Installation, Operation, and Maintenance

Trane® Firewall Router Solution

⚠ SAFETY WARNING

Only qualified personnel should install and service the equipment. The installation, starting up, and servicing of heating, ventilating, and air-conditioning equipment can be hazardous and requires specific knowledge and training. Improperly installed, adjusted or altered equipment by an unqualified person could result in death or serious injury. When working on the equipment, observe all precautions in the literature and on the tags, stickers, and labels that are attached to the equipment.

July 2020

BAS-SVX069F-EN

Introduction

Read this manual thoroughly before operating or servicing this unit.

Warnings, Cautions, and Notices

Safety advisories appear throughout this manual as required. Your personal safety and the proper operation of this machine depend upon the strict observance of these precautions.

The three types of advisories are defined as follows:

⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It could also be used to alert against unsafe practices.
NOTICE	Indicates a situation that could result in equipment or property-damage only accidents.

⚠ WARNING

Proper Field Wiring and Grounding Required!

Failure to follow code could result in death or serious injury.

All field wiring MUST be performed by qualified personnel. Improperly installed and grounded field wiring poses FIRE and ELECTROCUTION hazards. To avoid these hazards, you MUST follow requirements for field wiring installation and grounding as described in NEC and your local/state/national electrical codes.

⚠ WARNING

Personal Protective Equipment (PPE) Required!

Failure to wear proper PPE for the job being undertaken could result in death or serious injury.

Technicians, in order to protect themselves from potential electrical, mechanical, and chemical hazards, MUST follow precautions in this manual and on the tags, stickers, and labels, as well as the instructions below:

- **Before installing/servicing this unit, technicians MUST put on all PPE required for the work being undertaken (Examples; cut resistant gloves/sleeves, butyl gloves, safety glasses, hard hat/bump cap, fall protection, electrical PPE and arc flash clothing). ALWAYS refer to appropriate Safety Data Sheets (SDS) and OSHA guidelines for proper PPE.**
- **When working with or around hazardous chemicals, ALWAYS refer to the appropriate SDS and OSHA/GHS (Global Harmonized System of Classification and Labelling of Chemicals) guidelines for information on allowable personal exposure levels, proper respiratory protection and handling instructions.**
- **If there is a risk of energized electrical contact, arc, or flash, technicians MUST put on all PPE in accordance with OSHA, NFPA 70E, or other country-specific requirements for arc flash protection, PRIOR to servicing the unit. NEVER PERFORM ANY SWITCHING, DISCONNECTING, OR VOLTAGE TESTING WITHOUT PROPER ELECTRICAL PPE AND ARC FLASH CLOTHING. ENSURE ELECTRICAL METERS AND EQUIPMENT ARE PROPERLY RATED FOR INTENDED VOLTAGE.**

©2020 Trane

⚠ WARNING

Follow EHS Policies!

Failure to follow instructions below could result in death or serious injury.

- **All Trane personnel must follow the company's Environmental, Health and Safety (EHS) policies when performing work such as hot work, electrical, fall protection, lockout/tagout, refrigerant handling, etc. Where local regulations are more stringent than these policies, those regulations supersede these policies.**
- **Non-Trane personnel should always follow local regulations.**

Copyright

This document and the information in it are the property of Trane, and may not be used or reproduced in whole or in part without written permission. Trane reserves the right to revise this publication at any time, and to make changes to its content without obligation to notify any person of such revision or change.

Trademarks

All trademarks referenced in this document are the trademarks of their respective owners.

Revision History

- Update to terminology: Tracer SC replaced with Tracer BAS controller.

Table of Contents

Overview 6
- Purpose 6
- Background 6
- Trane Firewall Router Solution 6
- Place a Digi Transport WR21 Firewall in Front of the Tracer BAS Controller 6

Project Planning 8
- Choosing the Appropriate Firewall Router Kit 8
  - Internal Mount Kit (Part# WR21-NOCELL-TRANEKIT-INTERNAL) 8
  - External Mount Kit (Part# WR21-NOCELL-TRANEKIT-EXTERNAL) 8
- Project Development Tools 8

Qualifying Your Customer Site 11

Configuration Requirements 12
- Determine the IP addresses Before Configuring the Digi WR21 12
- WR21 Ethernet Configuration 12
  - Connecting to the WR21 12
  - Configuring the WAN Interface of the WR21 13
  - Configuring the LAN Interface of the WR21 14
  - Configuring the Firewall 15
  - Configure a Tracer BAS Controller with a New IP Address 16
  - Physical Connections 17
- Configuring Trane Connect Remote Access 18
- Test the Connectivity to the Trane Cloud 18

Firewall Router Order Process 19
- Register with INS 19
- Accessing the INS Online Store 19
- Selecting Firewall Router Items 19
- Individual Components 20
- Submitting an Order 21
- Order Confirmation 21

Installing the Firewall Router 22
- Internal Kit Installation 22
- External Kit Installation 22

Customer Remote Access Configuration 23
- Tunnel Negotiation 23
- PPP Connection Configuration 23
- Firewall Configuration 25

Pre-shared Key and Account Creation 25
VPN Client Configuration for iPhone/iPad Connection 26
VPN Configuration for Microsoft® Windows 7 Operating Systems 27
VPN Configuration for Android Operating Systems 31
Setting Up Remote Access For Customers 35
Setting Up Trane Connect Remote Access 35
Registering a Tracer BAS Controller or Tracer Concierge with TIS Command Center 35
Modifying a Previously Registered Tracer BAS Controller. 36
Customer Admin Initial Account Creation 38
Logging in to Trane Connect 41
Creating Additional Trane Connect Users 41
Configure the LAN IP Address on a PC 44

Overview

Purpose

The purpose of this document is to help you prepare, select, order, implement, and support a standard firewall solution for secure remote access. This document describes how to determine the appropriate Trane Standard Firewall installation type, as well as installation instructions for each kit to achieve secure remote access for both Trane and customers.

Background

Trane requires secure remote access to a customer's Tracer BAS for troubleshooting and diagnostics, and to update the Tracer BAS when needed. The preferred method for remote access is to use Trane Connect Remote Access. Trane recommends using Trane Connect Remote Access to securely connect to the Tracer BAS. Trane Connect Remote Access is built into many Tracer BAS controllers, including Tracer SC/SC+ and Tracer Concierge, allowing Trane technicians and customers to securely access their Tracer BAS while away from the office. Refer to the *Trane Connect Remote Access How-To Guide*, BAS-SVU22 for more details.

Trane's recommended best practice is to install Tracer BAS controllers behind the customer's firewall on the network (LAN/WAN), ideally with the assistance of the customer's IT staff. In some scenarios, a firewall already exists but is misconfigured; in other cases there is no firewall. A Digi Transport WR21 firewall, installed into the BAS network. provides an additional layer of security when other scenarios exist outside of the recommended best practices.

Trane Firewall Router Solution

Trane has created a standard solution, process, and support system for Trane offices to use when a Tracer BAS controller is directly exposed to the public Internet.

The Firewall Router solution is available in two pre-packaged kits:

- Kit #1 – An internal assembly designed for installation inside a medium or large Tracer BAS.
- Kit #2 – An external assembly designed for remote mounting.

Both kits contain all necessary components:

- Digi firewall router
- Mounting hardware, power supply or power connector
- Pre-configured firewall for easy installation and startup
- First year maintenance plan
- Trane Product support

Additional support includes:

- Online store (www.industrialnetworking.com/Trane)
- CSET blocks and estimator assemblies
- First year replacement program (RMA)
- Virtual Private Network (VPN) accounts for customer remote access

The Firewall router solution is delivered pre-configured. It ships directly to your office at pre-negotiated pricing from an online store that maintains firewall router supplies for Trane.

Place a Digi Transport WR21 Firewall in Front of the Tracer BAS Controller

Scenario:

Your customer's Tracer BAS has one or more IP ports (for example, HTTP, HTTPS, BACnet, SSH) that are "exposed" to the Internet and there is no IT staff to add or configure a firewall to block them.

Solution:

Place a Digi Transport WR21 firewall in front of Tracer BAS controller.

This solution can provide an additional layer of security when installed between the customer's network equipment and a Tracer BAS controller. The two figures below show the network before and after the Digi Transport WR21 firewall was installed.

Figure 1. Customer network prior to installation of Digi WR21Transport firewall

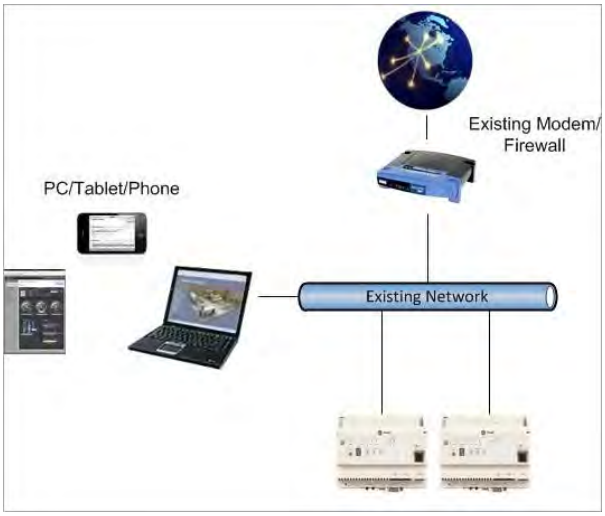
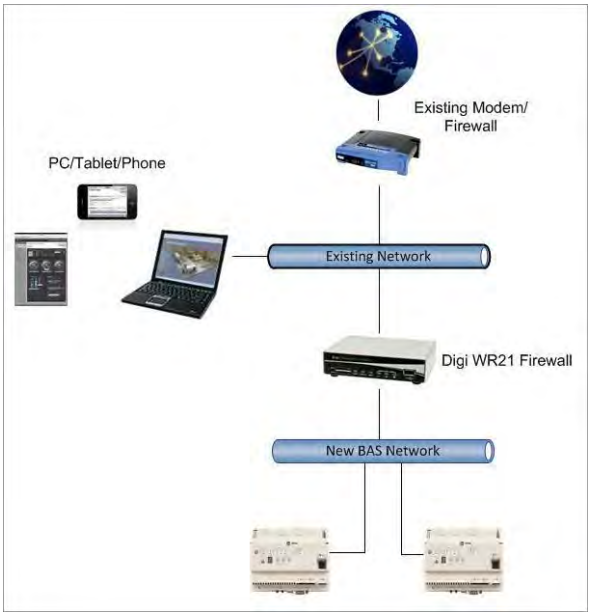


Figure 2. Customer network after installation of Digi WR21Transport firewall



Project Planning

Choosing the Appropriate Firewall Router Kit

Internal Mount Kit (Part# WR21-NOCELL-TRANEKIT-INTERNAL)

If there is room within the Tracer BAS enclosure, order the Internal Mount Kit. The firewall router must be installed inside the Trane enclosure or in close proximity to the enclosure.

Packaging includes:

- Firewall router
- DIN rail
- Locking barrel to wire power supply (wire to PM014)
- Ethernet patch cable (1 ft)

External Mount Kit (Part# WR21-NOCELL-TRANEKIT-EXTERNAL)

If there is no room within the Tracer BAS enclosure, or installation within the enclosure is not desired, order the External Mount Kit. The firewall router must be installed in close proximity to the enclosure.

Note: *Location must not be more than 300 ft from the Tracer BAS controller due to Ethernet cabling restrictions.*

Packaging includes:

- Firewall router
- 120V power supply ready to plug into an electrical wall outlet
- Ethernet patch cable (1 ft)

Project Development Tools

There are two tools that have been created to support the development of your projects: CSET Shapes and Estimator Assemblies. Estimator assemblies are provided for the Trane Firewall Router solution, which include both firewall router kits (see the following figures for examples).

Figure 3. Trane Estimator Assemblies for contracting projects

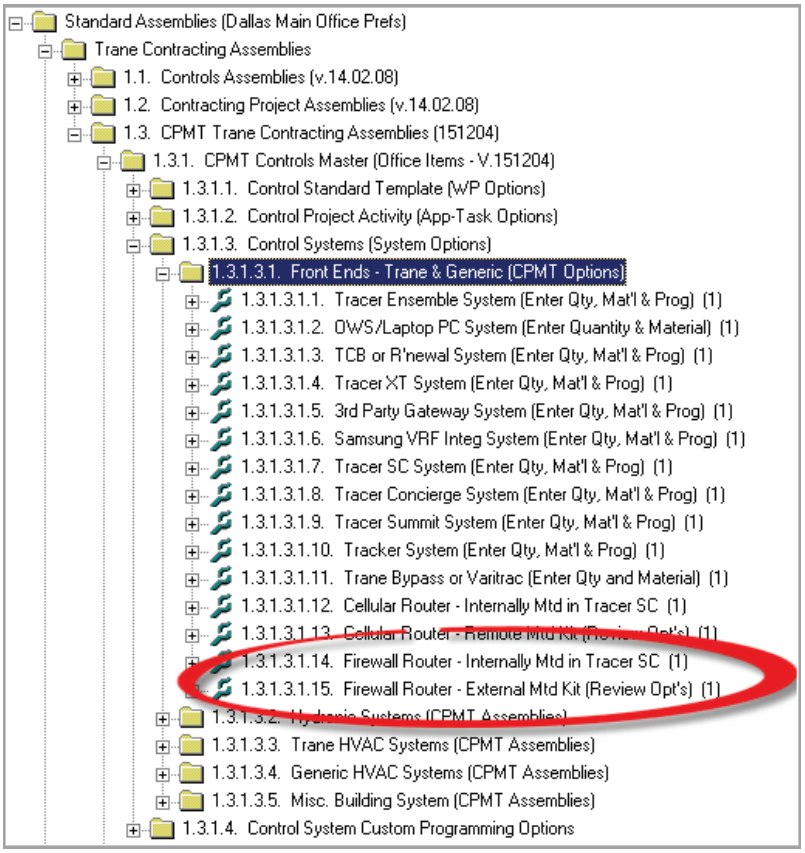


Figure 4. Trane Estimator Assemblies for service projects

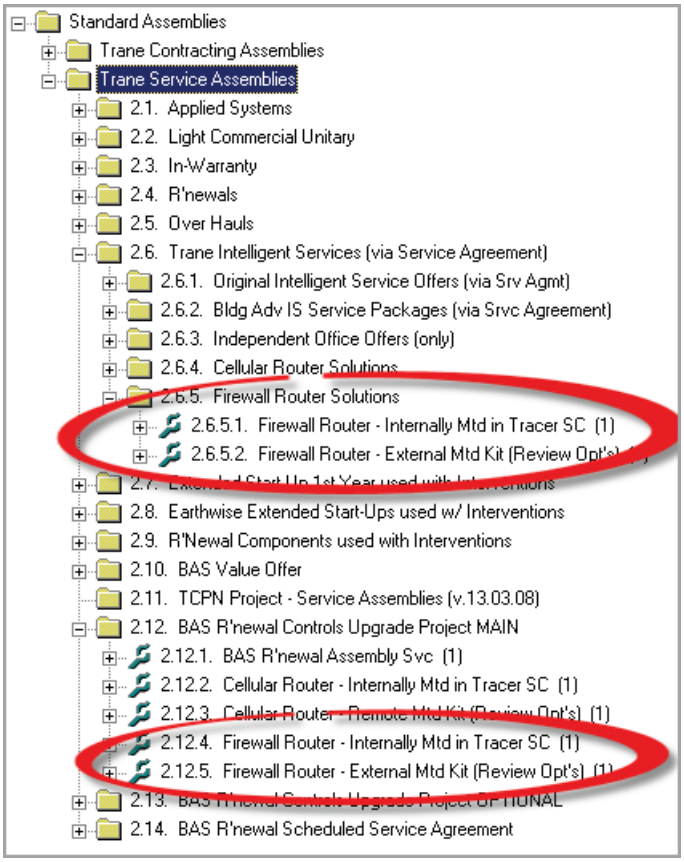


Figure 5. Firewall router assembly estimate (Internal Mount Kit)

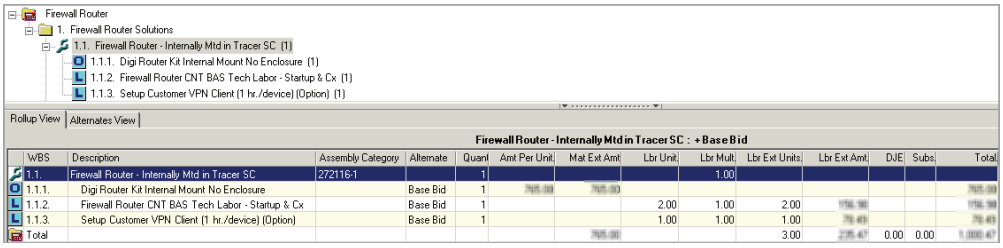
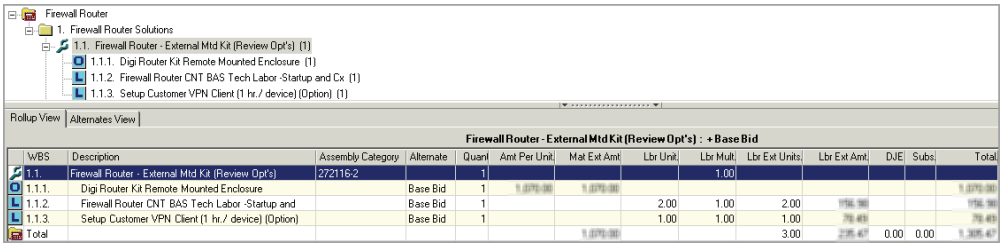


Figure 6. Firewall router assembly estimate (External Mount Kit)



Qualifying Your Customer Site

The following questions have been designed to assist you in determining whether the Digi Router firewall solution is appropriate for your customer.

Is the Tracer BAS on a "shared network" or an "isolated network"?

A shared network is one in which the Tracer BAS controller exists on the same network as other business related IT assets (for example, printers, PCs). An isolated network is one in which the Tracer BAS controller (and other BAS related devices) are isolated on another network from other business related IT assets.

If the Tracer BAS controller is on a shared network, careful consideration must be given to ensure that business related IT assets are not disrupted. To avoid this possibility, it is recommended that no changes be made to the existing networking equipment. This solution can be installed in front of the Tracer BAS to block the inbound ports.

Does the customer have an IT staff?

This solution is meant to be deployed when the customer does not have an IT staff. If your customer does have an IT staff and the Tracer BAS controller is on the customer's network you should communicate the proposed changes to existing network equipment to the IT staff in order to follow Best Practices.

Does your customer need remote access?

This solution is meant to block inbound IP ports to the Tracer BAS controller without making changes to existing network equipment. Trane Connect Remote Access is the preferred method for remote access for both Trane employees and customers. If needed, the Digi WR21 can be configured to allow customer remote access through VPN (L2TP/IPSEC). Some configuration changes may be required on the existing network equipment in order to facilitate this remote access.

Is there other equipment on this site that is communicating with the Tracer BAS controller?

All BAS communicating devices must be installed behind the Digi WR21 Firewall on the BAS Network in order for this solution to work. This includes Tracer BAS controllers, Tracer UC600s communicating through BACnet/IP, and non-Trane BACnet devices. If you cannot place all BAS communicating devices onto this BAS Network, this solution will not fit the needs of your project.

Configuration Requirements

Because every environment is different, the Digi WR21 will likely require some small changes to the configuration. This section will cover the initial setup of the router and the IP address changes necessary for the Digi WR21 and the Tracer BAS controller to match your installation.

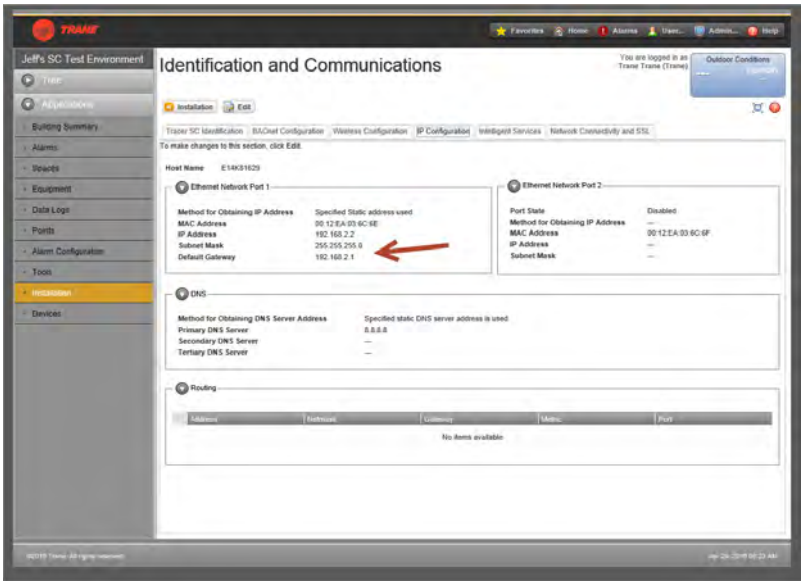
Determine the IP addresses Before Configuring the Digi WR21

1. Log into the Tracer BAS controller and then navigate to the IP Configuration page (**Installation>Identification and Communication>IP Configuration)**. Verify that the IP address is configured for whichever Ethernet port is connected to the Internet.
2. Determine if the relevant Ethernet port that Tracer BAS controller is utilizing is either a DHCP address or a static IP.

- If the Tracer BAS controller is configured to **Obtain IP Address Automatically using DHCP**, make a note of this for configuration of the Digi WR21.
- If the Tracer BAS controller is utilizing a static IP address, write down the IP address, Subnet Mask, Gateway and DNS addresses.

Example: In the configuration shown in the following figure, the IP address of a Tracer SC is 192.168.2.2, the subnet mask is 255.255.255.0 and the gateway is 192.168.2.1.

Figure 7. Tracer SC Identification and Communications



WR21 Ethernet Configuration

Connecting to the WR21

1. Connect a computer to LAN 1 of the WR21 router.
2. Update the computer's IP address to 192.168.209.20. Use 255.255.255.0 for the subnet mask. The default gateway and DNS IP addresses can remain blank. If you have questions on how to make these changes, refer to "Configure the LAN IP Address on a PC," p. 44.
3. Log into the router by entering 192.168.209.1 in the address bar of a web browser.

- Username: root
- Password: s27Fd^m9

Configuring the WAN Interface of the WR21

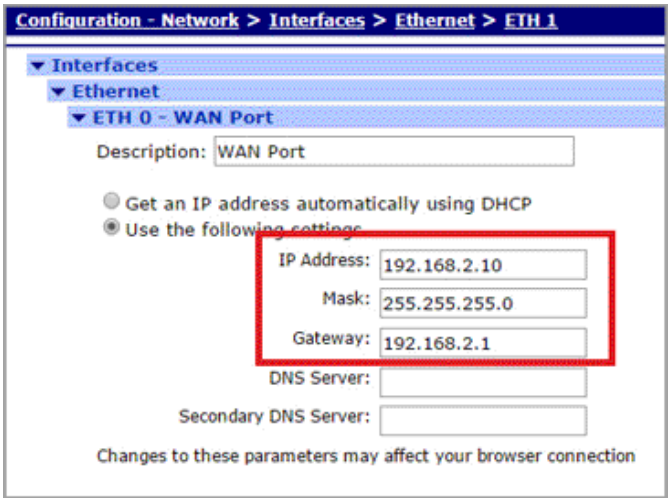
1. Click **Networks** in the left-hand menu.
2. Navigate to the Ethernet settings by clicking (in the right-hand window) on **Interfaces**, then **Ethernet**.

The first Ethernet port listed, **ETH 0**, is the WAN port (labeled LAN 0 on the physical device).

3. Click on **ETH 0 – WAN Port** to edit the configuration.

   Example: The following figure shows an IP address of 192.168.2.10, a subnet mask of 255.255.255.0 and a Gateway of 192.168.2.1.

Figure 8. ETH 0 (WAN Port) configuration



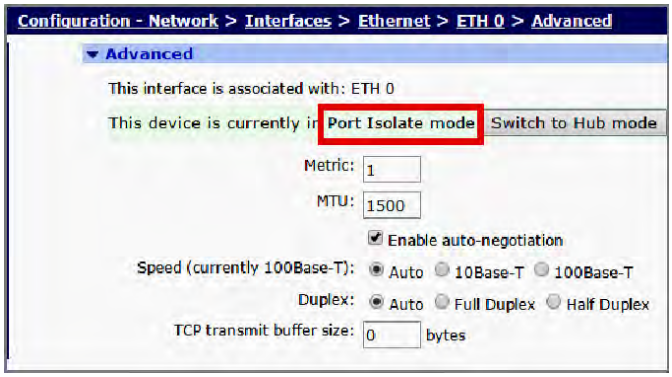
4. Using the settings obtained from the Tracer BAS controller in previous steps, enter the **IP Address**, **Mask**, **Gateway**, and **DNS Server** in the appropriate boxes.
5. If the Tracer BAS controller was configured to obtain an IP address automatically using DHCP, **ETH 0** should instead be set to **Get an IP address automatically using DHCP**.

Note: *ETH 0 and ETH 1 must have addresses on separate IP networks. The DIGI WR21 ships with* ***ETH 1 – Internal Network*** *configured to utilize the 192.168.209.0/24 (192.168.209.0-192.168.209.255) subnet. If this range is already in use on the customer network, you will need to follow the steps in the "Configuring the LAN Interface of the WR21" section below.*

6. Click **Apply**.
7. Expand the **Advanced** tab.

   The second line should read: **The device is currently in Port Isolate mode**.

Figure 9. ETH 0 (WAN Port) configuration (Advanced tab)



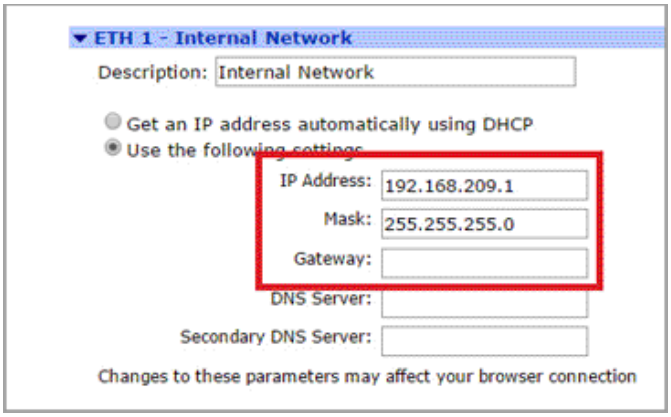
8. If the device is in Hub mode, click the **Switch to Port Isolate mode** button.
9. If the change in step 9 was required, click **Save Configuration**, which opens the **Save Configuration dialog**.
10. Click **Save All**. After the save operation is complete, reboot the WR21.

Configuring the LAN Interface of the WR21

1. The second Ethernet port listed, **ETH 1**, is the LAN port (labeled LAN 1 on the physical device). **ETH 1** will be physically connected to the Tracer BAS controller.

   Example: The following figure shows an IP address of 192.168.209.1, a subnet mask of 255.255.255.0 and no Gateway.

Figure 10. ETH 1 (LAN Port) configuration



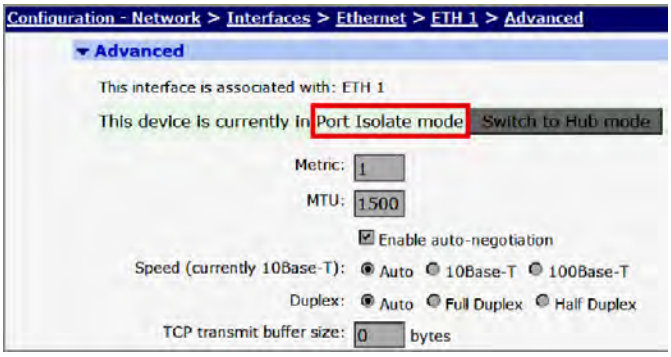
2. Click on **ETH 1 – Internal Network** to edit the configuration.
3. Enter a new IP address on a network not already in use. It is recommended that the last octet of the IP address remain .1 and that the subnet mask remain 255.255.255.0. The Gateway, DNS Server and Secondary DNS Server fields can remain blank.

Note: *If you have more than one device on your BAS Network, you will need an external Ethernet switch as there is only one available port (**ETH 1**) on the DIGI WR21.*

4. Click **Apply**.
5. Expand the **Advanced** tab.

The second line should read: **The device is currently in Port Isolate mode**.

Figure 11. ETH 1 (LAN Port) configuration (Advanced tab)



6. If the device is in Hub mode, click the **Switch to Port Isolate mode** button.
7. If the change in step 6 was required, click **Save Configuration**, which opens the **Save Configuration dialog**.
8. Click **Save All**. After the save operation is complete, reboot the WR21.

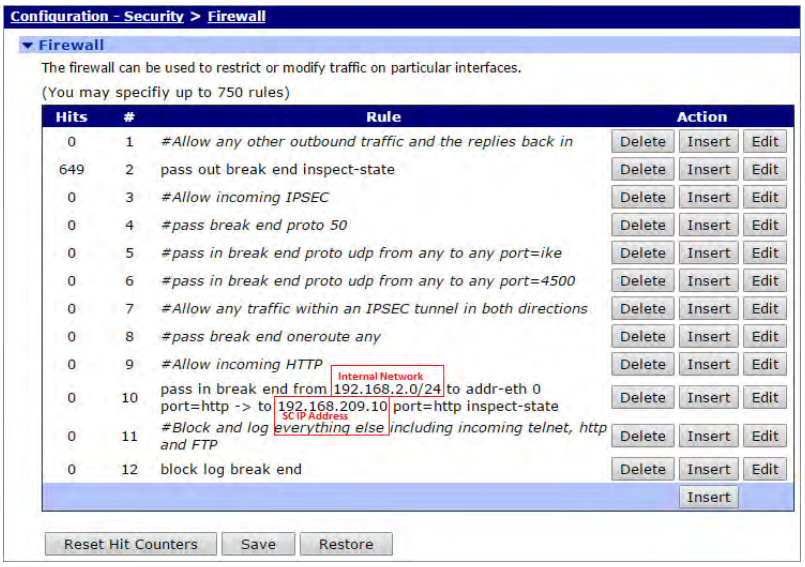
Configuring the Firewall

If you would like the customer to retain access to the Tracer BAS for devices on the customer network, a firewall rule should be added to the DIGI WR21. This will not allow Internet users to access the Tracer BAS.

Note: *This section should only be followed if the ETH 0 IP address is a non-routable private IP address. (i.e. 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).*

1. Click **Security** from the left hand menu, then **Firewall** from the window on the right.
2. Click the **Edit** button on line 10. Replace 192.168.2.0/24 with the IP address and prefix length used to configure **ETH 0**. See the following figure for reference.

Figure 12. Configuring the firewall



Note: *The number to be used for the prefix length can be determined by comparing the subnet mask taken from the Tracer BAS controller to the table below.*

Table 1. Subnet Mask to Prefix Length

Subnet Mask	prefix Length
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28

3. Click the **Ok** button to the right of line 10 to complete the edit, then the **Save** button to save the changes. Finally, scroll down and click **Apply** to apply changes.
4. After all changes have been made, save the configuration by clicking on **Save configuration** in the left hand menu, then **Save all** in the right window.

Example: if the subnet mask used was 255.255.255.128, then 192.168.2.0/25 should be used in the firewall rule. Replace 192.168.209.10 with the new IP address of the Tracer BAS controller. If the Tracer BAS controller was configured to **Obtain IP Address Automatically using DHCP**, choose a static IP address to use instead. This address can be any address that is on the same subnet as the IP address used for **ETH 1 – Internal Network**, excluding x.x.x.0, x.x.x.1, or x.x.x.255 (when using a mask of 255.255.255.0). If your subnet mask is different, consult www.subnet-calculator.com for a list of valid IP addresses in a given subnet.

Configure a Tracer BAS Controller with a New IP Address

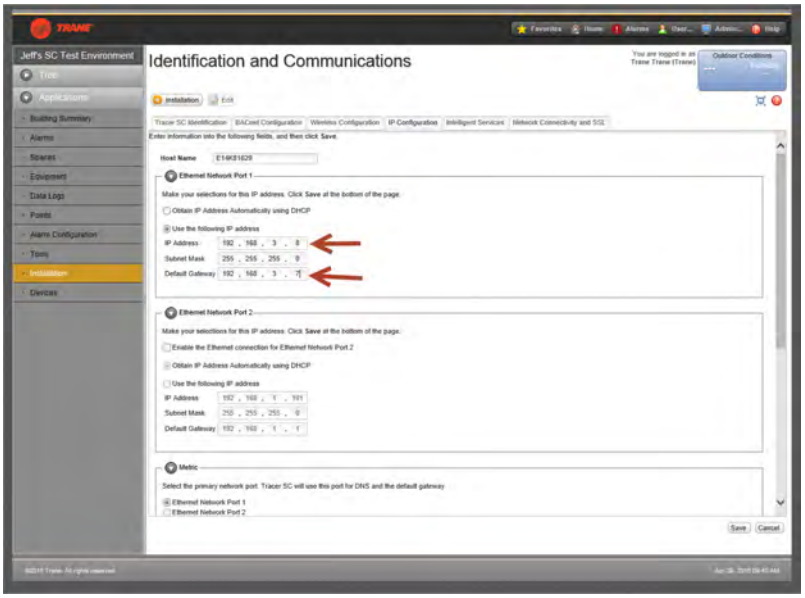
Because the original IP addresses from the Tracer BAS controller were removed and placed them on the WAN port of the Digi device, It is necessary to change the IP addresses in the Tracer BAS controller.

1. Log in to Tracer BAS controller and then navigate to the IP Configuration page (**Installation>Identification and Communication>IP Configuration)**
2. Enter the new IP address, Subnet Mask and Default Gateway of the Tracer BAS controller.

Note: *For the IP address, choose an IP not already in use on the LAN side of the WR21 (**ETH 1**). This should match the IP address used to configure the firewall rules in the previous steps (the example address used was 192.168.209.10). For the Gateway, enter the same IP address you entered on the **ETH 1** configuration of the WR21 in the prior steps in this document (In this example 192.168.209.1 was used).*

3. After you have entered the information above, click **Save**.

Figure 13. Configure Tracer SC with new IP address



Physical Connections

After the Tracer BAS controller and the Digi WR21 have been configured, the next part of the process is to physically connect them.

1. Remove the Ethernet cable end that is connected to the Tracer BAS controller and connect it to the LAN 0 port on the Digi WR21.
2. Connect a second Ethernet cable to the LAN1 port on the Digi WR21 to the Tracer BAS controller. Use the same port on the Tracer BAS controller that you removed the Ethernet cable from.

Example: The following figures show the network before physical connection changes and after the physical connection changes.

Figure 14. Network prior to physical connection

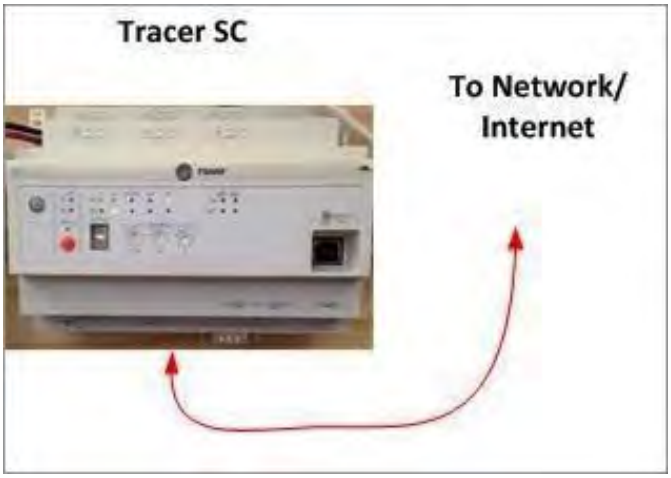
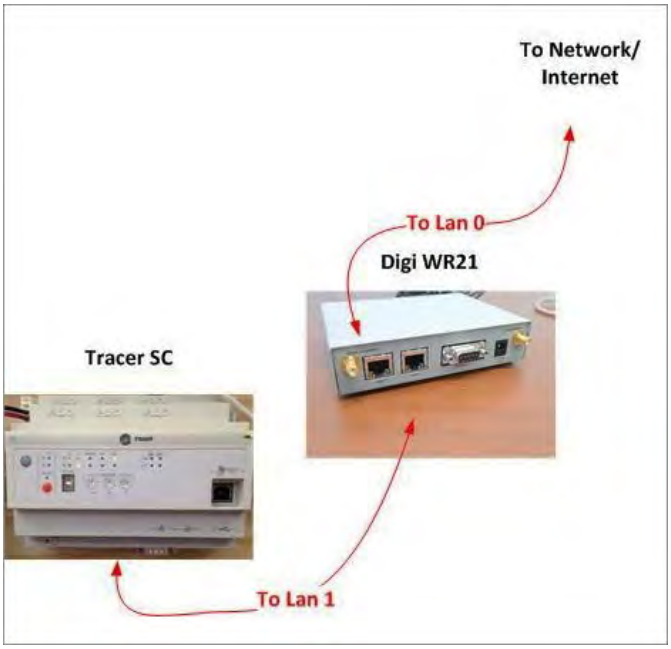


Figure 15. Network after physical connection changes



Configuring Trane Connect Remote Access

Follow the instructions in the *Trane Connect Remote Access How-to-Guide*, BAS-SVU22 to enable Trane Connect for your Tracer BAS controller.

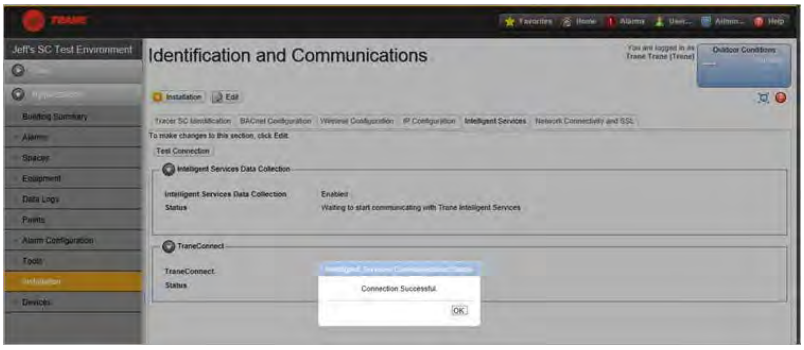
Test the Connectivity to the Trane Cloud

After the Digi WR21 has been installed, it is necessary to test the Trane Connect Remote Access connection.

1. Log into the Tracer BAS controller and navigate to **Installation > Identification and Communications**, and then select the **Intelligent Services** Tab.
2. Click the **Test Connection** button to verify the Tracer BAS controller can still communicate through Trane Connect Remote Access. See the following figure.

   Access to the Tracer BAS is now possible for Trane employees through https://mybuilding.trane.com Command Center.

Figure 16. Test connection successful



Firewall Router Order Process

The Firewall Router solution ordering process consists of the following tasks:

- Register with INS (Industrial Networking) web site at www.industrialnetworking.com/Trane.
- Log in using new ID and password to access the INS online store with Trane pricing.
- Select the appropriate Firewall Router Kit and/or accessories.
- Submit order to INS
- Receive order confirmation from INS

Register with INS

The first step in the order process is to register with INS as a Trane User.

1. Request an INS online store login: e-mail*trane-support@industrialnetworking.com*, or telephone Trane support at 800–889–1461. Be prepared to provide the following information: **first and last name, email address, phone number, Trane branch name, and Trane office code**. (For security purposes, all order acknowledgements will be sent to the primary contact).

Note: *In addition to the primary contact, more users can be can be added as authorized purchasers. Supply the users' contact information and INS will be send user names and passwords.*

2. After the above information is provided, you will be instructed to log into the INS online store.

Note: *Select the My Account Link at the top of the page to log in. To change your password, navigate to* ***settings>update password****.*

Accessing the INS Online Store

After you have registered as a Trane user, you can now access the INS online store. Navigate to the INS online store for Trane at www.industrialnetworking.com/Trane and enter your e-mail and password, which opens the INS online store for Trane.

Important: *Make sure you access the INS online store exclusively set up for Trane at www.industrialnetworking.com/Trane,* ***NOT*** *www.industrialnetworking.com.*

Selecting Firewall Router Items

Select the appropriate Firewall Router Kit (for internal or external mounting).

The Trane Firewall Router Products and Services home page contains the following components:

- Internal Mount Kit
- External Mount Kit
- Individual Components

The kits have been created to make it easy to order and install a firewall router for your Tracer BAS controller. Refer to the following tables for firewall router kit details.

Table 2. Firewall router kit (Internal) packaged contents

Internal Mount Kit PN# WR21-NOCELL-TRANEKIT-INTERNAL (contents)	
• Digi Firewall Router • DIN rail • Locking Barrel to bare wire • Ethernet patch cable (1 ft)	

Table 3. Firewall router kit (External) packaged contents

External Mount Kit PN# WR21-NOCELL-TRANEKIT-EXTERNAL (contents)	
• Digi Firewall Router • 120V power supply • Ethernet patch cable (1 ft)	

Individual Components

In addition to the Firewall Router Pre-packaged Kits, all parts can be ordered separately.

Table 4. Firewall Router Parts and Accessories

Component	Specific Part	Part Number
Power 	Standard Operating Temperature Power Supply	76000823
	Locking Barrel to bare wire	76000821
	Extended Operating Temperature Power Supply	76000752
Mount 	Wall Mount	76000775
	DIN Rail Mount	76000879
	Enclosure	PC1210
Ethernet Cable 	Cat5e Patch Cable Unshielded	N/A 0.5 m, 10 m length options

Submitting an Order

Add the firewall router items to the INS shopping cart and submit your order. (There are two payment options available: credit card or purchase order).

Note: *For Trane offices in California, Georgia, Pennsylvania, and Texas, the Tax Resale certificate number must be provided at the time of order placement.*

Order Confirmation

After INS receives your order, you will receive an order confirmation with shipping and tracking details.

Installing the Firewall Router

Installation procedures will vary depending on whether adequate space is available to mount the firewall router inside the Trane enclosure.

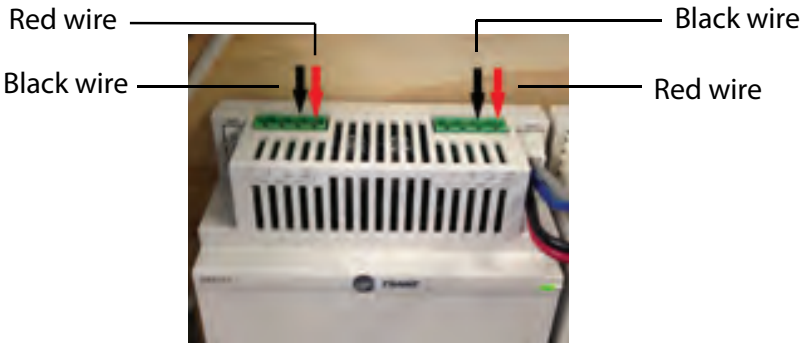
Internal Kit Installation

If adequate space is available within the Trane enclosure, use the Internal Mount Kit (Part# WR21-NOCELL-TRANEKIT-INTERNAL).

1. Attach the provided DIN rail to the Digi firewall router.
2. Mount the Digi firewall router inside the Trane Enclosure.
3. Connect the Digi firewall router to Ethernet Port 2 on the Tracer BAS controller using an Ethernet cable.
4. Connect power to the firewall router:
   - Use the provided locking barrel connector to bare wire connector (Part #76000821)
     – Connect the PM014 power supply to the bare wire. Connect the locking barrel connector to the Digi firewall router.

       The locking barrel connector has a black and red wire. There are two IMC terminal connections on the PM014 power supply. Connect both wires into either the left or the right IMC terminal connection. (See the following figure.)

Figure 17. PM014 power supply IMC terminal connections



External Kit Installation

When inadequate space is available within the Trane Enclosure , or you prefer to install the Digi firewall router inside the Trane Enclosure, use the External Mount Kit (Part# WR21-NOCELL-TRANEKIT-EXTERNAL).

1. Table-mount the firewall router next to an electrical receptacle and within Ethernet distance of the Trane Enclosure.

   Alternatively, you may wish to utilize the remote enclosure (available separately) on a wall near the electrical receptacle.
2. Connect the Digi firewall router to Ethernet Port 2 on the Tracer BAS controller using an Ethernet cable.

   Note: *Maximum cable length is 300 ft.*
3. Connect power to Digi firewall router by utilizing the included 120V power supply.

Customer Remote Access Configuration

Trane Connect Remote Access is the preferred method for secure remote access to a Tracer BAS for both Trane employees and customers. Alternatively, when access to additional devices on the BAS network is needed (i.e. non-Trane gateway device), the Digi WR21 can be utilized as a VPN endpoint. If only Trane personnel require access, TraneConnect should be used, and this section can be skipped.

If the Digi WR21 is being placed downstream of another router or firewall and NAT is being used (the WR21 does not have a public IP assigned on LAN 0), then the upstream router will need to permit/forward the following ports: UDP/1701, UDP/4500, and UDP/500.

Note: *If the customer is using Windows 7, and the WR21 does not have a public IP address, the customer must apply a registry fix. Navigate to the Trane Technologies IT Security Sharepoint site. Locate the link to the NAT Registry fix. Click to open and then double-click on the file labeled* ***NAT-T Registry fix.reg*** *to apply the settings to the registry. Click Yes in the registry editor warning box to apply the new settings. When complete, restart the PC.*

Tunnel Negotiation

If the Digi WR21 is behind a NAT Firewall (the Digi does NOT have a public IP address) then tunnel negotiation settings must be updated. If the WR21 has been supplied with a public IP address, the following procedure can be skipped.

1. On the WR21 configuration page, click on **Network** in the left hand menu.
2. In the right-side window, navigate to **Virtual Private Networking (VPN)>IPsec>IPsec Tunnels>IPsec 0 TraneVPN>Tunnel Negotiation**.
3. Select the check box next to **Negotiate a different IP address and Mask**
4. In the box next to **IP Address**, enter the public facing IP address of the internet-connected edge router.
5. In the box next to **Mask**, enter 255.255.255.255.
6. Click **Apply** when complete.

Figure 18. Digi WR21 VPN setup

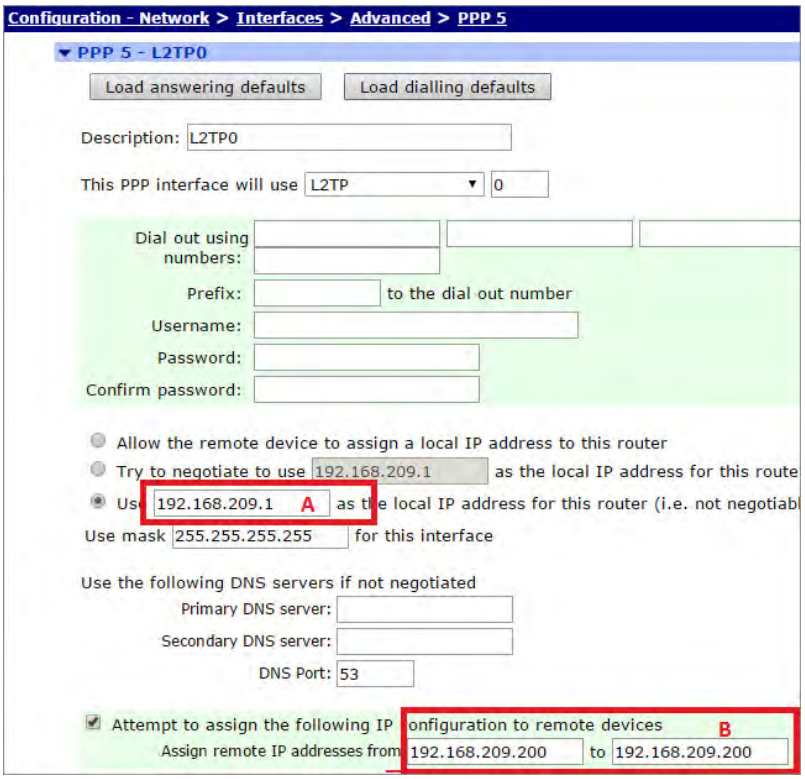
PPP Connection Configuration

If the configuration for ETH 1 (network attached to LAN 1 of the Digi WR21) has been changed from the default of 192.168.209.0, the PPP interfaces assigned to VPN access must also be updated. If the default network of 192.168.209.0 has been retained, the following procedure can be skipped.

1. Click on the **Network** link in the left hand menu.
2. In the right-hand window, navigate to **Interfaces>Advanced>PPP 5 – L2TP0**
3. In **box A** (see figure below), enter the IP address used to configure **ETH 1** earlier in the document.

4. In **box B** (see figure below), change the first three octets to match the network assigned to **ETH 1**, leaving the final octet as 200.
5. Repeat these steps for **PPP 6 – L2TP1** and **PPP 7 – L2TP2**.

Figure 19. Digi WR21 PPP setup



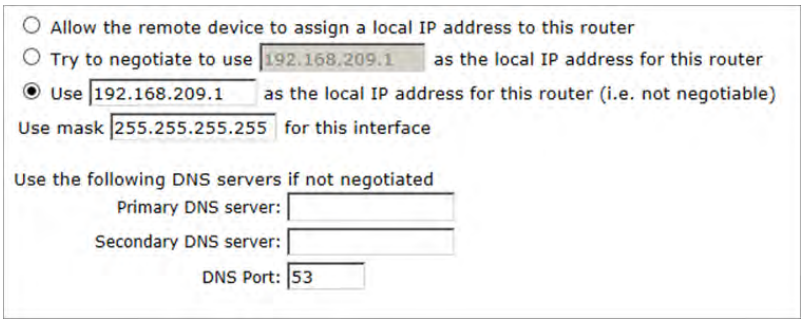
If the LAN IP address has been modified to reflect the BAS network (192.168.2.X):

However, you are UNABLE to establish connectivity to the Tracer BAS (Ping or Web browser)

- VPN is established.
- Can remotely access the LAN interface for configuration.

The following figure shows the default configuration:

Figure 20. PPP default configuration



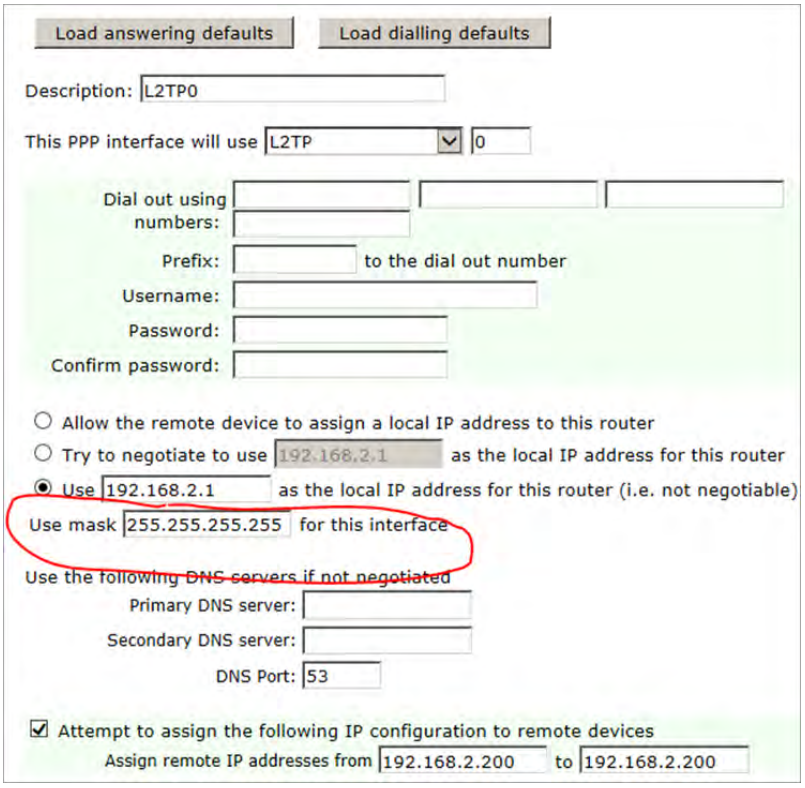
If the LAN address has been modfied:

- You must modify PPP 5, PPP 6, and PPP 7 IP address and mask.

– Configure the mask as 255.255.255.255, as shown in the following figure. (The mask is not the same as the Tracer BAS controller network mask.)

– The IP address range must be configured with addresses that are NOT used on the Tracer BAS controller network.

Figure 21. Modifying PPP settings



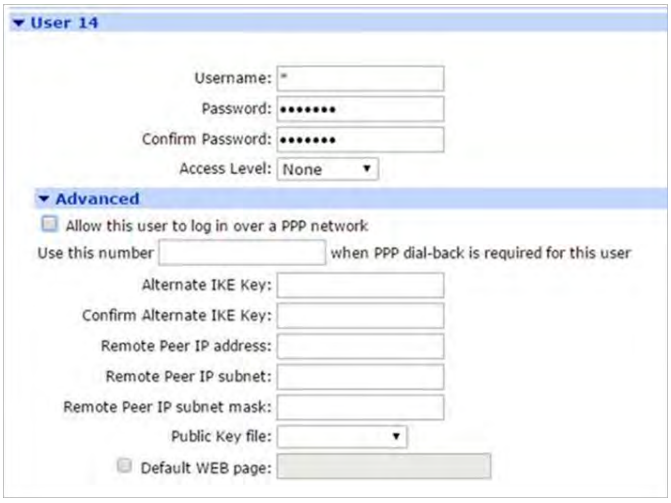
Firewall Configuration

1. In the left-hand menu, click **Security**.
2. In the right-hand window, click on **Firewall**.
3. Click on the **Edit** button next to line 4. Remove the comment symbol (#) at the beginning of the line, then click **OK**.
4. Repeat this process for lines 5, 6, and 8. When complete, click the **Save**, then **Apply**.

Pre-shared Key and Account Creation

1. Click on **Security** in the left hand menu.
2. In the right hand window, click on **Users**, then **User 10 – 14**.
3. Under **User 14,** enter an * (asterisk) symbol in the **Username** field as shown in the following figure.

Figure 22. Setting up users for pre-shared key and account creation



4. Enter a complex password (8 characters, a mix of letters, numbers, and characters is recommended) in the **Password** field.
5. Enter the same password in the **Confirm Password** field. This password will act as the common pre-shared key when configuring the VPN connection on a client device
6. Next, individual user accounts must be created:
   a. Click on one of the remaining users in this section. Assign a username and password in the appropriate boxes.
   b. To prevent VPN user accounts from having access to change router settings, select **None** in the **Access Level** drop-down box.
7. Click **Apply** when complete.

VPN Client Configuration for iPhone/iPad Connection

1. On the home screen, tap **Settings**.
2. Tap **General** and navigate to the **VPN** button on the right.

Figure 23. iPhone/iPad VPN configuration

3. Tap **Add VPN Configuration**.

Figure 24. iPhone/iPad Add VPN Configuration

4. Tap **Type** and select **L2TP**. Tap **Back**.
5. In the **Description** field, enter a name for the connection. For example, VPN to Digi.
6. In the **Server** field, enter the IP Address of the Digi router.
7. In the **Account** field, enter your VPN username.
8. In the **Password** field, enter your VPN password.
9. In the **Secret** field, enter the IPSec shared secret key found on the IPSec shared key page.
10. Set **Send all Traffic** to OFF.
11. Tap **Save**.
12. Connect to the VPN by sliding the VPN button to ON. The L2TP VPN with IPSEC connection is established.

Figure 25. iPhone/iPad VPN Settings

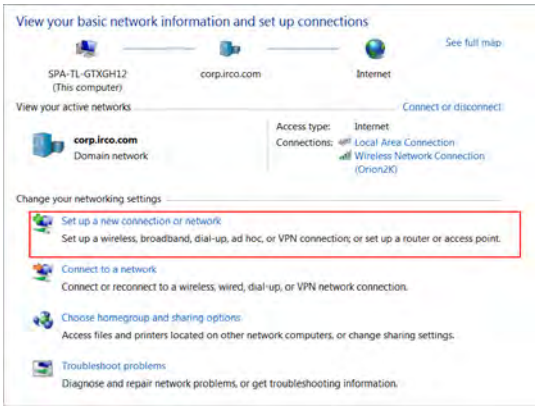
VPN Configuration for Microsoft® Windows 7 Operating Systems

Note: *For Microsoft Windows 10, consult the system help topics for instructions.*

To set up a new VPN connection on Microsoft Windows 7:

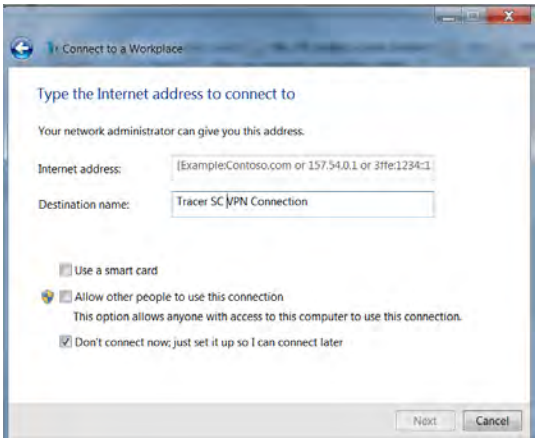
1. Open the **Network and Sharing Center** applet from the Windows Control Panel.
2. Click on **Set up a new connection or network**.

Figure 26. Windows 7 Connect to a Network



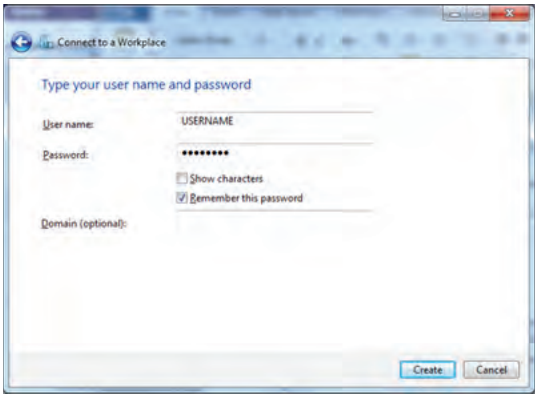
3. Select **Connect to a workplace**. Click **Next**. If prompted, select **No, I'll create a new connect**. Click **Next**.
4. Select **Use my Internet connection (VPN)**.

Figure 27. Windows 7 Connect to a Workplace



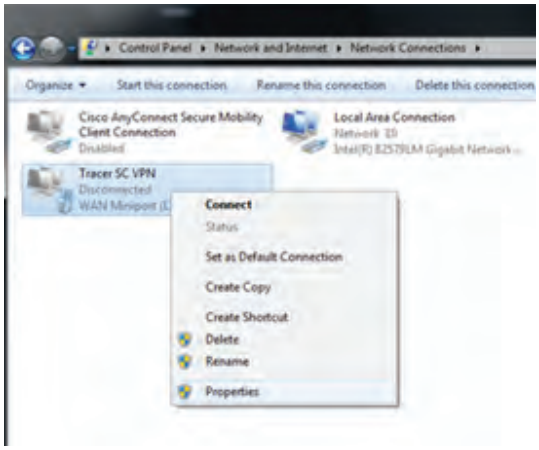
5. In the **Internet address** field, enter the IP address provided by INS.
6. In the **Destination name** field, enter a name to identify the connection, such as Tracer BAS VPN. This field is for identification purposes only.
7. Select **Don't connection now; just set it up so I can connect later**.
8. Enter your **User name** and **Password** provided by INS. To avoid entering the VPN connection password on each connection, select **Remember this password**.
9. Leave the **Domain** field blank.
10. Click **Create** to create the VPN connection.

Figure 28. Create the new VPN



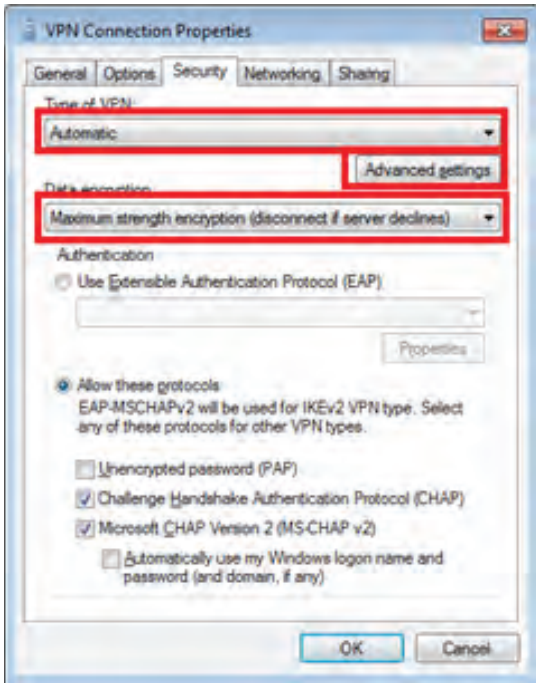
11. Click **Close**.
12. Return to the Network and Sharing Center and click **Change adapter settings**.
13. Find the VPN connection you just created. Right click on the connection and select **Properties**.

Figure 29. Change adapter settings



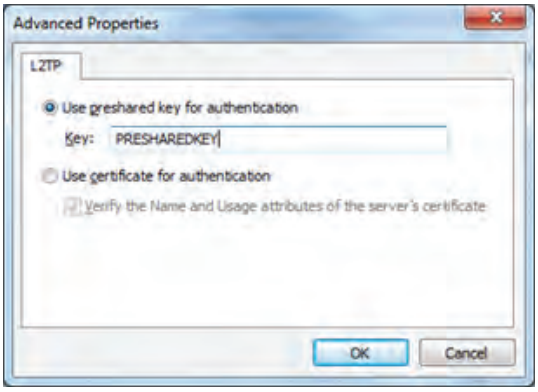
14. Click the **Security** tab.
    a. In the Type of VPN drop-down box, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**.
    b. In the Data encryption drop-down box, select **Maximum strength encryption**.
    c. Click **Advanced Settings**.

Figure 30. Configuring the VPN connection properties



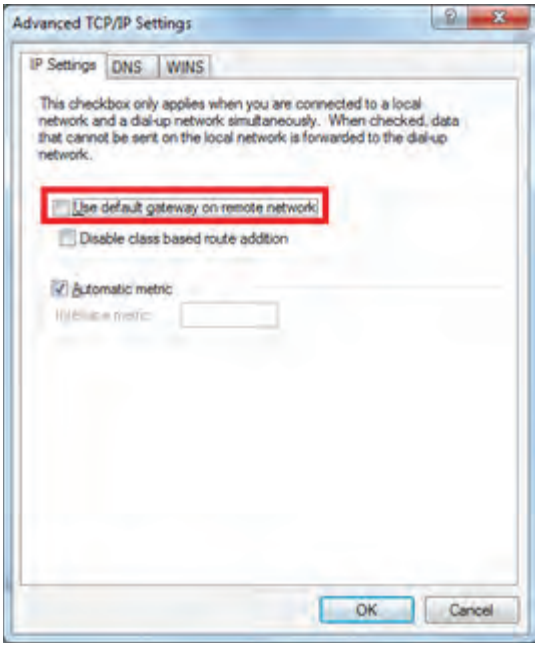
d. Select **Use preshared key for authentication** and enter the preshared key provided by INS.

e. Click **OK**.



15. Click the **Networking** tab.
    a. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
    b. Click **Advanced...**
    c. Uncheck **Use default gateway on the remote network**, then click **OK**.

Figure 31. Configuring the network (default gateway)



d. Click **OK** twice more to save your changes.

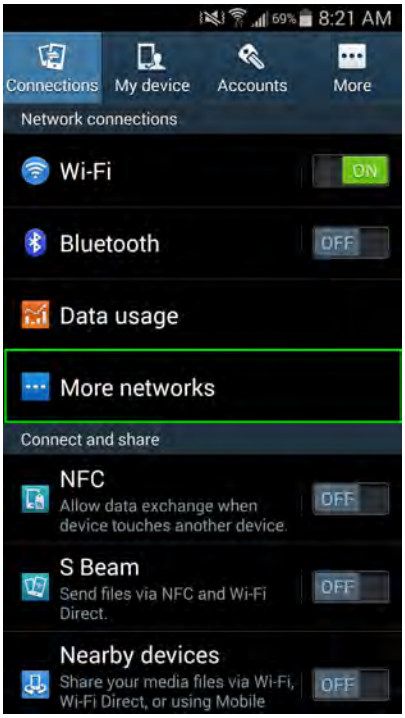
16. To activate the new VPN connection:
    a. Return to the Network and Sharing Center and click **Connect to a network**.
    b. Select the newly created connection.
    c. Verify that the user name and password were entered and click **Connect**.
    d. When the connection completes, open a Web browser and connect to the Tracer BAS using its local IP address.
17. To disconnect from the VPN, return to the Network and Sharing Center. Click on the VPN connection and click **Disconnect**.

VPN Configuration for Android Operating Systems

Depending on the model and version of your Android device, the selections described in the following procedure may vary.

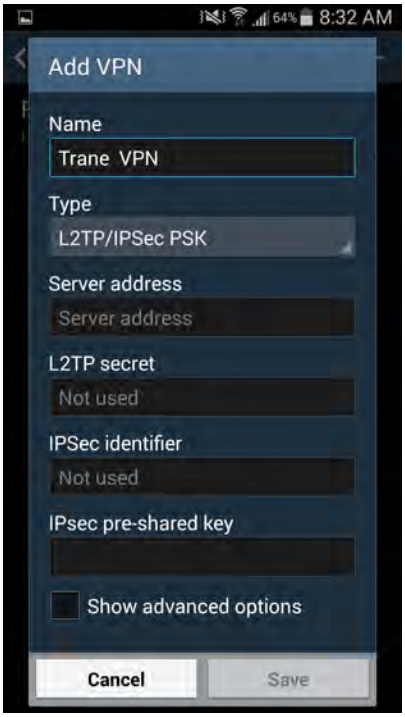
1. Open **Settings**.
2. In the Wireless and Networks section, tap **More networks.**

Figure 32. Adding more networks



3. Tap **Basic VPN**.
4. Tap the menu button to add a VPN as shown in the following figure.

Figure 33. Add a VPN



5. In the **add VPN** window:

a. Enter a name for the VPN. This name will identify the VPN connection on the Android device.

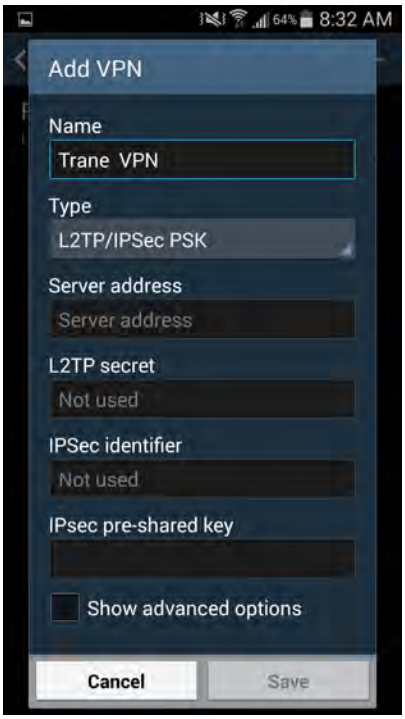
b. Under **TYPE**, select **L2TP/IPSec PSK**.

c. In the **SERVER ADDRESS** field, enter the IP address provided by INS.

d. In the **FORWARDING ROUTES** field, enter the network on which the Tracer BAS controller resides. For example, if the IP address of the Tracer BAS controller is 192.168.2.10, the FORWARDING ROUTES should be 192.168.2.0/24.

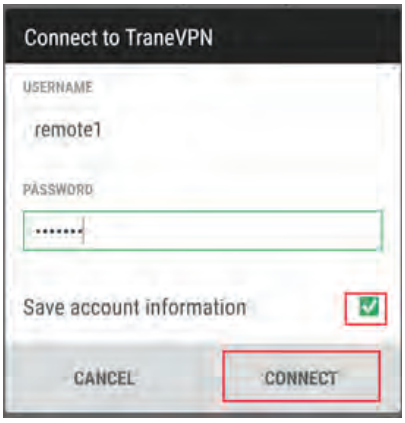
e. All other setting should be left at their default values. Tap **Save**.

Figure 34. Configuring the new VPN



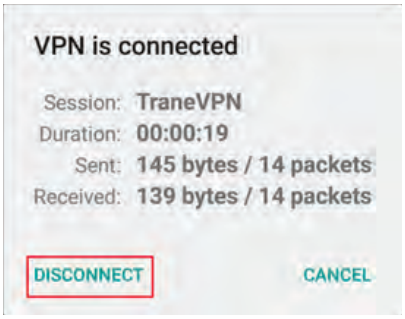
6. A new connection appears on the VPN menu. Tap the new connection to initiate.
7. Enter the username and password provided by INS. To save the credentials for future use, select **Save account information**.
8. Tap **Connect** to connect to the VPN.

Figure 35. Connecting to VPN



9. To disconnect from the VPN, return to the VPN setting screen. Tap the name of the VPN connection and tap **Disconnect**.

Figure 36. Disconnect VPN session



Setting Up Remote Access For Customers

When customers require remote access to their facilities through the cellular router solution, utilizing Trane Connect is easy to use and built into Tracer BAS controllers, including Tracer SC/SC+ and Concierge. The following procedure describes how to set up Trane Connect Remote Access for your customer. If some sections do not apply to your specific scenario, skip to the appropriate section. For more information, refer to the *Trane Connect How-to-Guide,* BAS-SVU22.

Setting Up Trane Connect Remote Access

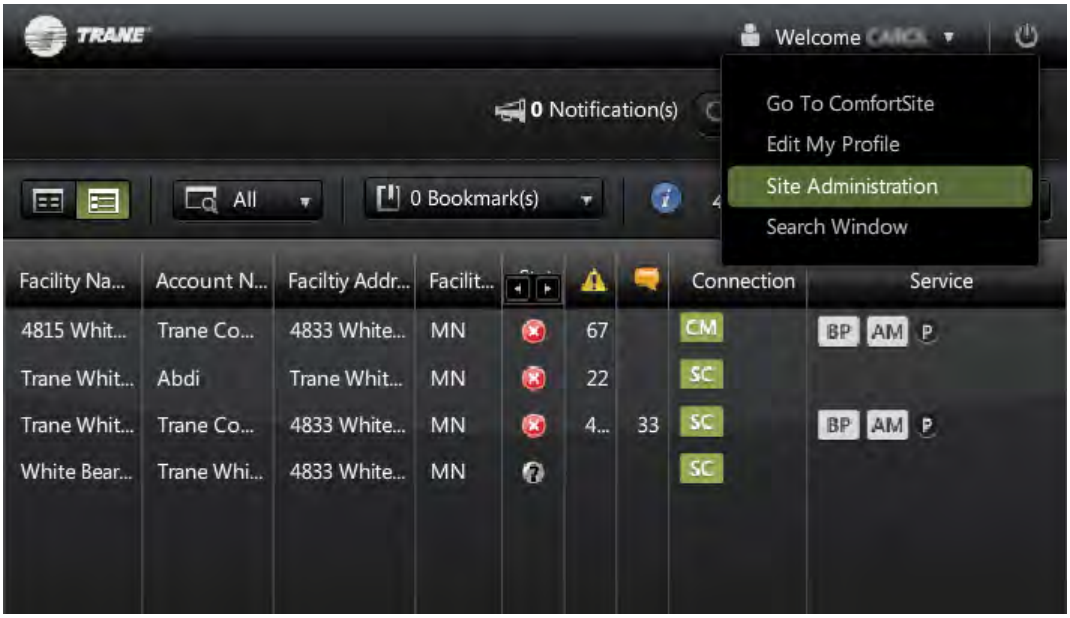
This section describes the process of setting up Trane Connect Remote Access to enable safe and secure remote access to the Tracer BAS.

Registering a Tracer BAS Controller or Tracer Concierge with TIS Command Center

The following procedure describes how to register a new Tracer BAS controller in the TIS Command Center (mybuilding.trane.com). Trane Offices and Trane technicians use this interface to self-register Tracer BAS controllers in the TIS Command Center and to set up Trane Connect.

1. Log on to mybuilding.trane.com. Click on **TIS Command Center**, then click **Site Administration** from the **Welcome** drop-down list. The Account Overview page opens (see Figure 38, p. 36).

Figure 37. Navigating to Site Administration (TIS Command Center)



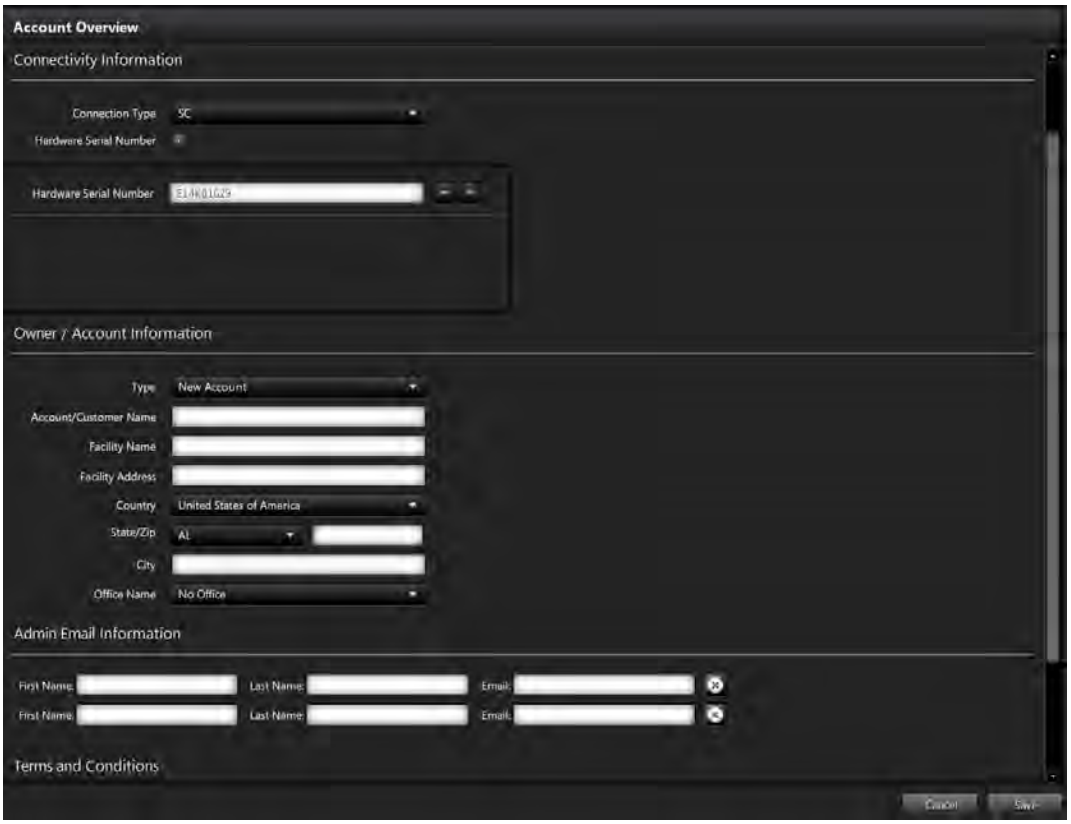
2. In the **Connectivity Information** section, select SC from the **Connection Type** drop-down list. Then enter the Tracer BAS controller's hardware serial numbers in the provided fields.
3. In the **Owner/Account Information** section, select an existing account or enter a new one.
4. Enter the name and address of the facility in the provided fields.
5. Select a Trane office from the **Office Name** drop-down list.
6. In the **Admin Email Information** section, enter the name and e-mail address of the

individual who will serve as the Trane Connect customer administrator for the facility. (This information is only required if setting up remote access for customers.)

Only two customer Admins can be created for each Tracer BAS controller. The Customer Admin user is the only user who can set up other customer users. A customer user can remotely access a Tracer BAS using Trane Connect.

7. Agree to the Terms and Conditions and then click **Save**.
8. Proceed to "Customer Admin Initial Account Creation," p. 38, if setting up remote access for customers.

Figure 38. Registering a Tracer BAS controller (TIS Command Center)

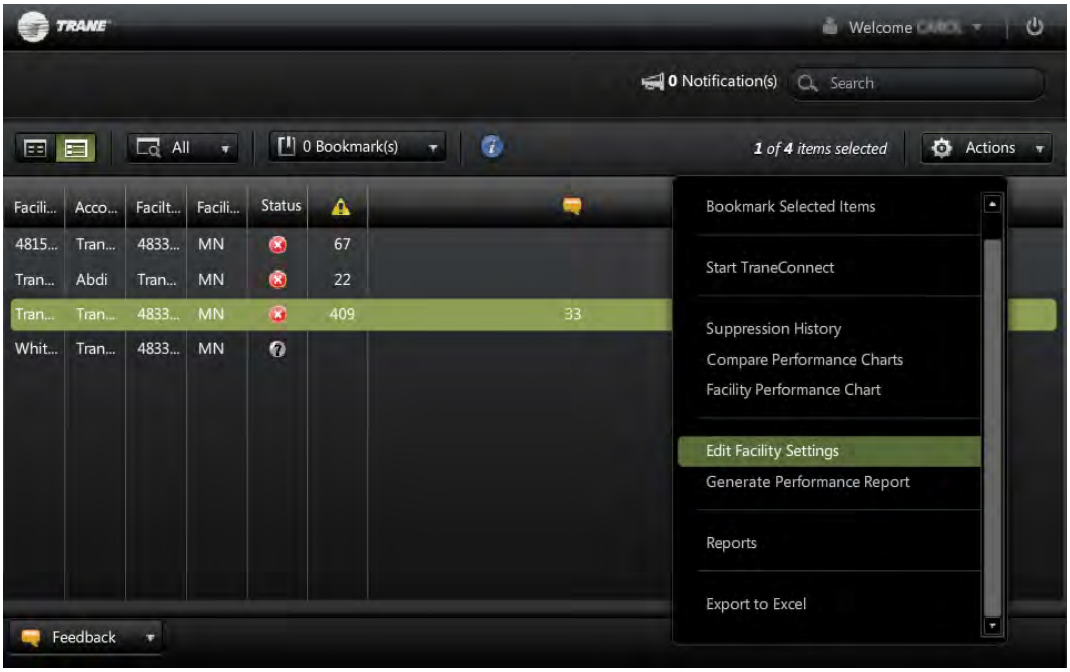


Modifying a Previously Registered Tracer BAS Controller

The following process describes how to add a new customer administrator to an existing Tracer BAS controller in TIS Command Center (mybuilding.trane.com).

1. In TIS Command Center, select the Tracer BAS controller (facility) and then click **Edit Facility Settings** from the **Actions** menu (see Figure 39, p. 37).

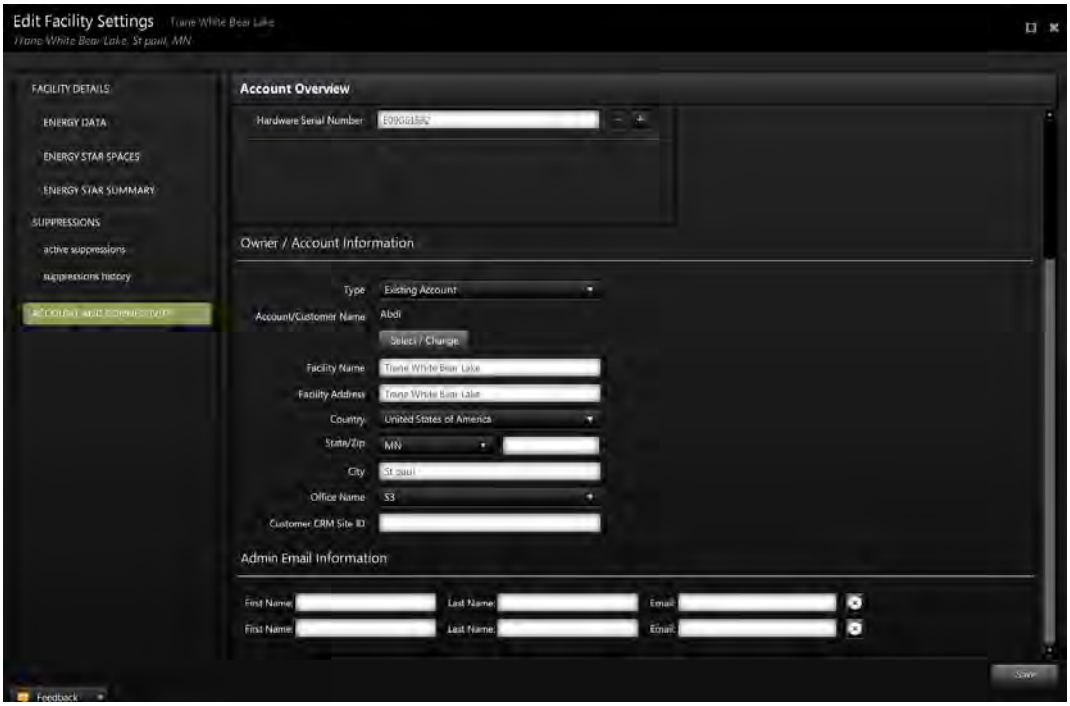
Figure 39. Edit a Facility (TIS Command Center)



2. From the left-hand menu, click **Account and Connectivity**. The Edit Facilities page opens (Figure 40, p. 38).
3. In the **Admin Email Information** section, enter the name and e-mail address of the individual who will serve as the Trane Connect Remote Access customer administrator for the facility. (This information is only required if setting up remote access for customers.)

   Only two customer Admins can be created for each Tracer BAS controller. The Customer Admin user is the only user who can set up other customer users. A customer user can remotely access a Tracer BAS using Trane Connect Remote Access.
4. Agree to the Terms and Conditions and then click **Save**.
5. Proceed to "Customer Admin Initial Account Creation," p. 38, if setting up remote access for customers.

Figure 40. Add a customer administrator (TIS Command Center)



Customer Admin Initial Account Creation

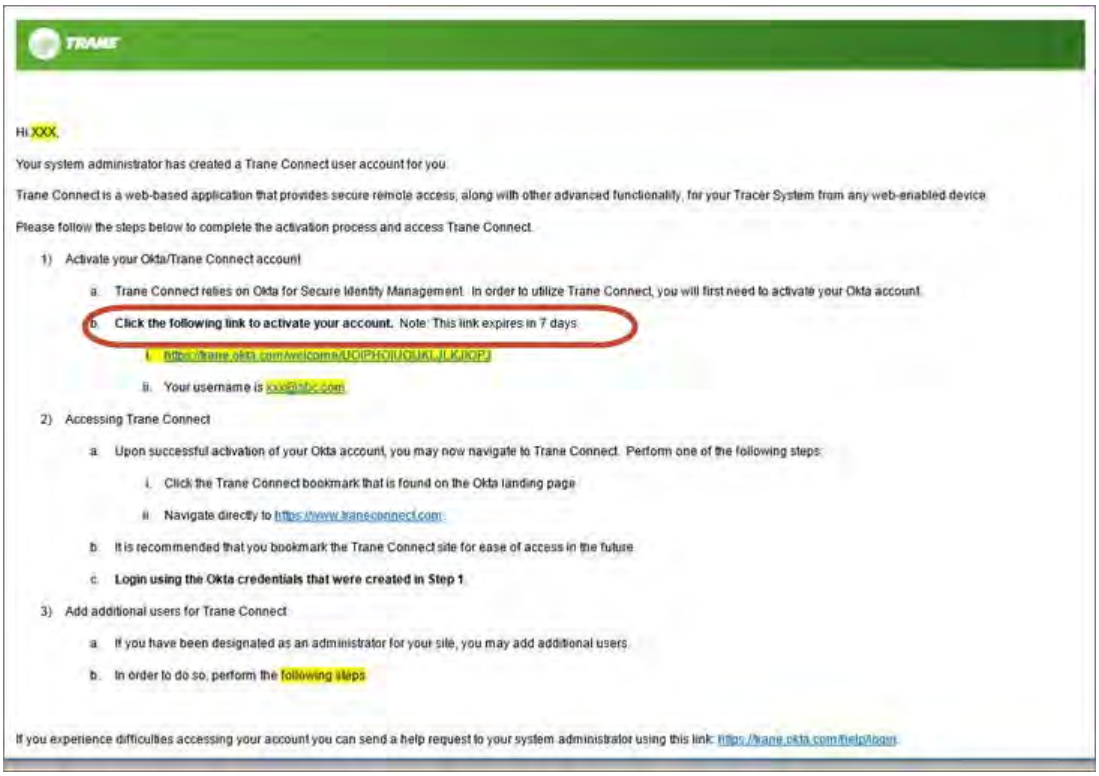
The customer admin who was defined in TIS Command Center will receive a “Welcome to Trane Connect” e-mail message. Trane Connect utilizes Okta, a User Authentication tool, to do the following:

- Synchronize Trane Active Directory users with Trane Connect users.
- Authenticate customers with Trane Connect.

To authenticate a new customer admin account:

1. Upon receipt of the “Welcome to Trane Connect” e-mail, click on the activation link (see the following figure).

   Important: *The customer administrator* ***must activate the link in the e-mail within 7 days*** *or the account activation will expire.*



Hi XXX,

Your system administrator has created a Trane Connect user account for you.

Trane Connect is a web-based application that provides secure remote access, along with other advanced functionality, for your Tracer System from any web-enabled device.

Please follow the steps below to complete the activation process and access Trane Connect.

1) Activate your Okta/Trane Connect account

   a. Trane Connect relies on Okta for Secure Identity Management. In order to utilize Trane Connect, you will first need to activate your Okta account.

   b. **Click the following link to activate your account.** Note: This link expires in 7 days.

      i. https://trane.okta.com/welcome/UOIPHOIUOIJKLJLKJIOPJ

      ii. Your username is xxx@hbc.com

2) Accessing Trane Connect

   a. Upon successful activation of your Okta account, you may now navigate to Trane Connect. Perform one of the following steps:

      i. Click the Trane Connect bookmark that is found on the Okta landing page

      ii. Navigate directly to https://www.tranesconnect.com

   b. It is recommended that you bookmark the Trane Connect site for ease of access in the future.

   c. **Login using the Okta credentials that were created in Step 1.**

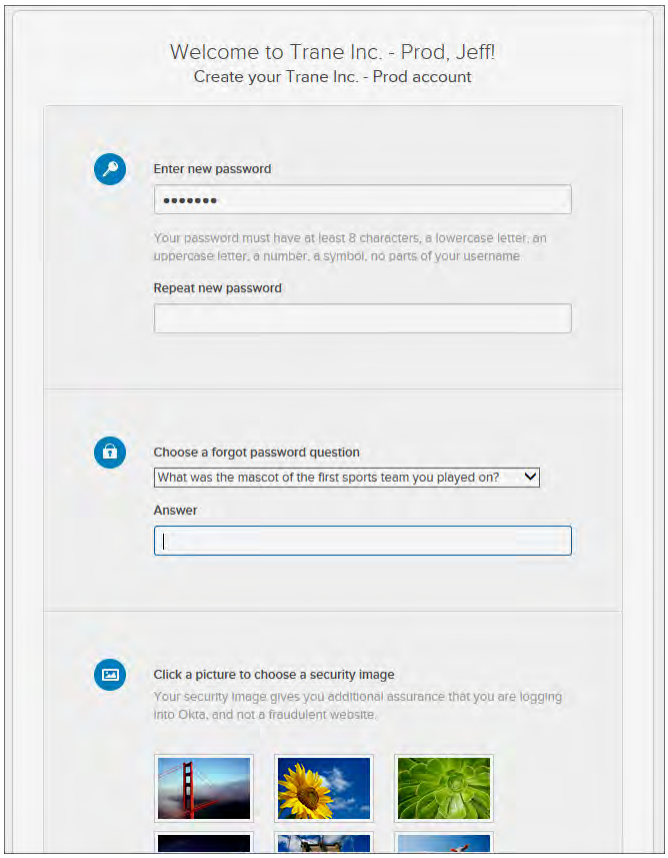
3) Add additional users for Trane Connect

   a. If you have been designated as an administrator for your site, you may add additional users.

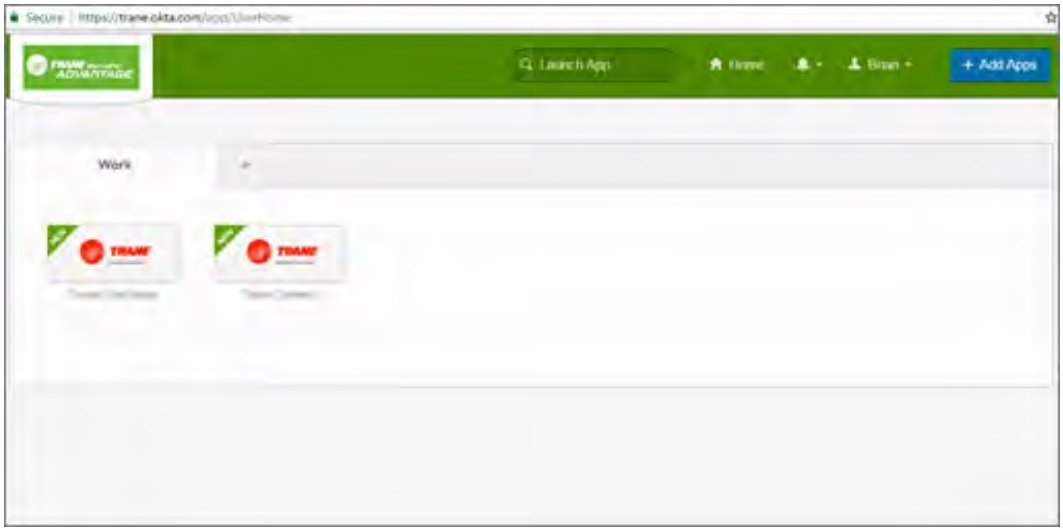
   b. In order to do so, perform the following steps

If you experience difficulties accessing your account you can send a help request to your system administrator using this link: https://trane.okta.com/help/login

2. The account creation screen appears after clicking the activation link (see the following figure). Enter and re-enter a new password, select a security question/answer, and select a security image that will be presented upon subsequent logins.



Upon successful account creation and login, the customer activation screen appears (see the following figure).



3. Click the Trane Connect image, which opens traneconnect.com.

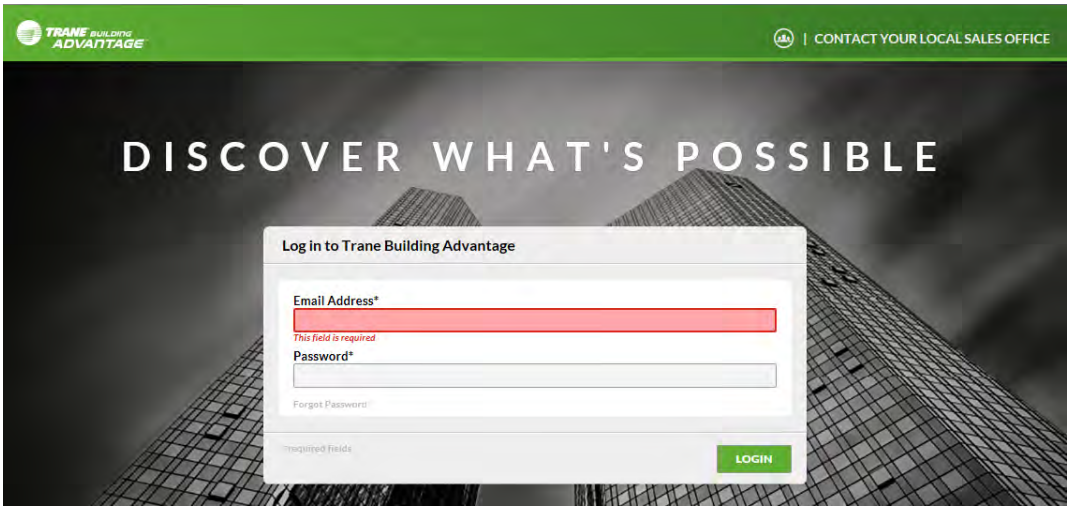
   Note: *Customers who have more than one site will see a list of multiple sites.*

Logging in to Trane Connect

After customer administrators have activated their accounts from the Welcome to Trane Connect e-mail, they are now able to access Trane Connect.

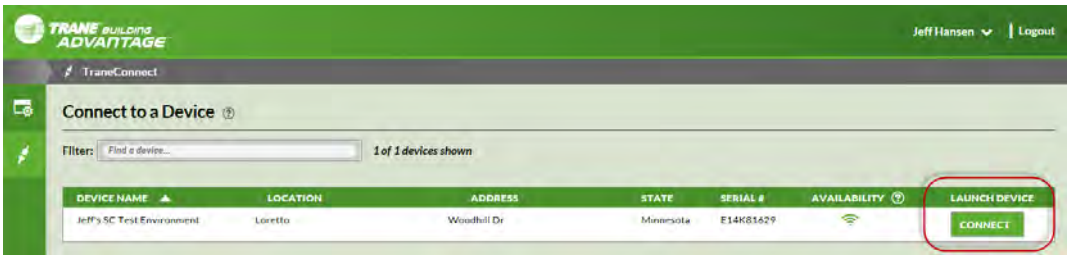
1. Navigate to TraneConnect.com. The Trane Connect login page opens (see the following figure).
2. Enter the credentials that were created in the Customer Account Creation procedure and then click the Login button. The **Connect to a Device** page opens, in which displays a list of devices that you can securely connect to.

   Note: *It is recommended that users create a bookmark for traneconnect.com in order to navigate directly to the site on subsequent visits.*



3. Select the device to which you want to connect. Click on the **Connect** button in the Launch Device column to open the Tracer BAS user interface. A new browser tab is launched, which displays a login page for the device.

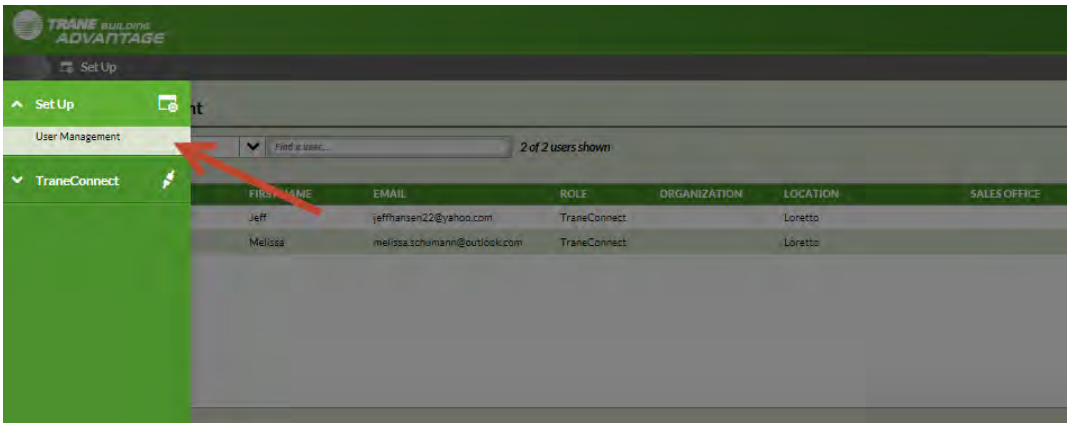
   Note: *Multiple devices can be accessed simultaneously in separate browser tabs.*



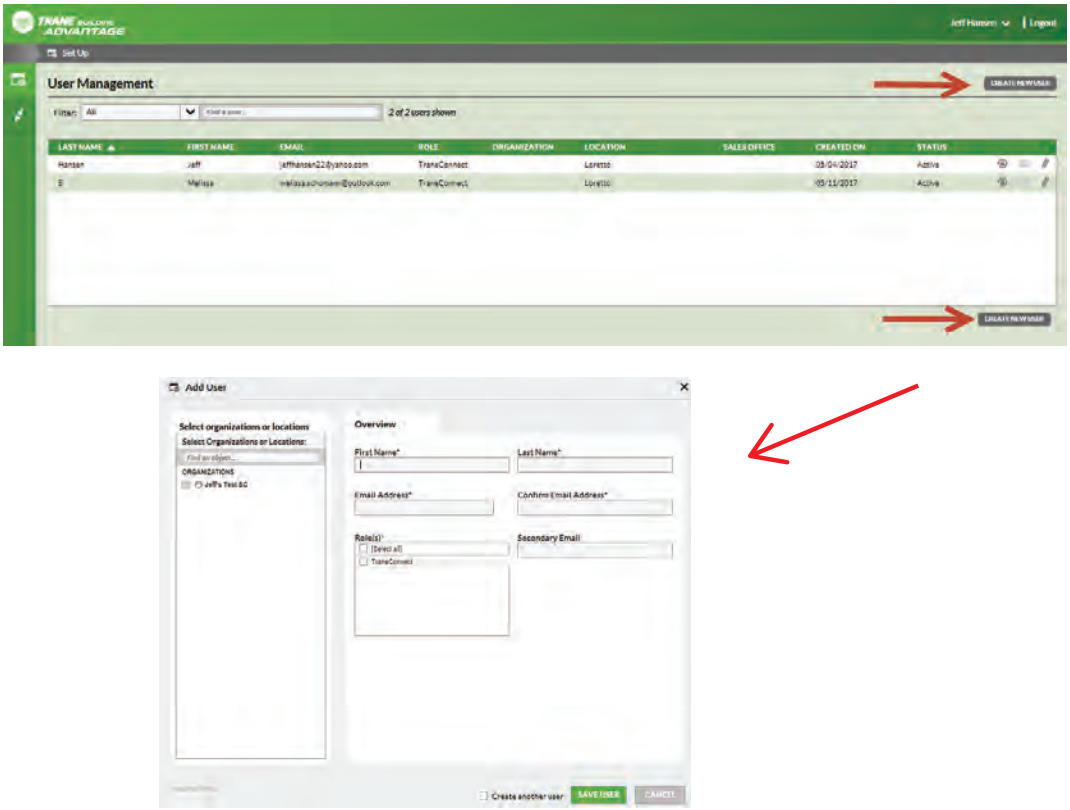
Creating Additional Trane Connect Users

Customer admins have the ability to create and delete accounts for additional users for each device.

1. Log into Trane Connect. Click the Set Up icon located at the top of the left navigation menu, then select **User Management** (see the following figure). A list of current users is displayed.



2. From the upper-right portion of the screen, click **Create New User**. The **Add User** dialog box appears.



3. Search for the user's location/organization in the search box. Enter the user information, Trane Connect role, and appropriate devices for the user.
4. When complete, click **Save User**.

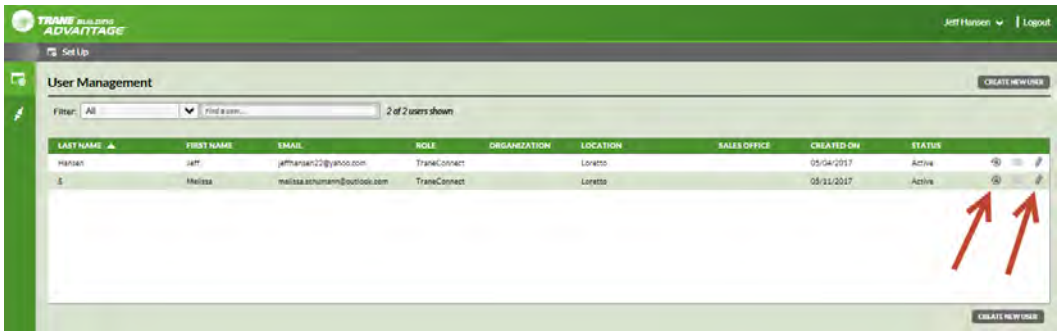
   The user will receive a Welcome to Trane Connect e-mail.

   Important: *The new user **must activate the link in the e-mail within 7 days** or the account activation will expire.*

   Trane Connect utilizes a User Authentication tool called Okta to do the following:

- Synchronize Trane Active Directory users with Trane Connect users.
- Authenticate customers with Trane Connect.

If a user requests the e-mail be resent, or if a user profile must be edited, click the appropriate icon located in the individual user list (see the following figure).

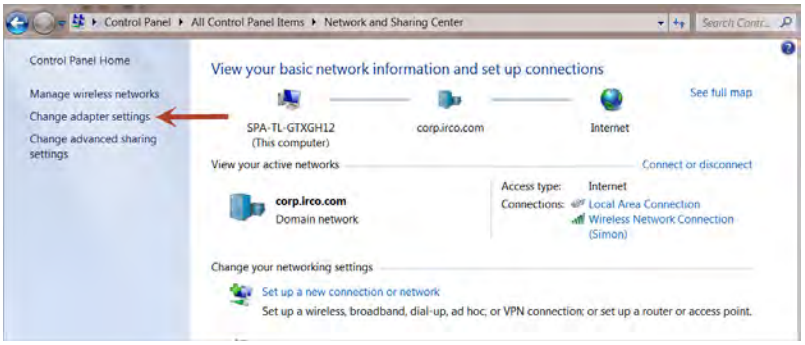


Configure the LAN IP Address on a PC

When configuring the Digi WR21 router, it is often necessary to connect to different IP addresses and often DHCP will be disabled. Therefore, you must manually configure your IP address to connect to a specific IP.

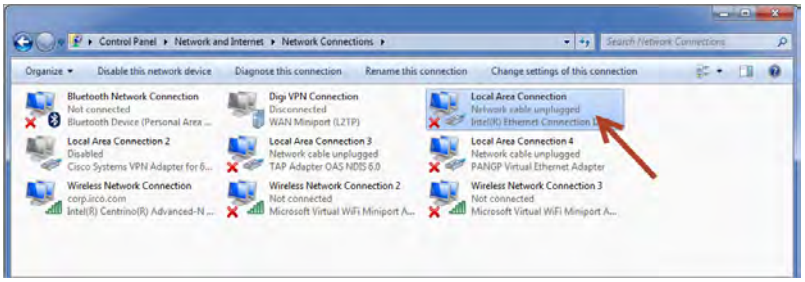
1. On a Microsoft Windows PC, click **Start** (or the windows icon) in the bottom left corner, then select **Control Panel**
2. Navigate to **Network and Sharing Center**. On the left side of the new window, select **Change adapter settings**

Figure 41. Change Adapter Settings



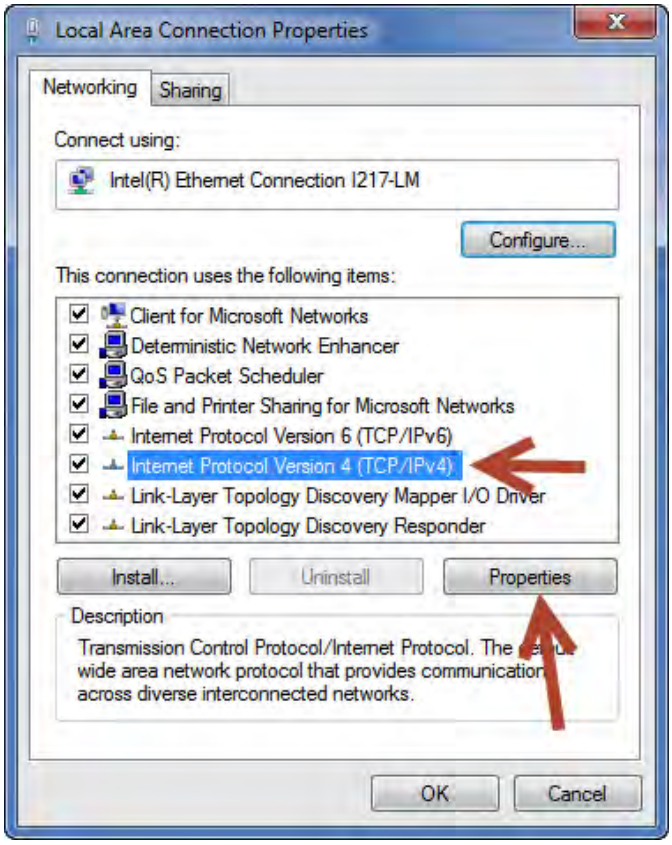
3. Locate the connection named **Local Area Connection**, and then right click on this and select **Properties**

Figure 42. Selecting Local Area Connection



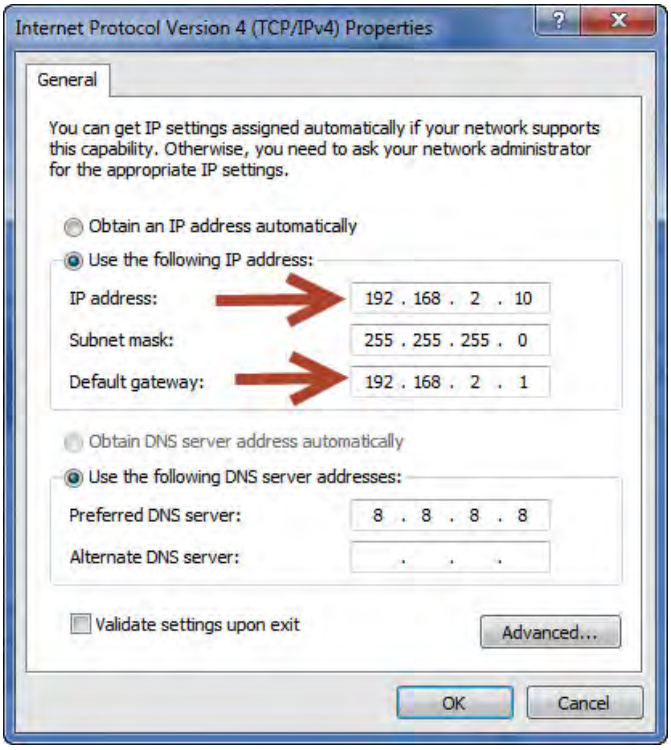
4. The Local Area Connection Properties dialog box appears. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 43. Selecting Internet Protocol Version 4 (TCP/IPv4)



5. Enter the IP information: To connect to a device at a specific IP, for example 192.168.2.1, then this IP will be the **Default Gateway**. Enter another IP address just a few numbers higher than the Default Gateway to serve as the computer's **IP address**. In the following figure, I 192.168.2.10 was used. The **Subnet Mask** will always automatically populate after you enter the IP address, and use 8.8.8.8 as the DNS address.

Figure 44. Entering IP information



6. Click **OK**, then **OK** again to exit. You can reach the target IP (192.168.2.1 in the above figure) by opening a web browser and typing in the IP address (example: http://192.168.2.1).

Trane - by Trane Technologies (NYSE: TT), a global innovator - creates comfortable, energy efficient indoor environments for commercial and residential applications. For more information, please visit trane.com or tranetechnologies.com.

Trane has a policy of continuous product and product data improvements and reserves the right to change design and specifications without notice. We are committed to using environmentally conscious print practices.

BAS-SVX069F-EN 20 Jul 2020
Supersedes BAS-SVX069E-EN (August 2017)

©2020 Trane