

Integriti Connectivity Guide

Introduction

The Integriti controller can establish and maintain communications with the Integriti software via a diverse range of paths, including TCP, Skytunnel and USB.

The Integriti software is equipped with a range of features to make establishing a connection as simple as possible under most circumstances, however there are some scenarios where additional technical understanding on the part of the commissioning technician will be required to establish a connection.

TCP Connection Direction

The TCP protocol establishes bi-directional communication between two devices in a similar fashion to a telephone call, in that there is a caller and an answerer.

These are commonly called the “client” (caller) and “server” (answerer).

The direction of the TCP connection is said to be either “outbound” (from the perspective of the client) or “inbound” (from the perspective of the server).

Knowing and understanding the “direction” of the connection is vitally important in diagnosing and correcting networking issues, as all routers will treat inbound and outbound connections in a different manner.

Under most circumstances, routers will by default, allow an outbound connection to be made, however will not allow inbound connections without additional configuration.

Network Address Translation (NAT)

Most Internet connected networks are arranged in a topology that utilizes Network Address Translation (NAT). This involves using a single “public” IP address on the Internet, to provide service to multiple devices on the “local” network.

The effect of this is that without specific configuration of the router, it is not possible for a device on the “local” network to receive inbound connections from the “public” network, as the router does not have enough information to determine which local device to route the connection to.

Outbound connections are however usually allowed for all devices on the local network.

Protocols

The controller and software utilize a range of communications protocols which are suited to different applications.

- **TCP:** The basic transport layer used to encapsulate (carry) higher layer protocols (IRIP, HTTP and SkyTunnel)
- **UDP:** The basic transport layer used for controller Peer to Peer communications
- **HTTP:** This protocol is used to transfer web-pages from a web-server to a web client. This protocol is also used to exchange data using Web Services. This protocol is used between the Integrity software and controller to facilitate automatic discovery and enrollment on a local network.
- **IRIP:** Inner Range's proprietary communications protocol which is used to provide streaming communications between Integrity controllers and Integrity Servers. This protocol uses TCP Port 4711 and is an outbound connection from the Controller, and an inbound connection to the Integrity Software.
- **Skytunnel:** Inner Range's cloud based connectivity solution, which uses TCP port 40844, and is an outbound connection from both the Controller and Integrity Software.

Connectivity Requirement Summary

- **Ongoing Controller to Software IRIP communications**
 - TCP Port 4711 accessible inbound to the Integrity Software and outbound from the Integrity Controller
- **Controller Discovery and Automatic Enrollment**
 - TCP Port 80 accessible inbound to the Integrity Controller and Outbound from the Integrity Software
 - TCP Port 4711 accessible inbound to the Integrity Software and outbound from the Integrity Controller
- **Integrity software Client to Server communications**
 - TCP Port 44000 accessible inbound to the Integrity Server and outbound from the Client Software
- **SkyTunnel**
 - TCP Port 40844 accessible outbound from both the Integrity Controller, and Integrity Software

SkyTunnel Connectivity Options

The SkyTunnel service is intended to enable simplified connectivity between controllers and the integrity software, as well as alarm reporting to Multipath Enabled central stations, or central stations using the Patriot automation system.

The following services are currently supported via SkyTunnel

- Temporary Controller connections to Integrity CS *for Upload / Download / Review*

- Temporary Controller connections to Integriti Pro *for Upload / Download / Review*
- Permanent Controller connections to Integriti Pro *for Upload / Download / Review and ongoing System Administration*
- Alarm Reporting to Multipath-IP Enabled Monitoring Stations
- Alarm Reporting to Monitoring Stations using the Patriot Automation System
- Connections from the Integriti Mobile application (on smart devices) to the Integriti Controller

The following services are NOT available via SkyTunnel

- Connections from Client Software to Server Software
- Connection of LAN modules to the Controller using CLOE modules
- Connection of UNIBUS modules
- Connections from the Integriti Mobile application (on smart devices) to the Integriti Server (this is however available via a direct HTTP connection)
- Connections to any 3rd party systems such as CCTV or Intercom Systems

Controller Connectivity

Direct TCP (Local Network)

On a local network, the Integriti Software is able to automatically discover Integriti Controllers connected to the local network. This allows installers to easily connect to controllers without needing to configure comms tasks manually through the keypad.

Note: If you have already configured an Integriti comms task using the keypad, and then attempt to enroll a controller using the Auto-Discovery feature, the connection will not work correctly. See the section on “Deleting existing Comms Tasks” for information on how to resolve this issue.

Controller Discovery

Enrolling a controller for direct TCP communications on a local LAN is a two-step process involving the following protocols

- **HTTP:** Outbound from Integriti Software on Port 80, Inbound to Integriti Controller
- **IRIP:** Outbound from Integriti Controller on port 4711, Inbound to Integriti Software

The Integriti software scans the local network (or a user supplied IP Address range) for Integriti controllers by making requests to the controller’s in-built HTTP Server. This process involves an outbound HTTP request from the server to the controller on TCP port 80.

The process of enrolling a controller on the local network is a two-step process in which the server makes an outbound HTTP request to the controller on port 80, this configures the controller to make a TCP connection to the server on port

4711. This connection is outbound from the controller and inbound to the server.

Enrollment

Once a controller has been discovered, the server will send a HTTP request on port 80 to the controller (outbound from the Integrity Software, and Inbound to the Controller) which will configure the controller to begin IRIP communications on port 4711 to the Integrity Software (outbound from the Controller and inbound to the Integrity Software).

This process occurs when the “Connect” button is pressed, with progress displayed in the connection dialog.

Common Issues – See Troubleshooting Section

- Controller is already enrolled to another server
- Controller does not have a valid IP Address
- Firewall blocks outbound HTTP Connection
- Firewall blocks inbound IRIP Connection
- HTTP Connect Request corrupted or blocked by Proxy Server

Direct TCP Connection (Internet or WAN)

In cases where the Controller is not on the same local network as the Integrity Software or is connecting via the Internet (when not using Skytunnel), additional router configuration will be required. It will also be necessary to manually configure the Integrity comms task through the keypad.

Note: This configuration is not suitable for use with Integrity CS. In cases where the CS software and controller are not on the same local network, Skytunnel should be used as an alternative.

Definitions

Throughout the remainder of this section, the following terminology will be used

- **Public IP Address:** The IP address of the router on the public network (usually the internet) which the controller will need to connect to
- **Private IP Address:** The IP address of the Integrity Software on the local network

In environments where you want to connect controllers via the Internet, you can determine the public IP address to use either from the router configuration interface (usually available by entering the IP Address of the default gateway into a web browser).

Alternatively, in Internet connected environments, it can also be determined using a web service such as <http://www.whatismyip.com/>

If you need to connect controllers across two networks which are not connected to the internet, but are not on the same local network, the on-site network administrator should be able to provide you with the public IP address to be used.

Once the public IP Address is known, port-forwarding (and possibly firewall) rules will need to be added to the router to route port 4711 to the Local IP Address of the Integriti Software

Note: The process for adding port-forwarding rules is different for every make and model of router, and is described in the documentation supplied with the router. Alternatively, the on-site network administrator can perform this task.

Once port forwarding rules have been established, you will need to manually configure an Integriti comms task on the controller through the keypad.

1. Log in using the Installer PIN (by default press [0] [1] [OK])
2. Press [Menu] [7] [3] [1]
3. The screen will show
Comms Task To Program
CT:01
This is the "Comms Task Home Screen"
4. Press [OK]
5. Press the right-arrow until the screen shows
Comms Task Type:
Integriti
6. Press [OK]
7. Enter the **Public** IP Address of the server
8. Press [OK]
9. Select "Ethernet" as the first path
10. Place a Y under the C option on the following screen
11. On the screen which shows GIP, place a Y under the P option
12. Press [Menu] [7] [3] [1] to return to the Comms Task Home Screen
13. Press [9] to activate the comms task.
14. In the Integriti software's Navigation Tree, you should now see a new controller named "Auto Discovered (xxxxxx)" where x is replaced by the serial number of your controller.
 - a. If you do not see an auto-discovered controller, see the Common Issues section, and perform the actions specified in the troubleshooting section
15. Right-Click on the newly discovered controller in the navigation tree and press "Connect (Auto)"
16. Observe that the controller connects and begins the data synchronization process

Skytunnel Connection

Troubleshooting

In the event that a controller fails to connect either using Direct TCP or Sky Tunnel or there are some common causes which can be rectified using the following procedures.

Controller is already enrolled to another server

Diagnosis

When the “Connect” button is pressed in the connection dialog, the status window shows one of the following errors.

- IRIP_ERR_MAX_INSIGHT
- The controller is already paired with another server...

Resolution

Delete the existing comms task using an Elite Keypad in accordance with the section “Deleting an existing Integrity Comms Task”

Controller does not have a valid IP Address

Diagnosis

Using an Elite Terminal, perform the following steps at the Keypad.

1. Log in using the Installer PIN (by default press [0] [1] [OK])
2. Press [Menu] [1] [9]
3. Press the Down [v] arrow until the IP Address field is visible
4. Observe the IP Address
 - a. If the value is all zeros, an unexpected or obviously wrong continue to the Resolution section of this section.

Resolution

If it is expected that the local network has a DHCP server, check cabling and the status of the DHCP Server. After any changes are made, it is best to power-cycle the controller and repeat the “diagnosis” step of this procedure.

If there is no DHCP Server and the controller is supposed to have a static IP Address, perform the following.

Using an Elite Terminal, perform the following steps at the Keypad.

1. Log in using the Installer PIN (by default press [0] [1] [OK])
2. Press [Menu] [7] [3] [4]
3. The screen will show
NIC To Program
NIC:01
4. Press [OK]
5. Enter the static IP Address, Subnet Mask and Gateway Address
6. Ensure that the flag under the D option is set to N

Firewall blocks outbound HTTP Connection

Diagnosis

If the controller has a correct IP Address and can be pinged from the server, it may be possible that a firewall (either on the server machine or an intermediary router) is blocking the outbound HTTP Connection.

To test this, use the following procedure.

Note: It is important to ensure that the machine you perform this test from is the machine that is running the Integriti Controller Server. This can be determined by looking at the service control manager and ensuring that the "Integriti Controller Server" is present and running.

1. Open a web browser and enter the following in the address bar and press [Enter].
`http://<controller IP Address>/cgi-bin/basic.xml`
Where <Controller IP Address> is replaced with the controller's IP Address.
2. If the browser shows an XML document containing the serial number and version information of the controller, then you have outbound HTTP connectivity to the controller.
 - a. If the browser shows an error indicating that it cannot connect to the controller, then you do not have outbound HTTP connectivity to the controller
 - b. If the browser shows any other error (such as 404: File Not Found, or 500 Internal Server Error) it is most likely that the controller has an IP Address clash with another device which has a web-server
 - c. If the browser connects successfully, but the Integriti software shows an "HTTP Error 407 Proxy authentication required" this indicates that the site is running a transparent proxy server that has been "Locked Down" This issue should be referred to the customer's IT Department for resolution.
 - i. If the customer's IT department is not willing or able to offer assistance, you can use the Skytunnel connection procedure OR the procedure for "Direct TCP (Internet or WAN)" to establish connectivity.

Resolution

1. Determine which firewall software is installed on the computer running the Controller Server.
2. Add the necessary routing / port-forwarding rules to permit the connection, repeating the diagnosis procedure at each step
 - a. Consult the documentation for the firewall software which is in use and create a rule allowing TCP Port 80 outbound from the server, and inbound to the controller.
 - b. Contact the on-site network administrator and request that the port 80 be opened outbound from the server, and inbound to the controller.

Firewall blocks inbound IRIP Connection

Diagnosis

If the Integrity controller connection dialog displays the following

Sent HTTP Request to Controller

And the connection does not subsequently complete, then this is a fairly good indication that the inbound TCP connection on TCP port 4711 has been blocked by a firewall, or is not routable via a NAT.

Additional Diagnostic Measures

For additional diagnosis, you can use the “Telnet” application on another computer on the same network to attempt to connect to the Integrity Controller Server on port 4711. If you don’t have the Telnet application installed on your computer, see section “Installing the telnet client” in the Appendix.

From another computer on the same network as the controller perform the following steps

1. Open a DOS window by clicking **Start**, type **cmd** in the **Start Search** box, and then press **ENTER**.
2. **Type** `telnet <controller server IP> 4711`
 - a. If the window contents is cleared, and you are presented with a blank screen, the connection has been successful.
 - i. Close the DOS window with the red “x” in the top right corner of the window.
 - b. If you receive an error message, it means that you do not have connectivity to the controller server. Proceed to the resolution section to correct any firewall issues

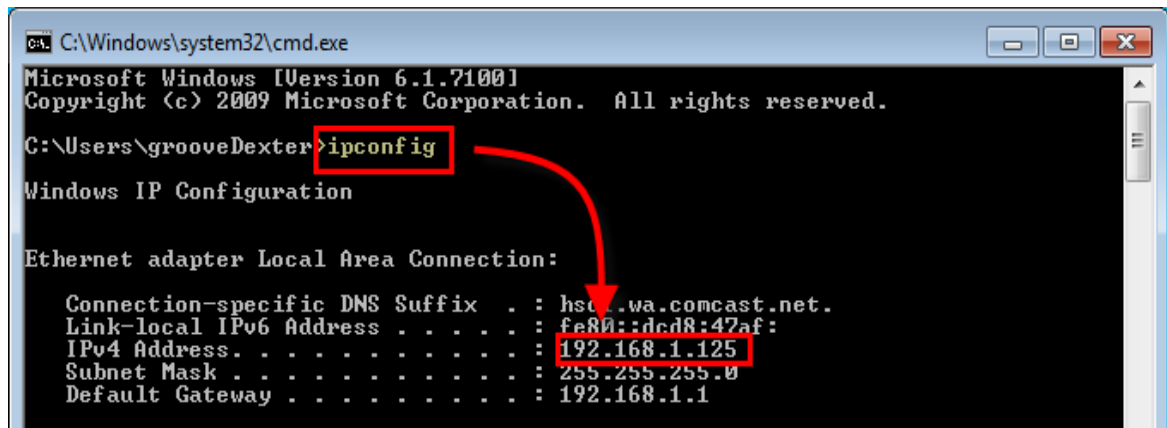
Resolution

1. Determine which firewall software is installed on the computer running the Controller Server.
2. Add the necessary routing / port-forwarding rules to permit the connection, repeating the diagnosis procedure at each step
 - a. Consult the documentation for the firewall software which is in use and create a rule allowing TCP Port 4711 outbound from the server, and inbound to the controller.
 - b. Contact the on-site network administrator and request that the port 4711 be opened outbound from the server, and inbound to the controller.

Appendix

Finding your local IP Address

Open a DOS Window, Type **ipconfig** and Press **[Enter]**.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\grooveDexter>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : hsdsl.wa.comcast.net.
    Link-local IPv6 Address . . . . . : fe80::dcd8:42af:
    IPv4 Address. . . . . : 192.168.1.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

groovyPost

You'll see your IP address listed right above the subnet mask, usually it will say IPv4 Address and follow the prefix **192.168.1.#** or **192.168.0.#** for home networks as shown in the screenshot above.

Deleting Existing Integriti Comms Tasks

Using an Elite Terminal, perform the following steps at the Keypad.

5. Log in using the Installer PIN (by default press [0] [1] [OK])
6. Press [Menu] [7] [3] [1]
7. The screen will show
Comms Task To Program
CT:01
This is the "Comms Task Home Screen"
8. Press OK, to begin to enter the Comms task edit screen and see the type of Comms Task. Note if the type of Comms Task is "Integriti"
9. Press the back arrow [<] to return to the Comms Task Home Screen.
10. If the type of Comms task not "Integriti", press the Down [v] arrow and repeat the process from step 3 (noting that it will now show a different number where it previously showed "CT:01"). Otherwise proceed to the next step.
11. Press the [Off] key. This will change the number of the Comms task to Zero.
12. Press [OK]
13. The Keypad will display
Delete CT01?
14. Press OK. The comms task has now been deleted.
15. Press [END] to log out of the keypad.
16. In the rare case that there is more than 1 Integriti comms task, repeat the process.

Installing the telnet client

1. Open a DOS window by clicking **Start**, type **cmd** in the **Start Search** box, and then press **ENTER**.
2. Type the following command:
pkgmgr /iu:"TelnetClient"

3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
4. When the command prompt appears again, the installation is complete.