Linear®
Building On Innovation.

eMerge™
Browser Managed Security Platform

eMerge 50P
eMerge 5000P

Initial Software Setup Guide

May 2013

Linear LLC
1950 Camino Vida Roble
Suite 150
Carlsbad, CA 92008
www.linearcorp.com

Contents

Introduction

Overview

This guide describes the initial software setup for the following eMerge systems:

- eMerge 50P
- eMerge 5000P

The setup instructions assume that the hardware installation has been completed for the following system components:

- The eMerge Network Controller. For installation instructions, refer to the installation guide for your system.
- All eMerge Network Nodes to be included in the system. For installation instructions, refer to the *Network Node Hardware Installation Guide*.

Note:

For eMerge *VR,* follow any steps in this guide that have not already been covered by using your specific *NetVR Hardware Installation Guide*. After completing the additional portions of this guide, use your specific *eMerge NetVR Setup and Configuration Guide* to configure your cameras.

Completing the Initial Software Setup

The initial software setup process for an eMerge system includes the following steps:

- Setting IP values for the controller, as described in the following section.
- Reconnecting to the network and logging into the eMerge Security Application. See page 6.
- Using the administrative console to set up and enable nodes. See page 7.

Once the process is complete, you can use the eMerge Security Application's administrative console to configure inputs, outputs, readers, cameras, and other security resources for the system.

Setting IP Values for the Controller

This section describes how to set IP values for the controller. Later you will be able to log into the eMerge Security Application and use its administrative console to change any of these initial values.

Note:

The controller is configured with a factory default IP address of 192.168.0.250. If this is not a valid address on a corporate network that is available for use, you will need to reset the controller's IP address to one provided by the corporate IT organization before connecting it to the corporate network.

To allow you to reset the controller's IP address before connecting to the corporate network, the hardware installer should have set up a small network by putting an Ethernet switch between the controller and the PC you will use for the configuration. This procedure is described in the hardware installation guide for your system.

To set controller IP values:

1. Make sure the PC you will use for the configuration is connected to the controller via an Ethernet switch, and that the PC's IP address has been changed to a static value of 192.168.0.x (where x is a number between 100 and 200, and not 250).
2. Open a browser window on the configuration PC.
3. In the address field, enter the default IP address for the controller: **192.168.0.250**
4. Press **ENTER**.

5. If the **Initmode** page does not appear, select **Setup : Site Settings : Network Controller** and click the link in the **Initmode Settings** section.
6. In the **Network Settings** section, obtain the following values from network administrator and enter them in the appropriate boxes:
   - The static IP address to assign to the controller.
   - The appropriate subnet mask.
   - The gateway IP address.
   - DNS (Domain Name Server) IP addresses.

   Important:

   If you change the IP address of the controller, take note of the new address, because you will need it to log in later.

7. In the **Initmode Settings** section, select **No** from the drop-down.

   This ensures that the **Initmode** page will not automatically redisplay when you reboot. It is set to **Yes** only to allow you to change controller IP values during the initial software setup.

   Note:

   Later you will be able to log into the Security Application and return to the **Initmode** page by selecting **Setup : Site Settings : Network Controller** and clicking the link in the **Initmode Settings** section.

8. Enter values for any of the settings in the **Time Settings** section. These settings are described in About the Network Controller time settings.

   Important:

   For NetVR appliances, it is highly recommended that you configure a Timeserver to ensure the NetVR recordings and security camera times are synchronized correctly. If you do not have a Timeserver, locate a public NTP server. See the *eMerge NetVR Setup and Configuration Guide* for more information on Date/Time Setup.

   You can change values in the **Email Settings** section later, if you decide to use email alerts.

9. In the **Web Server Settings** section, change the default HTTP port number (80) **only** if the network administrator provides a different port number.
10. Click **Save**.

    The web server restarts, and beeps when done.

Note:

If you set **Initmode** to **No** and do **not** change any IP address values, click **Save**, and then **Reboot** and **OK**. You will hear two beeps when the system shuts down, and one when it restarts. The eMerge Security Application may take several minutes to restart.
Refresh the browser, then proceed to step 12.

11. Browse to the IP address set for the controller.
12. The Software License page opens.
    - ❍ Check to accept the terms.
    - ❍ Click **Apply**.
13. The system login screen opens.
14. Connect both the controller and the configuration PC to the corporate network. All further configuration work can be done through the corporate network.

Once the eMerge Security Application restarts, you can log in and use its administrative console to configure inputs, outputs, readers, and other security resources for the system. For login instructions, see page 6.

About the Network Controller Time Settings

Use of an NTP network time server ensures that the controller will be synchronized regularly with the exact time used by all other network resources. For the controller to synchronize its own time, at least one time server must be designated. If no time server is available, the controller clock may drift slightly over time.

The available controller time settings are as follows:

- **Current Network Controller Time**: This displays the current time of the controller clock.
- **Manually Set Date/Time**: If there will be no network time server available for the controller, select a date and time from the **Manually Set Date/Time** drop-downs to manually set the time for the controller.

Note:

If you set the time manually, be sure to set it to standard time, not daylight savings time. The **Timezone** setting will automatically adjust for daylight savings time (summer time).

- **Timeserver 1, Timeserver 2, Timeserver 3**: The default name in each of these fields is ntp.ubuntu.com. If your system is installed on a network with Internet access, this default setting need not be changed.

Note:

If there is no Internet access:

- The network administrator must supply you with a local network timeserver name, or the time will have to be manually set.
- If the time must be manually set, remove the time server name from this field, to avoid having the controller spend several minutes searching for this server.

Until the search times out, you will not be able to continue editing the settings on this page.

- **Timezone**: Select the appropriate time zone for your area from the drop-down. The default preset value in this field is US/Eastern.

Logging Into the eMerge Security Application

Once you have configured initial IP settings for the controller and the system has restarted, you can reconnect to the network and log into the Security Application.

To log into the eMerge Security Application:

1. Open a browser window on the configuration computer.
2. In the address box, enter the IP address that you set for the controller.
3. Press **ENTER**.

   On the page that appears, the **Activation Key** and **Product Key** boxes should contain the correct keys for your system. If these keys are not entered into the system, you will need to enter them manually. The activation and product keys are included on a license label that is shipped with the system.
4. After reviewing the license agreement, click **Apply** to accept it.

   Important:

   Click **Apply** only once.
5. At the Login page, enter the username “admin.”
6. Enter the password “admin.”
7. Click **Go** to display the administrative console for the eMerge Security Application.
8. You can now use the administrative console to set up nodes, as described on page 7.

Important:

If the controller IP address or username and password for your NetBox or NetBox Extreme system are unknown, the system login settings will need to be reset to the factory defaults. For instructions, refer to the hardware installation guide for your system.

Setting Up Nodes

Network nodes handle communications to and from the controller, as well as the power distribution to other application blades in the system. Each node supports up to seven application extension blades in any combination.

The way you set up a node will depend on whether it is on the same IP subnet as the controller or on a different subnet. If the node and controller are on the same subnet, you can use the procedure below. If the node and controller are on different subnets, you will need to use the Network Node Configuration utility, as described on page 8.

Note:

For information on how nodes and the controller use the network, see page 10. For information on installing node hardware, refer to the *Network Node Hardware Installation Guide*.

Setting Up Nodes Located on the Same Subnet as the Controller

To configure and enable a node:

1. Log in to the eMerge Security Application.
2. Select **Setup : Site Settings : Network Nodes**.
3. Select the node you want to enable from the **Name** drop-down.
4. Click the **Rename** link under the Name drop-down and enter a name that will help you identify the node.

   Note:

   Do not change the value in the Unique Identifier field.

5. Select the **Enabled** check box to the right of the Name drop-down. This allows the communication of security data between the controller and the node.
6. Click **Save**.
7. On the **Network** tab of the **Network Nodes** page, you can now set the node's IP address.

   For assistance, in setting the node's IP address and configuring card readers, door locks, and other security resources, refer to the online Help.

Setting Up Nodes Located on Different Subnets than the Controller

If a node is unable to multicast its ID to the controller because they are on different subnets, you will need to use the Network Node Configuration utility (nnconfig.exe). This program lets you use your PC or laptop while connected on the same subnet as the node to:

- Change the IP address settings for the node.
- Give a node the specific IP address of the controller with which it should connect.
- View IP information for available controllers on the network.

You can download a copy of nnconfig.exe from the eMerge Support Tools web site at www.emerge50p-5000p.e3links.com

Note:

The computer to which you download nnconfig.exe must be on the same subnet as the node. You cannot put a router between the computer and the node.

When you launch nnconfig.exe, you will see two drop-downs at the top of the Network Node Configuration window, **Interface** and **Show**:

- The **Interface** drop-down lists all network interfaces configured on your computer. You can select the network interface (IP address) from which you want to work with nnconfig.exe. If there is only one network interface configured, the drop-down will list that IP address but it will be grayed out.
- The **Show** drop-down allows you to choose which node types will appear in the list box. You can also select **Controllers Only** to display only controllers. With the default setting, **All**, all node types and any controllers available on the network are displayed.

Note:

You cannot use nnconfig.exe to change the IP settings for a controller. Any available controllers will appear in the list box each time the controller announces itself on the network. This display is temporary, but it will allow you to see the controllers’ IP information.

To specify IP settings and a controller address for a node:

1. Connect your computer to the network on the same subnet as the node whose IP address settings you wish to change.
2. Launch **nnconfig.exe**.

3. The program listens for the node's multicast message and lists the IP address and unique identifier for each node on that subnet. It may take a few minutes for the program to discover the nodes that exist on the subnet.
4. Click a node in the list to select it. The node’s IP address information will appear in the text boxes below the list box.
5. Change any of the node’s IP settings—**IP Address**, **Netmask**, and **Gateway**—to the values that have been assigned to the device by the network administrator.
6. Clear the **Auto Discover NC (multicast)** check box, which is selected by default.
7. Enter the controller’s static IP address into the **NC IP Address** text box.
8. Click **Save**. The node should now find the controller and connect.

Note:

If the controller is behind a NAT router (Network Address Translation), ensure that the controller IP address is configured in the DMZ of the router and enter the router IP address in the NC IP Address text box.

If a node and the controller are on different subnets, routers and firewalls may not allow the node to connect with controller. In this case it is necessary to open TCP Port 7262 on the router in front of the controller, to allow the node to connect to the controller. It is strongly suggested that the network administrator be involved in this configuration.

How Nodes and the Network Controller Use the Network

When a node boots, it initially selects for itself a temporary random IP address in the zeroconf address space (169.254.X.Y, where X and Y are randomly selected). The node then multicasts for a controller at 224.0.72.62 UDP port 7262, and presents its Unique Identifier (UID).

A controller answers the multicast at 224.0.72.62 UDP port 7262, providing its own IP address, and presents an addressing method for the node. See *About the Network Controller Time Settings* on page 4.

Note:

There are three node IP addressing methods available: DHCP, Network Controller-provided, and Static. It is strongly recommended that you use static IP addresses.

If a node is unable to multicast its ID to the controller—for example, because it is on a different network—you will need to use the Network Node Configuration utility (nnconfig.exe) to give the node a static IP address. For more information, see page 8.

Once a proper IP address for the node is selected, further communications between the node and the controller occur directly between their respective IP addresses, using TCP port 7262.

Network Port Usage Table

The following table describes the network ports that must be open to the controller.

Table 1. Network Port Usage

Port number	Usage
TCP Port 80	Must be open to the controller for browser access to the eMerge Security Application. This can be configured on a different port.
TCP Port 443	Must be open to the controller for browser access to the eMerge Security Application using HTTPS (SSL). This can be configured on a different port.
TCP Port 7262	Must be open to the controller for communications between the controller and nodes. Be sure that this port is open through routers and firewalls for any nodes on different subnets from the controller.
TCP Port 22	Must be open to the controller for SSH access to the controller.
TCP Port 3000	Must be open to the controller for the Video Management System virtual inputs to communicate camera up/down and motion detection messages.
TCP Port 3306	Must be open to the controller for PostgreSQL report usage.
TCP Ports 20, 21	When using active FTP, these ports must be open to the FTP server for FTP backups from the controller. When using passive FTP, port 20 will not be required. Ports must also be left open to the controller for FTP server responses. The network administrator must set up these ports.
TCP Port 554	Must be open for streaming H.264 video streams.
TCP Port 22609	Must be open for communication between clients and NetVR or eMerge *VR*.
TCP Port 3010	Must be open to the controller for communication with NetVR appliances.
TCP Port 3011	Must be open as the OVID communication port for NetVR appliances.

Index