IM02606006E

Administration White Papers Foreseer 6.3

Powering Business Worldwide

Administration White Papers: Foreseer 6.3

Publication date 12/07/15

Whitepapers in this Guide

Basic Foreseer Server Maintenance Instruction

By Drew Anderson

Foreseer Senior Technical Support

January 14, 2013

Summary – This document describes some of the basic tenets for maintaining the Foreseer Server after install is complete.

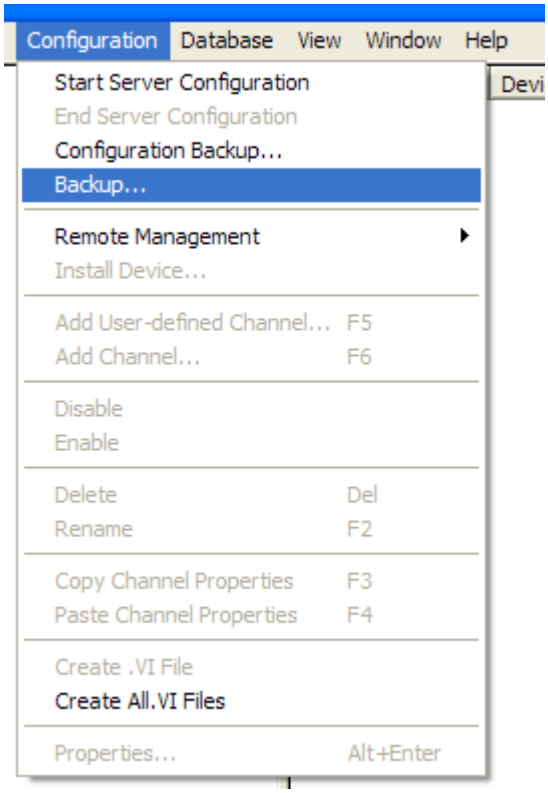
Foreseer App Affected –

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☒	Foreseer Web-Views				

Setting the Automatic Foreseer Server Configuration Backup – A Foreseer Server configuration backup (.arq file) contains all the essential information to restore the Foreseer Server to an as-is state (when the backup was created) in the event of a catastrophic failure. NOTE: the .arq file contains the information to restore the Foreseer Server, but does not restore data.

The Foreseer Server can be programmed to create configuration backups during a regularly scheduled interval. It is highly recommended that this be set up.

1. Open the Foreseer Server interface.
2. Click on the menu CONFIGURATION>BACKUP…



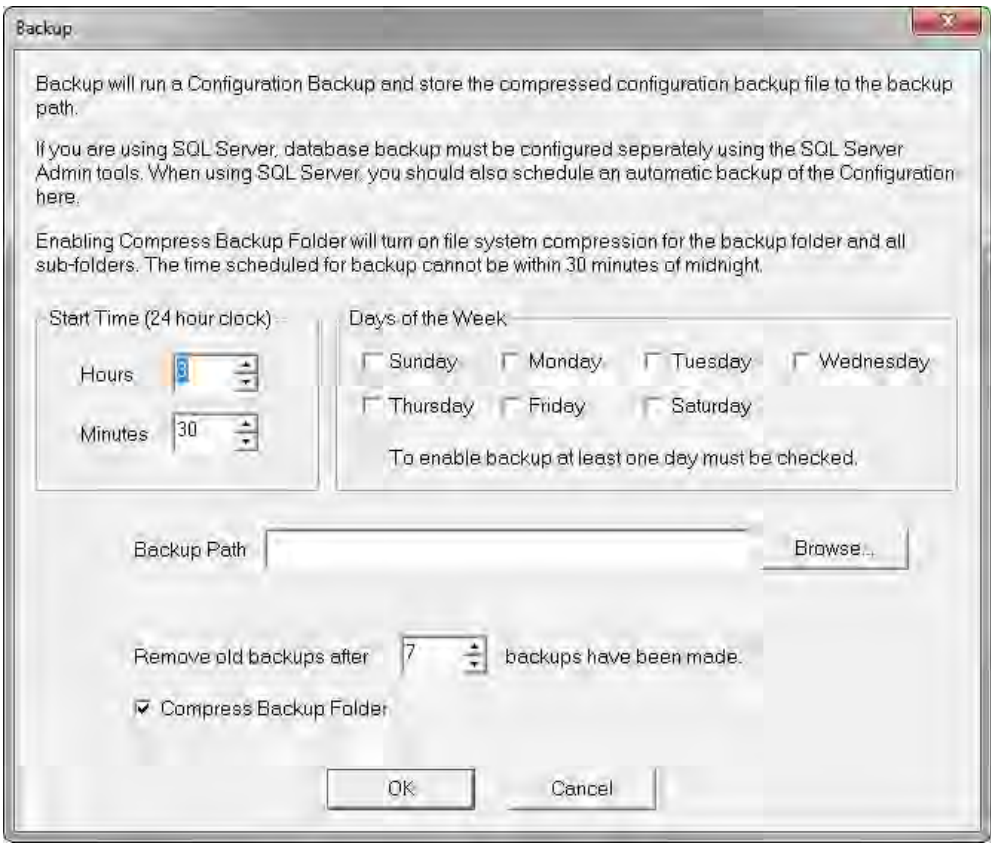
3. A configuration backup dialog box will show. Setting the automatic backup parameters involves four items that need to be configured.

    a. Start Time (24 hour clock) – This is the time, in 24-hour format, that Foreseer will initiate the configuration backup.

    b. Days of the Week – Select the day of the week the backup is to take place. It is recommended that all seven days be selected.

    c. Backup Path – This is the path where the backup (.arq) will be placed. This path can be local or remote on a shared network drive.

    d. Remove old backups after – Depending on the size of the Foreseer Server, backups can be very large (>100 mb). This setting will automatically delete the oldest configuration (FIFO – First In First Out).



Periodic Log File Review – The Foreseer Server log file report contains a large amount of data that provides information on items such as software and driver version levels, miscellaneous software messages, driver notes, and minor and major errors in the system. A new Foreseer log file is created each time the Foreseer Server is restarted as either an application or a service. Starting with version 5.1, a new log file can be initiated manually through WebConfig if the current log file is too big to be read thoroughly.

A lot of varying messages can be written to the log file. The messages are a good indicator of the general health of the Foreseer Server software as well as the field devices that Foreseer is communicating with. Entries do not necessarily mean that a problem is occurring.

A periodic review is a good idea. Primarily, entries that are of interest are those that begin with "ERROR" after the time and date header. Should any of these occur, provide the log file to Eaton/Foreseer Technical Support.

If Technical Support is Required – There may come a time when technical support for the Foreseer Server is required. There are some preliminary steps that can be taken to help the process along.

1. Be prepared to send the following to Foreseer Technical Support:

- Current Log File
- System Configuration
- Screenshots of the problem
- Point values from the actual device display (if a device on Foreseer is the issue)
- A wiretap of the device in question (if a device on Foreseer is the issue)

2. When you call Technical Support, most troubleshooting will be handled from the Foreseer Server system. Being at the server computer will greatly increase the troubleshooting capabilities during the call. Foreseer versions up to, and including, 5.0 will have to be done at the Server system. Foreseer versions 5.1 and higher can be done through a WebConfig interface if it has been configured per site preferences.

Technical Support Contact – The Technical Support Team can be contacted for non-emergency issues between 7AM and 5PM MST. Support for emergency issues (the Foreseer System is completely down) is available 24-7, 365 days a year for customers with an active service contract.

For all Foreseer Server software or Foreseer hardware technical support issues, call:

1-800-356-3292 option 8

Upon calling Technical Support, a service request number (SR) will be created and provided to you for future reference.

Recommendation for OS Maintenance

By Drew Anderson

Foreseer Senior Technical Support

January 14, 2013

Summary – Microsoft constantly releases updates and security patches for their supported operating systems (OS). This whitepaper is a statement of Eaton/Foreseer's recommendations of maintaining the Foreseer Server OS.

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☐	Foreseer Web-Views				

Operating System Affected –

☐	2000	☐	XP	☒	2003	☒	2008	☒	2008 r2
☒	32-bit	☒	64-bit						

Statement of Maintenance Recommendation – Eaton recommends that the Foreseer Server OS be maintained according to the end user's corporate policies. This includes all standard OS and critical security patches.

Recommended Preparatory Actions – Following are actions that are recommended to take prior to the application of any OS maintenance or security patch updates are applied to the Foreseer System.

1. A current Foreseer Server configuration backup needs to be made and stored off-server. Refer to the "Making a Foreseer Server Configuration Backup" whitepaper for instructions, if needed.
2. If possible, apply the update during a time when personnel will be available. This is in the case of a server or service failing to restart for any reason. This will reduce the downtime of the server to a minimum.
3. Ensure that a physical or soft copy of the latest Foreseer Server is available in the event the system needs to be rebuilt after an update failure.
4. If archived data is stored locally, it's recommended that a backup be made according to corporate database policies.

Making a Foreseer Server Configuration Backup

By Drew Anderson

Foreseer Senior Technical Support

July 22, 2009

Summary – Having a current, updated Foreseer Server configuration backup is vital to proper management of the Foreseer Server. A current backup would contain all the most recent changes made to the system There are two essential reasons for keeping a current backup –

Recovery from system failure

Provides Technical Support with a copy of your active system, which aids in diagnosis of various issues.

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☒	Foreseer Web-Views				

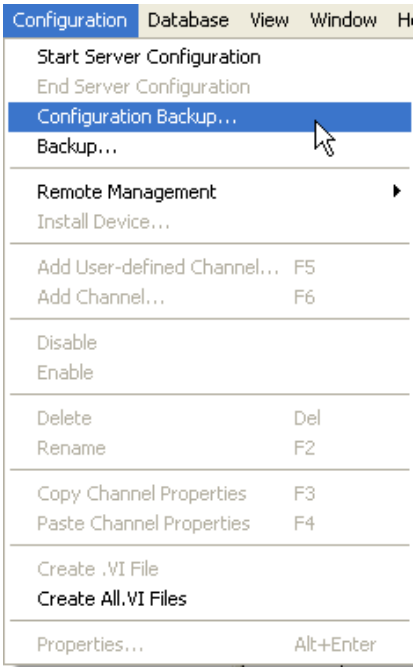
When to Make a Configuration Backup – First and foremost, make a configuration backup prior to making any changes on the Foreseer Server application. This would include device/channel name changes, setting alarm limits, making WebViews changes, and making any type of device communication parameter alterations.

After any changes are complete, another configuration backup should be processed. This ensures that those changes could be recovered in the event of a system failure. This would eliminate having to do the same changes over once more.

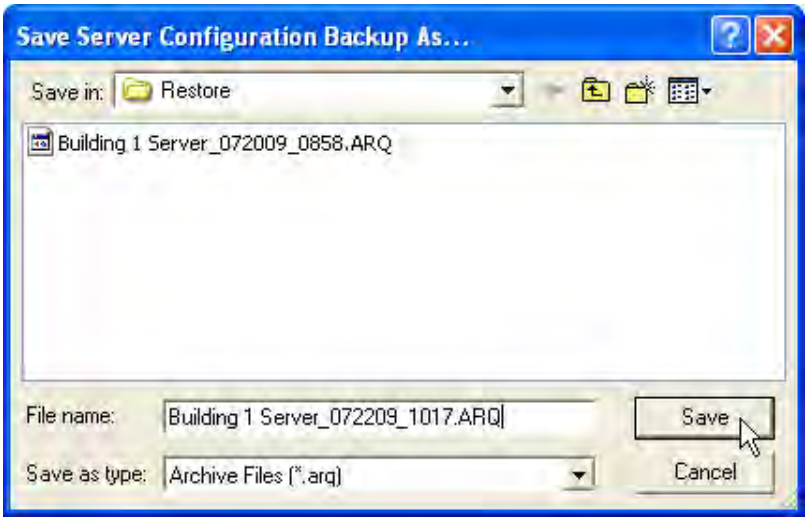
Beneath the SYSTEM CHANNEL device, in the Foreseer Server device tree, there is a channel called Configuration Backup. This channel will indicate if a backup is required. If the channel value is "Outdated," then perform a backup.

Making a Configuration Backup – Making a Foreseer Server configuration backup is a simple process.

1. In Foreseer Server, go to the menu CONFIGURATION and select CONFIGURATION BACKUP…



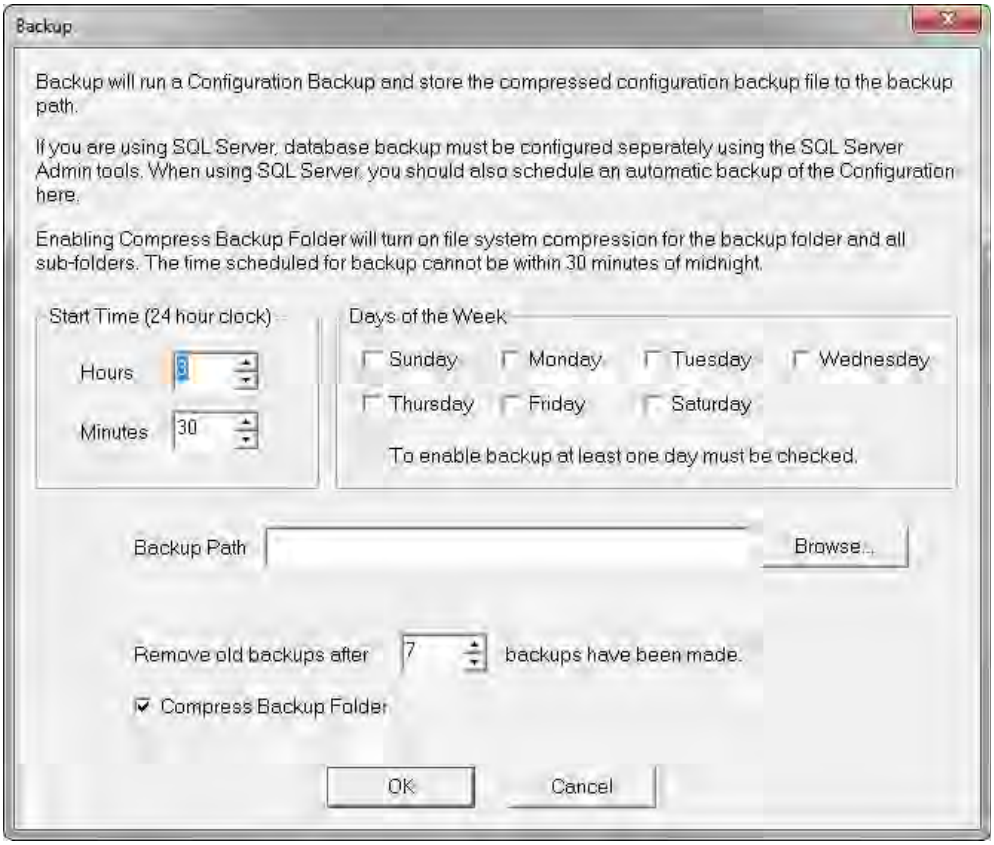
2. A standard Windows SAVE AS… dialog box will appear.
3. By default, the backup path is in the RESTORE folder in the Foreseer install path. You can browse to any functional path for the backup.
4. Give the backup a meaningful name. An example would be in the format of SERVERNAME_DATE_TIME. It would look like Facility1_072209_1546. The .arq extension will automatically be placed at the end.



5. Press the SAVE button. A message box will appear once the configuration backup is complete.

Automatic Configuration Backups – Foreseer Server can be configured to automatically create configuration backups. This should always be done, but should never take the place of a manual backup prior to making changes. Setting up the automatic configuration backup is a simple process.

1. Go to the menu CONFIGURATION and select BACKUP.
2. This will open a BACKUP dialog box.



3. Setting up the time and day of week options is self-explanatory. Hours are done in 24-hour format.
4. The Backup Path is a valid drive/folder path. The backup folder does not have to be local to the computer. A shared drive can be used.
5. Remove old backups is a setting to determine how many backups to keep in the backup folder. By default it is set to 7 and this works fine. A setting of less than 3 is not recommended. Backups are deleted in a FIFO – First In First Out – order.
6. There is an option to compress the backup folder, however, the .arq backup that is made is already highly compressed and will not compress further to any noticeable degree.
7. Press the OK button to save the settings.
8. At the set time and day, a new configuration backup will be created automatically.

NOTE: Even with the automatic backups configured, you will still want to be in the habit of manually creating backups prior to making any changes to the system.

Final Thought – The primary purpose of a configuration backup is for recovery after a system failure. That being said, it does not help to have a current configuration backup saved on the local drive if the local drive is what has failed. Once a backup is made, make a copy of the backup and store it on another drive.

Running a Wiretap on Foreseer Server

By Drew Anderson

Foreseer Senior Technical Support

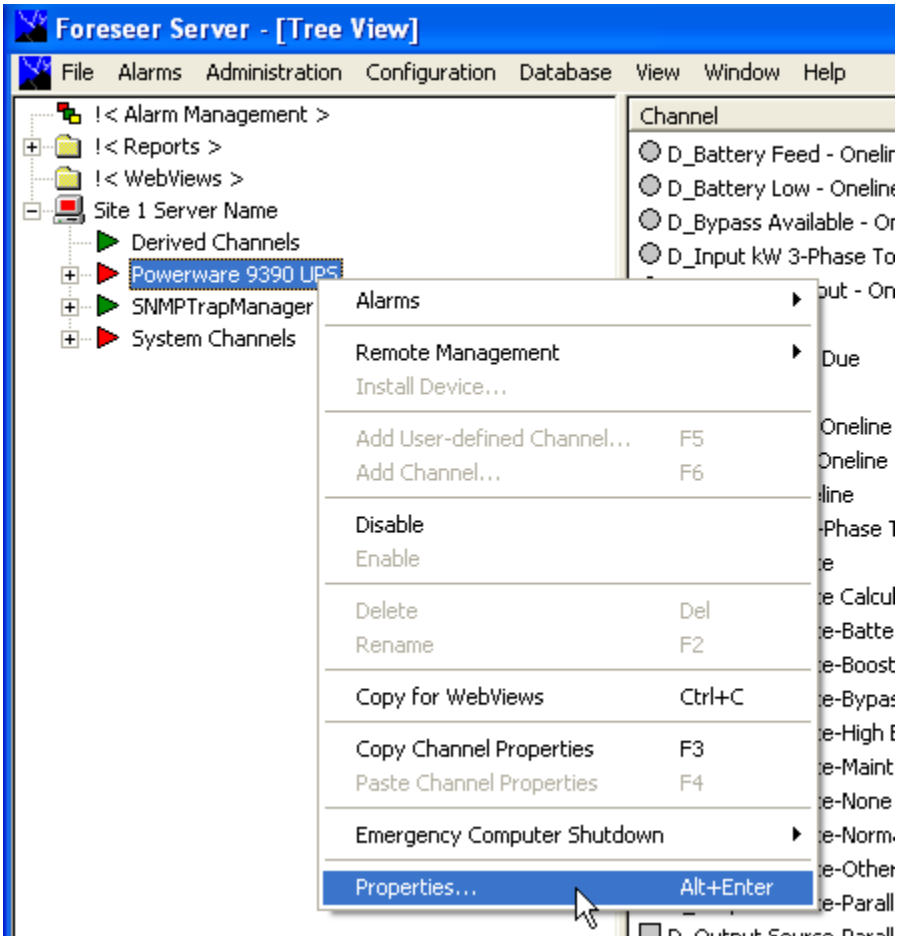
July 22, 2009

Summary – Foreseer communicates with most field devices through constant poll and response activity. Often times, as part of a troubleshooting situation, it is necessary to examine the communication traffic as it is occurring. A live capture of that traffic can be accomplished through the Wiretap function built in to the Foreseer Server.

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☒	Foreseer Web-Views				

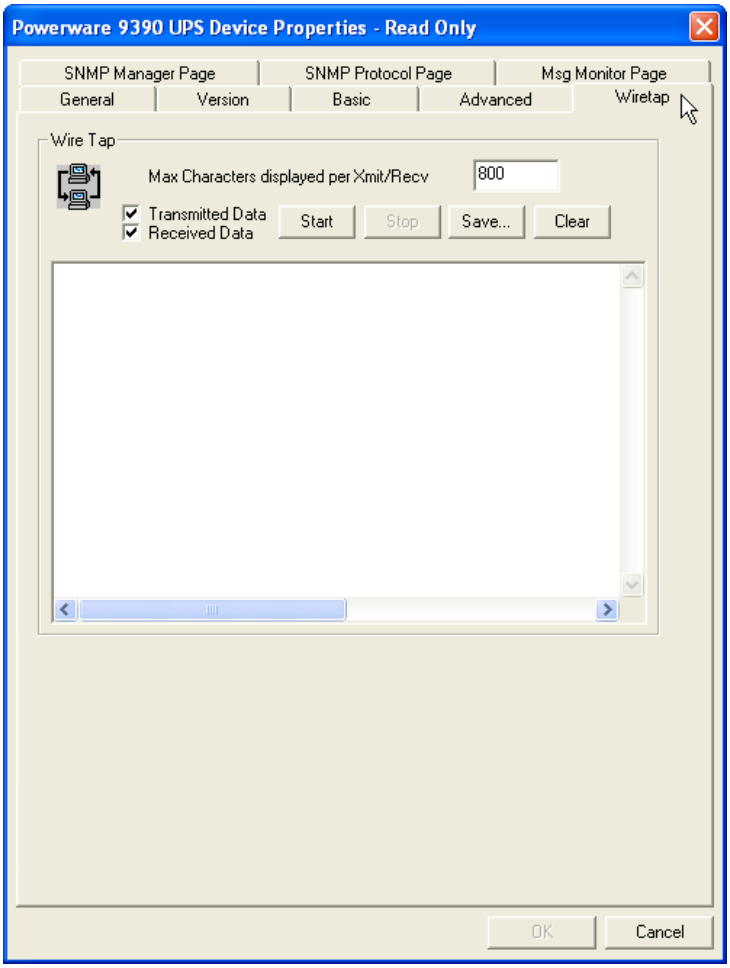
Running the Wiretap – Wiretaps can only be run through the Foreseer Server application. Wiretaps cannot be obtained through either the Foreseer Client or Foreseer WebViews interface.

1. If the Foreseer Server is running as an application, you'll see it on the task bar. If it is started as a service, the Foreseer Server icon will be present in the system tray by the clock. Bring up the Foreseer Server using the respective method.
2. If it is not already expanded, expand the device tree. The device tree is located beneath the site server name.
3. Locate the device to be wiretapped in the device tree. Right-click and select PROPERTIES in the pop-up menu.

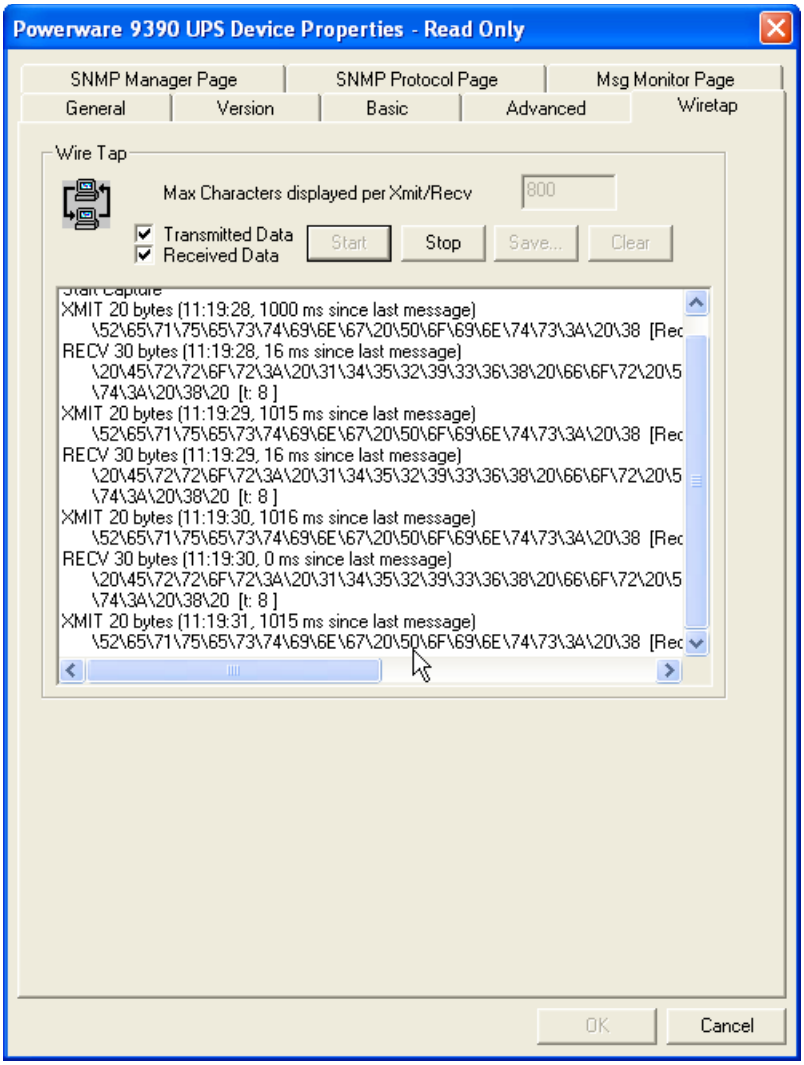


4. The device's associated properties box will open. Note: device property appearance will vary dependent on the device type. Several tabs will be identical, but more tabs may be distinctive only to that device type.

5. Click on the WIRETAP tab.



6. To start the wiretap, press the START button. The main text box on the window should start displaying text. Note: if the device is on a string with multiple devices, you may not see text right away as the communications works its way through the string.



1. Allow the wiretap to run for a minimum of 60 seconds (1 minute).
2. Press the STOP button.
3. Press the SAVE button. A standard Windows Save dialog box will open (regardless of whether the wiretap is run from a main server computer or a DAE). Give the wiretap a distinctive name. For example: Powerware UPS CA-1B Wiretap.txt.
4. Make note of where the file is saved as Foreseer Technical Support will need to view the actual file for proper troubleshooting.
5. Press the CANCEL button to close the properties dialog box.

Misc. – When viewing a wiretap, XMIT is the poll going from Foreseer to the respective device. RECV is the response of the device. Even if 0 bytes are being received, viewing the wiretap can be useful as the wiretap header (not visible in the main wiretap window but in the saved file) can provide useful information, such as .dll and .vi version information.

Wiretaps can only be done at the device level. They cannot be done at the channel level. When you open the properties dialog box, the title should include the device name as well as "Device Properties – Read Only". If the dialog box includes the \\Server Name\Device Name\Channel Name, as well as the tabs General, Basic, and Advanced (as shown below), then your at the channel level and not at the device.

Understanding the Basics of Comtrol DeviceMaster and Moxa NPort Port Configurations for Troubleshooting

By Drew Anderson

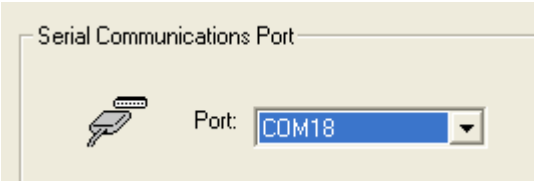
Foreseer Senior Technical Support

August 20, 2009

Summary – All serial communication devices connected to Foreseer must use some type of serial port. Since the majority of computers only provide one or maybe two ports, additional ports must be configured. The Foreseer system architecture uses either Comtrol DeviceMaster RTS or the new Moxa Nport 6650 series devices to create the additional ports necessary. Understanding how these ports are setup and mapped out will make your understanding of the Foreseer Server communication paradigms much more clear. This will also make any type of troubleshooting easier when it requires possibly moving a device string from one port to another.

☒	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☐	Foreseer Web-Views				

General Theory – If you were to access the properties of any serial device installed on Foreseer, you'd see that the devices is installed to a particular COM port.



In Foreseer, devices can be installed on COM port 1 all the way to COM 1024, if that many ports have been installed. Running a System Configuration report will also provide the COM port information for all installed devices.

```
Entes IO A Meter 2              Unit: 1     COM18, 9600, 8, none, 1        Online
                                            Serial
            Driver File: vi\4-Modbus3.dll
            Driver Version: 4, 3, 402, 0
            Common Library Version: 4.1.16.0
            Vi File: 4-Entes IO A Meter.vi
            Vi File Version: r.0.0
```

Both the Comtrol DeviceMaster and the Moxa Nport 6650 devices can provide multiple port count additions to the computer system. These include 1, 2, 4, 8, 16, and 32 port units. Eaton/Foreseer specs only two of these – 8 and 16 – but supports all port count configurations.

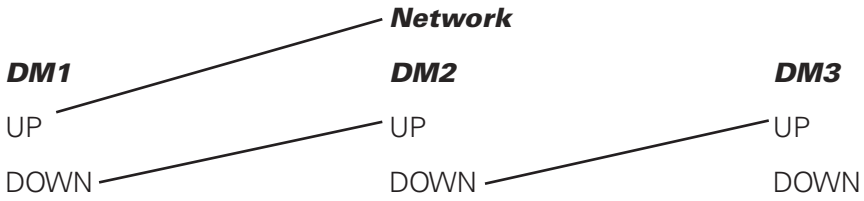
When viewing the back of the DeviceMasters or the Nport 6650, you'll notice that there are several RJ45 connections.

Comtrol DeviceMaster 16-port

One each of the units, there are two Ethernet ports and 16 serial ports.

On the back of the DeviceMaster, the two Ethernet ports are labeled "UP" and "DOWN." A standard network patch cable from a switch, router, hub, or any network port would connect to the UP connection. The DOWN is used to connect additional DeviceMasters (or Moxa units) when there are limited number of network ports available.

To chain multiple DeviceMasters through the UP/DOWN ports, you would patch them together as such:



The Console port on the Moxa is for an alternate programming method which is not covered under this White Paper.

The ports on the Moxa are numbered 1 – 16 from left to right.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

The ports on the Comtrol are number 1 – 16 top to bottom, left to right.

1	3	5	7	9	11	13	15
2	4	6	8	10	12	14	16

Now, here comes the tricky part. Up to four ports may be taken internally by the computer system. Because of that, it is standard Foreseer practice to offset the COM numbers on both Comtrol DeviceMaster and Moxa Nport units by 5. The table below, diagrams out how that would be done. This is the setup for two units.

	Physical Port	Foreseer COM
Unit 1	1	5
	2	6
	3	7
	4	8
	5	9
	6	10
	7	11
	8	12
	9	13
	10	14
	11	15
	12	16
	13	17
	14	18
	15	19
	16	20

	Physical Port	Foreseer COM
Unit 2	1	21
	2	22
	3	23
	4	24
	5	25
	6	26
	7	27
	8	28
	9	29
	10	30
	11	31
	12	32
	13	33
	14	34
	15	35
	16	36

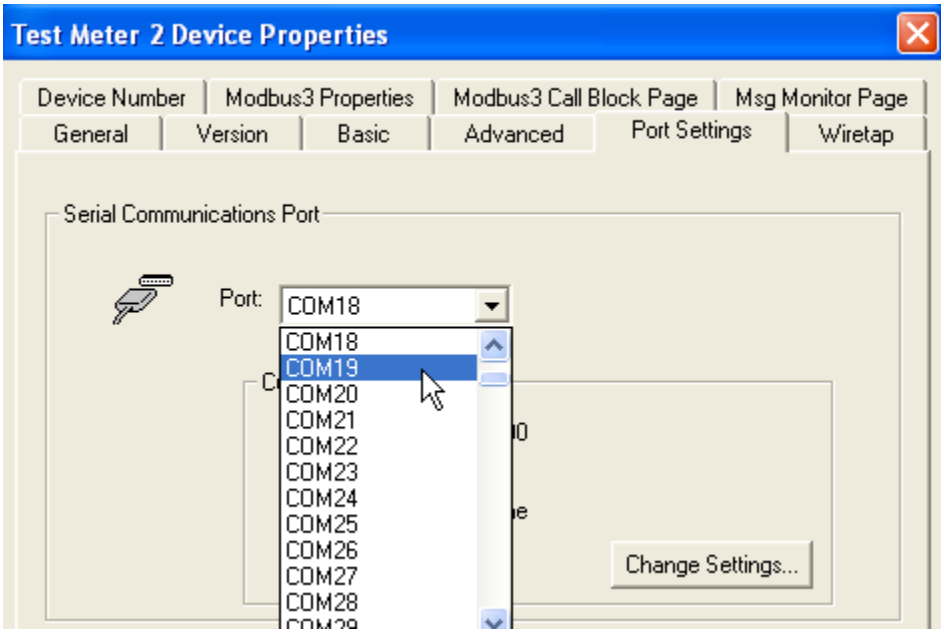
Notice that while the physical ports on the Comtrol/Moxa unit will always be 1 -16, the associated Foreseer COM port will continue to increase by the respective number of ports. If a third 8-port unit was added, the Foreseer COM ports would be 37-44.

Keep these offsets in mind when working in Foreseer and looking at the PORT setting in a device's property on Foreseer Server. If the PORT is COM18, then that device would be physically connected to port 14 on the first unit.

Swapping Ports When Troubleshooting – Whether you have a single device connected to a port that is offline or if you have a string of multiple devices offline, one of the best methods to isolate the problem is to move the problematic string to an alternate port. This is easiest to do when spare ports are available but can be accomplished even when all ports are being used.

Let's start by assuming that there is a spare port available on the Comtrol/Moxa unit.

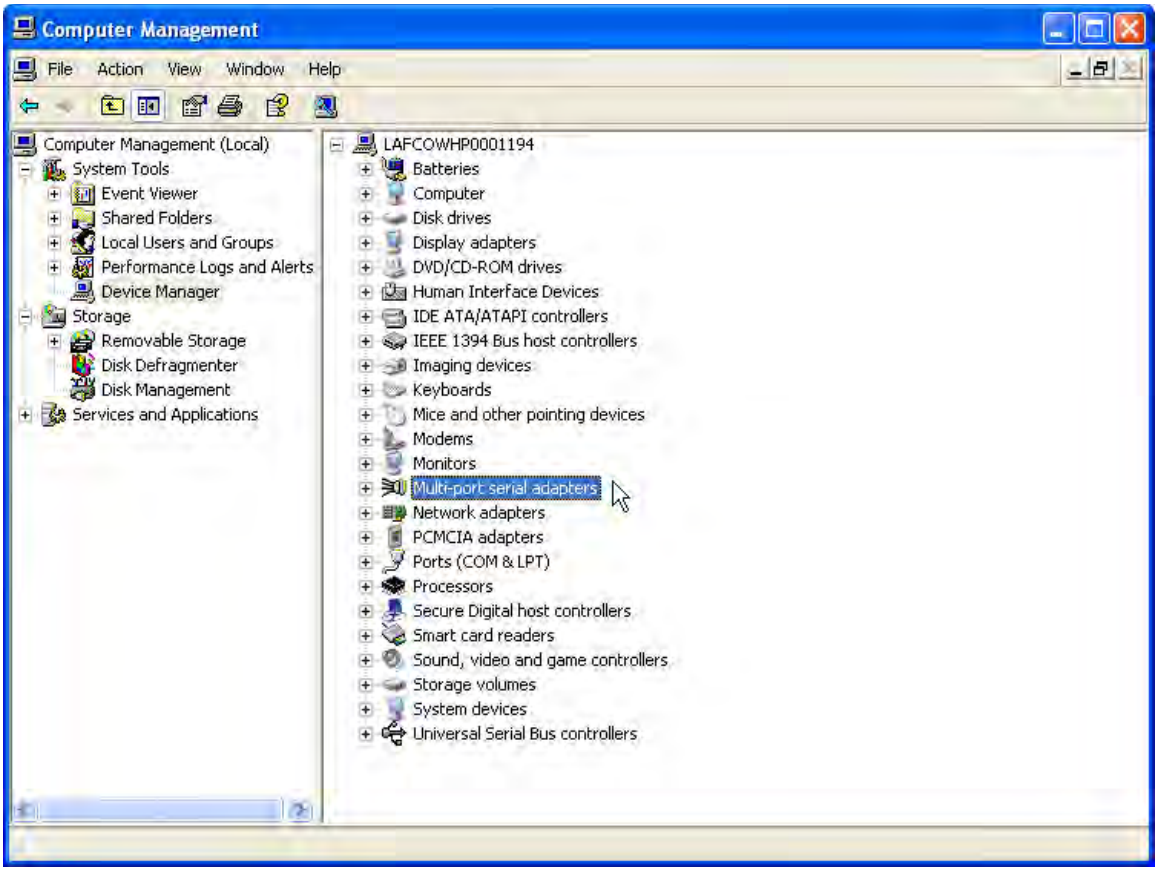
1. Determine the physical spare port number and convert it to what the COM setting in Foreseer will be. If the spare port is port 15 on the unit, then the Foreseer COM port that you will use is COM19. Use the table above to help determine the port assignments.
2. Disable the device in Foreseer Server.
    - Right-click on the device and select DISABLE from the pop-up menu.
3. Access the device's properties and go to the PORT SETTINGS tab.
    - Right-click on the device and select PROPERTIES from the pop-up menu.
4. Using the Port: drop-down box, find COM19 and click on it.



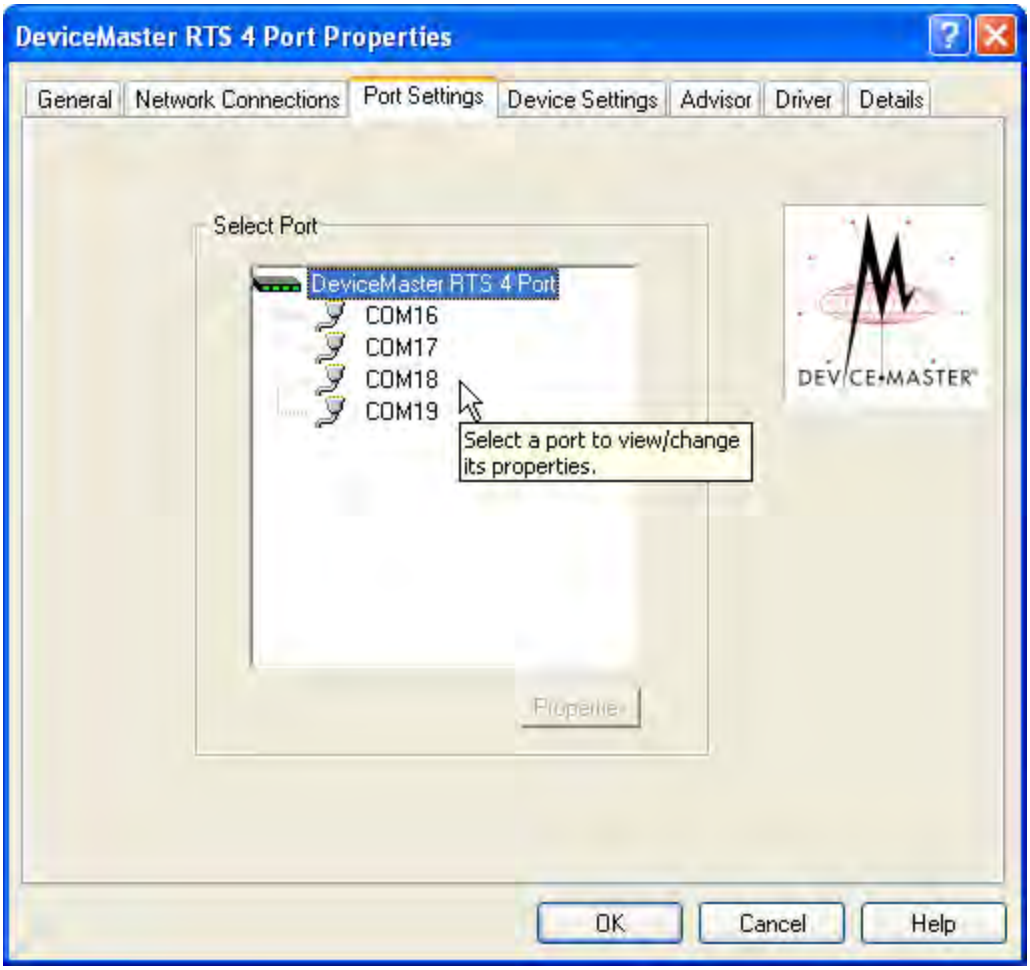
5. Press the OK button to save and close the properties box.
6. Physically move the cable from its current port to port 15 on the back up the Comtrol/Moxa.
7. Re-enable the device in Foreseer.
8. Right-click on the device and select ENABLE in the pop-up menu.
9. Minimize all open windows so you can see the computer's desktop.

For Comtrol DeviceMasters

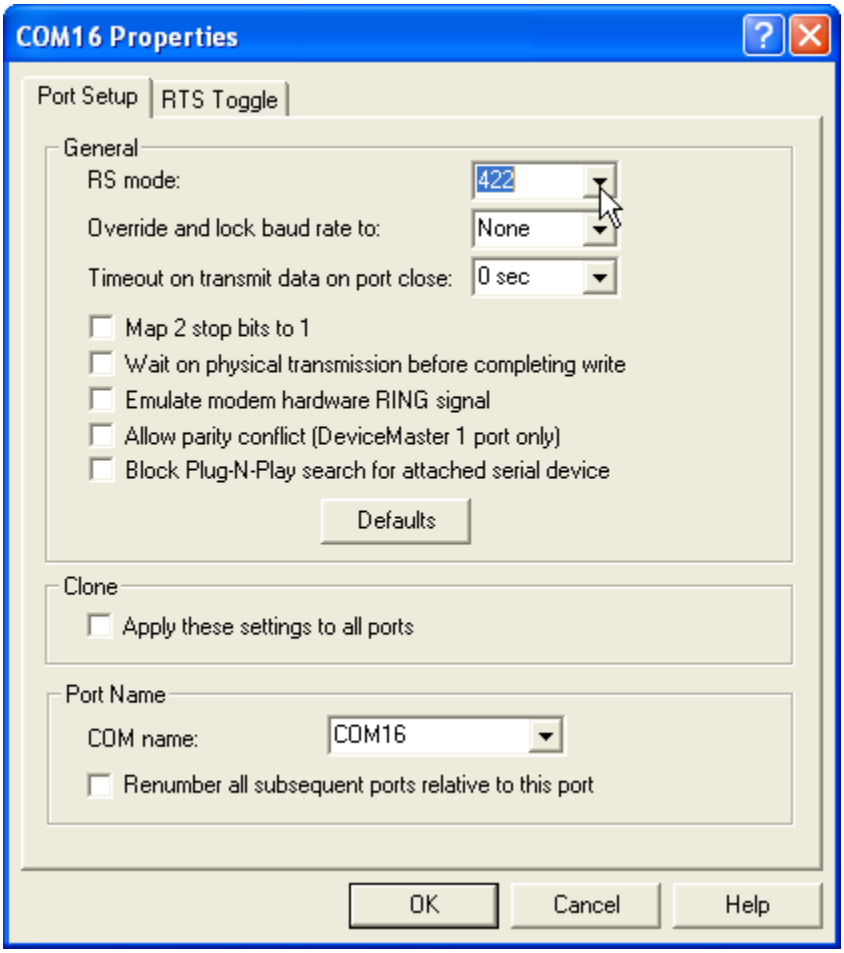
1. Right-click on the My Computer icon and select MANAGE from the pop-up menu. This will open the Computer Management window.
2. In the left split window, find and single-click on Device Manager. This will list out the installed hardware devices on the computer.



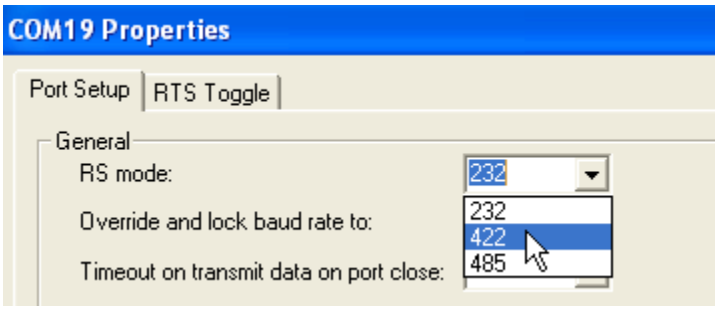
3. Locate Multi-port serial adaptors in the list and expand by pressing the "+".
4. Select the DeviceMaster that has the ports you need to work with. This is simple enough if you have only once installed. But if you have multiple DeviceMasters installed, you'll need to do some searching to find the unit you need.
5. Double-click on the unit in the Multi-port serial adapter list. This will open the properties of that specific unit.
6. Go to the Port Settings tab. This tab will list out all the ports on that specific unit. NOTE: These ports will be enumerated to match what is in Foreseer. So COM16 on the list will be COM16 in Foreseer. However, in the example shown below, since there are only four ports installed, COM16 to COM19 correspond to physical ports 1 – 4 on the back of the unit.



7. Single-click highlight the original COM port and press the PROPERTIES button.



8. Take note of the RS mode selection at the top of the properties dialog. On standard systems, all other options remain at default. Press the OK button to close this window.
9. Now single-click highlight the new COM port and press the PROPERTIES button.
10. Set the RS Mode to match that of the original COM port.



11. Press the OK button to save the setting change. You'll receive a warning about disconnecting hardware. Nothing needs to be done. Press the OK button.

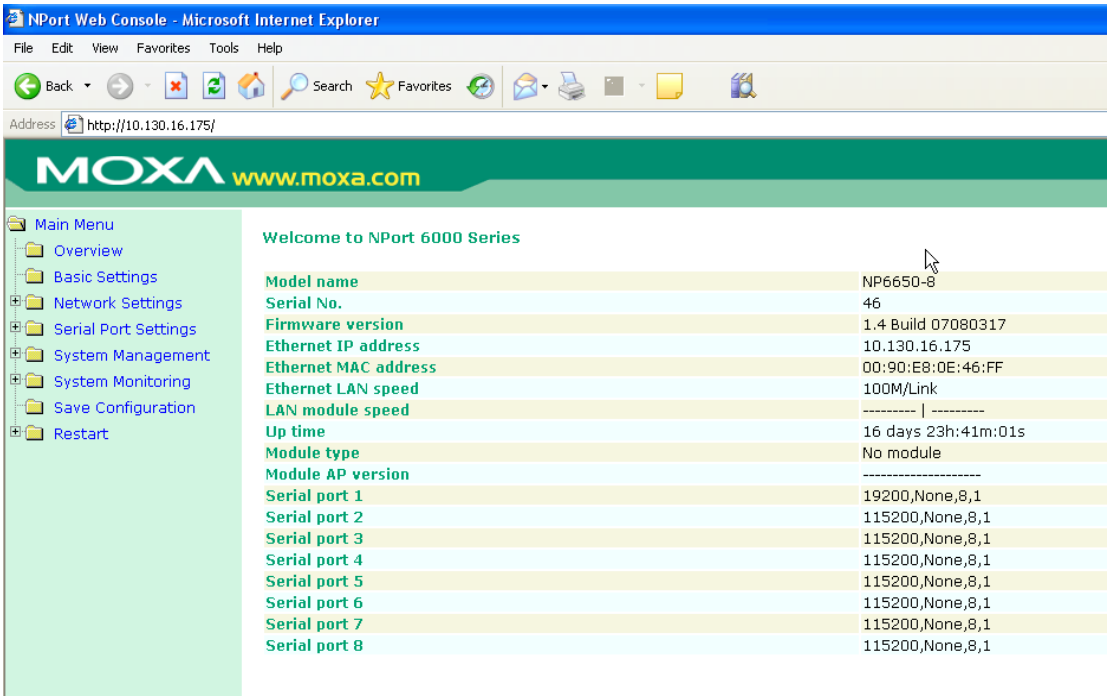
12. While it isn't always necessary, it's a good habit to power cycle the DeviceMaster after making changes to port settings. Power cycling can be performed one of two ways: remotely through the webpage or physically unplugging/plugging in the unit.

After the changes, evaluate the communication state of the device or device string. If the device is now online, then a bad port has been identified. If the device remains offline, and all settings have been properly adjusted, then you'll need to start looking at alternate possibilities for failure, such as the device itself, cabling, or converters.

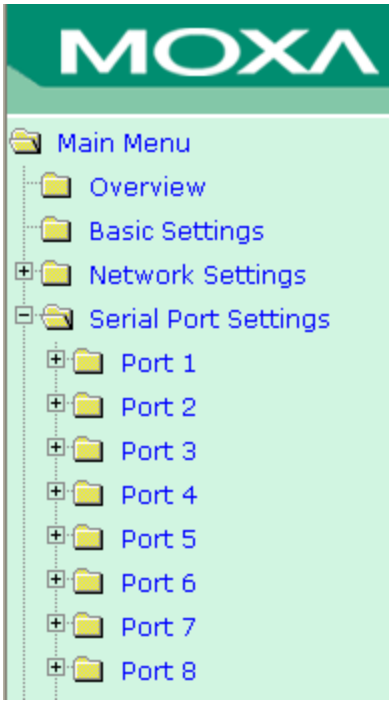
For Moxa Nport

Similar to DeviceMasters, when moving cables around, individual ports need to set up to match. Unlike DeviceMasters, which hold their settings local to the Foreseer Server computer, Moxa Nports keep their settings on the Nport unit.

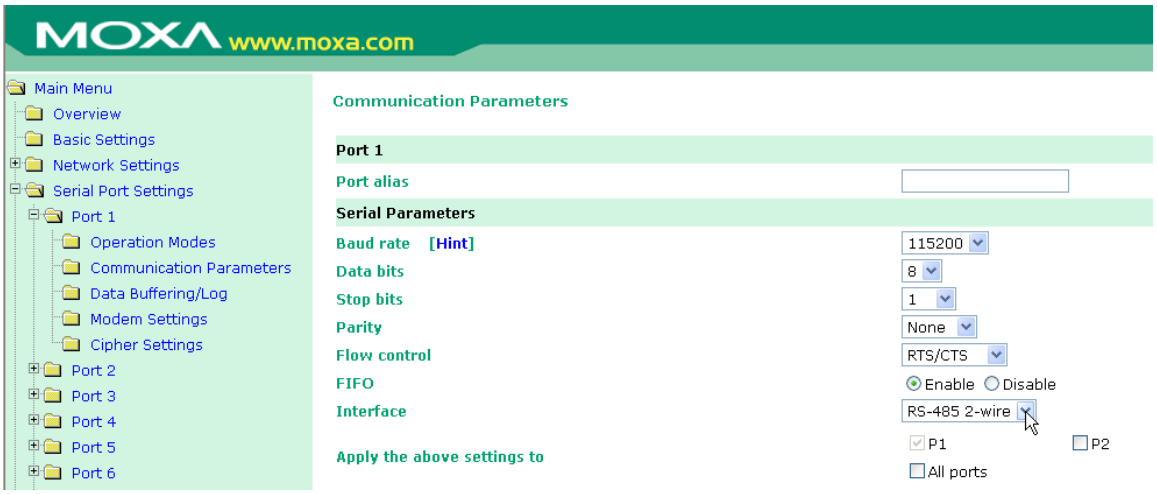
1. Open an internet browser window (IE, Firefox, Opera) and direct the URL to the IP address of the Moxa Nport.
2. Older units will log directly to the Moxa webpage, newer units will prompt for a password. The default user/password is admin/no password.
3. The Moxa unit homepage will open.



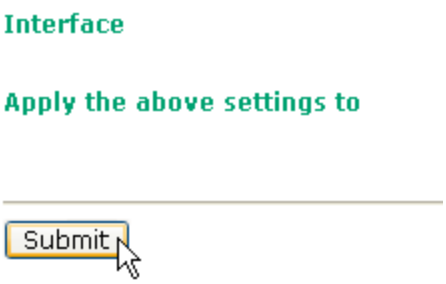
4. Navigation is done through the menu on the left. To modify ports, expand out the Serial Port Settings menu. The number of ports you'll see may vary depending on the specific port count of your unit.



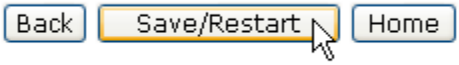
5. Unlike the DeviceMaster which offers continuously enumerated ports, each Moxa webpage for your unit(s) will always start at Port 1. Using the mapping described in the General Theory section, locate the corresponding port the device string is currently plugged into.
6. Expand the port properties by clicking on the "+".
7. Click on Communications Parameter.
8. Take note of the Interface setting the port is currently set to.



9. Now go to the spare Moxa port that you will be moving the string to. In Communication Parameters, match the Interface setting. In most standard setups, all other settings will remain at default.
10. The Moxa Nport will need to be rebooted to save and load the setting change. Click on the SUBMIT button below the settings.



11. A new window will open. Click on the SAVE/RESTART button. This will restart the Moxa Nport. The restart will take approximately 30 seconds.



After the restart, through the Foreseer Server, validate the communication status of the device. Did the problem follow the device string or stay with the port.

Final Notes

The steps above are for basic troubleshooting only. Integrated systems may take on any level of complexity depending on the device type and protocol and the number of devices on a string. Every device type behaves differently from every other device, but the same troubleshooting tips apply. The steps above are one of the basic steps taken to help isolate an issue and track down the cause.

If you require further assistance, call Eaton/Foreseer Technical Support at 1-800-356-3892 option 8.

Updating Foreseer Device Drivers (.dll's)

By Drew Anderson

Foreseer Senior Technical Support

Summary – Foreseer Server device drivers (.dll's) are periodically revised with changes that may necessitate updating the existing files on an active Foreseer Server. The process is simple and safe when the specified instructions are followed. When working with Technical Support, the engineers may review your driver levels and put together a zipped file containing the updated drivers for your system. This white paper lays out the process for updating Foreseer Server device drivers.

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☐	Foreseer Web-Views				

Update Steps –

1. Download the zipped file provided by Foreseer Technical Support.
2. Make a Foreseer Server configuration backup (.arq).
   - Menu CONFIGURATION>CONFIGURATION BACKUP…
3. Run a System Configuration report for possible reference later.
   - The report can be run from either WebViews, the Foreseer Web Configuration utility, or from Foreseer Server, which ever works best for you.
4. Make note of any offline devices prior to the update.
5. Locate the Foreseer Server install path in Windows Explorer. If you're unsure of where the application is installed, view a log file report. In the first few lines of the report, the path for Foreseer will be shown.
6. Shutdown the Foreseer Server application (stop the Foreseer Server service if running as a service).
7. Once you locate the install path, go into the VI folder.
8. In the VI folder, create a new sub-folder called "Old Drivers" if it does not already exist.
9. Copy ALL files with the .dll extension into the Old Drivers folder.
10. Extract the .dll files from the zipped file provided by Technical Support into the VI folder. You should receive a prompt to overwrite the existing files.
11. Once all the files are extracted to the VI folder, restart Foreseer Server.
12. Verify that all devices that were communicating prior to the update come online with the new drivers. If the device fails to come online, that was online prior to the update, contact Technical Support. Be prepared to provide

a Log File report, the System Configuration Report created in Step 3, and a new System Configuration report for comparison.

13. Create a new Foreseer Server configuration backup. This backup will contain the newest drivers.

Notes –

1. Should any type of error occur during the update process, there are two safeguards in place to help recover the system.
    - If a new driver creates a problem, by keeping the existing drivers in a separate folder, we can quickly and easily restore the previous version of the driver. This is the easiest process and usually resolves any error the updated driver might cause until it can be further investigated.
    - The second safeguard is the Foreseer Server configuration backup that was created in Step 2. Having this backup can be used to restore the system to the state it was in prior to the update.
2. For any assistance or additional details about the process, please contact Eaton/Foreseer Technical Support at 800-365-3292 option 8.

Emergency Preparedness and Your Foreseer Server System

By Drew Anderson

Foreseer Senior Technical Support

Summary – Blizzards, hurricanes, thunderstorms, earthquakes and other natural or manmade disasters are going to occur. It is vital for facility management to have a monitoring system that stays functional during those times or can be recovered to a functional state quickly in the event that damage does happen. This document details some considerations and steps to take in order to prepare the Foreseer Server for a possible emergency situation.

Foreseer App Affected –

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☐	Foreseer Web-Views				

Items One and Two: Software and Backups – In the event of a major system failure, two items will make it easier to restore the Foreseer System to a functional state. Item one is the Foreseer Server software. The second is a current Foreseer Server configuration backup. With these two items, the Foreseer Server can be installed and restored in a matter of minutes.

The Foreseer Server software should be stored in a location that protects the media from damage and can be easily found when needed. If you do not have your Foreseer media, contact Eaton-Foreseer Technical Support and you will be assisted in obtaining replacement media. Technical Supports contact information is on the title page of this document.

Not having a current Foreseer Server configuration backup (.arq file) can take the process of restoring a functional system from a few minutes to hours or even weeks. Always keep a current .arq on both the Foreseer system CPU and off the CPU on media that can be stored away from damaging elements and recovered quickly. Whitepapers are available if you're unfamiliar with creating a Foreseer Server configuration backup.

Emergency Power – The Foreseer Server and its peripheral hardware (DeviceMasters, Moxas, network switches, converters) will provide little benefit if they are not placed on UPS power. If the power on any of the listed components fails, the monitoring for that portion of the system is gone. Always have all critical components of the Foreseer Server on UPS power to ensure that it stays functional during a power outage but as long as emergency power is available to the facility.

Peripheral Hardware (DeviceMasters and Moxa NPorts) – Like the Foreseer Server, there is programming required for both the Comtrol DeviceMasters and the Moxa NPort Device Servers.

Settings for the Comtrol DeviceMasters need to be recorded by hand. The setting are available through COMPUTER MANAGEMENT>DEVICE MANAGER>MULTIPORT SERIAL ADAPTERS. Information that will be required to set up these peripheral devices on a replacement system includes:

1. Unit IP Address, Subnet Mask, Default Gateway
2. Number of ports on the unit
3. Port listing (Com5, Com6… Com20, etc)
4. RS mode for the port (RS232, RS422, RS485)
5. Any special baud rate overrides that are set for that specific port.

Settings for the Moxa NPorts can be exported through the unit's webpage (whitepaper: Exporting and Importing a Moxa Configuration File.pdf). The exported files, as with the backups from the system, are best kept in a safe location where they can be recovered and restored quickly.

Review of Current Device Communication States – Run a System Configuration Report. The report will be a snapshot of the current state of all devices installed on the Foreseer Server. It's beneficial to keep the report on hand so in the event that the system needs to be recovered, you have an accurate record of device communication states. This will prevent needless troubleshooting for an offline device when the state existed previously.

Naturally, you will want to correct all offline devices prior to an emergency situation. However, the offline state may exist for any number of logical reasons: device is turned off or disabled for maintenance, some hardware component within the communication string or on the device has failed, etc.

Miscellaneous – A few last items that should be kept on hand include:

1. A drawing package of the Foreseer Server System and its peripherals.
2. A list of all IP addresses of all the components of the system.
3. A list of configured Windows OS groups that begin with "PXS".
4. A list of users within any configured PXS groups.
5. A record of any message management settings.
    a. Services information
    b. Subscriber information
    c. Notification list setup

Eaton/Foreseer Server Recovery Procedures and Timeline Considerations

By Drew Anderson

Foreseer Senior Technical Support

Summary – As with any computer system, there is always a possibility of hardware and/or software failure. This document covers the procedures and timeline considerations should the Foreseer Server hardware/software fail for whatever reason.

☐	Foreseer Server V2	☒	Foreseer Server V4.0	☒	Foreseer Server V5.0
		☒	Foreseer Server V4.1	☒	Foreseer Server V5.1
		☒	Foreseer Server V4.3	☒	Foreseer Server V5.2
☒	Foreseer Server V6				
☐	Foreseer Thick Client V2				
☐	Foreseer Thick Client V4				
☒	Foreseer Web-Views				

Foreseer Server Hardware Failure (Foreseer only) – There are two parts to this possible issue. The Foreseer Server application is loaded on one system and the SQL database that Foreseer archives data to is loaded on another system. This section will cover restoring Foreseer to working order in the event of a CPU failure. The steps covered will provide the basic information needed to restore the system. If more information is required, please contact the technical support number on the coversheet. This section assumes that a functioning replacement CPU with an OS loaded has been supplied.

1. Install and configure the Moxa NPort 6650 and/or Comtrol DeviceMaster device servers.
   - Time required: 1 to 4 hours
2. Install the Foreseer Server software
   - Time required: 15 minutes
3. Restore a Foreseer Server configuration backup
   - When prompted to reconnect to a database or start new, select <YES> to reconnect to the existing database.
   - Time required: 10 minutes
4. Reestablish communications with all devices
   - Time required: 10 minutes to ? (Assuming that all the devices were online prior to the hardware failure and that the Moxa and/or Comtrol device servers are configured correctly, this step may take a very short period of time.
5. Reestablish connection back to the database
   - Time Required: 10 minutes

What is required prior to an event?

1. A Foreseer Server configuration (.arq) kept in a safe location off system.
2. Notes on all configuration settings for the Moxa and/or Comtrol device servers.
    - Moxa –
        * IP addresses of each unit
        * Port counts of each unit (1, 2, 4, 8, or 16 ports)
        * Port and Foreseer comm port associations (for example: port 5 on the Moxa unit corresponds to Foreseer comm port 9).
        * Exported configuration text file from each Moxa NPort unit
        * Access to the Moxa NPort Windows Driver Manager software
    - Comtrol –
        * IP addresses of each unit
        * Port counts of each unit (1, 2, 4, 8, or 16 ports)
        * Port and Foreseer comm port associations (for example: port 5 on the Moxa unit corresponds to Foreseer comm port 9).
        * Access to the Comtrol DeviceMaster RTS driver
3. Current System Configuration Report – The system config report details:
    - Device Names
    - Drivers and driver versions
    - Unit ID's, IP addresses, comm parameters
    - Device communication states at the time the report was run.
4. Listing of created PXS groups and users.

SQL Server Hardware Failure (SQL only) – Should a SQL server computer go down, there are some steps that can be followed to get it back online. Make note, Foreseer does not require the SQL server to be online to maintain monitoring. If the SQL server is down, Foreseer will continue to pull data from the devices and display it. It will not, however, archive the data. A gap in the data will occur for the duration that the SQL system is down. This procedure assumes that the databases are being backed up according to corporate policy and that a SQL dba is available to restore the databases in the event a new CPU is installed or everything has to be reinstalled.

1. Review the SQL Server Properties in the Foreseer Server for SQL server connection string (IP address or computer name), the use of either a SQL Administrator (sa) or user access account, and any non-default drives folders for data storage.
    - Time required: 10 minutes
2. Install SQL per corporate standards, keeping the following Foreseer requirement in mind:
    - Mixed mode required
    - Time required: 1-2 hours

3. Using the information gathered from Foreseer SQL Server properties, create folders specified in the data and log file path settings. If the settings in Foreseer were left blank, nothing will need to be done.

    - Time required: 10 minutes

4. Restore the active databases for the time period. If you need help determining which databases are the active databases, contact Foreseer Technical Support at the number on the coversheet.

    - Time required: 1-2 hours

5. Restart the Foreseer database session. If problems occur, contact Foreseer Technical Support.

    - Time required: <10 minutes

6. After the database is successful connected with Foreseer, copy over the remaining databases.

    - Time required: >1 hour (extremely dependent on the number and sizes of the databases)

Foreseer Software Corruption – Should the Foreseer software install become corrupt or unusable for whatever reason, recovery is basic.

1. Using the Foreseer Server install disk, reinstall the software. The Foreseer install wizard will guide you through a basic install process. If Foreseer remains installed from the previous instance, the install .msi application will provide the option to repair or remove the install. Select repair.

    - Repairing, or even completely reinstalling over the original install, only affects the runtime files. The files containing any customization (WebViews, server configuration, etc) will not be overwritten.

    - The Foreseer configuration files are NOT backwards compatible. You will need to install the same version (or higher). Right-clicking on the Foreseer.exe file under the root install folder, selecting PROPERTIES, and then clicking on the VERSION tab will provide information on the currently installed version.

    - If you do not have the Foreseer Server install software, contact Technical Support. Be prepared to provide the currently installed version.

    - Time required: 10 minutes

Contacting Foreseer Server Software Support

By Drew Anderson

Foreseer Senior Technical Support

Summary – The details below provide some direction for contacting Foreseer Server Software Technical Support.

Hours of Operation – Eaton Corporation Foreseer Technical Support will be available to receive calls number between the hours of 8am and 5pm MST, Monday through Friday.

All after-hours and weekend emergency calls will be responded to by phone within two (2) hours of the initiated call. Emergency after-hour calls are for system failures (the Foreseer monitoring system has failed due to the following conditions: the Foreseer Server will not boot or a total failure of the Foreseer Server data monitoring network to collect data).

Contact Number (Business Hours) – Eaton Corporation Foreseer Technical Support can be reached at:

(800) 356-3292 option 8

The first available technical support engineer will answer the call. If all support engineers are busy, the caller will be given the opportunity to leave a voice message. Notification of the voice message goes to all support engineers and the first available will respond.

If an engineer does not answer the phone, please leave a voice message. It will be returned as soon as possible.

Contact Number (After-Hours) – Eaton Corporation Foreseer Technical Support can be reached at:

(800) 356-3292 option 8

The call will be answered by an answering service. The answering service will gather some information and then contact the on-call technical support engineer, who will return the call within two hours of initiation.

The answering service will request some basic information, including:

- Caller's Name
- Caller's Phone Number
- Company
- Description of the problem
- Duration the problem has been occurring

What Technical Support May Need – There are a number of tools within the Foreseer Server application that provide troubleshooting assistance. Nearly 100% of the calls for support will require the caller to have access to the Foreseer Server application, either by direct contact with the system or via a remote interface (Remote Desktop, VLC, etc).

The caller should be prepared to provide the following:

1. Log File Report

2. System Configuration Report
3. Wiretap (for a field device issue)

Directions for obtaining these three items can be found in the Foreseer Ownership Documents package.

Other files that may be requested for more in-depth troubleshooting include:

4. Operating System Event Logs
5. Operating System Application Logs
6. Various screen capture images

The Technical Support Process Overview – After initiating a call to Foreseer Technical Support, the following is a general process that may be encountered:

1. The technical support engineer will start gather data through a discussion with the caller. Some of the items that may be discussed, include:
    - What the issue is
    - How long has the issue been occurring
    - What may have changed to cause the issue
    - What steps has the caller taken to troubleshoot the issue?
2. A request for various reports or files may be requested, including:
    - Reports (Log Files, System Configuration Reports, Up-Down Logs, Audit Logs, Alarm History Reports, Wiretaps)
    - System Configuration backups (.arq file)
    - System Logs
    - Screenshots
3. A review of requested files will take place.
4. A possible solution will be made. If that solution does not resolve the issue, further tests or files may be requested.
5. All calls will be issued a Service Request (SR) number that will be unique and provide a reference for tracking the call(s), files, and steps provided.

What Can the Caller Expect From Technical Support – Upon calling Foreseer Server Software Technical Support, the caller can expect a professional, individualized, and diligent pursuit to the solution of the issue.

What Can be Expected From the Caller – If a call is made to Foreseer Server Software Technical Support, the technical support engineer should be able to expect the following from the caller – access to the Foreseer Server Software, the ability to retrieve files from the computer (with limited intervention from the support engineer), and the willingness to provide the information and files requested.