Step 1 - First Power Up

(A) - Before turning on the Appliance

1/ Ensure that the ES100 listening port AND Outbound Email ports are connected to the network

2/ Ensure that the TAP (if being used) is powered up

3/ Connect the AC power cord (provided)

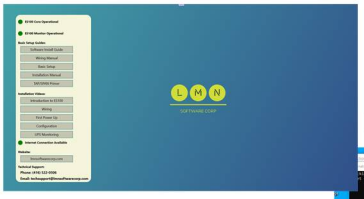
4/ The EdgeSentry ES100 will boot into Windows and prompt you for a Username and Password

5/ Enter "admin" and "letmein" (no quotation marks)

6/ You may be prompted at this time to change the default admin password

7/ Once Windows has loaded you will see the ES100 Assistant on the screen - minimize the display and look for a message about IP Address configuration:

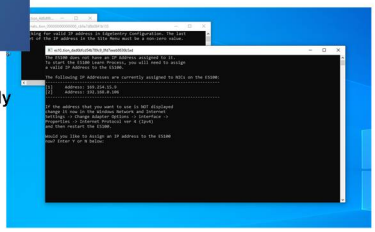
Minimize this...



Note that the Assistant will automatically revert to the foreground periodically.

It is also possible to confim the address using the ES100 Configuration Tool - in the "Site Information" Menu.

Look for this...

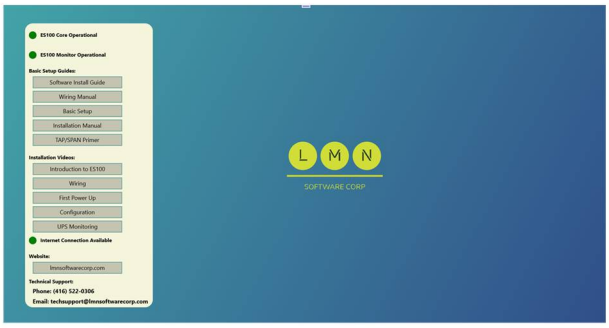


If the networked system is NOT complete -
leave the system in this state (power it down if you like) and finish the remaining work on the network prior to putting the ES100 into "Learn" mode.

If the networked system IS complete -
Verify that a correct IP Address is displayed under the second heading. If both IP Addresses displayed start with 169.254.... then verify that the outbound network port is connected to a DHCP server.

Alternatively you can manually configure a static IP for listening port and restart the server. The IP Address Utility should display that port next to the [2]. When the correct IP address is listed next to the [2] press "Y" and <Return>, and then [2] and <Return> followed by any key to exit.

Once the IP Address is set from the ES100, the system enters "Learn" mode.
Your screen will look like this:



Once the "Learn" process is completed (about 24-26 hours), the next step is to set up the system using the Configuration Tool client software. All remaining setup steps are done from the Configuration Tool and there is NO further setup required at the ES100.

Step 2 - ES100 Configuration Tool

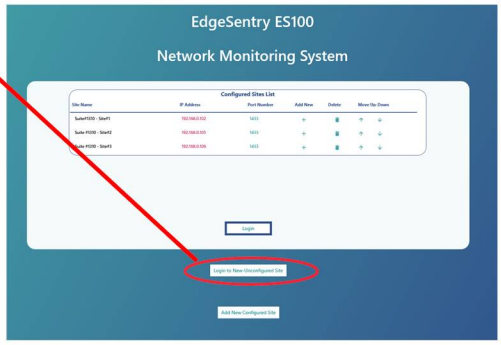
(A) - Load the ES100 Configuration Tool software from the USB provided or from the LMN website: www.lmnsoftwarecorp.com

The ES100 Configuration Tool:

- Displays the learn status
- Is used to label and authorize all the network devices
- Is used to authorize network connections
- Is used to set up email notifications and automated reporting
- (optional) is used to create alerts on use of specific ports

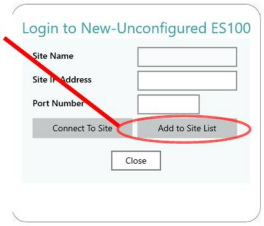
First Log On:

The splash screen will display a list of all configured systems (if any). To add a new system to the software, Click on the **Login to New Unconfigured Site** button.



You will be prompted to input the **Site Name**, **IP Address** and **connection port number** (default is 1433).

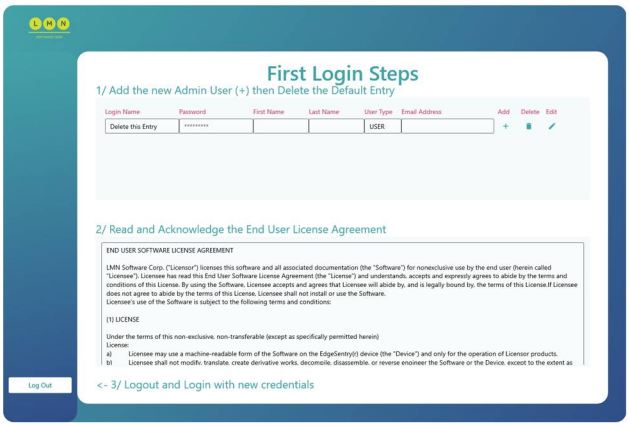
Click "Add to Site List".



Now click on "Connect to Site".

You'll be taken to the "New Site" page where you will asked to set up at least ONE Administrator and to read the End User License Agreement. New users can be added by an administrator later from the **Configure Site -> Users** menu.

When completed, you will need to log out of the system prior to continuing.



Five Steps to complete the First Login:

1/ Add at least **ONE new Administrator** account - Adminstrators can log into the Configuration Tool Software whereas Users ONLY have access to the Dashboard Software

2/ **Delete the dummy account** ("Delete this Entry")

3/ Read and acknowledge the **End User License Agreement**

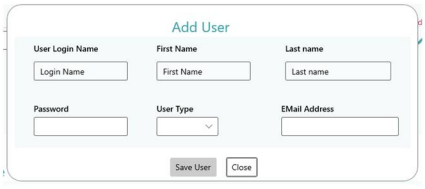
4/ **Log out**

5/ **Log in again using the new credentials**

1/ Click the ADD button to display the Add User dialog box

Click ADD to display the Add User dialog box

Set a Login name, set the User Type to "Admin" and input a password (other fields are informational only)



draft: 1.0 Nov 2021

Step 2 continued - Setting up Users

2/ Delete the dummy password shown

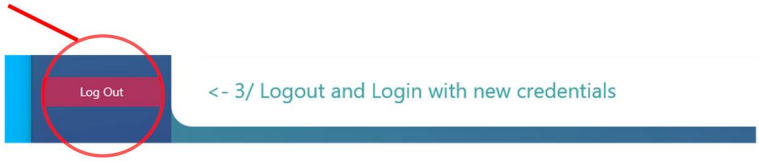
Delete this entry once you have added at least one new ADMIN user.

Passwords must contain a lower case letter, an upper case letter, a number and a special character. Usernames and passwords are restricted from being SQL keywords.

3/ - Read the End User License Agreement and click the Acknowledge Checkbox at the bottom of the page

Click the checkbox to acknowledge

4/ - Click Logout

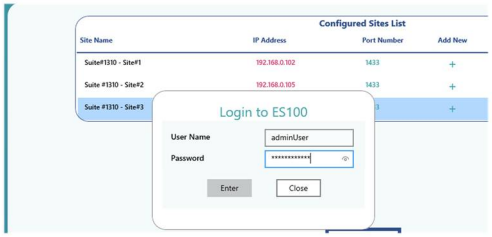


5/ Login with the new username and password

Select the New site from the Configured Site List

Log into the newly configured site by clicking it (it will be highlighted in blue) and then selecting "**Login**".

You will then be prompted for the username and password you configured - press "**Enter**". The Configuration Tool Software will now connect to the ES100.



If you have multiple seats of Configuration Tool or Dashboard software, add the new site by clicking "Add New Configured Site" at the login page of the Configuration Tool or the Dashboard software

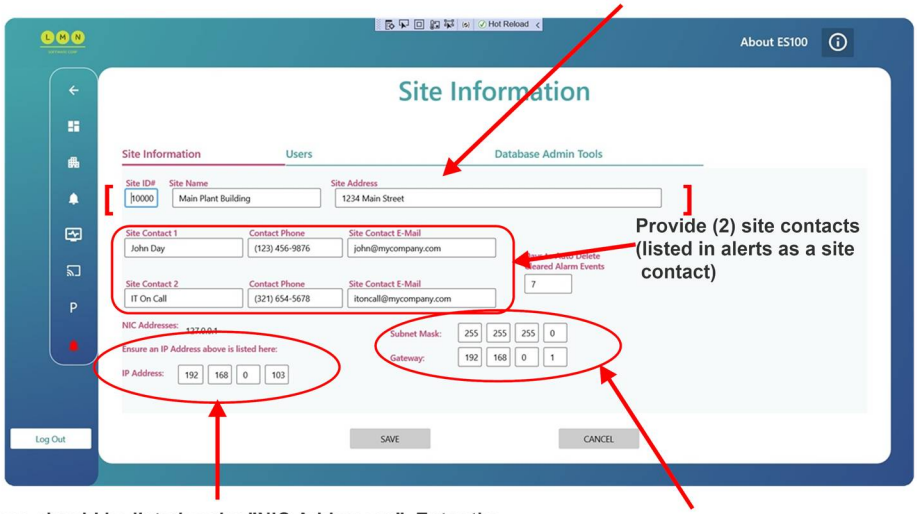
draft: 1.0 Nov 2021

Step 3 - Configuration

(A) - Input basic Site Information- used for Alerts and Dashboard Display

Click the Site Menu Icon

(i) Assign a unique number to the site
(ii) input the site's Name (used in Alerts and Reports)
(iii) provide the site address (informational only)



Provide (2) site contacts (listed in alerts as a site contact)

The site's IP Address should be listed under "NIC Addresses". Enter the address in the spaces next to IP Address and press SAVE. If the IP address has not already been set in the system, the sensor will start to collect information from the network and the "Learn Percentage " indicator on the Dashboard will start to increment.

Enter the site's Subnet Mask and Gateway - this information is used to determine Off LAN connections.

(B) - Set up Outbound Email Account and Alerts

Click the Notification Icon

Enter the outgoing account:
- e-mail address
- server address
- "from" address (can be any address)
- server port number
- password
- SAVE and then Refresh (note the password will be blank)

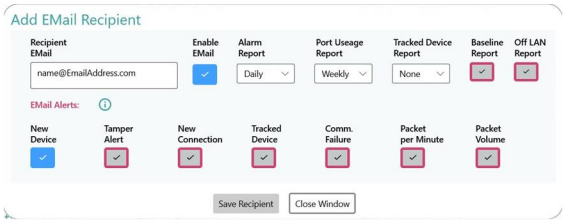
Click to send Test e-mail

If using a Gmail account (as shown here) you will have to turn ON "Less Secure Account Access" in your Google Account - (Manage Google Account, Security)

Add an Email Recipient for Alerts and Reports

- Note that the **Tracked Devices and Baseline Reports** will not be functional and should be turned off until after the learn process is completed.

- Similarly only **New Device** and **Tamper Alerts** should be selected until after the Learn process is completed.



NOTE: Be cautious about enabling/sending alerts before you know the quantity of alerts that the system will send.

Step 4 -Authorizing Devices

(A) - The system's Learn process takes about 24 hours to complete

Click the Dashboard Icon

The Learn status is shown in the top center of the Dashboard

When the Learn status reaches 100% the Learning, Alarming and Reporting indicators will all be in Green.

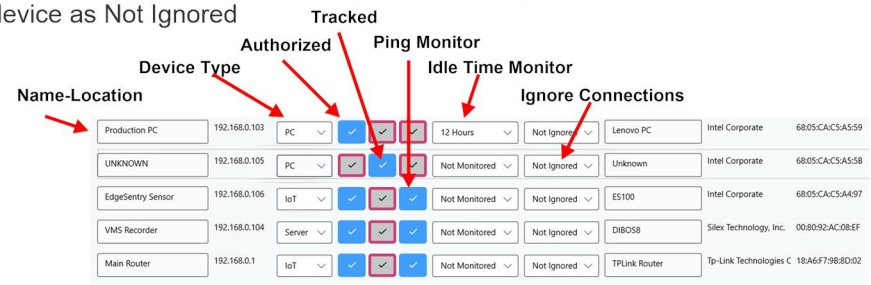
(B) - Set up the Information for each Device

- note that this is a critical step for the emailed alerts and reports to be readable

Click the Devices Icon

For each device on the system:

- provide it with a name and location
- Assign it a **TYPE**:
  - **PC**: standard PC on the network
  - **Server:** a PC that must be always available on the network
  - **IoT**: a device that is custom purpose (camera, door controller, intercom)
- **Authorize** it (or not) - Authorize if this is a known-trusted device on the system
- Flag the device for Communications **Tracking** (default to OFF)
- Set the device to be **PING Monitored** (default to ON for IoT, Server Devices)
- Set the device to be **Idle Time monitored** (default to OFF)
- Leave the device as Not Ignored



Key Definitions:

Device Type: **PC -**any general purpose computing device that is general purpose and may be turned off. If a PC is to be monitored, consider using Idle Time Monitoring, as using PING Monitoring will cause alerts when the device is turned off
SERVER - A specialized computing device that is critical to the operation of the system and that is expected to be on at all times.
IoT - A special purpose device - Camera, Intercom Door Controller, thermostat which is expected to be on the network at all times

Authorized: **If checked, the device is a known authorized entity on the network. If you want to be alerted when it becomes active on the network delete the entry. Avoid leaving the device on the system and unauthorized - remove the device from the network.**

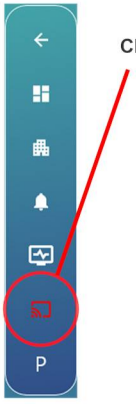
PING Monitor: If checked, the device will be monitored using ICMP pings, use this for devices that support ICMP and are expected to be on the network (powered up) at all times - alternatively you can use Idle Time monitoring to alert if the device does not communicate for a specific amount of time.

Ignore Connections If a device is causing massive amounts of alerts but needs to remain on the network you can choose to ignore inbound, outbound or all connections. This should be considered a last resort as the system will NOT collect information about this device.

draft: 1.0 Nov 2021

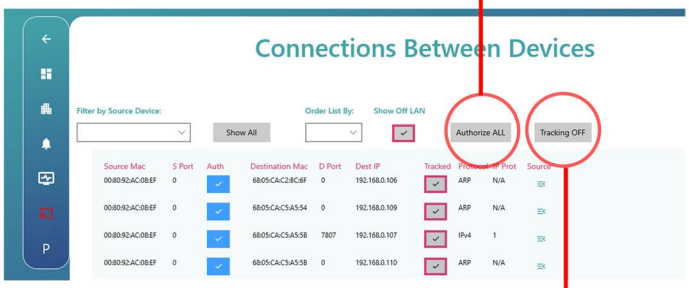
Step 4 -Authorizing Connections and Ports

1/ Authorize ALL Connections



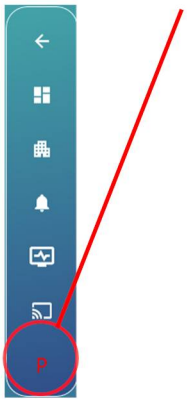
Click the Connections Icon

If all devices on the network have been authorized then Authorize ALL connections.



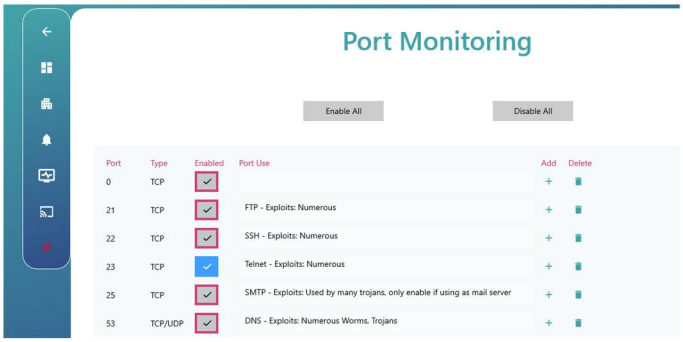
Turn tracking ON if you want to have the device connection recorded in the Tracking Report. Try to use this selectively as the Tracking Report can get very long quickly! The system will automatically stop tracking devices once there are more than 5000 tracked devices listed.

2/ Set up Port Monitoring (Optional)



Click the Ports Icon

If you have a list of "authorized" ports and protocols for your network, make sure they are NOT enabled in this menu. If you enable any of the other "risky" ports you will be alerted with a "New Device" level alert when that port is used. Ports can be added or removed from this list.



3/ More Information

- More detailed information is available in the **ES 100 Manual**
- installation Videos and tutorials are posted on our **web site: lmnsoftwarecorp.com**
- Contact us by **phone** or **e-mail**:

Sales and Marketing Questions:

Jeff Leite

jleite@lmnsoftwarecorp.com

(303) 995-5182

Technical Questions:

John Day

john@ lmnsoftwarecorp.com

(416) 522-0306