ISONAS™

PURE IP ACCESS CONTROL

Knowledge Base Article

Connecting Devices to Pure Access

Table of Contents

Document Version

(KBA0201PureAccessConnections.Docx)

Date of Revision	Revision	Author	Description
8/9/2016	**1.0**	**Jason Clement**	**Initial Release**
12/5/2017	**1.1**	**David Tamarchenko**	**Update: Add by IP and Show Reader Info**
1/18/2017	**1.2**	**MS**	**Add by IP Range**
8/16/2018	**1.3**	**MS**	**Advanced Connectivity**

1: INTRODUCTION

This knowledge base article will review how to connect ISONAS devices to Pure Access Cloud. These devices will initiate a connection from inside the network out to Pure Access. For those familiar with DBCrystal this is the opposite of how devices were configured. In addition, ISONAS has added a new tool to make this addressing streamlined and easy for the installer.

2: PLANNING AND CONFIGURATION

2.1: Network Configuration

2.1.1: IP Addressing

The recommended setting for ISONAS devices connecting to Pure Access is DHCP. When using DHCP ensure that the DHCP has the correct default gateway and DNS address configured. These settings are critical for the device to connect outside the network (gateway) and to resolve the Pure Access address to an IP address (DNS).

Static addresses can be used with ISONAS devices connecting to Pure Access. When assigning static addresses ensure all of the following items are configured with the correct address:

1. IP Address
2. Subnet Mask
3. Gateway
4. DNS Address

2.1.2: Firewall

When connecting ISONAS devices to Pure Access the device (client) initiates the connection to Pure Access. This setting is "Client Mode" for ISONAS devices (see figure 3 on next page). Since the device initiates the connection out to Pure Access minimal firewall configuration is needed. If your firewall is blocking outbound ports or ephemeral ports (see description below) then rules may need to be added to the firewall to ensure a connection can be made.

RC-03 and RC-04 devices will initiate a connection on port 55533 and Pure Access will use an ephemeral port to complete the connection.

PowerNet™ IP-Bridge devices will initiate a connection on port 55533 and Pure Access will use ports 10001-10003 to complete the connection. IP-Bridges come in either two or three door units. For a two door unit ports 10001 and 10002 will be used, for a three door unit the same ports are used in addition to 10003.

An ephemeral port is a random port used to complete a TCP connection for the session. This is typically a random port between 49152 and 65535. The port number is used only for that connection period and will change if the connection is reset. ***In most cases this is not an issue unless severe security restrictions are placed on a network.***

Figure 1 - RC-03 Example Connection

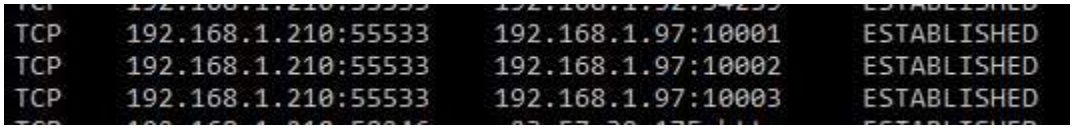


Figure 2 – IP-Bridge Example Connection

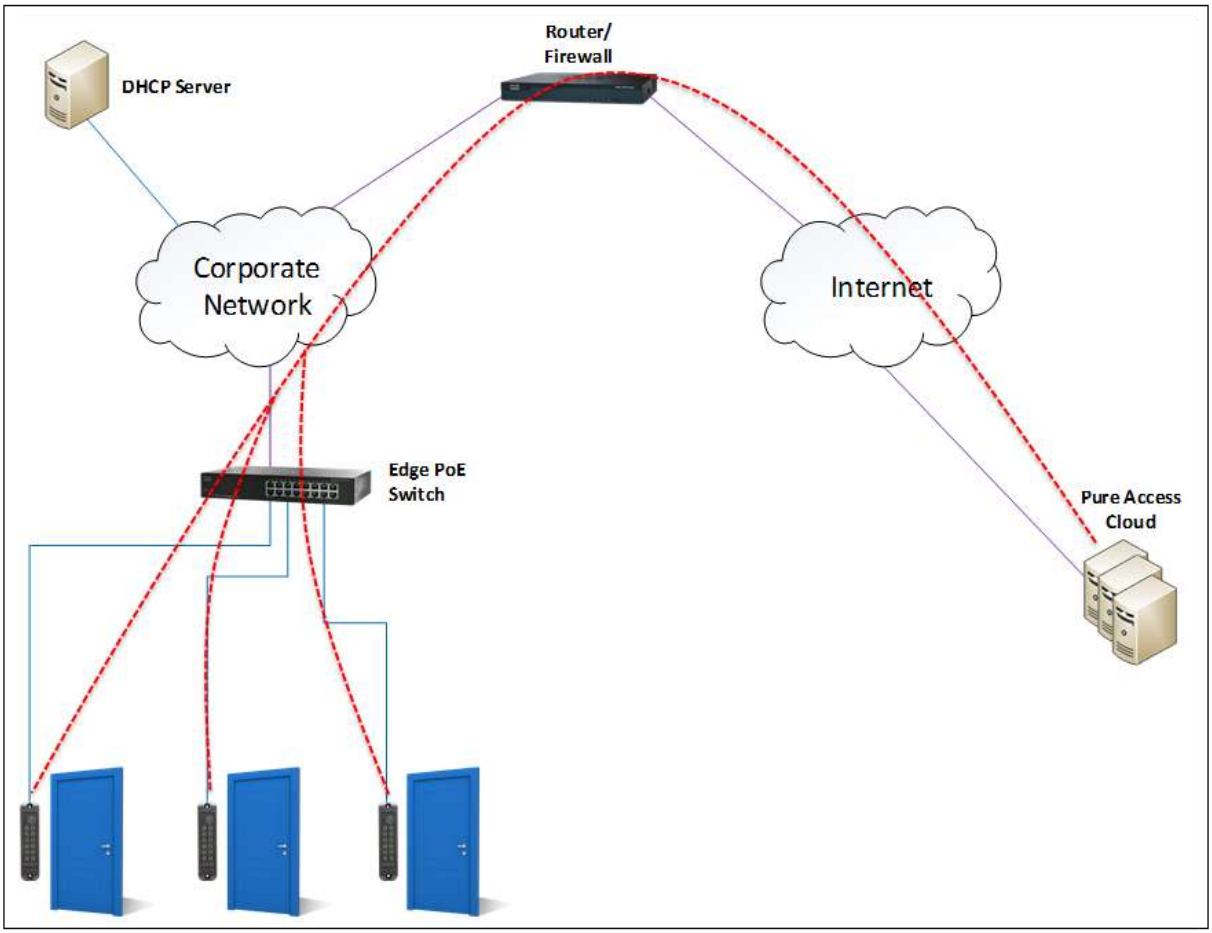


Figure 3- PowerNet Connections

2.1.3: Multiple NAT/Firewall Configurations

Tech Tip!

Configure your devices in your shop before installing them on site. This will allow for easy install and easier troubleshooting if devices do not connect.

Multiple NATs are strongly discouraged as they can cause communication issues for the ISONAS devices. Multiple Firewalls are also strongly discouraged for the same reason. If these must be used for security purposes, ensure that all rules are configured properly and that the IP address and Ports are free to communicate through the multiple layers of Firewall and/or NAT.

2.2: CONFIGURING ISONAS DEVICES

2.2.1: Configuration Tool Overview

The Configuration Tool is a program that allows an installer to configure ISONAS devices. It broadcasts out on the local network to find these devices. Once they are found, the devices can then be configured to connect to Pure Access. The IP addressing method is configured with this program as well. In addition, integrators can test the network configuration to ensure the network environment is properly configured and ready to add ISONAS devices.

2.2.2: Using the Configuration Tool

First simply download the Configuration Tool from the ISONAS website www.isonas.com under the **Quick Links** section on the homepage. Run the application (see figure 4 on next page). Clicking on "Discover Units" will find any ISONAS devices on the local area network.

2.2.3 Advanced Connectivity Tests

Clicking on "Connection Test" will run through a series of network tests to determine if the network segment that the Configuration Tool is running on can make a connection to Pure Access. The following tests will be run:

Test 1: Pings the specified DNS server (Google DNS by default) 4 times and averages the response time to confirm DNS connectivity

Test 2: Finds routing info for ISONAS Pure Access Cloud using the specified DNS server (Google DNS by default)

Test 3: Tests connectivity to ISONAS Pure Access Cloud by pinging the environment 4 times and averaging the response times.

Test 4: Simulates a device connection by ensuring a simulated ISONAS reader can make a connection to Pure Access through port 55533.

As these tests are completed you will see a pass or fail result. You can then select "export report" to see the details results and recommendations on how to correct failures. From here connect with your onsite network representative to make the appropriate adjustments to the network settings.

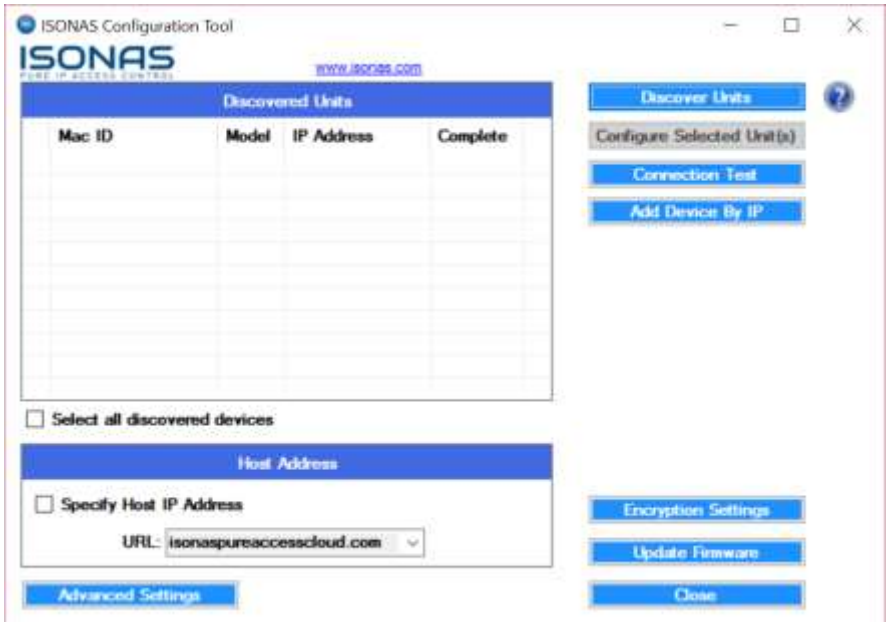


Figure 4 - Configuration Tool

After finding the devices on the network we can now proceed to configuring these devices. Clicking on "Advanced Settings" will bring up the options needed to fully configure these devices. After clicking on this option there are now two available options. The first setting allows you to change how the device connects and the second will set either DHCP (preferred and default) or static (see figure 7 on page 7).

If no devices show up or you do not see all devices, check the following items:

1. Verify that all devices are powered up and fully booted. A fully booted RC-03 will have the top LED on with a color of red. A fully booted IP-Bridge will have the top left LED on with a color of green. See figures 5 and 6 on the next page.
2. Verify that the windows PC the Configuration tool is running on is connected to the correct network and has a valid IP address for that network.

3. Ensure that all devices are on the same subnet and network. The Configuration Tool uses broadcast packets on the network to find the devices. Broadcast traffic is dropped by routers so only devices on the network segment the Configuration Tool is running on will be seen.
4. If using VLAN's verify with the IT Administrator that all the switch ports devices are plugged into are on the correct VLAN.

Figure 5 – Fully Booted RC-03

Figure 6 – Fully booted IP-Bridge

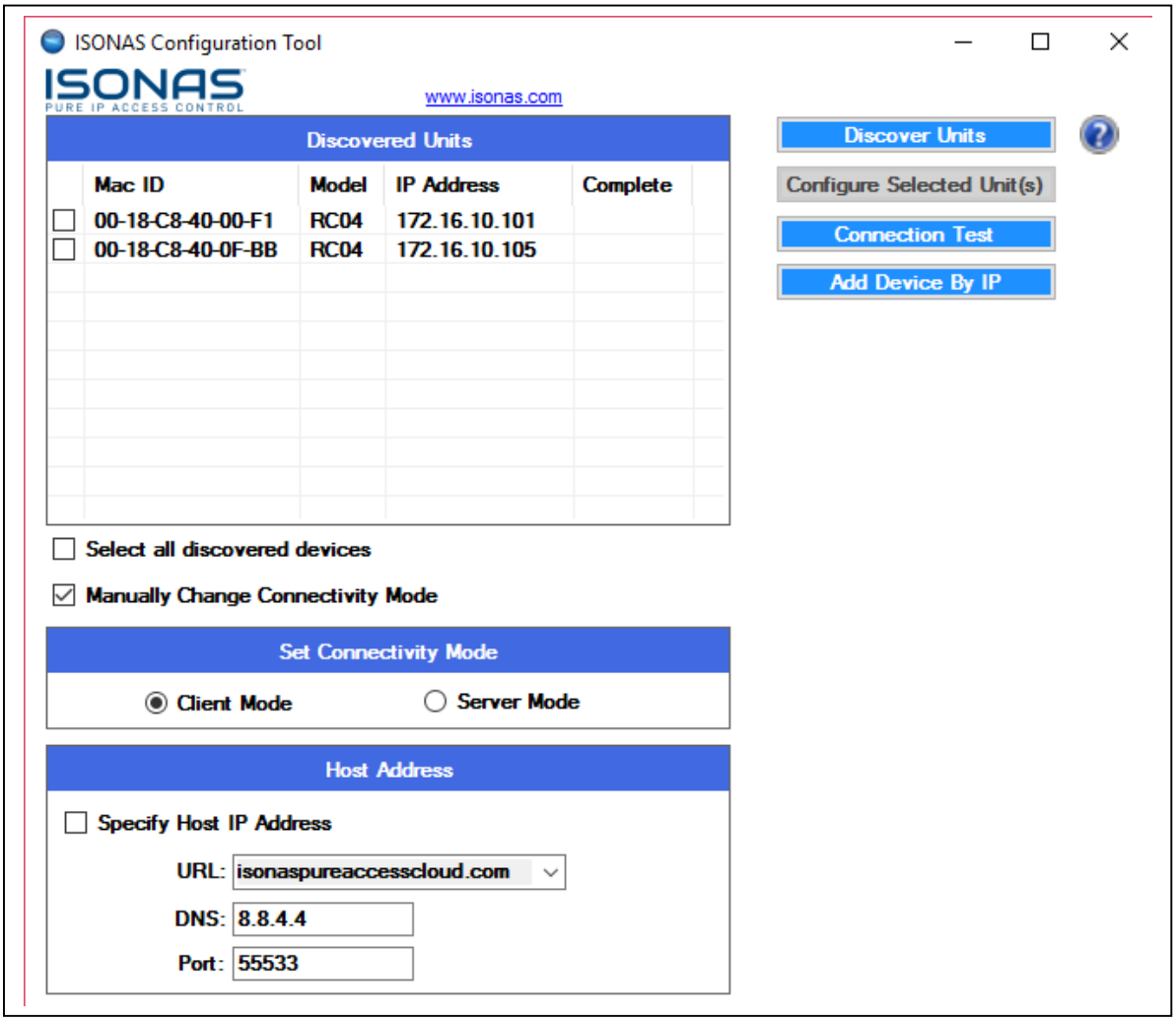


Figure 7 - Configuration Tool Advanced

All devices must be set to "Client Mode". This configures the device to initiate the connection out to Pure Access. The Host Address URL can be accessed via the dropdown menu. This will most likely be isonaspureaccesscloud.com though, if this is a demo system, it may be on isonaspureaccessdemo.com. The DNS should be left at default as this is a free Google DNS service provided. If this value is changed ensure it is a working DNS server.

All devices are set to DHCP by default. DHCP is the recommended IP addressing method for Pure Access™. If a static address is used ensure that all values are correct, especially the default gateway!

Once all values have been set highlight the device in the "Discovered Units" window and click "Configure Selected Unit". The "Complete" column should say Yes, the Configure button should have a green check mark next to it and the unit should reboot (see figure 8 below).

The "Configure all Units" option can be used unless static addresses are being assigned. When using static address units must be configured individually.

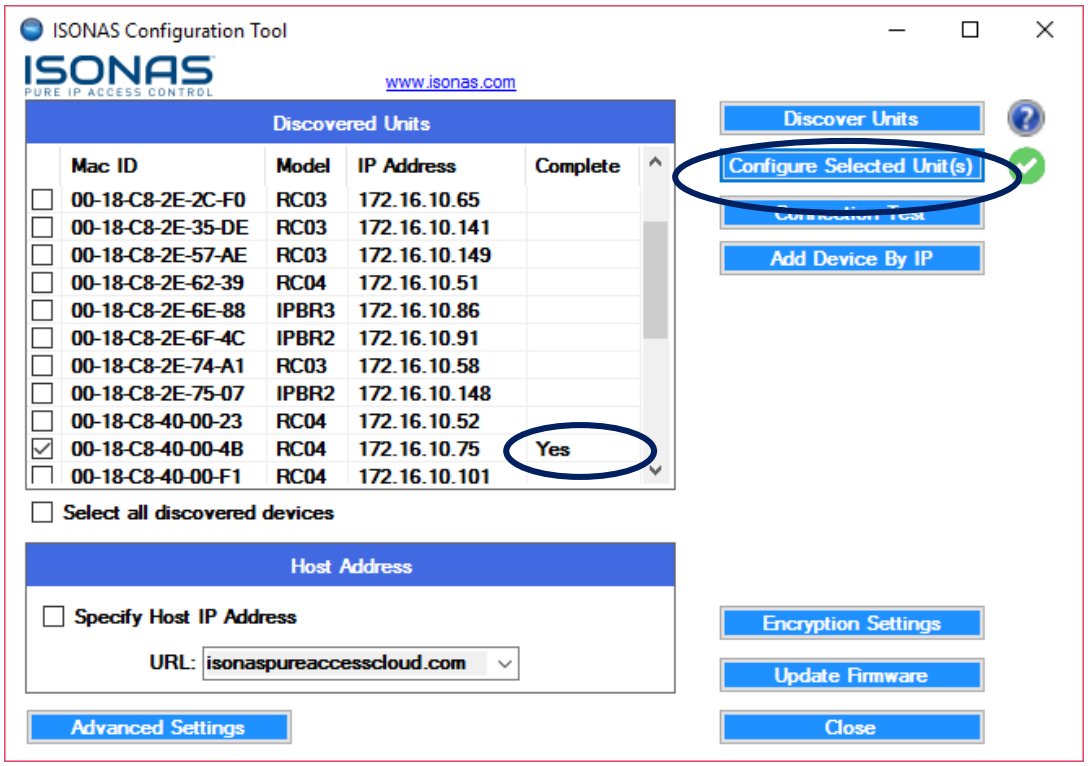
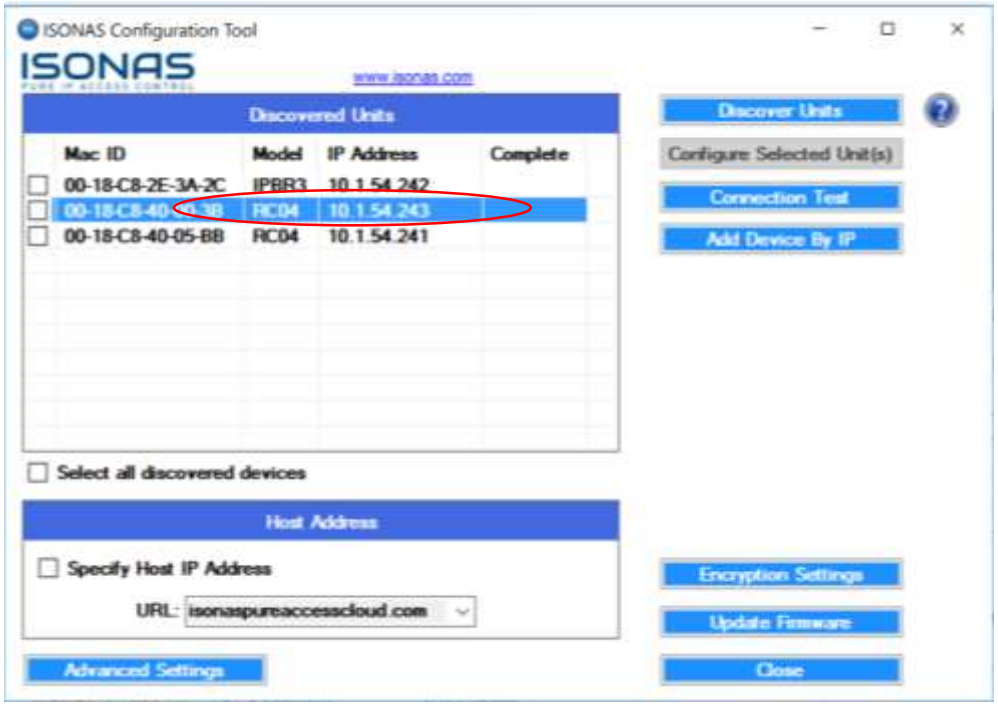


Figure 8 - Configure Selected Unit

From here your devices have been configured to point to Pure Access Cloud. The next step is to login to your Pure Access portal, register your software and begin adding your access points by using their MAC addresses. From here you can complete the configuration of your system!

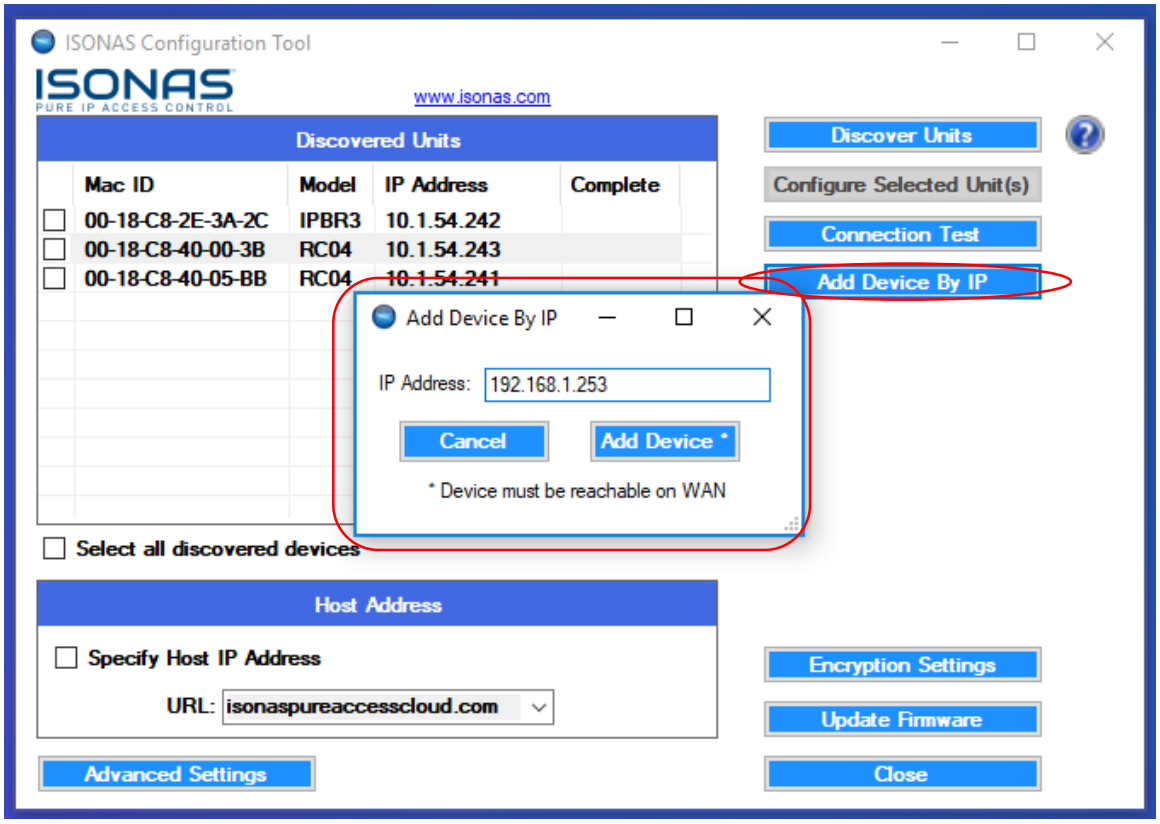
2.2.4 Reviewing Existing Settings on a Device

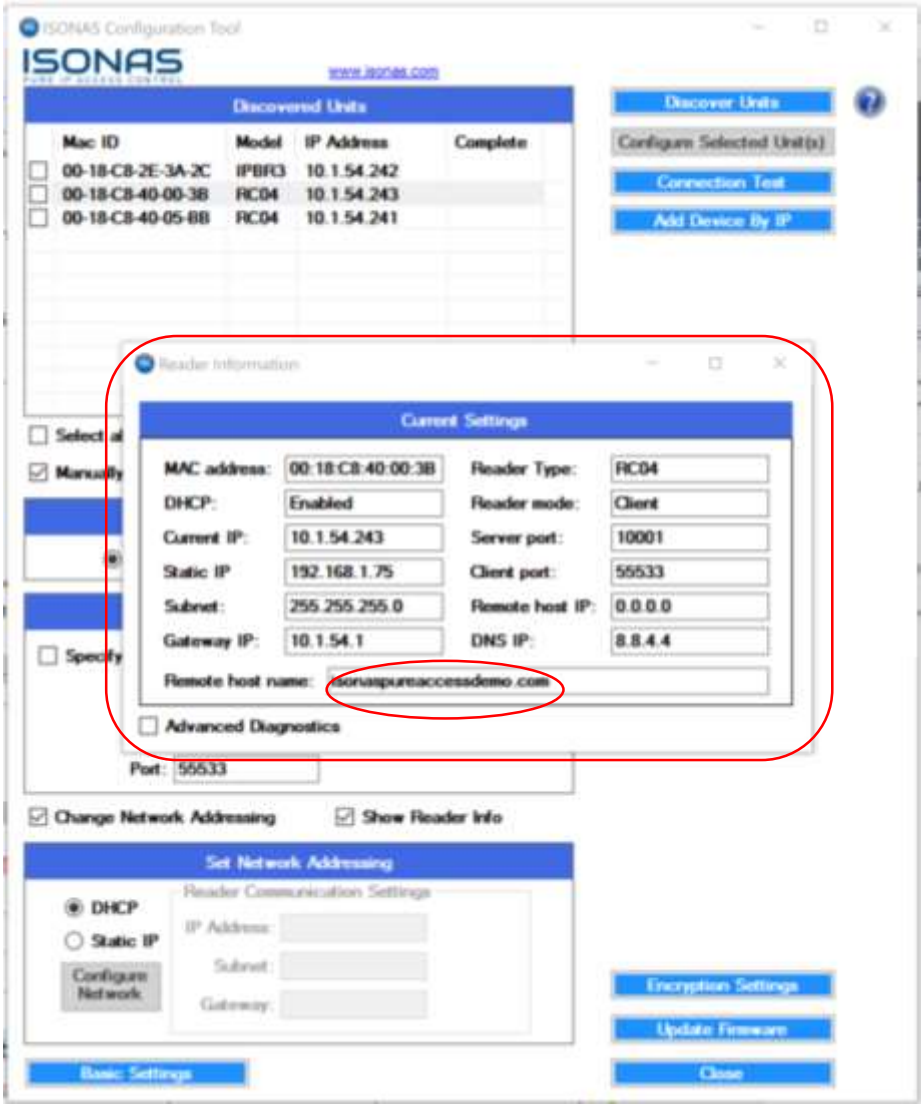
If you would like to see the current configuration of a device, you must discover the unit first and then you can highlight it in the discovered units field and click on "Advanced Settings". Once the "Show Reader Info" box is checked, a "Current Information" window will appear, and all current settings will be shown. This allows you to see if the settings require a re-configuration or not.



2.3 Configuring Access Points by IP Address or an IP Range

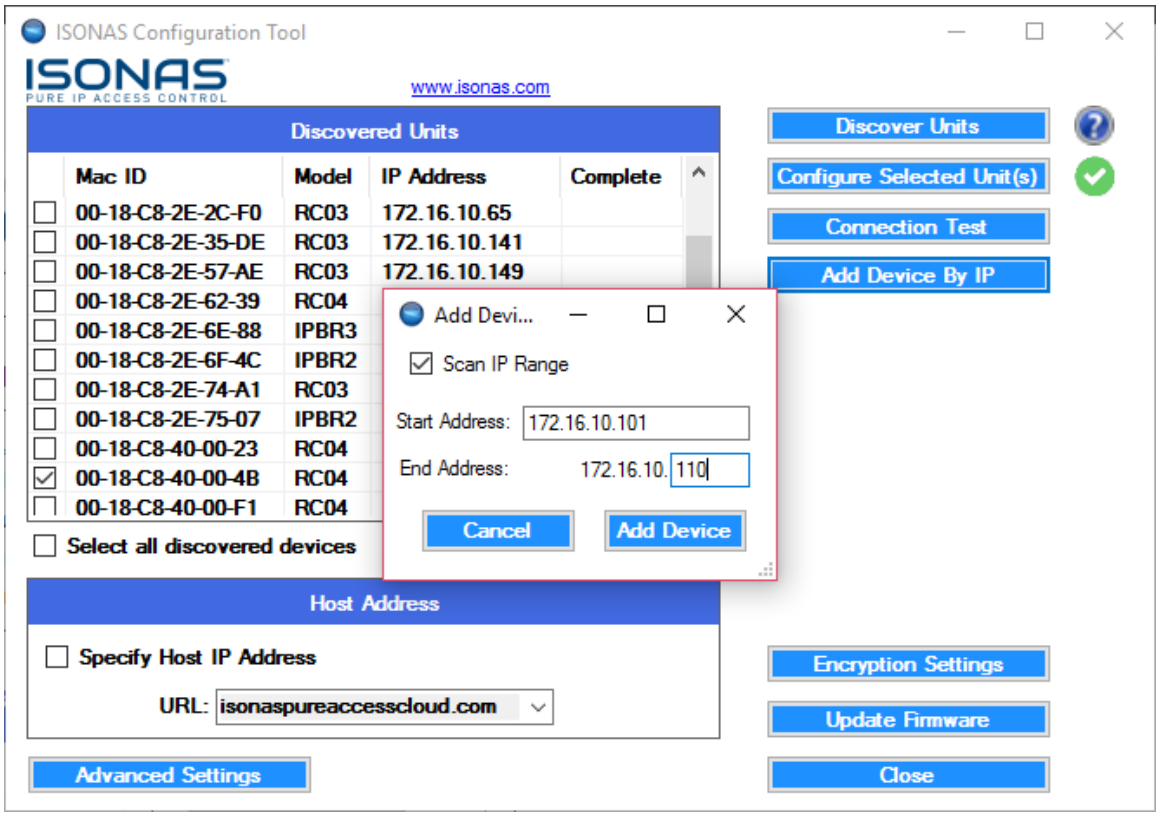
A second way to configure your devices is to connect to them directly, even across subnets. If the IP address of the device or devices is already known, and you can "ping" it on your network, you can click on "Add Device by IP" then manually enter one device at a time.


ISONAS Configuration Tool
ISONAS
PURE IP ACCESS CONTROL
www.isonas.com
Discovered Units
Mac ID
Model
IP Address
Complete
00-18-C8-2E-3A-2C
IPBR3
10.1.54.242
00-18-C8-40-00-3B
RC04
10.1.54.243
00-18-C8-40-05-BB
RC04
10.1.54.241
Discover Units
Configure Selected Unit(s)
Connection Test
Add Device By IP
Add Device By IP
IP Address:
192.168.1.253
Cancel
Add Device *
* Device must be reachable on WAN
Select all discovered devices
Host Address
Specify Host IP Address
URL:
isonaspureaccesscloud.com
Encryption Settings
Update Firmware
Advanced Settings
Close



2.3.1 Scanning an IP Range to Discover Devices

Another way to configure devices is to use the configuration tool to scan an IP address range.
Simply Select the Add Device by IP, then select the Scan IP Range check box. Enter the start address and the last octet of the end address and select add device.



From here you simply select the units that are discovered by selecting the check box or select all discovered devices and configure them to the appropriate url.

For more information on how to set up your access points, check out our YouTube channel for further details.

For more information:

Web: www.ISONAS.com **E-mail:** support@ISONAS.com

Tel: 800-581-0083 (toll-free) or 303-567-6516 (CO)

Fax: 303-567-6991

ISONAS Headquarters:

4750 Walnut Street, Suite 110, Boulder, Colorado 80301 USA