



# FireWorks 9.2 Network Application Guide

**Copyright**

© 2023 Carrier  
All rights reserved.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.

**Trademarks and patents**

The Edwards name and logo are trademarks of Carrier.

The FireWorks name and logo are trademarks of Carrier.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

**Version**

This document applies to Windows 10 computers running FireWorks 9.2 software.

**Contact information**

For contact information, see [www.edwardsfiresafety.com](http://www.edwardsfiresafety.com).

# Content

## **Important information iii**

Limitation of liability iii

Advisory messages iii

Disclaimers iii

## **Introduction 1**

Referenced documents 1

Important notes 1

Backup server gets points from iO, FX, and VS control units 3

Tool for monitoring ports in Redundant Network 4

Tracking Network Activity on a Redundant Fireworks 4

Watchdog cards 4

D6600/D6100 Communications Receiver and OH Network Receiver 4

VESDA nodes 4

## **Setting up a nonredundant FireWorks network 5**

Introduction 5

Equipment requirements 5

Prerequisites 6

Disabling FIPS algorithm 7

Turning Windows Defender Firewall off and on 7

Nonredundant server and client setup 7

## **Setting up a redundant FireWorks network 10**

Introduction 10

Equipment requirements 12

Prerequisites 13

Setting up the SQL cluster 14

Setting up SQL mirroring 17

Setting up a client workstation 21

Server in Charge state 23

To use Integrated Security / Windows authentication you must log in as Administrator with  
Network Setups 23

## **Troubleshooting practices 24**

### **Troubleshooting the file distribution system 33**

Introduction 33

Firewall unopen port issues 33

Locked files 35

Damaged stored directory on client workstation 35

### **Appendix A Network software SKUs 37**

### **Appendix B SQL Mirroring utility functions 39**

### **Appendix C Changing the SQL server type 42**

Introduction 42

Changing from SQL Server 2019 Express to SQL Server 2019 Standard 42

Changing from SQL Server 2019 Standard to Express 43

## **Appendix D Firewall exceptions required for networking 44**

- Inbound rules for computers in redundant networks 44
- Inbound rules for computers in nonredundant networks 46
- Inbound rule to allow pinging across the network 48
- Allowing file and print sharing 52

## **Appendix E DNS and Machine Detection 54**

- DNS and machine detection tool for redundant network 54
- Client-Server Synchronization 54

## **Appendix F FireWorks Shared Resource Folder 56**

- Introduction 56
- Creating the shared folder on the primary server computer 57
- Mapping the shared folder on the backup server 59
- Mapping the shared folder on the witness server 60
- Testing the shared folder read/write permissions 60
- Adding the common user to the SQL properties 60

## **Appendix G Setting Up Dual NIC Environment 63**

- Introduction 63
- How to configure a dual NIC environment 63
- Dual NIC failover and recovery 64

## **Glossary 65**

# Important information

## Limitation of liability

To the maximum extent permitted by applicable law, in no event will Carrier be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Carrier shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Carrier has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Carrier assumes no responsibility for errors or omissions.

## Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

---

**WARNING:** Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

---

---

**Caution:** Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

---

**Note:** Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

## Disclaimers

This document is intended for use with a dedicated FireWorks life safety network consisting of UL 864 Listed Ethernet switches, and FW-UL6 Windows 10 workstations and server computers configured as a cluster (i.e., a flat workgroup network). The workstations and servers are not members on a domain or attached to a domain network.

Domain networks are outside the scope of this document, whether the FireWorks computers are domain members or not. While the information may be valid, some procedures will fail without the domain administrator's password privileges.



# Introduction

Instructions in this guide are written with the assumption that your FireWorks network is built on a dedicated fiber network. This is a requirement for UL Listing, and results in the best network performance.

If you are not using a dedicated fiber network, you will need to work closely with the site IT department as the potential variations in configuration make it impossible to present specific directions in this guide.

## Referenced documents

The following documents are referenced in this publication:

- *MN-FVPN Firmware Upgrade Installation Sheet* (P/N 3102373)
- *MN-NETRLY4 Firmware Upgrade Installation Sheet* (P/N 3102372)
- *FW-UL6WW10 FireWorks Workstation Installation Manual* (P/N 3102213)
- *FW-UL6SW10 FireWorks Server Installation Manual* (P/N 3102221)

## Important notes

Here are some points to bear in mind as you proceed:

- We strongly recommend that you print this document and follow it step-by-step, crossing off each step as you complete it. Leaving out steps or performing the steps out of order greatly increases the risk of failure.
- If you are using MN-FVPN modules or MN-NETRLY4 modules in a redundant network you must update the firmware as described in the following publications:

*MN-FVPN Firmware Upgrade Installation Sheet* (P/N 3102373)

*MN-NETRLY4 Firmware Upgrade Installation Sheet* (P/N 3102372)

- A global time server must be available to the computers in the FireWorks network to keep them in sync. This is often handled by the operating system but must be enabled. Mirroring will not start if the primary server computer and the backup server computer are out of sync. For more information, see *FireWorks Network Time Protocol Application Guide* (P/N 3102871).

There are numerous ways to set up a Windows Time Service for your network. If you do not know how to do this, we strongly recommend that you engage the site IT department. There are also plenty of resources available on the Internet.

For example, a YouTube search for “Windows Time Service” finds a video titled “40 Windows Time Service.wmv” (<https://www.youtube.com/watch?v=iqAxtlNk-8w>).

- The primary server computer, the backup server computer, and the witness computer in a redundant network SQL cluster must all be set for the same time zone.
- You must establish your computer naming convention and change the computer names before you install FireWorks. If you want to change the computer names later you must uninstall both FireWorks and SQL Server, change the names, and then re-install FireWorks and SQL Server. For more information on computer names, see Appendix E “DNS and Machine Detection” on page 54.
- The primary and backup server computers use Microsoft SQL Server 2019 Standard while the witness and any client computers use Microsoft SQL Server 2019 Express.

- FW-UL6 computers support multiple network connections. FireWorks has been tested and we recommend only using one of the NICs. If you use multiple NICs, work with the site IT department to choose the appropriate network connection for your application. Be aware that each network adapter can have a different IP address, and changing the network connection, or changing the IP address of the network adapter can cause unexpected results.
- We highly recommend that you should have a host file in place whether you decide to configure your system to use static IP addresses or DNS names. Having a host file has been tested and proven to significantly assist communication throughout the FireWorks network. Please review the “Troubleshooting Practices” area below for more details on how to set one up.
- Various ports must be opened on the FireWorks computers to allow the servers and clients to communicate. For a complete list of ports, see Appendix D “Firewall exceptions required for networking” on page 44.

The easiest way to ensure that the ports are available is by turning Windows Firewall off. This may not be feasible in all situations. Turning Windows Firewall off may negatively impact security policies and should be discussed with the onsite IT personnel.

- On FW-UL6 computers, under Local Area Connection properties, the Internet Protocol Version 6 (TCP/IPv6) is not selected by default (i.e., the check box is cleared). If you want to use TCP/IPv6, you must select the check box. TCP/IPv6 requires local IT support, this has not been tested by Edwards and we recommend TCP/IPv4.
- We recommend that you use the Windows Update utility to turn off automatic updates, whether you have a dedicated or a nondedicated network. Updates may require a restart or render the computer unusable. Always apply updates and patches manually, so that you retain supervision and control of the update process. Automatic updates are disabled on FW-UL6 computers.
- Filtering at a client computer will not affect event printing or event history. Printing and history filtering are determined by settings at the server where reports are printed, and history is stored.
- After the first database mirroring process, the system may repeat prompt messages regarding mirroring. If this occurs, simply click OK to acknowledge and continue.
- You can run System Builder from any station at any time. Any programming changes you make (e.g., changes to maps, devices, etc.) will be stored properly in the project database. However, to see the result of your changes in real time, you must have System Control up and running at every station including the station from which you made the changes.
- If you have System Builder open on two different computers on the network and System Control is not running on at least one of them, when you make changes in the same area, (e.g., the same node), the changes you made from one computer may not be visible on the other computer in real time. If this happens, do not worry. No data is lost. Simply restart System Builder on the second computer.
- Putting a primary server in local mode will have the effect of putting the system globally into local mode.
- If you are filtering out trouble events on the server, when you acknowledge a trouble event at a client workstation the server does not pass the acknowledgement to any clients that subsequently connect to the server. There isn't an issue if the trouble event restores beforehand.



- The File Distribution system runs in the background and keeps your maps and other resources in sync. Changes to any resources are not refreshed automatically but rather when you browse to that map. This can often be seen when you first start a client or station, and the site map is blank.
- When you create or modify a user or role on one station, and then you try to access it on a different station without restarting both stations first, you may see an "Info: Default user set." Error message. If this happens, simply delete the user/role, and then re add it.
- If there is an error that the system detects before System Control is fully initialized it will go to the diagnostics status form. If this happens before the system is ready to display the form, you will notice that the screen flashes a bit. When this happens, simply go to the menu item status "Diagnostics Status" and select, any information will be readily available there.
- If you delete a node on one station and do not restart all of your systems you may see a warning message when you try to bring up the node status. The warning is harmless and can be dismissed.
- If you find any of your stations on the network in the situation where they appear to have control but the Acknowledge button is unavailable, log out and then log back in again to make the Acknowledge button available so you can acknowledge points.fr
- If you are utilizing UL PC's All Servers and Clients must be on the same OS revision as this is what has been tested by Edwards.
- When System Control starts for the first time on a redundant client or on a nonredundant client station you may briefly see the following error message before System Control shuts down:

"Error starting System Control: No Text with ProductID = 0..."

If this happens, simply restart System Control and it should start normally.

- The Primary and Backup Server computers in a redundant FireWorks network are designed to be manned workstations just like any other Client workstation in the network. They are suitable for an operator to conduct the day-to-day life safety operations required by your site. The only station that is not to be used by an operator is the Witness Server.

Likewise, the Server computer in a nonredundant FireWorks network is designed to be a manned workstation just like any other Client workstation in the network. However, if they are unmanned you must make provisions to periodically acknowledge events. If there are more than a couple of thousand active points on the server the system can become unstable.

- For systems with Redundant Servers, the operators must understand how the overall system operates. Panels and Panel Networks have 2 connections to the FireWorks Redundant Server system – 1 for each of the Servers, then the FireWorks workstations get their data from the active Server. If the primary Panel/Panel Network connection fails for any reason, the FireWorks Primary Server and all Workstations will post a single fault, that being that the FireWorks active Server has lost communications with the Panel/Panel Network, but they will not receive any points from the backup communication connection. In this scenario, the Backup Server will receive and post the points from the Panel/Panel Network, but they will not be visible to the active Server or Workstations and the only way the operators can send commands to the Panel/Panel Network is to log onto the Backup Server. If the operator changes the active FireWorks Server to the Backup, they will see the Panel/Panel Network that has the connection.

## Backup server gets points from iO, FX, and VS control units

If iO/FX/VS control units are configured to talk to both the primary and backup servers in Redundant FireWorks, then physical backup server does get points from the iO/FX/VS control unit. If primary server is shut down and backup server becomes logical primary, points from the iO/FX/VS control unit comes to it. Points from the same account get to the primary and the backup servers.

You can program two FireWorks IP Dialer Accounts in the control unit's configuration utility. One IP account for the FireWorks Redundant Network primary server PC IP address and one for the FireWorks Redundant Network backup server PC IP address. This way events are sent to both FireWorks Redundant Network Servers.

## Tool for monitoring ports in Redundant Network

- Created a batch file C:\FireWorks\MiscFilesAndOCXsForInstall\PortsMonitoring.bat which tracks the processes using the ports on the system and outputs the results to C:\Fireworks\log\PortsInformation.txt.
- User can use the process ID to check which process is using the particular port ID with the help of Task Manager.

## Tracking Network Activity on a Redundant Fireworks

- When the system is setup in a redundant network version of FireWorks, we are tracking the entire network activity in the log file present at C:\Fireworks\log\NetworkActivity.txt. All we do is ping each machine defined in the system builder and capture the output. This could be helpful for users and tech support if the machines in network are having trouble communicating with each other.

## Watchdog cards

- To meet UL Listing requirements, all server and workstation computers on the FireWorks network must have watchdog cards. FW-UL6 workstation/server computers meet this requirement.
- Watchdog cards must be added and programmed when creating the FireWorks project. Refer to *System Builder Help* for instructions.
- Watchdog card failures are local to the computer and are not annunciated across the network.

## D6600/D6100 Communications Receiver and OH Network Receiver

To accomplish no single point of failure in redundant network applications:

- When using D6600/D6100 digital alarm communication receivers (DACR), connect one DACR to the primary server and another DACR to the backup server.
- When using OH Network Receiver, install FW-IPMON1000 on the primary server and on the backup server.
- For each server-receiver combination, use separate accounts with the same Contact ID (CID) events defined in each account. This doubles the programming effort, but fortunately CID strings now automatically populate.
- On maps, for each CID event, you can drop a point from each receiver account (i.e., two icons adjacent to each other) or you can drop the corresponding points from each account to the same device icon or TSA.

## VESDA nodes

A redundant network uses two FW-HSSX1 VESDA Modbus High Level Interface modules for each VESDA node. The FW-HSSX1 modules must be kept in sync so that events are reported properly and consistently to the primary and backup servers. This means that when you issue an HLI Refresh command from the primary server you must also issue an HLI Refresh command from the backup server, and vice-versa.

# Setting up a nonredundant FireWorks network

## Introduction

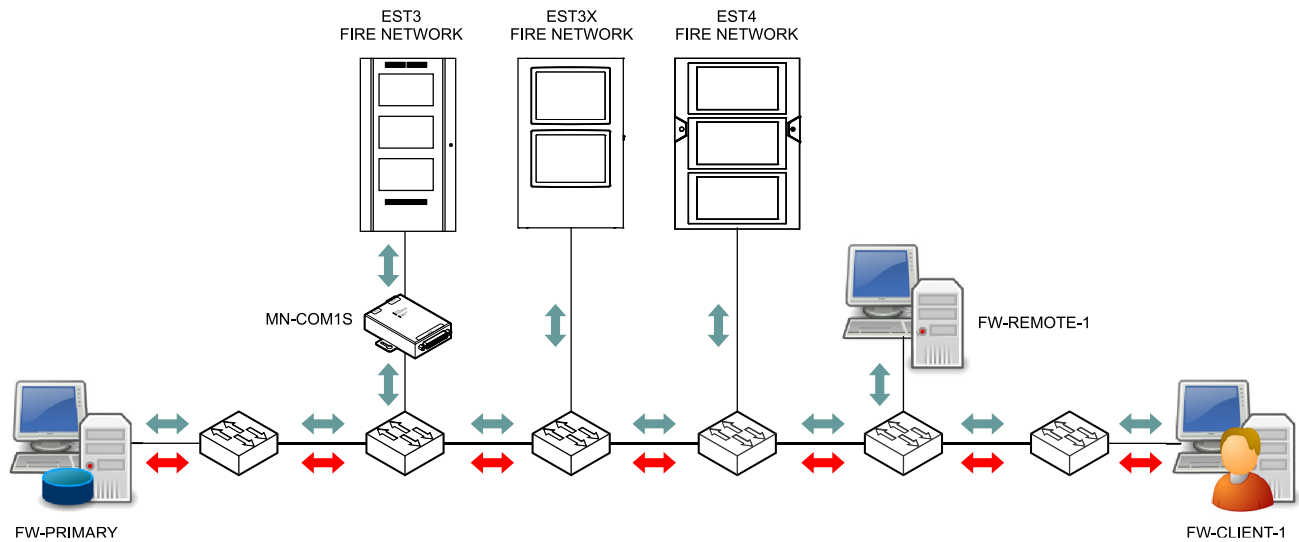
A nonredundant FireWorks network consists of a primary server computer and one or more client workstation computers connected to one or more of the following:

- EST3, EST3X, and EST4 fire networks
- VESDAnet networks
- D6600/D6100 receivers
- FireWorks remote clients

**Note:** For UL Listed systems, use MN-FNS series Ethernet switches. Remote client connections are ancillary. This means that you may use third-party Ethernet switches to connect remote clients.

Figure 1 below shows a basic nonredundant FireWorks network.

**Figure 1: Nonredundant FireWorks network**



**Legend for Figure 1**

Arrow	Description
	Communication path between the FireWorks server computer and the fire networks
	Communication path between the active client workstation computer and the FireWorks server computer

## Equipment requirements

The computer equipment required for a UL Listed nonredundant network system is shown in Table 1. For more information, see the following:

- *FW-UL6WW10 FireWorks Workstation Installation Manual* (P/N 3102213)
- *FW-UL6SW10 FireWorks Server Installation Manual* (P/N 3102221)
- *FW-UL7 FireWorks UL7 Computer Installation Manual* (P/N 3102881)

For applications that do not require UL Listing, you may use third-party (off-the-shelf) computers that meet the minimum system requirements of a FW-UL6 Windows 10 workstation/server computer. For minimum system requirements, see *FireWorks 9.2 Software Installation Guide* (P/N 3100034).

**Note:** FireWorks software is not UL Listed when installed on third-party computers.

**Table 1: Minimum computer equipment requirements**

	Quantity	Hardware/software [4]	Function
Nonredundant server	1	FW-UL6SW10/FW-UL7S FireWorks server computer with FireWorks 9.2 OS image FW-UL7S FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC) FireWorks 9.2 software (FW-CGSUL) SQL Server 2019 Express Version 15.0.2000.5, Build 17763 [1]	Primary communication path between FireWorks and other systems/equipment on the nonredundant network. The primary server may also serve as a system control point.
Clients	1 to 15 [2]	FW-UL6WW10/FW-UL7W FireWorks workstation computer with FireWorks 9.2 OS image FW-UL7W FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC) FireWorks 9.2 software (FW-CGSUL) SQL Server 2019 Express Version 15.0.2000.5, Build 17763 [1]	Alternate system control point. Clients communicate to other systems/equipment on the nonredundant network through the primary server.
Remote clients	1 to 15 [3]	Third-party computer running FireWorks 9.2 Remote Client	Remote annunciation of system events. Remote clients are considered ancillary.

[1] Included in the FireWorks 9.2 software.

[2] Depends on the number of nonredundant client licenses you purchase.

[3] Depends on the number of remote client licenses you purchase.

[4] You may not install FW-UL6 computers and FW-UL7 computers on the same network. This has not been tested and is not recommended.

## Prerequisites

1. The network requires at least two computers, one for the server, and one for a client. The maximum number of client computers is determined by the software options you have purchased. (See Appendix A for an explanation of the model numbers used.)
2. All computers in the network must be running the same version of Windows 10 and FireWorks 9.2.
3. Established computer names. In our example we use:  
Nonredundant server: FW-Primary  
Client computer: FW-Client-1
4. Make sure the FIPS algorithm is disabled on every computer on the FireWorks network.
5. Make sure Windows Defender Firewall is turned off while you are setting up the system. After you finish setting up the system and verify that it is working properly, you can turn Windows Defender Firewall back on.

## Disabling FIPS algorithm

1. Open the Microsoft Management Console.  
In the Search box on the Windows task bar, type: mmc, and then click Run as administrator.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies, click the Security Options folder.
6. In the middle pane, right-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing, and then click Properties.
7. On the Local Security Setting tab, select Disabled, and then click OK.
8. Restart the computer.

## Turning Windows Defender Firewall off and on

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Overview group, click Windows Defender Firewall Properties.
7. On the Domain Profile, Private Profile, and Public Profile tabs, set Firewall state for Off.

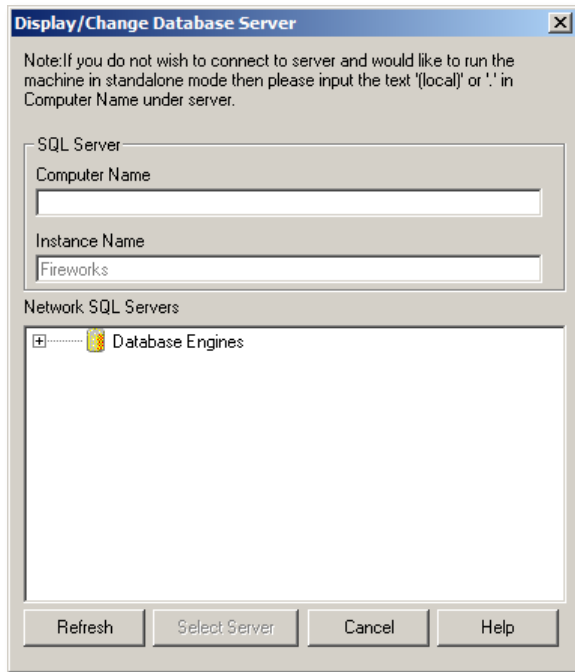
To turn Windows Defender Firewall back on, repeat the procedure above except on the Domain Profile, Private Profile, and Public Profile tabs, set Firewall state for On. Make sure that the SMB blocking rules are not enabled as file sharing is needed in the system. These exceptions are only in workstation images. To disable the rules, go to the "Inbound rule" section in the firewall and disable the rules for TCP 445, 139 and UDP ports 137, 138.

## Nonredundant server and client setup

### To set up the nonredundant server and clients:

1. Plug the USB software key into the computer, and then install the FireWorks 9.2 software. For more information, see *FireWorks 9.2 Software Installation Guide* (P/N 3100034).
2. When prompted, enter the PINs for all the software products you purchased, starting with FW-CGSUL. Refer to Appendix A "Network software SKUs" on page 37 for a description of product SKUs.

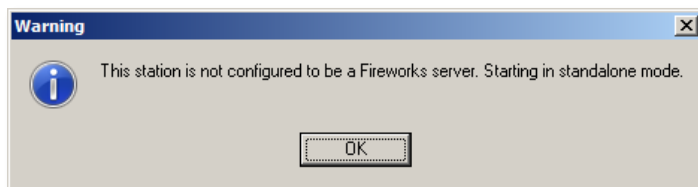
3. When prompted to load SQL Server 2019 Standard, click No. This will automatically install SQL Server 2019 Express.
4. After the installation has finished, start System Builder. FireWorks recognizes your setup by reading the PINs on the software key, and then opens the Display/Change Database Server dialog box shown below.



5. In the Computer Name box, type the computer name of the server computer.

If you do not know the computer name, in the Search box on the Windows task bar, type: about, and then click About your PC in the search results. The computer name is listed under Device specifications. Type the name exactly as it appears there.

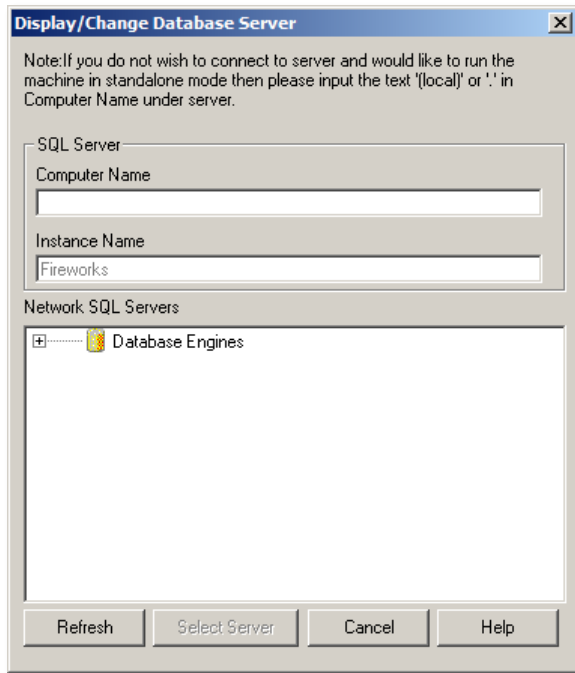
6. Click Select Server.
7. Click OK to acknowledge the warning message.



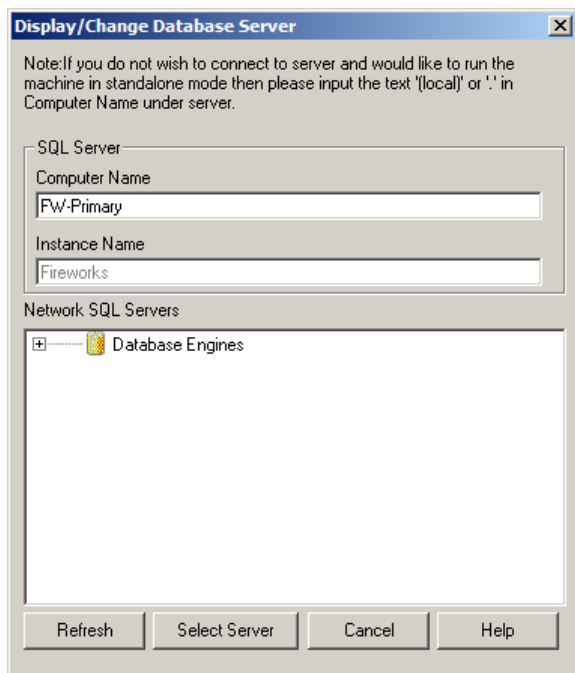
8. After System Builder starts, add the server computer and client computers to the project. For details, see “Adding a server workstation” and “Adding a client workstation” under “Setting up nonredundant networks” in *System Builder Help*. We strongly recommend using the clients IP address in the “address” field, if you have issues with IP addresses then use the computer’s name in this field.

To find your IP address, right-click the Windows Start button, click Network Connections, and then click Status. On the Status page, click Properties for the adapter that you are using for your network connection, and then look for the IPv4 address under IP Settings.

9. On the client computer, start System Builder. FireWorks recognizes your setup by reading the PINs on the software key, and then opens the Display/Change Database Server dialog box shown below.



10. In the Computer Name box, the machine's IP address or computer name can be entered. We recommend using the IP address first, if this gives you issues than you can try the computer name of the server computer, and then click Select Server.



The clients are now connected to the server, and the nonredundant network setup is complete.

11. Turn Windows Defender Firewall back on (see "Turning Windows Defender Firewall off and on" on page 7).
12. Add the required firewall exceptions (see Appendix D "Firewall exceptions required for networking" on page 44).

# Setting up a redundant FireWorks network

## Introduction

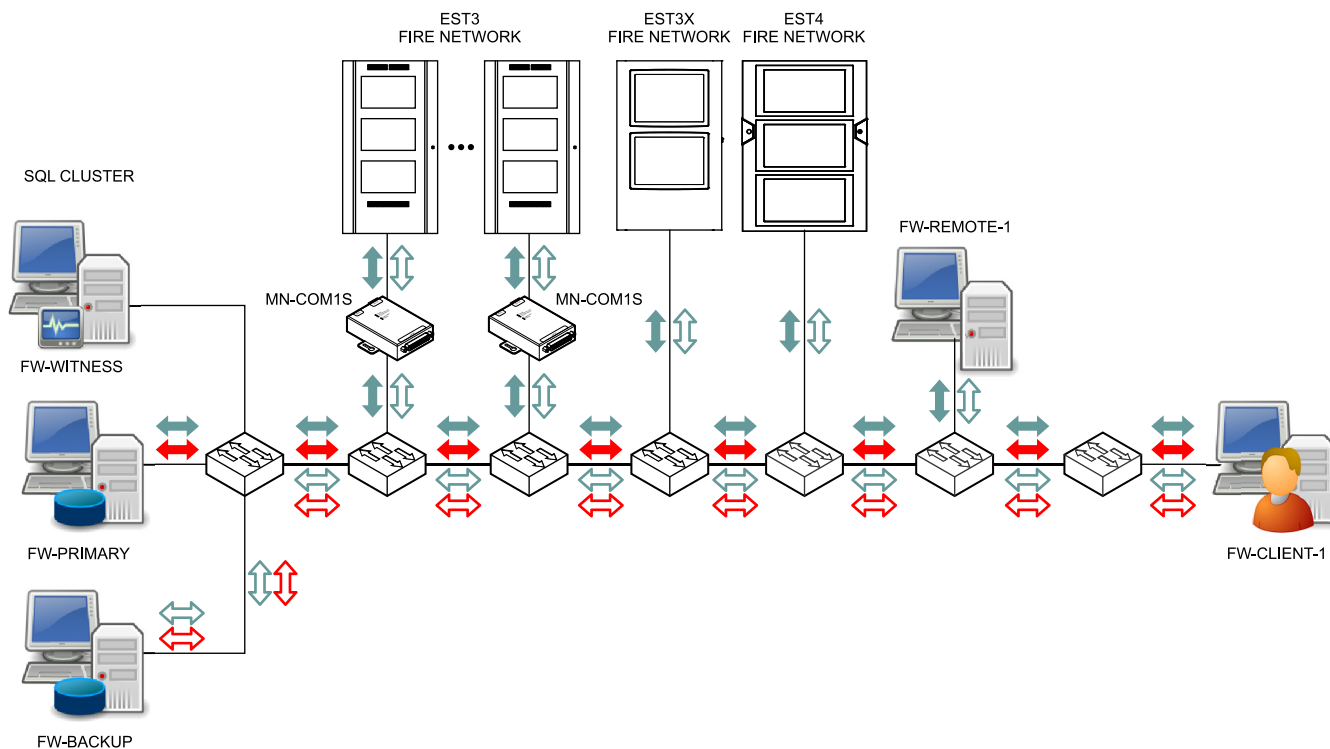
A redundant FireWorks network consists of a primary server computer, a backup server computer, and a witness computer (collectively called an SQL cluster), one or more client workstation computers, and one or more of the following:

- EST3, EST3X, and EST4 fire networks
- VESDAnet networks
- D6600/D6100 receivers
- FireWorks remote clients

**Note:** For UL Listed systems, use MN-FNS series Ethernet switches. Remote client connections are ancillary. This means that you may use third-party Ethernet switches to connect remote clients.

Figure 2 below shows a basic redundant FireWorks network.



**Figure 2: Redundant FireWorks network**



**Legend for Figure 2**

Arrow	Description
	Communication path between the primary server computer and the fire networks when the primary server computer is the primary server
	Communication path between the backup server computer and the fire networks when the backup server computer is the primary server



Arrow	Description
	Communication path between the active client workstation computer and the primary server computer when the primary server computer is the primary server
	Communication path between the active client workstation computer and the backup server computer when the backup server computer is the primary server

A redundant FireWorks network makes use of an advanced database survivability technique known as *database mirroring*. Mirroring is a Microsoft SQL Server technology that has proven to be very robust. It is used in commercial applications that require a high degree of reliability and limited down times.

Mirroring requires a minimum of three computers: a primary server computer, a backup server computer, and a witness computer. The three computers are collectively known as an *SQL cluster*. The witness computer provides arbitration for the applications and for the other server computers, determining which database is currently active. This provides survivability and flexibility because a failure at either server computer in the cluster lets the system continue operation with no loss of data integrity.

For mirroring to provide database integrity as intended, two of the three computers in the SQL cluster must always be running and be visible to each other. This is a key design parameter.

So that there is no single point of failure, each EST fire network, VESDAnet network, and D6600/D6100 on the redundant FireWorks network has a parallel communication path to the primary server computer and to the backup server computer. The backup server computer takes on the role of the primary server if the primary server computer should fail or is taken out of service. You can also use the backup server computer to manually issue commands and view the status of the system. However, the LEDs and events in the New Event List on the backup server may not be in sync with the primary server.

**Note:** The primary server computer and the backup server computer in the SQL cluster may be used as a manned operator station; the witness computer cannot. However, using the primary and backup servers as manned operator stations is not recommended as Microsoft SQL does not prioritize updating the operator display on the servers even though the information has been passed to the remote workstations.

EST control units report only to the server that they are directly connected to. A single EST3/EST3X/EST4 node will report via separate communication paths to the primary server computer and to the backup server computer. If a failure happens on the communication path to the primary server computer any subsequent event will show on the backup server computer but not on the primary server computer. You may attempt a manual switch to the backup server computer but any failures on the backup server's communication path would manifest the same as the scenario described previously.

The backup server may also be unmanned. For this reason, it defaults to the FireWorks local mode so that after an event activates and restores it will be automatically acknowledged by FireWorks on the backup server. With the backup server in "local mode" and sending acknowledges to the panel if the panels are in proprietary mode said acknowledges will come back to the primary and some point may seem to self-acknowledge.

If the site requires that the LEDs and event queues on the backup server be synchronized with the primary server computer, then the EST fire network must be configured for proprietary mode. In proprietary mode, an acknowledgement at one gateway port is passed to the other gateway ports, which sends the acknowledgement to any FireWorks server attached to that gateway port. See the control unit's documentation for instructions on setting the project for a proprietary marketplace.

The witness computer is a critical component of the redundant network SQL cluster. Bear these points in mind:

- The witness computer may not be used as a system control point. Since it is crucial to the viability of the cluster, it must be always on.
- If the witness computer fails or becomes unavailable, a witness failure event is annunciated across the network. You should have a contingency plan in place for this event.
- The witness computer has a watchdog card and must be placed in an area where a watchdog failure trouble buzzer can be heard, as this failure event is not otherwise annunciated at any point in the network.

## Equipment requirements

The computer equipment required for a UL Listed system is shown in Table 2. For more information, see the following documents:

- *FW-UL6WW10 FireWorks Workstation Installation Manual* (P/N 3102213)
- *FW-UL6SW10 FireWorks Server Installation Manual* (P/N 3102221)
- *FW-UL7 FireWorks UL7 Computer Installation Manual* (P/N 3102881)

For applications that do not require UL Listing, you may use third-party (off-the-shelf) computers that meet the minimum system requirements of an FW-UL6 Windows 10 workstation/server computer. For minimum system requirements, see *FireWorks 9.2 Software Installation Guide* (P/N 3100034).

**Table 2: Minimum computer equipment requirements**

	Quantity	Hardware/software [6]	Function
Primary redundant server	1	FW-UL6S/FW-UL6SW10 FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 Enterprise LTSC)  FW-UL7S FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC)  FireWorks 9.2 software (FW-CGSUL)  SQL Server 2019 Standard Version 15.0.2000.5, Build 17763	Primary communication path between FireWorks and other systems/equipment on the redundant network.  The primary server may serve as a system control point. [5]
Backup redundant server	1	FW-UL6S/FW-UL6SW10 FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 Enterprise LTSC)  FW-UL7S FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC)  FireWorks 9.2 software (FW-CGSUL)  SQL Server 2019 Standard Version 15.0.2000.5, Build 17763	Primary communication path between FireWorks and other systems/equipment on the redundant network — <i>if the primary server fails or is taken out of service</i> .  The backup server may serve as a system control point. [5]
Witness	1	FW-UL6W/FW-UL6WW10 FireWorks 9.2 workstation computer (FireWorks 9.2 OS image, Windows 10 Enterprise LTSC)  FW-UL7W FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC)  FireWorks 9.2 software (FW-CGS)  SQL Server 2019 Express Version 15.0.2000.5, Build 17763 [2]	Maintains database integrity so state changes are not lost when the primary server and the backup server switch roles.  The witness <i>may not</i> serve as a system control point.
Clients	1 to 30 [3]	FW-UL6W/FW-UL6WW10 FireWorks 9.2 workstation computer (FireWorks 9.2 OS image, Windows 10 Enterprise LTSC)  FW-UL7W FireWorks 9.2 server computer (FireWorks 9.2 OS image, Windows 10 IoT Enterprise LTSC)  FireWorks 9.2 software (FW-CGSUL)  SQL Server 2019 Express Version 15.0.2000.5, Build 17763 [2]	Alternate system control point. Clients communicate to other systems/equipment on the redundant network through the primary server.

	Quantity	Hardware/software [6]	Function
Remote clients	1 to 15 [4]	Third-party computer running FireWorks 9.2 Remote Client	Remote annunciation of system events. Remote clients are considered ancillary.

[1] Requires SQL Server Standard 2019 installation DVD, ordered separately. Order FW-SQL5UP or FW-SQL15UP if you are upgrading a FireWorks 8.x redundant network.

[2] SQL Server 2019 Express is installed automatically when you install FireWorks 9.2. FW-CGS is required only to monitor the watchdog card and provide audible notification of computer problems.

[3] Depends on the number of redundant client licenses you purchase.

[4] Depends on the number of remote client licenses you purchase.

[5] The primary server computer and the backup server computer in the SQL cluster may be used as a manned operator station; the witness computer cannot. However, using the primary and backup servers as manned operator stations is not recommended as Microsoft SQL does not prioritize updating the operator display on the servers even though the information has been passed to the remote workstations.

[6] You may not install FW-UL6 computers and FW-UL7 computers on the same network. This has not been tested and is not recommended.

## Prerequisites

1. The primary server, the backup server, the witness, and the clients must be on the same network.
2. Established computer names. In our example we use:

Primary server: FW-Primary  
Backup server: FW-Backup  
Witness server: FW-Witness

3. All computers in the network must be running the same version of Windows 10 and FireWorks 9.2. All computers on the network must use the same time and language settings.
4. The user must have two copies of SQL Server 2019 Standard Edition SP1, one for the primary server and one for the backup server.

If you have purchased the appropriate PINs and software licenses, the required copies of SQL Server 2019 Standard are included with your purchase. Refer to Appendix A "Network software SKUs" on page 37 for a description of product SKUs.

5. Turn Windows Defender Firewall off while you are setting up the system. After you finish setting up the system and verify that it is working properly, you can turn Windows Defender Firewall back on. (see "Turning Windows Defender Firewall off and on" on page 7).
6. Add the required firewall exceptions (see Appendix D "Firewall exceptions required for networking" on page 44).
7. To accomplish the required mirroring, you will need either:

A shared folder that is on the primary server. Create the folder, share it, and use it as a common folder for all three computers. To do this you must create a common "administrator" user with the same name and password on all three servers. Note: FWUL6 computers are configured with an Administrator user account with ESTFW for the password.

— or —

A shared folder on a network-attached storage (NAS) device. The shared folder must be accessible to the FireWorks administrative user who sets up mirroring. The folder should have full read/write/execute (R/W/E) permissions.

## Notes

- Be sure to get assistance from the site IT department when creating the shared folder. If this is not done correctly the first time, it takes much longer to troubleshoot.
- Make sure FIPS Algorithm is disabled on all computers on the network. If not, mirroring will not work.

**Disclaimer:** Domain networks are outside the scope of this document, whether the FireWorks computers are domain members or not. While the information may be valid, some procedures will fail without the domain administrator's password privileges.

## Setting up the SQL cluster

The SQL cluster consists of the primary server, the backup server, and the witness. The general steps for setting up the SQL cluster are:

1. Install FireWorks on the primary server, and then add the primary server, the backup server, and the witness to the project database.
2. Install FireWorks on the backup server.
3. Install FireWorks on the witness, and then change the SQL logon password to the Windows administrator password.
4. Create a shared folder that is read/write accessible from all three computers in the SQL cluster.
5. Set up SQL mirroring. If you have a UL7S you'll need to disable TLS1.3 first. Simply go to the following path in the registry: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols and find and delete the TLS 1.3 folder. Then restart your PC

**Note:** If you are setting up a redundant system on a third-party computer, you will need to perform all the steps in this guide on the operating system's Built-In "Administrator" account. This account is normally disabled in the operating system by default. To enable it, simply go to Computer Management >> Local Users and Groups >> Administrator >> uncheck "Account is disabled".

### Setting up the primary server

Setting up the primary server consists of installing FireWorks, naming the primary and backup SQL servers, and then adding a primary server, a backup server, and a witness to the project database.

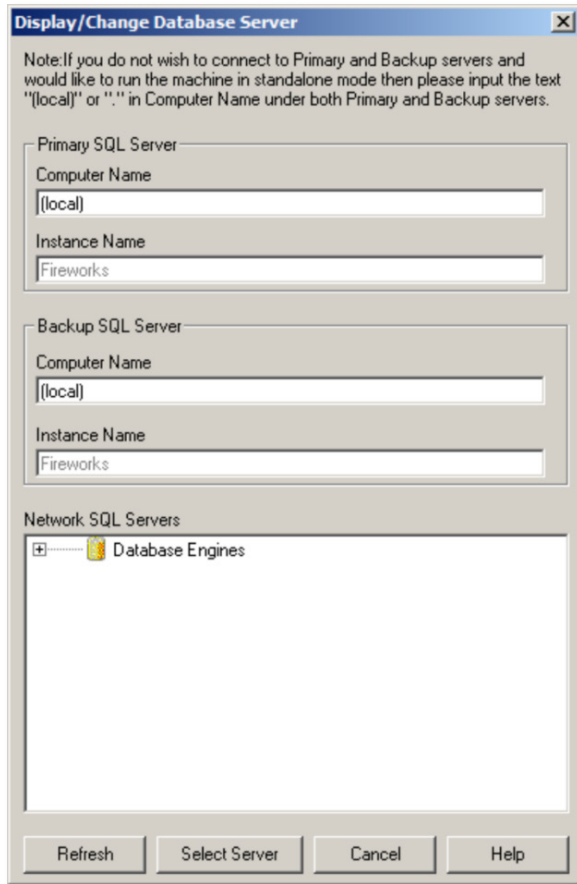
#### To install FireWorks on the primary server:

1. Plug the USB software key into the computer, and then install FireWorks 9.2. For more information, see *FireWorks 9.2 Software Installation Guide* (P/N 3100034).
2. When prompted, enter the PINs for the software products you purchased, starting with FW-CGSUL. Refer to Appendix A "Network software SKUs" on page 37 for a description of product SKUs.
3. When prompted to load SQL Server 2019 Standard, click Yes.
4. Insert the SQL Server 2019 Standard for FireWorks Redundant Networks disc (P/N 7460008) into the DVD drive, and then follow the instructions displayed on the screen.

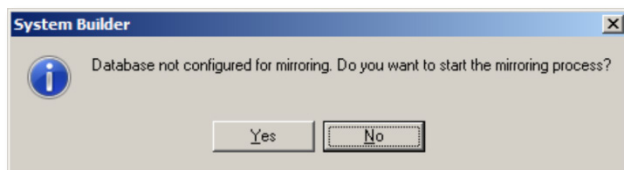
The next step is to name the primary and backup SQL servers.

### To name the primary and backup SQL servers:

1. After the installation has finished, start System Builder. FireWorks recognizes your setup by reading the PINs on the software key, and then opens the Display/Change Database Server dialog box.
2. In the Display/Change Database Server dialog box, verify that the computer name for the primary and backup server is: (local). This means that FireWorks installed as a stand-alone workstation.



3. Under Primary SQL Server, the machines IP address or computer name can be entered. We recommend using the IP address first, if this gives you issues than you can try the primary server's name.  
  
If you do not know the computer name, on the Start menu, right-click Computer, and then click Properties. The computer name is listed under Computer name, domain, and workgroup settings. Type the name exactly as it appears there.
4. Under Backup SQL Server, the machines IP address or computer name can be entered. We recommend using the IP address first, if this gives you issues than you can try type the computer name of the backup server's name.
5. Click Select Server, and when prompted to start the mirroring process, click No, and then click OK.



The next step is to add a primary server, a backup server, and a witness to the project. If you wish, you can also add any clients to the project at this time.

**Tip:** If you have an existing project, restore the project before you add the primary server, the backup server, the witness, and any clients.

**To add a primary server, a backup server, and a witness to the project:**

1. Start System Builder.
2. Add a primary server. For details, see “Adding a primary server” in *System Builder Help*.
3. Add a backup server and witness. For details, see “Adding a backup server and a witness server” in *System Builder Help*.

**Tips:** If you have client workstations, you can add them now. For details, see “Adding a client workstation” under “Setting up redundant networks” in *System Builder Help*. Lastly, we strongly recommend when adding these machines to your project that you use the machines IP address in the “address” field if you have issues with IP addresses then use the computer name in this field.

**Setting up the backup server**

Setting up the backup server is the same as setting up the primary server, except that you *do not* add the primary server, the backup server, and the witness to the project database. For instructions, see “Setting up the primary server” on page 14.

**Note:** Since there is a high likelihood that the backup server could be unmanned, it is automatically configured for local mode. See *System Builder Help* for any questions on local mode.

After you name the primary and backup SQL servers, start System Builder, and then verify that the project includes the primary server, backup server, and witness that were added to the project on the primary server.

**Setting up the witness**

Setting up the witness consists of installing FireWorks, and then changing the SQL Server (FIREWORKS) logon password to let the Administrator user account automatically log on to the FireWorks instance on the SQL server.

**Installing FireWorks on the witness**

1. Plug the USB software key into the computer, and then install FireWorks 9.2. For more information, see *FireWorks 9.2 Software Installation Guide* (P/N 3100034)
2. When prompted, enter the PINs for all the software products that you purchased, starting with FW-CGS. Refer to Appendix A “Network software SKUs” on page 37 for a description of product SKUs.
3. When prompted to load SQL Server 2019 Standard, click No. This will automatically install SQL Server 2019 Express.

**To change the SQL Server (FIREWORKS) logon password:**

1. Set the SQL Server (FIREWORKS) logon password to use the administrator password.

If you have trouble changing the SQL logon password, download the file “Assigning SQL Administrator User” from the My-Eddie website for more information.

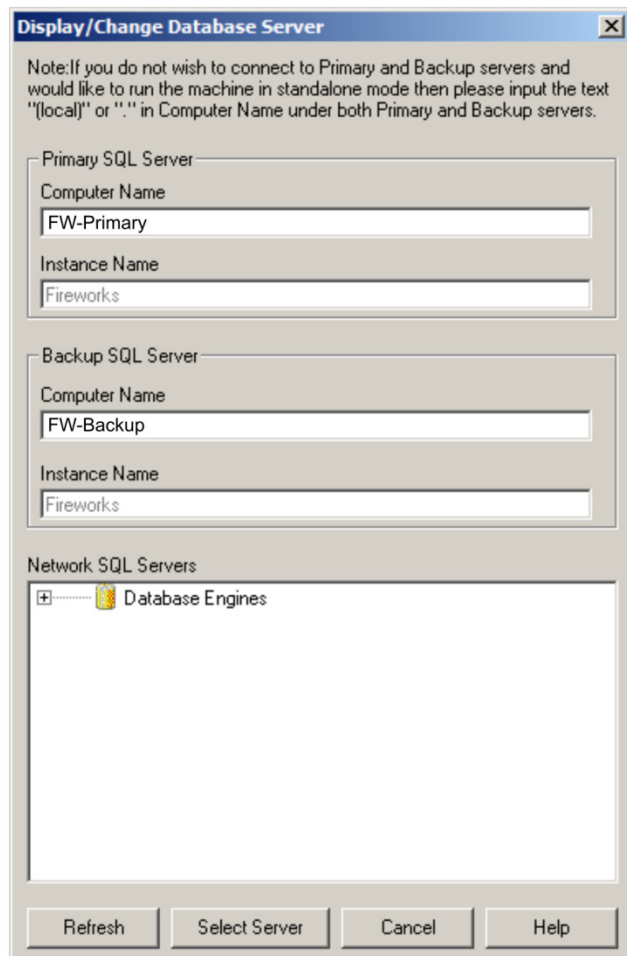
**Creating a shared folder**

Create a shared folder on the root of the C: drive on the primary server, and then map the shared folder on the backup server and on the witness. If you have trouble creating a shared folder, download the file “Creating shared folders for redundant networks” from the My-Eddie website for more information.

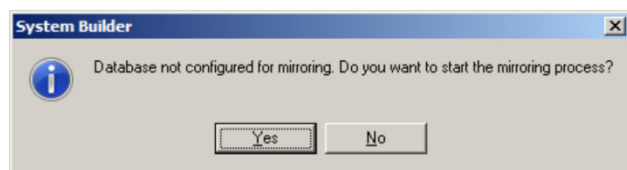
Verify each computer in the SQL cluster has read/write access to the shared folder. For example, create a temporary folder on one computer, and then verify you can open it on the other computers. Delete the temporary folder on a different computer, and then verify it is deleted on the others.

## Setting up SQL mirroring

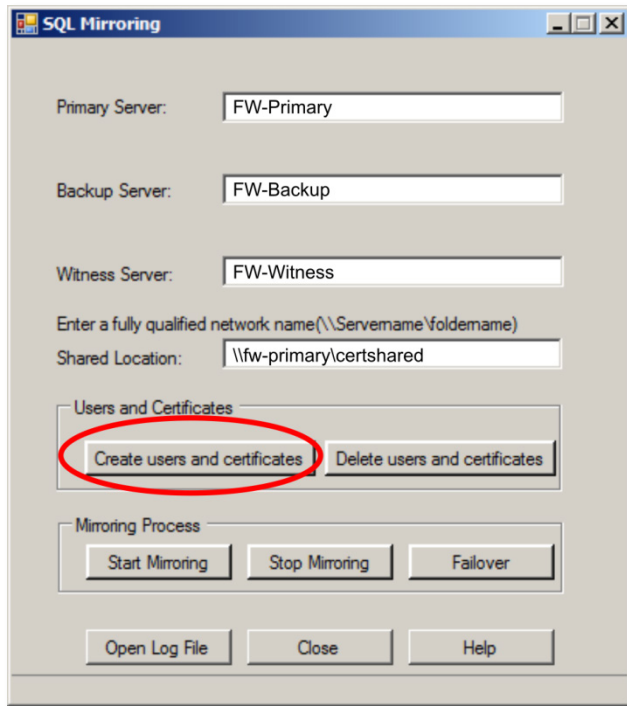
1. On the primary server, start System Builder.
2. In the Display/Change Database Server dialog box, verify that the computer names are correct. If not, the mirroring process will fail.



3. Click Select Server, and when prompted to start the mirroring process, click Yes.

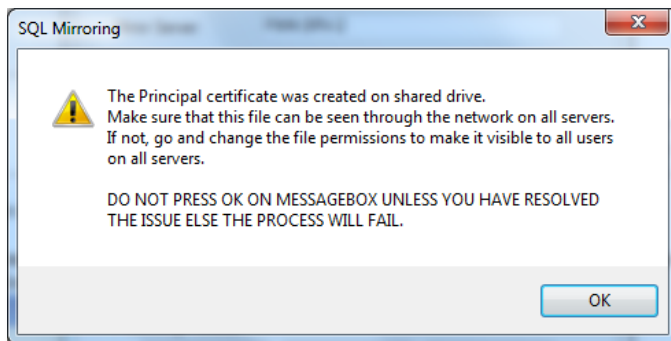


4. In the SQL Mirroring dialog box, type the names of the primary server, the backup server, and the witness, and then type the path of the shared folder as shown below.



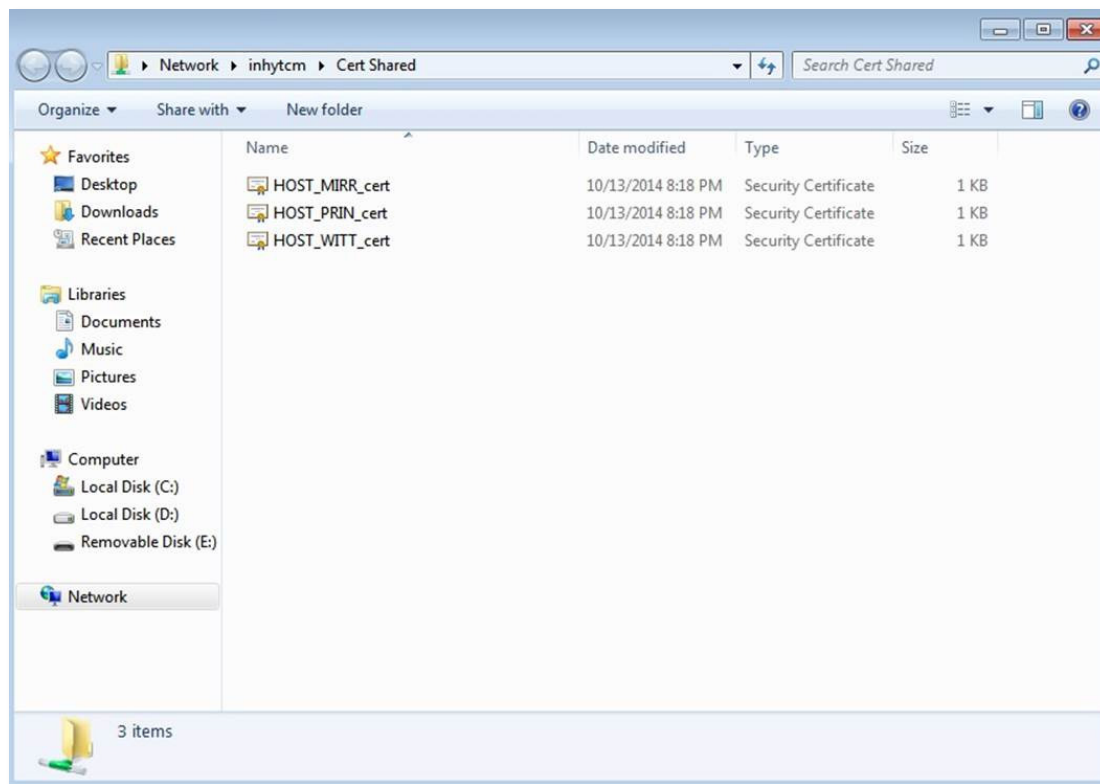
5. Click Create Users and Certificates. The users and certificates allow SQL Server to talk between the three servers.
6. As each certificate is created, the SQL Mirroring utility displays the message box shown below. Verify that the certificate file is visible in the shared folder on both server computers and on the witness computer, and then click OK.

**Note:** Do not click OK until you verify that the certificate file is visible in all three shared folders. This gives you the opportunity to fix permission problems without having to restart the process from the beginning.



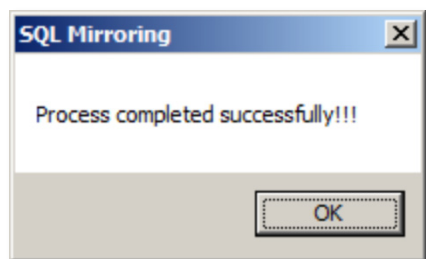


When all three certificates have been created, the shared folder should look like the following illustration:



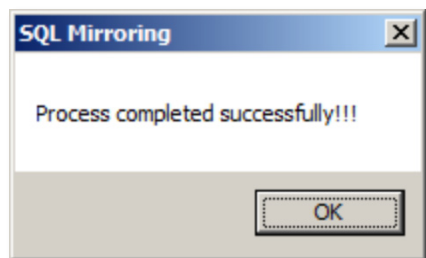
If you do not see any of the certificate files on any of the servers, then you need to physically go to the computer with the shared folder and change the permissions of that certificate file to allow users read/write/execute access.

7. The creation process may take several minutes. Wait until you see the following message box, and then click OK.



8. In the SQL Mirroring dialog box, click Start Mirroring.

The utility displays a progress bar. The startup may take up to 5 minutes. Allow the utility to work without interruption. When the mirroring process is finished, click OK.



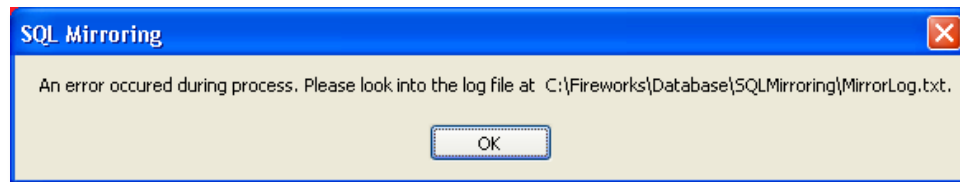
9. Click Close to close the SQL Mirroring dialog box.

The mirroring process is now complete, and System Builder will proceed to open.

### Error conditions

If there was something wrong with the settings you entered, the mirroring process will fail. The SQL Mirroring utility displays the message shown in Figure 3 below.

Figure 3: SQL mirroring error message



Be prepared to send the log file to Technical Support. The file is:  
C:\FireWorks\Database\SQLMirroring\MirrorLog.txt

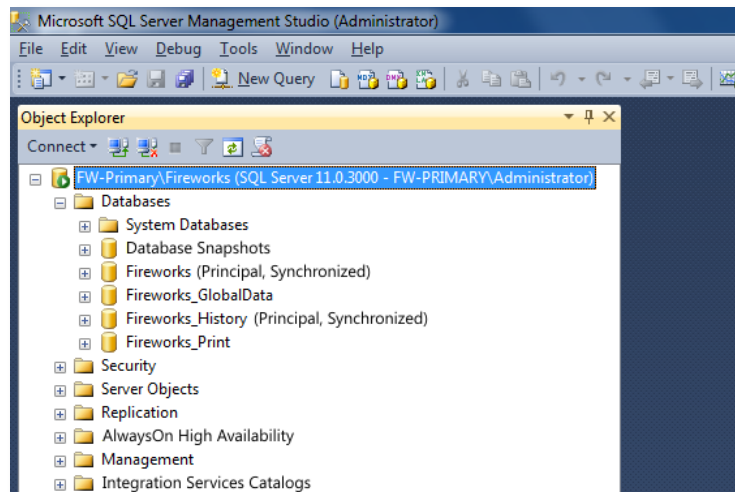
If you choose, you can open the log file from the SQL Mirroring dialog box by clicking Open Log File.

You can use the Microsoft SQL Server Management Studio to verify the correct operation of SQL mirroring. This can be done at any of the computers in the cluster.

### To verify the mirrored system:

1. On the Start menu, under Microsoft SQL Server 2019, click SQL Server Management Studio. (Startup may be delayed, depending on your network.)
2. Select the desired server from the Server Name list. This will be one of the suggested server names:  
Primary server = FW-Primary  
Backup server = FW-Backup  
Witness server = FW-Witness
3. Enter the credentials in the Login and Password boxes.  
Login = sa  
Password = Fi rew0rks\*  
**Note:** The character 0 in the password is the number zero, not the letter O.
4. Click Connect.
5. Expand the Databases folder.
6. Verify the status of the databases FireWorks and FireWorks\_History databases on the primary server. These must show "Principal, Synchronized" as shown in Figure 4 on page 21.

Figure 4: Verifying mirroring



## Setting up a client workstation

Client workstations are added to the FireWorks project on the primary server. For details, see “Adding a client workstation” under “Setting up redundant networks” in *System Builder Help*.

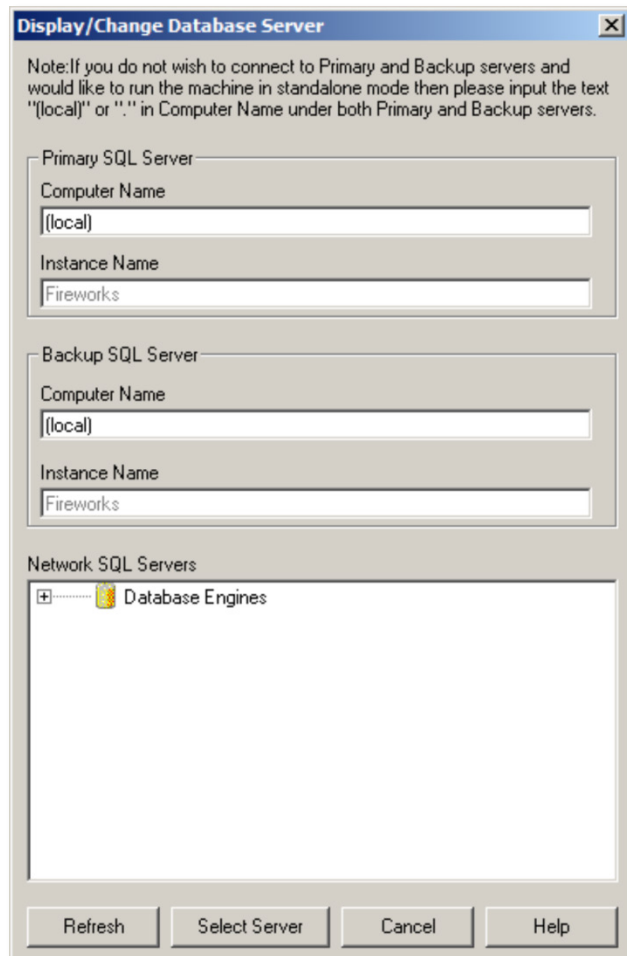
### Installing FireWorks on a client workstation

1. Plug the USB software key into the computer, insert the FireWorks installation disc (P/N 85012-0019) into the DVD drive, and then follow the on-screen instructions.
2. When prompted, enter the PINs for the software products that you purchased, starting with FW-CGSUL. Refer to Appendix A "Network software SKUs" on page 37 for a description of product SKUs.
3. When prompted to load SQL Server 2019 Standard, click No. This will automatically install SQL Server 2019 Express.

The next step is to name the primary and backup SQL servers.

### To name the primary and backup SQL servers:

1. After the FireWorks installation has finished, start System Builder. FireWorks recognizes your setup by reading the PINs on the software key, and then opens the Display/Change Database Server dialog box.
2. In the Display/Change Database Server dialog box, verify that the computer name for the primary and backup server is: (local). This means that FireWorks is installed as a stand-alone workstation.



3. Under Primary SQL Server, type the computer name of the primary server.  
If you do not know the computer name, on the Start menu, right-click Computer, and then click Properties. The computer name is listed under Computer name, domain, and workgroup settings. Type the name exactly as it appears there.
4. Under Backup SQL Server, type the computer name of the backup server.
5. Click Select Server. The clients are now connected to the server, and the nonredundant network setup is complete. If the client cannot reach either of these two servers, then it posts an error message.
6. Turn Windows Defender Firewall back on (see “Turning Windows Defender Firewall off and on” on page 7).
7. Add the required firewall exceptions (see Appendix D “Firewall exceptions required for networking” on page 44).

## Server in Charge state

There is a state called “server in charge” that can be used to easily represent on a map which server is in charge. How to use this can be seen in the following document, “Using Virtual Points for visual notification of Server in Charge in Redundant Fireworks”.

## To use Integrated Security / Windows authentication you must log in as Administrator with Network Setups

User from Windows Users group cannot connect to the remote SQL Server. Get the error "Login failed. The login is from an untrusted domain and cannot be used with Integrated authentication". Google search indicates that the issue is SPN records on 2 machines. The recommended tool "Kerberos Configuration Manager for SQL" produced an error "There was an issue with accessing User Account information from the system" when run.

On stand-alone systems, user from "Users" group is able to run with Integrated security. On Network system (both redundant and non-redundant) user from "Users" group will be able to run only with SQL Server credentials. Run "C:\Fireworks\Exe\ModifyConnectionString.exe" and replace "Integrated Security" part in connection strings for Fireworks and Fireworks History to "User Id=sa; Password=Firew0rks\*".

# Troubleshooting practices

## Recommended startup for FireWorks on a redundant network

1. Exit FireWorks System Control and System Builder on all computers, in this order:
  - a. Clients
  - b. Witness
  - c. Backup server
  - d. Primary server
2. Start System Control on all computers, in this order, give a minute or two between if you can:
  - a. Primary server
  - b. Backup server
  - c. Witness
  - d. Clients

This will avoid possible bouncing issues that could arise if the backup is also starting at the same time.

## Changing the FireWorks platform, or upgrading from a nonredundant to redundant network (SKUs FW-RS25UP or FW-RS15UP)

If you have installed the wrong FireWorks platform, for example, you wanted to install a redundant network but instead you installed a nonredundant network, use the procedure below to change the FireWorks platform.

**Note:** We strongly recommend that you perform a full backup prior to uninstalling FireWorks.

### To change the FireWorks platform:

1. Uninstall FireWorks.
  - a. On the Start menu, click Control Panel, and then click Programs and Features.
  - b. In the program list, right-click FireWorks, and then click Uninstall.
2. Uninstall SQL Server 2019.
  - a. On the Start menu, click Control Panel, and then click Programs and Features.
  - b. In the program list, right-click Microsoft SQL Server 2019 (64-bit), and then click Uninstall.

Be sure to minimize the Programs and Features window so you can see the dialog boxes and progress messages associated with the uninstall.

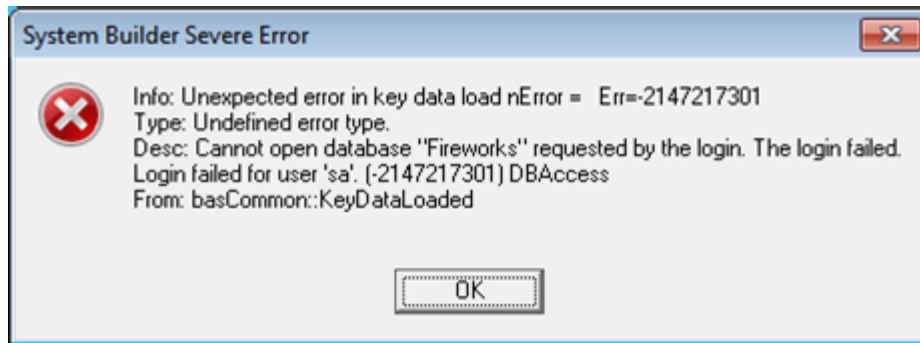
In the Setup Support Rules dialog box, click OK.

In the Select Features dialog box, select FireWorks in the "Instance to remove features from" list, click Next, click Select All, and then click Next.

In the Removal Rules dialog box, click Next, verify the selections, and then click Remove.
  - c. For all remaining items beginning with "Microsoft SQL Server," right-click the item, and then click Uninstall.
  - d. Select Microsoft VSS Writer for SQL Server 2019, right-click, and then click Uninstall.
  - e. Acknowledge any residual status or error messages resulting from the uninstalls.
3. Delete the C:\FireWorks folder and all its subfolders.
4. Delete the C:\Programs\Microsoft SQL folder and all its subfolders.
5. Restart the computer.
6. Reinstall FireWorks and the appropriate SQL Server edition.

### Database enters a suspended state

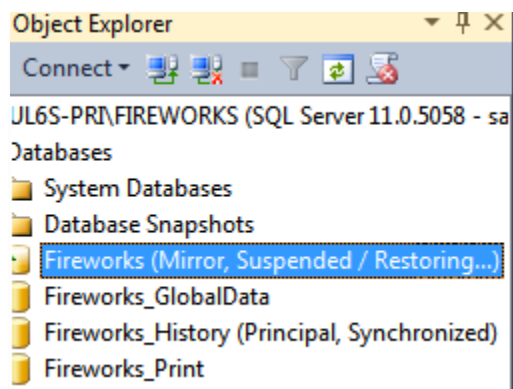
After failover or when hardware issues cause multiple computer restarts, the database can enter a “Suspended / Restoring” state that is not automatically corrected. When this happens, FireWorks displays the following error message:



When suspended, the mirror copy of the database is not available. The principal database is running without sending any logs to the mirror server, a condition known as running exposed. A session can also become SUSPENDED because of redo errors or if the administrator pauses the session. SUSPENDED is a persistent state that survives partner shutdowns and startups.

Figure 5 below shows how a database that is in a suspended state looks in the Microsoft SQL Server Management Studio.

**Figure 5: Database in a suspended state**



### To bring the database out of suspended state:

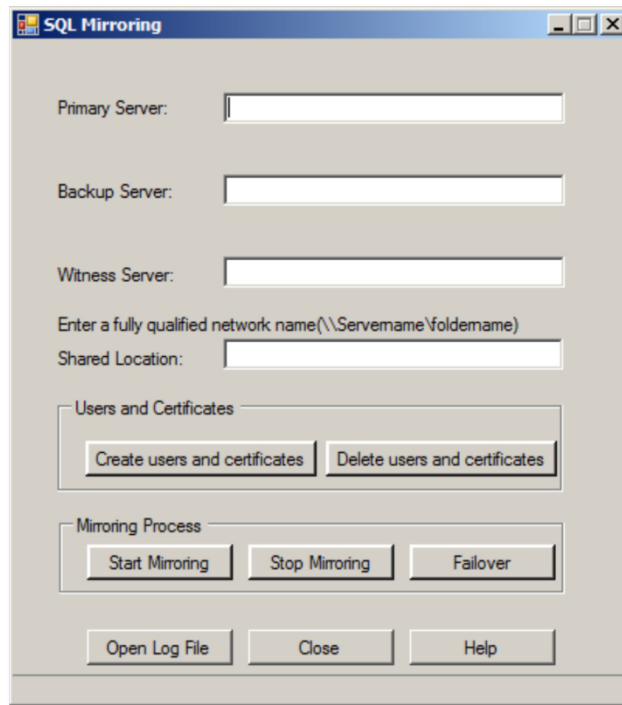
- Connect to the database engine of the either partner.
- Click on New Query for the standard bar.
- Now Enter the following Transact-SQL query in order to resume the database mirroring:
- `ALTER DATABASE Fireworks SET PARTNER RESUME;`

Right click on Fireworks database and select refresh. If database is still in Suspended state then:

- On the Start menu, in the Edwards Software\Fireworks\Utilities\Network folder, click SQL Mirroring (Redundant Networking only).
- Enter the required values, and then click Stop Mirroring. See Figure 6 on page 26.

- Click Delete Users and Certificates.
- When the process is complete, click Create Users and Certificates.
- Click Start Mirroring. The database state will return to “Principal, Synchronized.”

Figure 6: SQL Mirroring utility dialog box



### FireWorks does not start on redundant network systems

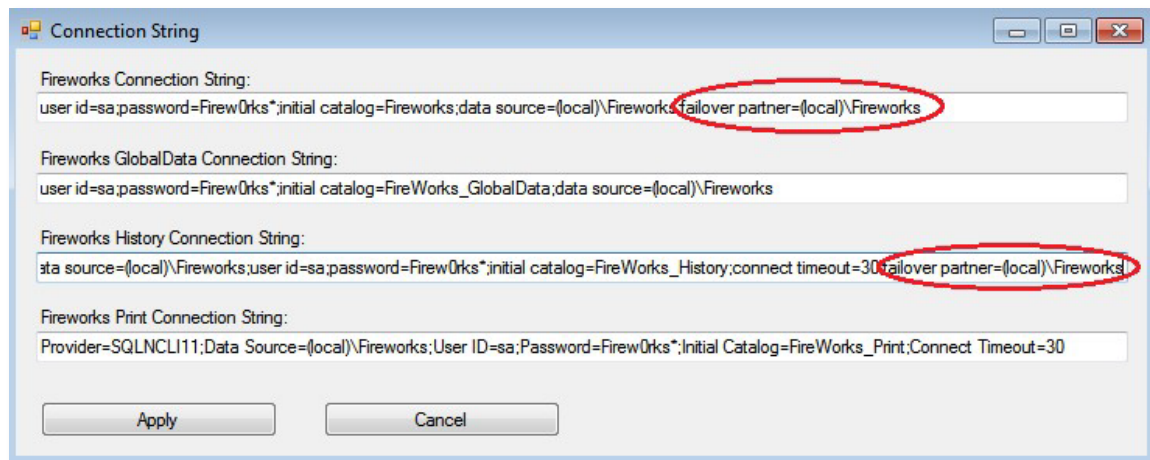
This issue may occur on redundant network systems when the database has failed over to the backup server and the connections strings were not set up correctly. FireWorks may report a database connection error or an error connecting with user “sa.”

#### To diagnose and correct this issue:

1. On the Start menu, in the Edwards Software\Fireworks\Utilities\Network folder, click Repair Connection Strings.



2. In the Connection String dialog box, verify that the Fireworks Connection String box and the Fireworks History Connection String box both include the Failover Partner delimiter, and that the delimiter correctly specifies the backup server and database instance.



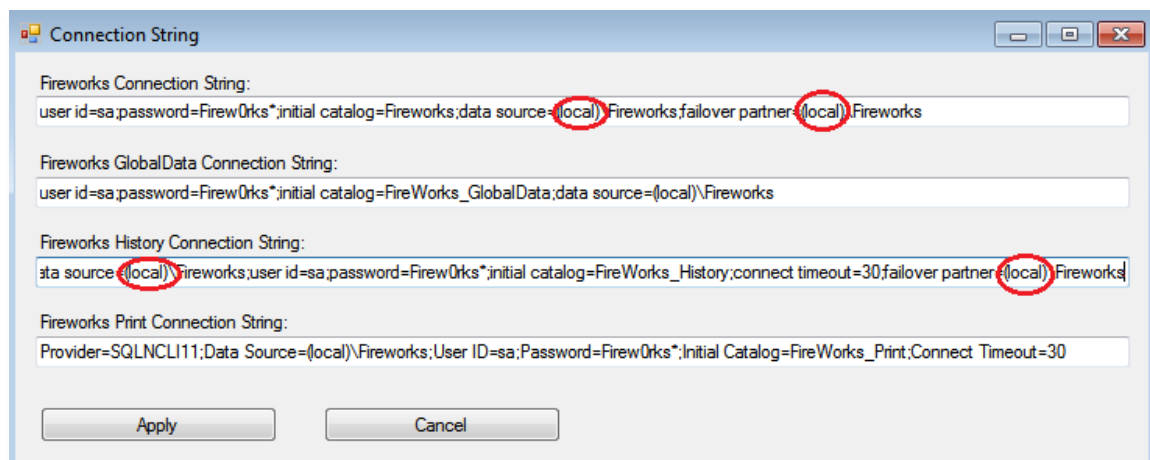
3. If the Failover Partner delimiter is missing; at the end of the current connection string, type: ; Failover Partner=(local)\Fireworks.
4. Click Apply, and then close the Connection String dialog box.
5. Start System Builder.

#### A client is not connecting to the primary and backup servers in a redundant network

1. On the Start menu, in the Edwards Software\Fireworks\Utilities\Network folder, click Repair Connection Strings.
2. In the Connection String dialog box, in the Fireworks Connection String box and in the Fireworks History Connection String box, verify that the correct server names are used to path to the FireWorks database instance.

For the Data Source delimiter, replace (local) with the primary server's computer name (e.g., FW-Primary)

For the Failover Partner delimiter, replace (local) with the backup server's computer name (e.g., FW-Backup)

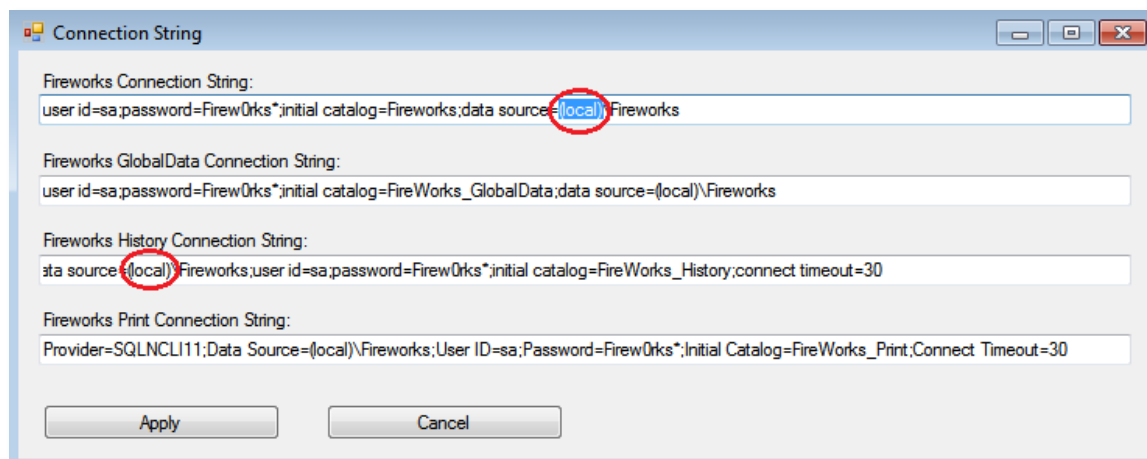


3. After the server names are replaced in their respective strings, press Apply, and then close the utility.
4. Start System Builder and it should open.

### A client is not connecting to the primary server in a nonredundant network

1. On the Start menu, in the Edwards Software\Fireworks\Utilities\Network folder, click Repair Connection Strings.
2. In the Connection String dialog box, in the Fireworks Connection String box and in the Fireworks History Connection String box, verify that the correct server name is used to path to the FireWorks database instance.

For the Data Source delimiter, replace (local) with the primary server's computer name (e.g., FW-Primary)



3. After the server's name is replaced, press Apply, and then close the utility.
4. Start System Builder and it should open.

### Your client or backup is not connecting to the primary server in a redundant or non-redundant network once firewall is on

You may encounter that once you enable the appropriate rules and turn your firewall on, your client or backup does not speak to the primary server. The steps to solve this are as follows

1. Shutdown Fireworks across all machines
2. Download Wireshark application for free from their website and install it on the client
3. With the Firewall still on, launch Fireworks across all machines, launch Wireshark and start capturing data. In the top bar enter "tcp. port == 8088" to filter the data being shown to display only traffic on TCP port 8088
4. More than likely, you'll notice that the traffic on port 8088 is not your machines IPv4 addresses and instead it's their IPv6 address.
5. Turn Wireshark off, turn Fireworks off and then go to your ethernet ports network settings and turn off IPv6 on all machines
6. Launch Fireworks again and now your backup or client should communicate to the server with the Firewall on

### Other considerations

- There can be only one event printer per server on the system. The printers used on all the servers must be the same make and model and must be configured identically.
- Having two or more computers with the same computer name wreaks havoc on the system. Typos in Host file are difficult to deduce.
- On large systems there may be a startup delay of one or two minutes. This is by design, so that all the required initialization is complete before events are received from the fire panels. This optimizes event processing speed.

- The network version of FireWorks contains a File Distribution system that will automatically sync your resource files.

This feature runs automatically in the background and normally requires no actions for correct operation. While you can modify your project on any server or client, the File Distribution system works from the primary server to push changes out to the clients and backup files. This means that you should always run System Builder from the primary server.

If you have trouble synchronizing resources across the FireWorks computers, download the file “How to troubleshoot the FireWorks File Distribution System” from the My-Eddie website for more information.

- Any undefined events that come into the server propagate to currently connected clients and are logged to history. Undefined events are not passed to clients that connect subsequently.

#### **Server address mismatch between configuration file and SQL database causes open/restore operation to fail**

- In redundant network applications, open/restore operations can fail when there is a server address mismatch between the configuration file and the SQL database, and the SQL server instance on the primary server is in the mirror state.
- For the open/restore operation to work correctly, the primary server must be the principal SQL server instance and the backup server must be the mirror SQL server instance. When this is not the case, Fireworks software performs a SQL failover to reverse their roles. A server address mismatch prevents the SQL failover from working properly.
- A server address mismatch typically occurs when the system is initially set up using computer names to identify the servers, and then later changed to use IP addresses, or vice-versa.

#### **To resolve the issue:**

1. Run C:\Fireworks\Exe\ModifyConnectionString.exe to view the connection strings used in configuration file.
2. In System Builder, right-click the primary server icon, and then click Edit properties.
3. In the Edit Properties dialog box, in the Address box, type server address taken from the “data source” portion of the Fireworks Connection String to match the server addresses in the database and the configuration file.
4. Repeat the above steps for the backup server except type the server address taken from the “Failover Partner” portion of the Fireworks Connection String.

#### **System Control posts error during initial startup on a network setup**

- During initial startup of System control on redundant/non-redundant setup, if you get an error stating "Sitemap is not loaded" on backup server or client machines, then wait for a couple of minutes and click on "Previous Map" icon on Map Display window. This refreshes the image on the map. If this does not work out, restart the System control application.
- This happens because the maps/images/sounds files must be copied from primary server to backup and clients. Due to the high network activity, there might be a delay in copying the files over to the other system and when system control is invoked in between the file might not be present which results in the error.

#### **Multiple display and control center status indicators in System Control may not update correctly when you restart the gateway control unit**

- When you restart the gateway control unit (i.e., the control unit that provides the Gateway Type III port used to connect to FireWorks), the control unit temporarily drops communication through the port. When communication is reestablished, System Control retrieves a status report, and then reconciles the Event List with the status report.
- Depending on your system, the status report that System Control retrieves may be incomplete. For example, it may not contain points disabled at startup. If this happens, events displayed in System Control may not match the events on the system. To correct this, you must manually reconcile the Event List.

**Note:** You must have the System Command user right to manually reconcile the Event List. If the System Commands command on the Application menu is not available, your user account does not have sufficient user rights. See System Builder Help or System Control Help for instructions on how to assign user rights.

The Node Status Form “F2” will not show “Reset”, Lamp Test, or Alternate Sensitivity status from the EST4. ID 2993, ID 2994, and ID 3004.

### **Redundant Fireworks/System Builder [Restore project]**

This operation should not be attempted when any Station has a Network Fault active while System Control application is running. This station System Control with Network Fault active will not receive the shutdown notification for system changes.

If a user gets into this scenario, below are the steps for coming out of it:

1. The user must open SQL management studio on primary server.
2. Verify if the Fireworks and Fireworks\_history database status is Principal/Synchronized.  
If it is, right click on the database and stop SQL mirroring.  
If it is not, right click on database and failover the database.
3. Now right click the database and stop SQL mirroring.
4. After this, you can go ahead and restore the database.

### **Nonredundant Fireworks System Builder [Import from Client]**

Import operation should not be performed at the same time and same node from both server and client station. This is not the use case in the field.

If user perform import for same node and same time from server and client station, and from client station user get node lock and other message, below are the steps for coming out of it:

1. The user must wait until Import is completed on Server side.
2. Close System Builder on the server and then restart System Builder on the client side.
3. By doing so, System Builder will have updated information and will be in sync with server.

### **Primary computer displaying “Named Pipes” error upon opening**

When attempting to open System Control on the primary server computer, you may get the following or similar message, “A network-related or instance-specific error occurred while establishing a connection to SQL server.” FireWorks displays this message when there is a database fail-over issue. To verify whether it is a fail-over issue, start Microsoft SQL Management Studio on the backup server computer, and then verify that the Fireworks database instance indicates it is the principal database.

To fix this issue, open the Windows Services app on the backup server computer, and then stop then start SQL Server (FIREWORKS). Verify that the Fireworks database instance on the primary server computer indicates it is the principal database and that the Fireworks database instance on the backup server computer indicates it is the mirror database. System Control on the primary server computer should open without any issues.

### **Fatal SQL error due to 2 out of 3 Cluster Machines going offline/changing active FireWorks issue**

You may encounter that if for some reason two out of three of your cluster machines go offline, once they come back online and you try to get Fireworks working again, Fireworks may start behaving strangely. The main thing you may encounter is that your ability in Fireworks to change who is the active primary machine (selecting “Change Active Fireworks Server”) will not behave currently. You will notice that the machine you are trying to set as primary will quickly turn back to backup.

The solution to this issue is simple. By opening your database on your backup machine, you will notice that it is most likely set to “Principal”, we want to set it back to “Mirror” so that our primary machine gets forced back into

the principal role. To do this, on the backup machine, go to Windows services and stop and start your “SQL Server (FIREWORKS)” service. Once done, check your both your primary and backup databases, your primary should be “Principal” and your back should be “Mirror”. Open Fireworks again and attempt to “Change Active Firework Server”, you should no longer face any issues. Even if you never got the “Changing Active Fireworks” issue, we still recommend executing the steps above if 2 out of 3 machines in your cluster went offline.

### **Primary or Mirrored Database does not stay on Primary and switches to Backup**

We have occasionally seen where when after the system fails to the backup the system will try to switch back to the primary itself and cause the system to behave badly.

If you encounter this (during testing) you should perform one of the following:

Switch from “Integrated Security” to SQL Server Security:

1. Start ModifyConnectionStaring.exe (in C:\Fireworks\EXE)
2. In “Fireworks Connection String” replace “integrated security=True;” with “User Id=sa;Password=Firew0rks\*”.
3. In “Fireworks History Connection String” replace “integrated security=SSPI;” with “User Id=sa;Password=Firew0rks\*”.

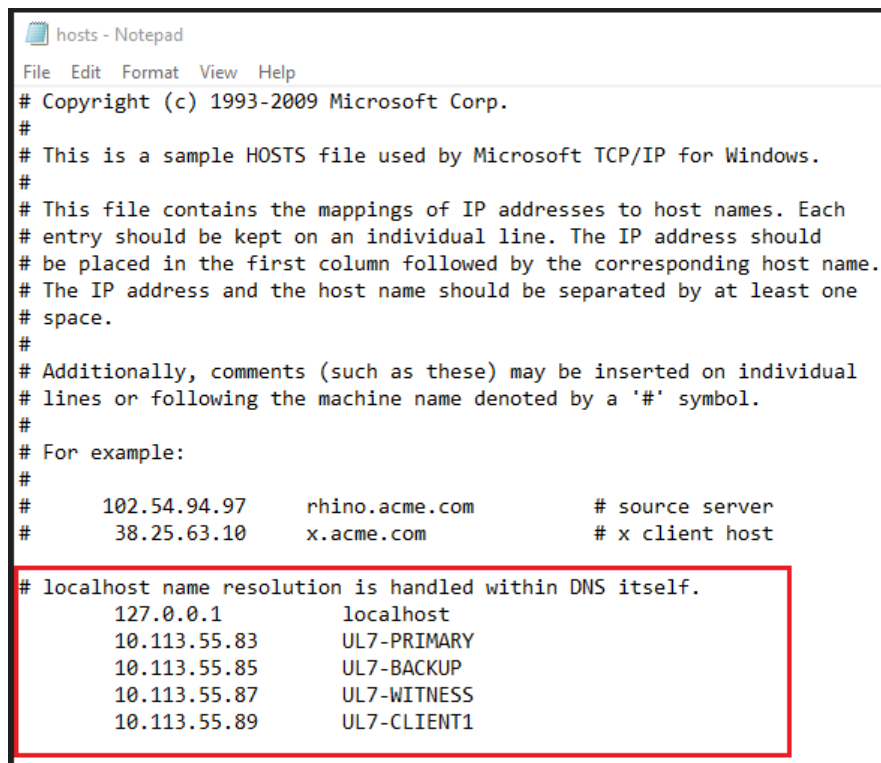
Reset the database by making sure Primary is principal and Backup is mirror:

1. In the backup machine, go to SQL management studio, it will most likely be “Principal” in the database
2. While on the backup machine, go to Windows services and find “SQLServer (Fireworks)”
3. Right click on it >> press “Stop” >> Then “Start” it again
4. Go back to the backup machines SQL studio and it should now be set to Mirror, then if you check your primary machine its database should be set to principal
5. Try again and your system should work as expected

### **Setting up your host file**

Unless you have a DNS server, we strongly recommend setting up a host file in your system. Each computer in your system should have one configured. Every Windows 10 image will have a default one. What we want to do is edit it by replacing its contents with our system's information.

We want to enter the IP address of one of our computers followed by its computer name. Then on a new line we want to enter the next machine. We want to continue doing this until all machine's IP's and computer names have been listed. Use the picture below as a guide on how yours should look. Only edit the red area:



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       10.113.55.83      UL7-PRIMARY
#       10.113.55.85      UL7-BACKUP
#       10.113.55.87      UL7-WITNESS
#       10.113.55.89      UL7-CLIENT1
```

### Synchronizing Node status in client machines with server

When restoring a project in network setup, be sure to check your communications status on the clients.

If you find that your node communications status is not correct and in sync, you should restart system control on the server.

If you are not using DNS, you should not put any server addresses in the IPv4 setup properties. Putting values in may cause the system to behave erratically as it tries to connect to an invalid DNS Server.

# Troubleshooting the file distribution system

## Introduction

FireWorks nonredundant and redundant networks use a file distribution system to keep maps, icons, and other important files synchronized across all client workstation computers.

### Normal behavior

Each client workstation computer is synchronized with the *logical* primary server computer (identified in System Control Network Status). The synchronization process may take several minutes to complete the first time the *logical* primary server computer and a client workstation computer synchronize, depending on how many maps and other files you have. Afterwards, synchronization only takes a second or so.

FireWorks creates a log file on the *logical* primary server computer each time it and a client workstation are synchronized. The log file is in the "C:\Fireworks\Log" folder. The file's name is "(Workstation Address).TXT".

FireWorks networks use a hub and spokes design. The hub is the *active* FireWorks server computer. On a redundant FireWorks system the *active* FireWorks server computer might change.

Typically, the synchronization works fine and the contents of the "(Workstation Address).TXT" file will be "Archives match. No files transferred." If files were recently changed, this file will contain the list of files that were transferred.

### Abnormal behavior

If you suspect that a workstation has not been updating properly, please check the "C:\Fireworks\Log\Workstation Address).TXT" file on the *logical* primary server computer. It may contain a request to take action.

## Firewall unopen port issues

The port for FWK\_Unison must be opened between the server computers and the client workstation computers. If you are using an FW-UL6 computer, this port already exists in the firewall. You just need to enable it.

### To create the inbound exception rule manually:

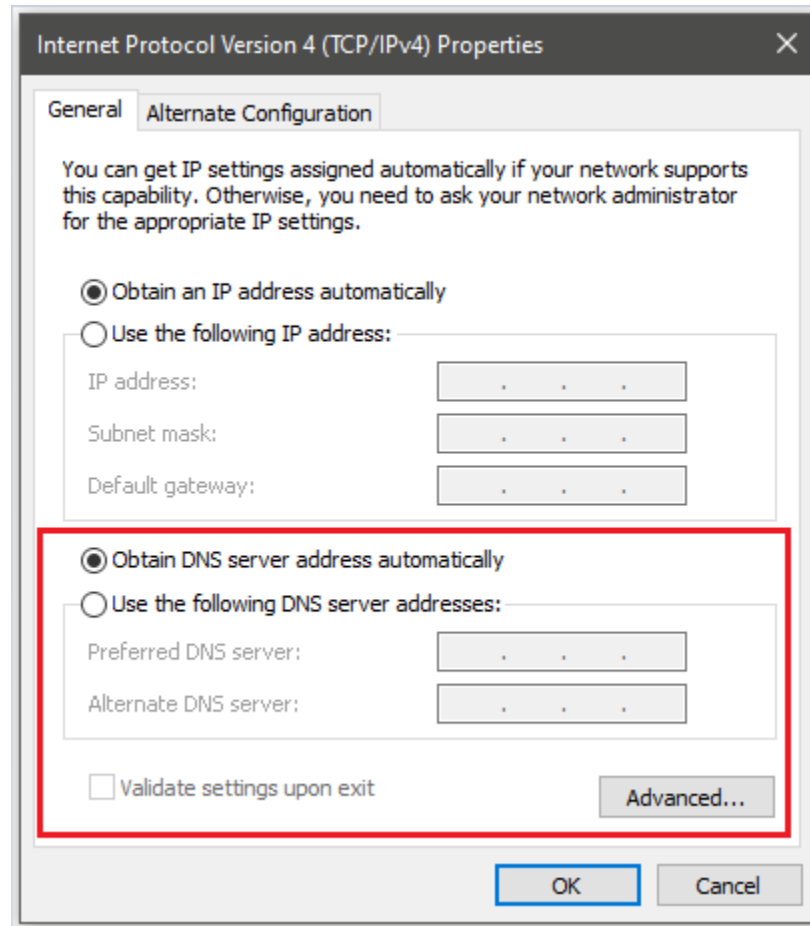
1. In the Search box on the Windows task bar, type: `mmc`, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On the File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. Click Program and in the browse menu go to the following path: "C:\Fireworks\exe\FWK\_Unison.exe" and press Next.

9. Select "Allow the connection," and then Press Next. On the next window leave all three Firewalls checked, then press Next.

10. On the final window, give the inbound exception rule a name. Once done, press Finished below.

The name of the exception in the Firewall is "Unison Exe Firewall Inbound Exception Rule". Make sure to access the firewall through MMC, open a group policy snap in, and then find the Firewall. We recommend you follow this method. Otherwise, you may not get full access to the Firewall.

If you are not using DNS, you should not put any server addresses in the IPv4 setup properties. Putting values in may cause the system to behave erratically as it tries to connect to an invalid DNS Server.



If while using IP address, you notice your database is not responsive or are after a failover your system automatically fails over back to the previous setting you may be experiencing a "Reverse DNS lookup".

The way to solve this issue is to use a hosts file, you need one on each PC in the network.

The file will be the same on each station.

The hosts file goes in the following directory C:\Windows\system32\drivers\etc there may be one there already, in that case you edit it.

The format of the file is for example as such, with an entry for each PC in your FireWorks Network.

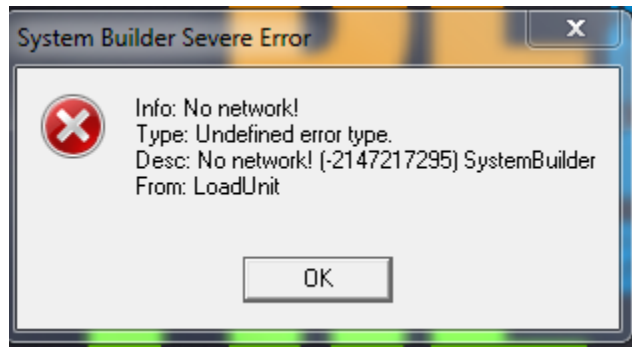
```
10.113.55.218 FW-PRIMARY
10.113.55.217 FW-BACKUP
10.113.55.219 FW-CLIENT1
```



### Working on your database project on a PC with an Edwards Key but not a FireWorks Key.

Edwards still supports this with an EST3 SDU key allowing builder to run and allowing off line modifications to the project database, You will need to have Network connection on the PC though. If you do not you will see this message from the system.

Mode they will send and accept Acknowledgement messages from FireWorks.



### Effects of Local vs. Proprietary Modes

If the Edwards Panel is in Proprietary Mode they will send and accept Acknowledgement messages to and from FireWorks.

If an Edwards Panel is in proprietary mode and accepts an Acknowledge message, it also shares it or propagates that message to all the other panels in the fire panel network. So if a user at panel one or a FireWorks station at panel one sends an Acknowledge message the panel will propagate this to all panels. So in the end the FireWorks in proprietary mode functions just like another panel. As well an acknowledge is shared out all ECP ports.

Proprietary mode also affects the FireWorks sending of a panel silence to the EST3 or EST4 Network. If in Local mode and not Proprietary mode, then on the Acknowledge of the last active point in FireWorks for that Node FireWorks will send a panel silence. This causes the FireWorks operation to mirror the panel operation, that is make the panel stop beeping when all points have been acknowledged.

If you have a Redundant Network and you acknowledge a point at one of the servers, based on the sentence above it will after some brief period automatically acknowledge at the other server.

You can tell FireWorks what mode the panel is in via the Node Properties Form, the default is "Local". This information is in the gateway files but is not read. If you set this to "Local" FireWorks will not send Acknowledges to the panel because it does not expect the panel to accept them.

### Locked files

When a file has been updated on both systems, but is somehow different, the log file will show a line containing "<-?->". When this occurs, update the file manually on both computers to see if that resolves the issue.

### Damaged stored directory on client workstation

There may be times when the stored directory on a workstation has been damaged. If you see a log file with output like the following, take the appropriate action as stated in the log file.

```
Fatal error: Warning: inconsistent state.  
The archive file is missing on some hosts.  
For safety, the remaining copies should be deleted.  
Archive ar433240 on host FWK-SRV-2 is MISSING  
Archive ar6a60c1 on host FWK-R320-CLN-17 should be DELETED
```

Please delete archive files as appropriate and try again or invoke Unison with `-ignorearchives` flag.

This output states that file `ar6a60c1` must be deleted on host `FWK-R320-CLN-17`. The file is located in the `"C:\Users\{Logged in user}\.Unison"` directory. If you can't find the file, use the File Explorer to locate the file and delete it.

Once the file has been deleted, the File Distribution System will be able to recreate the file with the proper contents and determine what to do next. This will generally happen within a few minutes when the File Distribution System works on synchronizing files on this workstation again. No restart is required. The File Distribution System continually polls the workstations looking for changed files to distribute.

If you are unable to determine what the File Distribution System is telling you, please contact your support team.

# Appendix A

## Network software SKUs

See Table 3 below for a list of network software SKUs. Figure 7 shows you how to interpret the SKU numbers.

Figure 7: FireWorks networks SKUs

**FW – NCZZFP**

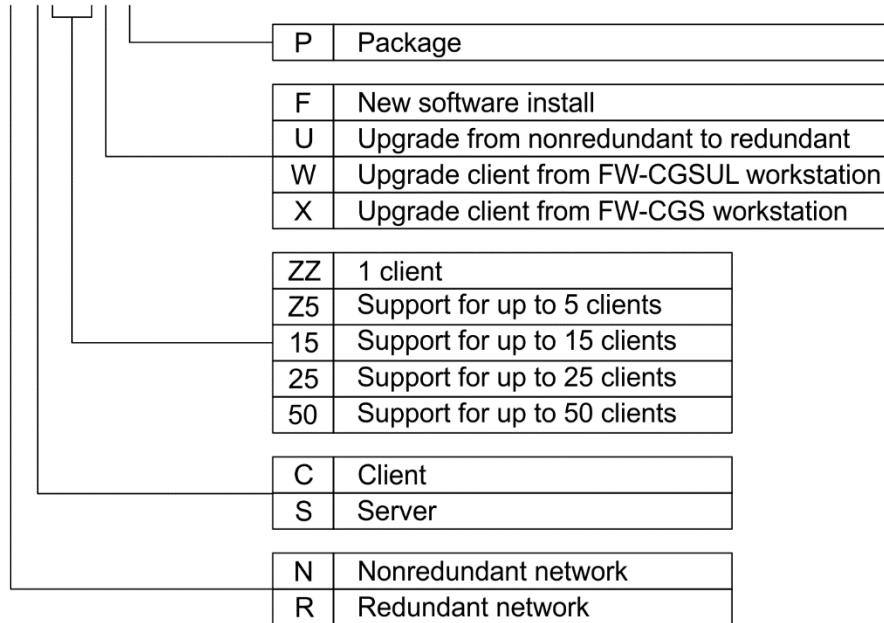


Table 3: SKU descriptions

Type	SKU	Description	Notes
Client	FW-NCZZFP	New nonredundant system client license. Requires UL6W Class workstation computer and FW-CGSUL or FW-CGS. HASP key PIN.	Nonredundant network client workstation.
Client	FW-RCZZFP	New redundant system client license. Requires UL6W Class workstation computer and FW-CGSUL or FW-CGS. HASP key PIN.	Redundant network client workstation. Will automatically connect to primary server IP.
Server	FW-NSZ5FP	New 5 seat nonredundant server license. Includes FW-CGSUL. Requires UL6S Class server computer and FW-CGSUL. HASP key PIN set for servers.	Nonredundant server. Supports up to five nonredundant clients for a total of six possible points of control.
Server	FW-NS15FP	New 15 seat nonredundant server license. Includes FW-CGSUL. Requires UL6S Class server computer and FW-CGSUL. HASP key PIN set for servers.	Nonredundant server. Supports up to 15 nonredundant clients for a total of 16 possible points of control.
Server	FW-RSZ5FP	New 5 seat redundant server license. Includes FW-CGSUL. Requires UL6S Class servers. HASP key PINs set for servers.	Redundant service server license set. Supports up to 5 IP client workstations. Includes 3 FireWorks servers, 2 full MS SQL, and 1 MS SQL Express licenses for primary, backup, and witness servers and 5 clients.

Type	SKU	Description	Notes
Server	FW-RS15FP	New 15 seat redundant server license. Includes FW-CGSUL. Requires UL6S Class servers. HASP key PIN set for servers.	Redundant service server license set. Supports up to 15 IP client workstations. Includes 3 FireWorks servers, 2 full MS SQL, and 1 MS SQL Express licenses for primary, backup, and witness servers and 15 clients.
Server	FW-RS25FP	New 25 seat redundant server license. Includes FW-CGSUL. Requires UL6S Class servers. HASP key PIN set for servers.	Redundant service server license set. Supports up to 25 IP client workstations. Includes 3 FireWorks servers, 2 full MS SQL, and 1 MS SQL Express licenses for primary, backup, and witness servers and 25 clients.
Server	FW-RS50FP	New 30 seat redundant server license. Includes FW-CGSUL. Requires UL6S Class servers. HASP key PIN code set for servers.	Redundant service server license set. Supports up to 30 IP client workstations. Includes 3 FireWorks servers, 2 full MS SQL, and 1 MS SQL Express licenses for primary, backup, and witness servers and 50 clients.
Server	FW-SQL5UP	5 Seat FireWorks Redundant Server Package for updating FireWorks 8.x redundant networks	Includes two redundant server licenses, five client access licenses (CALs), and two SQL Server 2019 Standard DVDs.
Server	FW-SQL15UP	15 Seat FireWorks Redundant Server Package for updating FireWorks 8.x redundant networks	Includes two redundant server licenses, 15 client access licenses (CALs), and two SQL Server 2019 Standard DVDs.

## Appendix B

### SQL Mirroring utility functions

The SQL Mirroring utility also provides the following functions:

- Delete users and certificates
- Stop SQL mirroring
- Start SQL mirroring

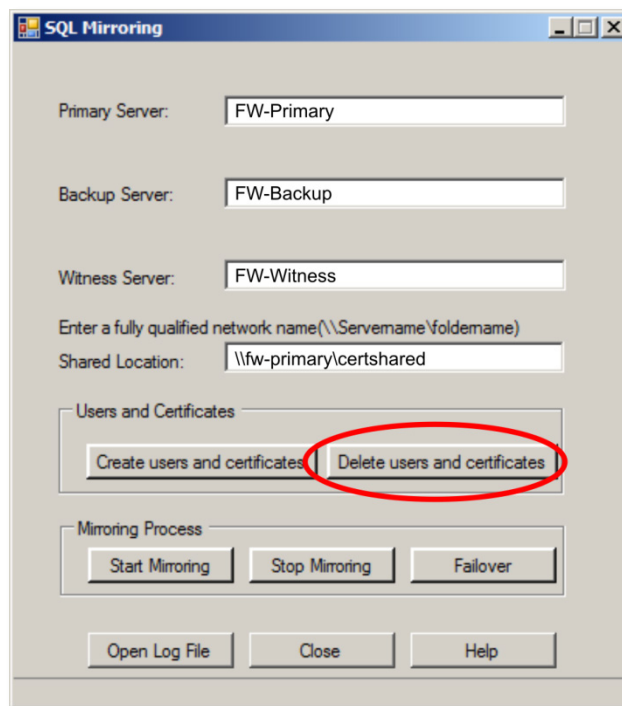
Use these functions only as described here, or with assistance from the Edwards Technical Support staff.

#### Deleting users and certificates

Scenario: This is used if you want to take the computer back to their initial condition, or if the computer name of one of the servers was changed after the mirroring process started.

Implementation: Enter all the fields as shown in Figure 8 below, and then click Stop Mirroring. Wait for the utility to complete the process, and then click Delete Users and Certificates. Again, wait for the utility to complete the process.

Figure 8: Delete users and certificates



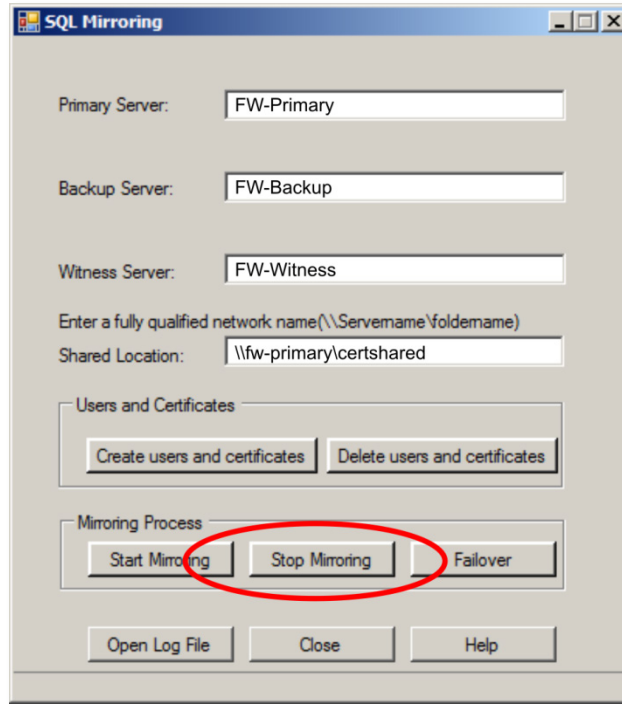
Make sure that you recreate the users and certificates before trying to set up again.

#### Stop mirroring

Scenario: This is used if you want to manually stop the mirroring process. Don't do this unless instructed to by the Edwards Technical Support staff.

Implementation: Enter all the fields as shown in Figure 9 on page 40, and then click Stop Mirroring to stop the mirroring process.

Figure 9: Stop mirroring



Once you click Stop Mirroring (or open a different project, create a new project, or restore an old project), you will be asked if you want to start SQL mirroring the next time you start System Builder. If not, run `C:\Fireworks\Database\SQLMirroring\ClearMirroringTables.bat`.

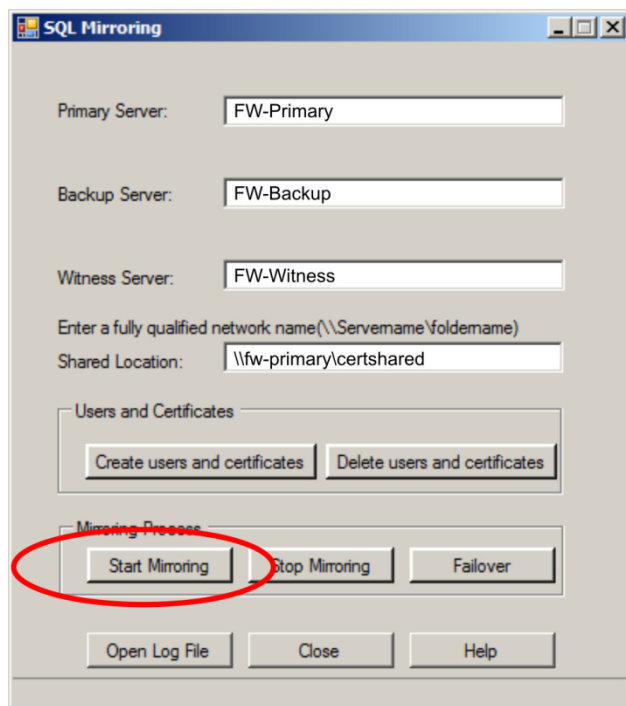
### Starting mirroring after the FireWorks restore function

Database backup and restore operations can be performed normally using the FireWorks software. No extra steps are required, but these functions can only be performed from the primary server. Backup and restore operations should not be done from the backup or witness servers, or from any client computer.

Once the database is restored you will need to restart the mirroring function. On starting, System Builder displays a message box that lets you start the SQL Mirroring utility. Repeat the procedure given in "Setting up SQL mirroring" on page 17.

The Create Users and Certificates process (step 5 in Setting up SQL mirroring") is required only once for the FireWorks network. You don't need to repeat it after a restore.

Figure 10: Start mirroring



### Troubleshooting mirroring failures

A document with useful troubleshooting information is stored on your computer during the FireWorks installation.

# Appendix C

## Changing the SQL server type

### Introduction

This topic shows you how to switch between SQL Server 2019 Express and SQL Server 2019 Standard.

In summary, the process is to manually remove (uninstall) the incorrect edition of SQL Server 2019, and then let the FireWorks installation wizard install the correct edition of SQL Server 2019.

This may be required if, for example, you installed SQL 2019 Server Express by mistake on a redundant network server, which requires SQL 2019 Server Standard.

This topic can be used as a reference in these scenarios:

- Users want to convert their stand-alone FireWorks computer to a redundant or nonredundant FireWorks network server.
- Users inadvertently installed SQL Server 2019 Express on a primary or backup server computer.
- Users inadvertently installed SQL Server 2019 Standard on a client computer.
- Users inadvertently installed SQL Server 2019 Standard on a witness computer.

### SQL Server editions

The following table shows the editions of SQL Server 2019 that are required for each type of FireWorks computer.

Computer	SQL 2019 Server edition
Primary server (redundant network)	SQL Server 2019 Standard
Primary server (nonredundant network)	SQL Server 2019 Express
Backup server	SQL Server 2019 Standard
Witness	SQL Server 2019 Express
Client computer	SQL Server 2019 Express
Stand-alone computer	SQL Server 2019 Express

**To determine which edition of SQL Server 2019 is installed on a computer:**

1. On the Start menu, in the Edwards Software\Fireworks\Utilities folder, click Key and Database Verify.

## Changing from SQL Server 2019 Express to SQL Server 2019 Standard

**To change from SQL Server 2019 Express to SQL Server 2019 Standard:**

1. Right-click the Windows Start button, and then click Apps and Features.

If your preferences are set so that the Control Panel is not displayed as a menu, you'll see the Adjust Your Computer's Settings page. In the Programs group, click Uninstall A Program.

2. In the Apps & Features list, right-click Microsoft SQL Server 2019 (64-bit), and then click Uninstall.
3. In the SQL Server 2019 dialog box, click Remove.

This starts the Remove SQL Server utility. You'll work through several pages displayed by the utility.



4. On the Setup Support Rules page, click OK.
5. On the Select Instance page, make sure that FIREWORKS is selected in the Instance to Remove Features From list, and then click Next.
6. On the Select Features page, click Select All, and then click Next.
7. On the Removal Rules page, click Next.
8. On the Ready to Remove page, click Remove.
9. When the utility displays the Complete page, showing that the removal was completed successfully, close the dialog box, and then restart the computer.
10. Install FireWorks. When prompted to load SQL Server 2019 Standard, click Yes.

## Changing from SQL Server 2019 Standard to Express

**To change from SQL Server 2019 Standard to SQL Server 2019 Express:**

1. Repeat steps 1 through 9 in "Changing from SQL Server 2019 Express to SQL Server 2019 Standard" on page 42.
2. Install FireWorks. When prompted to load SQL Server 2019 Standard, click No.

# Appendix D

## Firewall exceptions required for networking

Firewall inbound rules are required for FireWorks to work properly when Windows Defender Firewall is turned on. This section provides instructions for adding the required Firewall exceptions. If you have any company specific ports that are required for your business, please be sure to create them in the same location as the ones below.

**Note:** In the Firewall's inbound rule area you will see the following SMB ports: TCP 445, 139 and UDP 137, 138. These ports are enabled by default and are set to block these ports. To set up your system you will need to disable these rules as file sharing will be needed throughout the configuration

### Inbound rules for computers in redundant networks

#### Port inbound rules

Port inbound rules control connections to specified ports. Make sure that every computer in the redundant network has the TCP port inbound rules listed in Table 4 below and that the inbound rules are enabled.

**Table 4: Port inbound rules for redundant network computers**

Name	TCP Port	Purpose
445 Inbound	445	Filesharing
5022 Inbound	5022	SQL Mirroring
5023 Inbound	5023	SQL Mirroring
5024 Inbound	5024	SQL Mirroring
8088 Inbound	8088	Client and Server communications

#### To add port inbound rules:

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. On the Rule Type page, click Port, and then click Next.
9. On the Protocol and Ports page, click TCP and then in the Specific local ports box, type the port number (e.g., 8088), and then click Next.
10. On the Action page, click Allow the connection, and then click Next.

11. On the Profile page, select the Domain, Private, and Public check boxes, and then click Next.
12. On the Name page, in the Name box, type the inbound rule's name (e.g., 8088 Inbound), and then click Finish.

### Program inbound rules

Program inbound rules control connections to specified programs. Make sure that every computer on the redundant network has the program inbound rules listed in Table 5 below and that the inbound rules are enabled.

Please note that FireWorks 9.2 includes a new OH Network Receiver and SQL version. The firewall exceptions for older versions are also listed below. Please make sure to only make/enable exceptions for the version that your system will be using.

**Table 5: Program inbound rules for redundant network computers**

Name	Program path
Web Client Inbound	%SystemDrive%\Fireworks\EXE\FWK_RemoteAccessServer.exe
OHLite Version 3.1.1 Inbound	C:\oh-networkreceiver\jre\bin\javaw.exe
OHLite Version 4.1 Inbound	C:\program files (x86)\adoptopenjdk\jre-16.0.1.9-hotspot\bin\javaw.exe
SQL Browser Inbound	%ProgramFiles%\Microsoft SQL Server\90\Shared\sqlbrowser.exe
SQL 2012 Server Inbound	%ProgramFiles%\Microsoft SQL Server\MSSQL11\FIREWORKS\MSSQL\Binn\sqlservr.exe
SQL 2019 Server Inbound	%ProgramFiles%\Microsoft SQL Server\MSSQL15\FIREWORKS\MSSQL\Binn\sqlservr.exe
Unison Inbound	%SystemDrive%\Fireworks\EXE\FWK_Unison.exe

### To add program inbound rules:

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. On the Rule Type page, click Program, and then click Next.
9. On the Program page, in the This program path box, type the program's path and file name (e.g., %SystemDrive%\Fireworks\EXE\FWK\_Unison.exe), and then click Next.
10. On the Action page, click Allow the connection, and then click Next.
11. On the Profile page, select the Domain, Private, and Public check boxes, and then click Next.
12. On the Name page, in the Name box, type the inbound rule's name (e.g., Unison Inbound), and then click Finish.

Firewall inbound rules are required for FireWorks to work properly when Windows Defender Firewall is turned on. This section provides instructions for adding the required Firewall exceptions.

### **IP Address inbound rules**

You may encounter that even with the ports and program exceptions created above, your system may still not operate correctly with the firewall on. A solution to this is to create a firewall exception using the IP address of the machines in your redundant system. Create an inbound IP address exception of each machine in your redundant system on each machine.

#### **To add IP Address inbound rules:**

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. On the Rule Type page, click Custom, and then click Next.
9. On the Program page, leave All programs selected and press Next.
10. On the Protocol and Ports page, leave everything default which should allow Any protocol and All Ports, then click Next.
11. On the Scope page, under Which remote IP address does this rule apply to? Select These IP Addresses and then press Add. This will open a new window called IP Address, enter the IP address of the machine you would like to create an exception for, then press OK. This will close the IP Address window. Repeat these steps for all the machines in your redundant system, once you have entered them all, press Next.
12. On the Action page, select Allow the connection and then click Next.
13. On the Profile page leave all three firewall options checked and press Next.
14. On the Name page, enter a name for the IP Address exception we just created and press Finished.

## **Inbound rules for computers in nonredundant networks**

### **Port inbound rules**

Port inbound rules control connections to specified ports. Make sure that every computer in the nonredundant network has the TCP port inbound rules listed in Table 6 on page 47 and that the inbound rules are enabled.

**Table 6: Port inbound rules for nonredundant network computers**

Name	TCP Port
8088 Inbound	8088

**To add port inbound rules:**

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. On the Rule Type page, click Port, and then click Next.
9. On the Protocol and Ports page, click TCP and then in the Specific local ports box, type the port number (e.g., 8088), and then click Next.
10. On the Action page, click Allow the connection, and then click Next.
11. On the Profile page, select the Domain, Private, and Public check boxes, and then click Next.
12. On the Name page, in the Name box, type the inbound rule's name (e.g., 8088 Inbound), and then click Finish.

**Program inbound rules**

Program inbound rules control connections to specified programs. Make sure that every computer on the redundant network has the program inbound rules listed in Table 7 below and that the inbound rules are enabled.

Please note that FireWorks 9.2 includes a new OHLite and SQL version. The firewall exceptions for older versions are also listed below. Please make sure to only make/enable exceptions for the version that your system will be using.

**Table 7: Program inbound rules for nonredundant network computers**

Name	Program path
Web Client Inbound	%SystemDrive%\Fireworks\EXE\FWK_RemoteAccessServer.exe
OHLite Version 3.1.1 Inbound	C:\oh-networkreceiver\jre\bin\javaw.exe
OHLite Version 4.1 Inbound	C:\program files (x86)\adoptopenjdk\jre-16.0.1.9-hotspot\bin\javaw.exe
SQL Browser Inbound	%ProgramFiles%\Microsoft SQL Server\90\Shared\sqlbrowser.exe
SQL 2012 Server Inbound	%ProgramFiles%\Microsoft SQL Server\MSSQL11.FIREWORKS\MSSQL\Binn\sqlservr.exe
SQL 2019 Server Inbound	%ProgramFiles%\Microsoft SQL Server\MSSQL15.FIREWORKS\MSSQL\Binn\sqlservr.exe
Unison Inbound	%SystemDrive%\Fireworks\EXE\FWK_Unison.exe

### **To add program inbound rules:**

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.
8. On the Rule Type page, click Program, and then click Next.
9. On the Program page, in the This program path box, type the program's path and file name (e.g., %SystemDrive%\Fireworks\EXE\FWK\_Unison.exe), and then click Next.
10. On the Action page, click Allow the connection, and then click Next.
11. On the Profile page, select the Domain, Private, and Public check boxes, and then click Next.
12. On the Name page, in the Name box, type the inbound rule's name (e.g., Unison Inbound), and then click Finish.

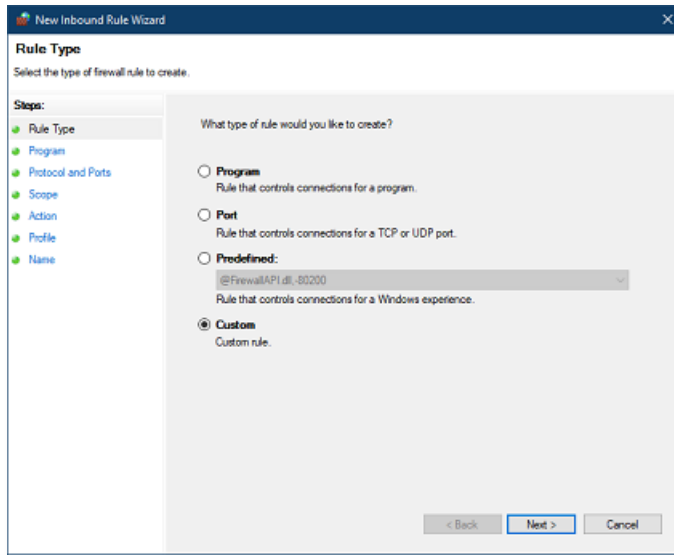
## **Inbound rule to allow ping across the network**

To allow ping across the FireWorks 9.2 network, you must add the following inbound rule to every computer on the network.

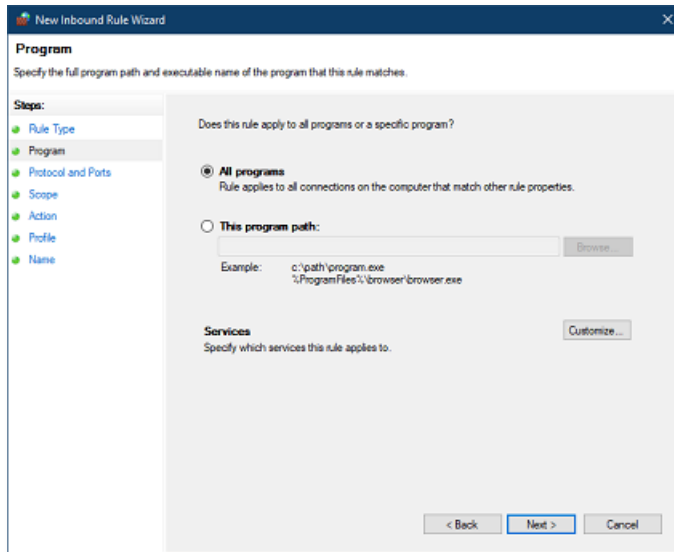
### **To add an inbound rule that allows ping across the network:**

1. In the Search box on the Windows task bar, type: mmc, and then click Run as administrator to open Microsoft Management Console.  
Click Yes to allow Microsoft Management Console to make changes.
2. On File menu, click Add/Remove Snap-In.
3. In the Add or Remove Snap-ins dialog box, in the Available Snap-ins list, select Group Policy Object, and then click Add.
4. In the Select Group Policy Object dialog box, verify Group Policy Object is set for Local Computer, click Finish, and then click OK.
5. In the console tree, under Local Computer Policy\Computer Configuration\Windows Settings\Security Settings, open the Windows Defender Firewall with Advanced Security folder, and then click Windows Defender Firewall with Advanced Security – Local Group Policy Object.
6. In the middle pane, in the Getting Started group, click Inbound Rules.
7. On the Action menu, click New Rule to start the New Inbound Rule Wizard.

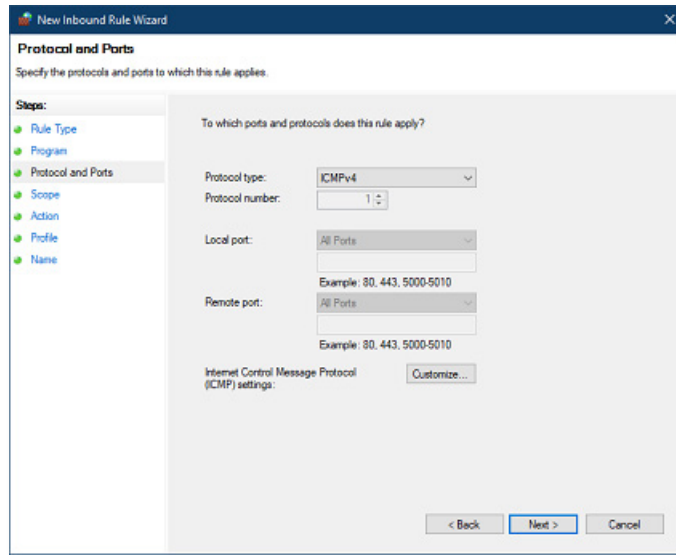
8. On the Rule Type page, click Custom, and then click Next.



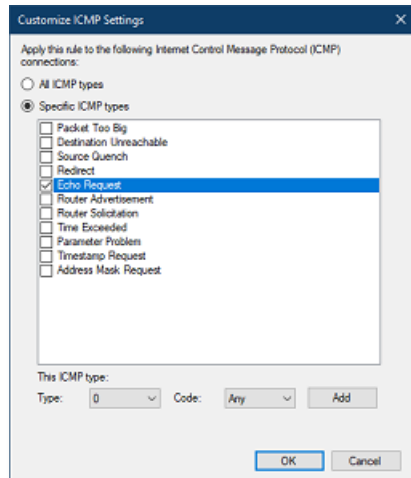
9. On the Program page, click All programs, and then click Next.



10. On the Protocol and Ports page, in the Protocol type list, select ICMPv4, and then click Customize.



11. On the Customize ICMP Settings dialog box, click Specific ICMP types, and then select Echo Request.



Click OK, and then click Next.



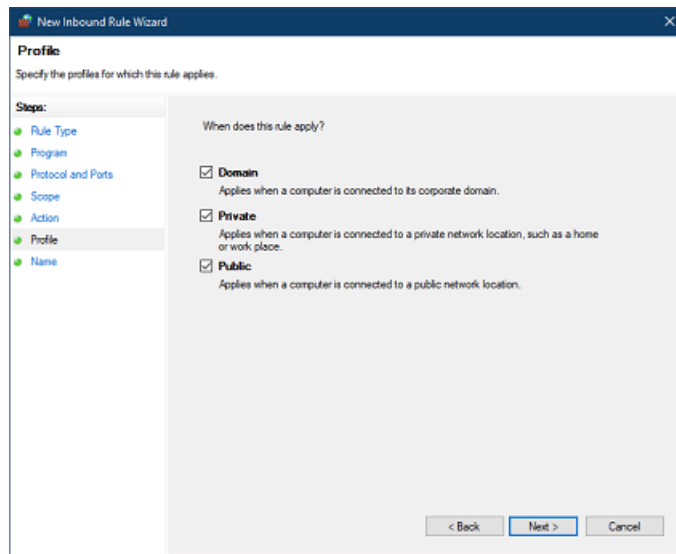
12. On the Scope page, select Any IP address for both, and then click Next.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Scope' page. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' It contains two sections: 'Which local IP addresses does this rule apply to?' and 'Which remote IP addresses does this rule apply to?'. Both sections have a radio button selected for 'Any IP address'. Below each section is a text box for 'These IP addresses:' with 'Add...', 'Edit', and 'Remove' buttons. A 'Customize...' button is also present. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

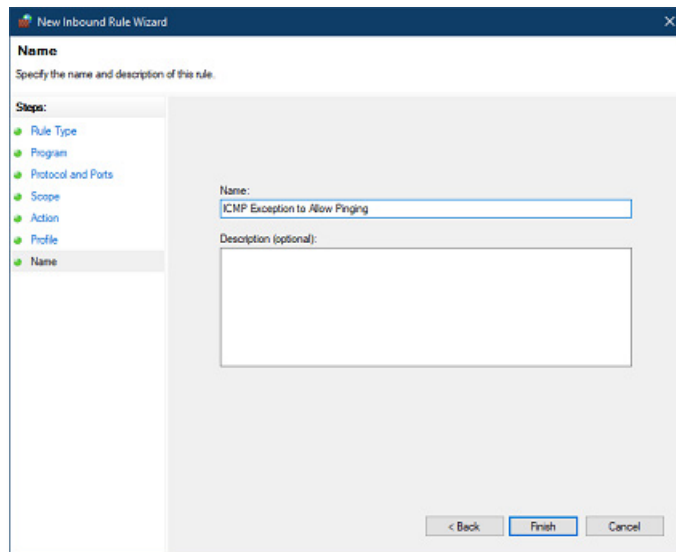
13. On the Action page, click Allow the connection, and then click Next.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' page. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action (selected), Profile, and Name. The main area is titled 'Specify the action to be taken when a connection matches the conditions specified in the rule.' It contains a section 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. Each option has a brief description. A 'Customize...' button is located below the 'Allow the connection if it is secure' option. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

14. On the Profile page, select Domain, Private, and Public, and then click Next.



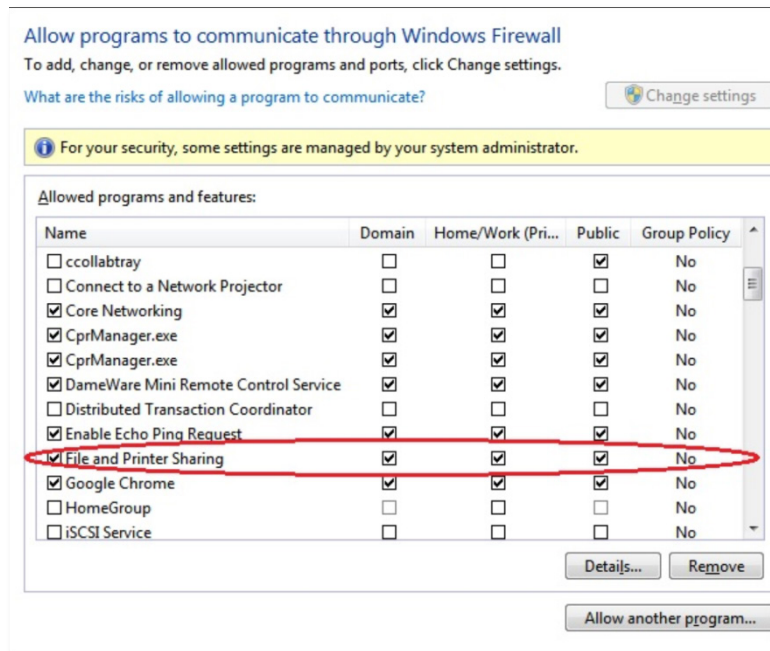
15. On the Name page, type: ICMP Exception to Allow Pinging, and then click Finish.



## Allowing file and print sharing

1. From Control Panel, open Windows Defender Firewall.
2. Click Allow an app or feature through Windows Defender Firewall.

3. Configure File and Print Sharing as shown below.



## Appendix E

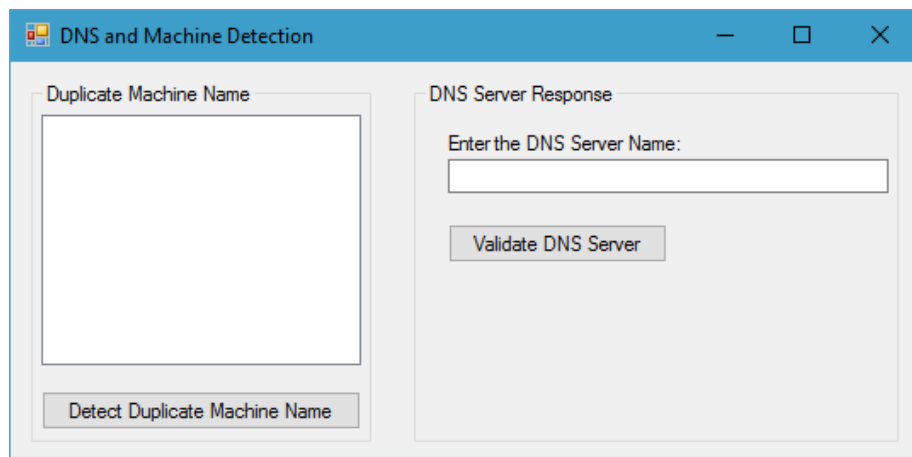
### DNS and Machine Detection

#### DNS and machine detection tool for redundant network

Created a tool in C:\Fireworks\exe\ DNS and Machine Detection.exe which detects machines in network having same names and validates whether DNS is working or not. This can be used for troubleshooting the redundant network.

This is used for troubleshooting when clients/servers in network version, connect/disconnect randomly.

**Figure 11: DNS and Machine Detection**



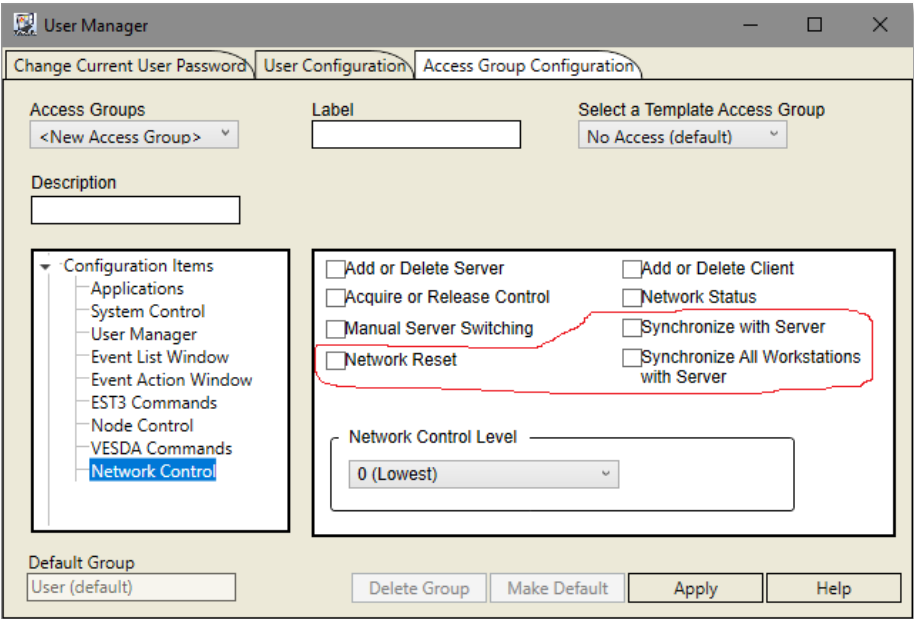
#### Client-Server Synchronization

In network mode, a new menu item “Synchronize All Workstations with Server” has been added to the “Functions” menu. This menu item is only enabled if this Server/Client machine is in control. When selected, the “Synchronize with Server” event is broadcast to all Client Workstations and they all synchronize.

A new item has been added to System Configuration’s Network tab with “FWNETWORK\_SYNC\_TIMEOUT” as a name, “Synchronization with Server timeout value (in minutes)” as a description and 0 as a default value. When the property value “t” is greater than 0 and it is a Client Workstation then these Workstations will automatically synchronize with the server every “t” minutes.

GUI elements for setting “Synchronize with Server” and “Network Reset” are missing from Network Control Configuration Items in User Manager. Together with “Synchronize All Workstations with Server” a total of three new check boxes are added.

Figure 12: User Manager – Network Control - Access Group Configuration



# Appendix F

## FireWorks Shared Resource Folder

### Introduction

This section is intended for dedicated FireWorks redundant networks consisting of UL 864 Listed Ethernet switches, FW-UL6WW10 workstation computers, and FW-UL6SW10 server computers configured as an SQL cluster (i.e., flat workgroup network). The workstations and workstation/servers are not members on a domain or attached to a domain network.

If you have computers on a z-network system, described by being on a domain as a non-member or as a domain member, these networks will be outside the scope of this document. The information may be valid; however, the process will fail without a domain administrator password for privileges.

This section tells you how to create a shared resource folder for FireWorks 9.1 (and later) redundant networks. To facilitate mirroring, which is required for FireWorks redundant network operation, you must have a shared resource folder that is common to all three computers in the SQL cluster (i.e., the primary server computer, the backup server computer, and the witness computer).

FireWorks uses an automation tool to automatically build the SQL cluster, which consists of the primary server computer, the backup (mirror) server computer, and the witness computer. For the automation tool to run correctly you need a shared resource folder common to the three computers in the SQL cluster.

For the SQL cluster shared resource folder to work properly with the automation tool you need the following:

- A common Windows user with administrator rights. With UL6 PCs the common user can be administrator as it is an SQL user as well as a Windows user while being a common user on the three computers (primary, backup, witness) cluster.
- The common user must have a password.
- A common shared folder (certshared).
- All three computers in the SQL cluster must have read/write access to the shared folder.
- Create networked mapped drives to the FW-Primary certshared folder from the mirror server (FW-Backup) and then the FW-Witness PC.

The general steps for creating a shared folder for redundant network applications are:

1. Create the shared folder on the primary server.
2. Map the shared folder on the backup server and on the witness server.
3. Test the shared folder read/write permissions.
4. Add the common user to the SQL properties on the primary server computer, on the backup server computer, and on the witness computer.

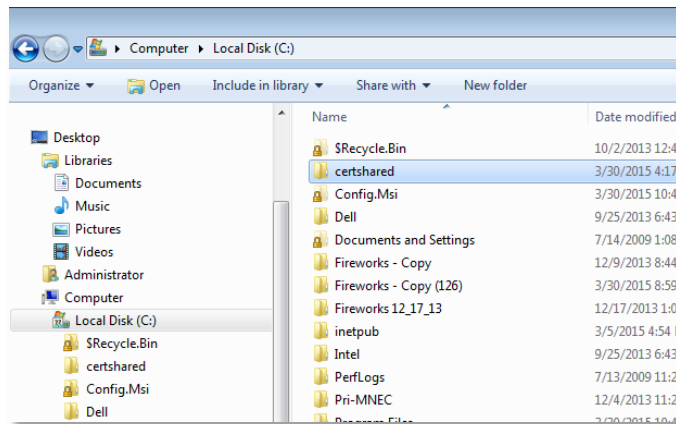
## Creating the shared folder on the primary server computer

The following steps will allow the creation of a common shared folder called certshared.

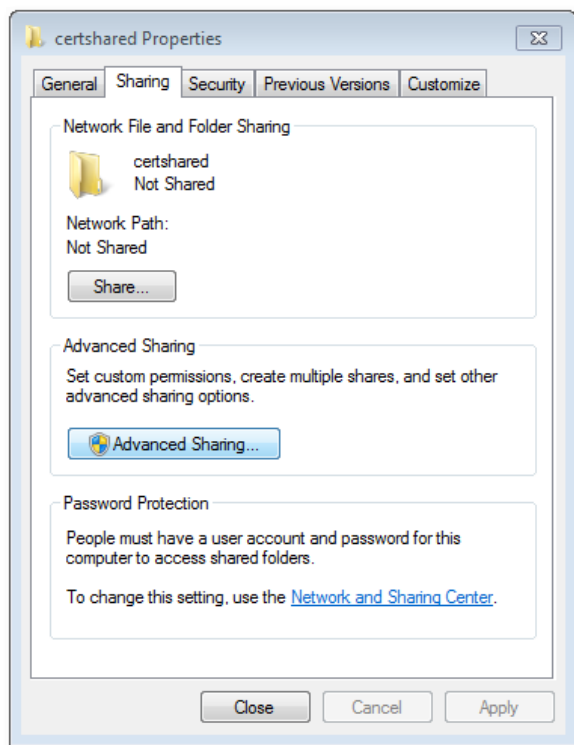
### To create the shared folder:

1. On the primary server computer, start Windows Explorer, and then create a new folder in the root of the C:\ drive.
2. Right-click the folder you just created, click Rename on the shortcut menu, and then type: `certshared`.

You should have a folder like the one shown below.

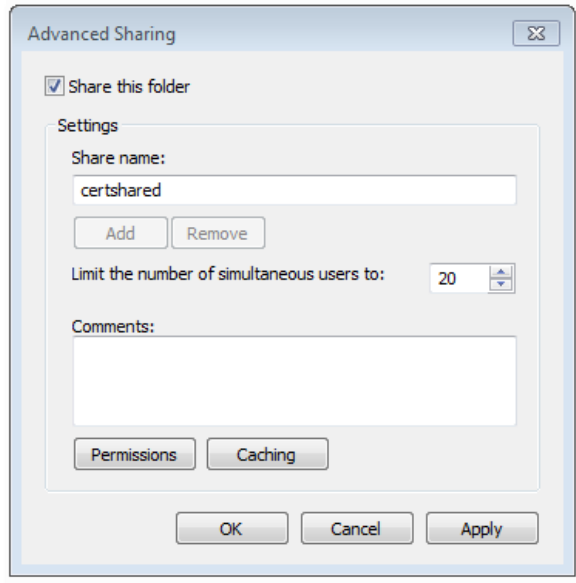


3. Right-click the certshared folder, and then click Properties on the shortcut menu.
4. On the certshared Properties dialog box, click the Sharing tab. See the figure below.

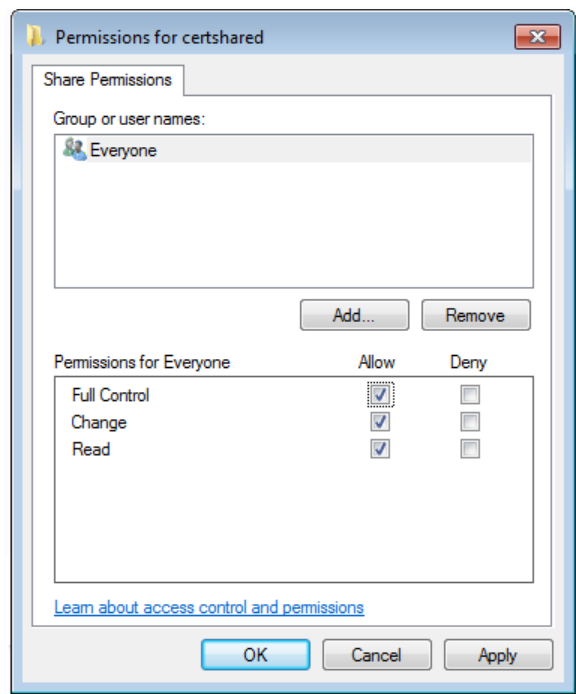


5. On the Sharing tab, click Advance Sharing.

6. On the Advanced Sharing dialog box, check the Share this folder check box. See the figure below.



7. Under Settings, click Permissions.
8. On the Permissions for certshared dialog box, under Permissions for Everyone, check the Allow check box for Full Control and for Change. See the figure below.

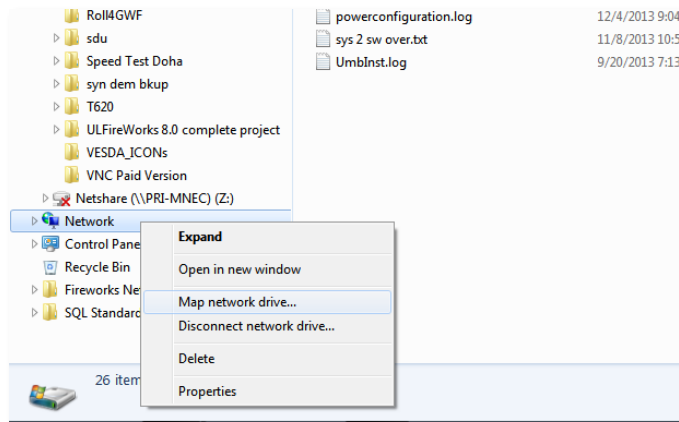


9. Click Apply, and then click OK.
10. Click Close. The folder share process is complete.

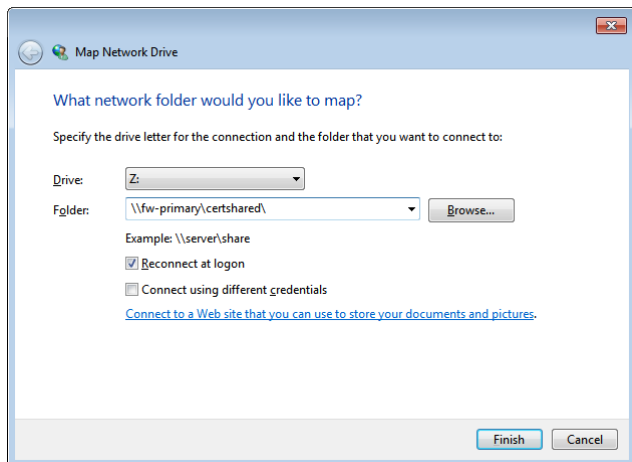


## Mapping the shared folder on the backup server

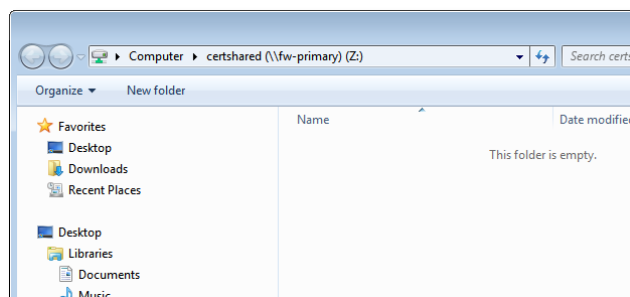
1. On the backup server (FW-Backup), click the Start button, and then click Computer.
2. Right-click the Network icon, and then click Map network drive on the shortcut menu. See the figure below.



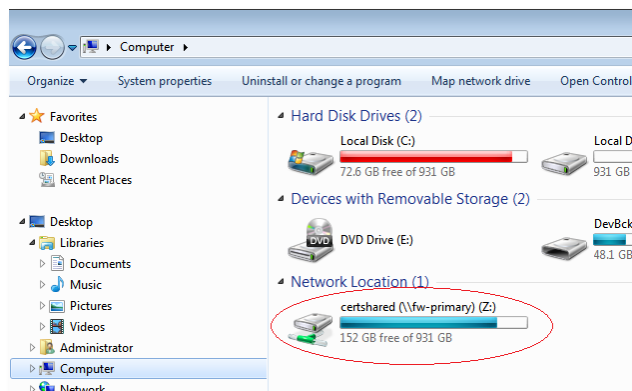
3. In the Map Network Drive dialog box, select a drive letter, and then in the Folder box, type: \\fw-primary\certshared. See the figure below.



4. Click Finished. If you mapped the shared folder correctly, the folder should automatically open. See the figure below.



When the connection and map drive is successful, you'll have a Z: drive on the backup server that represents the shared folder on the primary server.



## Mapping the shared folder on the witness server

To map the shared folder on the witness server (FW-Witness), follow the procedure in “Mapping the shared folder on the backup server” on page 59.

## Testing the shared folder read/write permissions

1. Open the shared folder on the backup server (FW-Backup), and then create a new folder.
2. Open the shared folder on the primary server (FW-Primary), and then make sure that it contains the new folder you just created.
3. Delete the new folder from the shared folder on the primary server (FW-Primary), and then make sure that the shared folder on the backup server (FW-Backup) is empty.

## Adding the common user to the SQL properties

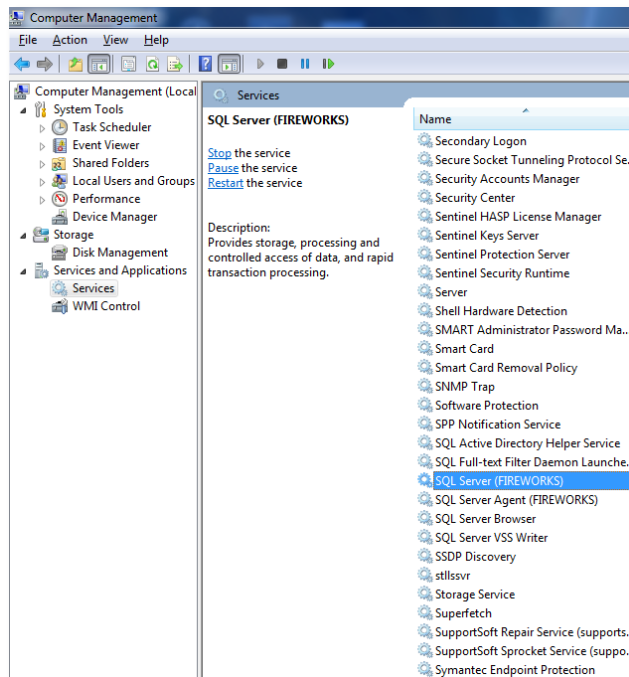
This section is not required when using FW-UL6 workstations and workstation/servers on a UL listed redundant network.

**Note:** If the automation process tool has issue with writing to the shared resource folder, then it will be necessary to add the common user to the SQL properties.

1. On the primary server, in the Search box on the Windows task bar, type: `computer`, and then open the Computer Management app by clicking Run as administrator.
2. In the navigation pane on the left, expand Services and Applications, and then click Services.

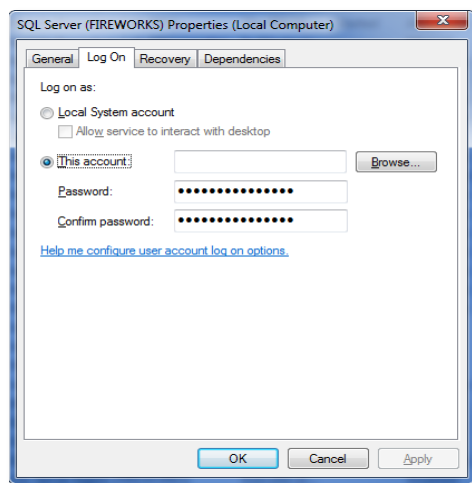
3. In the Services list, right-click SQL Server (FIREWORKS), and then click Properties on the shortcut menu.

You can use the scroll bar to locate the service, or you can select any service in the list, and then press the S key on the keyboard until the service is selected. See the figure below.



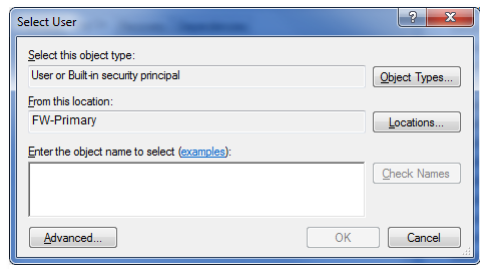
4. In the SQL Server (FIREWORKS) Properties dialog box, on the Log On tab, click This account. See the figure below.

Enter the password. For FW-UL6 computers the password is the Windows login password ESTFW.

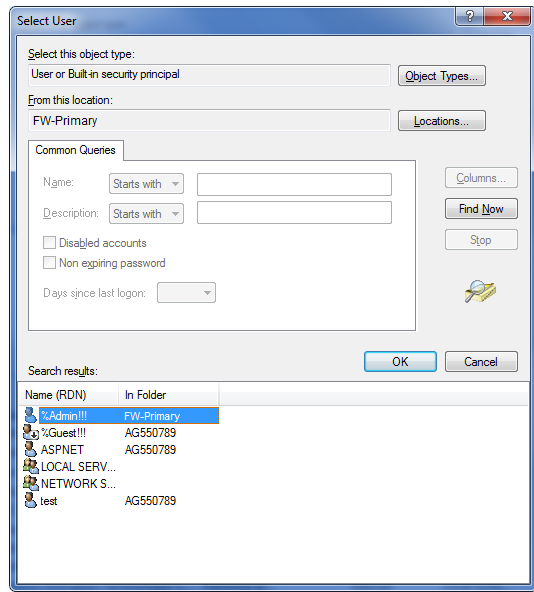


Click Browse.

5. In the Select User dialog box, click Advanced. See the figure below.



6. Click Find Now, and then select %Admin!!!.



7. Click OK, then click OK, and then click Apply.

**Note:** The password required is the Administrator password. For FW-UL6S and FW-UL6W computers, use ESTFW.

8. Right-click SQL Server (FIREWORKS), and then click Stop. Right-click SQL Server (FIREWORKS) again, and then click Start.
9. Repeat the above steps on the backup server (FW-Backup) and on the witness server (FW-Witness).
10. Open the automation tool, click Delete Certificates, and then Create Certificates.

# Appendix G

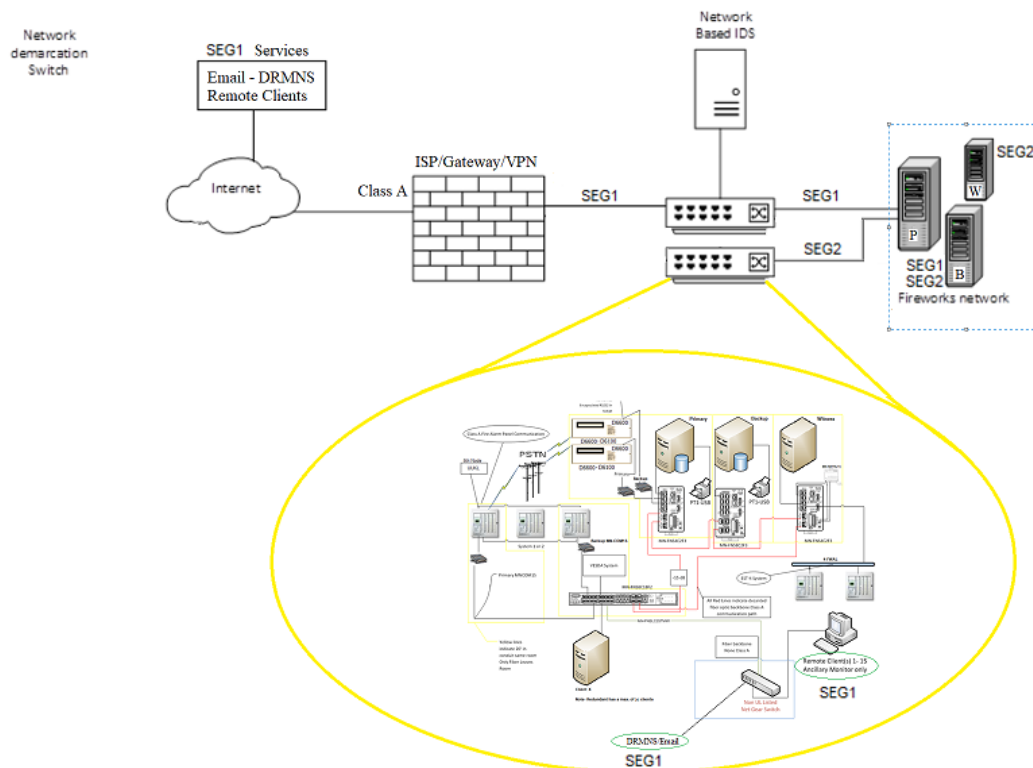
## Setting Up Dual NIC Environment

### Introduction

For optimal cyber security you may consider configuring your Fireworks system to work in a dual NIC environment. The way this would work is that you would have first NIC dedicated for anything that goes to the outside web, this is where your email server or remote clients would talk on. Then your second NIC would be dedicated to your Firework network, this is the network your Fireworks redundant or non-redundant and panels would reside. The purpose of this set up is that under the unfortunate event that a cyber-attack happens on NIC one, your second NIC (Fireworks network) would not be directly affected.

### How to configure a dual NIC environment

Setting up the dual NIC environment will be similar to your single NIC system. Open the second NIC's network configuration windows and fill in the same fields you did for your first NIC but taking the second network into account. You'll only want to do this on server machines, so on your primary and back on a redundant and on the server pc on a non-redundant system. Once this is done you should be able to successfully ping other items that are in that second network. Below is a diagram on how the dual NIC environment should look on a redundant system:



## Dual NIC failover and recovery

On a network Primary Restoral if you notice that the “Acquire control” feature is greyed out, specifically after trying to restore back to the primary. The best way to get the Primary to effectively interact with the rest of the redundant system is to select network reset, and due to it not automatically reconciling you must do the reconcile manually, see steps below.

The following are recovery steps to take if your system experiences a failover from Primary to Backup with a Dual NIC setup.

- Step 1 - Verify that both networks have recovered.
- Step 2 - From Primary select (Functions) navigate to (Network Reset) click.
- Step 3 - Verify the Primary changes from the Backup state to Primary server state.

This point your system is synchronized and communicating.

**Problem statement:** If you are using more than one NIC on a Redundant FireWorks Network setup, there are some configuration changes that MUST be made to your system to prevent unexpected issues with the system and make it more stable. The issues can manifest themselves with Server crashes, half transfers (that results in clients stop getting deltas from the panel) and other anomalies based on simple things like errors on the network.

The issue stems from how FireWorks tells when a system should transfer.

In the simplest form when a server such as the Primary Server can't see one of the other servers database (perhaps do to network issues or a NIC fail, etc) it will initiate a transfer. However if you have two NIC's the Primary database server may after some time switch to connecting utilizing the other NIC. This puts the system in an unexpected and possibly unrecoverable state, it breaks our design.

**Solution:** We must prevent the servers from transferring and utilize the not intended NIC interface. We propose doing this via the firewall.

The customer needs to know ahead of time which NIC (with which IP) is planned to be used from the Server to Server connection, we call that in our documents the “Fire Network” NIC 2. We must not allow SQL to use the other NIC generally used for off premise “Internet” purposes. Using this information they need to make a Firewall rule

The fix is to block the inbound traffic to the second NIC IP address for port 1433, TCP protocol (used by SQL Server).

In more detail:

1. At the command prompt, type: wf.msc.
2. Right click on “Inbound Rules” and select “New Rule...”.
3. Select “Custom” for Rule Type and click “Next”.
4. Keep “All Programs” checked and hit “Next”.
5. Select “TCP” for protocol type, select “Specific Ports” for “Local port” and type 1433 (used by SQL Server), click “Next”.
6. In “Which local IP addresses does this rule apply to?” select “These IP addresses, click “Add...” and type IP address of another NIC (not used y SQL Server). Hit OK, then hit “Next”.
7. In “Action” select “Block the connection”, hit “Next”.
8. Keep all profile checked and hit “Next”.
9. Enter “Fireworks: Close SQL Server Port 1433 for specific local IP address” for name and hit “Finish”.
10. New rule will appear in the list of Inbound Rules.

# Glossary

Access	File and directory access permissions granted to FireWorks users, using Windows tools. Possible permissions are: read, write, and execute. See also <i>Read</i> , <i>Write</i> , and <i>Execute</i> .
Backup server	The (physical) backup server hosts a FireWorks server and SQL databases.
Client	A FireWorks client is responsible for showing the status of the FireWorks network. A client is able to execute nearly all the commands that a server can. See also <i>control</i> .
Control	The FireWorks network consists of several computers, each having roughly the same capability. Certain actions, such as sending commands to a panel, should only be done by one responsible party in the FireWorks network. This computer is considered to have <i>control</i> . Control can be passed to any server or client in the FireWorks network by means of the Function menu commands Acquire Control and Release Control.
Execute	A type of file and directory access permission. The execute permission grants the ability to execute a file. This permission must be set for executable programs, including shell scripts, to allow the operating system to run them. When set for a directory, this permission grants the ability to access file contents and metadata if its name is known, but not to list the files inside the directory, unless the read permission is also in effect. See also <i>Read</i> and <i>Write</i> .
Logical backup server	The logical backup server can be on either the primary server or the backup server. The logical backup server shows all activity in the FireWorks network using local mode and is the backup computer in charge of the FireWorks network.
Logical primary server	The logical primary server can be on either the primary server or the backup server. The logical primary server shows all activity in the FireWorks network and is the primary computer in charge of the FireWorks network.
Nonredundant FireWorks network	In a nonredundant network, a FireWorks server coordinates activity with one or more FireWorks clients. Customers needing multiple locations to administer their life safety systems would use this configuration.
Primary server	The (physical) primary server hosts a FireWorks server and SQL databases.
Read	A type of file and directory access permission. The read permission grants the ability to read a file. When set for a directory, this permission grants the ability to read the names of files in the directory, but not to discover any further information about them such as contents, file type, size, ownership, or permissions. See also <i>Write</i> and <i>Execute</i> .
R/W/E	Read, write, and execute. File and directory access permissions. See also <i>Read</i> , <i>Write</i> , and <i>Execute</i> .
Redundant FireWorks network	In a redundant network, a FireWorks <i>server cluster</i> coordinates activity with one or more FireWorks clients. Customers needing multiple locations to administer their Life Safety Systems would use this configuration. This is the most highly survivable configuration.
Remote (web) client	The FireWorks remote client is an application that connects to a FireWorks server and shows the activity in the FireWorks network. (It is sometimes referred to as the <i>web client</i> application.) The remote client cannot perform any commands on panels.
Server	A FireWorks server is responsible for communicating with all network resources, such as panels. It is also responsible for coordinating activity between all FireWorks clients.
SQL cluster	The redundant FireWorks network is controlled by three computers: primary server, backup server, and witness server. The primary and backup servers both run FireWorks and host mirrored databases. The witness server is needed by Microsoft SQL to mirror the databases.
SQL Database mirroring	Using three computers to host SQL databases to provide a reliable database to other systems. The databases continue to work as long as two of the three systems are operational.
SQL Server Express Edition	The typical package used by FireWorks to host its databases.
SQL Server Standard Edition	The more capable version of SQL Server that supports mirrored databases.

Stand-alone FireWorks	A system in which a single computer runs FireWorks. This is the configuration used by most customers.
Witness server	This server is needed by Microsoft SQL Standard Edition to ensure the survivability of the SQL databases shared by all FireWorks computers.
Write	A type of file and directory access permission. The write permission grants the ability to modify a file. When set for a directory, this permission grants the ability to modify entries in the directory. This includes creating files, deleting files, and renaming files. See also <i>Read</i> and <i>Execute</i> .