SEATTLELAB
COMMUNICATION & SECURITY SOLUTIONS

SLNET SECURE

SLNet Secure

Installation, Configuration, Administration, and User Guide

Version 9.5.0.0

High Performance SSH Server for Windows

Contents

Introduction **1**
Full-Featured SSH Service 1
SSH User Security 1
Hand Held RF Device Support 1
SAP Console compatibility 1

Architecture **2**

SLNet Secure System Requirements **3**
SLNet Secure pre-requisites 3

Upgrading from a Previous Release **4**

SLNet Secure Features **5**
High Performance 5
Access to Windows's Common Command Shell 5
Direct Access to Custom Applications 5
Security 5
Secure Logon 5
Terminal Emulation 5
Logging 5
Remote Administration 5

What's New in the SLNet Secure Release **6**
Licensing 6
Windows 2016 and 2019 support 6
64 bit Console Support 6
Improved Performance and Reliability 6
Unicode and UTF-8 support 6
User Status 6
Event Logging 6
Multi-layer configuration – user, network 6
Security 6

SLNet and Windows Security **7**

Device Security **7**
Handheld device security 7
Secure Shell (SSH) 7

Installation of SLNet Secure **8**

Configuration **9**
SLNet Secure Cfg 9
Service tab 10
Stop, Start and Restart SLNet Secure 10
Alternative Ways to Start and Stop SLNet Secure 10

License Tab 11
Get a License Key 11
Add a License Key 12
Connected Users Tab 14
Default User Tab 15
AutoLogonIPv4 Tab 16
Add a single IP address and User ID 16
Add IP addresses using a mask 17
Add a range of IP addresses and User ID 18
Edit an auto logon entry 19
Delete an auto logon entry 20
AutoLogonIPv6 Tab 21
Add a single IP address and User ID 21
Add a range of IP addresses and User ID 22
Edit an auto logon entry 23
Delete an auto logon entry 24
Advanced Config Tab 25
sshd_config file 26
SLNet Secure logging: 26
Default Programs Tab 27
Create a new user profile 28
Edit user profile 29
Delete user profile 29
About Tab 30

Logging on to SLNet Secure 31
How to connect using the OpenSSH client 32
How to connect using PuTTy 33
Exiting an SLNet Secure session 34

SLNet Secure Entries in Windows Event Viewer 35
Logging Message examples 35

Appendix A. Troubleshooting 36
A.1: Before You Contact SLNet Technical Support 36
A1.1: SeattleLab Professional Services 36
A1.2: Contacting SLNet Specialists 36

Published by:
SeattleLab

www.SeattleLab.com

© 2020 SeattleLab Limited. All Rights Reserved.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of SeattleLab.

SLNet®, SLNetRF®, and SeattleLab® are trademarks of SeattleLab. Other brands or products are the trademarks or registered trademarks of their respective holders and should be treated as such.

Any errors, corrections, suggestions, or omissions should be sent to support@seattlelab.com.

SLNET Secure V2.0

This page intentionally left blank.

Introduction

SLNet Secure follows in the success of our SLNet Telnet product. It is similarly efficient and flexible whilst incorporating the modern SSH standard. The architecture, performance and features are robust enough for large enterprises, yet affordable and flexible enough for any small business.

SLNet Secure server runs on any Windows 2016, 2019 or 2022 server. SLNet Secure enables an unlimited number of users to work invisibly and simultaneously on any Windows server without interfering with one another or the server console user. Additionally, SLNet Secure optimizes the SSH protocol between Radio Frequency (RF) devices and Microsoft Windows servers.

Full-Featured SSH Service

- Allows **unlimited concurrent connections** for any device running terminal emulation, including RF devices.
- Users can be placed **directly** into custom applications or access the Common Command Shell.
- Use **existing** character-based and DOS/Console applications to run multi-users without modification.
- Written in open Internet standards to work with any SSH client. **No proprietary** client software is required.
- Remote users can work invisibly and simultaneously on the same server without interfering with the server console user.

SSH User Security

- Completely **preserves** Windows security protocols.
- Requires user authentication by the **Windows security** authority.
- Gives administrators the ability to configure SLNet **permissions** on a user-by-user basis.
- Allows **restriction of** logon rights to specific groups.
- Gives users the same permissions as if they were working at the console.
- **Firewall** can be used to **restrict** logon rights to specific IP addresses or address ranges.
- Provides end to end **encryption**

Hand Held RF Device Support

- SLNet allows **unlimited, concurrent RF devices** connections.
- Ready for real-time use with any wireless radio frequency (RF) device that supports the SSH protocol.
- Users can access Windows 2016, 2019 or 2022 hosts from a device.
- Support small screen sizes.
- **No extensive application rewrites** or the investment of learning new and cumbersome wireless APIs.

SLNet Secure adds an extra level of security by creating an SSH Tunnel between the RF devices and the SLNet Server, details of which are found within this document.

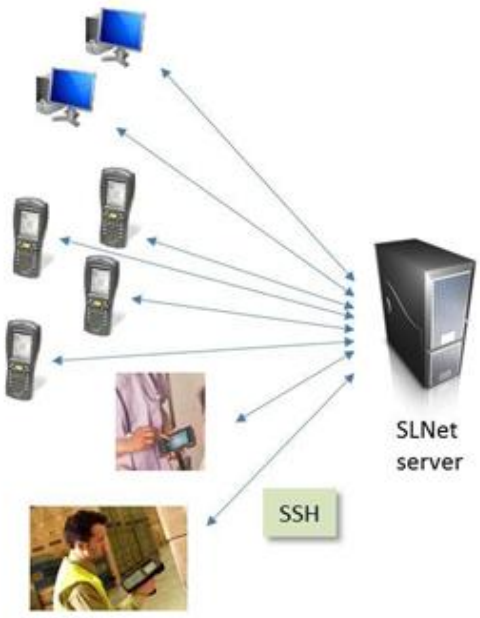
SAP Console compatibility

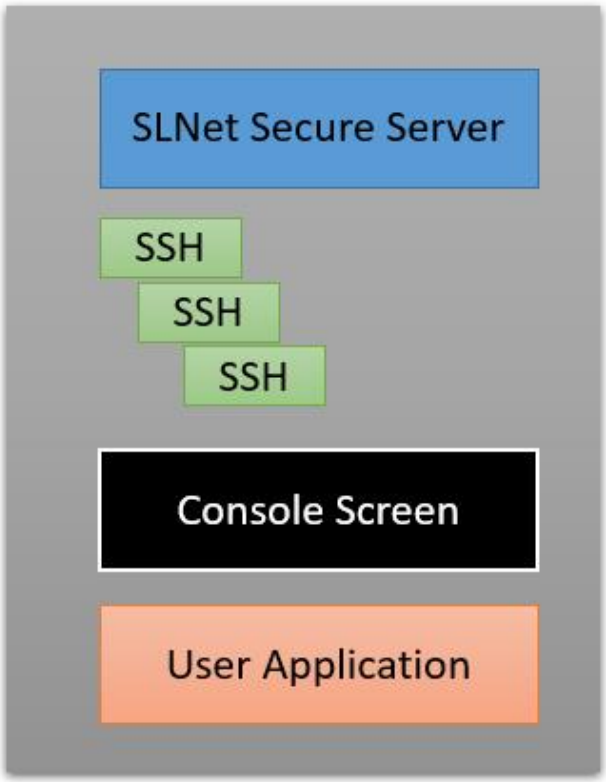
- SLNet is the standard for interfacing to the SAP Console from RF devices. It is in use at major organizations worldwide. They chose SLNet because of its outstanding performance and reliability. It installs in a few minutes and delivers a powerful solution for organizations from a few people to thousands.

.

Architecture

The SLNet Secure server handles a large number of connections (thousands) by handling all connections, terminal emulation and character translation through an individual console for each user that connects up to the user's application through an MS-DOS prompt.





SLNet Secure System Requirements

SLNet Secure supports Windows Server 2016, 2019 and 2022.

The SLNet service itself uses only a minimal amount of system resources, requiring eight megabytes of disk space in your root system directory (the directory where Windows is installed on your system) and 4 megabytes of system RAM for the initial connection.

SLNet Secure pre-requisites

The following are pre-requisites for installation of SLNet Secure:

1) Ensure .Net Framework is installed. This is included in the installation script but ideally you should ensure that Version 4.8 or higher is installed

2) Check if the Windows operating system has its own SSH server. If there is an Open SSH service, ensure it is disabled

.

Upgrading from a Previous Release

If you are a previous SLNet user of 2.6, 4.1, 5.x or 6.x versions, SLNet Secure allows a forward migration path. SLNet Secure implements a different protocol to previous SLNet versions. This means you can migrate RF terminals to the SSH protocol, whilst leaving other devices running as they did previously on Telnet.

You can install SLNet Secure onto the same server as previous versions of SLNet if your licensing agreement permits this and both versions will run in parallel. SLNet Secure is installed with a 14 day trial license, this provides time to test configurations and get things working as you want them. Once this license has expired you will need to request a permanent SLNet Secure license from sales@seattlelab.com

Instructions for requesting a license can be found on page 11.

SLNet Secure Features

High Performance

SLNet communicates via Winsock Sockets to the terminals and via Pipes to SLCon and the Windows Console Applications. To minimize impact on the CPU resources, the SLNet programs are heavily multi-threaded and asynchronous.

Access to Windows's Common Command Shell

Users who SSH into SLNet Secure can have full access to Windows' Common Command Shell. SLNet is completely configurable by the administrator, who can choose to disable access to the Command Shell on a user-by-user basis.

Direct Access to Custom Applications

SLNet Secure offers you the power to define default custom applications for users as soon as they log in.

Security

Users run in their own appropriate security context, with all their own permissions in place, just as if they had logged in from the main console. This completely preserves all Windows's C2 security features.

Secure Logon

SLNet Secure ensures encryption of usernames and passwords for secure logon over the network.

Terminal Emulation

SLNet provides ANSI terminal sequences (compatible with the VT-100 and VT-220) for cursor positioning and formatted screen handling. It supports colors, UTF-8 characters, Unicode characters and custom key sequences.

Logging

SLNet can insert a record in the Windows event log every time a user connects or disconnects along with a record of what process the user executed and the resulting data and screens from that process.

Remote Administration

SLNet can be administered locally or remotely.

.

What's New in the SLNet Secure Release

Licensing

For security purposes SLNet Secure is licensed to specific servers. A license key tied to the server ensures you can track your SLNet licenses and prevent unauthorized uses. When SLNet Secure is installed on a target server, it activates temporarily and provides a license request file that you email to the SeattleLab license group. A license key file is generated and sent back to you.

Windows 2016, 2019 and 2022 support

SLNet Secure fully supports Windows 2016, 2019 and 2022 servers.

64 bit Console Support

SLNet Secure fully supports 64 bit Console applications such as SAPConsole 7.3.

Improved Performance and Reliability

SLNet Secure can handle thousands of user connections with modest requirements. SSH sessions tend to be more robust that the equivalent Telnet session.

Unicode and UTF-8 support

SLNet Secure has full support for international languages – single and double byte character sets. You can set the font and code page to meet any need.

User Status

The SLNet Secure console shows all connected users and a list of remote IP Addresses.

Event Logging

SLNet logging has been simplified so you can choose to log Event Viewer or file. It is now easy to switch between full debug or critical level messages.

Multi-layer configuration – user, network

SLNet offers a powerful way to manage customizations by allowing to users authenticate using their source address network or IP Address. This allows for simpler automation of RF users. Each RF users can also be customized to ensure a particular default profile.

Security

SLNet can lock down terminals so they can only reach specific applications and be prevented from getting to a command prompt.

SLNet and Windows Security

SLNet abides by all Windows security features. It does not alter nor change any security settings or privilege levels set by normal Windows mechanisms.

When a SSH user logs into your system via SLNet Secure, he or she must be a valid user that you or another administrator created using the Windows User Manager or Active Directory Manager. SLNet sets that user's process to run in the security context appropriate to that user. The user then has exactly the same privileges he or she would have on your machine if they sat down in front of it and logged in on the console by pressing the `CTRL ALT DELETE` keys.

Windows allows you to grant or withhold privileges on a user-by-user basis to every object on the system. Using Windows Explorer, for example, you may choose which individual users can have access to any given file you create. SLNet abides by these exact same access restrictions. It does not and cannot alter any privileges set by Windows.

Device Security

Handheld device security

The wireless data transmitted between the RF Guns and the Base Station is usually encrypted at the network level using WEP, WPA, WPA2, etc.

In the past this was only way to secure Telnet traffic passing through the network. Now with SLNet Secure the connection can be protected using the SSH protocol.

Secure Shell (SSH)

A Secure Shell (SSH) provides an encrypted link between the RF device and the SLNet Secure Server. This ensures privacy end to end, regardless of the network architecture. To set up an SSH, you configure an SSH client to connect to the standard port 22 on the SLNet machine. Once the SSH session has been established, the user experience will be identical that of a legacy Telnet session.

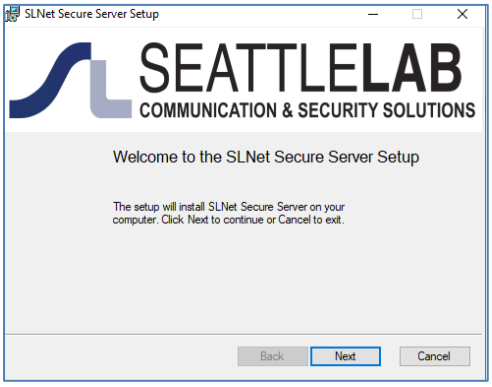


Installation of SLNet Secure

Before installing SLNet Secure, you must first log on as a member of the Administrator's user group.

Download the SLNet Secure installation file from the SeattleLab web site or obtain from a reseller and put it on the local drive of the Windows server.

Double click the .msi file to start the installation process.



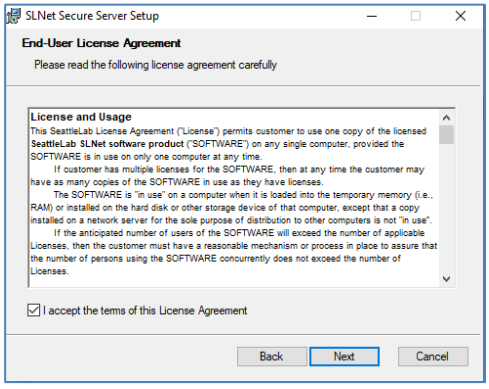
Click ***Next*** to continue.



Read the License Agreement.

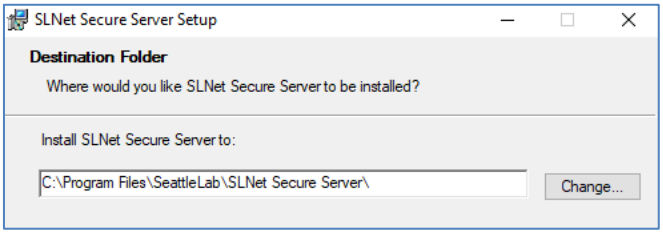
Check "I accept the terms of this license agreement."

Click ***Next*** to continue.



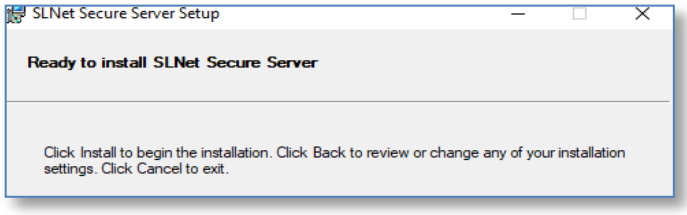
Change the destination folder for the SLNet software if needed. The default installation path is *C:\Program Files\SeattleLab\SLNet Secure Server*

Click ***Next*** to continue.



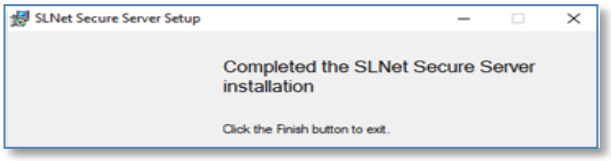
Click ***Install*** to continue.





Installation of SLNet Secure is complete. Click ***Finish***.



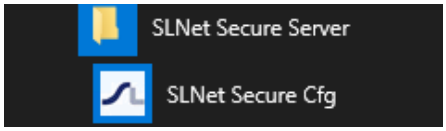


Configuration

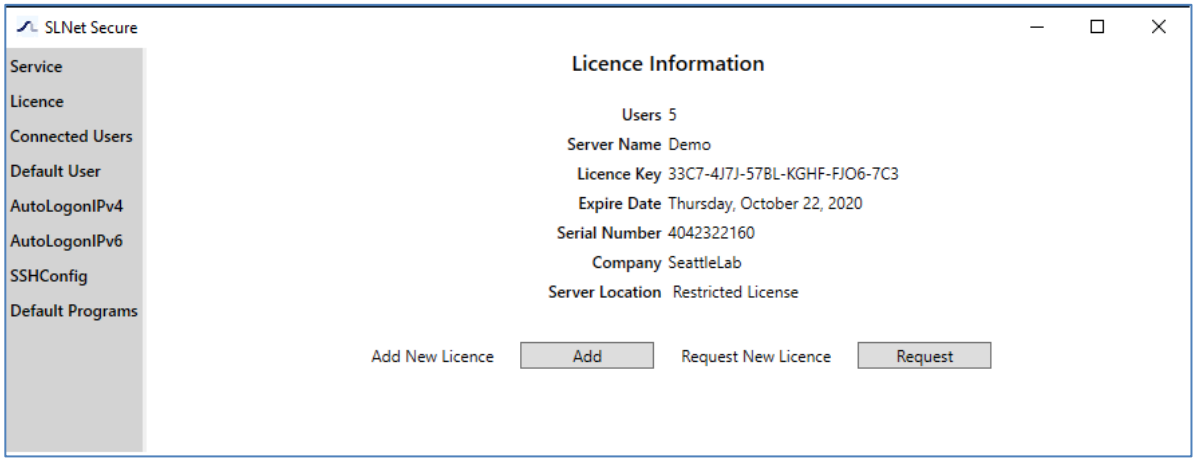
SLNet Secure Cfg

SLNet Secure offers a powerful selection of options for customization of your SSH remote login needs.

Go to Start programs and select ***SLNet Secure Server*** then ***SLNet Secure Cfg***



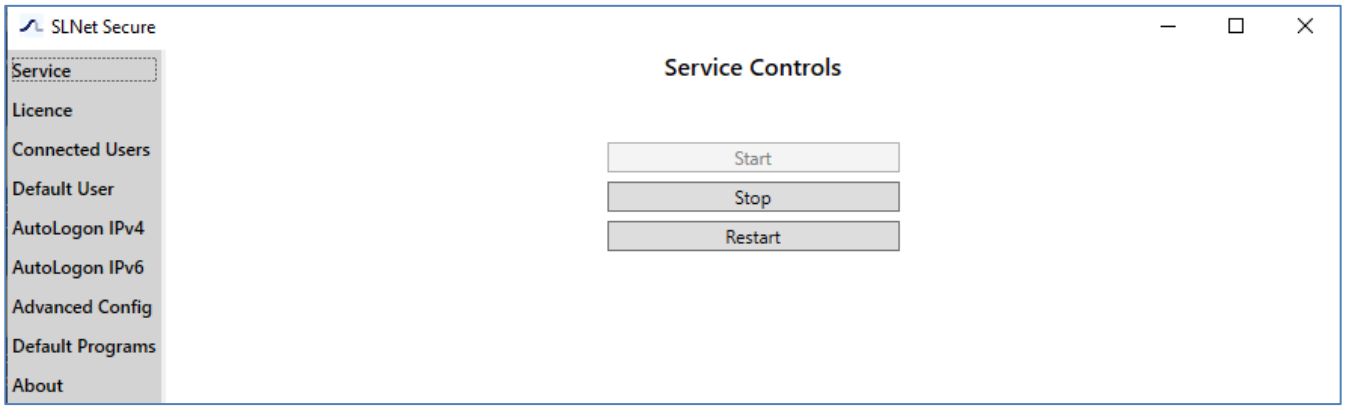
The SLNet Secure configuration panel is displayed.



Until you enter a valid license key, SLNet is in a demonstration mode with a temporary license key that expires.

If you have a License Key, click on [Add] to load your valid SLNet Secure License Key file.

Service tab



Stop, Start and Restart SLNet Secure

*Select **Stop*** to stop the SLNetSecure Server service
Select ***Start*** to start the SLNetSecure Server service
Select ***Restart*** to restart the SLNetSecure Server service

If you stop the SLNetSecure Server service, the service is completely inactivated. It is removed from memory and is no longer listening on the SSH socket. SSH users who attempt to connect to your Windows system will receive a connection refusal message.

Alternative Ways to Start and Stop SLNet Secure

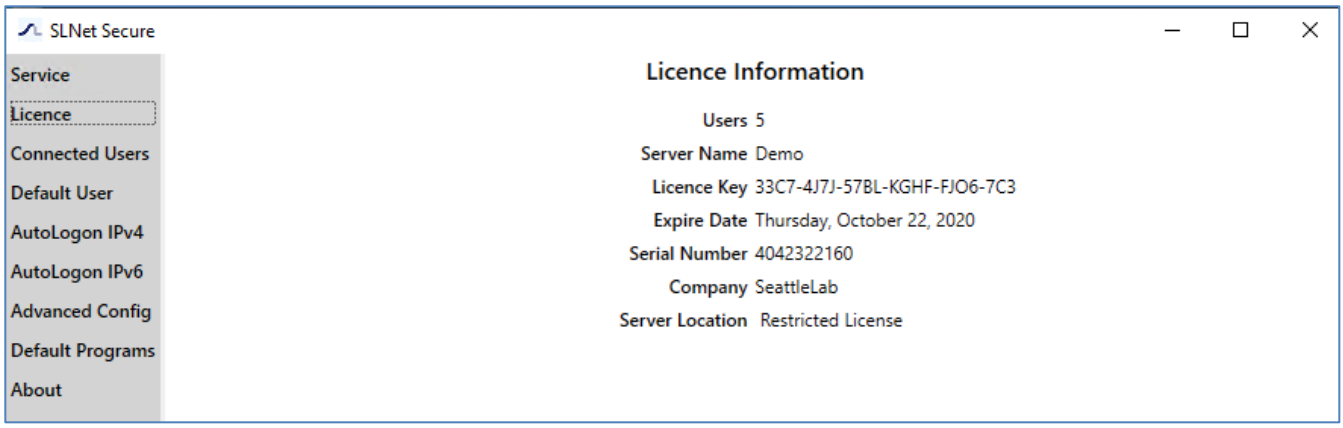
SLNet can also be started or stopped directly from a Windows command prompt that is opened with “Run as Administrator”

```
net start slnetsecure

net stop slnetsecure
```

License Tab

SLNet Secure is licensed by server and the number of concurrent users.
It will install with a temporary license key that expires.



Get a License Key

To request a permanent license key click the ***Request*** button to generate a file to email to the SeattleLab license department. An email will be returned to you with the license key.

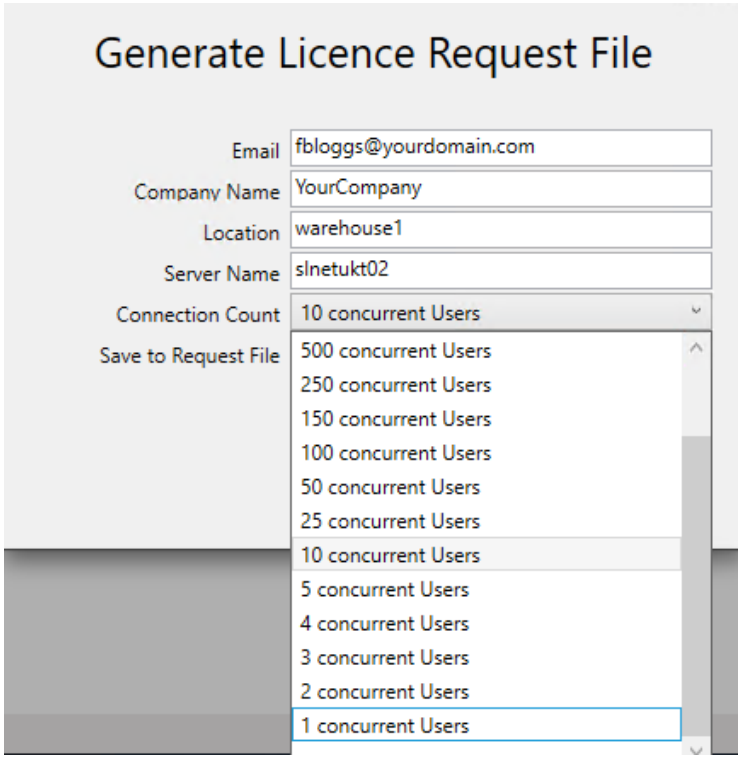
You must pay for your SLNet License first before a license key will be sent to you.

Enter the Email Address that the license key should be sent to. Then enter your company name, server location, server name and desired user count.

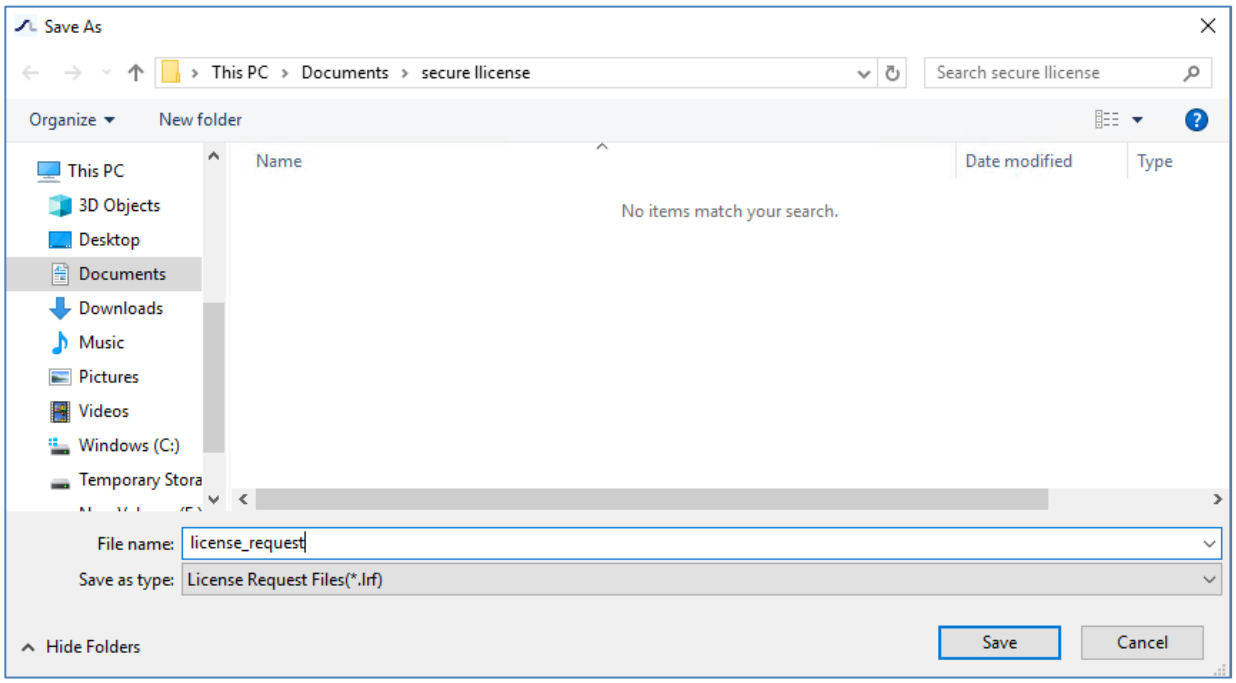
The License Key is based on the **Company Name, Server Location, Server name,** and **User Count**.

The server must use static MAC addressing. If dynamic MAC addressing is used and the MAC address changes the license will not work.

Click ***Save*** to save the license request file on this server.



Enter a name for the file, then select Save to save it to this server

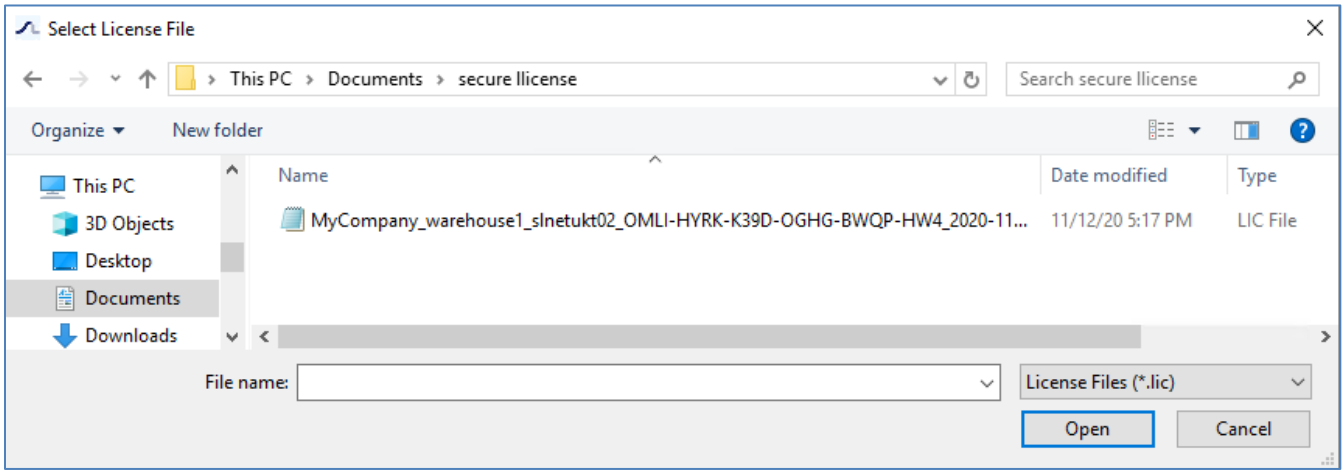


Select ***OK*** to leave the license request screen

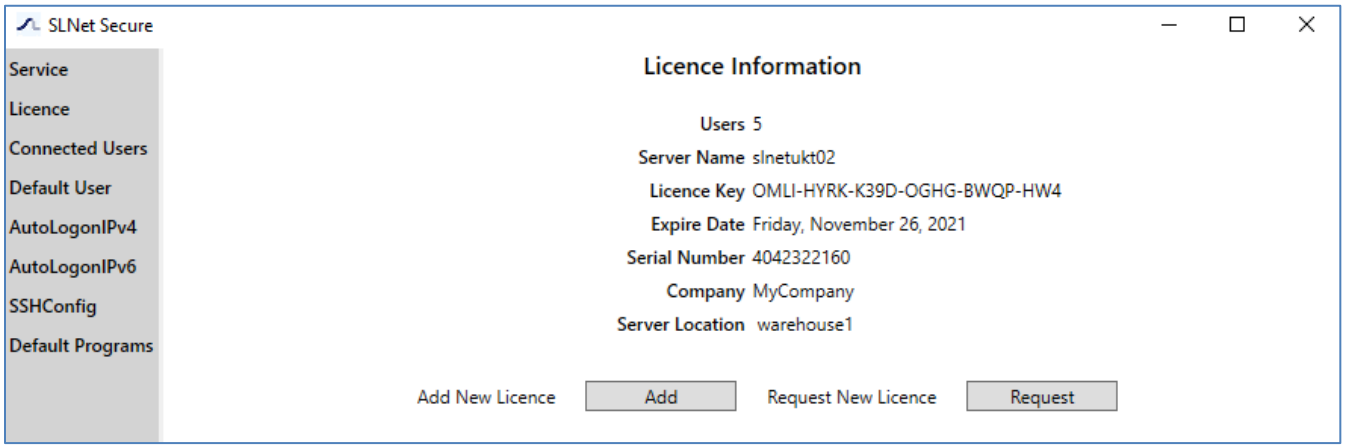
Email the **`.LRF`** file to licensing@seattlelab.com.
You will receive a **`.LIC`** license file in your email within two business days.

Add a License Key

To add your license file into SLNet Secure, click on the ***Add*** button and locate the directory where you saved the license file, then select ***Open***

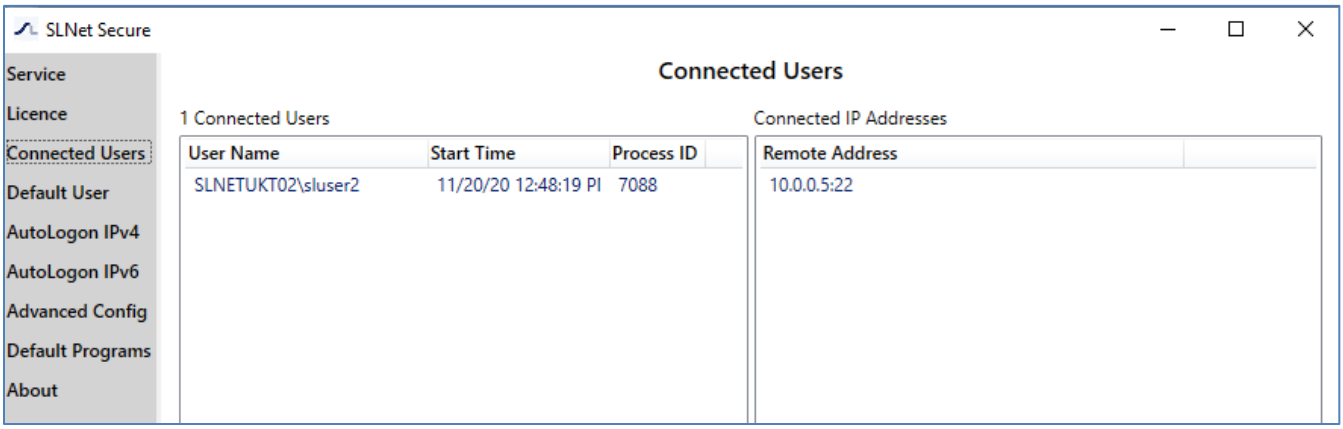


The License tab will be updated with the details of the new license.



Connected Users Tab

The Connected Users tab will monitor which users are connected to your server.



Connected Users section:

The **User Name** column shows the server name\windows user name
The **Start Time** column shows the date and time the user connected
The **Process ID** column shows the windows process ID

Connected IP Addresses section:

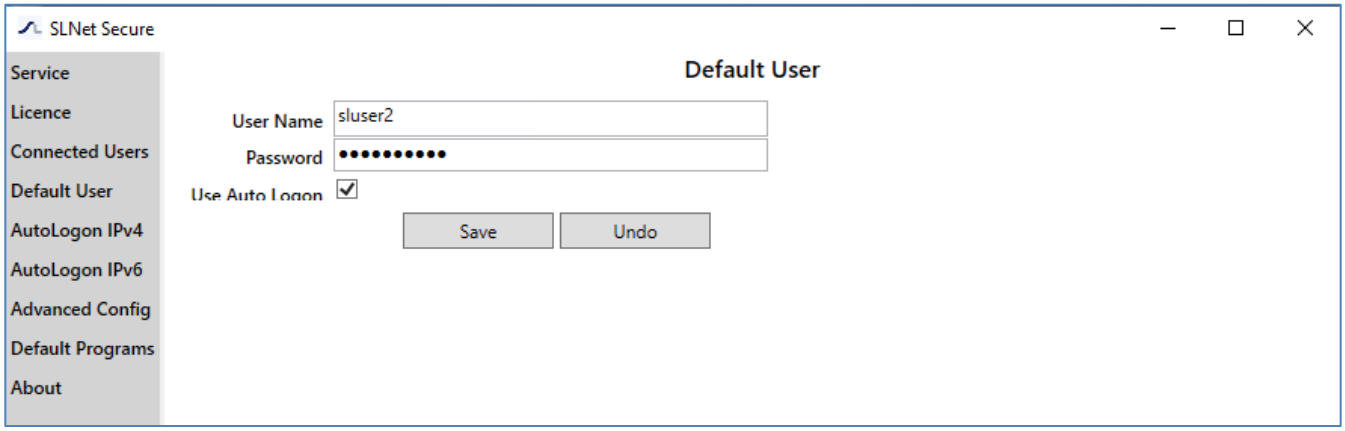
The **Remote Address** column shows the user's IP address and the port connected to.

Default User Tab

If you want all SSH connections to log in with the same Windows user account:

Click the ***Use Auto Logon*** box and enter the Default user name and password. Then select ***Save***. All terminals will be logged on as this Windows user account

The User Name and Password must not be left blank



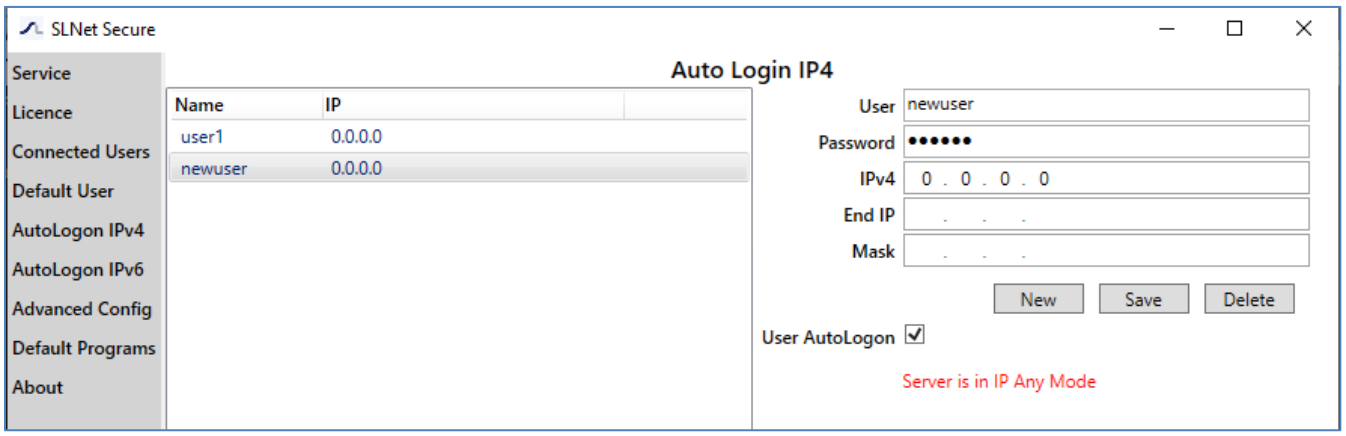
AutoLogonIPv4 Tab

SLNet Secure can automatically logon a user from a device that connects from a specific IP address or range of addresses.

This enables a shared user ID to be used from a single IP address or a secured range of IP addresses.

Add a single IP address and User ID.

Click the ***New*** button



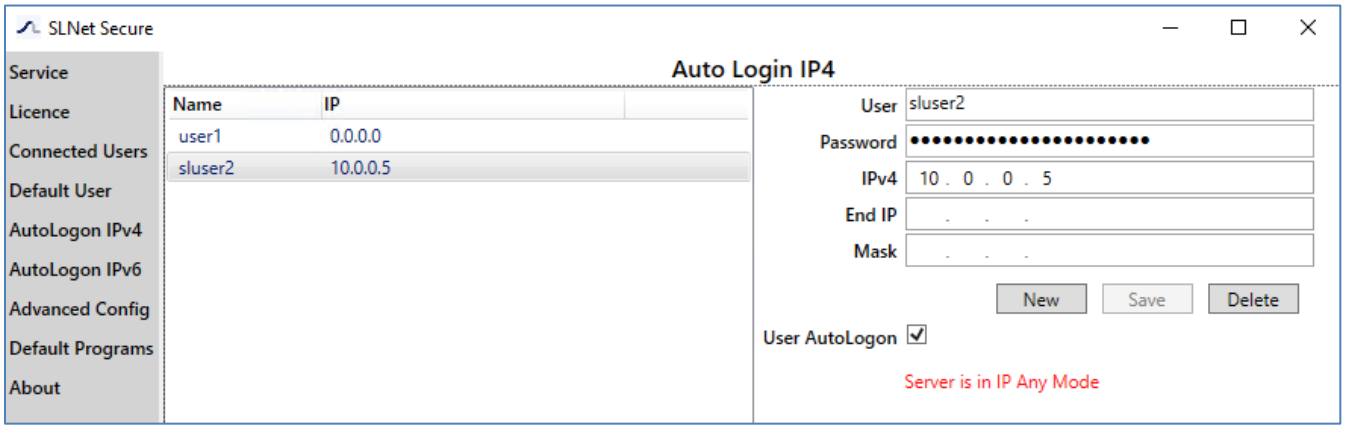
User: Overtype **newuser** with the user name

Password: Enter a password

IP4: Enter IP4 address

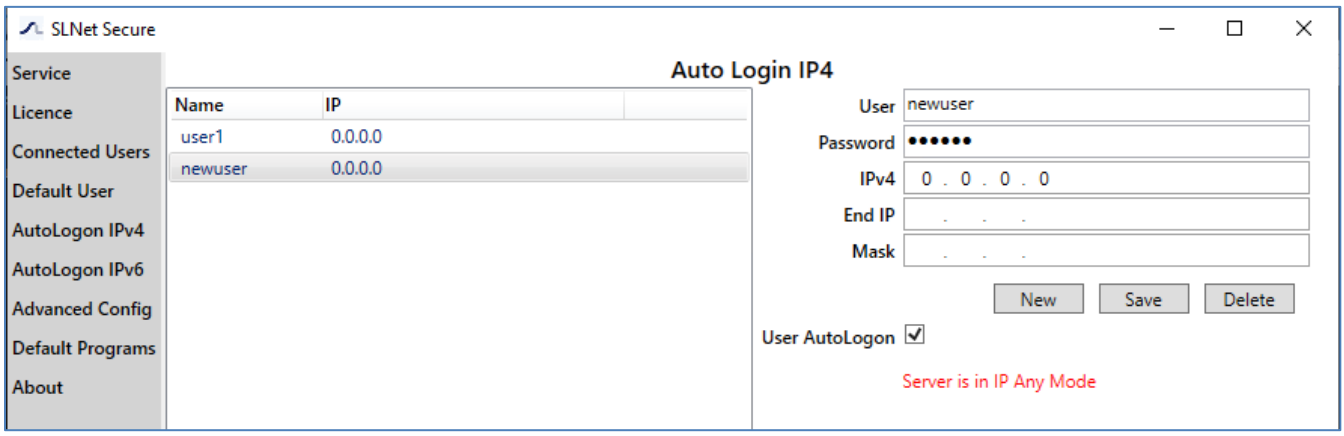
Click the ***Save*** button

Click the ***User Auto Logon*** box if not already enabled



Add IP addresses using a mask

Click the ***New*** button



User:: Overtype **newuser** with the user name

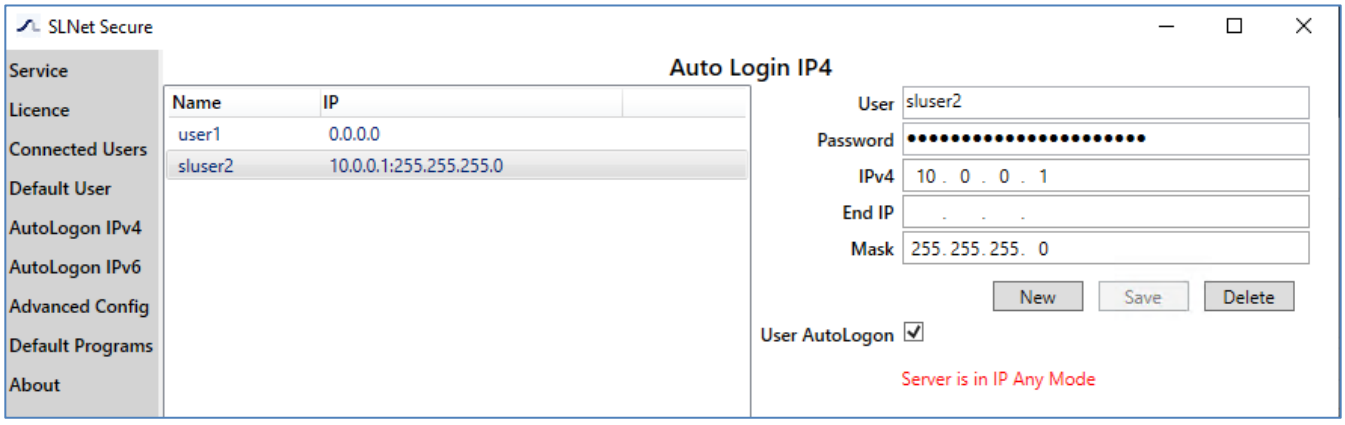
Password: Enter a password

IP4: Enter the starting IP4 address

Mask: Enter subnet mask

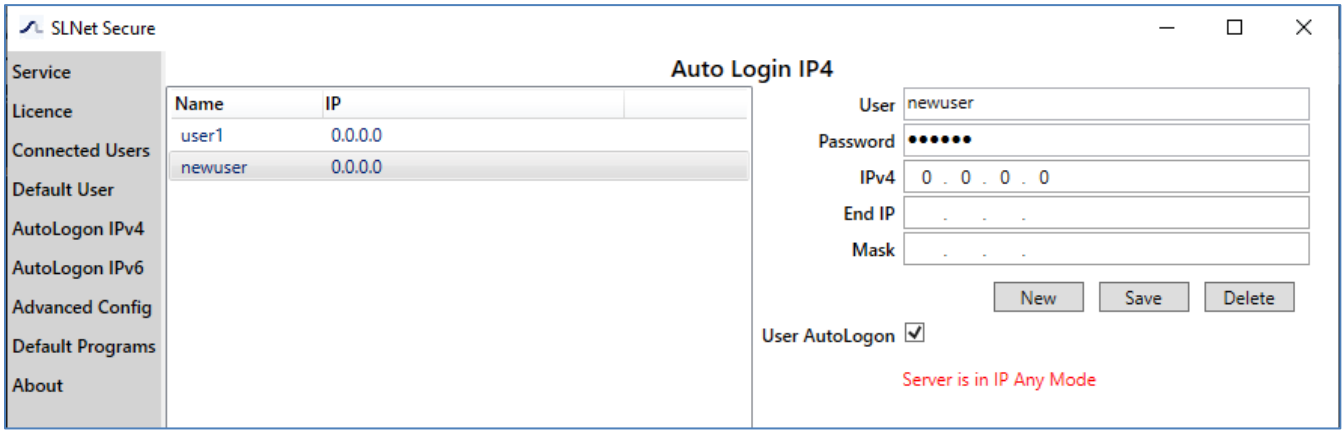
Click the ***Save*** button

Click the ***User Auto Logon*** box if not already enabled



Add a range of IP addresses and User ID

Click the ***New*** button



User:: Overtype **newuser** with the user name

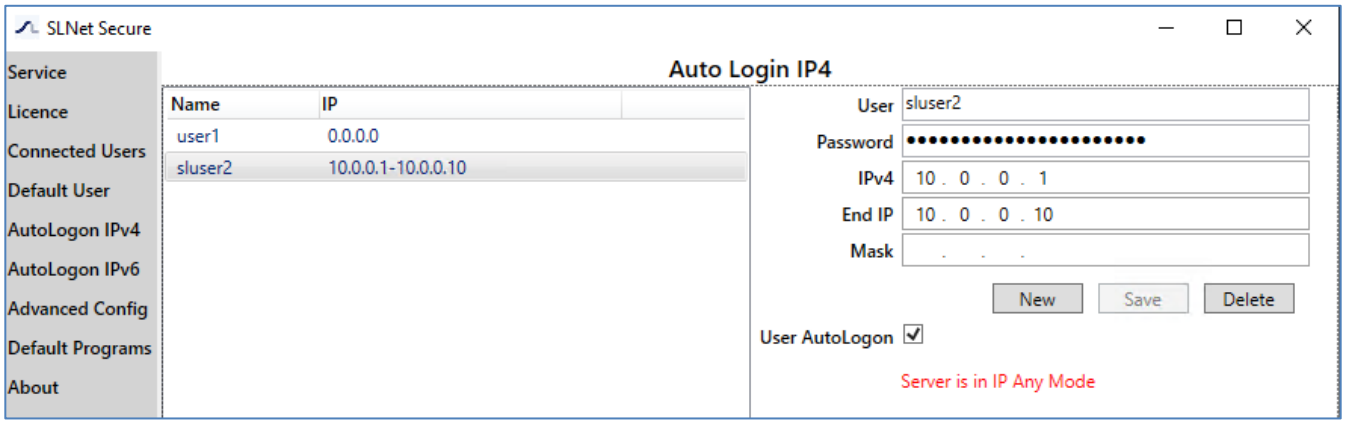
Password: Enter a password

IP4: Enter the starting IP4 address

End IP: Enter the last IP4 address

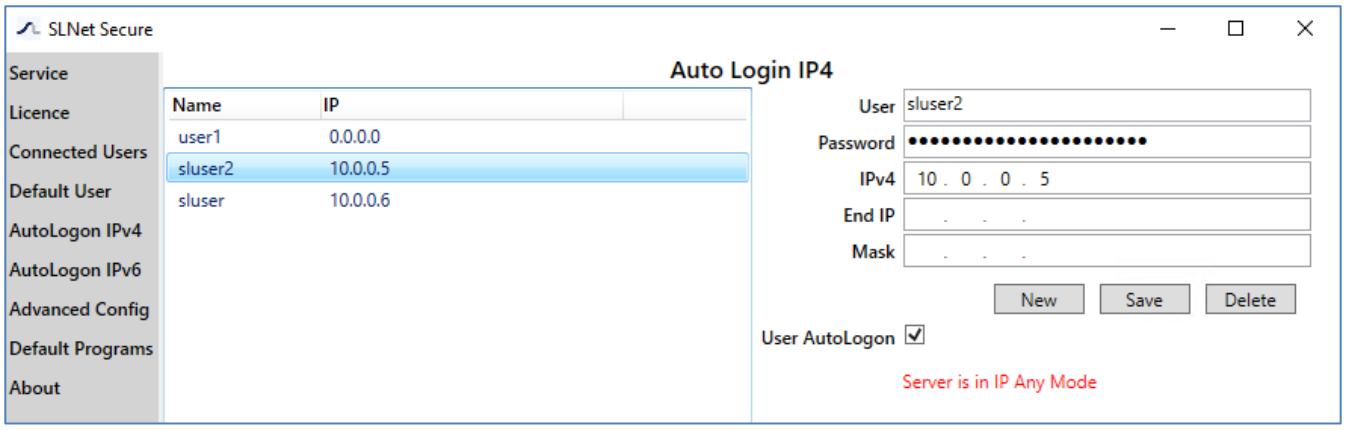
Click the ***Save*** button

Click the ***User Auto Logon*** box if not already enabled

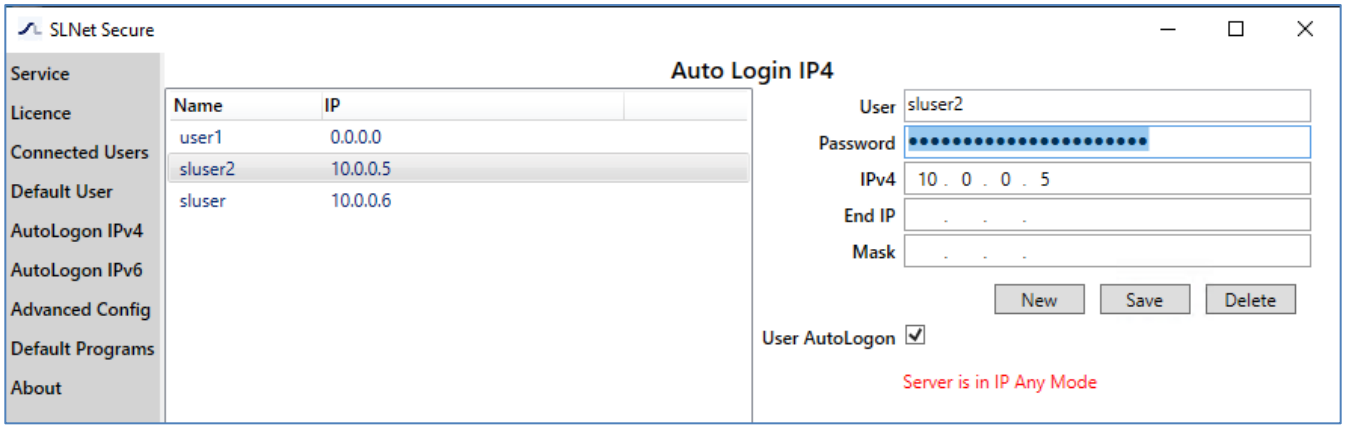


Edit an auto logon entry

Select the entry to edit in the list on the left of the screen



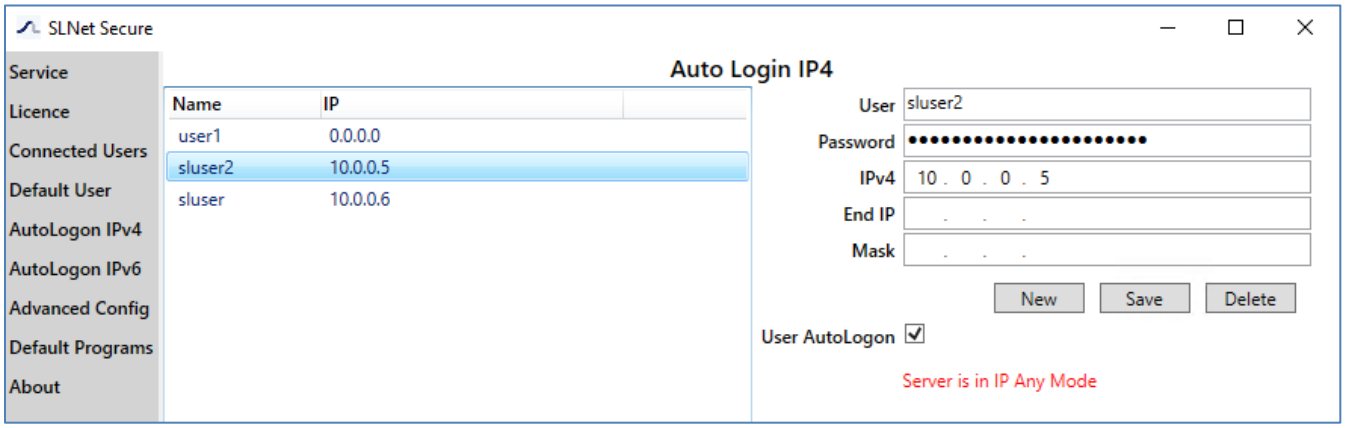
Mark the text to be edited on the right of the screen which will be highlighted blue.



Make any changes the select ***Save***

Delete an auto logon entry

Select the entry to delete in the list on the left of the screen
Click the ***Delete*** button
Select ***Yes*** to confirm



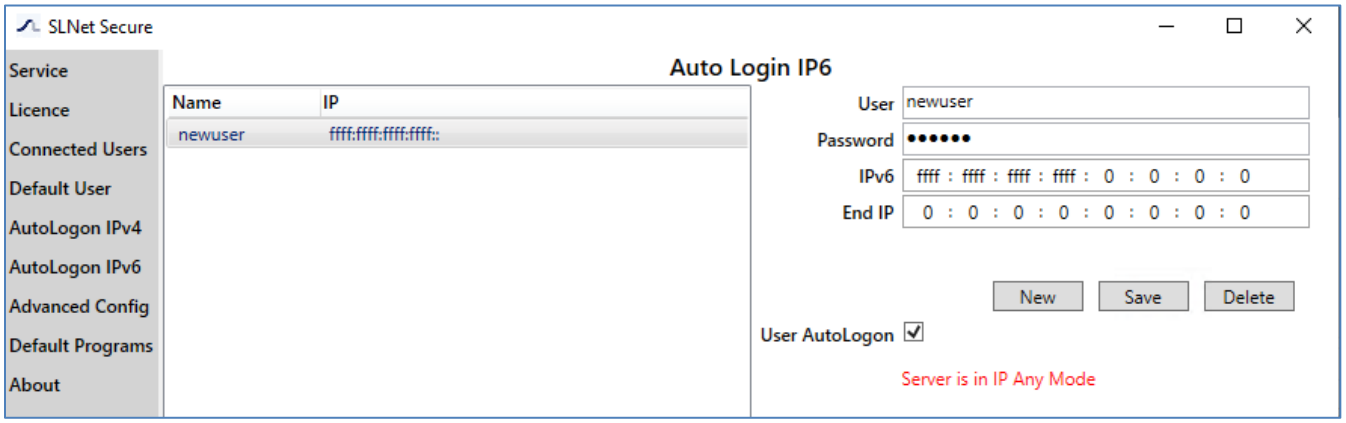
AutoLogonIPv6 Tab

SLNet Secure can automatically logon a user from a device that connects from a specific IP address or range of addresses.

This enables a shared user ID to be used from a single IP address or a secured range of IP addresses.

Add a single IP address and User ID.

Click the ***New*** button



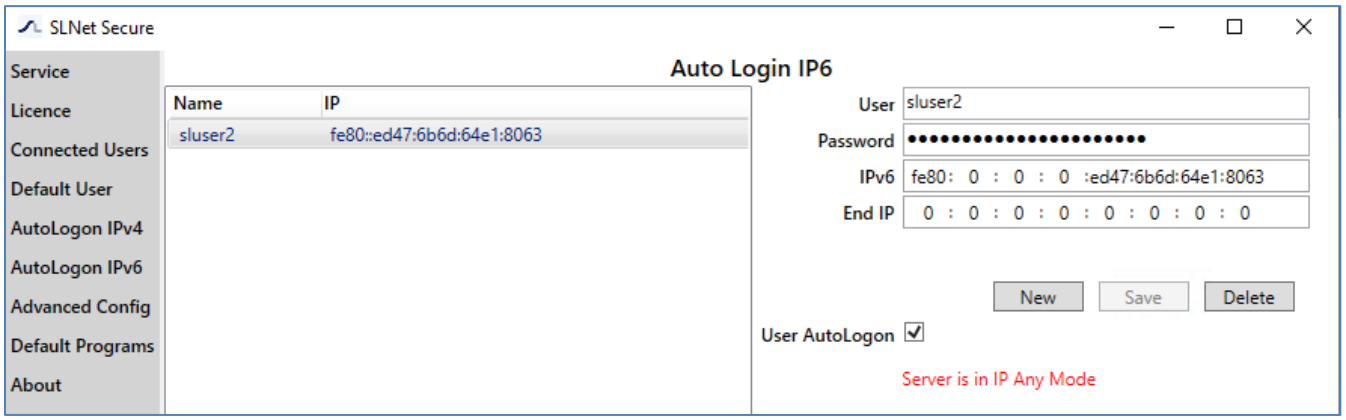
User:: Overtype **newuser** with the user name

Password: Enter a password

IP6: Enter IP6 address

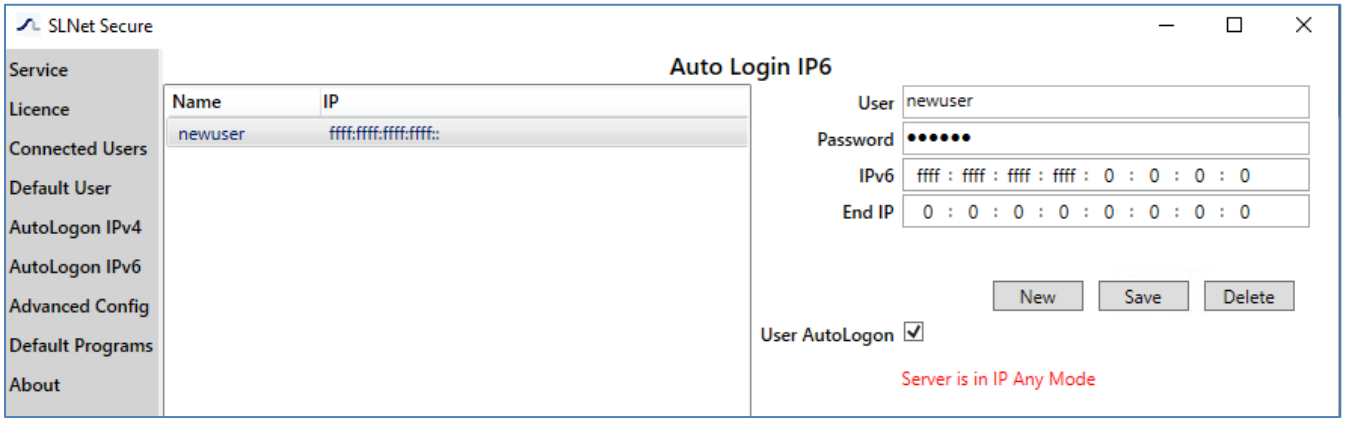
Click the ***Save*** button

Click the ***User Auto Logon*** box if not already enabled



Add a range of IP addresses and User ID

Click the ***New*** button



User: Overtype **newuser** with the user name

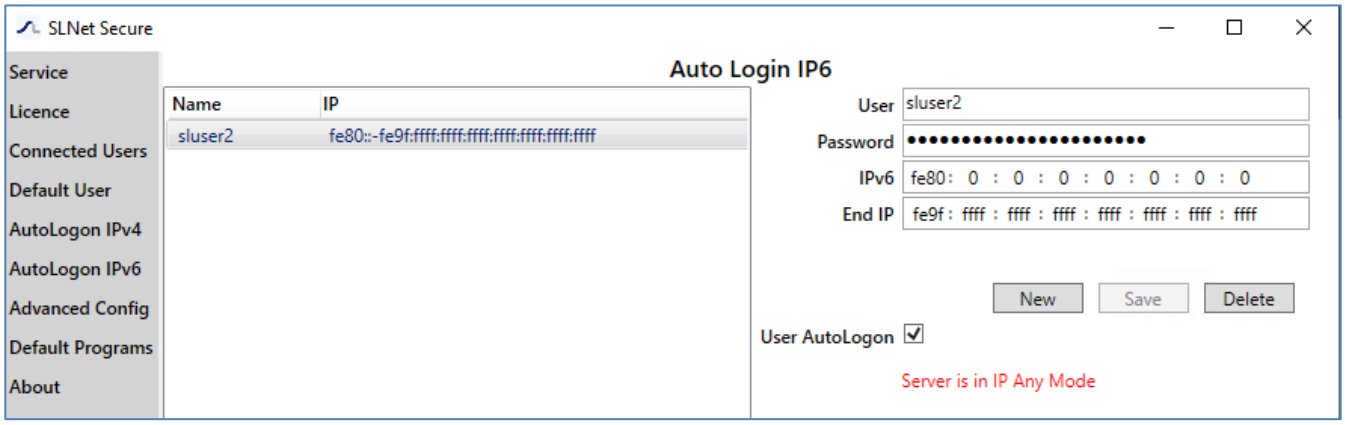
Password: Enter a password

IP6: Enter the starting IP6 address

End IP: Enter the last IP6 address

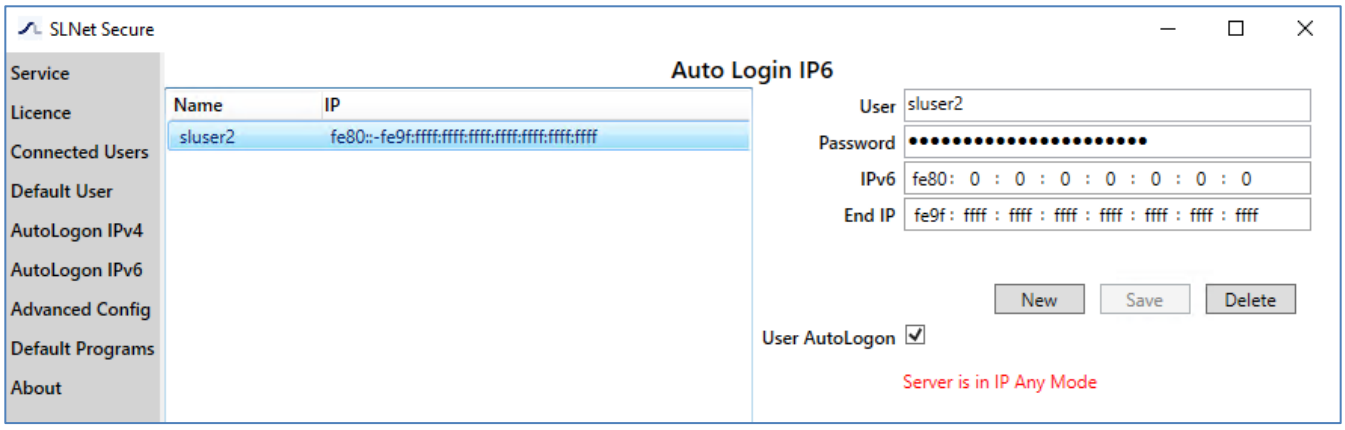
Click the ***Save*** button

Click the ***User Auto Logon*** box if not already enabled

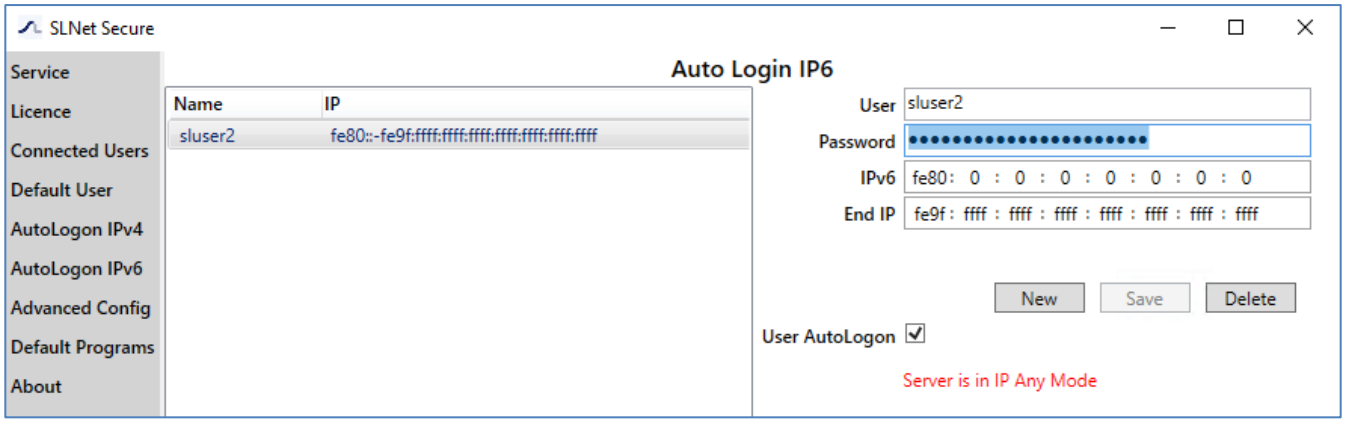


Edit an auto logon entry

Select the entry to edit in the list on the left of the screen



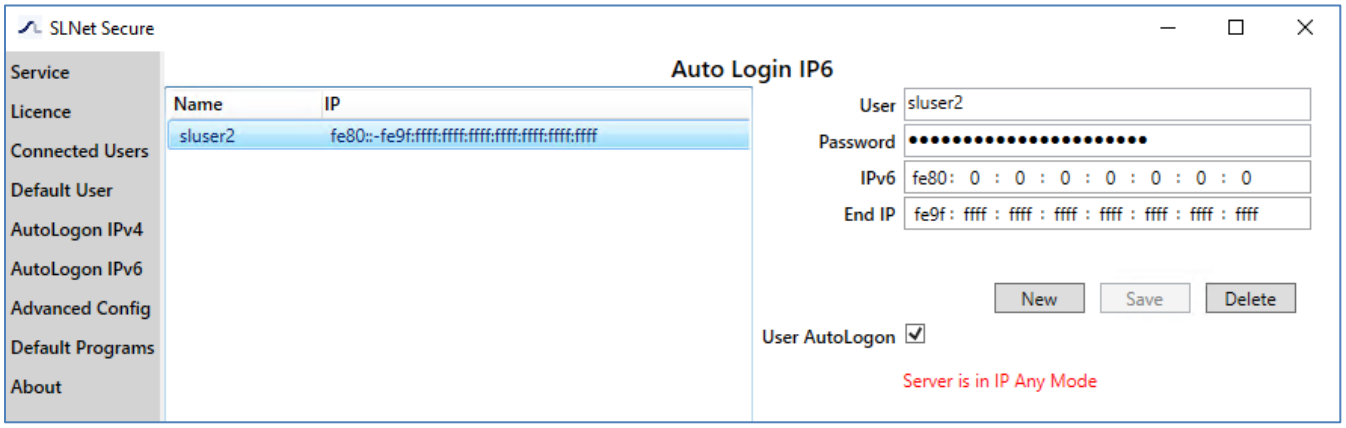
Mark the text to be edited on the right of the screen which will be highlighted blue.



Make any changes then click ***Save***

Delete an auto logon entry

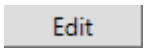
Select the entry to delete in the list on the left of the screen
Click the ***Delete*** button
Select ***Yes*** to confirm

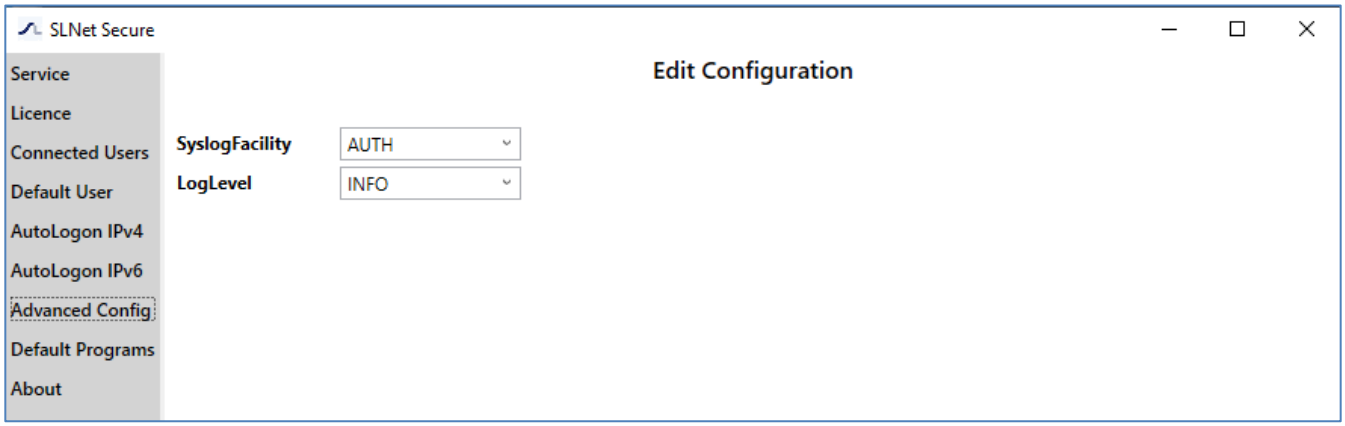


Advanced Config Tab

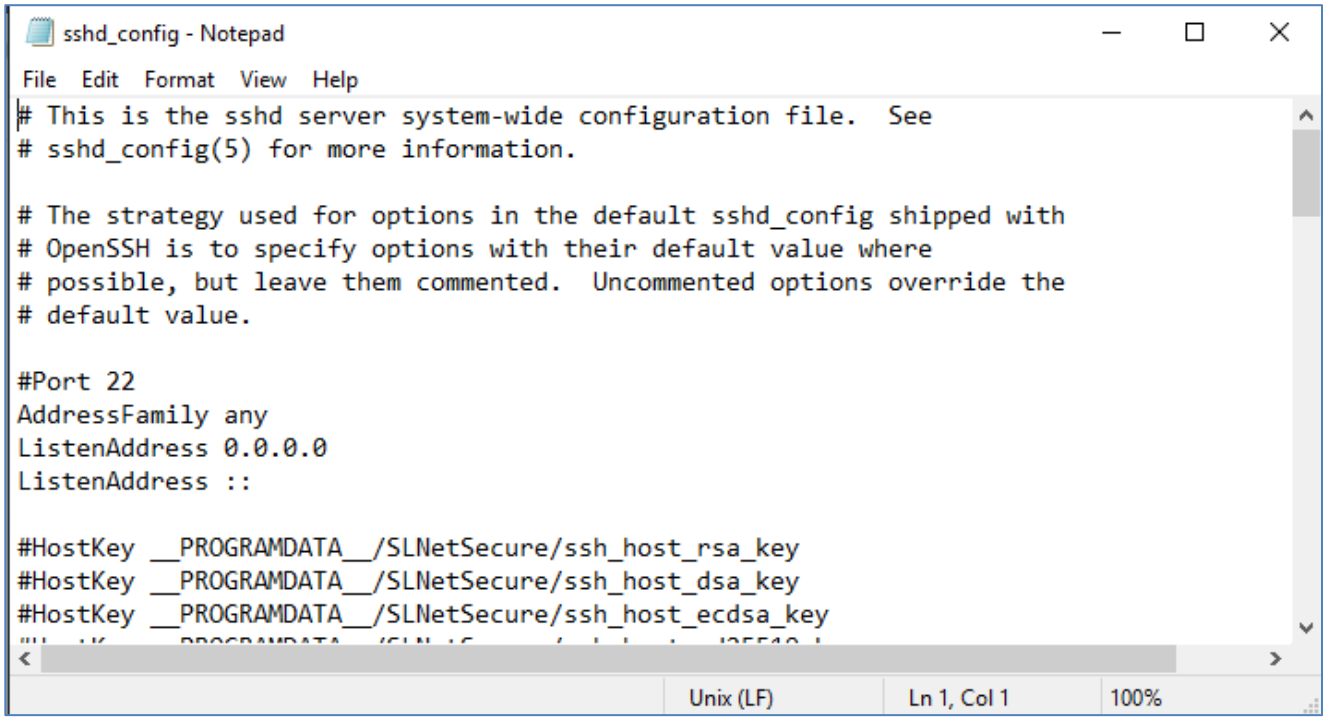
The Advanced Config tab is used to edit the sshd_config file which is an ASCII text based file where the different configuration options of the SSH server are configured.

To edit the sshd_config file click ***Edit*** which opens the file in Notepad.

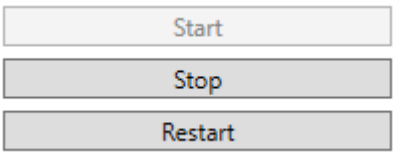




Make your changes, then from the Notepad menu select ***File, Save***
Then close the file by selecting ***File, Exit.***



Then go to the Service tab and click ***Restart*** to restart the SLNetSecure Server service.



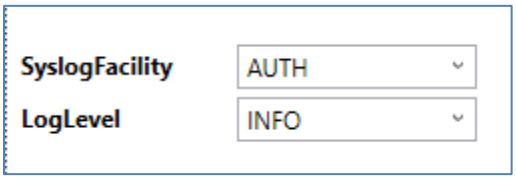
sshd_config file

During installation, SLnet Secure creates sshd_config in the path %programdata%\SLnetSecure\sshd_config. SLnet Secure reads ssh configuration data from %programdata%\SLnetSecure\sshd_config. If the file is absent when the SlnetSecure Server service starts, it generates one with the default configuration.

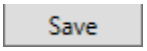
To see which configuration options are supported for your version of Windows operating system refer to the OpenSSH documentation which can be viewed on the Microsoft documentation web site.

SLNet Secure logging:

Select the logging level by choosing the desired option from the SyslogFacility and LogLevel drop-down lists.



Select ***Save***



If you need file based logging, set SyslogFacility to LOCAL0. Logs will be generated under %programdata%\slnetsecure\logs.

For trouble-shooting set SyslogFacility to LOCAL0 and Loglevel to Debug3 then restart the SLNet Secure service.

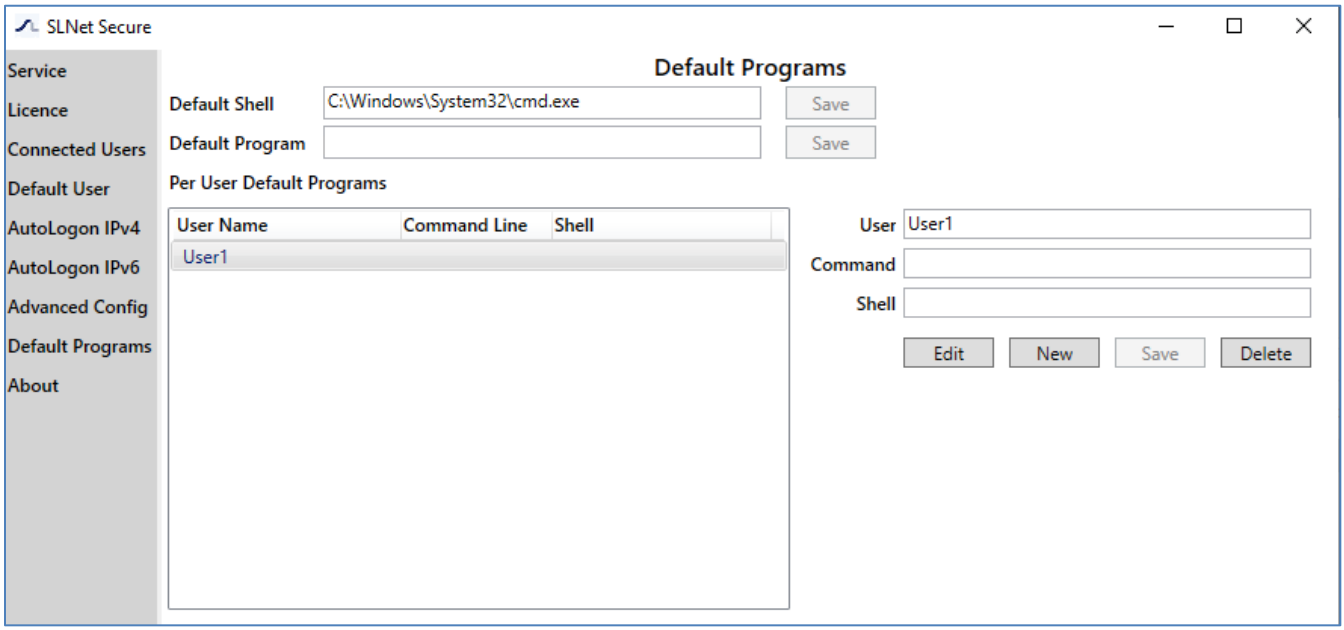
Default Programs Tab

In the Default User tab you can set the shell and start application for the default user and other users.

You can add as many custom user profiles to SLNet Secure as needed.

All SLNet Secure users must have an existing Windows user account.

SLNet Secure allows you to define system access on a user-by-user basis. It also allows you to automatically customize the start for each user - for example, all users are presented with the Windows Common Command Shell or SAP Console.



The **Default Shell** and **Default Program** is used for any user who logs onto SLNet Secure but does not have a custom profile.

Default Shell: For use with most applications, the *Default Shell* field should be left as configured upon installation. This default path allows access to the system command shell. Opening the command shell allows console applications to run properly as well as giving access to the prompt in the command shell if desired.

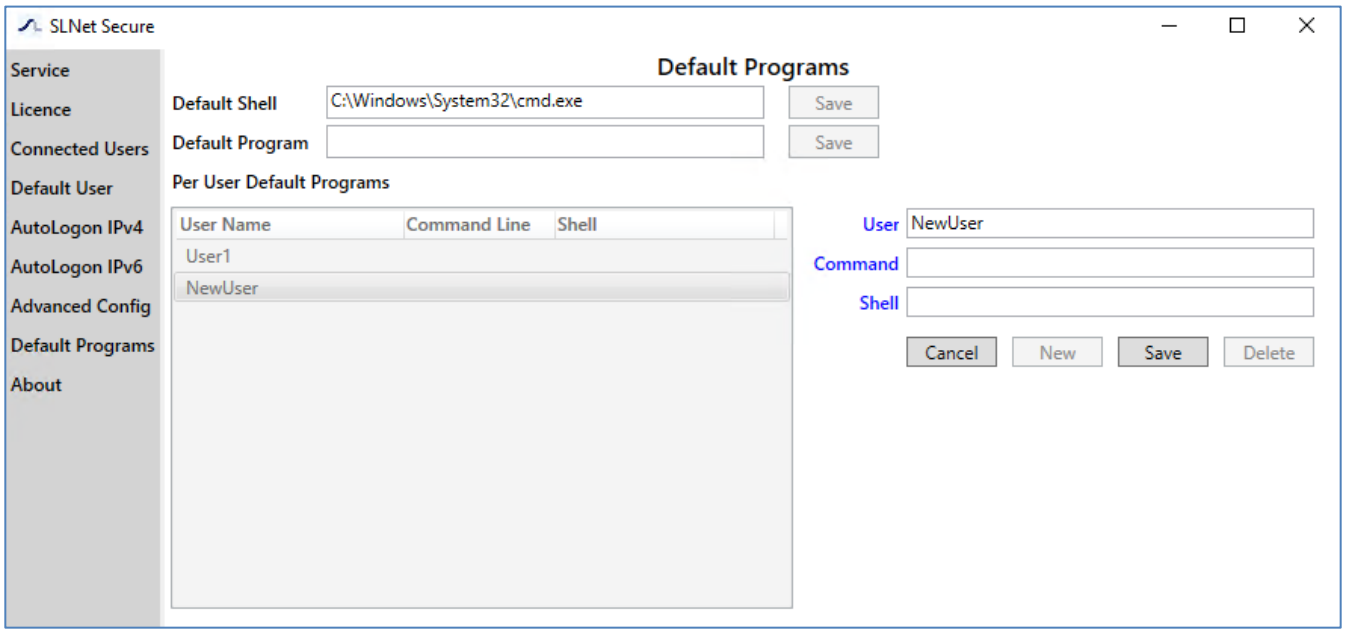
When used with SAPConsole 7.10 and above the *Default Shell* field should be changed to point to sapcnsl.exe.

Default Command: To put users directly into your own custom application, enter the full path to the application startup command followed by any required parameters. The full path must be entered in the format of either the Universal Naming Convention (UNC) or drive letters

Create a new user profile

Click ***New*** to add a new user. It must be a valid windows user account

If Use Autologon is enabled on the Default User tab then all users will login as the Default User.

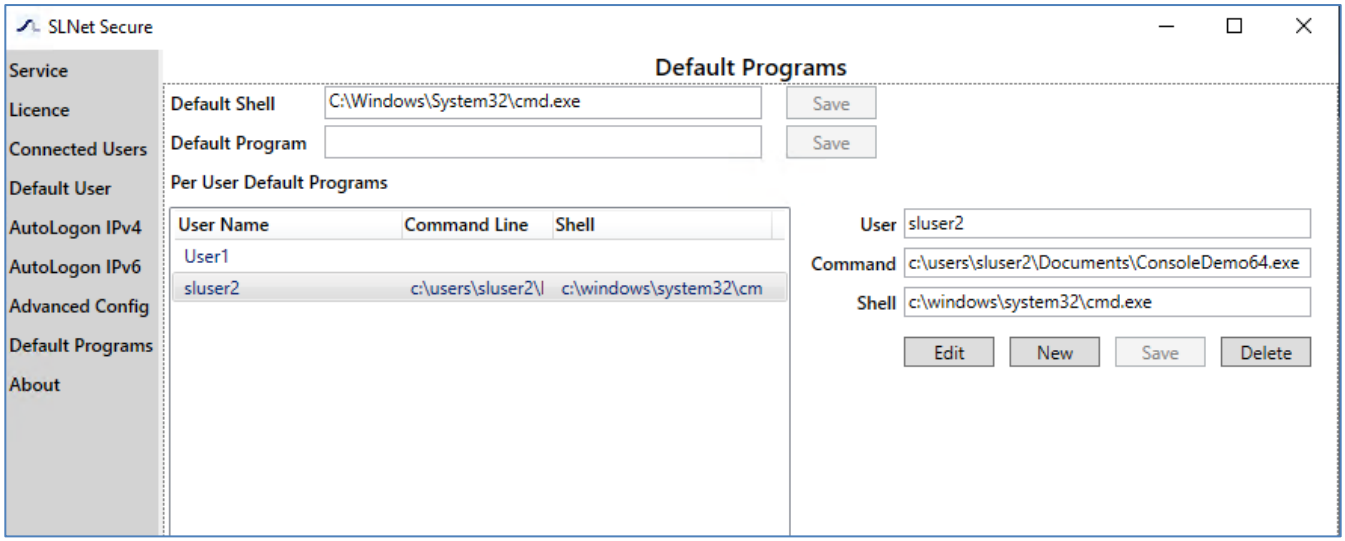


User: Overtype **NewUser** with the user name

Command: To put the user directly into your own custom application, specify the full path to the application startup command followed by any required parameters. The full path must be entered in the format of either the Universal Naming Convention (UNC) or drive letters,.

Shell: Enter the path to the desired shell for the user.

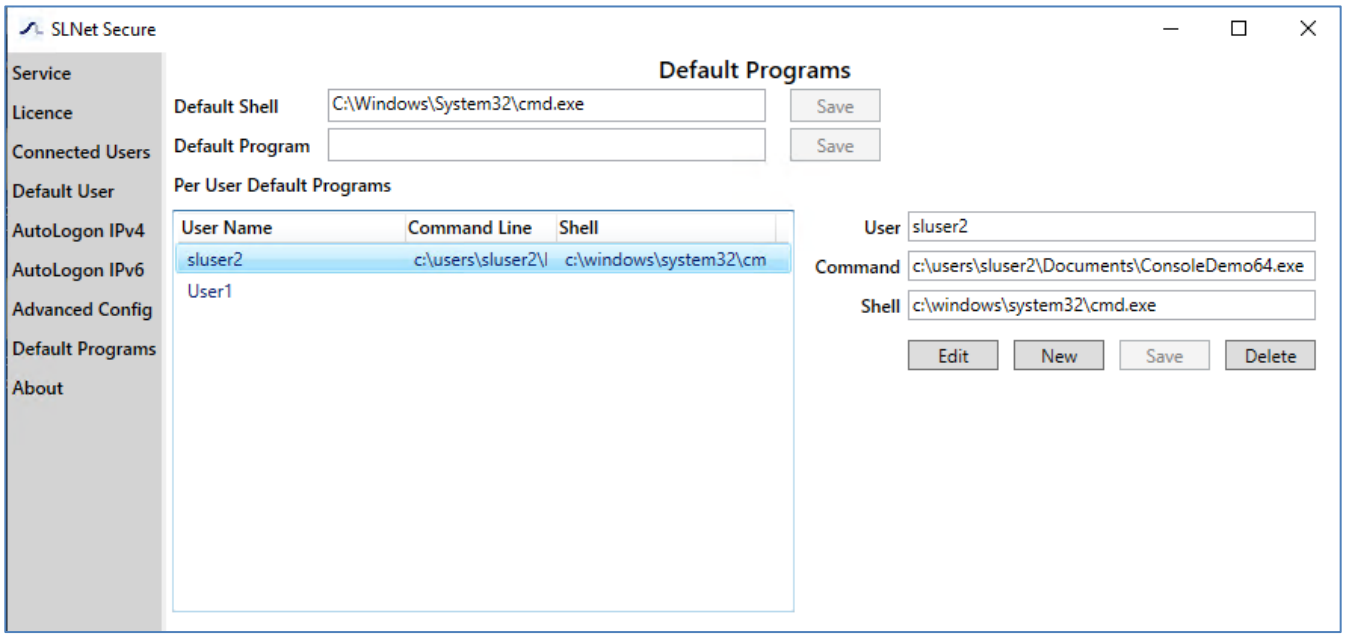
Then select ***Save***



Edit user profile

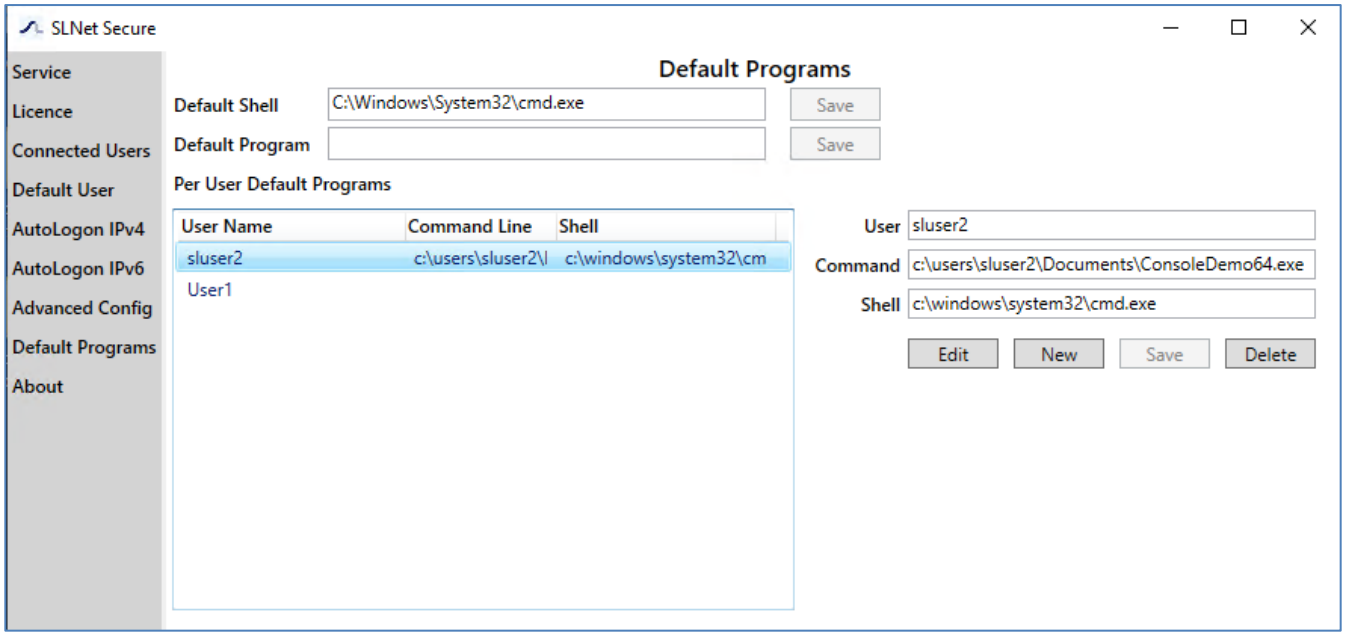
Select a user profile from the **Per User Programs list**, then amend either of the **User**, **Command** or **Shell** values.

Click ***Save*** to save changes.



Delete user profile

Select a user profile from the **Per User Programs list**
Click the ***Delete*** button
Select ***Yes*** to confirm



About Tab

This tab displays the software release version and copyright information.
Please quote the version number when speaking to SLNet technical support.



Logging on to SLNet Secure

SLNet Secure includes the standard OpenSSH client. SLNet Secure is also compatible with all SSH compliant third party clients.

A SSH client can be any of a variety of devices: a process on a UNIX machine, a Macintosh running Terminal, a network terminal, a dumb terminal attached to Terminal Server, a Windows terminal emulator, etc.

Many SLNet users connect through handheld terminals to their applications such as warehouse inventory systems, SAP (SLNet usage is recommended in SAP's documentation), etc. These RF devices can emulate a variety of terminal types.

When you first log on to a new device, you will be presented with an alert that the authenticity of the server or device that you are connecting to cannot be verified. This is normal and a security measure. The SSH client will show you the host key that was presented by the server. To ensure that the server you are connecting to is the actual server you intended to connect to (and not a spoof or man-in-the-middle), you should confirm its identity.

When you initially launch a SSH client, it is not connected to anything. You need to initiate a SSH connection. From some SSH device, you do so by placing default settings in the SSH client software.

Manual Logon

When a user connects to the SLNet server via a SSH session, they will be prompted for:
Logon: (username)
Password: (password)

Automatic Logon

With SLNet you can set up an auto logon using a default user account for authentication or by IP address. With auto logon any device connecting to SLNet will automatically be logged on without having to enter a user name or password and will be placed in the shell specified in the User Profile.
Instructions for configuring a global Default User Logon can be found on page 14 of this manual.

Automatic Logon by IP address

SLNet can automatically logon a user from a device that connects from a specific IP address or a range of addresses. This enables you to have a shared user ID be used from a single IP address or a secured range of IP addresses.
Instructions for configuring Auto Logon by IP Address can be found on pages 16-24 of this manual.

How to connect using the OpenSSH client

Open the SSH terminal on your machine and run the following command:
ssh *your_windows_username@SLNetSecureServer_ip_address*

Then type in your password and hit ***Enter***.

The OpenSSH client is located in **C:\Program Files\SeattleLab\SLNet Secure Server**

Example connection using OpenSSH client from a new device:

```
C:\Users\SLAdministrator>"C:\Program Files\SeattleLab\SLNet Secure Server\ssh"
sluser2@10.0.0.5
The authenticity of host '10.0.0.5 (10.0.0.5)' can't be established.
ECDSA key fingerprint is SHA256:CFjM0pMo3BG5HW0yWfGeJCNNI+0IHRUIFqaE+NOzoc8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.5' (ECDSA) to the list of known hosts.
Sluser2@localhost's password:*********
```

Example connection using OpenSSH client from a device that has connected before:

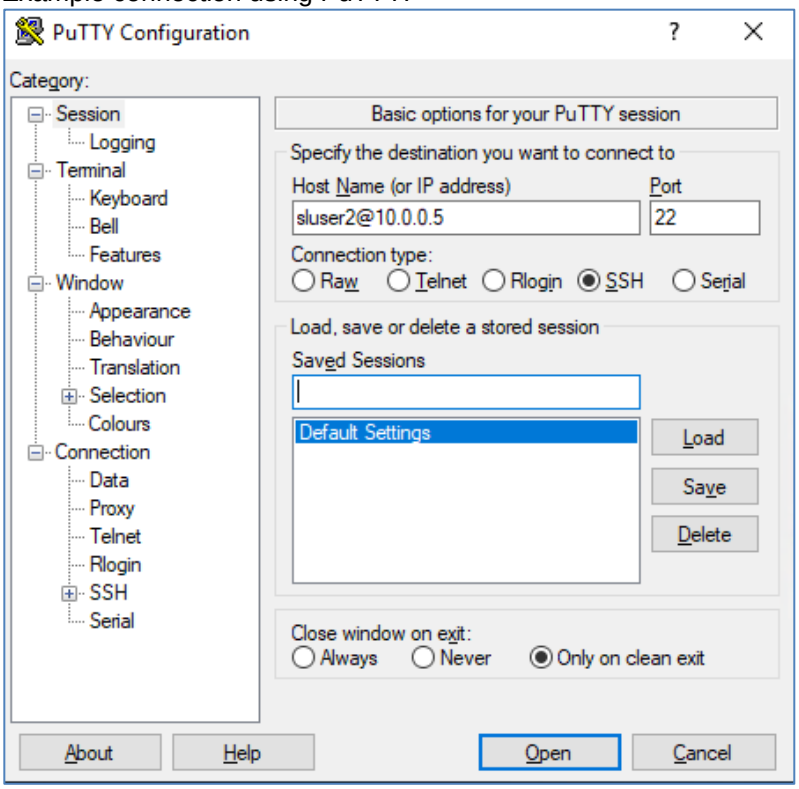
```
C:\Users\SLAdministrator>"C:\Program Files\SeattleLab\SLNet Secure Server\ssh"
sluser2@10.0.0.5
Sluser2@localhost's password:*********
```

Type **Exit** or close the window to disconnect

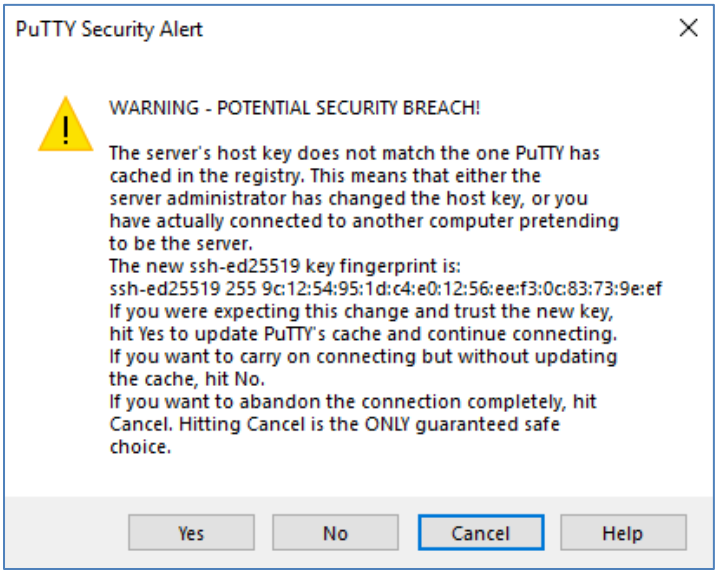
How to connect using PuTTy

Install and launch the PuTTY client
The Session category should be loaded as default
Select Connection type: ***SSH*** **-** this will enter the default SSH port ***22***
In the **Host Name (or IP address)** box enter ***your_windows_username@SLNetSecureServer_ip_address***
Click ***Open***

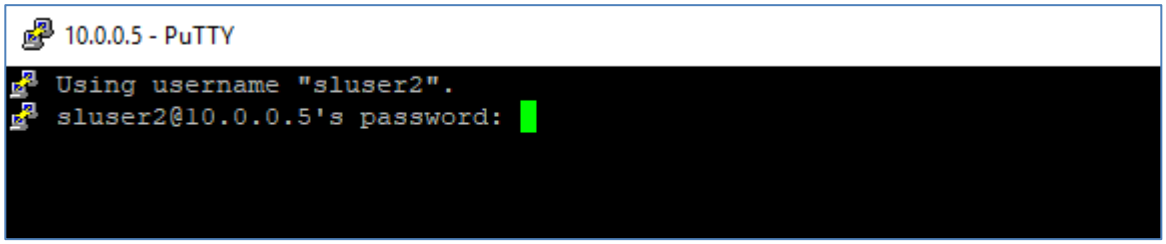
Example connection using PuTTY:



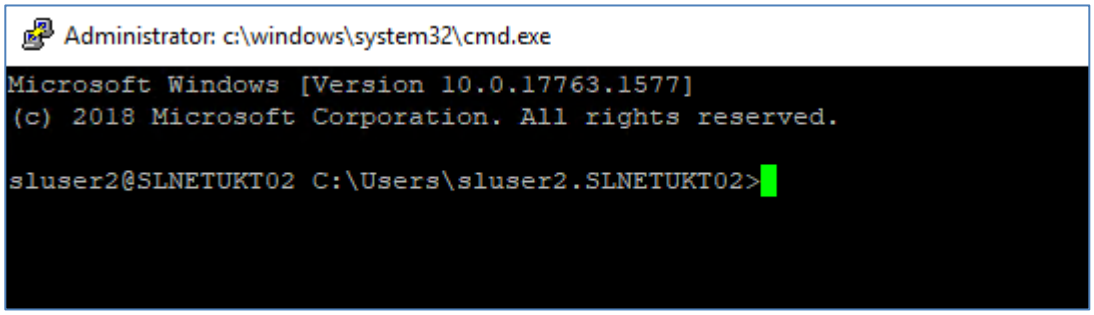
If this is the first time the device has connected you will see this security message, so click ***Yes***



Enter the password and press ***Enter***



When a user has successfully logged on, they will be taken to the shell specified in the Default Programs tab for the user or the default shell if there isn't a profile for the user. The default shell is the Windows Common Command Shell.



Type ***Exit*** or close the window to disconnect

Exiting an SLNet Secure session

If logged into a backend application such as SAPConsole or Oracle, you should first properly exit the application. If at that time the SLNet Secure session does not disconnect you can either turn of your RF terminal or type EXIT at the MSDOS prompt if connecting from a PC

SLNet Secure Entries in Windows Event Viewer

SLNet Secure keeps a record of its activities by entering messages in the Windows Event Log as events occur.

In order for SLNet Secure to write events to the Windows Event log, SyslogFacility should be set to *Auth* on the Advanced Config tab.

To view event logs for SLNet Secure, open the Windows Event Viewer, open the SLNetSecure group, then open Admin or Operational log.

Logging Message examples

- If the user exceeds the authentication attempts an error message is logged to the SLNetSecure Admin log. The number *2* will appear in the Event column and the error message will be: “sshd: error: maximum authentication attempts exceeded for *Username* from *IP_Address* port *XXXXX* ssh2 [preauth]
- If a user logs in successfully and the password is accepted an information message is logged to the SLNetSecure Operational log. Then number 4 will appear in the Event column and the information message will be: “Accepted password for *Username* from *IP_Address* port *XXXXX* ssh2

Appendix A. Troubleshooting

SLNet Secure is designed to be a powerful solution to your SSH connection needs.

Problems usually occur when you have made a change in your environment. This may be an operating service pack, a security change, new device, or changing users.

A.1: Before You Contact SLNet Technical Support

In order to do our best for you, we require accurate and timely information in the formats we request. Our records show that over 50% of all incidents reported are resolved as permission problems or not following the directions in the documentation.

Here are steps to follow before you call our technical support team:

1. Review the Windows Event log. It is a good source for error messages on security and connectivity.
2. Validate that a user has a good connection to your network and a valid Windows account.
3. Verify that the user has permission to log on locally to the server that SLNet Secure is installed on.
4. Turn on SSH logging through the Advanced Configuration tab. Often you will find the user has entered invalid characters or data.

When you contact SLNet technical support, please let us know your Windows operating system release and hardware environment, SLNet Secure version, and a complete description of your question or issue (let us know if you can recreate it), and ensure you have access to the SLNet Secure server.

A1.1: SeattleLab Professional Services

If you need special assistance with customization of SLNet Secure, please contact our technical support group to arrange for billable professional services time.

A1.2: Contacting SLNet Specialists

Customers with active maintenance support contracts have access to technical specialists in a number of ways:

Email	
- Sales - Technical Support	sales@seattlelab.co.uk slticket@seattlelab.co.uk
To Log a Ticket	Email slticket@seattlelab.co.uk
ChatBot	Visit our website www.seattlelab.com One our representatives should be online. If not, you can send us details of your enquiry via the ChatBot and a ticket will be automatically logged
By Telephone	Phone us on +44 20 9167 7133. Our hours of business for our offices are available on our web site www.seattlelab.com

We'll "do what it takes" to assist you with your questions or problems.

This page intentionally left blank.