



SOLIDWORKS SNL & PDM Firewall Settings

This document outlines settings that should be modified on the SolidNetwork License Manager server when a firewall is in use. Firewall exceptions required by SOLIDWORKS PDM are also discussed. The steps and screen shots used in this guide are for Windows 10, but Windows 11 and various versions of Windows Server will be similar.

Contents

Before we get started – You'll need the following.....	2
Accessing The Firewall Settings.....	2
Create Two Inbound Rules	3
Fine Tuning The Rules	4
Optional: Create Two Outbound Rules	5
Firewall Rules For Opening By Port.....	6
License Manager Settings.....	6
Troubleshooting Windows Firewalls.....	7
SOLIDWORKS PDM Firewall Rules	8
For the Archive Server	8
For the SQL Server.....	8
For the Web Server.....	8
Not working like it should?	9



Before we get started – You’ll need the following

- The SolidNetwork License Manager should already be installed on the server.
- An administrative account and access to the server.

Accessing The Firewall Settings

This first section illustrates how to create rules for a Windows firewall. It is possible to define rules that open by program or open by port. This example opens by program, which is more secure. It should be noted that SOLIDWORKS recommends opening by port. Port instructions are on page 6.

1. Open the Windows Control Panel. It may help to find the item you are looking for by viewing by *Small icons*, as shown in Figure 1.

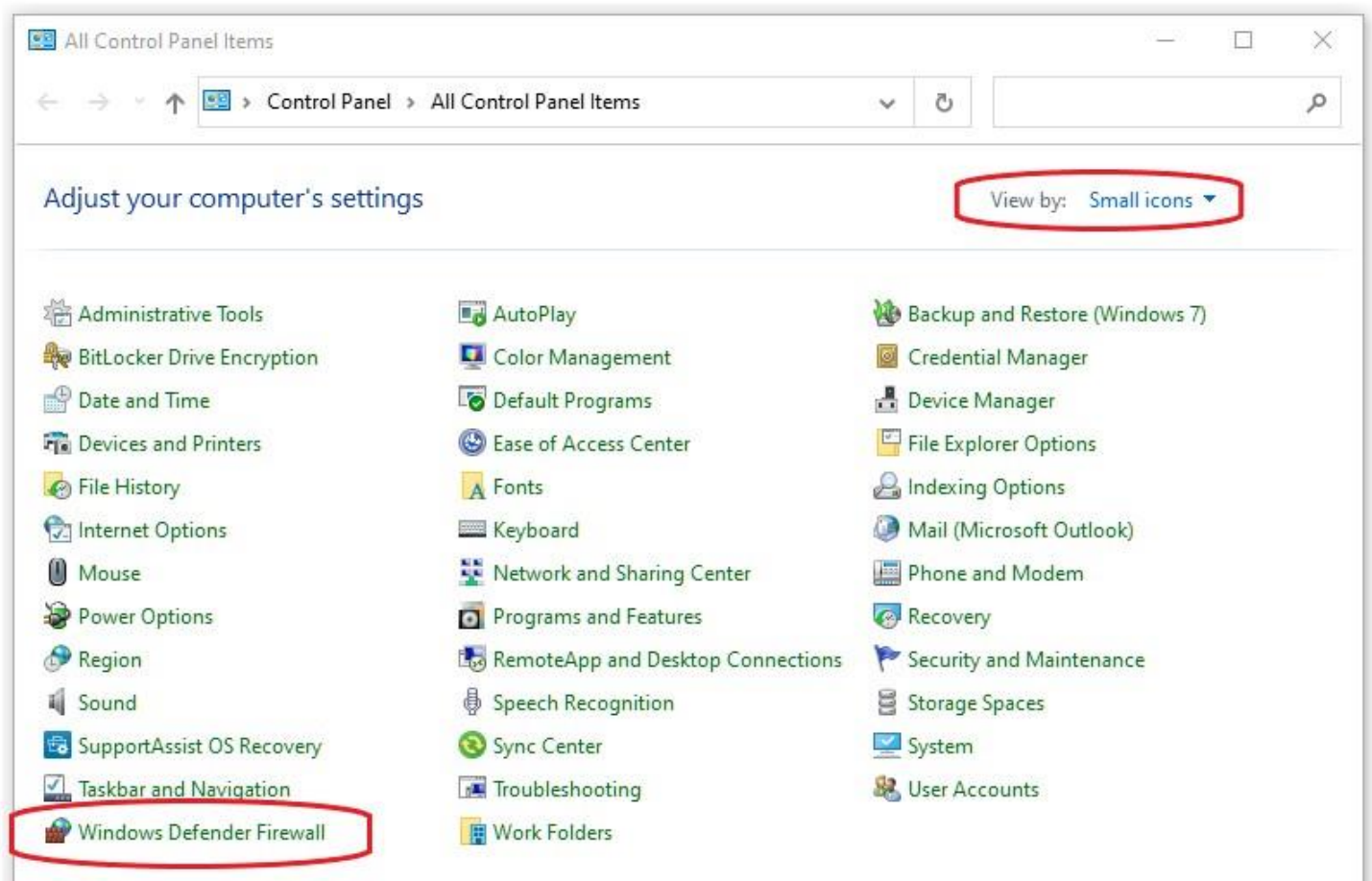


Figure 1: The Windows Control Panel.

2. Select "Windows Defender Firewall".
3. Click "Advanced Settings" in the Windows Firewall window (see Figure 2).

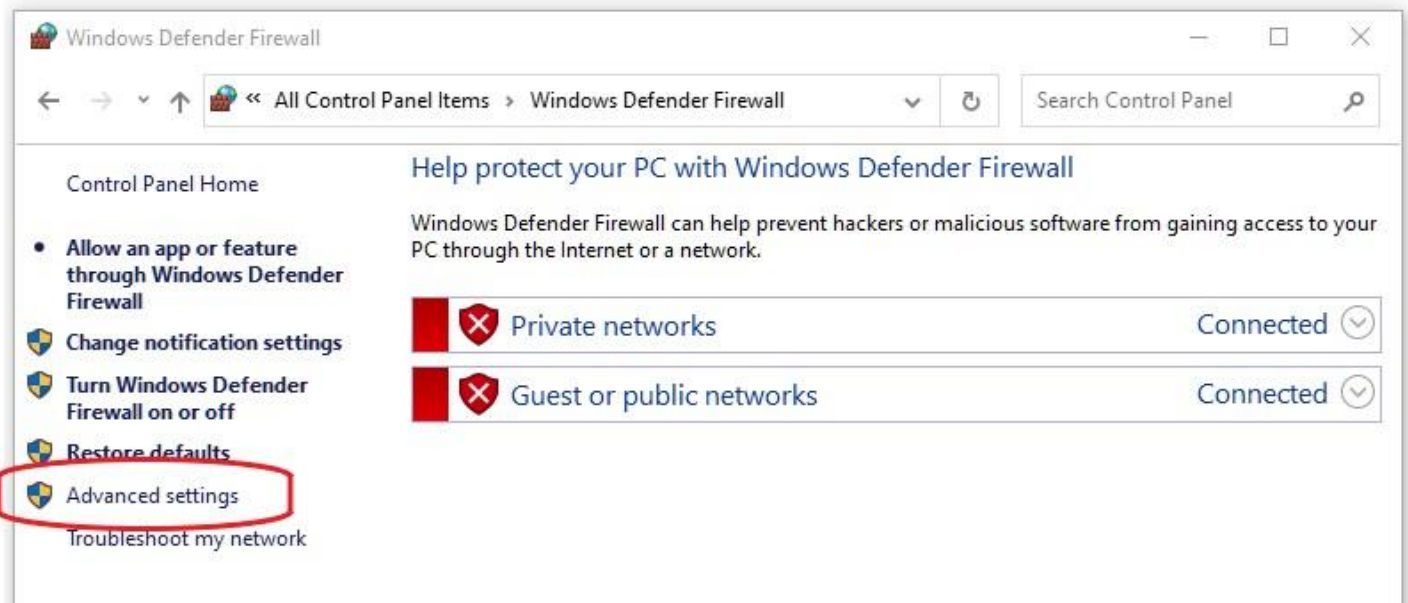


Figure 2: Accessing firewall Advanced settings.

Create Two Inbound Rules

In order to limit the scope of what is allowed through the firewall, it will be necessary to create two inbound rules. We will create one rule for each of the programs **Imgrd.exe** and **sw_d.exe**.

1. In the Advanced Settings window (shown in Figure 3), select Inbound Rules, and then click New Rule...

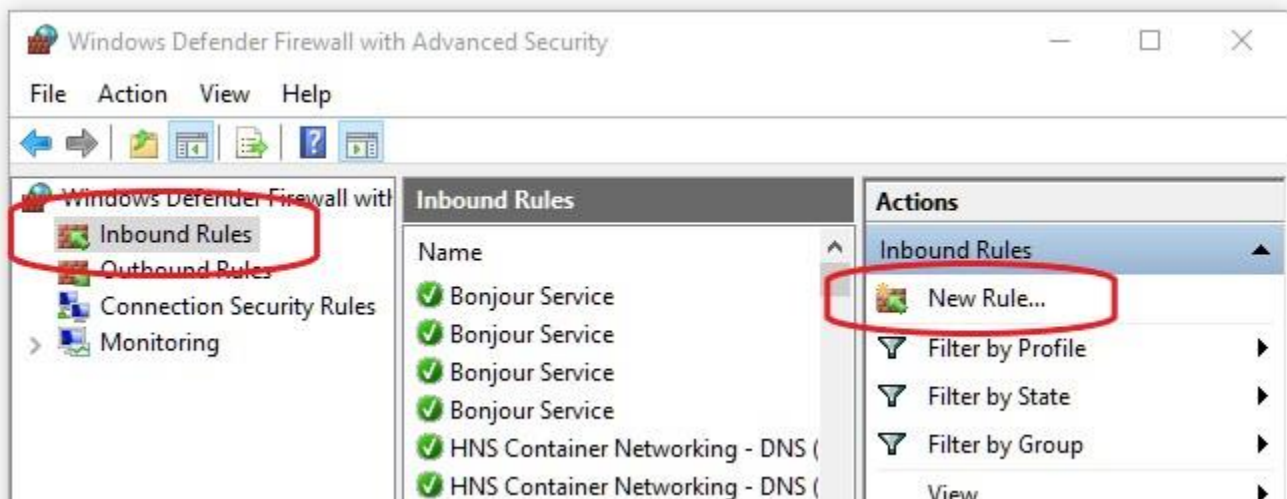


Figure 3: Creating a new inbound rule.

2. The New Inbound Rule Wizard will open. There are 5 sections to this wizard. Use these settings to create the rule.
 - Rule Type: select *Program*
 - Program: select *This program path*, then browse to “C:\Program Files (x86)\SOLIDWORKS Corp\SolidNetWork License Manager” and select the file **lmgrd.exe**.
 - Action: select *Allow the connection*
 - Profile: uncheck *Public*. The rule should only apply to *Domain* and *Private* networks.
 - Give the rule a name. In our case, we will name it **SNL Inbound lmgrd**.
3. To create the second rule, follow these same steps, but instead of selecting **lmgrd.exe** as the program, select **sw_d.exe**.
4. Name the second rule **SNL Inbound sw_d**.

Fine Tuning The Rules

The Inbound Rules list should now contain the two rules just created, as shown in Figure 4.

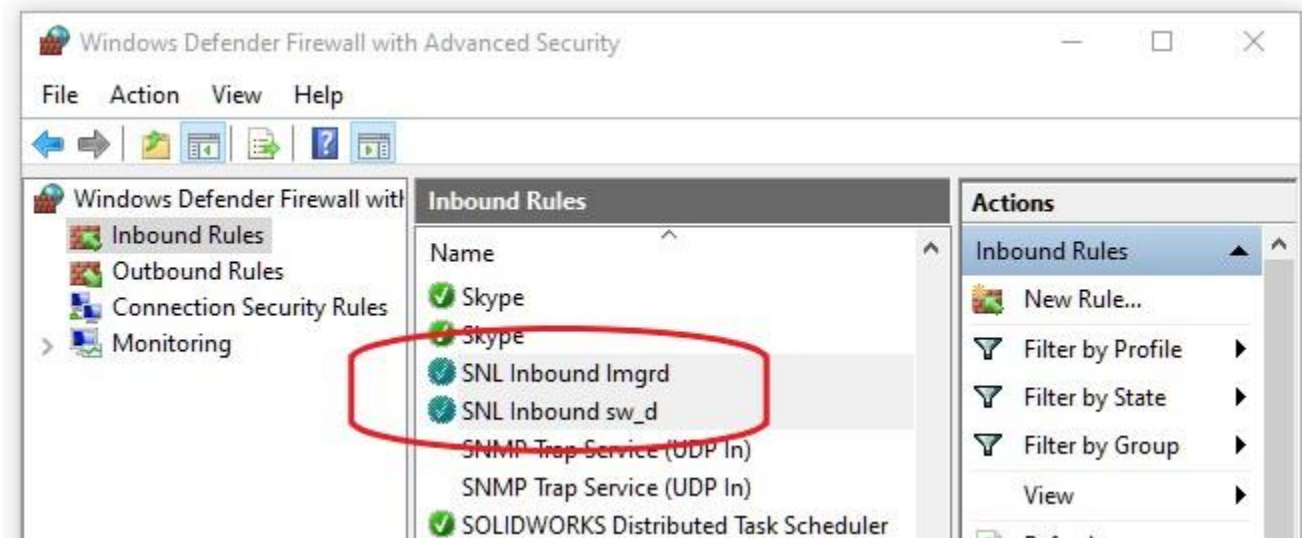


Figure 4: Newly created inbound rules.

Double click on one of the new rules to bring up its properties. There should be 8 tabs at the top of the rule's Properties window, shown in Figure 5.

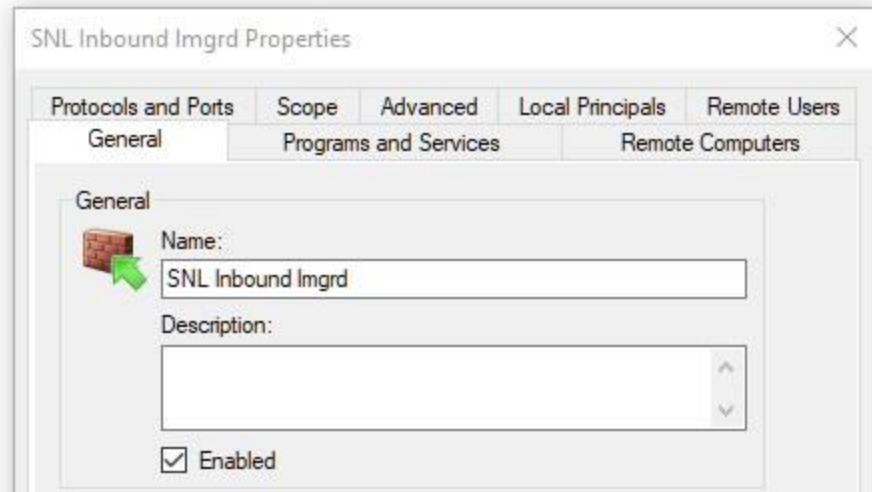


Figure 5: Firewall rule properties.

Most of the properties can be left at their default settings, with a few exceptions. After changing any property, make it a point to click the Apply button prior to moving on to the next tab.

- In the **Protocols and Ports** tab, specify the Protocol type as **TCP**.
- In the **Advanced** tab, you should change two settings:
 - In the section titled **Profiles**:, clear **Public**. Leave **Domain** and **Private** checked.
 - In the section titled **Interface types**:, click the **Customize** button and ensure the only option checked is **Local area network**.

Set these properties for each of the new rules.

Optional: Create Two Outbound Rules

Test using only inbound rules first. In most environments, the two inbound rules should be enough to allow appropriate communication between the server and client computers. In certain scenarios, it may be necessary to create outbound rules as well.

To create outbound rules, follow the same steps used to create inbound rules. The sole difference will be to select Outbound Rules as shown in Figure 6. All other steps will be exactly the same.



Figure 6: Creating outbound rules.





Firewall Rules For Opening By Port

Opening by port is the recommended method of opening a firewall for the SOLIDWORKS SolidNetwork License Manager. These steps are a condensed version of the steps described earlier in this document.

1. Select Start -> Control Panel -> Security and System -> Windows Defender Firewall.
2. In the left pane, click the "Advance settings" link.
3. Select "Inbound Rules" and right-click to choose "New Rule".
4. Select "**Port**" and click "Next".
5. Select "**TCP**", type in **25734** for the "**Specific local port**" field, and click "Next".
6. Select "**Allow the connection**" and click "Next".
7. Clear "Public" and click "Next".
8. Enter a name for the rule and click "Finish". Optionally add a description.
9. Repeat Steps 3 through 8 for port **25735**.

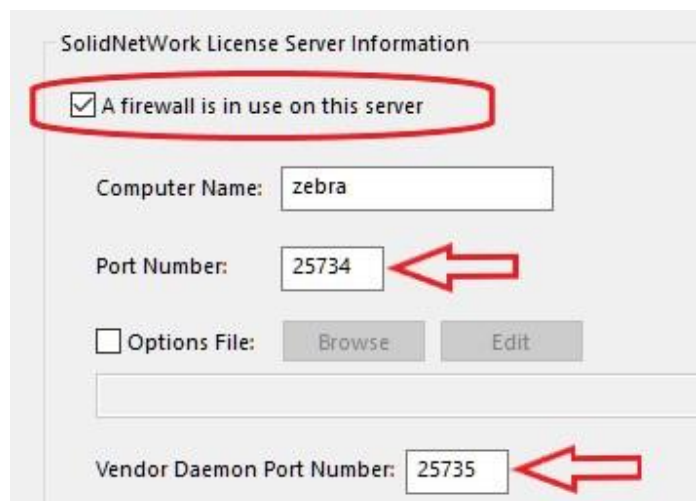
License Manager Settings

After creating firewall rules, make sure the SolidNetwork License Manager is set to utilize the firewall.

1. Open the SOLIDWORKS SolidNetwork License Manager program on the server.
2. In the Server Administration tab, click the Modify button.
3. Select "Activate/Reactivate your product license(s)" and click Next.
4. Ensure "A firewall is in use on this server" is selected (checked), and the ports specified are those chosen to be opened in the firewall. The default port numbers are 25734 for the "Port number", and 25735 for the "Vendor Daemon Port Number".

If it was not necessary to make any changes in the SolidNetwork License Manager, click Cancel. There is no need to go any further. Otherwise, continue with the next step.

5. Click Next -> Select All -> and select "Automatically over the internet".
6. Enter your email address and click Next.
7. You should receive a confirmation that the activation succeeded. Click Finish.
8. Return to the Server Administration tab of the license manager. Stop, then Start the License Server, then click OK to close.



SolidNetWork License Server Information

A firewall is in use on this server

Computer Name: zebra

Port Number: 25734

Options File: Browse Edit

Vendor Daemon Port Number: 25735

Figure 7: Default port numbers.





Troubleshooting Windows Firewalls

In standard SOLIDWORKS network license installations, it isn't always necessary to take any action whatsoever to alter ports or add rules to the firewall. Often, Windows handles everything just fine with no extra input. Sometime, though, it may be necessary to bypass the firewall for purposes of troubleshooting. Turning off the firewall completely is not recommended, but allowing inbound connects on your private network is usually safe on the short term for reasons of diagnosing problems. If SOLIDWORKS users are having trouble obtaining a license, use the following method to allow all incoming packets on your private network temporarily (see Figure 8).

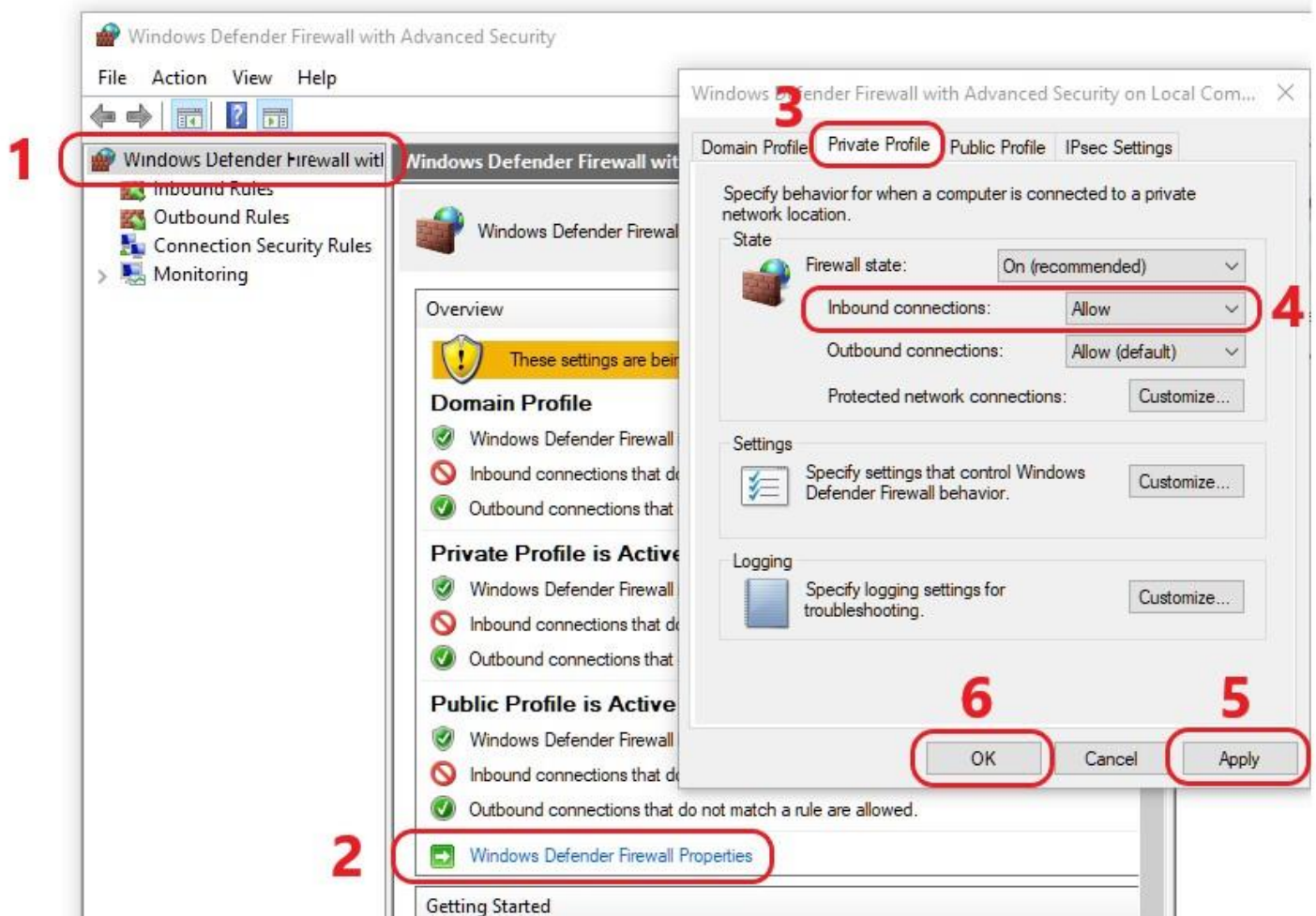


Figure 8: Allowing all inbound connections.

1. Select "Windows Defender Firewall with Advanced Security".
2. Click "Windows Defender Firewall Properties".
3. Select the "Private Profile" tab.
4. Change *Inbound connections*: from **Block (default)** to **Allow**.
5. Click Apply, then click OK.





If SOLIDWORKS users were not able to obtain a license, and setting Inbound connections to **Allow** suddenly allows users to obtain a license, there may be something set inappropriately in the Windows Firewall settings. Another possibility is rules were added that restrict communications on the required ports. Speak to your IT person or network administrator for assistance.

When finished troubleshooting firewall issues, make sure to set the *Inbound connections*: from **Allow** back to **Block (default)**.

SOLIDWORKS PDM Firewall Rules

There are a number of ports that must be open on the server for PDM to work properly. Use the same process outlined at the beginning of this document to add the rules listed below. Create port rules that enable TCP and UDP ports for inbound SOLIDWORKS PDM traffic. Open the ports for the archive server first. Then follow the same instructions to open the ports for the SQL server (and web server if using the Web2 interface).

For the Archive Server

New Inbound Rule -> **Port** -> **TCP & 3030** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **UDP & 3030** -> "Allow the connection" -> clear **Public**.

For the SQL Server

New Inbound Rule -> **Port** -> **TCP & 1433** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **UDP & 1433** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **TCP & 1434** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **UDP & 1434** -> "Allow the connection" -> clear **Public**.

For the Web Server

New Inbound Rule -> **Port** -> **TCP & 80** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **UDP & 80** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **TCP & 443** -> "Allow the connection" -> clear **Public**.

New Inbound Rule -> **Port** -> **UDP & 443** -> "Allow the connection" -> clear **Public**.





Not working like it should?

If things didn't go as planned, please contact CADimensions Technical Support for further assistance. If you have an existing case, please contact the Application Engineer you are working with; otherwise [submit a new case online](#).

