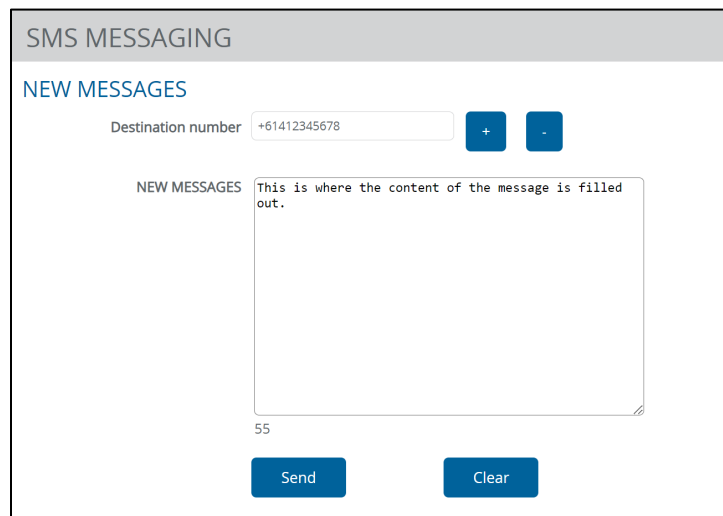


number for the current destination number field. To add a destination number, select the  button and to remove the last destination in the list, select the  button.

Figure 9-6 SMS – New message



SMS MESSAGING

NEW MESSAGES

Destination number  

NEW MESSAGES

This is where the content of the message is filled out.

55

Enter recipient number in the **Destination number** field. It should begin with the “+” symbol followed by the country calling code.

For example:

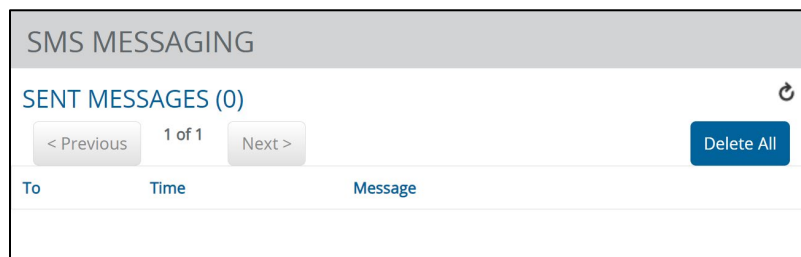
To send a message to the mobile destination number 0412345678 in Australia (country calling code 61), enter “+61412345678”.

After entering the required recipient numbers, type your SMS message in the **New Messages** field. As you type your message, a counter shows how many characters you have entered out of the total number available for your chosen encoding scheme. When you have finished typing your message and you are ready to send it, click **Send** button.

Outbox

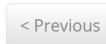
The outbox displays all sent messages.

Figure 9-7 SMS - Outbox



SMS MESSAGING

SENT MESSAGES (0) 

 1 of 1  

To	Time	Message
----	------	---------

Click **Delete All** to delete all messages and empty the outbox.

Dynamic DNS

Dynamic DNS (DDNS) allows your NTC-550 Series router to associate an easy-to-remember domain name such as **[yourdomainname].com** with the regularly changing IP address assigned by your carrier. This feature allows you to connect to the NTC-550 Series router and its internal network more easily for maintenance.

Figure 9-8 Services – Dynamic DNS

The screenshot shows the 'DYNAMIC DNS' configuration page. At the top, there's a header 'DYNAMIC DNS' and a sub-header 'DYNAMIC DNS CONFIGURATION'. Below this, there's an 'Enable' toggle switch set to 'On'. Underneath, there's a 'Dynamic DNS' dropdown menu showing 'www.dhs.org'. Below that are input fields for 'Hostname' (containing 'www.myhostname.com'), 'Username' (containing 'demouser@example.com'), 'Password' (masked with dots), and 'Verify password' (also masked with dots). At the bottom, there is a blue 'Save' button.

To use DDNS, you will need to sign up for a DDNS provider which is supported by the NTC-550 Series router. The supported providers are DHS.org, No-IP, DynDNS, easyDNS, and ZoneEdit. To configure DDNS on the NTC-550 Series router you will require your unique hostname from the provider, as well as your username and password which you used to sign up with the provider.

To configure DDNS:

1. Set the **Enable** toggle to **On**.
2. In the **Dynamic DNS** field select the provider you have signed up with.
3. In the **Hostname** field, enter the custom hostname which you added to your provider.
4. In the **Username** field, enter the username which you used to sign up to your provider.
5. In the **Password** field, enter the password which you used to sign up to your provider.
6. In the **Verify Password** field, re-enter the password which you used to sign up to your provider.
7. Click **Save** button to apply the configuration.

DNS server

The NTC-550 Series router can be configured to use custom DNS servers if required.

Figure 9-9 DNS configuration

The screenshot shows the 'DNS SERVER' configuration page. At the top, there's a header 'DNS SERVER' and a sub-header 'DNS SERVER CONFIGURATION'. Below this, there are input fields for 'Primary DNS server' (containing '9', '9', '9', '9') and 'Secondary DNS server' (containing '1', '1', '1', '1'). Below these are two more input fields: 'DNS cache size' (containing '1000' with a range '(0~5000)') and 'DNS local TTL' (containing '3600' with a range '(0~86400 seconds)'). At the bottom, there is a blue 'Save' button.

To set the DNS servers:

1. In the **Primary DNS server** field, enter the primary DNS server.
2. In the **Secondary DNS server** field, enter the secondary DNS server.
3. In the **DNS Cache Size** field, enter the size of the cache that should be kept on the router.
4. In the **DNS local TTL** field, enter the time to live (TTL) , which is the duration for which a cached request remains in the router.
5. Click the **Save** button to save the configuration.

GPS

The NTC-550 Series router is equipped with GPS which allows the use of location-based services, to monitor field deployed hardware or find the current location of the NTC-550 Series router. The GPS Status window provides up to date information about the current location and the current GPS signal conditions (Position Dilution of Precision (PDOP), Horizontal Dilution of Precision (HDOP), and Vertical Dilution of Precision (VDOP)) of the router.

GPS Configuration

The GPS Configuration page allows you to configure the settings related to GPS and displays information about the GPS connection.

Figure 9-10 GPS – GPS configuration

GPS CONFIGURATION

Enable ☒ On ☐ Off

GPS APPLICATIONS

GPS STATUS

Positioning data source Stand-alone GPS

Date & time GMT+1100 (Australian Eastern Daylight Time)

Latitude & longitude S, E

Altitude & GEOID height m, m

Horizontal speed 0 km/h

Vertical speed 0 km/h

PDOP, HDOP & VDOP ,

Standalone GPS device status Normal

Mobile assisted GPS device status Invalid

Number of satellites 39

SATELLITE STATUS

Index	System	GNSS SV ID	Health status	SV status	SNR	Elevation	Azimuth
1	GPS	16	✓	track	34	23	36
2	GPS	21	✗	track	10	21	338
3	GPS	26	✓	track	27	38	70
4	GPS	28	✓	track	20	27	136
5	GPS	31	✓	track	16	58	133
6	GPS	2	✗	search	0	31	319
7	GPS	3	✗	search	0	74	206

To enable GPS, set **Enable** toggle to **On** and click **Save** button.

Clicking the **Open Google Maps** button opens a Google Maps page with the current GPS location pinned.

The **GPS Status** and **Satellite Status** sections provide an overview of the current GPS details and details of the satellites which are in use.

Assisted GPS

Assisted GPS enables your router to download GNSS data which supplies orbital data to the GPS receiver, enabling it to lock to the satellites more rapidly. The GNSS data is stored on the router to assist the GPS in locating the router.

Figure 9-11 GPS – Assisted GPS

ASSISTED GPS

ASSISTED GPS CONFIGURATION

Enable ☒ On ☐ Off

Maximum retry count (1~5)

Retry delay (5~60) minutes

Auto update period (0=disable, 1~24) hours

GNSS data last update N/A

GNSS data expires N/A

AGPS last update N/A

To setup automatic updates of GNSS data, set the **Enable** toggle key to the **ON** position and then set the automatic retry options. For each retry, the router checks for an updated GNSS data file and downloads the GNSS data if newer than the currently stored data.

The **GNSS data last update** field represents the time that the GNSS data file was created, the **GNSS data expires** field indicates the time until this data is valid, and the **A-GPS last update** field specifies the last time the router attempted to retrieve an update to the GNSS data.

When you have finished configuring the settings, click **Save** button to save the settings.

GPS Odometer

The GPS Odometer is used to record the distance that the router has travelled.

Figure 9-12 GPS – GPS odometer

GPS ODOMETER

ODOMETER CONFIGURATION

Enable

Threshold (1~100) meter

Measurement system

ODOMETER STATUS

Odometer reading 0.0 meter

Start time Invalid Date

The table below lists the GPS Odometer details.

Table 9-12 GPS – GPS Odometer Items

Item	Description
Odometer Configuration	
Enable	Set to On to enable GPS Odometer
Threshold	Enter the required value. It specifies the minimum distance that the router must travel from its current position before the Odometer reading increases.
Measurement system	Select the unit of measurement for the Odometer reading. The options are metric and imperial .
Odometer Status	
Odometer reading	The distance that the device has travelled since the time listed in the Odometer start time field.
Odometer start time	The time that recording of distance travelled began.

Click **Save** to save the settings.

Click **Reset** to reset the odometer reading to zero and the odometer start time to the current time.

GPS Geofence

The GPS Geofence allows you to designate a circular area and then use the router's GPS position to monitor when the NTC-550 Series router moves out of or into that area. You can configure notifications to be sent when the unit enters or exits the area. Notification types are set on the Event notification configuration page.

Figure 9-13 GPS – GPS Geofence

GPS GEOFENCE

GEOFENCE CONFIGURATION

Enable
☒ On
☐ Off

Coordinate units
DMS (Degrees/Minutes/Seconds)

Measurement system
metric

Save

GEOFENCE LIST

+ Add

Name	Latitude (DMS)	Longitude (DMS)	Radius (km)	Status	Notification		
DemoFence	S35° 17' 31.9992"	E150° 00' 38.0016"	500	in	None		

The table below lists the GPS Geofence Configuration details

Table 9-13 GPS – GPS Geofence Configuration Items

Item	Description
Enable	Set to On to enable GPS Geofence. When On, your currently defined Geofences appear in the Geofence list, see below.
Coordinate units	Select how to display the Coordinate units. The options are Decimal degrees and DMS (Degrees/Minutes/Seconds)
Measurement system	Select the type of Measurement system to display the radius of the geofence. Options are metric (kilometres) and imperial (miles).

Click **Save** to save the settings.

The Geofence List displays the list of the Configured geofences and their details.

The table below lists the details of the Geofence List.

Table 9-14 GPS Geofence List Items

Item	Description
Name	Name given to the geofence during configuration.
Latitude (decimal degrees)	Latitude of the center of the geofence.
Longitude (decimal degrees)	Longitude of the center of the geofence.
Radius (km)	Radius of the geofence.
Status	In , if the router is inside the radius. Out , if the router is outside the radius.
Notification	The event that triggers a notification. See Add Geofence in next section for the available notification types.
	Click to edit that Geofence. The user interface is the same as the add Geofence configuration screen, see next section below.
	Click to delete that geofence.

To add a new geofence click **+Add** button in the Geofence List. The Geofence configuration page displays.

Figure 9-14 GPS – GPS Geofence – Geofence configuration

GEOFENCE CONFIGURATION

Name

Latitude ° ' "

Longitude ° ' "

Radius (≥ 0 km)

Notification

The table below lists the new geofence configuration details.

Table 9-15 GPS – New Geofence Configuration Items

Item	Description
Name	Enter a name for the geofence. The geofence is added to the Geofence List with this name.
Latitude	Enter the latitude of the center of the geofence.
Longitude	Enter the longitude of the center of the geofence.
Radius	Set the radius of the Geofence.
Notification	Select an event to trigger a notification. The options are: None – This effectively turns the Geofence function off, although the router continues to monitor the location of the device with respect to the Geofence settings. To properly disable the Geofence function, set the Geofence operation toggle key to the off position. Entry – A notification is triggered when the router enters the Geofence radius. Exit – A notification is triggered when the router leaves the Geofence radius. Entry/Exit – A notification is triggered when the router crosses the Geofence radius line.
Open Google maps button	The Open Google Maps button serves the following purposes: • When no latitude and longitude has been entered, the Google maps button displays the router's current location on the map. • When coordinates have been entered, clicking on the Google maps button checks that your coordinates go to where you expect them to be.

Click **Save** to save the settings and add new geofence or complete editing a geofence.

To configure event notifications, click **Event Notification Configuration** link. It will direct you to Event Configuration section.

Remote management

OMA-LWM2M

The OMA Lightweight M2M (OMA-LWM2M) protocol was designed by the Open Mobile Alliance to provide remote device management specifically for M2M devices. It is less taxing on the system and network than OMA-DM and TRS-069. OMA-LWM2M runs over UDP and supports asynchronous notifications when a resource changes.

It provides:

- Firmware upgrades
- Device monitoring and configuration
- Server provisioning

To configure the Lightweight M2M client, set the Enable LwM2M toggle key to **On** position.

Figure 9-15 OMA-LWM2M configuration

The screenshot displays the 'LWM2M CONFIGURATION' interface, which is divided into two main sections: 'LWM2M CLIENT CONFIGURATION' and 'OVERRIDE SERVER SETTINGS'.

LWM2M CLIENT CONFIGURATION

- LwM2M endpoint:** ntc_502:219943231100012
- Enable LwM2M:** A toggle switch set to 'On'.
- Management wwan profile no.:** A dropdown menu showing 'Default route'.
- Management port:** A text input field containing '1-65535'.

OVERRIDE SERVER SETTINGS

- Override enable:** A toggle switch set to 'On'.
- Override once:** A toggle switch set to 'Off'.
- Server URI:** An empty text input field.
- Registration lifetime:** A text input field containing '600', with a note '(60~86400) seconds'.
- Bootstrap server:** A toggle switch set to 'Off'.
- Queue mode:** A toggle switch set to 'Off'.
- Security mode:** A dropdown menu showing 'Pre-Shared Key'.
- Client identity:** A text input field containing 'Test'.
- PSK coding:** A dropdown menu showing 'hex'.
- PSK key:** A text input field containing 'abcd1234'.

A blue 'Save' button is located at the bottom center of the configuration area.

The table below lists the LWM2M Configuration details.

Table 9-16 LWM2M Configuration items

Item	Description
LWM2M Client Configuration	
LWM2M Endpoint Name	This is the unique ID the device will use to identify itself with Lwm2M servers.
Enable Lwm2M	Set to On to enable Lwm2M. The configuration settings display.
Management wwan profile no.	Select the wwan profile to use with Lwm2M client. Any profile, except default route, will require VLAN mapping. Refer to VLAN settings section for VLAN setup.
Management port	Enter the port used for client management. UDP port 5683 is the default port for unencrypted communication. UDP port 5684 is the default port for secure communication.
Override Server Settings	
Override Enable	Set to On to enable Override settings. The configuration settings display. The Lwm2M client maintains the list of servers that it will connect to as part of its internal state. Enabling this setting will allow a user to specify new server details that will override whatever current settings the client has.
Override Once	Enable this option to apply the new server details only once, when the client is restarted (normal flow for configuring/reconfiguring the client) and disable this option to apply the new server details every time the client restarts (used for debugging/troubleshooting.)
Server URI	Enter the URI of the Lwm2M server to connect to. It must be a fully specified CoAP or CoAPS URI, including port number, e.g. coap://server.com:5683 or coaps://server.com:5684.
Registration Lifetime	Specify the interval (in seconds) at which the Lwm2M client will send registration updates (i.e. heartbeat messages) to the server.
Bootstrap server	Set to On , if the new server is an Lwm2M bootstrap server
Queue mode	When set to On , the UDP binding mode is reported to the server as queued (UQ binding mode). When set to Off , it is reported as not queued (U binding mode)
Security mode	Select the security mode to be used to connect to the server. The options are No Security and Pre-shared Key . If Pre-shared key is selected the below fields display.
Client Identity	Enter the identity key associated with your pre-shared key.
PSK coding	Select the type of coding for the for the key. The options are hex and text
PSK key	Enter the key. The key can be a hexadecimal string or a plain text string depending on the PSK coding type selected

Supported LWM2M objects

The table below lists the supported object IDs on the NTC-550 Series router. For further information on the objects, refer to the [Open Mobile Alliance LWM2M registry](#).

Table 9-17 LWM2M supported objects

Object	Object ID	Note
LWM2M Server	1	
LWM2M Access Control	2	
Device	3	
Connectivity Monitoring	4	
Firmware Update	5	
Location	6	
APN Connection Profile	11	
System Log	10259	Custom object
Runtime Database Access	10260	Custom object
Phone Module Info	33040	Custom object

Timeouts

Most mobile networks use stateful firewalls or NAT where the timeout for UDP is approximately 1-2 minutes. If this applies to you, we suggest either configuring the LwM2M client with a registration lifetime that falls within this period (e.g. 60 seconds) or using the queued ("UQ") UDP binding mode.

SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NTC-550 Series router (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

Figure 9-16 SNMP Configuration

The image shows a web-based configuration interface for SNMP. It is divided into two main sections: 'SNMP CONFIGURATION' and 'SNMP TRAPS'. In the 'SNMP CONFIGURATION' section, there is a toggle for 'SNMP' set to 'On'. Below it, the 'SNMP Port' is set to '161' (with a range of 1-65535), the 'Version' is set to 'v1v2c' via a dropdown, the 'Read-only community name' is 'public', and the 'Read-write community name' is 'private'. A 'Download MIB' button is present. The 'SNMP TRAPS' section has a toggle for 'SNMP TRAPS' set to 'On'. It includes fields for 'Trap destination', 'Heartbeat interval' (43200 seconds), 'Trap persistence time' (500 seconds), and 'Trap retransmission time' (21600 seconds). There are 'Send heartbeat' and 'Save' buttons at the bottom.

Configuring SNMP

6. Set the **SNMP** toggle to **On** to enable SNMP.
1. In the **SNMP Port** field, enter the SNMP port to be used.
2. Use the **Version** dropdown to set the SNMP version to be used. Available options are **v1v2c** and **v3**.
3. In the **Read-only community name** enter the read community name of the network.
4. In the **Read-write community name** enter the write community name of the network.
5. Select the **Save** button below the **SNMP Traps** section to apply the configuration.

Configuring SNMP traps

The NTC-550 Series router can be configured to send SNMP traps to a central SNMP Network Management System (NMS) when certain events occur. To configure the SNMP traps:

1. Set the **SNMP Traps** toggle to **On**.

2. In the **Trap Destination** field, enter the address of the SNMP NMS.
3. In the **Heartbeat interval** field, enter the interval in seconds which the NTC-550 Series router should send a heartbeat.
4. In the **Trap persistence time** field, enter the interval in seconds that the NTC-550 Series router should attempt to send a specific trap after the initial occurrence that triggered the trap.
5. In the **Trap retransmission time** field, enter the interval in seconds that the NTC-550 Series router should wait before retransmitting the trap.
6. Use the **Send heartbeat** button to send a test heartbeat.
7. Select the **Save** button to save and apply the settings.

TR-069

The Technical Report 069 (TR-069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol and provides several benefits for the maintenance of a field of CPEs:

- Simplifies the initial configuration of a device during installation
- Enables easy restoration of service after a factory reset or replacement of a faulty device
- Firmware and software version management
- Diagnostics and monitoring

Note: You must have your own compatible ACS infrastructure to use TR-069. To access and configure the TR-069 settings, you must be logged into the router with the root account.



When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

The NTC-550 Series router sends “inform” messages periodically to alert the ACS server that it is ready. These inform messages can also be configured to accept a connection request from the ACS server. When a connection is established, any tasks queued on the ACS server are executed. These tasks may be value retrieval or changes and firmware upgrades.

To access the TR-069 configuration page, click the **Services** tab on the top menu bar, and in the **Remote management** section, click **TR-069**.

Figure 9-17 TR069 configuration

TR-069

TR-069 CONFIGURATION

Enable TR-069
☒ On
☐ Off

ACS URL

ACS username

ACS password
☐

Verify ACS password
☐

Connection request username

Connection request password
☐

Verify connection request password
☐

Connection request port

Management wwan profile no.

Enable periodic ACS informs
☒ On
☐ Off

Inform period

Randomise initial inform
☐ On
☒ Off

LAST INFORM STATUS

Start at

End at

TR-069 DEVICEINFO

Manufacturer

Manufacturer OUI

Model name

Description

Product class

Serial number

To configure TR-069:

1. Set **Enable TR-069** toggle key **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. In the **ACS username** field to specify the username used by the server to authenticate the CPE when it sends an "inform" message.
4. In the **ACS password** and **Verify ACS password** fields, enter the password used by the server to authenticate the CPE when it sends an "inform" message.

5. In the **Connection request** username field, enter the username that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
6. In the **Connection request password** and **Verify password** fields, enter the password that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.
7. In the **Connection request port** field, enter the port that the request should connect to.
8. In the **Management wwan profile no.** field, enter the WAN profile that should handle the request.
9. The inform message acts as a beacon to inform the ACS of the existence of the router. Select **Enable periodic ACS informs** toggle key to **On** to turn on the periodic ACS inform messages.
10. In the **Inform Period** field, enter the number of seconds between the inform messages.
11. Select the **Save** button to save the settings.

Internet of Things

MQTT

The MQTT page is used to configure the NTC-550 Series router to use the MQTT protocol. MQTT is a standards-based messaging protocol used for machine-to-machine communication. Information is sent to clients in the form of a 'topic'. The NTC-550 Series router can be configured to send device information and neighbouring cells as a topic to common IoT monitoring applications, such as Microsoft Azure IoT Hub and Amazon IoT, using MQTT.

Figure 9-18 MQTT Client

MQTT CLIENT

MQTT CLIENT CONFIGURATION

MQTT client enable ☒ On ☐ Off

Save

CLIENT LIST **+ Add**

Name	Client ID		
IoT MQTT Demo Server	myclientid		

Configuring MQTT

Prerequisites

To configure MQTT on the NTC-550 Series router, you need to create the device on your external MQTT client provider, and generate certificates and keys as required for secure authentication. Refer to your external MQTT provider's documentation for the required authentication configuration.

To configure MQTT:

1. Set the **MQTT client enable** toggle to **On**.
2. Click **+Add** button to add a new client. The **MQTT Client Setting** page displays.

Figure 9-19 MQTT – MQTT Client configuration

MQTT CLIENT

MQTT CLIENT SETTING

Name

Host name

Client ID

MQTT port MQTT: 1883, MQTTS: 8883, default: automatic

Auth username

Auth password

Keepalive (0-65535) secs

MQTT protocol

CA file Not uploaded

Client cert file Not uploaded

Client key file Not uploaded

DEVICE ID DATA

Enable

CELL REPORT

Enable

GPS LOCATION

Enable

The table below lists the MQTT Client Setting configuration details.

Table 9-18 MQTT Client Settings configuration items

Item	Description
Name	Enter the name of the client to identify the client on the NTC-550 Series router
Host name	Enter the Hostname of your client
Client ID	Enter Client Id of the client. The Client Id may match the name of your client provider, for example, the name of your AWS IoT 'Thing'.

Item	Description
MQTT port	Enter the port MQTT should be initiated over.
Auth username	Enter the username of the connection.
Auth password	Enter the password of the connection.
Keepalive	Enter the number of seconds that the connection should be kept alive.
MQTT protocol	Enter the version of MQTT that should be used.
CA file	Upload the Certificate Authority file.
Client cert file	Upload the client certificate file generated as part of your client's configuration.
Client key file	Upload the client key file generated as part of your client's configuration.

3. Click **Save** to save the settings.
4. Configure MQTT topics. You can configure any one or all the available clients.

Figure 9-20 MQTT – MQTT Client Configuration – MQTT topics

DEVICE ID DATA

Enable ☒ On ☐ Off

Publish topic string

Publish QoS ▼

Minimum publish interval seconds

CELL REPORT

Enable ☒ On ☐ Off

Publish topic string

Publish QoS ▼

Minimum publish interval seconds

GPS LOCATION

Enable ☒ On ☐ Off

Publish topic string

Publish QoS ▼

Minimum publish interval seconds

Drift interval metres

Table 9-19 MQTT Client Topic Items

Item	Description
Device ID Data	
Enable	Set to On to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • At most once • At least once • Exactly once At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
Cell Report	
Enable	Set to On to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • At most once • At least once • Exactly once At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
GPS Location	
Enable	Set to On to enable the topic
Publish topic string	Enter a string which will identify the topic on the MQTT client.

Item	Description
Publish QoS	Select the Publish QoS (Quality of Service) for the topic. Three options are available: • At most once • At least once • Exactly once At most once is the lowest level of QoS in MQTT, which offers a best-effort delivery mechanism where the sender does not expect an acknowledgment or guarantee of message delivery. At least once guarantees the message delivery but potentially exists duplicate messages. Exactly ensures that messages are delivered exactly once without duplication
Minimum publish interval	Set the minimum publish level in seconds. This is the amount of time the NTC-550 Series router will wait before attempting to publish a message.
Drift interval	Enter the radius. If the device drifts beyond this radius, the message is sent.

- Click **Save** to create the client. The client displays in the MQTT client list.

Figure 9-21 MQTT – MQTT Client Configuration – MQTT client list

CLIENT LIST		+ Add	
Name	Client ID		
IoT MQTT Demo Server	myclientid		

- Click  to edit the client.
- click  to delete the client.

Cumulocity agent

The Cumulocity agent page allows you to configure a cumulocity agent on the NTC-550 Series router which facilitates communication and data exchange between the router and the Cumulocity IoT platform. It enables centralized management and monitoring of devices.

To access the Cumulocity agent page navigate to **Services > Internet of Things > Cumulocity agent**.

Figure 9-22 Cumulocity Agent

CUMULOCITY AGENT

AGENT CONFIGURATION

Agent ☒ On ☐ Off

Version 1.1.2

Device ID 219743243300074

Status stopped

Registered No

[Clear credentials](#)

Server

GPIO analog measurements seconds (0=disable)

GPS position update interval seconds (0=disable)

GPS position event seconds (0=disable)

System resources measurements seconds (0=disable)

Connection signal measurements seconds (0=disable)

ModBus TCP port

ModBus read only

ModBus serial port

Log level

[Save](#)

The table below lists the Cumulocity Agent configuration details.

Item	Description
Agent	Set toggle to On to enable the agent.

Item	Description
Version	Version of the Cumulocity platform.
Device ID	Router's serial number. A unique identifier for the router in Cumulocity.
Status	Status of the agent.
Registered	Displays if the device is registered with the Cumulocity platform.
Clear credentials button	Click to clear credentials related to an existing cumulocity configuration.
Server	Enter the URL of the Cumulocity platform.
GPIO analog measurements	Enter the time interval at which the General Purpose Input/Output GPIO measurements are communicated.
GPS position update interval	Enter the time interval at which the GPS position is communicated.
GPS position event	Enter the time interval to generate a GPS position event. A GPS position event is generated by the device to report its current geographic location, using the c8y_Position fragment.
System resources measurements	Enter the time interval at which system resource measurements such as CPU usage, memory consumption, disk, and network I/O are communicated.
Connection signal measurements	Enter the interval at which the cellular signal measurements are communicated.
ModBus TCP port	Enter the server port for ModBus TCP connection. Default port is 502.
ModBus read only	Enter 0 to disable, 1 to enable.
ModBus serial port	Enter the device serial port for ModBus connection. Default port is /dev/ttyHS1
Log level	Enter the log level to be communicated. The available log levels are: • 1 – dmesg • 2 – ipsec • 3 – logread • 4 – ntcagent

Serial data status

It shows the details of configured and running data streams.

Figure 9-23 Serial Data Status

SERIAL PORTS		
Host port : Serial port (generic)		
Baud rate : 115200		
Data bits : 8		
Stop bits : 1		
Parity : None		
RX count (bytes) : 0		
TX count (bytes) : 0		
UDP CONNECTIONS		
Server listening on port : 1		
Client list	Local address : Port	Peer address : Port
	0.0.0.0:1	0.0.0.0:*

Data stream manager

The data stream manager allows you to create mappings between two endpoints on the router. These endpoints may be physical or virtual, for example, a serial port connected to the router's USB port could be configured as an endpoint or you could configure a TCP Server as an endpoint. You can then configure a virtual data tunnel or "stream" between the endpoints.

The data stream manager provides a wide range of possibilities including the forwarding and translation of data between any of the endpoints. For example, you could send the GPS data from the built-in module to a TCP server running on the router. In each case, the logical flow of the stream is from Endpoint A to Endpoint B.

Customers interested in developing their own applications to create custom endpoints and streams can contact Lantronix about our Software Development Kit.

Endpoints

To create a data stream, you must first define endpoints. The NTC-550 Series router allows you to define the following types of endpoints:

- Serial port (generic)
- TCP server
- TCP client
- UDP server
- UDP client
- GPS data (for devices with GPS receiver)
- User defined executable
- RS232 port
- RS485 port
- RS422 port

- Modem emulator
- PPP server
- IP modem
- TCP connect-on-demand
- DNP3 master

To access the Endpoint page, navigate to **Services > Data Stream Manager > Endpoints**.

To add an endpoint, select the required **Endpoint type**, the configuration settings for the endpoint display. Once you set the values for all the configuration fields for an endpoint and click Save, the endpoint displays in the Endpoints List.

Serial Port (generic) Endpoint

When a USB to Serial cable is used, this creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

Figure 9-24 Serial Port endpoint Configuration

TCP Server Endpoint

This creates a TCP server endpoint with the following options available.

Figure 9-25 TCP Server Endpoint Configuration

ADD TCP SERVER ENDPOINT

Endpoint name

Port number

1-65535

Keep alive

☒ On ☐ Off

Keep Count

1-50

Keep idle

1-10000

Keep interval

1-1000

Max children

1-20

Save

Cancel

TCP Client Endpoint

This creates a TCP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

Figure 9-26 TCP Client Endpoint Configuration

ADD TCP CLIENT ENDPOINT

Endpoint name

IP address

Port number

1-65535

Keep alive

☒ On ☐ Off

Keep Count

1-50

Keep idle

1-10000

Keep interval

1-1000

Time out

1-1000

Save

Cancel

UDP Server Endpoint

This creates a UDP server endpoint with the following options available.

Figure 9-27 UDP Server Endpoint Configuration

ADD UDP SERVER ENDPOINT

Endpoint name

Port number 1-65535

Max children 1-20

UDP Client Endpoint

This creates a UDP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

Figure 9-28 UDP Client Endpoint Configuration

ADD UDP CLIENT ENDPOINT

Endpoint name

IP address

Port number 1-65535

Time out 1-1000

GPS Data Endpoint

This creates a GPS data endpoint.

Figure 9-29 GPS Data Endpoint Configuration

ADD GPS DATA

Endpoint name

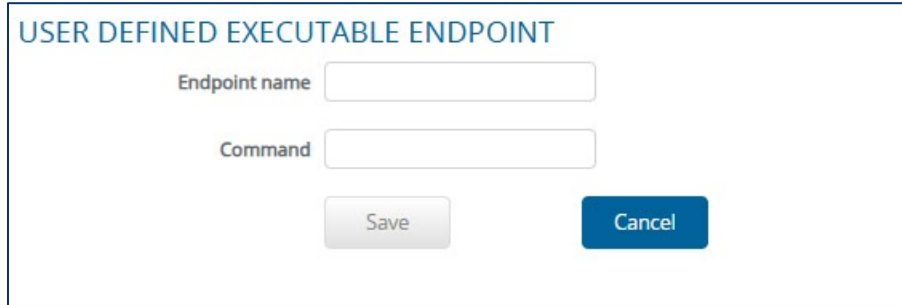
User Defined Executable Endpoint

Allows you to specify an executable and parameters to be used as an endpoint. For example, the following executable reads the phone module temperature every second.

```
while true; do rdb_get wwan.0.radio.temperature; sleep 1; done
```

The temperature can then be sent to another endpoint.

Figure 9-30 User Defined Executable Endpoint Configuration



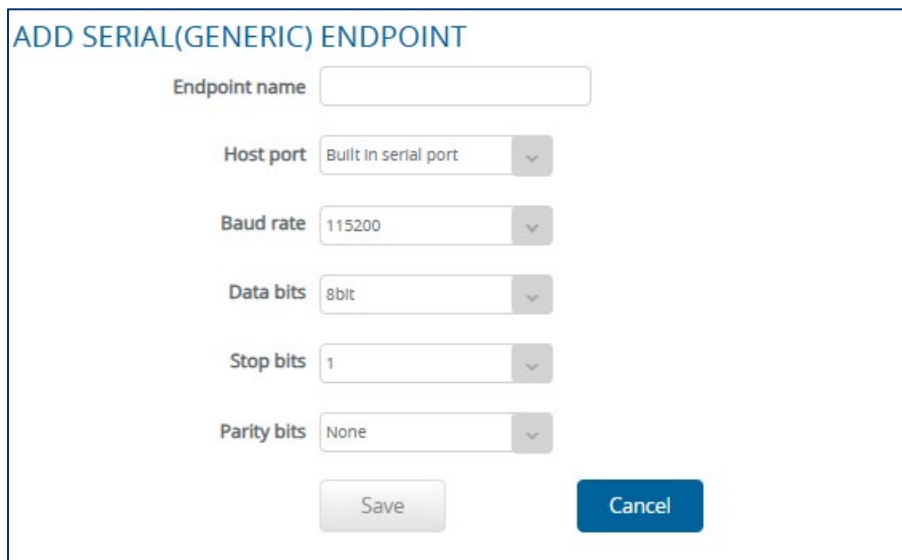
A dialog box titled "USER DEFINED EXECUTABLE ENDPOINT". It contains two text input fields: "Endpoint name" and "Command". Below these fields are two buttons: "Save" (light gray) and "Cancel" (blue).

RS232/RS485/RS422 Port Endpoints

These endpoint types all use the built-in serial port.

When one of these endpoints is used to create a stream, the hardware switches to accommodate the chosen serial communication interface.

Figure 9-31 RS232/RS485/RS422 Port Endpoints Configuration



A dialog box titled "ADD SERIAL(GENERIC) ENDPOINT". It contains several configuration fields: "Endpoint name" (text input), "Host port" (dropdown menu showing "Built in serial port"), "Baud rate" (dropdown menu showing "115200"), "Data bits" (dropdown menu showing "8bit"), "Stop bits" (dropdown menu showing "1"), and "Parity bits" (dropdown menu showing "None"). At the bottom are "Save" (light gray) and "Cancel" (blue) buttons.

Modem Emulator Endpoint

Modem emulator allows you to connect legacy equipment such as an RTU or PLC to the serial port of the router in place of a traditional dial-up modem. The NTC-550 Series router emulates the dial-up modem's behaviour and passes the serial data over the IP network.

Figure 9-32 Modem Emulator Endpoint Configuration

MODEM EMULATOR ENDPOINT (MODEM_EMULATOR)

Endpoint name

Host port

Built in serial port

Baud rate

115200

Data bits

8bit

Stop bits

1

Parity bits

None

Hardware flow control

None

Software flow control

None

DSR action

Always

DCD action

Always

DTR action

Ignore

RI action

Always

Enable auto answer

On

Off

Circuit auto answer rings

0

ADVANCED STATUS

Echo enable

On

Off

Quiet mode

On

Off

Send OK on carriage return

On

Off

Suppress line feeds

On

Off

Send OK on unknown command

On

Off

Verbose mode

On

Off

Save

Cancel

Table 9-20 Modem Emulator Endpoint Configuration Items

Item	Description
Modem Emulator endpoint	
Endpoint name	Enter a name for the endpoint
Host port	Select the serial port to use. If no USB-to-Ethernet adapter is connected, the only available selection is the Built-in serial port.
Baud rate	Select baud rate. The serial (V.24) port baud rate. By default the serial line format is 8 data bits, No parity, 1 Stop bit. Refer to the AT (V.250) AT Command Manual if you need to change the serial line format.
Data bits	Select data bits. The default serial line data bits setting used is 8. Options include 5 – 8 bits.
Stop bits	Select stop bits. The default stop bit setting is set to 1. However, the stop bit setting can be set to 2 bits if required.
Parity bits	Select parity bits. Parity is the means to detect transmission errors. An extra data bit is transmitted with each data character and is arranged in a fashion such that the number of 1 bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then this shows the data must be corrupt. Options include none, odd or even. The default setting is none for no parity checks.
Hardware flow control	Select hardware flow control • None – Serial port flow control off • RTS/CTS - Serial port uses RTS/CTS flow control
Software flow control	Select software flow control • None • Xon/Xoff
DSR action	Select the Data Set Ready action. This is an output from the modem and this configuration determines the pin's behaviour. • Always – DSR is always on. • Registered – When connected to a remote CSD endpoint, sets pin to “on” when modem is in data mode. • Session established – When connected to PPP endpoint, sets pin on when PDP is connected, when connected to IP modem endpoint, sets pin to on when modem is in online state (e.g. data connection is established). • Never – DSR is always off. • Mimic DTR – mimics the DTR pin.
DCD action	Select DCD action. Determines how the router controls the state of the serial port Data Carrier Detect (DCD) line. • Always On – DCD is always on.

Item	Description
	• Connect – DCD is on when a connection is established in response to an ATD command or DTR dial. • Session established – Pin is on when PPP session is in progress or modem is in an online state (e.g. data connection is established). • Always Off – DCD is always off.
DTR action	Select DTR action. Determines how the router responds to change of state of the serial port DTR line • Ignore – Take no action • Enter Command State – when connected to PPP endpoint, this is equivalent to disconnect. When connected to IP modem endpoint, this enters online command state (e.g. process AT commands without dropping the connection). • Disconnect – terminates connection.
RI action	Select RI action. Determines how the router controls the state of the serial port RI (Ring Indicator) line. • Always On: RI is always on. • Incoming Ring: RI is on when an incoming connection request is received. • Always Off: RI is always off
Enable auto answer	When enabled, the router accepts incoming connections.
Circuit auto answer rings	Select a value. Sets the number of incoming rings after which the router will answer incoming circuit switched data calls. The default value is Off. The other available options are from 1 to 12.
Advanced Status	
Echo enable	Enables echo on the serial side. All commands are echoes. This can be turned on/off via ATE1 and ATE0 commands. Recommended setting for this option is On .
Quiet mode	When On , there is no output from the modem on the serial side, i.e. you do not see OK, Connect etc. Recommended setting for this option is Off .
Send OK on carriage return	If enabled, will print OK every time CR is received on the serial side. Recommended setting for this option is On .
Suppress line feeds	If enabled, line termination is using CR (13). If disabled, line termination is CR LF (13 10). Recommended setting for this option is Off.
Send OK on unknown command	Will send OK when an unknown/invalid AT command is received. Recommended setting for this option is On .
Verbose mode	The modem returns messages to the computer to indicate the return status of commands and interrupts such as incoming call and call progress. Recommended setting for this option is On.

PPP Server Endpoint

Figure 9-33 PPP Server Endpoint Configuration

PPP SERVER ENDPOINT (PPP)

Endpoint name

PPP server IP address · · ·

PPP client IP address · · ·

MTU 128-16384

MRU 128-16384

Raw PPP mode

Disable CCP

Table 9-21 PPP Server Endpoint Configuration Items

Item	Description
PPP server IP address	Enter IP address of the PPP server. This defaults to the router's current IP address.
PPP client IP address	Enter IP address of the PPP client. This defaults to the next IP address in the DHCP range after the router's address.
MTU	Enter maximum transmission unit size of packets sent by the PPP server.
MRU	Enter the maximum receive unit size of packets received by the PPP server.
Raw PPP mode	This option is provided for compatibility with legacy devices that assume there is a line available and do not require dial commands to be issued first. Raw PPP mode is turned Off by default.
Disable CCP	This option is provided for use with devices that do not support the compression control protocol. The router uses the compression control protocol and the toggle key is in the Off position by default.

IP Modem Endpoint

This endpoint can be used to connect to the modem emulator endpoint to achieve similar functionality to PAD Daemon. It allows a data stream from the serial port to a TCP/UDP server/client and provides modem control lines and AT interpreter on the serial side.

Figure 9-34 IP Modem Endpoint Configuration

ADD IP MODEM ENDPOINT

Endpoint name

Outgoing connections enabled ☐ On ☐ Off

Incoming connections enabled ☐ On ☐ Off

Mode ▼

Exclusive mode ☐ On ☐ Off First TCP connection has priority

No send delay ☐ On ☐ Off Selecting ON will disable Nagle algorithm

Keepalive ☐ On ☐ Off

Keepalive count 1-50

Keepalive idle 1-10000 seconds

Keepalive interval 1-1000 seconds

Table 9-22 IP Modem Endpoint Configuration Items

Item	Description
Outgoing connections enabled	Enables or disables the ability of the router to initiate outbound network connections i.e. act as a networking client. It will attempt to connect to the remote server when relevant activity is detected on the serial side e.g. ATD dial command.
Incoming connections enabled	Enables or disables the ability of the router to accept incoming network connections i.e. act as a networking server. When an incoming connection from a remote client is detected, the router simulates a dial-in call on the serial line.
Mode	Sets the IP modem to either TCP or UDP mode.
Exclusive mode (TCP mode only)	When this is Off , any new client connection disconnects the previous client connection and uses a new client instead.
No send delay	Disables Nagle algorithm. Disabling this is sometimes important so that serial data is sent as soon as possible instead of waiting for a more optimal block

Item	Description
	of data for Ethernet. Enabling this effectively reduces latency but increases the amount of network traffic.
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active. When enabled the below fields display.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	Enter the duration between two successive keepalive retransmissions.

TCP Connect-on-demand Endpoint

The TCP connect-on-demand endpoint allows data to be buffered and then sent to a TCP server when the buffer has been filled. It is primarily useful in situations where you do not want 'keep alive' packets to keep the socket open and create an overhead when the TCP data connection is not in use.

Figure 9-35 TCP Connect-on-demand Endpoint Configuration

ADD TCP CONNECT-ON-DEMAND ENDPOINT

Endpoint name

Primary server IP address

Port number 1-65535

Backup server IP address Leave blank if backup server not required

Port number 1-65535

Inactivity timeout 0-10000 seconds, 0 Disconnect immediately

Minimum transmit buffer size 576-1500

Start ID Send this ID to server when connected

End ID Send this ID to server before disconnecting

Keep alive ☒ On ☐ Off

Keep Count 1-50

Keep idle 1-10000

Keep interval 1-1000

Table 9-23 TCP Connect-on-demand Endpoint Configuration Items

Item	Description
Primary server IP address	Enter IP address of the TCP server to which the router should attempt the initial connection.
Port number	Enter the port number that the TCP server operates on.
Backup server IP address	Enter IP address. If connection to the primary server fails, the router will attempt to connect to this address.
Port number	Enter the port number that the backup TCP server operates on.
Inactivity timeout	Enter the period, in seconds, that the socket is considered idle/inactive if no packets are sent. The timer begins at the end of the last sent packet. The valid range is 0-10000 seconds. If this field is set to 0, the client disconnects immediately after sending a packet.
Minimum transmit buffer size	Enter the number of bytes that must be reached before the client decides to transmit.
Start ID	This is a string which, if configured, is sent before any serial data is sent, every time the client connects <START ID><SERIAL DATA>
End ID	This is a string which, if configured, is sent after all serial data, just before the client disconnects <START ID><SERIAL DATA><END ID>
Keepalive	Keepalive sends a message to check that the link is still active or to keep it active. When enabled the below fields display.
Keepalive count	Enter the number of keepalive messages to send.
Keepalive idle	Enter the duration between two keepalive transmissions when in idle condition.
Keepalive interval	Enter the duration between two successive keepalive retransmissions.

The configured endpoints display in the Endpoints List.

Figure 9-36 Endpoints List

ADD ENDPOINTS

Endpoint type
None

ENDPOINTS LIST

Name	Type	Summary		
Serial-generic	Serial	Dev name:/dev/ttyHS1 Baud rate:115200 Parity:none Data bits:8 Stop bits:1		
UDP	UDP Server	Max children:1 Port number:1		

Click to edit that endpoint and click to delete that endpoint

Data stream

When you have created the required endpoints, you can then proceed to set up a data stream. A data stream sends data from one endpoint to another, performing any transformation of the data as required. When a stream is added, an underlying process on the router checks the validity of the stream, checking for conflicts and illogical configurations.

Important:



- When any changes to the Data stream manager configuration are detected, all data streams are stopped and restarted as per the new configuration.
- Multiple Modbus clients cannot connect simultaneously to Modbus serial slaves connected to the router.

To access the Data stream page, navigate to **Services > Data Stream Manager > Data Stream**

Figure 9-37 Data Stream List

DATA STREAM LIST

+ Add

Name	Endpoint A	Mode	Endpoint B	Mode	Enabled	Status

Every Data stream requires two endpoints, Endpoint A and Endpoint B. In all cases, the flow of data is from Endpoint A to Endpoint B.

To create a new Data stream:

1. Click **+Add** in the Data Stream List, the Edit Data Stream page displays.

Figure 9-38 Edit Data Stream Configuration

EDIT DATA STREAM

Activate ☒ On ☐ Off

Name

Endpoint A name

Endpoint A mode

Endpoint B name

Endpoint B mode

2. Set **Activate** toggle to **On** to activate the Data stream.
3. In the **Data stream name** field, enter a name for the Data stream.
4. For **Endpoint A name** field, select one of the endpoints you created previously. This endpoint should be the starting point of the stream.
5. For **Endpoint A mode** field, select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it leaves this endpoint. For example, if Endpoint A type is Serial port (generic), the Mode can be set to various Modbus server and client types. This means that upon arrival at Endpoint A, the data will be transformed into the chosen Modbus format, ready to be sent to Endpoint B.
6. For **Endpoint B name** field, select one of the endpoints you created previously. This endpoint should be the destination of the stream.
7. For **Endpoint B mode** field, select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it arrives at this endpoint.
8. Click **Save**, the new Data stream displays in the Data Stream List.

Figure 9-39 Data Stream List with created Data Stream

DATA STREAM LIST							+ Add	
Name	Endpoint A	Mode	Endpoint B	Mode	Enabled	Status		
MyDataStream	Serial-generic	Raw	UDP	Raw	1	Running	Edit	Delete

Click  to edit that Data stream, Click  to delete that Data stream.

Event Configuration

The NTC-550 Series router can be configured to send notifications when certain events occur on the router. These notifications can be used for proactive monitoring of events such as unit reboots and Ethernet link changes.

Figure 9-40 Event Notification – Configuration

EVENT NOTIFICATION CONFIGURATION

Enable On Off

Maximum event buffer size (100-10000)

Maximum retry count (1-20)

Event notification log file

Unit ID E651D9

EVENT NOTIFICATION TYPES AND DESTINATIONS MAPPING

Event ID	Event notification type	Destination profile
1	Unit powered up	Default
2	Unit rebooted	Default
3	Link status change	Default
4	WWAN IP address change	Default
5	WWAN Registration change	Default
6	WWAN Cell ID change	Default
7	WWAN technology change	Default
8	Number of connected Ethernet interfaces change	Default
10	Login status	Default
15	Digital input change	Default
16	Analog input threshold	Default
17	Digital output change	Default
20	FOTA/DOTA status	Default
23	USB connection change	Default
24	GPS GEOFENCE status change	Default
25	Low voltage threshold triggered	Default

Save

Event Notification Configuration

To configure Event Notifications:

1. Enable event notifications by setting the **Enable** toggle to **On**.
2. In the **Maximum buffer event size** field, specify the buffer size for event notifications which failed to be delivered or are yet to be sent.
3. In the **Maximum retry count** field, enter the number of times the NTC-550 Series router should attempt to deliver the notification in the event of a delivery failure.
4. If required, adjust the output location of the **Event notification log file**.
5. For each of the **Event Notification Types** select the **Destination Profile** which should send the notification when the notification is triggered. For details on how to configure the Destination Profiles, view the [Destination Configuration](#) section.
6. Click **Save** to apply the configuration.

Destination configuration

The **Destination Configuration** page allows for the configuration of the Event Destination List, which specifies where notifications should be sent when they are triggered.

Figure 9-41 Log – Event destination list

Name	Email address	SMS number	TCP address	UDP address	Custom command
Default					

Multiple destinations can be configured and assigned to different event types, depending on what notifications need to be sent.

To configure or edit an event destination:

1. Click **+Add** button to add a destination or the  button to edit an existing destination. The Event Destination Profile Settings page opens.

Figure 9-42 Services – Event configuration – Destination Configuration – Event Destination Profile settings

EVENT DESTINATION LIST

EVENT DESTINATION PROFILE SETTINGS

Destination name

Email address

SMS number

TCP address

TCP port 1-65535

UDP address

UDP port 1-65535

Custom command

- In the Destination name field enter a name to identify the destination profile. This name will appear on the Event Notification Configuration page, in the Destination Profile column.

Note: The Email address, SMS number, TCP address, UDP address and Custom command fields listed below are all optional. Complete the fields which should be included when a notification is sent. The TCP port and UDP port fields are required if using a TCP address or UDP address.



- In the **Email address** field, enter an email address to receive the notification.
- In the **SMS number** field, enter a phone number to receive the notification as an SMS.
- In the **TCP address** and **TCP port** fields, enter a TCP address and TCP port to receive the notification over TCP.
- In the **UDP address** and **UDP port** fields, enter a UDP address and UDP port to receive the notification over UDP.
- In the **Custom command** field, enter a custom command to execute when the notification is triggered. The command should be a bash compatible command.
- Select the **Save** button to save the destination profile.
- Apply the destination profile by returning to the **Event Configuration > Event Notification Configuration** page.
- Set the **Destination profile** dropdown on the appropriate Event Notification and Destination Mapping item to the new destination.

Figure 9-43 Services – Event Configuration – Destination profile mapping

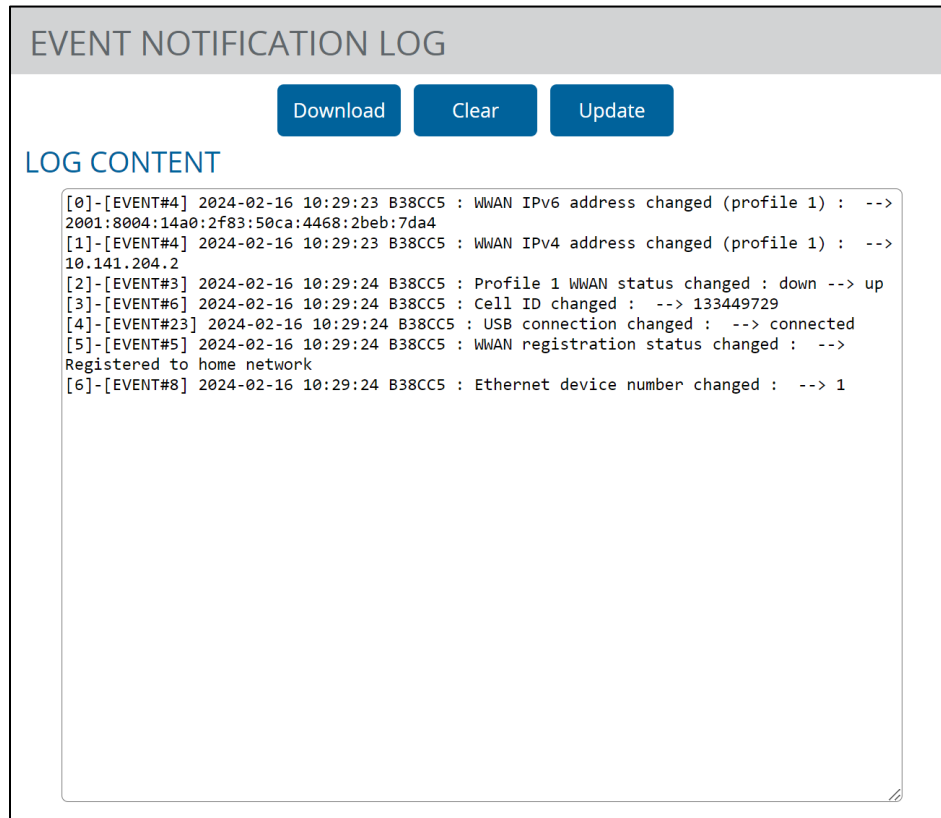
Event ID	Event notification type	Destination profile
1	Unit powered up	MyCustoml ▼ Default MyCustomDestination

- Click **Save** button at the bottom of the **Event Notification Configuration** page.

Event notification log

The **Event Notification Log** displays a log of Events which have been triggered. Click **Update** button to refresh the content in the Log Content window. Click **Download** button to download a log file for review in an external application. Click **Clear** button to clear the log.

Figure 9-44 Services – Event Configuration – Event notification log



Email Settings

The email settings page is used to configure the SMTP server to be used to deliver Event Notifications (configured in the Event notification configuration section).

Figure 9-45 Email Client Setting

EMAIL CLIENT SETTING

EMAIL SERVER SETTINGS

From:

CC:

Email server address (SMTP):

Email server port: (STARTTLS:587, SSL/TLS:465, Default:25)

Encryption: ▼

Enable authentication: ☒ On ☐ Off

Username:

Password:

Confirm password:

Email test recipient:

The table below lists the Email Server Settings Configuration Details

Table 9-24 Email Server Settings Configuration Items

Item	Description
From	Enter Email address that should represent sender of the email notification.
CC	Enter Email address or addresses that the notification should be sent to.
Email server address (SMTP)	Enter Domain name of the SMTP server that the email should be sent through.
Email server port	Enter the port that the SMTP server is expecting email on. The port varies depending on the encryption type used, refer to your email provider's SMTP instructions on which port is correct. The available encryption types are STARTTLS (Port 587) , SSL/TLS (Port 465) , or Default (Port 25) .
Encryption	Select the encryption type from the drop-down. Available types are STARTTLS , SSL/TLS , None .
Enable authentication	Set toggle to On if the SMTP server is expecting authentication.
Username	Enter Username to authenticate with the SMTP server.
Password	Enter Password to authenticate with the SMTP server.

Item	Description
Confirm password	Re-enter the password to authenticate with the SMTP server.
Email test recipient	Enter recipient email address here after completing the previous details to test the SMTP configuration.
Send test email button	Click to send the test email to the address configured in the Email test recipient field.

Click **Save** to save and apply the settings.

Low power mode

The Low power mode page provides an overview of the power profiles and allows you configure them. Up to five power profiles can be configured and all of them can be active simultaneously.

To access the Low power mode page, navigate to **Services > Low power mode**.

LOW POWER MODE				
POWER PROFILE LIST				
Name	Status	Sleep mode	Wake mode	
Profile1	On Off	Scheduled	Ignition	
Profile2	On Off	Scheduled	Ignition	
Profile3	On Off	Scheduled	Ignition	
Profile4	On Off	Scheduled	Ignition	
Profile5	On Off	Scheduled	Ignition	
Save				

The **Status** column indicates whether the profile is active, while the **Sleep mode** and **Wake mode** columns display the method set for router sleep and wake functions.



Important: When configuring multiple power profiles, be careful so that they do not overlap or conflict with one another, for example, configuring a schedule which wakes up the unit when another profile has it scheduled to be in low power mode.

Click  to edit that profile.

Figure 9-46 Low Power Mode Configuration

LOW POWER MODE

POWER PROFILE SETTINGS

Profile ☐ On ☐ Off

Profile name

SLEEP SETTINGS

Sleep mode

Schedule sleep at HHMM (24 hour format)

WAKE SETTINGS

Wake mode

The table below lists the Low Power Mode configuration details.

Table 9-25 Low Power Mode Configuration Items

Item	Description
Power Profile Settings	
Profile	Set to On to activate the profile
Profile name	Enter a name for the profile.
Sleep Settings	
Sleep mode	Select Sleep mode from the following options: • Sleep triggered by Ignition pin • Sleep after timer • Sleep at scheduled time The Sleep mode selects the condition for the router to enter sleep mode.
Remain awake after ignition off	Enter the duration for which the router should remain awake after ignition is off, when Sleep mode is selected as Sleep triggered by Ignition pin .
Sleep after timer	Enter the duration after which the router should go to sleep mode, when Sleep mode is selected as Sleep after timer .
Schedule sleep time	Enter the time when the router should go to sleep mode, when Sleep mode is selected as Sleep at schedule time .
Wake mode	Select Wake mode from the following options: • Wake up triggered by Ignition pin • Wake up triggered by bt button • Wake at scheduled time The Wake mode selects the condition for the router to wake up.

Item	Description
Schedule wake up at	Enter the time when the router should wake up, when the Wake mode is selected as Wake at scheduled time .

Click **Save** to save the settings, the configured profile displays in the Power Profile List.

IO configuration

The NTC-550 Series router is equipped with a 6-way terminal block connector providing three identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible proximity sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) using external resistors
- Analogue 0V to 30V input
- Digital input (the I/O voltage measured by the iMX283 LRADC and the software making decision about the input state) with the threshold levels configurable in software
- Open collector output.

To access the IO configuration page, navigate to **Services > IO configuration**.

Figure 9-47 IO Configuration

IO CONFIGURATION

IO functionality ☒ On ☐ Off

Pull up voltage 3V

IO manager debug level error notice info debug

PIN CONFIGURATION

Pin	Mode	Pull up	Threshold	Value
1	Digital Input	☒ On ☐ Off	1.6	Low
2	Digital Input	☐ On ☒ Off	1.6	High
3	Digital Input	☒ On ☐ Off	1.6	Low

Save Cancel

Use the pull up voltage options to select the desired output voltage of the I/O pins. The pull up voltage you select will be the same for each pin when pull up is enabled for that pin. Each pin is capable of outputting either 3 V or 8.2 V.

The table below lists the IO configuration details.

Table 9-26 IO Configuration Items

Item	Description
IO Configuration	
IO Functionality	Enables the configuration of the input and output pins on the four-way terminal block connector.
Pull up voltage	Specifies the output voltage of the I/O pins.
IO Manager Debug level	Use the slide bar to adjust the level of detail you would like to see in the log for IO messages. A higher debug level displays more detailed messages in the log file.
Pin Configuration	
Pin	The I/O pin number corresponding to the pin on the 6-way terminal block connector that you wish to configure.
Mode	The mode of operation for the corresponding pin. Available options are: Digital Input – The corresponding pin accepts digital input. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column displays whether the signal received on the pin is High or Low. The default value is High. When the I/O pin is shorted to ground the value changes to Low. Digital Output – The corresponding pin outputs a digital signal. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column contains a toggle key allowing you to set whether the output signal is High or Low. When set to Low, the output of the I/O pin is 0 V. When set to High, the output of the I/O pin is 5 V. Analogue input – The corresponding pin accepts an analogue signal. Pull up may be on or off and both 3 V and 8.2 V are available as pull up voltages. The value column displays the current voltage detected on the pin. Namur input – NAMUR is a sensor standard using low-level current signals. It can supply two different signal levels depending on the state of the switch and is commonly used in hazardous or explosive locations where compact sensors are required. When a pin is set to NAMUR mode, Pull up is turned on and the global Pull up voltage is set to 8.2 V. These settings may not be changed for as long as a pin is set to NAMUR mode as they are required settings according to the NAMUR IEC 60947-5-6 standard.

Item	Description
	The value column displays whether the signal received on the pin is High or Low. • Contact closure input –A common type of digital input where a sensor or switch opens or closes a set of contacts as a result of a process change. An electrical signal is then used to determine whether the circuit is open or closed. When a pin is set to Contact closure input, Pull up is enabled for that pin and may not be turned off as long as the pin remains configured as a Contact closure input. Global pull up voltage may be either 3 V or 8.2 V.
Pull up	Use the pull up toggle keys to turn the pull up On or Off for the corresponding pin. When turned On, the pull up voltage output is the value specified in the “Pull up voltage” option in the IO configuration section of this dialog box.
Threshold	Displays the current voltage threshold configured for the I/O pin.
Value	The value column displays whether the voltage detected on the line is low or high or allows you to set the output value to high or low. This can be useful for applications where monitoring of the transition between low and high is used to trigger an action.

Click **Save** to save the settings.



Important: Please refer to the SDK Developer Guide for hardware information about the Input/Output pins, wiring examples and configuration of the pins via the command line interface. There are also wiring examples in Appendix J of this User Guide.

10. System

Log

The Log section allows you to download the System logs, Diagnostic logs and IPSec logs on the router.

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NTC-550 Series router. To access the System Log page, navigate to **System > Log > System log**

The Log Filter Level allows you to select the type of logs you want to download

Table 10-1 Log – System Log Filter Level

ITEM	DEFINITION
Debug	Shows extended system log messages with full debugging level details.
Info	Shows informational messages only.
Notice	Shows normal system logging information.
Warning	Shows warning messages only.
Error	Shows error condition messages only.

Once you have selected the Log Filter Level, click **Download** to download the log file.

The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

System log settings

To access the System log settings, navigate to **System > Log > System log settings**.

Log data is stored in RAM and therefore when the unit loses power or is rebooted the RAM will lose any log information stored in the RAM. To ensure that log information is accessible between reboots of the router there are two options:

- Enable the Log to non-volatile memory option.
- Use a Remote syslog server.

Figure 10-1 Log – System log settings

SYSTEM LOG SETTINGS

LOG CAPTURE LEVEL

Log capture level Notice

VOLATILE LOG

Log buffer size (KB) 256 100-512

NON VOLATILE LOG

Log to non-volatile memory On Off

Log file size (KB) 5000 500-5000

REMOTE SYSLOG SERVER

IP / Hostname [:PORT] 192.168.2.1:514

Save

Log capture level

The log capture level defines the amount of detail that the system log stores. This setting also affects the Display level setting on the System log page, for example, if this is set to a low level, such as “Error”, the System log will not be able to display higher log levels.

Table 10-2 Log - System Log Settings – Log Capture Level

Item	Definition
Debug	Shows extended system log messages with full debugging level details.
Info	Shows informational messages only.
Notice	Shows normal system logging information.
Warning	Shows warning messages only.
Error	Shows error condition messages only.

Volatile Log

The size of the volatile log buffer can be configured to store larger logs if required. The default is 256KB.

Non-volatile Log

When the router is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512kb of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory.

While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

Remote syslog server

The router can be configured to output log data to a remote syslog server. This is an application running on a remote computer which accepts and displays the log data. Most syslog servers can also save the log data to a file on the computer on which it is running allowing you to ensure that no log data is lost between reboots.

To configure the NTC-550 Series router to output log data to a remote syslog server enter IP address or hostname of the syslog server in the **IP / Hostname [:PORT]** field in Remote Syslog Server section. You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514. If you do not specify a port number, the router will use the default UDP port 514. Click **Save** to save the setting.

Figure 10-2 Log – System log settings – Remote syslog server



Diagnostic log

The router may be configured to enable the collection of diagnostic logs for the purpose of troubleshooting problems. These log files are intended for use by Lantronix technicians. By default, this feature is disabled and should only be enabled if you are trying to find out the cause of a problem and are instructed to enable this by Lantronix technical support staff.

Figure 10-3 Log – Diagnostic log configuration and download

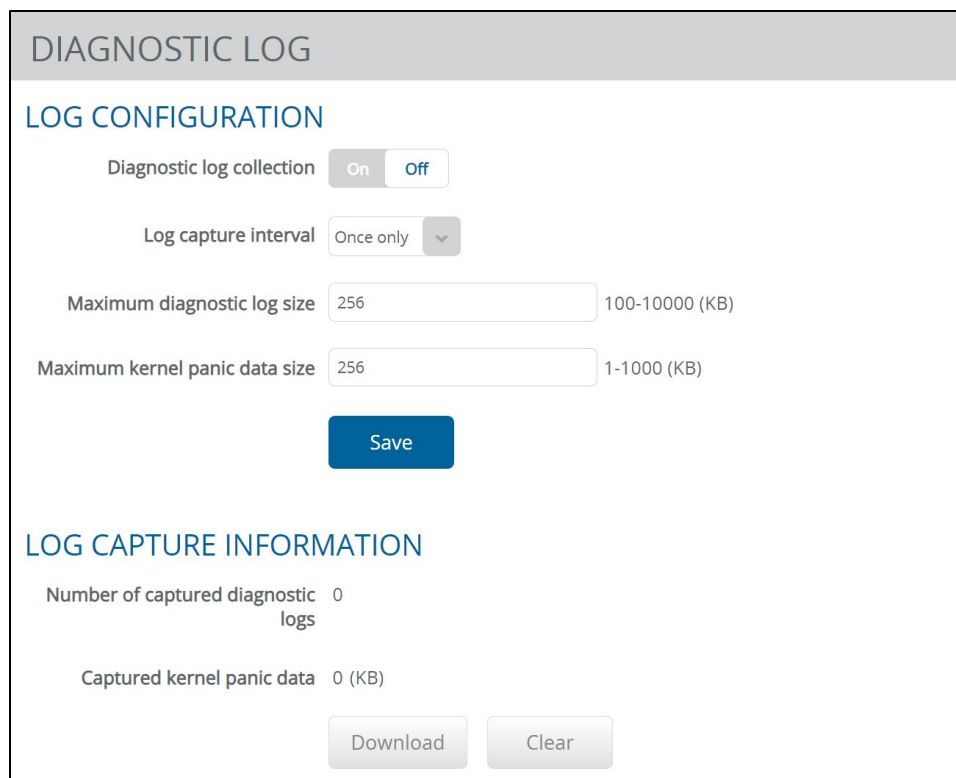


Table 10-3 Diagnostic log descriptions

Item	Description
Diagnostic log configuration	
Periodic log collection	Turn on this toggle key to enable diagnostic log collection.
Log capture interval	Select the interval at which the router should collect diagnostic log data.
Maximum periodic log size (KB)	Enter the maximum size of the log file in kilobytes.
Maximum kernel panic data size (KB)	Enter the maximum size of the kernel panic data file in kilobytes.
Save button	Click to save Log Configuration.
Log capture information	
Number of captured periodic logs	Displays the number of captured periodic logs.
Captured kernel panic data (KB)	Displays the total size of captured kernel panic data in kilobytes.
Download button	Click to download all captured logs.
Clear button	Click clear all captured periodic logs.

IPSec log

The IPSec Log allows you to identify and troubleshoot issues with the IPSec VPN connection. To access the IPSec Log page, navigate to **System > Log > IPSec log**.

Figure 10-4 Log - IPSec Log

IPSEC LOG

common level the common level for all types

Please set the level for each type

app	0 (auditing)	applications other than daemons
dmn	0 (auditing)	Main daemon setup/cleanup/signal handling
mgr	0 (auditing)	IKE_SA manager, handling synchronization for IKE_SA access
ike	0 (auditing)	IKE_SA/ISAKMP SA
chd	0 (auditing)	CHILD_SA/IPsec SA
job	0 (auditing)	Jobs queuing/processing and thread pool management
cfg	0 (auditing)	Configuration management and plugins
knl	0 (auditing)	IPsec/Networking kernel interface
net	0 (auditing)	IKE network communication
asn	0 (auditing)	Low-level encoding/decoding (ASN.1, X.509 etc.)
enc	0 (auditing)	Packet encoding/decoding encryption/decryption operations
lib	0 (auditing)	libstrongswan library messages
esp	0 (auditing)	libipsec library messages
tls	0 (auditing)	libtls library messages
tnc	0 (auditing)	Trusted Network Connect
imc	0 (auditing)	Integrity Measurement Collector
imv	0 (auditing)	Integrity Measurement Verifier
pts	0 (auditing)	Platform Trust Service

To use the IPSec log, set the log level for each type of log that should be captured. The following log levels are available:

Table 10-4 IPsec log descriptions

ITEM	DEFINITION
Off	No logs collected.
0 Auditing	Auditing is the lowest log level, providing minimal information. This level is typically used for logging only critical security events or administrative actions that have a significant impact on the VPN.
1 Control Flow	Control Flow logging provides information about the establishment and termination of IPsec VPN connections and security associations (SAs). Control Flow includes details about the negotiation of encryption and authentication parameters, as well as key exchange protocols like IKE (Internet Key Exchange).
2 Debug Control Flow	Debug Control Flow logging provides more detailed information than the standard Control Flow level. Debug Control Flow includes additional debugging information related to the establishment and management of IPsec SAs.
3 Raw Data Dumps	Raw Data Dumps logging is a very verbose level that includes detailed packet-level information. Raw Data Dumps logs raw data, such as the contents of IPsec packets and payloads.
5 Private Data Dumps	Private Data Dumps logging is the highest log level and provides the most detailed information. Private Data Dumps logs sensitive and private data, such as encryption keys and other security-related information. This level should only be used in a secure environment for advanced debugging or security analysis.

Once the log level has been set, click **Save** button to apply the log configuration.

As logs are collected, they are visible in the Log Content section at the bottom of the page. Click **Update** button to refresh the Log Content window.

Click **Download** button to download and view the logs in an external tool

Watchdog

Periodic ping

The Periodic ping page is used to configure the behaviour of the Periodic Ping monitor function.

When configured, the Ping watchdog feature transmits controlled ping packets to 1 or 2 user specific IP addresses. Should the watchdog not receive responses to the pings, it will reboot the device in a last resort attempt to restore connectivity.

Caution should be exercised when using this feature in situations where the device is intentionally offline for a particular reason (e.g. user configured PDP session disconnect, or the Connect on demand feature enabled). The ping watchdog feature expects to be able to access the internet at all times and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.

The ping watchdog being a last resort standalone backup mechanism, it will continue to do its job and reboot the device even when the Connect on demand session is idle, or the PDP context is disabled by the user. It is

recommended to disable this feature if Connect on demand is configured, or if the PDP context will be intentionally disconnected on the occasion.

The feature operates as follows:

1. After every “Periodic Ping timer” configured interval, the router sends 3 consecutive pings to the “First destination address”.
2. If all 3 pings fail the router sends 3 consecutive pings to the “Second address”.
3. The router then sends 3 consecutive pings to the “Destination address” and 3 consecutive pings to the “Second address” every “Retry timer” configured interval.
4. If all retry pings in step 3 above fail the number of times configured in “Fail count”, the router reboots.
5. If any ping succeeds, the router returns to step 1 and does not reboot.

Figure 10-5 Watchdog – Periodic ping and reboot configuration

The screenshot shows the 'WATCHDOG' configuration page. It is divided into two main sections: 'PERIODIC PING' and 'PERIODIC REBOOT'.

PERIODIC PING Section:

- Enable:** A toggle switch set to 'On'.
- First destination address:** A field with IP address 192.168.2.1.
- Second destination address:** A field with IP address 192.168.2.6.
- Periodic Ping timer:** A numeric field set to 0, with a range of (300-65535) secs.
- Retry timer:** A numeric field set to 0, with a range of (0=disable, 60-65535) secs.
- Fail count:** A numeric field set to 0, with a range of (1-65535) times.

PERIODIC REBOOT Section:

- Enable:** A toggle switch set to 'On'.
- Force reboot every:** A numeric field set to 5, with a range of (5-65535) mins.
- Random delay before reboot:** A dropdown menu set to '1 minute'.

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

To configure the ping watchdog:

1. Enable the ping watchdog by setting the **Enable** toggle to **On**.
2. In the **First destination address** field, enter a website address or IP address to which the router will send the first round of ping requests.
3. In the **Second destination address** field, enter a website address or IP address to which the router will send the second round of ping requests.
4. In the **Periodic Ping timer** field, enter a number between 300 and 65535 for the number of seconds the router should wait between ping attempts. Setting this to 0 disables the ping watchdog function.
5. In the **Retry timer** field, enter a number between 60 and 65535 for the number of seconds the router should wait between retry ping attempts, i.e. pings to the second destination address.
6. In the **Fail count** field, enter an integer between 1 and 65535 for the number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the ping watchdog function.
7. Click **Save** button to save the configuration.

Periodic reboot

The router can be configured to automatically reboot after a period of time specified in minutes. While this is not necessary, it does ensure that in the case of remote installations, the router will reboot if some anomaly occurs.

To configure Periodic reboot:

1. Set the **Enable** toggle to **On**.
2. In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.
3. If you have configured a forced reboot time, select a time for **Random delay before reboot** from the drop-down list. Randomly delaying the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured Force reboot every time and then randomly selects a time that is less than or equal to the **Random delay before reboot** time setting. After that time has elapsed, the router reboots.



Important: *The Random delay before reboot time is not persistent across reboots; each time the router is due to reboot, it randomly selects a time less than or equal to the time set for Random delay for reboot.*

4. Click **Save** button to save the settings.

System configuration

LDAP Settings

The LDAP Settings allows you to configure a Lightweight Directory Access Protocol (LDAP) on the NTC-550 Series router. The LDAP allows the router to use a centralized directory service for user authentication and authorization.

Figure 10-6 LDAP Settings

LDAP SETTINGS

LDAP CONFIGURATION

SSH and WEBUI Login via LDAP ☒ On ☐ Off

Use LDAPS ☐ On ☒ Off

Registered Yes

[Clear credentials](#)

LDAP Basedn DC=IICATS,DC=LOCAL

LDAP Binddn CN=Users

LDAP Server List iicats:389 iicats:636

LDAP Admin Binddn CN=Administrator,CN=Users,DC=IICATS,DC=LOCAL

LDAP Admin Bind Password

LDAP CA Cert /etc/ssl/certs/nslcd/IICATS-ROOTCS-B64.pem

LDAP CA Cert Directory /etc/ssl/certs/nslcd

[Save](#)

Table 10-5 LDAP Configuration

ITEM	DEFINITION
SSH and WEBUI Login via LDAP	Set to On to enable SSH and WEBUI login via LDAP.
Use LDAPS	Set to On to enable use of LDAP over SSL/TLS, a secure version of LDAP.
Registered	Displays whether the LDAP server is registered on the router.
Clear Credentials button	Click to clear credentials related to an existing LDAP configuration.

ITEM	DEFINITION
LDAP Basedn	Enter the LDAP Base Distinguished Name. It specifies the starting point within the LDAP directory tree from which searches will be performed.
LDAP Binddn	Enter the LDAP Bind Distinguished Name of the LDAP entry used to authenticate (bind) to the LDAP server.
LDAP Server List	Enter the IP address or Hostname of the LDAP server and port number. (IP address/Hostname:Port)
LDAP Admin Binddn	Enter the LDAP Admin Bind Distinguished Name, which refers to a special Bind DN with administrative privileges in the LDAP directory.
LDAP Admin Bind Password	Enter the password for the LDAP Admin Bind DN used.
LDAP CA Cert	Enter the complete path of the Certificate Authority (CA) certificate that is used to validate the SSL/TLS certificate presented by an LDAP server when connecting over LDAPS (LDAP over SSL/TLS).
LDAP CA Cert Directory	Enter the path for the directory where the LDAP CA certificate is located.
Save button	Click to save the settings.

Restore factory defaults

Restoring factory defaults will reset the NTC-550 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NTC-550 Series router. There are three levels of factory reset:

- Installer reset
- Carrier reset
- Full factory reset

The availability of the above levels depends on your [Runtime Configuration](#) settings.

Installer reset

The installer reset only resets settings that have changed after the NTC-550 Series was installed. The settings that are included are those that were likely changed through the web interface. This reset level is generally the first one that should be attempted, as it will reset less important configurations.

Carrier reset

The carrier reset will reset the device with the carrier-defined default settings to operate on the network. This also resets the user-configured options to their default settings. This reset should be attempted after trying the installer reset.

Full factory reset

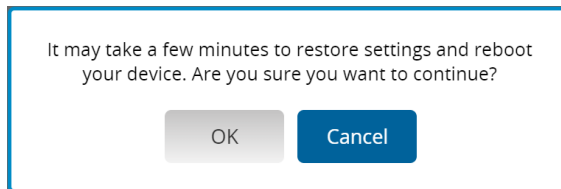
The full factory reset is generally used for refurbishment or to remove an erroneous configuration. This will remove all settings including the carrier settings that are required for the device to operate on the network. All configurations and settings are completely removed.



Important: The full factory reset will require the NTC-550 Series to be completely reconfigured.

To complete a reset at any level

1. In the **Restore Factory Defaults** page, select the **Clear HTTPS certificate** checkbox if you want to clear the HTTPS certificate.
2. Select the appropriate reset level.
3. You will be prompted to confirm. Select the **Ok** button to proceed with the reset.



4. Wait for the router to reset and reboot, then access the device through the web interface at **https://192.168.1.1**

Web server setting

Allows you configure whether the NTC-550 Series router web server uses HTTP or HTTPS and the server port. Additionally, you can generate a web server certificate by entering data in all the fields in the **Web Server Certificate** section.

Figure 10-7 Web server setting configuration

WEB SERVER SETTING

HTTPS ☒ On ☐ Off

HTTP ☐ On ☒ Off

Redirect HTTP to HTTPS ☒ On ☐ Off

Save

WEB SERVER CERTIFICATE

Certificate serial number 06FF3B256DB90352FD7BE41A59002A9A651601E8

Not before Apr 4 05:29:40 2023 GMT

Not after Jul 7 05:29:40 2025 GMT

Server key size 2048

Country AU

State NSW

City Lane Cove

Organization Casa Systems

Generate server certificate

UPLOAD WEB SERVER CERTIFICATE

Alternatively, please provide a web server certificate in a .zip file that contains the certificate and key file.

Administration settings

The Administration settings page allows you to update administration credentials and Web UI login limits.

Web UI credentials

Use this section to update the password for the different users that have access to the NTC-550 Series router via the web interface. Select the **Username**, enter the current password for the that user and then enter a new password. Click **Save** button to confirm the changes.

Figure 10-8 Administration settings – Web UI credentials configuration

WEB UI CREDENTIALS

Username admin

Current password

New password i

Confirm new password

Save

Web UI login limits

The Web UI login limits section allows you to configure the timeout and lock setting for access to the web interface. It is designed to improve security by reducing the risk of brute force attacks on the web interface.

Figure 10-9 Administration settings – Web UI login limit configuration

WEB UI LOGIN LIMIT

Incorrect login attempt limit (3-5)

Login lock duration (1-10 minutes)

IP login attempt limit (5-8)

LAN IP address lock duration (5-10 minutes)

WAN IP address lock duration (10-20 minutes)

Session timeout (5-60 minutes)

Save

Table 10-6 WebUI login limits configuration items

Item	Description
Incorrect login attempt limit	Enter the number of times an incorrect password can be entered into the web interface before it locks access and does not allow any further attempts.
Login lock duration	Enter the amount of time the login lock lasts.

Item	Description
IP login attempt limit	Enter the number of logins that can be attempted from one IP before any further attempts are locked out.
LAN IP address lock duration	Enter the amount of time an IP attempting to log in from the LAN is forbidden from trying to login.
WAN IP address lock duration	Enter the amount of time an IP attempting to log in from the WAN is forbidden from trying to login.
Session timeout	The amount of time in minutes that a logged in session lasts on the web interface without any activity. The web interface will log out the current user after the configured time.

SSH credentials

Use this section to update the root user password for SSH access to the NTC-550 Series router.

Figure 10-10 Administration – Administrator credentials configuration

SSH CREDENTIALS

Username root

Current password 

New password  

Confirm new password 

Settings backup/restore

The Settings Backup and Restore page allows you to backup or restore the router's configuration or to reset it to factory defaults. To view the settings page, you must be logged into the web user interface as root using the password admin. The backup / restore functions can be used to easily configure many NTC-550 Series routers by configuring one router with your desired settings, backing them up to a file and then uploading that file to multiple NTC-550 Series routers.

To access the Settings Backup and Restore page, navigate to **System > System configuration > Settings backup/restore**.

Figure 10-11 System configuration - Backup and restore

SETTINGS BACKUP AND RESTORE

SAVE A COPY OF CURRENT SETTINGS

Password  

confirm password 

Save

RESTORE SAVED SETTINGS

Select file to upload **Choose a file** Not uploaded

Password 

Restore

Creating a settings backup

To create a settings backup, in the Save a Copy of Current Settings section, Click the **Save** button. The configuration will download. If you wish to protect the configuration with a password, enter a password into the **Password** and **Confirm password** fields, then click **Save**.

Restoring a settings backup

To restore a settings backup:

1. in the Restore **Settings** section, click **Choose a file** for the **Select file to upload** field.
2. Locate and upload the saved configuration.
3. If the file was saved with a password, enter the password, then click **Restore**. You will be prompted to confirm, select **Ok** to proceed. The device will reboot with the saved settings.

Figure 10-12 Systems configuration – Restoring a settings backup confirmation

It may take a few minutes to restore settings and reboot your device. Are you sure you want to continue?

OK **Cancel**

Site and location settings

The Site and location settings allows you to add a name that displays in the System information section of the Status page. This can be useful for identifying the particular device you are using when you have a fleet of them in various locations.

Figure 10-13 System configuration – Site and location settings

Enter the values for **Site name** and **Location** fields. Click **Save** to save the settings

Runtime configuration

Runtime Configuration allows you to load a configuration file containing carrier-specific settings such as default settings, MBN changes which is not possible via the web user interface. It is used for late binding of carrier configurations at the time of installation.

Figure 10-14 System configuration – Runtime configuration upload

To apply runtime configuration:

1. Click the **Choose a file** button, locate the configuration file and select it.
2. **Uploaded** displays next to the button.
3. Click the **Apply** button to install the configuration file.
4. The device automatically reboots after successful upload of the configuration file.

SSH key management

Secure Shell (SSH) is UNIX-based command interface and network protocol used to gain secure access to a remote machine, execute commands on the remote machine, and transfer files between machines.

SSH uses RSA public key cryptography for both connection and authentication. Two common ways of using SSH are:

- Use automatically generated public-private key pairs to encrypt the network connection and then use password authentication to log on.
- Use a manually generated public-private key pair to perform the authentication and allow users or programs to log in without using a password.

To access the SSH key management page, navigate to **System > System configuration > SSH Key Management**.

Figure 10-15 System configuration – SSH server configuration

SSH SERVER CONFIGURATION

SSH SERVER SETTINGS

SSH Protocol Protocol 2

Password Authentication enable
On Off

Key Authentication enable
On Off

Save

HOST KEY MANAGEMENT

Key type	Date
ssh_host_dsa_key	2024-02-12 17:50:01
ssh_host_rsa_key	2024-02-15 10:16:38
ssh_host_ecdsa_key	2024-02-15 10:16:38
ssh_host_ed25519_key	2024-02-15 10:16:38

Generate keys
Get keys
Get public keys
Upload keys

CLIENT KEY MANAGEMENT

Username	Hostname	Key type	Delete

Clear
Upload

SSH Server Configuration

To configure the SSH server settings:

1. Select the **SSH Protocol** to use. Protocol 2 is more recent and is considered more secure.
2. Select the type of authentication you want to use by setting the **Password Authentication enable** and **Key Authentication enable** toggle keys to **On** or **Off**. Note that you may have both authentication methods on, but you cannot turn them both off.
3. Click the **Save** button to confirm your settings.

Host key management

The Host key management section allows you to manage the SSH keys on the NTC-550 Series router.

Figure 10-16 System configuration – SSH server configuration – Host key management

HOST KEY MANAGEMENT	
Key type	Date
ssh_host_dsa_key	2024-02-27 10:17:16
ssh_host_rsa_key	2024-02-27 10:17:32
ssh_host_ecdsa_key	2024-02-27 10:17:32
ssh_host_ed25519_key	2024-02-27 10:17:32
Generate keys Get keys Get public keys Upload keys	

Click the **Generate Keys** button to generate new keys. Use caution when selecting the **Generate Keys** button, as this invalidates any previously generated keys.

Click the **Get Keys** button to download the generated private and public keys. You will be asked to enter a password for the keys file.

Figure 10-17 System configuration – SSH server configuration – Host key management – Password

Enter the password for the keys file

Password

confirm password

In the **Password** field enter a password and in the **confirm password** field, re-enter the password. Click the **OK** button to download the keys file.

Click the **Get Public Keys** button to download just the public keys.

Click the **Upload keys** button to upload a keys file. You will be prompted to enter the password created in the **Get Keys** step to upload the file. The keys will replace the previously generated keys.

Client key management

The Client key management page allows you to upload client keys to the NTC-550 Series router and enables key based SSH access to the NTC-550 Series router. Click the **Upload** button to upload the public key of your SSH client. The key displays in **Client key management** window. Click  in the **Delete** column to remove that key. Click **Clear** to clear all the uploaded keys.

Figure 10-18 System configuration – SSH server configuration – Host key management – Password

CLIENT KEY MANAGEMENT			
Username	Hostname	Key type	Delete
root		rsa2	
Clear		Upload	

LED operation mode

The LED operation mode page allows you to control the operation of the LED indicator lights on the NTC-550 Series router. There are two modes available, **Always on** and **Turn off after timeout**. Setting the mode to **Always on** sets the indicator LEDs to be lit when the device is on. Setting the mode to **Turn off after timeout** sets the indicator LEDs to turn off after the timer has expired.

Figure 10-19 LED operation mode

LED OPERATION MODE	
LED OPERATION MODE SETTING	
Mode	Turn off after timeout
LED power off timer	10 (1-65535 minutes)
Save	

Setting the LED operation mode

To set the LED operation mode:

1. Select the **Mode** to use. Options are **Always on** and **Turn off after timeout**.
2. If using the **Turn off after timeout** mode, set the LED power off timer to the number of **minutes** that the indicator LEDs should be lit after the device has started.
3. Click the **Save** button to save and apply the configuration.

A/B system configuration

The A/B system configuration page allows you to switch between an active and previous firmware. Switching between firmware allows you to restore a previous firmware for troubleshooting in the event of an issue with the current firmware. Restoring a previous firmware should only be used for troubleshooting.

Figure 10-20 A/B System configuration

A/B SYSTEM CONFIGURATION			
CURRENT STATUS			
Bank	Firmware version	Module firmware version	Status
A	1.2.12.0		Standby
B	1.2.15.0		Active
<button>Switch active bank</button>			

To switch the active bank, Click the **Switch active bank** button. You will be prompted with the following message:

Figure 10-21 A/B System configuration - Confirmation

Switching active banks will cause the device to reboot, breaking communications temporarily while the device reboots. Switching to a bank with older firmware should only be done for the purposes of troubleshooting and can result in loss of remote access. Please use it with caution. Are you sure you want to switch to the standby bank?

OK Cancel

To proceed click the **OK** button. Once the reboot is complete, the previous firmware will be restored. To switch active banks again, return to this screen and select the **Switch active bank** button.

Firmware upgrade

The Firmware upgrade page allows you to upload firmware files to update the NTC-550 Series router. The firmware upgrade will be applied to the Standby bank, to ensure the current firmware can be restored in the event of an issue.

Figure 10-22 File uploads

Bank	Firmware version	Module firmware version	Status
A	1.2.12.0		Standby
B	1.2.15.0		Active

UPGRADE FIRMWARE

Select firmware to upload Not uploaded

Reset to default config

The system must be rebooted to complete the firmware upgrade. Please choose when you would like the reboot to occur.

Reboot

Updating the router firmware

The firmware update process involves first uploading the recovery image firmware and then updating the main firmware image.

To update the NTC-550 Series router's firmware:

1. Power on the router as described in the Installing the router section.
2. Log in to the router with the root user account (See the Advanced configuration section for details)
3. Click the **System** tab from the top menu bar, then click the **Firmware upgrade** menu item.
4. In the Upgrade Firmware section click section, click **Choose a file** button. Locate the firmware image file on your computer and select **Open**.
5. If required set the **Reset to default config** toggle to **On** to reset the NTC-550 Series router to the default configuration.
6. Select an option for Reboot filed. The options are **Immediately** and **Scheduled**. If you select **Scheduled** option, the **Date** and Time **settings** display.

Reboot: Scheduled

Date: Nov 2024

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Time: 03:20 PM

7. Set the required **Date** and **Time**.
8. Click **Upgrade** button to upgrade the firmware.

SD Card

The SD card page displays available space and contents of micro-SD card. You can click **Upload** to add a file to the SD Card. In the below example the SD card contains a firmware file. Click  to install the firmware and click  to remove the file.

Figure 10-23 SD Card Display

FILE UPLOADS				
SD CARD (FREE SPACE: 14.70GB)			<button>Upload</button>	
File name	Date	Size	Install	Delete
ntc_552_1.2.61.0_root.star	2025-06-10	163703054		

Access control

The Access control pages are used to configure the remote and local access to the router.



Note: All remote access to the router is disabled by default.

Figure 10-24 Access control configuration

ACCESS CONTROL

REMOTE ACCESS CONTROL

HTTP enable ☒ On ☐ Off

HTTP port

8080

1-65535

HTTPS enable ☒ On ☐ Off

[Update server certificate if necessary.](#)

HTTPS port

443

1-65535

HTTPS source IP allow list

Comma-separated list of unicast IP addresses and/or network IP addresses (with /mask where mask is a plain number). If it is blank, all IP addresses are permitted.

SSH enable ☒ On ☐ Off

SSH port

22

1-65535

Ping enable ☒ On ☐ Off

LOCAL ACCESS CONTROL

HTTP enable ☒ On ☐ Off

HTTPS enable ☒ On ☐ Off

SSH enable ☒ On ☐ Off

Save

Table 10-7 Access control configuration items

Item	Description
Remote Access Control	
HTTP enable	Enable or disable remote HTTP access to the router.
HTTP port	When HTTP is enabled (see previous) you can set the HTTP management port. Enter a port number between 1 and 65534 to use when accessing the router remotely.
HTTPS enable	Enable or disable remote HTTPS access to the router using a secure connection.
HTTPS port	When HTTPS is enabled you can set the HTTPS remote access port. Enter a port number between 1 and 65534 to use when accessing the router remotely over a secure HTTPS connection.
HTTPS source IP allow list	When HTTPS is enabled (see Enable HTTPS above) you can enter a 'whitelist' of IP addresses that will be permitted to access the router. Enter a list of comma-separated unicast IP addresses. You may also enter IP addresses in CIDR notation, however, no spaces are permitted.

Item	Description
	Note that if this field is left blank, all IP addresses will be permitted to access the router.
SSH enable	Enable or disable Secure Shell access to the router.
SSH port	When SSH is enabled you can set the SSH access port. Enter the port number for remote SSH access. The port number must be between 1 and 65534.
Ping enable	Enable or disable remote ping responses on the WWAN connection.
Local Access Control	
HTTP enable	Enable or disable local HTTP access to the router. The default setting is disabled.
HTTPS enable	Enable or disable local secure HTTP access (https). The default setting is enabled.
SSH enable	Enable or disable local Secure Shell on the router. The default setting is enabled.
Save button	Click to save the configuration.

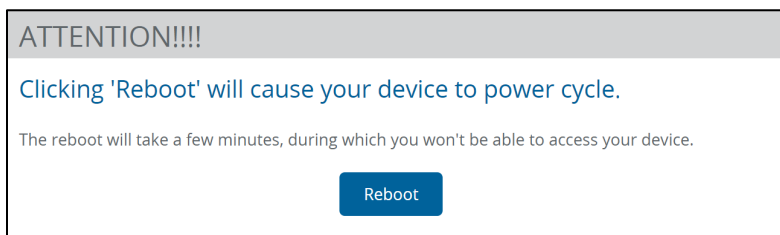
Reboot

The Reboot option in the System section performs a soft reboot of the device. This can be useful if you have made configuration changes you want to implement.

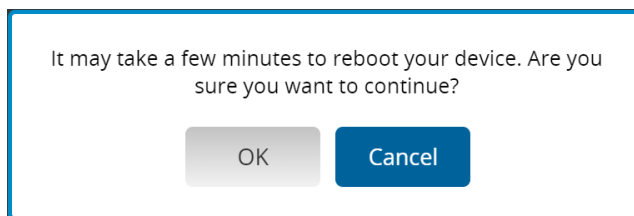
To reboot the NTC-550 Series:

1. Click the **System** tab from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.

Figure 10-25 Reboot



3. The NTC-550 Series router displays a warning that you are about to perform a reboot.
4. If you wish to proceed, select the Reboot button.

Figure 10-26 Reboot – Reboot confirmation

5. A warning popup will advise that "It may take a few minutes to reboot your device. Are you sure you want to continue?"
6. Click **OK** to continue with the reboot process.

Field test

The Field test page contains LTE, LTE SCELL and NR5G cell information which may be useful when troubleshooting signal strength issues. To access this page, navigate to **System > Field test**.

Figure 10-27 Field Test

FIELD TEST

LTE PCELL INFORMATION

PCI	EARFCN	Band	Bandwidth
409	3148	7	20MHz

LTE SCELL INFORMATION

CC ID	PCI	EARFCN	Band	Bandwidth	UL configured	State

5G NR SERVING CELL INFORMATION

CC ID	Cell ID	DL ARFCN	UL ARFCN	Band	Band type	DL BW	UL BW	DL max MIMO	UL max MIMO
7	188	176500	167500	5	SUB6	5MHz	5MHz	2	1
8	188	640332	13107	78	SUB6	60MHz	5MHz	4	1

Table 10-8 LTE PCELL Information

LTE PCELL INFORMATION	
PCI	Physical Cell ID of the LTE Cell.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
Band	The current LTE band.
Bandwidth	The current LTE bandwidth.

Table 10-9 LTE SCELL Information

LTE SCELL INFORMATION	
CC ID	Component Carrier ID.
PCI	Physical Cell ID of the LTE Cell.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.
Band	The current LTE band.
Bandwidth	The current LTE bandwidth.
UL Configured	If the Up Link is configured.
State	The current state of the LTE SCELL.

Table 10-10 NR5G Serving cell information

NR5G Serving Cell Information	
CC ID	Component Carrier ID.
Cell ID	The physical cell identifier.
DL ARFCN	Downlink Absolute Radio Frequency Channel Number.
UL ARFCN	Uplink Absolute Radio Frequency Channel Number.
Band	The NR5G band.
Band Type	The type of the NR5G band, e.g. Sub6 or mmWave.
DL BW	Downlink bandwidth.
UL BW	Uplink bandwidth.
DL max MIMO	Downlink maximum Multiple Input Multiple Output.
UL max MIMO	Uplink maximum Multiple Input Multiple Output.

Encrypted debuginfo

The Encrypted debuginfo page contains NR5G cell information which may be useful when troubleshooting signal strength issues.

Click the **Generate** button to force the NTC-550 Series router to create a debug file. A success message will appear when the debug file generation is complete. Click the **Download** button to download the generated file.

Figure 10-28 Encrypted debuginfo download



USB-OTG

The USB-OTG page allows you to enable or disable the USB port. By default, the port is enabled.

To access the USB-OTG page navigate to **System > USB-OTG**.

Figure 10-29 USB-OTG Configuration

When the port is enabled, the USB-OTG page displays the current status of the USB port, i.e. whether it is in **Device mode** or **Host mode**.

By default, **Automatic mode** is set to **On**, allowing the router to intelligently choose the correct mode. If you wish to manually override this selection, turn **Automatic mode** to **Off** and manually select either **Host** or **Device** mode.

Storage

The Storage page provides configuration options with relation to USB and SD storage devices.

To access the Storage page, navigate to **System > Storage**.

Figure 10-30 Storage Settings Configuration

The Storage Device List displays any connected storage devices and summarises the type, file system, size, used and available space on each device. Additionally, an eject button is provided to unmount the storage device so you can safely remove it.

Storage devices connected to the router can be shared using the Samba protocol. The table below lists the Network Samba Storage Settings Configuration details

Table 10-11 Network Samba Storage Settings Configuration Items

Item	Description
Storage access	Set to On to enable Samba sharing function
Verbose logging	Set to On to provide additional logging data in the system log. This should generally only be used when debugging to avoid generating excessively long logs.
Authenticated Access	
Username	The username to be used for authenticated access to the storage device. This is configured as smbuser and cannot be changed.
Password	Enter the password to be used for authenticated access to the storage device.
Verify password	Re-enter the password to be used for authenticated access to the storage device.
Read-only	Set to On to provide read-only access to the files on the connected storage device(s). When read-only access for authenticated accounts is turned on, the guest access read-only option is hidden and guests are permitted read-only access also.
Guest access	
Guest access	Set to On to enable guest access to the storage device.
Read-only	Set to On , to provide read-only access to the files on the connected storage device(s) for guest users. If the authenticated account has Read-only enabled then this option is not available and read-only access is automatically granted to guest users.

Click **Save** to save the settings.

Voltage Monitor

The Voltage Monitor page displays the Current Input Voltage and allows you to set a threshold voltage for event notification.

To access the Voltage Monitor page navigate to **System > Voltage Monitor**.

Figure 10-31 Voltage Monitor Configuration

VOLTAGE MONITOR

VOLTAGE MONITOR CONFIGURATION

Current input voltage 11.788131

Event notification threshold 8v to 38v

EVENT NOTIFICATION CONFIGURATIONS

Event notifications can be configured on the following page:
[Event Notification Configuration](#)

Save

In the **Event notification threshold field**, enter the value for threshold voltage. If the voltage drops below this value, notification is generated.

Click **Save** to save the settings

Click the **Event Notification Configuration** link to go to Event Notification Configuration page.

11. Help

The **Help** page displays a link to the help document.

Figure 11-1 Help Page



Appendix A. Configuring Radio Access Technologies

This device supports the following modes of operations in various combinations

- **LTE** (3GPP Core Network Option 1)
- **5G Non Standalone** (3GPP Core Network Option 3x)
- **5G Standalone** (3GPP Core Network Option 2)

Please refer to the following table to understand which modes of operation are possible and how to configure them.

Table A-1 RAT/Band Selection table

Mode	Allowed RAT			Supported	How to Configure	
	LTE	5G NSA	5G SA		RAT Selection Menu	Band Selection Menu
LTE Only	Yes	No	No	Yes	Select LTE only	Select LTE Frequency Bands
LTE + 5G NSA	Yes	Yes	No	Yes	Select LTE + 5G NR	Select LTE + NSA Frequency Bands
5G NSA Only	No	Yes	No	No	–	–
LTE + 5G NSA + 5G SA	Yes	Yes	Yes	Yes	Select LTE + 5G NR	Select LTE + NSA + SA Frequency Bands
LTE + 5G SA	Yes	No	Yes	No	–	–
5G NSA + 5G SA	No	Yes	Yes	No	–	–
5G SA Only	No	No	Yes	Yes	Select 5G NR	Select SA Frequency Bands

Use this table in conjunction with the settings described in sections **6.2.1.3 RAT selection** and **6.2.1.2 Band selection** of this guide.



Note: 5G Standalone Mode is not supported when utilising mmWave frequency bands.

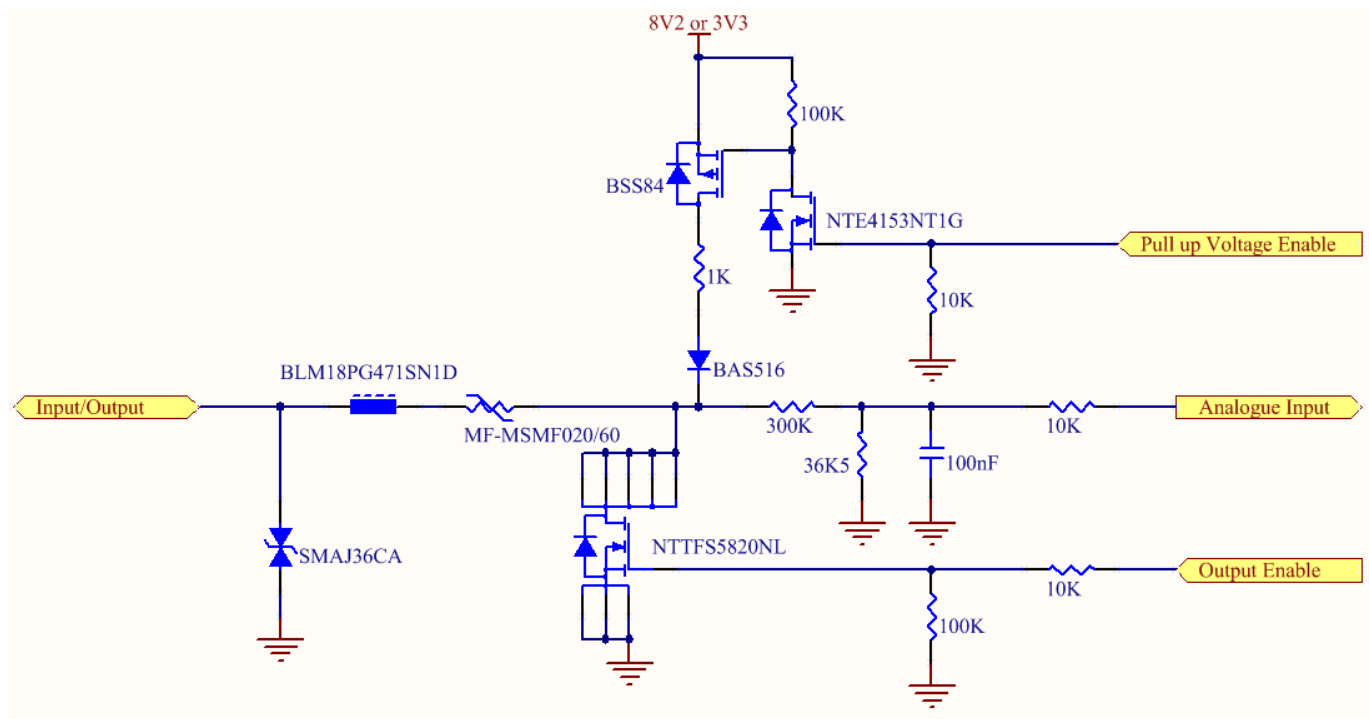
Appendix B. Inputs / Outputs

The NTC-550 Series router is equipped with a 6-way terminal block connector providing 3 identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) by the use of external resistors
- Analogue 2.7V to 30V input
- Digital input (the I/O voltage measured by the Analogue input and the software making a decision about the input state) with the threshold levels configurable in software
- Open collector output.

Hardware Interface

The interface of the 3 multipurpose inputs/outputs are based on the circuit diagram below



The Input/Output label is the physical connection to the outside world. There are protection devices and resistor dividers to condition the signal prior to it going into the processor. The three labels to the right are the interface to the processor. Output Enable activates the Transistor which provides an open collector (ground) output and can sink 200mA at 230C. It is protected by a resettable fuse and transient protection diode. If used with the pull up resistor, which can be activated by the Pull up Voltage Enable pin, then you can have a High or Low output rather than open drain. The resistor can be pulled up to 3V3 for Cmos compatible output or 8.2V by software. The Analogue Input pin can read values from 0V to 30V. It is divided by a resistor network to read appropriate levels in the processor. Depending on the sensor type used, the pull up resistor can be switched on or off. If using the NAMUR sensor configuration, the pull up will be activated to 8V2 by default.

Wiring examples

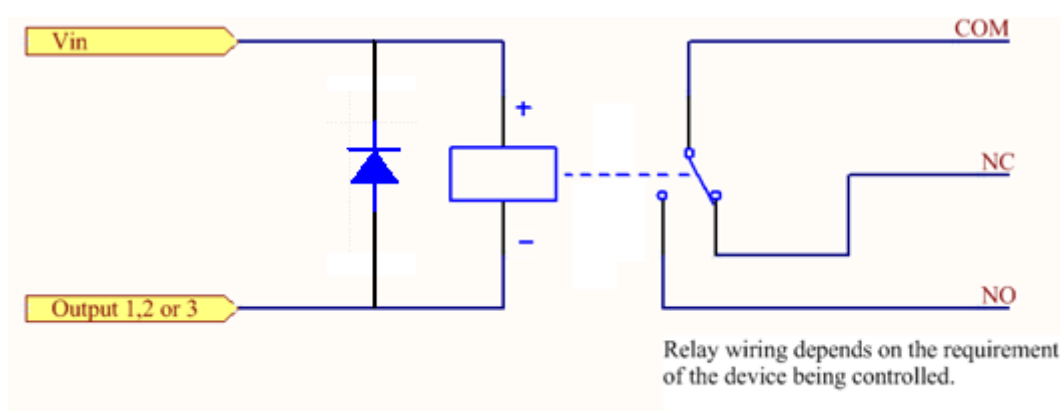
The following examples are shown as a guide as to what can be achieved by the I/O features. It is up to the system integrator to have enough knowledge about the interface to be able to achieve the required results.



Important: Lantronix does not offer any further advice on the external wiring requirements or wiring to particular sensors, and will not be responsible for any damage to the unit or any other device used in conjunction with it. Using outputs to control high voltage equipment can be dangerous. The integrator must be a qualified electrician if dealing with mains voltages controlled by this unit.

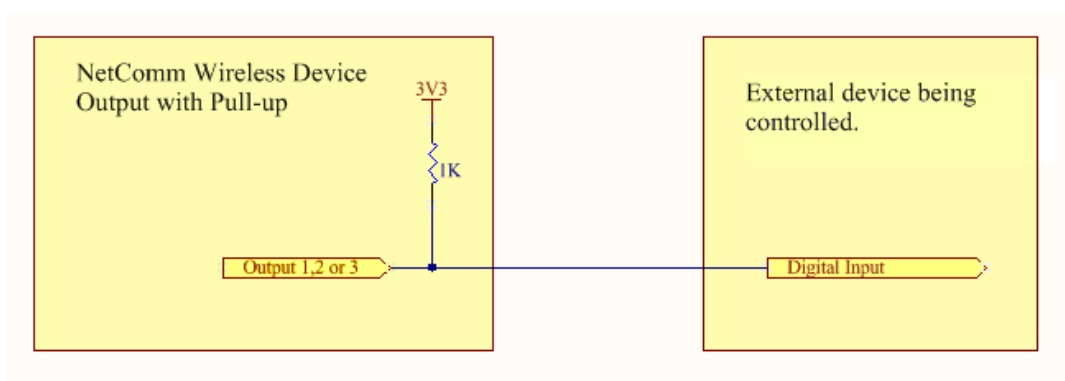
Open Collector Output driving a relay

Any output can be configured to control a relay. This is an example where the transistor will supply the ground terminal of the solenoid. External voltage is supplied to the other side of the solenoid.



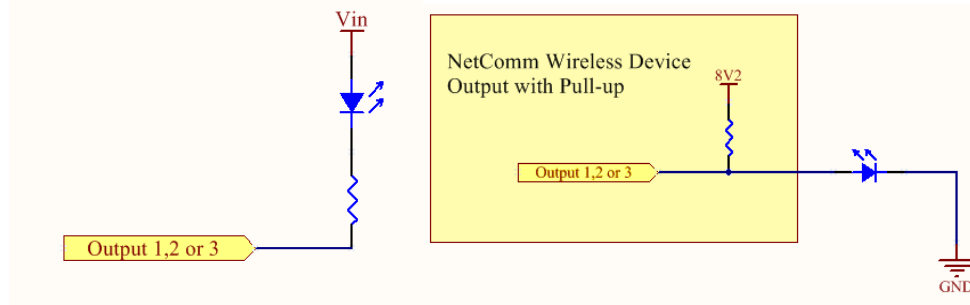
Logic level output

An output can be used with the pull up resistor to provide a logic level output which would be suitable to control an external digital device.



LED output

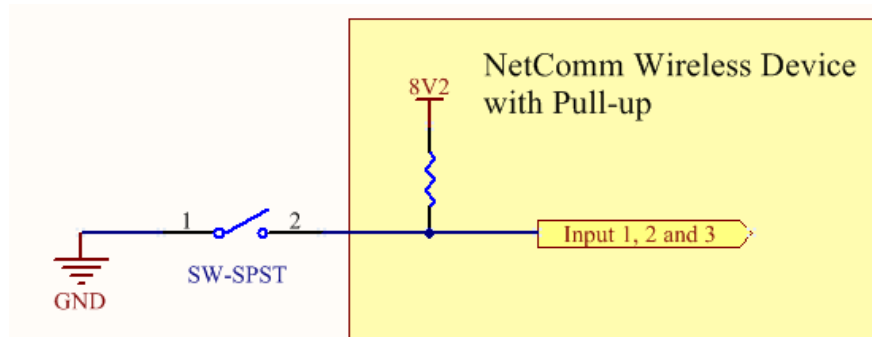
An LED can be controlled by simply providing an open collector ground to an externally powered LED Resistor value and Voltage will need to suit the LED type used. Alternatively, an LED can be powered using 8V2 via 1K resistor. The suitability of the LED will need to be investigated.



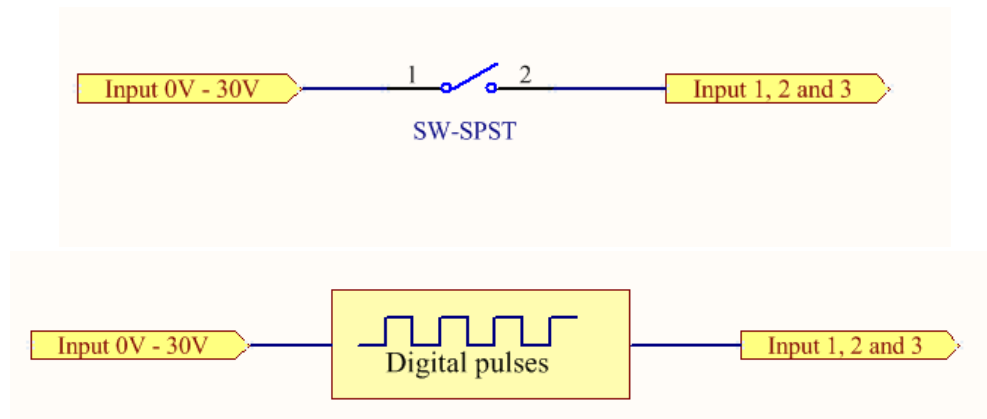
Digital inputs

There are several ways to connect a digital input. A digital input can be anything from a simple switch to a digital waveform or pulses. The unit will read the voltage in as an analogue input and the software will decode it in a certain way depending on your configuration.

Below is a contact closure type input, which is detecting an Earth. Pull up is activated for this to work.

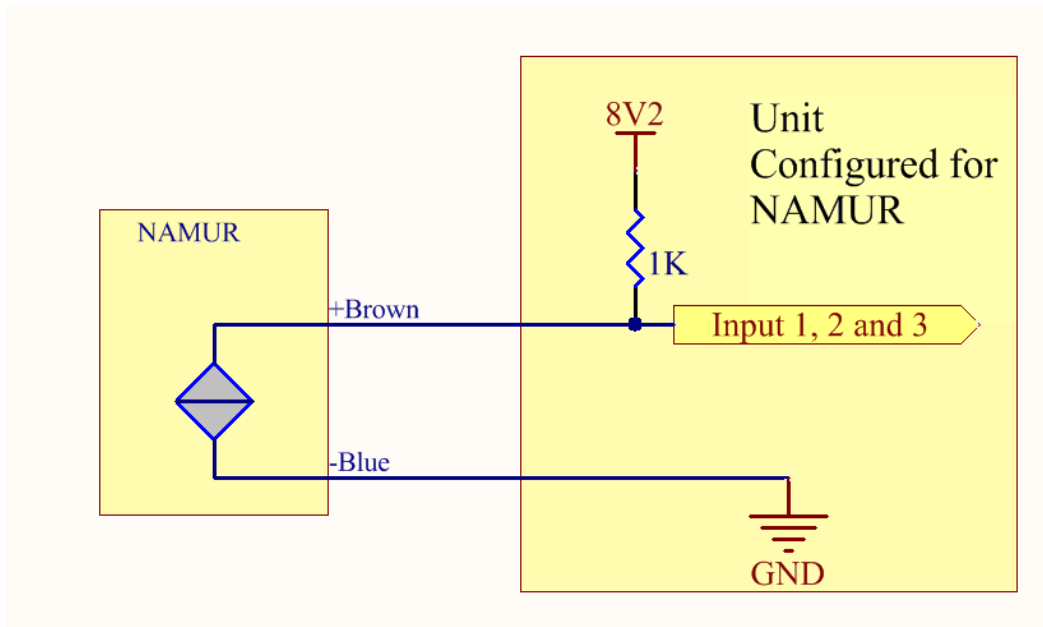


The following input detects an input going high. The turn on/off threshold can be set in the software.



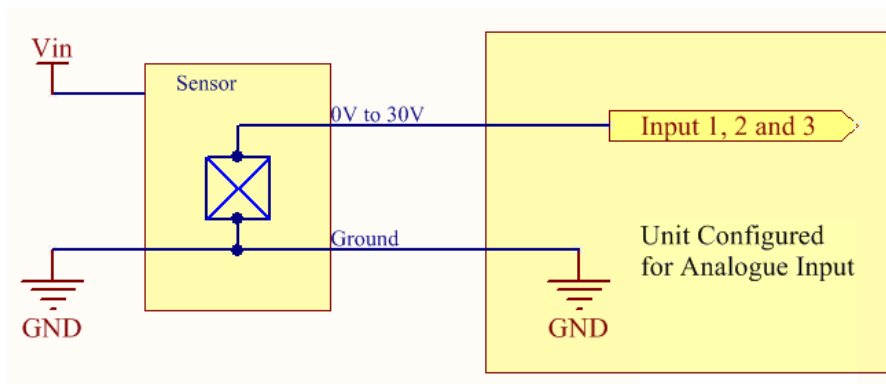
NAMUR sensor

A NAMUR sensor is a range of sensors which conform to the EN 60947-5-6 / IEC 60947-5-6 standards. They basically have two states which are reflected by the amount of current running through a sense resistor.



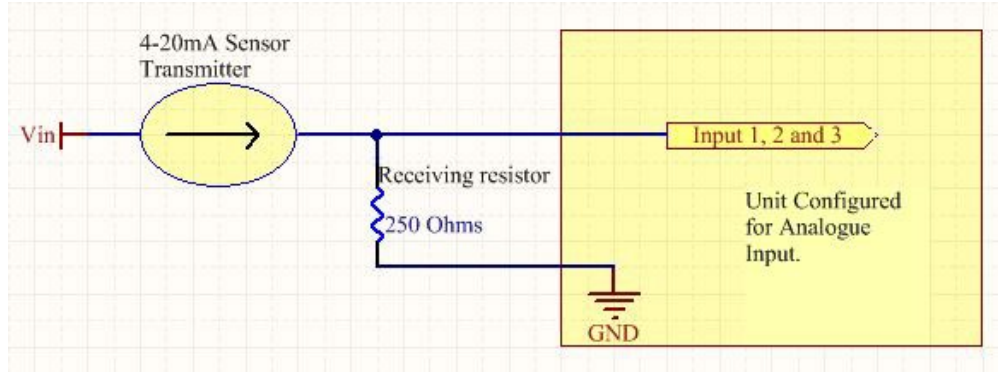
Analogue Sensor with Voltage output

There are various analogue sensors that connect directly to the unit which can provide a voltage output. These would require an external power source which may or may not be the same as the unit itself. The voltage range they provide can be between 2.7V and 30V. Some common sensor output ranges include 0V to 10V. These would work on the unit, The pull up resistor is not activated in this case.



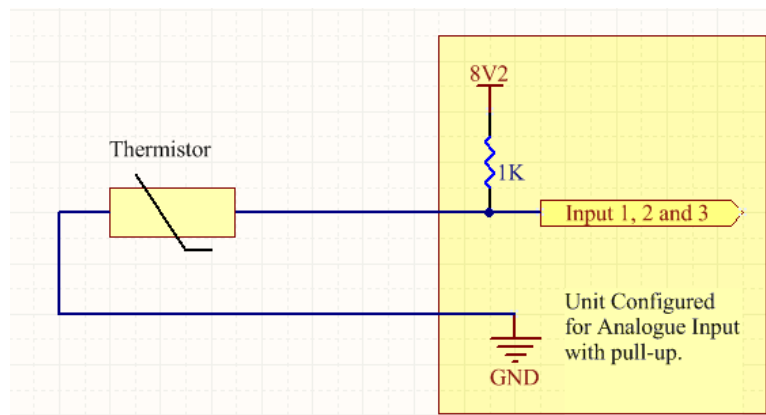
Analogue Sensor with 4 to 20mA output

Another common type of sensor type is the 4-20mA current loop sensor. It provides a known current through a fixed resistor, usually 750 ohms thus producing a voltage of 3v to 15V at the input. The sensor would require an external power source which may or may not be the same as the unit itself. It will also require an external resistor. The internal pull up resistor is not activated.



Analogue Sensor with Thermistor

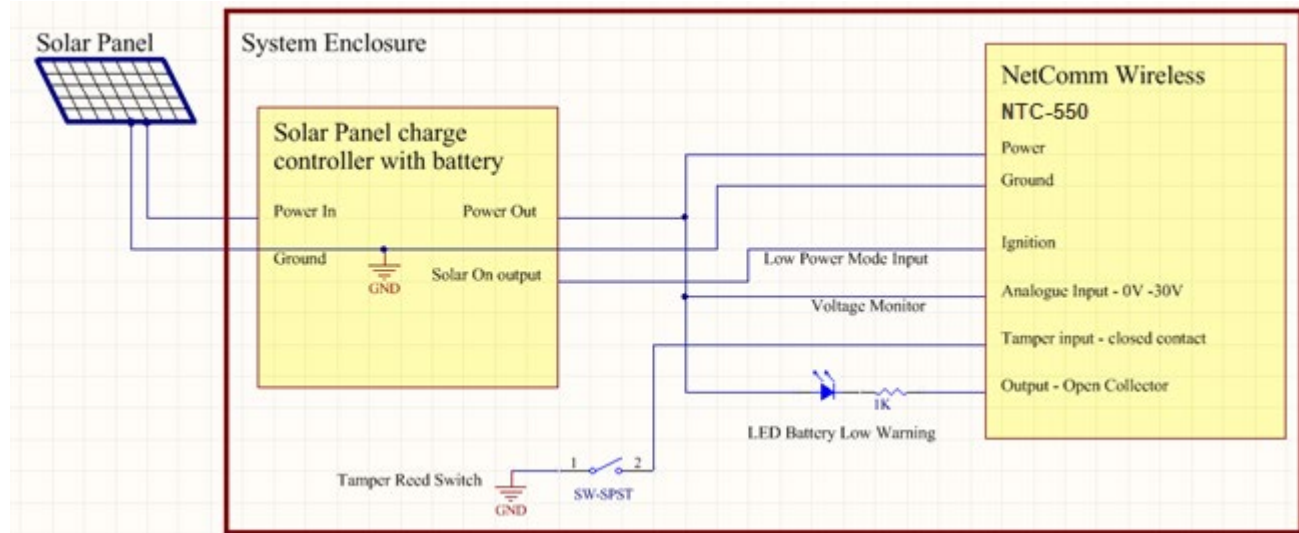
Some sensors work by changing resistance due to a change, such as temperature, light etc. These may be wired up to an external or internal power source and the resistance can be read into the analogue signal. This will require some software calibration like scaling or offset to map the voltage received to the sensor resistor value. An example below shows the internal pull-up voltage and 1K resistor activated. The voltage received depends on the combination of resistors and the value of the resistance of the sensor itself.



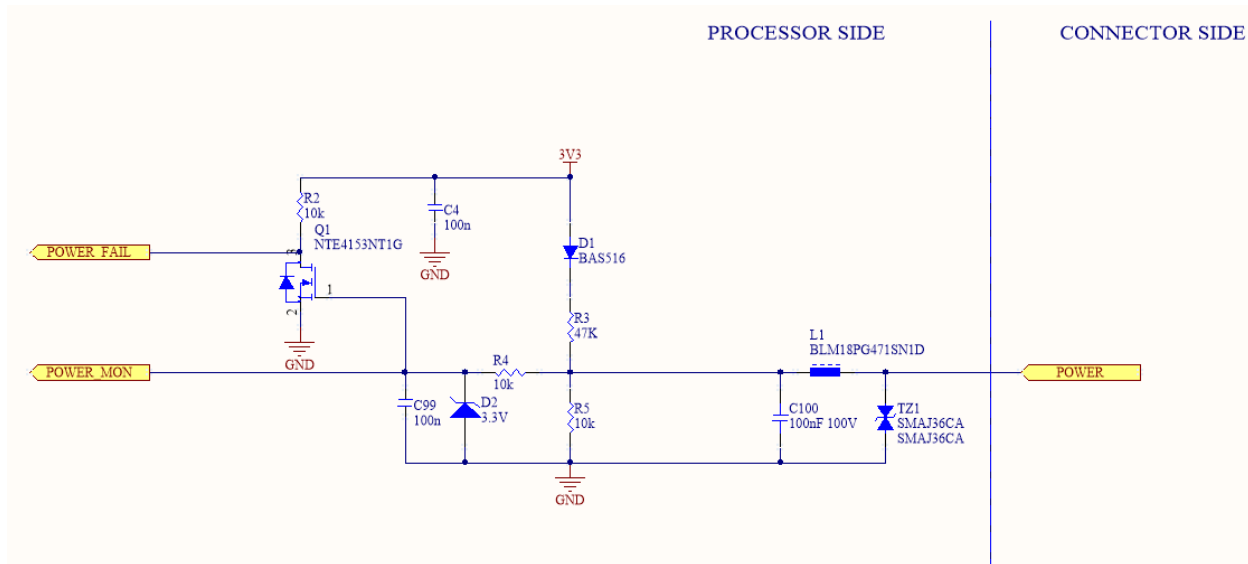
Note: Need to choose NTC with maximum temperature to have impedance > 500 Ohms

System Example – Solar powered router with battery backup

The previous examples of wiring can be used to come up with a system. The following test case is an example of how the I/O's can be used to enhance a simple router setup.



Power detection (ignition) input



The Power detection or Ignition input will detect the presence of three states from the connector side (outside world). It will detect three states, those being High, Low and Unconnected (floating).

The detection uses both analogue and digital inputs to the microprocessor.

- This is the “LOW” state:
If input voltage at POWER port is less than 0.5V the transistor Q1 is shut, POWER FAIL is asserted high advising micro that no Backup Power is present on POWER port.
- This is the “Floating” state:
If voltage at POWER port is 0.5-3V POWER FAIL signal de-asserts but POWER MON signal can be measured by ADC of micro and advise the system that there is little or no connection to the unit.
- This is the “HIGH” state:
If voltage at POWER port is higher than 3.3V (which normally is an indication of presence of decent power source), the POWER FAIL is still de-asserted, the POWER MON will measure from 3.3V up to whatever voltage is detected. The maximum detection voltage is 30V and clamps to anything above 36V.

The states can be adjusted in software to fine tune the transition points between the states.

Appendix C. Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

Lantronix, Inc. 48 Discovery, Suite 250, Irvine, CA 92618 USA

Product Family:

NTC-550 Series

Conforms to the following standards or other normative documents:

Country	Specification
USA	In progress
Canada	In progress
EU	See EU Declaration of Conformity (figure C-1)
United Kingdom	See UK Declaration of Conformity (figure C-2)
Safety	EN IEC 62368-1 AS/NZS 62368-1

EU Declaration of Conformity

Figure C-1 EU Declaration of Conformity





EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-552
Rated: 12Vdc, 3A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:



ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)

- EN IEC 62368-1:2020/A11:2020

EMC Directive (2014/30/EU)

- EN 301 489-1 V2.2.3 (2019-11) Class B
- EN 301 489-17 V3.2.4 (2020-09)
- EN 301 489-19 V2.2.1 (2022-09)
- EN 301 489-52 V1.2.1 (2021-11)
- EN 55032:2015/A11:2020, Class B
- EN 55035:2017+A11:2020
- EN 61000-3-2:2014 Class A
- EN 61000-3-3:2013

RF Radio Directive (2014 / 53 / EU)

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)
- EN 303 413 V1.2.1 (2021-04)

Health Directive (2014 / 53 / EU)

- EN IEC 62311:2020

RoHS 2011/65/EU(RoHS 2.0) & and its subsequent amendments Directive (EU) 2015/863

- EN 62321-2:2021

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: 

Name: Steve Burrington

Date: 26 Jun 2025

Title: Vice President RnD

CERT-XXXXXX rev A

EU Statements

Table C-1 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този NTC-550 Series отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53/EU. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: https://www.lantronix.com/products/ntc-550-series/ Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи наоткрито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento NTC-550 Series je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: https://www.lantronix.com/products/ntc-550-series/ Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr NTC-550 Series overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: https://www.lantronix.com/products/ntc-550-series/ EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät NTC-550 Series in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: https://www.lantronix.com/products/ntc-550-series/ EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betrieben werden.
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme NTC-550 Series vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: https://www.lantronix.com/products/ntc-550-series/ EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.

Code	Language	Statement
en	English	Hereby, Lantronix, Inc., declares that this NTC-550 Series is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.lantronix.com/products/ntc-550-series/ EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el NTC-550 Series module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: https://www.lantronix.com/products/ntc-550-series/ Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NTC-550 Series ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: https://www.lantronix.com/products/ntc-550-series/ Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil NTC-550 Series est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante: https://www.lantronix.com/products/ntc-550-series/ Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé à l'extérieur
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að NTC-550 Series sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisýfirlýsingarinnar er að finna á eftirfarandi internetfangi: https://www.lantronix.com/products/ntc-550-series/ Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngutakmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo NTC-550 Series è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.

Code	Language	Statement
		Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: https://www.lantronix.com/products/ntc-550-series/ Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzato all'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka NTC-550 Series atbilst Direktīvas 2014/ 53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: https://www.lantronix.com/products/ntc-550-series/ ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekšējās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruojama, kad šis NTC-550 Series atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: https://www.lantronix.com/products/ntc-550-series/ ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel NTC-550 Series overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: https://www.lantronix.com/products/ntc-550-series/ EU kennisgeving van gebruiksbepalingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan NTC-550 Series jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta 'konformità tal-UE huwa disponibbli flindirizz tal-internet li ġej: https://www.lantronix.com/products/ntc-550-series/ Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jiġihaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a NTC-550 Series megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: https://www.lantronix.com/products/ntc-550-series/ EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne NTC-550 Series er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU.

Code	Language	Statement
		Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: https://www.lantronix.com/products/ntc-550-series/ EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukes utendørs.
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że NTC-550 Series jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności EU jest dostępny pod następującym adresem internetowym: https://www.lantronix.com/products/ntc-550-series/ Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este NTC-550 Series está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: https://www.lantronix.com/products/ntc-550-series/ Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest NTC-550 Series respect cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: https://www.lantronix.com/products/ntc-550-series/ Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај NTC-550 Series у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: https://www.lantronix.com/products/ntc-550-series/ Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta NTC-550 Series v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: https://www.lantronix.com/products/ntc-550-series/ Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že NTC-550 Series enterprise Wi-Fi IoT module spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.

Code	Language	Statement
		Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: https://www.lantronix.com/products/ntc-550-series/ Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että NTC-550 Series tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: https://www.lantronix.com/products/ntc-550-series/ EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna NTC-550 Series står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: https://www.lantronix.com/products/ntc-550-series/ EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

UK Declaration of Conformity

Figure C-2 UK Declaration of Conformity





UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250 Irvine, CA 92618 USA
Model Name: NTC-502
Rated: 12Vdc, 1.5A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:



ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Electrical Equipment Regulations 2016

- EN IEC 62368-1:2020/A11:2020
- EN IEC 62311:2020

Electromagnetic Compatibility Regulations 2016

- EN 301 489-1 V2.2.3 (2019-11) Class B
- EN 301 489-17 V3.2.4 (2020-09)
- EN 301 489-19 V2.2.1 (2022-09)
- EN 301 489-52 V1.2.1 (2021-11)
- EN 55032:2015/A11:2020, Class B
- EN 55035:2017+A11:2020
- EN 61000-3-2:2014 Class A
- EN 61000-3-3:2013

Radio Equipment Regulations 2017

- EN 301 908-1 V15.2.1(2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.2.1 (2022-02)
- Draft EN 301-908-25 V15.1.1_15.0.9 (2021-06)

RoHS
UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).
2011/65/EU(RoHS 2.0) & and its subsequent amendments Directive (EU) 2015/863

- BS EN 62321-2:2021

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: 
 Name: Steve Burrington

Date: 26 Jun 2025
 Title: Vice President RnD

CERT-XXXXXX rev A