## Contents

Server Guide .......................................................................................................................... 6

About this Document .............................................................................................................. 6

Launching the Program ........................................................................................................... 7

To manually launch Foreseer on the Server PC: ................................................................. 7

Getting Started ...................................................................................................................... 8

System Requirements ............................................................................................................ 8

- Minimum Hardware Requirements .................................................................................... 8

Hardware and Security Considerations ................................................................................. 9

Supported Environments ....................................................................................................... 9

- Supported Operating Systems ........................................................................................ 9
- Supported Database Platforms ......................................................................................... 10
- Supported Browsers ........................................................................................................ 10

Exiting the Program .............................................................................................................. 10

Security Considerations for Interactive Remote Access ...................................................... 11

SQL Server Express Installation ......................................................................................... 11

Backing Up the Server Configuration .................................................................................. 11

Automatic Configuration Backups ....................................................................................... 12

Recommended Secure Hardening Guidelines ..................................................................... 13

Secure Configuration Guidelines ......................................................................................... 14

Foreseer Fundamentals .................................................................................................... 18

- Menu Bar .......................................................................................................................... 19

- Tree View Menu Commands ........................................................................................... 20

Installing Devices .................................................................................................................. 22

- Installing Multiple Devices ............................................................................................. 26

- Serial Connection ............................................................................................................ 27

- Device Channel Selection ............................................................................................... 28

- Deleting Devices and Channels ....................................................................................... 29

Server Properties .................................................................................................................. 30

- Server Properties - General ............................................................................................ 30

- Server Properties - Remote ............................................................................................. 32

- Server Properties - Database .......................................................................................... 33

- Server Properties - Redundant Systems ......................................................................... 34

Device Properties .................................................................................................................. 36

- Device Properties - General ............................................................................................ 36

To access General Device Properties: .................................................................................. 37

- Device Properties - Version ............................................................................................. 38

To access Version Devices Properties: .................................................................................. 39
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Administration</td>
<td>93</td>
</tr>
<tr>
<td>Client Connection Password</td>
<td>93</td>
</tr>
<tr>
<td>LDAP Properties</td>
<td>96</td>
</tr>
<tr>
<td>LDAP Setup</td>
<td>96</td>
</tr>
<tr>
<td>Directory Search</td>
<td>97</td>
</tr>
<tr>
<td>Binding and Authorization</td>
<td>98</td>
</tr>
<tr>
<td>Shortcuts and Branch Access</td>
<td>99</td>
</tr>
<tr>
<td>WebViews</td>
<td>100</td>
</tr>
<tr>
<td>HTTP WebViews Server Properties</td>
<td>100</td>
</tr>
<tr>
<td>HTTPS WebViews Server Properties</td>
<td>102</td>
</tr>
<tr>
<td>Server Service</td>
<td>107</td>
</tr>
<tr>
<td>Server Service</td>
<td>108</td>
</tr>
<tr>
<td>Server Properties</td>
<td>108</td>
</tr>
<tr>
<td>Security and User Groups</td>
<td>109</td>
</tr>
<tr>
<td>Authorization Levels</td>
<td>109</td>
</tr>
<tr>
<td>Accounts</td>
<td>110</td>
</tr>
<tr>
<td>User Group Privilege Details</td>
<td>112</td>
</tr>
<tr>
<td>Updating User Groups</td>
<td>112</td>
</tr>
<tr>
<td>Redundant and Remote Servers</td>
<td>113</td>
</tr>
<tr>
<td>Primary Server Setup</td>
<td>113</td>
</tr>
<tr>
<td>Setting up a Redundant Server</td>
<td>114</td>
</tr>
<tr>
<td>Adding the Redundant Server as a Remote on the Primary Server</td>
<td>120</td>
</tr>
<tr>
<td>Synchronizing the Redundant Server</td>
<td>122</td>
</tr>
<tr>
<td>Add Remote Server</td>
<td>123</td>
</tr>
<tr>
<td>Message Management</td>
<td>125</td>
</tr>
<tr>
<td>Message Management</td>
<td>125</td>
</tr>
<tr>
<td>Message Management Properties</td>
<td>125</td>
</tr>
<tr>
<td>Message Management Properties - Channel Message Settings</td>
<td>126</td>
</tr>
<tr>
<td>Message Management Properties - Modems</td>
<td>128</td>
</tr>
<tr>
<td>Message Management Properties - Notifications List</td>
<td>130</td>
</tr>
<tr>
<td>Message Management Properties - Services</td>
<td>134</td>
</tr>
<tr>
<td>Message Management Properties - Subscribers</td>
<td>135</td>
</tr>
<tr>
<td>Channel Message Services</td>
<td>138</td>
</tr>
<tr>
<td>Channel Message Services</td>
<td>138</td>
</tr>
<tr>
<td>Channel Message Services - Default</td>
<td>139</td>
</tr>
<tr>
<td>Channel Message Services - Critical</td>
<td>141</td>
</tr>
<tr>
<td>Channel Message Services - Caution</td>
<td>143</td>
</tr>
</tbody>
</table>
Channel Message Services - Acknowledge ................................................................. 145
Channel Message Services - Normal ........................................................................ 147
Channel Message Services - SNMP ......................................................................... 149
SNMP Virtual Agent .................................................................................................. 151
SNMP ........................................................................................................................ 151
SNMP Installation ...................................................................................................... 152
SNMP Properties ........................................................................................................ 152
SNMP Properties - Agent .......................................................................................... 152
SNMP Properties - Resend Traps .............................................................................. 153
SNMP Properties - Security ....................................................................................... 154
SNMP Properties - Traps .......................................................................................... 155
SNMP Setup ................................................................................................................ 156
Menu Reference .......................................................................................................... 159
Menu Reference .......................................................................................................... 159
File Menu ..................................................................................................................... 159
Alarms Menu ............................................................................................................... 160
Alarms Management ................................................................................................... 160
Alarm Latching ............................................................................................................. 161
Acknowledging and Rearming Alarms ....................................................................... 162
Administration Menu .................................................................................................. 163
Configuration Menu .................................................................................................... 164
Configuration Backup .................................................................................................. 166
Database Menu ............................................................................................................ 167
Database SQL ................................................................................................................ 167
Appendix ....................................................................................................................... 169
Server Guide

Foreseer ® is designed to manage your critical site or entire enterprise by monitoring power and environmental inputs from equipment, sensors, and other systems. Monitored points include Meters (analog) and Status (digital) inputs which open a detailed window into the past, present and future performance of your equipment. The unique networked architecture and modular design make Foreseer a cost-effective approach to managing your mission-critical site while maintaining unique analysis and multi-vendor connectivity capabilities. Foreseer is a single integrated system which provides real-time and historical views into the operation of the power and environmental conditions that support your critical operation.

Foreseer is an easy-to-use application consisting of a Server that provides a browser-based interface called WebViews. The Foreseer Server functions as a centralized storage location for information and WebViews acts as a retrieval and display terminal for that information. WebViews allows a User to observe real-time data, respond to events and alarms, as well as graph archived data and project potential failure for every data input. Your system has been pre-configured during installation with equipment, critical data points and other views specific to your operation. The configuration is readily modified to meet changing monitoring needs.

While multiple WebViews clients can access the Server and view its resident data, security functions control who has modification privileges to particular program features. Password authorization can be specified to protect the Foreseer configuration from inadvertent alteration while still allowing its information to be viewed. System Administration controls who has access to select program features by specifying User authorization and overseeing Server Management.

Through the Server, the WebViews client offers an enhanced display of up to 20 channel traces in a Historical Graph based on the available database. A real-time Burst Graph plots values as they are reported while a ProGraph™ feature forecasts future performance by extrapolating the data the channel already has archived, allowing you to anticipate adverse conditions before they become serious problems. Authorized Users also can request Reports and manage Alarms on an individual basis. An integral Message Management feature allows specified personnel to be alerted in the event of certain alarms through a variety of notification services including alpha/numeric paging and email.

Foreseer may be equipped with additional software modules specifically designed to enhance its data monitoring and display capabilities. In addition to Device Drivers, which provide the interface to each of the monitored devices, the Simple Network Management Protocol (SNMP) Virtual Agent ™ allows alerts, or traps, to be sent to a specific Network Management Systems (NMS) to report alarms. The WebViews Editor allows authorized users to customize Foreseer WebViews to accurately depict every aspect of the site. Predefined objects can be dragged and dropped in place, user-drawn objects can be animated, and bit mapped images such as pictures and converted AutoCad files can be used as realistic or representative backgrounds for various WebViews.

The Foreseer Server Application runs under various versions of the Microsoft ® Windows operating systems. See the Release Notes for the latest updates to supported operating systems.

About this Document

Much of the operation of Foreseer should be familiar to those who have used the Microsoft
Windows operating system. Foreseer’s help facility furnishes more detailed information on program operation. Server assistance is always readily available by selecting the Help Index command under the Help Menu. A Help window organizes assistance by Contents, which groups help topics by subject.

In addition, specific colors are used to identify certain program elements:

- **Menu Commands**
- **Window Titles**
- **Keyboard Keys**
- **Toolbar Commands**
- **Parameter Fields**
- **Foreseer Features**

You can exit online assistance at any time simply by closing the Help window.

**Launching the Program**

To manually launch Foreseer on the Server PC:

- Select Foreseer Server from the Windows All Programs > Foreseer sub menu.
- Double-click on the Shortcut to Foreseer Server icon (if created).
- Locate the Server icon in the Foreseer group created at program installation and double-click on it.

Regardless of the method used to launch the Foreseer Server, the progress of its Startup is displayed in a dialog box.
Getting Started

Foreseer is designed to be quick and easy to install and initially configure. Initiating the Foreseer Server for data gathering consists of verifying that the Server PC meets minimum system requirements and then and the appropriate equipment to be monitored.

Installing Devices, like Server configuration, is guided by a Wizard and implements a series of default parameters based on the associated equipment. Any user with Administrative Authorization then can edit the various Device settings to more closely conform to company requirements through either its Meters (analog) or Status (digital) Channel Properties dialog box.

System Requirements

Foreseer has certain hardware and software requirements; exceeding these prerequisites will enhance the performance of the program. It’s essential that you run Foreseer on server class machines. Refer to the Release Notes for the current recommended minimum hardware, operating system, and database requirements.

Minimum Hardware Requirements

To run Foreseer, you will need a server class machine with

- A minimum of two quad-core processors
- 16 GB of RAM
- 100 GB of free drive space.
Hardware and Security Considerations

Foreseer also has certain hardware and software prerequisites that must be addressed prior to installing the program on the Server. Hardware prerequisites consist of completing the Configuration Checklist for all of the Devices to be monitored, then establishing physical connections between the Server and the Devices to be monitored.

Security Considerations consist of the following best practices:

- Physical access to server hosting Foreseer and the associated system should be restricted, monitored and logged at all times.
- Physical access to the communication lines should be restricted to reduce the risk of intrusion.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.
- Access to physical ports and removable media should be controlled and limited.
- Do not connect unauthorized USB device, CD/DVD or SD card for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB, CD/DVD or SD card slot, scan the device for malwares and virus.
- Foreseer servers should be deployed on systems with limited access to the inter-net and less trusted networks. The use of email and other functions not necessary for Foreseer to operate should be limited and protected appropriately.

You should restrict access to ports through the Windows Firewall. Foreseer needs the following ports:

- Port 80 (disabled by default in Apache), required only if you allow HTTP access to WebViews and WebAdmin. HTTP access is inherently insecure and is not recommended.
- Port 81, (disabled by default in the Foreseer web server), required for HTTP access for the WebConfig utility. HTTP access is inherently insecure and is not recommended.
- Port 443, required for HTTPS access for WebViews and WebAdmin.
- Port 444, required for HTTPS access for the WebConfig utility.
- Port 2100, required for Remote/Redundant Foreseer Servers.

SQL Server may require additional ports.

Before proceeding it is recommended that you complete the Configuration Checklist to use as a reference during program installation. Refer to the end of this guide for a copy for a printable copy of the Configuration Checklist.

Supported Environments

Supported Operating Systems

<table>
<thead>
<tr>
<th>Windows Desktop Operating Systems</th>
<th>Message Manager</th>
<th>PowerXpert Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Embedded</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Windows 10 Professional, x64  X  X
Windows 10 Enterprise, x64  X  X

Windows Server Operating Systems  Server & Message Manager
Windows Server 2012 R2 Std  X
Windows Server 2012 R2 Datacenter  X
Windows Server 2016  X

Supported Database Platforms

- SQL Server 2012 Express w/ Advanced Services, Std., Ent, Ent Core, Business Intelligence, SP2
- SQL Server 2014 Express w/ Advanced Services, Std, Ent, Business Intelligence
- SQL Server 2016 Express w/ Advanced Services, Std, Ent, Business Intelligence

Supported Browsers

- Internet Explorer 11 - 11.0.46 or later
- Safari
  - MacOS minimum requirement – MacOS 10.12 “Sierra” and later
  - iOS minimum requirement – iPad platforms with iOS 10.0 and later
- Chrome - 61.0 or later
- Edge - 41.0 or later

Exiting the Program

Exiting terminates the current Foreseer Server session. There are several ways to quit the program:

- Select the Close command under the Foreseer icon in the application’s title bar.
- Click on the Windows Close button in the application’s title bar.
- Select the Exit command in the Foreseer menu.
- Simultaneously press the Alt and F4 keys.

Regardless of the method you choose to quit the Foreseer application, you are prompted to confirm that you wish to terminate the session. Press OK to end the current session; Cancel returns to program operation.

☑ Administrative Authorization is required to Exit the application.
Security Considerations for Interactive Remote Access

Interactive remote access to Foreseer or third party communication interfaces should be limited and secured. Windows Remote desktop access should be configured according to the following:

- Only allow log in from specific hosts. You can use white list using the Windows Firewall.
- Use client encryption Network Level Authentication (NLA).
- Limit access to users in a designated remote access group; e.g., create a group in Active Directory and assign users or user.
- Limit access to explicit machines; i.e., white list access.
- Always prompt for client credentials; i.e., do not store credentials.
- Delete temporary folders when session ends.
- Apply account lockout policy (< 30 minutes default).

SQL Server Express Installation

SQL Server 2016 Express is shipped with Foreseer 7 and installation is straightforward. SQL Server 2016 Express uses .NET 4.6.

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.

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

The Backup archive includes the Foreseer Server configuration data files are not backed up in this procedure. Data backups are NOT handled by Foreseer but by SQL Server in accordance to your corporate data backup policy.

To back up a Foreseer Server configuration:

1. Select Configuration Backup in the Configuration menu to display the Save Server Configuration Backup As dialog box.
2. Foreseer will initiate the backup process and create a single archive file in the \ Restore\ directory of your Foreseer server installation.
3. When finished, Foreseer will report “Backup completed successfully” and provide the name and location of the archive file. Click OK to finish.

Automatic Configuration Backups

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 of the directories under the Foreseer installation directory. Otherwise, the backup process may fail.

To schedule regular backups:

1. Select Backup in the Servers Configuration menu.
2. Specify when the backup is to be performed. 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.

3. Check the Day(s) of the Week on which the backup is performed. Daily backups are strongly encouraged and recommended.

4. Enter or browse to the desired backup path.

5. You can adjust the maximum number of backups that are stored in the specified path.

6. Click OK to enable the displayed Data Backup settings. Archiving will be performed automatically at the scheduled time on the selected day(s).

Recommended Secure Hardening Guidelines

Foreseer is designed with Cybersecurity as an important consideration. A number of Cybersecurity features are now offered in the product which, if implemented as per the recommendations in this section, will minimize Cybersecurity risk. This section provides information and guidelines on how to securely deploy and maintain a Foreseer installation. By following the guidelines provided here within, sites can play a proactive role in minimizing Cybersecurity risks.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys best practices and the latest technologies in its products and solutions; making them more secure, reliable and
competitive for our customers. Eaton also offers Cybersecurity Best Practices white papers to its customers that can be referenced at

http://www.eaton.com/cybersecurity

Secure Configuration Guidelines

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset identification and Inventory</td>
<td>Keeping track of all the devices in the system is a prerequisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner that uniquely identifies each component. To facilitate this, Foreseer is capable of generating a System Configuration Report. This report provides information about devices - including IP address and port assignment. For more details, refer the WebViews Guide for a description on using WebViews Reports.</td>
</tr>
<tr>
<td>Physical Protection</td>
<td>Industrial control devices lack cryptographic protections at protocol level, at physical ports and at controller mode switches leaving them exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. Foreseer is designed with the consideration that it would be deployed and operated in a physically secure location.</td>
</tr>
<tr>
<td>Authorization and Access Control</td>
<td>It is extremely important to securely configure the logical access mechanisms provided in Foreseer to safeguard from unauthorized access. Eaton recommends that the available access control mechanisms be used properly to ensure that access to the system is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions.</td>
</tr>
<tr>
<td>- Ensure default credentials are changed upon first login. Foreseer should not be commissioned for production with Default credentials; it's a serious Cybersecurity flaw as default credentials may be published in manuals.</td>
<td></td>
</tr>
<tr>
<td>- No password sharing – Make sure each user is assigned their own unique and dedicated password vs. sharing passwords. Security monitoring features of Foreseer are created with the expectation that each user has their own unique password. Security controls are weakened as soon as the users start sharing the password.</td>
<td></td>
</tr>
<tr>
<td>- Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a users duties.</td>
<td></td>
</tr>
<tr>
<td>- Perform periodic account maintenance (remove unused</td>
<td></td>
</tr>
</tbody>
</table>
### Recommended Secure Hardening Guidelines

**Server Guide**

Foreseer 7.0

MN152019EN

February 2018

www.eaton.com

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Change passwords and other system access credentials whenever there is a personnel change. Eaton recommends that following secure considerations be implemented by customers while deploying Foreseer:</td>
</tr>
</tbody>
</table>
|                   | 1. Securely configuring User groups, roles and privileges  
|                   | 2. Securely configuring web server and client white listing  
|                   | 3. LDAP configuration and Windows security configuration  
|                   | 4. Security User Group Access Information  
|                   | 5. Changing Foreseer default user account  
|                   | 6. Configuring Interactive Remote Access  
| Network Security  | Foreseer provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open up a big security hole if it’s not configured securely.                                                                 |
|                   | • Eaton recommends segmentation of networks into logical enclaves and restricting the communication to host-to-host paths. This helps protect sensitive information and critical services, and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control.  
|                   | • Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices.  
|                   | Please review detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for Foreseer to operate smoothly.  
|                   | The following additional network security controls should be considered when deploying Foreseer.  
|                   | • Internet/ Email restrictions: Internet and email traffic to Foreseer is not recommended. Additional network controls and Windows Firewall should be used to filter unnecessary traffic from Foreseer nodes.  
|                   | • Traffic control and filtering: Configure Windows Firewall to limit unnecessary traffic to Foreseer  
|                   | • Foreseer uses port 80, 81 for accessing web server over HTTP. These ports should be allowed in firewall for uninterrupted operation of Foreseer application. HTTP is by default disabled on Foreseer web server. Usage of HTTPS is recommended as HTTP communication is unencrypted and unsecured. |
can lead to compromise of sensitive information.

- Foreseer uses port 443,444 for accessing web server over HTTPS. These ports should be allowed in firewall for uninterrupted operation of Foreseer application.
- Foreseer supports Remote/Redundant Servers on TCP port 2100. If Foreseer is configured to support remote/redundant servers, allow TCP port 2100 in firewall.

It is possible to obtain a System Configuration report from Foreseer. Information regarding IP addresses and Ports used can be found in this report.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Security</td>
<td>Foreseer supports Microsoft SQL Server. Eaton recommends following best practices for securely maintaining the database:</td>
</tr>
<tr>
<td></td>
<td>Physical Security: Verify physical security to the machine hosting the Foreseer server database. Physical access to these machines should be access controlled, monitored and logged at all times.</td>
</tr>
<tr>
<td></td>
<td>Logical access: Restrict logical access to database on the basis of roles and permissions. Change default credentials on first use. Do not share passwords of one account with multiple people. Change password on personnel change or as per the organization's password policy.</td>
</tr>
<tr>
<td></td>
<td>Auditing: All access to the database including administrative and maintenance activities should be logged and maintained for at least 3 months or as per organization's policy.</td>
</tr>
<tr>
<td></td>
<td>Backup &amp; Restore: Databases should be properly backed up at a secure location so that it can be restored at any point of time in case of any failure.</td>
</tr>
<tr>
<td></td>
<td>Patching and Updating: Regularly update database software to latest secure supported version.</td>
</tr>
<tr>
<td></td>
<td>Database should be store behind firewalls and, by default all traffic should be disabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logging and Event Management</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored; including all administrative and maintenance activities.</td>
</tr>
<tr>
<td></td>
<td>Ensure that logs are backed up; retain the backups for a minimum of 3 months or as per organization's security policy.</td>
</tr>
<tr>
<td></td>
<td>Perform log review at a minimum every 15 days.</td>
</tr>
</tbody>
</table>

Eaton recommends configuring Windows audit policy on Foreseer Server. Please find the recommended configurations below:

- If Windows Authentication is used, it can be configured to log user logins.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Maintenance</td>
<td>Best Practices</td>
</tr>
<tr>
<td></td>
<td>Apply Firmware updates and patches regularly</td>
</tr>
<tr>
<td></td>
<td>Due to increasing CyberAttacks on Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released.</td>
</tr>
<tr>
<td></td>
<td>CST, Customer Success Team is available for customer to contact at</td>
</tr>
</tbody>
</table>
|                     |   o For callers within the domestic United States.  
|                     |     ▪ Direct: 800-356-3292  
|                     |     ▪ For callers outside of the United States  
|                     |       ▪ 1-828-651-0786, Opt 2, 4, 1, then 2  
|                     |     ▪ Email  
|                     |       ▪ cst@eaton.com |
|                     | Customer notification and update process is manually managed through our Customer Care Contracts administration and through CST. Future notification and delivery methods are being reviewed to determine how/if we can provide them electronically but that is currently not an option. |
|                     | Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site - http://eaton.com/cybersecurity |
|                     | Please contact CST, immediately in case of any vulnerability found in Foreseer. |
|                     | Conduct regular Cybersecurity risk analyses of the organization /system. |
|                     | Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment |
and within Eaton’s own development cycle process. Eaton can provide guidance and support to your organization’s effort to perform regular cybersecurity audits or assessments.

**Plan for Business Continuity / Cybersecurity Disaster Recovery**

It’s a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure off site backups include:

- Backup of the latest f/w copy of Foreseer. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Foreseer.
- Backup of the most current configurations.
- Documentation of the most current User List.
- Save and store securely the current configurations of the device.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>and within Eaton’s own development cycle process. Eaton can provide guidance and support to your organization’s effort to perform regular cybersecurity audits or assessments.</td>
</tr>
</tbody>
</table>
Foreseer employs dialog boxes to enter program information such as the properties which govern its various operations. Consistent with Windows displays, the information in some dialog boxes is grouped in categories under tabbed headings. Clicking on a tab selects that category and brings it to the front of the dialog box where the settings may be reviewed and altered. Scroll bars are automatically enabled whenever a dialog box selection list exceeds the available display area.

**Menu Bar**

The **Menu Bar** offers the standard Windows **File** and **Help** menus, as well as application-specific **Administration**, **Configuration**, and **Database** menus containing commands that are unique to Foreseer. Many of the commands are also available in the right-click, context-sensitive **Tree View**. Any grayed commands cannot be performed on the selected item, within the active window, or because the current User does not have **Administrative Authorization**.

**Tree View**

The **Tree View** display scheme, previously called the **Devices** window, has expanded functionality.
The left pane of the Tree View display lists all associated Foreseer Servers as well as their subordinate Devices and Channels. The list, like Windows Explorer, is expanded and contracted by clicking on the "+" and "−" preceding the desired icon. Selecting a Device displays summary information about its resident channels as well as the State, Value and Type of each.

Selecting a Server, Device or Channel displays summary information about its constituent components in the right pane of the window. 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.

The use of leading characters (such as "*" and "!") in list names are used to ensure critical elements sort at the top of the list in larger Server configurations and cannot be included in device/channel naming.

The Tree View also allows Reports to be created and viewed on the Server.

Tree View Menu Commands

Selecting a Server, Device or Channel and right-clicking presents a context-sensitive menu that allows certain Foreseer actions and responses to be performed depending on the highlighted system component. Multiple items of the same type (Devices, for instance) can be selected for manipulation or modification as a group; channels of the same type (Meters or Status) may be selected from different Devices for functions such as graphing.
Alarms

Alarm Acknowledge - allows an alarm condition to be acknowledged on the selected channel(s). Once acknowledged, a channel's representative icons turns blue. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu if necessary.

Alarm Rearm - allows alarm monitoring to resume on the chosen channel(s). A System Generated Note that includes the time of the rearming and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu if necessary. This command is only available for channels with an acknowledged alarm.

Alarm Ack/Rearm - permits an alarm condition to be acknowledged and the selected channel(s) to be rearmed so testing of acquired Values against set Alarm Limits resumes immediately. Acknowledged, a channel's icon turns blue. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu if necessary.

Disarm - suspends Alarm Limit testing for the selected Device(s) or channel(s). Channel data, however, continues to be archived. Disarming a channel is useful when making repairs to avoid reporting nuisance alarms.

Rearm - resumes Alarm Limit testing for the selected Device(s) or channel(s).

Install Device... - allows you to Install Devices on the Foreseer Server so that they may be monitored and added to the Client WebView.

Add User-Defined Channel... - permits the User to create new Derived Channels.

Add Channel... - permits the User to create a new Meters (Analog) or Status (Digital) Channel. This command is not available for all Devices.

Disable - suspends data archiving for the selected Device(s) or channel(s). Disabling is useful when making repairs to avoid archiving inappropriate readings and is necessary in order to Delete or Rename a Device or channel.

Enable - resumes data archiving for the selected Device(s) or channel(s).

Delete - permanently deletes the selected Server, Device or Channel from the Server database. Once removed, its archived information is no longer available. Deleting a Device or Channel should
be done with discretion as removing it can have an adverse affect on Foreseer WebViews configurations.

Rename - permits the selected Device or Channel to be renamed in response to changing conditions. It should be noted that renaming a Device or Channel should be done with discretion as changing a name can have an adverse affect on Foreseer WebViews 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. 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 the Properties are being copied from. These settings then can be individually modified as necessary. If copying from a Device (rather than a single channel), only those channels with the same Name will have their Properties pasted.

Properties... - displays the Device Properties, Meters (Analog), or Status (Digital) Channel Properties, depending upon which is selected.

Installing Devices

You can add new equipment to the Foreseer Server using either a step-by-step installation procedure (outlined in this topic) or by loading a .csv file that contains information about a list of devices. The Device Installation Wizard guides you through the procedure, prompting the necessary information and applying default parameters based on a standard list of monitored points for each Device. Individual settings for these points may be changed later (refer to Channel Properties).

You cannot install a device that has more than 1000 channels

To install a Device on the Foreseer Server:

1. Right-click in the Devices window and select Install New Device to access that dialog box. Locate the Configuration Checklist for the new equipment, then click Next> to continue.
2. Select the appropriate Device from the list of supported equipment and click Next>.
TCP/IP protocol must be installed on the Server PC regardless of the type of Device connection.

3. Accept the suggested Name for the Device, or enter another unique description, up to 24 characters, then click Next > to continue. Note that "_" and "-" are the only non-alphanumeric
characters allowed in the name.

4. Specify whether the interface between the Server and the Device is a Network or a Serial Connection, as well as the appropriate type, and click Next.>

5. Enter the necessary Device Connection information:
6. For a Network Device, enter its IP Address or URL/Web address. This Address must be correct or the Server will be unable to communicate with the target equipment. Click OK to accept the entry and return to the Device Installation Wizard window.

7. Selecting Serial Connection prompts additional interface information. A Direct Serial Connection requires that you specify the COM Port to which the Device is connected and its communications settings. Accept the displayed serial Port or assign another from the drop down list of selections in the Serial Communications Port field.

8. Press the Settings button to display the Port’s Properties dialog box containing additional serial interface parameters. Click OK to enable the displayed parameters and return to the Device Installation Wizard window.

9. Once the Device connection is properly configured, click Next> and Foreseer will attempt to establish connections with the specified equipment.

10. Verify that the information displayed about the Device corresponds to the information recorded on your Configuration Checklist. If not, Cancel the installation and recheck the Device. With the correct Device information displayed, click Next>.

11. With the target Device and the interface connection defined, click Finish to complete the installation. The new equipment will appear in the Devices window. Install any additional Devices, if necessary, using the same procedure for each.

If installation is unsuccessful or the Device information does not appear in the Identification window, go <Back and check that all configuration entries are proper and that hardware connections with the equipment are correct. After verifying the configuration and connections, once again attempt to install the Device. Contact Eaton Corporation - Foreseer Technical Support if Device installation problems persist.

12. With all Devices properly installed, click No to terminate the installation process. You may wish to select newly installed equipment in the Server’s Tree View and review the default settings assigned to each of its input channels. The Properties vary slightly depending on whether it is a Meter (analog) or Status (digital) channel and they only can be changed by a User with Administrative authorization. Refer to Channel Properties for more information on these data
Installing Multiple Devices

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,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.
- **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.

**Examples:**

**Modbus device installs:**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Type</th>
<th>Protocol</th>
<th>Unit ID</th>
<th>IP Address</th>
<th>Port Number</th>
<th>Driver Specific Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>PX Meter 1</td>
<td>PowerXpert Meter 4000 TCP</td>
<td>10.22.50.30</td>
<td>502</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PX Meter 2</td>
<td>PowerXpert Meter 150 TCP</td>
<td>10.22.50.50</td>
<td>951</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SNMP device installs:**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Type</th>
<th>Protocol</th>
<th>Unit ID</th>
<th>IP Address</th>
<th>Port Number</th>
<th>Driver Specific Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW 5125 1</td>
<td>Powerware UPS 5125 SNMP</td>
<td>10.22.50.32</td>
<td>161</td>
<td>public</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PW 5125 2</td>
<td>Powerware UPS 9395 SNMP</td>
<td>10.22.50.75</td>
<td>,</td>
<td>public</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Nothing device installs:**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Type</th>
<th>Protocol</th>
<th>Unit ID</th>
<th>IP Address</th>
<th>Port Number</th>
<th>Driver Specific Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nothing 1</td>
<td>7-Nothing</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- The Foreseer Web Configuration Utility (see the help/manual for that utility for specific instructions). Use the Upload Files feature of Web Configuration. These files should be uploaded to the Server/Vi location.
• The Foreseer Server. Instructions for loading the device list file follows: 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.

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.

Serial Connection

The Device's Port Settings must be specified if a Direct Serial or VIM II connection is used. Either choice requires that you specify the Serial Communications Port and its settings. It also requires that TCP/IP Protocol be previously installed and enabled.

To configure a Direct Serial Connection at the Foreseer Server:

1. Accept the displayed Port, or assign another one if necessary. Click on the associated arrow to display a drop list of those Ports currently available.
2. Press the Settings button to display the named Port’s Properties dialog box containing additional serial interface parameters.

3. Press the OK button to enable the displayed Port Settings and return to the Device Installation Wizard.

The process for entering the necessary configuration settings for a VIM II Direct Serial Connection is similar. After specifying the communications Port and Device Settings for the VIM II, you are prompted to specify the VIM II Address and Port. Click OK to enable the displayed parameters and return to the Device Installation Wizard.

Device Channel Selection

The Device/Channel Selection dialog box is used in configuring a number of Foreseeer functions. Listed Devices and channels are referenced to their respective Servers and must exist there to be available for selection. Clicking on the “+” preceding a Device icon expands its list of configured channels; selecting a channel highlights it.
Deleting Devices and Channels

Devices and channels are easily deleted from the Foreseer Server, rendering their previously archived data no longer available on the current database. In most cases, to restore a channel once it has been removed from the Server configuration, its associated Device must be deleted and re-installed before it is again available.

**Administrative Authorization** is required to Delete Devices and Channels.

To remove a Channel from the Foreseer Server:

1. Choose the **Start Server Configuration** command in the **Configuration menu**. The **Server Configuration Mode** System Channel turns yellow and

```
********SERVER CONFIGURATION MODE********
```

is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the **Tree View** if necessary to locate and select the desired Device or channel, then right-click and choose **Disable** to temporarily suspend data gathering activity.

3. With the desired Device or channel highlighted, right-click to access the context-sensitive
4. Choose **Delete** and you are cautioned that all information about the chosen component will be permanently purged from the Server.
5. Press **Yes** to remove the component from the Server.
6. In the case of a deleted channel, highlight the parent Device once again and choose **Enable** from the context-sensitive menu to restore data gathering.
7. Choose the **End Server Configuration** command in the **Configuration menu** to conclude Server configuration and restore normal Foreseer data gathering activity.

**Server Properties**

The Server Properties dialog box, accessed through the Server Properties command in the Administration menu, allows a number of general settings to be specified. They are organized under four tabs:

**General** provides the name of the Foreseer Server whenever it is reported, such as in Message Management and in Report titles. It also quantifies the information that is written to the Log file. Other settings permit the Server to be enabled as a password-protected user rather than a local system account when running as a service, enabling a delay in startup, and Watchdog Processing support to ensure ongoing system operation.

Remote settings allow WebViews Administrative users to restart the Foreseer application on the Server, perform a complete reboot of the Foreseer Server computer, and upload newer releases of Foreseer software and Device Drivers to the Foreseer Server.

Database specifies a Retry Time, in seconds, after which Foreseer will attempt to reconnect to SQL Server. Foreseer will continue to retry connections, using the specified interval between tries, until a connection is established. The retry attempts can be temporarily disabled to avoid nuisance alarms, or this feature can be disabled entirely through the check box.

Redundant System identifies the Server as a backup to ensure continued site monitoring in the event the principal Server fails. A single redundant Server is designated as a Stand-Alone. In instances where there is more than one such Server, it must be identified as the Primary or Secondary Redundant in the backup system.

**Server Properties - General**

**The Server Properties** dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **General Properties** identifies the Server and configures startup. Click on other tabs to present those **Server Properties**.
Foreseer Server Properties are easily modified to meet your monitoring needs.

To specify General Server Properties:

- Administrative Authorization is required to access Server Properties.

1. Select Server Properties... in the Administration menu.
2. The Logging Level determines the amount and type of data that are logged on the Server. This setting should not be altered unless directed to do so by Eaton personnel.
3. Normally, the Foreseer Server runs as a Service and, by default, uses the local system account (User Name and Password) for access functions. In this case, the User Name should remain blank. If you wish to enable the Server to run as a specific User, enter the appropriate User Name, Password and Domain information.
4. The Startup Delay provides a time to wait, in seconds, before the Foreseer Server itself starts.
5. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Server Properties.
Server Properties - Remote

The **Server Properties** dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. **Remote Properties** allow the Server application and operating system to be rebooted from a Foreseer Client. Software upgrades and Device Driver uploads also can be performed from an authorized Client. Click on other tabs to present those **Server Properties**.

![Server Properties dialog box](image)

Foreseer **Server Properties** are easily modified to meet your monitoring needs.

To specify **Remote Server Properties**:

- **Administrative Authorization** is required to access **Server Properties**.

1. Select **Server Properties...** in the **Administration menu**.
2. Click on the **Remote** tab to display those **Server Properties**. Remote Server settings, by default, are enabled as indicated by the associated checkbox. Modifying any of the following remote settings requires **Server Administration** permission on the accessing Client.
Allow Remote Restart of the Server Application permits connected Clients to restart the Foreseer application on this Server.

Allow Remote Restart of the Operating System on this computer permits connected Clients to remotely perform a complete reboot of the Foreseer Server computer.

This operating system restart should be disabled on Foreseer Servers where Auto-login is not used.

Allow Remote Upgrade of the Server Application and Device Drivers permits authorized Clients to upload newer releases of Foreseer software and Device Drivers to the Server.

3. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Server Properties.

Server Properties - Database

The Server Properties dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. Database Properties determine historic database settings. Clicking other tabs presents those Server Properties.
Foreseeer Server Properties are easily modified to meet your monitoring needs.

To specify Database Server Properties:

- **Administrative Authorization** is required to access Server Properties.

1. Select Server Properties...in the Administration menu.
2. Click the Database tab to display those Server Properties. The dialog box initially identifies the Type of database. The Database Server Name identifies a remote SQL Database Server whenever it is reported, such as in Message Management, Report titles and for Heartbeat functions. The Name can be a maximum of 29 characters, but the field should remain blank if a local SQL Database Server is being used.
3. Enter the Account Name and Password to access a remote SQL Database Server if authentication is different from the local (Windows) system account. Initially, the Account Name is the same as the Administrative Authorization (both passwords are "Admin" by default), but the Account Name is an independent security function protecting SQL Database Server access. Leaving the Account Name field blank forwards the local system account information (as shown above) for login authentication and access to the database.
4. Specify the time (in seconds) between retries if connection with the remote SQL Server is lost. Setting the Retry Time to "0" disables this feature. With a Retry Time entered, you can also check the "Temporarily disable the connection retry..." box to manually suspend operation of this automatic feature, if desired, for maintenance or other reasons.
5. Press OK to enable any changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Server Properties.

Server Properties - Redundant Systems

The Server Properties dialog box identifies important Foreseeer Server settings and allows a number of administrative functions to be performed. Redundant Properties identify the Server as a backup to endure continued site monitoring in the event the principle Server fails. Click on other tabs to present those Server Properties.
Foreseer **Server Properties** are easily modified to meet your monitoring needs.

**To specify Redundant System Properties:**

1. Select **Server Properties**... in the Administration menu.
2. Click on the **Redundant System** tab to display those **Server Properties** and specify the type:
   - **Stand-Alone** is for applications where a single redundant Server is being employed.
   - **Primary and Secondary Redundant** are used in instances where there is more than one backup Server being maintained as part of a redundancy system. Only one Server may be specified as the **Primary Redundant** Server and its **Computer name or IP Address** must be entered to identify it to the **Secondary Redundant** Server(s).
3. Press **OK** to enable any changes, **Cancel** to close this dialog box without changes, or click on the other tabs to review those **Server Properties**.
Device Properties

The **Device Properties** dialog box furnishes operational information on each monitored piece of equipment. This information can be viewed, but not modified unless the Server is in the configuration mode and the User has **Administrative Authorization**. Simply click on the appropriate tab for the desired information:

**General** - Provide a Description of the Device, its Log Messages limit and Identification Information.

**Version** - Reports a variety of information that could help in determining the source of a problem.

**Basic** - Reports if the Device is Disabled or Disarmed.

**Advanced** - Reports Device Communications Settings.

**Port Settings** - Identify the Device's Communications Port and current settings.

**Wiretap** - Displays the actual data stream between the Server and the Device to confirm proper communications.

There may also be an additional tab containing parameters specific to the particular Device.

Device Properties - General

**Device Properties** is a dialog box which furnishes operational information on each monitored piece of equipment. **General Properties** provide a Description of the Device, its Log Messages limit and power Identification Information. Clicking in a field below displays its function: Clicking other tabs presents those **Device Properties**.
Foreseer Device Properties may be for display only, or they can be modified through this dialog box by a User with Administrative Authorization.

To access General Device Properties:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

"********SERVER CONFIGURATION MODE********"

is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired Device.

3. With the desired Device highlighted right-click to access the context-sensitive menu to view its General Properties.
4. Modify the Log Messages field as necessary and click OK.
5. Press OK to enable these changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Device Properties.
6. Select End Server Configuration in the Configuration menu to restore the Server to normal operation.

Device Properties - Version

Device Properties is a read-only dialog box which furnishes operational information on each monitored piece of equipment. Version Properties report a variety of information that could help in determining the source of a problem. Clicking in a field below displays its function: Clicking other tabs presents those Devices Settings.
Foreseer Device Properties may be for display only, or they can be modified through this dialog box by a User with Administrative Authorization.

To access Version Devices Properties:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and “********SERVER CONFIGURATION MODE********”

   is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired UPS.

3. With the desired UPS highlighted, right-click to access the context-sensitive menu.
4. Choose the **Properties** command and click on the **Version** tab. Information includes the current Foreseer and Device Driver **Library Versions**. Additional fields identify the software **Driver** for the chosen Device and furnish software **Copyright** information.

5. Press **OK** or click on the other tabs to review those **Device Properties**.

6. Select **End Server Configuration** in the **Configuration menu** to restore the Server to normal operation.

**Device Properties** - Basic

**Device Properties** is a dialog box which furnishes operational information on each monitored piece of equipment. **Basic Properties** allow a Device to be **Disabled** or **Disarmed**. Clicking in a field below displays its function: Clicking other tabs presents those **Device Properties**.
Foreseer Device Properties may be for display only, or they can be modified through this dialog box by a User with Administrative Authorization.

To access Basic Device Properties:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

```
********SERVER CONFIGURATION MODE********
```

is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired Device.

3. With the desired Device highlighted, right-click to access the context-sensitive menu.
4. Choose the **Properties** command to display the equipment's operational parameters and click on the **Basic** tab.

5. **Disable** or **Disarm** the **Device Status** as necessary (while in the Server Configuration mode) and click **OK**, or simply view the **Properties** as read-only information.

6. Press **OK** to enable these changes, **Cancel** to close this dialog box without changes, or click on the other tabs to review those **Device Properties**.

7. Select End Server Configuration in the **Configuration menu** to restore the Server to normal operation.

**Device Properties - Advanced**

**Device Properties** is a dialog box which furnishes operational information on each monitored piece of equipment. **Advanced Properties** are comprised of the Device’s **Communications Settings**. Clicking in a field below displays its function: Clicking other tabs presents those **Device Properties**.
Foreseer Device Properties may be for display only, or they can modified through this dialog box by a User with Administrative Authorization.

> These values should only be changed if instructed to do so by Eaton Technical Support.

To access Advanced Devices Properties:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

```
SERVER CONFIGURATION MODE********
```

is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired Device.
3. With the desired Device highlighted right-click to access the context-sensitive menu.

4. Choose the Properties command to display the equipment's operational parameters and click on the Advanced tab.

5. Modify the Communications Settings as necessary (while in the Server Configuration mode) and click OK, or simply view the Properties as read-only information.

6. Press OK to enable these changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Device Properties.

7. Select End Server Configuration in the Configuration menu to restore the Server to normal operation.

Device Properties - Port Settings

Device Properties is a dialog box which furnishes operational information on each monitored piece of equipment. Port Properties identify the Device's Communications Port. Clicking in a field below displays its function: Clicking other tabs presents those Device Properties.
Foreseer **Device Properties** may be for display only, or they can modified through this dialog box by a User with **Administrative Authorization**.

**To access Port Properties:**

1. Choose the **Start Server Configuration** command in the **Configuration menu**. The **Server Configuration Mode** System Channel turns yellow and

   "********SERVER CONFIGURATION MODE********"

   is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the **Tree View** if necessary to locate and select the desired Device.

3. With the desired Device highlighted right-click to access the context-sensitive menu.
4. Choose the **Properties** command to display the equipment's operational parameters and click on the **Port Settings** tab.

5. Modify the **Communications** interface as necessary (while in the Server Configuration mode) and click **OK**, or simply view the **Properties** as read-only information.

6. Press **OK** to enable these changes, **Cancel** to close this dialog box without changes, or click on the other tabs to review those **Device Properties**.

7. Select **End Server Configuration** in the **Configuration menu** to restore the Server to normal operation.

**Device Properties - Wiretap**

*Device Properties - Wiretap* is a dialog box which furnishes operational information on each monitored piece of equipment. **Wiretap Properties** display the actual data stream between the Server and Device to confirm proper communications. Clicking in a field below displays its function: Clicking other tabs presents those **Device Properties**.
Foreseer Device Properties may be for display only, or they can be modified through this dialog box by a User with Administrative Authorization.

You should only use this feature if instructed to do so by Eaton Technical Support.

To access Wiretap Devices Properties:

1. Choose the Start Server Configuration command in the Configuration menu. The Server Configuration Mode System Channel turns yellow and

"********SERVER CONFIGURATION MODE********"

is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the Tree View if necessary to locate and select the desired UPS.
3. With the desired UPS highlighted right-click to access the context-sensitive menu.

4. Choose the Properties command to display the equipment’s operational parameters and click on the Wiretap tab.
5. Modify the Max characters per transmission block as necessary and check to display Transmitted and/or Received Data.
6. Click Start and the contents of the data transmission are displayed in the scrolling list box. You can Stop the display, Save... its contents to a file, or Clear it at any time.
7. Press OK to enable these changes, Cancel to close this dialog box without changes, or click on the other tabs to review those Device Properties.
8. Select End Server Configuration in the Configuration menu to restore the Server to normal operation.

User Defined Equations

The User-Defined Equation Properties dialog box is only available for a Derived Channel (analog or digital) and contains its transfer Equation. The Equation already is configured for any default channels that are created when the Device Install procedure is performed. You have the ability to Test the Equation before placing the channel into service to ensure that it produces the desired result.
To establish **User-Defined Equation Properties**:

- **Administrative Authorization** is required to alter **Channel Equation Properties**.

1. Choose the **Start Server Configuration** command in the **Administration menu**. The **Server Configuration Mode** System Channel turns yellow and

   "**SERVER CONFIGURATION MODE**"

   is displayed in the Windows title bar to confirm operational status.

2. Expand the list in the left pane of the **Tree View** if necessary to locate and select the **Derived Channels** folder, then right-click and choose **Disable** to temporarily suspend data gathering activity.
3. With the Derived Channels folder highlighted, right-click to access the context-sensitive menu.
4. Choose Add User-Defined Channel.. and the New User-Defined Channel dialog box is displayed.

5. Give the new channel a Name and specify whether it is a Derived Analog or Derived Digital Channel.
6. Click OK and the channel's Properties are displayed.
7. Click on the User-Defined Equation tab to display that Channel Properties dialog box for the chosen input.
8. Type the desired Equation into the space provided.
9. With the desired Equation entered, click Test to evaluate it; the result is displayed in the associated Channel field.
10. With the proper **Equation** entered, click **OK** to accept the display and return to the previous Foreseer window or click on the other tabs to review those **Channel Properties**.

Mathematical operators that are valid in the transfer **Equation** are:

- **Input Values**: `[Channel] = value`
- **Unlimited Variables**: `x = 3` creates a variable `x` and assigns the value of "3" to it.
- **Channel Variables**: `x = [Channel 1] + [Channel 2]`

**Conditional Statements**:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals</td>
</tr>
<tr>
<td>+</td>
<td>Add</td>
</tr>
<tr>
<td>-</td>
<td>Subtract</td>
</tr>
<tr>
<td>*</td>
<td>Multiply</td>
</tr>
<tr>
<td>/</td>
<td>Divide</td>
</tr>
<tr>
<td>+=, -=, *=, /=</td>
<td>Math operators applied to lvalue using rvalue</td>
</tr>
<tr>
<td>%</td>
<td>Modulus (remainder of a division)</td>
</tr>
<tr>
<td>%=</td>
<td>Modulus applied to lvalue using rvalue</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>Logical and</td>
</tr>
<tr>
<td>!</td>
<td>Logical not</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td>==</td>
<td>Comparison</td>
</tr>
<tr>
<td>-,+</td>
<td>Unary operators</td>
</tr>
<tr>
<td>^</td>
<td>Power (x ^ 2 is x squared)</td>
</tr>
<tr>
<td>++, --</td>
<td>Increment, decrement</td>
</tr>
<tr>
<td>sin</td>
<td>Sine</td>
</tr>
<tr>
<td>cos</td>
<td>Cosine</td>
</tr>
<tr>
<td>tan</td>
<td>Tangent</td>
</tr>
<tr>
<td>asin</td>
<td>Arcsine</td>
</tr>
<tr>
<td>acos</td>
<td>Arccosine</td>
</tr>
<tr>
<td>atan</td>
<td>Arctangent</td>
</tr>
<tr>
<td>log</td>
<td>Natural log</td>
</tr>
<tr>
<td>log10</td>
<td>Base 10 log</td>
</tr>
<tr>
<td>exp</td>
<td>Exponential</td>
</tr>
<tr>
<td>sqrt</td>
<td>Square root</td>
</tr>
<tr>
<td>int</td>
<td>Integer (truncation)</td>
</tr>
<tr>
<td>abs</td>
<td>Absolute value</td>
</tr>
<tr>
<td>red(chan)</td>
<td>Test for critical alarm condition</td>
</tr>
<tr>
<td>yellow(chan)</td>
<td>Test for cautionary alarm condition</td>
</tr>
<tr>
<td>green(chan)</td>
<td>Test for normal state</td>
</tr>
<tr>
<td>prev(chan)</td>
<td>Previous reported channel value</td>
</tr>
<tr>
<td>blue_count()</td>
<td>The number of channels currently in an Acknowledged alarm state</td>
</tr>
<tr>
<td>red_count()</td>
<td>The number of channels currently in a Critical alarm state</td>
</tr>
<tr>
<td>yellow_count()</td>
<td>The number of channels currently in a Cautionary state</td>
</tr>
<tr>
<td>green_count()</td>
<td>The number of channels currently in a Normal state</td>
</tr>
<tr>
<td>setBit(n)</td>
<td>Sets bit n</td>
</tr>
<tr>
<td>checkBit(chan, n)</td>
<td>Checks bit n of the specified channel</td>
</tr>
<tr>
<td>rtime(n)</td>
<td>Real-time clock value</td>
</tr>
<tr>
<td>pulse(n)</td>
<td>Reports TRUE (pulses) for one scan once every n minutes</td>
</tr>
<tr>
<td>min(chan, reset)</td>
<td>Check the channel's minimum value with reset</td>
</tr>
<tr>
<td>max(chan, reset)</td>
<td>Check the channel's maximum value with reset</td>
</tr>
<tr>
<td>intg(chan, reset)</td>
<td>Integrate the channel's value with reset</td>
</tr>
<tr>
<td>rand(min, max)</td>
<td>Generate a random number between the specified minimum and maximum</td>
</tr>
</tbody>
</table>

In addition, the following representative numeric values are available for use in transfer Equations:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>pi</td>
<td>3.14159265358979323846</td>
</tr>
<tr>
<td>e</td>
<td>2.71828182845904523536</td>
</tr>
<tr>
<td>gamma</td>
<td>0.57721566490153286060</td>
</tr>
<tr>
<td>deg</td>
<td>57.29577951308232087680</td>
</tr>
<tr>
<td>phi</td>
<td>1.61803398874989484820</td>
</tr>
<tr>
<td>TRUE</td>
<td>1.0</td>
</tr>
<tr>
<td>FALSE</td>
<td>0.0</td>
</tr>
</tbody>
</table>

To include another channel in the Equation, click on the Insert Channel button and locate it in the
Select Channel dialog box. Highlight the channel and press OK to insert it into the Equation at the cursor location.

Channel Properties

Foreseer is shipped with some pre-configured Device settings. These parameters are defined...
during Server Device installation. You may selectively enter your own settings, if desired. Although any channels Properties reside at the Foreseer Server, they are available for display and/or modification by authorized WebViews users.

To alter Channel Properties:

1. Expand the list if necessary by clicking on the “+” preceding its associated Devices name, then select the desired channel within the Tree View. A Meter (analog) channel is identified by a circle, a Status (digital) channel is a square, a text channel is indicated by a “T” and a clock symbol designates a date channel.
2. Right-click to display the context-sensitive menu and select Properties to access its Channel Properties dialog box.
3. Click on the desired tab in order to access those Channel Properties. The tabs differ slightly depending on whether it is a Meter (analog) or a Status (digital) channel.

Meters Channels

Meters Channel Properties

The Meters Channel Properties dialog box defines an analog channel’s operational settings, which may be reviewed and changed if necessary by clicking on the appropriate tab:

- **Administrative Authorization** is required to alter Meter Channel Properties.

  - **General** - Identifies the channel and how its data are archived on the Foreseer Server.
  - **Basic** - Specifies the channel’s alarm thresholds and associated messages, as well as defining its relative importance.
  - **Advanced** - Specifies a channel’s alarm delays and their thresholds.
  - **User-Defined Equation** - Contains the Transfer Equations for Derived Channel.

Meters Properties - General

The Meters Properties dialog box defines an analog channel’s operational parameters. General Meters Properties identify the channel and how its data are archived on the Server. Clicking in a field below displays its function: Clicking other tabs presents those Meters Channel Properties.
Foreseer is shipped with some default Meters Channel Properties based on the associated Device. These standard settings, which are downloaded during Server Device Installation, are easily altered to meet your monitoring needs.

To modify General Meters Channel Properties:

1. Expand the hierarchical list if necessary by clicking the "+" preceding its corresponding Device, then select the desired analog channel. Meters Channels are identified by a circle icon.
2. With the channel highlighted, right-click to display the context-sensitive menu.
3. Choose the Properties command to display the analog input's **General Channel Properties** dialog box. The Channel State and Current Value fields reflect the existing input and cannot be changed.
4. Enter a Description of the channel, if desired, to more easily identify it.
5. Enter the desired display Units for this channel's readings. The Units are reported in conjunction with the channel's Current Value.
6. Specify an Archive method for storing this channel's data on the Foreseer Server database. It may be the AVERAGE Value reported, or the MINIMUM, MAXIMUM, FIRST or LAST reading over the archive interval for this analog channel.
7. You optionally can Disable or Disarm the Channel from this dialog box.
8. With the desired General settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those **Meters Channel Properties**.

Meters Properties - Basic

The **Meters Properties** dialog box defines an analog channel's operational parameters. **Basic Meters Properties** activate and define the channel's alarm thresholds, associated Messages and relative importance. Clicking in a field below displays its function: Clicking other tabs presents those **Meters Channel Properties**.
Foreseer is shipped with some default Meters Channel Properties based on the associated Device. These standard settings, which are downloaded during Server Device Installation, are easily altered to meet your monitoring needs.

To modify Basic Meters Channel Properties:

1. Expand the hierarchical list if necessary by clicking the “+” preceding its corresponding Device, then select the desired analog channel. Meters Channels are identified by a circle icon.
2. With the channel highlighted, right-click to display the context-sensitive menu.
3. Choose the Properties command to display the analog input’s **General Channel Properties** dialog box.
4. Click on the Basic tab to display that **Meters Channel Properties** dialog box for the chosen input.
5. You can enable each of the four alarm levels that is to be monitored for this channel, if desired, by checking the appropriate Hi or Lo box to activate monitoring of the channel's Cautionary (yellow) and/or Critical (red) Limits. Devices are installed in Foreseer with many pertinent alarms enabled to furnish users with comprehensive alarm notification. This default could result in multiple alarms for a single event, especially between analog and digital points for a particular Device. If these standard settings are determined to be excessive or redundant, you can disable the appropriate Cautionary or Critical Alarm, adjust its corresponding threshold Limit or create a Filter at the Client to screen out inconsequential or nuisance alarms.
6. Optionally enter a value (in the channel’s display Units) for each of the excursion Limits that is to be monitored.
7. Enter an Alarm Message for each of the enabled events, if desired. Messages may be independently assigned to the Hi and Lo Limits to appear in conjunction with the alarm condition whenever it is reported.
8. Assign the channel an alarm Priority (1 = highest, 9999 = lowest). Whenever any of its assigned Limits is exceeded, the channel can be listed in the Alarm Management window based on its relative Priority.
9. With the desired Basic settings specified, click **OK** to accept the current entries and return to the Tree View or click on the other tabs to review those **Meters Channel Properties**.

**Meters Properties - Advanced**

The **Meters Properties** dialog box defines an analog channel’s operational parameters. Basic **Meters Properties** activate and define the channel’s alarm thresholds, associated Messages and relative importance. Clicking in a field below displays its function: Clicking other tabs presents those **Meters Channel Properties**.
Foreseer is shipped with some default **Meters Channel Properties** based on the associated **Device**. These standard settings, which are downloaded during Server **Device Installation**, are easily altered to meet your monitoring needs.

To modify **Advanced Meters Channel Properties**:

- **Administrative Authorization** is required to alter **Meter Channel Properties**.

1. Expand the hierarchical list if necessary by clicking the "+" preceding its corresponding Device, then select the desired analog channel. **Meters Channels** are identified by a circle icon.
2. With the channel highlighted right-click to display the context-sensitive menu.
3. Choose the Properties command to display the analog input’s General Channel Properties dialog box.
4. Click on the Advanced tab to display that Meters Channel Properties dialog box for the chosen input.
5. You can specify the Ack Holdoff, the delay after a channel alarm has been acknowledged (or silenced) before it is again rearmed, in seconds. Acquired data continues to be displayed during the Holdoff period, but the channel’s Current Value is no longer compared to its defined Alarm Limits. The default Holdoff of one hour may be manually overridden at any time using the Rearm command, or when the alarm is acknowledged.
6. Similarly indicate the Re-Arm delay, the period of time before alarm monitoring is automatically restored to a disabled channel, (also in seconds). Rearming a channel manually resumes testing of its acquired Current Value against its enabled Alarm Limits.
7. Optionally enter a Delay Alarm interval (in seconds) before an alarm detected on this channel is reported.
8. Disable alarm Latching, if desired, to automatically remove the channel from the active alarm list if its Value returns to within specification and minimize the reporting of minor or nuisance alarms. This approach could, however, result in missed alarms on channels that are experiencing momentary events. Enable Latching to continue to report the channel’s alarm state (even if its Current Value returns to within specification) until the condition is acknowledged. The alarm also must be Enabled under the Basic tab in the Meters Channel Properties dialog box.

All detected alarms are available through the Foreseer Client’s Alarm History Reports.

You also may wish to assign a Hysteresis Value, the threshold above and below which a new
alarm is reported. Hysteresis is used to eliminate nuisance alarms when the channel's current reading is near its Alarm Limit. Once an alarm occurs, the input level must drop below or rise above the threshold Value specified in the channel's display Units (i.e., volts, amps, Hz, kVA, kw, etc.), then exceed the Limit once again before a new alarm is reported for the channel. Note that this attribute is only available for non-Latching alarms.

9. Use the Enable Scaling setting to manually establish alternate Minimum and Maximum Raw and Scaled Values for this channel, if desired. Only integer Values are acceptable entries and these settings should only be altered at the direction of Eaton personnel.

10. With the desired Advanced settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Meters Channel Properties.

Status Channels

Status Channel Properties

Foreseer is shipped with some Status Channel settings preset. These parameters are defined during Device Installation. The Status Channel Properties dialog box defines a digital channel's operational settings, which may be reviewed and changed if necessary by clicking on the appropriate tab:

- **General** - Identifies the channel and what constitutes True and False digital signals.
- **Basic** - Activates the channel's alarm monitoring feature in addition to defining its associated Message, alarm state, alarm level and relative importance.
- **Advanced** - Specifies a channel's alarm delays and thresholds.
- **User-Defined Equation** - Contains the Transfer Equations for Derived Channel.

Status Properties - General

The Status Properties dialog box defines a digital channel's operational parameters. General Status Properties identify the channel and what constitutes True and False signals. Clicking in a field below displays its function: Clicking other tabs presents those Status Channel Properties.
Foreseeer is shipped with some default Status Channel Properties based on the associated Device. These standard settings, which are downloaded during Server Device Installation, are easily altered to meet your monitoring needs.

To modify General Status Channel Properties:

- **Administrative Authorization** is required to alter Channel Properties.

1. Expand the hierarchical list if necessary by clicking the “+” preceding its corresponding Device, then select the desired digital channel. Status Channels are identified by a square icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.
3. Choose the Properties command to display the digital input’s **General Channel Properties** dialog box. The Channel State and Current Value fields reflect the existing input and cannot be changed.
4. Enter a Description of the channel, if desired, to more easily identify it.
5. Optionally enter the condition that represents the channel when its Current Value is True String, followed by its False String entry.
6. You also can Disable or Disarm the Channel from this dialog box.
7. With the desired General settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Status Properties.

**Status Properties - Basic**

The **Status Properties** dialog box defines a digital channel’s operational parameters. **Basic Status Properties** activate the channel’s alarm monitoring feature in addition to defining its associated Message, alarm state, alarm level and relative importance. Clicking in a field below displays its function: Clicking other tabs presents those **Status Channel Properties**.
Foreseeer is shipped with some default Status Channel Properties based on the associated Device. These standard settings, which are downloaded during Server Device Installation, are easily altered to meet your monitoring needs.

To modify Basic Status Channel Properties:

- **Administrative Authorization** is required to alter Channel Properties.

1. Expand the hierarchical list if necessary by clicking the “+” preceding its corresponding Device, then select the desired digital channel. Status Channels are identified by a square icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.
3. Choose the Properties command to display the digital input's **General Channel Properties** dialog box.
4. Click on the Basic tab to display that **Status Channel Properties** dialog box for the chosen input.
5. Enable Alarm reporting for this channel, if desired, by checking its corresponding box.
6. You can enter an Alarm Message corresponding to an enabled excursion. The Message appears in conjunction with the alarm condition when it is reported.
7. Optionally, specify whether the digital channel reports an alarm on a True (1) or False (0) Value and whether the condition represents a Critical or Cautionary event.
8. Assign the channel an alarm Priority (1 = highest, 9999 = lowest). Whenever any of its assigned Limits is exceeded, the channel can be listed in the **Alarm Management** window based on its Priority.
9. With the desired Basic settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Status Properties.

**Status Properties - Advanced**

The **Status Properties** dialog box defines a digital channel's operational parameters. Advanced Status Properties specify the channel's delays and thresholds in an alarm condition. Clicking in a field below displays its function: Clicking other tabs presents those **Status Channel Properties**.
Foreseer is shipped with some default Status Channel Properties based on the associated Device. These standard settings, which are downloaded during Server Device Installation, are easily altered to meet your monitoring needs.

To modify Advanced Status Channel Properties:

- **Administrative Authorization** is required to alter Channel Properties.

1. Expand the hierarchical list if necessary by clicking the “+” preceding its corresponding Device, then select the desired digital channel. Status Channels are identified by a square icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.

3. Choose the Properties command to display the digital input's General Channel Properties dialog box.

4. Click on the Advanced tab to display that Status Channel Properties dialog box for the chosen input.

5. You can specify the Ack Holdoff, the delay after a channel alarm has been acknowledged (or silenced) before it is again rearmed, in seconds. Acquired data continues to be displayed during the Holdoff period, but the channel's Current Value is no longer compared to its defined Alarm Value. The default Holdoff of one hour may be manually overridden at any time using the Client's Rearm command, or when the alarm is acknowledged.

6. Similarly indicate the Re-Arm delay, the period of time before alarm monitoring is automatically restored to a disabled channel, (also in seconds). Rearming a channel manually resumes testing of its acquired Current Value against its enabled Alarm Limits.

7. Optionally enter a Delay Alarm interval (in seconds) before an alarm detected on this channel is reported.

8. Disable alarm Latching, if desired, to automatically remove the channel from the active alarm list if its Value returns to within specification and minimize the reporting of minor or nuisance alarms. This approach could, however, result in missed alarms on channels that are experiencing momentary events. Enable Latching to continue to report the channel's alarm state (even if its Current Value returns to within specification) until the condition is acknowledged. The alarm also must be Enabled under the Basic tab in the Status Channel Properties dialog box.

☑ All detected alarms are available through Foreseer Alarm History Reports.
9. With the desired **Advanced** settings specified, click **OK** to accept the current entries and return to the **Tree View** or click on the other tabs to review those **Status Properties**.

**System Channels**

**System Channels** monitor critical Foreseer Server operations. These predefined channels change color when a state change is detected. Their individual **Meters** (analog) or **Status** (digital) **Channel Properties** may be modified once they have been added to the system, although alteration is not recommended.

---

The reported **System Channels** are:

**Active Client Connections** indicates the number of Foreseer Clients currently communicating with the Server.

**Archive Elapsed Time** reports the interval between High-resolution data archives.

**Configuration Backup** indicates when a change has been made to the Server configuration and a system backup is recommended.

**Database Archiving** reports when the data are being properly logged into the Server database.

**Database Backup** alarms when a scheduled data backup operation was unsuccessful.

**Database Status** reports the current condition of the Server’s database. This channel alarms if any problems are detected in accessing the database.

**Disk Free Space** displays the amount of disk space available on the local hard drive on which...
**Foreseeer Server Application** is installed. This channel alarms when its analog input value drops below the **Lo Caution** and **Critical Limits** set in its **Basic Channel Properties** dialog box.

**Major Server Version** reports structural changes to the Server configuration, like renaming, adding or deleting a Device or Channel which would significantly impact remote Foreseeer Client displays and necessitate that they update their configurations. **Major Server Version** changes require enabling the **Server Configuration Mode**. A **Configuration Backup** should be performed when **Major** changes are reported to the Server.

**Minor Server Version** reports when incidental changes have been made to the Server configuration. **Minor** changes, such as altering a **Channel’s Properties**, are accomplished without entering the **Server Configuration Mode**.

**Server Configuration Mode**, when yellow (as shown above), indicates the Server is in the Configuration Mode. In this “live” modification state, data continue to be archived and alarms reported for all enabled Devices.

**System Alarm** indicates a system-wide problem such as the Server is unable to load a device driver. Refer to the **Log File** for more information.

**System Warning** indicates minor system problem has been detected. Refer to the **Log File** for more information.

**User Defined Channels**

- Renaming or deleting existing channels or Devices can have an adverse effect on Foreseeer WebViews links.

**User Defined Channels**

User-defined channels can be analog, digital, text or date-based to address specific monitoring needs. A Text Channel is used to enter a text string (or optionally a User-defined channel can be used to assign a text string to a text channel), such as the Devices serial number for quick retrieval. A Date Channel can be used, for example, to generate an alarm notification that it is time to perform a scheduled maintenance procedure.

To create a User-Defined Channel:

- **Administrative Authorization** is required to **Add** a derived channel.

1. Choose the **Start Server Configuration** command in the **Configuration menu**. The **Server Configuration Mode** System Channel turns yellow and
"********SERVER CONFIGURATION MODE********

" is displayed in the Windows title bar to confirm operational status.

2. Click on the Derived Channels folder in the left pane of the Tree View to highlight it.
3. Choose Add User-Defined Channel... in the Configuration menu (or right-click and select the command from the context-sensitive menu) and the New User-Defined Channel dialog box is displayed.

4. Enter a Name for the new user-defined channel (observing the character restrictions) and indicate whether it is a Derived Analog or Digital Channel Type.
5. A Text Channel is used to enter a text string, such as a Device’s serial number:
6. A **Date Channel** can be used to automatically generate an alarm notification that it is time to perform a scheduled maintenance procedure.

7. Press **OK** to create the specified channel. It is added to the Derived Channels list and loaded with some default parameters. Analog and Digital Channel settings can be modified in their respective **Meters** or **Status Channel Properties** dialog box.

✔ For more information about User Defined Equations, you can request training as well as a detailed white paper from Eaton's Customer Success Team.
8. Choose **End Server Configuration** in the **Configuration menu** to return to normal Foreseer operation.

**Text Channel Properties - General**

The **Channel Properties** dialog box defines a **Text Channel**’s operational parameters. **General Text Channel Properties** identify the channel and its function. Clicking in a field below displays its function.
Forseeer is shipped with some default Channel Properties. These standard settings, which are downloaded during channel creation, are easily altered to meet your monitoring needs.

To modify General Derived Text Channel Properties:

- **Administrative Authorization** is required to alter General Derived Text Channel Properties.

1. Expand the hierarchical list if necessary by clicking the "+" preceding the Derived Channels folder, then select the desired channel. Text Channels are identified by a "T" icon.
2. With the channel highlighted right-click to display the context-sensitive menu.
3. Choose the Properties command to display the Text Channel's **General Properties** dialog box. The Channel State and Current Value fields reflect the existing input and cannot be changed.
4. Enter the Value that this channel’s reading represents, such as a Device serial number.
5. Enter a Description of the channel, if desired, to more easily identify it.
6. You can temporarily Disable the Channel from this dialog box by checking the appropriate box.
7. With the desired General settings specified, click OK to accept the current entries and return to the Tree View.

**Date Channel Properties - General**

The **Channel Properties** dialog box defines a Date Channel's operational parameters. **General Date Channel Properties** identify the channel and its function. Clicking in a field below displays its function: Clicking other tabs presents those Date Channel Properties.
Foreseer is shipped with some default Channel Properties. These standard settings, which are downloaded during channel creation, are easily altered to meet your monitoring needs.

To modify **General Date Channel Properties**: 

- **Administrative Authorization** is required to alter **Date Channel Properties**.

1. Expand the hierarchical list if necessary by clicking the "+" preceding the Derived Channels folder, then select the desired channel. **Date Channels** are identified by a clock icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.

3. Choose the Properties command in to display the derived input’s General Channel Properties dialog box. The Channel State and Current Value fields reflect the existing input and cannot be changed.

4. Enter a Description of the channel, if desired, to more easily identify it.

5. Enter the date and time that represents the channel's true Value state.

6. You can manually Disable or Disarm the Channel from this dialog box.

7. With the desired General settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Date Channel Properties.

Date Channel Properties - Basic

The Date Channel Properties dialog box defines a Date Channel's operational parameters. Basic Date Channel Properties activate the channel's alarm monitoring feature in addition to defining its associated Message, Alarm Type and relative Priority. Clicking in a field below displays its function: Clicking other tabs presents those Date Channel Properties.
Foreseer is shipped with some default Channel Properties. These standard settings, which are downloaded during channel creation, are easily altered to meet your monitoring needs.

To modify Basic Date Channel Properties:

- **Administrative Authorization** is required to alter **Date Channel Properties**.

1. Expand the hierarchical list if necessary by clicking the "+" preceding the Derived Channels folder, then select the desired channel. **Date Channels** are identified by a clock icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.

3. Choose the Properties command to display the digital input's General Channel Properties dialog box.

4. Click on the Basic tab to display that Date Channel Properties dialog box for the chosen input.

5. Enable Alarm reporting for this channel, if desired, by checking its corresponding box.

6. You can enter an Alarm Message corresponding to an enabled excursion. The Message appears in conjunction with the alarm condition when it is reported.

7. Specify whether an alarm on this derived channel represents a Critical or Cautionary event.

8. Assign the channel an alarm Priority (1 = highest, 9999 = lowest). Whenever any of its assigned Limits is exceeded, the channel can be listed in the Foreseer Client's Alarm Management window based on its Priority.

9. With the desired Basic settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Date Channel Properties.

Date Channel Properties - Advanced

The Channel Properties dialog box defines a derived Date Channel's operational parameters. Advanced Date Channel Properties specify the channel's reporting delays in an alarm condition. Clicking in a field below displays its function: Clicking other tabs presents those Date Channel Properties.
Foreseer is shipped with some default Channel Properties. These standard settings, which are downloaded during channel creation, are easily altered to meet your monitoring needs.

To modify Advanced Date Channel Properties:

- **Administrative Authorization** is required to alter Date Channel Properties.

1. Expand the hierarchical list if necessary by clicking the "+" preceding the Derived Channels folder, then select the desired channel. Date Channels are identified by a clock icon.
2. With the desired digital channel highlighted, right-click to display the context-sensitive menu.

3. Choose the Properties command to display the digital input’s General Channel Properties dialog box.

4. Click on the Advanced tab to display that Date Channel Properties dialog box for the chosen input.

5. You can specify the Ack Holdoff, the delay after a channel alarm has been acknowledged (or silenced) before it is again rearmed, in seconds. Acquired data continues to be displayed during the Holdoff period, but the channel’s Current Value is no longer compared to its defined Alarm Value. The default Holdoff of one hour may be manually overridden at any time using the Rearm command, or when the alarm is acknowledged.

6. Similarly indicate the Re-Arm delay, the period of time before alarm monitoring is automatically restored to a disabled channel, (also in seconds). Rearming a channel manually resumes testing of its acquired Current Value against its enabled Alarm Limits.

7. Optionally enter a Delay Alarm interval (in seconds) before an alarm detected on this channel is reported.

8. With the desired Advanced settings specified, click OK to accept the current entries and return to the Tree View or click on the other tabs to review those Date Channel Properties.

**Equation**

Equation converts the Derived Channel raw input value into the reported display Units.

Mathematical operators that are valid in the transfer Equation are:

- **Input Values:** \([\text{Channel}] = \text{value}\)
- **Unlimited Variables:** \(x = 3\) creates a variable \(x\) and assigns the value of “3” to it.
- **Channel Variables:** \(x = [\text{Channel 1}] + [\text{Channel 2}]\)
- **Conditional Statements:**
  
<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals</td>
</tr>
<tr>
<td>+</td>
<td>Add</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><code>-</code></td>
<td>Subtract</td>
</tr>
<tr>
<td><code>*</code></td>
<td>Multiply</td>
</tr>
<tr>
<td><code>/</code></td>
<td>Divide</td>
</tr>
<tr>
<td><code>+=, -=, *=, /=</code></td>
<td>Math operators applied to lvalue using rvalue</td>
</tr>
<tr>
<td><code>%</code></td>
<td>Modulus (remainder of a division)</td>
</tr>
<tr>
<td><code>%=</code></td>
<td>Modulus applied to lvalue using rvalue</td>
</tr>
<tr>
<td>`</td>
<td></td>
</tr>
<tr>
<td><code>&amp;&amp;</code></td>
<td>Logical and</td>
</tr>
<tr>
<td><code>!</code></td>
<td>Logical not</td>
</tr>
<tr>
<td><code>&gt;</code></td>
<td>Greater than</td>
</tr>
<tr>
<td><code>&gt;=</code></td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td><code>&lt;</code></td>
<td>Less than</td>
</tr>
<tr>
<td><code>&lt;=</code></td>
<td>Less than or equal to</td>
</tr>
<tr>
<td><code>==</code></td>
<td>Comparison</td>
</tr>
<tr>
<td><code>-</code>, <code>+</code></td>
<td>Unary operators</td>
</tr>
<tr>
<td><code>^</code></td>
<td>Power ((x ^ 2 \text{ is } x \text{ squared}))</td>
</tr>
<tr>
<td><code>++</code>, <code>--</code></td>
<td>Increment, decrement</td>
</tr>
<tr>
<td><code>sin</code></td>
<td>Sine</td>
</tr>
<tr>
<td><code>cos</code></td>
<td>Cosine</td>
</tr>
<tr>
<td><code>tan</code></td>
<td>Tangent</td>
</tr>
<tr>
<td><code>asin</code></td>
<td>Arcsin</td>
</tr>
<tr>
<td><code>acos</code></td>
<td>Arccosine</td>
</tr>
<tr>
<td><code>atan</code></td>
<td>Arctangent</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Natural log</td>
</tr>
<tr>
<td><code>log10</code></td>
<td>Base 10 log</td>
</tr>
<tr>
<td><code>exp</code></td>
<td>Exponential</td>
</tr>
<tr>
<td><code>sqrt</code></td>
<td>Square root</td>
</tr>
<tr>
<td><code>int</code></td>
<td>Integer (truncation)</td>
</tr>
<tr>
<td><code>abs</code></td>
<td>Absolute value</td>
</tr>
<tr>
<td><code>red(chan)</code></td>
<td>Test for critical alarm condition</td>
</tr>
<tr>
<td><code>yellow(chan)</code></td>
<td>Test for cautionary alarm condition</td>
</tr>
<tr>
<td><code>green(chan)</code></td>
<td>Test for normal state</td>
</tr>
<tr>
<td><code>prev(chan)</code></td>
<td>Previous reported channel value</td>
</tr>
<tr>
<td><code>intg(chan, reset)</code></td>
<td>The number of channels currently in an Acknowledged alarm state</td>
</tr>
<tr>
<td><code>red_count()</code></td>
<td>The number of channels currently in a Critical alarm state</td>
</tr>
<tr>
<td><code>yellow_count()</code></td>
<td>The number of channels currently in a Cautionary state</td>
</tr>
<tr>
<td><code>green_count()</code></td>
<td>The number of channels currently in a Normal state</td>
</tr>
<tr>
<td><code>setBit(n)</code></td>
<td>Sets bit n</td>
</tr>
<tr>
<td><code>checkBit(chan, n)</code></td>
<td>Checks bit n of the specified channel</td>
</tr>
<tr>
<td><code>rtime(n)</code></td>
<td>Real-time clock value</td>
</tr>
<tr>
<td><code>pulse(n)</code></td>
<td>Reports TRUE (pulses) for one scan once every n minutes</td>
</tr>
<tr>
<td><code>min(chan, reset)</code></td>
<td>Check the channel's minimum value with reset</td>
</tr>
<tr>
<td><code>max(chan, reset)</code></td>
<td>Check the channel's maximum value with reset</td>
</tr>
<tr>
<td><code>intg(chan, reset)</code></td>
<td>Integrate the channel's value with reset</td>
</tr>
<tr>
<td><code>rand(min, max)</code></td>
<td>Generate a random number between the specified minimum and maximum</td>
</tr>
</tbody>
</table>

In addition, the following representative numeric values are available for use in transfer **Equations:**
In addition, the following representative numeric values are available for use in transfer Equations:

The following Equations are used to define Set-Point, Digital and Tri-State Control Points:

*The syntax must be entered exactly* or the equation will not work properly.

### Set-Point Control

**Variable Name:**

```
_SETPOINT_       The current Set-Point value.
```

**Comment Fields:**

```
_CAPTION_      A single line of text to be displayed at the top of the dialog box.
_MIN_          The maximum allowed Set-point value.
_MAX_          The maximum allowed Set-point value.
_FLOAT_        The Set-Point value is a floating point number
```

**Example:**

```
_SETPOINT_=72;

//
// _CAPTION_="A sample line of text to be displayed at the top of the dialog box"
// _MIN_=66
// _MAX_=76
//

[Liebert AC 1Setpoint]=_SETPOINT_;

//
// the following line of code is required to set the channel
// value to the current set-point
//
// _SETPOINT_;
Digital Control

Variable Name:  
_TWOSTATE_  
The current Control Point state (0 or 1).

Comment Fields:  
_CAPTION_  
A single line of text to be displayed at the top of the dialog box.  
_TITLE0_  
The radio button label for state 0.  
_TITLE1_  
The radio button label for state 1.

Example:

_TWOSTATE_ =1;

//  
// _CAPTION_ ="A sample line of text to be displayed at the top of the dialog box"
// _TITLE0_ ="State 0 button label"
// _TITLE1_ ="State 1 button label"
//

if(_TWOSTATE_ ==0)  
// add the control code for state 0
else  
// add the control code for state 1

//  
// the following line of code is required to set the channel  
// value to the current state  
//

_TWOSTATE_;  

Tri-State Control

Variable Name:  
_TRISTATE_  
The current Control Point state (0,1 or 2).

Comment Fields:  
_CAPTION_  
A single line of text to be displayed at the top of the dialog box.  
_TITLE0_  
The radio button label for state 0.  
_TITLE1_  
The radio button label for state 1.  
_TITLE2_  
The radio button label for state 2.

Example:

_TRISTATE_ =2;
// _CAPTION_ ="Tri-State Control Sample"
// _TITLE0_ ="State 0 button label"
// _TITLE1_ ="State 1 button label"
// _TITLE2_ ="State 2 button label"
//
// if(_TRISTATE_==0)
// add the control code for state 0
else if(_TRISTATE_==1)
// add the control code for state 1
else if(_TRISTATE_==2)
// add the control code for state 2
else
// code to handle an illegal or unexpected value
//
// the following line of code is required to set the channel
// value to the current state
//
/TRISTATE/;

An option has been added to allow some fixed strings to be used for the values of a Tri-State control. Remember to select the same format option for all channel states. The options are:

- Off, On, Auto
- Disabled, Enabled, Auto
- Stop, Start, Auto
- Off, Low, High

- Off, Low and High

Reports

Foreseer Reports

Foreseer Reports produce ASCII text files that furnish important insights into system performance by providing predefined information. All of the archived information required to produce a Report already resides at the Foreseer Server and can be reviewed locally, printed and distributed to concerned departments or incorporated into other documents.
**Reports** are created and maintained at the individual Server and cannot be modified by the Foreseer Client.

The Foreseer **Report** formats are:

**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.

**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.

Choose `<Reports>` in the left pane of the **Tree View** to access this Foreseer function. The list of **Reports** in a particular format is expanded by clicking on the "+" which precedes its associated folder; pressing "-" contracts them. The last three **Reports**, including the time and date they were last **Run** and their file size, are displayed. You can **Retrieve** any of these **Reports** or **Run** new ones. A retrieved **Report** can be viewed, printed or incorporated into other documents, if desired.

**A Report** must be **Run** before its data can be **Retrieved**.
Running Reports

Running a Foreseer Report compiles data which is then Retrieved for display, print or incorporation into other programs.

To Run a Foreseer Report:

- Administrative Authorization is required to Run a Report.

1. Choose <Reports> folder in the left pane of the Tree View and click on the "4" preceding it to display the list of available Report Types.
2. Select the desired Report format by highlighting its folder.
3. Right-click and choose the Run Report command to compile the chosen Report. Display of the date, time and file size indicates that the Report has finished Running.
4. Open the folder, highlight the Report and double-click on it to display it.

Retrieving Reports

Foreseer Reports that have been Run can be viewed and printed, if desired. A Report can also be saved as a text file imported into word processing or spreadsheet programs for further manipulation or incorporated into other documents.

To Retrieve a Foreseer Report:

> Administrative Authorization is required to Run a Report.

1. Choose <Reports> folder in the left pane of the Tree View and click on the "+" preceding it to display the list of available Report Types.
2. Select the desired Report folder and once again click on the "+" preceding it to display the last three available Reports of that Type.
3. Highlight the desired text file, double-click on it and the Report is displayed as a Notepad document where it can be saved as a text document and incorporated into other applications.
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**:  

- Click on `<Reports>` in the left pane of the **Tree View**, followed by the "+" to expand the list of available **Reports**.  
- Select the Alarm, Audit or Notes History Custom folder.

 должна быть доступна административная авторизация для выполнения отчета (Administrative Authorization) .
3. Right-click, select Run Report and 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.

4. Indicate whether the Report will be for a Predefined Time Interval or over a Selected Time
Range by clicking on 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.

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

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

6. 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.

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

8. Highlight the desired Device(s) and/or channel(s) and press 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. Uncheck the Include System Up/Down Notes in Report field if you do not want this information in a Custom Notes History.
9. With the desired output criteria specified, click OK and the Custom History report is Run.
10. Open the appropriate Custom History folder, select the completed Report and press Retrieve 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.

![Custom Search String Dialog Box]

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.
System Administration

System Properties

System Administration

System Administration is an advanced Foreseer function which dictates various aspects of program operation. It includes the ability to:

- **Administrative Authorization** to access System Administration.
- Login, Logoff, and Change the Server Password
- Change Passwords
- Start and End Database Sessions
- Start and End Server Configuration Sessions
• **Backup** and **Check** Databases  
• **Backup** the Server Configuration  
• **Device Installation**  
• Modify **Meters** (analog) or **Status** (digital) **Channel Properties**  
• **Add** or **Delete** a Device or Channel  
• **Add User-Defined Channels**  
• Configure **Message Management**  
• Modify **Server Properties**

### File Management

Foreseer has made it easy to update program software modules as they are released. You can upload Device driver files. When issued, these files are installed in the Update VI folder. You can also create VI files.

#### To update driver files:

1. Choose the Start Server Configuration command in the **Configuration menu**. The Server Configuration Mode System Channel turns yellow and "********SERVER CONFIGURATION MODE********" is displayed in the Windows title bar to confirm operational status.

2. To update Device driver files, select the desired Device, and choose the **Disable** command from either the **Configuration menu** or the right-click menu.

3. Right-click and choose **Unload Driver** to automatically remove the outdated file.

4. Right-click again and specify **Load Driver**. The file is retrieved from the **Update VI** folder and installed automatically.

5. With the Device still selected, choose **Enable** from the **Configuration menu** or right-click menu.

6. With all file updates completed, choose **End Server Configuration** in the **Configuration menu** to restore normal Server operation.

### Administrative Administration

Password protection ensures that only authorized personnel are allowed to alter the Foreseer Server configuration or halt its data gathering and system monitoring operations. When enabled, a security **password** must be entered before most Server functions can be accessed. The first attempt to alter protected Server settings requires the **Administrative Password**. The **password** is entered in the **Administrative Password** dialog box; asterisks are displayed to maintain system security. The accepted entry automatically becomes part of the **System Log** and is available for review in that **Foreseer Report**. Once entered, the user has access privilege to all protected Server functions and does not have to enter the **password** again during the current session.
The Administrative and Client Connection Passwords may be changed, or assigned at a later time if one was not specified during initial Server configuration. The Change Passwords dialog box permits these Foreseer Server authorizations to be altered. Changing a Password does require entry of the Old password before you are allowed access the New password field.

To change the Server's current Administrative password:

1. Select Change Passwords... under the Administration menu and the Change Server Password dialog box is displayed.

2. Click on the Change Administrative Password or the Change Client Connection Password button to display the appropriate dialog box.

3. Enter the Old Password; asterisks are displayed to maintain system security. If no Password
was previously assigned, simply **Tab** to the **New Password** field.

4. Enter the desired **New Password**.

   **Password**s are case-sensitive; therefore "USER," "User" and "user" are all recognized as different **Passwords**.

5. Type the same character string in the **Verify New Password** field to validate the **New Password**.

6. Click **OK** to save the **New Password**.

**Client Connection Password**

A password is used to prevent an unauthorized Foreseer Client from accessing the Server and modifying its configuration, such as changing channel properties. This **Client Connection Password** must agree with the **Server Password** entered on the Client or they will not be able to establish communications. The **Connection Password** may be changed by a **User** with **Administrative Authorization** privileges.

To change the Server's **Client Connection Password**:

1. Select **Change Passwords...** in the **Administration menu** to access the **Change Server Passwords** dialog box.

2. Click on the **Change Client Connection Password** button to display that dialog box.

3. Enter the **New Password**, then again in the **Confirm** field in order to verify the change. Observe the same naming conventions as those used for other Foreseer passwords, such as case sensitivity. Foreseer is shipped with "special" as the default **Client Connection Password**. This default allows **Users** with older versions of the Foreseer Client software that do not support this security feature to have access to the Server.

4. Click **OK** to implement the **New Password**. Be aware that all subscribing Foreseer Clients must know and enter the **New Password** locally or they no longer will be able to access the Server.
Do not specify a Client Connection Password on a network hosting Clients running a prior version of Foreseer, or they will not be able to communicate with the Foreseer Server.

LDAP Properties

LDAP Setup

To enable LDAP authentication to Foreseer, you will need to:

- Select Use LDAP as the Primary Security Provider
- Select whether your LDAP server uses Kerberos or Plaintext to authenticate.
- Choose if your LDAP server uses user principle name for user accounts.

You must also specify the credentials for the account that is used to access the LDAP server, including the domain, user name, and user password.
Directory Search

You must set the base distinguished name (dn) that Foreseer will use to run queries on the directory server. The subtree search starts from this distinguished name. You must also set the query depth (Search Scope).

The filter that preloaded in the Search Filter was designed to find user objects in most situations. However, you can enter your own string tailored to your system. The example shown in the following figure has such a string.

The final field specifies the attribute that will return all groups to which a user belongs. If you use a different attribute you need to replace the default string.
Binding and Authorization

This tab associates groups to which a user belongs to Foreseer groups, granting that user rights within Foreseer. Essentially, you specify the attribute that returns the distinguished name in the user DN Attribute field and then map objects that define user groups in LDAP in the appropriate Foreseer group field. Typically, you will be matching on common name (CN) objects, as is shown in the example. If you wish to grant membership in a Foreseer group to multiple LDAP user groups, separate these object definitions with a comma. For more about Foreseer groups, see the *Foreseer Server Guide*. 
Shortcuts and Branch Access

Foreseer has two "superuser" groups: PXSauthADMIN and PXSauthROOT. You can also map these to LDAP user groups. For more about Foreseer user groups, see the Foreseer Server Guide.
WebViews

HTTP WebViews Server Properties

HTTP WebViews Server Properties

The **HTTP WebViews Server Properties** dialog box is used to configure the Foreseer Server for non-secure Web Browser access, thereby allowing Device status and data to be observed as well as furnishing limited Foreseer Report and Alarm Management functions. Simply click on the appropriate tab for the desired settings:

**General** - Allows you to Enable the HTTP (non-secure) WebViews Server, specify the Port to Listen to for HTTP connection and define the Maximum Number of Connections the Browser is permitted at one time.
Authentication - Provides a way to test the privilege (Windows user group) memberships for any Windows Account.

HTTP WebViews Server Properties - General

The **HTTP WebViews Server Properties** dialog box is used to configure the Foreseer Server for non-secure Web Browser access.

**General Properties** Enable HTTP Server operation, specify the **Maximum Number of Connections** the Browser is permitted at one time and define the **Refresh Interval**. Clicking in a field below displays its function: Clicking other tabs presents those **HTTP Server Properties**.

![HTTP WebViews Server Properties](image)

To view **General HTTP Server Properties**:

1. Select **WebViews Server** > **HTTP Server**... in the **Administration menu** and the **HTTP WebViews Server Properties** dialog box is displayed.
2. Click on the **General** tab to display those **HTTP Server Properties**.
3. Check the appropriate **Enable the HTTP (non-secure) WebViews Server** to activate this Foreseer function.
You will have to restart the Server application to enable (or disable) this function.

4. If necessary, alter the **Port to listen on**. The default value should be adequate in most cases. If you change the port, you must also change the port number in the `WebviewsFileMonitor.exe.config` file in the `C:\Program Files\Eaton Corporation\Eaton WebViews File Monitor` folder (this is the default location).

5. With the desired settings displayed, press **OK** to close this dialog box or click on the other tabs to review those **HTTP WebViews Server Properties**.

**HTTP WebViews Server Properties - Authentication**

This tab provides a way to test the privilege (Windows user group) memberships for any Windows Account.

Click the **Account Test** button and enter the account information to test privileges.

**HTTPS WebViews Server Properties**
HTTPS WebViews Server Properties

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for secure Web Browser access, thereby allowing Device status and data to be observed as well as furnishing limited Foreseer Report and Alarm Management functions. Simply click on the appropriate tab for the desired settings:

**General** - Allows you to Enable the HTTP (secure) WebViews Server, specify the Port to Listen to for HTTPS connection and define the Maximum Number of Connections the Browser is permitted at one time.

**Authentication** - Provides a way to test the privilege (Windows user group) memberships for any Windows Account.

**Server Certificate** - Allows a secure connection to be established between the Foreseer Client and the WebViews Server.

### HTTPS WebViews Server Properties - General

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseer Server for non-secure Web Browser access. **General Properties** Enable HTTPS Server operation, specify the Maximum Number of Connections the Browser is permitted at one time and define the Refresh Interval. Clicking in a field below displays its function: Clicking other tabs presents those HTTPS Server Properties.
Foreseer HTTPS WevViews Server Properties settings are easily established to permit Web Browser access.

To view **General HTTPS Server Properties**:

1. Select **WebViews Server> HTTPS Server...** in the Administration menu and the **HTTPS WebViews Server Properties** dialog box is displayed.
2. Click on the **General** tab to display those **HTTPS WebViews Server Properties**.
3. Check the appropriate **Enable the HTTPS (secure) WebViews Server** to activate this Foreseer function.

![Properties: HTTPS (Secure) WebViews Server](image)

- You will have to restart the Server application to enable (or disable) this function.

4. If necessary, alter the **Port to listen on**. The default value should be adequate for these settings in most cases. If you change the port, you must also change the port number in the `WebviewsFileMonitor.exe.config` file in the `C:\Program Files\Eaton Corporation\Eaton WebViews File Monitor` folder (this is the default location).
5. With the desired settings displayed, press **OK** to close this dialog box or click on the other tabs to review those **HTTPS WebViews Server Properties**.
HTTPS WebViews Server Properties - Authentication

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseeer Server for Web Browser access. **Authentication Properties** furnishes a level of security by requiring **Passwords** to view HTTPS Server information as well as request **Reports** and **Acknowledge** alarms. Clicking in a field below displays its function: Clicking other tabs presents those **HTTP Server Properties**.

![Properties: HTTPS (Secure) WebViews Server](image)

Click the **Account Test** button and enter the account information to test privileges.

HTTP WebViews Server Properties - Server Certificate

The **HTTPS WebViews Server Properties** dialog box is used to configure the Foreseeer Server for Web Browser access. **Server Certificate Properties** ensure only authorized Users can access the Server through a Web Browser. Clicking in a field below displays its function: Clicking other tabs presents those **HTTPS Server Properties**.
Foreseer HTTPS WebViews Server Properties settings are easily established to permit Web Browser access. In this example, the necessary security files are generated through the utility supplied with Foreseer, openssl.exe.

To set HTTPS WebViews Server Certificate Properties:

1. In Windows Explorer, locate the file in the Foreseer Server folder and double-click on it. The DOS screen displays the prompt:

   OpenSSL>

2. To generate a Private Key Password, type and enter:

   genrsa -des3 -out server.key 1024

3. You are prompted for a pass phrase that will be used as the Private Key Password. It is recommended your entry be at least eight characters and include numbers and letters.

   Record the Password and store it in a secure location. You will not be able to use your Private Key or Server Certificate without it and, once entered, it cannot be recovered.
4. To generate a **Certificate Signing Request** at the **OpenSSL>** prompt, type and enter:

   `req -new -key server.key -out server.csr`

5. Enter your **Private Key Password** once again at the **pass phrase** prompt. You will be requested to enter information which will become part of your **Server Certificate** identification. This information will be verified by the Certificate Authority.

6. Enter your **Country Name** as a 2-letter code.

7. Enter your complete **State** or **Province Name**. Do not use abbreviations.

8. Enter your **Locality Name**, typically the city in which your company resides.

9. Enter your **Organization Name**. This entry must be your official company name as it appears on the Articles of Incorporation.

10. Optionally enter your **Organizational Unit Name** to identify your department within your company.

11. Enter your **Common Name**. This entry is extremely important. It is the URL for the HTTPS Server that is entered in the Web Browser and it must be correct or Foreseer Users will be warned that they cannot access the HTTPS Server. This entry can be an IP Address.

12. Enter the **Email Address** of the System Administrator.

13. Optionally enter a **Challenge Password** and the screen returns to the **OpenSSL>** prompt.

14. If desired, you can generate a temporary (30-day) **Self-Signed Certificate** by entering the following:

   `req -x509 -key server.key -in server.csr -out server.crt`

15. Enter your **Private Key Password** as requested and the Self-Signed Certificate is created.

16. Type **quit** to exit the Open SSL utility.

17. Locate the **server.key** and **server.crt** files in the **Server** folder and copy the **server.key** file into the Server **certs** folder. A **server.csr** which is also generated should be submitted to Verisign with your certification application.

18. In the Foreseer Server application, select **HTTPS Server...** in the **Administration menu** to display its **General Properties**.

19. Check the **Enable the HTTPS (secure) Server** setting to activate this function.

20. Change the **Port to listen on**, the **Maximum Number of Connections** and the **Refresh Interval**, if required.

21. Change the **Authentication** and **Connection Keep-Alive** settings if necessary. The default settings should be adequate in most cases.

22. Click on the **Server Certificate** tab.

23. Enter your encrypted **Private Key Password** (pass phrase), then enter the **Password** a second time to **Verify** it.

24. Click **OK** then reboot the Server to enable the new HTTPS settings.

Any Client wishing to view the HTTPS WebViews Server will have to enter the correct **Private Key Password** or access is denied. A secure connection is indicated by padlock in the Browser status bar.

**Server Service**
Server Service

The Foreseer Server must run as a Service within the Windows operating system under the local system (User Name and Password) account. In rare installation instances, the Server initially may have to be defined as a Service, or it may be desirable to uninstall it as a Service for other reasons. The Server Service Setup dialog box allows installation and removal of the Server as a service. Simply locate the ServiceSetup.exe file in the Foreseer Server program folder and double-click on it to display that dialog box. Select Install or Uninstall and click OK to execute the desired function.

Server Properties

The Server Properties dialog box identifies important Foreseer Server settings and allows a number of administrative functions to be performed. Simply click on the appropriate tab for the desired settings:

- **Administrative Authorization** is required to access Server Properties.

  - **General** - Identifies the Server and configures Server startup.
  - **Remote** - Allows Server restart and software upgrade operations to be performed remotely.
  - **Database** - Determines historic database settings.
  - **Redundant** - Identifies the Server as a backup to endure continued site monitoring in the event the principle Server fails.
Security and User Groups

WebViews allows a user to view installed devices on the Foreseer Server and the system status using a standard web browser (see the Release Notes for supported versions). A user's visual access level and rights can be closely controlled through WebViews authentication and authorization. Viewing access can be granted to the entire system or to the granularity of viewing a single page. Control of the system can be broad-based or locked down entirely.

Authorization Levels

The authorization level granted to a user will depend on the authorization options that are in effect for the HTTP and HTTPS servers and the credentials the user presents to the server. Under no circumstances will the WebViews HTTP(S) server allow access to any file or folder above the root of the WebViews folder.

Authentication requires that a user provides both a Username and Password (their credentials). The user's credentials are passed to the Windows default security provider for validation. The credentials must represent a valid Windows user account and depending on the Security Policies at your site, the account may need the Log on locally permission on the computer where the server is running. After the credentials have been validated, the server then checks to see what groups the user is a member of.

The WebViews server currently provides three classes of authorization: ADMIN, ROOT and TOP (or Branch). The ADMIN authorization class grants the user all rights. ROOT authorization grants an account the right to view the Tree and View Alarms. TOP (Branch) authorization grants a user the ability to view a specific branch of the tree.

A TOP level folder is defined as a folder that is a direct child of /WebViews (the root folder). When an account has TOP authorization, they have access to the TOP (branch) folder and all channels and folders under (or descendants of) the branch folder. If an account has membership in both the TOP group and the ROOT group, the user will be granted the higher-level ROOT authorization (or rights).

ADMIN authorization is requested by using the root path of /WebAdmin/ instead of /WebViews/. An account that is a member of the ADMIN group (PXSAUTHAPPADMIN) will be granted all rights.

When a user has been authorized at the Branch level, they may not view or access any data or pages outside of the branch they have been authorized for. The WebViews server will cache the last credentials that were presented and the rights associated with the credentials. As long as the Internet Explorer session persists, WebViews will check the credentials presented by the browser with the current request against the cached credentials. If they match, the WebViews server can skip the time-consuming step of further Authentication and Authorization.

When a new session is started or the cached rights are not sufficient for the current request, WebViews will reply to the request with an HTTP 401 status code. A 401 status is known as an Authorization Challenge. When the browser receives a challenge, it will present the user with a Login dialog. The user has three tries (the three-strike rule) to provide credentials that the server will accept. If the user cannot provide valid credentials, the browser typically displays a blank page. The WebViews server uses HTTP Basic Authentication. The browser encodes the credentials supplied by a user and sends it to
the WebViews server in the HTTP Authorization header field.

**Caution:** As the credentials are only encoded (not encrypted), they are subject to being intercepted and decoded. To keep credentials secure it is highly recommended that the site uses the HTTPS (secure) server when authorization is enabled. The HTTPS server uses 256-bit encryption which guarantees that even if the information that is sent is intercepted, it cannot be decoded.

A WebViews folder tree can be graphically represented as such:

<table>
<thead>
<tr>
<th>Top Level</th>
<th>Subfolder Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBVIEWS</td>
<td>/webviews</td>
</tr>
<tr>
<td>BASEMENT</td>
<td>/webviews/basement</td>
</tr>
<tr>
<td></td>
<td>UPS 1 /webviews/basement/ups 1</td>
</tr>
<tr>
<td></td>
<td>ATS 1 /webviews/basement/ats 1</td>
</tr>
<tr>
<td>FLOOR 1</td>
<td>webviews/floor 1</td>
</tr>
<tr>
<td></td>
<td>GEN A webviews/floor 1/gen a</td>
</tr>
<tr>
<td></td>
<td>GEN B webviews/floor 1/gen b</td>
</tr>
<tr>
<td>FLOOR 2</td>
<td>webviews/floor 2</td>
</tr>
<tr>
<td></td>
<td>AC 1 webviews/floor 2/ac 1</td>
</tr>
<tr>
<td></td>
<td>AC 2 webviews/floor 2/ac 2</td>
</tr>
<tr>
<td></td>
<td>AC North webviews/floor 2/ac north</td>
</tr>
</tbody>
</table>

WEBVIEWS is at the **Root** level. BASEMENT, FLOOR 1, and FLOOR 2 are the **Top** level. The devices would be at the **Branch** level.

A **Top** level folder is a direct child of the root folder (WebViews in the example tree). **Top** folders define a branch which includes the **Top** folder and all folders that are descendants of the **Top** folder. Basement, Floor 1, and Floor 2 are all **Top** folders. The Floor 1 branch includes the following folders: /WebViews/Floor 1, /WebViews/Floor 1/Gen A and /WebViews/Floor 1/Gen B.

**Accounts**

Accounts are managed by Windows and may be Local Users or Domain accounts. To allow a specific right, create a Local Group (local to the computer where the Foreseer Server is installed and running) from the following Foreseer Group Names:

<table>
<thead>
<tr>
<th>User/Security Group</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>PXSauthNONE</td>
<td>- Enables all authentication requirements, including access to the Web Configuration utility.</td>
</tr>
<tr>
<td></td>
<td>- A user login will not be required to view pages, edit pages, acknowledge/rearm alarms, change channel properties, etc.</td>
</tr>
<tr>
<td></td>
<td>- Grants administrator permission to everyone.</td>
</tr>
</tbody>
</table>

This group should be used with extreme care. It grants full access to
everyone that can connect to Foreseer.

<table>
<thead>
<tr>
<th>Role</th>
<th>Rights</th>
</tr>
</thead>
</table>
| PXSauthADMIN          | - All rights, except access to Web Configuration utility  
                        - Members have all rights in WebViews  
                        - Members can edit (WebAdmin URL) if licensed |
| PXSauthAPPADMIN       | - Members can access the Web Configuration Utility and gain all rights (the same as PXSauthADMIN) |
| PXSauthROOT           | - View all branches with view alarm permission  
                        - Members can view all WebViews pages (full access to the WebViews tree)  
                        - Members can view Alarms, Reports, and Channel Properties |
| PXSrightViewTree      | - View all branches of the tree                                                                 |
| PXSrightViewAlarms    | - Members can view the Alarm Management page but cannot acknowledge/rearm alarms  
                        - Members can view all WebViews pages  
                        - Grants permission to view active alarms |
| PXSrightViewProps     | - Grants permission to view a channel’s properties  
                        - Members can view all WebViews pages |
| PXSrightAlarmActs     | - Grants permission for alarm management (ack/rearm)  
                        - Members can acknowledge/rearm alarms from Alarm Management  
                        - Members can view all WebViews pages (full access to the WebViews tree) |
| PXSrightControl       | - Grants permission to access a channel’s control ability  
                        - Members can access dialogs to change Setpoint, Tri-State, and Two-State Control channels and activate Switch LED or Switch Rocker ActiveX Controls |
| PXSrightEditProps     | - Grants permission to edit a channel’s properties  
                        - Members can view Channel Properties  
                        - Members can view all WebViews pages |
| PXSrightAppAdmin      | - Members can access the Web Configuration Utility and gain all rights (the same as PXSauthADMIN) |

Some of the rights also imply others as follows:

- PXSrightViewAlarms ....................PXSrightViewTree  
- PXSrightAlarmActs ........................PXSrightViewAlarms, PXSrightViewTree  
- PXSrightEditProps .....................PXSrightViewProps, PXSrightViewTree  
- PXSrightViewProps .....................PXSrightViewTree

Note: You can test each account if you wish through the Authentication tab on either the HTTP or HTTPS server dialog box. Click the Account Test button and then enter the Username and Password for a Windows User. If you wish, you can also specify a branch of the WebViews tree to
User Group Privilege Details

<table>
<thead>
<tr>
<th>Foreseer User group</th>
<th>Foreseer WebConfig</th>
<th>WebAdmin</th>
<th>WebViews</th>
<th>View - Alarm management</th>
<th>Edit(Ack/ rearm) Alarm management</th>
<th>View-Channel Properties</th>
<th>Edit Channel’s Properties</th>
<th>View Active Alarms</th>
<th>Channel’s Control ability</th>
<th>View all Branches of WebViews pages</th>
<th>Edit all Branches of WebViews pages</th>
<th>View reports</th>
<th>Data Analysis</th>
<th>Data Analysis Add Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>PXSauthADMIN</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSauthROOT</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSrightViewTree</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSrightViewAlarms</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSrightViewProps</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSrightAlarmActs</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSrightControl</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes5</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PXSrightEditProps</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSauthAPPADMIN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PXSbranch+folder</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Requires another right to be able to access reports. To view reports, a user must have the combination of PXS-rightViewTree + PXSrightViewAlarms + PXSrightViewProps.
2. Requires another right to be able to access reports. To view reports, a user must have the combination of PXS-rightViewAlarms + PXSrightViewProps.
3. Requires another right to be able to access reports. To view reports, a user must have the combination of PXS-rightViewProps + PXSrightViewAlarms.
4. Requires another right to be able to access reports. To view reports, a user must have the combination of PXS-rightAlarmActs + PXSrightViewProps.
5. Requires another right to be able to get to the control. To have channel control ability, a user must have the combination of PXSauthROOT + PXSrightControl.
6. Requires another right to be able to access reports. To view reports, a user must have the combination of PXS-rightEditProps + PXSrightViewAlarms.

Updating User Groups

Foreseer queries the list of users and groups at startup, therefore if you make a change to either the list of users or to groups this won’t be read until the next time the WebViews Server starts. To force a query of the list of users and groups, you can do one of two things:

- Restart the Foreseer Server itself.
Redundant and Remote Servers

Primary Server Setup

When you synchronize a Redundant Server from a Primary Server, a partial configuration backup is transferred to the redundant server. This backup contains all device configuration parameters and includes WebViews as well. It does not change items such as the Database connection settings. Note that the Redundant Server will perform a restart in order to restore and implement the updates from the primary server. Also note that both server names must be identical.

On the Primary Server, perform the following steps with Foreseer running as an application:

1. On the Primary Server, select Administration > Server Properties.

2. Navigate to the ‘Redundant System’ tab and select the ‘Primary Redundant’ setting. Fill in the computer name or IP address of the Primary Redundant system. Click OK.
Do not use 127.0.0.1 or any other form of loopback addressing. This is not supported!

Setting up a Redundant Server

Perform the following steps on the server that will be designated Redundant.
1. Create a new Foreseer server by launching the Foreseer application. Select Install New Server. Click Next to Continue.
2. Enter the name of the server. This must be identical to the name on the primary server. Click Next to continue.

3. Enter the database information. The Redundant Server requires its own SQL Server Instance. The Primary and Redundant cannot use the same instance of SQL Server. Click Next.
4. Do not enter a password. If an admin password is used on the Primary Server, it will be set automatically once the redundant relationship has been completed. Click Next.
5. Click Finish to complete the Server Configuration wizard. This will create the new server configuration and Foresee will finish launching as an application.

6. When the new configuration starts, access Administration>Server Properties.
7. On the Redundant System tab, select the Secondary Redundant radio button. Click OK.

8. If the site is using Message Manager, select Message Management->Configure Required Connections...

10. Enter the Static IP Address or Resolvable Computer Name of the Primary Server. Click OK.
11. Check the box next to the address to activate the setting for the Primary IP Address. You can also change the delay (1 minute is usually adequate). Click OK to save the changes. You may now shut-down Foreseer as an application and start it as a service.

Adding the Redundant Server as a Remote on the Primary Server

The following must be carried out in the Primary Server using WebConfig. Ensure that the proper Windows groups are created and the required users are added.

1. Right-click the name of the server. Select Start Server Config Mode.
2. Right-click the name of the server. Select Add Remote...

3. On the Pop Up window (Make sure pop-ups are allowed in Internet Explorer) Fill in the following information:
   1. Name – Must be named Redundant
   3. Updates – leave at 2 seconds.
   4. Connection Password – the default connection password is special (case-sensitive, all lower-case letters).
   5. Verify Password – re-enter default connection password from step d.
4. Click OK. The remote should be added to the server tree.

Note: If the process fails to add the Redundant server check the Windows Firewall settings to make sure that Port 2100, Port 2101, and HTTPS is open for traffic in both directions. You may need to temporarily turn Windows Firewall off to test. If the Redundant connects when the Firewall is off consult with the end customer for Firewall exceptions to be made.

5. End server configuration. In the right-side workspace of WebConfig, you should see that the Redundant is connected, but lists its Needs Update field as Needs Sync.

<table>
<thead>
<tr>
<th>State</th>
<th>Server</th>
<th>Needs Update</th>
<th>Version</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Local</td>
<td></td>
<td>6.2.60</td>
<td>Foresee</td>
</tr>
<tr>
<td>Redundant</td>
<td>Needs Sync</td>
<td></td>
<td>6.2.60</td>
<td>Foresee</td>
</tr>
</tbody>
</table>

Synchronizing the Redundant Server

- Not all changes on the Primary server will set the ‘Needs Sync’ flag under the ‘Needs Update’ header, typically channel properties will not but you can always perform a synchronization to ensure the systems have identical settings.

1. Right-click on the Redundant Server and select ‘Synchronize Redundant Server’.
2. The following message will display. Click OK to continue.

3. At this time a partial configuration backup is generated from the Primary server, transferred to the Redundant server and a restart of the Redundant server is initiated. The WebConfig tree will display a SYNC IN PROGRESS message. While this process is occurring, the WebConfig webpages may appear unresponsive. This is completely normal.

**** SYNC IN PROGRESS - READ ONLY ****

4. During the startup of the Redundant server an automatic database fix and check will occur. This is performed to implement any changes to devices or channels that may have occurred on the Primary Server.

Both Servers should now be fully synchronized.

Add Remote Server

A local Foreseer Server can serve as host to a remote Foreseer Server. Once defined, the Remote
Server appears on the Tree View as another computer and can be modified locally. A Password provision adds another layer of security by restricting access to authorized personnel.

To add and connect to a Remote Server, you will need to use the web configuration utility.

You can access the Web Configuration Utility at the following URL: https://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.

If you must designate a specific port for communicating with the WebViews server, the syntax of the URL will be slightly different: https://machine:port_number/Support/WebConfig.htm

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

**Message Management**

**Message Management** establishes an automatic escalation procedure in response to user-specified alarms. When an alarm is detected, Foreseer proceeds to call each person in the appropriate Notification List in the order shown until the alert is acknowledged. The Status portion of the Message Management window reports the notification is being performed and its ongoing progress. If everyone on the List is called without receiving an acknowledgment, Foreseer can repeat the entire procedure until the alarm is acknowledged, thereby ensuring a response. There are also provisions for suspending or stopping individual calls (as well as the entire notification procedure once it has been initiated) using the Messages menu or the integral Messages tool-bar.

- You can download the contents of the Data Analysis window as a .csv file by clicking Save Data.

Messaging parameters initially are Setup in the MsgMan utility (launched through Start All Programs > Foresee > MsgMan) by defining Modems and Services, then Subscribers are entered and Notification List compiled. Finally, Channel Message Settings are assigned to the appropriate inputs within the Foresee Server interface (Message Management command in the Administration menu). Once these parameters are established, Client Connections are specified to complete the configuration of this messaging feature.

To Configure Message Management, it must first be set up as a service.

**Message Management Properties**

Foresee includes the ability to notify personnel when an alarm condition is detected using a variety of methods. The Message Management Properties dialog box defines system Subscribers and the method in which they are alerted. Message Management functionality is set up by furnishing the necessary information in the following order:

- Administrative Authorization is required to access Message Management Properties.
The following settings are accessed through the Windows Control Panel by selecting Message Management. You must first install the Message Manager as a service to access these.

**Modems** - Specify the Modem(s) used to send the alarm notification to be configured.

**Services** - Identify the types and providers of the notification service used by the Foreseer Server Message Management feature, such as alpha/numeric paging, email, a printer or output to one of the Server’s COM ports.

**Subscribers** - Identify who is eligible to be contacted in the event of a specific alarm condition and provides the basis for the Notification List used in Foreseer Server Message Management operations.

**Notification List** - Determine the sequence and timing of who is alerted by the Foreseer Server Message Management feature, and is comprised of the specific people to contact under certain alarm conditions.

The following setting accessed through Foreseer Server itself.

**Channel Message Settings** - Allow independent Notification Lists to be assigned to each channel's alarm state—Critical, Cautionary, Acknowledged or Normal—to alert concerned personnel to the change.

**Message Management Properties - Channel Message Settings**

The Message Management dialog box specifies the conditions under which personnel are notified when an alarm condition is reported. Channel Message Settings allow independent Notification Lists to be assigned to each channel's alarm state—Critical, Cautionary, Acknowledged, Normal or, (optionally) SNMP - to alert concerned personnel to the change.

If upgrading a down level version of Foreseer, any channel with a previously assigned Notification Lists will use it for reporting Critical and Cautionary alarm states. Acknowledged and Normal state conditions are not assigned Channel Messages by default; they must be entered manually by the User.
Foreseer **Message Management Properties** settings are easily established to meet your alarm notification needs. You may wish to establish different **Channel Message Settings** for various conditions.

To specify **Channel Message Settings**:

- **Administrative Authorization** is required to access **Message Management Properties**.

1. Select **Setup** in the **Administration menu / Message Management** sub-menu to display the **Message Management** dialog box.
2. Select the desired channel to highlight it, then click the **Edit** button to display the **Channel Message Settings** dialog box.
3. Enter the necessary information under each tab—**Critical**, **Caution**, **Acknowledge**, **Normal** and (SNMP)—as appropriate.
4. Press **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** window.
5. With the desired **Channel Message Settings** specified, click **OK** to accept the current entries and return to the previous Foreseer window or click on the other tabs to review those **Message Management Properties**.
6. Click **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** window.
You can modify **Channel Message Settings** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Channel** and click **Edit** to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen **Channel**.

**Message Management Properties - Modems**

The **Message Management** configuration utility (accessed through the Start > Foreseer > MsgMan) specifies the conditions under which personnel are notified when an alarm condition is reported. **Modems** allows those hardware devices used by the Foreseer Server **Message Management** feature to be identified and configured. Clicking in a field below displays its function: Clicking other tabs presents those **Message Management Properties**.

![Message Manager Configuration](image)

To configure a new **Modem** for use:
Administrative Authorization is required to access Message Management Properties.

1. Select Message Management in the Windows Control Panel (Message Management must first be set up as a service).
2. Click on the Modems tab. Any modems already configured within Windows also are listed (and available for selection).
3. Click New... and the Modem Properties dialog box is displayed.

![Modem Properties dialog box]

4. Enter a unique Name to identify the new Modem.
5. Review the default Connection Settings for the Modem and change them if necessary. These Settings must be correct or Foreseer cannot forward alarm information to your Modem.

    ![Modem Properties dialog box]

6. Verify the Port setting and change it to the communications Port to which the Foreseer Server modem is attached, if necessary.

If using a Windows modem for Alpha Paging functions, it must be configured in the Control Panel to 2400 Baud Rate, 7 Data Bits, Even Parity and 1 Stop Bit or communications may not be established.
7. Similarly verify the Baud rate for the device, altering it as required. The Baud rate is available from the device’s manual or the paging company. Also review the Data Bit, Parity and Stop Bit settings to ensure that they are correct for the named modem. most alpha paging companies require a Baud Rate of 2400 with 7 Data Bits, Even Parity and 1 Stop Bit.

8. Enter any special Modem initialization Strings. Typically this setting remains blank. If the modem does not respond with an “OK,” refer to its operation manual to determine a Modem Init string (with a maximum of 80 characters) that will work properly.

9. Also enter any required Modem Dial String characters. This setting should only be specified if the Modem Dial String is not “ATDT.”

10. With the proper Modem parameters displayed, click on the Services tab to establish those **Message Management Properties**. You can now use that modem in the appropriate new services that you add.

You can similarly modify **Modem Properties** in response to changing personnel assignments and contact conditions. Simply highlight the desired Modem and click Properties... to access its dialog box. Then use the procedure above to alter any of the attributes associated with the Modem. A Foreseer-configured Modem is removed from the list simply by highlighting it and clicking Remove: a Windows-installed Modem can only be removed within that Setting in the operating system’s Control Panel.

**Message Management Properties - Notifications List**

The **Message Management** dialog box specifies the conditions under which personnel are notified when an alarm condition is reported. **Notification Lists** determine the sequence and timing of who is alerted by the Server Message Management feature and are comprised of the specific people to contact under certain alarm conditions. These Lists are compiled using Foreseer Subscribers entries and can be used to establish procedures that alert remote personnel to alarms via a a variety of output Services. A separate Notification List can be assigned to each of four independent alarm states—Critical, Cautionary, Acknowledged or Normal—for each channel. Clicking in a field below displays its function: Clicking other tabs presents those **Message Management Properties**.
Foreseer Message Management Properties settings are easily established to meet your alarm notification needs. You may wish to establish multiple Notification Lists for various conditions.

To create a Notification List:

- **Administrative Authorization** is required to access Message Management Properties.

1. Select Message Management in the Windows Control Panel (Message Management must first be set up as a service).
2. Click on the Notification Lists tab to access that dialog box.
3. Click on New... to display the Notification List Properties dialog box.
4. Enter a **Name** to identify the **Notification List**, then click **Add**... to display a list of configured **Subscribers**.

5. Select all of the **Subscribers** who are to be included in the named **List** and, with the desired personnel highlighted, press **OK** to return to the **Notification List Properties** dialog box. A person's place in the contact queue can be changed by highlighting their **Subscriber Name** and
then moving them Up or Down one position at a time. You can delete individual entries simply by highlighting them and clicking Remove.

- The person must exist as a Subscriber to be available for inclusion in a Notification List.

6. Click on the Advanced tab to display those Notification List Properties.

7. Enter the desired Frequency of Calls to specify the number of times the Notification List will be called as well as how many times each individual on the List will be called until a response is received.

8. Specify the Delay to determine how long after an alarm is reported before messaging is initiated on the Notification List. Also designate whether this Delay is observed the first time the List is called.

9. Enable the desired Call Properties to indicate whether to call the entire Notification List regardless of whether a response is received, allow higher priority Lists to take call precedence, and if listed personnel using the same Service should be notified with the same call.

10. Press OK to return to the Notification List within the Message Management window.

11. With the desired Notification List settings specified, click on the Channel Message Settings to specify those Message Management Properties.
You can similarly modify Notification Lists in response to changing personnel assignments and contact conditions. Simply highlight the desired List and click Properties.. to access its dialog box. Then use the procedure above to alter any of the attributes associated with the Notification List such as its Subscriber Names, Frequency of Calls or the Delays.

Message Management Properties - Services

The Message Management dialog box specifies the conditions under which personnel are notified when an alarm condition is reported. Services allows the types and providers of the notification service used by the Foreseer Server Message Management feature to be identified and configured. Services include alpha/numeric paging, Windows Messaging and SMTP mail, a printer or output to one of the computer's COM ports and command line operation. Clicking in a field below displays its function: Clicking other tabs presents those Message Management Properties.

Foreseer Message Management Properties settings are easily modified to meet your alarm notification needs.

To establish a Message Service:
1. Select **All Programs > Foreseeer > MsgMan** in the Windows Start Menu (Message Management must first be set up as a service).
2. Click on the **Services** tab to see a display of existing communications methods.
3. Click **New**... and a pop-up menu gives you the choice of selecting an Alpha Page, Numeric Page, **Printer Output to COM Port**, **SMTP Mail** or **Command Line Service**. On selection, the appropriate **Service Properties** dialog box is displayed.
4. Specify the necessary **Service Properties** based on the type of messaging system.
5. With the proper **Services** parameters displayed, click on the **Subscribers** tab to specify those **Message Management Properties**.

You can similarly modify **Services Properties** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Service** and click **Properties**... to access its dialog box. Then use the procedure above to alter any of the attributes associated with the **Service**. A **Service** is removed from the list by highlighting it and clicking **Remove**.

**Message Management Properties - Subscribers**

The **Message Management** dialog box specifies the conditions under which personnel are notified when an alarm condition is reported. **Subscribers** identifies who is contacted in the event of an alarm condition and provides the basis for the alarm **Notification Lists** used in the Server **Message Management** feature. The notification or message can be repeated at specified intervals until successful. Clicking in a field below displays its function: Clicking other tabs presents those **Message Management Properties**.
Foreseer **Message Management Properties** settings are easily established to meet your alarm notification needs. **Subscribers** lists the personnel who can be notified and determines when they are available. Multiple entries can be made to reach an individual at different locations using different notification methods. Personnel can be temporarily removed from the **Subscribers** list in the event they are **Unavailable** due to sickness, vacation or other reasons.

To enter someone as a **Subscriber**:

1. **Administrative Authorization** is required to access **Message Management Properties**.

2. Select **Message Management** in the Windows Control Panel (Message Management must first be set up as a service).
3. Click on the **Subscribers** tab to display that dialog box.
4. Click **New...** and the **Subscriber Properties** dialog box is displayed.
4. Enter a **Subscriber Name** to identify the new person and click **New...** to display their **Available Time Properties** dialog box.
5. Specify when the named Subscriber is available for paging by designating the Start and End Time which define the period that person can be notified. The corresponding display changes to report the total Availability Time. Also check the appropriate Days of the Week for which those Time entries apply. Multiple entries can be made for a Subscriber to accommodate differing Services, but the Available Times should not overlap.

6. Select the notification Service from the drop list that is displayed by clicking the associated arrow. You are required to enter additional information such as the Pager ID (Alpha) or Pager Phone Number (Numeric) that is to be called if Paging is the chosen method, or the IP Address if the Service is SMTP Mail.

7. Click OK to add the person to the Subscribers list and make him available for inclusion in Notification Lists. With the desired Available Time settings selected and the Subscriber Properties dialog box displayed, check the box preceding the appropriate Times to activate them for that person.

8. Repeat the process to add more people to the Subscribers list.

9. With the proper Subscriber parameters displayed, click on the Notification Lists tab to establish those Message Management Properties.

You can similarly modify Subscribers in response to changing personnel assignments and contact conditions. Simply highlight the desired Name in the Subscriber Properties dialog box and click Properties... to access their contact information. Then use the procedure above to alter any of the messaging attributes specific to that Subscriber such as the Time they are available or their Phone Number. Individual entries are deleted from the Subscribers list by highlighting them and clicking Remove.

Channel Message Services

Channel Message Services

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The Channel Message Settings dialog box identifies the individuals who are alerted and the information that is included in the notification message. Channel Message Settings are specified as follows:

- **Administrative Authorization** is required to access Channel Message Settings

**Default**

- **Critical** - specifies the Notification List and message sent when a Critical alarm is detected on a Foreseer channel.

- **Caution** - specifies the Notification List and message sent when a Cautionary alarm is detected on a Foreseer channel.

- **Acknowledge** - specifies the Notification List and message sent when a Foreseer channel is Acknowledged after reporting an alarm condition.
Normal - specifies the Notification List and message sent when a Foreseer channel returns to **Normal** operation after reporting an alarm condition.

SNMP - addresses the Simple Network Management Protocol Virtual Agent option, specifying the Trap Numbers and when the Foreseer Client sends alerts to a supervisory Network Management System (NMS).

**Channel Message Services - Default**

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The **Channel Message Settings** dialog box identifies the individuals who are alerted and the information that is included in the notification message. **Default Channels** are those that have been specified in a Default Notification List to alert the specified personnel if an alarm is detected on this channel. Clicking in a field below displays its function: Clicking other tabs presents those **Channel Message Settings**.
Foreseer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Default Channel Message Settings:

1. Select Message Management in the Administration menu.
2. Select a channel and click Edit to view the Channel Message Settings dialog box, or simply double-click on the desired channel.
3. Click on the Default tab to access that Channel Message property.
4. Check **Use Default Notify Lists** to enable that setting for the current channel. Enabling this setting automatically alerts the personnel specified in the **Default Notification Lists** that an alarm has been detected on this channel. Independent **Default Notification Lists** can be defined at the Channel, Device and Server level.

5. Click on the other **Channel Message Setting** tabs to specify their parameters; or, you can simply Copy these settings to other dialog tabs as appropriate.

6. Click **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** dialog box.

You can modify **Channel Message Settings** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Channel** and click **Edit** to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen **Channel**.

**Channel Message Services - Critical**

Foreseeer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The **Channel Message Settings** dialog box identifies the individuals who are alerted and the information that is included in the notification message. **Critical Channel Messages** are those associated with the transgression of a **Critical Alarm Limit** setting and typically impact normal operation of the site. Clicking in a field below displays its function: Clicking other tabs presents those **Channel Message Settings**.
Foreseeer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Critical Channel Message Settings:

- **Administrative Authorization** is required to access Channel Message Settings.

1. Select Message Management in the Administration menu.
2. Select a channel and click Edit to view the Channel Message Settings dialog box, or simply double-click on the desired channel.
3. Click on the Critical tab to display those Channel Message properties.
4. Specify the Notification List to be used to alert personnel to a **Critical** alarm condition on this channel. Also check the **Always notify regardless of Client connections** setting if this list of people should always be alerted to a **Critical** alarm on this channel.

5. Specify the message to be sent with the notification. If using a Numeric paging Service, enter the desired message in the field provided. If notifying personnel through an Alpha paging Service, specify the type of message to be sent (Standard or Custom) and whether to include the Server, Device and Channel Name in the message. A Standard message can be appended with an additional note, if desired, and can include the alarm message as well. Selecting **Edit the Custom Message** for either the Alpha paging or Command Line Service opens a dialog box allowing special response instructions to be entered.

Clicking on **Edit the Command Line** similarly displays the **Edit the Custom Message** dialog box to allow a specific message to be appended to the out call. Command Line instructions may be applied directly through that Message Management Service.

- The chosen Notification List must contain a Subscriber to the Command Line Service to activate this setting.

6. With the proper **Critical** parameters displayed, click on the other **Channel Message Setting** tabs to specify their parameters; or, you can simply **Copy these settings to other dialog tabs** as appropriate.

7. Click **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** dialog box.

You can modify **Channel Message Settings** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Channel** and click **Edit** to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen **Channel**.

**Channel Message Services - Caution**

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The **Channel Message Settings** dialog box identifies the individuals who are alerted and the information that is included in the notification message. **Caution Channel Messages** are associated with the transgression of a Cautionary Alarm Limit setting and are an alert to the potential of more serious site problems. Clicking in a field below displays its function: Clicking other tabs presents those **Channel Message Settings**.
Foreseer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Caution Channel Message Settings:

1. Select Message Management in the Administration menu.
2. Select a channel and click Edit to view the Channel Message Settings dialog box, or simply double-click on the desired channel.
3. Click on the Caution tab to display those Channel Message properties.
4. Specify the **Notification List** to be used to alert personnel to a **Cautionary** alarm condition on this channel. Also check the **Always notify regardless of Client connections** setting if this list of people should always be alerted to a **Cautionary** alarm on this channel.

5. Specify the message to be sent with the notification. If using a Numeric paging **Service**, enter the desired message in the field provided. If notifying personnel through an Alpha paging **Service**, specify the type of message to be sent (Standard or Custom) and whether to include the **Server**, **Device** and **Channel Name** in the message. A **Standard** message can be appended with an additional note, if desired, and can **Include the alarm message** as well. Selecting **Edit the Custom Message** opens a dialog box allowing special response instructions to be entered.

Clicking on **Edit the Command Line** similarly displays the **Edit the Custom Message** dialog box to allow a specific message to be appended to the out call **Command Line** instructions may be applied directly through that **Message Management** **Service**.

- The chosen **Notification List** must contain a **Subscriber** to the **Command Line Service** to activate this setting.

6. With the proper **Caution** parameters displayed, click on the other **Channel Message Setting** tabs to specify their parameters; or, you can simply **Copy these settings to other dialog tabs** as appropriate.

7. Click **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** dialog box.

You can modify **Channel Message Settings** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Channel** and click **Edit** to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen **Channel**.

**Channel Message Services - Acknowledge**

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The **Channel Message Settings** dialog box identifies the individuals who are alerted and the information that is included in the notification message. **Acknowledge Channels** are those whose active alarms have been answered by authorized personnel. Clicking in a field below displays its function: Clicking other tabs presents those **Channel Message Settings**.
Foreseer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Acknowledge Channel Message Settings:

- **Administrative Authorization** is required to access Channel Message Settings.

1. Select Message Management in the Administration menu.
2. Select a channel and click **Edit** to view the Channel Message Settings dialog box, or simply double-click on the desired channel.
3. Click on the **Acknowledge** tab to display those Channel Message properties.
4. Specify the Notification List to be used to alert personnel to an Acknowledged alarm condition on this channel. Also check the Always notify regardless of Client connections setting if this list of people should always be alerted to a Acknowledged alarm on this channel.

5. Specify the message to be sent with the notification. If using a Numeric paging Service, enter the desired message in the field provided. If notifying personnel through an Alpha paging Service, specify the type of message to be sent (Standard or Custom) and whether to include the Server, Device and Channel Name in the message. A Standard message can be appended with an additional note, if desired, and can Include the alarm message as well. Selecting Edit the Custom Message opens a dialog box allowing special response instructions to be entered.

Clicking on Edit the Command Line similarly displays the Edit the Custom Message dialog box to allow a specific message to be appended to the out call Command Line instructions may be applied directly through that Message Management Service.

☑️ The chosen Notification List must contain a Subscriber to the Command Line Service to activate this setting.

6. With the proper Acknowledge parameters displayed, click on the other Channel Message Setting tabs to specify their parameters; or, you can simply Copy these settings to other dialog tabs as appropriate.

7. Click OK to save the Channel Message Settings and return to that tab within the Message Management dialog box.

You can modify Channel Message Settings in response to changing personnel assignments and contact conditions. Simply highlight the desired Channel and click Edit to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen Channel.

Channel Message Services - Normal

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The Channel Message Settings dialog box identifies the individuals who are alerted and the information that is included in the notification message. Normal Channels are those that have returned to within their Cautionary or Critical Alarm Limits after reporting an alarm condition. Clicking in a field below displays its function: Clicking other tabs presents those Channel Message Settings.
Foreseeer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Normal Channel Message Settings:

- **Administrative Authorization** is required to access Channel Message Settings

1. Select Message Management in the Administration menu.
2. Select a channel and click **Edit** to view the Channel Message Settings dialog box, or simply double-click on the desired channel.
3. Click on the Normal tab to display those Channel Message properties.
4. Specify the **Notification List** to be used to alert personnel that this channel has returned to within its **Alarm Limits**. Also check the **Always notify regardless of Client connections** setting if this list of people should always be alerted to a **Normal** status subsequent to an alarm on this channel.

5. Specify the message to be sent with the notification. If using a Numeric paging **Service**, enter the desired message in the field provided. If notifying personnel through an Alpha paging **Service**, specify the type of message to be sent (**Standard** or **Custom**) and whether to include the **Server**, **Device** and **Channel Name** in the message. A **Standard** message can be appended with an additional note, if desired, and can **Include the alarm message** as well. Selecting **Edit the Custom Message** opens a dialog box allowing special response instructions to be entered.

Clicking on **Edit the Command Line** similarly displays the **Edit the Custom Message** dialog box to allow a specific message to be appended to the out call **Command Line** instructions may be applied directly through that Message Management **Service**.

- The chosen **Notification List** must contain a **Subscriber** to the Command Line Service to activate this setting.

6. With the proper **Normal** parameters displayed, click on the other **Channel Message Setting** tabs to specify their parameters; or, you can simply **Copy these settings to other dialog tabs** as appropriate.

7. Click **OK** to save the **Channel Message Settings** and return to that tab within the **Message Management** dialog box.

You can modify **Channel Message Settings** in response to changing personnel assignments and contact conditions. Simply highlight the desired **Channel** and click **Edit** to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen **Channel**.

**Channel Message Services - SNMP**

Foreseer includes the ability to notify particular personnel when a certain channel reports a change in alarm status. The **Channel Message Properties** dialog box identifies the personnel who are alerted and the information that is included in the notification message. **Normal Channel Messages** are those that have returned to within their **Cautionary** or **Critical Alarm Limits** after reporting an alarm condition. Clicking in a field below displays its function: Clicking other tabs presents those **Channel Message Properties**.
Foreseer Channel Message Settings are easily created to meet your alarm notification needs. You may wish to establish different Channel Message Settings for various conditions.

To specify Normal Channel Message Settings:

1. Select Message Management in the Administration Menu.
2. Select the desired channel and click Edit to view the Channel Message Properties dialog box.
3. Click on the Normal tab to display those Channel Message Properties.
4. Specify the Notification List to be used to alert personnel that this channel has returned to
within its Alarm Limits. Also check the Always notify regardless of Client connections setting if this list of people should always be alerted to a Normal status subsequent to an alarm on this channel.

5. Specify the message to be sent with the notification. If using a Numeric paging Service, enter the desired message in the field provided. If notifying personnel through an Alpha paging Service, specify the type of message to be sent (Standard or Custom) and whether to include the Server, Device and Channel Name in the message. A Standard "Channel Normal" message is appended as well. Selecting Edit the Custom Message opens a dialog box allowing special response instructions to be entered.

Clicking on Edit the Command Line similarly displays the Edit the Custom Message dialog box to allow a specific message to be appended to the outcall notification. Global Command Line instructions may be applied directly through that Message Management Service.

6. With the proper Normal parameters displayed, click on the other Channel Message Properties tabs to specify their parameters; or, you can simply Copy these settings to other dialog tabs as appropriate.

7. Click OK to save the Channel Message Settings and return to that tab within the Message Management dialog box.

You can modify Channel Message Settings in response to changing personnel assignments and contact conditions. Simply highlight the desired Channel and click Edit to access the dialog box again. Then use the procedure above to alter any of the attributes associated with the chosen Channel.

**SNMP Virtual Agent**

**SNMP**

Simple Network Management Protocol (SNMP) provides a framework for communication between various internetwork devices using the TCP/IP protocol. SNMP employs a Manager/Agent model. The Network Management System (NMS) monitors and controls one or more Agents. The Agent, in this case the Foreseer Client, has the ability to asynchronously send alerts, or traps, to specified Managers to report predefined events.

The optional Foreseer **SNMP Virtual Agent** (tm) allows an SNMP trap to be sent from the Client to a Network Management System (NMS) to furnish enterprise-wide notification of critical events like utility power failures. By adding SNMP, the NMS can monitor critical events occurring within all of the equipment supported by Foreseer. The **SNMP Virtual Agent** sends traps to a supervisory NMS when three types of alarms are detected:

- System Alarms when they occur.
• Communication Alarms when they occur, are acknowledged or cleared.
• Channel Alarms are handled on an individual basis and traps can be sent either when they occur, are acknowledged or cleared. In addition, traps may be resent for all active alarms (or for all unacknowledged alarms) within a user-specified time period.

There are 25 predefined Cautionary and 25 predefined Critical traps available through the Foreseer SNMP Virtual Agent. They may be used to identify unique channels, or they may group channels by category. It is possible to use a single Trap Number multiple times.

On Microsoft operating systems the Microsoft SNMP software extension must be installed and setup, then the Virtual Agent SNMP Properties defined before this Foreseer feature can be enabled. You must always define the Virtual Agent Properties.

SNMP Installation

The Microsoft SNMP agent software must be installed on the Foreseer Server PC as a service of the Windows operating system.
To configure the Microsoft SNMP agent on Windows Server 2003, see http://support.microsoft.com/kb/324263.

To configure the Microsoft SNMP agent on Windows Server 2008, see http://social.technet.microsoft.com/Forums/en-US/windowsserver2008r2networking/thread/ce5ec0fe-30a8-4b6e-a6ae-a4d1b8c9d047/

SNMP Properties

Foreseer's SNMP Properties dialog box specifies the nature of the relationship between the Foreseer Client and the supervisory Network Management System (NMS). Its SNMP Properties settings may be reviewed and modified if necessary by clicking on the appropriate tab:

- **Administrative Authorization** is required to access SNMP Properties

**Agent** - Are optional entries that include information about the user to Contact and the physical Location of the Foreseer Client PC.

**Traps** - Identify each Community to which the Foreseer Agent belongs.

**Security** - Identify those Communities from which the Foreseer Client will Accept requests.

**Resend Traps** - Offer options for handling the retransmission of Traps to the Network Management System.

**SNMP Properties - Agent**

The SNMP Properties dialog box specifies the nature of the relationship between the Foreseer Client and the supervisory Network Management System (NMS). Agent Properties are optional.
entries that include information about the Foreseer User and the physical Location of the Client PC. Clicking in a field below displays its function: Clicking other tabs presents those SNMP Properties.

To modify SNMP Agent Properties:

1. Choose the SNMP Properties... command from the Administration / Message Management > sub-menu to display that dialog box.
2. Click on the Agent tab to display those settings.
3. Check Enable the SNMP Agent to activate Foreseer SNMP operation. This box must be checked or the SNMP Virtual Agent will not function.
4. Optionally enter the Contact, the name of the person in charge of the SNMP interface, and the Location of the Foreseer Client equipped with the SNMP interface.
5. The Agent DLL Directory reports the location within the Server PC of the installed SNMP Agent (typically the Foreseer folder) and cannot be altered.
6. With the desired Agent settings specified, click OK to accept the current entries and return to the previous Foreseer window or click on the other tabs to review those SNMP Properties.

SNMP Properties - Resend Traps

SNMP Properties specify the nature of the relationship between the Foreseer Client and the supervisory Network Management System (NMS). Resend Traps Properties offer options for handling the retransmission of traps so that alarms will not be overlooked at the NMS. Clicking in a field below displays its function: Clicking other tabs presents those SNMP Properties.
Foreseer **SNMP Properties** settings are easily specified to meet your reporting needs.

To modify **SNMP Resend Traps Properties**: 

1. Choose the **SNMP Properties...** command from the Administration / Message Management> sub-menu to display that dialog box.
2. Click on the **Resend Traps** tab to display those settings.
3. Specify whether to the **Resend traps for all alarms** or for only unacknowledged alarms. You also can choose to disable the **Resend Traps** feature completely.
4. Specify the **Resend Interval**, the delay in minutes, before a trap is resent. One of the **Resend Options** must be enabled to access this feature.
5. With the desired **Resend Traps** settings specified, click **OK** to accept the current entries and return to the previous Foreseer window or click on the other tabs to review those **SNMP Properties**.

**SNMP Properties - Security**

**SNMP Properties** specify the nature of the relationship between the Foreseer Client and the supervisory Network Management System (NMS). **Security Properties** identify those Communities from which the Foreseer Client will Accept requests. Clicking in a field below displays its function: Clicking other tabs presents those **SNMP Properties**.
Foreseeer **SNMP Properties** settings are easily specified to meet your reporting needs.

To modify **SNMP Security Properties**:

1. Choose the **SNMP Properties...** command from the **Administration / Message Management** sub-menu to display that dialog box.
2. Click on the **Security** tab to display those settings.
3. Click **Add..** to enter the Community Name of an NMS that is to receive Foreseeer SNMP traps and press **OK**. While “public” is included by default, you can **Edit...** or **Remove** it (or any other Community Name) by selecting it and pressing the appropriate button.
4. With the desired **Security** settings specified, click **OK** to accept the current entries and return to the previous Foreseeer window or click on the other tabs to review those **SNMP Properties**.

**SNMP Properties** - Traps

**SNMP Properties** specify the nature of the relationship between the Foreseeer Client and the supervisory Network Management System (NMS). **Traps Properties** identify each **Community** to which the Foreseeer **Agent** belongs and its respective **IP Address**. In other words, these are the Network Management Systems that will receive traps from the Client. Clicking in a field below displays its function: Clicking other tabs presents those **SNMP Properties**.
Foreseer SNMP Properties settings are easily specified to meet your reporting needs.

To modify SNMP Trap Properties:

1. Choose the SNMP Properties... command from the Administration / Message Management> sub-menu to display that dialog box.
2. Click on the Traps tab to display those settings.
3. Click Add to enter the Community Name of an NMS that is to receive Foreseer SNMP traps and press OK.
4. Click Add... to enter the IP Address of the Community shown then press OK. This Address must be correct or Foreseer will be unable to establish communications with the listed host.
5. Repeat the process to enter the Community Name and IP Address for each NMS that is to be notified with Foreseer traps. You can Edit... or Remove entries by selecting them and pressing the appropriate button.
6. With the desired Traps settings specified, click OK to accept the current entries and return to the previous Foreseer window or click on the other tabs to review those SNMP Properties.

SNMP Setup

There are 25 predefined Cautionary and 25 Critical traps available through the Foreseer SNMP Virtual Agent. They may be used to identify unique channels, or they may group channels by category. It is possible to use a single Trap Number multiple times. It is suggested that when creating a large number of traps for many channels, it may be helpful to group sets of channels under a common Trap Number.
To establish traps for specific Foreseer channels:

**Administrative Authorization** is required to access **SNMP Traps**

1. Choose **Setup** from the **Message Management** sub-menu in the **Administration menu**.
2. Click on the **Channel Message Settings** tab in the **Message Management** dialog box to list all of the configured channels by **Server**, **Device** and **Name**.
3. Locate and select the channel that will send a trap in response to a **Cautionary** and/or **Critical** alarm. Multiple channels may be chosen for the same trap by holding down the **Ctrl** key and highlighting them, or use **Shift** key to select all of the channels between clicks.

4. Click **Edit**, or simply double-click on the selected channel(s), to display the **Channel Message Settings** dialog box.
5. Click on the **SNMP** tab to assign those attributes. Independent **Trap Numbers** may be selected for the channel(s) from the **Critical** and **Cautionary Alarm** drop lists, as well as enabling the **Alarm Events** that initiate a trap.
6. Optionally assign Foreseer Text messages to specific traps under the Critical and Cautionary tabs. A detected alarm on one of the chosen channels will relay a trap to the Network Management System, where it is displayed in the Event Browser. If no message is specified under these two Local Properties tabs, the message sent to the NMS is the message entered on the Foreseer Server. A Local Channel Properties message overrides the Server's Channel Properties message in instances where comments have been entered at both locations. Click OK to accept the displayed SNMP settings.
7. Repeat Steps 5-8 to assign additional traps to additional channels, then close the **Message Management** dialog box.

8. Copy the Foreseer.MIB file from the Client onto a diskette and load it on the NMS.

9. Open the file to determine what messages are being sent with what traps, then decide which are appropriate for your installation. For instance, OpenView(R) for Windows NT employs the following wild-card characters:

<table>
<thead>
<tr>
<th>Character</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
<td>Server Name</td>
</tr>
<tr>
<td>$2</td>
<td>Foreseer Server/Channel Field</td>
</tr>
<tr>
<td>$3</td>
<td>Alarm Message (determined in Step 7)</td>
</tr>
<tr>
<td>$4</td>
<td>Current Alarm Channel Value (includes high/low threshold exceeded)</td>
</tr>
</tbody>
</table>

10. Select **SNMP Properties** in the **Administration / Message Management >** sub-menu to further alter any necessary parameters.

## Menu Reference

### Menu Reference

#### File Menu

The **File** menu furnishes one basic program command: the ability to quit the program:
Exit - terminates the current Foreseer Server session. If enabled during initial Server configuration, you are required to have Administrative Authorization to quit the program.

Alarms Menu

The Alarms menu allows you to respond to reported alarm conditions in several ways. This menu also is accessed by right-clicking with the mouse pointer positioned in the Tree View. Any grayed commands are not available for the currently chosen Server, Device or Channel. Multiple Devices or Channels of the same type may be chosen for modification using the standard Windows Shift-Click and Ctrl-Click selection methods.

The Alarms menu offers the following Foreseer commands:

Alarm Acknowledge - Allows an alarm condition to be acknowledged on the selected channel(s). Once acknowledged, a channel’s representative icons turns blue. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu if necessary.

Alarm Rearm - Allows alarm monitoring to resume on the chosen channel(s). A System Generated Note that includes the time of the rearming and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu. This command is only available for channels with an acknowledged alarm.

Alarm Ack/Rearm - Permits an alarm condition to be acknowledged and the selected channel(s) to be rearmed so testing of acquired Values against set Alarm Limits resumes immediately. Acknowledged, a channel’s icon turns blue. A System Generated Note that includes the time of the acknowledgment and the Name of the channel is logged automatically. A User Note can also be entered to further document the condition. Additional Notes may be entered through the Add Note... command in the Administration menu.

Alarms Management

The Foreseer Server allows for limited Alarm Management responses. Channel alarm conditions can be Acknowledged and Rearmed through the Alarms menu and the Tree View. A Note may be required to further document the situation.
To access the Foreseer Server Alarm Management capabilities:

[Box]

- **Administrative Authorization** may be required to Acknowledge and/or Rearm alarms.

1. The desired alarm channel(s) can be highlighted in the left pane of the **Tree View**. Multiple channels may be selected by holding down the **Ctrl** key and clicking on them individually. Holding down the **Shift** key while clicking on two channels selects all channels between them.
2. With the desired channel(s) selected right-click and choose the desired **Alarm** command—Acknowledge, Rearm or Ack/Rearm.

---

**Alarm Latching**

**Alarm Latching** is a toggle state which determines whether an alarm condition continues to be reported if the channel's **Current Value** returns to within its assigned **Critical** or **Cautionary Alarm Limits**. When **Enabled** the channel's highest alarm state is reported regardless of its **Current Value**; disabled, a channel is automatically removed from the **Status Bar's** **Active Alarm Totals** if its **Value** returns to within its specified **Limits**. Note that the alarms must be **Enabled** and **Limits** assigned under the **Basic** tab in the channel's **Meters** or **Status Channel Properties** dialog box. The **Re-Arm** period (one hour by default) is specified under the **Advanced** tab in the channel's **Meters** or **Status Channel Properties** dialog box.

**Hysteresis**, when **Enabled**, determines the threshold **Value** before a new alarm is reported for a **Meters** channel. Hysteresis is used to eliminate nuisance alarms when the channel's input is near its **Alarm Limit**. Once an alarm occurs, the input level must drop below or rise above the threshold **Value** then exceed the **Limit** once again before a new alarm is reported. The particular threshold **Value** is specified in the channel's display **Units** (i.e., volts, amps, hz, kVA, kw, etc.). Note that this
attribute is only available for non-Latching alarms.

Acknowledging and Rearming Alarms

Acknowledgment suspends limit testing on the alarm channel in order to allow the problem to be serviced although the channel’s Value continues to be calculated and archived. The context-sensitive Tree View menu allows limited alarm response at the Server. More comprehensive responses to alarm conditions are available through the Foreseer WebViews client.

**Administrative Authorization** may be required to Acknowledge and/or Rearm alarms.

To acknowledge a channel alarm:

1. Click on the affected channel to highlight it. Multiple channels may be selected by holding down the **Ctrl** key and clicking on them individually. Holding down the **Shift** key while clicking on two channels selects all channels between them.
2. Choose **Alarm Acknowledge** from the **Alarms menu**. You can also choose **Alarm Ack/Rearm** to immediately Rearm the channel and resume testing of its acquired Value against its set Alarm Limits.
3. If a **Password** was specified, you are prompted to enter the **Administrative Authorization** before proceeding. Another authorized user can temporarily log on to acknowledge an alarm without affecting the current user’s session. This allows the response to be recorded under that person’s name, or he has the option of becoming the currently logged in user.
4. You are also prompted to enter a Foreseer **Note** in the **Channel Acknowledgment and Rearm**
Notes dialog box to document additional information or observations about the alarm condition(s). The Note is limited to 256 characters and includes the time and date it was entered, as well as other relevant information. Once Acknowledged, the channel's icon turns blue to indicate its state. Additional Notes may be entered through the Add Note... command in the Administration menu if necessary.

**Administration Menu**

The Administration menu contains various system functions. Many Administration commands display a dialog box which requires additional input before the particular operation can be performed. Any grayed commands cannot be performed on the selected item or within the active window.

- **Administrative Authorization** is required before proceeding with any of these commands.

The Administration menu offers the following Foreseer commands:

- **Login...** - records the beginning of the current User's session.
- **Logoff...** - records the end of the current User's session.
- **Change Password...** - allows the current Administrative and Change Database Password to be altered.
- **Add Note...** - opens the Add Note dialog box, allowing user observations to be entered into the
database.

**Message Management** > - allows you to **Setup** the **Message Management** feature and **Configure Required Connections**. It also accesses the (optional) **SNMP Properties**.

**WebViews Server** > - allows an **HTTP** (non-secure) or an **HTTPS** (secure) WebViews Server to be created and viewed through a Microsoft Internet Explorer.

**Trusted Web Clients...** - is a list of IP addresses or machine names defining the set of web clients allowed to access WebViews / WebAdmin.

**Extension Plugins...** - is reserved for future program enhancements.

**Unload Driver** - is a **File Management** function which 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 function should only be performed at the direction of Eaton technical support.

**Load Driver** - is a **File Management** function which automatically loads the appropriate Device driver from the **Update VI** folder. Multiple Devices of the same **Type** may be selected for loading without shutting the system down. This function should only be performed at the direction of Eaton technical support.

**Server Properties...** - displays the **Server Properties** dialog box, allowing certain program parameters to be altered.

### Configuration Menu

The **Configuration** menu is used to alter the "shape" of the Server. Functions include modifications like remote Server management as well as adding and deleting Devices and channels. Any **grayed** commands cannot be performed on the selected item or within the active window.

> **Administrative Authorization** is required before proceeding with any of these commands.

The **Configuration** menu offers the following Foreseer commands:

**Start Server Configuration** initiates changes on the Foreseer Server. The **Server Configuration Mode** System Channel turns yellow and

```
********SERVER CONFIGURATION MODE********
```

is displayed in the window's title bar to confirm edit status.

**End Server Configuration** terminates changes to the Foreseer Server and returns to normal operation.

**Configuration Backup...** displays the **Configuration Backup** dialog box, allowing the Foreseer Server...
configuration to be saved as an archive file.

**Backup...** displays the **Backup** dialog box, setting automatic configuration backups.

**Install Device...** allows you to **Install Devices** on the Foreseer Server so that they may be monitored and added to the WebViews.

**Install Devices from List...** allows you to **Install Multiple Devices** through a .CSV file on the Foreseer Server so that they may be monitored and added to the WebViews **Views**.

**Add User-Defined Channel...** permits the User to create new **Derived Channel**.

**Add Channel...** permits the User to create a new **Meters** (Analog) or **Status** (Digital) Channel. This command is not available for all Devices.

**Disable** suspends all data archiving to the Foreseer Server for the selected Device or channel. Disabling is useful when making repairs to avoid archiving inappropriate readings and is necessary in order to Delete or Rename the Device or channel.

**Enable** resumes data archiving for the selected Device(s) or channel(s).

**Disarm** stops testing the channel values against specified alarm limits, preventing alarms from being issued.

**Rearm** resumes testing channel values against alarm limits.

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

**Rename** permits the selected Device or Channel to be renamed in response to changing conditions. It should be noted that renaming a Device or Channel should be done with discretion as changing a name can have an adverse effect on Foreseer WebViews 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. 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 the **Properties** are being copied from. 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 .VI (Device Driver) template based on the selected Device's settings. This file template can then be used to define other similar Devices.
Create All .VI Files generates .VI (Device Driver) templates for all Devices on the selected Server. These file templates can then be used to define other similar Devices.

Refresh Tree forces a refresh of all devices in the tree.

Properties... displays the selected Device Properties or channel's (Meters or Status) Properties dialog box, allowing its parameter settings to be reviewed or altered.

Configuration Backup

The Server configuration can be saved in order to retain Channel Properties and other system settings for subsequent Foreseeer sessions. It is strongly recommended this System Administration function be performed after initial system configuration as well as before and after any significant modifications (or when performing batch changes in larger configurations) to ensure maximum disaster recovery capability. The Server Configuration Mode System Channel reports when structural changes have been to the Server configuration. The Backup archive includes all Foreseeer Server configuration files, which are compressed to conserve disk space.

This procedure does not backup data, Log or Report files— it is recommended that these files routinely be backed up to a network drive.

To Backup a Foreseeer Server configuration:

1. Select Configuration Backup in the Configuration menu to display the Backup Completed dialog box.

2. Foreseeer indicates when the archiving process is successfully completed. Click OK to return to the window that was active prior to the backup operation.
For Outpost Only: If an *.ARQ file is in the Config Restore folder when the Server is started, it will delete the current Data and VI folders, move the *.ARQ file into the Restore folder and restore it. This is also a new destination for the Upload Files command. It is important to remember that the restore is automatic at the next restart and that the Data and VI folder contents will be deleted.

Database Menu

The Database menu is used to perform various Foreseer functions related to the databases. Any grayed commands cannot be performed.

Administrative Authorization is required before proceeding with any of these commands.

The Database menu offers the following Foreseer commands:

- **Start Database Session** - initiates data acquisition from the connected equipment by the Foreseer Server.
- **End Database Session** - suspends data acquisition from the connected equipment by the Foreseer Server.
- **Check Databases** - verifies the integrity of the Foreseer Server databases in the event the program was terminated improperly.
- **Fix Databases** - corrects any problems detected during the Check Databases process.
- **SQL Server Properties** - launches the SQL Server Setup dialog box.

Database SQL

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.
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: [Edit] Lab VM

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: [Server] Password: [********] Verify: [********]

To use Windows Authentication mode for SQL Server, you will need to enter the credentials for the Windows Account that SQL Server will use. If this is not a new server install, the account information must be set from the Server Properties - General tab.

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: [Edit]...
Log File Path: [Edit]...

[OK] [Cancel]
Appendix

4CR tm ProGraph tm and Foreseer SNMP Virtual Agent tm are trade marks and Foreseer

4CR(tm), ProGraph(tm) and Foreseer SNMP Virtual Agent(tm) are trademarks and Foreseer(R) is a registered trademark of Eaton Corporation.

About Foreseer Server

The About Foreseer Server dialog box displays version, release date and copyright information on the currently installed copy of the application. It also provides a telephone number to obtain technical assistance and an itemized list of the System Configuration options.

Ack Holdoff

Ack Holdoff defines (in seconds) the delay interval after a channel alarm has been acknowledged (or silenced) before it is automatically rearmed. Acquired data continues to be displayed, but the channel's Current Value is no longer compared to its defined Alarm Limits. The default Holdoff period of one hour may be manually overridden at any time using the Foreseer Client's Rearm command, or when the alarm is acknowledged.

Add Button

Add includes the currently highlighted item(s) in the selection list.

Adding Notes

The Foreseer Notes feature fulfills a unique and timely function by recording any supplemental information relevant to a particular event when it occurs. Simply choose the Add Note... command in the Administration menu. The Add a Note dialog box permits the System Administrator to enter Notes which 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. Foreseer Notes can also be entered in the course of Acknowledged and Rearming alarms.
Address

Address is the target device’s IP Address in a network installation. This Address **must** be correct or network connections cannot be established between the Foreseer Server and the target Device.

Add Slave

Includes the identified Slave Server Name in the associated list box for Heartbeat function.

Administrative Authorization

Password protection ensures that only authorized personnel are allowed to alter the Foreseer Server configuration or halt its data gathering and system monitoring operations. When enabled, a security password must be entered before most Server functions can be accessed. The first attempt to alter protected Server settings requires the **Administrative Password**. The password is entered in the **Administrative Password** dialog box; asterisks are displayed to maintain system security. The accepted entry automatically becomes part of the **System Log** and is available for review in that **Foreseer Report**. Once entered, the user has access privilege to all protected Server functions and does not have to enter the password again during the current session.

The **Administrative** and **Client Connection Passwords** may be changed, or assigned at a later time if one was not specified during initial Server configuration. The **Change Passwords** dialog box
permits these Foreseer Server authorizations to be altered. Changing a **Password** does require entry of the **Old password** before you are allowed access the **New password** field.

To change the Server's current **Administrative password**:

1. Select **Change Passwords...** under the **Administration menu** and the **Change Server Password** dialog box is displayed.

2. Click on the **Change Administrative Password** or the **Change Database Password** button to display the appropriate dialog box.

3. Enter the **Old Password**; asterisks are displayed to maintain system security. If no **Password** was previously assigned, simply **Tab** to the **New Password** field.

4. Enter the desired **New Password**.

5. Type the same character string in the **Verify New Password** field to validate the **New Password**.

6. Click **OK** to save the **New Password**.

---

**Passwords** are case-sensitive; therefore "USER," "User" and "user" are all recognized as different **Passwords**.
Agent DLL Directory

Is the directory location within the Server PC of the installed SNMP Agent, typically the Foreseer folder.

Alarm Events

Determines when the specified Critical Alarm and Cautionary Alarm Traps are sent to the supervisory NMS in response to a Limit excursion detected on this channel.

Alarm Message

Is the display text corresponding to the channel's Cautionary (yellow) and Critical (red) Alarm Limits, if Enabled. Messages may be independently assigned to the Hi and Lo Limits for each Meters (analog) channel level event. A Status (digital) channel can have only one Message.

Alarm on Value

Specifies whether a False (0) or a True (1) value triggers an alarm for this digital channel.

Alarm Type

Specifies whether an alarm reported on this channel represents a Cautionary (yellow) or a Critical (red) Alarm Limit excursion.

Alarm Updates

Specifies how often the <Alarm Management> display is updated with alarm information from the Remote Server.

Alpha Message

Allows you to identify the type of message that is to be sent with the alert issued when an alarm is reported on this channel and is the normal Message Management notification method. A Standard Alarm Message is specified in the channel's Meters (analog) or Status (digital) Basic Properties dialog box and applies to Critical and Cautionary alarm conditions. The message "Acknowledged" is automatically sent for an Acknowledged state and "Channel Normal" for a Normal state. Checking the appropriate boxes also includes the Server, Device, Channel Name and/or Alarm Message. You can enter an additional Alpha Message to Include in the notification as well as the alarm message. Selecting Edit the Custom Message opens a dialog box allowing alternative response instructions to be entered.
Apply

Enables the **COM Port Settings** shown. This command can be used to verify communications with the Foreseer Server and before proceeding with **Device Installation**.

Archive

Specifies the analog channel **Value** that is archived to the Foreseer Server database. It may be the **AVERAGE**, or the **MINIMUM, MAXIMUM, FIRST, LAST, NULL** or **NONE** reading over the archive interval.

Available Time

Specifies when the named **Subscriber** is available for paging by designating the **Start** and **End Time** which define the period that person can be notified. Enter the times or use the associated arrows to scroll to the appropriate **Time**. The corresponding display changes to report the total **Availability Time**.

Baud Rate

Is the data transfer rate between Foreseer and the messaging device. Other **Rates** are available by pressing the associated arrow. The **Baud Rate** is available from the device’s manual or the service company.

Bits Per Second

Is the baud rate transmitted through the serial interface each second. Other **Bit** selections are available by pressing the associated arrow.

Border Display

Determines the type of **Border** used to delineate the data in the Browser display. You may wish to try all three settings to determine which looks best on the Browser(s) accessing the Web Server.

Browser Format

Determines how the Web Server data is displayed. **Browser Based**, the default, attempts to determine the type of Browser on-the-fly and present the Web Server information in an appropriate format. This setting is particularly useful in instances where the Server may be accessed by multiple Browser types and should only be changed if all potential Web Browsers use the same format.
Call Again

Re-initiates the call highlighted in the **Status** area of the *Message Management* window.

Call Entries

Specifies the length of time recorded messages are kept before being automatically deleted from the list.

Call Now

The **Call Now** dialog box, displayed when the **Test Call** button is pressed in the *Notification Lists* window, allows you to verify that *Message Management* notifications are performed properly.

```
Test Call Messages

Provide the messages that you wish to send when the notification list is called.

Messages

* Numeric Message: 

* Alpha Message: 

Outcall Test

* Command Line Message: 

* SNMP Message: 

Priorities

Primary: Normal

Secondary: Normal

OK Cancel
```

Call Properties

Determine whether to call the entire *Notification List* even if an alarm acknowledgment is received and messaging is terminated, allow higher priority *Lists* to take call precedence, and if listed personnel using the same *Service* should be notified with the same call.
Cancel Button

Exits this dialog box without making any changes.

Cautionary Alarm Trap Numbers

The number of the Trap, ranging from 200-224 in the Foreseer SNMP Virtual Agent, that will be sent to the Network Management System (NMS) in response to a Cautionary Alarm for this channel.

Channel Disabled

When checked, alarms are not reported and data is not archived for this channel. Disabling a channel is useful when performing Device maintenance or making repairs to avoid archiving inappropriate readings.

Channel Disarmed

When checked, suspends alarm reporting for this channel. Data, however, continues to be archived. Disarming a channel is useful when performing Device maintenance or making repairs to avoid reporting nuisance alarms.

Channel State

Is a fixed entry reporting the current alarm status of the input as Normal, Cautionary, Critical or Acknowledged.

Channel Updates

Specifies how often the <Alarm Management> display is updated with channel information from the Remote Server.

Channel Value

Reports the result of Testing the displayed Equation.

Characters per Message

Is the maximum number of characters allowable in the paged message. Consult the pager manual or the paging company for the limitation of the device.
Close Button

Shuts this dialog box and retains the displayed settings.

Command Line

Is the command to execute for this user-defined Service. For example, entering C:exe (or simply Notepad.exe if the application is in the search path) would launch Windows Notepad program.

Communication Retries

Is the number of times communications are attempted when a Device command is unsuccessful.

Community Names

Is the list of Communities to receive Foreseer SNMP traps.

COM Port

Is the Foreseer Server serial port through which Device or TABS communications are sent. An alternate Port may be chosen from those available in the associated drop list. When installing devices, clicking on the Configure... button in the COM Port Service Properties dialog box displays the COM Properties dialog box, allowing these communications settings to be changed.

COM Properties

The COM Properties dialog box defines the communications parameters between the Foreseer Server and a directly connected serial Device. These variables must agree with the settings on the target Device or communications cannot be established.
Configure Required Connections

This optional notification configuration procedure identifies which Foreseer Clients and/or Remote Servers are required to be connected to this Server to perform Message Management functions. If any one of the listed Servers or Clients becomes disconnected from this Server, the Message Management option begins its messaging routine to alert personnel of alarms.

To configure required connections:

1. Select the Configure Required Connections... command from the Administration menu / Message Management> sub menu to display the Required Connection Settings dialog box.
2. Click on the Add... button to access the Enter Client IP Address dialog box.

3. Furnish the network Address or Computer Name. By IP Address is used for network connections to a fixed Server (the default of 127.0.0.1 is reserved for Foreseer Servers and Clients which are installed on the same PC); By Computer Name allows you to dynamically connect to a Client computer which does not have a fixed Address. Click OK to continue.

4. Check the box preceding the Address to enable Server access by that connection.

5. Specify the Startup Delay in which the Server will ignore any Remote Servers or Clients that become disconnected before initiating messaging. This Delay is in effect whenever the Server is initialized or when modification are made.
6. Repeat the process to **Add...** other Foreseer Clients or Remote Servers to the list.
7. Click **OK** to accept the displayed **Required Connection Settings** and return to normal operation.

**Connection Password**

Is an optional level of security which requires a **Password** in order to access a Remote Server. The **Password** must be entered a second time to **Verify** it.

**Connection Time-out**

Specifies how long before connections with the Remote Server time-out.

**Connect to this Server at Startup**

Automatically initiates connection with this Remote Server when the **Foreseer Server Application** is launched.

**Connect UPS is a registered trademark of Powerware Corporation**

**ConnectUPS(R)** is a registered trademark of Powerware Corporation.

**Contact**

Is the name of the person in charge of the Foreseer SNMP interface.

**Copy Button**

Duplicates the selected Foreseer object(s) on the clipboard.

**Copy Messages**

Copies the information displayed in the **Messages for Message Caller** list box to the clipboard for printing or incorporation into other applications.

**Copy These Settings to Other Dialog Tabs**

Saves time and reduces the potential for data entry mistakes by pasting the messaging parameters shown under this tab in the **Channel Message Settings** dialog box into the chosen tab(s). This shortcut is recommended **only** for tabs that share the same messaging properties.
Create New Folder

Creates a new folder within the current Windows directory in which the specified File name will be saved.

Critical Alarm Trap Numbers

The number of the Trap, ranging from 200-224 in the Foreseer SNMP Virtual Agent, that will be sent to the Network Management System (NMS) in response to a Critical Alarm for this channel.

Current Device Settings

Identify the communications parameters between Foreseer and the connected Device. Note that these Settings cannot be modified from within the read-only Device Properties dialog box.

Current Value

Is a fixed entry showing the channel's last reported reading.

Database Administrative Account Name

Is the name of the Account Administrator used to access the SQL Database Server for configuration modification. The Name should remain blank for standard Windows Authentication. The administrative Account Name Password used to access the SQL Database Server is independent of the Administrative Password and can be altered by clicking on the Password button.

Database Backup

The Foreseer Server's archived database can be scheduled to be backed up automatically at specified intervals. The size of the Server database is determined by the number of channels and the rate at which the data is archived. A network drive is the recommended backup destination. The Backup archive includes Foreseer data files as well as logged Alarms and Notes, but does not include Server configuration information. Note that the use of the Jet database is now deprecated. (see Configuration Backup).

To schedule a Foreseer Server Database Backup of a Jet database:
Administrative Authorization is required to backup the Server database. SQL Server databases are archived according to individual company protocols—consult your Network Administrator for instructions.

1. Select Database Backup... in the Database menu to display that dialog box.

2. Specify when the backup is to be performed. 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 a tape drive and it cannot be within the half hour preceding midnight if archiving to another disk drive.

3. Check the Day(s) of the Week on which the database backup is performed. At least one day must be checked to enable this automatic feature.

4. Specify the media on which the backup is to be performed. If the archive is coordinated with an existing tape backup program, enter the maximum duration of the backup; if archiving to another drive, enter its destination path. Check Create a sub-directory for each backup, if desired, to generate an independent folder for each backup and specify how many subdirectories are retained before they are deleted from the system. Also check to include historic data in the backup or leave the selection blank to archive only the information logged since the previous data backup.
5. Click **OK** to enable the displayed **Data Backup** settings. Archiving will be performed automatically at the scheduled time on the selected day(s).

**Database Server Name**

Identifies the remote SQL Server where the database resides. This **Server Name** appears whenever it is reported, such as in **Message Management**, **Reports** and for Heartbeat functions. The **Name** can be a maximum of 29 characters and the field may be blank if a local SQL database engine is being used.

**Data Bits**

Are the number of **Data bits** in each transmission packet. Other values are available by pressing the associated arrow.

**Days of the Week**

Identifies the **Days** for which the displayed **Availability Time** entries apply.

**Defaults**

Restores the setting(s) to the original factory installed value(s).

**Delay Alarm**

When **Enabled**, is the period of time (in **seconds**) before an alarm detected on this channel is reported. The default is to report alarms immediately.

**Delays**

Determine how long after an alarm is reported before messaging is initiated on the **Notification List**, as well as whether this delay is observed the first time the **List** is called.

**Delete Master Heartbeat Device**

Removes this Server from Master Heartbeat duties.

**Description**

Is a user-entered comment identifying the channel.
Device Channel Count

Displays the Total number of data points on this Device tallied as Analog, Digital, Text and Time channels.

Device Description

Identifies the equipment, its current operational Status and the time of the Last Scan for data by the Foreseer Server.

Device Disabled

When checked, data are not being archived to the Foreseer Server for this Device. Disabling a Device is useful when making repairs to avoid archiving inappropriate readings.

Device Disarmed

When checked, Alarm Limit testing is suspended on all channels on this Device. Data, however, continue to be archived. Disarming a Device is useful when making repairs to avoid reporting nuisance alarms.

Directory List Box

Itemizes the files and folders within the current directory.

Disable All

Disables all optional settings for this screen.

Domain

Identifies the Domain to which the named User belongs.

Down Button

Clicking this button moves the selected person down one position in the Notification List.

Edit Button

Allows you to modify the selected item.
Edit Custom Message

The **Edit Custom Message** dialog box is reserved for sending specially formatted *Alpha Paging* or *Command Line* messages. Simply type the desired **Custom Message** in the text box provided. You also can **Insert the Server Name, Device Name, Channel Name, Alarm Message, Current Date** and/or **Current Time** into the text by placing the cursor in the desired location within the text box and then selecting these optional entries from the drop list below. With the **Custom Message** entered, click **OK** to save it for this channel alarm condition; **Cancel** deletes the **Message**. Note that this method requires more memory from the Foreseer application than the **Standard Alarm Message** format.

Enable

When checked, activates monitoring of a **Meters** (analog) channel's **Cautionary (yellow)** and **Critical (red)** Limits: a **Status** (digital) channel is either enabled or disabled. Alarm monitoring for all of a **Meters** channel's thresholds can be suspended by checking **Channel Disarmed** in its **General Properties** dialog box.

Enable Acknowledge Rearm

Permits a **User** to **Acknowledge** (and **Rearm**) alarm channels through the Web Server function. Note that this function is only available for HTTP/HTTPS Servers operating in the **Text Mode**.

Enable All

Enables all optional settings for this screen.
Enable Scaling

When enabled, allows you to apply a linear scaling factor to the channel’s Minimum and Maximum Raw and Scaled Values. Only integer Values are acceptable entries and this settings should only be altered at the direction of Eaton personnel.

Enable the ASCII Alarm Interface

When checked, activates the Foreseeer ASCII Alarm Interface function. Enabling or disabling this function requires that the computer be restarted before the state change takes effect.

Enable the HTTP Server

When checked, activates the Foreseeer Web Server function. Text Mode is a text-only presentation of Server information, WebViews Mode displays Foreseeer Views in the Browser similar to how they are presented on the Client. Enabling (or disabling) this function requires that the computer be restarted before the state change takes effect.

Enable the HTTPS Server

When checked, activates the Foreseeer HTTP Web Server function. Text Mode is a text-only presentation of WebViews Server information, WebViews displays Foreseeer WebViews in the Browser. Enabling (or disabling) this function requires that the computer be restarted before the state change takes effect.

Enable the Slave Heartbeat Function

Checked, the Heartbeat Function is activated on this Slave Server, its periodic signal sent to the displayed Master Server LAN or Dial-Up Address. Unchecked, this function is disabled.

Enable the SNMP Agent

Activates the optional Foreseeer SNMP interface. This box must be checked for the SNMP Virtual Agent to work; unchecked inhibits SNMP operation.

Enable the TABS Interface

Activates this Legacy alarm interface.

Ending Date Time

The date and time at which the Custom Report terminates.
Exclude Device or Channel

Displays the Device/Channel Selection dialog box, allowing individual Foreseer Server Devices and/or Channels to be excluded from a Custom Report. By default, all Devices and channels are included in the report.

Exclude String

Performs a text search omitting the criteria entered in the Custom Search dialog box. Be sure to observe the character restrictions.

False String

Is the operational State that will be reported for this channel when its Current Value is FALSE.

File Name

Is the user-selected name of the Foreseer file.

First-Char Timeout

Is how long (in milliseconds) to wait for a response from the Device after issuing a command.

Flow Control

Determines how the data transactions are handled between the Foreseer Server and the target Device. Other selections are available by pressing the associated arrow:

- Xon/Xoff - enables software handshaking between the Server and the Device.
- Hardware - enables hardware handshaking between the Server and the Device.
- None - no handshaking is enabled.

Foreseer Window

The Foreseer Server window presents the Tree View, as well as other application displays such as Meters (analog) and Status (digital) Channel Properties dialog boxes and the Online Help. Clicking on the right mouse button with the pointer inside the Tree View presents a context-sensitive menu.
Frequency of Calls

Specify the number of times the Notification List will be called as well as how many times each individual on the List will be called until a response is received. There is also a provision for specifying how many times the List will be recalled in the event none of the Subscribers responds to the initial notification.

Group Name

Identifies the collection of Foreseeer Clients who are Authenticated access to a Web Server, as well as whether they can Acknowledge and Rearm Alarms.

Heartbeat Interval

Is the number of minutes that elapse between each issuance of the named Slave Server's Heartbeat signal. The default Heartbeat Interval is 720 minutes (12 hours), but you may wish to stagger this Interval when multiple Slaves are being monitored.

Identification Information from Device

Reflects the basic configuration parameters that the Server obtained from the equipment during Device Installation including its Address and power ratings.

Include Device or Channel

Displays the Device/Channel Selection dialog box, allowing individual Foreseeer Server Devices and/or Channels to be included in a Custom History Report. By default, all Devices and channels are included in the report.

Include String

Performs a text search based on the criteria entered in the Custom Search dialog box. Be sure to observe the character restrictions.

Insert Channel

Displays the Select Channel to Insert dialog box, allowing existing inputs to be included in the Derived Channel transfer Equation.

Inter-Character Timeout
Is the period of silence (in milliseconds) to wait during a Device response before determining the message is complete.

IP Addresses

Is the list of TCP/IP Addresses for the SNMP Communities. These IP Addresses must be correct or Foreseer will be unable to establish communications with the listed host(s).

LDAP Binding

This tab associates groups to which a user belongs to Foreseer groups, granting that user rights within Foreseer. Essentially, you specify the attribute that returns the distinguished name in the user DN Attribute field and then map objects that define user groups in LDAP in the appropriate Foreseer group field. Typically, you will be matching on common name (CN) objects, as is shown in the example. If you wish to grant membership in a Foreseer group to multiple LDAP user groups, separate these object definitions with a comma. For more about Foreseer groups, see the Foreseer Server Guide.
LDAP Directory

You must set the base distinguished name (dn) that Foreseer will use to run queries on the directory server. The subtree search starts from this distinguished name. You must also set the query depth (Search Scope).

The filter that is preloaded in the Search Filter was designed to find user objects in most situations. However, you can enter your own string tailored to your system. The example shown in the following figure has such a string.

The final field specifies the attribute that will return all groups to which a user belongs. If you use a different attribute you’ll need to replace the default string.
LDAP Shortcuts

Foreseer has two "superuser" groups: PXAuthADMIN and PXAuthROOT. You can also map these to LDAP user groups. For more about Foreseer user groups, see the Foreseer Server Guide.
LDAP Testing

You can test an individual LDAP account to see what Foreseer groups are mapped to it. This is extremely useful in verifying that all of the settings are correct.
Limits

When Enabled, are the channel’s monitored Cautionary (yellow) and Critical (red) Alarm Limits. Independent Hi and Lo Limits can be set for both event levels.

List Details

Toggles the current Windows directory display between an alphabetical listing of its files and one which also furnishes each file’s Size, Type and the date it was last Modified.

Location

Is the location of the Foreseer Client equipped with the SNMP interface.
Log Messages

Reports the number of Messages that can be logged for this Device.

Look In

Is the Windows directory in which the desired File name is found.

Master Server Dial-Up Address

The secondary Address of the Master Server to which this Slave Server sends its Heartbeat signal. This IP (Internet Protocol) Dial-Up Networking Address is only used if the primary LAN Address connection fails.

Master Server LAN Address

The Local Area Network Address of the Master Server to which this Slave Server sends its Heartbeat signal. This IP (Internet Protocol) Address assumes the Master and Slave Servers exist on the same network. If this connection fails, the signal is sent via the secondary Dial-Up Networking.

Max Number of Connections

Limits the number of simultaneous active Browser connections permitted on the Server. Enter the desired number of allowable connections, bearing in mind that more connections will reduce the Server's response time for each request.

Max Number of Requests

Defines the data request limit for Web Browsers that support the Keep-Alive function, which maintains connection with the Web Server unless the specified Timeout period expires. Set the Max Number of Requests to "1" to disable this function.

Messages

Provides for a user-entered message to be assigned to an alarm notification sent via an alpha/numeric pager. The message must conform to the Service provider's character limitations. Optionally, the appropriate Alarm Message, entered in the errant channel's Meters or Status Basic Properties dialog box, can be included in the outgoing Alpha/Numeric message. When defining a channel's Messaging Properties, its Server, Device and Channel name also may be included in the message.
Messages Menu

The **Messages** menu is displayed when the **Message Management** window is active and allows you to control the notification process when an alarm is reported. Several of the commands are duplicated in the context-sensitive menu that is accessed by selecting a **Message** in the window’s **Status Display** and right-clicking.

The **Messages** menu offers the following Foreseer commands:

- **Save Message File** - Saves the contents of the **Message Management** window (excluding the information in the **Status** portion) to a file.
- **Stop Call** - Terminates calling the **Source(s)** currently highlighted in the **Status** area of the **Message Management** window.
- **Call Again** - Re-initiates calling to the **Source(s)** currently highlighted in the **Status** area of the **Message Management** window.
- **Remove Call** - Removes calling to the **Source(s)** currently highlighted in the **Status** area of the **Message Management** window.
- **Stop All Calls** - Terminates calling to all **Sources** currently listed in the **Status** area of the **Message Management** window.
- **Remove All Completed Calls** - Deletes all completed calls that are currently listed in the **Status** area of the **Message Management** window.
- **Suspend All Calls** - Postpones calling to all current and pending **Sources** listed in the **Status** area of the **Message Management** window for one hour.
- **Status Messages...** - Displays the **Status Messages** dialog box containing detailed call information on the selected **Source(s)**.
- **Show Title Tips** - When enabled, displays the complete message for the selected **Source(s)** in a pop-up tip window whenever the pointer is held over its **Status** field.
- **Properties** - Displays the Message Properties dialog box, permitting the period for which completed messages are retained and the duration for which pending calls are suspended to be specified.

Network Connection

The Device's **IP Address** must be entered when utilizing a ConnectUPS Network Adapter a **Network Device Connection** during **Device Installation**. Obtaining this **Address** is the responsibility...
of the user and *it must be correct* or the Server will be unable to communicate with the target Device. With the correct Device **IP Address** entered, click **Next >** to return to the **Device Installation Wizard**.

New Password

Is the new **Client Password** required to access this Foresee Server. You must repeat the entry in the **Confirm New Password** field to activate it.
Notification List

Identifies the personnel to be alerted to an alarm condition on this channel by Foreseer Message Management. An existing Notification List is selected from the drop list that is displayed by clicking on the associated arrow. You may optionally specify that Foreseer Always notify regardless of Client connections by checking that box to ensure that the proper personnel are appraised.

- If upgrading an earlier version of Foreseer, any previous channel with an assigned Notification List will use it for reporting Critical and Cautionary alarm states. Acknowledged and Normal state conditions are not assigned Channel Messages by default; they must be entered manually by the User.

Notification List Name

Identifies the Notification List that is used to initiate alarm messaging.

Numeric Page

Allows you to Enter the numeric message that is to be sent with the alert issued when an alarm is reported on this channel.

Parity

Is the Parity (Odd, Even, None, Mark or Space) of the transmission. Other selections are available by pressing the associated arrow.

Password

Is the current User’s Administrative Authorization; asterisks are displayed to maintain system security. The Foreseer Web Server function offers optional security by requiring a Password to view information, generate Reports and Acknowledge alarms.

- Passwords are case-sensitive; therefore "USER," "User" and "user" are all recognized as different Passwords.

Phone Number
Identifies the Dial-Up Networking connection this Slave Server uses when issuing its Heartbeat signal to the Master Server.

Port

Identify how the Device or modem is connected to the Foreseer Server. The possible Device connections are a Network or a Serial Communications interface.

Port to Listen on for HTTP

Is the port the Server will monitor for HTTP requests from Foreseer Clients. The default setting of "80" is the standard port and should not have to be changed under normal conditions.

Port to Listen on for HTTPS

Is the port the Server will monitor for HTTPS requests from Foreseer Clients. The default setting of "443" is the standard port and should not have to be changed under normal conditions.

Postfix Phone Number

Specifies any number(s) to be dialed following the Service Number, such as a Password.

Pre-defined Time Interval Report

Allows the Custom Alarm, Audit and Notes History Reports to be run over a fixed period of time. Choose the desired Time Interval from the selections available when you click on the associated arrow.

Prefix Phone Number

Specifies any initial number(s) to be dialed, such as a "9" to access an outside line. Characters should be separated by a comma, which represents about a 2-second pause.

Printer

Identifies the active printer and its connection: Click on Properties to change the printer setup. When specifying a Printer Service, you can only select from the drop list of Printers previously installed.
Printing Properties

Specify how the Alarm Message (up to 8 lines of text) is output by the Printer:

- Prefix each message with Date and Time appends a time stamp to the beginning of the Alarm Message.
- Print page after each message and Print page when messages fill printed page control whether each Alarm Message is output individually.
- Number of lines to space after each message allows you to specify a number blank lines to be inserted between Alarm Messages when they are printed on the same page.

Priority

Is a number from 1 (highest) to 9999 (lowest) which assigns a level of importance to an alarm detected on this channel.

Rearm

Is the period of time (in seconds) before alarm monitoring is automatically restored to a disarmed channel. Rearming manually resumes testing of a channel's acquired Current Value against its specified Alarm Limits. Check the box preceding this field to Enable the setting.

Redundant Server

Specifies whether the Server is part of a redundant backup system. A Primary Redundant Server synchronizes timing between all Secondary Redundant Servers. Only one Server can be designated as the Primary Redundant or timing problems will result when adding new Servers and Devices to the configuration. If the Server is not part of a redundant system, select Stand-Alone.

Refresh Interval

Is the period, in seconds, before Web Browsers update the information in the Server screen display. This is a global setting for all Browsers that are capable of automatically refreshing their display; a setting of "0" disables this function.

Remove Slave

Deletes the identified Slave Server Name in the associated list box for Heartbeat function.

Report Interval

Is the calculated span of the Custom Report based on the Starting and Ending Date/Time entries.
Resend Interval

Is the delay (in minutes) before a trap is resent. One of the Resend Options must be enabled to select this feature.

Resend Options

Allows you to resend traps for all alarms or only unacknowledged alarms once the delay specified in the Resend Interval has expired, or disable the Resend Traps feature completely.

Restore Defaults

Loads the default Windows Control Panel / COM Port settings.

Retry Time

Is the delay between attempts to reconnect to a disconnected SQL Server. The default Retry Time is 30 seconds: A setting of "0" seconds disables this feature until a new setting is entered.

Scan Interval

Is the delay (in milliseconds) between data polls of the Device.

Scan Time Watchdog

Monitors the Scan Interval for the Device. Assuming it is enabled and does is not reporting a communications alarm, a system error will be generated if the period between successful scans of the Device exceeds the specified Watchdog Time interval.

Secondary Data Path

Applies only to Jet databases and may be entered to designate an alternate location where Foreseer attempts to retrieve historical data when the requested information is not located in the active data directory. (The use of Jet is deprecated.) Typically, this is a larger hard drive located on the network that can provide the significant storage capacity required for the high-resolution data accumulated over time. The secondary location can be specified as the Database, Backup Path, if desired. You also can Browse... the network to locate the desired destination.

Separator Character

Separates the text between individual ASCII alarm outputs.
Service Name

Identifies the Service that is used to initiate the alarm notification or command.

Service Properties - Command Line

The Command Line Service Properties dialog box is used to configure a custom Message Management Service. It can be used to issue a notification via a Service which is not already defined through one of the existing out call options, or the command could launch another application. If a Command Line entry is made here, it is applied globally to all alarm channels subscribing to this Service. Specific Command Line instructions can be applied to individual channels using Foreseer Channel Message Settings.

If you intend to create Custom Messages for individual channels, leave the Command Line field blank.

Service Properties - Output to COM Port

The COM Port Service Properties dialog box is used to configure the parameters for that particular type of messaging Service. Clicking in a field below displays its function.
Service Properties - SMTP Mail

The **SMTP Mail Service Properties** dialog box is used to configure the parameters for Simple Mail Transfer Protocol messaging. An SMTP Server is required for this **Service** to be available to Foreseer.

In addition to specifying an email address and SMTP server, you can also specify a User-name and Password for the account.
Settings Button

Allows the serial interface settings to be specified for the named Port through the COM Properties dialog box.

Service Properties - Printer

The Printer Service Properties dialog box is used to configure the parameters for that particular type of messaging Service. Clicking in a field below displays its function.

![Printer Service Properties dialog box]

Significant Characters for Location Names

Specifies the number of significant characters identifying the alarm location.

Slave Server Name

Identifies the Slave Server to the Master Heartbeat Server. The Name shown must match the one that appears in the Slave Server's Properties dialog box exactly or the two computers will not communicate properly.

SMTP Server IP Address or Name

Is the Internet Protocol Address or Name of a Simple Mail Transfer Protocol Server.
Sound Horn

Alerts personnel via an audible signal whenever a specified alarm state is detected. These conditions—Critical (Red), Cautionary (Yellow) Acknowledge (Blue)—are enabled by checking the appropriate box(es).

Status Bar

The Status Bar displays context-sensitive messages which aid program activity, such as the operation resulting from selecting a particular menu command. The right side of the Status Bar shows when the Caps Lock (CAP), Numeric Lock (NUM) and Scroll Lock (SCRL) keys are active. The Status Bar itself can be hidden and displayed (default) by toggling the Status Bar command in the Windows menu; a check preceding the command indicates when it is enabled.

Status Messages

Displays the Status Messages dialog box containing detailed call information on the selected Source(s).

Stop All Calls

Terminates calling to all Sources currently listed in the Status area of the Message Management window.

Stop Bits

Are the number of Stop bits in the transmission. Other selections are available by pressing the associated arrow.

Stop Call

Terminates notification to the Source(s) currently selected in the Status area of the Message Management window.

Subscriber Name

Identifies the individual to whom the Properties apply.
Suspend All Calls

Postpones calling to all current and pending Sources listed in the Status area of the Message Management window for the period specified in the Message Properties dialog box.

Synchronize Remote's Clock on Connect

Automatically updates the current time on the Remote Server on connection.

TCP Port

Is the port through which the ASCII text alarm is output.

Temporarily Disable the Connection Retry

Allows you to temporarily disable the automatic retry connection feature when maintenance or other procedures are being performed on the SQL database Server. This setting can be unchecked manually to restore automatic reconnection, or is automatically reset when the local Server PC is rebooted.

Terminal Server Connection

When checked, indicates the Device is physically attached to a Terminal Server.

Test Button

Simulates an input to the displayed Equation and reports the result in the associated Channel field. Testing the Equation permits its operation to be verified before the channel is placed into service.

Test Call Button

Verifies proper operation of the selected call. The Call Now dialog box is displayed, allowing you to enter Alpha and/or Numeric Messages to be sent, as well as assign them Primary and Secondary Priorities. Click OK and the progress of the Test Call is reported in the Status portion of the Message Management window.

Timeout

Is the interval of inactivity (in seconds) before connections are terminated. The Timeout period applies to update Requests in Web Browsers that support the Keep-Alive Function as well as the ASCII Alarm Interface.
Title Bar

The Title Bar identifies the Foreseer application and the active window. Minimize, Maximize and Close, are standard Windows buttons which perform those program functions. These three operations are also available as commands, along with Windows Restore, Move and Size functions, by left-clicking on the Foreseer Server icon or right-clicking on the Title Bar itself.

True String

Is the operational State that will be reported for this channel when its Current Value is TRUE.

Unavailable

If checked, inhibits paging of this Person within any Notification List to which he or she belongs.

Units

Are the measurement units in which the channel’s data are reported.

Up Button

Clicking this button moves the selected person up one position in the Notification List.

Up One Level

Moves the active directory up one level in the Windows hierarchy.

User Name

Identifies the current Foreseer User.

Value

Is the date and time a Date Channel state is True, triggering an alarm condition.

Verify Password

Is a security feature that requires a New Password be entered a second time in order to confirm changing it.
**View Menu**

The **View** menu allows the Foreseer Server display (primarily the *Tree View*) to be customized. The commands are much like those used in Windows Explorer.

You can enable/disable the Tool bar and / or Status Bar, adjust the Split bar between the left and right window panes and format the information displayed in the right pane as Small Icons, a List or show the Details for each item. All currently open Views also are listed, a check preceding the active display.

The **View** menu offers the following Foreseer commands:

- **Status Bar** - when checked, enables the Foreseer Server *Status bar*.
- **Split** - automatically selects the Windows splitter for a *Tree View*, allowing the relative size of the window pane displays to be changed.
- **List** - when checked, displays the icons in right pane of the *Tree View* as a continuous alphabetical list.
- **Details** - when checked, shows detailed information about the component selected in left pane of the *Tree View* on the right side of the display.

**WebViews**

WebViews represent the latest generation of Foreseer enterprise monitoring. The WebViews web editor is not a fully functional web interface, nor is it a drawing and design tool. Rather it is a bridge between server programming and graphic user interface design. WebViews allows you to custom design all aspects of your site through an extensive collection of drawing tools and view it through Microsoft Internet Explorer.

WebViews allows you to create as much complexity as you like without learning the intricacies of web design. The first thing to remember when starting any project is to plan. The more planning you do initially, the less trouble you will encounter during the course of the project.

**Creating WebViews Folders**

You can create WebViews folders and populate these with devices and channels. The following details 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.

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

**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 \Program Files (x86)\Eaton Corporation\Foreseeer\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*

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

1. 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.
2. Right-click the location for the page in the WebViews tree and select Templates → Create Page from Template.
3. 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.
4. Click Open.
5. 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.
6. 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.

7. When you’ve selected a device, click Create.

**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. 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).

3. Click Save.

4. Check files for Page

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

6. Check Files for Tree

**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 multi-select channels.

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

**Design Considerations**

The Foreseer editor is relatively simple to learn. A user with a basic background in web design and image creation software should be proficient on the software in less than a day. Keep in mind that you can create many of the assets that you need inside the WebViews, but some elements such as .jpg, .gif, .png, and flash components require additional software to create.

When beginning a WebViews design, it is important to know what you want to create: what equipment drivers and channels you will have to add to the Server so you have the correct data in place; and what folder structure you will have to create on the for a logical separation of data. Keep in mind that if you are going to create templates from the page, you must plan for future expansion and include the largest number of channels and other objects that will ever be placed in the pages.
Any pages that you create based on the template that have less than the maximum amount of data can have extraneous channels and objects deleted. By incorporating the maximum number of potential objects at the outset, you can anticipate potential problems and change the design as necessary rather than reworking it later.

**Page Layout**

The WebView Editor is a web layout program designed to allow users the ability to create data interfaces with little or no knowledge of web software. However, as with any layout, it is important to plan ahead and simplify the structure of the page to consider future maintenance. The best way to get started is with a pencil and paper. Initially, block out areas for object placement using squares with general text descriptions to identify the objects that will fill the space. Once you have the basic layout for the page, decide which objects should be grouped for easy editing. You may want to group objects like images together, or place all the user interface objects in one layer group. It is not important that you get the layout exactly right because as the project progresses changes inevitably will be made. But if you get the basic elements in place, future changes are much less time-consuming.

Remember that the WebView Editor is not a drawing program, so you can not create vector or raster art. You are also limited by the web browser paradigm. In other words, line objects created in the editor may be square, horizontal or vertical, but curves, diagonals or rounded corners can only be introduced by placed image objects.

**Layer Groups**

It is very important to plan layers for your pages. Because you may be adding many elements to a page, including some that overlap, you will want an easy way to select objects. One of the features of the WebViews Editor are the Layer Groups, which allow you to turn the editing capabilities of any object that exists in a specific Layer Group on and off. To take full advantage of this capability, you must plan which objects are going to be at the lowest Z-index and which are going to be at the highest Z-index (Z-index is a DHTML value that places an object nearer or farther from a view based on an assigned number). The WebViews Editor has eight predefined layer groups.

Using layer groups for similar objects will speed up editing and revisions. Each "layer" consists of ten Z-index levels. Objects may be positioned inside an editable layer group and still not be individually editable using the Edit Layer command. The added Z-index levels inside the layer groups allow the user to move objects forward and backward in space. This is very important when creating complex interfaces with many overlapping objects. You can have objects positioned on Z-index "10" and Z-index "19," but both are editable when you are editing Layer "1." Be sure to isolate objects that may be difficult to select into separate layer groups once the layout is complete. This will provide the designer with maximum selection flexibility.

The following are the default Z-index settings of objects newly inserted into a WebViews page:

- **Layer 1**
  - Z-index "10-19"
- **Layer 2**
  - Z-index "20-29"
- **Layer 3**
  - Z-index "30-39"
- **Layer 4**
  - Z-index "40-49"
- **Layer 5**
  - Z-index "50-59"
- **Layer 6**
  - Z-index "60-69"
- **Layer 7**
  - Z-index "70-79"
- **Layer 8**
  - Z-index "80-89"
The default Z-index can be changed by selecting the object, double-clicking and altering the Z-index field in the Properties dialog box to reflect the appropriate level. The level can also be changed by using the Alt+1-Alt+8 keys to choose the layer group where you would like the new object to be created. If you choose to import objects into a specific layer, the object will be placed in the middle layer of the group. For example, if you choose Layer 1 to be the active layer, the object you import will be placed on Z-index "15" in the middle of the Layer 1 group.

The following documents where new objects are placed in the Z-index hierarchy if you simply import the object without first defining the working layer. As you can see, most objects are placed at the same level and require the user to manually change the Z-index setting in the object's Properties dialog box.

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channels</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Folder</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Line</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Animated Image</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Static Image</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Text Object</td>
<td>&quot;50&quot;</td>
</tr>
<tr>
<td>Flash Object</td>
<td>&quot;89&quot;</td>
</tr>
<tr>
<td>Hyperlink</td>
<td>&quot;89&quot;</td>
</tr>
<tr>
<td>IO Control</td>
<td>&quot;89&quot;</td>
</tr>
</tbody>
</table>

Flash and I.O. Comp Controls are exceptions to Z-index levels. These two object types are always at the top of the Z-index hierarchy no matter what level you try to assign them. This is due to the nature of the controls themselves as they create a separate window in the browser that is above all other content. You will not be able to place any design elements above these two objects to create layered or transparency effects; thus, the Flash and I.O Comp Control objects must have elements stacked beneath them.

To make the best use of these layering, it is important to turn the layer editing function on as you bring elements into the page. For instance, if you want the background images isolated for easy selection, you might bring those objects in while you are editing only Layer "1" (Alt+1). This will place the objects in the middle of the group at Layer "15" and allow you to edit them independent of your other content.

Window Menu

The Window menu enables Foreseer Server displays. When active, each of these toggle commands is preceded by a check.

The Window menu offers the following Foreseer command:

Tree View - makes the Foreseer Server Tree View, which lists all configured channels hierarchically, the active screen.