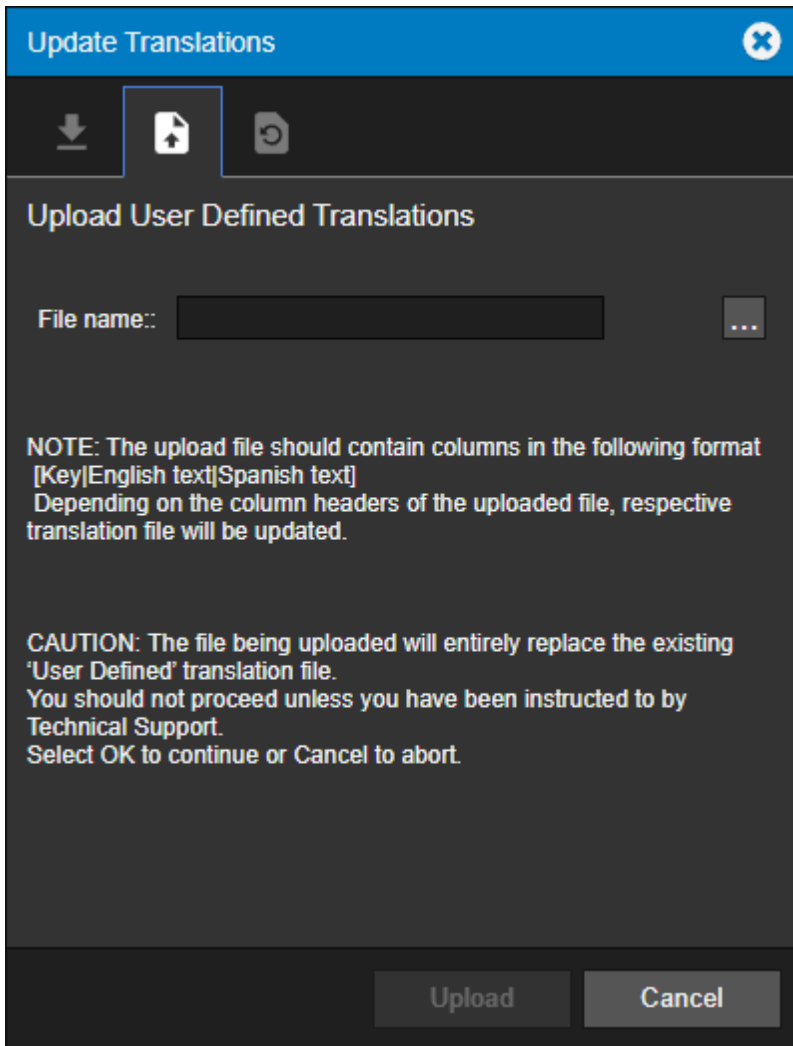
1. Select Update Translations from the Settings menu.



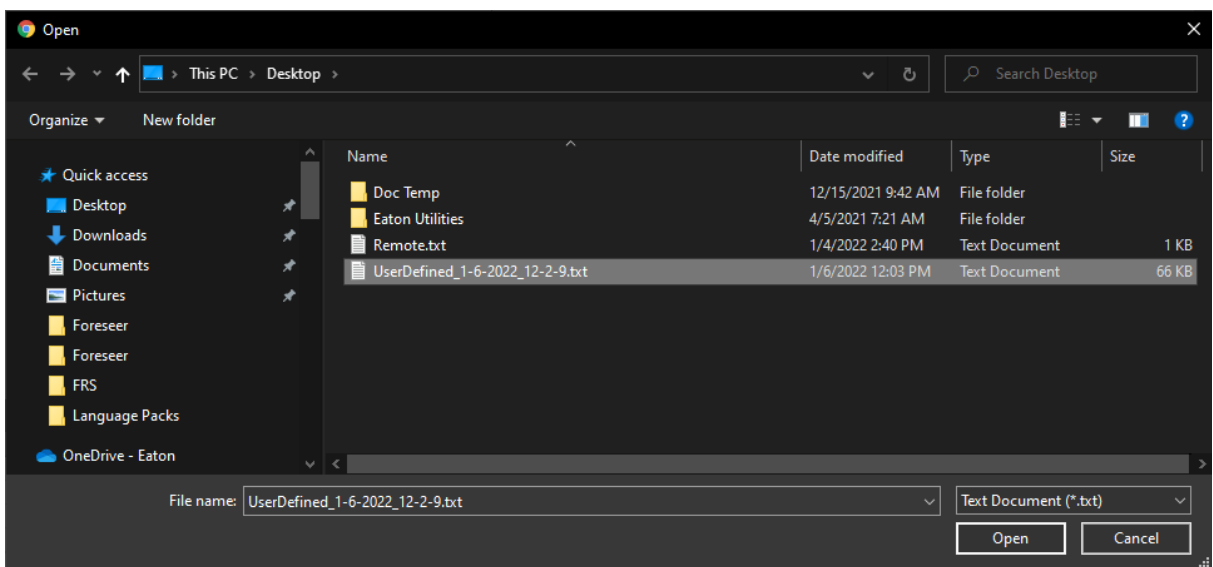
- ✓ The upload file should contain columns in the following format. For example, if Spanish were installed in the Foreseer environment:

Key | English text | Translation text

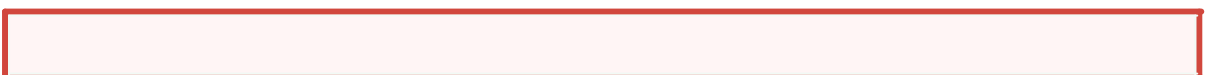
2. From the Upload User Defined Translations tab, click on the ellipse to locate the file.



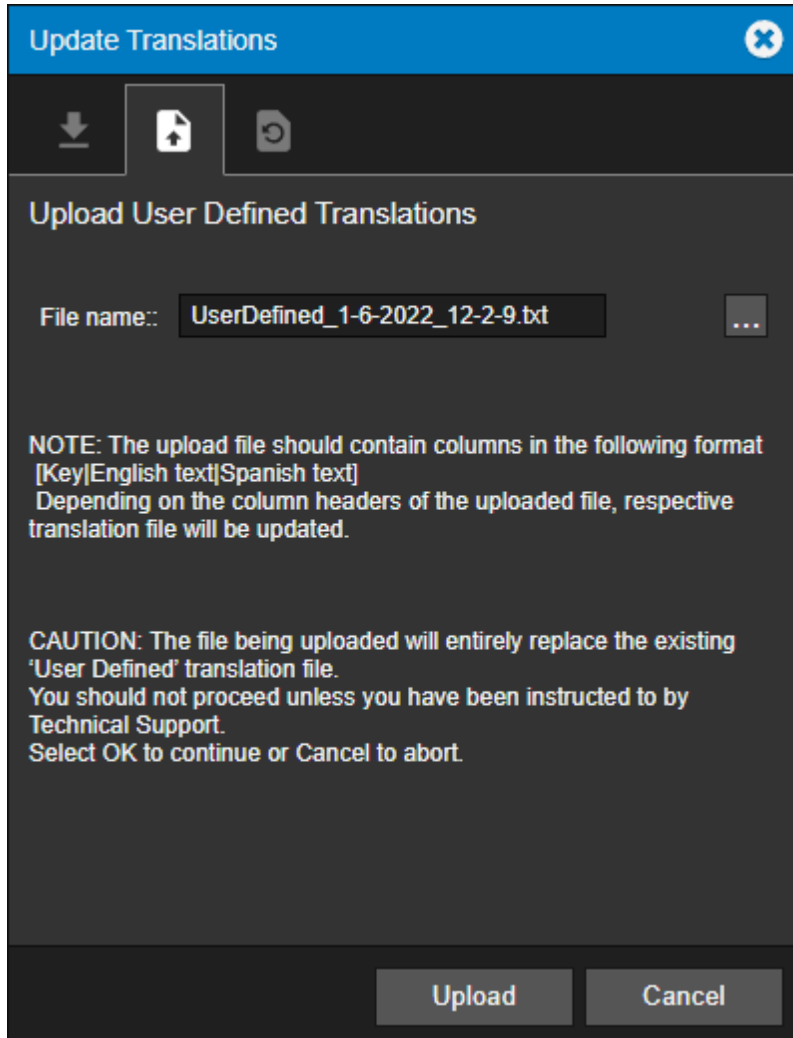
3. Select the filename to be uploaded into the Foreseer environment and click Open



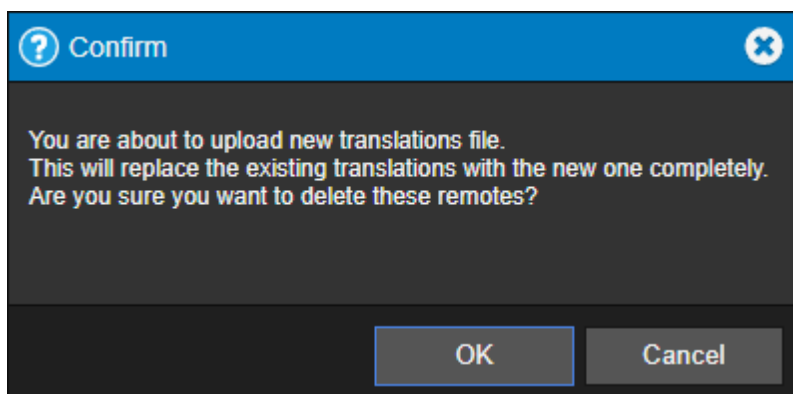
4. Click on Upload to continue.



⚠ The file being uploaded will entirely replace the existing User-Defined translation file. You should not proceed unless you have been instructed to by Technical Support.



5. Click on OK button to confirm the replacement of the Use Defined translations.



Restore Translations

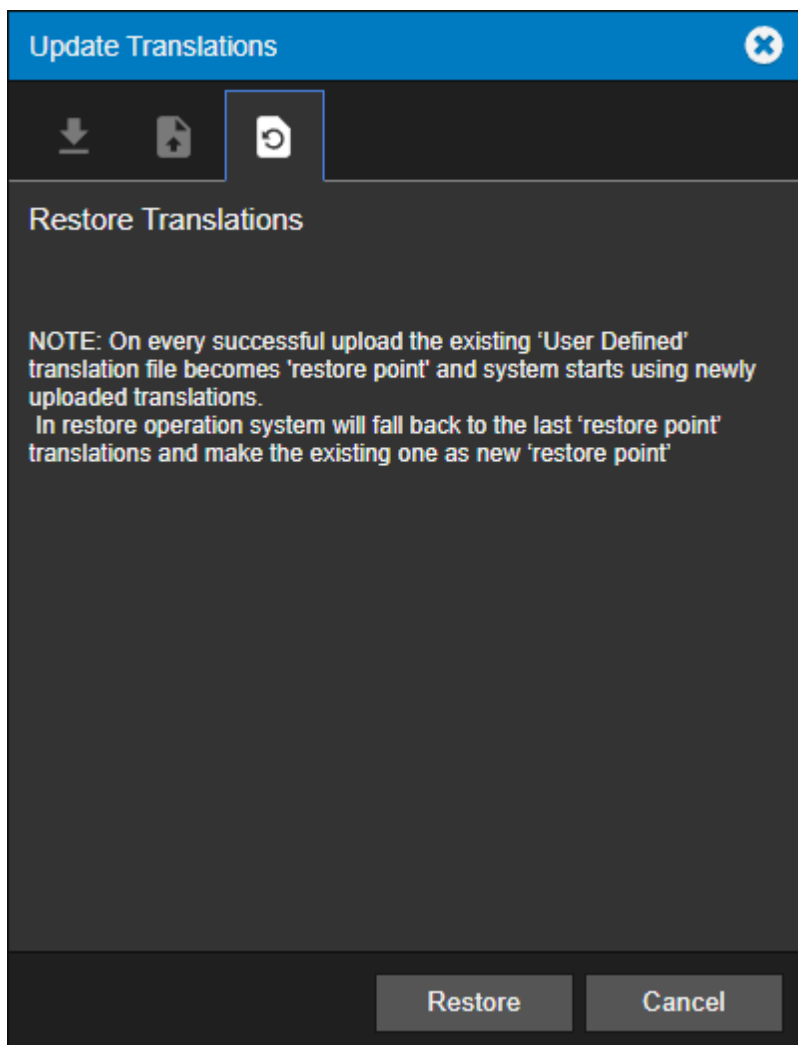
- ✔ Administrative authorization is required before proceeding with this command.

In the event that the User-Defined translations need to be restored, Foreseer provides a mechanism to restore your User Defined Translations based on the last restore point.

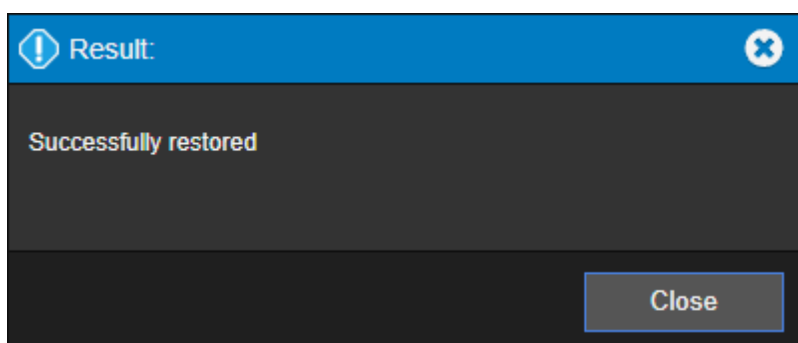
- ✔ On every successful upload, the existing User Defined translation file will become the restore point at which the system will then start using the newly uploaded translations. In a restore operation, the system will fall back to this restore point.

To Restore your User Defined translation file back to the restore point:

1. Click on the Restore button on the Restore Translations dialog.



2. Click on the Close button on the Successfully Restored Confirmation dialog.



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 Devices from List
- User Defined Fields
- Add Remote
- Copy for WebViews
- Restart WebViews
- Restart Server
- Restart Windows
- Add Note
- Get Log File
- Upload Files
- Open Older Log File
- Open Saved Wiretap
- Properties

Start Server Configuration

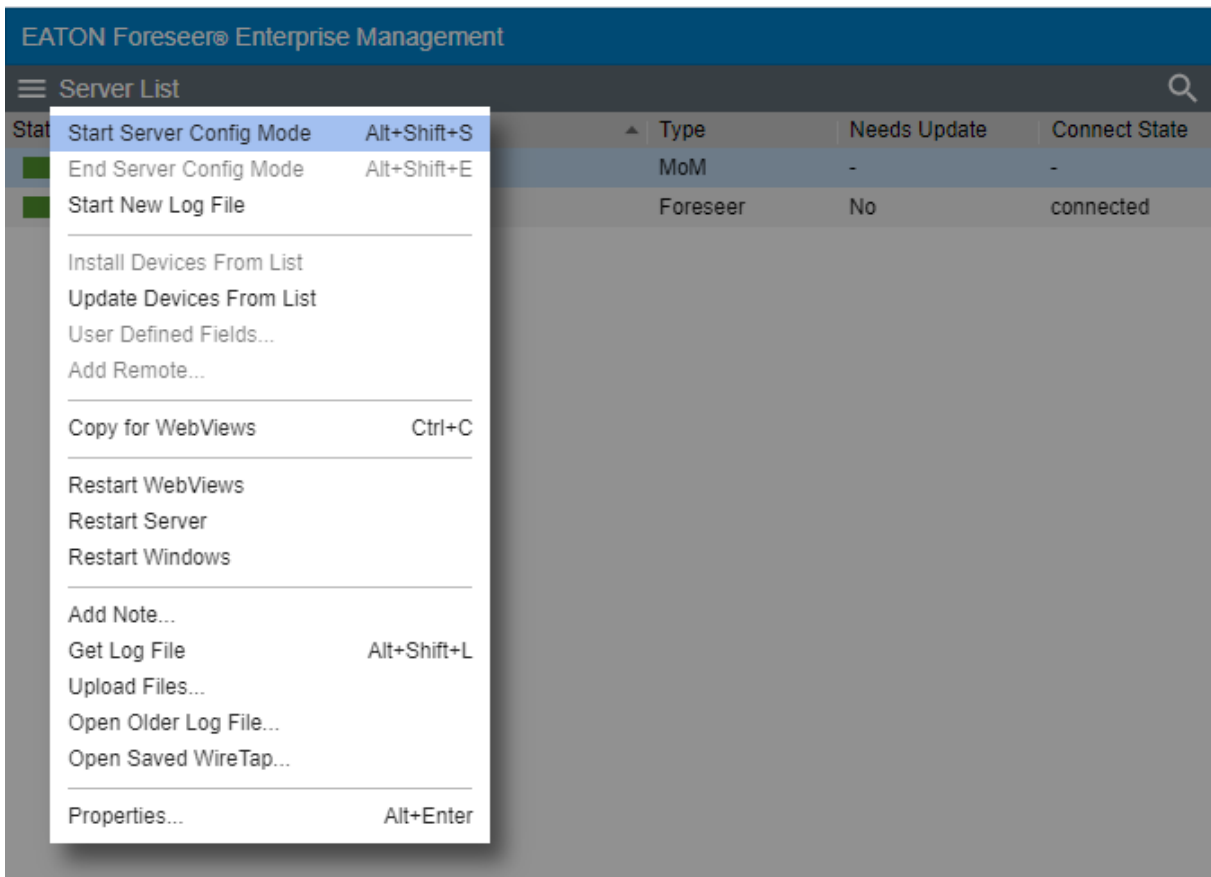
Certain configuration functions are only available when in Server Configuration mode; however, configuring backups is only available when not in Server Configuration mode. Functions that are only available in Server Configuration mode are:

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

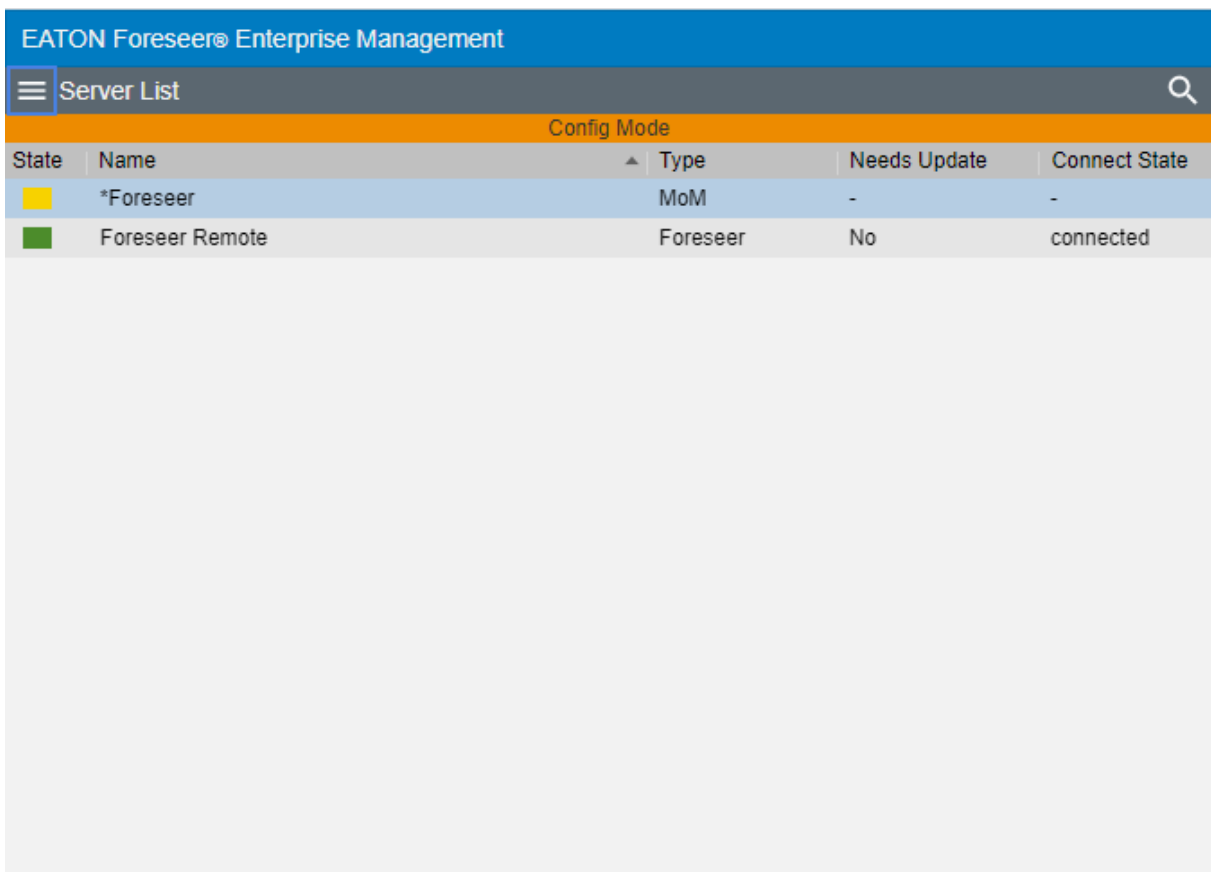
 Administrative Authorization is required in initiating Server Configuration mode.

To start Server Configuration mode:

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



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

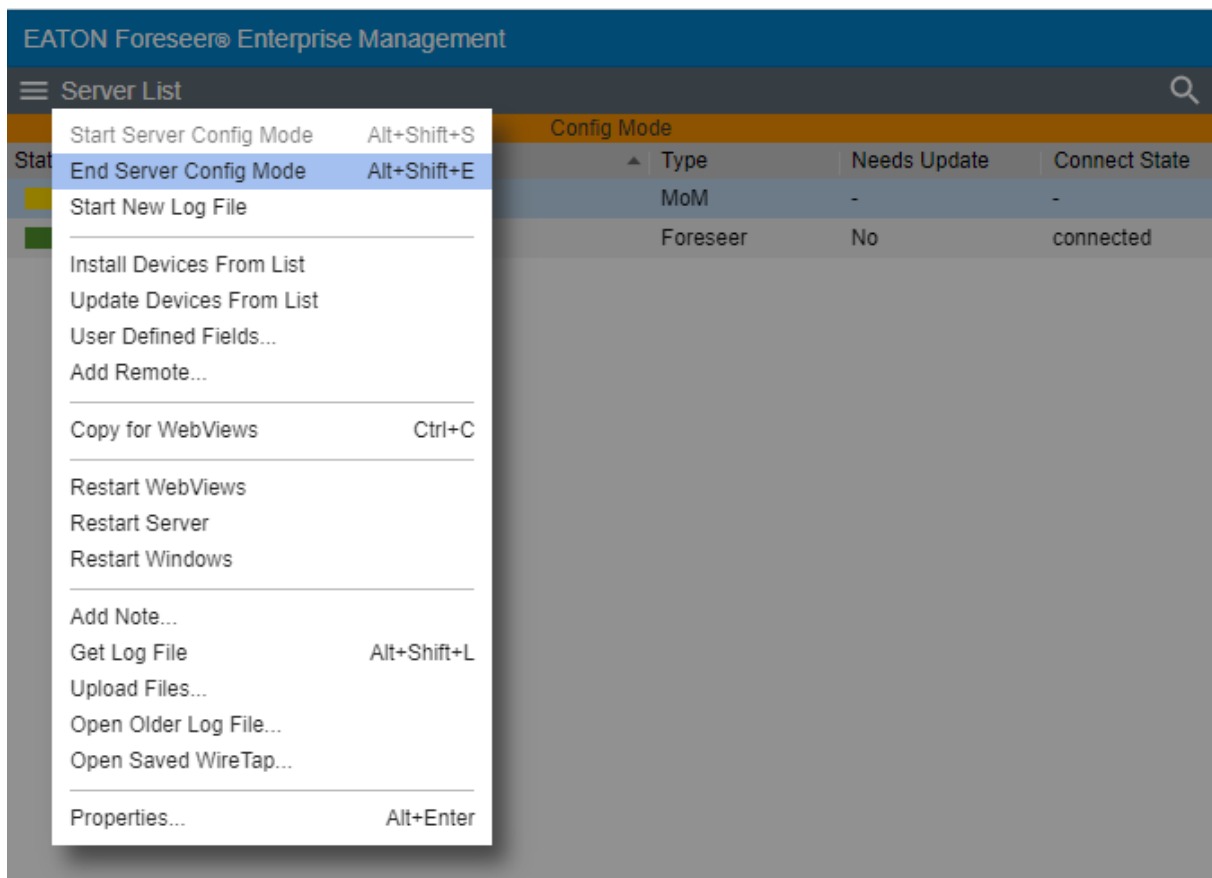


End Server Configuration

✔ 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

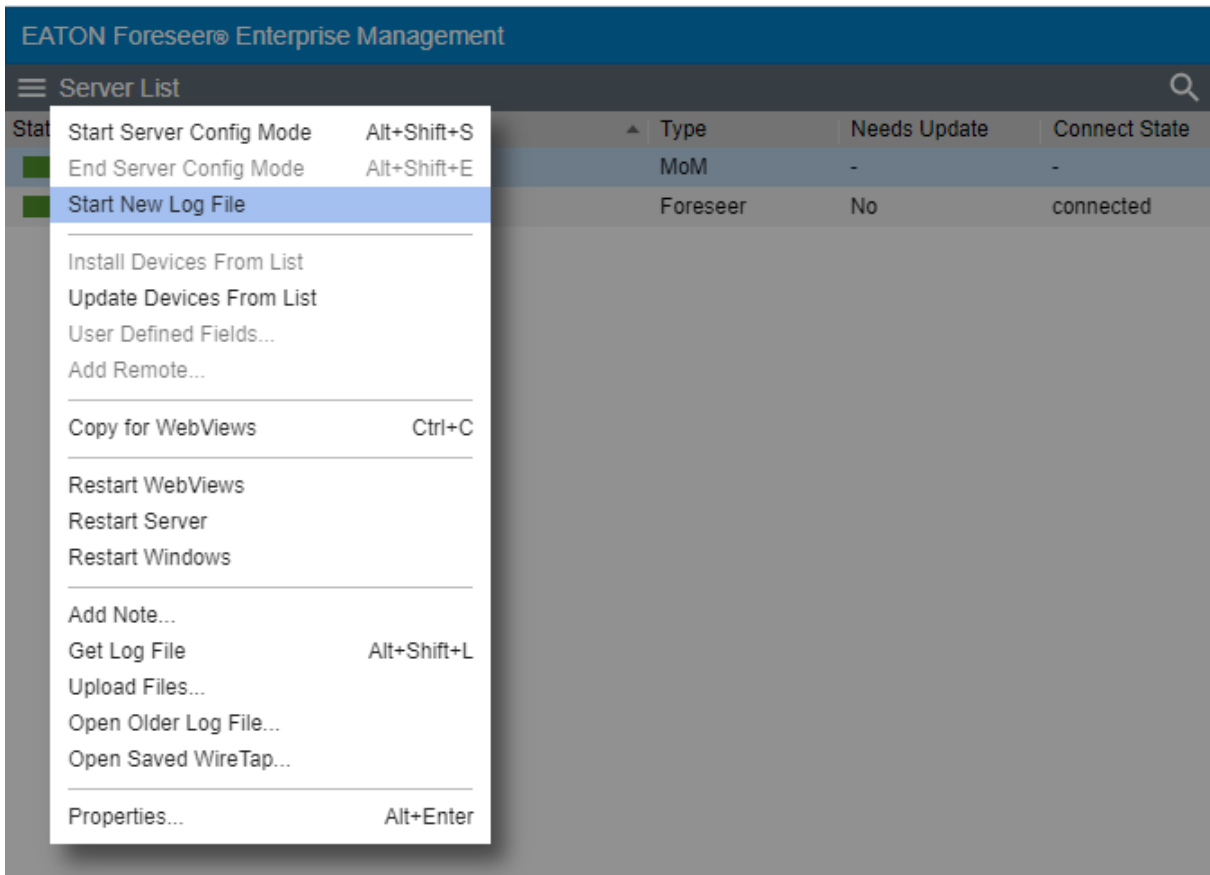
<Install Drive>\Eaton Corporation\Foreseer\LogFiles

folder.

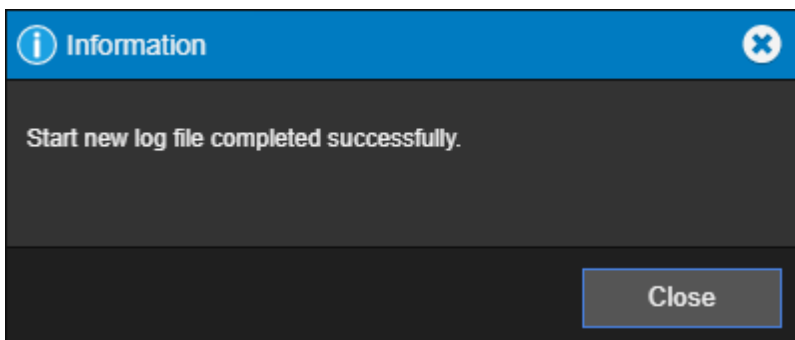
- ✔ The current LogFile.txt is located in the <Install Drive>:\Eaton Corporation\Foreseer\ directory and not in the LogFiles directory.

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.

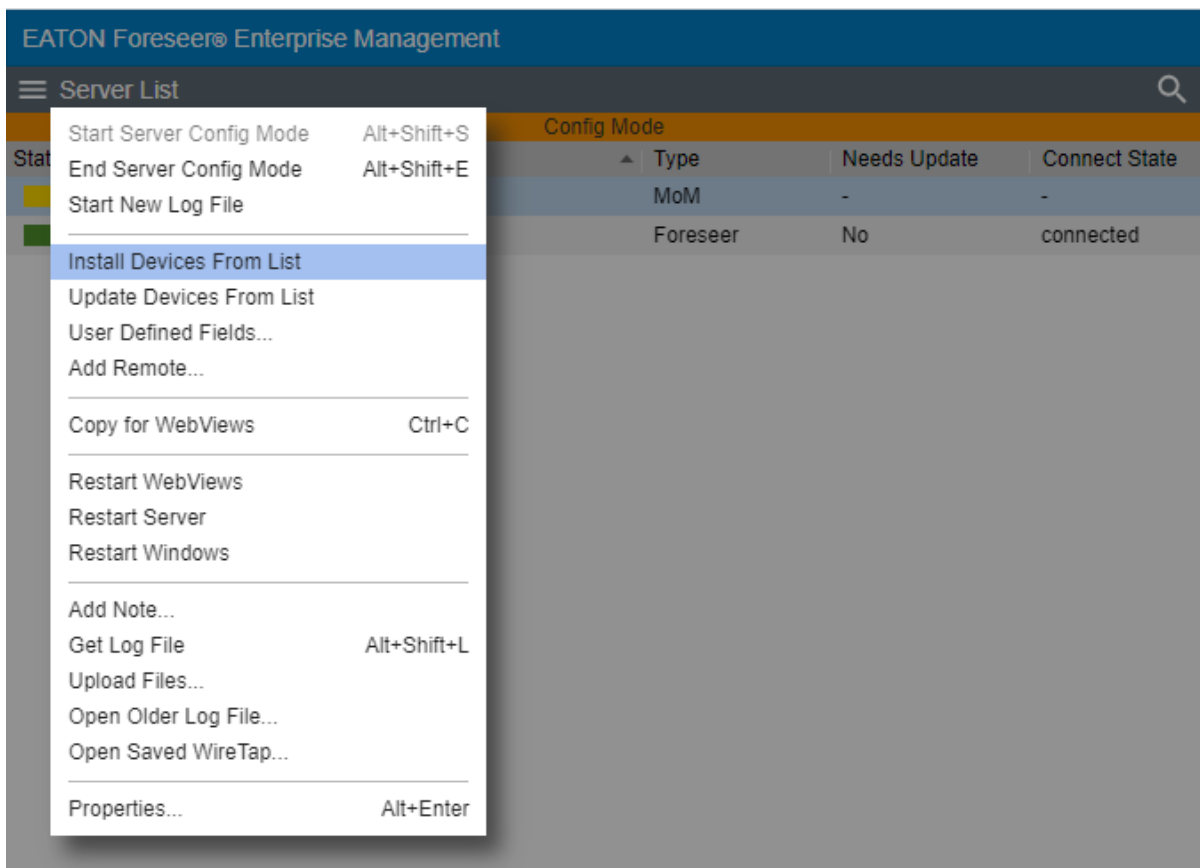
IP_address is the IP address for that device. Set this to none for the Nothing driver.

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.

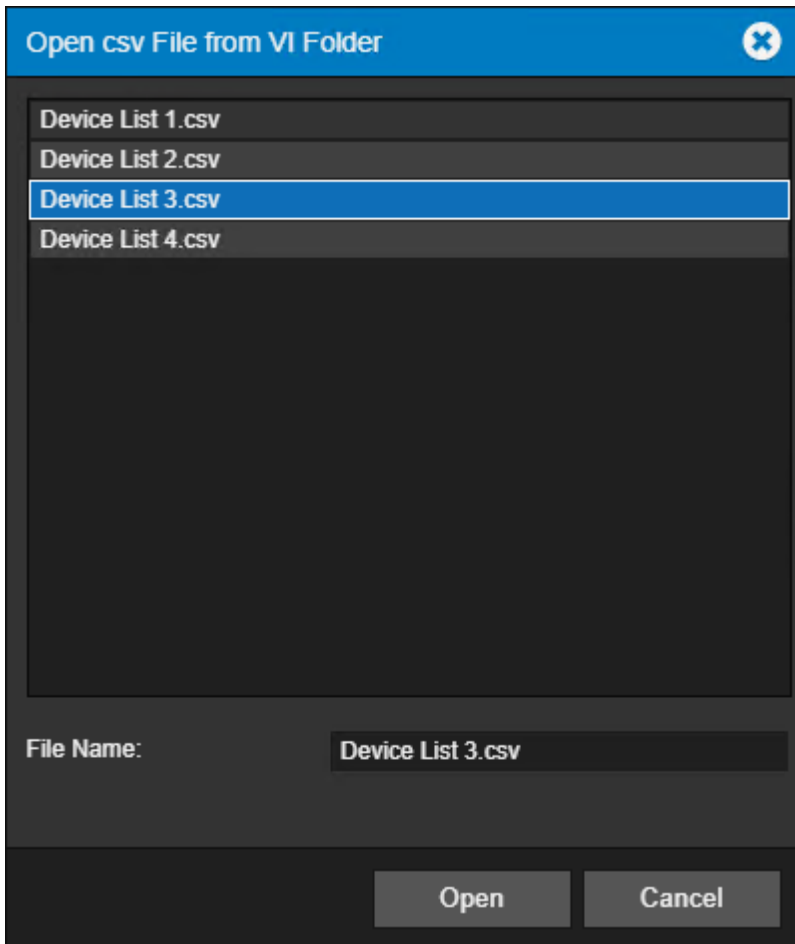
driver_specific_info is either the device ID (for Modbus) or the read community string for SNMP. Set this to none for the Nothing driver.

To add a device from list server:

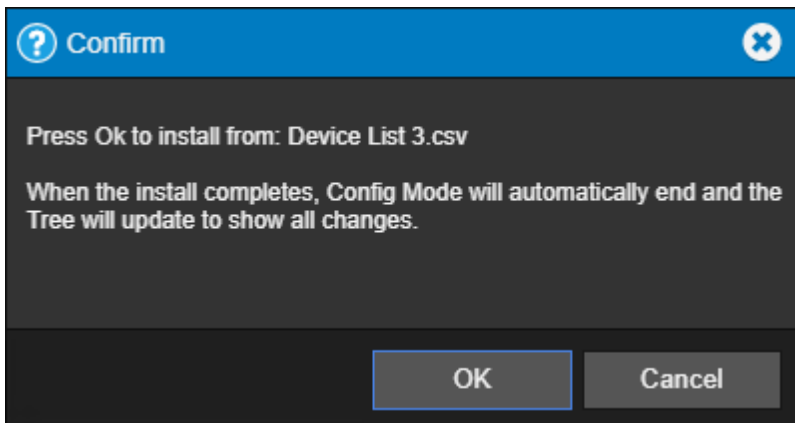
1. Select Install Device From List in the Server List menu.



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:

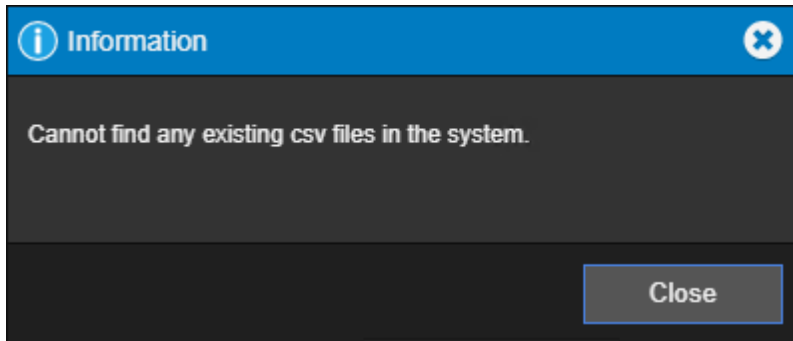
Nothing 1, None, PA-Pittsburgh, Custom Alarms, 7-Nothing.vi, none

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:

deviceName, deviceType, deviceLocation, alarmGroupName

-where-

deviceName – the case sensitive name of the existing device in the Foreseer server configuration

deviceType – 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.

deviceLocation – a string defining the location of the device.

alarmGroupName -a string defining a logical alarm grouping name.

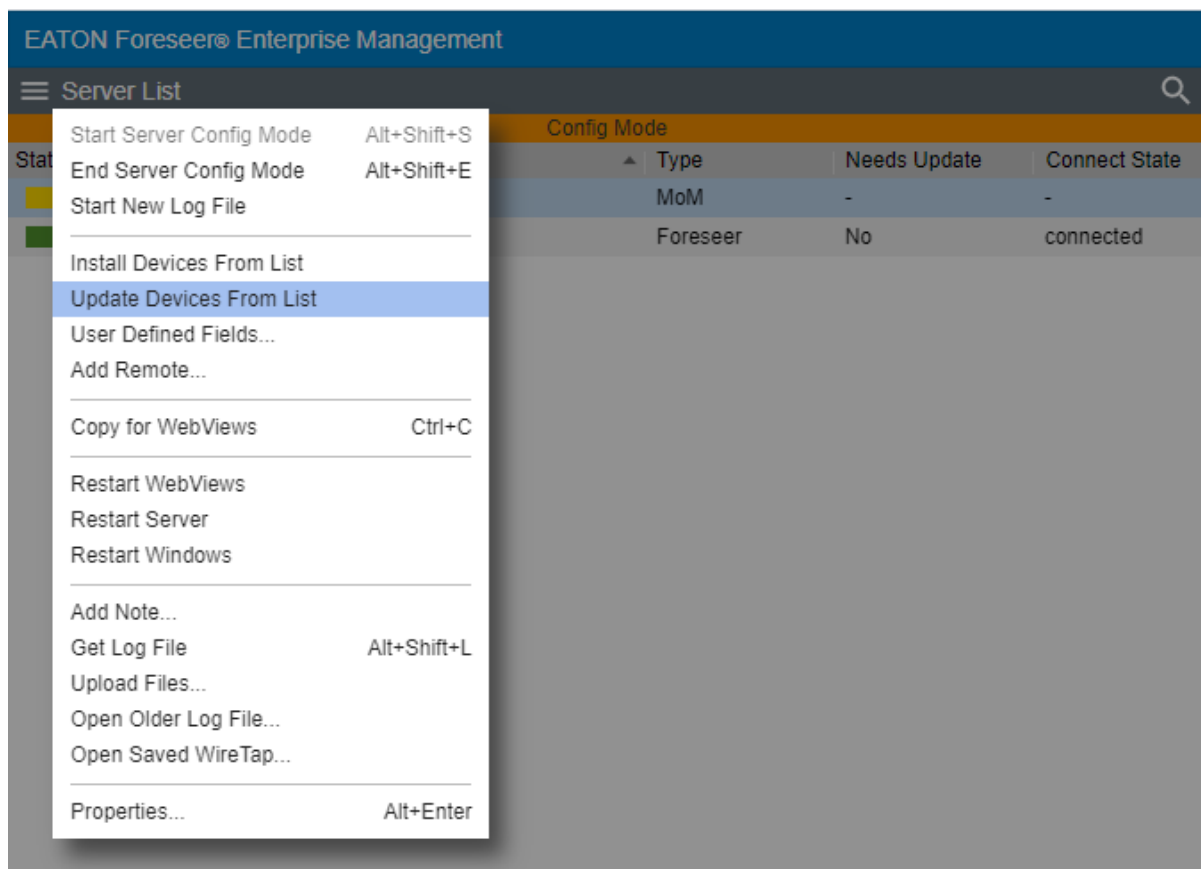
The Device Type, Device Location, and Alarm Group Name fields can be blank for situations where only one of the fields needs to be updated. The Device Name is always required in order for the Update process to find the existing device to update.

- ✓ 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.

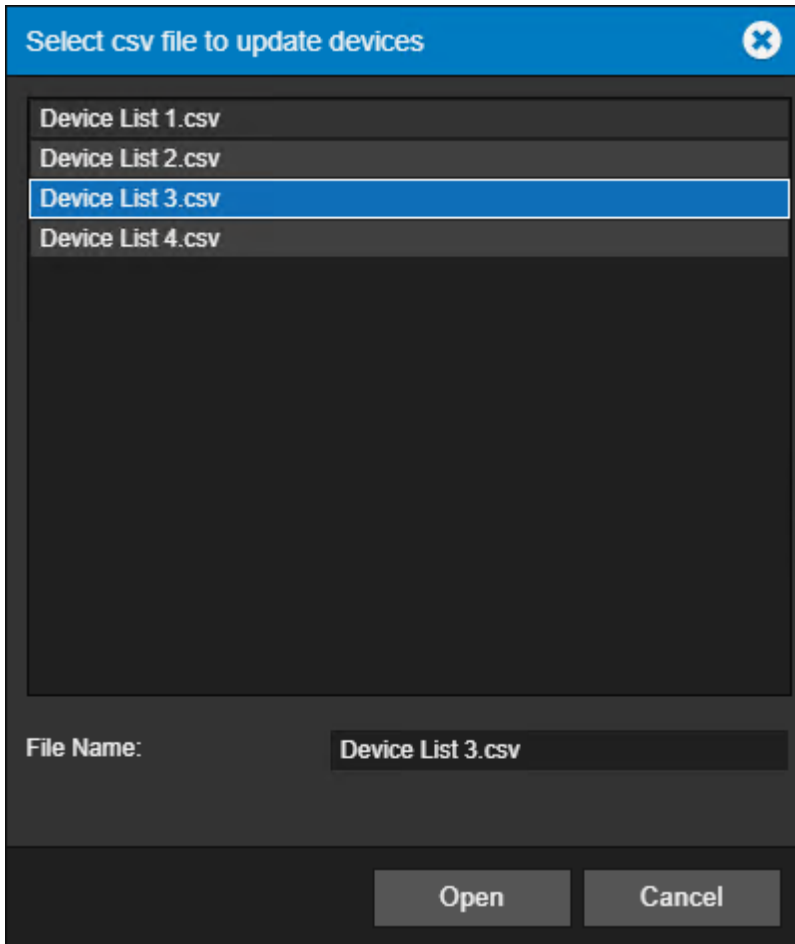
Modern cybersecurity standards prohibit .csv files from being uploaded to web servers like Foreseer using the Upload File feature. Therefore, you must make the appropriate provisions to manually copy this file into the VI directory via Windows File Explorer.

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

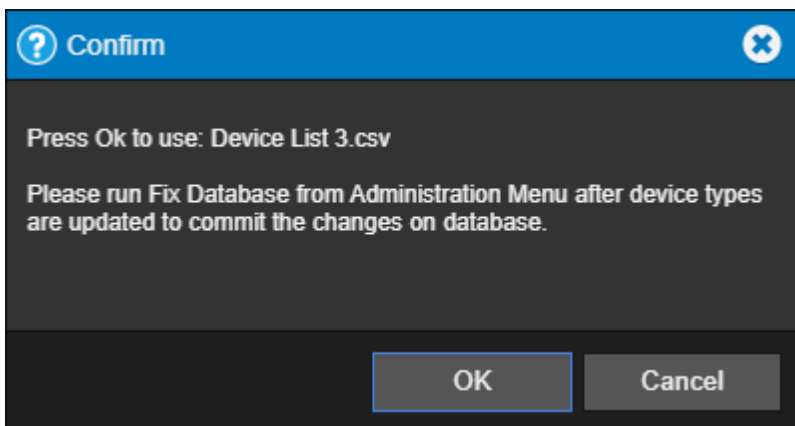
1. Select Update Device From List in the Server List menu.



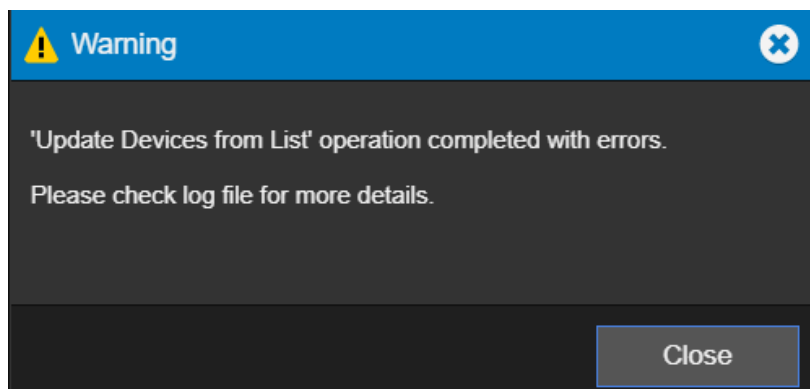
2. Select the appropriate CSV file from the list provided.



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.



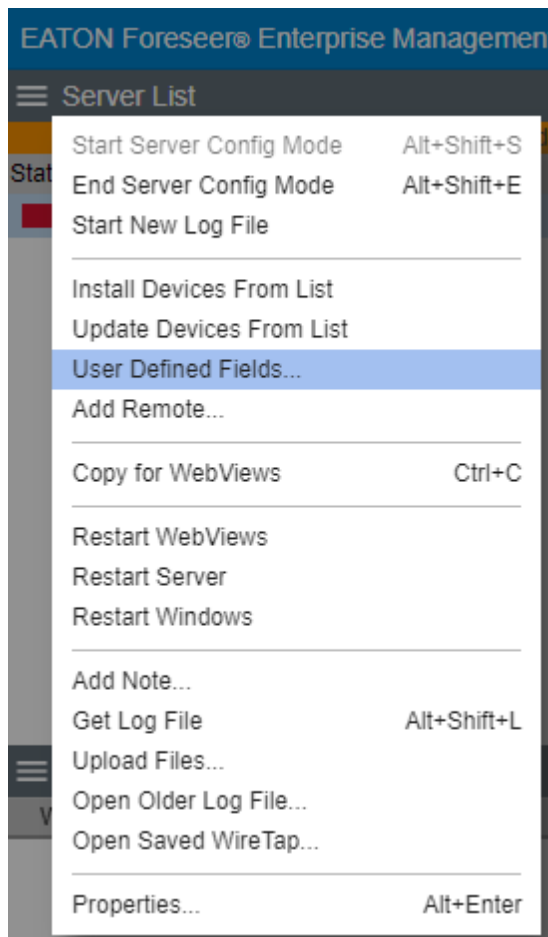
- ✔ Remember to perform a Fix Database operation in order to commit these changes into your SQL Server database.

User Defined Fields

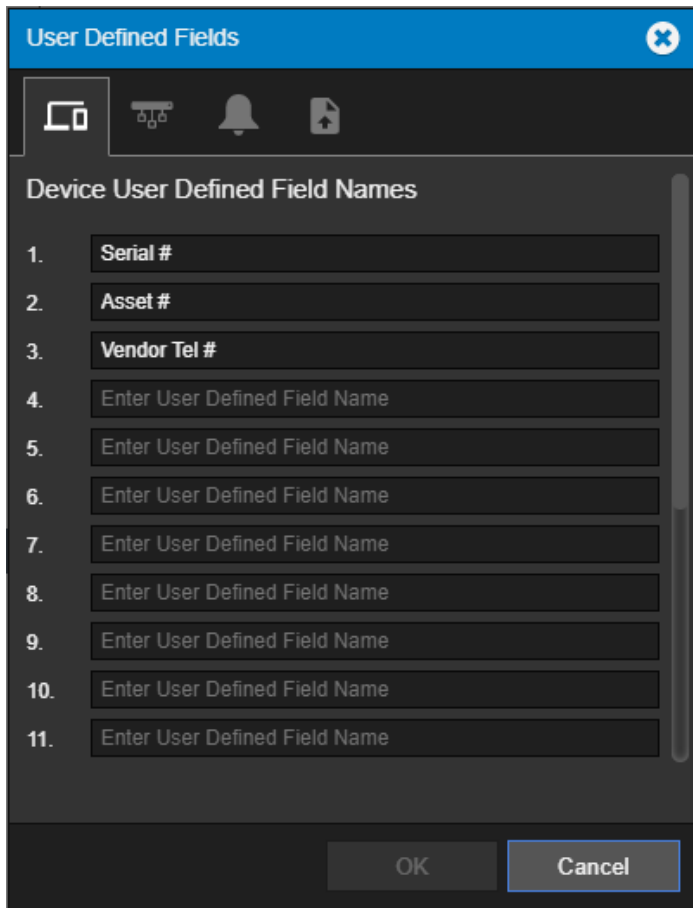
User Defined Fields provides users with the ability to add custom text-based properties to devices and channels within a configured system. This feature, accessible from the Server List menu during [Config Mode](#), allows a system administrator to define up to 20 custom properties for devices and channels globally in a configured system, as well as five additional custom alarm bands. Custom property definition can be achieved directly within WebConfig using a simplistic field editor.

For situations where custom properties for channels need defined in bulk fashion, the configuration dialog provides a CSV upload feature. This allows you to update the custom properties of channels in bulk fashion.

To access User Defined Fields configuration, start Server Configuration Mode and select the User Defined Fields option from the list of available menu options. You can follow the instructions below on updating User Defined Fields. Once complete, be sure to perform an End Server Configuration Mode. You can then make changes to any fields within the system.



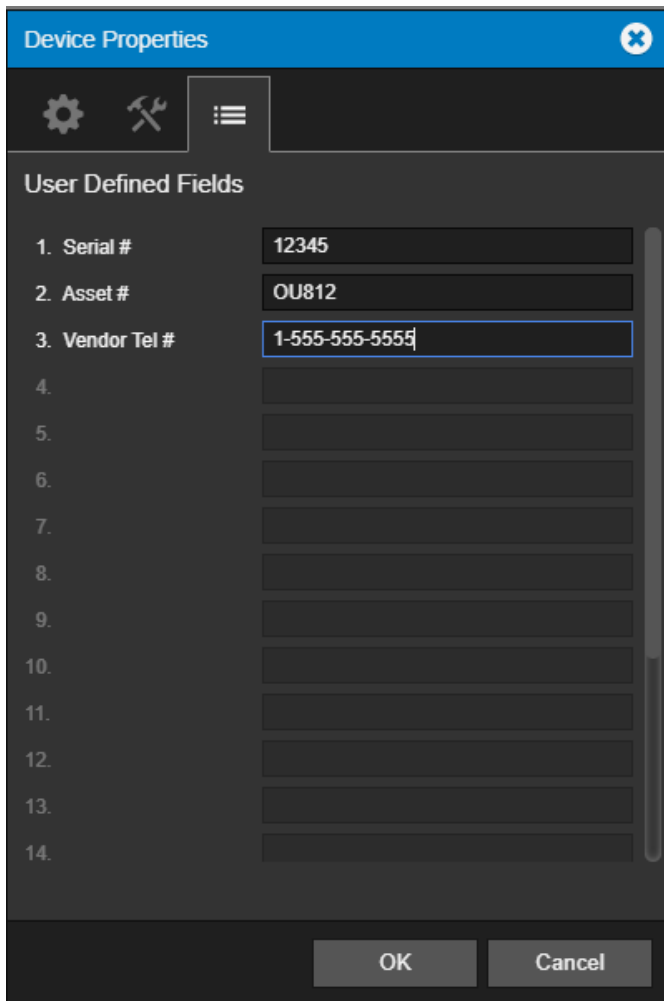
The first tab of the User Defined Fields configuration dialog is used to create custom device properties. A maximum of 20 custom properties can be added to devices globally. Using the dialog, simply enter your desired text descriptions for each property.



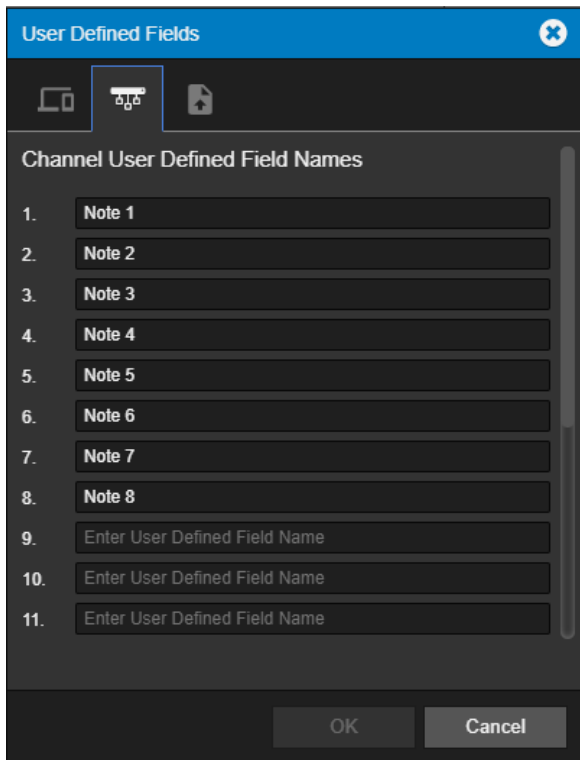
The image shows a 'User Defined Fields' dialog box with a blue header and a close button. Below the header is a toolbar with icons for a device, a tree view, a bell, and a document. The main area is titled 'Device User Defined Field Names' and contains a list of 11 numbered input fields. The first three fields are pre-filled with 'Serial #', 'Asset #', and 'Vendor Tel #'. The remaining eight fields are empty and labeled 'Enter User Defined Field Name'. At the bottom, there are 'OK' and 'Cancel' buttons.

Field Number	Field Name
1.	Serial #
2.	Asset #
3.	Vendor Tel #
4.	Enter User Defined Field Name
5.	Enter User Defined Field Name
6.	Enter User Defined Field Name
7.	Enter User Defined Field Name
8.	Enter User Defined Field Name
9.	Enter User Defined Field Name
10.	Enter User Defined Field Name
11.	Enter User Defined Field Name

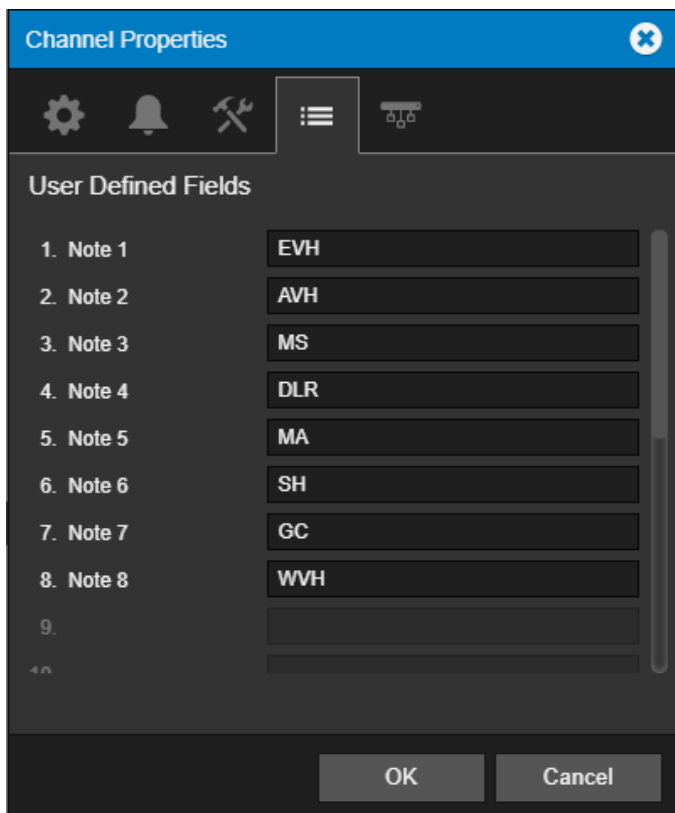
Accessing a device's properties will allow these fields to become available on the custom properties tab. Device custom property field values are limited to 255 characters.



The second tab of the User Defined Fields configuration dialog is used to create custom channel properties. A maximum of 20 custom properties can be added to channels globally. Using the dialog, simply enter your desired text descriptions for each property.

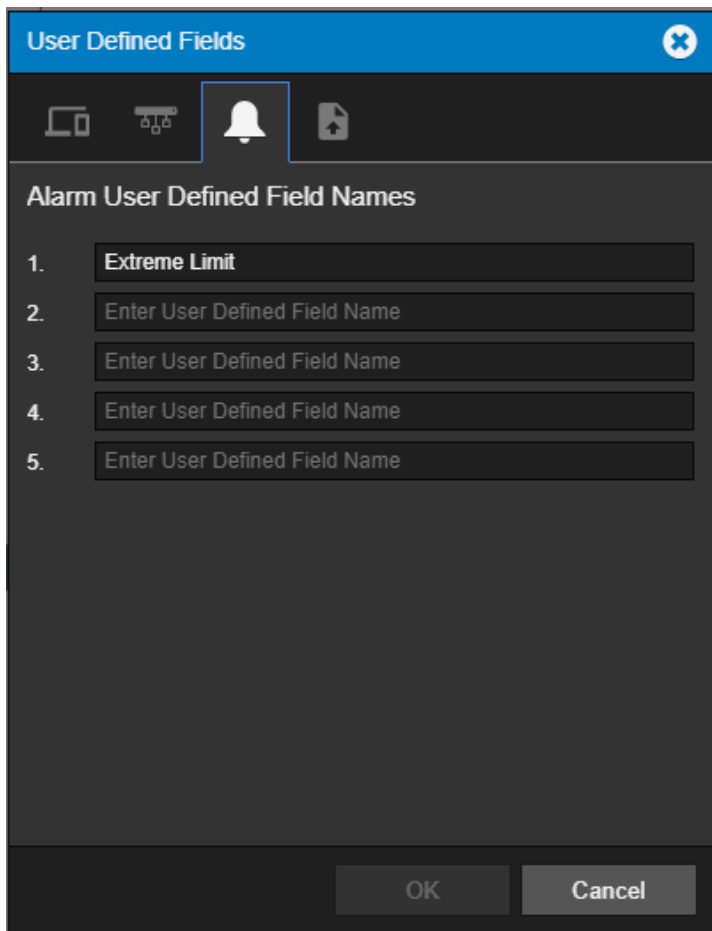


Accessing a channel's properties will allow these fields to become available on the custom properties tab. Channel custom property field values are limited to 255 characters.

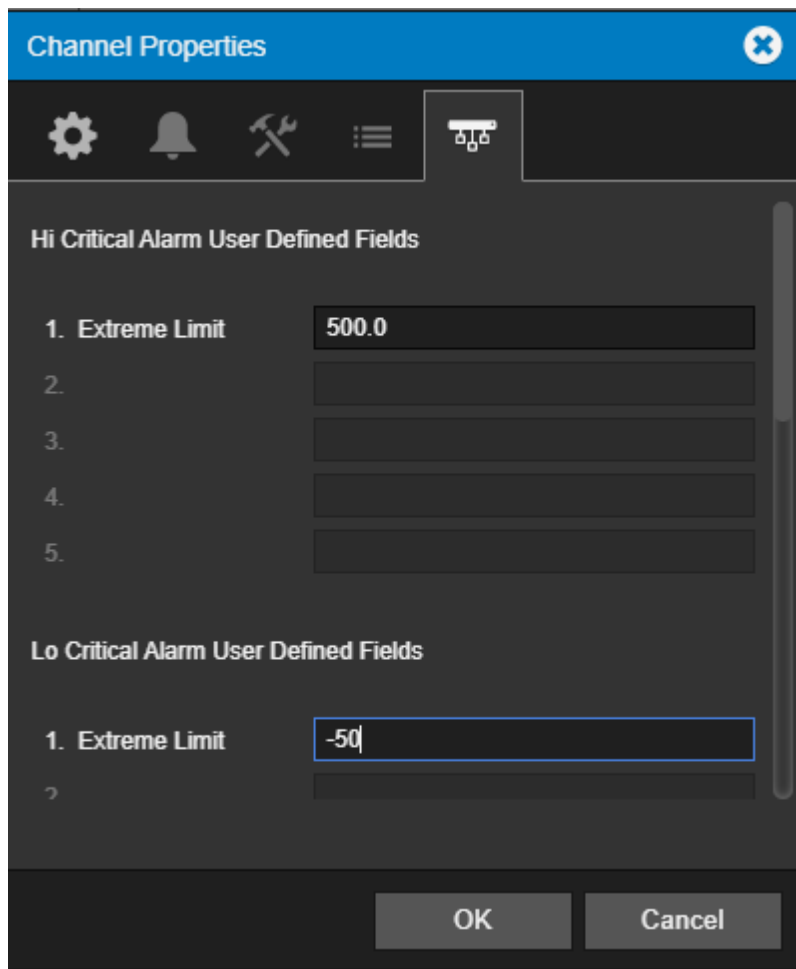


The third tab provides you with the ability to define custom alarm properties. You can define up to five (5) custom alarm properties, where analog channels have four groups of five, and digital and date channels can contain one group of five properties. Text channels

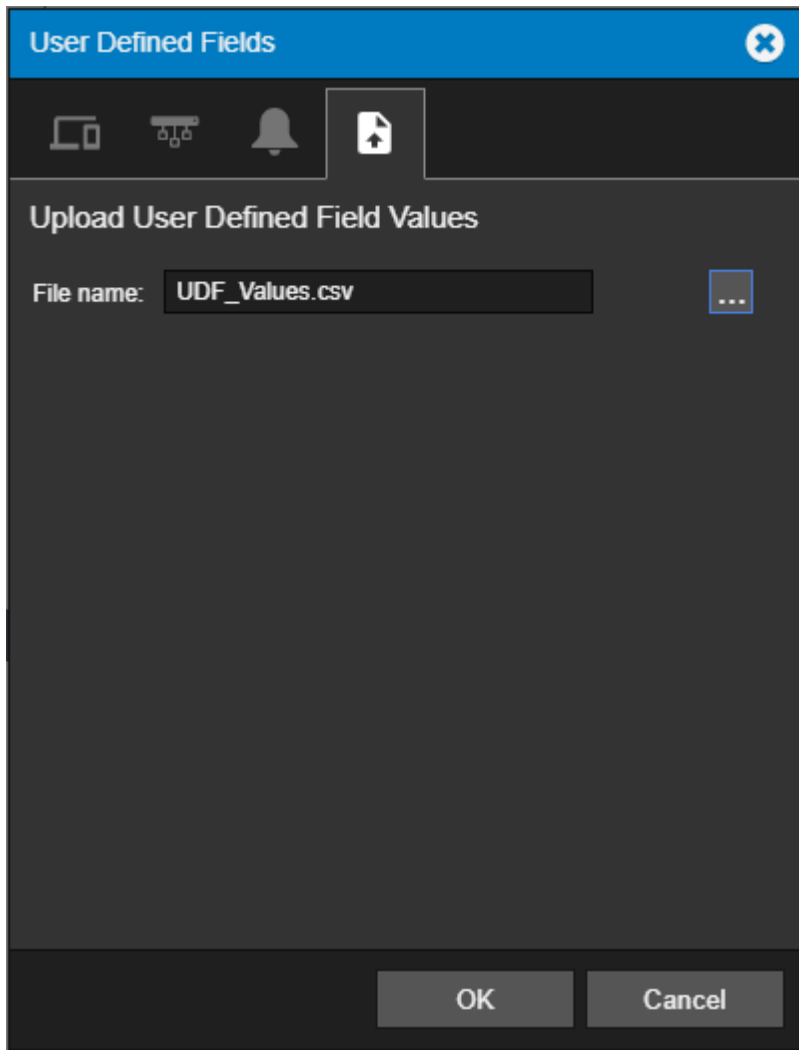
cannot alarm and, therefore, cannot be assigned custom alarm properties.



When you access a channel's properties, the last tab will provide you with the ability to adjust these alarm bands.



The fourth tab provides you with the ability to upload a configured CSV file to set custom properties for Channels. Press the Browse (...) button to navigate your file system and locate the CSV file you wish to upload.



The format of the CSV file is as follows:

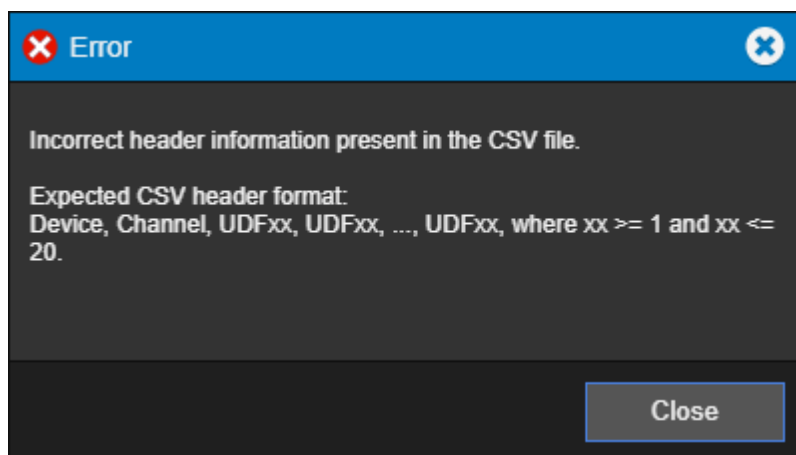
```
Device,Channel,UDF1,UDF2, UDF3  
Device1,Channelx,CustomValue1,CustomValue2,CustomValue3  
...
```

The first line of the CSV file defines the appropriate headers. The header will always include a position for the Device Name and Channel Name. In the example above, our system has three user defined property fields. Therefore, additional columns are added based on the numerical order of our custom properties. The number of UDF# fields in your header will dependent on how many custom properties you wish to initialize.

Subsequent lines will define the name of the Foreseer device, it's channel, and the values you wish to initialize the custom properties to. An example of how the format is applied using a CSV/spreadsheet editor is shown below.

	A	B	C	D	E	F	G
1	Device	Channel	UDF1	UDF2	UDF3		
2	IQ 260 1	D_kVAh Phase A	HOLLAND-598745	OATES-22	719-266-2837		
3	IQ 260 2	D_kVAh Phase A	HOLLAND-598745	OATES-22	719-266-2837		

In the event that your CSV file contains incorrect data, you may receive a message indicating the type of error encountered with your CSV file. You can also reference the Foreseer Log Report for additional help.



If you would like to define and set user defined fields that include custom alarm properties, you can add additional field parameters to the CSV header. The format of the CSV file would be as follows:

Device,Channel,UDF1, UDF2, UDF3, HCR1, HCA1, LCR1, LCA1
Device1,Channelx,CustomValue1, CustomValue2, CustomValue3,12,13,14,15

Note that when you are constructing a CSV file:

1. Analog channels may contain up to four groups of five header (e.g. HCR1...up to HCR5, HCA1...up to HCA5, LCR1...up to LCR5, and LCA1...up to LCA5) for each alarm band.
2. Digital and Date channels will support only one header (e.g. HCR1...up to HCR5).

User Defined Fields - Updating Values using CSV

The Upload User Defined Values feature is not limited to initially defining values. You can update device properties, as well as channel properties within the same file. In order to do so, there are few considerations that must be taken into account when doing so.

1. If you wish to update device values, then leave the Channel Column value blank provided that values to be updated are listed in the subsequent column.
2. Keeping any field value blank in the CSV file will retain the old value for that particular device or channel.

3. If you want to discard any field value for a device or channel, specify the corresponding value as "DelUDF" (case-insensitive) in the CSV file.

User Defined Fields - Database Storage and Updates

All User Defined Fields and their respective values are stored into Foreseer's XRef database. The XRef database contains two database tables that retains and persists this information. They include the following:

- `dbo.UDFName` - contains all User Defined Field Name definitions as configured from the User Defined Fields dialog.
- `dbo.UDFValue` - contains all User Defined Field property settings for channels within the Foreseer server configuration.

User Defined Field data from a Stand-Alone or MoM will be written to the database anytime a change in name or value in the device or channel occurs. For data from a remote server, data will be written to the database upon exiting server configuration or performing a database fix.

You can update user defined values for a device or channel from a remote using channel properties in the same manner as if they were local devices and channels.

User Defined Fields - Primary/Redundant Architectures

In situations where a Primary/Redundant server architecture is utilized, a change to any device or channel property will result in the Redundant server being marked as "Needs Sync" when viewing servers in WebConfig. Property values between the Primary and Redundant servers will be synchronized after a [Synchronize Redundant](#) operation has been performed.

User Defined Fields - Property Values and Report Inclusion

User Defined Field data can be retrieved and viewed with select standard reports built into Foreseer when they are generated in CSV format. The following reports include User Defined Field data:

- System Configuration Report
- Channel Report when check boxes for Include Alarm Details, Include Alarm Limits, and Include Alarm Messages are selected.
- Custom Alarm Report when the Include User Defined Fields check box is selected.

Add Remote

A local Foreseer Server can serve as host to a remote Foreseer Server (or an Outpost), expanding and enhancing system monitoring capabilities. Remote servers offer a unique advantage of distributing the acquisition of data.

A remote server using Outpost includes data buffering capabilities that prevent against the potential loss of high and medium resolution historic data. A remote server using Outpost will buffer up to 72-hours of historic data. In the event of a loss in communications exceeding more than 30 seconds, the local server will automatically back-fill gaps in historic data with buffered data collected by Outpost.

When you add a remote, 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.

✔ Administrative Authorization is required before proceeding with this command.

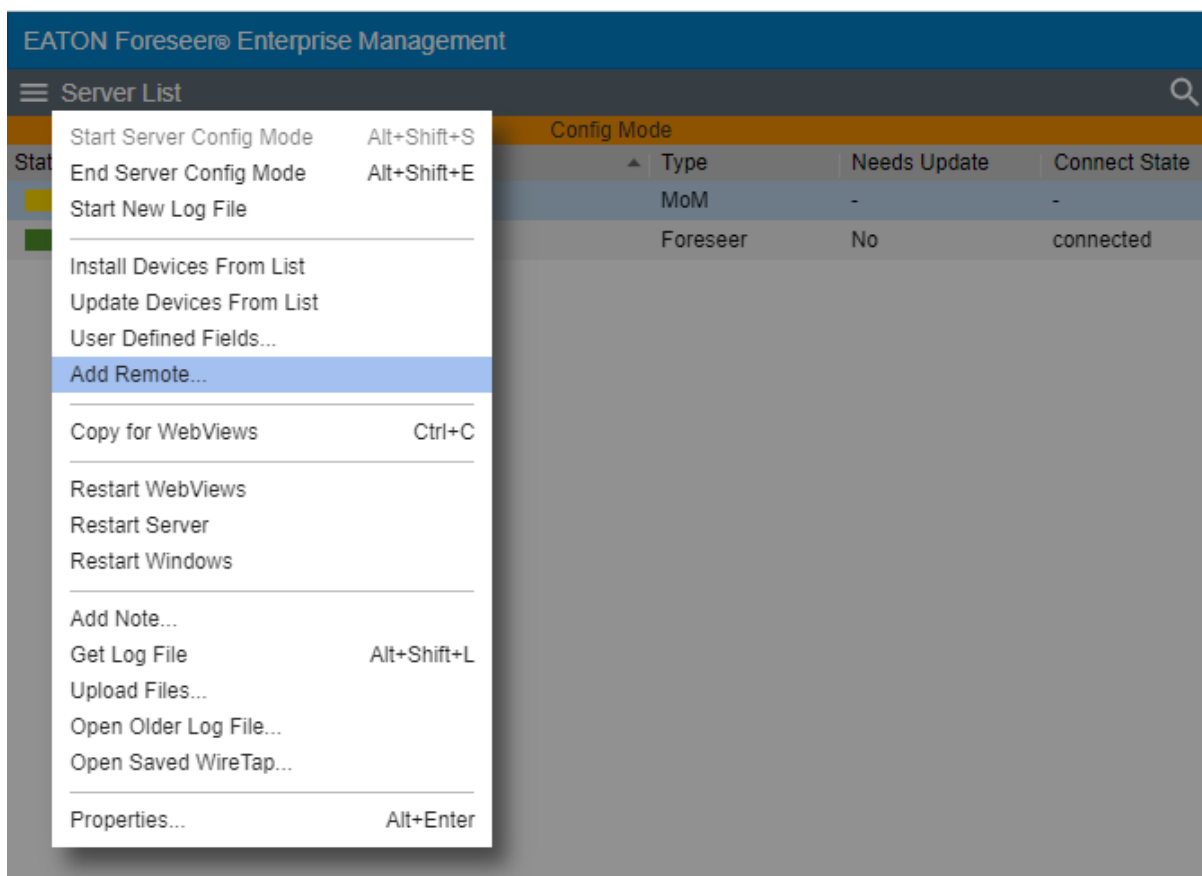
✔ Server Config mode must be active to run this command. Activate Config mode by right-clicking server and selecting Start Server Config Mode. The **** CONFIG MODE **** message should be displayed above the tree.

✔ The local Foreseer Server and Remote Server must be at the same software revision in order to fully communicate and exchange data.

If you upgraded your local Foreseer server from a prior software revision, ensure that your Remote Server has been updated before adding.

To add a remote server:

1. Select Add Remote in the Server List menu.



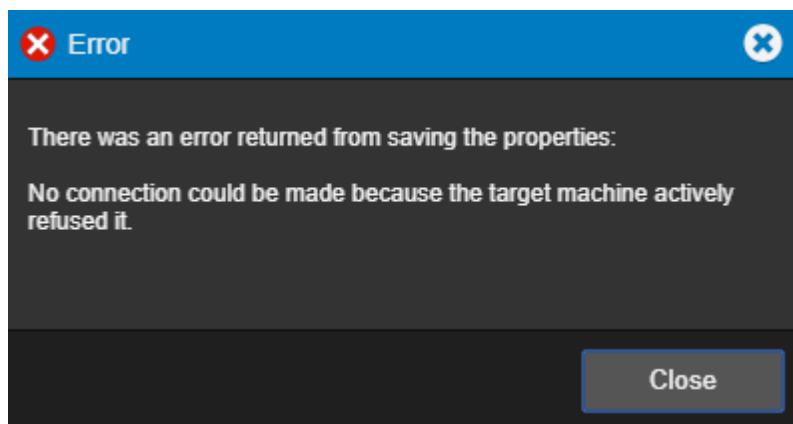
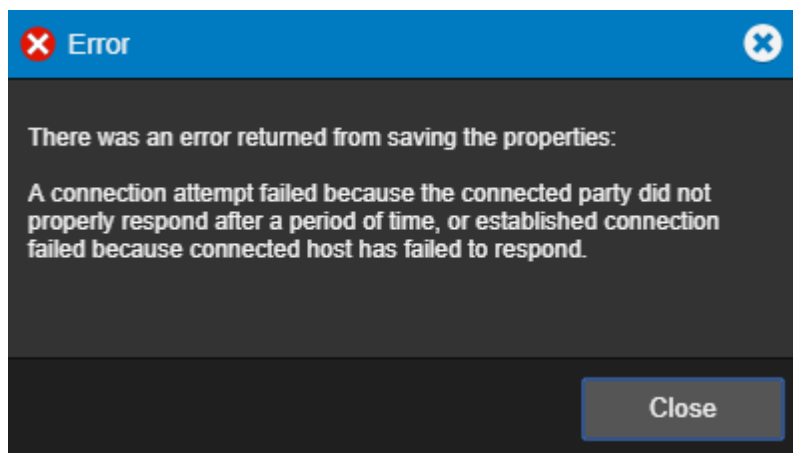
2. Identify the remote server by entering its Name and Remote Address; requiring Connection Password security is optional. If a password is specified for remote server access, the password must be entered a second time in the Verify Password field. If no password is specified, it defaults to "special".

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.

Buffered Data Retrieval

Remote servers (such as Foreseer Outpost) added to a MoM are automatically enrolled into Foreseer's Buffered Data Retrieval capabilities. Buffered Data Retrieval operations occur in situations where Foreseer may lose connectivity with the Remote for more than 30 seconds, potentially causing a loss of collected historical data.

Upon the device returning to a normal connected status, Foreseer will attempt to back fill gaps in high resolution and medium resolution historic trend data using data buffered by the Remote. A maximum of 72-hours of back fill data is supported by a Remote using Outpost.

No additional setup or configuration is necessary to enable this feature aside from ensuring that the remote is successfully added.

Buffered Data Retrieval Operations and Troubleshooting

Buffered Data is continually collected by a Remote server. Periodically, clean-up activities will be carried out automatically to preserve storage space and performance. If a Remote

server is removed or deleted from a MoM, clean-up activities will cease.

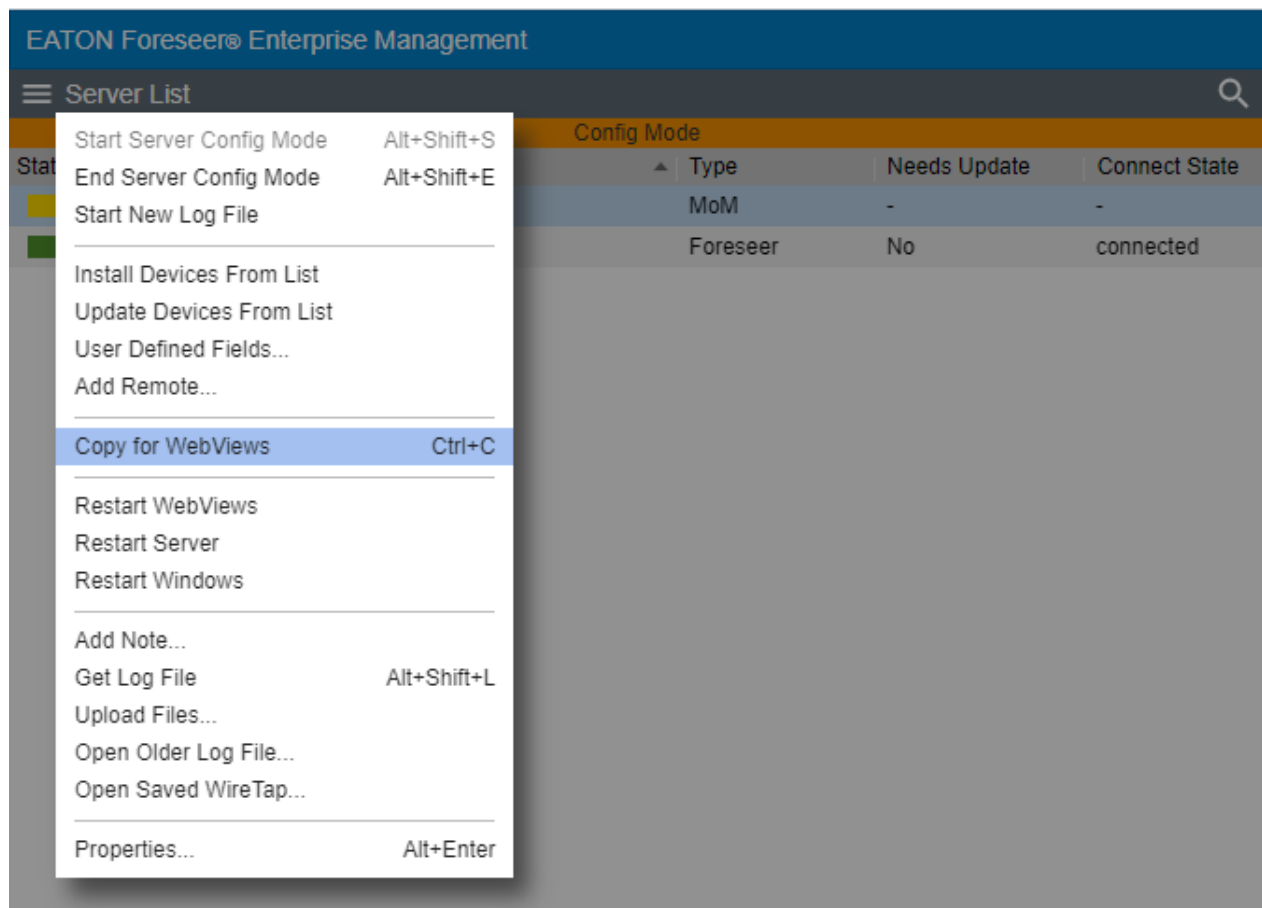
It is vital and important to ensure that timezone configurations between a Remote Server and MoM be in parity to ensure data is back filled properly. A different in time zones will disqualify back filling of buffered data. Time should also be synchronized as well to avoid incorrect data being back filled or nullified.

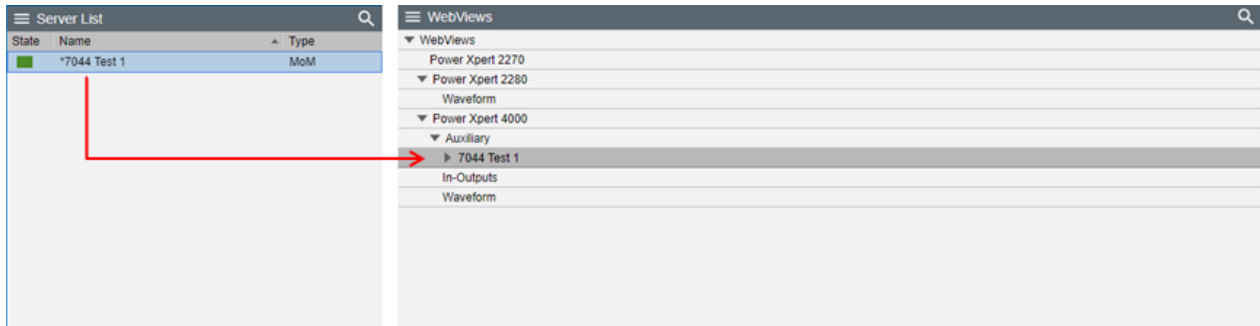
All device-based trend/historic data requested by Foreseer is stored into a new table in the *XRef* database named ***dbo.BackfillData***. The table contains all sample data requested that will be processed into Foreseer's high and medium resolution databases.

In situations where an SQL transaction fails to insert a record into high resolution or medium resolution tables, a table in the *XRef* database named ***dbo.BackfillErrorLog*** will contain error messages indicating why a failure may have occurred. This table will be automatically cleaned each time a new High Resolution database is created (typically at the beginning of a new month). Clean-up scripts will periodically check the database for data older than 90 days. If found, the older data will be deleted.

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.



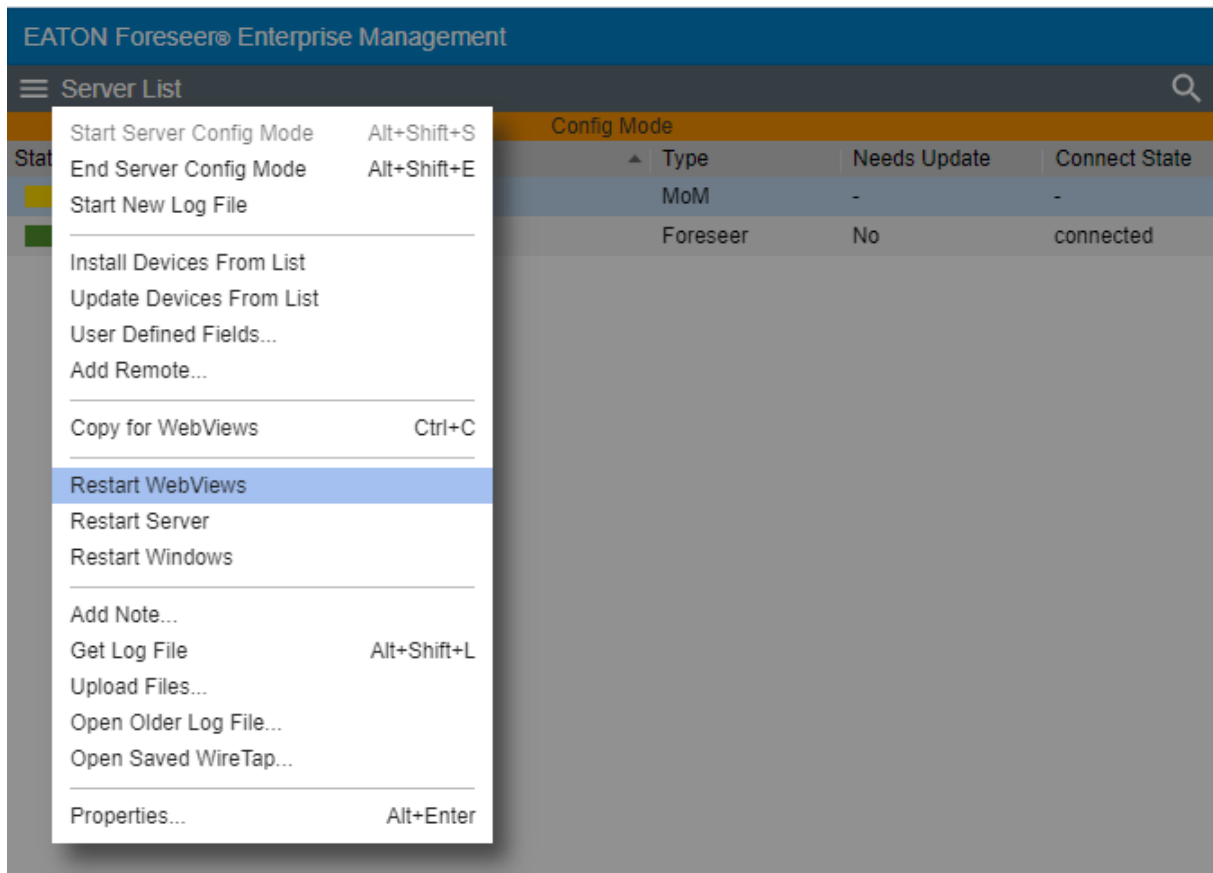


In the example shown above, “WebViews Copy”, the Local server is copied and then pasted into the Power Expert 4000 folder under WebViews. Note that the folder structure mimics the device structure under the server. Instead of copying the entire server, you can also copy individual devices and their channels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

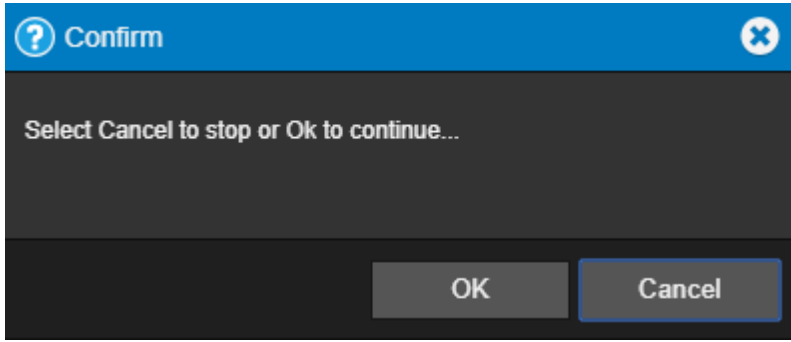
Restart WebViews

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.



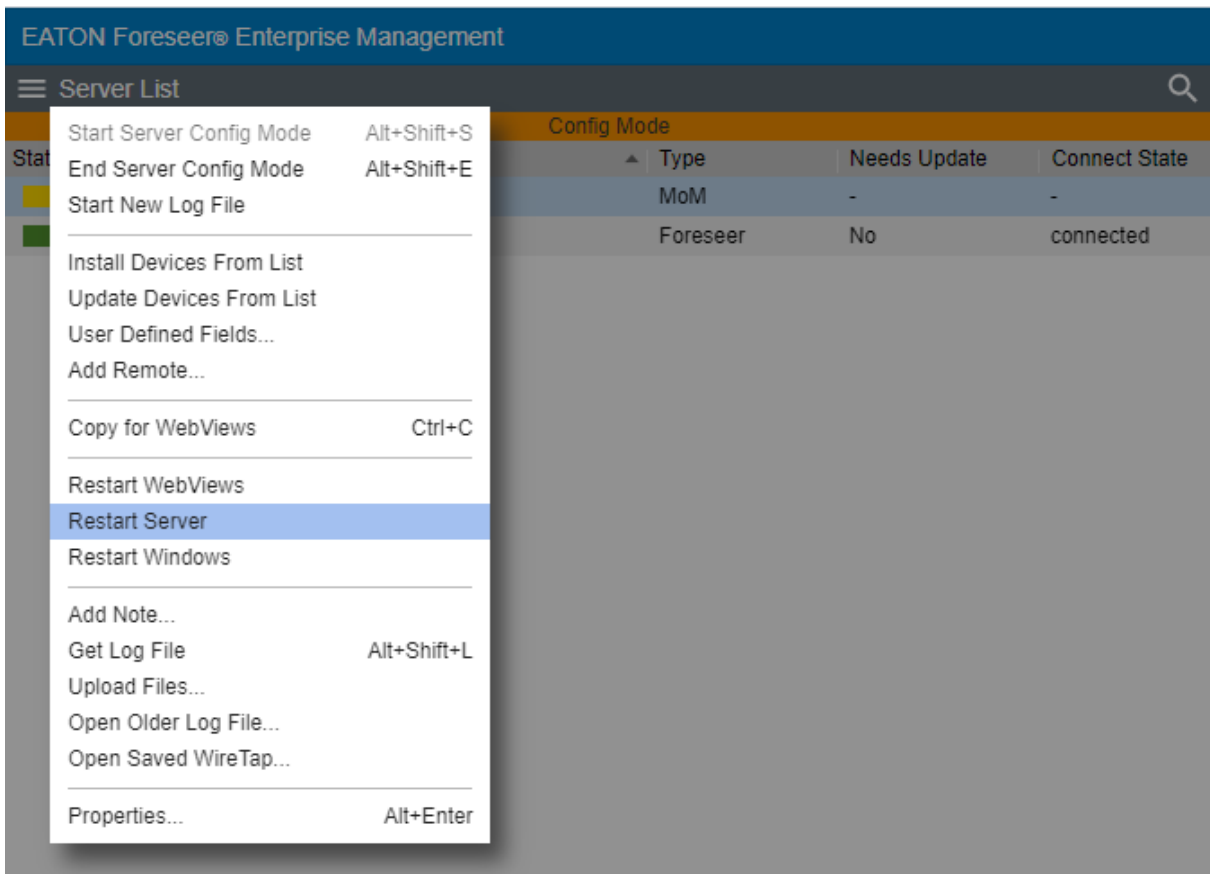
2. Select OK to continue or Cancel to stop



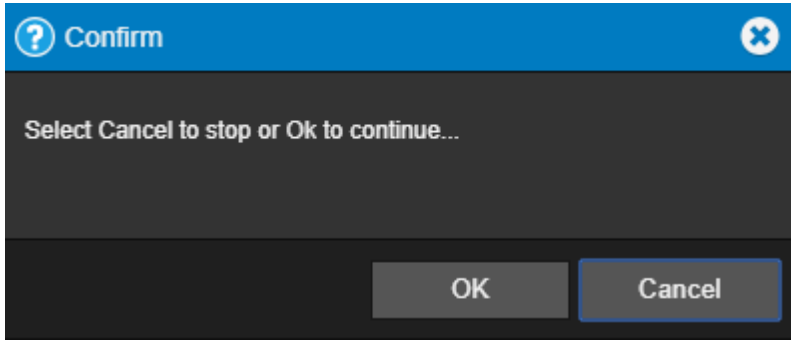
Restart Server

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.



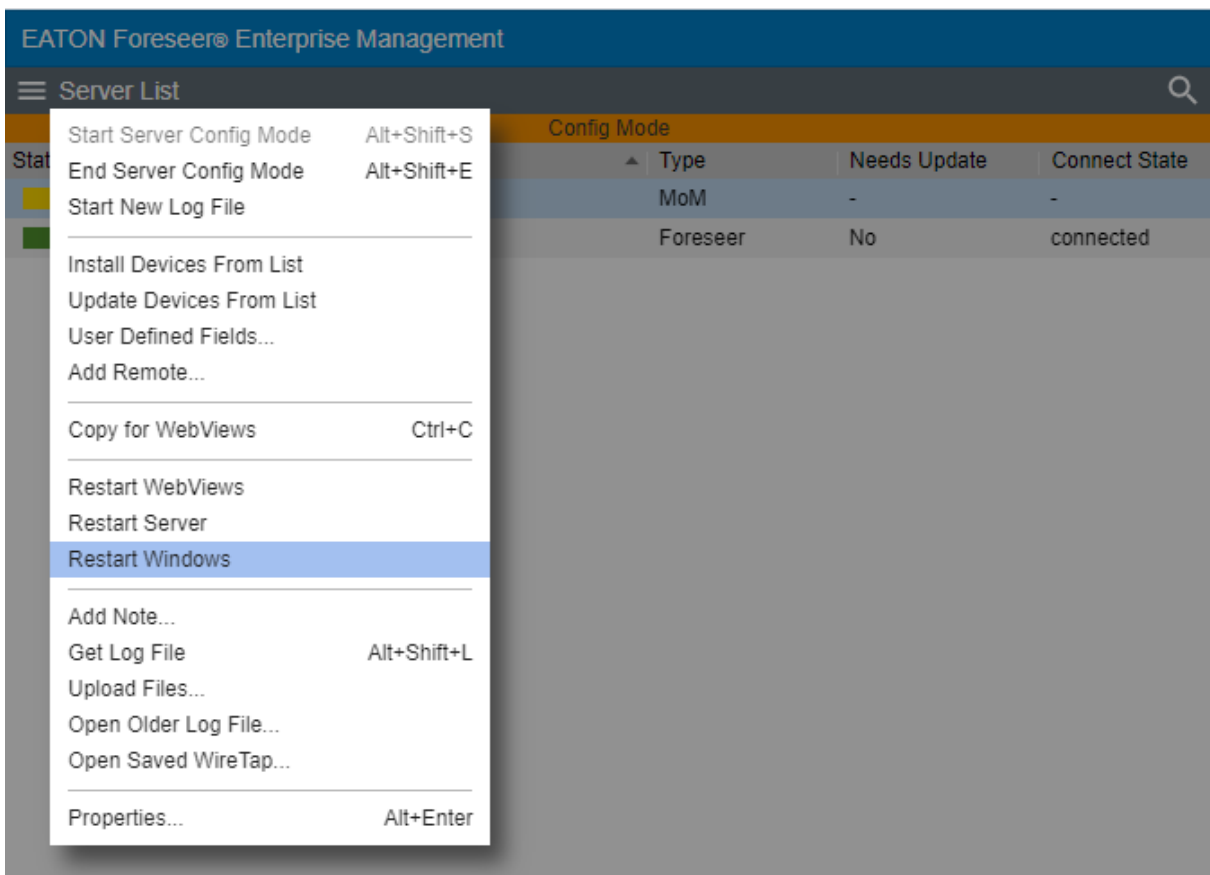
2. Select OK to continue or Cancel to stop



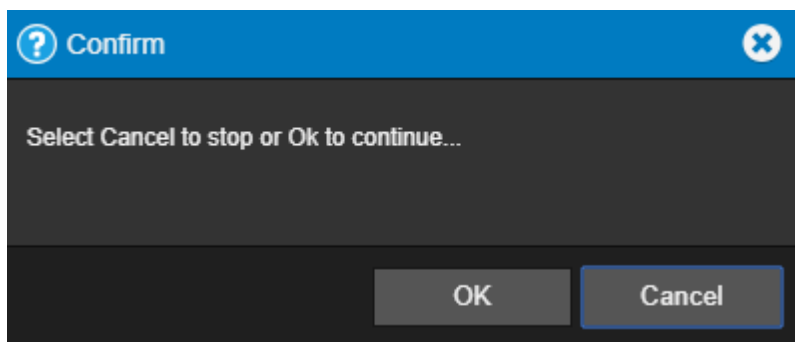
Restart Windows

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

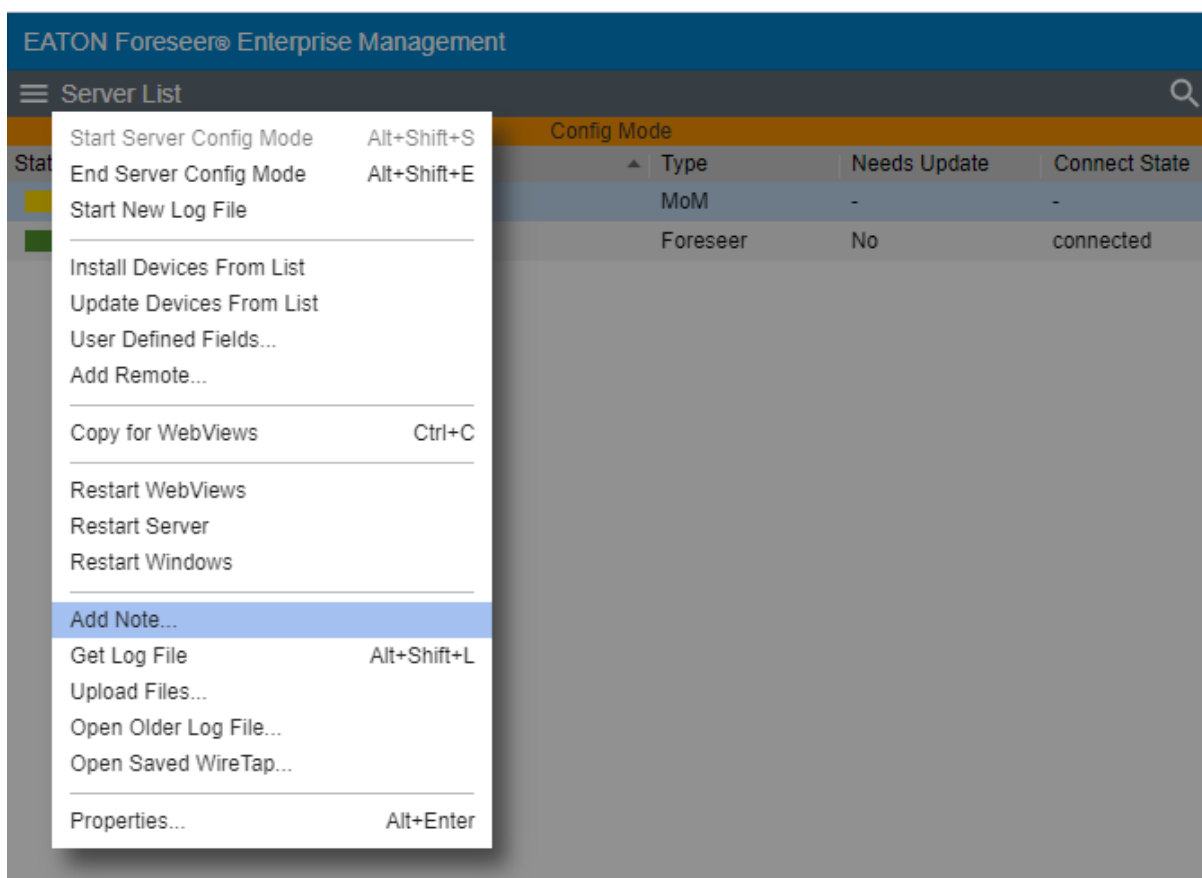


Add Note

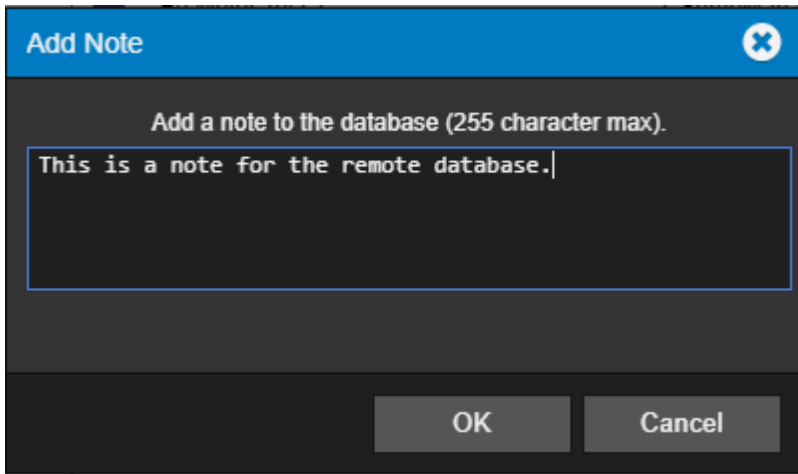
You can use the Add Notes feature to record any supplemental information relevant to a particular event when it occurs. The notes are logged into the Server's database and can be reviewed by authorized Foreseer clients or retrieved in Foreseer Reports. An unlimited number of real-time notes may be entered, 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:

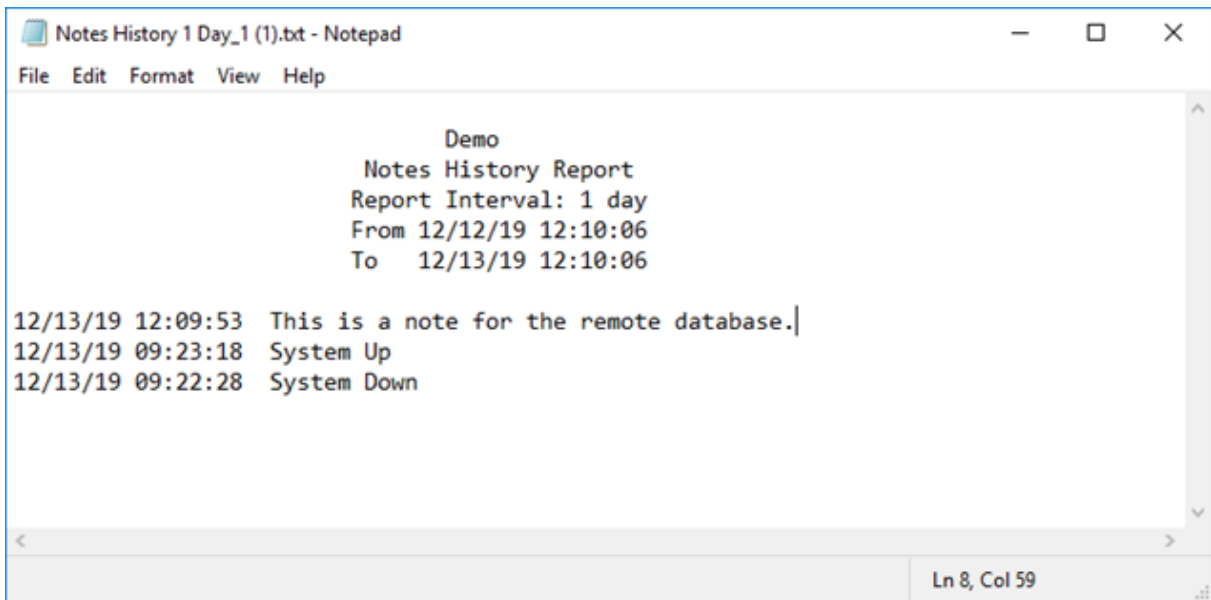
1. Select Add Note from the Server List menu



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

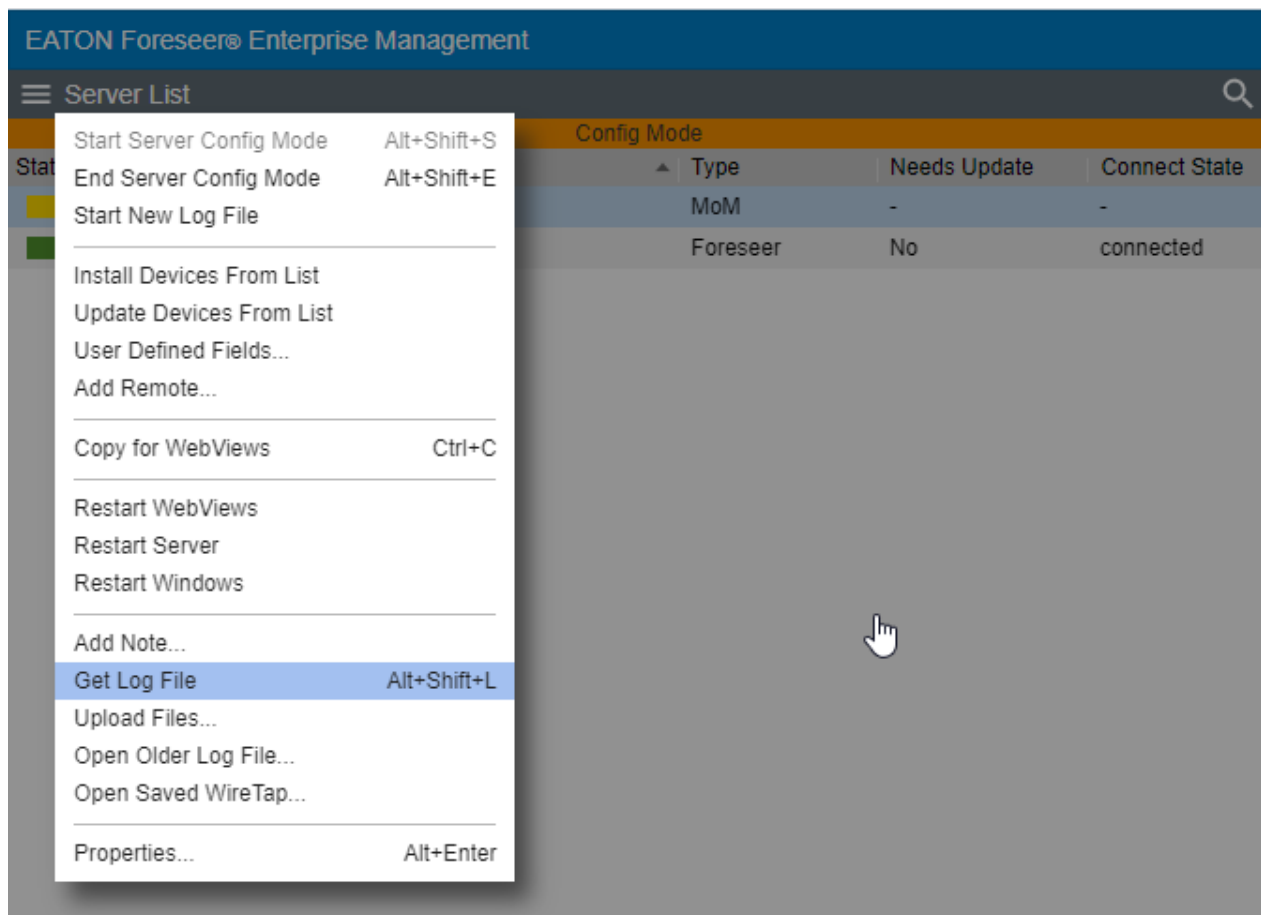


3. Select OK to continue.
4. The database note can now be reported on in the Notes History Report.



Get Log File

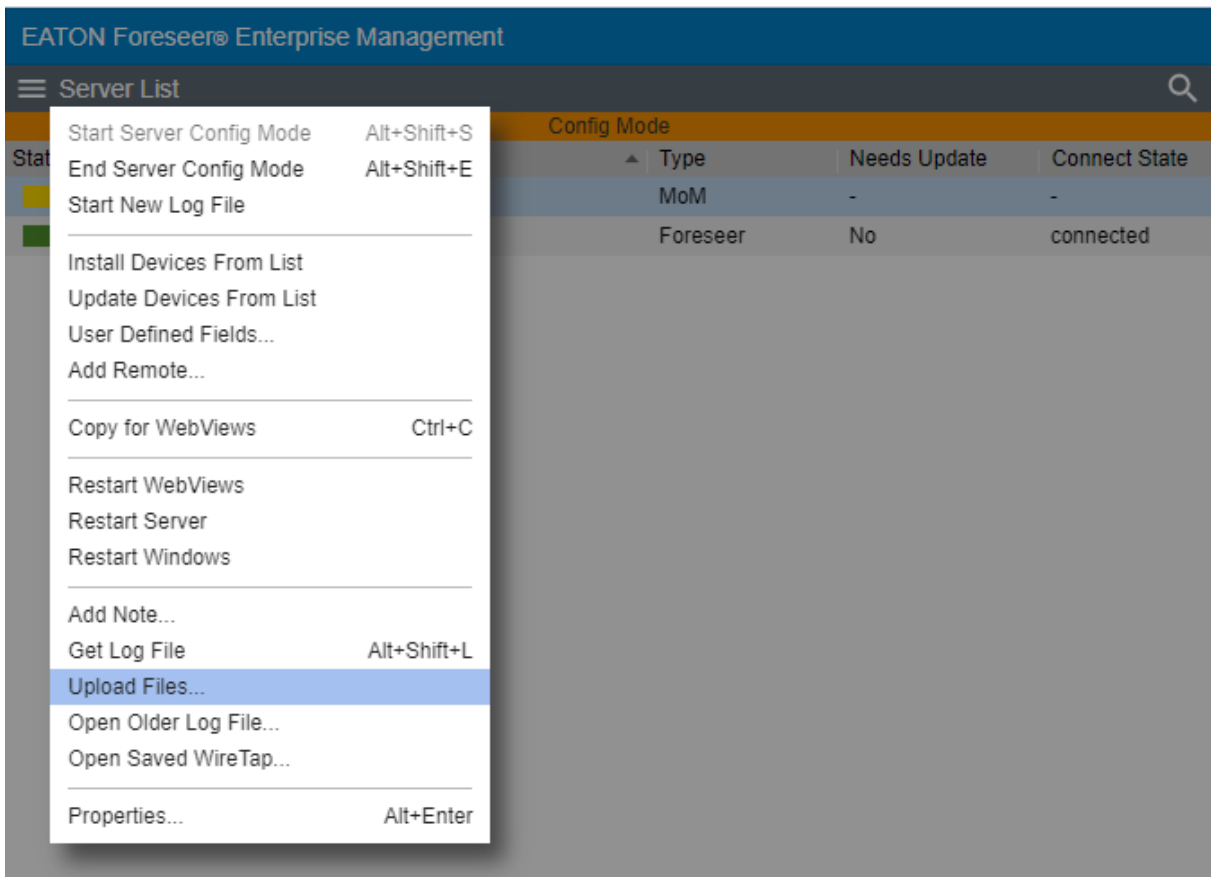
Get Log File will obtain the current Log File Report from the server.



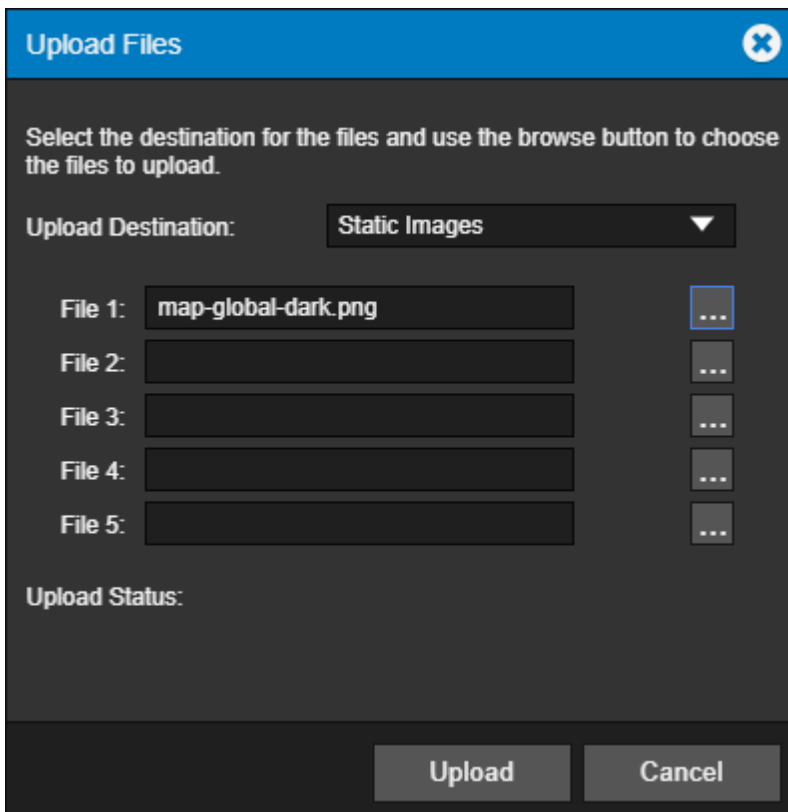
Upload Files

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. Using this feature, you can upload common files used by Foreseer including .VI driver files, and .ARQ backups for restoration purposes.

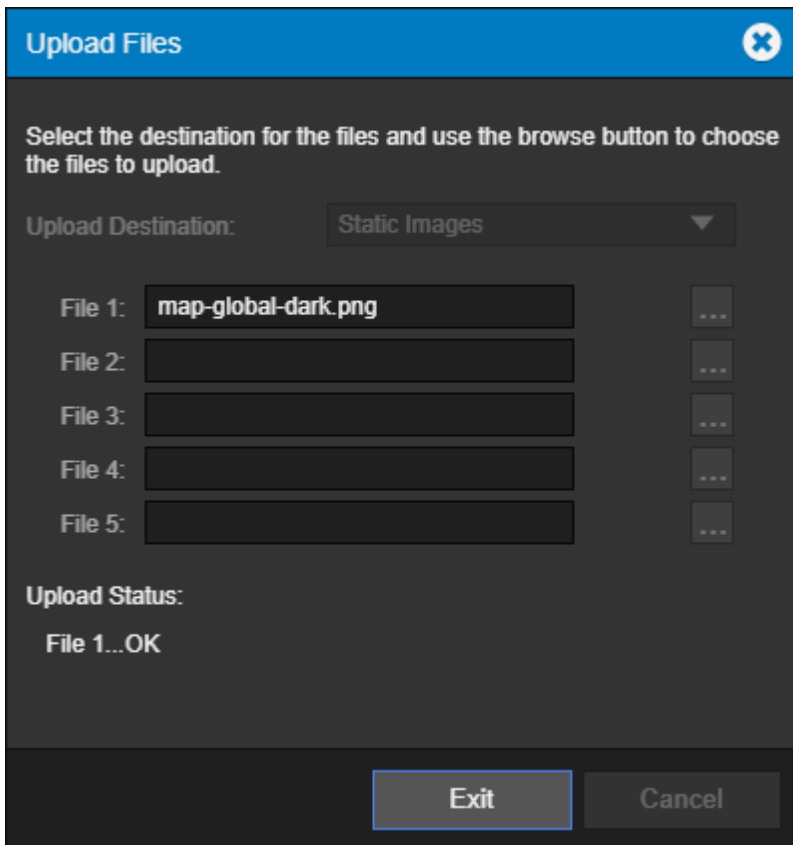
1. Select Upload Files from the Server List menu.



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

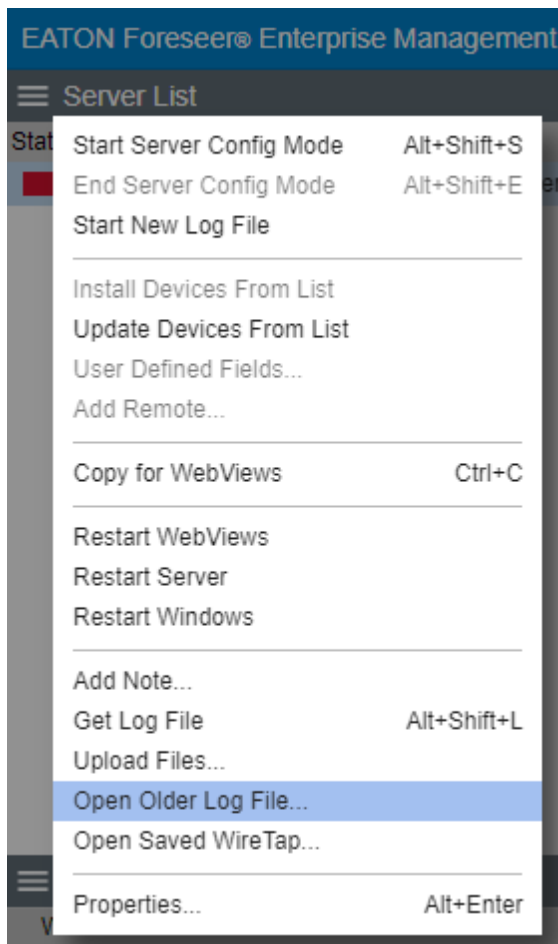
Upload destinations include:

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

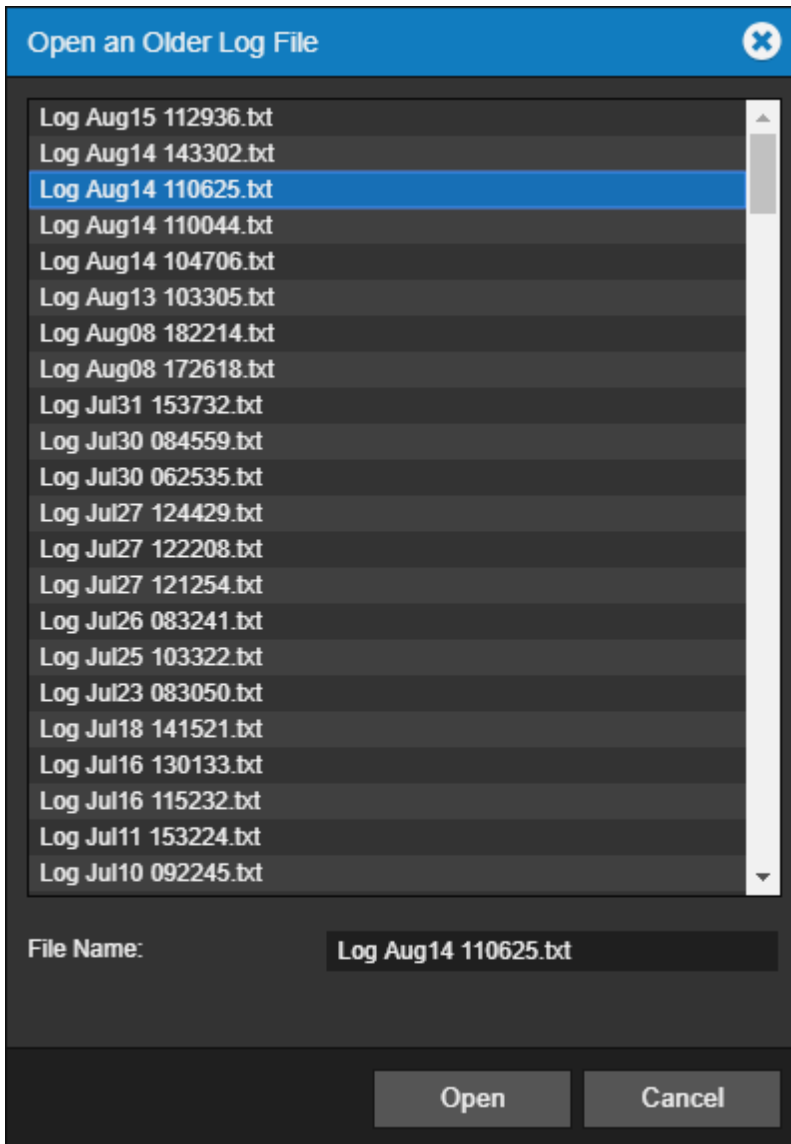
Open Older Log File

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.

```

Eaton Foreseer logfile - Log Aug14 110625.txt - Google Chrome
//localhost/React/download.py?file=Log%20Aug14%20110625.txt&type=logfile

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

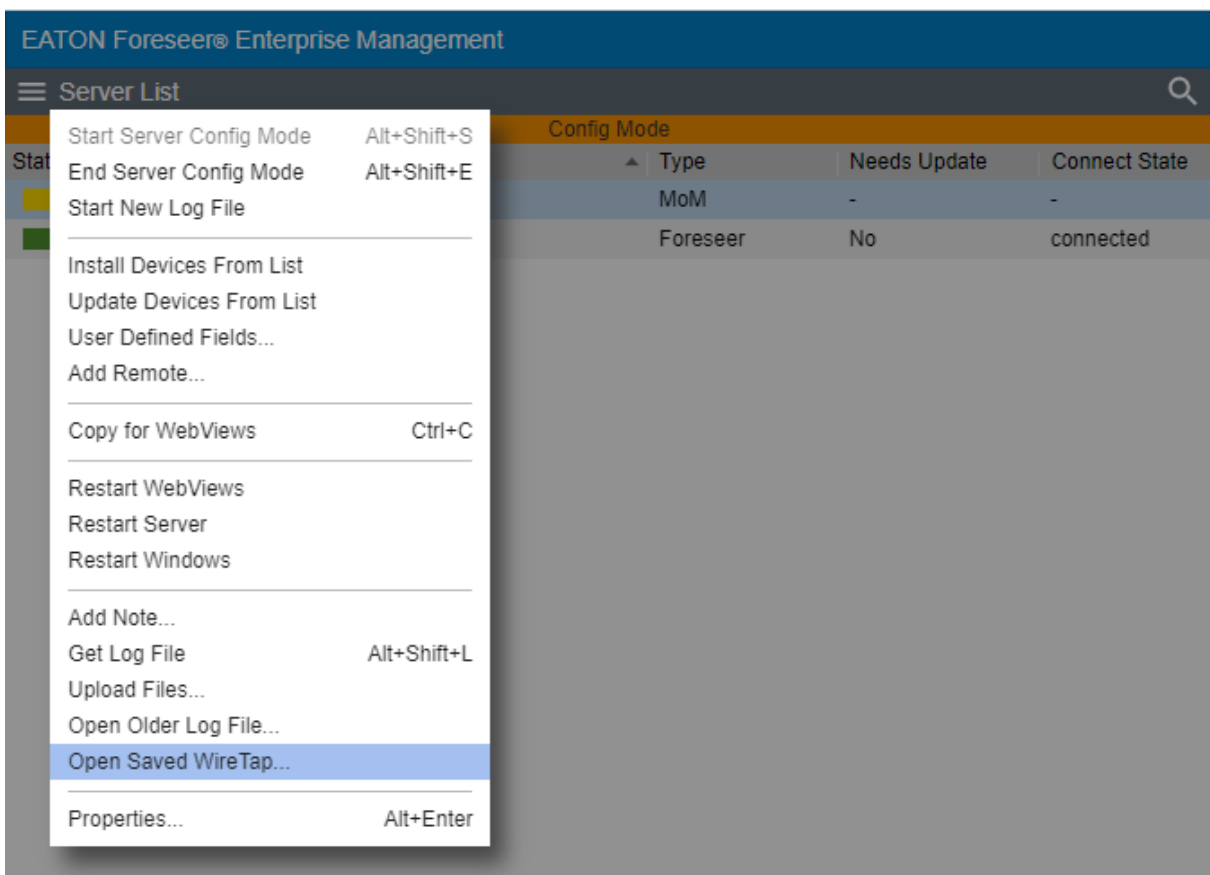
08/14/18 10:47:06: Initializing Eaton Foreseer, Version: 7.0.54.0
08/14/18 10:47:06: Working directory: C:\Foreseer\Branches\Foreseer 7R\BUILD\x64\Release\
08/14/18 10:47:06: Running as an application
08/14/18 10:47:06: ServiceThreadProc thread started with thread id: 0xdc8
08/14/18 10:47:07: Initializing 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.

```

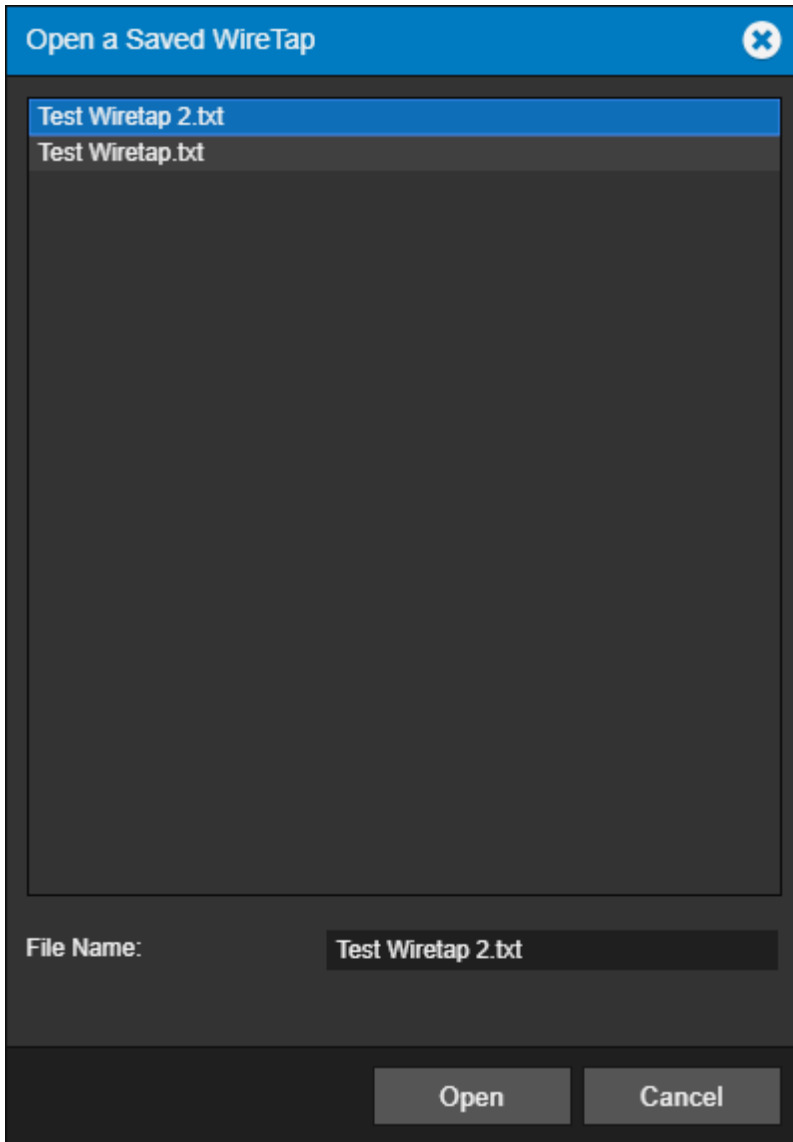
Open Saved Wiretap

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

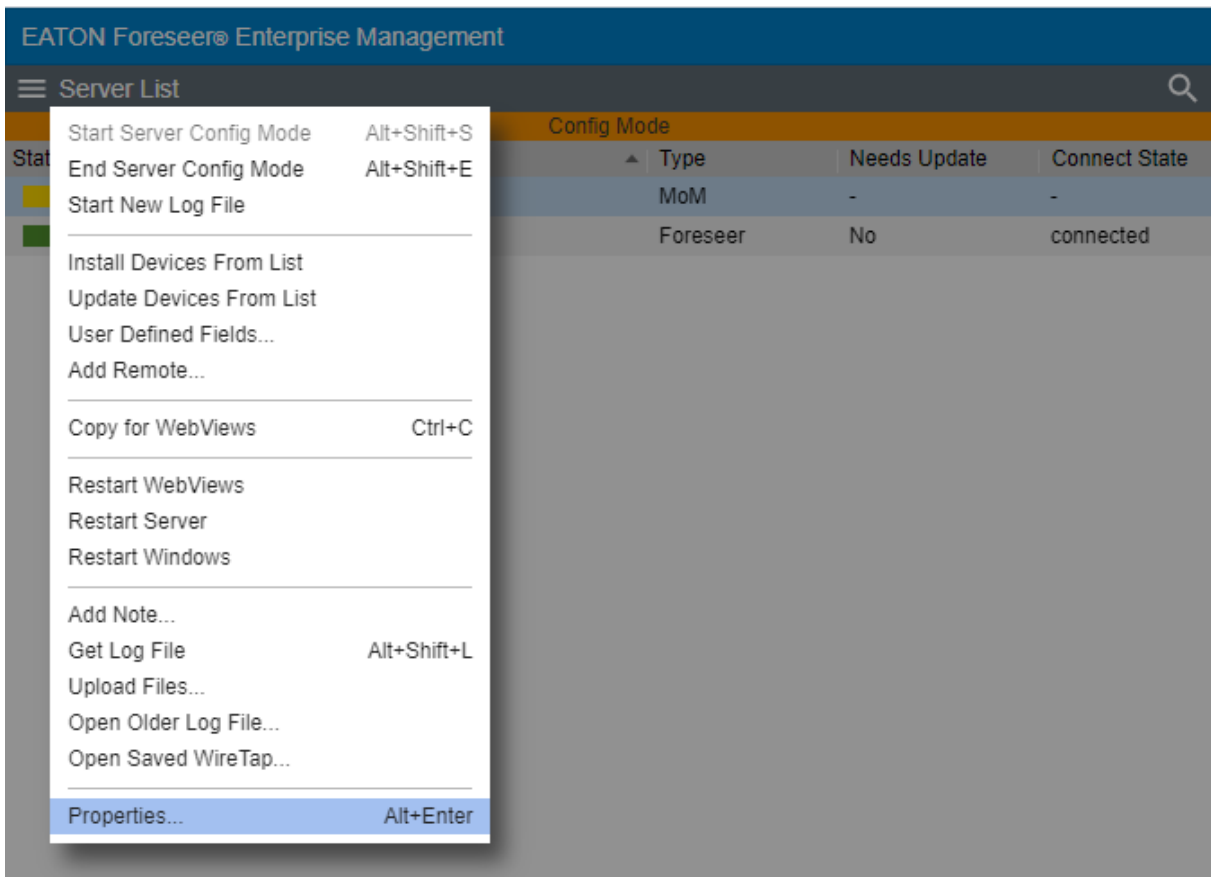
XMIT 12 bytes (16:42:35, 125 ms since last message)
 \81\AE\00\00\00\06\01\03\03\E7\00\36 [.....6]
RECV 9 bytes (16:42:35, 0 ms since last message)
 \81\AE\00\00\00\6F\01\03\6C [....o..1]
RECV 108 bytes (16:42:35, 0 ms since last message)
 \43\8A\8F\87\43\8A\5B\37\43\8A\39\27\43\F0\AD\12\43\F1\2D\F0\43\F1\2D\33\42 [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)

```

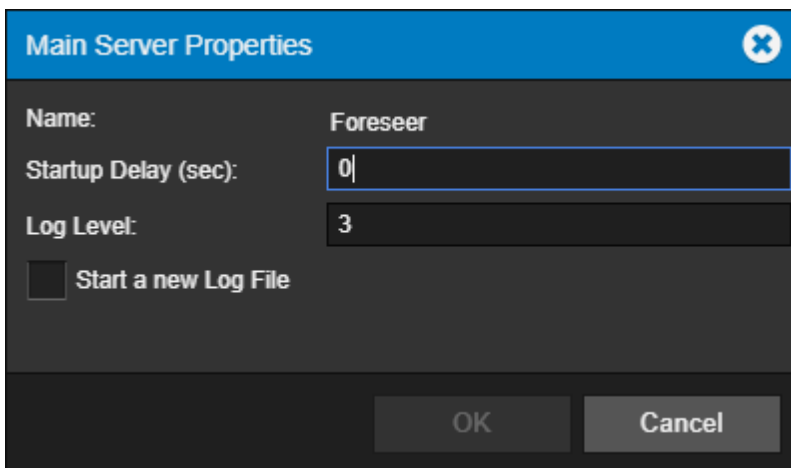
Properties

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

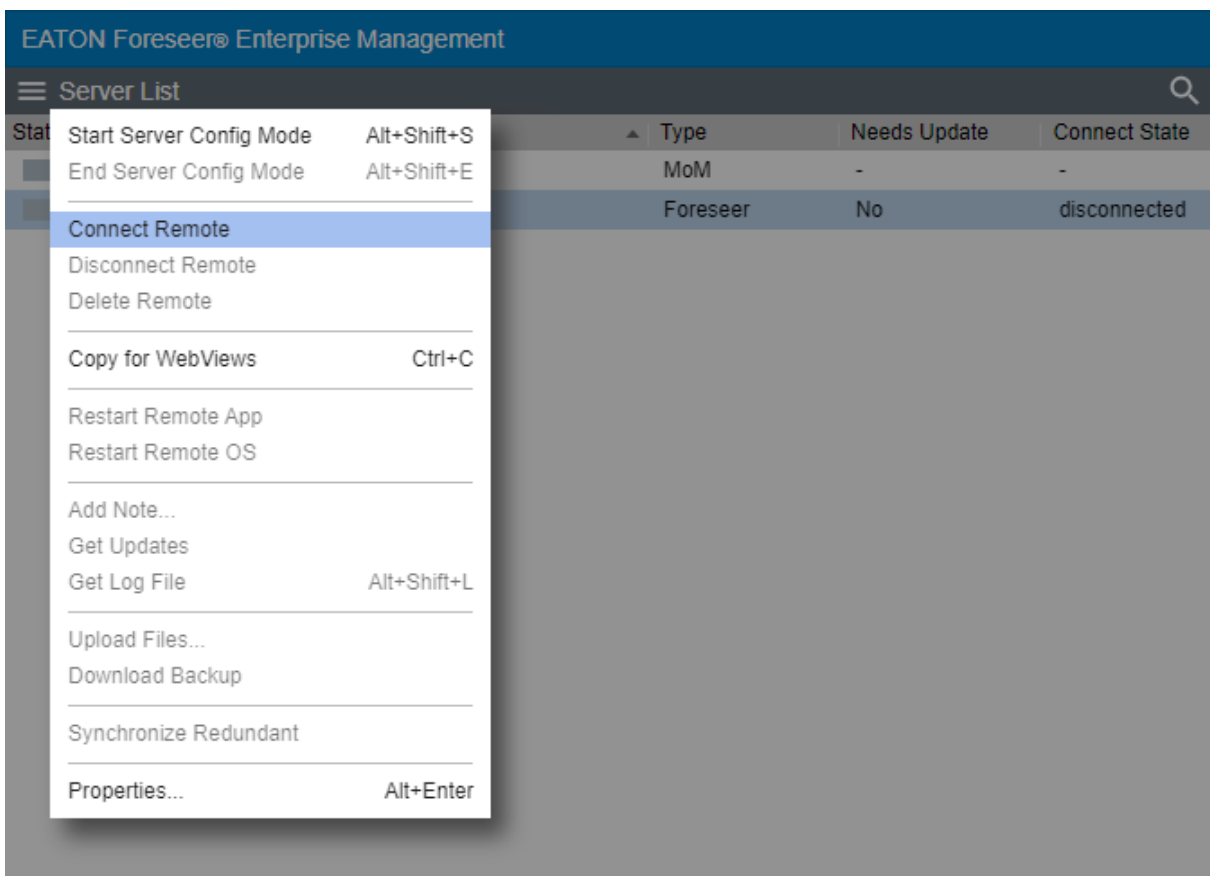
The Remote Server List menu provides access to all of the functionality that will be required to manage your Remote / Redundant Foreseer servers.

- 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.



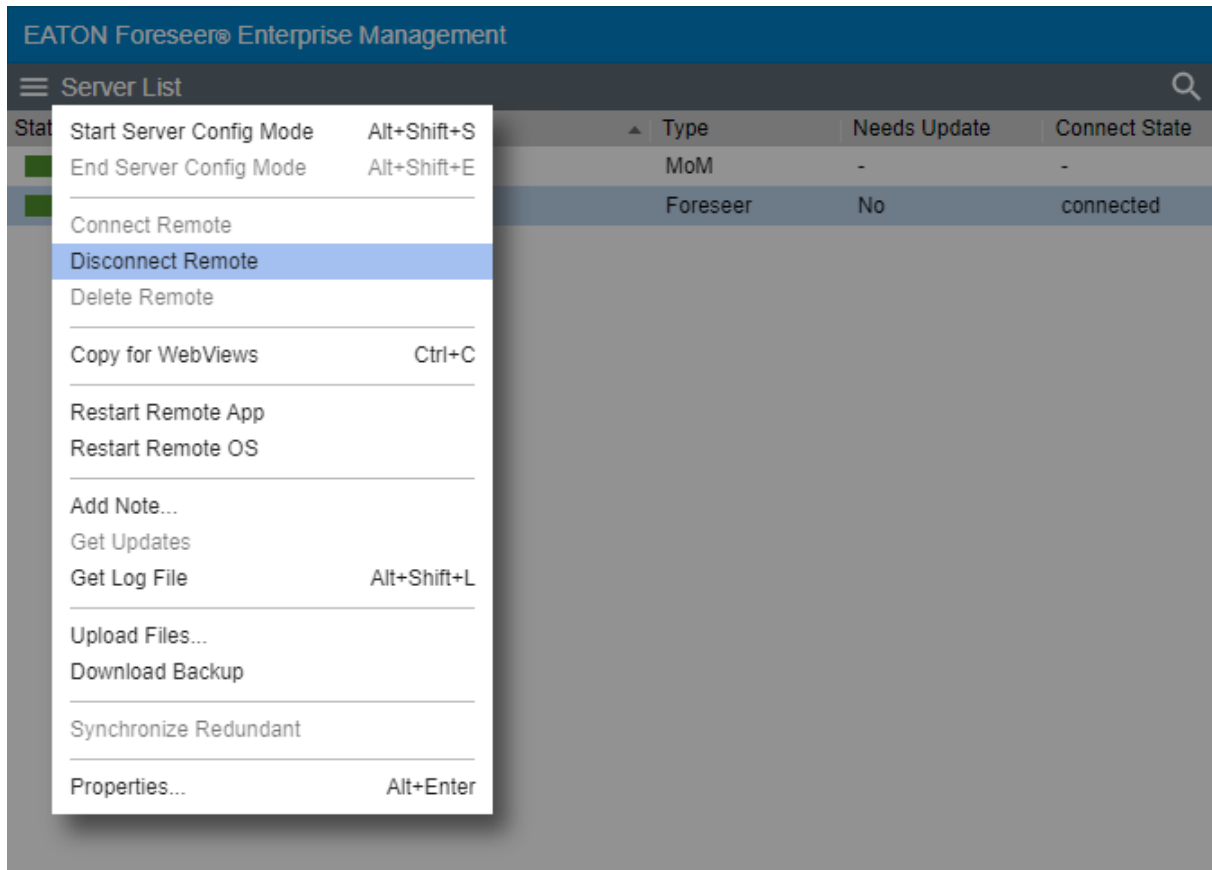
2. The remote server will now be connected to the local server

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.



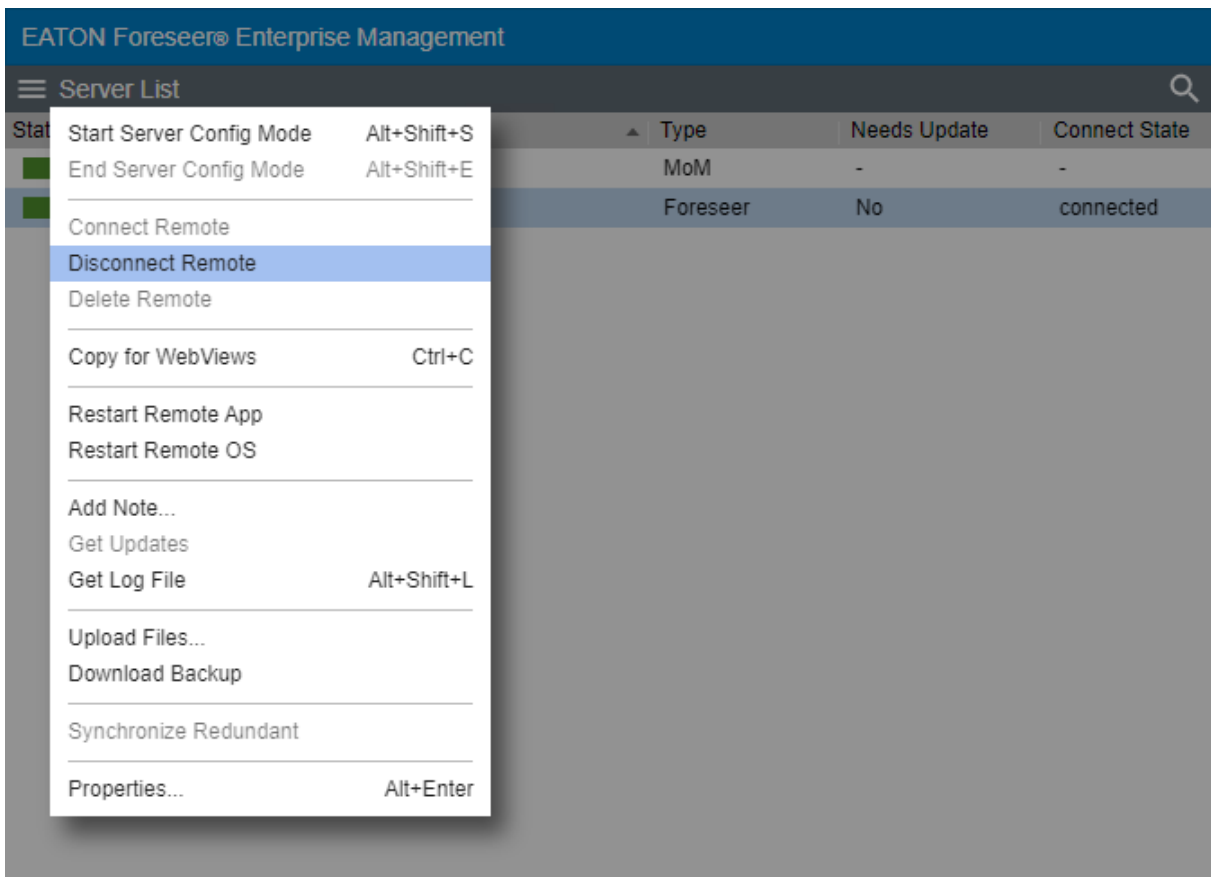
2. The remote server will now be disconnected from the local server

Delete Remote

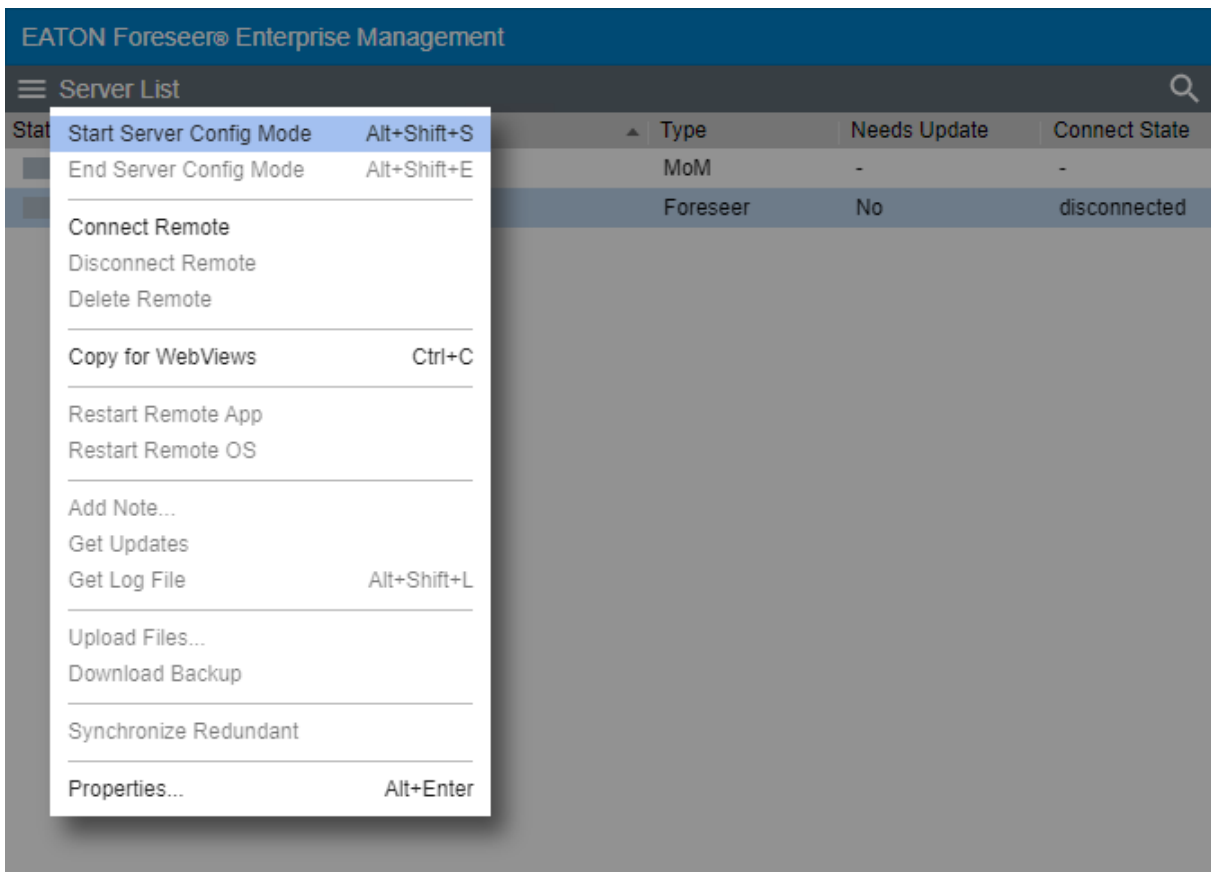
The Delete Remote function deletes the Remote Foreseer server from the local server.

To delete the remote server:

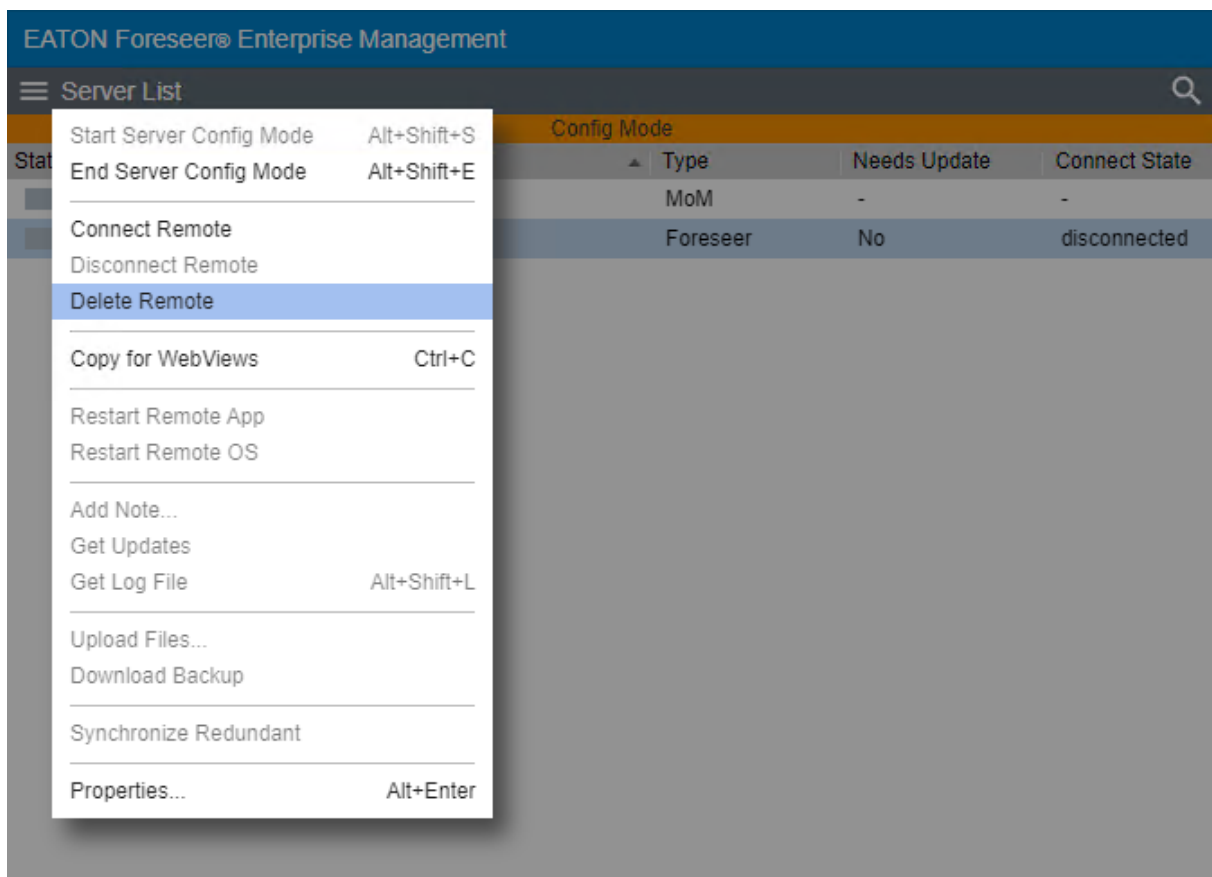
1. Select Disconnect Remote from the Server List menu.



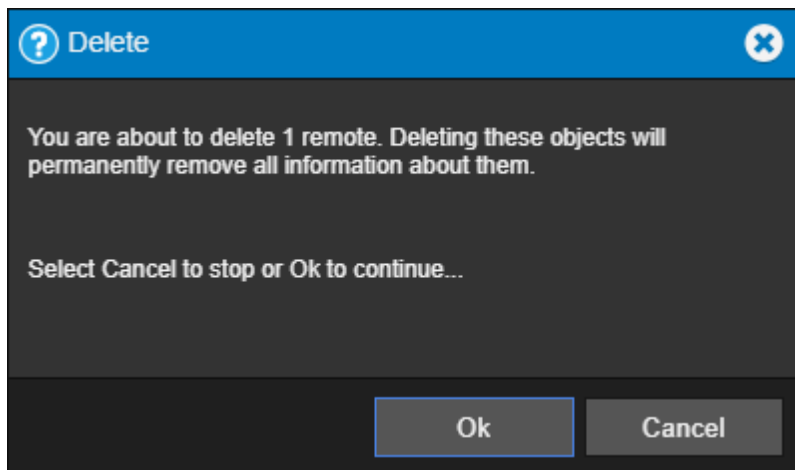
2. Select the local server and Start Server Config Mode



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

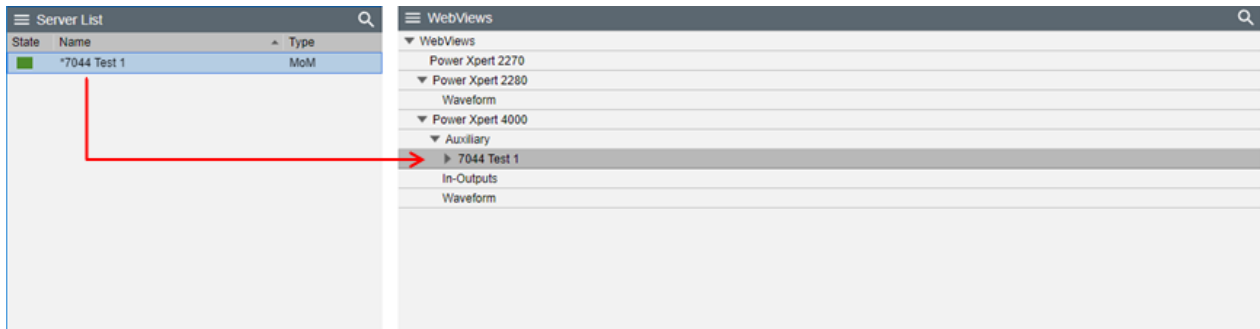


4. A confirmation dialog will appear. Click OK to continue.



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.

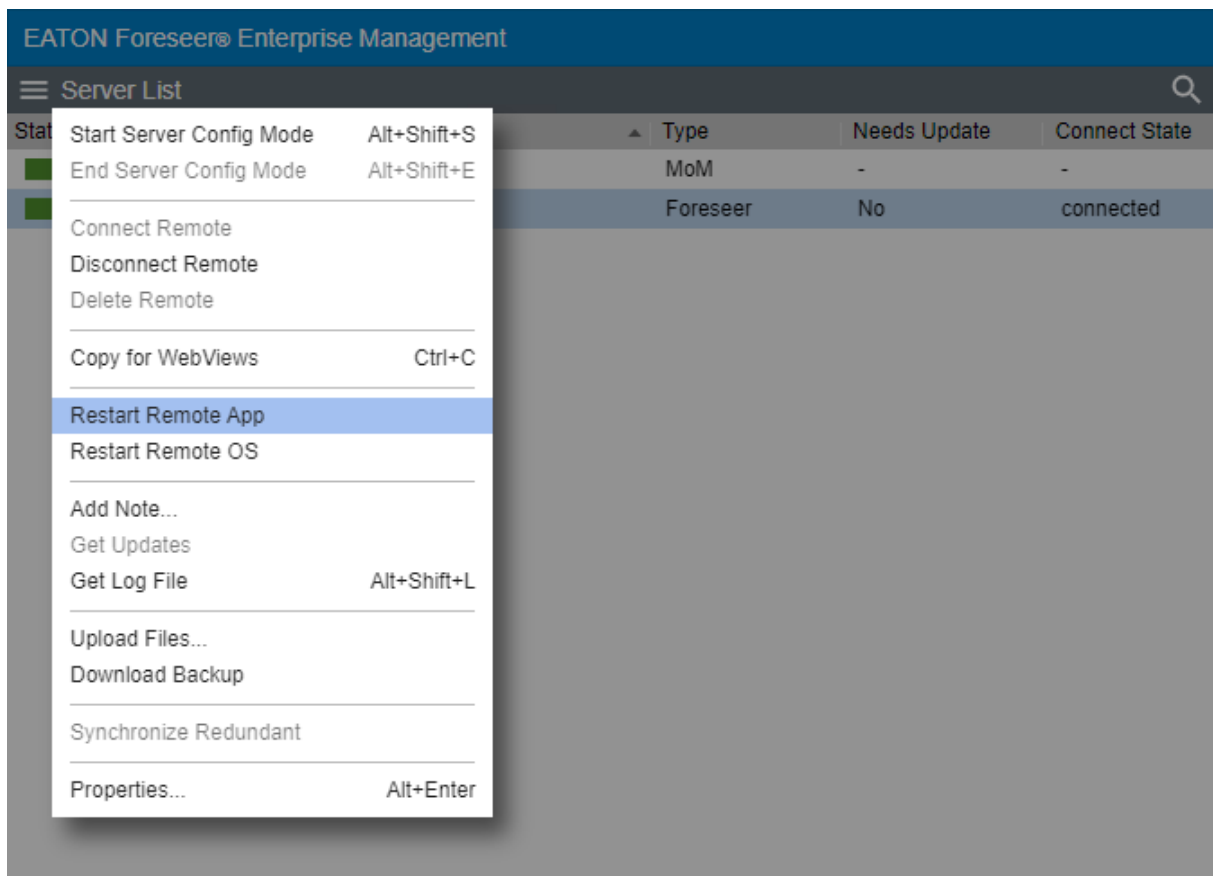


In the example shown above, “WebViews Copy”, the Local server is copied and then pasted into the Power Expert 4000 folder under WebViews. Note that the folder structure mimics the device structure under the server. Instead of copying the entire server, you can also copy individual devices and their channels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

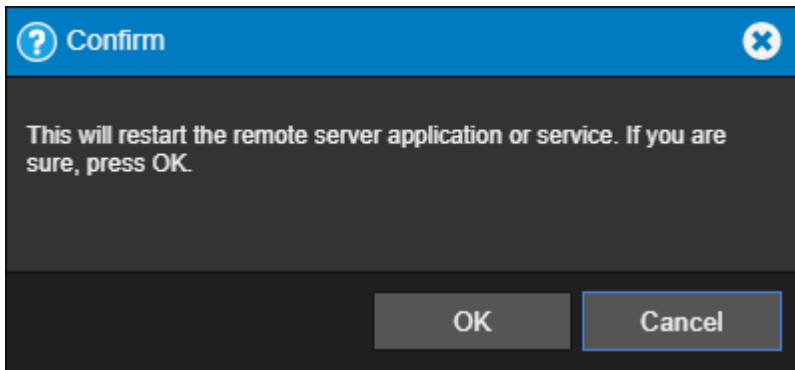
Restart Remote App

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.



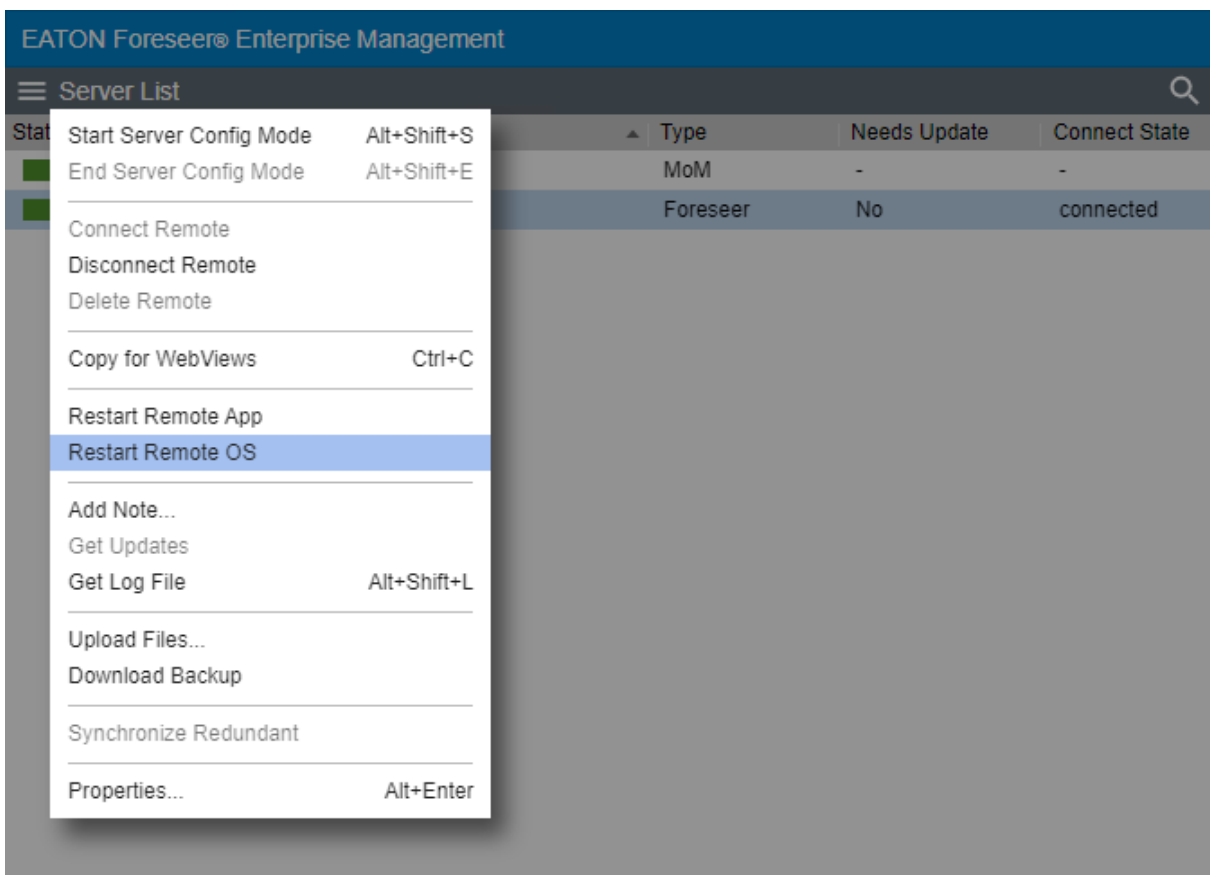
2. Select OK to continue this request.



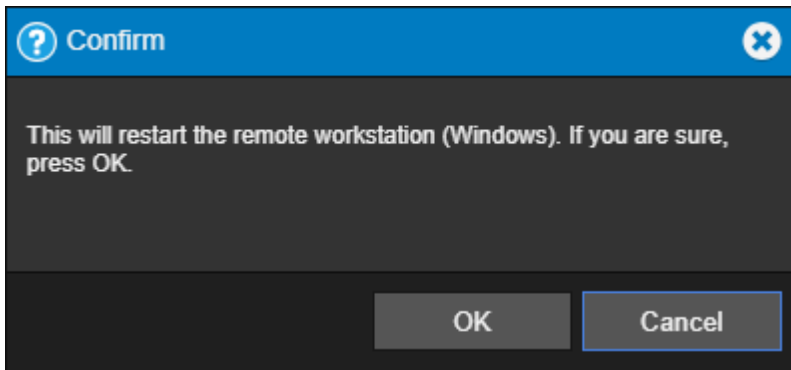
Restart Remote OS

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.

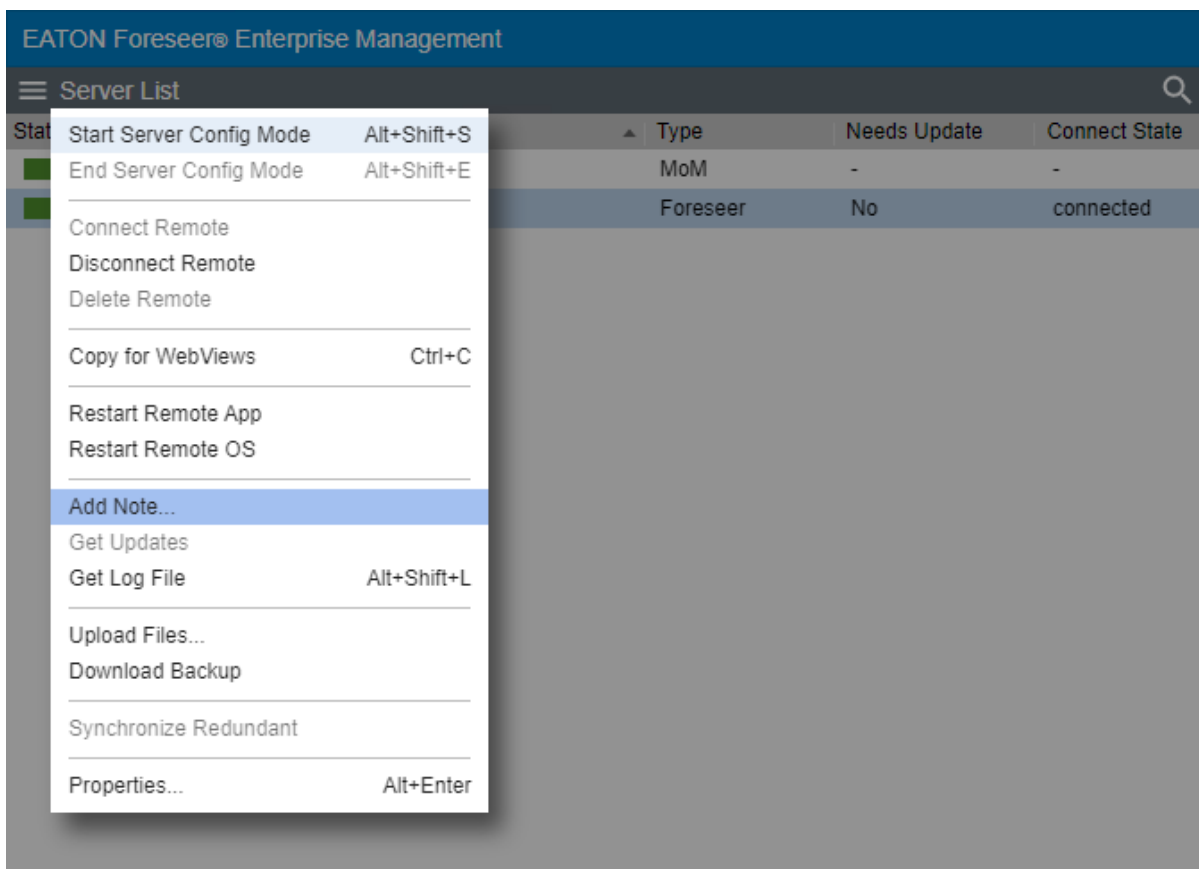


Add Note

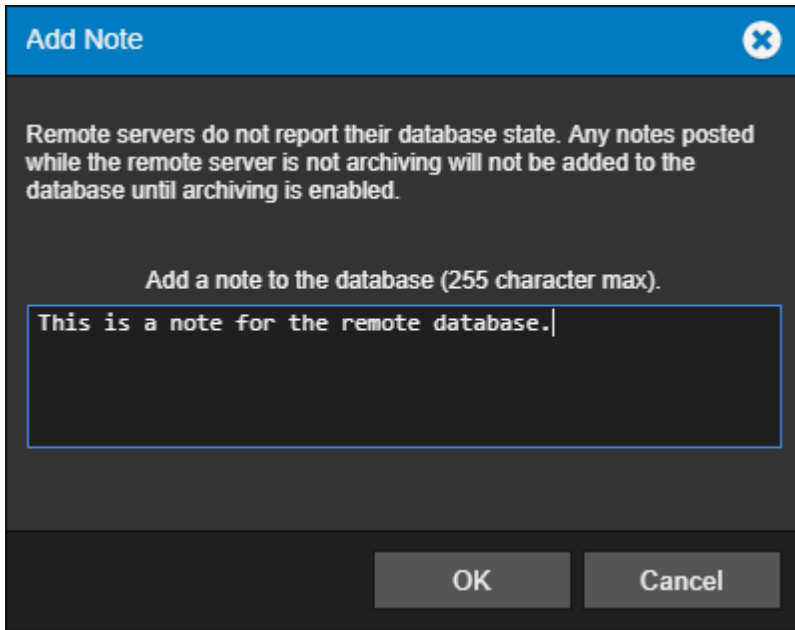
You can use the Add Notes feature to record any supplemental information relevant to a particular event when it occurs. The notes are logged into the Server's database and can be reviewed by authorized Foreseer clients or retrieved in Foreseer Reports. An unlimited number of real-time notes may be entered, 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:

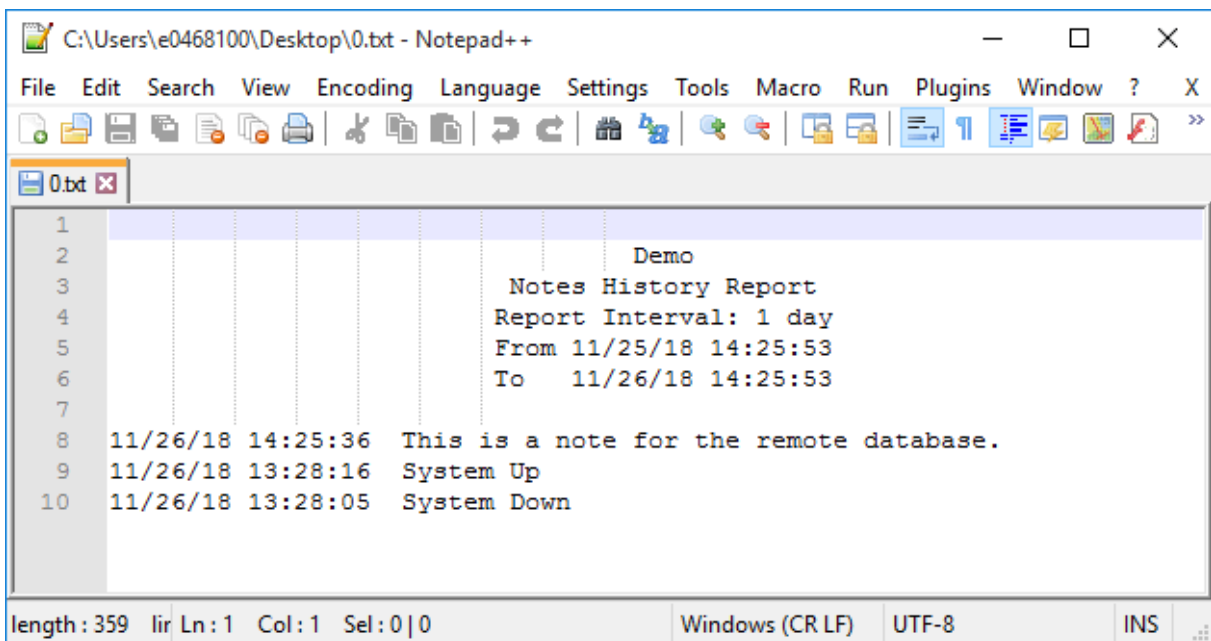
1. Select Add Note from the Server List menu



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

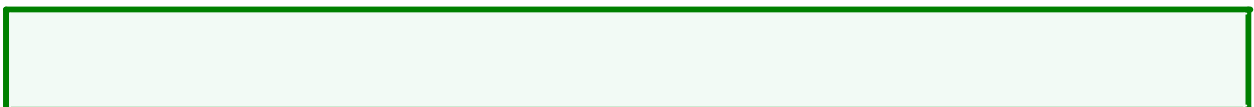


3. Select OK to continue.
4. The database note can now be reported on in the Notes History Report



Get Updates

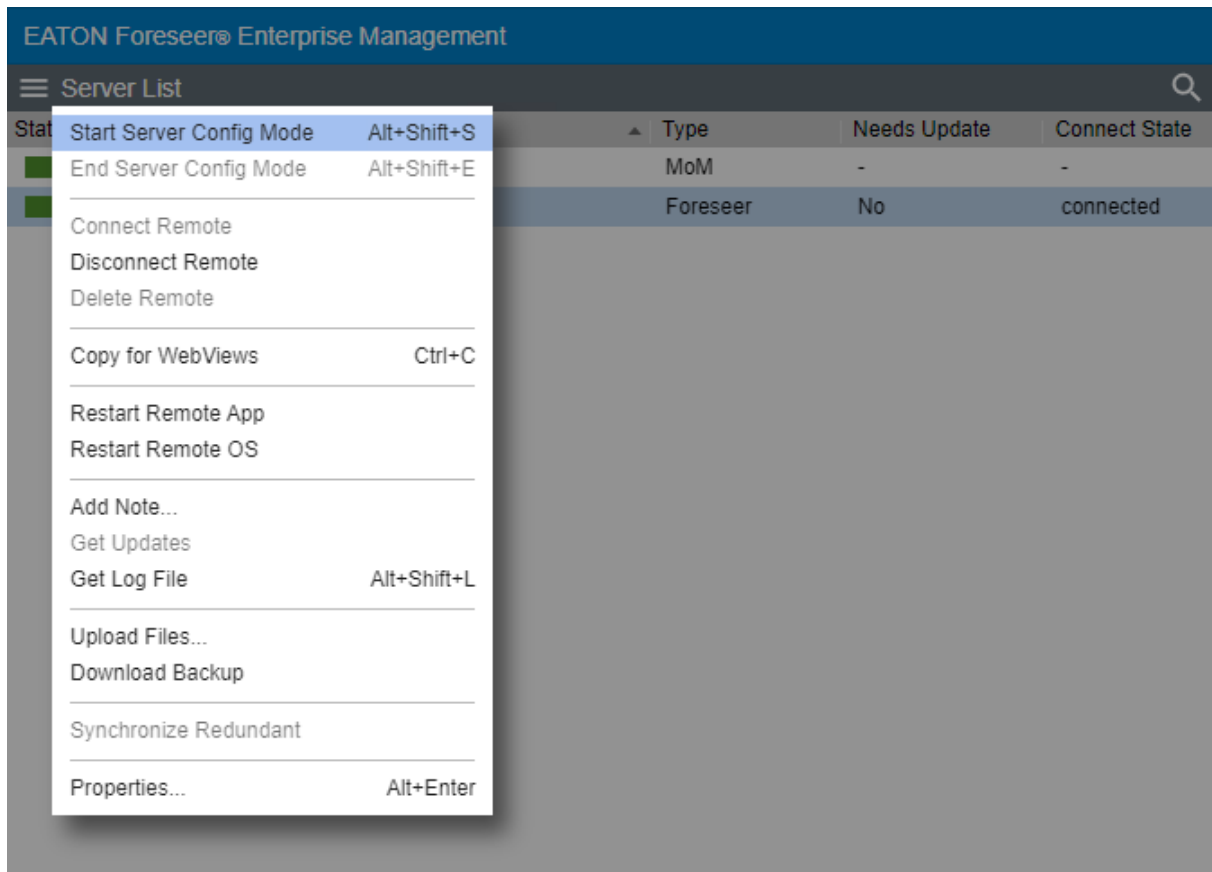
The Get Updates function is used to obtain any configuration changes that may have been applied to a remote server (such as Outpost). Changes that may need to be obtained using the Get Updates function include routine items such as adding or deleting devices, channels, or other elements on a remote.



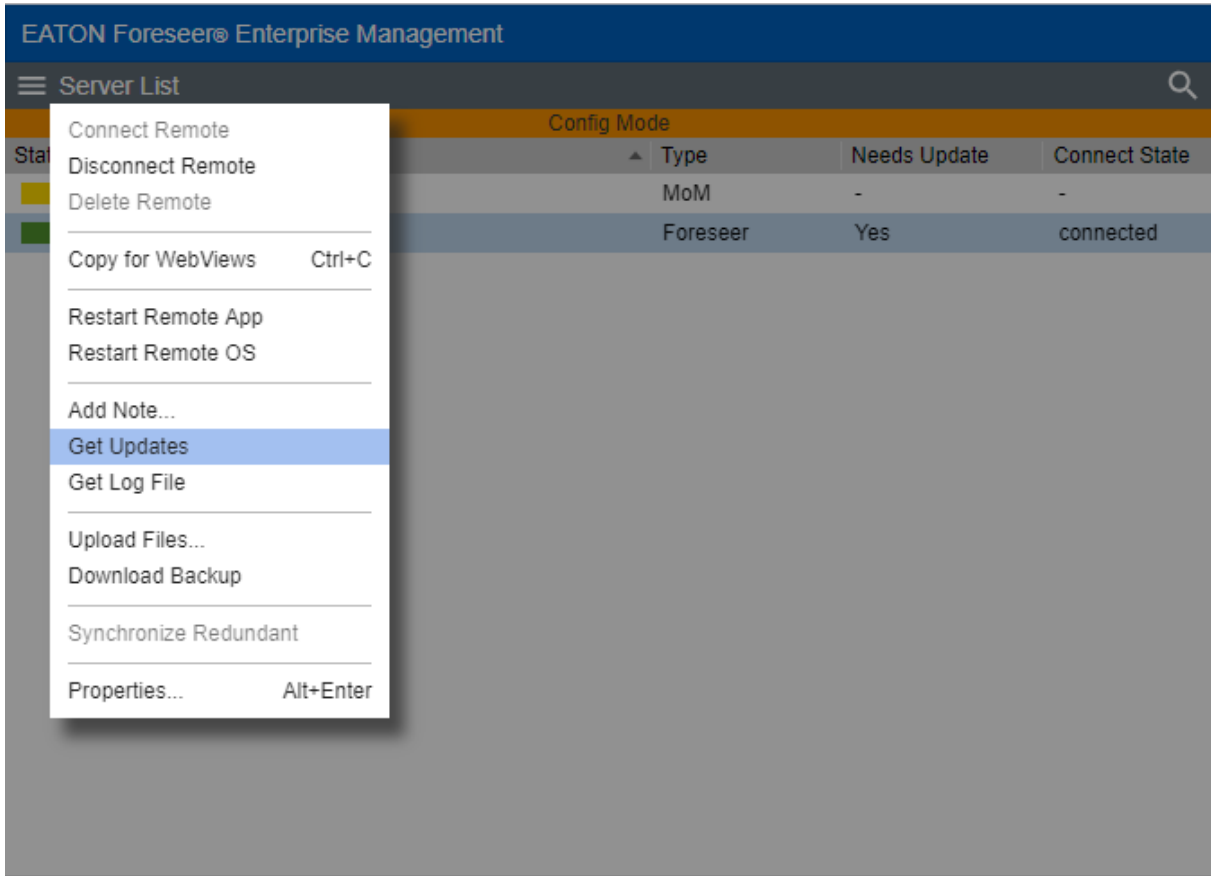
- ✔ The local Foreseer Server and Remote Server must be at the same software revision in order to fully communicate and exchange data.

If you upgraded your local Foreseer server from a prior software revision, ensure that your Remote Server has been updated before adding.

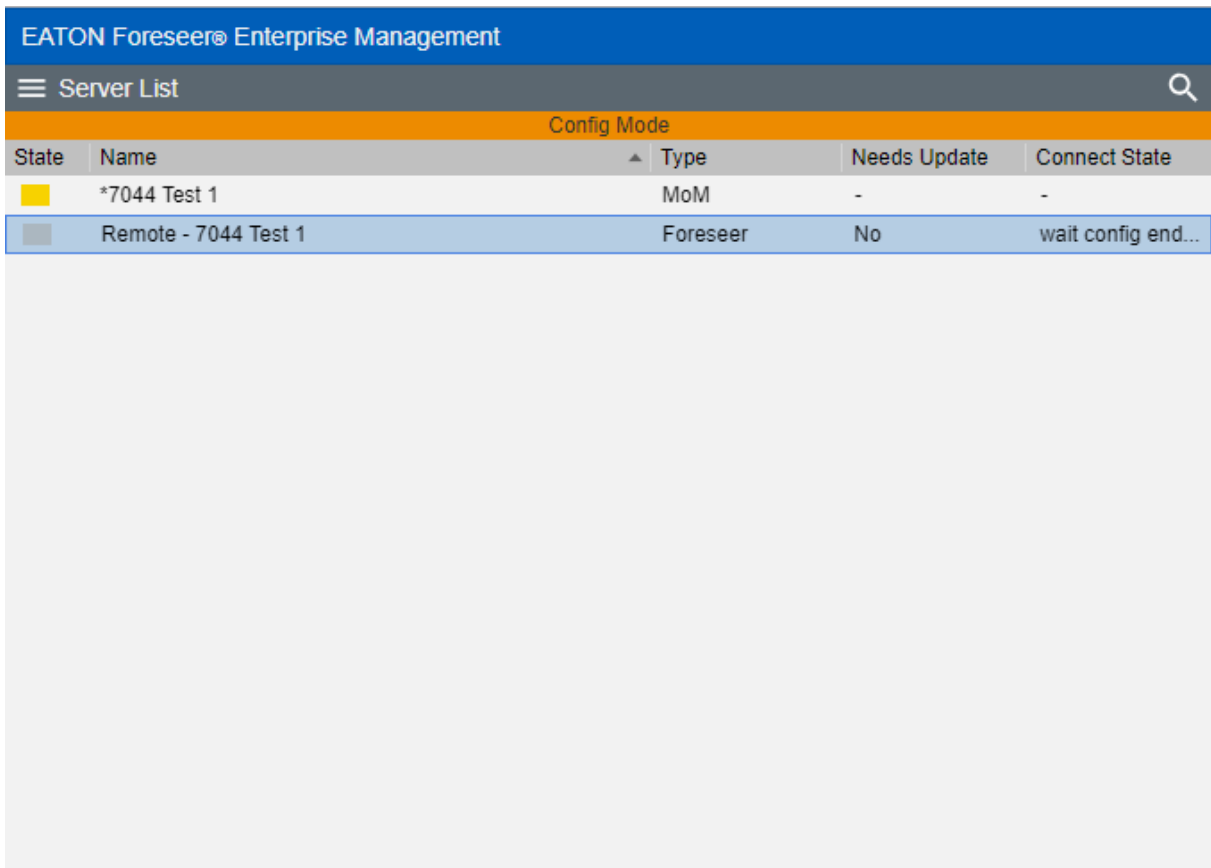
1. Start Server Config Mode Server List menu.



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.

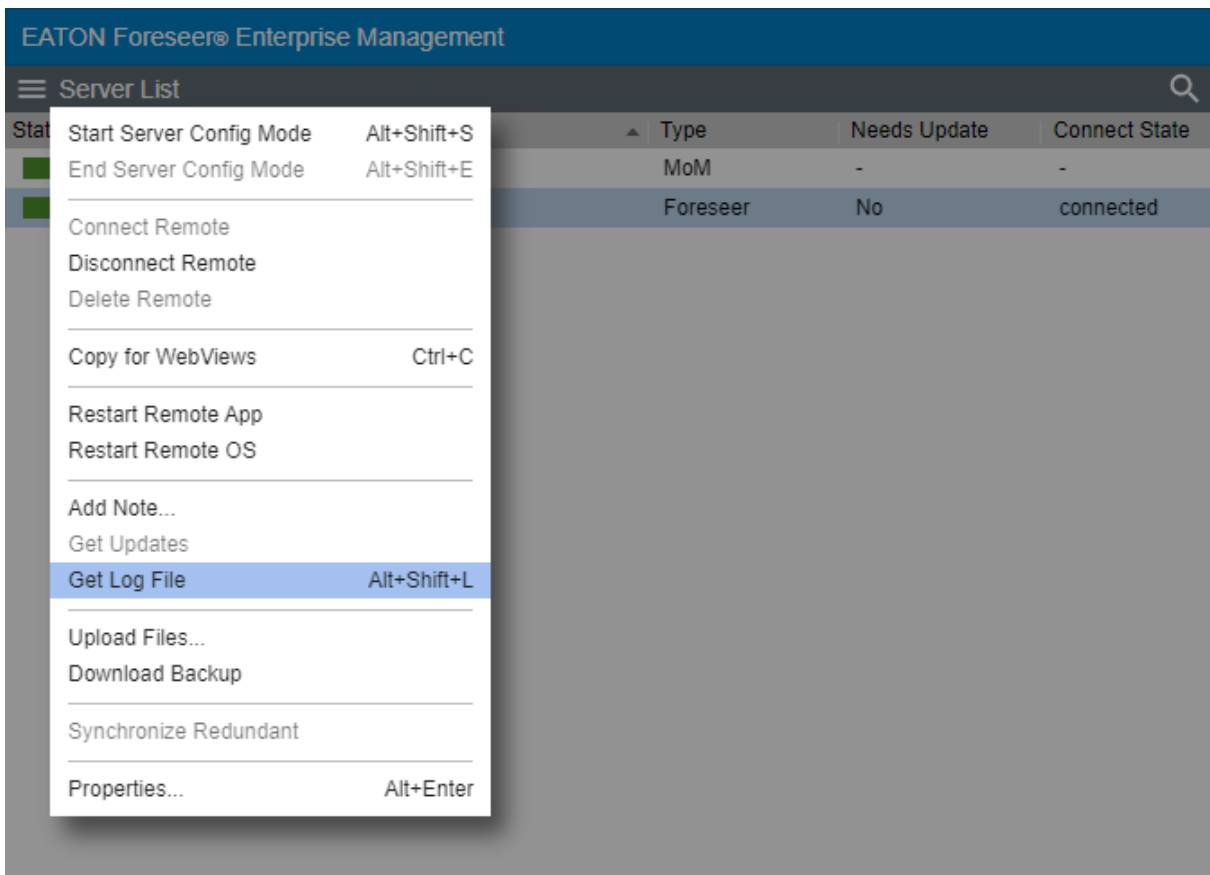


5. End Server Config mode and the system will be updated.

Get Log File

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

1. Select Get Log File from the Server List menu.



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

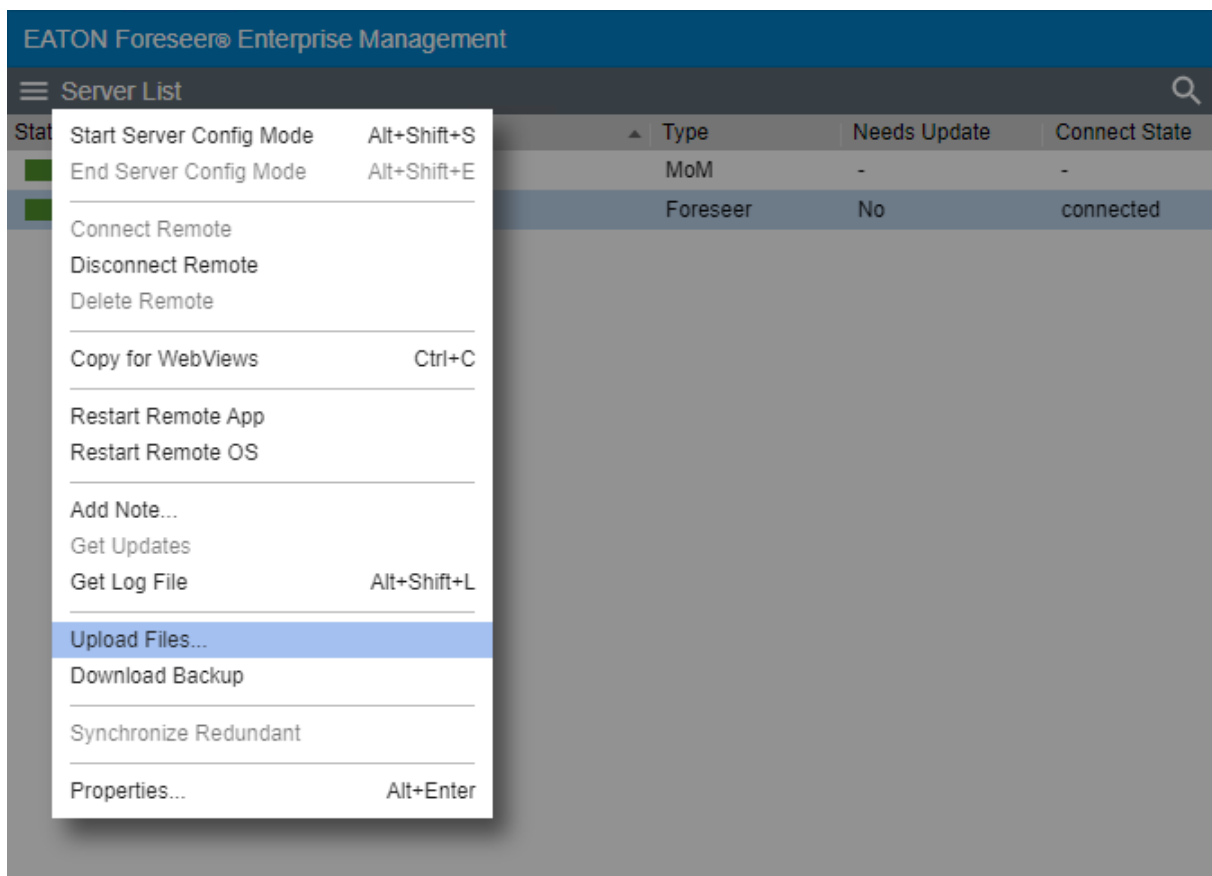
```
Log File Report
Report Time 12/01/20 15:32:24

12/01/20 15:32:24: Initializing Eaton Foreseer, Version: 7.3.292.0
12/01/20 15:32:24: Working directory: C:\Users\Administrator\Desktop\Release\
12/01/20 15:32:24: Running as an application
12/01/20 15:32:24: The UseRemoteInterface.yes file is present. Remote Interface (Outpost and MoMs) will be enabled.
12/01/20 15:32:24: ServiceThreadProc thread started with thread id: 0x194
12/01/20 15:32:24: Initializing Network Interfaces...
12/01/20 15:32:24: Initializing FileSystem Objects...
12/01/20 15:32:24: Establishing Server State...
12/01/20 15:32:24:     checking the Config Restore folders
12/01/20 15:32:24:     Creating server stores.
12/01/20 15:32:24:     processing existing server document.
12/01/20 15:32:24: Opening Server Document...
12/01/20 15:32:24: Reading Server Document: Version  0x073228
12/01/20 15:32:24:     Server Name: Local
12/01/20 15:32:24: Checking Account Impersonation...
12/01/20 15:32:24: Not using impersonation
12/01/20 15:32:24: Server Archive thread started with thread id: 0x2a6c
12/01/20 15:32:24: The last database session was ended without error.
12/01/20 15:32:24:     finishing network initialization.
12/01/20 15:32:24: Initializing Server Objects...
```

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 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

Upload Files

Enter administrative password for the remote.

Password:

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

Upload Destination: Update Vi

File 1: 7-C-H Meter IQ 250 TCP.vi ...

File 2: ...

File 3: ...

File 4: ...

File 5: ...

Upload Status:

Upload Cancel

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.

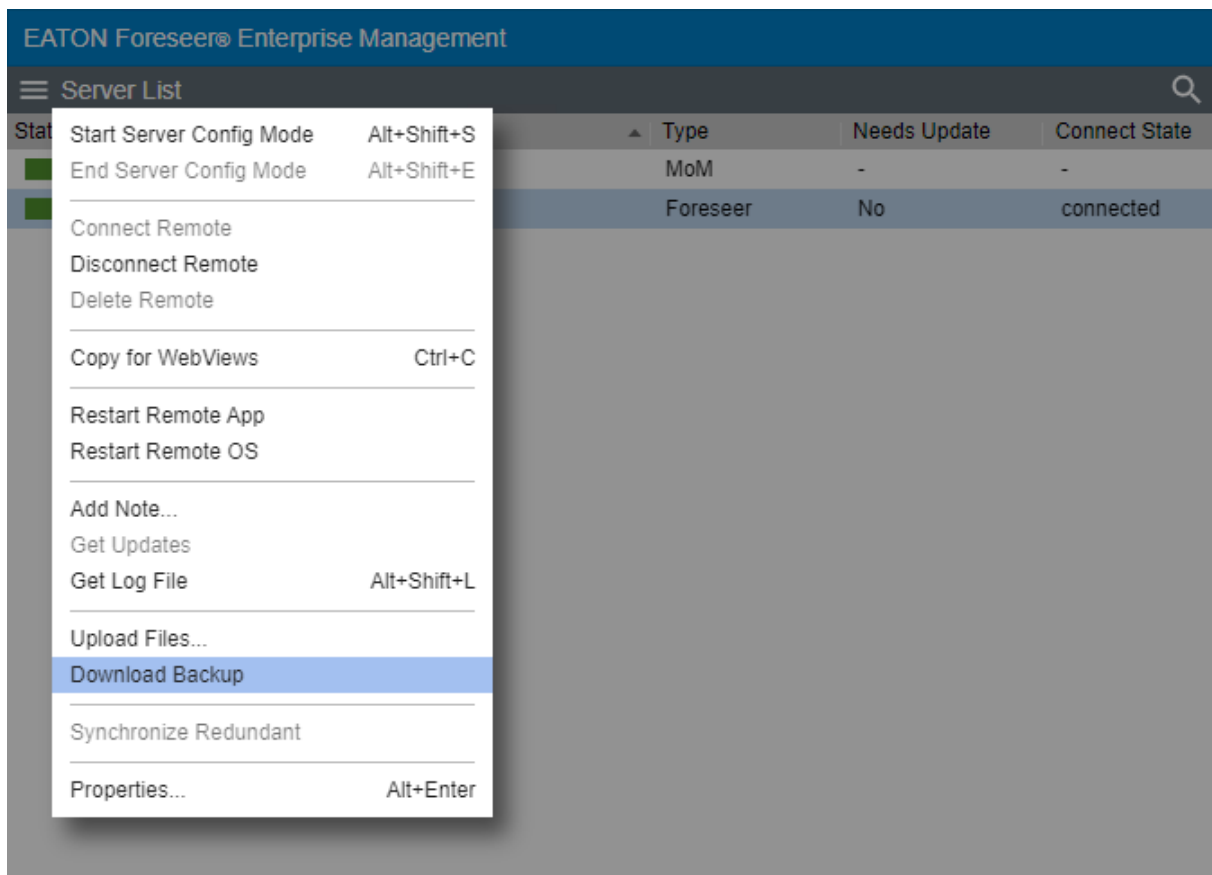
It is strongly recommended that a backup be performed after initial system configuration as well as before and after any significant modifications to ensure maximum disaster recovery capability. You must end server configuration mode before backing up the server configuration.

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

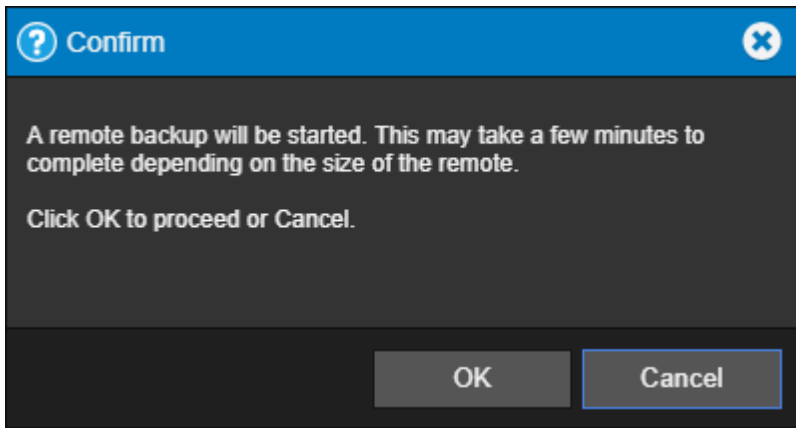
The backup archive (.ARQ) file includes the Foreseer Server configuration only, data files are not backed up in this procedure. Automatic configuration backups can be scheduled through the standalone Foreseer Configuration utility. Backups made through the Web Configuration Utility are automatically 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:

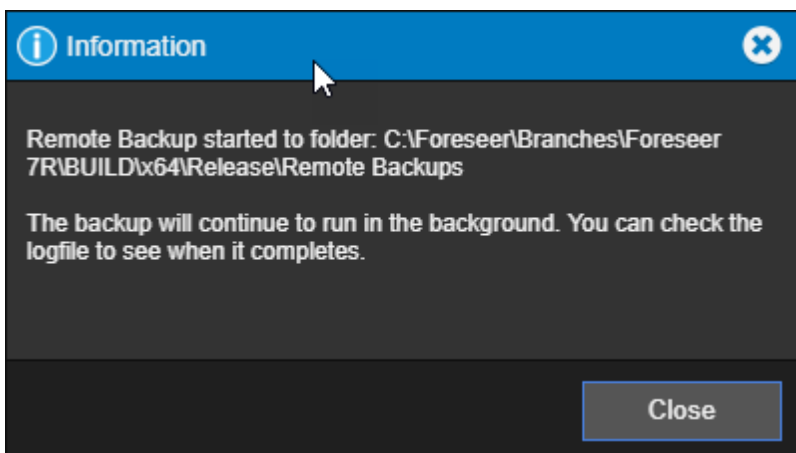
1. Select Download Backup from the Remote Server List Menu.



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



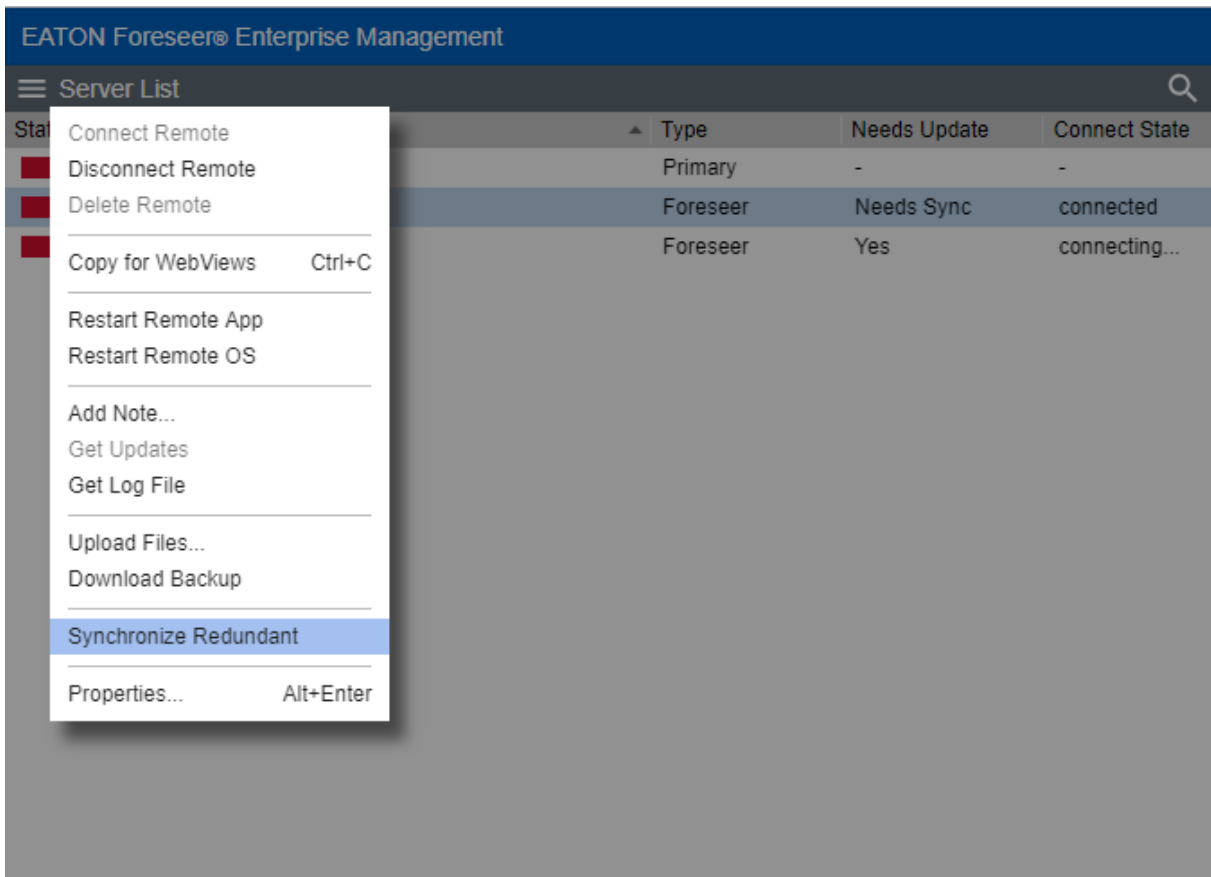
3. Another informational dialog will appear telling the user of the location of the remote backup. Click **Close** to continue



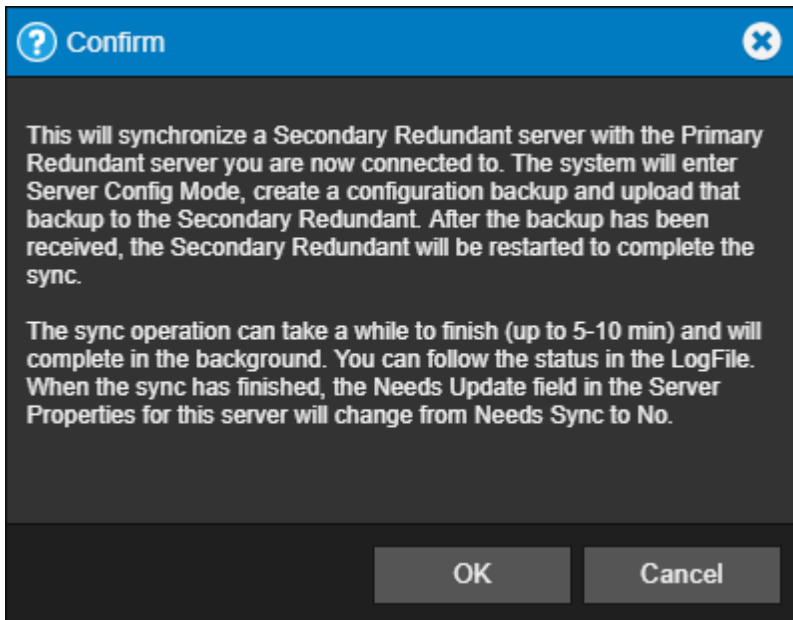
Synchronize Redundant

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

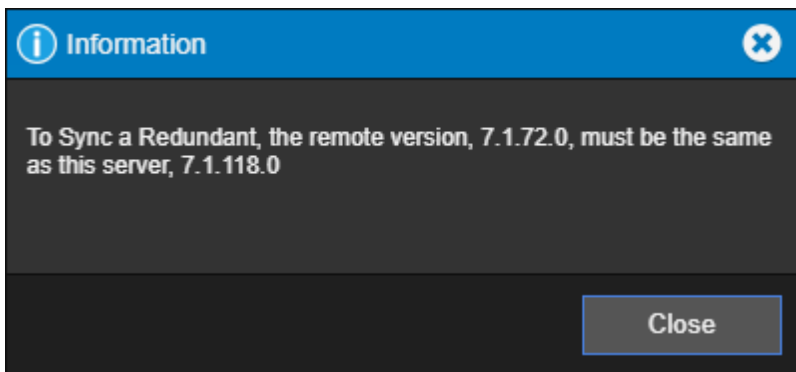
1. Highlight the redundant server that needs synchronizing.
2. Select Synchronize Redundant from the Server List menu.



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



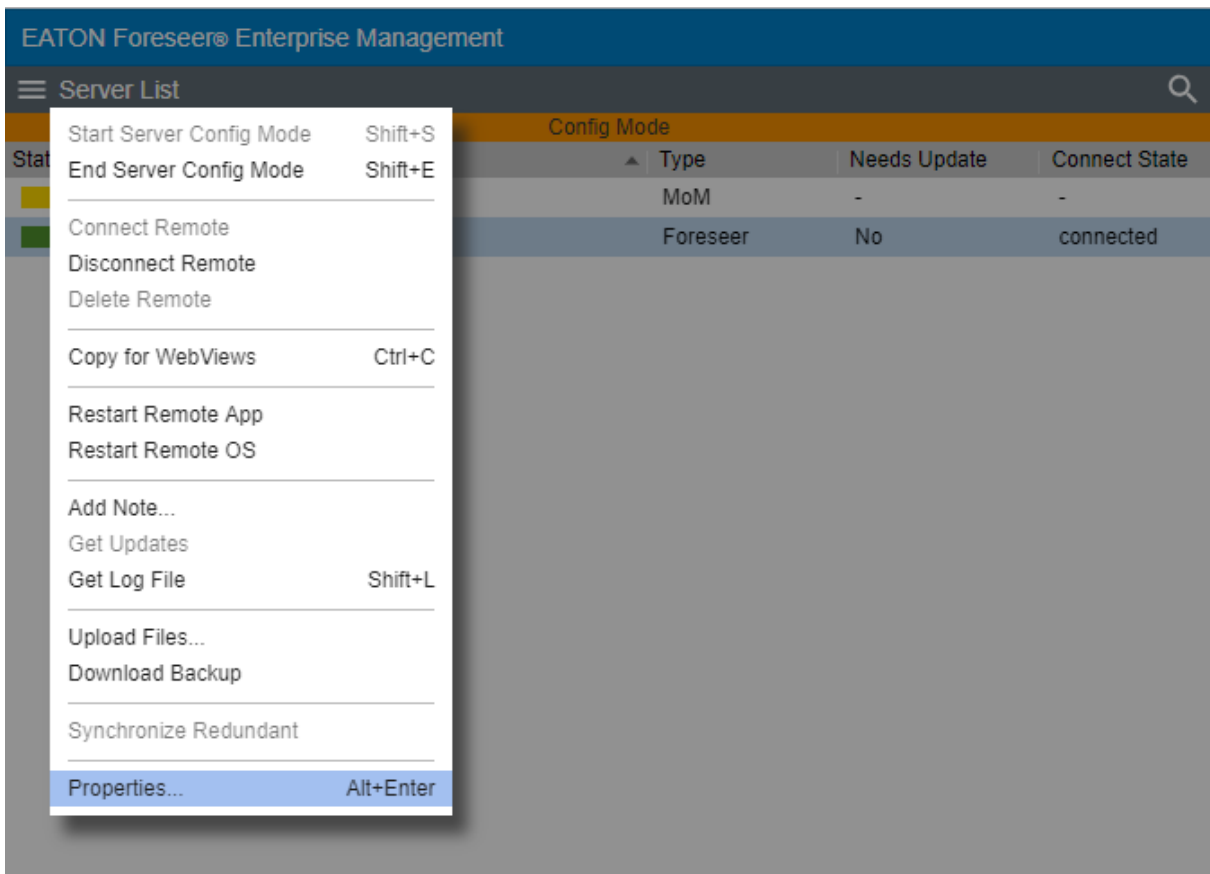
4. If the two environments are not an appropriate version, an information dialog will be displayed telling you about this discrepancy. The appropriate action will need to be taken to correct this issue.



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 Remote Server Properties dialog displays the remote connection properties

Remote Server Properties

Name: Foreseer Remote

Remote Address: 10.130.151.100:2100

Updates (sec): 2

Connection Password: *****

Verify Password: *****

Connect to this remote at startup

Synchronize Remote's clock on connect

This remote is a Redundant Server

This Remote sends waveform files

OK Cancel

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
- Add User-Defined Channel
- Delete
- Rename
- Copy for WebViews
- Copy Channel Properties
- Paste Channel Properties
- Create .vi File
- Load Driver
- Unload Driver
- Properties

Enable

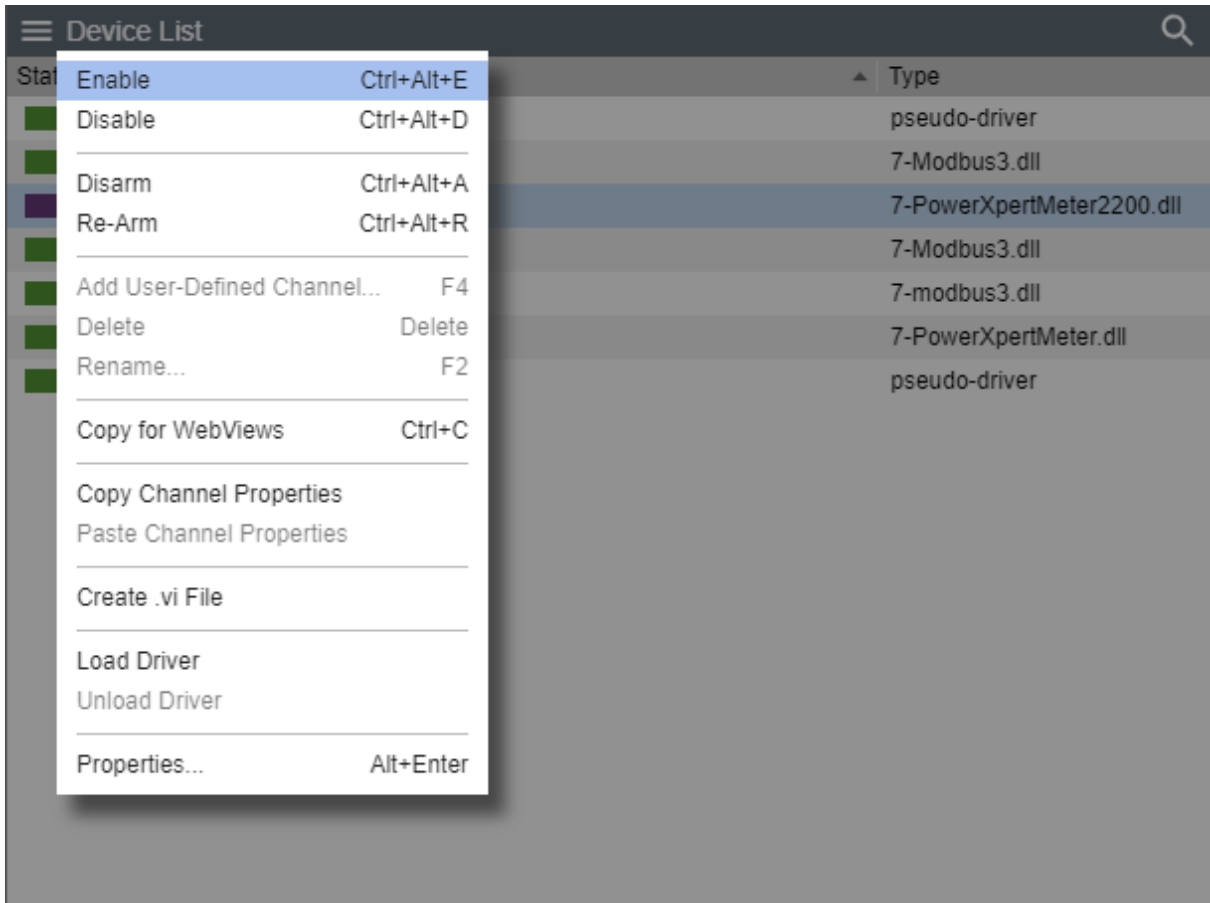
The enable function resumes all data archiving to the Foreseer Server for the selected Device.



✔ Administrative Authorization is required before proceeding with this command.

To Enable a device:

1. Select Enable from the Device List menu



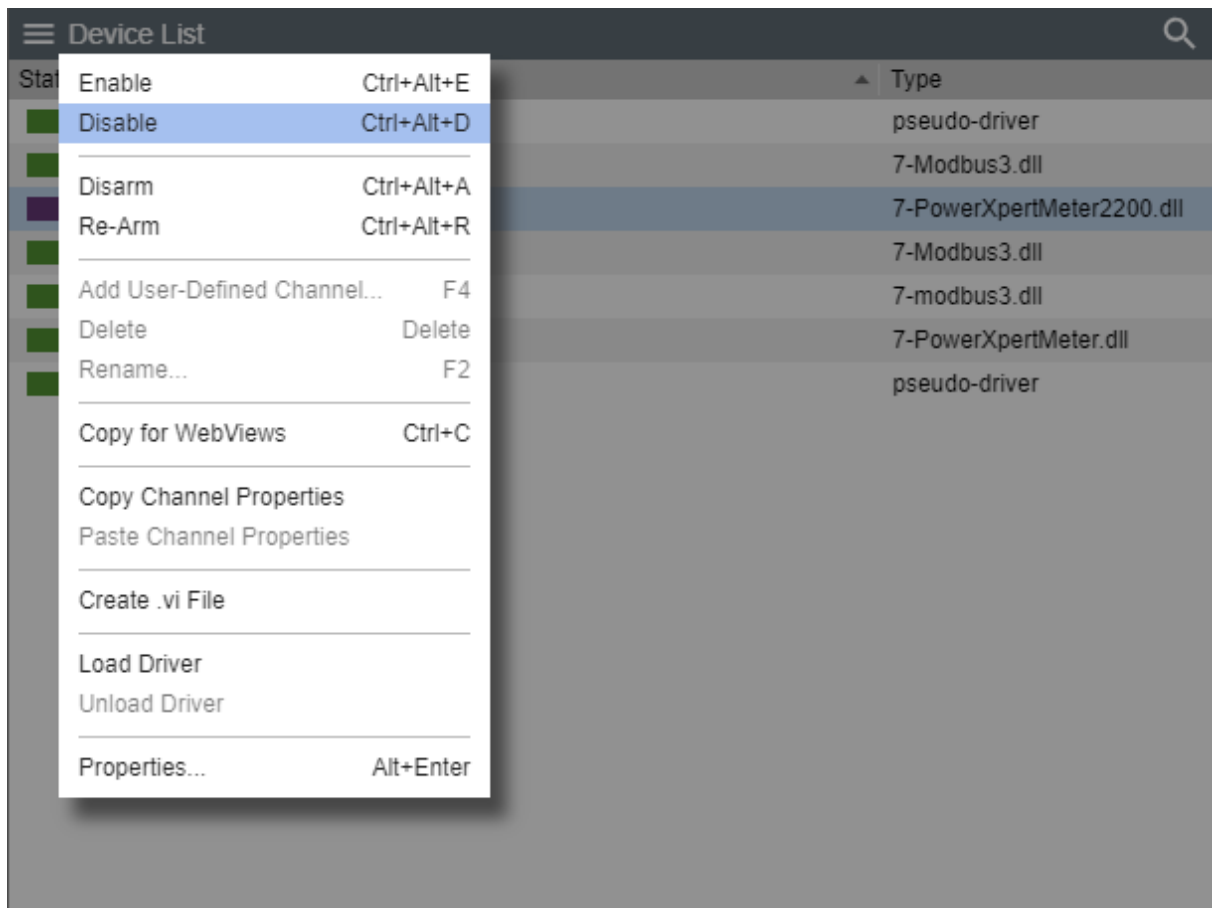
Disable

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:

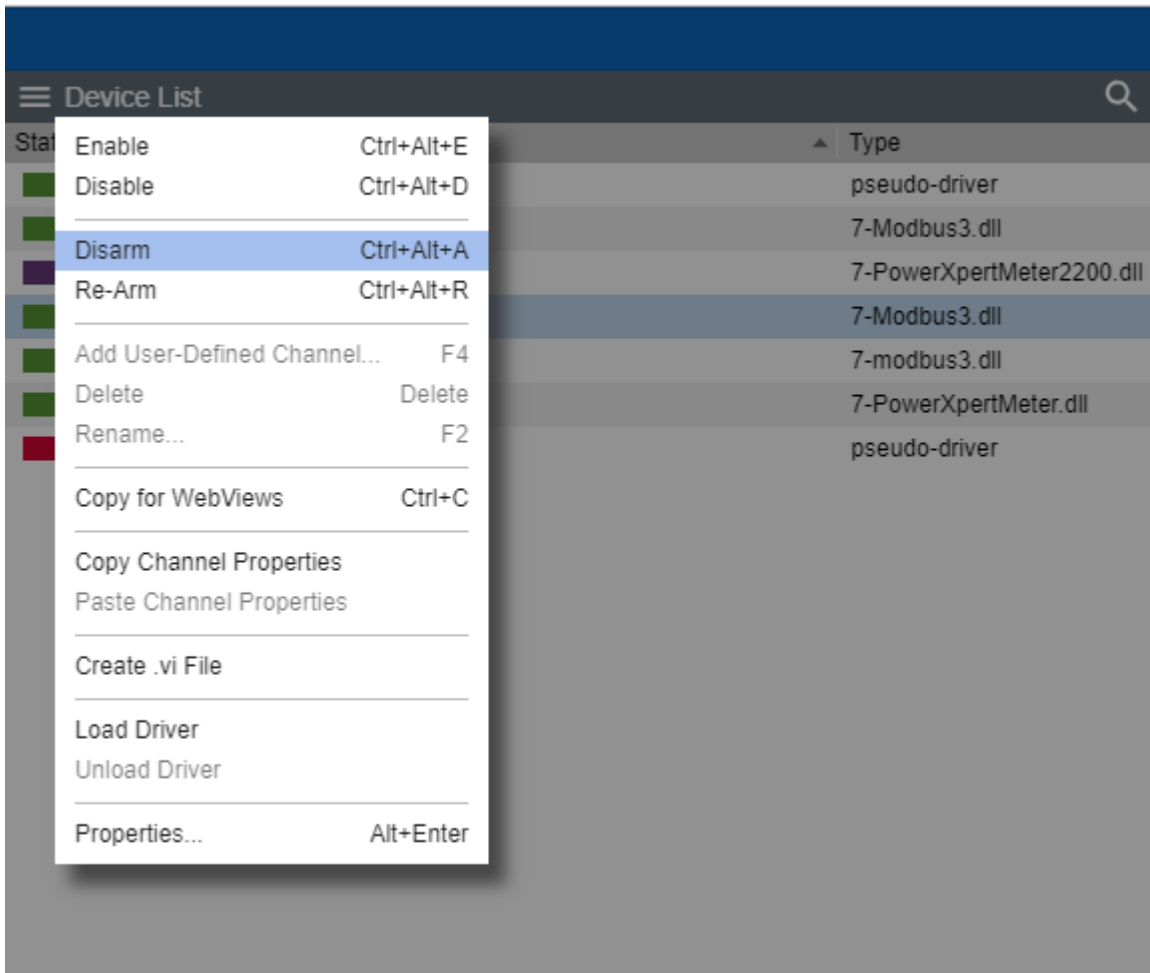
1. Select Disable from the Device List menu



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

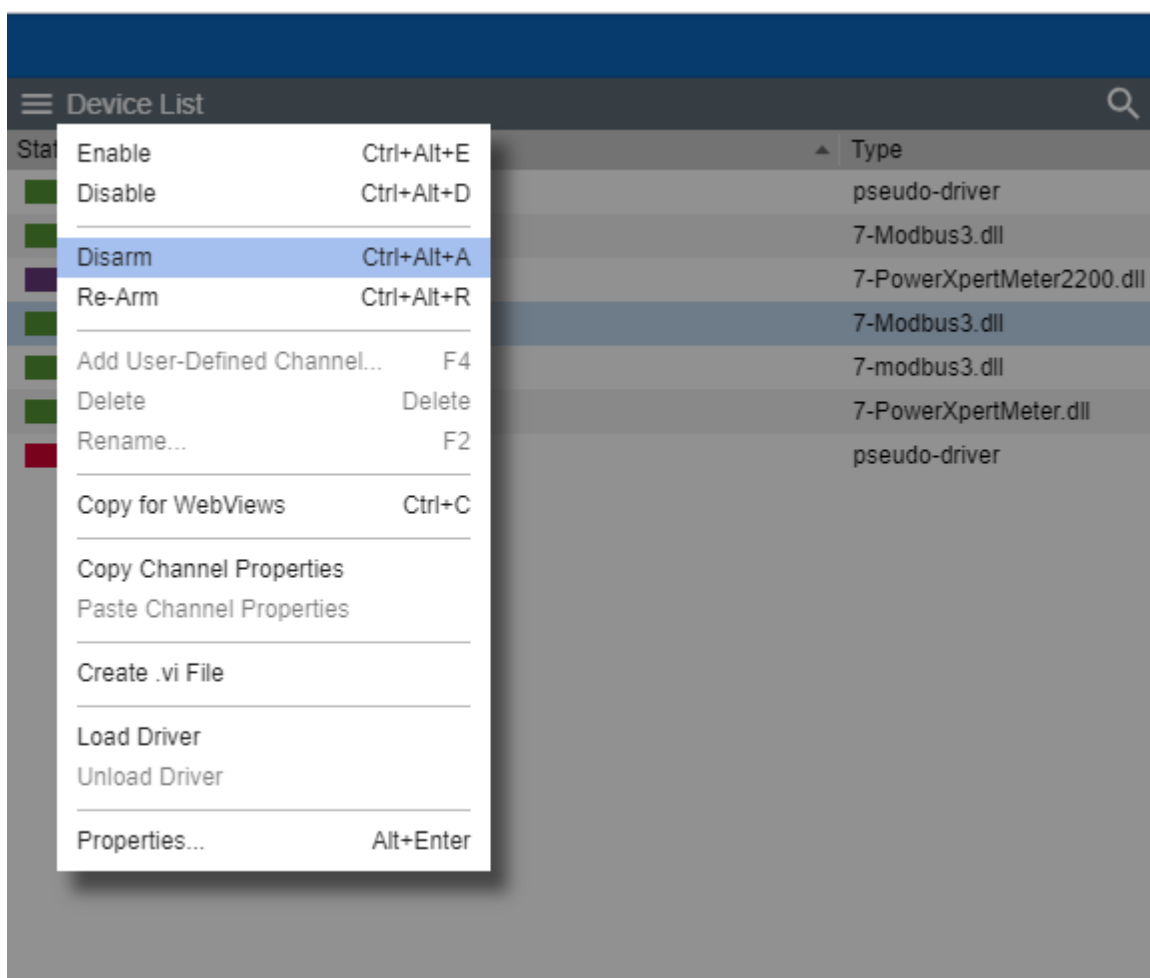
Device List			🔍
State	Name	Type	
■	Derived Channels	pseudo-driver	
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll	
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll	
■	IQ 250 1	7-Modbus3.dll	
■	Mits 9900 Aegis 1	7-modbus3.dll	
■	PowerXpert Meter1	7-PowerXpertMeter.dll	
■	System Channels	pseudo-driver	

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.

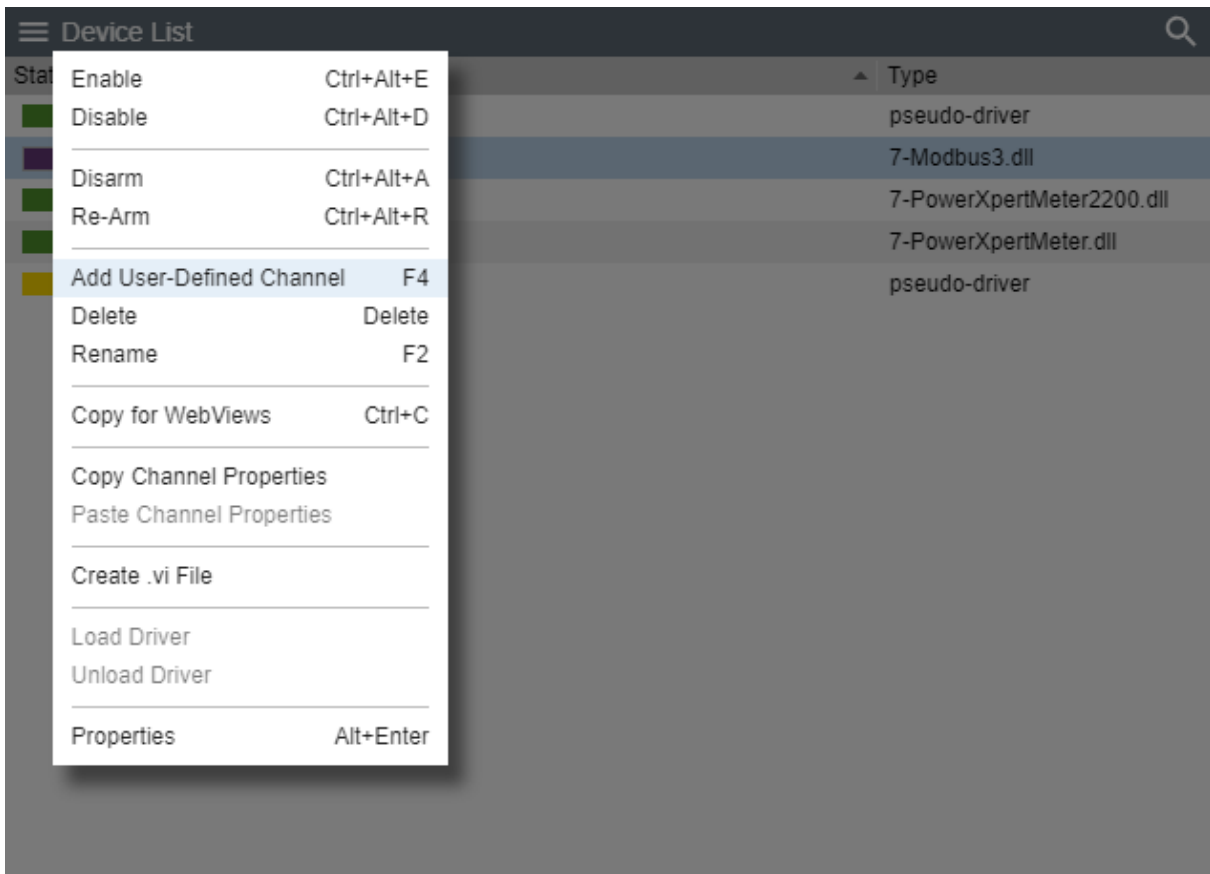
Device List		
State	Name	Type
■	Derived Channels	pseudo-driver
■	Eaton PXM 2270 Meter 1	7-Modbus3.dll
■	Eaton PXM 2280 1	7-PowerXpertMeter2200.dll
■	PowerXpert Meter1	7-PowerXpertMeter.dll
■	System Channels	pseudo-driver

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

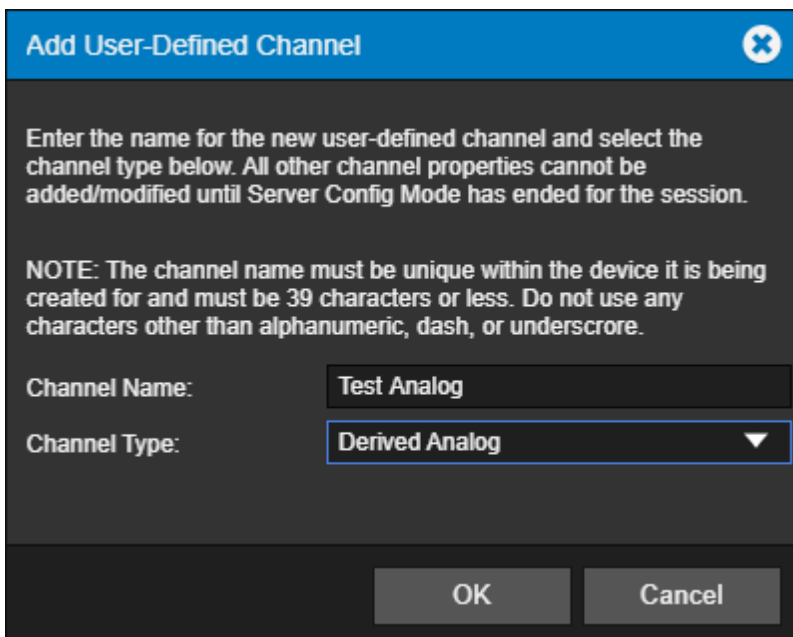
Enable	Ctrl+Alt+E
Disable	Ctrl+Alt+D
Disarm	Ctrl+Alt+A
Re-Arm	Ctrl+Alt+R
Add User-Defined Channel	F4
Delete	Delete
Rename	F2
Copy for WebViews	Ctrl+C
Copy Channel Properties	
Paste Channel Properties	
Create .vi File	
Load Driver	
Unload Driver	
Properties	Alt+Enter

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



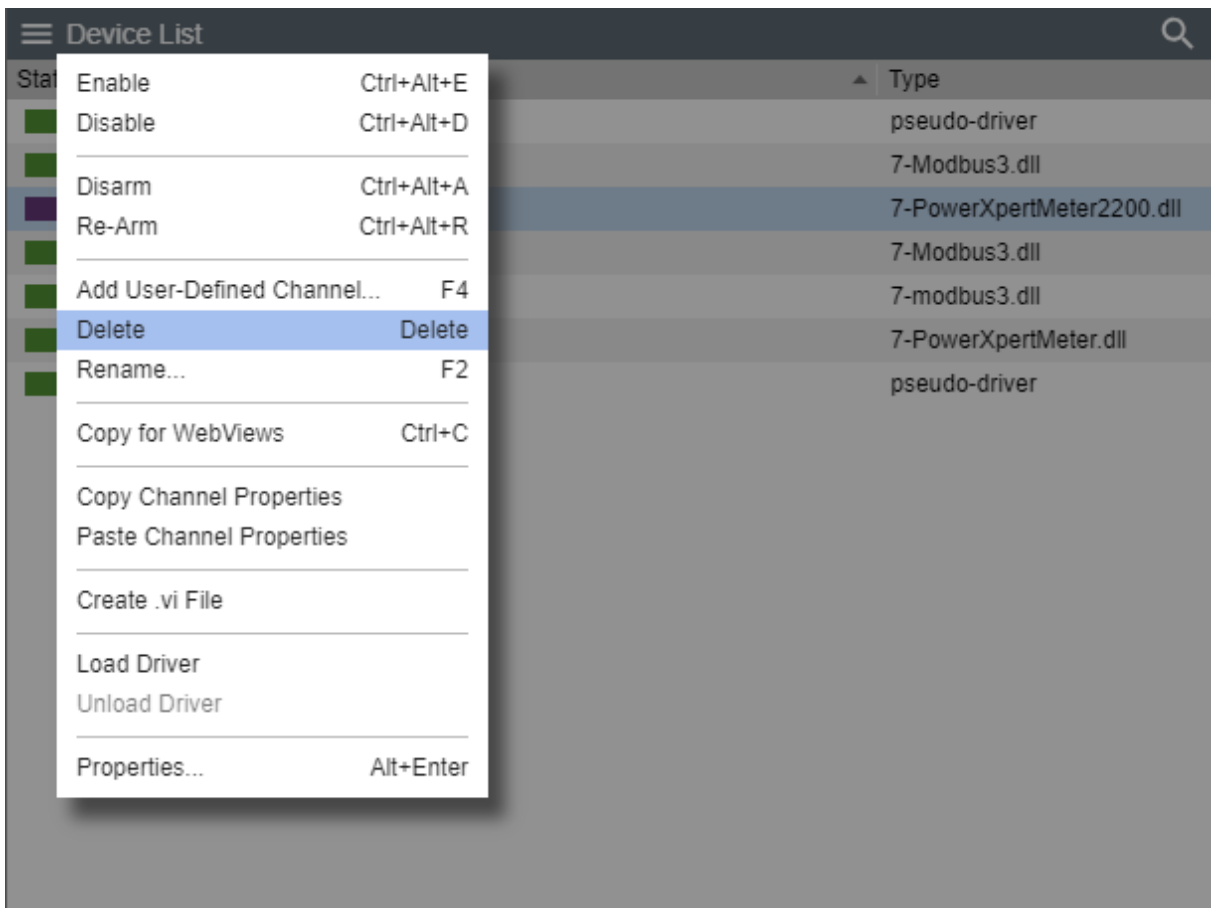
Delete

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.

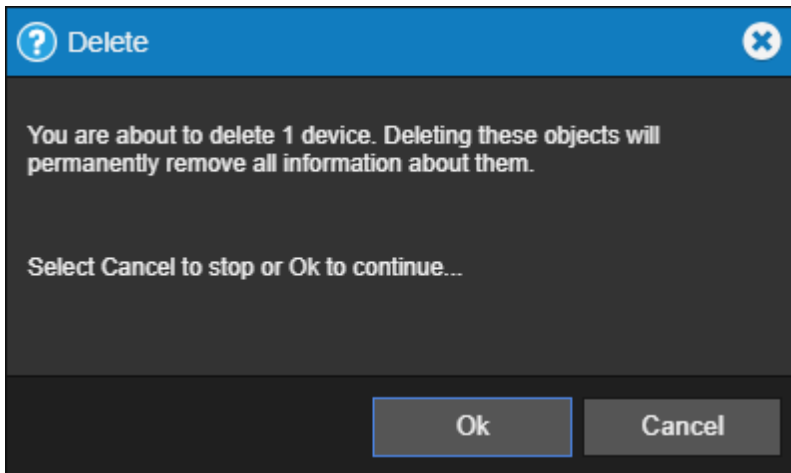
✔ Administrative Authorization is required before proceeding with this command.

To Delete a device:

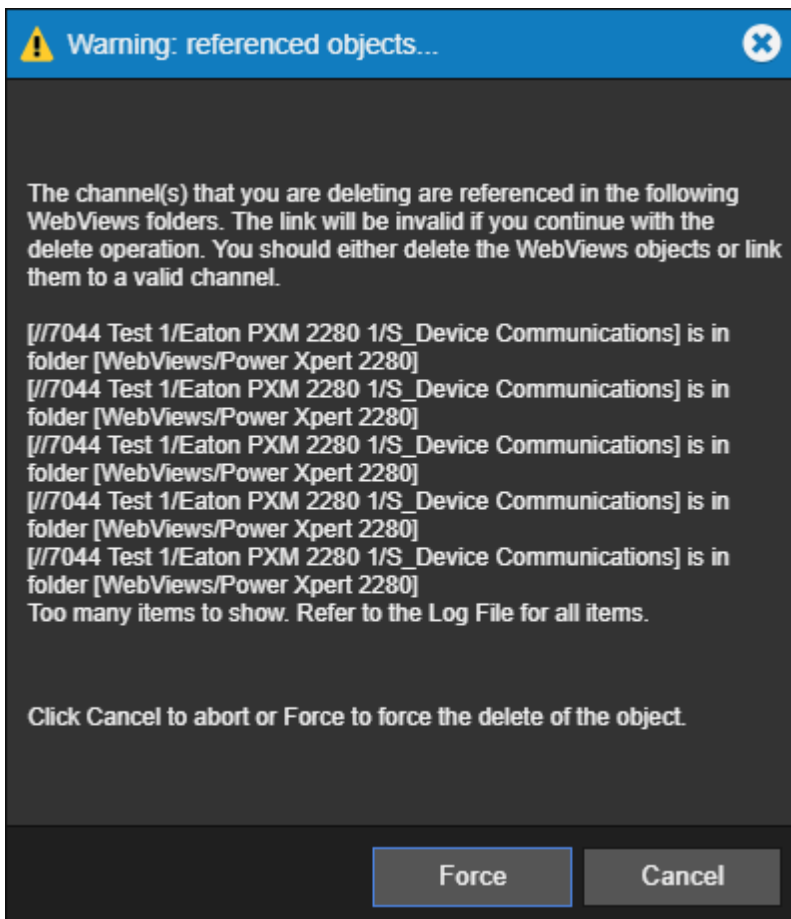
1. Select Delete a device from the Device List menu.



2. Confirm that you want to delete the selected device



3. If the selected device or its 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

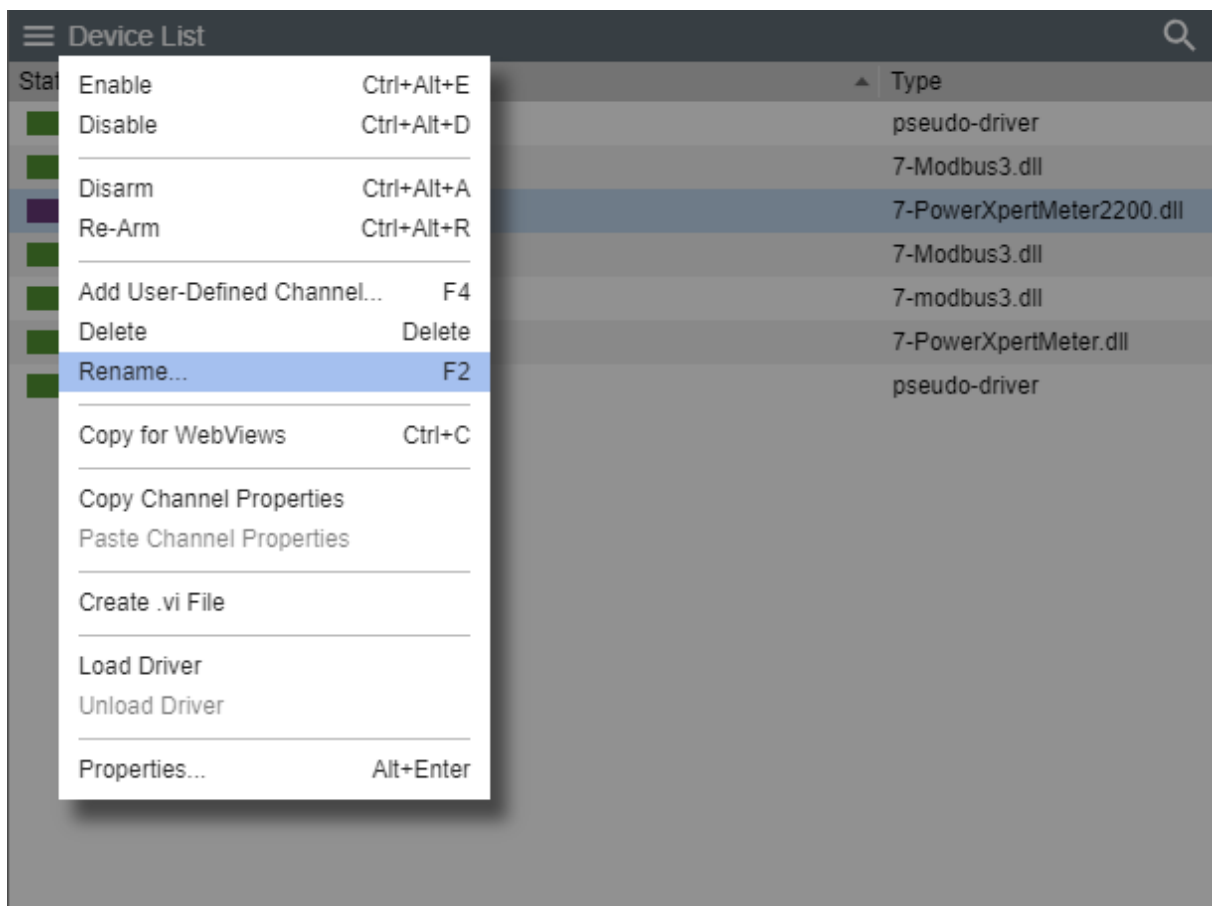
Rename

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.

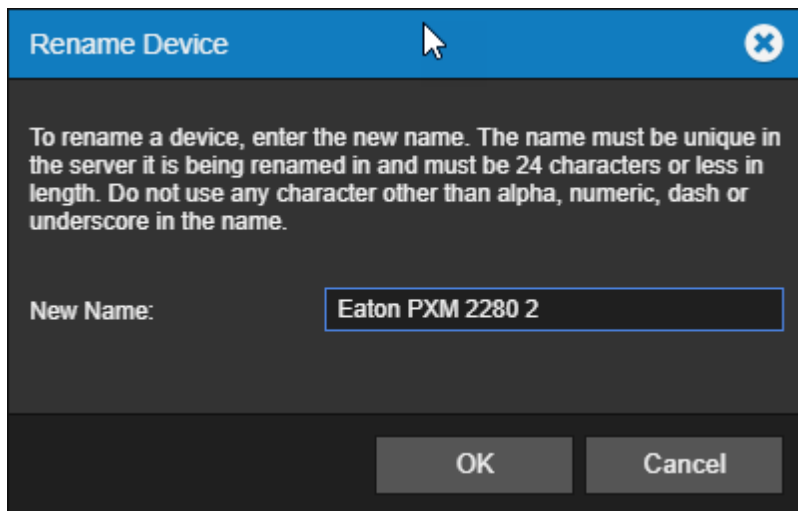
✔ Administrative Authorization is required before proceeding with this command.

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



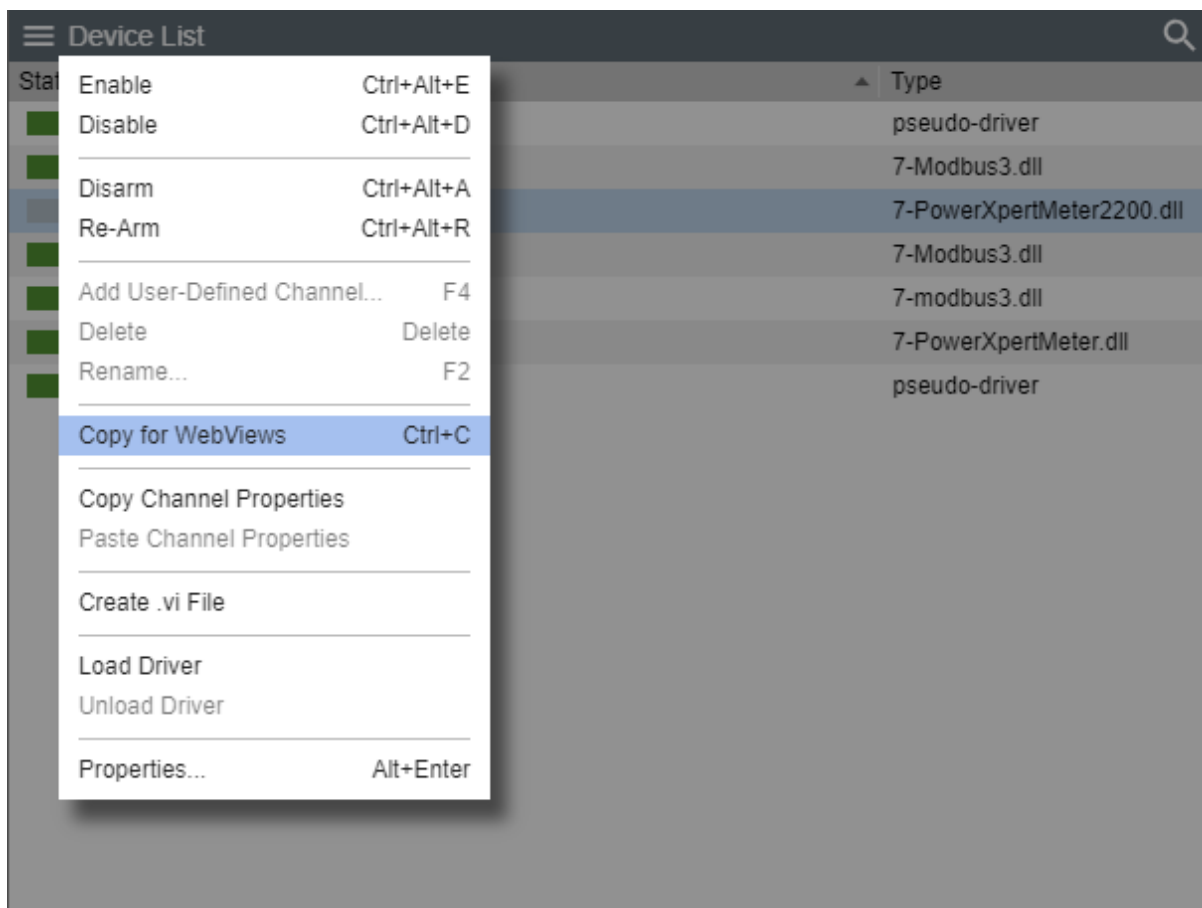
4. Select OK to accept the new name

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

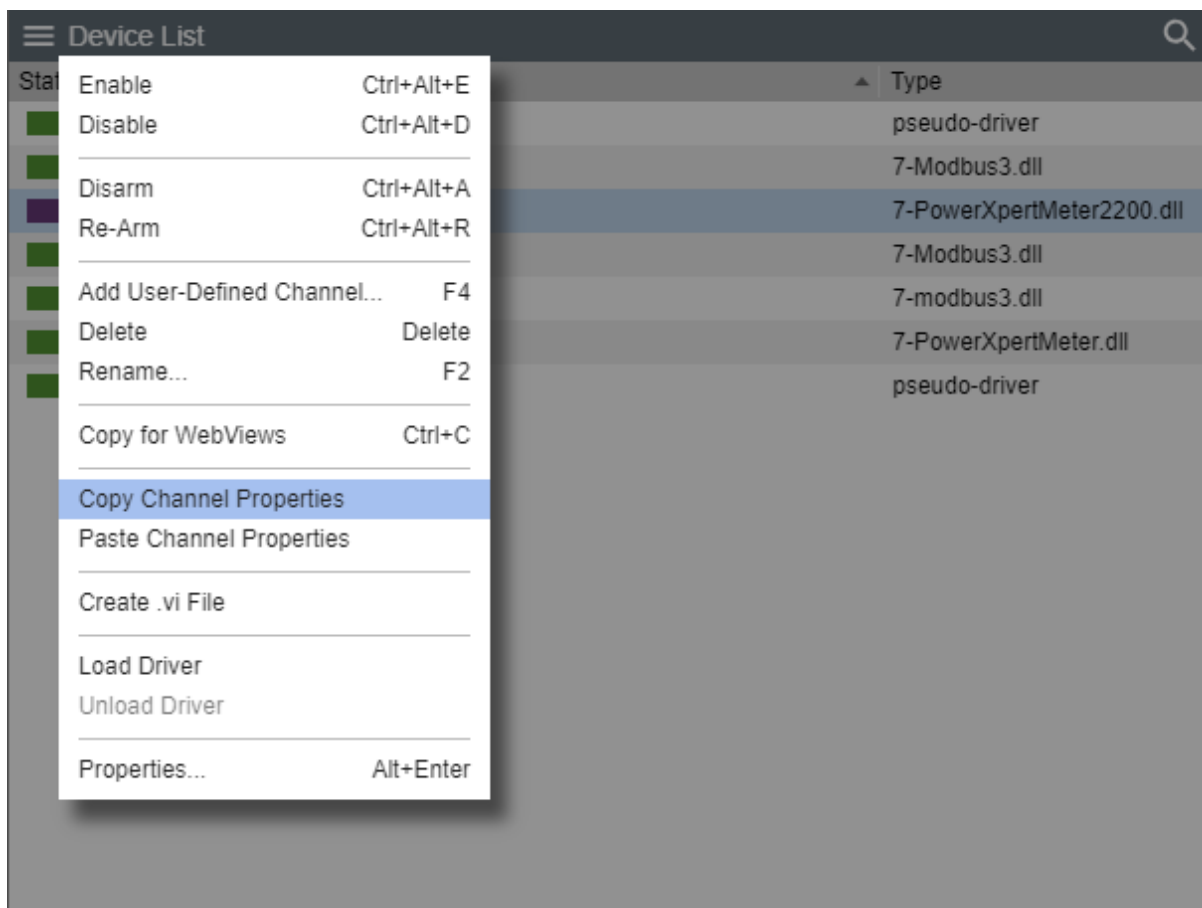


Copy Channel Properties

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

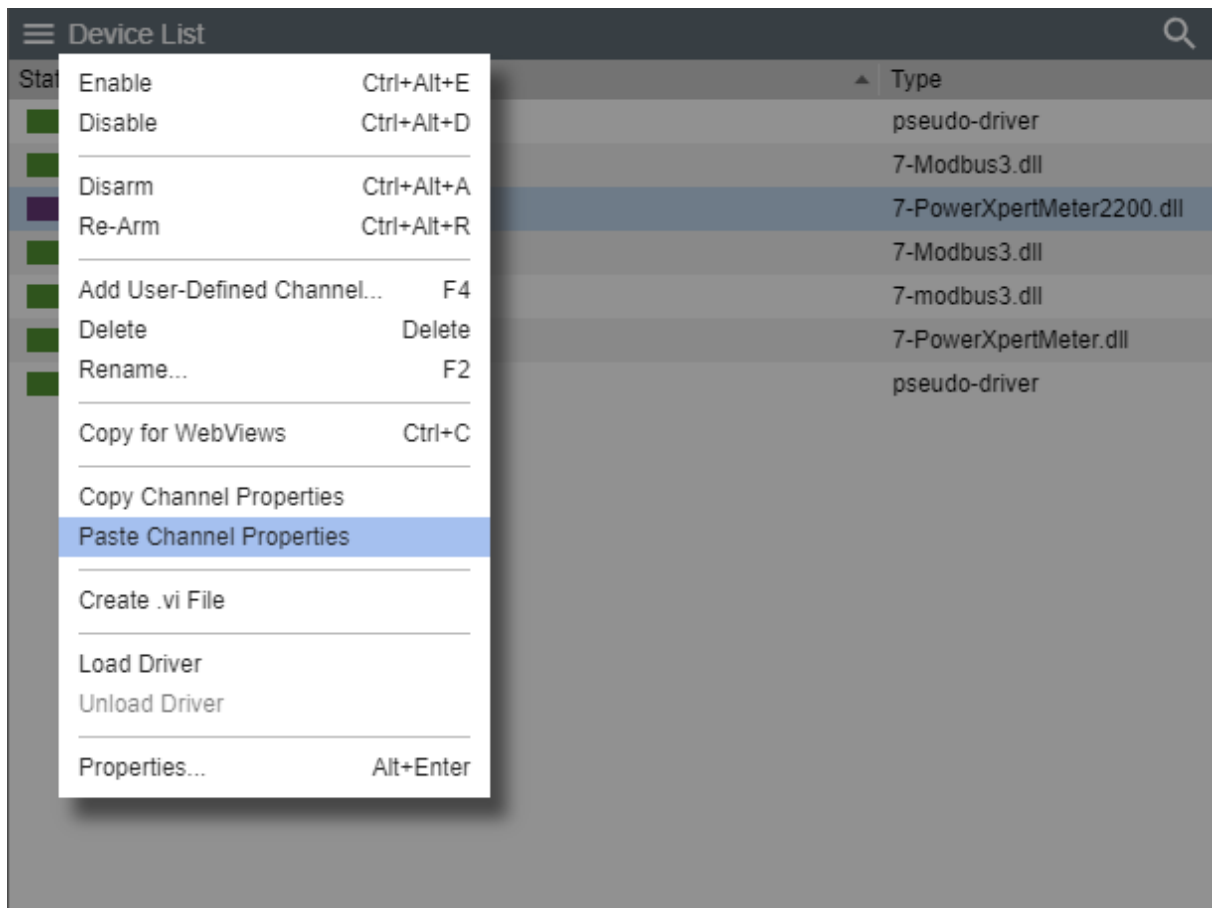


Paste Channel Properties

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

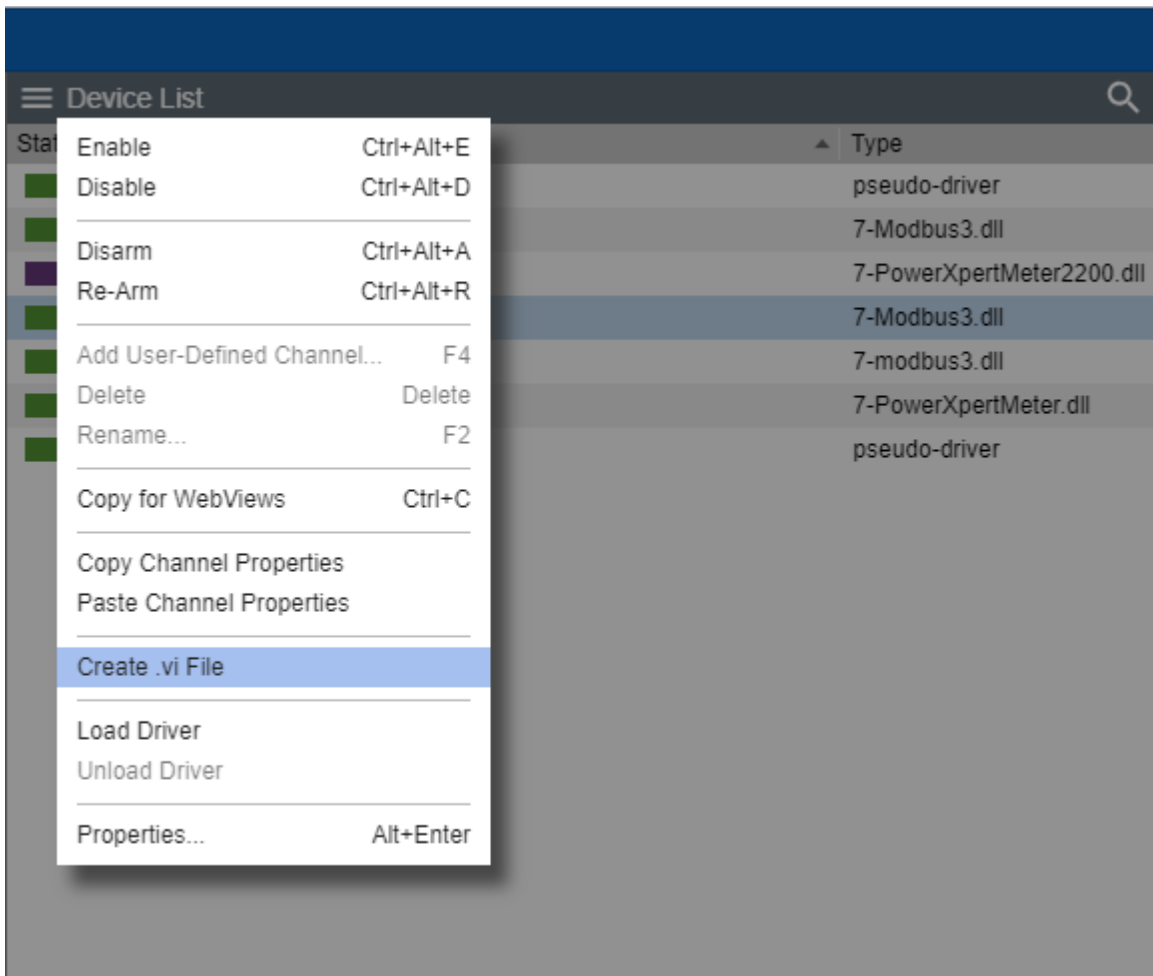


Create .vi File

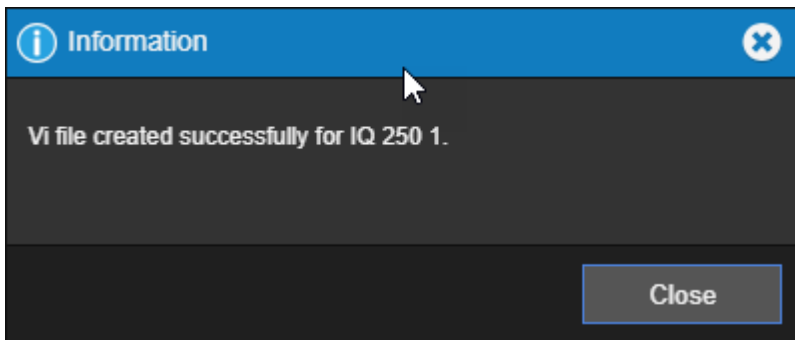
The Create .vi File command generates .VI (Device Driver) templates for all Devices on the selected Server. These device templates can then be used to define other similar Devices.

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

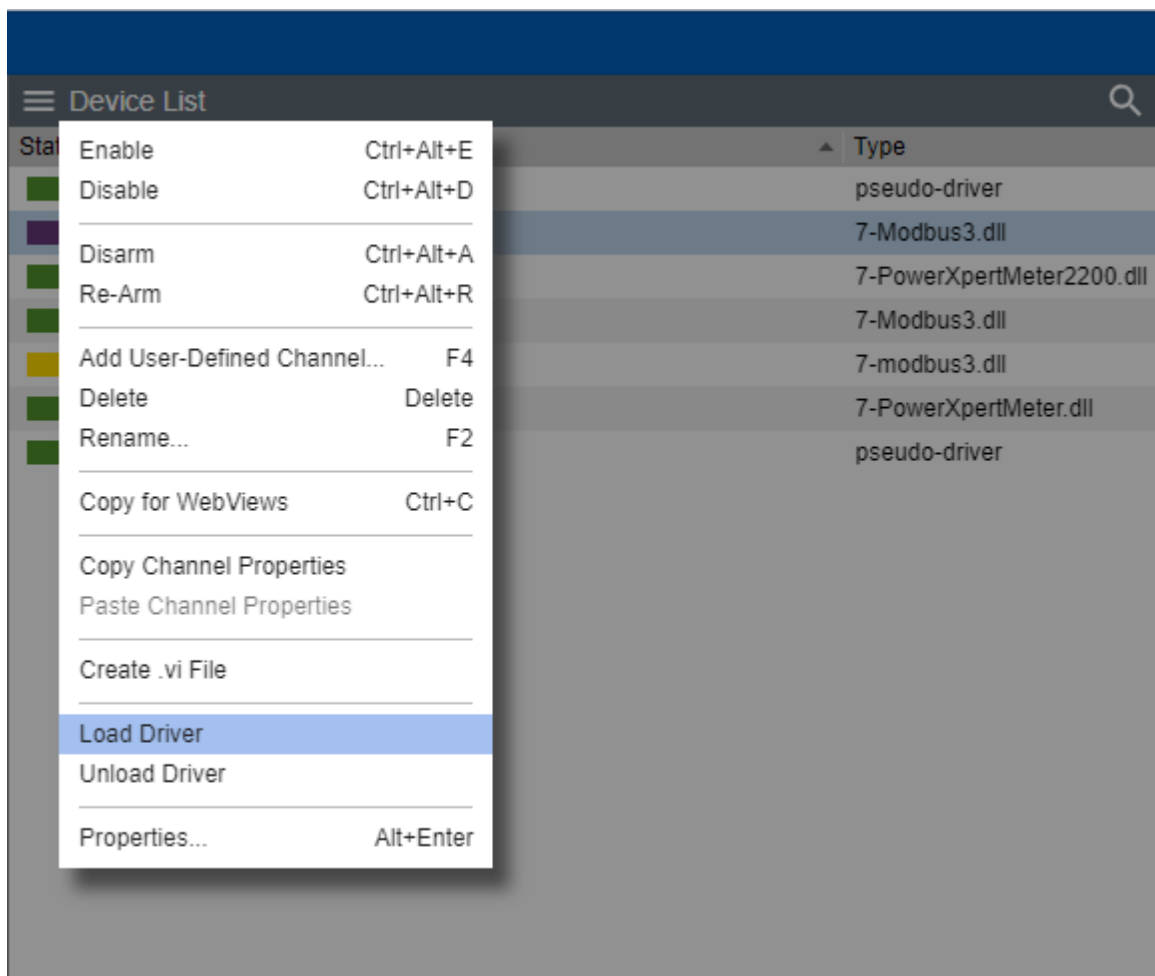
The Load Driver command are used strictly by driver developers. You can load the appropriate Device driver from the \Program Files (x86)\Eaton Corporation\Foreseer\Update VI folder.

- ✔ 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

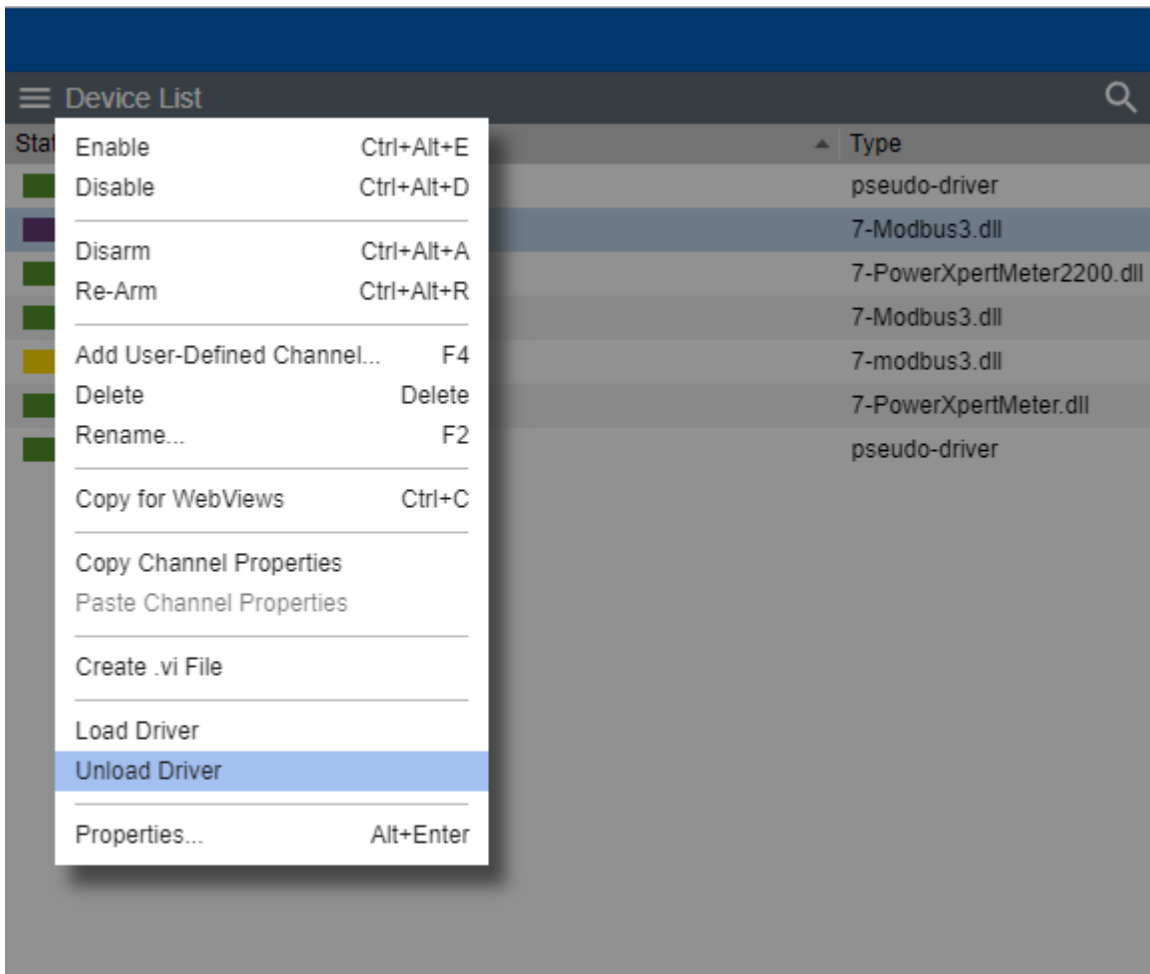
The Unload Driver commands are used strictly by driver developers. Unload clears the driver file for the selected Device. Multiple Devices of the same Type may be selected for unloading without shutting the system down.

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

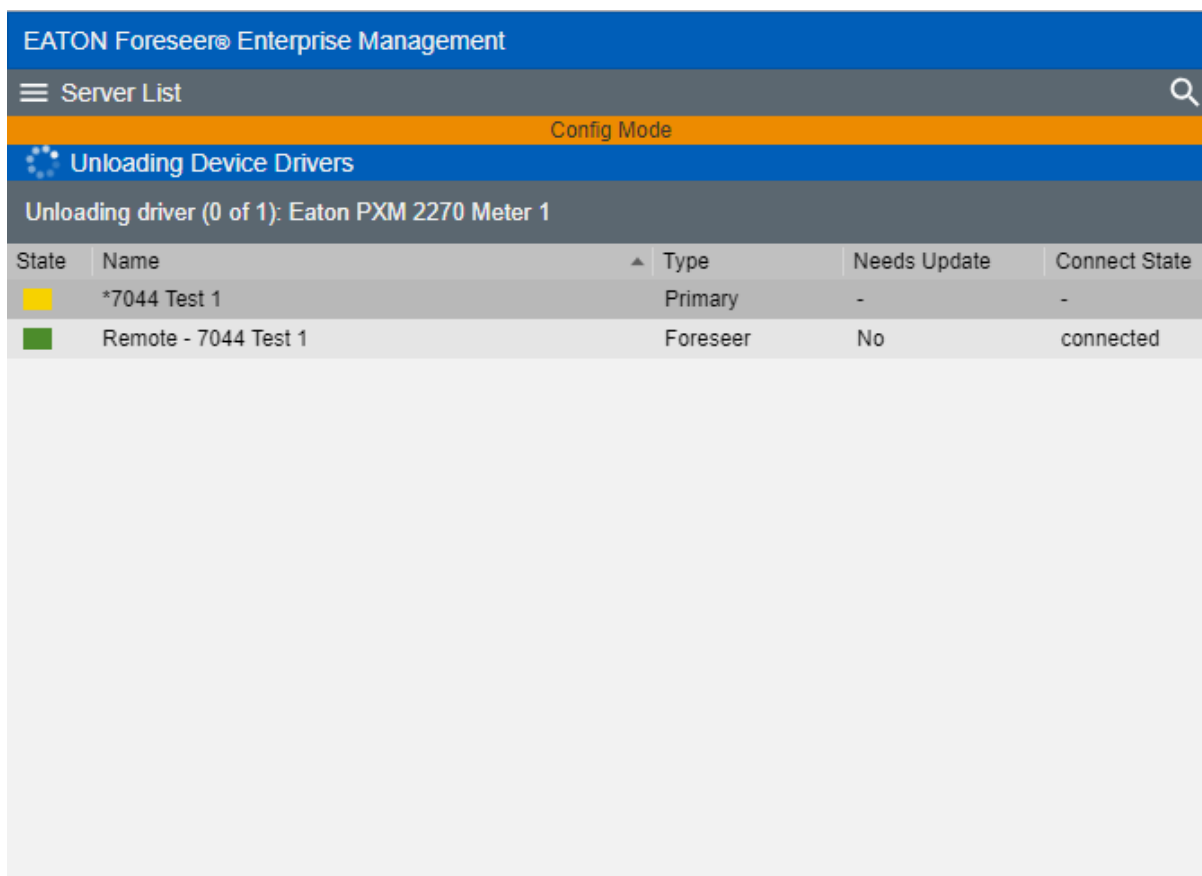
✔ Administrative Authorization is required before proceeding with this command.

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



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

Device Name: IQ 260 1

Device Status: Online

Driver Name: 7-Modbus3.dll

Device Location: US-PA-PITTSBURGH

Device Type: Meter

Driver Version: 7.3.41.0

Library Version: 7.3.0

Last Scan Time: 13:45:26 12/04/20

Alarm Group Name: Power Meters

Device Channel Counts:

Analog:	115
Digital:	5
Date:	1
Text:	3
Total:	124

OK Cancel

Device Properties

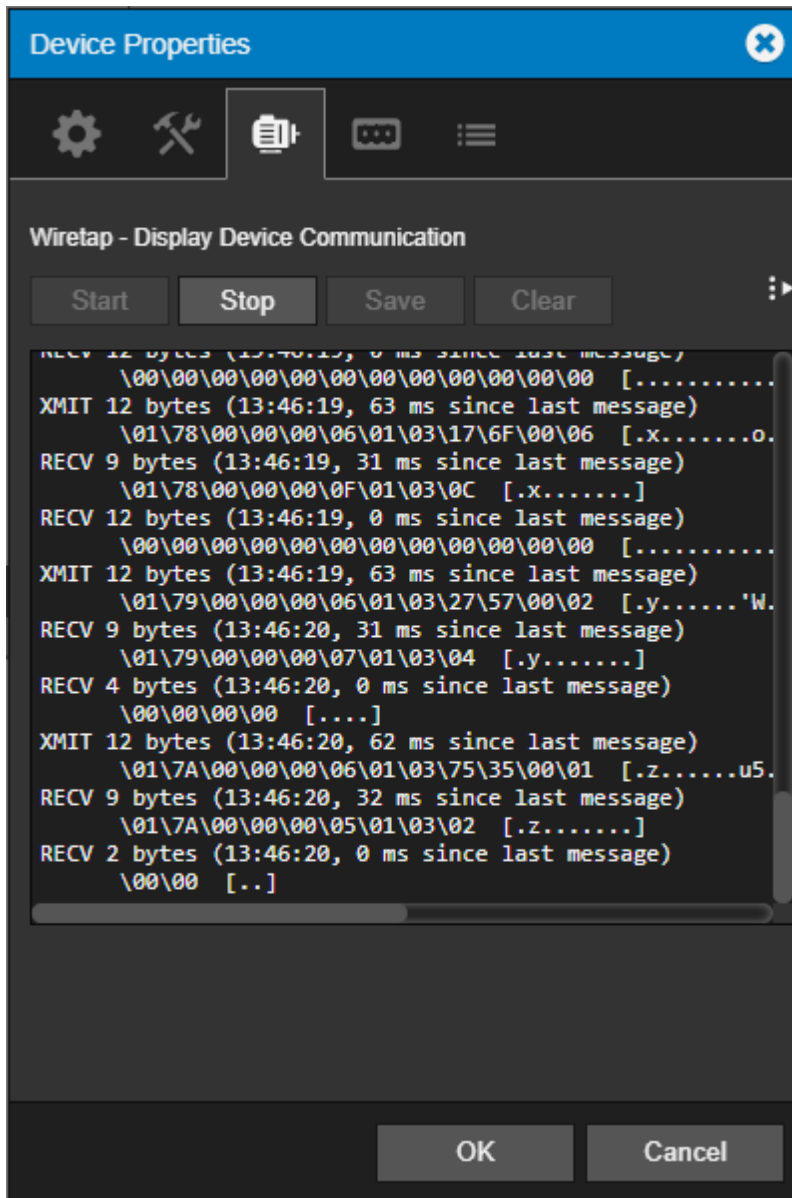
- Data Pipe Properties
- Device Identification
- Communications
- Watchdog Processing

The image shows a 'Device Properties' dialog box with a blue title bar and a close button. Below the title bar is a toolbar with five icons: a gear, a wrench and screwdriver (highlighted with a blue box), a server rack, a speech bubble, and a hamburger menu. The main area is divided into four sections: 'Data Pipe Properties' with fields for IP Address (10.130.151.100) and TCP Port (502); 'Device Identification' with a field for Device ID (1); 'Communications' with fields for Communication Retries (1), Scan Interval (msec) (1000), First-B Timeout (msec) (2500), and Inter-B Timeout (msec) (500); and 'Watchdog Processing' with a checked 'Enable Watchdog' checkbox and a 'Time (min):' field set to 5. At the bottom are 'OK' and 'Cancel' buttons.

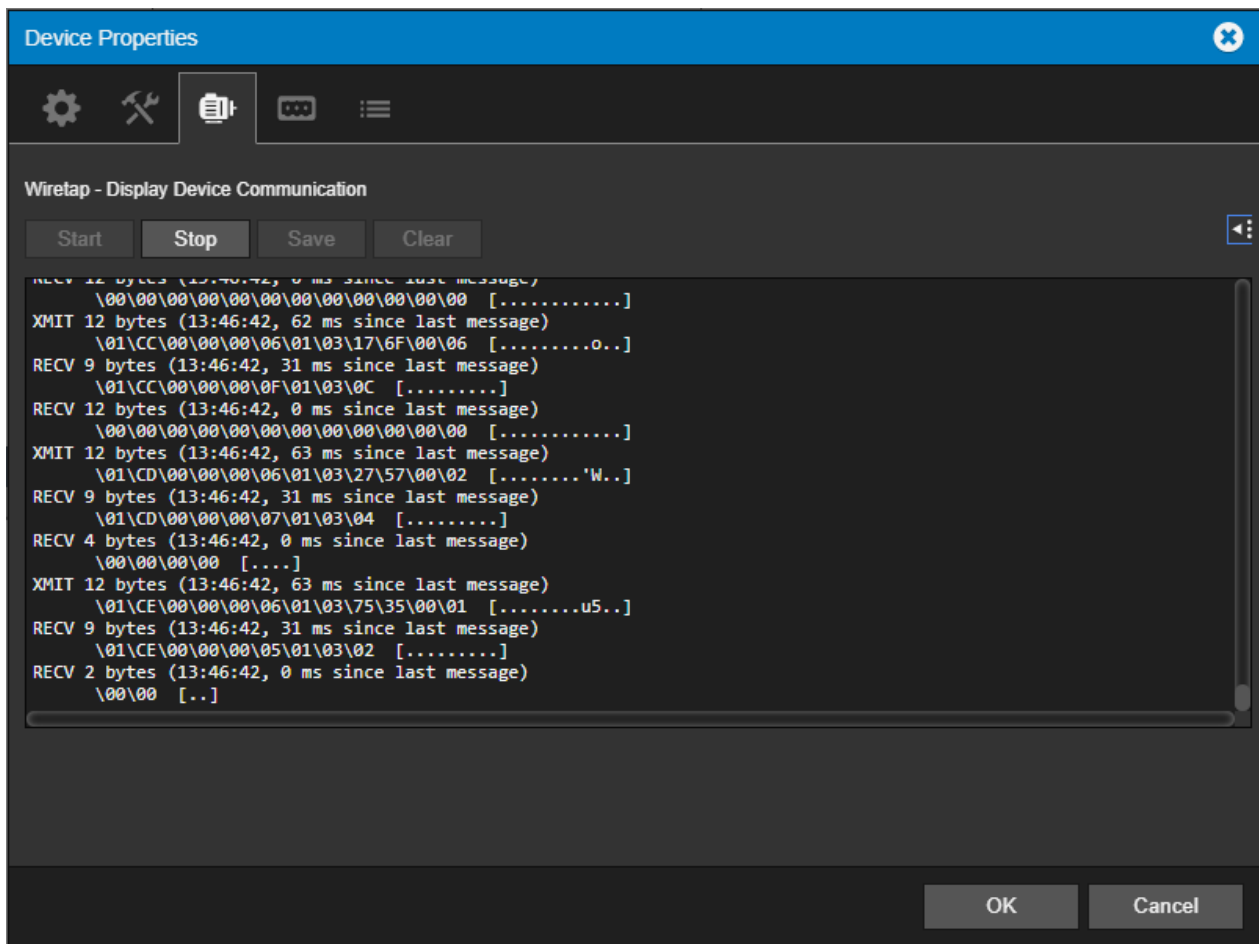
Section	Field	Value
Data Pipe Properties	IP Address:	10.130.151.100
	TCP Port:	502
Device Identification	Device ID:	1
Communications	Communication Retries:	1
	Scan Interval (msec):	1000
	First-B Timeout (msec):	2500
	Inter-B Timeout (msec):	500
Watchdog Processing	<input checked="" type="checkbox"/> Enable Watchdog	
	Time (min):	5

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.

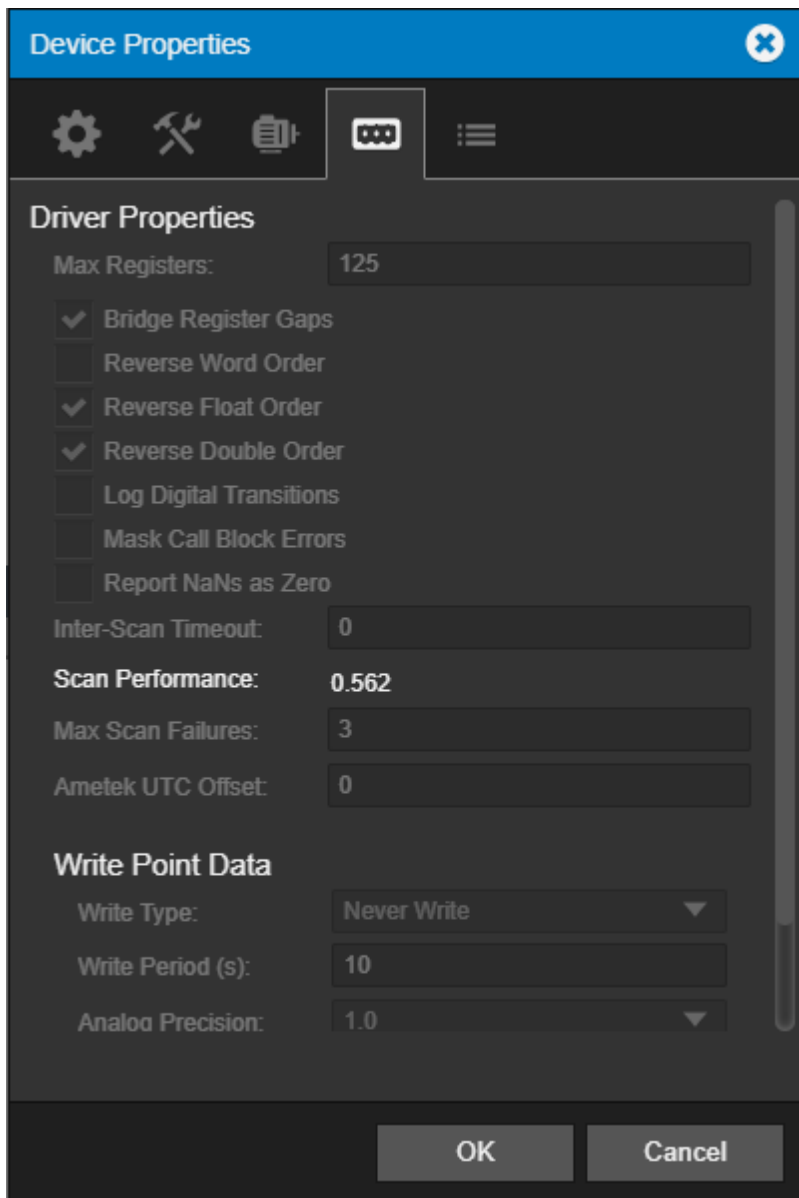


Device Properties - Wiretap (Expanded display)



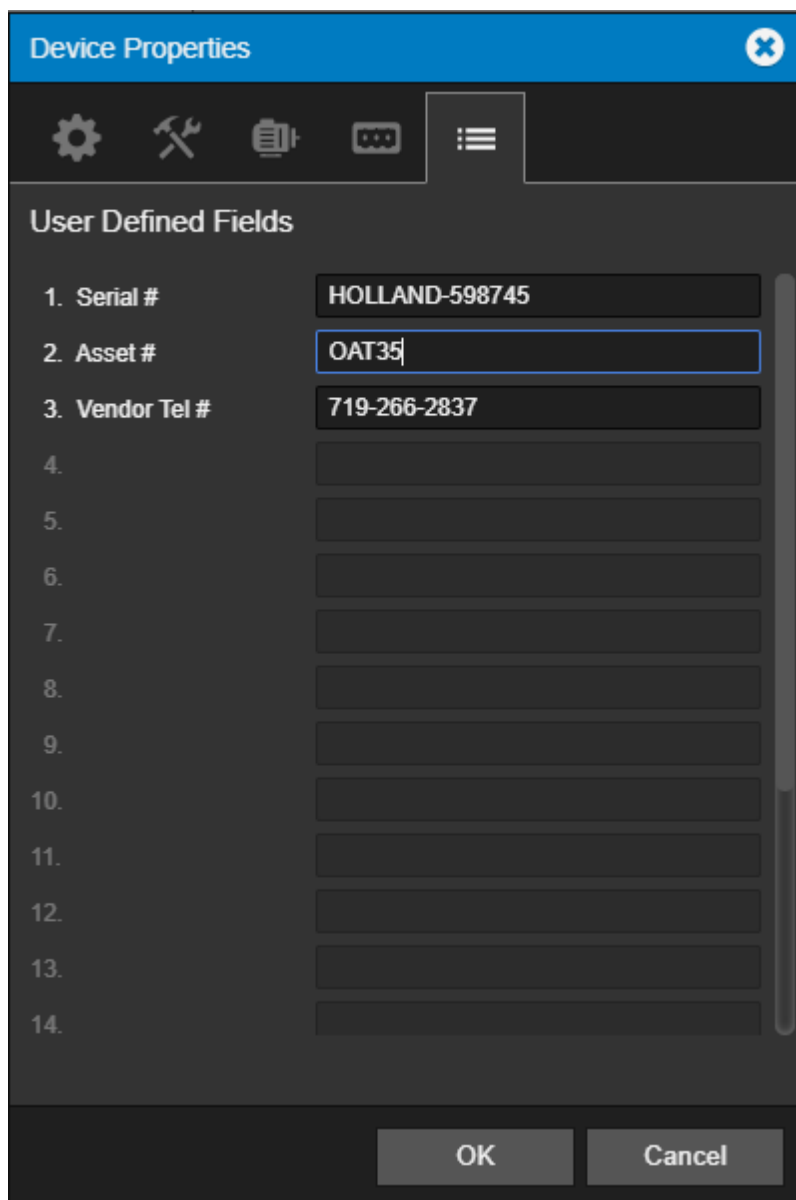
Device Properties - Driver Properties

Certain Foreseer communication drivers may include configurable driver properties that control characteristics in communications with field-bus devices. If supported, this tab may be visible. It's contents will vary depending on the type of device driver. Consult device driver documentation for additional information.



Device Properties - Custom Properties

The Custom Properties tab will display any custom channel properties that may have been defined or created in the system configuration.



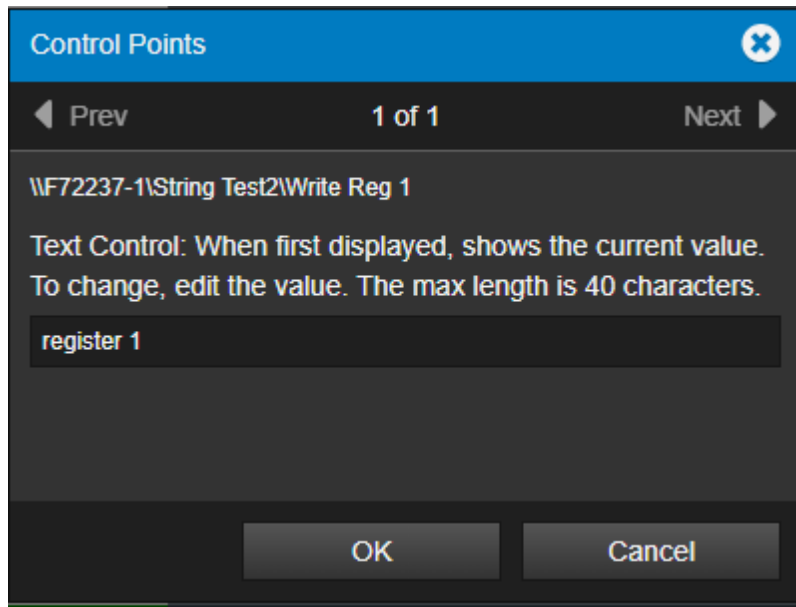
Text Control Points

Text Control Points allows a driver-defined Text channel (installed with a .vi file) to be used as a Text Control Point. A Text Control Point works similar to a regular Control Point. The main difference between regular and Text Control Points is that regular Control Points are user-defined Analog or user-defined Digital channels, using one of the Control Point equations, while Text Control Points are Text channels that are installed with a .vi file for the Modbus3 driver.

To create a Text Control Point after the channel has been installed with an appropriate .vi file, add the Text channel to a WebViews page and add a checkbox to the channel and save the page. To write a new Text value to a Text Control Point, select the checkbox for the channel on a WebViews page, and then from the Objects menu (at the top of the page), select Control. This will display a modal dialog with an edit control that shows the current channel value. To write a new value, edit the text in the edit control and select OK. All printable ASCII characters are allowed, but be careful to understand how the text values

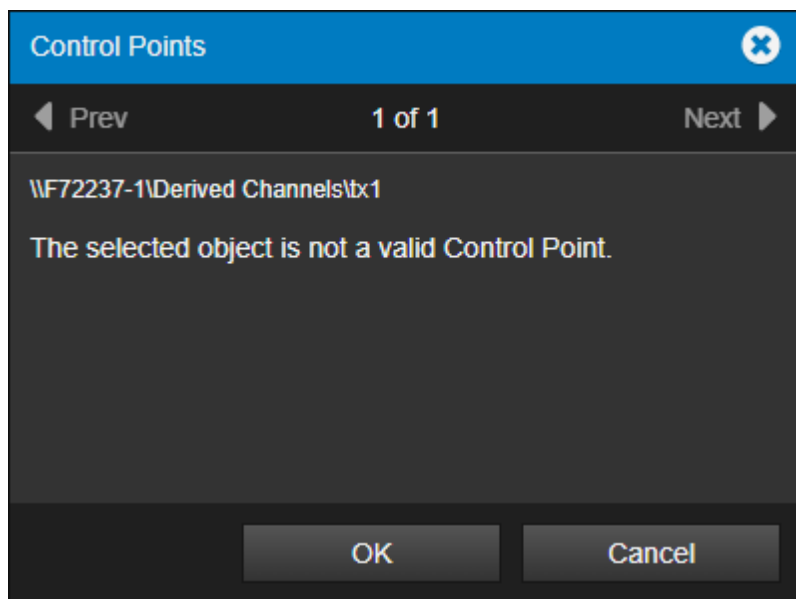
will be used to select which special characters you enter. For example, while quotes (double and single) are allowed, some applications may have issues with them. Be sure you understand how the channel values will be used.

If multiple Control Points are selected, you can use the “Prev” and “Next” buttons to move between the selected Control Points. The full channel name is always shown at the top of the modal dialog, so you can tell which channel you are changing if you have multiple Control Points selected.



When the server receives the request to write a new value, it will log a message to the server log (LogFile.txt) and write an Audit Log record showing the old value and the new value. The new value will be written to the selected channel, and verified by the driver after the write. To verify that the new value was written correctly, the driver will read the value of the register(s) that were written and verify that the value read matches the value written. If the value read does not match the value written, the driver will log an error message to the driver log (DriverLogFile.txt).

For a Text channel to be a valid Text Control Point, it must be a driver defined Text channel (not a user-defined channel). It must have a Read/Write status of eReadWriteAssign, and it must be using the 7-Modbus3.dll with version 7.5.0.2 or newer. If all of the requirements are not met, the following dialog will appear when the channel is selected as a Text Control Point:



Text Control Points must be installed with a .vi file. You cannot add the channel after the device is installed using "Add Channel". To add a writeable Text channel to a .vi file, the device must support writable Text channels, and meet the following requirements:

- Must use a supported Modbus3 driver (Version 7.5.0.2 or newer).
- Must be driver defined Text points: Type=TEXT with POINT=x (where x is not -1).
- Must be write on assignment: RW=READWRITEASSIGN
- Must be a Holding Register: RegType="H" with character DataType="C"
- The max string length supported is from NumRegs="xx" where there are 2 characters per register, so NumRegs="20" would be 40 characters.

The following is an example of the syntax for a writable Text channel in a .vi file:

```
POINT=2
  Name="Write Reg 2" Type=TEXT
  Desc="For Text Control Points"
  RW=READWRITEASSIGN
  Register="21"
  RegType="H"
  DataType="C"
  Bit="0"
  NumReg="20"
ENDPOINT
```

The Point number and Register number (2 and 21 in the above example) will be specific to the device you are installing (as well as the NumRegs value). The RW value must be READWRITEASSIGN, and the RegType must be H (Holding Register), and the DataType must be C (Character Data). The channel type must also be TEXT (Type=TEXT). The NumReg value will specify the maximum string length for the channel. There are 2 characters per register, so for the example above, the value 20 would be a maximum string length of 40. Please note that only specific Modbus devices will support writable Text channels.

When Channel Properties are displayed for writable Text channels, the Value field will not be present. The Value field is used to assign a user-defined Text channel a new value. The only way to assign a new value to a writable Modbus Text channel is to use the Text Control Point feature in a WebViews page. Remote Text channels from Outpost or Foreseer can be valid Text Control Points and be written the same way as local Text channels. All of the same rules apply for remote channels, they must be driver-defined Text channels installed on the remote with a .vi file. Just add them to a WebViews page the same way you would add a local channel.

If the device with a writable Text channel is offline when a new value is written from a Text Control Point, the value will not be written until the device comes online. If the server is restarted before the device comes online, the new value will not be written and would have to be written again. Although writing to a device that is offline is allowed, best practices would be to only write to devices that are online. Also, be aware that it may take a few seconds before the new channel value is shown after you write it. The amount of time will depend on the scan time of the driver and how many Modbus channels are in the device. Remote channels may take a few seconds longer for the new value to appear.

There is one known issue that when channel properties are displayed in WebViews/WebConfig for a remote Text Control Point channel, the Channel Value field will be displayed. Changing the value from this field will be ignored. Local Text Control Points will not show the Channel Value field in the properties.

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

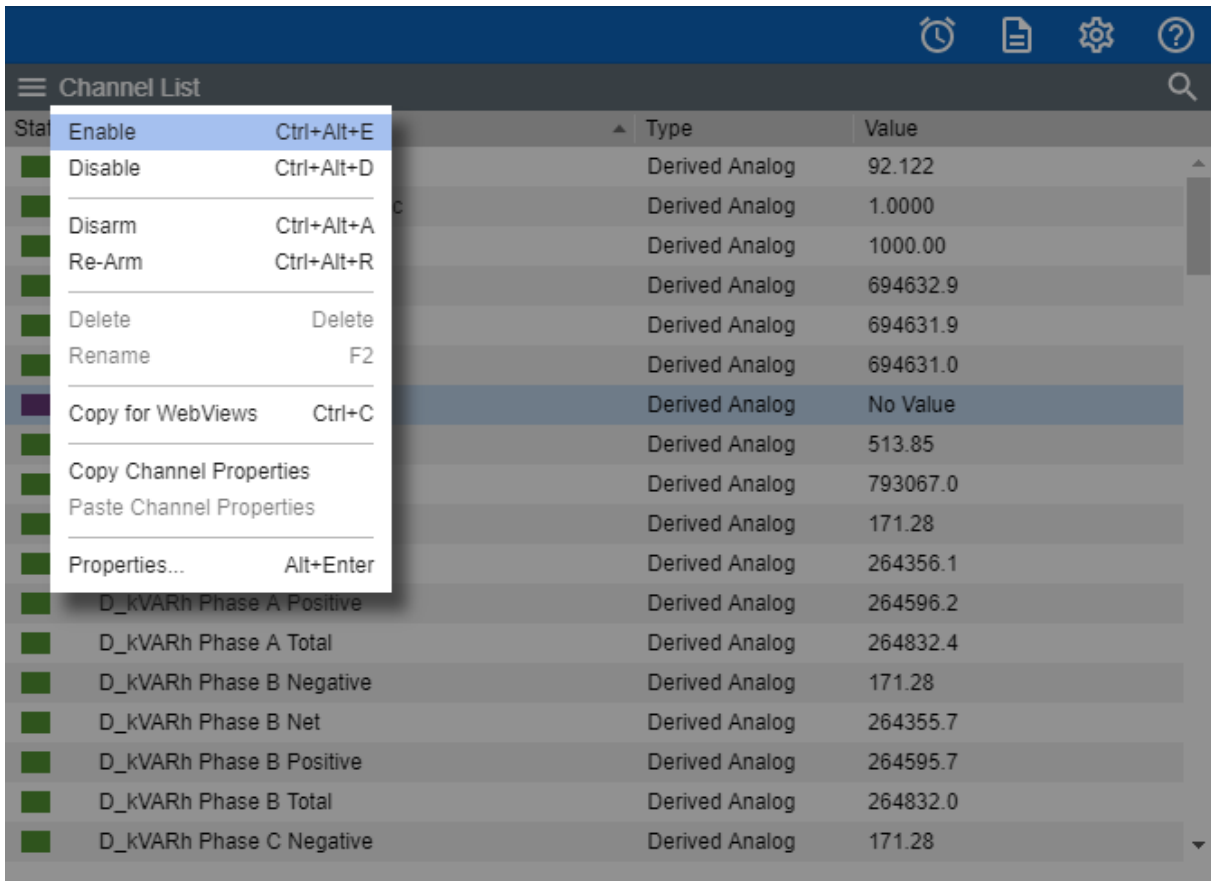
The enable command resumes data archiving for the selected Channel.

To Enable a channel:

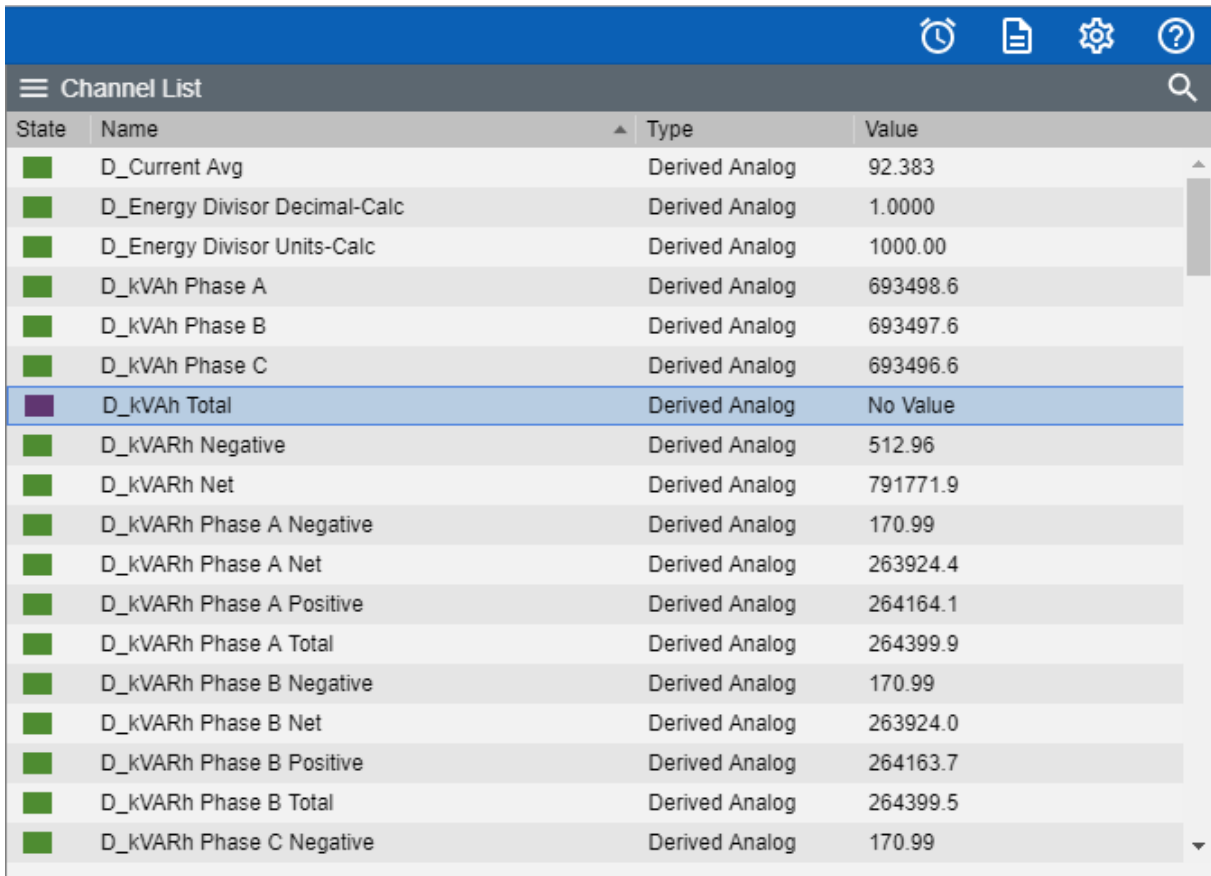
1. Select the channel you would like enabled:

Channel List			
State	Name	Type	Value
<input type="checkbox"/>	D_Current Avg	Derived Analog	92.213
<input type="checkbox"/>	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
<input type="checkbox"/>	D_Energy Divisor Units-Calc	Derived Analog	1000.00
<input type="checkbox"/>	D_kVAh Phase A	Derived Analog	694447.9
<input type="checkbox"/>	D_kVAh Phase B	Derived Analog	694446.9
<input type="checkbox"/>	D_kVAh Phase C	Derived Analog	694445.9
<input checked="" type="checkbox"/>	D_kVAh Total	Derived Analog	No Value
<input type="checkbox"/>	D_kVARh Negative	Derived Analog	513.70
<input type="checkbox"/>	D_kVARh Net	Derived Analog	792855.9
<input type="checkbox"/>	D_kVARh Phase A Negative	Derived Analog	171.23
<input type="checkbox"/>	D_kVARh Phase A Net	Derived Analog	264285.7
<input type="checkbox"/>	D_kVARh Phase A Positive	Derived Analog	264525.7
<input type="checkbox"/>	D_kVARh Phase A Total	Derived Analog	264761.9
<input type="checkbox"/>	D_kVARh Phase B Negative	Derived Analog	171.23
<input type="checkbox"/>	D_kVARh Phase B Net	Derived Analog	264285.3
<input type="checkbox"/>	D_kVARh Phase B Positive	Derived Analog	264525.3
<input type="checkbox"/>	D_kVARh Phase B Total	Derived Analog	264761.4
<input type="checkbox"/>	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

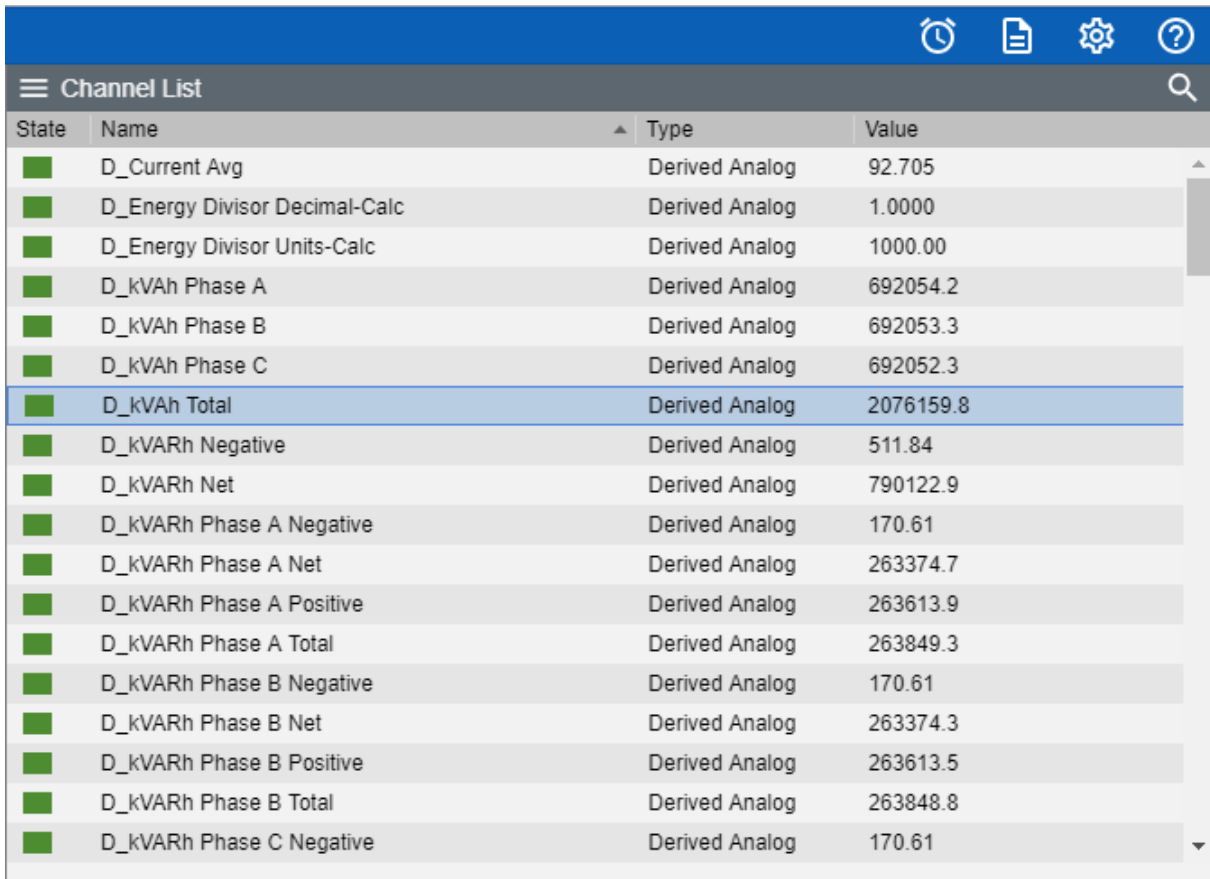


Disable

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

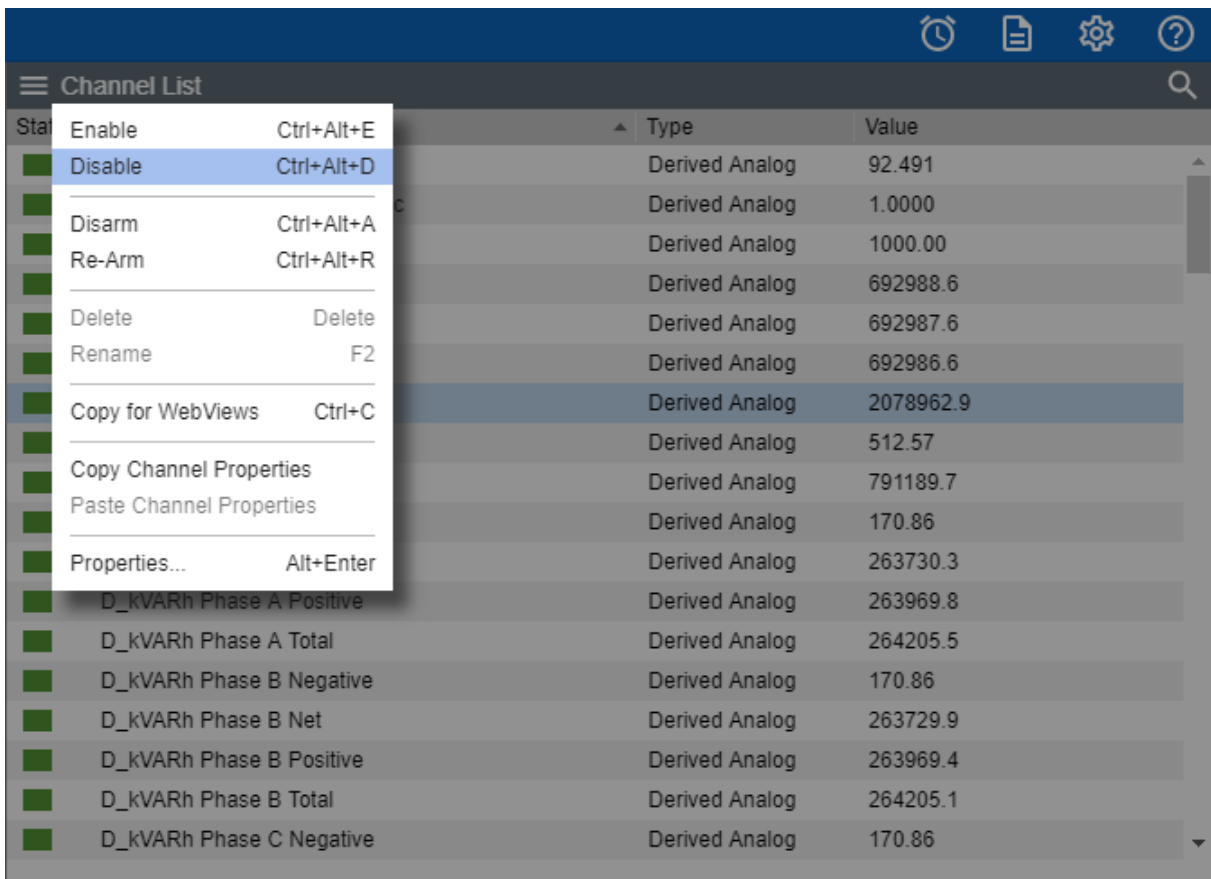
To Disable a channel:

1. Select the channel you would like disabled:

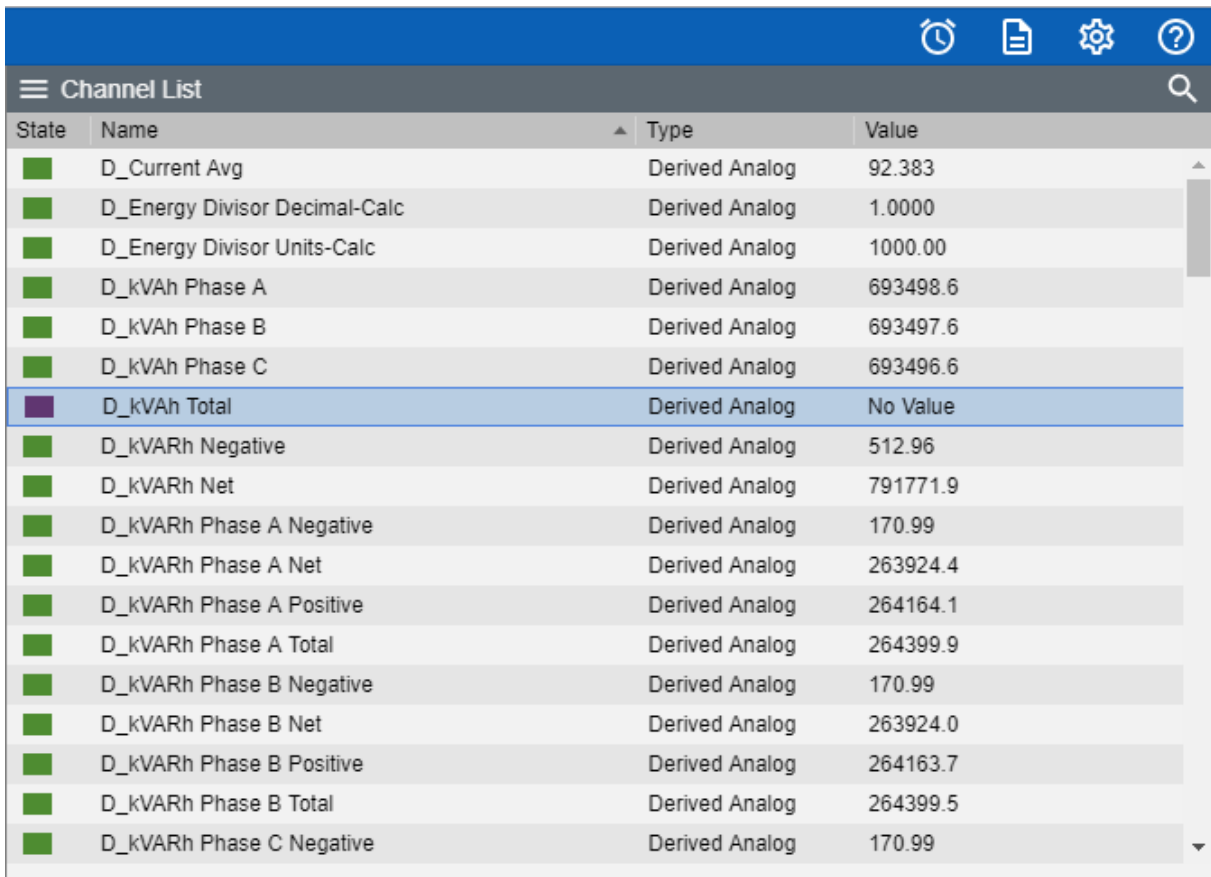


State	Name	Type	Value
■	D_Current Avg	Derived Analog	92.705
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	692054.2
■	D_kVAh Phase B	Derived Analog	692053.3
■	D_kVAh Phase C	Derived Analog	692052.3
■	D_kVAh Total	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

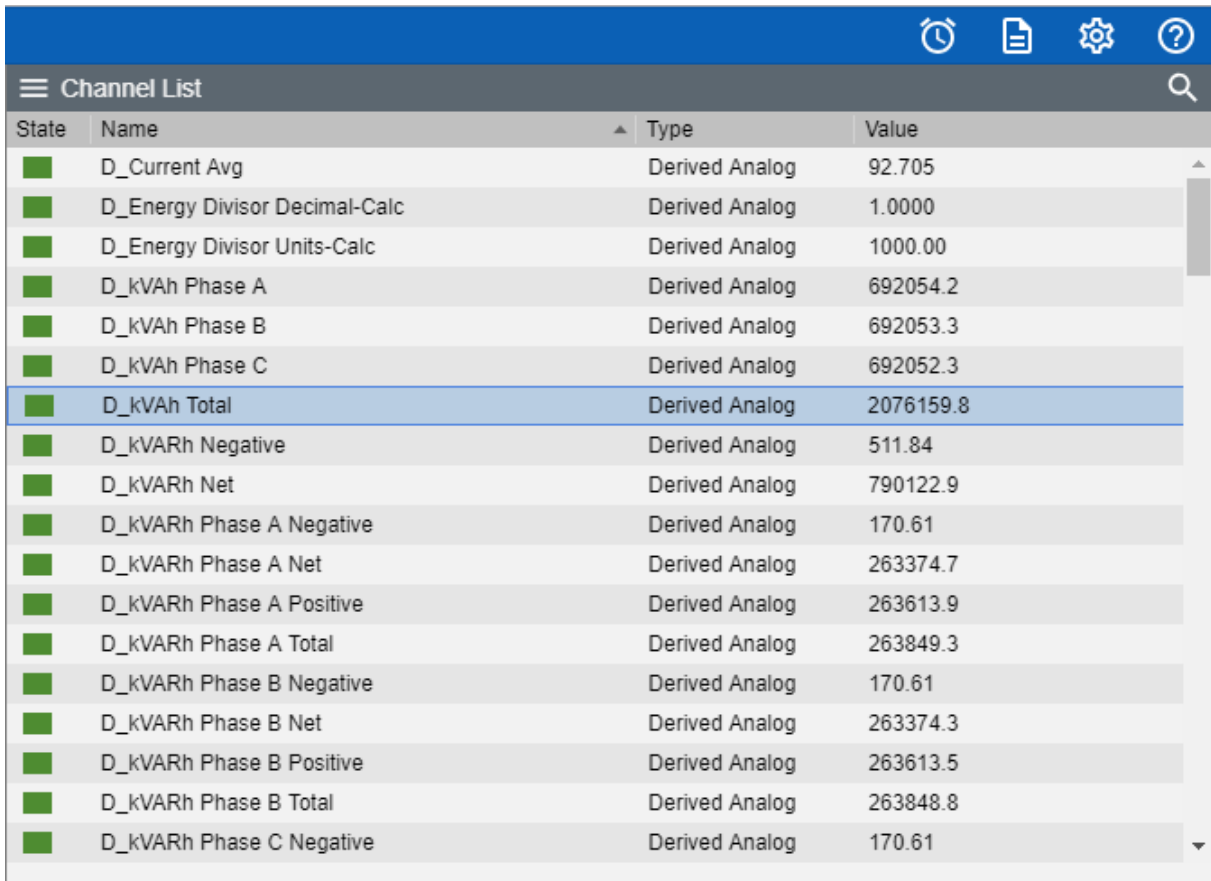


Disarm

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

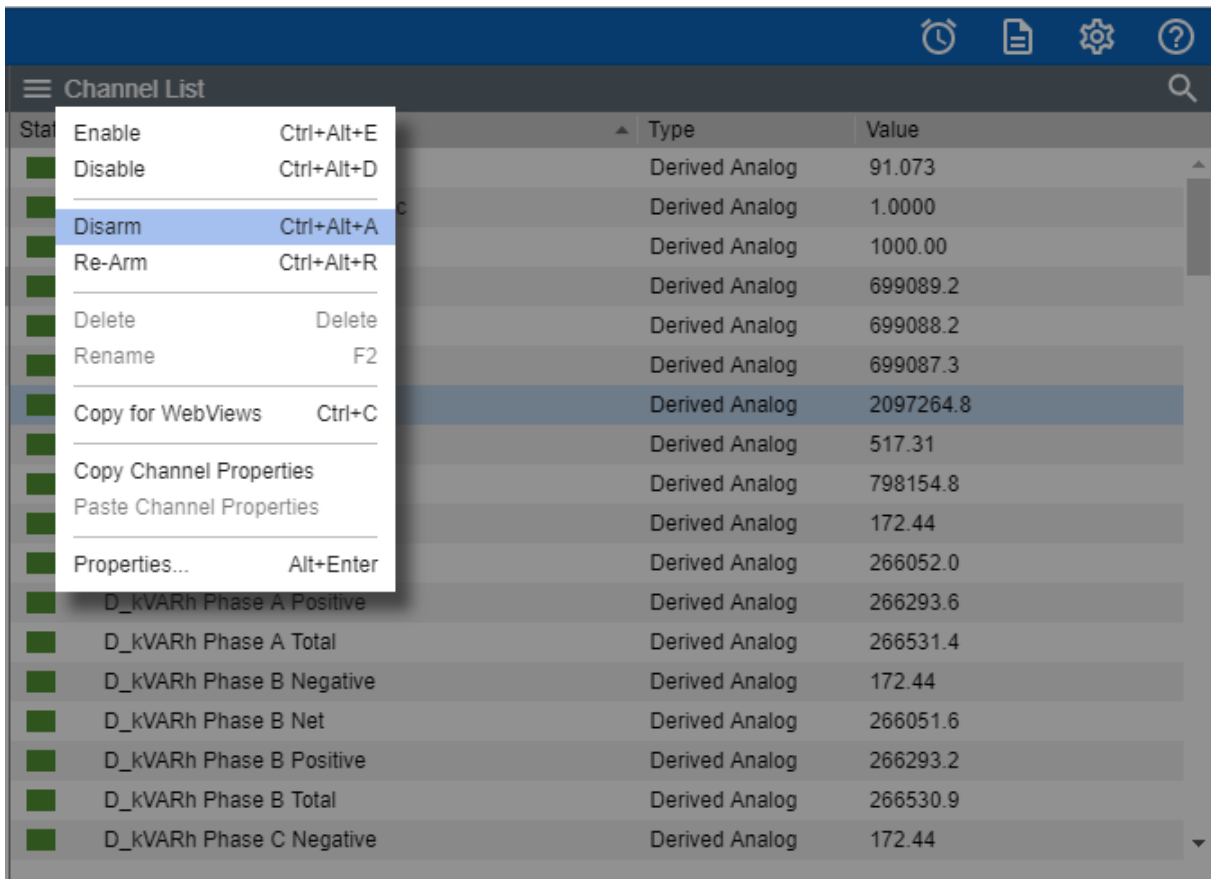
To Disarm a channel:

1. Select the channel you would like disarmed:

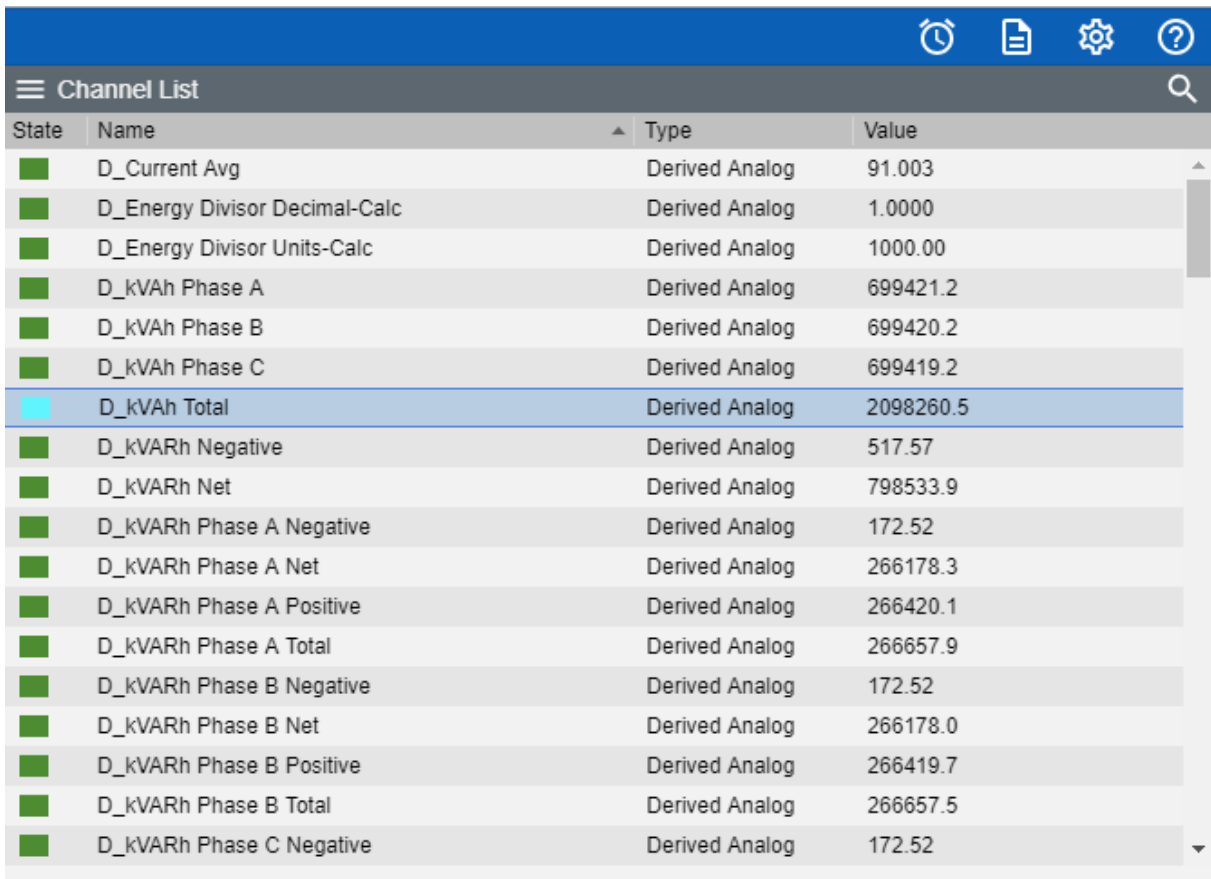


State	Name	Type	Value
■	D_Current Avg	Derived Analog	92.705
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	692054.2
■	D_kVAh Phase B	Derived Analog	692053.3
■	D_kVAh Phase C	Derived Analog	692052.3
■	D_kVAh Total	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

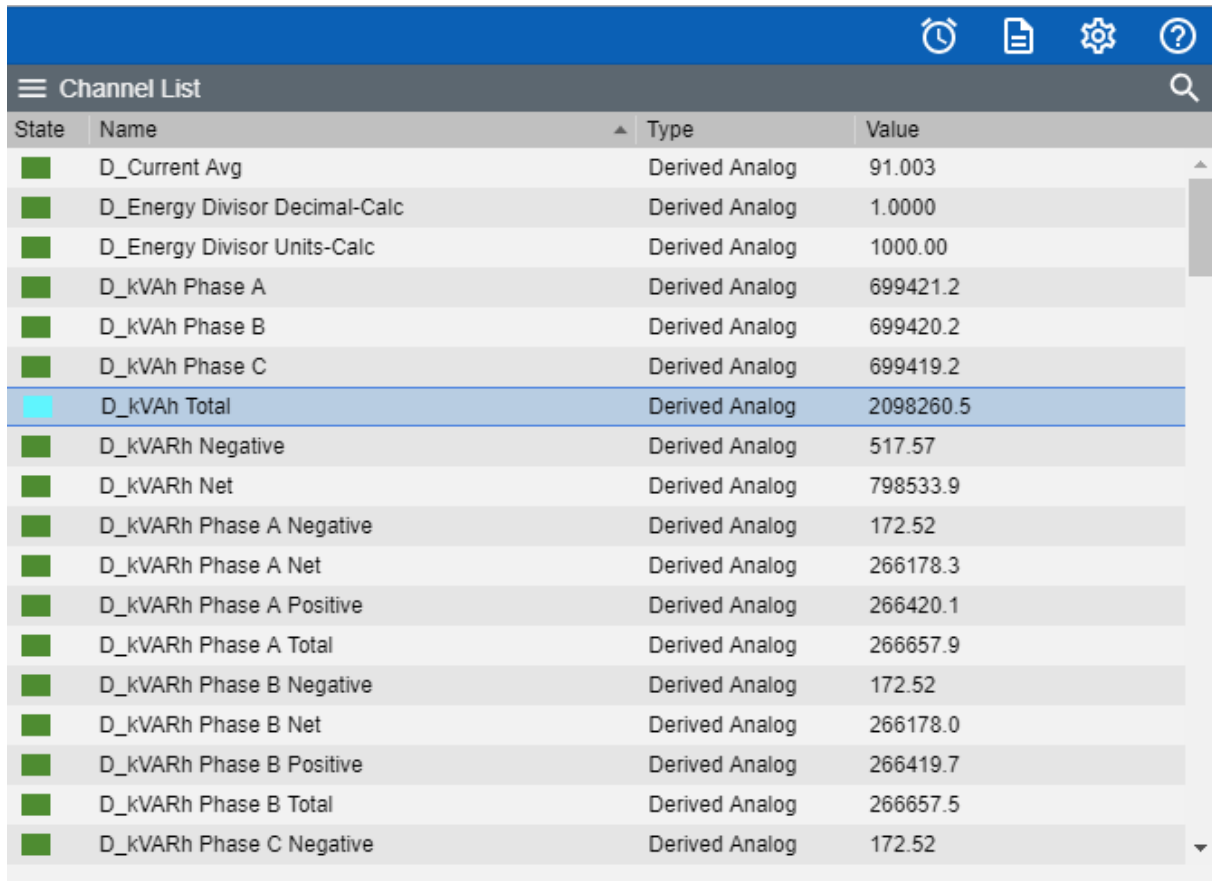


Re-Arm

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

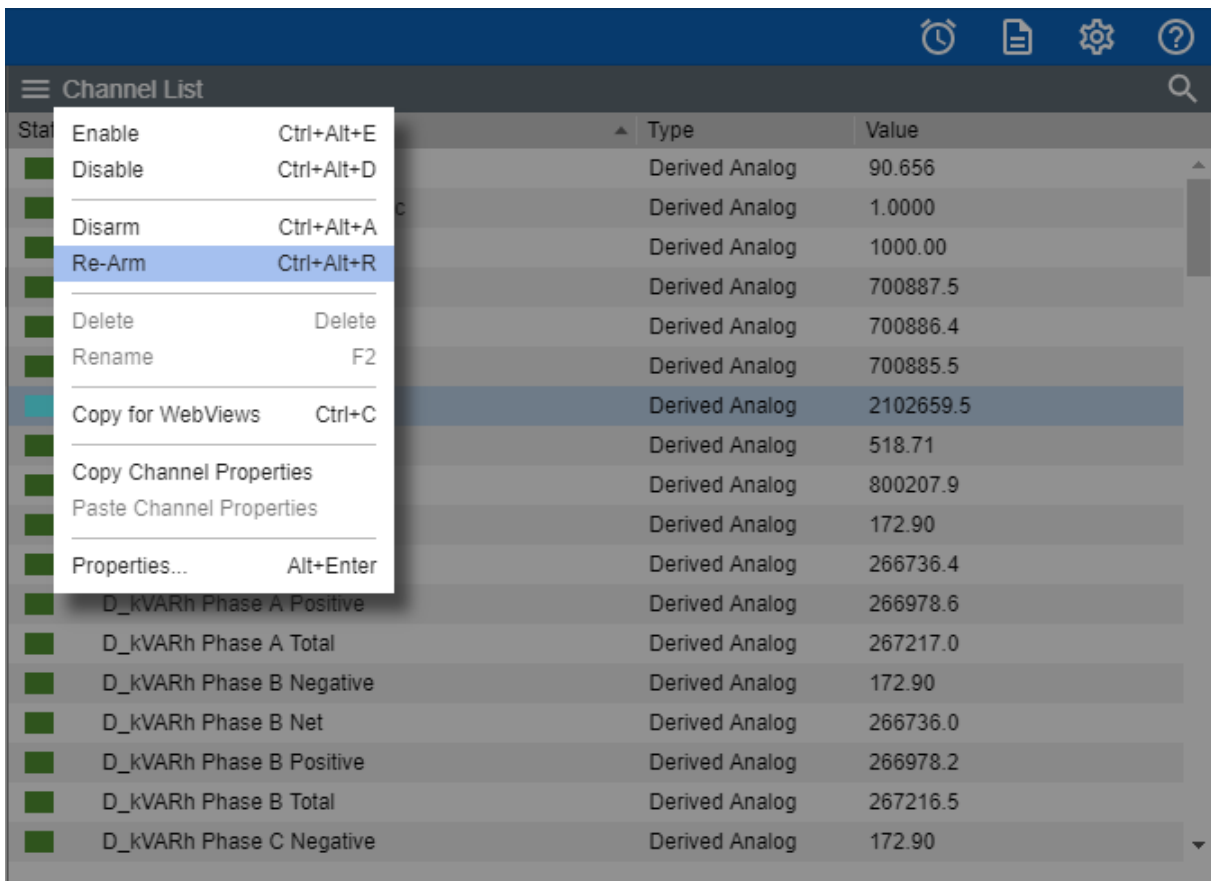
To Re-Arm a channel:

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

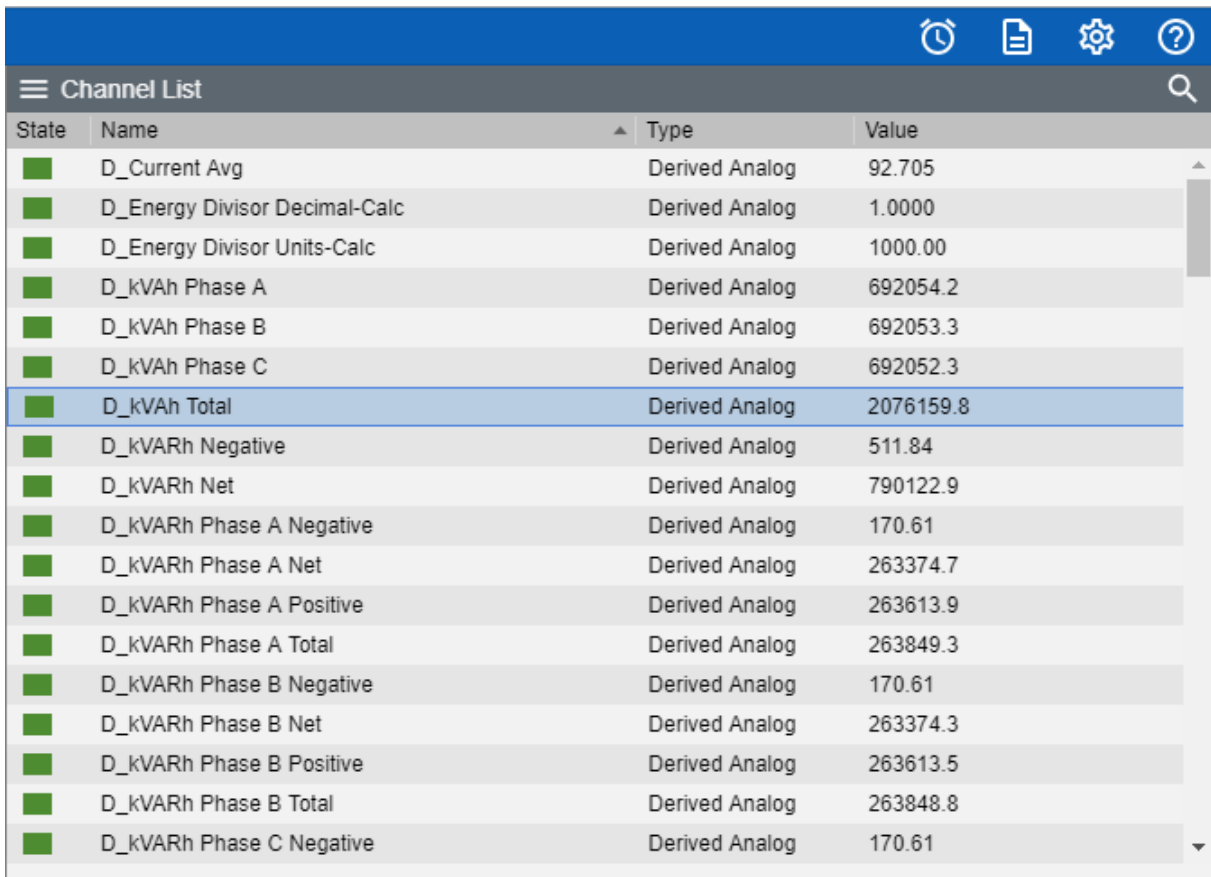


State	Name	Type	Value
■	D_Current Avg	Derived Analog	91.003
■	D_Energy Divisor Decimal-Calc	Derived Analog	1.0000
■	D_Energy Divisor Units-Calc	Derived Analog	1000.00
■	D_kVAh Phase A	Derived Analog	699421.2
■	D_kVAh Phase B	Derived Analog	699420.2
■	D_kVAh Phase C	Derived Analog	699419.2
■	D_kVAh Total	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



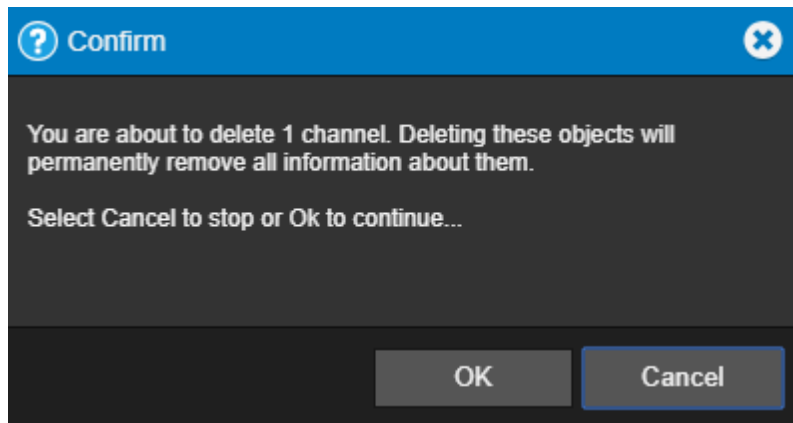
3. The channel will now be in a Re-Armed state



Delete

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

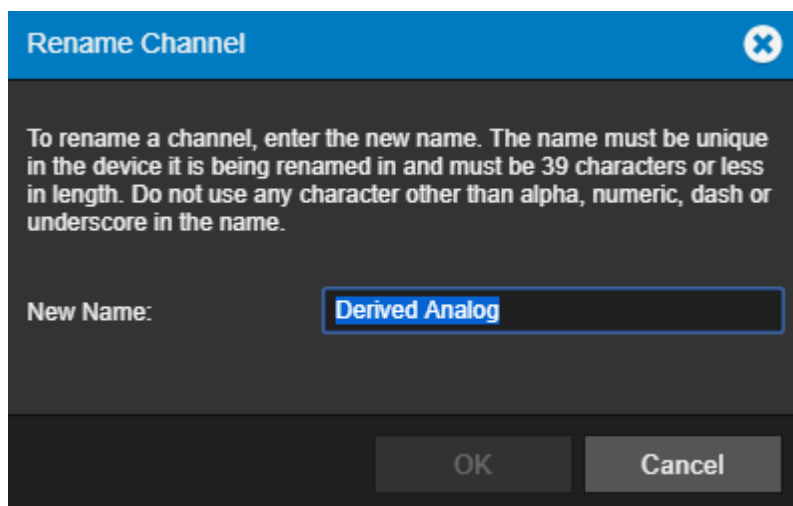
- ✔ Deleting a Channel should be done with discretion as removing it can have an adverse effect on Foreseer WebViews.



Rename

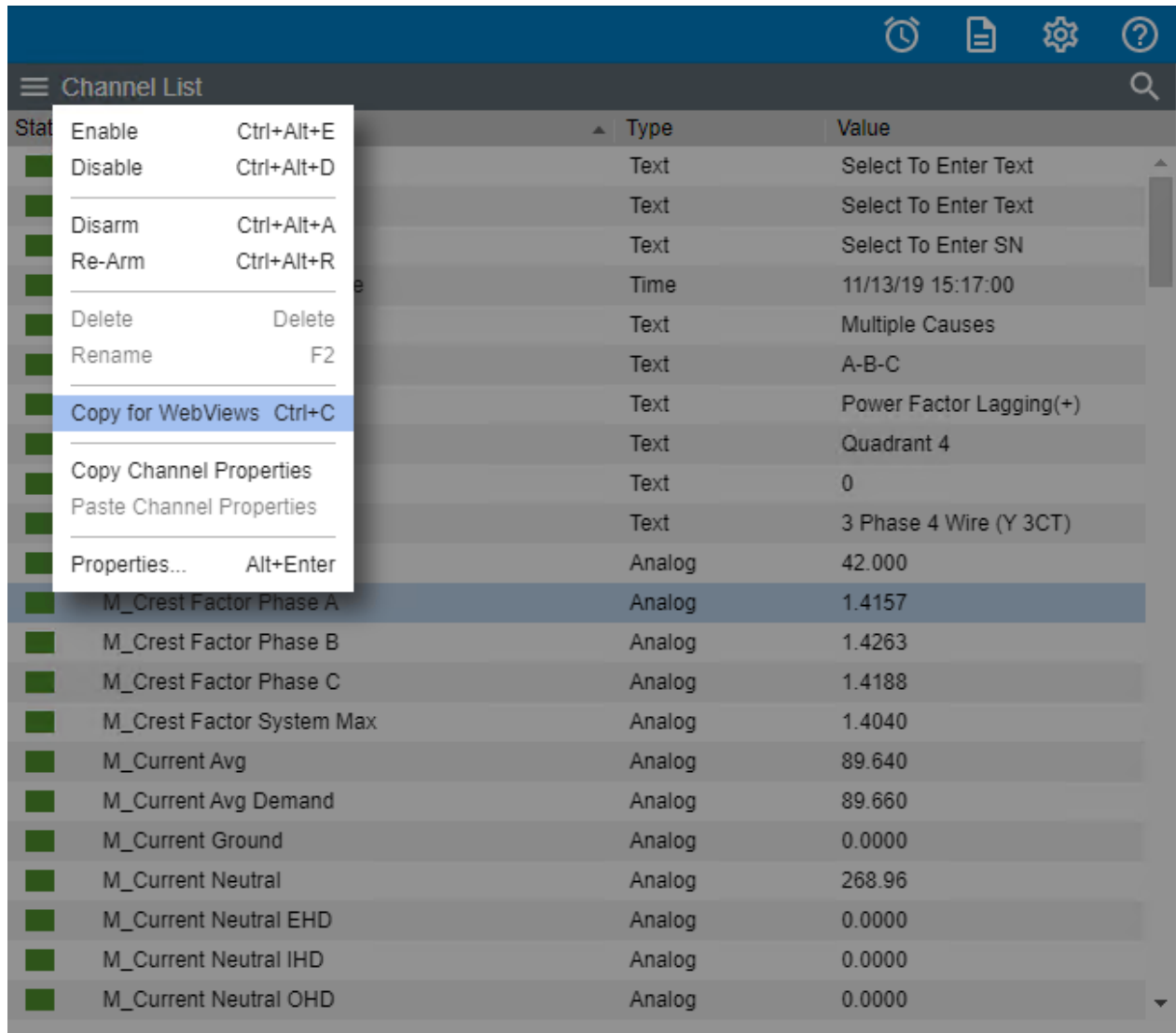
The Rename command renames the selected Channel.

- ✔ 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.

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	1.4120
M_Crest Factor Phase B	Analog	1.3966
M_Crest Factor Phase C	Analog	1.4002
M_Crest Factor System Max	Analog	1.4349
M_Current Avg	Analog	89.717
M_Current Avg Demand	Analog	89.738
M_Current Ground	Analog	0.0000
M_Current Neutral	Analog	269.26
M_Current Neutral EHD	Analog	0.0000
M_Current Neutral IHD	Analog	0.0000
M_Current Neutral OHD	Analog	0.0000

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

Paste Channel Properties

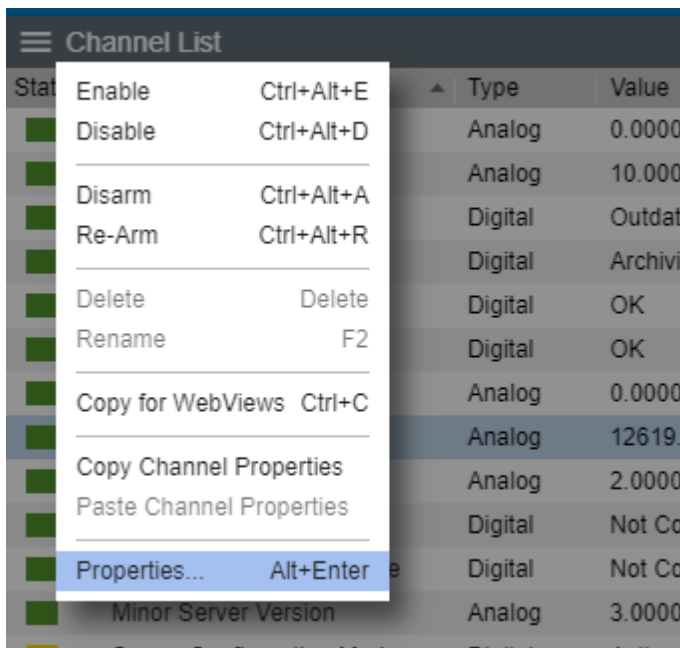
The Paste Channel Properties command pastes the previously copied properties into the currently selected channel as its operational parameters. It also is useful when duplicating numerous channel settings on multiple devices. In either case, the channel or device being pasted into must be of the exact 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.

Stat	Type	Value
Enable	Ctrl+Alt+E	
Disable	Ctrl+Alt+D	Select To Enter Text
Disarm	Ctrl+Alt+A	Select To Enter Text
Re-Arm	Ctrl+Alt+R	Select To Enter SN
Delete	Delete	11/13/19 15:17:00
Rename	F2	Multiple Causes
Copy for WebViews	Ctrl+C	A-B-C
Copy Channel Properties		Power Factor Lagging(+)
Paste Channel Properties		Quadrant 4
Properties...	Alt+Enter	0
M_Crest Factor Phase A	Analog	3 Phase 4 Wire (Y 3CT)
M_Crest Factor Phase B	Analog	42.000
M_Crest Factor Phase C	Analog	1.4261
M_Crest Factor System Max	Analog	1.4049
M_Current Avg	Analog	1.4357
M_Current Avg Demand	Analog	1.4214
M_Current Ground	Analog	90.902
M_Current Neutral	Analog	90.906
M_Current Neutral EHD	Analog	0.0000
M_Current Neutral IHD	Analog	272.75
M_Current Neutral OHD	Analog	0.0000

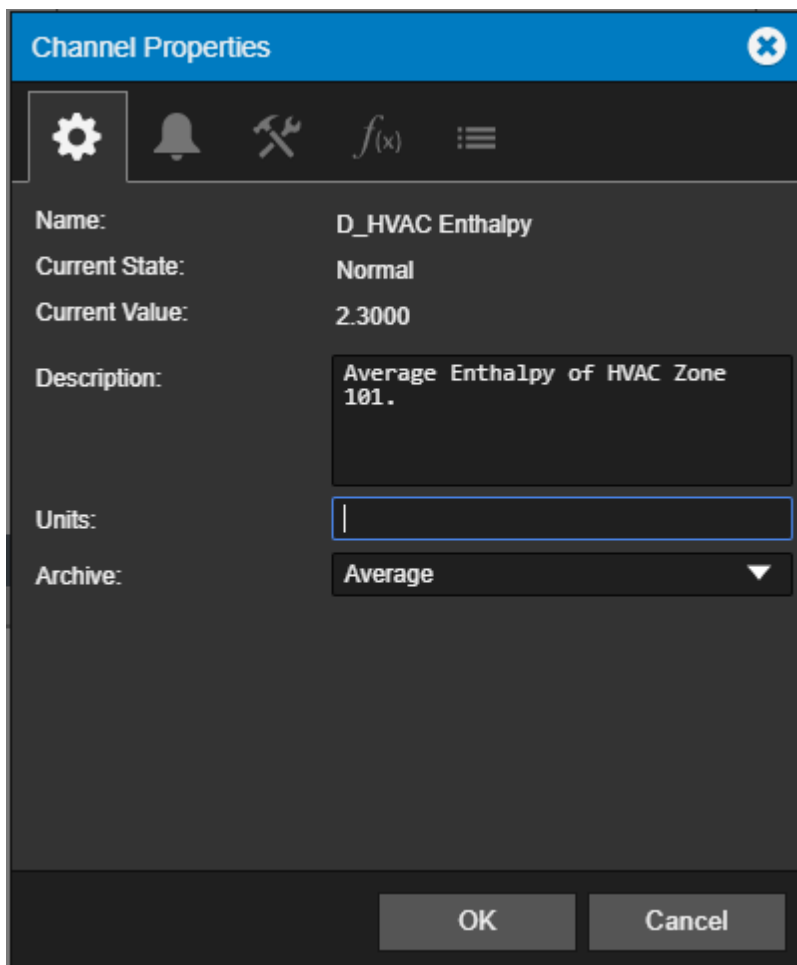
Properties

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

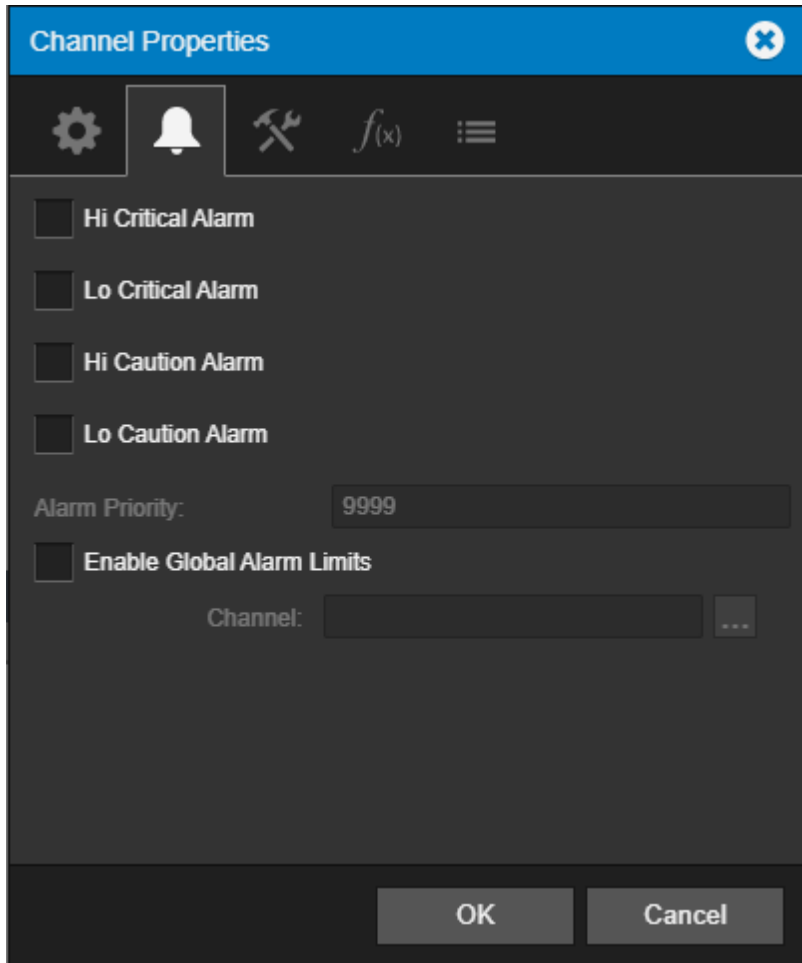
The Properties command furnishes operational information on the Channel. The General tab allows a channel to be Disabled or Enabled as well as providing selections that control how its data is archived on the Server.



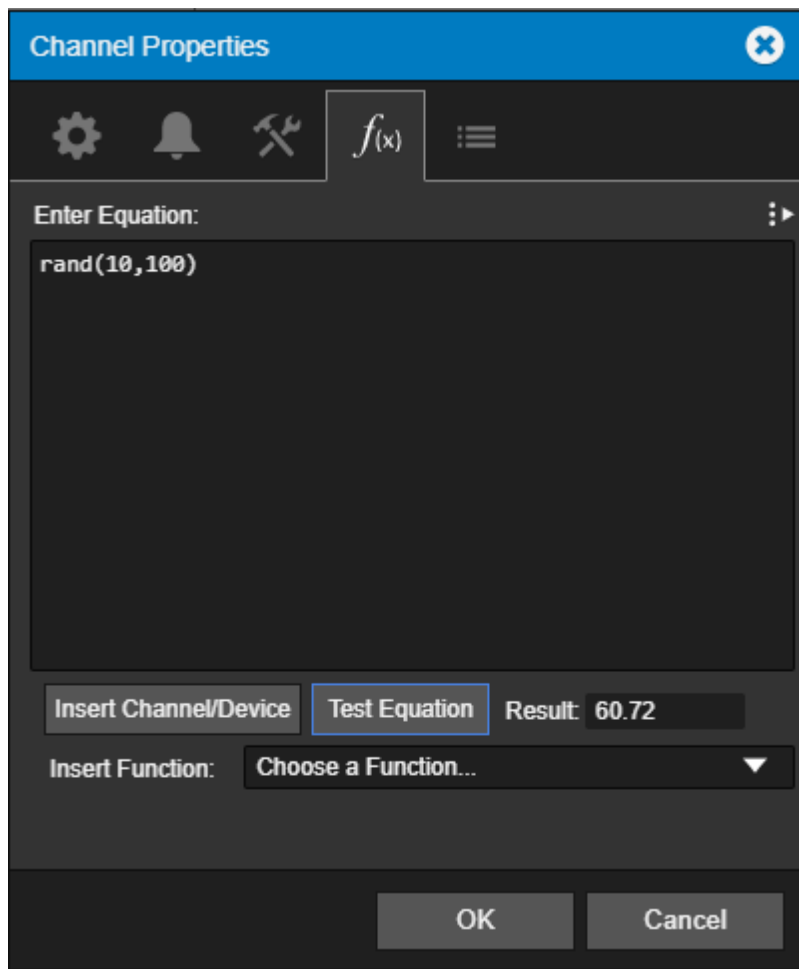
The General tab configures general information regarding the channel itself, including description, units of measure, and archive configuration.



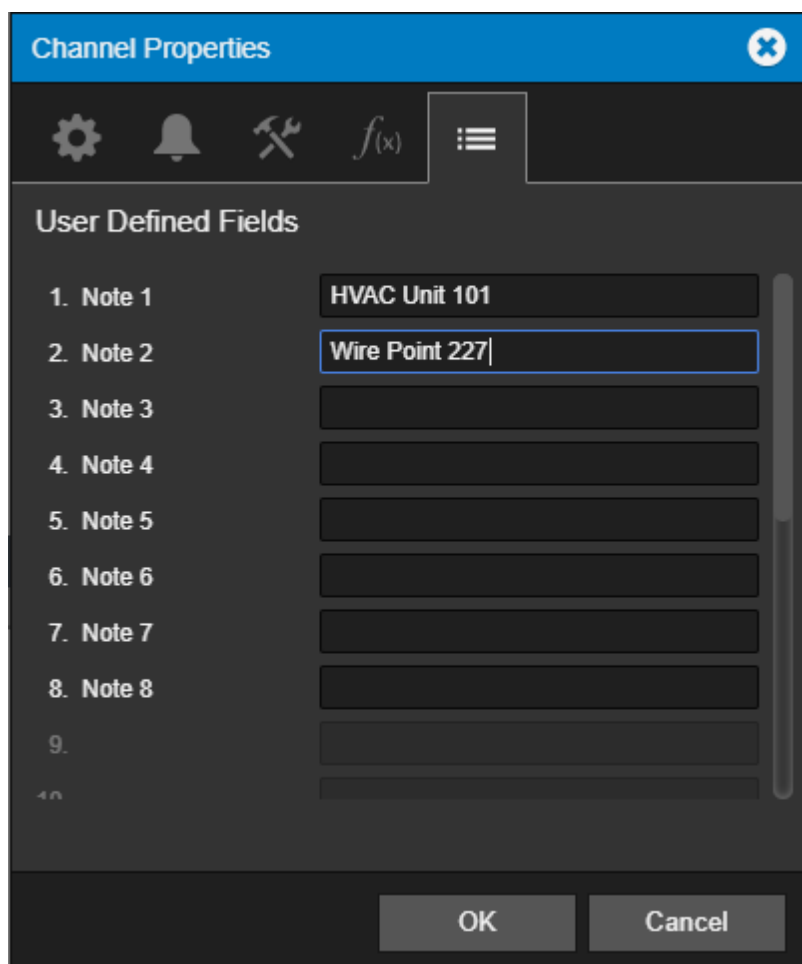
The Alarms tab provides the ability to adjust channel alarm characteristics, including alarm bands, messages, priority, and integration to global alarm limits.



The User-Defined Equation tab provides a viewer and editor for derived equations such as calculation, transfer logic, and other custom logic used by the system.



The Custom Fields tab provides a viewer and editor for any custom properties defined globally across the system configuration.



WebViews Menu

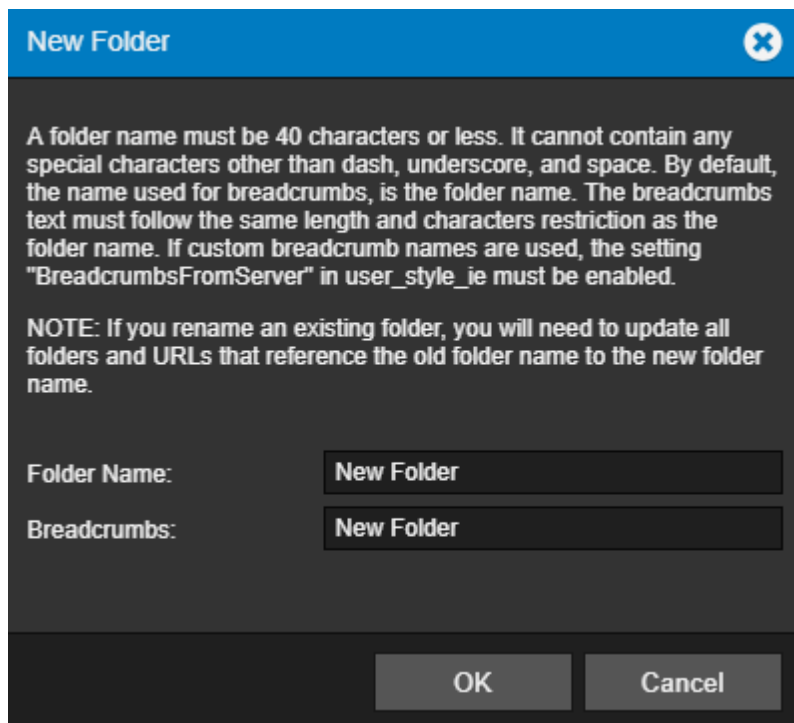
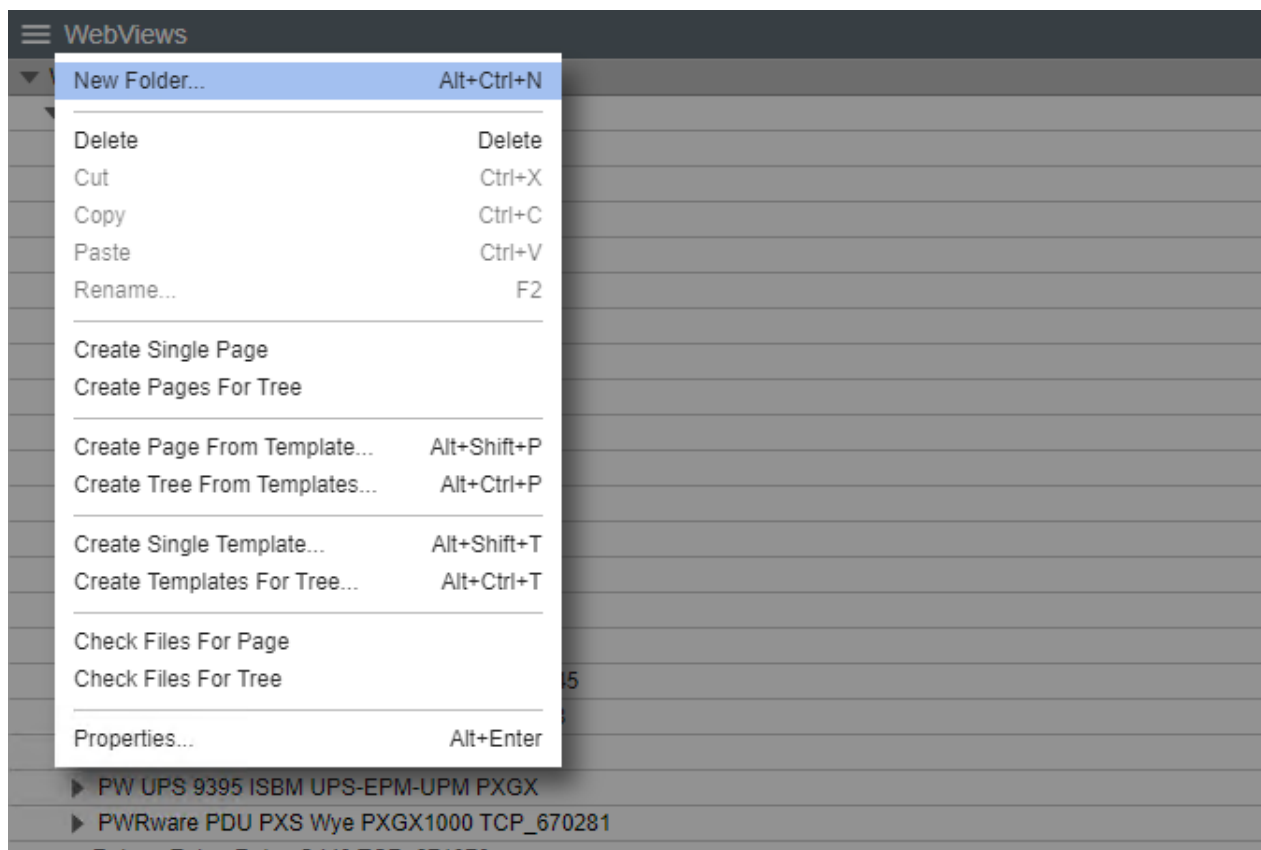
The WebViews List menu provides access to all of the functionality that will be required to manage your Foreseer WebViews files.

- 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

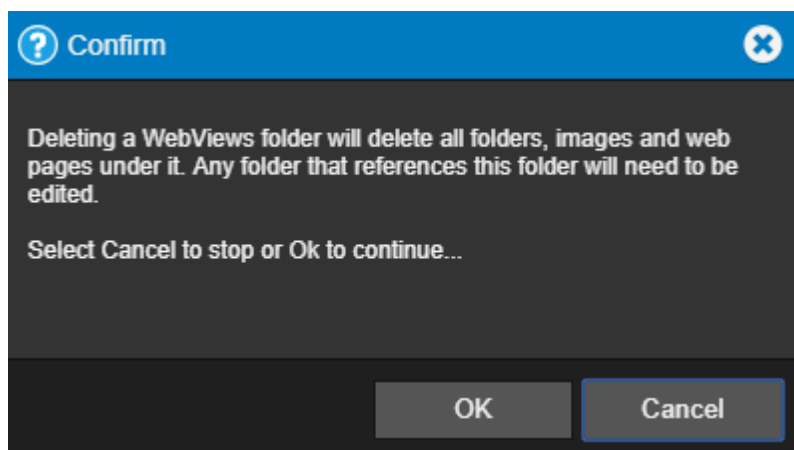
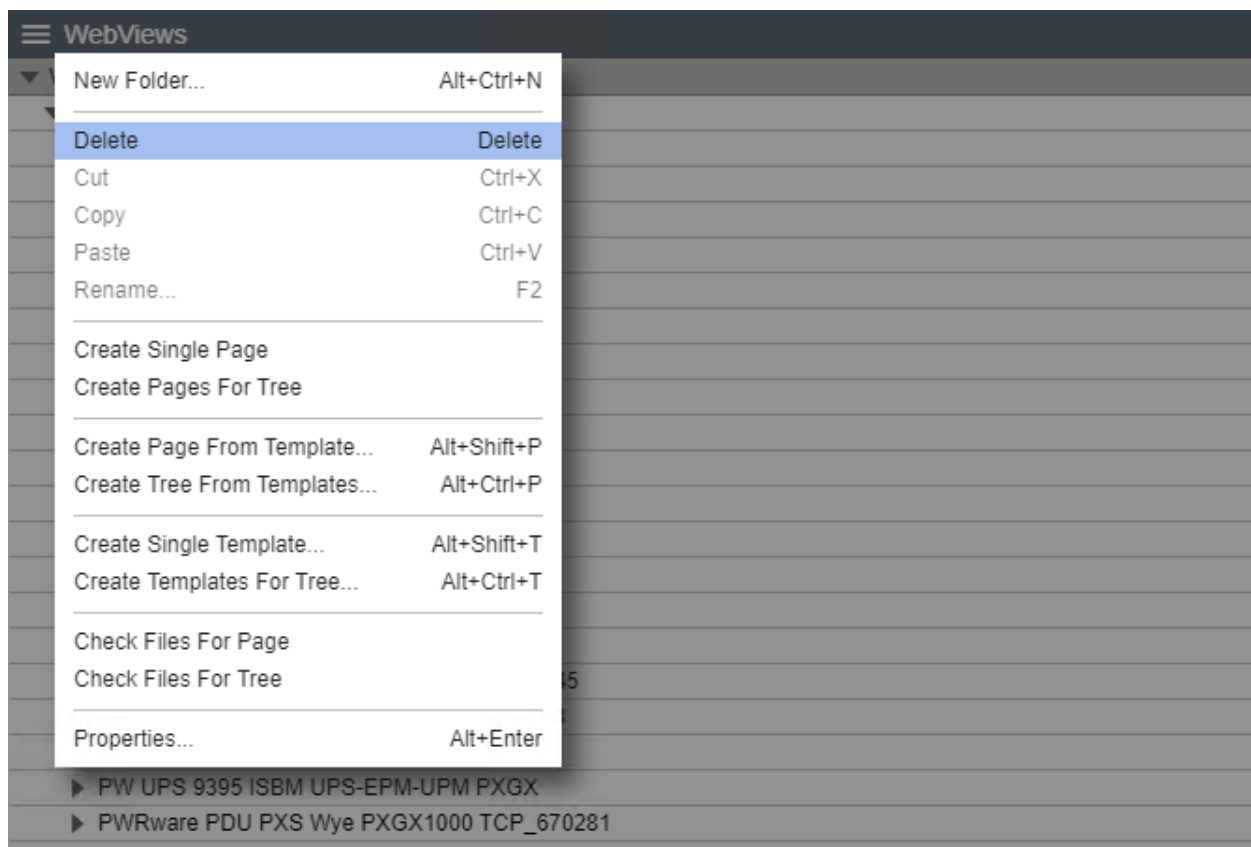
The New Folder command creates a new folder as a child of the currently selected folder.

The corresponding WebViews page is also created.



Delete

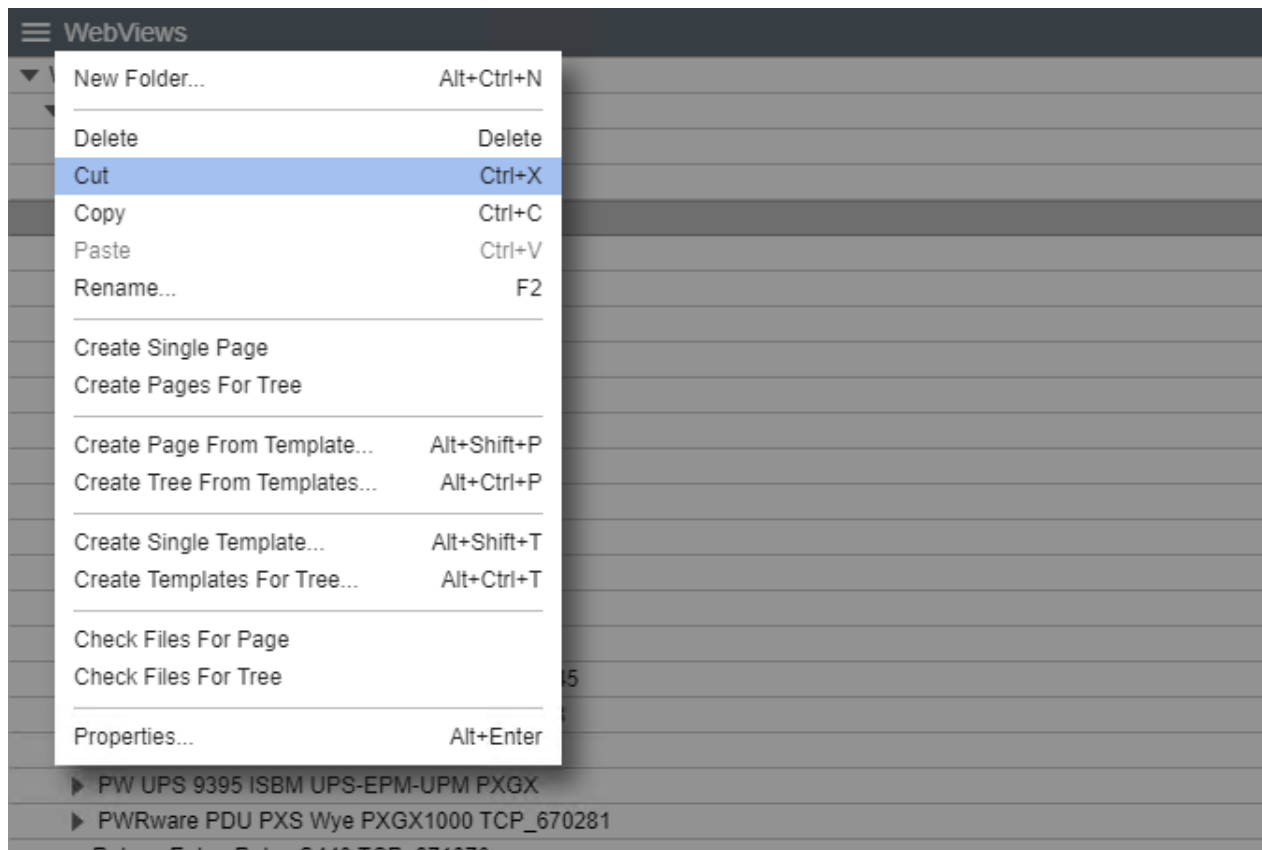
The Delete command deletes the currently selected folder and WebViews page.



✔ 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.

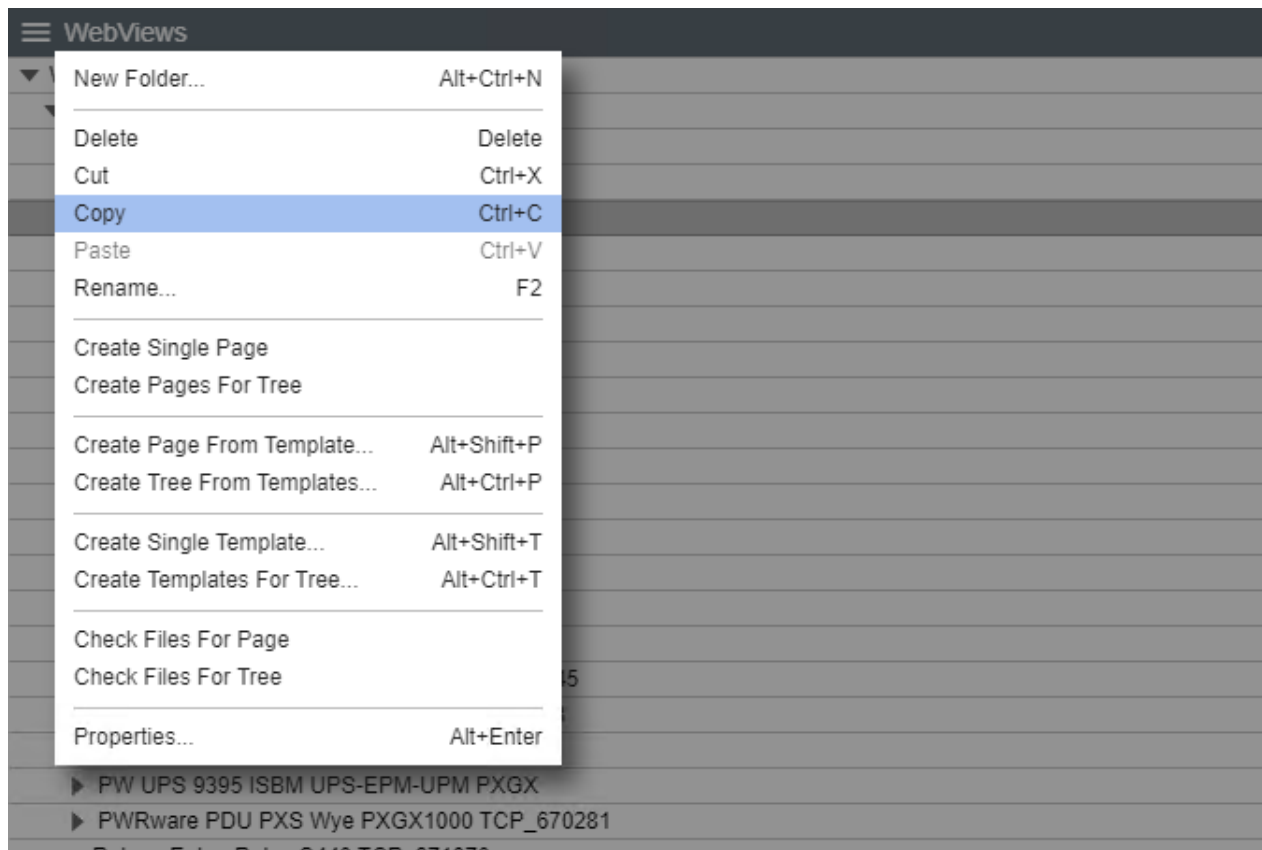
Cut

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.



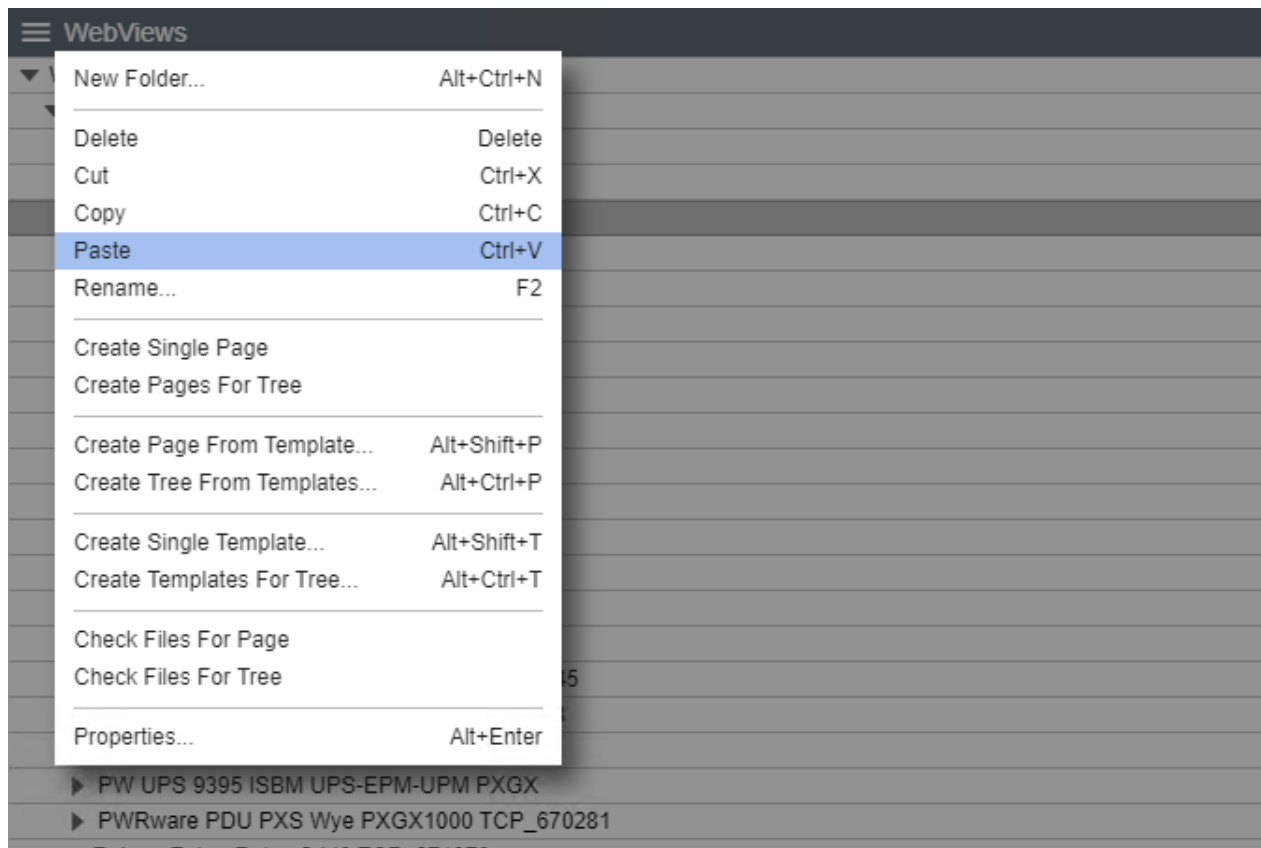
Copy

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



Paste

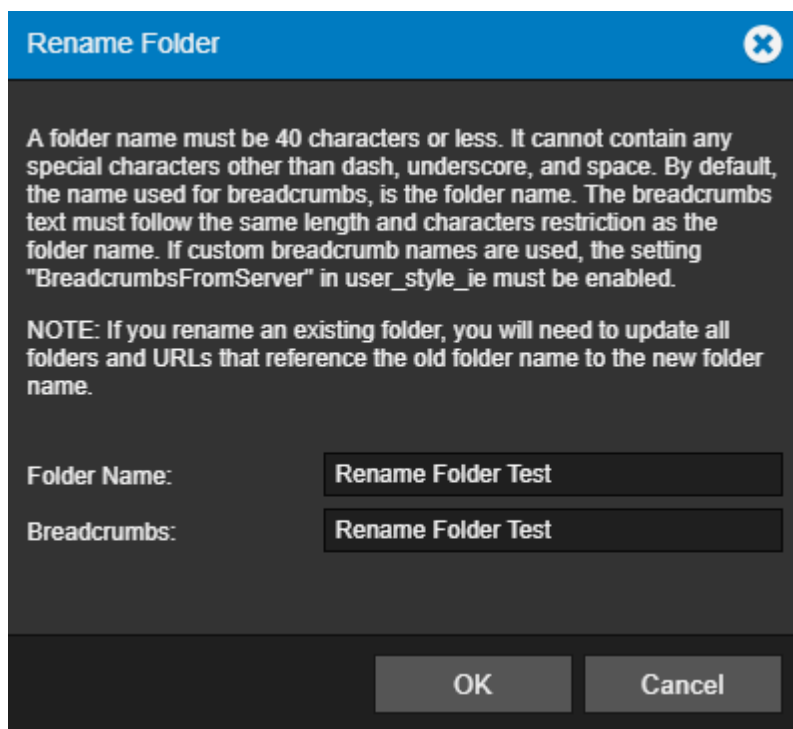
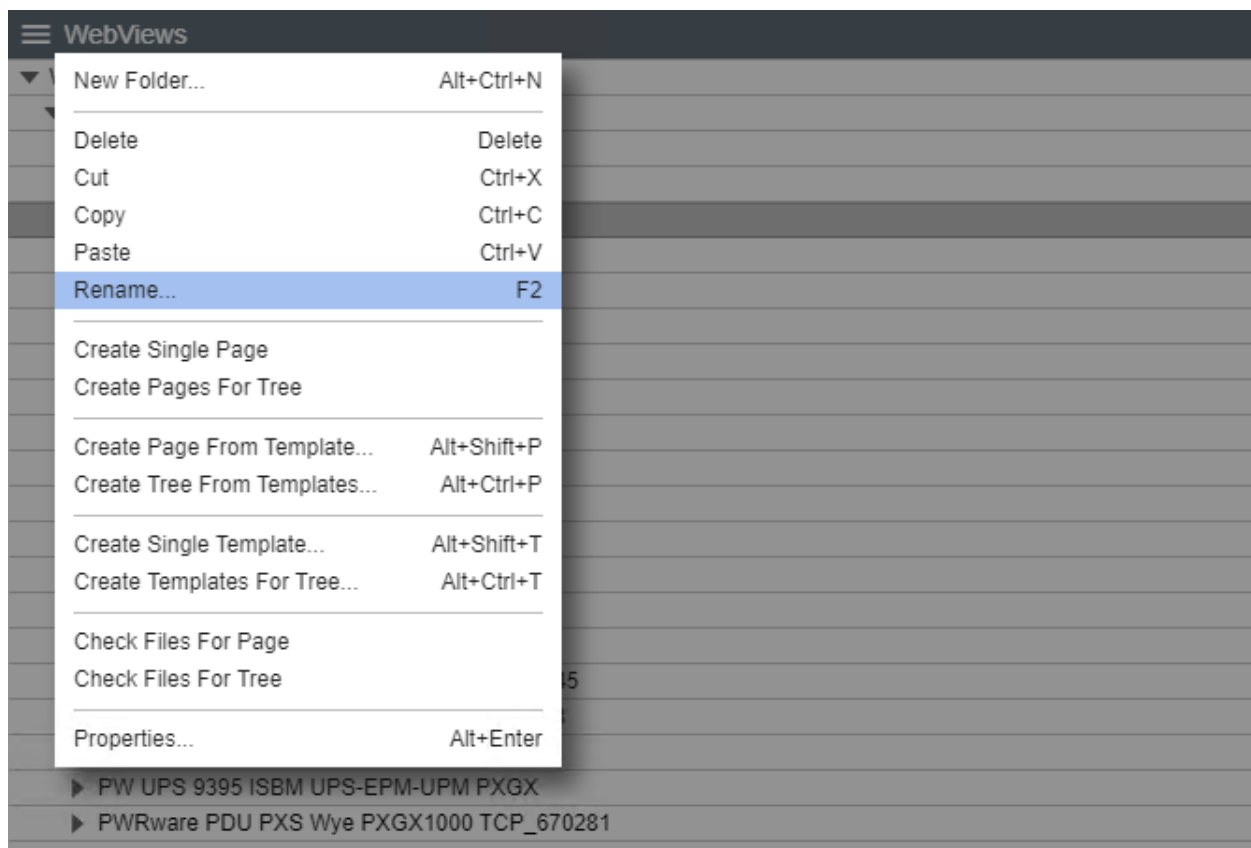
The paste command pastes the result of a Cut, Copy, or Copy Link operation as the child of the selected folder.



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.

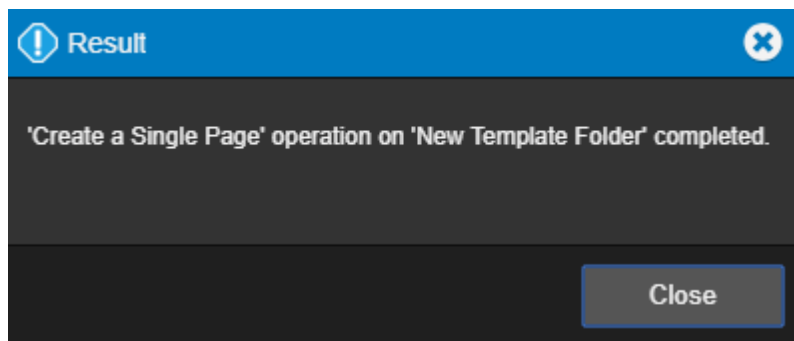
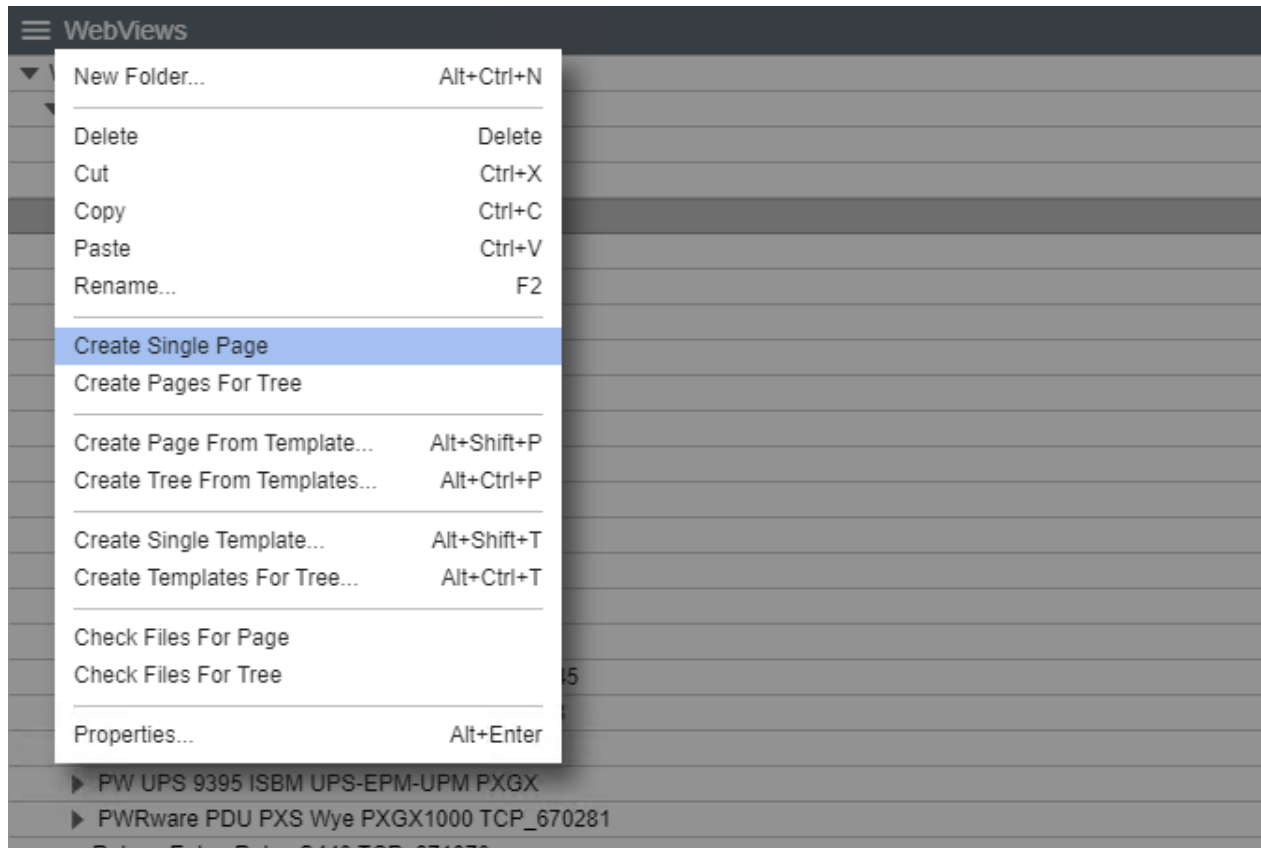
- ✔ If you rename an existing folder, you will need to update all folders and URLs that reference the old folder name to the new folder name.



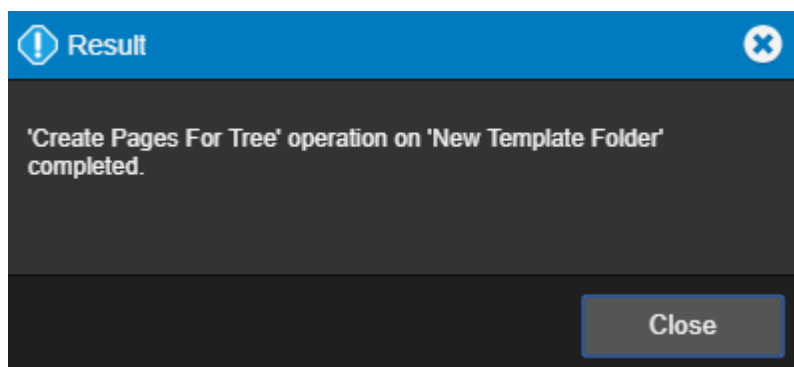
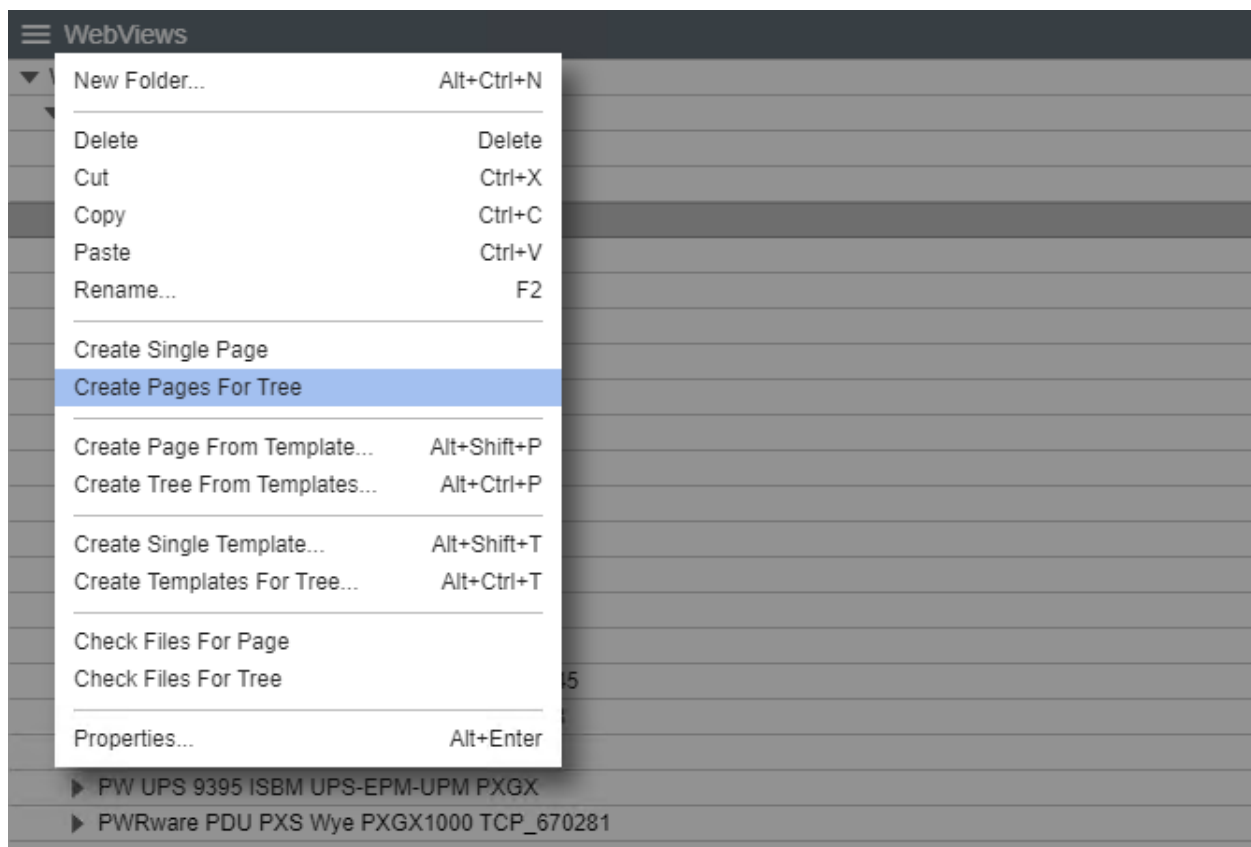
Create Single Page / Create Pages for Tree

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.

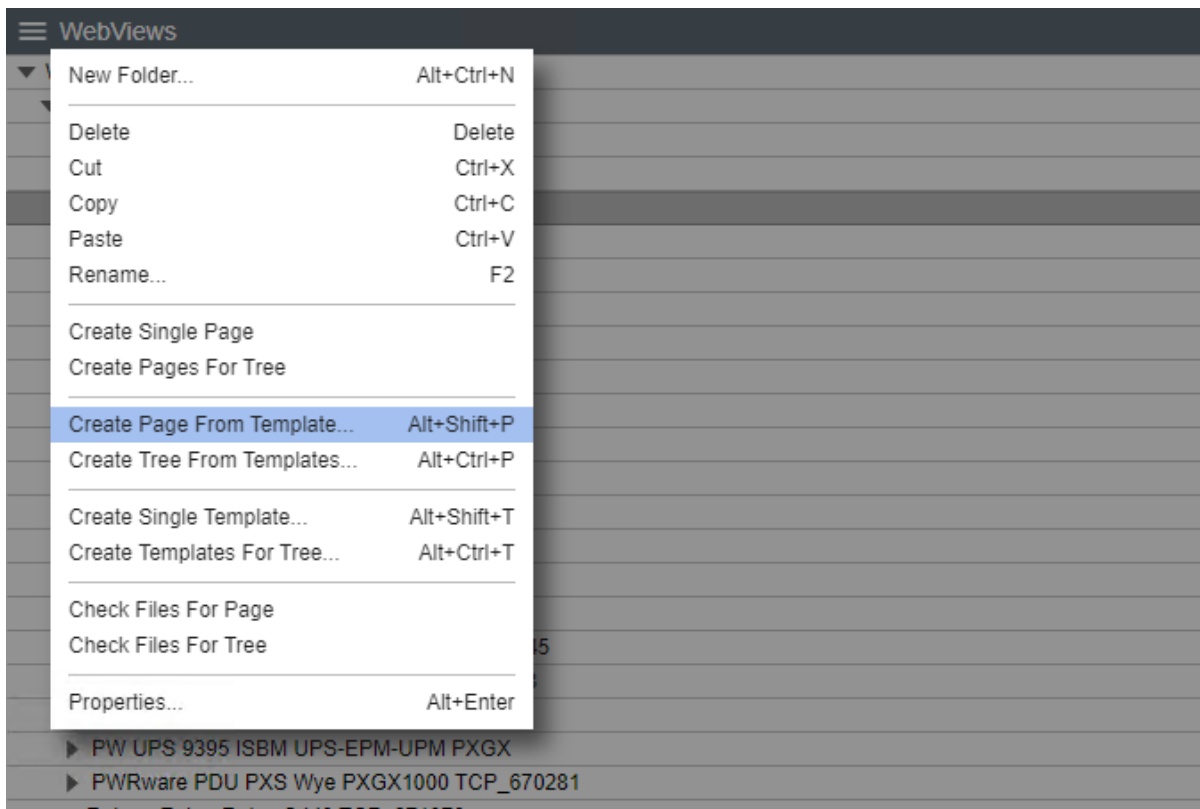


Create Page From Template / Create Tree from Templates

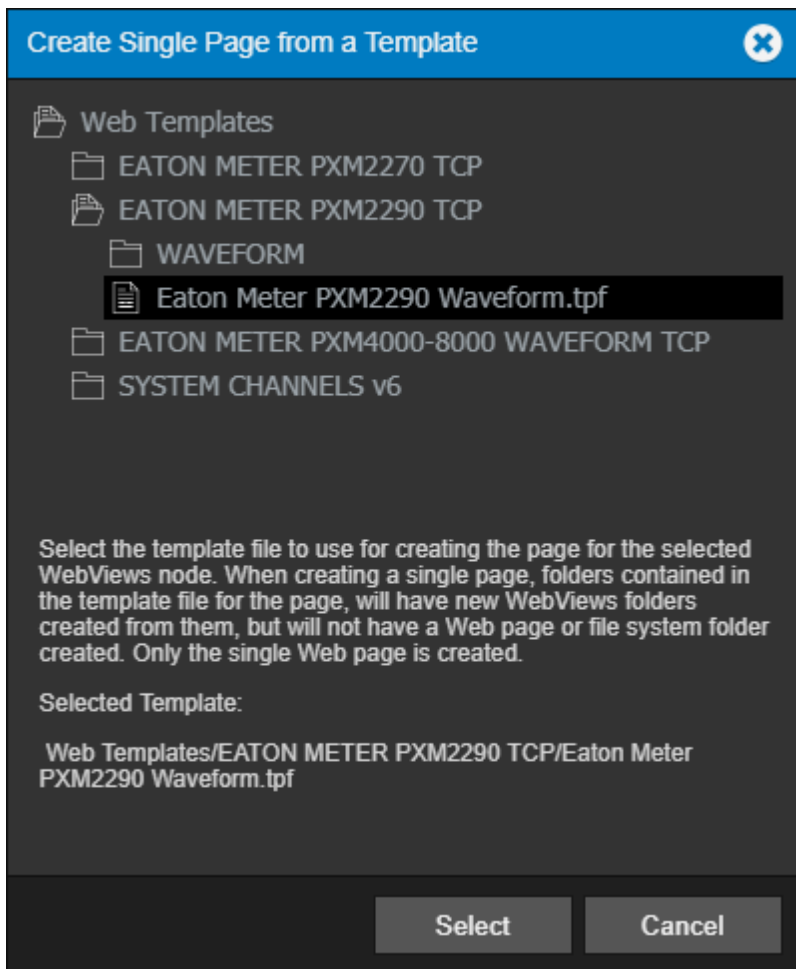
The Create Page From Template / Create Tree from Templates command creates a WebViews page or a section of the WebViews tree from the specified Template file. The page(s) can include specified Devices and their Channels.

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

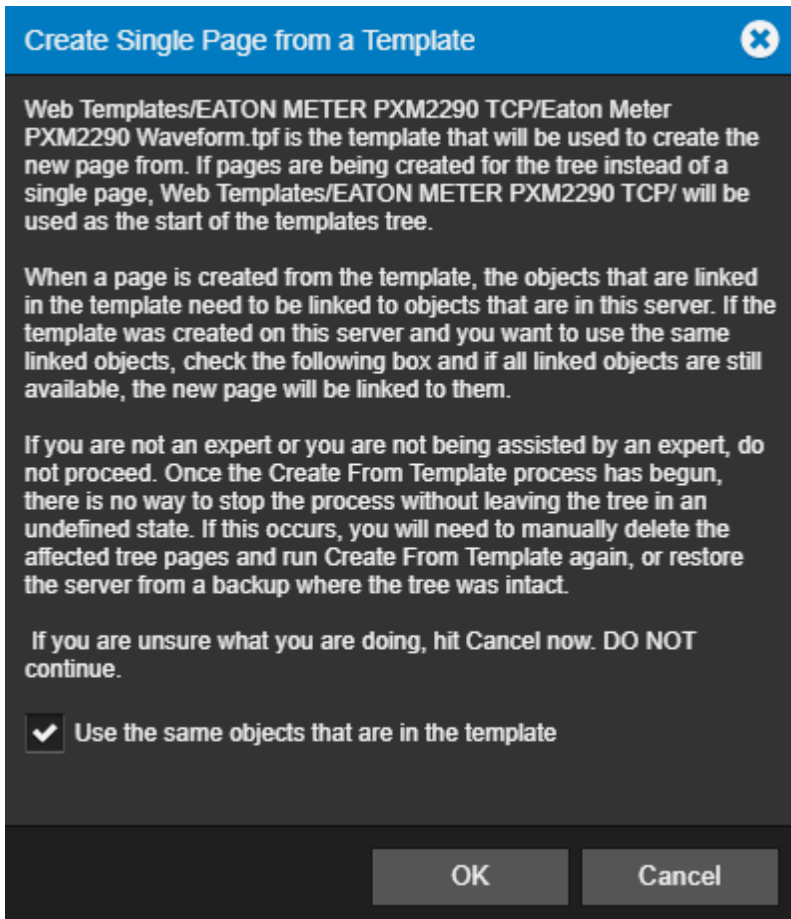
1. Highlight the location for the page in the WebViews panel and select Create Page from Template.



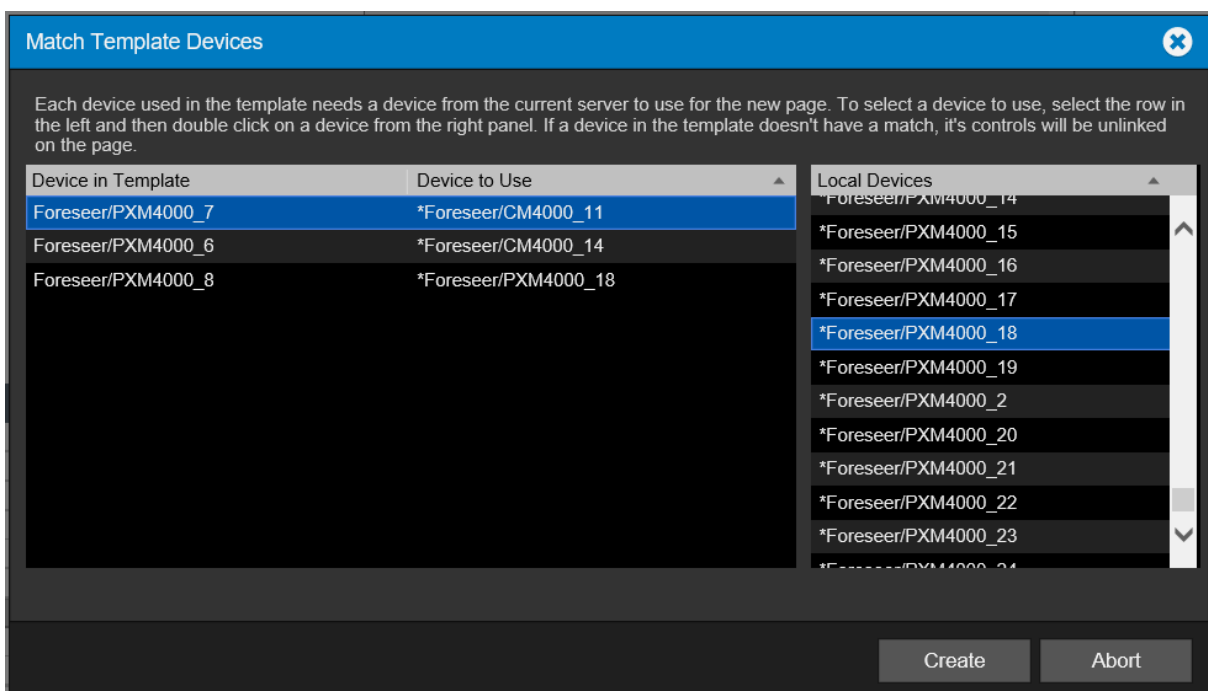
2. Select the .tpf template file to use. Template files for the currently selected folder in the templates tree are displayed. You can navigate through the tree to select files in other locations in the tree.



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.



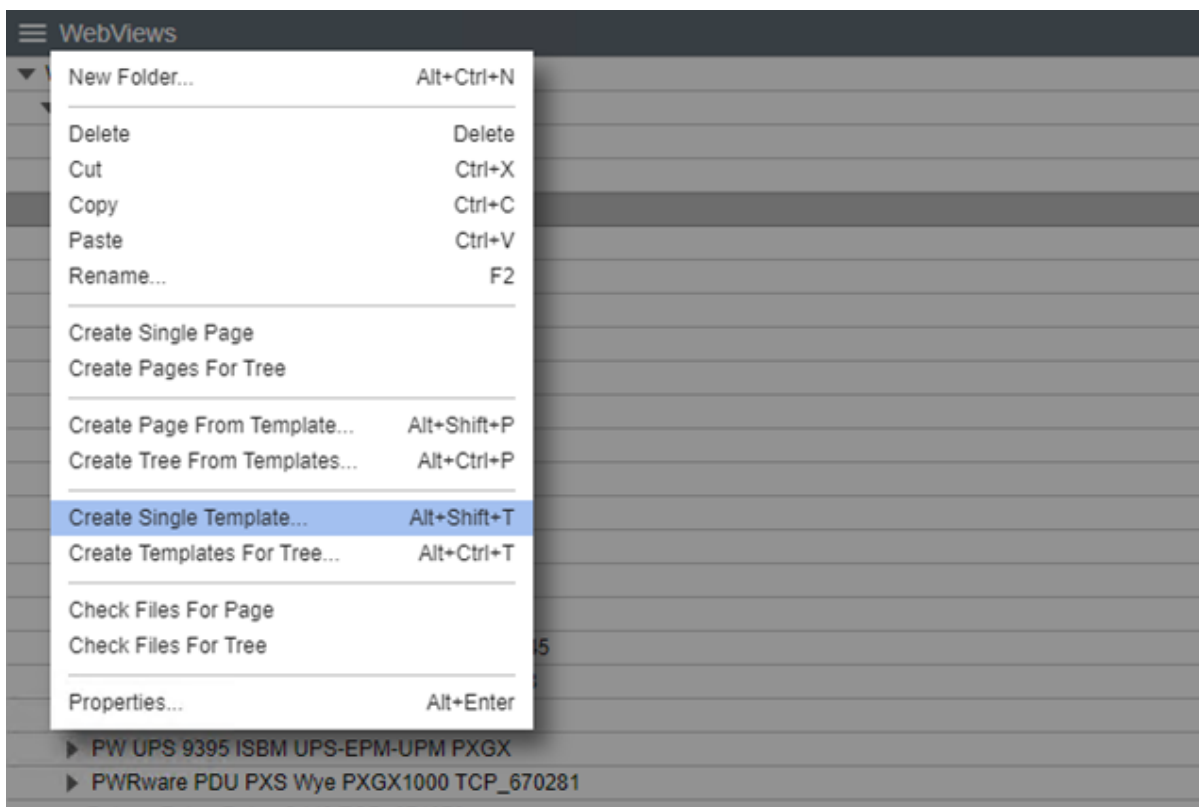
6. When you've selected a device, click Create.
7. The page is created and the WebViews folder should now show the set of channels from the selected device.

Create Single Template / Create Templates for Tree

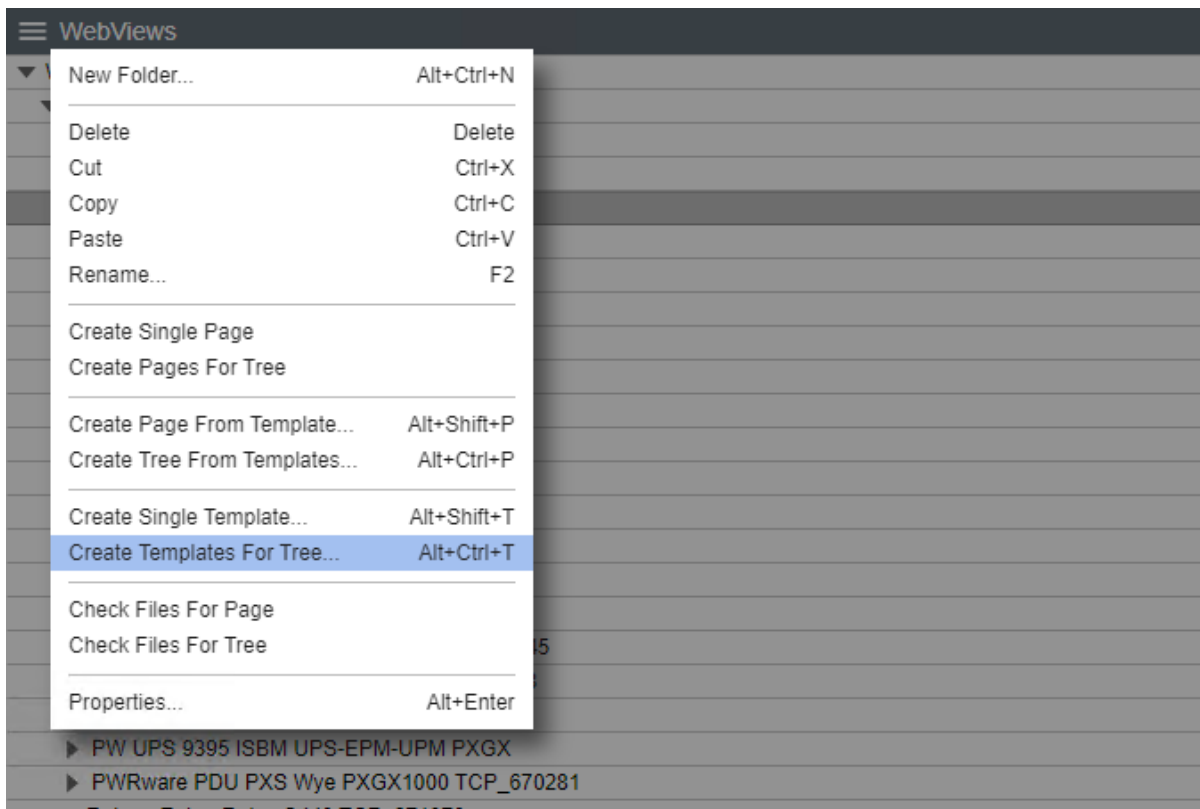
If you're using Create Single Template, the resulting template file is based on the selected WebViews page. This file can then be used to create a copy of this WebViews page at different locations in the tree. If you're using Create Templates for Tree, the resulting template file can be used to create 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:

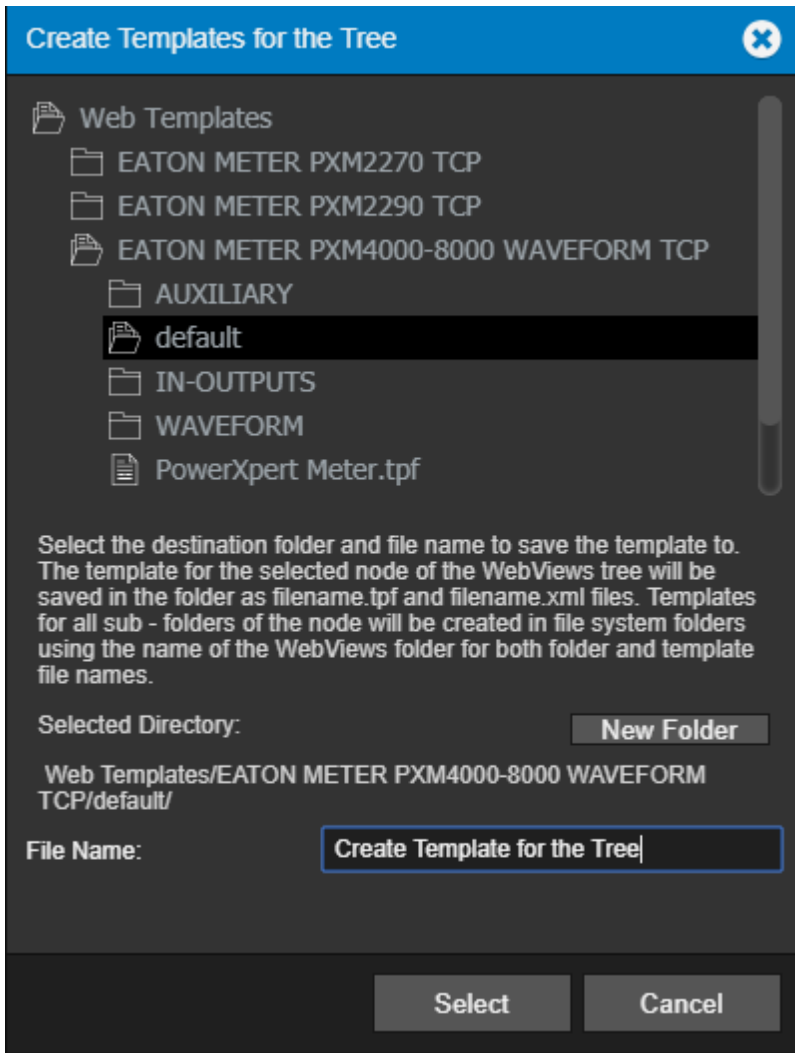
1. Highlight the location for the page in the WebViews panel and select Create Single Template.



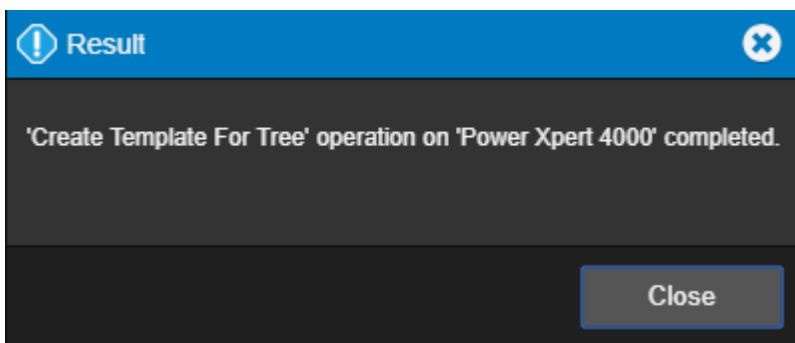
2. If you are using the Create Templates for Tree function, all of the child folders will also be included in the template file.



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.

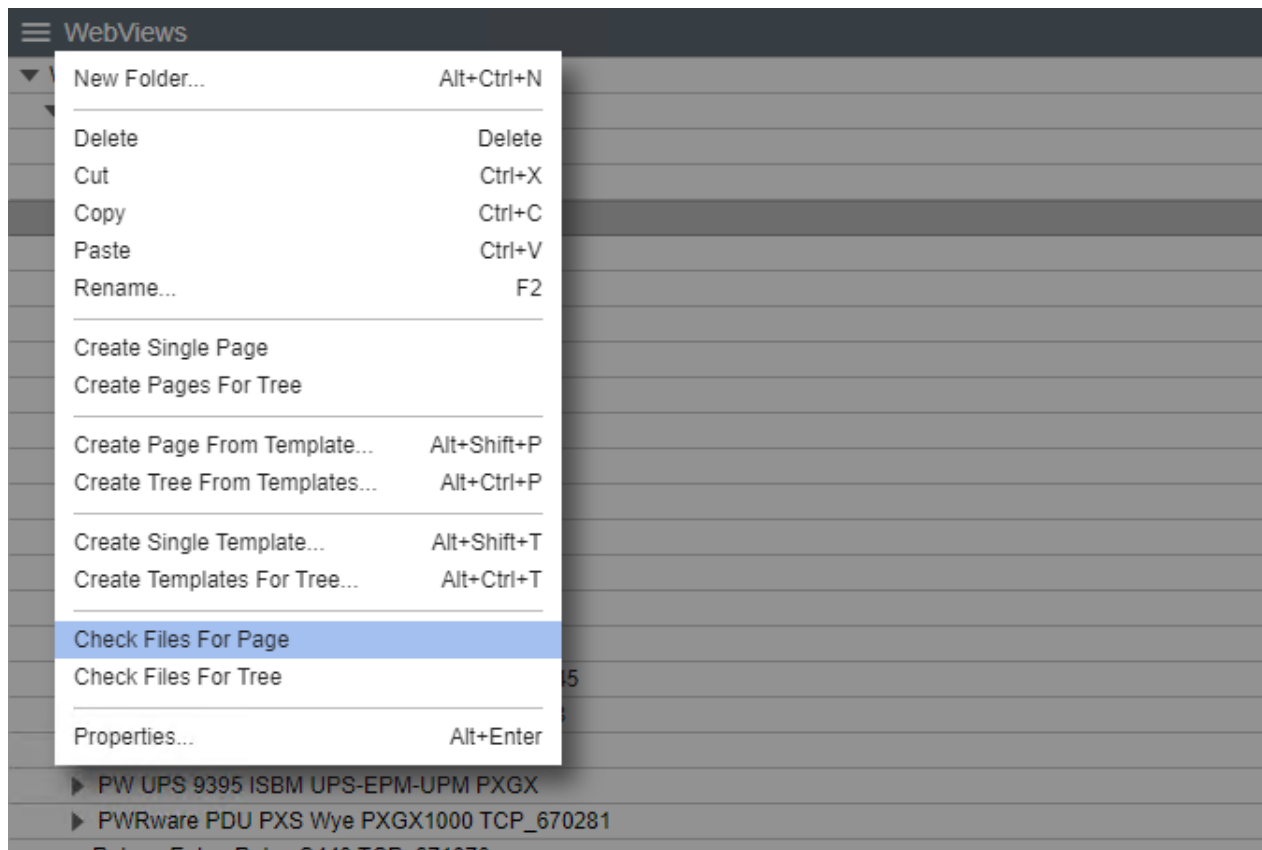


4. Click Select.



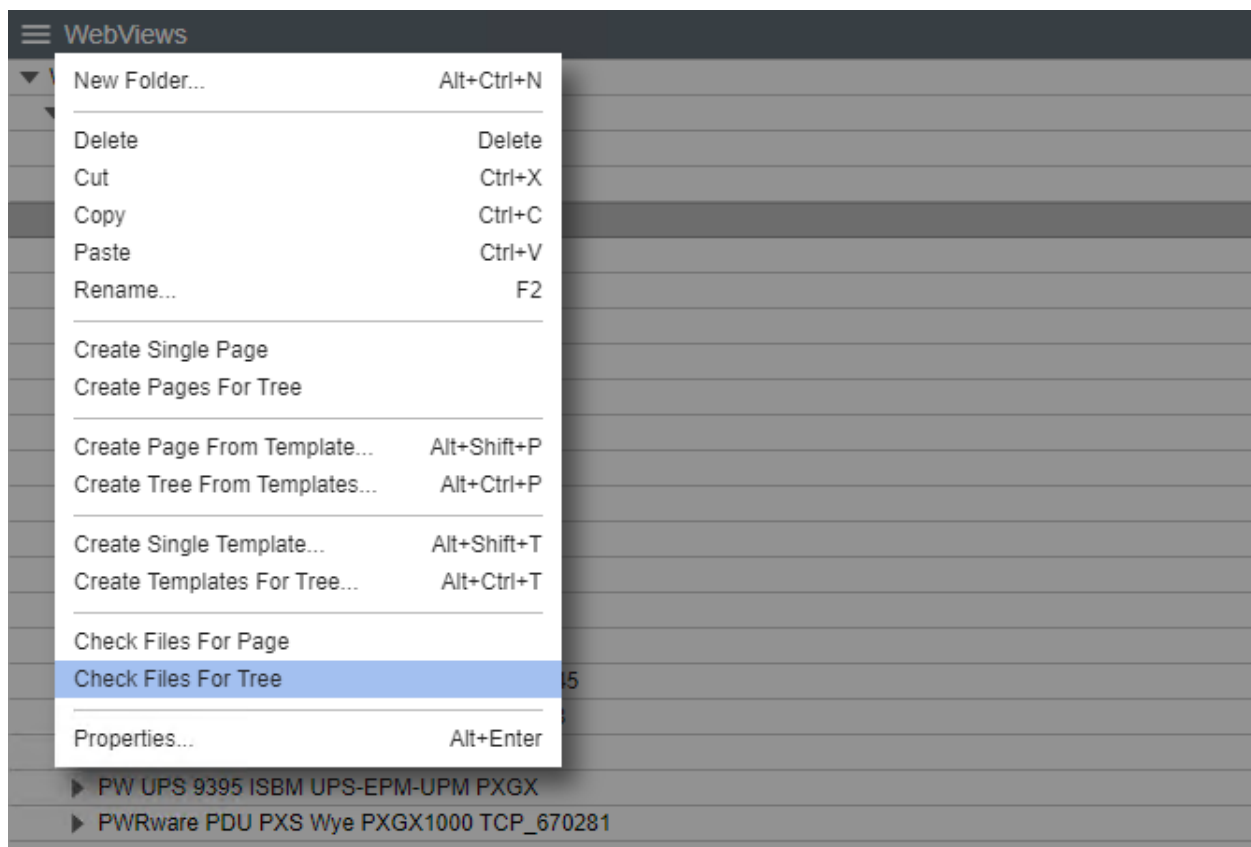
Check Files for Page

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



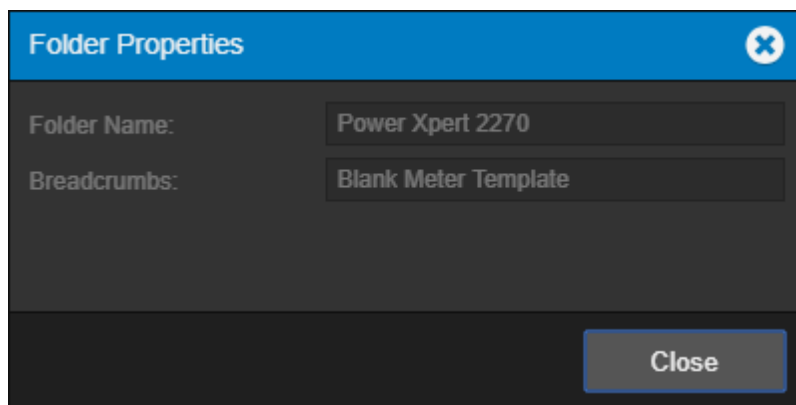
Check Files for Tree

- ✔ 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.



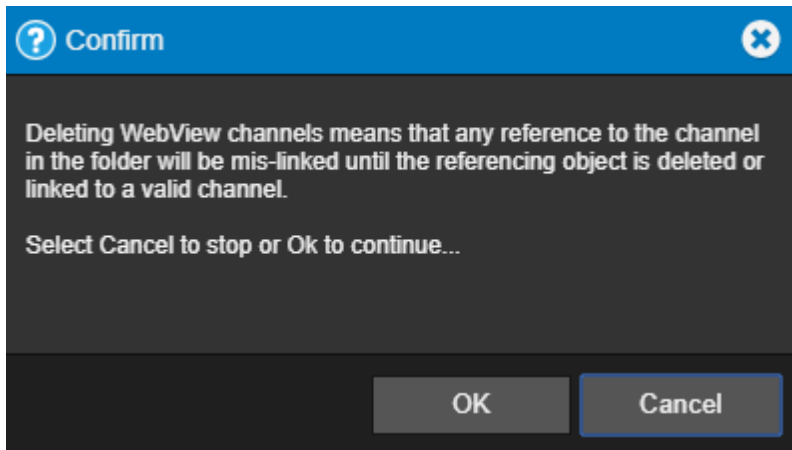
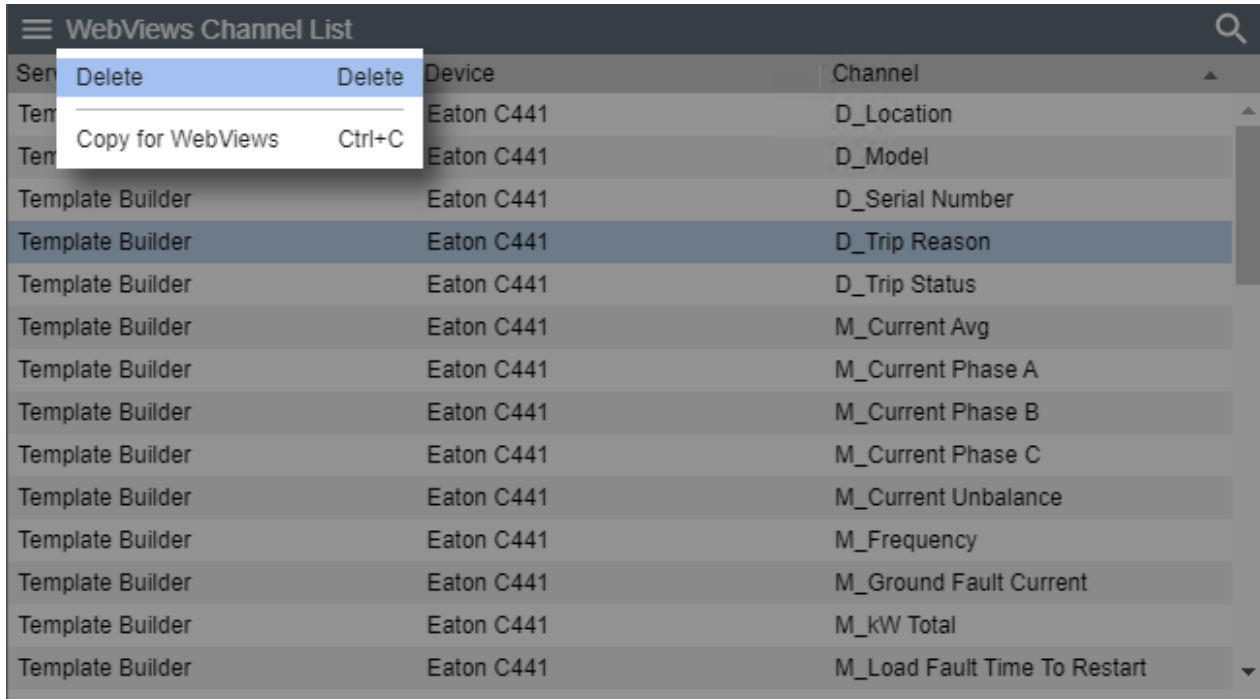
WebViews Channel List Menu

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

Copyright

Foreseer Web Configuration Guide – 7.5.800

Publication date 01/2022

Copyright © 2022 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.