IM02606007E

Foreseer Web Configuration Utility Guide: Foreseer 6.3

E·T·N

Powering Business Worldwide

Foreseer Web Configuration

User's Guide

Foreseer Web Configuration: User's Guide

Publication date 11/2015

Introduction

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.

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

Launching the Web Configuration Application

To access the Web Configuration Application, you must:

- run Microsoft Internet Explorer version 10 or 11:

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

You can access the Web Configuration Utility at the following URL: `http://machine/Support/WebConfig.htm`

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.

Note

If you must designate a specific port for communicating with the WebViews server, the syntax of the URL will be slightly different:

`http://machine:port_number/Support/WebConfig.htm`

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

Figure 1. Web Configuration Utility
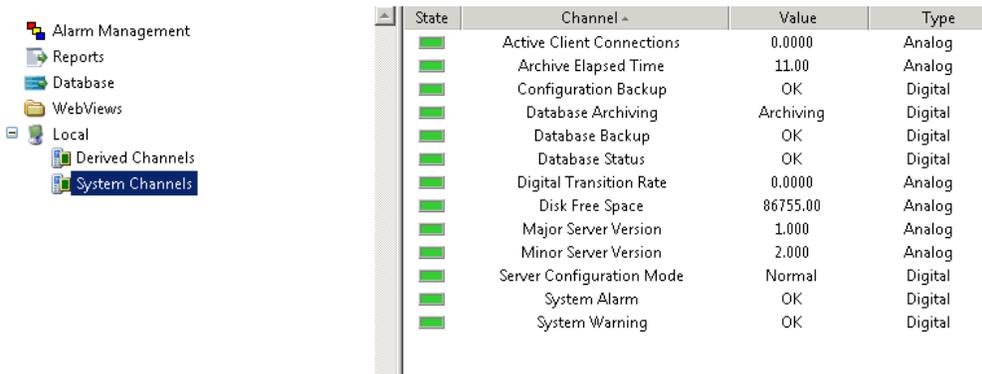
State	Channel ▲	Value	Type
	Active Client Connections	0.0000	Analog
	Archive Elapsed Time	11.00	Analog
	Configuration Backup	OK	Digital
	Database Archiving	Archiving	Digital
	Database Backup	OK	Digital
	Database Status	OK	Digital
	Digital Transition Rate	0.0000	Analog
	Disk Free Space	86755.00	Analog
	Major Server Version	1.000	Analog
	Minor Server Version	2.000	Analog
	Server Configuration Mode	Normal	Digital
	System Alarm	OK	Digital
	System Warning	OK	Digital

Tree View

The Tree View provides a hierarchical display of the Server configuration, much like Windows Explorer. The left pane lists all associated Foreseer Servers (as well as their subordinate Devices and Channels), the WebViews Tree, the Database Management icon, the Reports Access icon and the Alarm Management icon.

Figure 2. Tree
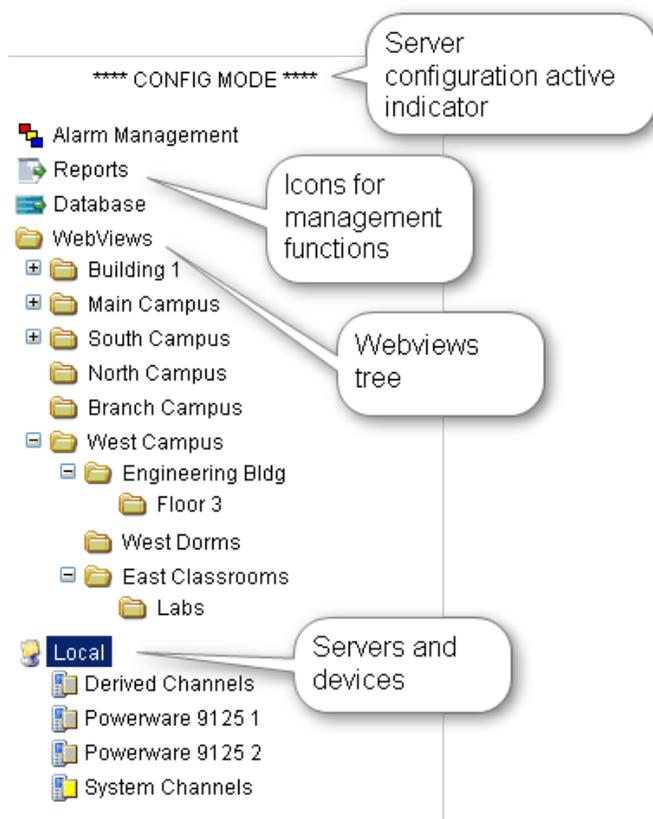
Selecting a Server, Device or Channel displays summary information about its components in the right pane. Listed Server information includes the Name, Address, frequency of Alarm and Channel updates, whether the connection is Enabled, whether the software Needs Updating and when the Last Update Check was performed. Device information lists its resident channels as well as the State, Value and Type of each.

Selecting an individual channel identifies its current State, Value and Type. Any of these listings may be resorted by clicking on the desired column heading. To sort Device channels alphabetically by Type, for example, click on that column heading; clicking the column header a second time resorts them in reverse order. Selecting a Server, Device or Channel and right-clicking presents a menu that allows Foreseer actions and responses to be performed depending on the chosen system component.

Right-Click Menus

You access the various configuration features of the utility by selecting objects in the tree and right-clicking. Available functions for configuring that object are listed in the menu. The following shows the menu for configuring Webviews.

Figure 3. Typical Right-Click Menu


```
New Folder...

Delete
Cut
Copy
Copy Link
Paste                          Ctrl+V
Rename

Create a Single Page
Create Pages for Tree
Templates                           ▶

Check Files for Page
Check Files for Tree
Fix the Tree

Properties
```
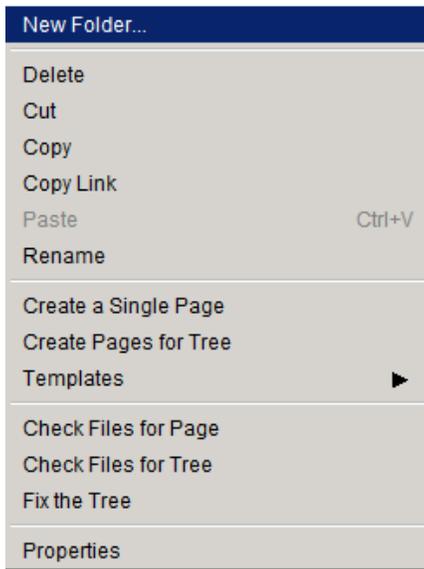
Server and Device Configuration

Server Configuration

The following sections detail the functions in the Server Configuration menu. To access this menu, right-click a server in the tree.

Figure 4. Server Right-Click Menu
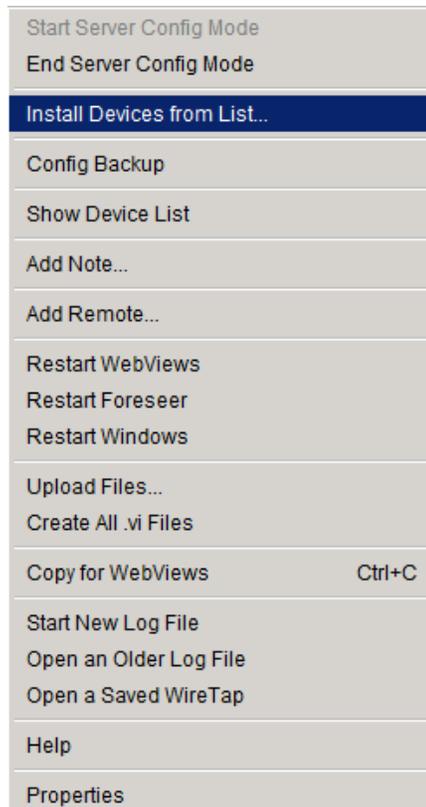
Start/End Server Configuration

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 (Server right-click menu)

- Add Remote (Server right-click menu)

- Unload Driver (Device right-click menu)

- Load Driver (Device right-click menu)

- Delete Device (Device right-click menu)

- Rename Device (Device right-click menu)

- Add User Defined Channel (Device right-click menu)

Add a List of Devices

Important

You cannot add more than 150 devices through a single list via the Web Configuration utility. If you must load more than 150 devices, use multiple lists or use the device list feature in either the Device Config application or the Foreseer server.

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_type,*device_name*,*vi_file_name*,*IP_address*,*driver_specific_info*

Where:

device_type	is either Modbus3, SNMPManager2, PowerSNMP, or Nothing. These are not case-sensitive. Nothing is a pseudo-device that contains derived channels.
device_name	is the name that will be used in Foreseer for the device.
vi_file_name	is the filename of the driver file for that device. This is in the *install_path*\Foreseer\vi folder.

Note

Some driver filenames may contain commas. Foreseer can correctly handle these.

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

For example, the following .csv file loads five separate devices Powerware UPS 5125 devices:

```
PowerSNMP,5125-1,5-Powerware UPS 5125 Xslot SNMP.vi,10.22.50.32,public
PowerSNMP,5125-2,5-Powerware UPS 5125 Xslot SNMP.vi,10.22.50.35,public
PowerSNMP,5125-3,5-Powerware UPS 5125 Xslot SNMP.vi,10.22.50.31,public
PowerSNMP,5125-5,5-Powerware UPS 5125 Xslot SNMP.vi,10.22.50.142,public
```

You must first upload a file to the *install_path*\Foreseer\vi folder on the server before you load it into Foreseer.

1. Right-click the Server, then select Upload Files.

2. In the Upload Files dialog box, select Server/Vi in the upload to list.

3. Use the Browse buttons to select one or more device list files to upload to the server.

4. Click Upload.

Figure 5. Upload Files Dialog Box
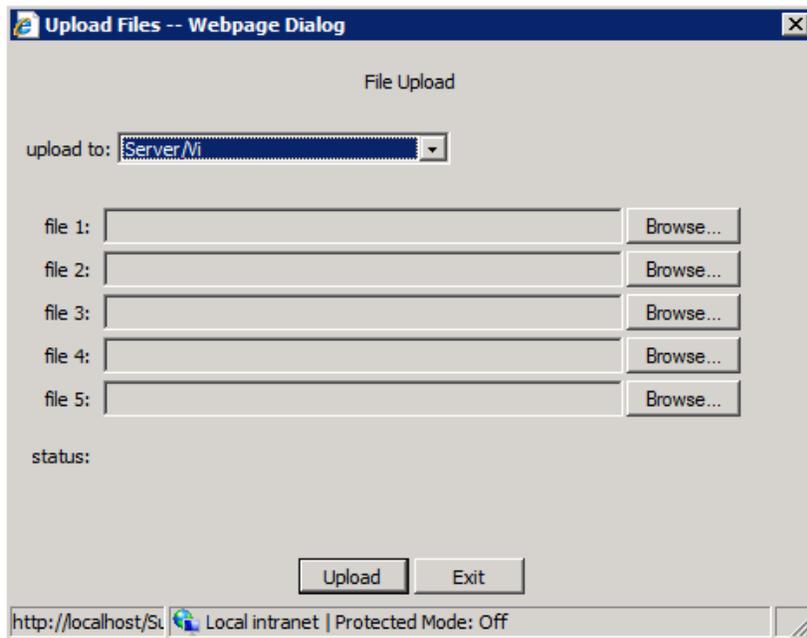
1. Right click the server and select the Start Server Configuration command. The ********SERVER CONFIGURATION MODE******** message appears in the window's title bar.

Note

If an administrative password is required to configure the server, a dialog box will appear in which you must provide that password.

Figure 6. The Install Devices from List Command
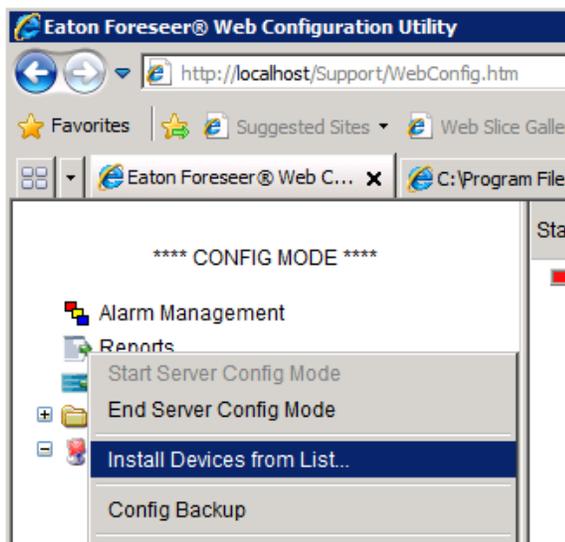
2. Right-click the Server, then select Install Devices from List.

3. In the Select CSV File dialog box, select the CSV file.

4. Click Open.

The file will be validated and, if no errors are found, loaded. Should errors be detected in the device list file, refer to the error dialog boxes and the log report.

Backing Up the Server Configuration

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 (*server_name* # End Server Config Mode

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 Config Backup in the Server right-click menu.

2. The utility reports back the name of the backup file in the Message from webpage alert box. In the example shown in the following figure, the file `\Program Files (x86)\Eaton Corporation\Foreseer\Restore\LOCAL AUG20 1412.ARQ` was written.

Figure 7. Backup File Name
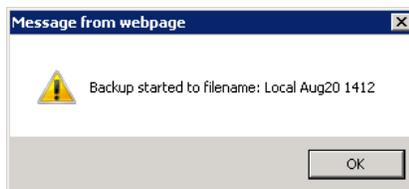
Device List

You can display a device list that includes information about the current state of the device and the driver used in the connection. The list appears in the right pane.

To display a device list:

•   Select Show Device List in the server right-click menu.

Notes

You can use the 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.

Figure 8. An example of note in a Notes History report

```
                     Local
              Notes History Report
              Report Interval: 1 day
              From 08/19/10 15:15:11
              To   08/20/10 15:15:11

08/20/10 15:15:01  This is a note
08/20/10 13:58:40  System Up
08/20/10 13:58:39  System Down
08/20/10 13:45:51  System Up
```

To create a note:

1. Select Add Note in the server right-click menu.

2. In the note editor dialog box, type a note (not exceeding 256 characters).

3. Click OK.

Adding a Remote Server

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

Note

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

To add a remote server:

1. Select Add Remote in the server right-click menu.

Figure 9. Remote Server Setup
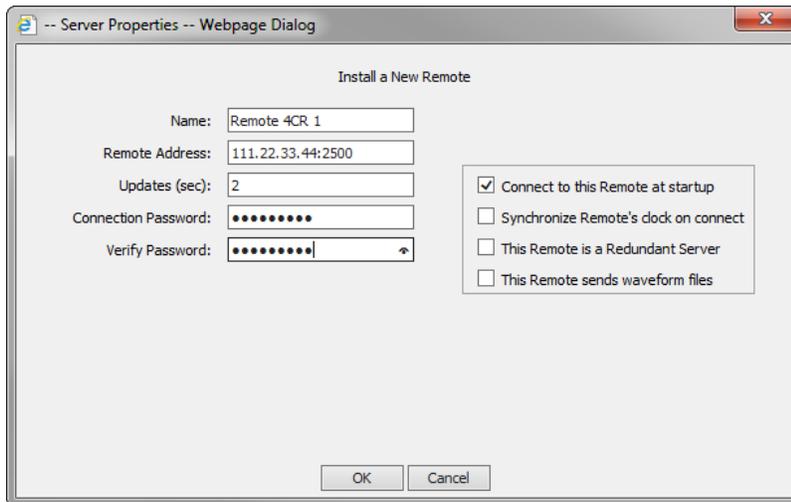
2. Identify the remote server by entering its Name and Remote Address; requiring Connection Password security is optional. If a password is specified for remote server access, the password must be entered a second time in the Verify Password field. If no password is specified, it defaults to "special".

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 Remote's 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 connection is established, the new Remote Server appears in the Tree View hierarchy.

A `Backups` folder is created containing subfolders 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 Remote's subfolder to ensure that a current backup is available.

Restart WebViews

Restarts the Foreseer web server (both http and https connections will be reset).

Restart Foreseer

This restarts the Foreseer server, and is identical to exiting and restarting the Foreseer server from it's standalone interface.

Restart Windows

This 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.

Upload Files

This 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.

Copy for Webviews

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 subfolder of its own under the server folder.

Figure 10. WebViews Copy

In the example shown in Figure 10, "WebViews Copy", the Local server is copied and then pasted into the Building 1 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.

Create All .vi Files

Generates `.vi` (Device Driver) templates for all Devices on the selected Server. These device templates can then be used to define other similar Devices.

Start New Log File

Stops writing 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 `\Program Files (x86)\Eaton Corporation\Foreseer\LogFiles` folder.

Open an Older Log File

Allows you to open and view any log file written to the `\Program Files (x86)\Eaton Corporation\Foreseer\LogFiles` folder.

Help

Launches the online help for the utility.

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.

Figure 11. The Server Properties Dialog Box
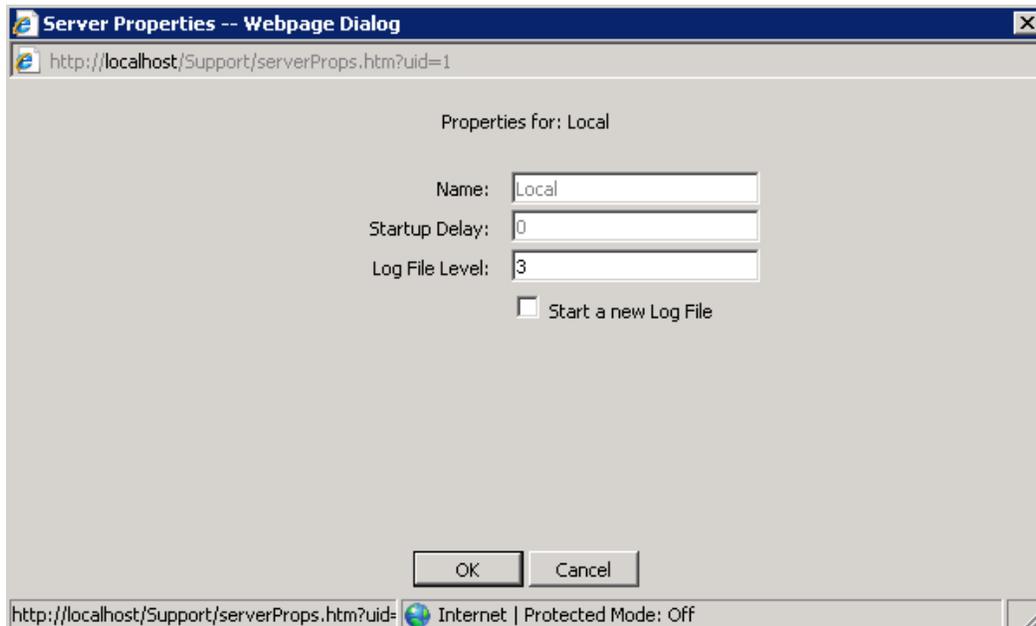
Device Configuration

The following sections detail the right-click menu functions for device configuration.

Enable/Disable

Disable 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. Enable resumes data archiving for the selected Device.

Disarm/Rearm

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

Unload/Load Driver

These functions are used strictly by driver developers. Unload clears the driver file for the selected Device. You can also load the appropriate Device driver from the `\Program Files (x86)\Eaton Corporation\Foreseer\Update VI` folder. Multiple Devices of the same Type may be selected for unloading without shutting the system down. This function should only be performed at the direction of Eaton technical support.

Delete

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 affect on Foreseer Client configurations.

Rename

Renames the selected Device. Renaming a Device should be done with discretion as changing a name can have an adverse affect on Foreseer Client configurations.

Add User-Defined Channel

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.

Copy for WebViews

Copies the selected channels to the target folder in the WebViews tree.

Copy Channel Properties

Copies all of the currently selected devices's 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 channel or Device being copied must be of the exact same type as the one the Properties are being pasted into.

Paste Channel Properties

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.

Create .vi File

Generates a `.vi` (Device Driver) template file based on the selected Device's settings. This file template can then be used to define other similar Devices.

Properties

Furnishes operational information on the Device. You cannot change settings in this dialog box, but instead must use the right-click context menu in the tree.

Channel Configuration

The following sections describe the functions in the Channel configuration right-click menu.

Enable/Disable

Disable suspends all data archiving to the Foreseer Server for the selected Channel. Enable resumes data archiving for the selected Channel.

Disarm/Rearm

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

Delete

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 affect on Foreseer Client configurations.

Rename

Renames the selected Channel. Renaming a Channel should be done with discretion as changing a name can have an adverse affect on Foreseer Client configurations.

Copy Channel Properties

Copies all of the currently selected channel's Properties to the Windows clipboard, allowing its settings to be pasted directly into another channel as its operational parameters. The channel being copied must be of the exact same type as the one the Properties are being pasted into.

Paste Channel Properties

Pastes the previously copied Channel Properties into the currently selected channel as its operational parameters. The channel being pasted into must be of the exact same type as the one the Properties are being copied from. These settings then can be individually modified as necessary.

Properties

Note

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

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 Basic tab configures the Channel's alarm thresholds, associated Messages and relative importance. The Advanced tab configures alarm behavior as well as the scaling functions. The User-Defined Equation tab defines the Transfer Equations for Derived Channels.

WebViews Configuration

You can create WebViews folders and populate these with devices and channels. The following sections detail the functions in the WebViews right-click menu.

New Folder

Creates a new folder as a child of the currently selected folder. The corresponding WebViews page is also created.

Delete

Deletes the currently selected folder and WebViews page.

Cut

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

Copies the current folder and pastes the copy as a child of the selected folder.

Copy Link

Copies a link to the selected folder, which when pasted provides a link to that folder instead of a copy. The link has the path to the target folder in its name and is shown with a blue folder icon.

Paste

Pastes the result of a Cut, Copy, or Copy Link operation as the child of the selected folder.

Rename

Renames the selected folder. If you are renaming a link, the target folder will be renamed as well.

Create a Single Page/Create Pages for Tree

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 `C:\Program Files (x86)\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 function 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.

Templates

Templates provide a way to build WebViews pages quickly by using one page as a model for others. The Templates menu provides the following functions:

Create Page from Template/Create Tree from Templates

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. Right-click the location for the page in the WebViews tree and select Templates # Create Page from Template.

2. Select the `.tpf` template file to use. Template files for the currently selected folder in the templates tree are in the right pane. You can navigate through the tree (left pane) to select files in other locations in the tree.

Figure 12. Selecting the Template File
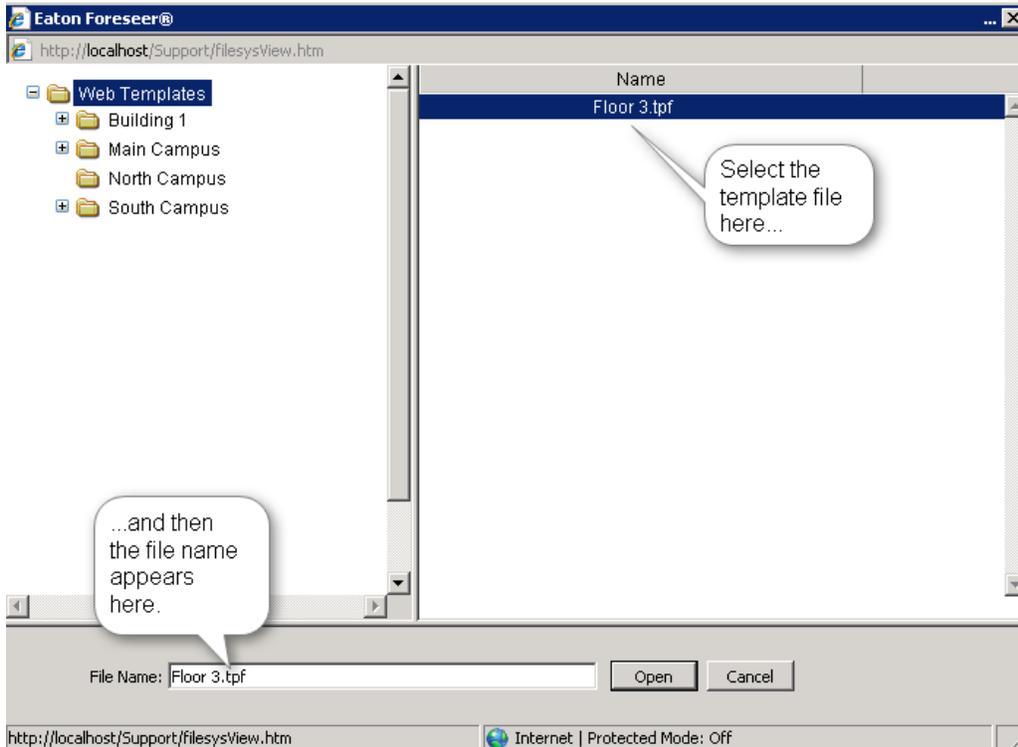
3. Click Open.

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 prepopulates 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.

5. 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.

Figure 13. Select a Device
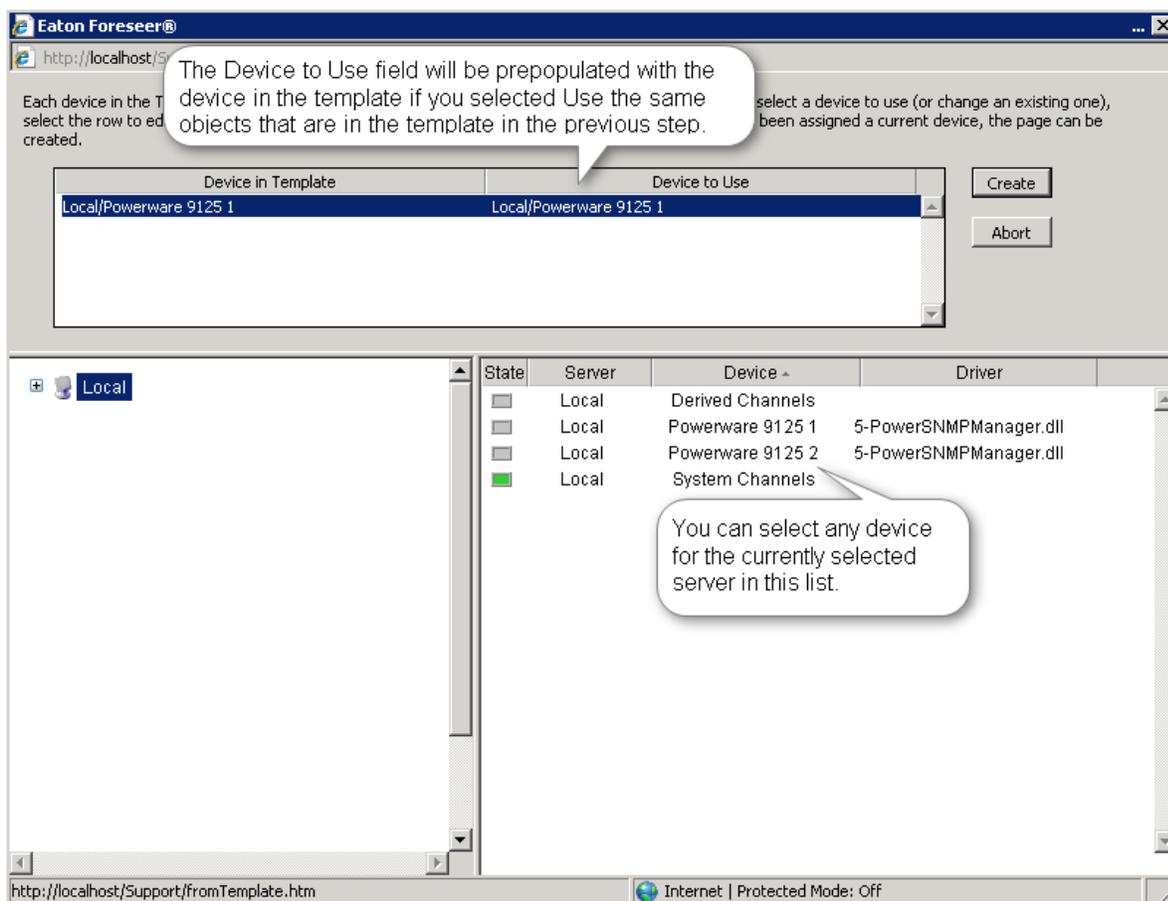
When you've selected a device, click Create.

6. The page is created and the WebViews folder should now show the set of channels from the selected device.

Create Single Template/Create Templates for Tree

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

file can be used to create a copy of the selected WebViews page and all of its children. You can use this function to rapidly recreate repeating tree structures throughout the WebViews tree. For both functions, you can specify the device to use when specifying attached channels.

To create a template file:

1. Right-click a folder in the WebViews tree and select Templates # Create Single Template or Templates # Create Templates for the Tree. If you are using the Create Templates for Tree function, all of the child folders will also be included in the template file.

2. Select a location in the Web Templates tree and specify a file name for the `.tpf` template file. You can use the New Folder button to create a new folder as a child of the folder currently selected in the Web Templates tree. This simply creates a folder in the Foreseer Server file system (under `\Program Files (x86)\Eaton Corporation\Foreseer \Web Templates`).

Figure 14. Creating a Template File
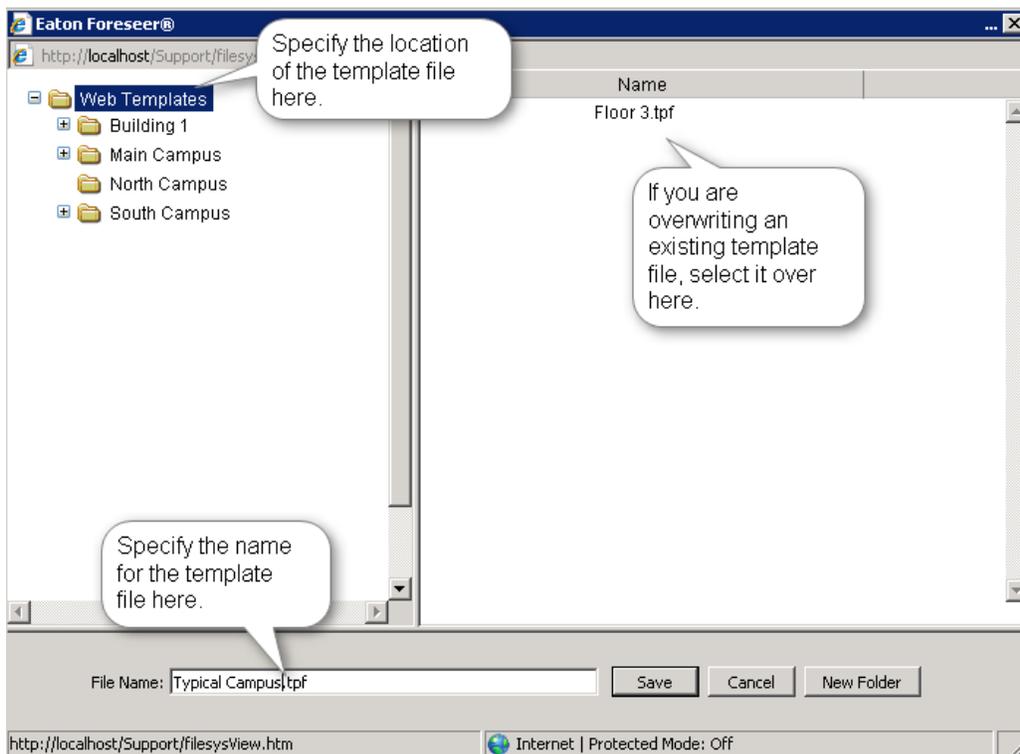
3. Click Save.

Check Files for Page

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

Check Files for Tree

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

Fix the Tree

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

Channel Configuration

You can delete a channel from a selected folder in the WebViews tree.

To delete a channel from a WebViews folder:

1. Select a folder in the WebViews tree.

2. In the right pane, select one or more channels. You can use Shift-click to select a range of channels and Ctrl-click to multiselect channels.

3. Right-click over one of the selected channels and choose Delete.

Database Configuration

The following sections detail the database configuration functions available in the Database right-click menu:

Start/Stop Database

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

Check Database

Runs a cursory check of the Foreseer databases. This check verifies the schemas, checks the channel map against the database, and verifies some of the tables. Results are written to the log, which you can review by generating a log through Reports.

Fix Database

This is a thorough check of the Foreseer databases, including allocation and consistency checks. If problems are found, this function will attempt to fix them. Results are written to the log, which you can review by generating a log through Reports.

Reports

To access reports in the Web Configuration Utility:

1. Click Reports in the tree.

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.

Forseer provides the following reports:

• Alarm History (1 Day, 7 Day, 30 Day) is a series of Reports listing all alarms detected over the last day, week and month. These three Report formats consist of all alarm conditions recorded within the respective interval. If no alarm events were detected during the period, that status condition is reported.

• Alarm History Custom permits the range and content of an Alarm History Report to be specified. It also lists the addition and deletion of Devices and channels to the Server configuration as well as when database sessions are started and stopped.

• Audit History Custom reports the addition and deletion of Devices and channels to the Server configuration as well as when database sessions are started and stopped.

• 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. This is not available in tab-delimited format.

• Channel Report furnishes parameters for all channels on a Server or for a selected Device.

• Log File reports all recorded events since the last system reset.

• Notes History (1 Day, 7 Day, 30 Day) reports all Notes logged over the last day, week and month.

• Notes History Custom permits the range and content of a Notes History Report to be specified.

• Previous Log File reports all events recorded in the previous Foreseer Server session.

• System Configuration enumerates all configured Devices, their operational parameters and current interface software version.

• System Up-Down reports each time the Foreseer program was launched and terminated.

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 Reports in the tree.

2. Click the appropriate custom report button in the right 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

3. 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 Pre-defined 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 Pre-defined Interval format, which always includes the current Server time as the Ending Time. In either case, the resulting Report Interval is calculated and shown.

    ## Note

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

4. With the reporting period defined, click on the Advanced tab to display those Custom Report parameters.

5. 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.

6. Expand the list under the appropriate Server to access its connected Devices and individual channels.

7. 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.

8. With the desired output criteria specified, click OK to run the Custom History report.

9. Click the link for the completed Report to display it.

Custom Search Strings

The ability to perform specific text searches on Custom History files can be extremely useful in locating archived information about a particular 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 wildcards 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.

Alarm Management

Alarm Management features:

- 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 any of the header categories in descending or ascending order

- Overall look can be changed using Themes or individual items such as background color

- Alarm Management can be displayed as a separate Window (the default) or a Dialog

- Alarm list updates can be temporarily suspended by pressing and holding the Ctrl or Shift keys

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.

Selecting alarms works the same way that file selection works in Windows Explorer (My Computer). A click selects a single row, Ctrl-click allows multiple select (or deselect), and Shift-click selects a range. To deselect all selected rows, press the Esc key or click a new item. Ctrl-A selects all rows. When rows are selected, clicking on a new item will deselect all and select just the new row. When selecting multiple rows, as long as the Ctrl or Shift keys are depressed, the list will remain frozen (no rows added or deleted). This allows selection to occur without the list changing underneath the mouse cursor. As soon as the Ctrl or Shift keys are released, the list will continue updating with new items added or cleared ones removed if required. If a new alarm occurs, where it will be added to the list depends on the current sort order and selected column.

In addition to active alarms, Disabled and Disarmed objects can optionally be included. To include these objects, Right-click anywhere in the window to display the context 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 right-click menu.

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

- Ack to acknowledge a Critical or Cautionary alarm.

- Rearm to return an acknowledged or disarmed object to the Normal state.

- Ack & Rearm to perform an Acknowledge and Rearm in one operation,

- Enable to return a disabled object to the Normal state.

Figure 15. Alarm Actions Dialog Box
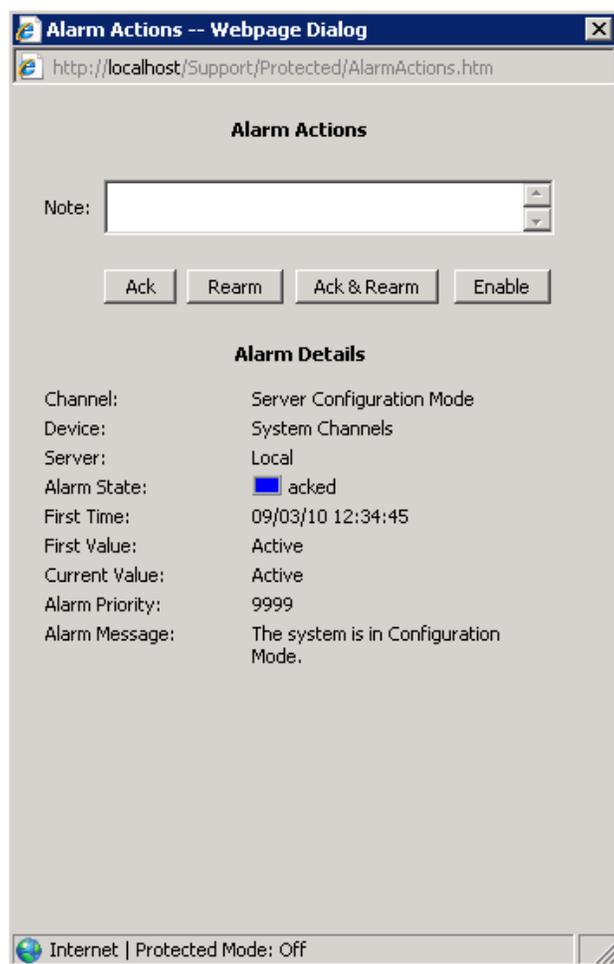
The Note field allows comments to be included about the Action. When an Action is performed, a Note is always entered into the database. The Note has two parts: the system and user parts. The system part is always entered and includes the object name, the Action name, the user name, the IP address where 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.

Note

For more information about notes, see the section called "Notes".

Depending on the state of the object, some Actions may not be valid (e.g. an Acknowledged alarm cannot be Acknowledged). If an invalid Action is attempted, the server will reply with an Object State Conflict response. As the state of an object is dynamic, it's not always apparent

if an Action is valid. An object may be acknowledgeable at the time it is selected, but it is possible that another user at a different workstation has acknowledged the alarm just before you. When multiple objects are selected and an invalid action results, a separate message will be displayed for each object that did not succeed. If this occurs, only the exceptions are displayed; all Actions that succeed do so silently. If in doubt, just review the current Alarm List or run a 1-Day Note Report to verify the Action. When running a Note Report, you may have to wait up to 15 seconds before the Action Note appears as the server buffers notes for efficiency.

Figure 16. Object State Conflict