Aurora Reverse Network License

AUR-RN1 / AUR-RN5 / AUR-RN10

Setup Guide

A Member of the Kaba Group

KEYSCAN ACCESS CONTROL SYSTEMS FROM KEYSCAN INC

Contents

About the Keyscan AUR-RN License

Keyscan's AUR-RN (reverse network) license is designed so that a programmed access control unit at a remote location initiates communication via an encrypted NETCOM6 over a private or public network back to a PC/server with encrypted communication software at a host location. Note the AUR-RN license is available in three connection configurations as follows:

- AUR-RN1 – one reverse network IP connection
- AUR-RN5 – five reverse network IP connections
- AUR-RN10 – ten reverse network IP connections

This document will refer to all three reverse network licenses as an AUR-RN license except where a difference applies.

Installation Coordination – Host & Remote Locations

The AUR-RN license involves installing and configuring reverse network encrypted communication software at a host location and installing hardware components at a remote location. Before you can complete the reverse network installation, you must coordinate certain settings between the two locations in order that the ACU/NETCOM6 at the remote location can establish network communication back to the server with the encrypted reverse network communication software at the host location.

- the technician installing the hardware components must have a host-location IP address that the control unit connects to on the network
- both the host and remote locations must use the same user-defined encryption key which is part of the programming procedures at each location
- the host location must know the serial # of the designated reverse network control board installed at the remote location
- a valid network path and connectivity must exist from the server with the encrypted reverse network communication application at the host location to the NETCOM6/reverse network control board at the remote location

Important

As networks can be highly complex structures with a labyrinth of routers, firewalls, and switches, as well as layers of security protocols, Keyscan recommends having a network administrator involved to establish a communication path between the two locations.

Please be aware that the installing technician's hardware documentation outlines the Installation Coordination – Host & Remote Locations information as well.

So you have a better understanding of how reverse network functions and what is required to set it up, Keyscan suggests that you review the entire document first, contact the installing technician at the remote location to exchange settings, and then begin configuring the software.

Host Location IP Address

The hardware technician must program the access control board with a host-location IP address along with other settings. The IP address the technician programs into the control board depends on the network configuration. We have provided two general network configuration outlines: an Internet/Intranet/WAN configured network that is

exposed publicly and a LAN that is closed. Refer to the network configuration that best approximates your network application. See the table and illustrations on the following pages for determining which host-location IP address to assign as well as other related settings.

You may have to consult with the network administrator for the correct IP address.

Table 1 – Network Configurations

Network Configuration - Internet/Intranet/WAN - Host Router or End Point with External IP Address				
Example	**Settings**	**Host Location**	**Remote Location**	
See Figure 1	IP Address Port # Gateway Encryption Key	Router with port forward or router table to server with Keyscan reverse network encrypted communication service Same encryption key/bit setting as remote location	**ACU**	programmed with host router or end point external IP address optional override port
			NETCOM6	programmed with static IP address or if using DHCP server dynamic IP Gateway (if static IP above) Port # of host router/end point Same encryption key/bit setting as host location
Network Configuration - LAN – Closed network with no public exposure				
See Figure 2	IP Address Port # Encryption Key	Server with Keyscan reverse network encrypted communication service Same encryption key/bit setting as remote location	**ACU**	programmed with IP address of host server with Keyscan reverse network encrypted communication service
			NETCOM6	programmed with static IP address or if using DHCP server dynamic IP Port # of Host PC/server Same encryption key/bit setting as host location

Figure 1 – Example of Internet/Intranet/WAN with Router or End Point External IP

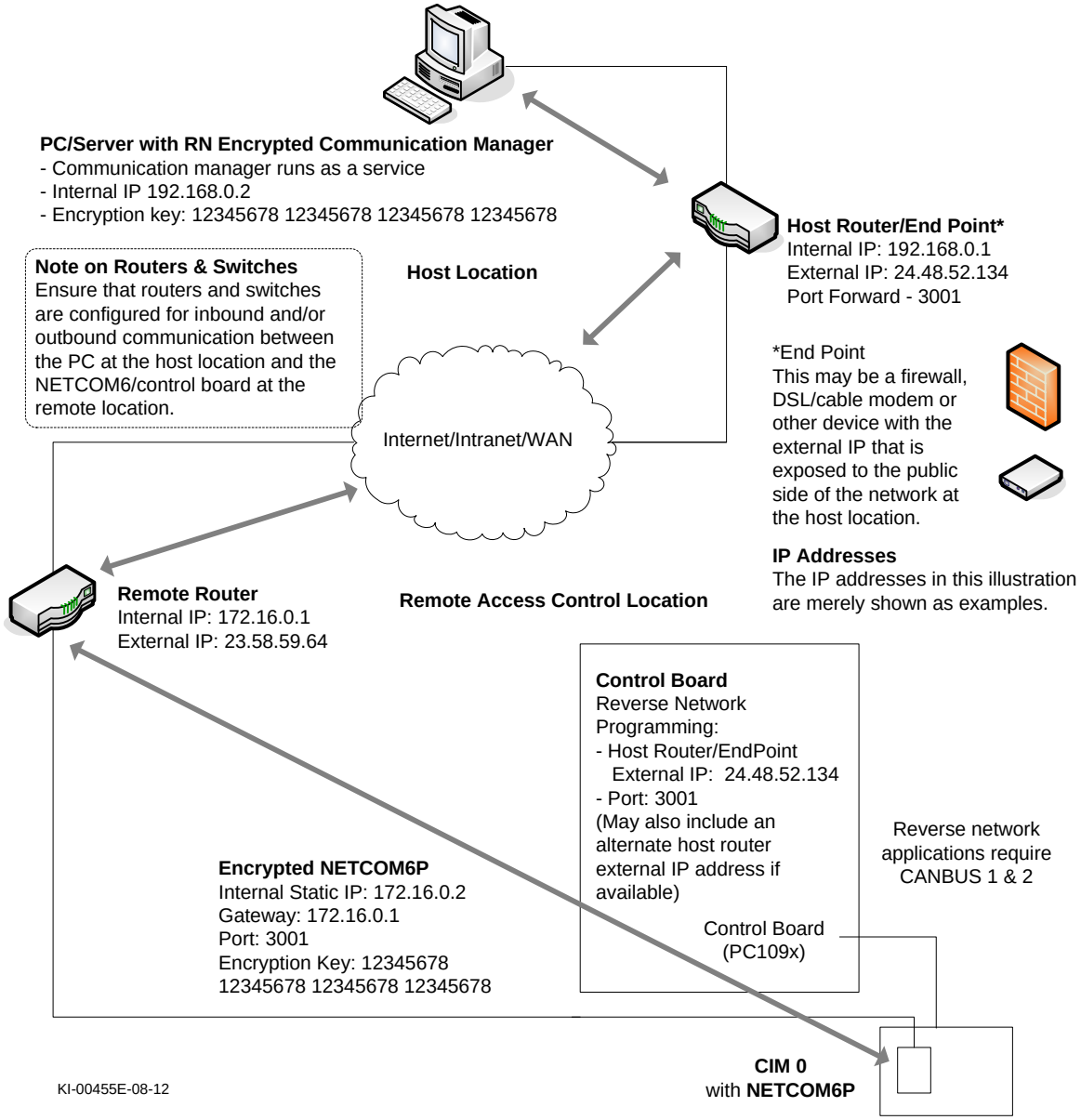
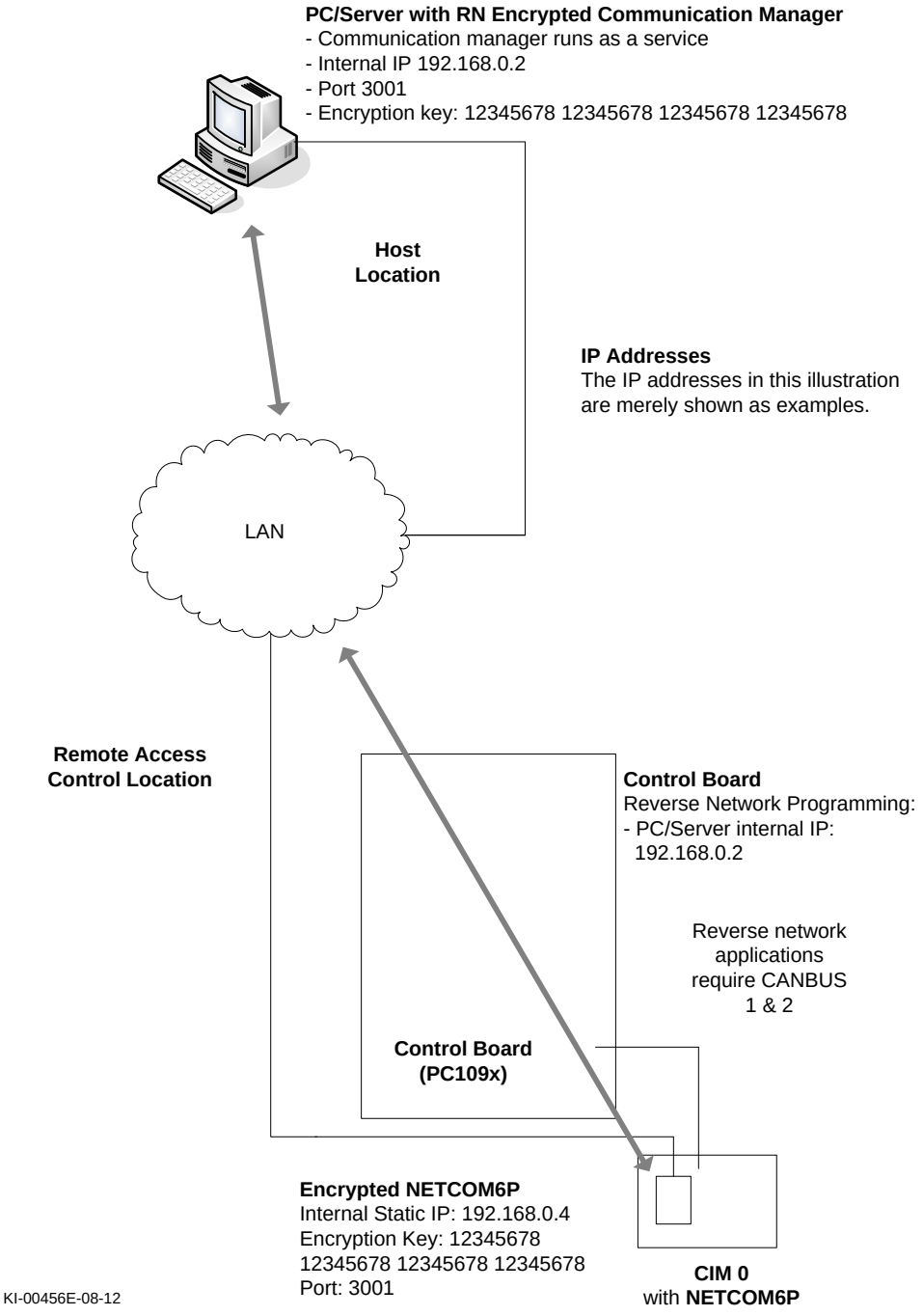


Figure 2 – LAN with no public exposure



Before You Start

Setting up the AUR-RN license for reverse network communication requires setup procedures at the host location on the following pages. Ensure that you have the following components and that you have coordinated settings with the technician installing the hardware at the remote location as outlined in Installation Coordination – Host & Remote Locations on page 3.

Host Location

- Verify you have the necessary parts outlined below
- Ensure that you have coordinated settings with the technician at the remote location
- Ensure that you have the serial # of the designated reverse network control board
- Register the AUR-RN License
- Install Reverse Network Encryption Communication
- Configure the Client with an encryption key
- Verify the reverse network communication service is running
- Ensure the server with the Reverse Network Encryption Communication software has a network path to the remote location NETCOM6/control board – coordinate with the network administrator

AUR-RN (Reverse Network) Parts List

Verify the AUR-RN license package contains the following items:

- AUR-RN License Number

Depending on the AUR-RN license purchased, you may establish the following reverse network IP address connections:

- AUR-RN1 – one reverse network IP connection
- AUR-RN5 – five reverse network IP connections
- AUR-RN10 – ten reverse network IP connections

AUR-RN Requirements

The AUR-RN license requires the following software:

- Aurora – version 1.0.1.0 or higher

Please note that Aurora is only compatible with PC109x control boards with firmware version 9.20 or higher. The PC109x control board may require a firmware upgrade chip.

AUR-RN License Registration

Please refer to one of the following sub-headings for registration. Until you register the AUR-RN license, the reverse network communication application will not run.

New Installation

For a new installation, install the Aurora software using the Aurora Installation DVD. Ensure that you install the

If this is a new installation, follow the instructions in the Aurora Client help for installation and software registration instructions before you begin to follow the AUR-RN setup instructions in this guide. Open the Client module; press the F1 key to access the help.

For registration instructions, select the Contents tab > Software Registration > How to Register Aurora. Follow the registration instructions.

For general setup procedures, select the Contents tab > Basic Setup > Basic Site Setup Procedures and click on the links outlined in the topic. When you have completed setting up your site, return to this guide for configuring the AUR-RN license starting on the next page.

Existing System

If you have an existing registered version of Aurora, and have purchased an AUR-RN license for Keyscan's reverse network communication, you only have to register the AUR-RN license. For registration instructions open the help form the Aurora Client software by pressing the F1 key, select the Contents tab > Software Registration > How to Register Aurora. Follow the registration instructions.

AUR-License – Setup Procedures

To setup the AUR-RN license for reverse network communication at the host location follow the all procedures as outlined on the succeeding pages.

Install the Reverse Network Communication

The reverse network communication must be installed on the server that communicates on the network with the NETCOM6/access control board at the remote location.

If you previously installed the reverse network communication, you can by-pass these procedures. If you are unsure, see Verify Reverse Network Communication Is Running below.

Steps to Install Reverse Network Communication

1. Before commencing, close any open applications including anti-virus programs.
2. Insert the Aurora Software DVD in the DVD drive.
3. From the Keyscan Aurora Installation screen, select Reverse Communication Installation button and follow the on-screen prompts.
4. When you have completed the installation, click on the red x in the upper right corner of the Keyscan Aurora Software Installation screen.
5. Remove the DVD from the drive.
6. If you closed an anti-virus application, you can now re-open it.

Firewalls & Network Filtering

Ensure that any firewalls or network filtering allow inbound communication on the PC that is receiving communication from the access control units.

Verify Reverse Network Communication Is Running

When the Aurora reverse network communication service was installed, it was automatically configured to start. However, if you wish to verify that the reverse network communication service is running review the steps below.

Verify Reverse Network Communication Service

To verify that the reverse network communication is running as a service in Windows, follow the steps below.

1. Select Start > Control Panel > Administrative Tools.
2. From the Administrative Tools window, select Services.
3. From the Services window, scroll down and double click on KeyscanAuroraReverseCommunications.
4. Ensure that Started is displayed opposite Service Status.
   - If the KeyscanAuroraReverseCommunications is stopped, click on the Start button.
   - If the the KeyscanAuroraReverseCommunications service is not listed in the Services screen, verify that the application has been installed.

5. If you made any changes, click on the OK button to exit. If you did not change any settings, click on the Cancel button to exit.
6. Close the Control Panel screens by clicking on the x in the upper right corner.

Create a User-Defined Encryption Key

This procedure is performed at the server used for operational communication with the NETCOM6/ACUs.

You will enter a user-defined encryption key. The same encryption key is also required at the remote location where the NETCOM6 is programmed by the installing technician. Be sure to record the encryption key and confirm with the installing technician that you are both using the same encryption key with the same bit setting.

About the Encryption Key

The encryption key must consist of 32 characters (AES 128 bit), 48 characters (AES 192 bit) or 64 characters (AES 256 bit). Characters can be as follows in any combination:

- alpha A—F
- numeric 0—9
- example of 128 bit key — A91376F1 C3621FBC DD68917E 1006B167

Steps to Set an Encryption Key

1. From the Aurora Client, select Settings > Application Utilities > Server Settings.
2. Select the symbol to the right of Communication Server and select the server where the reverse network communication service was installed.
3. In the Listening Port text box, port 3001 is entered by default. If another port is used, select 3001 in the text box and enter the correct port. The installing technician also must know this port.
4. Select the symbol to the right of Encryption Type and from the drop down list, click on the encryption type as noted above.
5. In the Encryption Key text box, enter an encryption key. Enter the appropriate number of characters depending on the bit setting:
   - NETCOM Encryption Key AES 128-bit — 32 characters
   - NETCOM Encryption Key AES 192-bit — 48 characters
   - NETCOM Encryption Key AES 256-bit — 64 characters
6. Click on the Save button.
7. Click on the back button until returned to the Client main screen.

Configure Control Boards for Reverse Network

When configuring the access control units in the Hardware Setup screen, note the following required settings:

- Communication is set on Reverse Network
- If more than 1 access control unit is on a communication bus, other than the master control board that has been programmed with the IP address of the host location and is connected to the NETCOM6, ensure that all other control boards specify the serial number of the master access control unit in the Master Access Control Unit field.

- If specifying more than 1 IP address in the Receiver Comms IP address field, use a dash – between the two IP addresses as shown in the following example
    - Example of 2 IP addresses: 192.168.100.12–192.168.100.18

Steps to Configure the Control Boards for Reverse Network

These procedures only cover adding an access control unit(s) to an existing site. If you require help setting up a site, press F1 on the keyboard to open the help. Select the Contents tab, Basic Setup > Basic Site Setup Procedures. Select the links and review the topics.

These procedures are performed from the Aurora Client.

Please remember that you are restricted in the number of connections you can make based on your Reverse Network license agreement.

1. Open Aurora and log in.
2. From the Client main screen, select the Site Management button menu > Hardware Setup.
3. If you have multiple sites, select the appropriate site from the Site Search – Hardware Setup directory screen.
4. From the Hardware Setup screen, select the symbol on the right side of the Add 8 Door Controller button.
    - By default, Add 8 Door Controller is listed. However, while the Hardware Setup screen is open, the Add … button lists the last type of hardware component selected.
5. From the drop down list, select the type of ACU control board you are adding.
6. From the Confirm Hardware Installation prompt, click on the Yes button.
    - If you have selected the wrong control unit series, click on No, and click on the Add …. Button. Remember the Add button lists the last series selected.
7. By default the Client software populates the Name field with Access Control Unit # 1. Each time you add a control unit the number increments by 1. You can leave the default name format (recommended) or change it. If you change it however, Keyscan recommends you retain a consistent naming format for all control units.
8. In the Serial Number text box, enter the access control unit serial number.
9. In the Password text box, you can leave the default password of KEYSCAN or if you elect to change it, the password has a maximum of eight characters. If you change the password, be sure to write it down and store it in a safe place. In the event you have to perform a disaster recovery at a later date to recover on-board data, without the password, you cannot communicate with the control board or access the data.
10. Opposite Status, leave the default setting on Active.
11. Click the symbol on the right side of the Regional Time Zone and select the time zone from the drop down list where the access control unit is located.
12. In the Hardware Notes text box, enter a brief description where the access control unit is physically located.
13. Opposite the Communication heading, select the symbol on the right and from the drop down list select Reverse Network.
14. Do one of the following steps:
    - If this is the control board that is designated as the master control board – it is connected to the NETCOM6 and has been programmed with the IP address of the host location, leave the Master Access Control Unit field on Not Assigned and go to the next step.
    - If this is a control board other than the master control board on the same communication bus, click on the symbol and select the serial number of the control unit designated as the master.

15. In the Receiver Comms IP text box, enter the IP address of the server which has the Reverse Network Communication installed.
16. If a secondary IP address exists with a connection to the server which has the Reverse Network Communication installed, you can specify the address in the Failure Comms IP text box.
17. Enter the computer name of the server with the Reverse Network Communication if it is other than the unit currently displayed in the Communications Server field.
18. Click on the Save button.
19. To add another access control unit, repeat the above steps.
20. Select the Back button to return to the main screen or the history navigation button for a previously viewed screen.

Verify Communication with the Remote Location

After you have installed and configured the Keyscan software for reverse network communication, Keyscan recommends contacting the installing technician at the remote location and verifying that the hardware has been installed, configured and connected.

When you have confirmed the hardware is operational, Keyscan suggests remaining in communication with the installing technician while you verify whether you have established communication with the remote location. The installing technician's documentation also includes how the control board System Status and Communication Status LEDs appear when communication is successful or unsuccessful.

1. From the Client main screen, select the Status button > Status.
2. From the Status screen, select Access Control Unit Status.
3. From the Access Control Unit Status screen, click on the  symbol on the box in the upper right corner of the screen and select the site from the list.
4. In the table, locate the row or rows with the access control units at the remote location.
5. Observe the Status column and the Communication Error Count:
   - If Status = Active / Communication Error Count = 0 communication is established
   - If Status = Inactive / Communication Error Count = 19 communication has been lost. See Troubleshoot Communication Issues.
6. Confirm with the installing technician if you have communication with the remote site or if necessary review the Troubleshoot Communication Issues to resolve potential communication difficulties.
7. Close the Access Control Unit Status & Status screens by clicking on the x buttons.

Troubleshoot Communication Issues

If communication difficulties arise, review the check list below to eliminate some of the more common installation errors. Review the host location list and ask the installing technician to review the hardware connections and program settings.

Host Location

- Has the Reverse Network license been registered?

- Has the correct listening port been specified
- Is the host location running the reverse network communication service
- Has the host location entered the same encryption key in the Application Utilities screen in the Client software?
- Does the host location have a valid network path from the server with the encrypted reverse network communication via any router/end points to the NETCOM6/control panel including the correct port settings for inbound and outbound communication?

Remote Location

- Are all jumpers or DIP switches on the control board properly configured?
- Are all wire connections at the terminal blocks correct?
- Has the NETCOM device been programmed with the correct IP address, gateway if required, and port settings?
- Has the NETCOM been programmed with the same encryption key that was specified at the host location?
- Has the control board been programmed with the correct host-location IP address?
- If the remote location has a router or end-point device, have the correct port settings been specified for inbound communication from the host and outbound communication to the host?

Control Board Communication Status LEDs

At the remote location, the control board has Communication Status LEDs which indicate whether or not a network connection has been established with the host location's server with the reverse network communication service. The table below outlines the Communication Status LEDs for the various series of control boards. Confer with the installing technician to verify the current status of the communication LEDs to determine if you have a valid network connection.

Table 2 – Control Board Communication Status LEDs

Control Board	Communication Status LEDs	LED State – Communication	LED State – No Communication
CA150	RD2 – Receive data	Frequent flashing	Inactive
	TD2 – Transmit data	Frequent flashing	4x on a call out/minute
CA250B, CA4500B CA8500B	RD4 – Receive data	Frequent flashing	Inactive
	TD4 – Transmit data	Frequent flashing	4x on a call out/minute

Important

You may require the services of a network administrator to resolve network issues and ensure the server with the encrypted reverse network communication manager at the host location has a valid path and connectivity to the NETCOM6/control board at the remote location.