



FILLING THE GAPS IN TECHNOLOGY



PEGASUS

User Manual

Table of Contents

1.	WYLMAN PEGASUS	3
2.	Safety Instructions	4
3.	Compliance Statements	5
4.	PEGASUS Overview	6-7
5.	Included Accessories	8-10
6.	Important Notes	11
7.	Getting Started	12
7.1.	Assigning PEGASUS Target	12-13
7.2.	Activation	13-17
7.3.	Deactivation	17-19
7.4.	Activating/Updating PEGASUS Shield	19-21
8.	Users	22
8.1.	Users Privileges	22
8.2.	Logging In	22-23
8.3.	Changing Passwords	23-24
8.4.	Resetting Passwords	24-25
9.	Options	26
9.1.	Session Settings	26
9.1.1.	Session Time	26-27
9.1.2.	Auto Logout and Shutdown	27
9.1.3.	Session Invitations	27-29
9.1.4.	Remote Access	29-30
9.1.5.	IP Watchdog	30-31
9.1.6.	Security	31-32
9.2.	Network Settings	32
9.2.1.	Network Adapters	32-34
9.2.2.	Wi-Fi Access Points	34-36
9.3.	PEGASUS Settings	36

9.3.1. PEGASUS Password	36
9.3.2. Auto Updates	36-37
9.4. System Time	37-38
9.5. Shield Manager	38-39
9.6. License Manager	39-40
9.7. Check for Updates	40-43
10. Sessions	44
10.1. Connecting PEGASUS to Target Machine	44
10.2. Demo Sessions	44
10.3. Session Invitation	45-46
10.4. View Session	46-49
10.5. Control Session	49-52
11. Index	53

1 WYLMAN PEGASUS

PEGASUS is the most secure remote desktop setup and the only one that provides end to end remote desktop access while effectively maintaining the air gapping of secured networks. It can be used in the most security sensitive systems.

Features:

1. Effectively maintains the air gapping of the remotely accessed computer
2. New approach achieving highest security
3. Easy User Interface
4. Can establish various types of connections with different privileges : Viewer, Controller
5. Doesn't require installation of any software to the accessed computer

For any questions please refer to <https://wylman.com/contact>

For any suggestions or for reporting technical issues contact support@wylman.com

2 Safety Instructions

Use the following safety guidelines to protect your PEGASUS from potential damage and to ensure your personal safety. Unless otherwise noted, each procedure included in this document assumes that the following conditions exist:

- You have read the safety information included.
- A component and/or attachment can be removed by performing the installation procedure in reverse order.
- If a third party attachment was used, you have read the safety instructions that came with it.



For best performance, only use the provided accessories and cables. Please contact us if cable(s) replacement or cable(s) different length is/are needed.



Repairs may only be done by a certified service technician. End user should only perform troubleshooting and simple accessory/cable replacement as authorized in this product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by WYLMAN is not covered under warranty. Read and follow the safety instructions that came with the product.



Handle PEGASUS and accessories with care. Although PEGASUS enclosure is very rigid, strong impact from drops can cause internal electronics to malfunction. Such damage will not be covered under warranty.



When disconnecting a cable, pull on its connector or on its pull-tab, not on the cable itself. As pulling connectors apart, keep them evenly aligned to avoid bending any connector pins. Also, before connecting a cable, ensure that both connectors are correctly oriented and aligned.



PEGASUS is secured with high security tamper proof screws, the screws must be checked for tampering marks before every use. If any tampering marks are noticed, DO NOT use PEGASUS and contact WYLMAN for support.



WARNING: This product is designed to be used indoors and in non-hazardous areas. Do not use this product in a hazardous classified areas as this may result in fires and/or explosions.



WARNING: To avoid damage to PEGASUS, use only the power supply provided. Do not use power supplies designed for other devices.

3 Compliance Statements

FCC Compliance Statement:

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RoHS Compliance Statement:

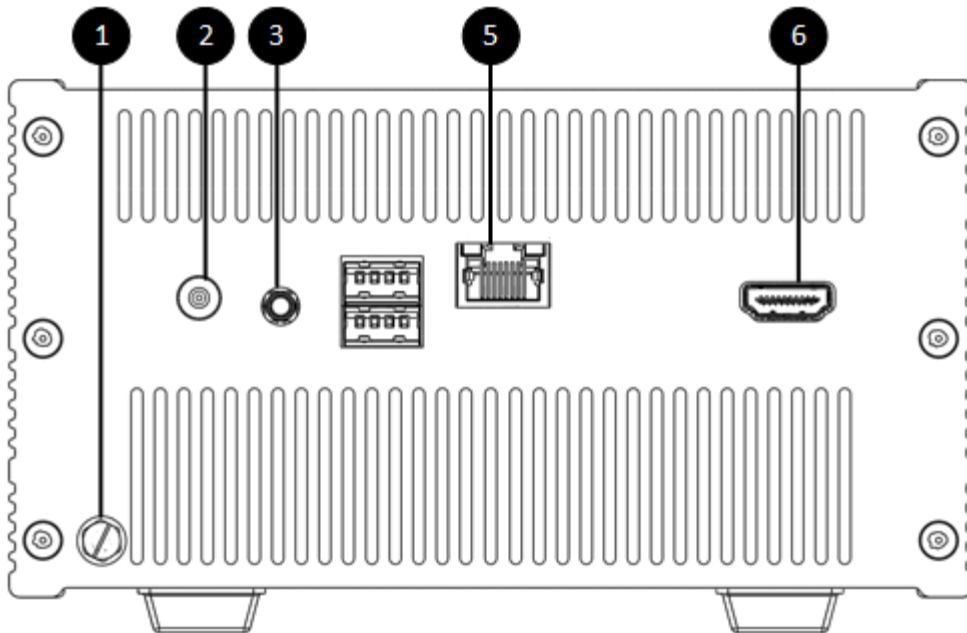
All components and solder alloys used in this product comply with the RoHS Directive. The RoHS Directive prevents all new electrical and electronic equipment placed on the market in the European Economic Area from containing more than agreed levels of lead, cadmium, mercury, hexavalent chromium, poly-brominated biphenyls (PBB) and poly-brominated diphenyl ethers (PBDE).

CE Compliance Statement:

This equipment is in compliance with the requirements of the following regulations: EN 55 022: CLASS A.

CE Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

4 PEGASUS Overview



1. Grounding Screw

It is recommended to connect the grounding screw to a clean/instrument ground bus.

2. 12VDC Power Input

Power input port; only user provided power supply.

3. Audio Output (3.5mm)

Optional audio output.

4. USB 2.0 Ports (x2)

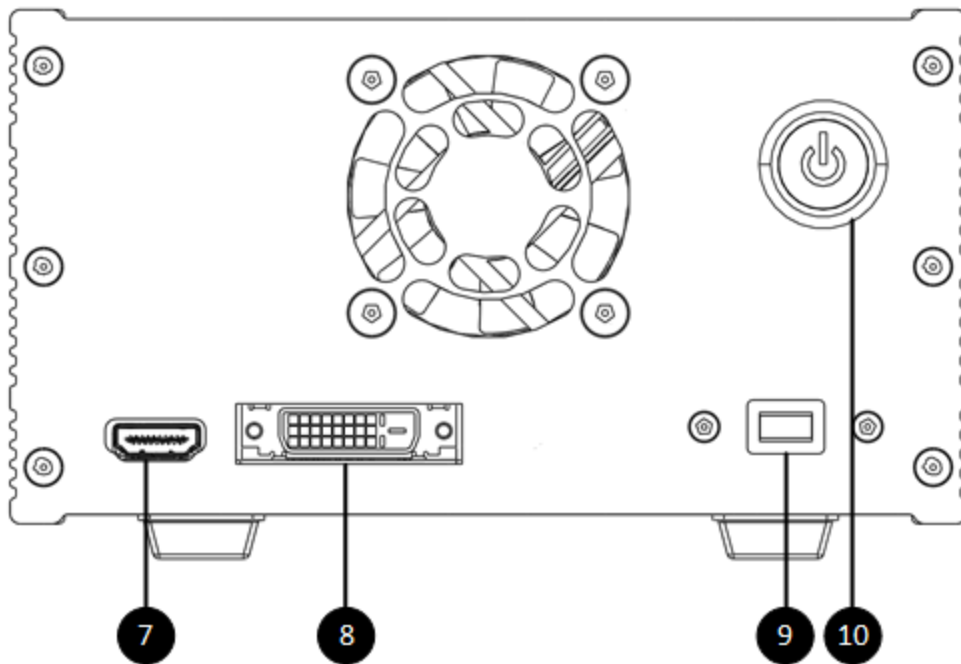
Optional expansion USB ports, can be used to connect external network adapters, Keyboard, mouse, etc. It does not support using any type of storage read and/or write devices; USB flash drive, external disc drive, etc.

5. Network Port (RJ45)

Optional wired network connection to connect to LAN and/or to the internet.

6. HDMI Output

Optional video output, can be used for PEGASUS configuration and/or monitoring.



7. HDMI Input

Optional HDMI input, can be used to receive video signal from Target computer.

8. DVI Input

Optional DVI input/VGA input with the DVI-VGA adapter (included), can be used to receive video signal from Target computer.

9. Keyboard & Mouse Port (Micro USB Type B)

Used to transfer the Keyboard & Mouse Commands from PEGASUS to Target Computer.

10. Power Switch

Used as the master on/off switch for PEGASUS.

5 Included Accessories

1. Power Supply



UL certified AC (100-240VAC) to DC (12VDC 5A maximum) adapter.

⚠ It is strongly advised to only use the included power supply.

2. PEGASUS Shield



USB 2.0 8GB USB drive. Preloaded with PEGASUS Target ID software. Refer to "**Activating/Updating PEGASUS Shield (Section 7.4)**" section for details on loading the PEGASUS Shield software to the USB drive.

⚠ Please make sure that the included PEGASUS Shield USB drive is labeled with the same serial number as your PEGASUS device. For security, these are the only USB drive that will work with your PEGASUS. Any other USB drive will be detected as a security thread and PEGASUS will immediately shutdown.

Although PEGASUS Shield USB drive has much more capacity than needed for its function, it is strongly advised to limit its use as intended in this manual.

3. HDMI Cable (6.6 ft)



High Speed HDMI Cable (30 AWG) Gold Plated with Ferrites (2M / 6.6 FT). This cable to be used to connect the Target machine HDMI output to PEGASUS HDMI input.

⚠ Although any HDMI cable would work, it is strongly advised to use this cable to maintain the RFI under the FCC legal limits. If your need different cable length please contact WYLMAN for support.

4. DVI-D Dual Link Video Cable (6.6 ft)



DVI-D Dual Link DVI Cable with Ferrites (2M / 6.6 FT). This cable to be used to connect the Target machine DVI output to PEGASUS DVI input.

⚠ Although any DVI cable would work, it is strongly advised to use this cable to maintain the RFI under the FCC legal limits. If your need different cable length please contact WYLMAN for support.

5. SVGA Cable (6 ft)




SVGA Cable with Ferrites (1.8 M / 6 ft). This cable to be used to connect the Target machine DVI output to PEGASUS DVI input (DVI to VGA adapter must be used, included).

⚠ Although any VGA cable would work, it is strongly advised to use this cable to maintain the RFI under the FCC legal limits. If your need different cable length please contact WYLMAN for support.

6. USB 2.0 Cable (6.6 ft)



USB 2.0 cable A-MicroB male with ferrites (2M / 6.6 FT). This cable to be used to connect the PEGASUS Keyboard and Mouse output to the Target machine.

 This cable must be connected to establish a session, even if the session was View only session.

7. VGA to DVI Adapter



Converts the VGA video signal to DVI video signal to be compatible with PEGASUS DVI input. To be used together with the VGA cable when the Target machine video output is VGA.

8. USB Ethernet Adapter




USB 2.0 to Ethernet 10/100Mbps, to be used when redundant communications is needed for PEGASUS.








9. USB Wi-Fi Adapter



USB 2.0 to Wi-Fi (2.4 GHz), to be used when wireless connection is needed for PEGASUS.

 Please make sure that the included network adapters are labeled with the same serial number as your PEGASUS device. For security, these are the only external network adapter that will work with your PEGASUS. Any other network adapter will be detected as a security thread and will be immediately disabled by PEGASUS.

6 Important Notes

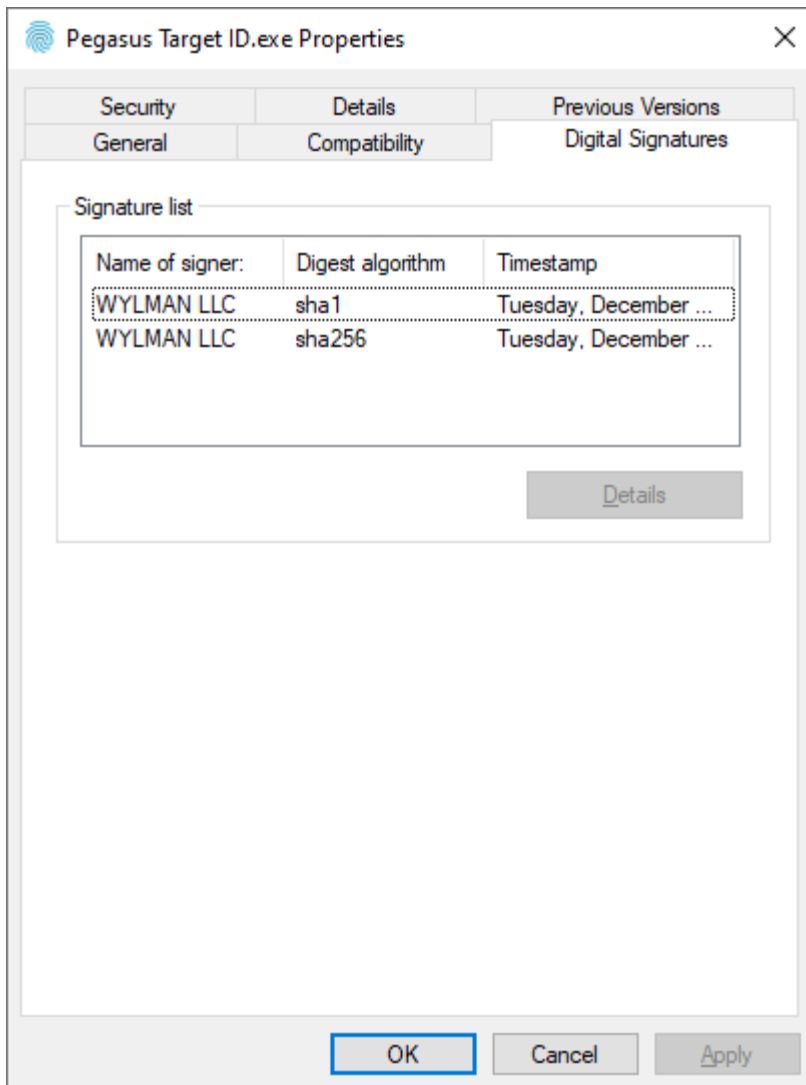
-  All passwords in the system are set to “WYLMAN” as default. It is strongly recommended to change the passwords on the first use and frequently.
-  If wireless connection is required, connect the Wi-Fi adapter included to PEGASUS using one of the available USB 2.0 ports.
-  If communication redundancy is required, connect the USB Ethernet adapter included and/or Wi-Fi adapter included to the available USB 2.0 ports.
-  Default passwords can be restored in case administrator password is lost. Please contact support@wylman.com for assistance with passwords reset.
-  If authentication between PEGASUS and Target machine using PEGASUS Shield fails, this may be due to unsynchronized time, please make sure that PEGASUS system time and Target machine time are synchronized.
-  If a hardware change was done to the Target machine or assigning a new Target machine, PEGASUS Shield must be reconfigured. Please contact support@wylman.com for assistance.
-  Before Launching PEGASUS Shield software, make sure PEGASUS is connected to Target machine using the provided USB cable, otherwise PEGASUS Shield will not work.

7 Getting Started

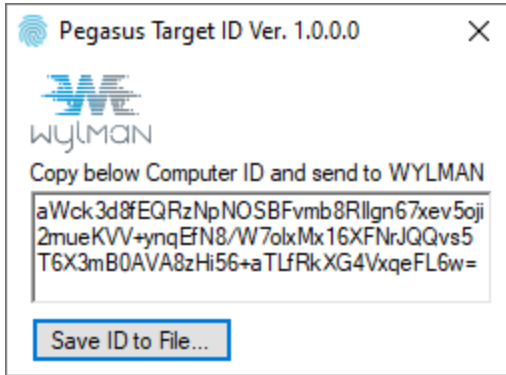
7.1 Assigning PEGASUS Target

PEGASUS will only work with the assigned PEGASUS Target Machine, to assign a target machine to PEGASUS follow this procedure.

1. Plug the provided PEGASUS Shield USB in the machine you want to assign as PEGASUS Target
2. Browse to the root folder on the USB drive, the USB should only have one file "Pegasus Target ID.exe"
3. Before running the program, right click on the file, select properties and then go to Digital Signatures Tab
4. Verify the program digital signature is made by WYLMAN LLC, this makes sure that you have a safe and untampered with program.




5. If you don't find the digital signature or it states anything else other than WYLMAN LLC, DO NOT RUN the program, remove the USB immediately and contact WYLMAN for support
6. If digital signature is verified, run Pegasus Target ID.exe
7. This software pulls the hardware ID of your machine, this ID is encrypted for your security





8. You may save the ID to a text file by pressing "Save ID to File" then email this file to WYLMAN to prepare your license (Typically takes 1 business day)
9. The ID may be provided to WYLMAN in a phone call if the user is not comfortable sending the encrypted text, call +1-832-632-4400 for assistance
10. Once the license has been prepared, WYLMAN will send an email (to the email on the account) notifying the user that the license is ready and PEGASUS can be activated

7.2 Activation

This procedure explains how to activate your PEGASUS.

 *Make sure the box include all contents mentioned in the paper manual. Do not mix and match serialized components.*


 This procedure assumes the user has read and completely understood the instructions in the paper manual, powered up PEGASUS and has a way of interfacing with it (direct using keyboard, mouse and a monitor or remotely using Microsoft Remote Desktop or TeamViewer).

 PEGASUS is configured to start automatically once the power supply has been connected. This insures that the device will restart after a loss of power event has been resolved.

 The procedure assumes that PEGASUS is connected to the internet.

Procedure

1. After PEGASUS finishes the initial boot, the main login screen will show, login using PEGASUS USER password


 All passwords in the system are set to "WYLMAN" as default. It's strongly advised to change the passwords on the first use and frequently.

For security, week passwords will not be allowed by the system.

2. After logging in, PEGASUS will continue to boot and a splash screen will popup



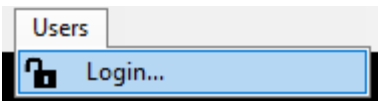
3. During this time the system is going through software checks, hardware check and files integrity checks. If any problem was detected, PEGASUS will state the problem on the Splash screen and shutdown. If this happens, contact WYLMAN for support

 Make sure no external removable drives are connected to PEGASUS, this will be detected as a security threat and PEGASUS will shutdown.

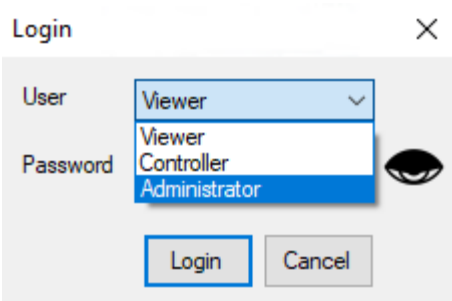
4. After all checks are passed, PEGASUS main screen will be shown



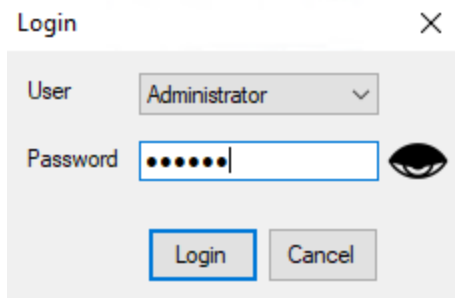
5. Go to Users -> Login



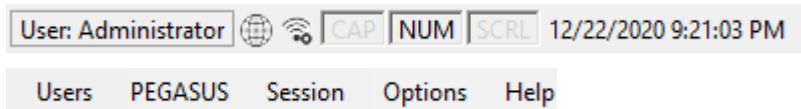
6. Select Administrator



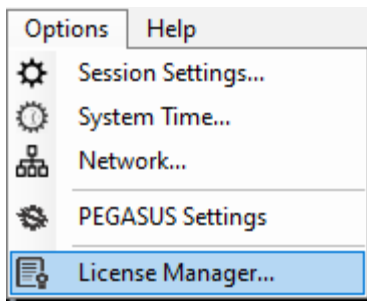
7. Type your password and press Login



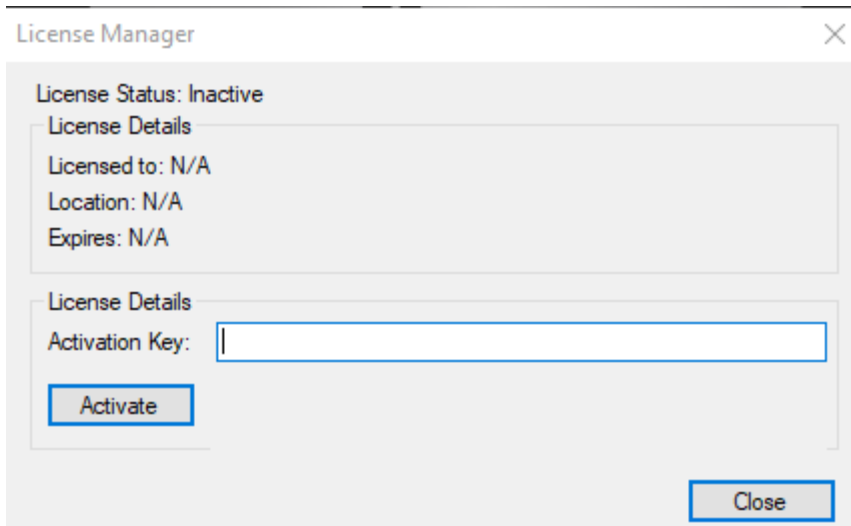
8. The status bar will now show the logged in user as Administrator and Administrator controls will be available on the menu bar




9. Go to Options -> License Manager



10. License Manager will popup



11. Enter your Activation Code, should be provided separately by an email from WYLMAN

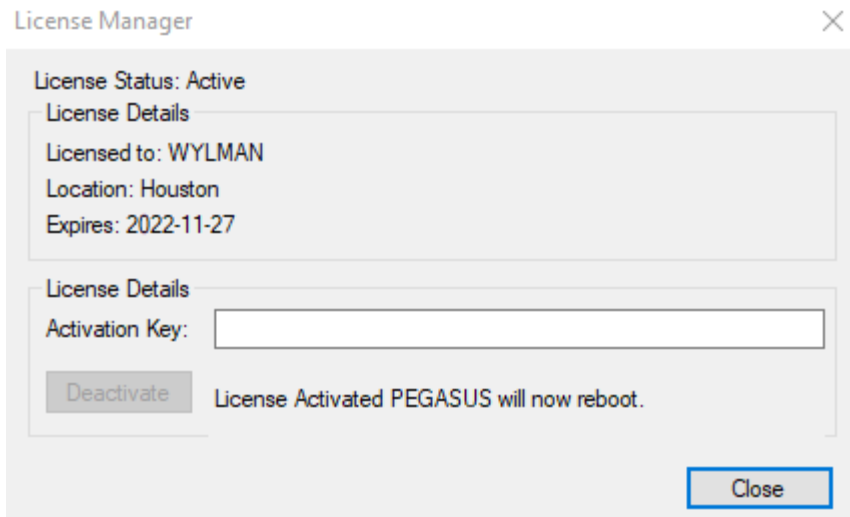
 Activation code will be needed to deactivate PEGASUS in case user wants to change the assigned target machine.

12. Click Activate

13. If the activation code is wrong an message stating "Activation Failed" will appear


14. If the activation code is correct, PEGASUS will be activated and will automatically restart to finalize the activation


process



7.3 Deactivation

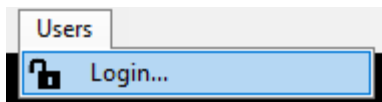
This procedure explains how to deactivate your PEGASUS. PEGASUS must be deactivated and reactivated in order to pair it with a different target machine.

 This procedure assumes PEGASUS is already activated.

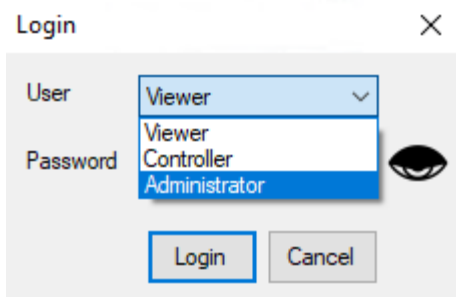
 The procedure assumes that PEGASUS is connected to the internet.

Procedure

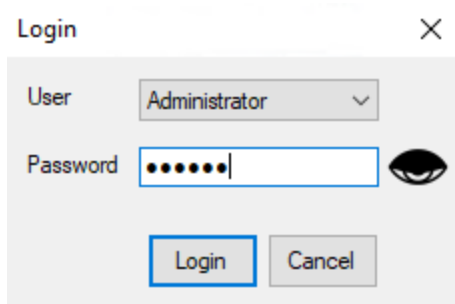
1. If Go to Users -> Login



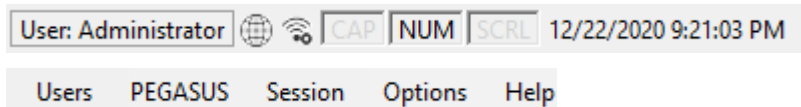
2. Select Administrator



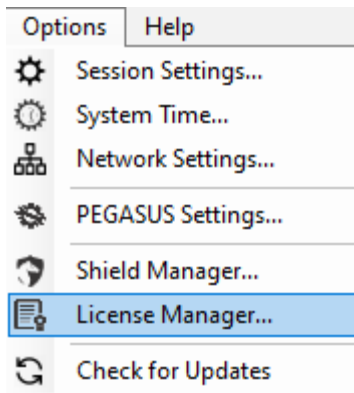
3. Type your password and press Login



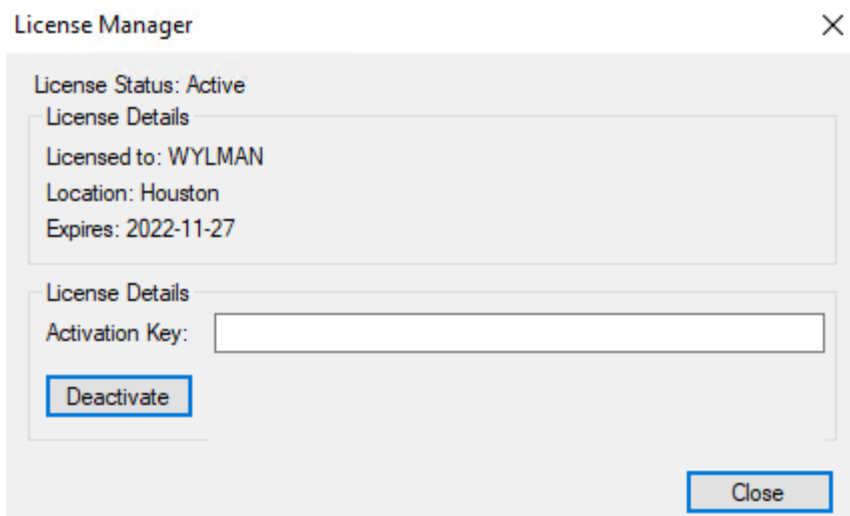
4. The status bar will now show the logged in user as Administrator and Administrator controls will be available on the menu bar



5. Go to Options -> License Manager

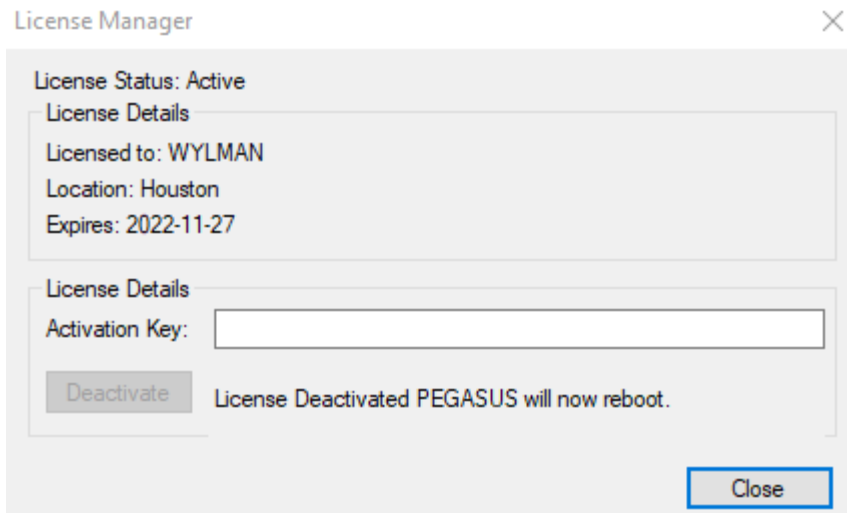


6. License Manager will popup




7. Enter your Activation Code used to activate PEGASUS
8. Click Deactivate, confirm deactivation request
9. If the activation code is wrong an message stating "Wrong Activation Code" will appear
10. If the activation code is correct, PEGASUS will be deactivated and will automatically restart to finalize the

activation process

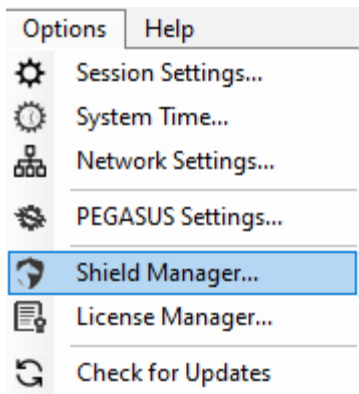


7.4 Activating/Updating PEGASUS Shield

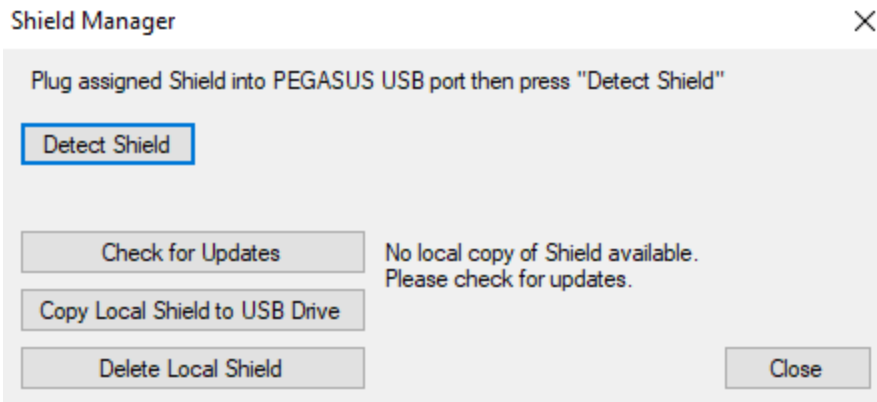
This procedure explains how to activate or update your PEGASUS Shield.

 This procedure assumes that PEGASUS has already been activated and connected to the internet and Administrator is logged in.

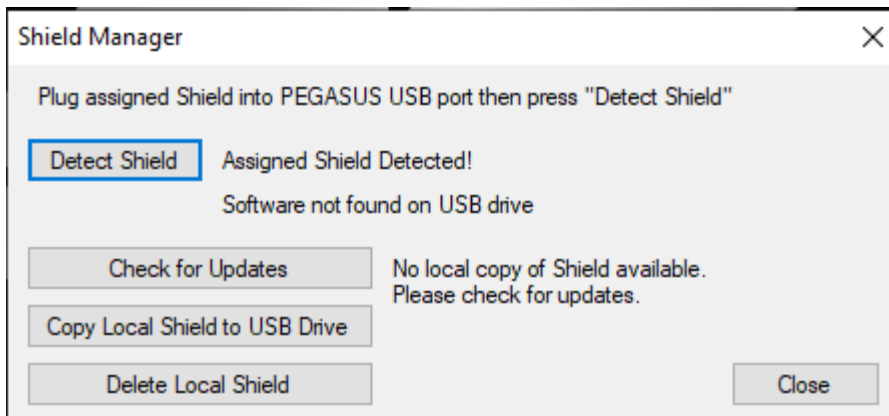
1. Go to Options -> Shield Manager



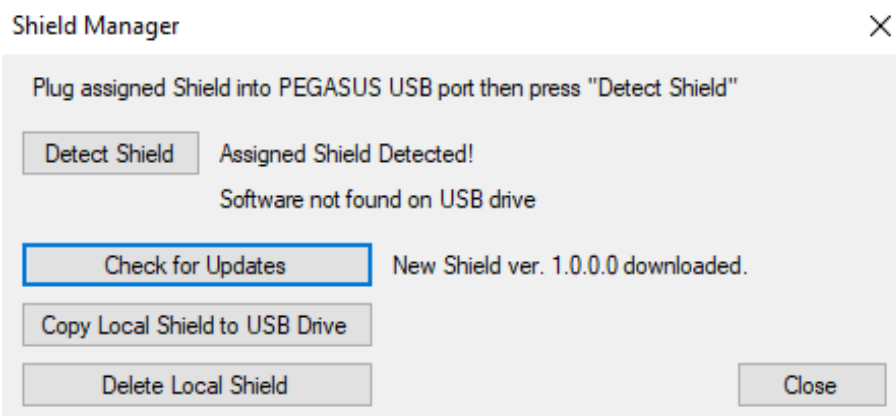
2. Plug in the PEGASUS Shield USB into a PEGASUS USB port
3. Click "Detect Shield"



4. If an unapproved USB drive was inserted, PEGASUS will detect it as a security threat and disable it and immediately shutdown.
5. If the assigned USB device was inserted it will be detected and the system will check on the PEGASUS Shield software version (if any) on it.



6. The system shows if there is a local copy of PEGASUS Shield software available and its version
7. Click Check for Updates
8. The system will connect to WYLMAN server and check for the latest PEGASUS Shield software available and download it if there is no local copy or the online software version is higher than the local copy, then show its version.



9. While PEGASUS Shield USB is still plugged in PEGASUS, click "Copy Local Shield to USB Drive", the software will be copied and the software will show a confirmation message
10. Remove PEGASUS Shield USB from PEGASUS



If the user is changing the target machine and need to download the new Shield software, the use must delete the local Shield copy before clicking "Check for Updates"

8 Users

8.1 Users Privileges

PEGASUS has four users, below we will explain the access privileges of each.

1. None:

If no PEGASUS users are logged in, there is absolutely no access to the user except to log in as a different user.

2. Viewer:

Viewer will be able to Shutdown PEGASUS and Start a View session, while in the session they can only view the desktop of the target machine.

3. Controller:

Controller will be able to Shutdown PEGASUS and Start a Control session, while in the session they can view the desktop of the target machine and control it's keyboard and mouse.

4. Administrator:


Administrator will have full access to the system setting, send invitation emails and can change password.

5. Power User:

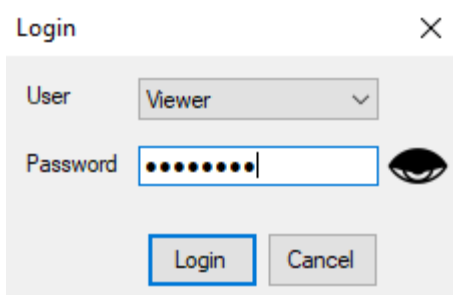
Power User is a maintenance only user and it is restricted for WYLMAN internal use only. It has same privileges as Administrator, in addition it can Set the PEGASUS password, reset all settings and access all license details.

8.2 Logging In

For a user to login, go to Users -> Login

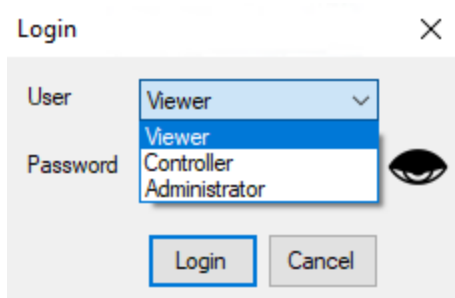
 All passwords in the system are set to "WYLMAN" as default. It's strongly advised to change the passwords on the first use and frequently.

For security, week passwords will not be allowed by the system.

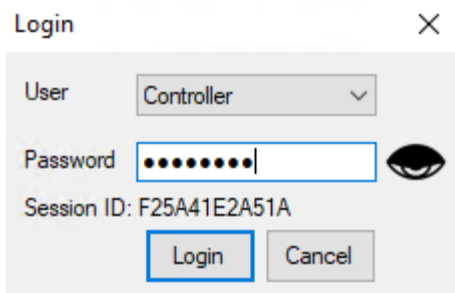


The screenshot shows a 'Login' dialog box. At the top left is the title 'Login' and a close button (X). Below the title bar, there are two input fields: 'User' and 'Password'. The 'User' field is a dropdown menu with 'Viewer' selected. The 'Password' field is a text box with masked characters (dots) and a toggle icon (an eye) to the right. Below the input fields are two buttons: 'Login' and 'Cancel'.

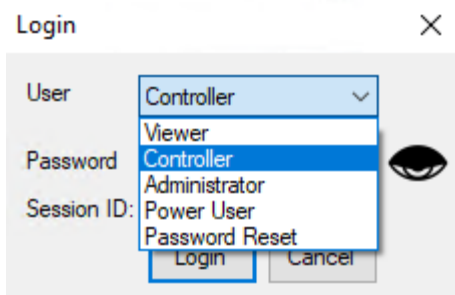
Select the user and type the password then click "Login".




To get access to hidden users, type a wrong password for any user selected and try to log in three times. After failing to login for three times, the system will display the Session ID



Also additional users will be added to the users list



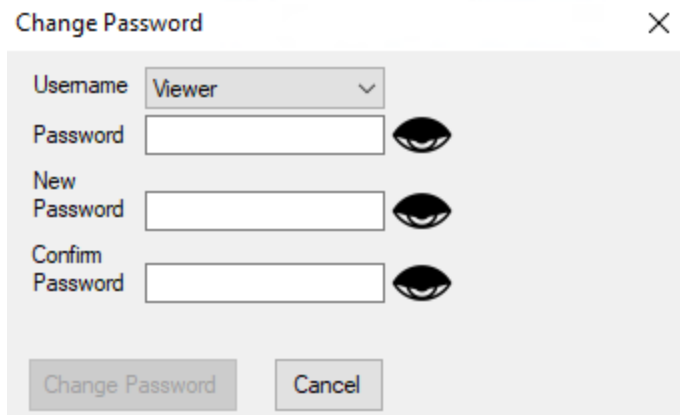
 Password Reset is not a user, however it is used to reset all PEGASUS password to the default password "WYLMAN" in case the administrator password is lost.

8.3 Changing Passwords

Administrator can change PEGASUS password and all users passwords.


To change PEGASUS password, refer to "**PEGASUS Password (Section 9.3.1)**" section.


To change a user password, go to Users -> Change Passwords



A dialog box titled "Change Password" with a close button (X) in the top right corner. It contains three input fields: "Username" with a dropdown menu showing "Viewer", "Password", "New Password", and "Confirm Password". Each password field has an eye icon to its right. At the bottom, there are two buttons: "Change Password" and "Cancel".

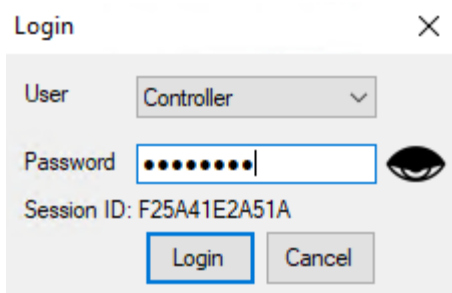
1. Select the user you want to change the password for
2. Type current password
3. Type new password and confirm the new password
4. Click change password.

 For security the new password cannot be empty, and cannot be an easy password. The system automatically check the password strength and only allow the change to a strong password.

 For the password change to succeed, current password must be correct, new password must be strong and matches new password confirmation.

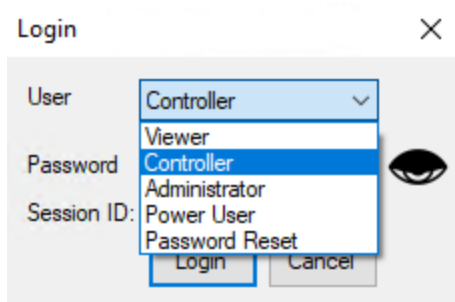
8.4 Resetting Passwords

If administrator password is lost, PEGASUS user must contact WYLMAN for support with passwords reset. To get access to Password Reset, type a wrong password for any user selected and try to log in three times. After failing to login for three times, the system will display the Session ID



A dialog box titled "Login" with a close button (X) in the top right corner. It contains a "User" dropdown menu showing "Controller", a "Password" field with masked characters (dots) and an eye icon to its right, and a "Session ID" field showing "F25A41E2A51A". At the bottom, there are two buttons: "Login" and "Cancel".

Also additional users will be added to the users list



Select Password Reset, provide the Session ID to WYLMAN support. WYLMAN support will provide you with the password reset token.


Select "Password Reset" user, enter the password reset token as the password, then click "Login".

If the Session ID provided to WYLMAN support was correct, and the password reset token typed correctly, all passwords will be reset to the default password "WYLMAN" including PEGASUS Password.

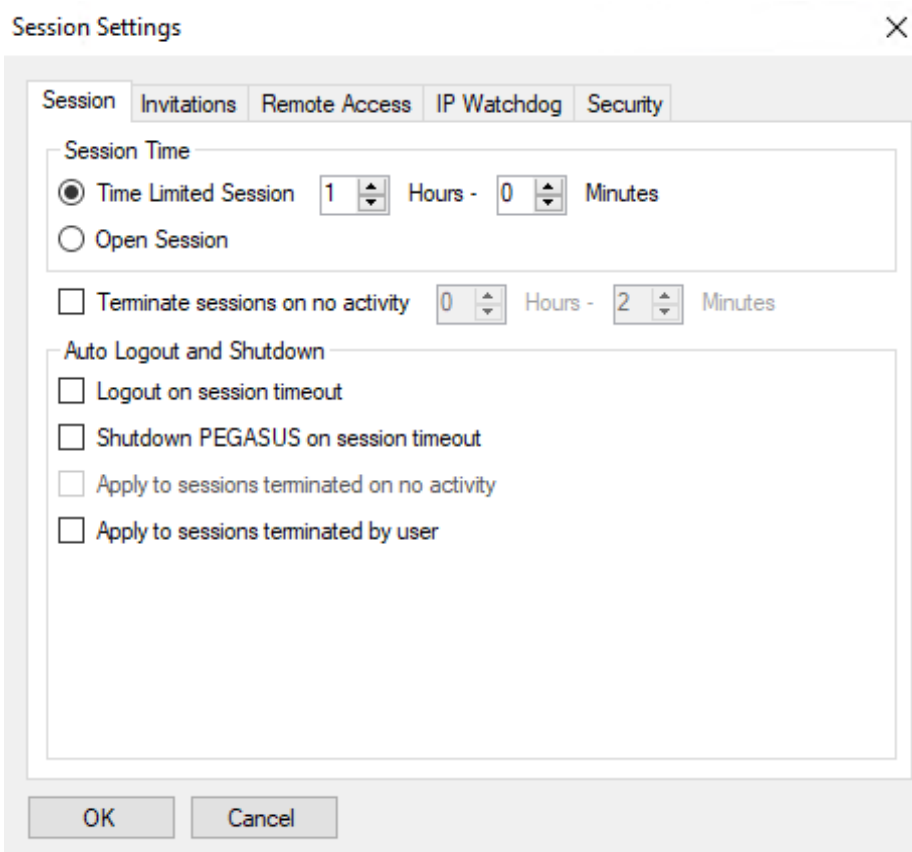
9 Options

9.1 Session Settings

9.1.1 Session Time

 This section assumes that Administrator is logged in.

To access Session Time go to Options -> Session Settings -> Session tab



Session Settings

Session | Invitations | Remote Access | IP Watchdog | Security

Session Time

Time Limited Session 1 Hours - 0 Minutes

Open Session

Terminate sessions on no activity 0 Hours - 2 Minutes

Auto Logout and Shutdown

Logout on session timeout

Shutdown PEGASUS on session timeout

Apply to sessions terminated on no activity


Apply to sessions terminated by user

OK Cancel

There are two time options for a session:


1. Time Limited Session

This option will limit the time of the session to the configured time in minutes and hours.


 Minimum allowed time limit is 1 minute and Maximum is 99 hours and 59 minutes.

2. Open Session

This option will keep the session open until it's terminated by user or by a pre-configured auto termination option.

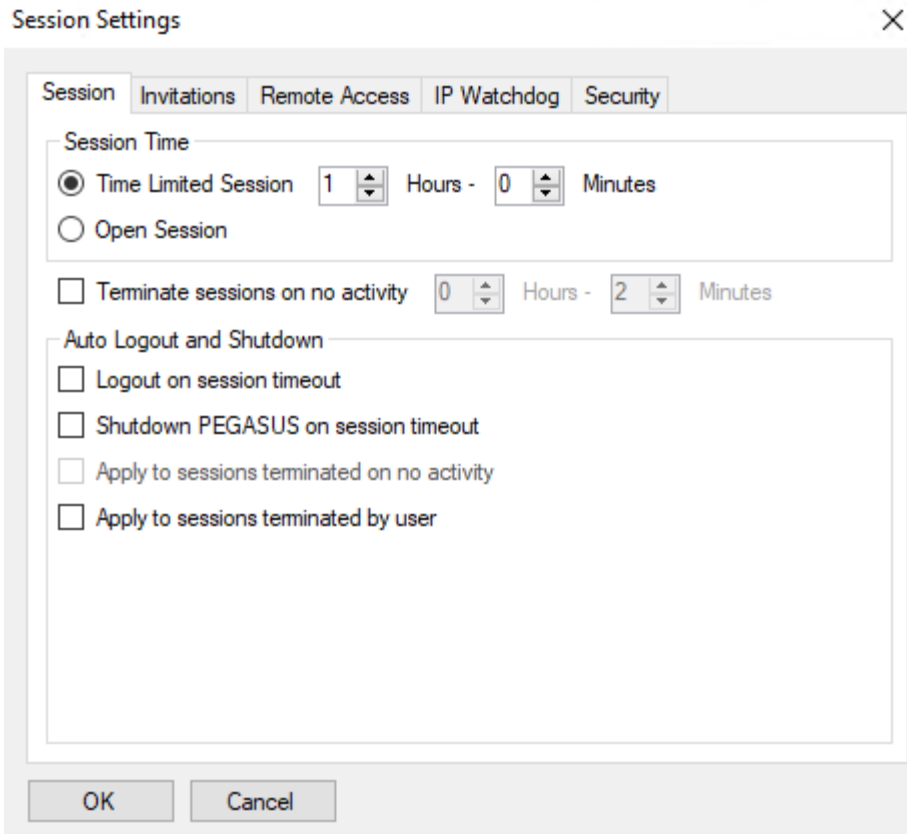
 Session time options are applied to both View and control sessions.

Additional option is provided to terminate sessions on no activity from the user, if enabled the session will terminate if the user had no activity for the configured time.

 Minimum allowed no activity time limit is 1 minute and Maximum is 99 hours and 59 minutes.

9.1.2 Auto Logout and Shutdown

This section explains the auto logout and shutdown options based on session termination for none security threat reasons.



Session Settings

Session | Invitations | Remote Access | IP Watchdog | Security

Session Time

Time Limited Session 1 Hours - 0 Minutes

Open Session

Terminate sessions on no activity 0 Hours - 2 Minutes

Auto Logout and Shutdown

Logout on session timeout

Shutdown PEGASUS on session timeout

Apply to sessions terminated on no activity

Apply to sessions terminated by user

OK Cancel

- Logout on session timeout

If enabled, the system will automatically logout the user when session ends on timeout.

- Shutdown PEGASUS on session timeout

If enabled, the system will automatically shutdown PEGASUS when session ends on timeout.

- Apply to sessions terminated on no activity

Available when session termination on no activity option is enabled. If enabled the system will apply the logout and shutdown settings on a session terminated on no user activity.


- Apply to sessions terminated by user


If enabled the system will apply the logout and shutdown settings on a session terminated by the user.

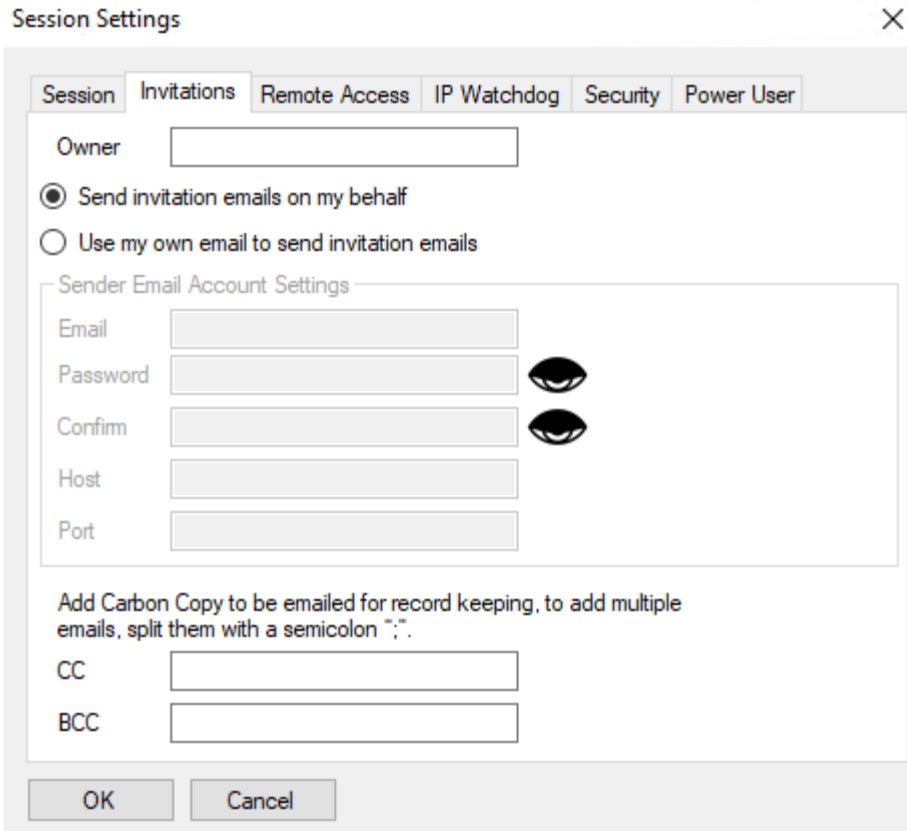
9.1.3 Session Invitations

The administrator may want to send session access credentials and/or instructions to the remote user. To access session

invitations go to Options -> Session Settings -> Invitations tab.

 The procedure assumes that Administrator is logged in.

 Sending invitations is optional for the ease of use and convenience of the user. The user may send the required credentials to the remote user in any other means.



Session Settings

Session Invitations Remote Access IP Watchdog Security Power User


Owner


Send invitation emails on my behalf

Use my own email to send invitation emails

Sender Email Account Settings

Email

Password 

Confirm 

Host

Port

Add Carbon Copy to be emailed for record keeping, to add multiple emails, split them with a semicolon ";".

CC

BCC

OK Cancel

- Owner

Write the name of the person or entity owns the Target machine; this is included in the invitation email to let the remote user know who sent the email.

- Options for email used for sending invitations:

1. Send invitation emails on my behalf

When selected, the system will be sending invitations from **pegasus@wylman.com**. This email is not monitored and configured to not keep records of any sent emails.

2. Use my own email to send invitation emails


When selected, the user can configure the email he wants to use to send invitations to remote user. Contact your system administrator or IT department for details on how to configure your own email.

- CC

Enter email(s) address(es) to be included by default in CC of the invitation emails. This is useful when the user wants to keep record of sent invitations.

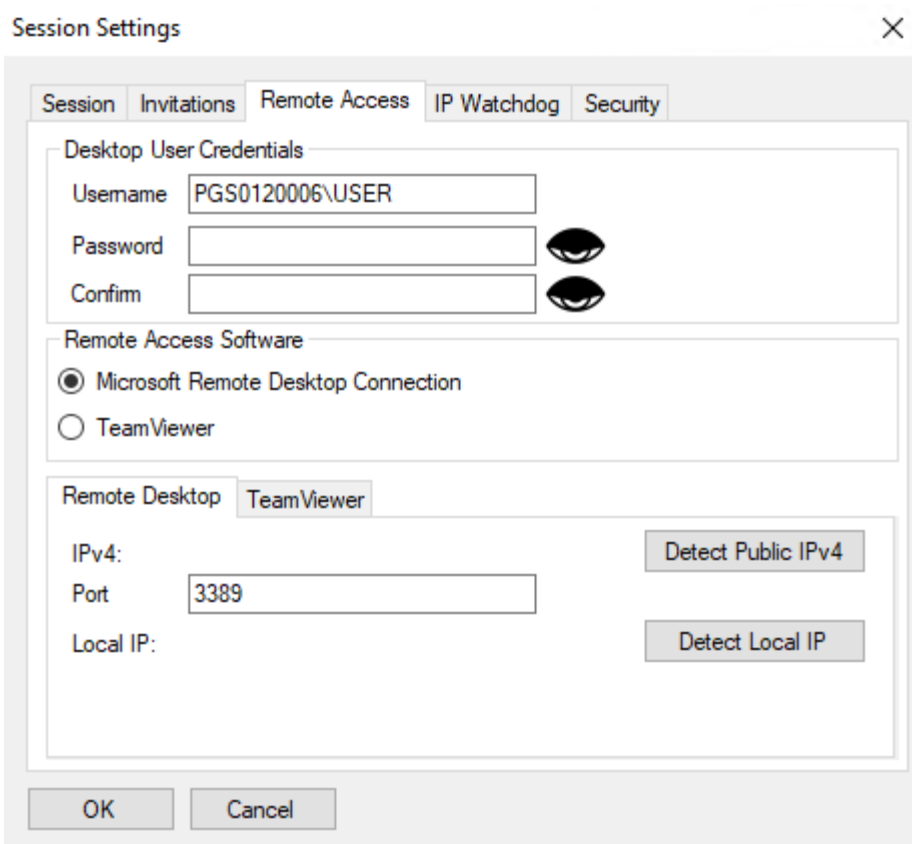
BCC

Enter email(s) address(es) to be included by default in BCC of the invitation emails. This is useful when the user wants to keep record of sent invitations without showing the email used for record keeping to the remote user.

 The email configurations made here will also apply to the notifications sent by the IP Watchdog.

9.1.4 Remote Access

This section is used to configure the remote access tool used by the remote user to access PEGASUS, this information also can be sent to the remote user in the invitation email.





Session Settings

Session Invitations Remote Access IP Watchdog Security

Desktop User Credentials

Username PGS0120006\USER

Password 

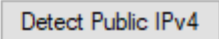
Confirm 

Remote Access Software

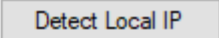
Microsoft Remote Desktop Connection

TeamViewer

Remote Desktop TeamViewer

IPv4: 

Port 3389

Local IP: 

OK Cancel

The desktop username and password will be required for the remote user to gain access to PEGASUS. The username is automatically detected and filled by the system. The password may be filled by the administrator to be able to send it in a session invitation email.


There are two remote desktop applications currently supported by PEGASUS

1. Microsoft Remote Desktop

When selected, the port number entered should match the port number used in the port forwarding configuration in the router. The system will automatically update the firewall settings to allow for the port to work. Changing the port number will require PEGASUS to restart to take effect.

To get the current public IPv4 address click on "Detect Public IPv4"

To get the current local IPv4 address click on "Detect Local IP"

 There is no need to manually detect the IPs before sending a session invitation, the system automatically detects the current IP and send them if they where picked to be included in the invitation email.

2. TeamViewer

When selected the system will automatically show the required credentials fields to access PEGASUS using TeamViewer

Session Settings

Session Invitations Remote Access IP Watchdog Security

Desktop User Credentials

Username

Password

Confirm

Remote Access Software

Microsoft Remote Desktop Connection

TeamViewer

Remote Desktop TeamViewer


ID

Password

Confirm

TeamViewer access requires the PEGASUS ID and the password, to get those credentials click on Launch TeamViewer to show the TeamViewer screen.

TeamViewer is pre-configured to generate a new very secure password every time PEGASUS restarts.

 WYLMAN does not provide TeamViewer accounts. TeamViewer is pre-configured for free personal use. It is up to the customer to decide if they are using PEGASUS for commercial use and using a paid TeamViewer account.

9.1.5 IP Watchdog

IP Watchdog function may be used if the user is using the Microsoft Remote Desktop to provide remote access to PEGASUS and does not utilize a static public IP.

IP Watchdog can monitor the changes in both local and public IPv4 addresses and send notification(s) to the user with the new IP(s).


One IP address must be picked for the IP Watchdog function to work. IP Watchdog will monitor the picked IP(s) and send notification(s) when a change is detected.


The frequency of checking the IP addresses can be configured between a minimum of 1 minute and a maximum of 60 hours.

If the user wants to get a notification of the current IP addresses whether a change of IP(s) was detected or not, enable the "Report IPs on Startup" option.

To send notifications to email(s), enable the "Email" option and type the email(s) to receive the notifications.

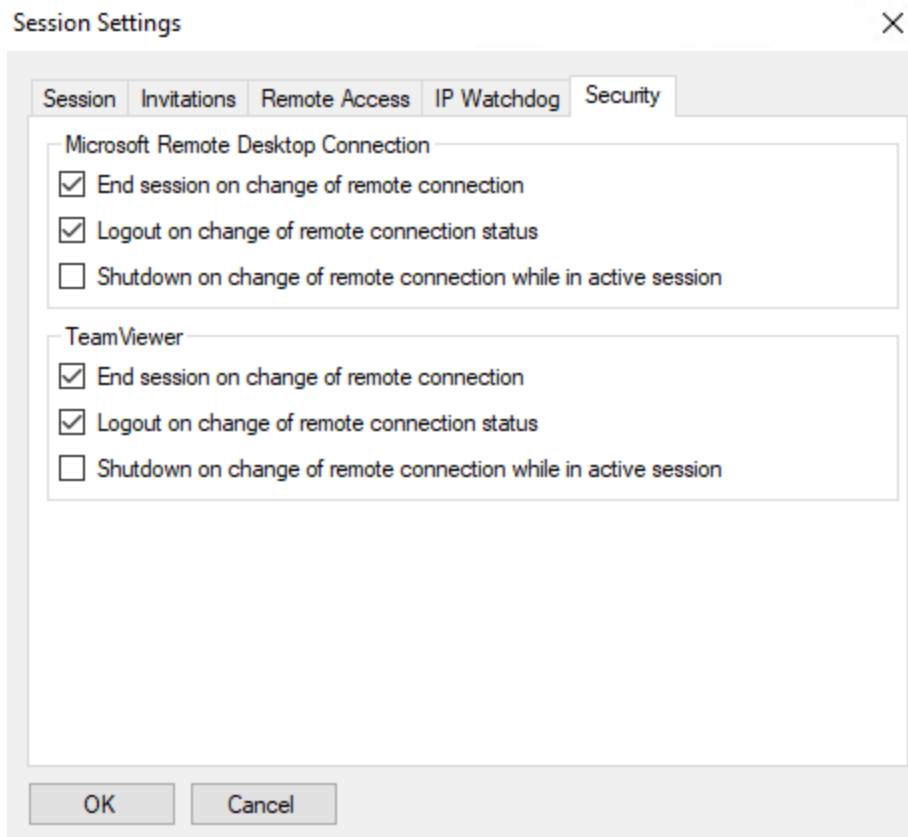
To send notifications to phone(s) by SMS, enable the "SMS" option and type the email(s) to receive the notifications.

 To send text message to a phone number, the phone number must be written in the below format:
number@carriergateway
Most carriers provide the gateway information on their websites. Please contact your carrier to find the gateway information.


 To send to multiple emails and/or phones, addresses must be separated by a semicolon " ; "

9.1.6 Security

PEGASUS has the ability to detect changes made to remote desktop connections made to it and provides the user with options to terminate the sessions, logout the user, or Shutdown PEGASUS in case a change was detected.



The administrator should select the security measures needed for their use. WYLMAN pre-configured the system with the advised security measures.

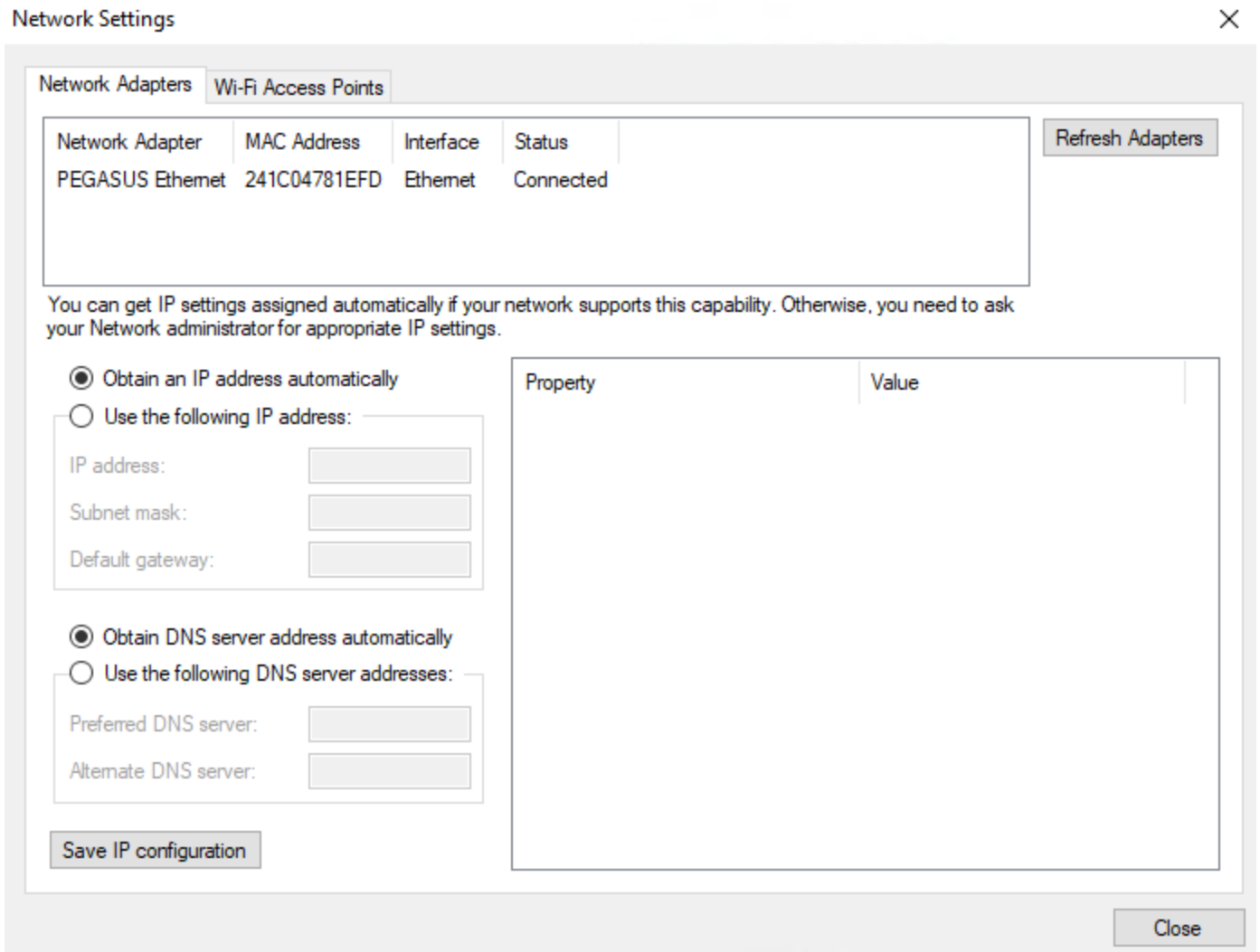
 Security measure configured logout and shutdown will always be active even if there is no active session.

9.2 Network Settings

9.2.1 Network Adapters


This section explains the PEGASUS Network Adapters options available for administrator.

To access Session Time go to Options -> Network Settings -> Network Adapters tab



The network adapter tab displays the available network adapters, their MAC addresses, Interface type and Status.

If a new adapter was connected or removed after opening this window, click "Refresh Adapters" to update the adapters list.

 For maximum security, PEGASUS will only allow the approved network adapters to work. Any external non-approved network adapters plugged in the PEGASUS it will be automatically disabled.

To view and/or modify a network adapter details, select it from the adapters list

The screenshot shows the 'Network Settings' dialog box with the 'Wi-Fi Access Points' tab selected. At the top, there are two tabs: 'Network Adapters' and 'Wi-Fi Access Points'. Below the tabs is a table listing network adapters:

Network Adapter	MAC Address	Interface	Status
PEGASUS Wi-Fi	98482779195D	Wireless80211	Not connected
PEGASUS Ethernet	241C04781EFD	Ethernet	Connected

To the right of the table is a 'Refresh Adapters' button. Below the table, there is a text box: 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your Network administrator for appropriate IP settings.'

Below the text box are two radio button options for IP configuration:

- Obtain an IP address automatically
- Use the following IP address:

Under the second option, there are three input fields:

- IP address: 192.168.0.82
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.0.1

Below these are two more radio button options for DNS configuration:

- Obtain DNS server address automatically
- Use the following DNS server addresses:

Under the second option, there are two input fields:


- Preferred DNS server: 192.168.0.1
- Alternate DNS server: 192.168.0.1

At the bottom left is a 'Save IP configuration' button. On the right side of the dialog, there is a large table showing properties for the selected 'PEGASUS Ethernet' adapter:

Property	Value
Name	PEGASUS Ethernet
Interface Type	Ethernet
Connection-specific DNS Suffix	
Description	Realtek PCIe GbE Family Controller
Physical Address	241C04781EFD
ID	{99035660-1884-41DA-AD30-FA...}
Speed	100 Mbps
Status	Connected
DHCP Enabled	Yes
IPv4 Address	192.168.0.82
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1

At the bottom right of the dialog is a 'Close' button.

When a network adapter is selected PEGASUS will show available details and IPv4 settings.

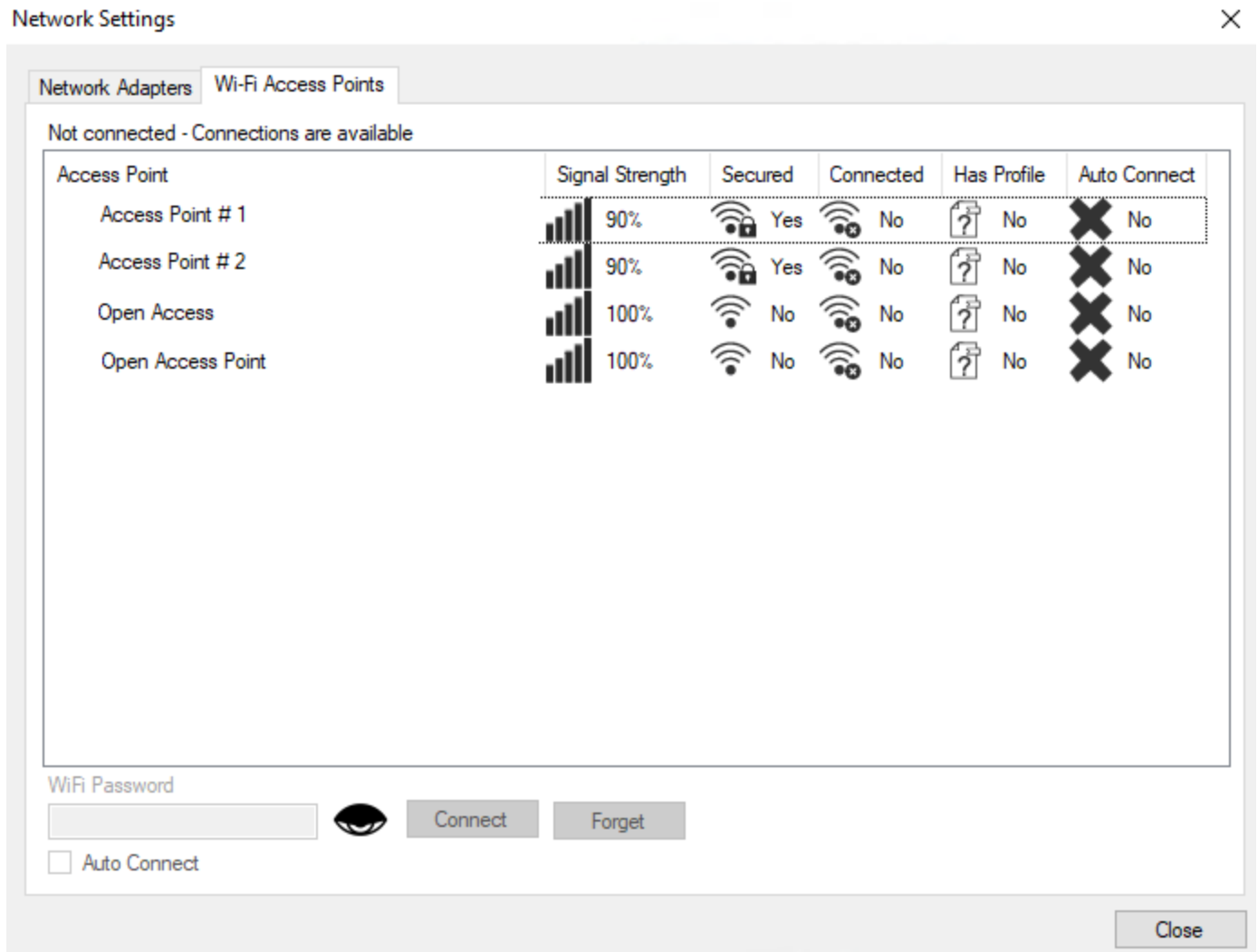
 Please contact your network administrator for help on how to configure your adapter(s) to connect to LAN and internet.

After making changes to adapter IPv4 settings, click "Save IP configuration" to apply the new settings.

9.2.2 Wi-Fi Access Points

This section explains the Wi-Fi options available for administrator.

To access Session Time go to Options -> Network Settings -> WiFi Access Points tab



The Wi-Fi Access Points tab displays the available Wi-Fi networks, their Signal Strength, Secured or not, Connected or not, has a local profile on PEGASUS system or not and whether configured for Auto Connect or not.

The list is continuously refreshed to show changes in the available access points and their properties.


If an access point has a profile, its previously used password (if any) can be retrieved and viewed by holding down the eye next to the password field. It also can be configured to be connected to automatically whenever it is available.

To connect to an access point, select it from the list, if it is secured, the password field will be enable to allow the user to enter the password then click "Connect".


The current connection status is displayed at the top of the access points list.

The current status of Network and Wi-Fi is always available on the status bar at the bottom of the PEGASUS main window.

An access point may be configured for Auto connect by selecting it and enabling the "Auto Connect" option. This option is only available for an access point that has a profile.

 A profile is automatically created for an access point after the first try to connect to it, whether the connection was successful or not.

To erase a profile of an access point, select the access point then click "Forget".


 If the profile was erased for an access point while it was connected, PEGASUS will automatically disconnect from the access point.

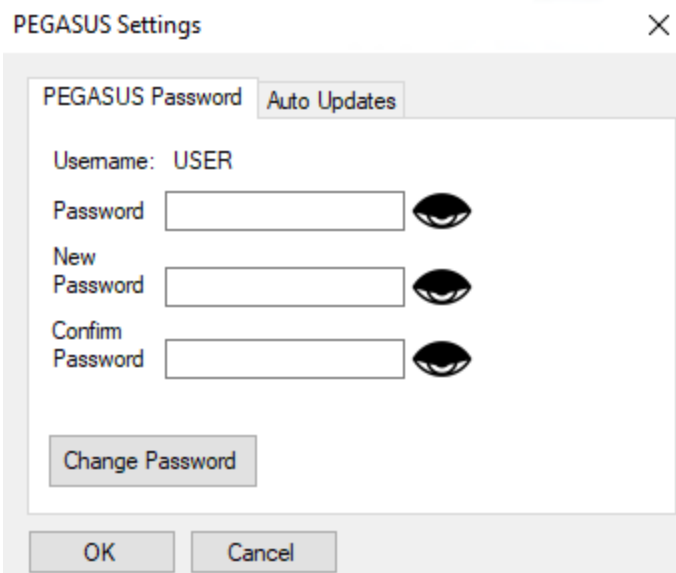
9.3 PEGASUS Settings

9.3.1 PEGASUS Password


This section explains how to change the PEGASUS Password.


To access Session Time go to Options -> PEGASUS Settings -> PEGASUS Password tab

 "WYLMAN" is the default PEGASUS password.



To change PEGASUS password, type the current password, the new password and confirm the new password.

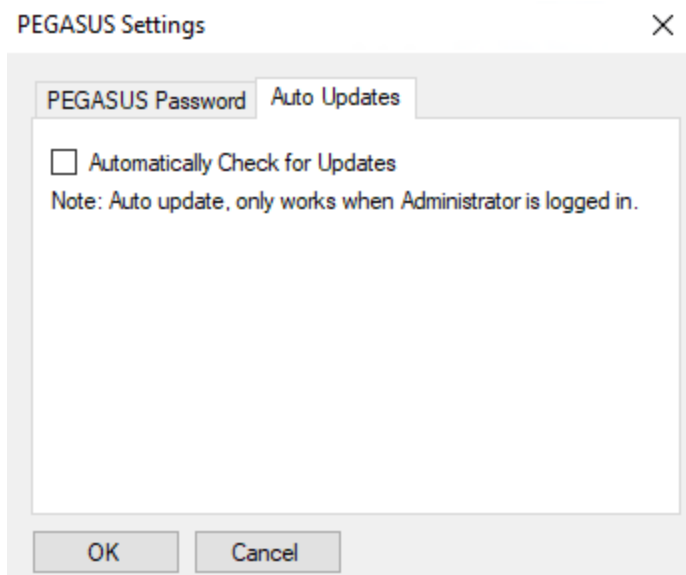
 For security the new password cannot be empty, and cannot be an easy password. The system automatically check the password strength and only allow the change to a strong password.

 For the password change to succeed, current password must be correct, new password must be strong and matches new password confirmation.

9.3.2 Auto Updates


This section explains how to change the automatic updates option..

To access Session Time go to Options -> PEGASUS Settings -> Auto Updates tab



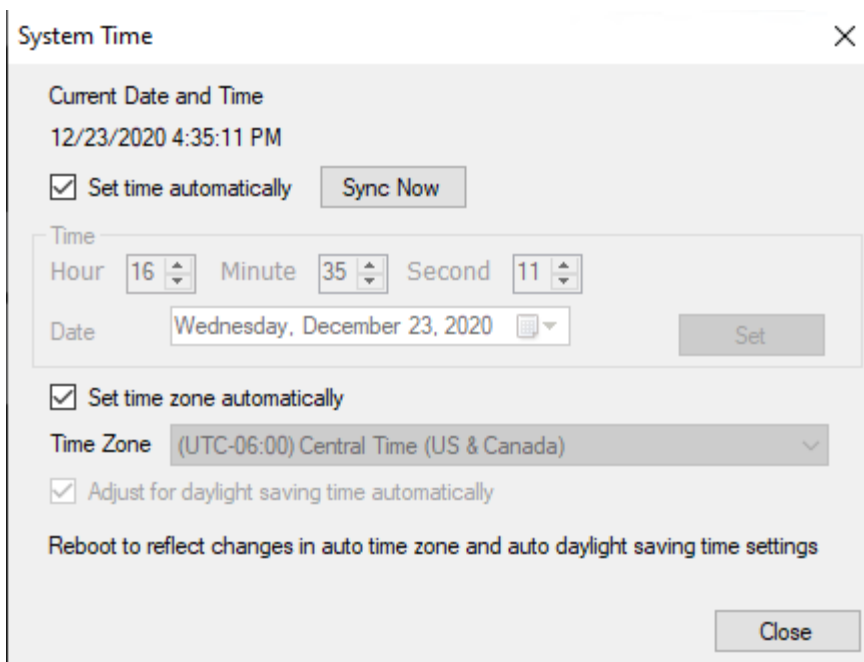
- Automatically Check for Updates


When enabled and only if PEGASUS is activated and when administrator is logged in, the system will automatically check on available updates.

 Refer to "**Check for Updates (Section 9.7)**" section for details on how to perform the PEGASUS update process.

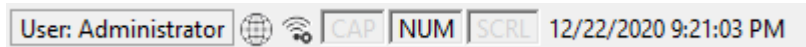
9.4 System Time

This section explains the PEGASUS system time options available for administrator.



 Automatic time synchronization, time zone setting, and Adjusting time for daylight saving time will only work if PEGASUS is connected to the internet.

This window displays the current system time and date. Time and date is also always visible on the status bar on the bottom of PEGASUS main screen.



- Set time automatically

When enabled, the system time will automatically and periodically be synchronized with Microsoft time server.

- Synch Now

Enabled when "Set time automatically" option is enabled. When pressed the system time will be synched with the Microsoft time server.

- Time Group

Enabled when "Set time automatically" option is disabled. Here administrator can manually define the system time and the press "Set" to set the time to the time and date configured.

- Set time zone automatically


When enabled time zone will be automatically set based on the detected location using the public IP address of the system.

- Time Zone

Enabled when "Set time zone automatically" option is disabled. When enable administrator can manually define the time zone for PEGASUS system.


- Adjust for daylight saving time automatically


Always disabled if "Set time zone automatically" option is enabled, otherwise it will be enabled based on the selected time zone and whether it supports daylight saving time or not.

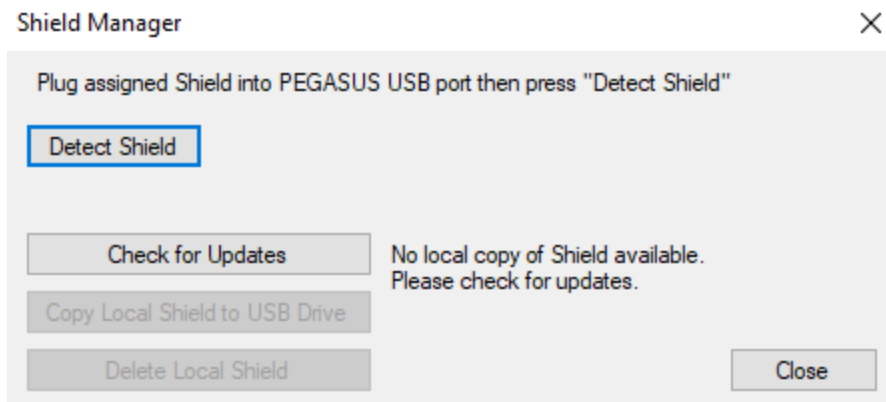
 PEGASUS time must be synchronized to the same time of the target machine for the session authentication using PEGASUS Shield to work.

9.5 Shield Manager

Shield Manager is used to confirm the authenticity of the accompanied PEGASUS Shield USB drive, Updating the Shield software, installing the Shield software on the USB drive. Those are necessary steps to be able to establish a session and to change the target machine.


 This option is only available after PEGASUS has been activated.

 Although PEGASUS Shield USB drive has a lot of extra space, WYLMAN strongly recommends not to use this drive for anything other than the intended use, which is the paring between PEGASUS and its target machine and authenticating sessions.




- Detect Shield

When clicked, the system will search for the authorized Shield USB drive, if found the system will search for the Shield software on the drive and display its version.

 For security, if the system detected any unauthorized USB drives, it will immediately shutdown.

- Check for Updates

When clicked, the system will check the online version of the Shield software and if higher than the local version, or if there is no local version available it will be downloaded and its version will be displayed.

 To check for available updates for PEGASUS Shield, PEGASUS must be connected to the internet.

- Copy Local Shield to USB Drive

When clicked and if the authorized Shield USB drive is inserted into PEGASUS, the local Shield software will be copied to the Shield USB drive.


- Delete Local Shield

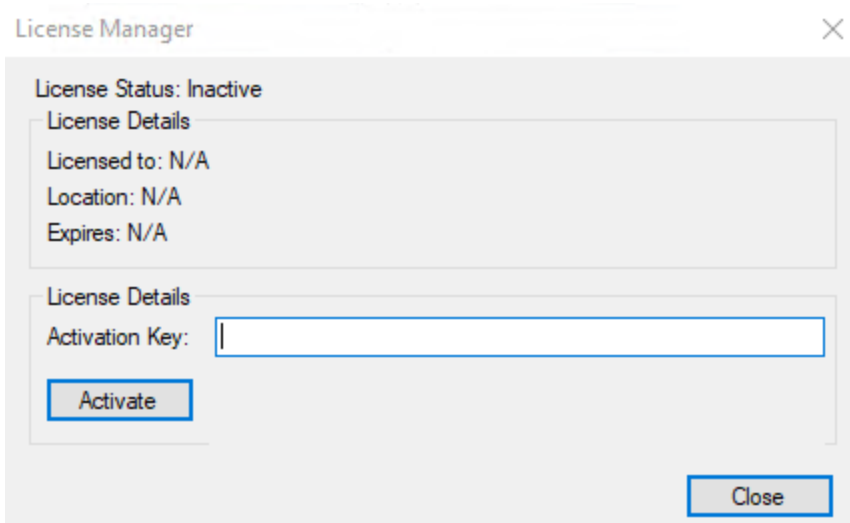
When clicked the local USB drive will be deleted. This is needed when changing target machines to be able to download the new Shield software.

9.6 License Manager

License manager is used to activate and deactivate PEGASUS.


To access License Manager go to Options -> License Manager


 PEGASUS must be deactivated before changing the target machine



The license status and license details are displayed.

To activate or deactivate PEGASUS the activation code must be used.


 If you have more than one PEGASUS device, DO NOT mix the activation code, if an activation code assigned to a different PEGASUS was used, it will be detected on the next startup and disabled.


 PEGASUS will automatically restart after activation or reactivation to complete the activation or reactivation process.

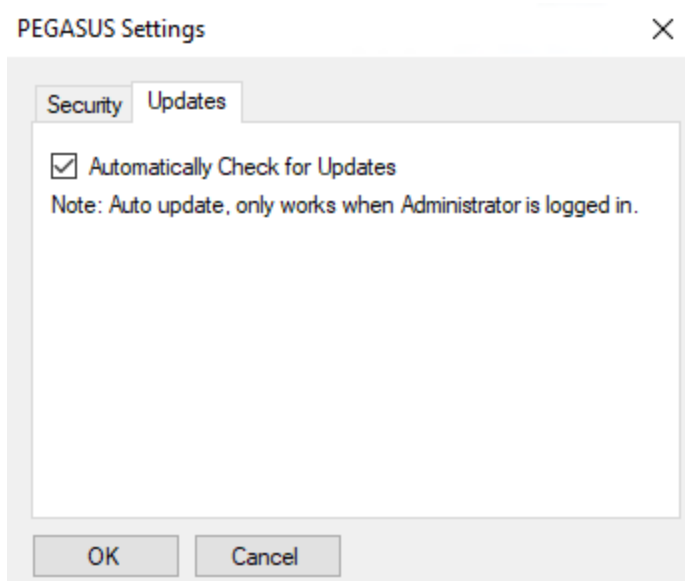
9.7 Check for Updates

Updates will be provided when needed, the updates will have new features and/or fixes for issues in the previous releases. There are two ways to check for updates:

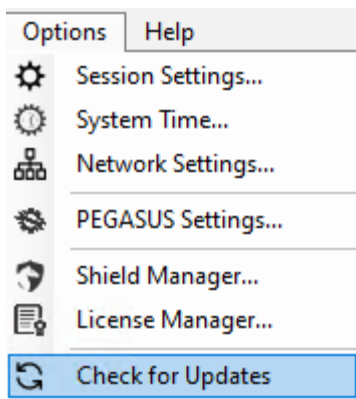
- Automatically check for Updates, to enable check the "Automatically Check for Updates" option under the "PEGASUS Settings -> Updates". When checked the program will automatically check for available updates on the startup.

 Updates will only be available if PEGASUS is activated.

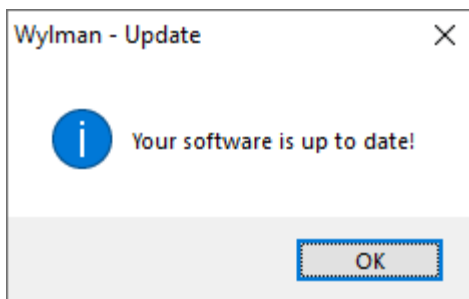
 Updates can only be checked (automatically or manually when Administrator is logged in).



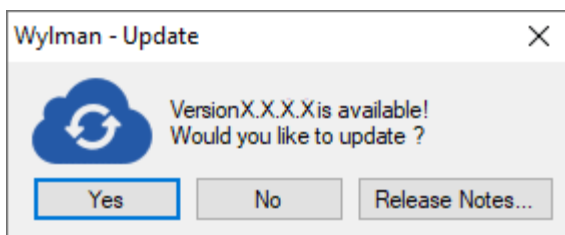
- Manually check for updates, can be done by clicking the "Check for update" button under the "Options" menu.



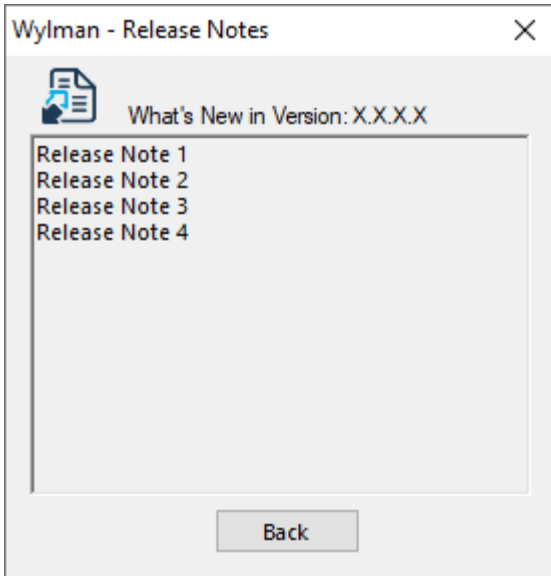
If no updates are available, below message will pop up:



If there is an available update, below message will pop up:

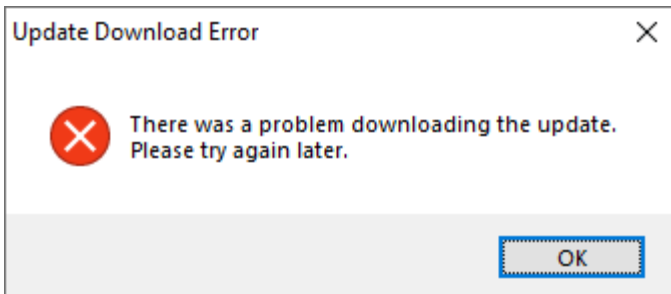



To view what's new in this update user may click on "Release Notes" button, this will show up the release notes for the new version as below:



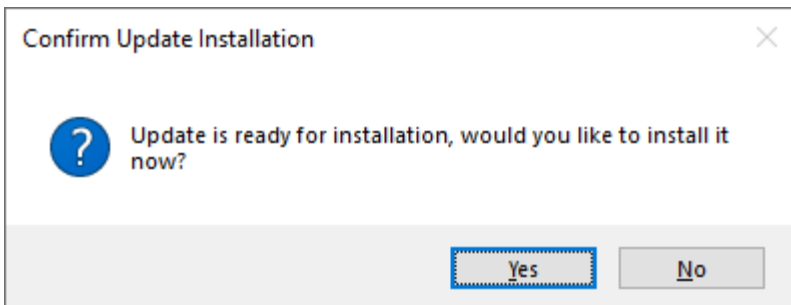
User may select to update the software or not. If selected "Yes", the new update will start downloading. Once finished downloading it will also verify the integrity of the downloaded file to make sure it is not corrupted and also to protect the user against getting an update file that was tampered with or been infected with a virus during the download process.


If the verification failed the user will get the message below:



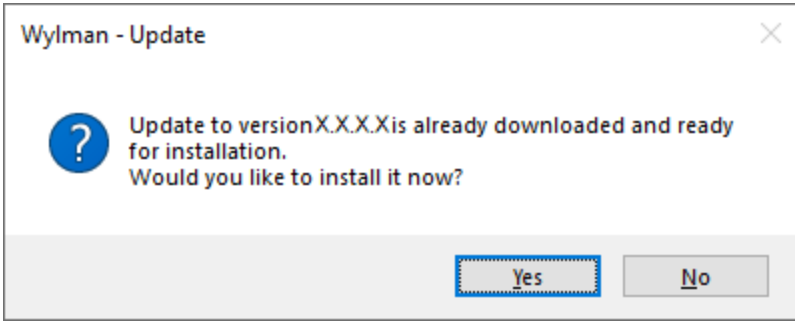
 *If getting problems with updates persisted, please contact WYLMAN for support.*

If verification succeeded, the user may choose to install the update right away, or click "No" to install it later.



 Clicking "Yes" will terminate the program and automatically start the installation process of the new version.

If user decides to postpone the installation, every time the program is restarted user will be asked for permission to install the downloaded update



10 Sessions


10.1 Connecting PEGASUS to Target Machine

Before starting a session, PEGASUS should be connected to the target machine.

There are two connections to be made between PEGASUS and target machine:


1. USB connection

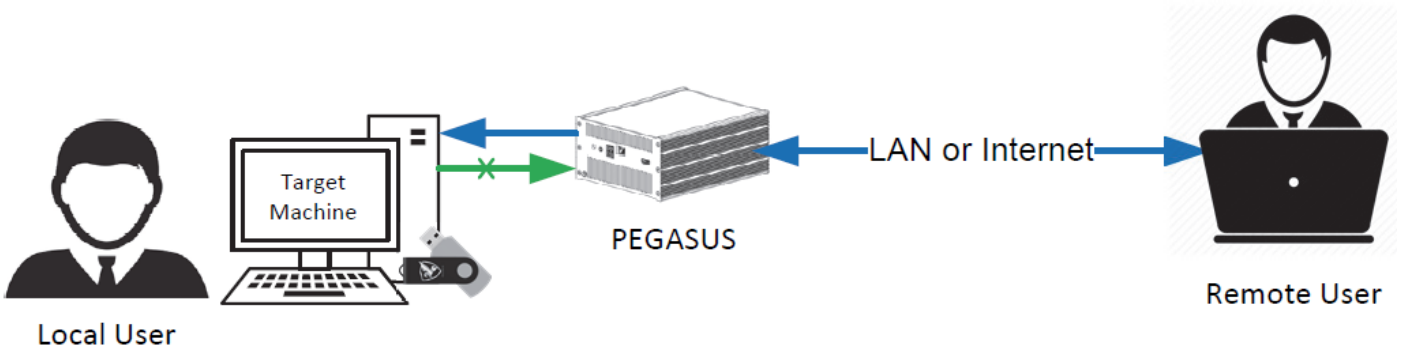
USB connection is used to send the keyboard and mouse commands from PEGASUS to the target machine.

 When PEGASUS is active, USB connection must be established to be able to run PEGASUS Shield software and authenticate and start a session, even if it was a view session.


2. Video connection

Video connection is used to get the desktop display of the target machine to PEGASUS. PEGASUS has 2 video inputs, HDMI and DVI.

 If the target machine has a VGA output, PEGASUS has VGA to DVI converter to be used with the VGA cable (both the cable and converter are included with PEGASUS accessories).




Typical System Configuration for a remote session

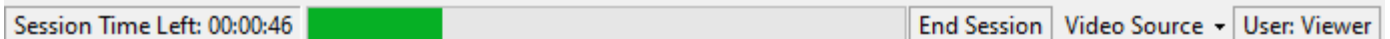
 When connecting the control USB cable to the target computer, confirm that PEGASUS keyboard and mouse have been detected in the device manager. If not detected as keyboard and mouse or was detected as a removable storage disconnect the USB immediately, this may be a sign of tampering with the device and it may not be secured. Contact WYLMAN for support.

10.2 Demo Sessions

Demo sessions are available for testing purpose. A demo session will allow 1 minute view or control session.

To start a demo session go to Session -> Start Demo Session


 This section assumes that PEGASUS is not activated and either Viewer or Controller is logged in.




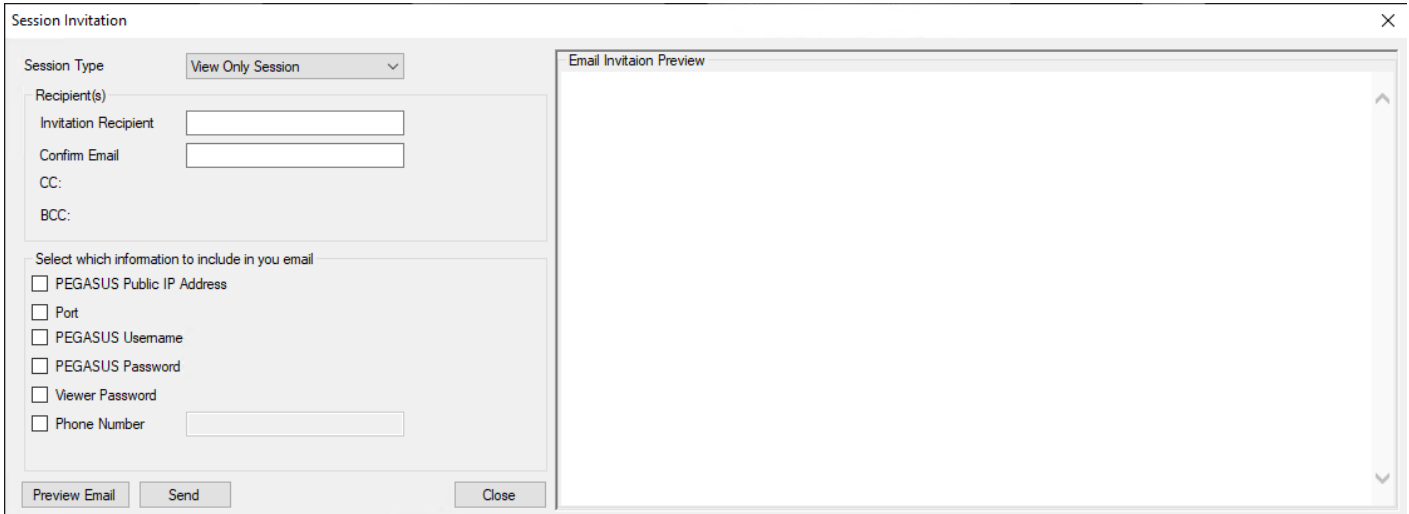
After a demo session expires or if it was terminated by user, to make another demo session PEGASUS must be restarted.

10.3 Session Invitation

The administrator may want to send session access credentials and/or instructions to the remote user. To access session invitations go to Session-> Session Invitation

 The procedure assumes that Administrator is logged in.

 Sending invitations is optional for the ease of use and convenience of the user. The user may send the required credentials to the remote user in any other means.



The email invitation can be configured to the preference of the user to include only the date they user wants to send in the invitation email to the remote user.

- Session Type

Select between View Only Session and Control session. This will automatically adjust the email to send the correct credentials for selected session.

- Invitation Recipient

Type the email address of the remote user. The email address must be confirmed, this to decrease the possibility of typos and make sure that the email will be sent to the intended recipient.

- PEGASUS Public IP Address

Available if Microsoft Remote Desktop Connection was selected in the session settings. If checked, PEGASUS public IP address will be included in the email.

- Port

Available if Microsoft Remote Desktop Connection was selected in the session settings. If checked, port used for Microsoft Remote Desktop connection will be included in the email.

- PEGASUS TeamViewer ID

Available if TeamViewer was selected in the session settings. If checked, PEGASUS ID will be included in the email.

- PEGASUS TeamViewer Password

Available if TeamViewer was selected in the session settings. If checked, PEGASUS TeamViewer password will be included in the email.

- PEGASUS Username

If check, PEGASUS username will be included in the email.

- PEGASUS Password

If checked, PEGASUS password will be included in the email.

- Viewer Password

Available if View Only Session was selected. When checked Viewer password will be included in the email.

- Controller Password

Available if Control Session was selected. When checked Controller password will be included in the email.

- Phone Number

When checked, administrator can type a phone number to be included in the email. This phone number to be used during the session authentication step.

- Preview Email

When clicked, a preview of the email to be sent will be displayed/updated.

- Send

When clicked, the invitation email will be sent.

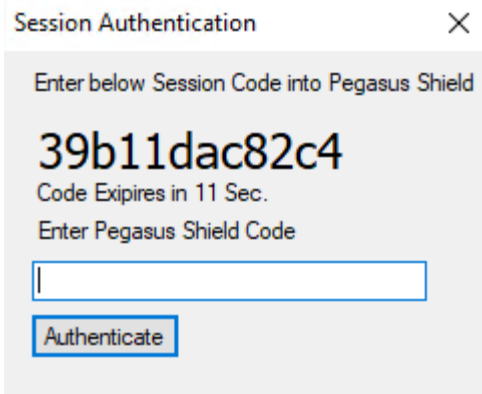
10.4 View Session

View session allows the remote user to only view the desktop of the target machine.

 This procedure assumes PEGASUS is activated and PEGASUS Shield software has been downloaded and copied to the Shield USB drive.

To start a view session, PEGASUS must be connected to internet or LAN (LAN will only allow Microsoft Remote Desktop Connection), powered up and connected to target machine, then follow the procedure below:

1. Remote user to gain access to PEGASUS using the credentials for either Microsoft Remote Desktop or TeamViewer
2. Remote user to login as Viewer
3. The status bar will show the logged in user as Viewer
4. Remote user go to Session -> Start Session
5. Session Authentication screen will popup



Session Authentication ×

Enter below Session Code into Pegasus Shield


39b11dac82c4


Code Expires in 11 Sec.


Enter Pegasus Shield Code


Authenticate

6. The displayed code should be given by the remote user to the local user by preferred means. Keep in mind that the authentication window is only 60 seconds


 The session authentication window is 60 seconds in which the PEGASUS code must be transferred to Shield, then Shield code transferred to PEGASUS. So the advised means of communication between local user and remote user is a phone call.

 To get the maximum of 60 seconds window wait for the current code to expire and a new code is shown then start the authentication process.


 The local user should have PEGASUS Shield USB plugged in the target machine and Shield software running and ready to authenticate the PEGASUS code.

 PEGASUS and target machine times must be synchronized for the authentication process to work. Refer to "**System Time (Section 9.4)**" section for details.

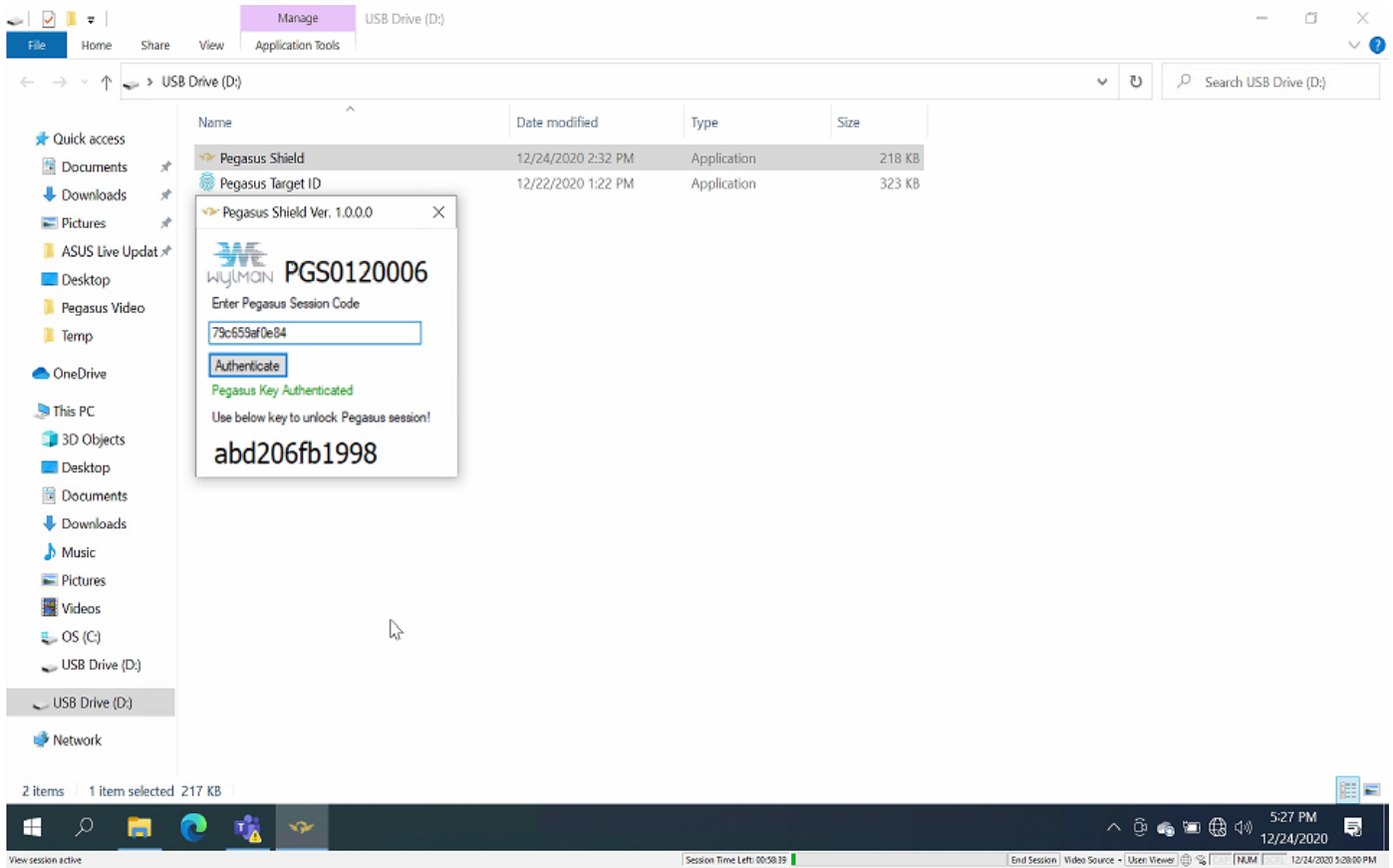
7. The local user enters the PEGASUS code provided by the remote user in PEGASUS Shield software, then click "Authenticate".
8. If the code is authenticated, PEGASUS Shield will display a the PEGASUS Shield Code.
9. If not authenticated, try again, you may want to wait for a new session code to be generated.

 If after many trials the code could not be authenticated, please contact WYLMAN for support.

7. The local user to provide the remote user with the PEGASUS Shield code
8. The Remote user to enter the PEGASUS Shield code into PEGASUS authentication window and click authenticate.
9. If authenticated the view session will start.
10. If not authenticated, try again.

 If after many trials the code could not be authenticated, please contact WYLMAN for support.

Now control session is active and the remote user can see the display of the target machine



The status bar at the bottom of the screen has some useful indications and controls for the remote user

- Session Type and status

View session active

- Session remaining time or duration(if open session was configured in the options)

Session Time Left: 00:58:39

- Time and Date

12/24/2020 5:28:00 PM

- Keyboard locks

CAP NUM SCRL

- Network and Wi-Fi Status



When mouse is hovering over either icon the respective status will be shown on the left side of the status bar

Connected to the Internet

- Logged in User

User: Viewer

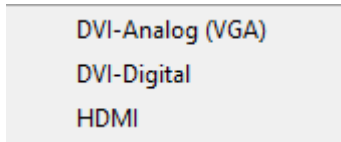
- Video Source

Video Source ▾

Remote user may click here to select the video source if the target machine desktop was not displayed.

Changing video source may not work correctly from the first time and restarting the session and/or PEGASUS may be required. PEGASUS remembers the last video source that was used, so it is advised that the local user would adjust this option before inviting a remote user for a session.

When clicked the below list will be displayed for the remote user to select the correct video source.



- End Session

End Session

Remote user may click here to end the view session, a confirmation will be required.

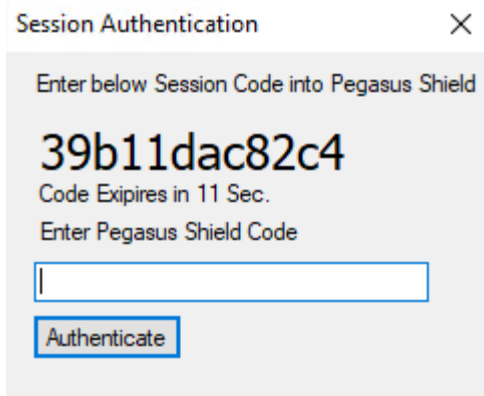
10.5 Control Session

Control session allows the remote user to have control of the desktop of the target machine.


This procedure assumes PEGASUS is activated and PEGASUS Shield software has been downloaded and copied to the Shield USB drive.


To start a control session, PEGASUS must be connected to internet or LAN (LAN will only allow Microsoft Remote Desktop Connection), powered up and connected to target machine, then follow the procedure below:


1. Remote user to gain access to PEGASUS using the credentials for either Microsoft Remote Desktop or TeamViewer
2. Remote user to login as Controller
3. The status bar will show the logged in user as Controller
4. Remote user go to Session -> Start Session
5. Session Authentication screen will popup




6. The displayed code should be given by the remote user to the local user by preferred means. Keep in mind that the authentication window is only 60 seconds


 The session authentication window is 60 seconds in which the PEGASUS code must be transferred to Shield, then Shield code transferred to PEGASUS. So the advised means of communication between local user and remote user is a phone call.

 To get the maximum of 60 seconds window wait for the current code to expire and a new code is shown then start the authentication process.


 The local user should have PEGASUS Shield USB plugged in the target machine and Shield software running and ready to authenticate the PEGASUS code.

 PEGASUS and target machine times must be synchronized for the authentication process to work. Refer to "**System Time (Section 9.4)**" section for details.

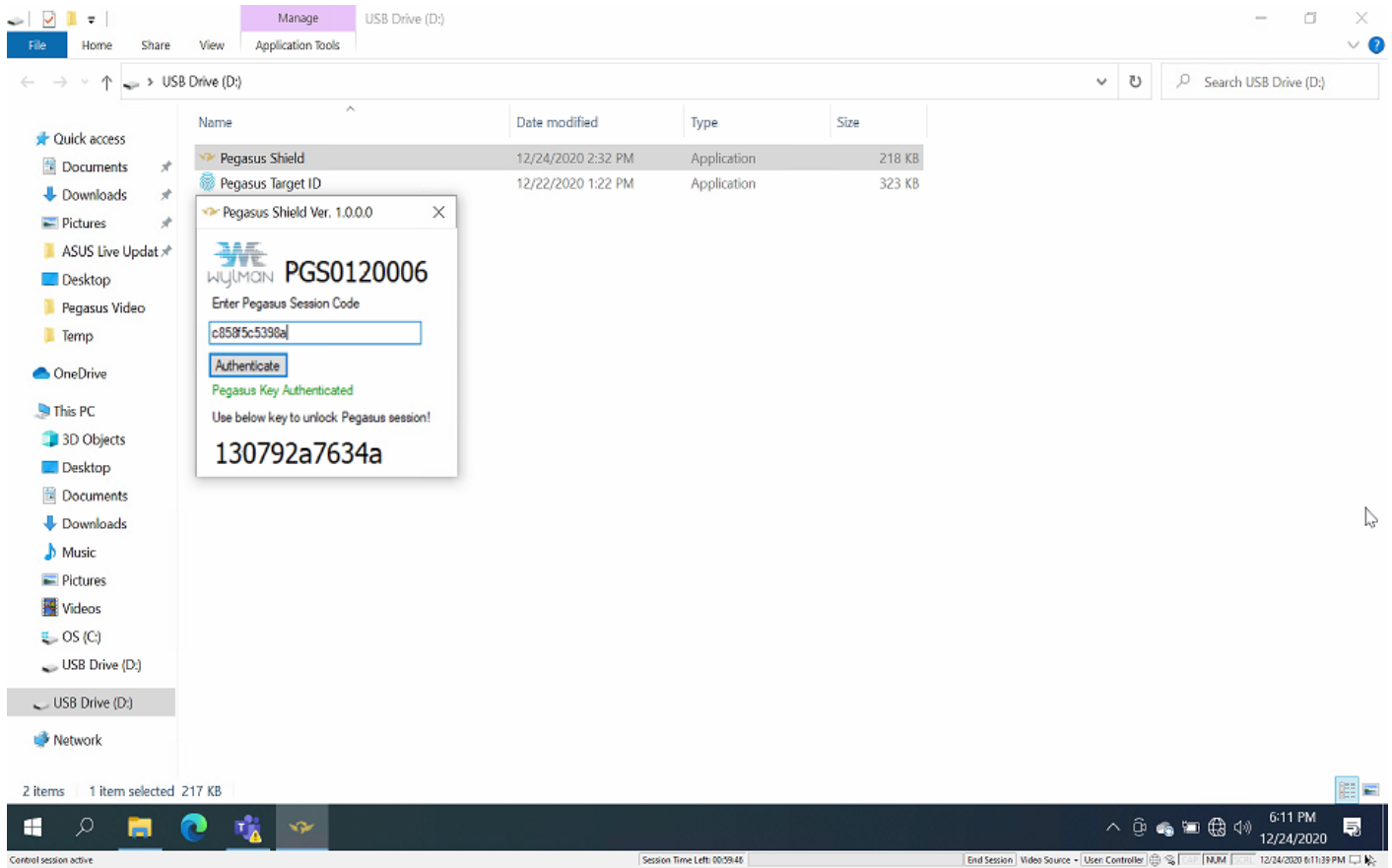
7. The local user enters the PEGASUS code provided by the remote user in PEGASUS Shield software, then click "Authenticate".
8. If the code is authenticated, PEGASUS Shield will display a the PEGASUS Shield Code.
9. If not authenticated, try again, you may want to wait for a new session code to be generated.

 If after many trials the code could not be authenticated, please contact WYLMAN for support.

7. The local user to provide the remote user with the PEGASUS Shield code
8. The Remote user to enter the PEGASUS Shield code into PEGASUS authentication window and click authenticate.
9. If authenticated the control session will start.
10. If not authenticated, try again.

 If after many trials the code could not be authenticated, please contact WYLMAN for support.

Now control session is active and the remote user can see the display of the target machine and after three seconds will gain control of the keyboard and mouse of the target machine



The status bar at the bottom of the screen has some useful indications and controls for the remote user

- Session Type and status

Control session active

- Session remaining time or duration(if open session was configured in the options)

Session Time Left: 00:58:39

- Time and Date

12/24/2020 5:28:00 PM

- Keyboard locks

CAP NUM SCRL

- Network and Wi-Fi Status



When mouse is hovering over either icon the respective status will be shown on the left side of the status bar

Connected to the Internet


- Logged in User

User: Controller

- Video Source

Video Source ▾

Remote user may click here to select the video source if the target machine desktop was not displayed.

 Changing video source may not work correctly from the first time and restarting the session and/or PEGASUS may be required. PEGASUS remembers the last video source that was used, so it is advised that the local user would adjust this option before inviting a remote user for a session.

When clicked the below list will be displayed for the remote user to select the correct video source.

- DVI-Analog (VGA)
- DVI-Digital
- HDMI

- End Session

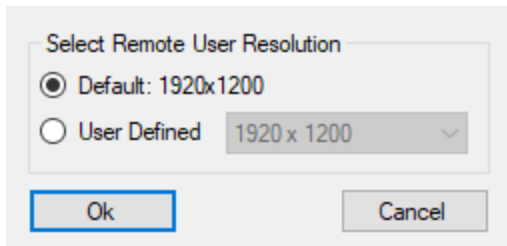
End Session

Remote user may click here to end the view session, a confirmation will be required.

- Screen scaling



If the remote user noticed that the target machine mouse pointer does not completely coincide on the pointer of the remote user computer, then scaling must be adjusted. Remote user first needs to find out the resolution of the display he is using to access PEGASUS. Then click on screen scaling, the below will popup




Select User Defined, then pick the resolution that matches the remote user computer resolution, than click ok. Now the two pointers should coincide.

- Pointer View



By default PEGASUS shows both the remote user pointer and the pointer of the target machine, this may bother some users. To only show the target machine pointer click on this button to hide the remote user pointer.

 It is advised to keep both pointers visible as it makes it easier to control the mouse if there are a video delay due to network connect speed.

11 Index

Activating/Updating PEGASUS Shield, 19-21
Activation, 13-17
Assigning PEGASUS Target, 12-13
Auto Logout and Shutdown, 27
Auto Updates, 36-37
Changing Passwords, 23-24
Check for Updates, 40-43
Compliance Statements, 5
Connecting PEGASUS to Target Machine, 44
Control Session, 49-52
Deactivation, 17-19
Demo Sessions, 44
Important Notes, 11
Included Accessories, 8-10
IP Watchdog, 30-31
License Manager, 39-40
Logging In, 22-23
Network Adapters, 32-34
PEGASUS Overview, 6-7
PEGASUS Password, 36
Remote Access, 29-30
Resetting Passwords, 24-25
Safety Instructions, 4
Security, 31-32
Session Invitation, 45-46
Session Invitations, 27-29
Session Time, 26-27
Shield Manager, 38-39
System Time, 37-38
Users Privileges, 22
View Session, 46-49
Wi-Fi Access Points, 34-36
WYLMAN PEGASUS, 3