

# Tait Core Networks

## Installation and Configuration Manual

MNB-00012-14 · Issue 14 · June 2023

## Contact Information

### Tait Communications Corporate Head Office

Tait International Limited  
P.O. Box 1645  
Christchurch  
New Zealand

### Imported into the EU by:

Tait Communications GmbH  
Stipcakgasse 40  
1230 Vienna  
Austria

### Imported into the UK by:

Tait Europe Limited  
Unit A, Buckingham Business Park, Anderson Road  
Swavesey  
Cambridge, CB24 4UQ  
United Kingdom

For the address and telephone number of regional offices, refer to our website:

[www.taitcommunications.com](http://www.taitcommunications.com)

## Copyright and Trademarks

All information contained in this document is the property of Tait International Limited. All rights reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, stored, or reduced to any electronic medium or machine-readable form, without prior written permission from Tait International Limited.

The word TAIT, TAITNET and the TAIT logo are trademarks of Tait International Limited.

All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturers.

By using a Tait product you are agreeing to be bound by the terms of the Tait Software Licence Agreement. Please read the Tait Software Licence Agreement carefully before using this Tait product. If you do not agree to the terms of the Tait Software Licence Agreement, do not use the Tait Product. The full agreement is available at [www.taitcommunications.com/our-resources/legal#Tait\\_Software\\_Licence\\_Agreement](http://www.taitcommunications.com/our-resources/legal#Tait_Software_Licence_Agreement).

## Disclaimer

There are no warranties extended or granted by this document. Tait International Limited accepts no responsibility for damage arising from use of the information contained in the document or of the equipment and software it describes. It is the responsibility of the user to ensure that use of such information, equipment and software complies with the laws, rules and regulations of the applicable jurisdictions.

## Enquiries and Comments

If you have any enquiries regarding this document, or any comments, suggestions and notifications of errors, please contact your regional Tait office.

## Updates of Manual and Equipment

In the interests of improving the performance, reliability or servicing of the equipment, Tait International Limited reserves the right to update the equipment or this document or both without prior notice.

## Intellectual Property Rights

This product may be protected by one or more patents or designs of Tait International Limited together with their international equivalents, pending patent or design applications, and registered trade marks, for a complete list please check

[www.taitcommunications.com/our-resources/legal#Intellectual\\_Property](http://www.taitcommunications.com/our-resources/legal#Intellectual_Property)

DMR only: The AMBE+2™ voice coding Technology embodied in this product is protected by intellectual property rights including patent rights, copyrights and trade secrets of Digital Voice Systems, Inc. This voice coding Technology is licensed solely for use within this Communications Equipment. The user of this Technology is explicitly prohibited from attempting to decompile, reverse engineer, or disassemble the Object Code, or in any other way convert the Object Code into a human-readable form.

## Environmental Responsibilities



Tait International Limited is an environmentally responsible company which supports waste minimization, material recovery and restrictions in the use of hazardous materials.

The European Union's Waste Electrical and Electronic Equipment (WEEE) Directive requires that this product be disposed of separately from the general waste stream when its service life is over. For more information about how to dispose of your unwanted Tait product, visit the Tait WEEE website at [www.taitcommunications.com/our-resources/compliance#WEEE](http://www.taitcommunications.com/our-resources/compliance#WEEE). Please be environmentally responsible and dispose through the original supplier, or contact Tait International Limited.

Tait will comply with environmental requirements in other markets as they are introduced.

# Contents

---

<b>Preface</b> .....	<b>7</b>
Scope of Manual .....	7
Document Conventions .....	8
Associated Documents .....	8
Publication Record .....	9
<b>1 Introduction</b> .....	<b>12</b>
1.1 Administration Application .....	12
1.2 Installation and Operation .....	13
1.2.1 Before You Start .....	13
1.2.2 Information Required .....	13
1.2.3 Equipment Required .....	13
<b>2 BIOS and iDRAC Settings</b> .....	<b>16</b>
2.1 Configuring BIOS Settings .....	16
2.1.1 BIOS and BMC Settings in the Kontron CG2400 .....	16
2.1.2 BIOS and BMC Settings in the Kontron CG2300 .....	17
2.1.3 BIOS and iDRAC Settings in the Dell R250 .....	19
2.1.4 BIOS Settings in the Sintrones SBOX-2620 or SBOX-2621 .....	24
<b>3 USB Installation</b> .....	<b>26</b>
3.1 USB Installation on a Sintrones Server .....	26
3.2 USB Installation on a Kontron Server CG2300/CG2400 .....	26
3.3 USB Installation on a Dell Server .....	27
<b>4 Remote Installation</b> .....	<b>28</b>
4.1 Remote installation on a Kontron Server CG2400 .....	28
4.2 Remote Installation on a Dell Server .....	31
<b>5 Installing TaitCentOS</b> .....	<b>35</b>
5.1 TaitCentOS Installation Process .....	35
5.2 Upgrading TaitCentOS .....	36
5.2.1 Uploading a TaitCentOS Upgrade Package .....	36
5.2.2 Installing the TaitCentOS Upgrade Package .....	36
5.3 Changing the Default IP Address Using the Network Configuration Tool .....	37
5.3.1 Changing the Network Settings on TaitCentOS 6 .....	37
5.3.2 Changing the Network Settings on TaitCentOS 7 .....	37

5.4	Migrating from TaitCentOS 6 to TaitCentOS 7 .....	42
5.5	Migrating from Solaris to TaitCentOS .....	42
<b>6</b>	<b>Installing Tait Ubuntu .....</b>	<b>43</b>
6.1	Automated Operating System Installation .....	43
6.2	Automated Tait Customizations .....	44
6.3	Network Configuration .....	44
6.3.1	Configuring Ethernet Bonding .....	45
6.3.2	Configuring the Hostname .....	46
6.4	Migrating from TaitCentOS to Tait Ubuntu .....	46
6.5	Migrating from Solaris to Tait Ubuntu .....	47
<b>7</b>	<b>Logging On to the Administration Application .....</b>	<b>49</b>
<b>8</b>	<b>Installing the Tait Packages Using TaitCentOS .....</b>	<b>50</b>
8.1	Software Installation or Upgrades .....	50
8.2	Recovering from a Failed Firmware Upgrade .....	53
<b>9</b>	<b>Installing the Tait Packages Using Tait Ubuntu .....</b>	<b>54</b>
9.1	Software Installation or Upgrades .....	54
9.2	Recovering from a Failed Firmware Upgrade .....	57
<b>10</b>	<b>Operations .....</b>	<b>58</b>
10.1	Logging on using SSH .....	58
10.1.1	Logging into a Container Using SSH (Tait Ubuntu only) .....	58
10.2	Logging on as 'root' .....	59
10.2.1	TaitCentOS Users .....	59
10.2.2	Tait Ubuntu Users .....	59
10.3	Logging in to a Tait Service .....	60
10.3.1	From the User Interface Home Page (TaitCentOS Only) .....	60
10.3.2	From the TaitNet Administration Application .....	60
10.4	Creating Your Custom 'ssh' Login Script .....	61
10.4.1	TaitCentOS .....	61
10.4.2	Tait Ubuntu .....	62
10.5	Installing License Files .....	63
10.5.1	Checking that the License File is Correct .....	63
10.5.2	Obtaining the Host ID .....	63
10.5.3	Obtaining the license.dat File .....	63
10.5.4	Installing License Files .....	64
10.6	Self-Signed SSL Certificates .....	64
10.6.1	Firefox Users .....	64
10.6.2	Chrome Users .....	66

10.6.3	Internet Explorer and Microsoft Edge Users .....	67
10.7	Using the Certificate from a Certification Authority (CA) .....	67
10.8	Changing Passwords .....	68
10.8.1	Changing the 'root' and 'taitnet' Passwords .....	69
10.8.2	Changing the iDRAC Password .....	69
10.9	Performing an Operating System Restart .....	70
10.10	Stopping/Starting the Services Software .....	71
10.11	Powering Down .....	72
10.12	Changing to a Local Time Zone .....	72
10.13	TaitCentOS Only - Collecting Logs From Other Network Equipment .....	73
10.13.1	Configuring the Base Stations .....	73
10.13.2	Configuring the Controller .....	73
10.13.3	Operating the Administration Application .....	73
10.13.4	General Information .....	74
10.13.5	tait_collector.conf File .....	74
<b>11</b>	<b>Basic Configuration .....</b>	<b>76</b>
11.1	Configuration .....	76
11.1.1	General .....	76
11.1.2	Tait Services .....	76
11.1.3	DNS .....	76
11.1.4	Network Time Protocol (NTP) .....	77
11.1.5	SNMP .....	77
11.1.6	Firewall - TaitCentOS .....	78
11.1.7	Firewall - Tait Ubuntu .....	80
11.1.8	SSL .....	81
11.1.9	Syslog .....	82
11.1.10	Anti Virus .....	82
11.2	Files .....	83
11.2.1	Logs .....	83
11.2.2	Backups .....	83
11.2.3	Firmware .....	84
11.3	Credentials .....	85
11.3.1	Password .....	85
11.3.2	Users .....	85
11.3.3	Authentication .....	86
<b>12</b>	<b>Administration Application Information .....</b>	<b>90</b>
12.1	IP Protocols and Default Ports .....	90
12.1.1	IP Protocols .....	90
12.1.2	IP Default Ports .....	91
12.2	Log Files .....	92
12.2.1	Installation and Upgrade Logs .....	92

<b>Appendix 1:Transferring an ISO Image to a USB Flash Drive .....</b>	<b>94</b>
A.1 Using Rufus for TaitCentOS .....	94
A.2 Using Rufus for Tait Ubuntu .....	96
A.3 Using dd for Tait Ubuntu on Linux .....	97
A.4 Using Win32DiskImager for TaitCentOS .....	98
<b>Appendix 2:Ethernet Bonding on TaitCentOS 7 DMR Networks .....</b>	<b>101</b>
A.1 Hardware Platform .....	101
A.2 Supported Redundant Configuration.....	101
A.3 Implementation .....	101
A.3.1 Requirements.....	101
A.3.2 Switch Configuration .....	102
A.3.3 Enabling Ethernet Bonding.....	102
A.3.4 Checking Ethernet Bonding .....	103
A.3.5 Removing Ethernet Bonding.....	104

# Preface

---

## Scope of Manual

This Installation and Administration Configuration Manual explains the steps required to configure the BIOS or iDRAC in the network servers, and to install TaitCentOS or Tait Ubuntu, and the Administration application.

It also explains the steps required to install TaitNet systems and configure them using the TaitNet Administration application.

It covers the following radio systems:

- TaitNet TN9300 DMR trunked (Tier 3)
- TaitNet TN9300 DMR conventional (Tier 2)
- TaitNet TN8291 MPT-IP trunked
- TaitNet TN9400 P25 Phase 1 and Phase 2 trunked

It also covers the following Tait services (products and software):

- TN9300 Node Controller\*
- TN9300 Channel Controller\*
- TN8291 Node Controller\*
- TN9400 RFSS Controller
- TN9400 Site Controller
- TN9500 Inter-Network Gateway
- T1541 Node Controller
- TN9361 SCADA Gateway
- Q9371 G.711 Connector\*
- PTTToX Connector
- PTTToX Client\*
- Data API Connector\*
- Channel Group Manager\*



The Tait Ubuntu operating system is only supported for the services listed above that are marked with an \*

# Document Conventions

Within this manual, two types of alerts may be given to the reader. The following paragraphs illustrate each type of alert and its associated symbol.



**This alert is used to warn about the risk of data loss or corruption.**



This icon is used to draw your attention to information that may improve your understanding of the equipment or procedure.

Text in the following format shows text that is displayed on your monitor:

Is this correct (y/n) [y]?

Text in the following format is text that you need to enter on your keyboard:

**cd /SP/network**

## Associated Documents

The following documents are published on the Tait Partner Portal website (<https://partnerinfo.taitcommunications.com>).

Publication	Number	P25	DMR	Analog
TaitNet MPT1327 System Manual	MNA-00019			✓
T1541 Operations Manual	MNA-00007			✓
T1561 Digital Audio Switch Series II Installation Manual	MNA-00011			✓
TaitNet MPT-IP System Manual	MNA-00026			✓
TN8271 Network Gateway Installation and Operation Manual	MNA-00028			✓
TN9300 DMR Trunked System Manual	MNB-00003		✓	
TN9300 DMR Channel Group System Manual	MNB-00010		✓	
TN9300 DMR Trunked Node Help	MNB-00002		✓	
Migrating TaitNet MPT Networks using the TN9500 System Manual	MNB-00009			✓
TN9500 Configuration Manual	MNB-00008			✓
TaitNet P25 Conventional Networks System Manual	MBA-00032	✓		
TN9400 P25 Trunked Network Maintenance Manual	MNC-00001	✓		



Publication	Number	P25	DMR	Analog
P25 and AS-IP Channel Group System Manual	MND-00002	✓		
Tait GridLink SCADA Communications Solution System Manual	MNE-00026		✓	
SCADA Gateway Installation and Configuration Manual	MNE-00020		✓	
TN9271 Analog Gateway Installation and Operation Manual	MNB-00017		✓	

Technical Notes are also published from time to time to describe applications for Tait products, to provide technical details not included in manuals, and to offer solutions for any problems that arise.

## Publication Record

Version	Publication date	Amended sections and pages
14	June 2023	<p>Updated for DMR/MPT-IP release TaitCentOS3.48/Tait Ubuntu 4.48 and later, and TN9400 2.26 and later</p> <ul style="list-style-type: none"> <li>■ <a href="#">Scope of Manual</a> updated</li> <li>■ <a href="#">Section 2.1.3 BIOS and iDRAC Settings in the Dell R250</a> updated</li> <li>■ <a href="#">Section 6.1 Automated Operating System Installation</a> updated</li> <li>■ <a href="#">Section 6.3 Network Configuration</a> updated</li> <li>■ <a href="#">Section 6.3.2 Configuring the Hostname</a> updated</li> <li>■ <a href="#">Section 10.8 Changing Passwords</a> updated</li> </ul>
13	December 2022	<p>Updated for DMR/MPT-IP release 3.46 and later, and TN9400 2.24 and later</p> <ul style="list-style-type: none"> <li>■ <a href="#">Section 2.1.1 BIOS and BMC Settings in the Kontron CG2400</a> updated</li> <li>■ <a href="#">Section 6.3.1 Configuring Ethernet Bonding</a> added</li> <li>■ <a href="#">Section 6.3.2 Configuring the Hostname</a> added</li> <li>■ <a href="#">Section 11.1.2 Tait Services</a> updated</li> </ul>
12	October 2022	<p>Updated for DMR/MPT-IP release 3.44 and later, and TN9400 2.22 and later</p> <ul style="list-style-type: none"> <li>■ Dell R250 replaces Dell R240</li> <li>■ Updated throughout for Tait Ubuntu operating system</li> <li>■ <a href="#">Appendix 2 Ethernet Bonding on TaitCentOS 7 DMR Networks</a> added</li> </ul>

<b>Version</b>	<b>Publication date</b>	<b>Amended sections and pages</b>
11	May 2022	<p>Updated for DMR/MPT-IP release 3.42 and later, and TN9400 2.20 and later</p> <ul style="list-style-type: none"> <li>■ Sintrones SBOX-2621 servers can only be booted up by a USB type 3.0 flash drive</li> <li>■ Section 2.1.2 Equipment Required updated</li> <li>■ Section 8.7 Changing Passwords updated</li> <li>■ Removed Section 4.13, use of feeds service no longer recommended</li> <li>■ Section 13.1.11 Anti Virus updated</li> </ul>
10	December 2021	<p>Updated for DMR/MPT-IP release 3.38.02 and later, and TN9400 2.16 and later</p> <ul style="list-style-type: none"> <li>■ Sintrones SBOX-2621 replaces Sintrones SBOX-2620</li> <li>■ Section 2.1.1 BIOS and BMC Settings in the Kontron CG2400 updated</li> <li>■ Section 2.1.3 BIOS and iDRAC Settings in the Dell R250 updated</li> <li>■ Footnote added to Section 2.6 Migrating from TaitCentOS 6 to TaitCentOS 7</li> </ul>
9	May 2021	<p>Updated for DMR/MPT-IP release 3.38 and later, and TN9400 2.14 and later</p> <ul style="list-style-type: none"> <li>■ TN9361 SCADA Gateway added to manual</li> <li>■ Server table updated in Section 2.1 Configuring BIOS Settings</li> </ul>
8	December 2020	<p>Updated for DMR/MPT-IP release 3.36 and later, and TN9400 2.12 and later</p> <ul style="list-style-type: none"> <li>■ "Notes for the Kontron CG2400" on page 13 added</li> <li>■ Section 2.5.1 Changing the Network Settings on TaitCentOS 6 updated to include instructions for setting the system hostname</li> <li>■ Section 2.5.2 Changing the Network Settings on TaitCentOS 7 updated to include instructions for setting the system hostname</li> <li>■ Section 13.1.7 Firewall - TaitCentOS updated</li> </ul>

Version	Publication date	Amended sections and pages
07	September 2020	<p>Updated for DMR/MPT-IP release 3.34 and later, and TN9400 2.10 and later</p> <ul style="list-style-type: none"> <li>■ Kontron CG2400 server added</li> <li>■ Section 2.1.1 BIOS and BMC Settings in the Kontron CG2400 added</li> <li>■ “Changing to UEFI Boot Mode (Optional)” added to Section 2.1.2 BIOS and BMC Settings in the Kontron CG2300</li> <li>■ Section 2.3 Installing TaitCentOS for the First Time updated to include TaitCentOS 7, the Kontron CG2400, and to rename subsections</li> <li>■ Section 2.5 Changing the Default IP Address Using the Network Configuration Tool updated, by being split into Section 2.5.1 Changing the Network Settings on TaitCentOS 6 and Section 2.5.2 Changing the Network Settings on TaitCentOS 7</li> <li>■ Section 2.6 Migrating from TaitCentOS 6 to TaitCentOS 7 added</li> <li>■ Section 8.4.1 Checking that the License File is Correct updated</li> <li>■ Section 8.7 Changing Passwords updated</li> <li>■ Section 8.11 Changing to a Local Time Zone updated</li> <li>■ Section 13.1.11 Anti Virus added</li> </ul>
06	May 2020	<p>Updated for DMR/MPT-IP release 3.32 (and 2.32) and later, and TN9400 2.08 and later</p> <ul style="list-style-type: none"> <li>■ Section 2.3.5 Installing TaitCentOS from the BMC Web Console added</li> <li>■ Section 2.3.6 Installing TaitCentOS from the iDRAC Virtual Console added</li> <li>■ Section 2.4 Upgrading TaitCentOS added</li> </ul>
05	December 2019	Updated for DMR/MPT-IP release 3.30 (and 2.30) and later, and TN9400 2.06 and later
04	May 2019	Updated for DMR/MPT-IP release 3.26 (and 2.26) and later, and TN9400 2.02 and later
03	November 2018	Updated for DMR/MPT-IP release 3.24 (and 2.24) and later
02	August 2018	Updated for release 2.22 and 3.22 and later
01	May 2018	First release

# 1 Introduction

---

TaitNet networks include DMR, MPT and MPT-IP, P25, conventional, trunked, simulcast and non-simulcast systems. Different kinds of network can connect through gateways, for example analog with digital, or Tait with third-party.

DMR Trunked networks use the Tait Ubuntu operating system (based on Ubuntu 22.04.LTS).

Two operating systems are currently available:

- TaitCentOS (based on CentOS 7)
- Tait Ubuntu (based on Ubuntu 22.04 LTS)

## TaitCentOS

The modularity of Tait products allows this Installation and Configuration Manual to cover the following networks running on TaitCentOS:

- TN9300 DMR conventional
- TN9300 DMR trunked
- TN8291 MPT-IP
- TN9400 P25 Phase 1 and Phase 2 trunked

## Tait Ubuntu

The modularity of Tait products allows this Installation and Configuration Manual to cover the following networks running on Tait Ubuntu:

- TN9300 DMR conventional
- TN9300 DMR trunked
- TN8291 MPT-IP

## 1.1 Administration Application


The TaitNet Administration application enables network administrators to enter and maintain the parameters and settings required at server level for Tait DMR Trunked networks.

It enables administrators to:

- View and edit network settings
- Monitor and stop/start Tait Services
- Monitor and download alarms and logs
- Backup/restore the configuration database
- Upload/install operating system updates and new application firmware and updates
- Implement authentication via RADIUS<sup>1</sup> or LDAP
- Add users and set security access

## 1.2 Installation and Operation

### 1.2.1 Before You Start

-  Only install the operating system version supplied by Tait, to ensure the correct configuration settings are installed and as a security precaution to ensure nothing else is installed. This version includes the TaitNet Administration application.

### 1.2.2 Information Required

Ensure that you have the following information at hand before beginning the installation:

- Host names
- IP addresses
- Subnet mask
- IP address of router/gateway
- IP Address of DNS server (optional)
- You should obtain the latest operating system patch file from Tait. It contains all the latest security updates and bug fixes. You can install these patches via the Administration application after you have finished installing the operating system. You should patch the operating system whenever a new patch becomes available.

### 1.2.3 Equipment Required

- IP-connected server with monitor, keyboard and mouse
- USB flash drive containing the operating system
- USB flash drive containing Tait network software



**A network cable must be plugged into the server (all server types) before you start the installation process. The network cable must be connected to a working network device, such as a switch. The Ethernet port you plug it into must be the one you will use during the normal operation of the server. Refer to "[Notes for the Kontron CG2400](#)" on page 14, when choosing which port to use on a Kontron CG2400 server. The cable must remain connected and active during the entire install process.**

-  Refer to "[Transferring an ISO Image to a USB Flash Drive](#)" on page 94 for instructions on how to load operating system software on to USB flash drives.

- 
1. Radius is not supported on TN9400 networks.

**i** In the installation instructions, the use of the term ‘select’ means highlight the item and press `Enter`.

Tait software can be installed on one of the following servers running the Tait operating system and Tait network software:

	<b>Kontron CG2400/ CG2300</b>	<b>Dell R250/ R240</b>	<b>Sintronex SBOX-2621</b>
<b>TN9300</b>	Yes	Yes	Yes
<b>TN9500</b>	Yes	Yes	No
<b>T1541</b>	No	No	No
<b>TN8291</b>	Yes	Yes	No

**Notes for the Dell R250 and Sintronex SBOX-2621**

If using a USB, the Dell R250 and Sintronex SBOX-2621 servers can only be booted up by a USB type 3.0 flash drive. When installing software on a Dell R250 or Sintronex SBOX-2621, please make sure your flash drive is compliant. The internet can provide tips on how to recognize a USB 3.0 flash drive (e.g. sometimes it has a blue insert). If problems arise, please contact Tait Technical Support.

**Notes for the Kontron CG2400**

When setting up the Kontron CG2400, the Ethernet cable must be plugged in to the PCI NIC port 0, which is in the PCI card that is installed in either slot 6 or 7 at the rear of the server. In the following example, the PCI card is in slot 7.

Ethernet cable in PCI NIC port 0



The installation steps are listed in the order in which they should be carried out.

1. BIOS and iDRAC settings:  
Either
  - Set up for USB installation, or
  - Set up for remote installation
2. Installing the operating system:
  - Install TaitCentOS or Tait Ubuntu

If the target server provides remote management capabilities (such as a Kontron CGxxxx or a Dell Rxxx), the installation process can be carried

out remotely, including mounting the operating system ISO image as a boot device.

Otherwise, you need to have physical access to the host server, connected to a keyboard and monitor. Insert the bootable USB drive with the ISO image in one of the host's USB ports to start the installation process.

- ① Before starting the installation process, make sure that there is no data on the host that needs to be preserved. Installing the operating system on a host will erase all existing data stored on the host and this operation is irreversible.

## 2 BIOS and iDRAC Settings

---

### 2.1 Configuring BIOS Settings

The intent of configuring the BIOS settings is for the following:

- The server will boot unattended and headless
- The server will power up automatically after a power failure
- The server is configured for performance rather than power saving
- Default users/passwords are configured
- Default remote login network settings are configured
- Booting from Network Interface Cards is disabled

#### 2.1.1 BIOS and BMC Settings in the Kontron CG2400

The following instructions are for configuring the BIOS settings in a Kontron CG2400.

1. Power on or reboot the server.
2. At the prompt, press F2 or Delete to access the BIOS.
3. Select `Main`.
4. Update `System Date and System Time`.
5. Select `Setup Menu`
6. Select `Server Management > Power Control Policy`
  - Select `Power Restore`
7. Select `Server Management > BMC Network Configuration > Configuration Address source`
  - Select `Static`
8. Fill in the `Station IP address1`, `Subnet mask` and `Router IP address` for the BMC.

Example:

Station IP address: 172.29.0.121

Subnet mask: 255.255.0.0

Router IP address: 172.29.0.254

- 
1. The Station IP is under the `Lan Channel 1` heading (marked as `MGMT` on the Ethernet ports at the rear of the server).



9. If the server is to be used with a P25 Site controller or RFSS, or has an E1/T1 card installed, you must disable secure boot. To do this, select `Security > Secure Boot`
  - Select `Disabled`
10. Press F4 to save and exit.
  - Press `y` to save changes.
11. The server will now reboot.

## 2.1.2 BIOS and BMC Settings in the Kontron CG2300

The following instructions are for configuring the BIOS settings in a Kontron CG2300.

1. Power on or reboot the server.
2. Wait for the RAID BIOS screen to finish initializing the drives and get ready to press F2 for the next step.
3. There will be a couple of quick screens with other text, then when the `Intel Server Board color graphics` screen appears, press F2 quickly. There is only a short time period of approximately 2 seconds for pressing the F2 key.
4. Select `Setup Menu`
  - a. Select `Main`
    - Select `Post Error Pause`
    - Select `Disabled`
    - Press `Escape` to return to `Setup Menu`
  - b. Select `Advanced`
    - Select `Power & Performance`
    - Select `CPU Power & Performance Policy`
    - Select `Performance`
    - Press `Escape` to return to `Advanced menu`
      - Select `System Acoustic Performance Configuration`
    - Select `Fan Profile`
    - Select `Performance`
    - Press `Escape` to return to `Advanced menu`
    - Press `Escape` to return to `Setup Menu`
  - c. Select `Server Management`
    - Select `Resume on AC Power Loss`
    - Select `Power On`
      - Scroll down the page to select `BMC LAN Configuration`
    - Configure the `Dedicated Management LAN Configuration` for

the remote server management

Example:

IP

address: 172.29.0.121

Subnet: 255.255.0.0

Gateway: 172.29.0.254

- Select User Configuration
- Scroll down to root user and set:  
Privilege to Administrator  
User Status to Enabled  
User Password to K1w1k1w1 (or whatever is appropriate)
- Press Escape to return to BMC LAN Configuration
  - Press Escape to return to Server Management
  - Press Escape to return to Setup Menu
- d. Select Boot Maintenance Manager
  - Select Legacy Network Device Order
  - Ensure all network devices are set to Disabled
  - Select Save changes and exit this sub-menu
    - Press Escape to return to Setup Menu
- e. Press F10 to save the configuration.
  - Press y to save and exit

5. The server will now reboot.

#### Changing to UEFI Boot Mode (Optional)



Requires TaitCentOS v7.07.06 or later, or Tait Ubuntu.

The following instructions are for changing the boot mode from Legacy to UEFI. When the boot mode is Legacy, the BIOS only loads the modules required for booting Legacy Operating Systems. When the boot mode is UEFI, the BIOS only loads the modules required for booting UEFI-aware Operating Systems.

1. Power on or reboot the server.
2. Wait for the RAID BIOS screen to finish initializing the drives and get ready to press F2 for the next step.
3. There will be a couple of quick screens with other text, then when the Intel Server Board color graphics screen appears, press F2 quickly. There is only a short time period of approximately 2 seconds for pressing the F2 key.
4. Select Setup Menu
5. Select Boot Maintenance Manager
6. Select Advanced Boot Options

7. Navigate to `Boot Mode` and press `Enter`. Select `UEFI`



8. Press `F10` to save and exit.
9. Install TaitCentOS v7.07.06 or later via USB drive (see [Section 3.2 USB Installation on a Kontron Server CG2300/CG2400](#)).

### 2.1.3 BIOS and iDRAC Settings in the Dell R250

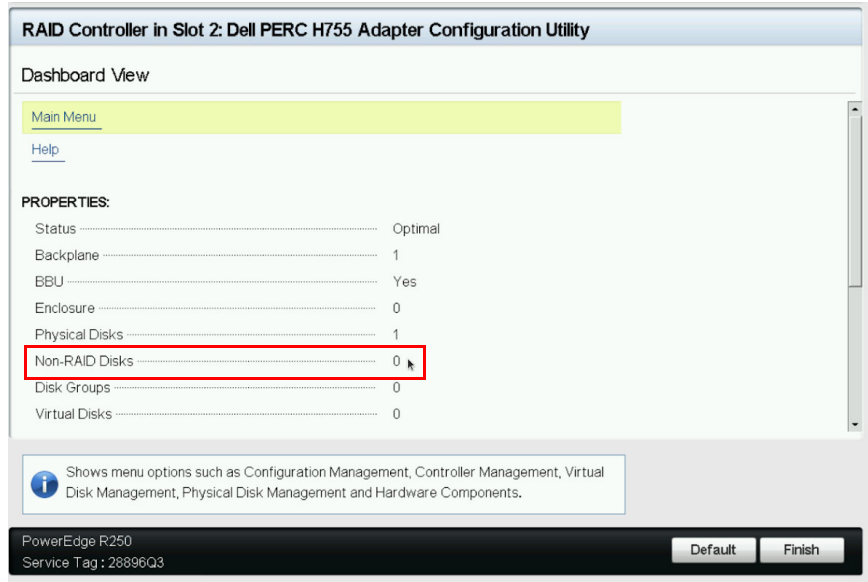
The following instructions are for configuring the BIOS and iDRAC settings in a Dell R250.

A keyboard and mouse or an iDRAC connection to the server is required.

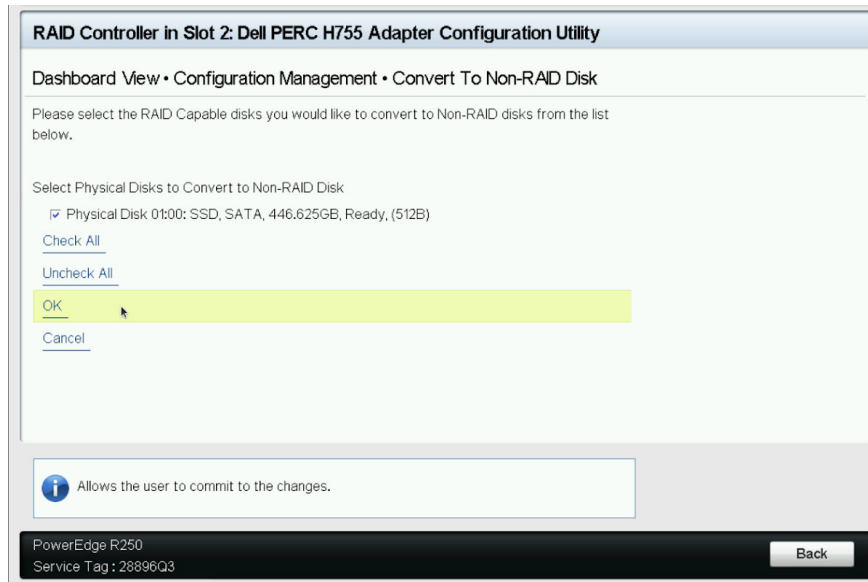
1. Power on the server and wait for 4 options to appear in the top left of the screen. Press `F2` to enter System Setup.
2. Wait for the System Setup Main Menu to appear.
3. From the System Setup Main Menu, select `Device Settings`:

- a. Select RAID Controller in Slot2: Dell PERC H755 Adapter Configuration Utility.

Check that the Non-RAID Disks counter is 1. If it is 1, proceed to Step 4, otherwise continue to b, below.

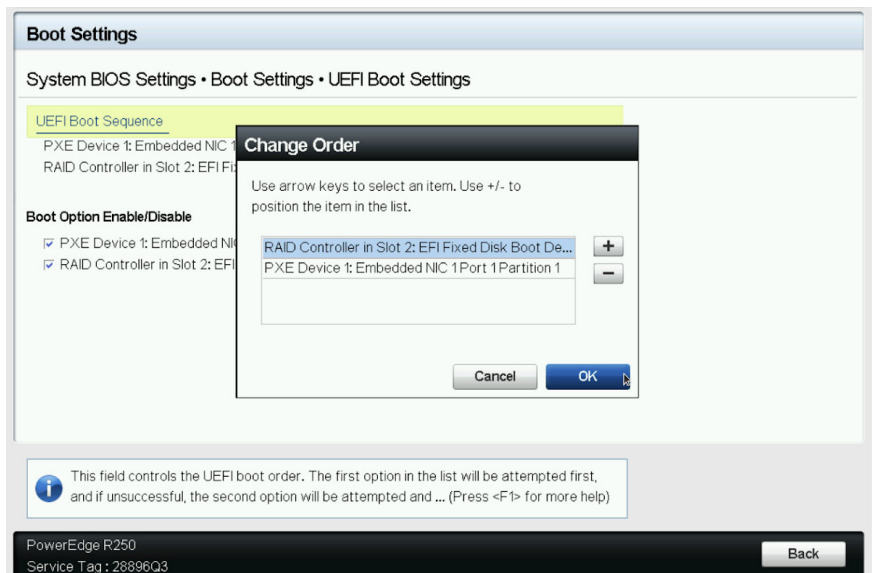


- b. If the Non-RAID Disks counter is not 1, scroll down the page until the ACTIONS section is visible and select Configure.
- c. Select Convert to Non-RAID Disk.  
Select the check box for the Physical Disk and then click OK to convert it to a Non-RAID disk.



- d. Select the check box for Confirm and click Yes.
- e. Click OK to complete disk conversion.

- f. Click Back to exit the RAID Controller settings.
  - g. Click Finish to exit the RAID card settings.
  - h. Click Finish to exit Device Settings.
4. Click Finish to exit System Setup.
  5. Click Yes to confirm that you want to exit and reboot.
  6. Wait for the system to reboot and for 4 options to appear in the top left of the screen. Press F2 to enter System Setup.
  7. Wait for the System Setup Main Menu to appear.
  8. Select System BIOS.
  9. From the System BIOS Settings menu select Memory Settings:
    - a. Change System Memory Testing to Enabled.
    - b. Click Back.
  10. From the System BIOS Settings menu select Boot Settings:
    - a. Select UEFI Boot Settings.
    - b. Select UEFI Boot Sequence.
    - c. If RAID Controller in Slot 2: xxxxxx is in the list, use the +/- buttons to move it to the top of the list. Click OK to confirm this change. If it is not in the list, contact Tait Technical Support.



- d. Click Back to return to Boot Settings.
  - e. Click Back to return to the System BIOS Settings menu.
11. From the System BIOS Settings menu select System Security:
    - a. Scroll down to AC Power Recovery and set to On.
    - b. Scroll down to the SECURE BOOT section and set Secure Boot

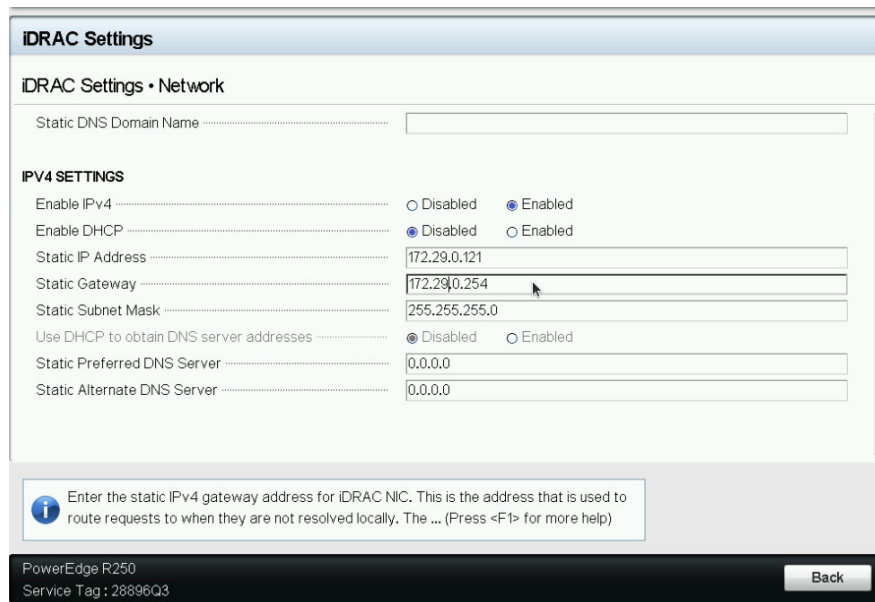
- to Disabled.
  - c. Click the Back button to exit System Security.
12. From the System BIOS Settings menu scroll down the page and select Miscellaneous Settings:
    - a. Ensure F1/F2 Prompt On Error is Disabled.
    - b. Click Back.
  13. Click Finish to exit System BIOS Settings and return to the System Setup Main Menu.
  14. When the Save Changes dialog box appears, click Yes.
  15. Click OK to return to the System Setup Main Menu.
  16. From the System Setup Main Menu, select iDRAC Settings.
  17. From the iDRAC Settings menu select Network:
    - a. Under NETWORK SETTINGS, set Enable NIC to Enabled.



- b. Set NIC Selection to Dedicated.
- c. Scroll down to IPV4 SETTINGS and set up the appropriate network settings for remote access.

**Example:**

Enable IPV4: Enabled  
 Enable DHCP: Disabled  
 Static IP Address: 172.29.0.121  
 Static Gateway: 172.29.0.254  
 Static Subnet Mask: 255.255.255.0



- d. Click Back to return to iDRAC Settings.
18. From the iDRAC Settings menu select Alerts:
  - a. Set up alert options as required.
  - b. Set SNMP community string to `tait_dmr` or `tait_p25` as required.
  - c. Click Back to return to the iDRAC Settings menu.
19. Scroll down the iDRAC Settings menu to select User Configuration:
  - a. Set as follows:
    - Enabled User: Enabled
    - User Name: admin
    - LAN User Privilege: Administrator
    - Serial Port User Privilege: Administrator
    - Change Password: Klw1klw1 (or whatever is appropriate)

**iDRAC Settings**

iDRAC Settings • User Configuration

User ID ..... 2

Enable User .....  Disabled  Enabled

User Name ..... admin

LAN User Privilege ..... Administrator

Serial Port User Privilege ..... Administrator

Change Password ..... Press <Enter> to input

PowerEdge R250  
Service Tag : 28896Q3

Back

- b. Click Back to return to iDRAC Settings.
20. Click Finish to exit iDRAC Settings and return to the System Setup Main Menu.
  21. When the Save Changes dialog box appears, click Yes.
  22. Click OK to return to the System Setup Main Menu.
  23. Click Finish to exit System Setup.
  24. Click Yes to confirm that you want to exit and reboot.

#### 2.1.4 BIOS Settings in the Sintrones SBOX-2620 or SBOX-2621

The following instructions are for configuring the BIOS settings in a Sintrones SBOX-2620 or SBOX-2621.

1. Power on or reboot the Sintrones server.
2. When the logo appears, or after the beep, press Delete to enter the BIOS.
3. Power settings:
  - a. Using the arrow keys for navigation, select Chipset > Pch\_IO\_Configuration > Restore AC Power Loss, and change the setting to Power On, using the plus (+) and minus (-) keys.
  - b. Press ESC to return to the main menu.
4. Passwords:
  - a. Select Security > Administrator Password.
  - b. Enter **K1w1k1w1** (or whatever is appropriate).



- c. Do not enter a User password since it will then be required on every boot. The Administrator password is only required when entering the BIOS setup.
5. Press F4 to Save & Exit. The server should now reboot.

# 3 USB Installation

---

## 3.1 USB Installation on a Sintrones Server

- ① Ensure that the USB port you use is USB 3.0 compliant.
  1. When there is nothing installed, the server will find and boot from a USB flash drive containing the operating system.
  2. If an operating system has been installed, to boot from a USB flash drive you need to change the boot order.
    - a. Insert the USB flash drive.
    - b. Power on/reboot the server and press F7 until the boot device menu appears.
    - c. Use the arrow keys to select the USB flash drive and press Enter to boot from it.
  3. Now proceed to [Section 5 Installing TaitCentOS](#) or [Section 6 Installing Tait Ubuntu](#).

## 3.2 USB Installation on a Kontron Server CG2300/CG2400

1. Insert the USB flash drive containing the operating system and power on/reboot the server.
2. If the 'USB Boot Priority' has been Enabled in the BIOS, the server will automatically boot from the USB flash drive.
3. Otherwise:
  - a. After the RAID BIOS screen has finished initializing the drives, there will be a couple of quick screens with other text. When the Intel Server Board color graphics screen appears, press F6 to enter the Boot Manager.
  - b. Use the arrow keys to select the USB flash drive and press Enter to boot from it.
4. Now proceed to [Section 5 Installing TaitCentOS](#) or [Section 6 Installing Tait Ubuntu](#).

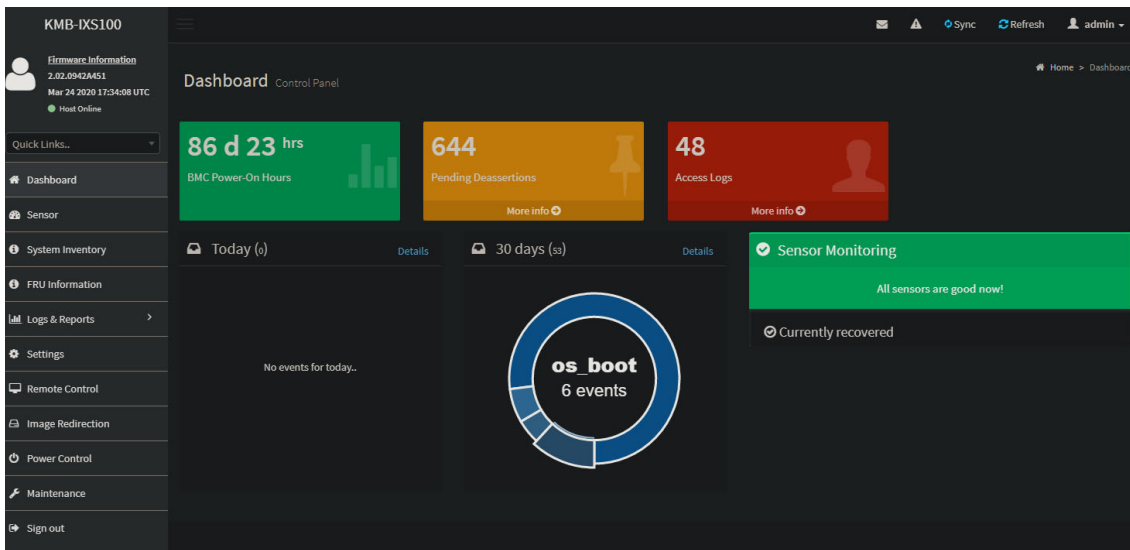
### 3.3 USB Installation on a Dell Server

- ① Ensure that the USB port you use is USB 3.0 compliant.
  1. Insert the USB flash drive containing the operating system.
- ① For version 6.90.05 and later of TaitCentOS installations, there are two options for installing from USB: standard and alternate. If, having selected standard, you get an error indicating that the installer cannot read the kickstarter file, retry using the alternate option.
  2. To boot from the USB flash drive, perform the following:
    - a. Power on/reboot the server and wait for 4 options to appear in the top left of the screen. Select `Boot Manager`.
    - b. Wait for the Boot Manager user interface to appear, then Select `One-shot BIOS Boot Menu`.
    - c. Select the USB flash drive. The server will then reboot.
  3. Now proceed to [Section 5 Installing TaitCentOS](#) or [Section 6 Installing Tait Ubuntu](#).

# 4 Remote Installation

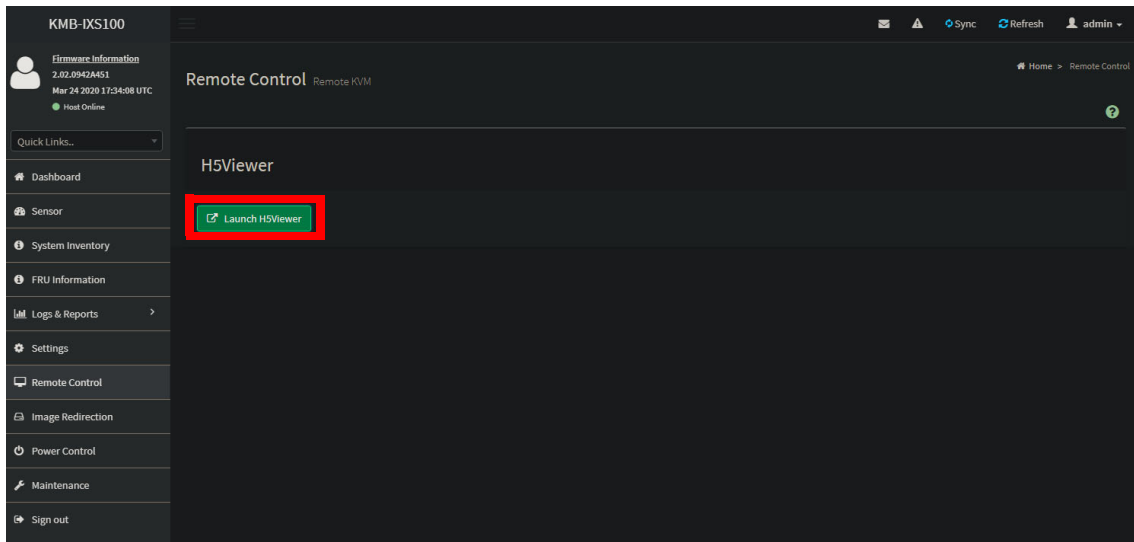
## 4.1 Remote installation on a Kontron Server CG2400

1. Connect to the BMC web console (`https://<IP address>`), and log in as an administrator. The default password is `admin`.
2. A warning is raised about the security of your connection. For instructions on connecting to an insecure site with a self signed certificate, refer to [Section 10.6 Self-Signed SSL Certificates](#).
3. The BMC dashboard is displayed.

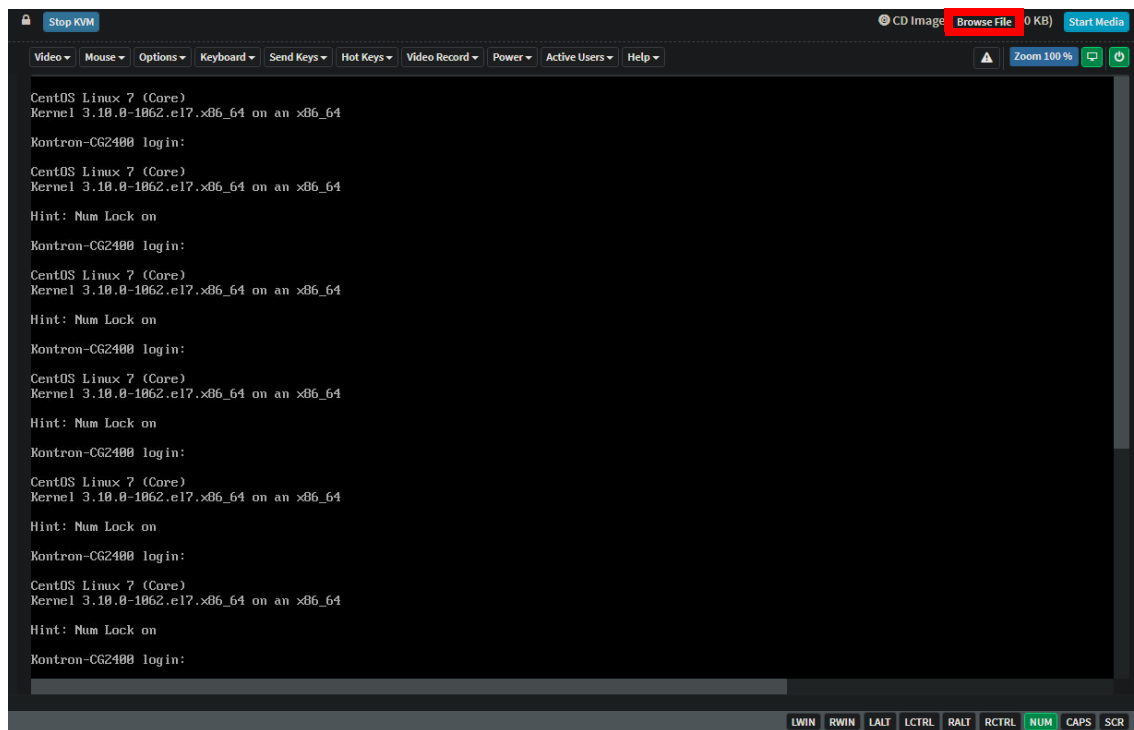


4. It is recommended that you change the default password:
  - a. Click on **Settings** in the navigation panel (on the left) and select **User Management**.
  - b. Select the **admin** user (it should be the second one in the list).
  - c. On the configuration page, tick the **Change Password** box and enter the new password in the **Password** and **Confirm Password** fields.
  - d. Scroll to the bottom and click **Save**.

5. Select Remote Control from the navigation panel.

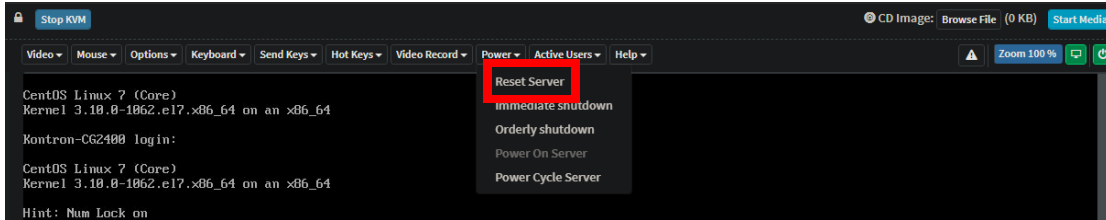


6. Click Launch H5Viewer
7. A new window should appear.

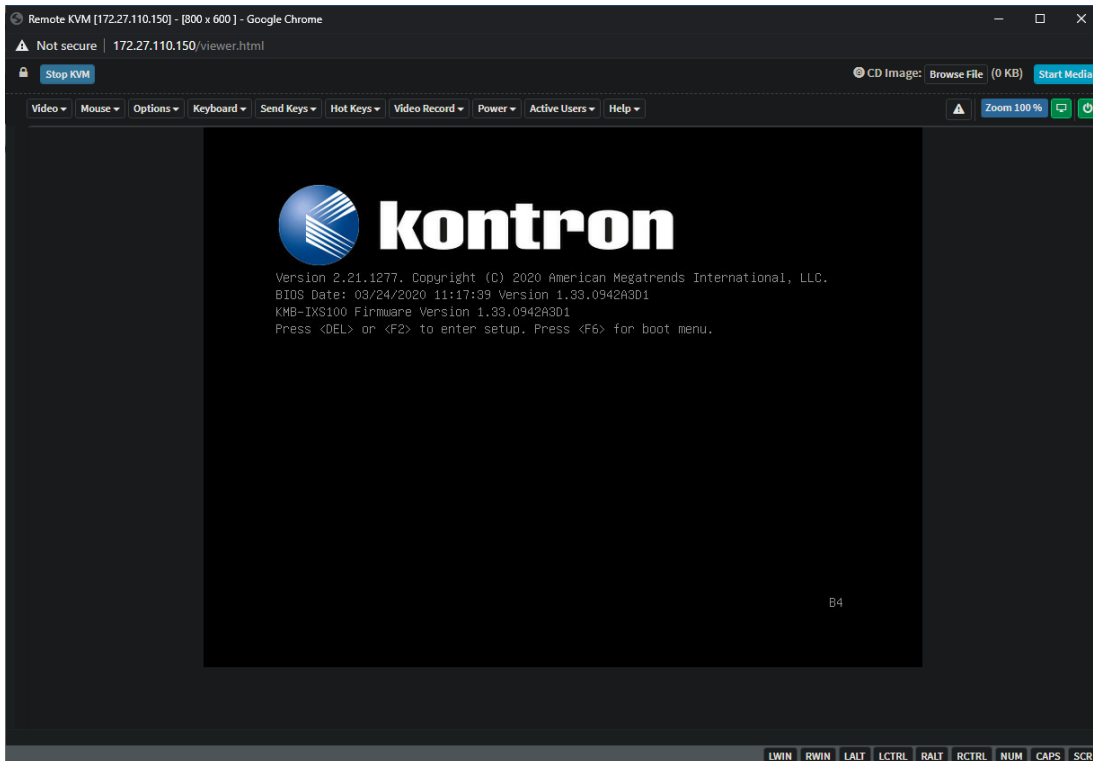


8. Click Browse File at the top right of the screen.
9. Upload the iso image containing the operating system.
10. Once the iso is loaded, click Start Media near the top right of the window.

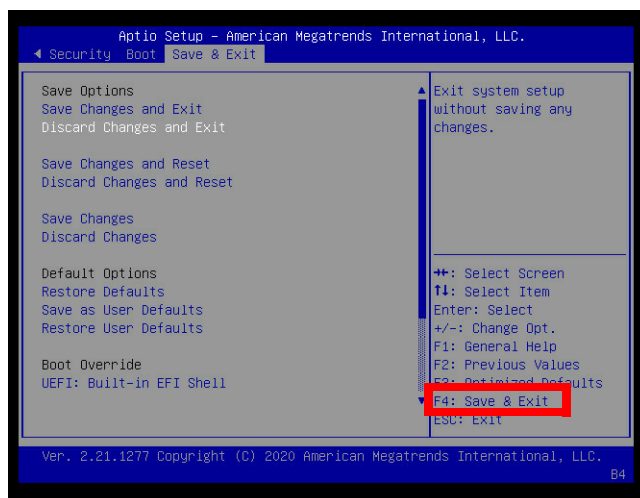
11. Click the Power drop down menu, and select Reset Server.



12. Click OK to confirm the reset. The BIOS screen should appear after a few seconds.



13. Press F2 to enter Setup. It may take a few seconds.



14. Use the arrow keys on the keyboard to navigate the BIOS menu. Move across to the right most menu option `Save & Exit` and press `Enter`. Use the arrow keys to navigate down to the `Boot Override` section and select `UEFI: AMI Virtual CDROM0 1.00` by pressing `Enter`. This will cause the server to reboot and begin installation of the OS.
15. Now proceed to [Section 5 Installing TaitCentOS](#) or [Section 6 Installing Tait Ubuntu](#).

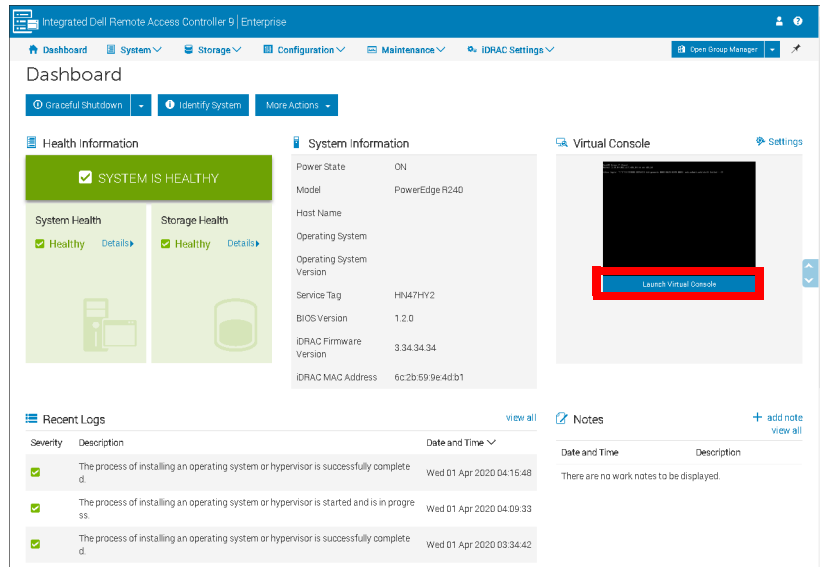
## 4.2 Remote Installation on a Dell Server



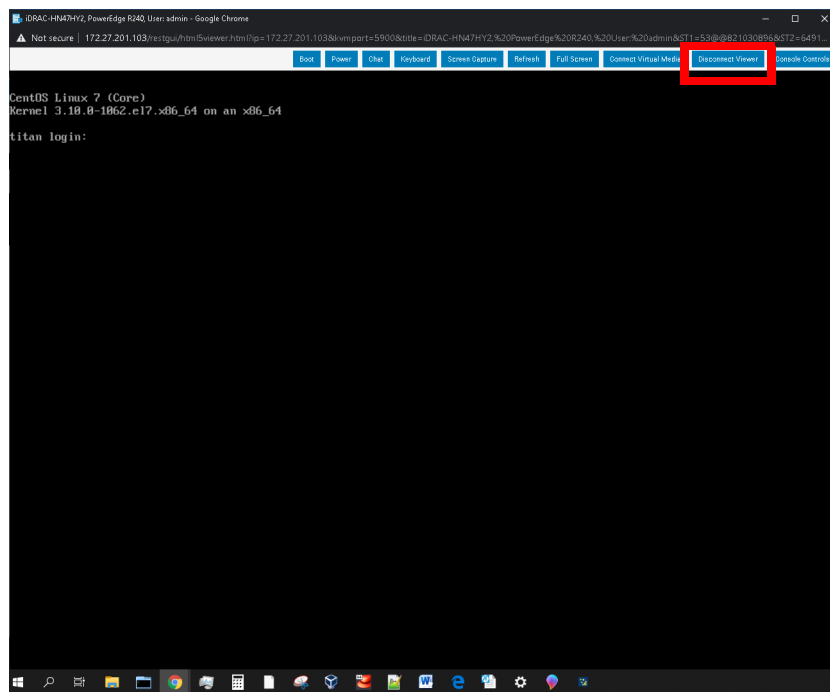
**It is recommended that the iDRAC firmware is upgraded to at least version 2.60.60.60 to launch the Virtual Console.**

1. Navigate to the web page of the iDRAC (`https:<ip address>`) and log in with an administrator level username and password.

2. Click Launch Virtual Console.



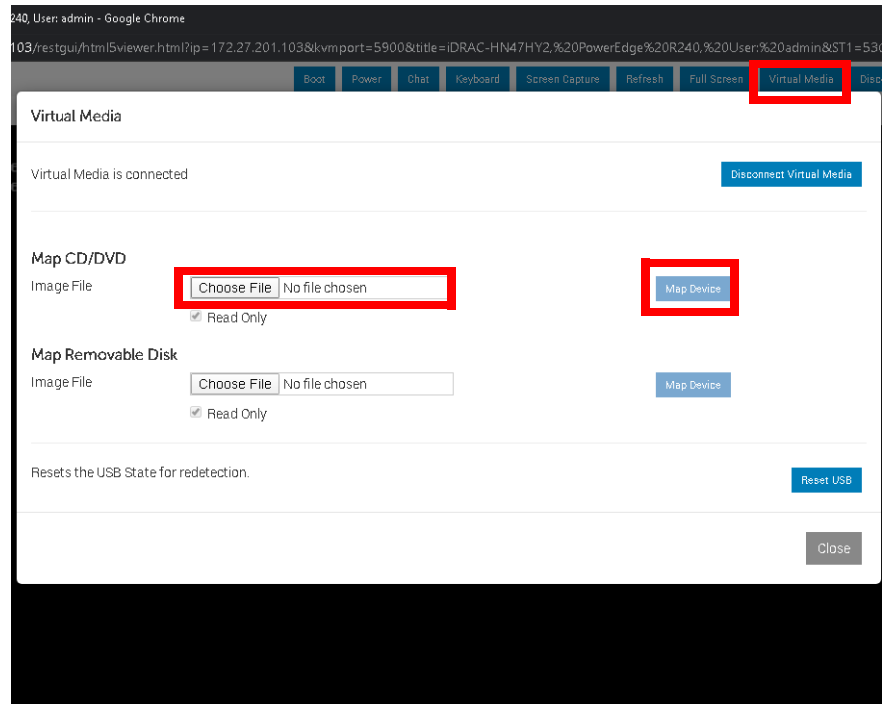
3. The iDRAC virtual console should appear.



4. From the iDRAC virtual console, map the operating system 7 iso image. To do this, select the Virtual Media tab, then click Choose



File under Map CD/DVD. Select the iso file required and click Map Device (blue button).



5. Select the Boot tab and select Virtual CD/DVD/ISO.
6. Select Yes to confirm boot action.



7. Select the Power tab and select Power Cycle System (Cold boot).
8. The system will boot from the virtual image you have mapped.
9. In the terminal window install the operating system. See [Section 5 Installing TaitCentOS](#) or [Section 6 Installing Tait Ubuntu](#).

- When the installation is complete, you will need to un-map the added device. To do this, select the Virtual Media tab and click Un-Map Device.



- Select the Power tab and select Power Cycle. The server will now boot using the newly installed operating system.

# 5 Installing TaitCentOS

---

## 5.1 TaitCentOS Installation Process

**TaitCentOS 7** If you are installing TaitCentOS 7, the following screen should appear.



There is only one option, `Install TaitCentOS 7`, press `Enter` and installation will commence.

**TaitCentOS 6** If you are installing TaitCentOS 6, there will be several options. Select the correct option for your server type, using the `Tab` key, and press `Enter`.

**TaitCentOS 7 and TaitCentOS 6** The install is automatic, and when it has finished the command prompt will be displayed. (A progress bar is displayed during the installation process.)

During the automatic install, the following default settings are applied:

- The firewall is set to disabled
- The root user password is set to `K1w1k1w1`
- The default network settings are set to
  - IP: `172.29.0.101`
  - Netmask: `255.255.0.0`
  - Gateway: `172.29.0.254`
- Time zone and clock are set to UTC

When the installation is complete, click `Reboot`. When the device restarts, remove the USB flash drive quickly, before the boot sequence starts.

**Notice** Should there be any installation failure, for example a power cut occurring during the procedure, then TaitCentOS will need to be reinstalled.

## 5.2 Upgrading TaitCentOS

- ① This section is only for upgrading TaitCentOS versions within the same major release, i.e. from version 7.08 to 7.09. To migrate from TaitCentOS 6 to TaitCentOS 7 requires a complete reinstallation, refer to [Section 5.4 Migrating from TaitCentOS 6 to TaitCentOS 7](#).

Periodically the server's operating system will need to be upgraded, which is done by uploading, then installing, the TaitCentOS upgrade package file.

- ① It is recommended that a configuration backup be made before performing the following upload/upgrade procedures. Refer to [Section 11.2.2 Backups](#).

### 5.2.1 Uploading a TaitCentOS Upgrade Package

1. Save the received upgrade packages to your PC.
2. Log in to the Administration application. You will need to have Administrator or Network Administrator access level.
3. Select Files > Firmware.
4. Click Upload.
5. On the Upload firmware pop up click Choose File.
6. Navigate to the folder on your PC where the TaitCentOS upgrade package file is located.
7. Select the file and then click Open.
8. A progress bar indicates how the upload is progressing.

### 5.2.2 Installing the TaitCentOS Upgrade Package

1. Put the server offline (refer to the relevant System Manual for details).
- ① The server will not go into offline mode until all current calls have been cleared down.
2. In the Administration application, select Files > Firmware.
  3. Select the correct TaitCentOS upgrade package file from the list of uploaded firmware files.

4. Click Install. The upgrade can take up to 20 minutes.  
(To confirm the installation is progressing, select Files > Logs and check that the counter on the latest upgrade log file is increasing.)
5. The server will automatically restart if the upgrade is successful. If the upgrade fails, it will report an error message and revert to the previous software version.
6. Put the server back online (refer to the relevant System Manual for details).

**Notice** Should there be any upgrade failure, for example a power cut occurring during the procedure, the TaitCentOS upgrade package will need to be re-installed.

## 5.3 Changing the Default IP Address Using the Network Configuration Tool

### 5.3.1 Changing the Network Settings on TaitCentOS 6

To change the network settings on systems running the TaitCentOS 6 operating system, refer to earlier issues of this manual (MNB-00012-11 and earlier).

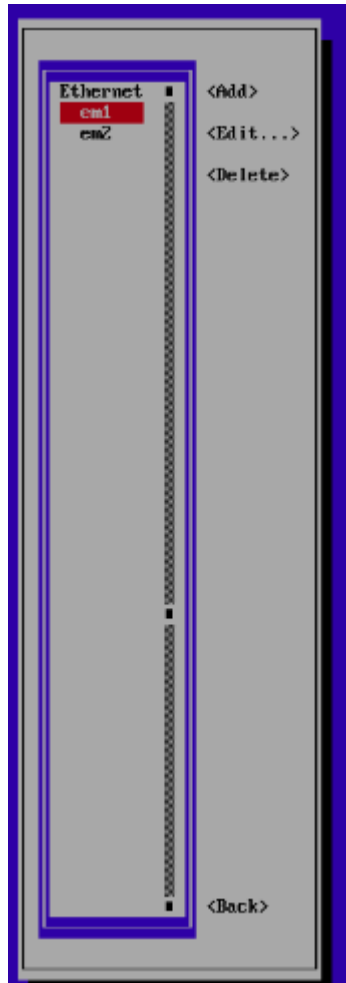
### 5.3.2 Changing the Network Settings on TaitCentOS 7

1. From the keyboard attached to the server, login in as the root user.
2. Enter `nmtui`. The NetworkManager TUI screen will appear.

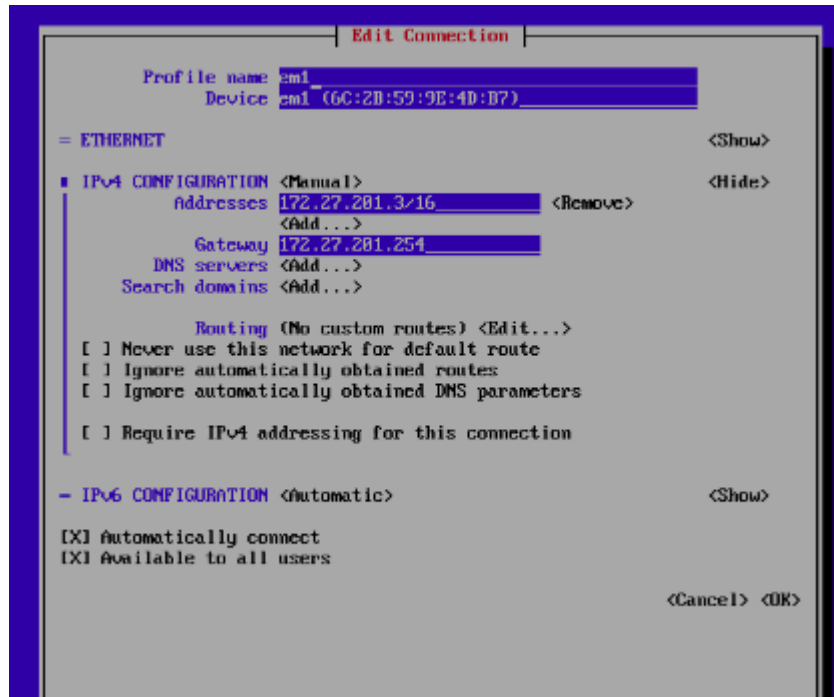


3. Select `Edit a connection`.

4. Select your device. Then select `Edit`.



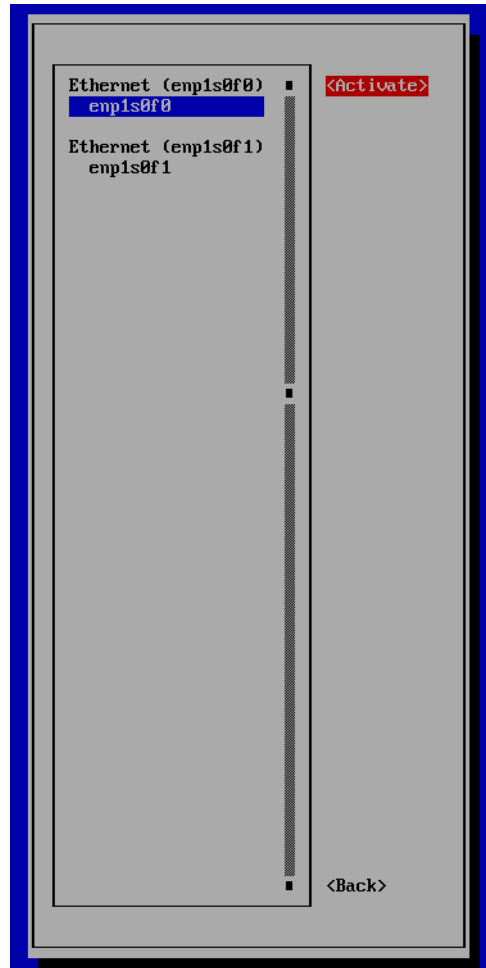
- The selected connection should appear.



- Update the Addresses and Gateway fields with the Static IP address and default Gateway IP information obtained from [Section 1.2.2 Information Required](#). Use the Tab key or Up arrow and Down arrow keys to navigate from field to field. When your settings have been updated, select OK.
- This will return to the page displayed in [Step 4](#).
- Select Back. This will return to the NetworkManager TUI.



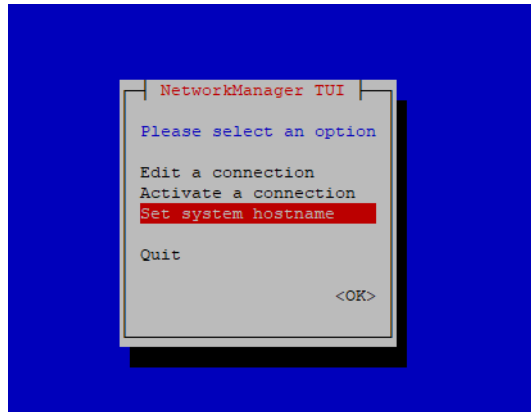
9. Select `Activate` a Connection, to display the following page.



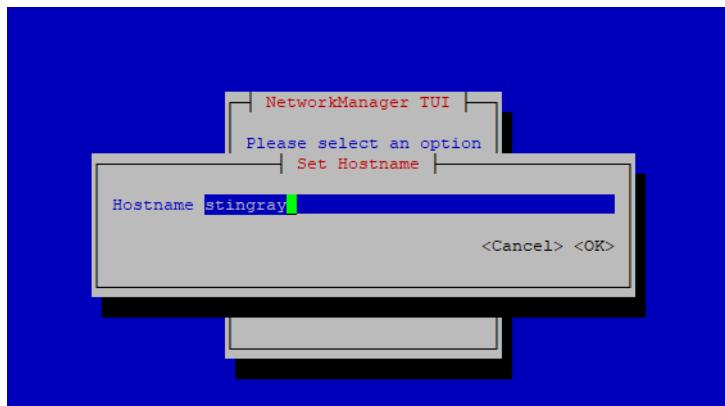
10. Select the edited connection, and select `Activate`. Then select `Back` to return to the previous page.
11. Set the hostname (this is required to be done now in case any applications require the system hostname for successful operation):



- a. Select `Set system hostname` from the NetworkManager TUI.



- b. Enter the hostname as required and select `OK` to return to the previous page.



**Notice** The system hostname can also be updated from the Administration Application WebUI, under Configuration > Network.

12. Select `Quit`. This will close the network configuration tool.
13. Enter `reboot` to restart the server with the new network configuration settings.

## 5.4 Migrating from TaitCentOS 6 to TaitCentOS 7

To migrate a server<sup>1</sup> from TaitCentOS 6 to TaitCentOS 7, refer to earlier issues of this manual (MNB-00012-11 and earlier).

## 5.5 Migrating from Solaris to TaitCentOS

To migrate existing DMR or MPT-IP controllers<sup>2</sup> from a server running the Solaris operating system to a server running TaitCentOS, refer to earlier issues of this manual (MNB-00012-11 and earlier).

- 
1. For TN9400 servers, refer to TN-3174 for detailed migration instructions.
  2. This applies to both version 3 and version 2 software for MPT-IP, DMR trunked and DMR conventional networks.

## 6 Installing Tait Ubuntu

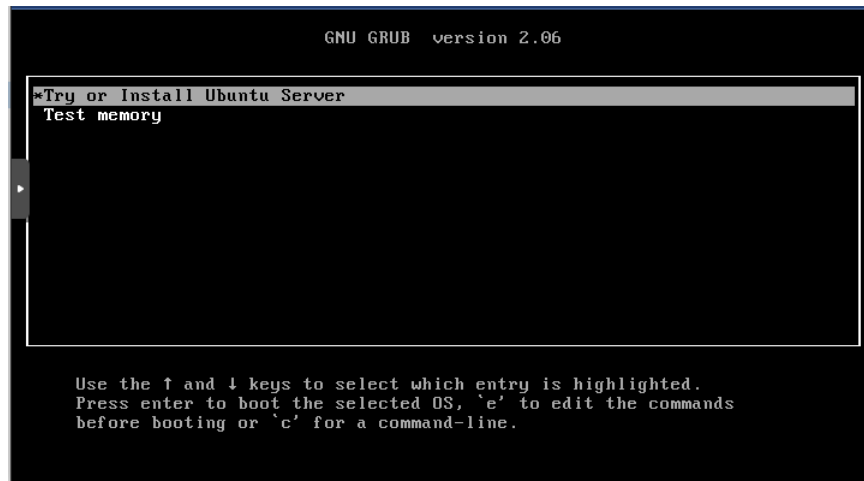
---

### 6.1 Automated Operating System Installation

When the host boots successfully, via the external USB drive or the remotely mounted ISO image, the following screen is displayed on the host's monitor or virtual console:



If you configured the host use the Legacy BIOS boot, the following is displayed:



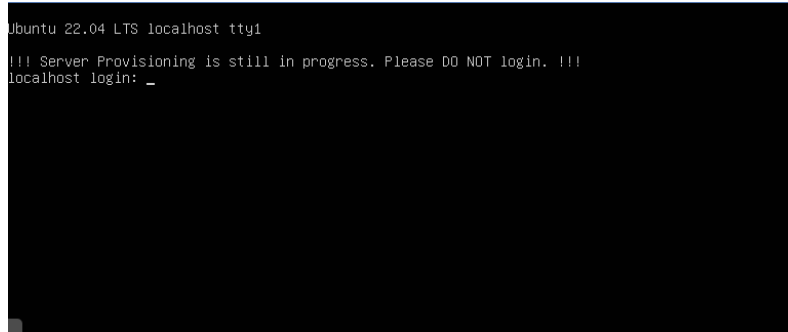
In both cases, you can select `Try or Install Ubuntu Server` to start the installation process manually, but the installation process will start automatically after a 30 second count down. The installation process is fully automated and requires no user input once it is started.

The host will automatically reboot itself once the installation is completed. Make sure you have removed the USB flash drive before the reboot sequence starts.

## 6.2 Automated Tait Customizations

The host will automatically apply Tait's customizations on its first boot after the OS installation.

**Do not** log on to the host at this point, as displayed by the following warning message:



```
ubuntu 22.04 LTS localhost tty1
!!! Server Provisioning is still in progress. Please DO NOT login. !!!
localhost login: _
```

The customization process is fully automated and requires no user input. You can safely ignore any messages displayed on the screen or the virtual consoles.

Once all the customizations have been applied, the host will automatically reboot itself again.

## 6.3 Network Configuration

The host is fully provisioned after the second reboot. It is now accessible on the network via its default IP address, which is 172.29.0.101. If you need to change the host's IP address manually, log on to the host by using the default username (`taignet`) and password (`taigt`).

The Tait Ubuntu server 22.04 uses Netplan to manage its network configuration, which is saved in a YAML file on the file system. The Tait customizations also need to be updated whenever a network configuration is changed. To make the network configuration process more user friendly and less error prone, Tait's customizations include a shell script to simplify this process.

To change the host's network configuration:


1. Log on to the host's console as the default user and run the following command as the root user via sudo:
 

```
tait_configure_network
```
2. This shell script requires three mandatory arguments:
  - `-i` (the interface name)<sup>1</sup>
  - `-a` (the IP address assigned to the specified interface in the CIDR format)
  - `-g` (the IP address of the gateway)
  - `-n` (the IP address of a name server - this is optional)

**Example**

The following example will assign IP address 172.29.0.200 in the 255.255.255.0 subnet to a network interface eth0 and configure it to use 172.29.0.1 and 172.29.0.254 as its gateway and nameserver respectively:

```
taitnet@localhost:~$ sudo tait_configure_network.sh -i
eth0 -a 172.29.0.200/24 -g 172.29.0.1 -n 172.29.0.254
```

 Remember to reboot the server after making network changes by entering `sudo reboot`

### 6.3.1 Configuring Ethernet Bonding

Instead of applying an IP address to a single network card you can bond two cards together and apply the IP address to the bond. This allows you to utilise both network cards to increase bandwidth and/or have a secondary network card take over if the primary fails.

**Procedure**

1. Log on to the host's console as the default user and run the following command as the root user via sudo:
 

```
tait_configure_network_bond.sh
```
2. The shell script requires four mandatory arguments:
  - either `--lacp` or `--active-backup` (this is the bonding mode)
  - `-i` (the two interfaces you wish to bond - they should be separated by a comma)
  - `-a` (the IP address assigned to the bond in the CIDR format)
  - `-g` (the IP address of the gateway)
  - `-n` (the IP address of a name server -this is optional)


**Example**

The following example will bond interfaces eth0 and eth1 using the active backup mode. It will also assign IP address 192.168.1.1 in the 255.255.255.0 subnet to the bond. It will also configure it to use 192.168.1.254 and 192.168.1.75 as its gateway and nameserver respectively.

---

1. To find an interface name, use the `ip addr` command, which will list all interfaces.

```
sudo tait_configure_network_bond.sh --active-backup -i
eth0,eth1 - a 192.168.1.1/24 -g 192.168.1.254 -n
192.168.1.75
```

 Remember to reboot the server after making network changes by entering **sudo reboot**


### 6.3.2 Configuring the Hostname

To configure a hostname for your server, log on to the host's console as the default user and run the following command as the root user via sudo:

```
sudo hostnamectl hostname <hostname>
```

The following example will assign the hostname angus to your server:

```
sudo hostnamectl hostname angus
```

 If you change the hostname you must stop and start any Tait services via the administration application.

## 6.4 Migrating from TaitCentOS to Tait Ubuntu

To migrate a server<sup>2</sup> from TaitCentOS to Tait Ubuntu:

1. Take a backup of the Administration application running on the server and download the backup file (refer to [Section 11.2.2 Backups](#)).
2. Log in to each application running on the server and perform manual backups for each one. Download the backup file for each application.
3. Extract the license files from each backup by unzipping each backup file.
4. Install Tait Ubuntu (refer to [Section 6.1 Automated Operating System Installation](#) for full instructions).
5. Install the required application(s) (refer to [Section 9.1 Software Installation or Upgrades](#)).
6. Restore the backup generated in Step 1 for the Administration application.
7. Restore the backup generated in Step 2 for each application.

---

2. For TN9400 servers, refer to TN-3174 for detailed migration instructions.

8. Install the license files extracted in Step 3 for each application (see [Section 10.5 Installing License Files](#)).

## 6.5 Migrating from Solaris to Tait Ubuntu

The following procedure can be used to migrate existing DMR or MPT-IP controllers<sup>3</sup> from a server running the Solaris operating system to a server running Tait Ubuntu.

1. Setup the controller application on the new server with Tait Ubuntu:
  - a. Install Tait Ubuntu (refer to [Section 6.1 Automated Operating System Installation](#) for full instructions).
  - b. Install the required application(s) (refer to [Section 9.1 Software Installation or Upgrades](#)).
2. Perform a manual backup of the Solaris controller application (select Files > Backups and click the Backup button). Download the backup file (the filename will have the prefix `manual_` as the backup was done manually).
3. Make a copy of the node resource parameters file<sup>4</sup> on the Solaris controller.
4. Make a note of the Local Parameter page settings on the Solaris controller (select Settings > Local Parameters), as these will not be restored.
5. Make a backup of the license file used on the Solaris controller.
6. Set the mode of the controller on the Solaris controller to offline.
7. Contact Tait Technical Support for the new license file to be installed on the new Tait Ubuntu platform. Use the license file which was backed up in Step 5 as a reference for the features which are to be enabled. Provide both the Host ID of the old Solaris platform and the Host ID of the new Tait Ubuntu platform.
8. Activate the controller application on the Tait Ubuntu platform with the new license generated (Settings > Local Parameters > Edit > upload license file under License section).
9. Restore the backup generated in Step 2 (Files > Backups > Upload. Upload the backup file then click the Restore button).

---

3. This applies to both version 3 and version 2 software for MPT-IP, DMR trunked and DMR conventional networks.


4. Version 3 nodes: DMR trunked is `tait_dmrnc.cfg`, DMR conventional is `tait_dmrcc.cfg`, and MPT-IP is `tait_mptipnc.cfg`.  
Version 2 nodes (all): `node.cfg`.

10. The node controller application should restart automatically. Check that the settings have been restored.
11. Configure the settings on the Settings > Local Parameters page based on the settings noted in Step 4.
12. Restore the backup node resource file from Step 3 to restore the node resource parameters which were enabled in the Solaris installation.
  - Refer to Section 7.24 of the DMR Trunked System Manual (MNB-00003-xx) or Section 6.22 of the MPT-IP System Manual (MNA-00026-xx) for more information on node resource files.
13. Set the Tait Ubuntu controller application mode to online (Local Parameters > Mode).
14. If switching controllers are configured (see Section 5.14 in MNB 0003-xx or Section 5.11 in MNA-00026-xx), the user may need to make changes to the IP addresses configured in Network > Nodes.

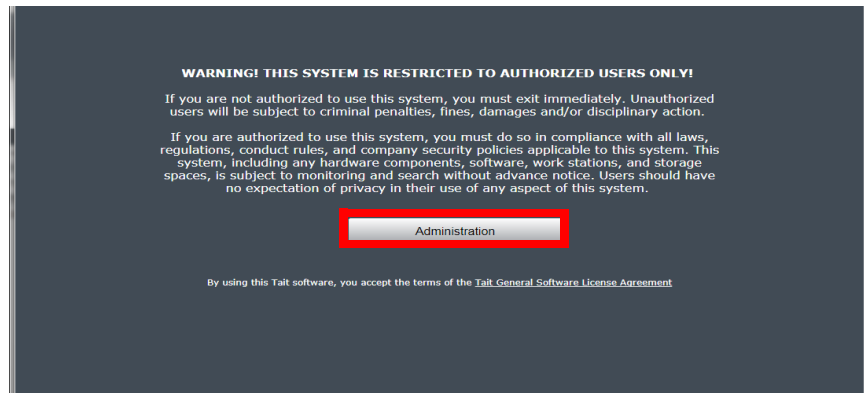


# 7 Logging On to the Administration Application

---

 Secure HTTP is used by default (https). You may need to prepend your IP address with `https://` in your browser to access the user interface.

1. Using your web browser, enter the following:  
**`https://nnn.nnn.nnn.nnn`**  
(where `nnn.nnn.nnn.nnn` is the IP address of your control node).  
Tait Ubuntu users will go directly to Step 3.
2. TaitCentOS users only:
  - a. Select the Administration application from the following screen:



3. Log in (the default username is `taitnet` and the password is `tait`).



# 8 Installing the Tait Packages Using TaitCentOS

---

This section outlines the procedure for software installation and upgrades using TaitCentOS. It can apply to the following Tait services:

- TN9400 RFSS Controller
- TN9400 Site Controller
- TN9300 Channel Controller
- TN9300 Node Controller
- T1541 Node Controller
- TN8291 Node Controller
- TN9500 Gateway
- Data API Connector
- G.711 Connector
- PTTToX Connector
- ClamAV package
- ClamAV updates

It can also apply to Operating System updates.

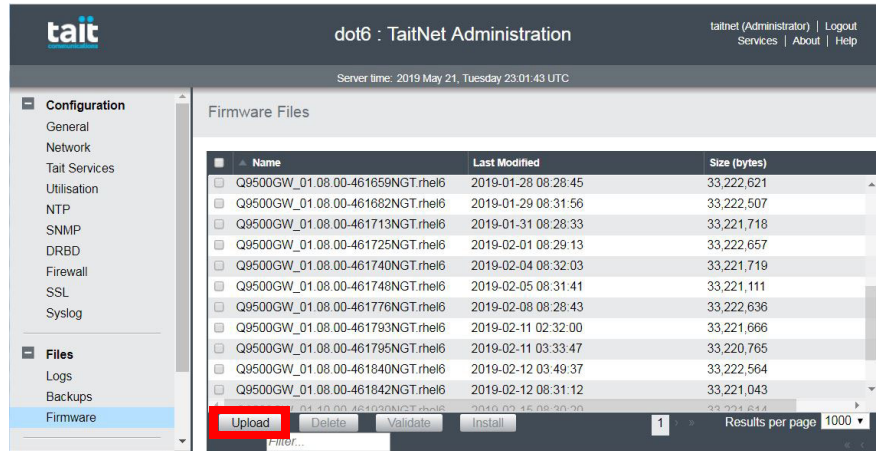
## 8.1 Software Installation or Upgrades

This is done from the TaitNet Administration application.

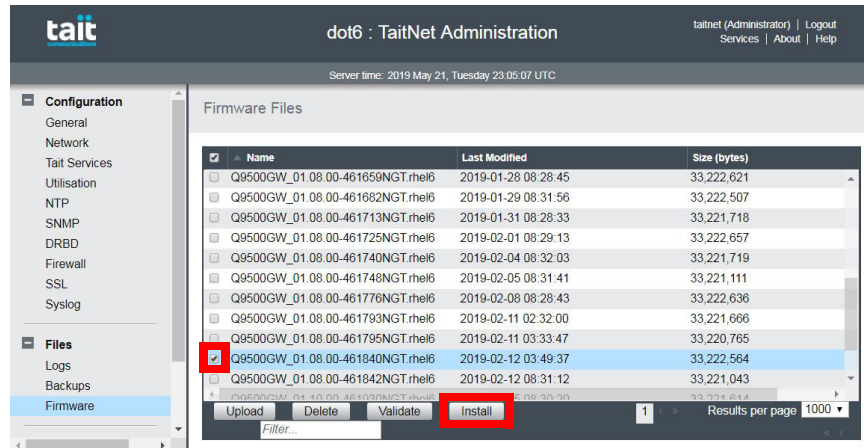
- ① For high availability gateways, always upgrade the standby gateway first.
- ① Secure HTTP is used by default (https). You may need to prepend your IP address with `https://` in your browser to access the user interface.

1. Log in to the Administration application.

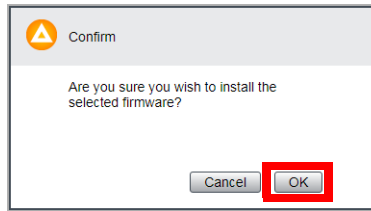
2. Select Files > Firmware from the left column menu.



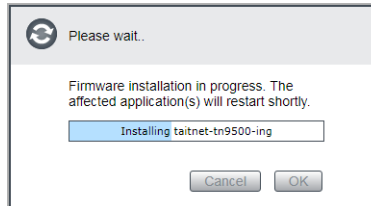
3. Click Upload, then click Choose file to select the upgrade package for installation. Navigate to the location of the firmware upgrade package and select the file. The firmware upgrade package file name will be in the format: `<application name>-<version number>-upgrade` (refer to release notes for `<application name>`).
4. Select the upgrade package by clicking the box next to the name of the upgrade package, then click Install.



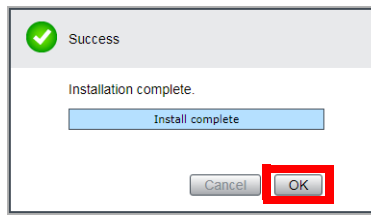
5. A confirmation box will appear. Click OK to continue.



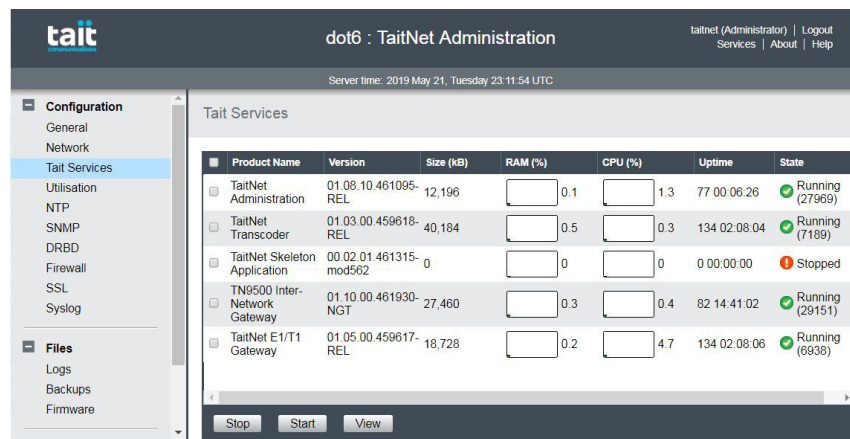
The installation may take several minutes while the software is installing. A progress bar is displayed:



6. A dialog box will appear when the installation has finished and will indicate if the installation was successful or not. Click OK to finish the installation.



7. To confirm a successful installation, select Configuration > Tait Services from the menu in the left hand column. The number of services listed depends on the application installed: typically three for the TN9500 and TN9400 RFSS controller; three for the TN9400 site controller and TN9300; and one for the TN8291. All should show a service status of Running.



8. If the upgrade fails, it will report an error message and revert to the previous software version.

## 8.2 Recovering from a Failed Firmware Upgrade

If a firmware upgrade has failed part way through (e.g. from a power cut), or fails to finish with the 'upgrade complete' message, the server may be left in a state where attempts to re-install the upgrade from the user interface will fail due to the server believing the upgrade has been completed.

The following instructions describe how to recover from a failed upgrade of the server firmware.

1. Log into the Administration application.
2. Select Files > Logs.
3. Check the `tait_upgrade` log file for one or more of the following messages (or similar):
  - There are unfinished transactions remaining. You might consider running `yum-complete-transaction` first to finish them.
  - Transaction Check Error: package `taitnet-<application name>-ing-00.01.00-426778UPD.el6.x86_64` is already installedor the log file may end before all the expected messages/steps have taken place, e.g. the end of the log file should show:
  - Updating: `taitnet-<application name>-ing-00.01.00-426808UPD.el6.x86_64 1/2`
4. To recover from this and guarantee a fully installed upgrade:
  - a. ssh into the server with root privileges
  - b. Resolve any uncompleted yum transactions by entering:  
`yum-complete-transaction`
  - c. Remove the package that the upgrade failed on (for the ING package enter):  
`yum remove taitnet-<application name>-ing.x86_64`
  - d. Reinstall the upgrade package from the user interface. As the configuration databases should still be intact, once the upgrade has been installed the configuration should automatically load back into the system.

# 9 Installing the Tait Packages Using Tait Ubuntu

---

This section outlines the procedure for software installation and upgrades using Tait Ubuntu. It applies to the following:

- Updates to the Administration application
- Operating system updates
- Anti Virus updates (pattern files and engine updates)
- Tait Services:
  - TN9300 Channel Controller
  - TN9300 Node Controller
  - TN8291 Node Controller
  - Data API Connector
  - G.711 Connector

Tait services are delivered as container ‘Images’ which are bundles that contain all the software and libraries necessary for the service to operate.

- ① If you are upgrading the Administration application, it will restart automatically.
- ① If you are upgrading the Operating System you may need to reboot the server afterwards. If a reboot is required a message will appear on the Configuration > General page.

## 9.1 Software Installation or Upgrades

This is done from the TaitNet Administration application.

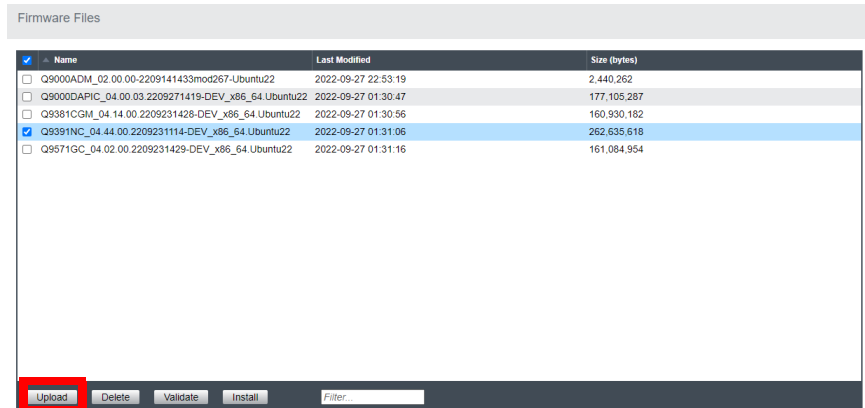
- ① Secure HTTP is used by default (https). You may need to prepend your IP address with `https://` in your browser to access the user interface.

1. Log in to the Administration application.

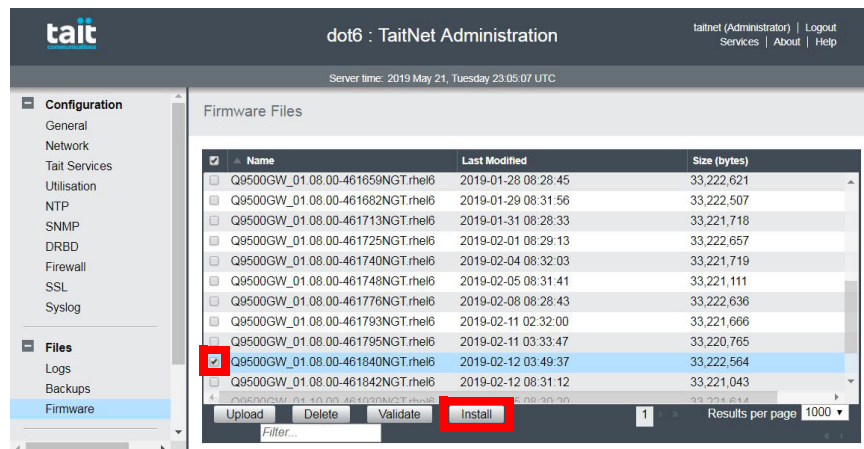
2. Log in (the default username is `taitnet` and the password is `tait`).



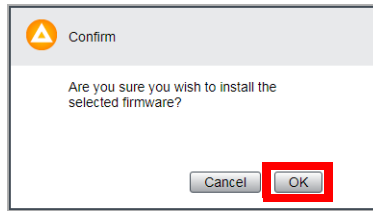
3. Select Files > Firmware from the left column menu.



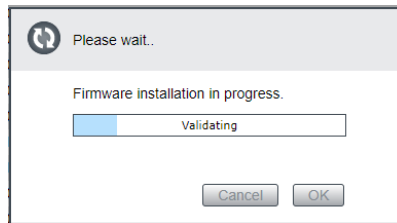
4. Click Upload, then click Choose file to select the upgrade package for installation. Navigate to the location of the firmware upgrade package and select the file. The firmware upgrade package file name will be in the format: `<application name>-<version number>-upgrade` (refer to release notes for `<application name>`).
5. Select the upgrade package by clicking the box next to the name of the upgrade package, then click Install.



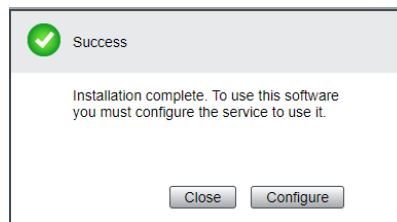
6. A confirmation box will appear. Click OK to continue.



The installation may take several minutes while the software is installing. A progress bar is displayed:

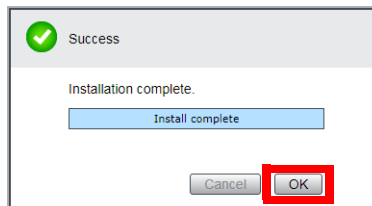


7. If you are upgrading a Tait service, go to Step 8. For all other upgrades, go to Step 9.
8. When upgrading a Tait service there is an extra step, as the installation merely copies the new container image into a repository on the server. To start using the new image you must configure the service to use it. At the end of the installation you will be prompted to do so with the following message:



If you click Configure, you will be taken to the configuration page for the service. Select the new version from the drop down list, ensure Enabled is selected and click Save.

9. A dialog box will appear when the installation has finished and will indicate if the installation was successful or not. Click OK to finish the installation.



10. If the upgrade fails, it will report an error message and revert to the previous software version.



## 9.2 Recovering from a Failed Firmware Upgrade

If a Tait service firmware upgrade has failed part way through (e.g. from a power cut), or fails to finish with the 'upgrade complete' message, just begin the upgrade again.

This also applies to Tait Ubuntu OS upgrades or Administration application upgrades, with the additional recommendation that the following events be reported to Tait Technical Support:

- If the upgrade fails but the Administration application is still working
- If the box will not boot at all or the Administration application will not start

# 10 Operations

---

This chapter explains how to carry out basic maintenance and operational tasks by logging onto the server running the administration application and using the operating system's command line interface and/or user interface.

## 10.1 Logging on using SSH

You can log in using an SSH terminal application.

1. Use an SSH terminal application to connect to the IP address of the server.
2. You should see the following prompt:  
login as:  
Enter **taitnet**
3. You will be asked for a password, the default is `tait`. Enter the password and press enter.
4. You should now be logged on to the server using the default command shell (bash).

When you are ready to logout, enter **logout** or just press Ctrl-d.

### 10.1.1 Logging into a Container Using SSH (Tait Ubuntu only)

1. On Ubuntu, Tait services operate in containers. To log into a container, you must first log onto the server as described above. Then enter the command:

```
docker ps
```

2. You will see a list of all running containers. for example:

CONTAINER ID STATUS	IMAGE PORTS	COMMAND NAMES	CREATED
54d5490a683b Up 2 minutes	taitnet-dmrnc-x86_64:04.44.00.2210201515-REL	"/init" tait_dmrnc	2 minutes ago
3bf2b51e031e Up 42 hours	traefik:v2.5.3 0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp	"/entrypoint.sh trae..." traefik_reverse-proxy_1	42 hours ago

3. Containers with names that begin with `tait_` are tait services. In the example above the container `tait_dmrnc` contains the DMR node controller. To log onto a container, enter:

```
docker exec -it <container_name> bash
```

The following container names may appear on your system:

- `tait_dmrnc` - DMR trunked node controller (tier 3)
- `tait_dmrcc` - DMR conventional channel controller (tier 2)

- `tait_dmrcg` - DMR channel group manager
  - `tait_ing` - TN9500 Inter-network gateway
  - `tait_dmrnc` - G7.11 connector
  - `tait_dapic` - Data API connector
  - `tait_mptip` - MPT-IP node controller
4. You should now be logged on to the container as the root user. You will be in the `/home/taitnet` directory. You can change into the folder containing the container software by entering:  
`cd <product_name>`  
 Where product name is the name of the container without “`tait_`”, e.g: `cd dmrnc` for the DMR node controller.
  5. When you are ready to logout, enter `logout` or just press `Ctrl-d`. This will return you to the command shell on the host server.

## 10.2 Logging on as ‘root’

### 10.2.1 TaitCentOS Users

Some tasks can only be carried out if you are logged in as root. To do this you use the UNIX `su` command.

1. Logon as user `taitnet` as described in Section 10.1 above.
2. At the prompt enter:  
`su -`
3. You will be prompted for the root password. The default is `K1w1k1w1`.
4. When you are done, press `ctrl-d` to logout. You will switch back to being the `taitnet` user.

### 10.2.2 Tait Ubuntu Users

1. Logon as user `taitnet` as described in Section 10.1 above.
2. To run a single command as root, enter:  
`sudo <cmd>`  
 You will be prompted for your password. This is not the root password, but the one you are logged in as, i.e. if you are logged in as the `taitnet` user and enter `sudo ls`, you will be asked for the `taitnet` password before the command runs.
3. To become root, enter:  
`sudo -i`

- ① Only users with sudo rights can use sudo. The taitnet user has sudo rights.

## 10.3 Logging in to a Tait Service

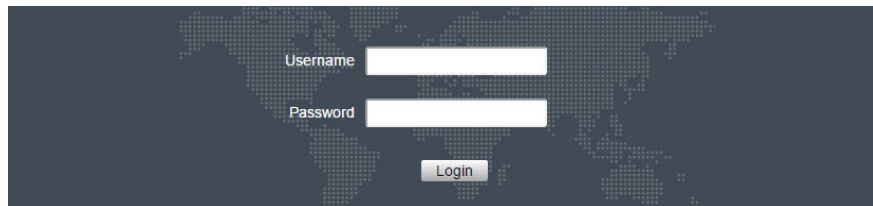
### 10.3.1 From the User Interface Home Page (TaitCentOS Only)

1. Open a PC browser and enter the IP address of the server where the Tait service application resides. From the landing page displayed, select the application you want to log in to.

- ① Secure HTTP is used by default (HTTPS). You may need to prepend your IP address with HTTPS:// in your browser to access the user interface.

- ① In case of proxy errors, for information on IP ports refer to the system or configuration manual of the product being logged on to.

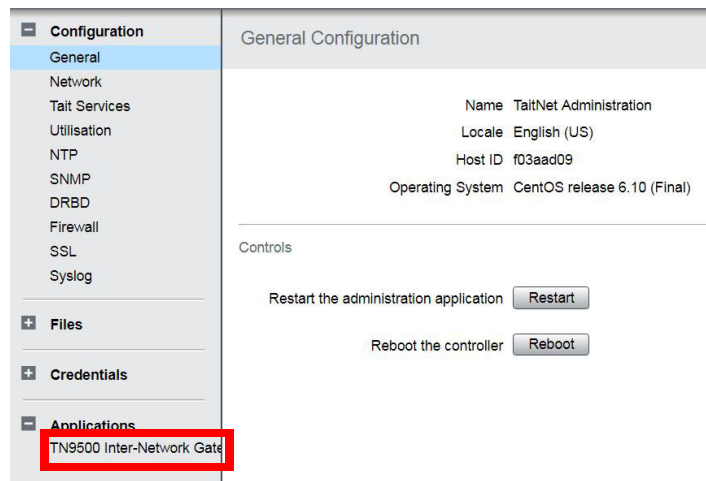
2. Log in (see Section 10.8 for the default passwords of Tait software).



A screenshot of a login interface. It features a dark background with a faint world map. There are two white input fields: the top one is labeled 'Username' and the bottom one is labeled 'Password'. Below the password field is a 'Login' button.

### 10.3.2 From the TaitNet Administration Application

1. Log in to the Administration application.
2. Select a Tait service from the Applications menu.



## 10.4 Creating Your Custom 'ssh' Login Script

### 10.4.1 TaitCentOS

It is recommended that you create a login script (in a banner file). This is the script that is displayed to the user when they log in from an external device (for example, using PuTTY).

A default banner file is included as part of the operating system installation (see "[TaitCentOS Sample login script](#)" on page 61). Use the following instructions if you want to create your own.

1. SSH into the controller with root privileges (see [Section 10.2 Logging on as 'root' for 'TaitCentOS Users'](#) on page 59).
2. Locate (or write) a file with the login script required.
3. Copy this file to the `/etc` directory, and name it `banner`:  

```
# mv <path to login script> /etc/banner
```
4. Change the ownership and group of the file to `root`:  

```
# chown root:root /etc/banner
```
5. Check the ownership and permissions:  

```
# ls -l /etc/banner
```
6. If permissions are not `-rw-r--r--` make them so:  

```
# chmod 644 /etc/banner
```

#### TaitCentOS Sample login script

```
“WARNING! THIS SYSTEM IS RESTRICTED TO AUTHORIZED  
USERS ONLY!
```

```
If you are not authorized to use this system, you must exit immediately.  
Unauthorized users will be subject to criminal penalties, fines, damages  
and/or disciplinary action.
```

```
If you are authorized to use this system, you must do so in compliance with  
all laws, regulations, conduct rules, and company security policies  
applicable to this system. This system, including any hardware  
components, software, work stations, and storage spaces, is subject to  
monitoring and search without advance notice. Users should have no  
expectation of privacy in their use of any aspect of this system.”
```

## 10.4.2 Tait Ubuntu

It is recommended that you create a login script (in an `issue.net` file). This is the script that is displayed to the user when they log in from an external device (for example, using PuTTY).

A default `issue.net` file is included as part of the operating system installation (see below) (see "[Tait Ubuntu Sample issue.net login script](#)" on [page 62](#)). Use the following instructions if you want to create your own.

1. SSH into the controller with root privileges (see [Section 10.2 Logging on as 'root' for 'Tait Ubuntu Users' on page 59](#)).
2. Locate (or write) a file with the login script required.
3. Copy this file to the `/etc` directory, and name it `issue.net`:  

```
# mv <path to login script> /etc/issue.net
```
4. Change the ownership and group of the file to `root`:  

```
# chown root:root /etc/issue.net
```
5. Check the ownership and permissions:  

```
# ls -l /etc/issue.net
```
6. If permissions are not `-rw-r--r--` make them so:  

```
# chmod 644 /etc/issue.net
```

**Tait Ubuntu Sample  
`issue.net` login  
script**

“Authorized users only. All activity may be monitored and reported.”

## 10.5 Installing License Files

Tait applications must have a valid license file installed before they can operate.

License files can only be generated by Tait and each application must have its own unique license. If the application has been set up by Tait, an appropriate license file will have been installed.

### 10.5.1 Checking that the License File is Correct

1. To display license information:
  - TN9300 controller: select Settings > License
  - TN9400 Site Controller: select Server > License
  - TN9400 RFSS Controller: select Server > License
  - TN9500 gateway: select Settings > License
  - TD9361 SCADA Gateway: select Settings > Local Parameters > License
  - G.711 Connector: select General > License
2. The license state will be displayed, and if it is up-to-date, the features that are enabled will also be displayed.
3. If you are setting up a new device from scratch, a new license file will be required.

To get a license file, Tait must be supplied with the Host ID of the server that the device will be installed on (see below), and a list of the features required.

### 10.5.2 Obtaining the Host ID

The Host ID can be found on the Configuration > General page in the Administration application user interface.

### 10.5.3 Obtaining the `license.dat` File

Once you have provided the Host ID and required features to Tait, a license file for the application will be supplied.

If you are getting multiple licenses, you may combine the license files into one file that can be installed on all the devices. Because the license file is a text file, you can easily combine the information, but each line must be the full text from the original file. Each device will only use the line in the license information that matches its Host ID.

Currently, license files cannot be combined for the TN9400.

## 10.5.4 Installing License Files

1. Click Edit, then click Upload from:
  - a. TN9300 controller - Settings > License.
  - b. TN9400 RFSS Manager - Configure > RFSS.
  - c. TN9500 gateway - Settings > License.
  - d. TD9361 SCADA Gateway - Settings > Local Parameters > License.
  - e. G.711 Connector - General > License.
2. Click Choose File, then navigate to the license file, select it and click Open.
3. Once the license file has uploaded, the device will check if the license is valid.

## 10.6 Self-Signed SSL Certificates

When your browser connects to the administration application's user interface for the first time, it raises a security warning. Normally, secure web sites have a security certificate issued by a trusted Certification Authority. This is to foil attempts by rogue web sites to pretend to be something they are not.

Tait devices create a self-signed certificate when they, or their firmware, is installed. Your browser raises a security warning because the security certificate was not issued by a trusted Certification Authority. The browser has a way of letting you override or bypass the security warning, as explained below.

You can be confident that you are not connecting to a rogue website pretending to be your controller, so follow the procedure below to tell the browser that the security certificate is OK. The browser then stores the security certificate and will not raise a warning on subsequent connections, unless the IP address of the controller changes. If the controller's IP address is changed, simply repeat the certification procedure.

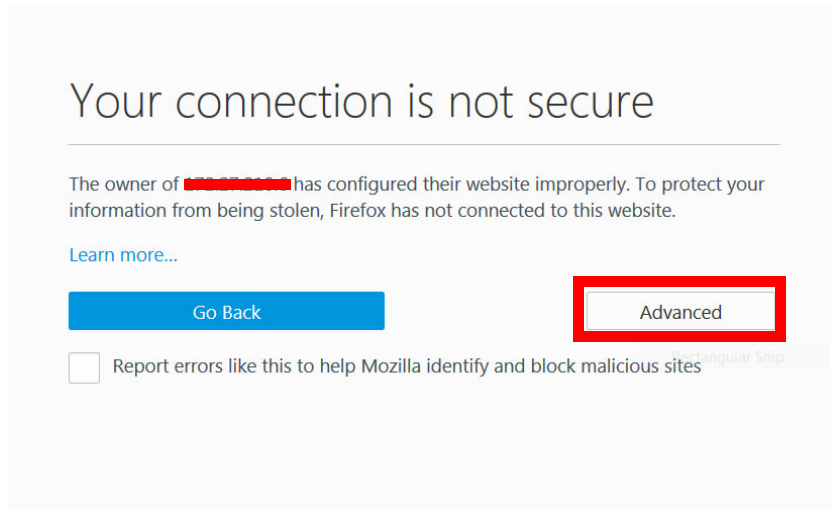
For more information, refer to <http://support.microsoft.com/kb/931850> or navigate to Configuration > SSL in your browser's Help, or refer to [Section 11.1.8 SSL](#).

### 10.6.1 Firefox Users

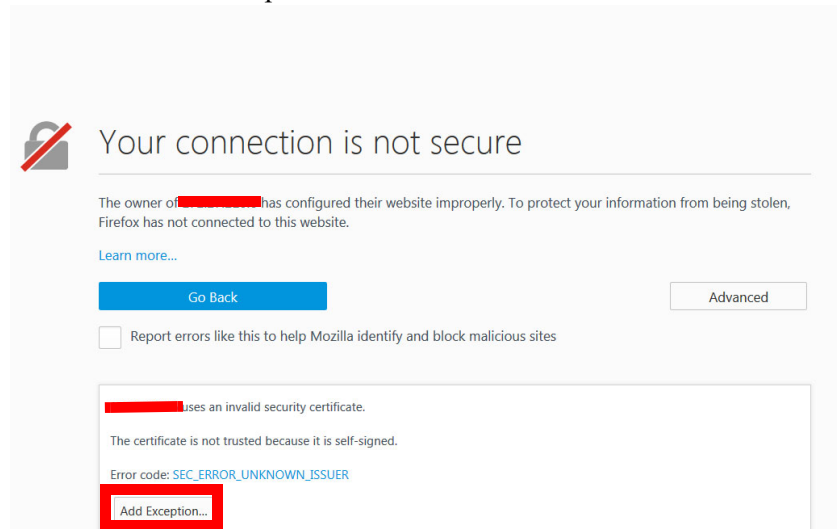
If Firefox is used, the following window appears when the user tries to access the controller user interface for the first time:



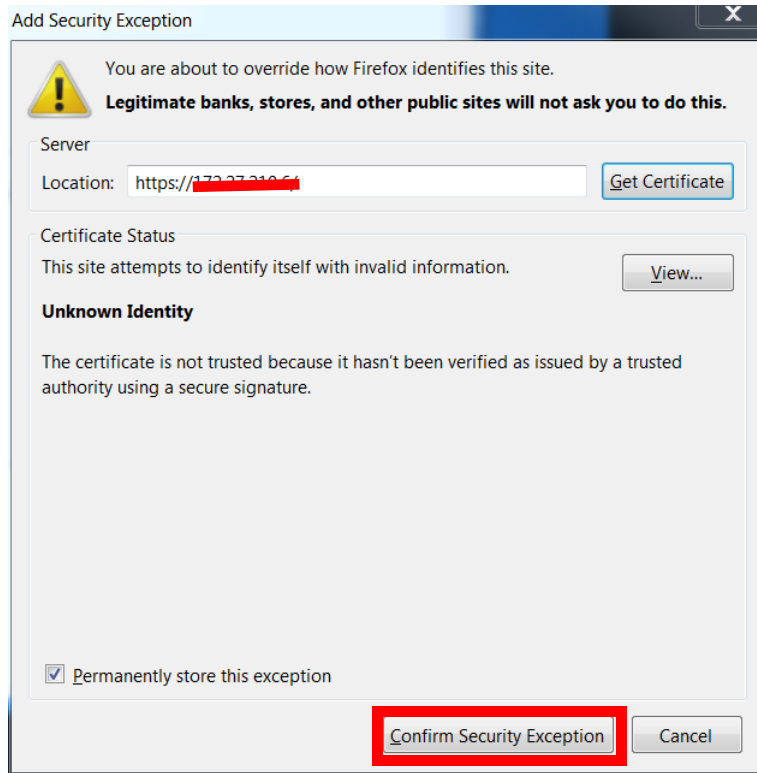
1. Click 'Advanced'.



2. Click 'Add Exception'.



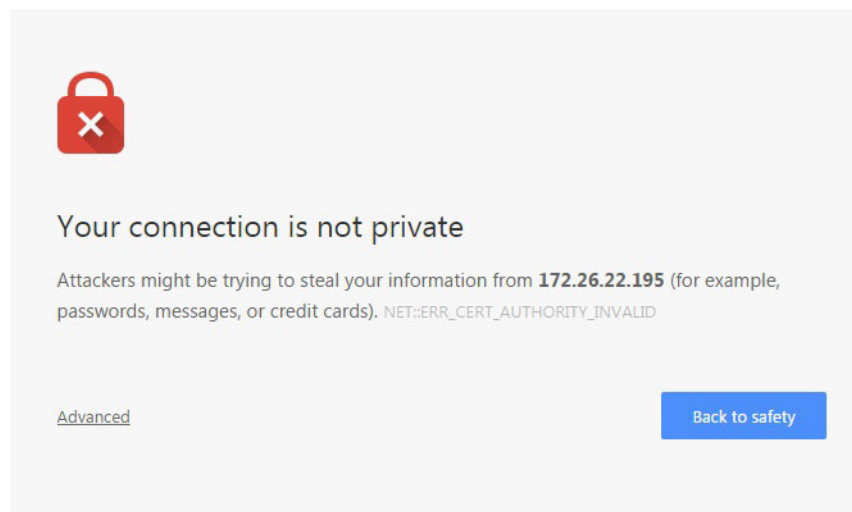
3. The Location field includes details specific to your controller. Without changing the default values, click ‘Confirm Security Exception’.




4. A secure connection to the controller user interface will be enabled in the browser.

## 10.6.2 Chrome Users

If Chrome is used, the following window appears when the user tries to access the controller user interface for the first time:



1. Click on Advanced.
2. Click on Proceed to <controller user interface IP address> (Unsafe).
3. Click Continue and log in as normal.

 This is only a temporary solution, that has to be repeated each time the controller is accessed.

### 10.6.3 Internet Explorer and Microsoft Edge Users


The controller user interface does not support Internet Explorer or Microsoft Edge.

## 10.7 Using the Certificate from a Certification Authority (CA)

By default, the Tait device generates its own self-signed certificate. This provides privacy by allowing traffic to be encrypted, but does not provide authentication. The result is that your browser displays a warning when connecting to the user interface. A user can bypass the warning but this calls into question the point of having a high security system

So, for maximum security we recommend the use of a certificate generated and signed by an external authority trusted by the browser.

The device allows you to upload a certificate generated by a trusted authority. For use on a public network this certificate may be obtained from a commercial provider. For use on a private network a certificate may be generated using the network's own certificate authority. This authority's certificate must be added to each browser's list of trusted authorities.

 To load your own certificate, see Section [10.6](#).

## 10.8 Changing Passwords

Tait networks are deployed with default weak passwords and it is the responsibility of the client to change them to strong passwords.

The defaults are:

- root<sup>1</sup>:  
    K1w1k1w1 (command line (SSH) login)
- taitnet:  
    tait (command line (SSH) login)
- iDRAC:  
    username: admin  
    password: K1w1k1w1
- BMC (Kontron CG2400)  
    username: admin  
    password: admin
- Administration application:  
    username: taitnet  
    password: tait
- TN9400 RFSS Controller:  
    username: taitnet  
    password: tait
- TN9400 Site Controller:  
    username: taitnet  
    password: tait
- RFSS Manager<sup>2</sup>:  
    username: taitnet  
    password: tait
- Fleet Manager<sup>3</sup>:  
    username: taitnet  
    password: tait

- 
1. There is no root on Tait Ubuntu; use `sudo` with your password instead. Only users with sudo rights can use `sudo`. The `taitnet` user has sudo rights.
  2. RFSS Manager default username is `admin` until TN9400 (version 2.26) is installed, whereupon it becomes `taitnet`.
  3. Fleet Managers running on version 2.20 up to and including 2.26 have two default usernames: `admin` and `taitnet`. From version 2.28 it is `taitnet` only.

- TN9300 DMR Trunked Node Controller<sup>4</sup>:  
    username: taitnet  
    password: tait
- TN9300 DMR Conventional Channel Controller<sup>4</sup>:  
    username: taitnet  
    password: tait
- TN9300 Channel Group Manager:  
    username: taitnet  
    password: tait
- TN8291 MPT-IP Node Controller<sup>4</sup>:  
    username: taitnet  
    password: tait
- T1541 Network Management Terminal:  
    username: admin  
    password: tait
- TN9500 Gateway:  
    username: taitnet  
    password: tait
- TN9361 SCADA Gateway:  
    username: taitnet  
    password: tait

### 10.8.1 Changing the 'root' and 'taitnet' Passwords

To change the password of a user, login as that user and enter:

```
passwd
```

You will be prompted to re-enter your current password. Next you will be asked to enter the new password that you wish to use. You will then be asked to confirm the new password.

- ⓘ Tait engineers will need the root password to provide support. If you change the root password, please ensure that you do not forget it.

### 10.8.2 Changing the iDRAC Password

- ⓘ Dell servers only

---

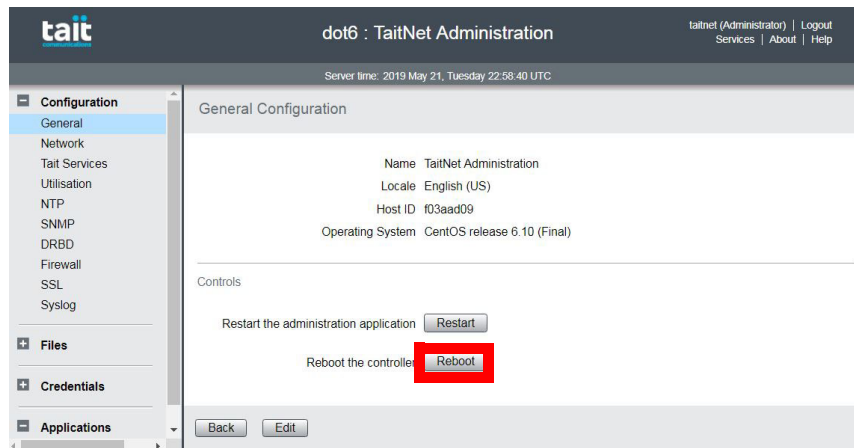
4. This applies to versions 4.xx and 3.28 and later. All version 2 controllers and version 3 controllers prior to version 3.28 have a default username of admin.

1. Connect a monitor, keyboard and mouse to the front of the Dell server.
2. Boot the server and wait for the Dell logo screen to appear during the early boot stages, then press the F2 key when 4 options appear in the top right corner of the Dell logo screen.  
After a period of approximately 1 minute, the System Setup screen appears.
3. Select `iDRAC Settings`.
4. Click `User Configuration` and change the password as required.
5. Click `Back`.
6. Click `Finish`.

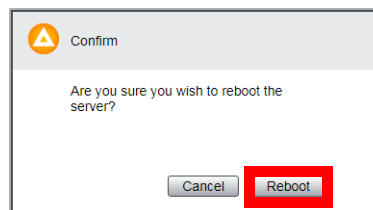
## 10.9 Performing an Operating System Restart

A full reboot can be performed using either the Administration application (recommended), or the SSH interface:

- In the Administration application select `Configuration > General` page, and click `Reboot`.



You will be asked to confirm the Reboot command.




It can take up to 5 minutes for the server to shut down and restart. The device software will automatically start after the server reboots.

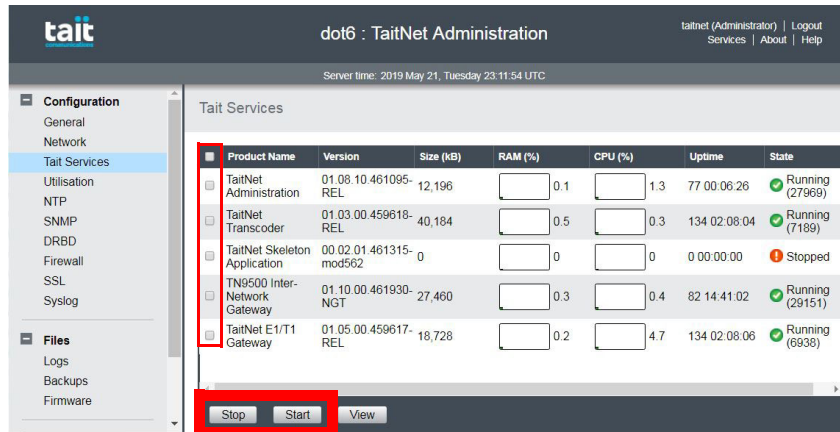
Connect to the user interface to confirm the controller has started.

- On the SSH interface login as root and enter the following:  
**reboot**

## 10.10 Stopping/Starting the Services Software

 Not all services can be stopped and started. Some sub-processes of an application can only be managed by the application itself. For more information refer to the online help of the service in question.

Log in to the Administration application's Configuration > Tait Services page to stop/start services by selecting the service and using the Stop/Start buttons as required.



Product Name	Version	Size (kB)	RAM (%)	CPU (%)	Uptime	State
TaitNet Administration	01.08.10.461095-REL	12,196	0.1	1.3	77 00:06:26	Running (27969)
TaitNet Transcoder	01.03.00.459618-REL	40,184	0.5	0.3	134 02:08:04	Running (7189)
TaitNet Skeleton Application	00.02.01.461315-mod562	0	0	0	0 00:00:00	Stopped
TN9500 Inter-Network Gateway	01.10.00.461930-NGT	27,460	0.3	0.4	82 14:41:02	Running (29151)
TaitNet E1/T1 Gateway	01.05.00.459617-REL	18,728	0.2	4.7	134 02:08:06	Running (6938)

For TaitCentOS users, the following also applies:

Alternatively, you could login to the server as root (see "[Logging on as 'root'](#)" on page 59). To stop the server enter:

```
taitnet-services stop
```

To start the server enter:

```
taitnet-services start
```

If the server is running or the software is hung, you can restart it by entering:

```
taitnet-services restart
```

## 10.11 Powering Down



**The server should always be powered down in a controlled fashion. You should always stop the software first, and you should never remove the power from the server unless it is powered off. Failure to follow this advice may lead to corrupt system files which will prevent the device operating.**

You may need to power down the server, for example if you are moving it to a new location, or you know of a scheduled power outage.

There are two ways to power off the server in a controlled manner:

- If you have access to the server hardware, simply press the power button.
- If you are shutting the machine down remotely, ssh to the device and switch to the root user. Enter the following:

```
poweroff
```

## 10.12 Changing to a Local Time Zone

Applies to Administration application version 1.16 and later.

- ⓘ Note that only one local time can be used per network. All servers in a network must be set to the same time zone, regardless of whether they are physically located in different time zones.

To change the time zone, log into the Administration application and set the desired time zone from the Configuration > General page.

The local time will be displayed in all log files as well as the alarms and call records pages on the user interface without a UTC offset.

The one exception is the status bar that is always displayed across the top of the user interface. It now has a time-date field in the middle that displays the current time and UTC offset of the controller in full date format as follows (for example):

```
Tuesday, 2014 February 11 12:51:57 UTC+00:00 (the controller local time is the same as UTC)
```

```
Tuesday, 2014 February 11 12:51:57 UTC+13:00 (the controller local time is 13 hours ahead of UTC)
```



## 10.13 TaitCentOS Only - Collecting Logs From Other Network Equipment

It is possible to collect logs from other network equipment (such as base stations or gateways) on the controller when installed with the administration application.

In this way a network administrator can centralize all the logs of a network in one place (e.g. all site base station logs to a TN9400 site controller, all gateway logs to an RFSS controller or all base station logs to a DMR controller).

- ① Note that this will add extra demand on the base station links, and it is important to check that there is enough bandwidth to collect the logs.
- ① Ensure the core network controller has enough disk space for the additional log file storage.

### 10.13.1 Configuring the Base Stations

1. Select Configure > Alarms > Syslog.
2. Click on Add and enter the IP address of the controller and select the type of information to log.  
The port used needs to match the port used on the controller (see Section 10.13.5 below).

### 10.13.2 Configuring the Controller

1. SSH to the controller.
2. Edit `/etc/rsyslog.d/tait_collector.conf` (see Section 10.13.5 below) and add the base stations to monitor, then save the file.
3. To apply the changes, enter the following command:  
**service rsyslog restart**

### 10.13.3 Operating the Administration Application

1. Log in to the Administration application WebUI.
2. Select Files > Logs > TaitNet Administration tab to view the collected logs of the base stations and/or other equipment.

## 10.13.4 General Information

The name format of the collected log files consists of the equipment name, followed by the date and time (`<equipment>_log_<date_time>.log`).

The current rules for archiving and purging log files on the Administration application will also apply to these new logs (see [Section 12.2 Log Files](#)).

On the server, current logs will be stored under `/var/log/syslog`.

When rotated, either manually or automatically, they will be moved to `/home/taitnet/admin/logs`, from where they will be visible in the Administration application.

To rotate the log files manually, enter the following command:

```
/usr/sbin/logrotate -f /etc/logrotate.d/tait-  
net_syslog
```

## 10.13.5 tait\_collector.conf File

Default file layout:

```
# Change/add/delete the following lines to enable this  
# host to accept syslog connections from other devices  
# such as Tait base stations.
```

```
# Remove the leading comment symbols (#) to enable the  
# setting.
```

—

```
# Provides UDP syslog reception  
$ModLoad imudp  
$UDPServerRun 514
```

—

```
# Provides TCP syslog reception  
$ModLoad imtcp  
$InputTCPServerRun 514
```

—

```
#:fromhost-ip,isequal,"172.29.0.201" /var/log/syslog/  
collector_1.log  
#& ~
```

—

```
#:fromhost-ip,isequal,"172.29.0.202" /var/log/syslog/  
collector_2.log  
#& ~
```

### File Information

- Depending on whether the equipment the logs are collected from uses UDP or TCP, make sure that the port `$UDPServerRun 514` or `$InputTCPServerRun 514` is the same.

- Add two lines to the file as follows:

```
:fromhost-ip,isequal,"[IP ADDRESS]" /var/log/sys-  
log/[NAME].log  
& ~
```

For example:

```
# Change/add/delete the following lines to enable this  
# host to accept syslog connections from other devices  
# such as Tait base stations.
```

```
# Remove the leading comment symbols (#) to enable the  
# setting.
```

—

```
# Provides UDP syslog reception  
$ModLoad imudp  
$UDPServerRun 514
```

—

```
# Provides TCP syslog reception  
$ModLoad imtcp  
$InputTCPServerRun 514
```

—

```
:fromhost-ip,isequal,"172.26.1.115" /var/log/syslog/  
DMR_site_1.log  
& ~
```

—

```
:fromhost-ip,isequal,"172.26.1.116" /var/log/syslog/  
DMR_site_2.log  
& ~
```

—

```
:fromhost-ip,isequal,"172.26.1.117" /var/log/syslog/  
DMR_site_3.log  
& ~
```

# 11 Basic Configuration

---

The following configuration procedures are done from the Administration application, and are indispensable to successful server and application operations. The headings below follow the Administration application's menu: i.e. Configuration, Files, Credentials.

Refer to the Administration application's online Help for detailed configuration information.

## 11.1 Configuration

Under the Configuration menu you can configure server settings, network parameters, firewalls and web server certificates. You can also monitor resource usage and the status of the services running on the server.

### 11.1.1 General

Select Configuration > General to view/edit settings that define the network server to which you are connected.

### 11.1.2 Tait Services

Select Configuration > Tait Services to view the status of the different services/applications running on the server.

#### Tait Ubuntu

From this page you can set the available versions of the containerized application to run. Users can also set the active IP of the HA cluster for applications that support high availability (HA). The Enabled checkbox allows users to stop and start containerized applications.

#### TaitCentOS


From this page you can also stop or start the different services, including this Administration application.

### 11.1.3 DNS

When remote hosts use dynamic IP addressing, applications such as the Data API Connector and PTTToX Connector can be configured to connect to them using their domain names instead of their IP addresses.

The Domain Name System (DNS) client feature is an optional feature that uses DNS lookup to find the IP address of a remote, or cloud based, host. It can be used, for example, to enable the TN9500 Inter-Network Gateway

to connect to cloud based hosts using their domain names instead of their IP addresses.

 It is recommended that this feature be maintained by network administrators or other IT-proficient users.

1. Select Configuration > DNS to view information for the DNS client feature. From this page, domain names can be added or deleted, and domain name server IP addresses can be maintained.
2. Enter the local domain name, and add other domain names as required to the search list. These parameters are optional.
3. Add at least one domain name server IP address. This will enable the DNS client feature.

#### 11.1.4 Network Time Protocol (NTP)

Use the NTP page to view/edit the settings that define Network Time Protocol (NTP) parameters. From this page you can also control NTP operation.

1. Select Configuration > NTP.
2. Select Edit.
3. Enter the IP addresses of up to three NTP servers.
4. Press Save.
5. Press Start to begin the NTP daemon service.
6. Pressing Synchronize will check the status of the synchronization of this server with at least one of the NTP servers specified.
7. Use the status area to monitor the state of the NTP service.

#### 11.1.5 SNMP

The Administration application can support the use of both SNMPv2c and SNMPv3 at the same time, so information for both can be maintained.


The different Tait devices can be monitored via their own MIBs (e.g. status), but the administration application server in general can be monitored using the standard UCD-SNMP-MIB (CPU, memory and disk statistics and system uptime).

As well as its own MIB traps, devices can also use traps from DISMAN-EVENT-MIB (in particular `dismanEventMIBNotifications => mteTriggerFired` OID 1.3.6.1.2.1.88.2.0.1).


1. Select Configuration > SNMP.

2. Select Edit.
3. For SNMPv2c, add or change the Read-only community string and enter up to two IP addresses to which SNMP traps will be sent.
4. For SNMPv3, add or change the user name and passphrase, and enter up to two IP addresses to which SNMP traps will be sent.
5. Click Save.
6. Click Start to begin the SNMP daemon on this server.
7. Use the status area to monitor the state of the SNMP service.

### 11.1.6 Firewall - TaitCentOS

-  If a GridLink server is installed, this firewall is no longer configurable and will not appear in the Administration Application UI. This is because the GridLink SCADA gateway manages the firewall instead.

Select Configuration > Firewall to view the firewalls for this server. From this page, firewalls can be stopped or started, and firewall configuration files can be uploaded, deleted, or installed.

-  This is for servers running on TaitCentOS only. Firewalls are created for the Tait Services (and the ports they use) running on this server.

#### Enabling the Firewall

To enable the firewall, go to the Administration Application page Configuration > Firewall and perform the following.

1. Select the appropriate configuration file for the product, e.g. `firewall-tn9400-access` for a TN9400 Access system.
2. Click Install.
3. If the service is not running, click Start.

#### Disabling the Firewall

To disable the firewall, go to the Administration Application page Configuration > Firewall and click Stop.

#### Downloading Firewall Configuration Files

The sample firewall configuration files can be downloaded by clicking on the names of the files.

#### Customizing Firewall Configuration Files

To customize the firewall settings, first download the `firewall_default` file and rename it. Open the file in an editor that respects Linux end of line characters and modify entries as required. An example of modification would be where it is desired to allow http access to the feeds folder. In this case, when editing the file, remove the `#` from the start of the line indicated in the file.

```
# Remove the comment from the following line to enable
http access i.e. for access to the 'feeds' folder via
http.
```

```
#-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport
80 --state NEW -j ACCEPT
```

When finished with editing the file, upload the renamed file to the controller and click the install button.

To test that the updated firewall file works, select the file and click Start:

- A test is performed to test the connectivity between the browser and the Administration Application. If at any point in the two minute test, the connection is broken, the firewall will be automatically disabled.
- If two minutes passes without a break, the firewall will stay enabled. This test prevents you from installing a firewall configuration that locks you out of the Administration Application.

Notes:

- Clicking the install button may not restart the firewall service automatically. If the firewall is not behaving as expected, try pressing stop followed by start to restart the firewall service.
- If the sample file is not renamed when customizing the firewall, it will be overwritten next time the firmware is upgraded with the default for that version of firmware.
- It is expected that customizing the firewall files will only be done by people who are experienced in configuring iptables (firewall service).

#### Debugging

Any packets dropped by the firewall are logged to `/var/log/messages` with the keyword `Firewall-Dropped`.

As the root user, the following commands can be used to get various degrees of information from the messages log.

#### Full Output

```
cat /var/log/messages | grep Dropped
```

...

```
May 1 22:36:09 akaroa-b kernel: Firewall-Dropped:
IN=em1 OUT=
MAC=d4:ae:52:bd:ea:de:d4:ae:52:cb:8c:9b:08:00
SRC=172.27.201.30 DST=172.27.201.31 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=42299 DF PROTO=TCP SPT=59975
DPT=7730 WINDOW=14600 RES=0x00 SYN URGP=0
```

```
May 1 22:36:12 akaroa-b kernel: Firewall-Dropped:
IN=em1 OUT=
MAC=d4:ae:52:bd:ea:de:00:07:7d:73:f1:b1:08:00
SRC=172.16.182.36 DST=172.27.201.31 LEN=52 TOS=0x00
PREC=0x00 TTL=126 ID=807 DF PROTO=TCP SPT=23925 DPT=80
WINDOW=8192 RES=0x00 SYN URGP=0
```

```
May 1 22:36:32 akaroa-b kernel: Firewall-Dropped:
IN=em1 OUT=
MAC=d4:ae:52:bd:ea:de:d4:ae:52:cb:8c:9b:08:00
SRC=172.27.201.30 DST=172.27.201.31 LEN=60 TOS=0x00
```

```
PREC=0x00 TTL=64 ID=37824 DF PROTO=TCP SPT=58564
DPT=7730 WINDOW=14600 RES=0x00 SYN URGP=0
```

```
May 1 22:37:03 akaroa-b kernel: Firewall-Dropped:
IN=em1 OUT=
MAC=d4:ae:52:bd:ea:de:d4:ae:52:cb:8c:9b:08:00
SRC=172.27.201.30 DST=172.27.201.31 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=33513 DF PROTO=TCP SPT=46781
DPT=7729 WINDOW=14600 RES=0x00 SYN URGP=0
```

...

#### Reduced Output

```
cat /var/log/messages | grep Dropped | sed 's/.*SRC/SRC/'
| sed 's/ .*SPT=/ SPT=/' | sed 's/ WINDOW.*//'
```

...

```
SRC=172.27.201.30 SPT=59975 DPT=7730
SRC=172.16.182.36 SPT=23925 DPT=80
SRC=172.27.201.30 SPT=58564 DPT=7730
SRC=172.27.201.30 SPT=46781 DPT=7729
```

...


#### Continuously Monitored Output

```
tail -f /var/log/messages | grep Dropped
```

## 11.1.7 Firewall - Tait Ubuntu

Whilst the Tait Ubuntu Administration application has no provision for firewalls, it is recommended that external firewalls should be used.

If a firewall is required on the server itself, then `iptables` is available and can be configured from the command line. A sample configuration file to allow access to the Administration application is given below.

 This example requires additional modification to work with the other Tait services.

```
#####
#####
# Start default rules, deleting/editing these lines is not
# recommended and may break your server.
*filter
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
```



```

-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -
j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 22 --
state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 443 --
state NEW -j ACCEPT
# End default rules
#####
#####

#####
#####
# Start tait_admin rules.
-A RH-Firewall-1-INPUT -p udp -m state -m udp --dport 161 --
state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 1443 -
-state NEW -j ACCEPT
# End tait_admin rules.
#####
#####

#####
#####
# Start Logging rules
-N LOGGING
-A INPUT -j LOGGING
-A LOGGING -m limit --limit 2/min -j LOG --log-prefix
"Firewall-Dropped: " --log-level 4
-A LOGGING -j DROP
# End Logging rules
#####
#####

COMMIT

```

## 11.1.8 SSL

Select Configuration > SSL to view the SSL certificate that is currently in use, and those SSL certificates that have been uploaded and that can be installed.

A default is provided, but a new SSL certificate/key pair for HTTPS access can be uploaded. You may use a self-signed certificate or one obtained from a certification authority.

1. On the DMR web browser, select Configuration > SSL.
2. To install a new certificate or revert to an earlier one, click the Edit button.
3. Under the SSL Certificate/Key Upload area, click Upload SSL certificate to load an SSL certificate file and Upload SSL Key to load an SSL key file.

- ① The SSL key needs to be decrypted before loading as there is no provision in this application for entering a passphrase for decrypting the key.
- 4. Once uploaded to the SSL Certificates area, select the certificate from the Uploaded list and press Install.
- 5. A prompt will appear to inform that the node needs to be rebooted for the certificate to take effect.
- 6. Once the reboot has been completed, the installed certificate will be active.
- 7. To revert to the default self-signed certificate provided by Tait, press Revert. This will also require a node reboot for the change to take effect.

### 11.1.9 Syslog

Use the Syslog page to view/edit syslog configuration settings.

1. Select Configuration > Syslog.
2. Click Edit.
3. Enter the IP addresses of up to two external syslog collectors.
4. Select the protocol to use for the formatting of the syslog messages.
5. Select the level of information required for syslog collection. Use the check box to enable the collection of audit trails. Use the Internal logs dropdown menu to select the level of logs to be collected, if any.

① Logs below the level selected will also be included. e.g. selecting the level `Notice` will also include logs from the `Informational` and `Debug` levels.

6. Click Save.

### 11.1.10 Anti Virus

① ClamAV comes with Tait Ubuntu, but for TaitCentOS users it needs to be installed separately.

ClamAV is an open source antivirus engine for detecting trojans, viruses, malware and other malicious threats.

ClamAV software does not come as part of the Administration Application, it is an optional extra that can be obtained from Tait Technical Support, and can be installed/upgraded from the Administration Application.



**Warning** Do not attempt to download and install ClamAV independently, as only the version contained in the package provided by Tait is supported by Tait products.

### Installing ClamAV (TaitCentOS)

ClamAV can be installed from the Administration Application by uploading and installing the ClamAV software installer (`clamav-xx.rhel7`) and its database updates package (`clamav-update-xx.rhel`). For ClamAV to operate, both these packages need to be installed.

After installing the ClamAV software packages (installer and database updates), refresh the screen to display the Anti Virus menu option.

The virus database can also be updated periodically by installing a virus database update package. These are also obtained from Tait support.

### Using ClamAV

1. Select Configuration > Anti Virus to view ClamAV scan details.
2. In the Controls area, the 'Quarantine infected files' option can be enabled so that infected files are moved to a quarantine directory on the server, otherwise they will be left in place.
3. In the Controls area, under Scan, click Start to start a scan. If a scan is in progress this will display Stop and can be used to cancel the scan.



By default, ClamAV scans are disabled.



Anti virus scans use significant CPU and disk resources; we advise that scans should be performed during network quiet times.

## 11.2 Files

The server generates and stores files of various types. You can view lists of available files from this menu and download them to your PC.

### 11.2.1 Logs

Select Files > Logs to view a list of log files that can be downloaded to your PC.

### 11.2.2 Backups

It is good practice to back up configuration files on a regular basis. This is especially important when changes are made.

The Administration application and Tait device configuration files are automatically backed up, but it is also a good idea to periodically perform

a manual backup, particularly when a lot of changes have been made to the configuration parameters.

#### Manual backup

1. Select Files > Backups.
2. Select Backup.



To download a copy of a backup file, click on the filename.

#### Restoring a backup

1. Select Files > Backups.
2. If you are loading a backup from an external source, select Upload then select Choose File to browse to the file, then select Open.
3. Select the file you wish to restore and select Restore.

The following databases are backed up by the Administration application:

- authentication database - contains information about authentication settings and users that have been manually configured via the user interface
- administration database (admin) - contains information about users that have been manually configured via the user interface

The format of the backup filename is as follows:

```
<application_name>_<database_name>_backup-  
<YYYYMMDDhhmmdd>.db
```


where *<application\_name>* is the Tait service (e.g. admin or ing), and *<database\_name>* is the database (e.g. authentication, tait\_admin or tait\_ing), and *<YYYYMMDDhhmmdd>* is the date and time of the backup.

### 11.2.3 Firmware

Select Files > Firmware to view the firmware versions currently stored in the server. Buttons allow you to delete, install or upload firmware files.

## 11.3 Credentials

The Administration application is used to configure centralized authentication, where required, and to create local user login entries, which can then be enabled on the controller.

-  It is recommended that local users should not be created if centralized authentication is used on your server.

### 11.3.1 Password


All users, except for those that have been disabled, or those who log in using LDAP or RADIUS, can change their own passwords.

To modify your password, follow these steps.

1. Select Credentials > Password.
2. Enter your current password.
3. Enter and re-enter the new password. A password can be up to 200 characters long. Control characters are illegal (ASCII 0-31 and 127).
4. Click Save.

### 11.3.2 Users

1. Select Credentials > Users and click Add. (To add a user you must have the Administrator access level.)
2. Enter a name into the Username box. This is the name that the user must enter to log in. A user name can be up to 140 characters long, spaces are permitted, but the following characters are illegal: \* ' ' " " \ ( ) & | ! = ~ < > , ;
3. Enter the user's full name into the Name box. Control characters are illegal (ASCII 0-31 and 127). When the user logs in to the server, it will display this name at the top of the page.
4. Optionally enter a comment.
5. Select the appropriate access level for the user.

-  Non-administrator users of other TaitNet applications only, such as the controller, should have their access level set to Disabled. It will be enabled from within the relevant TaitNet application.

### 11.3.3 Authentication

Connections to the server can be authenticated by a remote (i.e. centralized) service. Two remote authentication protocols are supported: LDAP and RADIUS.

Changes here should only be made by people experienced with the AAA architecture and authentication protocols.

- ❗ Any changes made to the authentication settings will result in all currently logged on remotely-authenticated users being logged out.
- ❗ If the RADIUS protocol is selected, the RADIUS configuration settings made in the Administration application will apply to most of the applications on the server<sup>1</sup>. If the LDAP protocol is selected, LDAP configuration settings apply to most of the applications on the server (see footnote), and the LDAP rules must also be applied to each of these applications on the server as required.

#### LDAP

The following information is required to configure a controller for LDAP:

- The IP address and port number (typically 389 for LDAP) of the LDAP server
- The search base for the LDAP server defines where the search begins in the LDAP directory. It prevents scanning the whole directory tree if only a specific branch is sufficient. This setting can affect the response time if the directory structure is complex with several entries.
- Group member attribute: specifies the name of the attributes used by LDAP groups to identify their members
- Bind DN: typically a user who is allowed to browse the LDAP directory and read user attributes
- Bind password: password required for the account allowed to browse the LDAP directory
- LDAP rules: mapping rules between local access levels and remote LDAP groups. This capability ensures that users belonging to a specific group are given a specific access level. A minimum of one rule is required.

- ❗ LDAP rules must also be set up on each controller in your network.

#### Configuration Procedure for LDAP


1. Select Settings > Authentication and click Edit.
2. Select LDAP from the Remote field drop down.
3. In the LDAP Server area enter the values for your network (as listed above).

---

1. TN9500 version 1.10.01 does not use the LDAP/RADIUS settings applied by the Administration application.

TN9400 version 2.04.05 does not use the LDAP/RADIUS settings applied by the Administration application.

4. In the LDAP CA Certificate area, click the Secure with Start TLS checkbox to enable secure communications with the remote LDAP server by utilizing an encrypted TLS connection, if required. The TLS protocol versions available are: TLS1.0, TLS1.1 and TLS1.2.
5. In the LDAP Rules area, click Add and create at least one rule.  
The table of rules is used to determine the access level of a user. Each rule is checked in order until a match is found. At least one LDAP rule must be defined if LDAP is selected as the authentication protocol. The LDAP rules associate local access levels to remote LDAP groups and/or user attributes.
6. Repeat for the next rule you want to define. You can define up to 10 rules. To add a rule to the bottom of the table click Add. Rules should be added in order of Access level, with the highest first in the table. The order is important because each rule is checked in order until a match is found, so to add a rule in the middle of the table, select the line above which you want the new rule to appear and click Insert.

 At least 1 rule needs to be specified, otherwise no users will be successfully authenticated by the LDAP server

The following rule table example is provided as an example:


<b>Id</b>	<b>Group DN (example)</b>	<b>Search Filter</b>	<b>Access Level</b>
1	cn=Controller_Administrator,ou=groups, o=support_services, o=client,dc=taitradio		Administrator
2	cn=Controller_Network_Administrator, ou=groups, o=support_services, o=client,dc=taitradio		Network administrator
4			Read only


In this example:

- Users belonging to Controller\_Administrator LDAP group will have Administrator access level
- Users belonging to Controller\_Network\_Administrator LDAP group will have Network administrator access level
- All other users under the LDAP search base (specified above) will get Read only access level (it is recommended that this rule is always included at the end of the rules table)

Optionally, additional Search Filters can be enabled for each access level. This will add a test against a user attribute.

For example, if `department=LMR_Operation` was added to the Search Filter column in row 4 (above) of the table, then only users with an attribute `department` with a value set to `LMR_Operation` would have Read only access.

 The Group DN and Search Filter fields can be used in combination to allow very flexible user filtering rules.

7. Click Save. The option to upload an LDAP CA certificate is now displayed in the LDAP CA Certificate area.
  8. To upload a CA certificate, click Upload.
-  If StartTLS is enabled, the CA certificate that signed the remote LDAP server certificate must be uploaded.
9. Click Save.



**If no LDAP user with Administrator access level is defined, then it is imperative that a local administrator account is created in Settings > Users so that local users and passwords can be added and updated.**

## RADIUS


The following information is required to configure RADIUS:

- The IP address and port number (typically 1812 for RADIUS) of the RADIUS server
- The shared secret password - this is used together with an MD5 hashing algorithm to encrypt passwords
- Optionally, predefined access levels can be configured for RADIUS authenticated users. This optional capability requires a specific configuration on the RADIUS server with the use of the IETF RADIUS Class attribute.

If no provision has been made on the server for this attribute, then this option should be left inactive, so that a default access level will be given to all users authenticated via RADIUS.

## Configuration Procedure for RADIUS

1. Select Settings > Authentication and click Edit.
2. Select RADIUS from the Remote field drop down.
3. In the RADIUS server area, enter the IP address, port number, and shared secret of the RADIUS server.
4. Access level from class attribute can be enabled, if required:
  - a. If enabled (checked), the WebUI access level given to an authenticated user will depend on the value of the IETF RADIUS Class attribute associated with a given user account in the RADIUS server.

-  If the option is enabled and no Class attribute is present, or the returned value does not match the expected values below, user access will be denied.

The expected Class attribute values to be provisioned on the RADIUS server should match the following:

- TN\_administrator, for Administrator access level
- TN\_network\_administrator, for Network administrator access level
- TN\_read\_only, for Read only access level



- ① If no RADIUS user with Administrator access level is defined, then it is imperative that a local administrator account is created in Settings > Users so that local users and passwords can be added and updated.
    - b. If disabled (unchecked), the access level for all RADIUS authenticated users will be set to the default: Network administrator.
  - ① Make sure that a local administrator account is created in Settings > Users so that local users and passwords can be added and updated.
5. Click Save.

# 12 Administration Application Information

---

## 12.1 IP Protocols and Default Ports

This section describes the IP protocols and IP ports of the Administration application. For information about the IP protocols and IP ports of the different installed Tait Services, refer to their system manuals or configuration guides.

### 12.1.1 IP Protocols

A variety of IP based protocols is used. In some situations firewalls must be configured to allow this traffic to pass across the IP bearer network.

The following table lists the Administration application ports and their usage.

Type	Usage	Ports/Protocols
ICMP	NMS and management PC to node controllers, network gateways, base stations, switches and routers	ICMP
Network Time Protocol (NTP)	Network synchronization	UDP 123
RADIUS authentication	RADIUS authentication server to/from node controllers, switches, base stations, network gateways and routers	UDP1813
LDAP	LDAP authentication server to/from node controllers, switches, base stations, network gateways and routers.	UDP 389
Remote Desktop Protocol (RDP)	SNMP Manager Remote Desktop. (Not required but preferred for VPN access if EnableMonitor is deployed.)	TCP 3389
Secure shell (SSH)	Node controllers, network gateways, base stations, switches and routers to NMS	TCP 22

Type	Usage	Ports/Protocols
Simple network management protocol (SNMP)	NMS to node controllers, network gateways, base stations, switches and routers	UDP 161/162
Syslog	Node controllers, network gateways, base stations, switches and routers to NMS	UDP 514
Web interface (https)	Management PC to node controllers, base stations, NMS, switches and routers	Various, see <a href="#">Section 12.1.2 IP Default Ports</a>

## 12.1.2 IP Default Ports

Each application has a resource configuration file (extension `.cfg`)<sup>1</sup>. This file provides some limited configuration parameters that cannot be changed when logged on to the Tait Service or Administration application. It is not recommended that they are changed unless Tait Technical Support has requested it. These parameters are read at startup and whenever the `reload-cfg` command is executed. The file has to be edited by a text editor such as 'vi'.

The following ports are the defaults used by the Administration application. If the default value of a port needs to be changed, the relevant configuration file for the application may be edited as required.

If the configuration file is missing, the default values listed below will be used.

### Administration Application

The configuration file for the Administration application is `/home/taitnet/admin/tait_admin.cfg` and the default port settings are:

- `https_port`: 1443
- `watchdog_server_port`: 2010
- `watchdog_application_port`: 2011

For the default ports used by the Tait service applications (e.g. TN8291, TN9300, TN9400, or TN9500), please refer to the relevant system manuals.

---

1. Version 3 nodes: DMR trunked is `tait_dmrnc.cfg`, DMR conventional is `tait_dmrcc.cfg`, and MPT-IP is `tait_mptipnc.cfg`. Version 2 nodes: `node.cfg`.

## 12.2 Log Files

The log files are initially stored as text files (.log) for 3 days. After 3 days, they are automatically gzipped for archive purposes, after which they are kept for a further 90 days before being automatically deleted.

The name format of the 3-day log files is `<name>_YYYYMMDD`. Once they have been gzipped, this becomes `<name>_YYYYMMDD_HHMMSS`. The `<name>` variable is dependent on the log file type and application involved, i.e. admin for Administration application. The file is rotated every night. For internal logs, the files can also be rotated on size (>10MB).

Log files can be downloaded from the user interface under Files > Logs (in both the Administration application and controller user interface) by clicking on an individual log file name.

### 12.2.1 Installation and Upgrade Logs

#### TaitCentOS only

`/root/install.log`

This is created by the TaitCentOS installer and contains a list of the packages installed as part of the operating system installation.

`/root/install.log.syslog`

This is created by the TaitCentOS installer and contains information about users/groups that have been created at installation.

`/root/ks-post.log`

This is created by the TaitCentOS installer and contains an output of the kickstarter post install stage. This file contains information regarding the installation status of the `taitnet` and `taitnet-admin` packages and any other customized changes made after installing the core OS.

`/var/log/taitnet-install.log`

This log file is created by the `taitnet` RPM and contains information on the installation status of the `taitnet` package. Any future downgrades and upgrades are appended to this log.

#### Tait Ubuntu only

`/var/log/installer/curtin-install-cfg.yaml`

This file contains the configuration used for the operating system installation.

`/var/log/installer/curtin-install.log`

This log file is generated during the operating system installation.

`/var/log/cloud-init-output.log`

This log file is generated by the operating system customization process.

**Administration app  
Logs in /home/  
taitnet/admin/  
logs**

`taitnet-admin-install.log`

This log file is created by the `taitnet-admin` RPM and contains information on the installation status of the `taitnet-admin` package. Any future downgrades and upgrades are appended to this log.

A separate file is created for each application installation

**Upgrade Logs in /  
home/taitnet/  
admin/logs**

`admin_upgrade_<YYYYMMDD>.log`

This log file contains information on the upgrade status of the selected package (Tait service or Administration application for example). Any future downgrades and upgrades are appended to this log for the day.

`admin_upgrade-error_<YYYYMMDD>.log`

This log file is only created if the upgrade failed and it contains the error information related to the upgrade. Any future downgrades and upgrades are appended to this log for the day.

**Audit Logs in /  
home/taitnet/  
admin/logs**

`admin-audit_<YYYYMMDD>.log`

This log file shows changes made by users on the user interface.

**Watchdog Logs in /  
home/taitnet/  
admin/logs**

`admin-watchdog_<YYYYMMDD>.log`

This log file confirms that the different processes of the Administration application are running properly.

# Appendix 1: Transferring an ISO Image to a USB Flash Drive

---

Bootable ISO images, such as the TaitCentOS or Tait Ubuntu ISO, can be transferred to a USB flash drive.

The Tait Ubuntu ISO can be transferred using Rufus. The Tait CentOS ISO can be transferred using either Win32DiskImager or another tool such as Rufus. Non-bootable ISO images, such as the TaitNet installation software, requires Win32DiskImager.

The advantage of Rufus over Win32DiskImager is that when the USB flash drive has been written to, the USB flash drive is still able to be read from and written to under Windows. This allows the user to add any additional scripts, configuration files etc. to the USB flash drive.

- ① Some TaitCentOS ISO images operate only when written to a USB flash drive via RUFUS, others operate only with Win32DiskImager.
- ① If using a USB, the Dell R250 and Sintrones SBOX-2621 servers can only be booted up by a USB type 3.0 flash drive. When installing software on a Dell R250 or Sintrones SBOX-2621, please make sure your flash drive is compliant. The internet can provide tips on how to recognize a USB 3.0 flash drive (e.g. sometimes it has a blue insert). If problems arise, please contact Tait Technical Support.

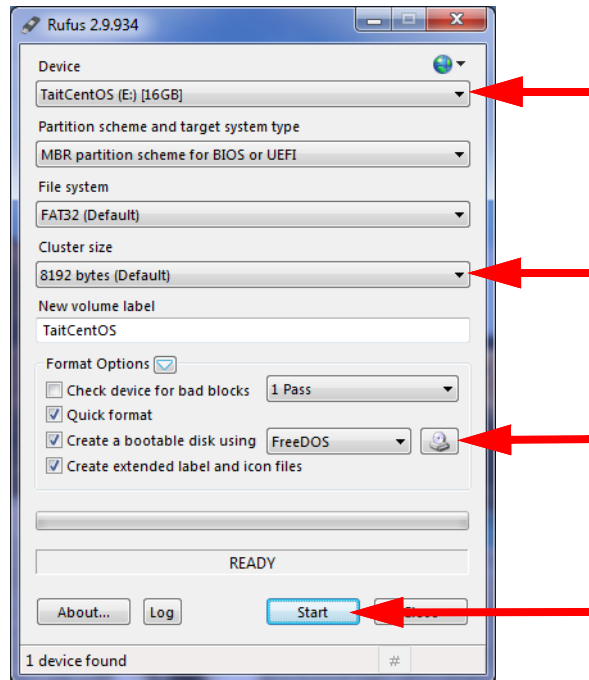
## A.1 Using Rufus for TaitCentOS

1. To create a bootable USB flash drive with TaitCentOS, first download and install the Rufus application.

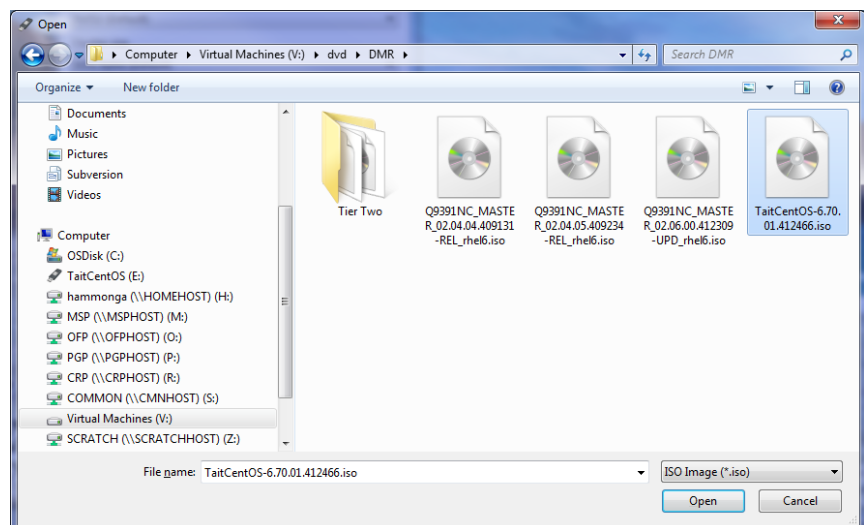
- ① Rufus cannot be used to write non-bootable ISO images, such as the TaitNet installation software.
- ① Only install the Tait supplied TaitCentOS version (i.e. not a commercial CentOS package), to ensure that the correct configuration settings are installed.

2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (TaitCentOS will require at least an 8GB flash drive.)

3. Run the Rufus program.



4. Check that the Device in the first drop down list is the same as the USB flash drive.
5. Click on the CD icon next to the drop down list containing 'FreeDOS'. This will open a dialog box to enable the selection of the ISO file to be written to the USB flash drive.
6. Select the ISO file and click Open, which takes you back to Rufus.

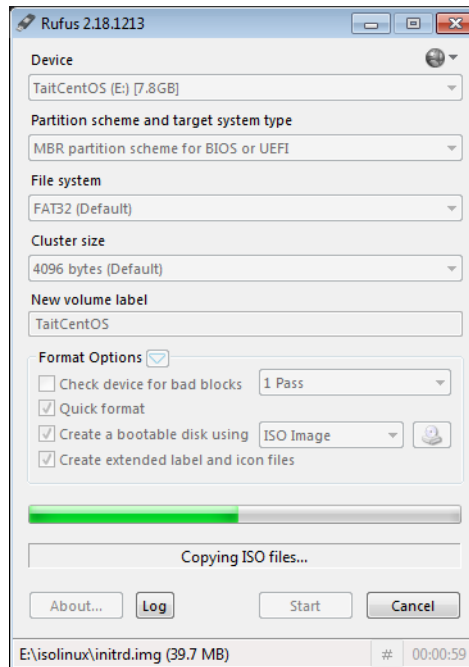


7. When ready to start the writing process, click Start.

- A dialog box will appear to confirm that a write operation is to be carried out. At this point double check that the correct device is being written to and then click OK.

Depending on how large the ISO file is and the write speed of the USB flash drive, it could take from less than a minute to half an hour or more to complete the write process.



- The progress of the USB flash drive write is displayed as follows:



- When the USB flash drive write has finished, the Cancel button will change to a Close button. Click Close to complete the process.
- Remember to safely eject the USB flash drive before physically removing it from the PC.

## A.2 Using Rufus for Tait Ubuntu

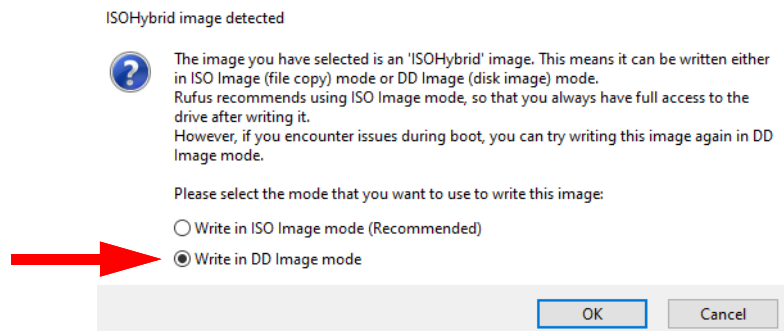
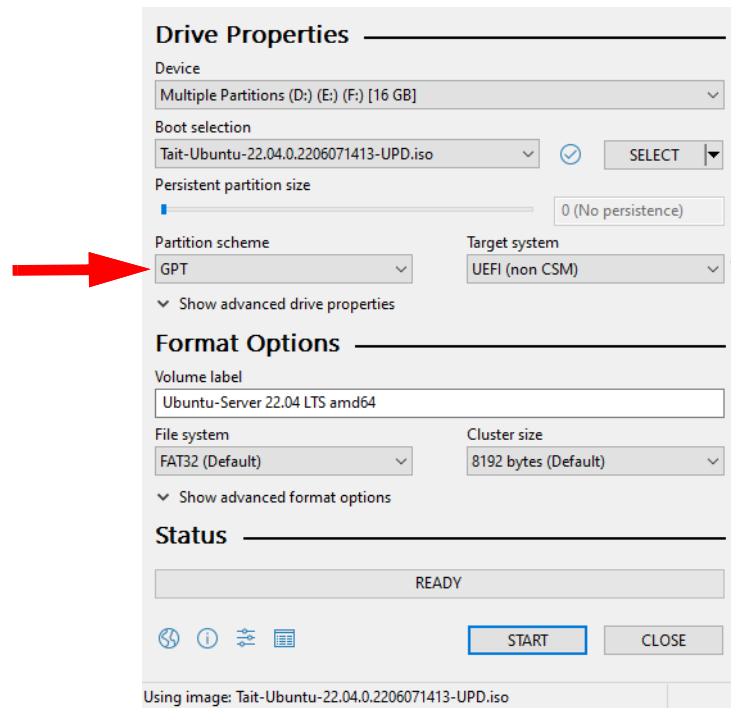
- To create a bootable USB flash drive with Tait Ubuntu, first download and install the Rufus application.

-  Rufus cannot be used to write non-bootable ISO images, such as the TaitNet installation software.
-  Only install the Tait supplied Tait Ubuntu version (i.e. not a commercial Ubuntu package), to ensure that the correct customization and configuration settings are installed.

- Insert a suitably sized USB flash drive into one of the PC's USB ports. (Tait Ubuntu will require at least an 8GB flash drive.)



3. Run the Rufus program.
4. Select GPT as the partition type and Write in DD Image mode when you are prompted (see screenshots below).



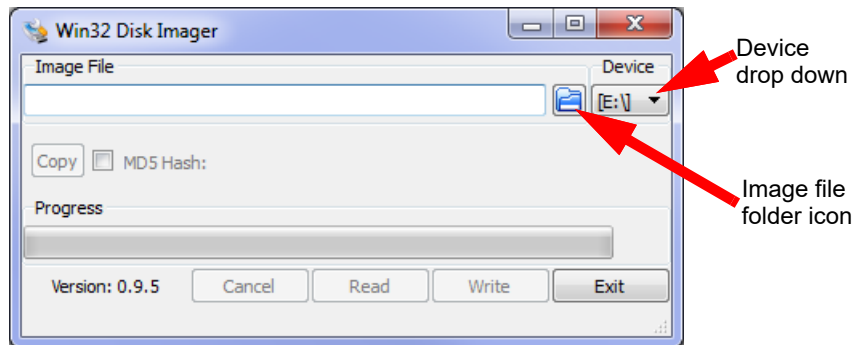
### A.3 Using dd for Tait Ubuntu on Linux

1. If you are using a Linux desktop, you can run the following command as root to flash the downloaded ISO image to a USB drive:  

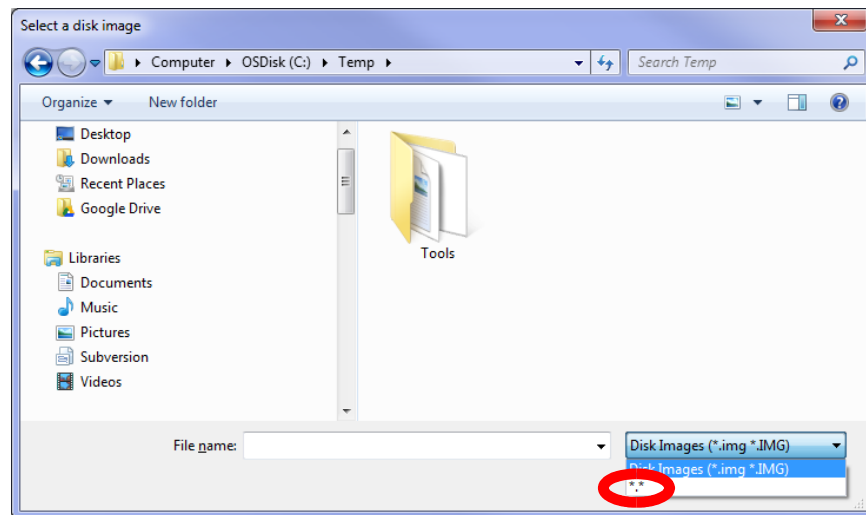
```
sudo dd if=<path to the iso file> dd=<path to the USB device> bs=1024k status=progress oflag=sync
```
2. Once the USB is flashed with the downloaded ISO file, it is capable of supporting both BIOS and UEFI boots.

## A.4 Using Win32DiskImager for TaitCentOS

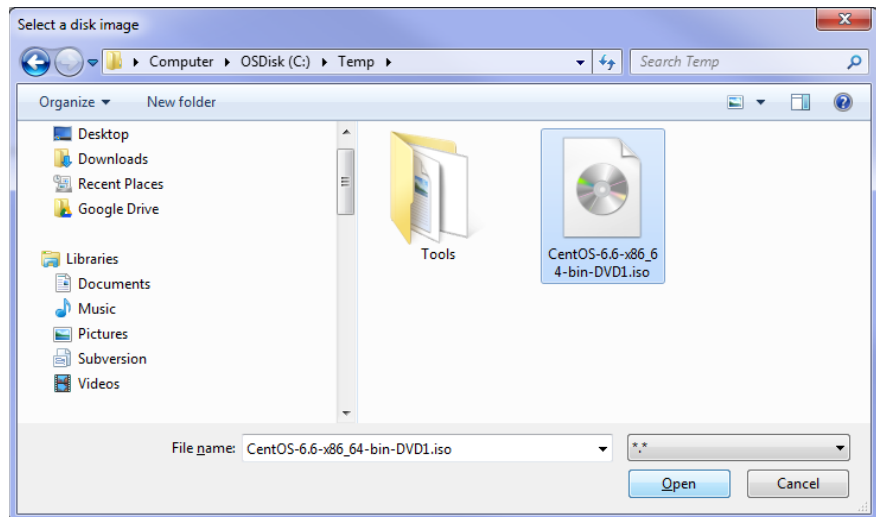
1. To create a USB flash drive with TaitCentOS or node controller software, first download and install the Win32DiskImager application.
- ① Only install the Tait supplied TaitCentOS version (i.e. not a commercial CentOS package), to ensure that the correct configuration settings are installed.
2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (TaitCentOS will require at least an 8GB flash drive, and for the node controller application 1GB or greater is required.)
3. Run the Win32DiskImager program.



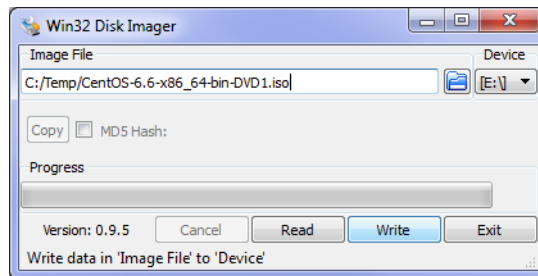
4. Check that the drive letter in the `Device` drop down list is the same as the USB flash drive. If you get this wrong, you could erase the wrong disk.
5. Click on the folder icon for the Image file.
6. Change the file filter from `Disk Images (*.img *.IMG)` to `*.*`



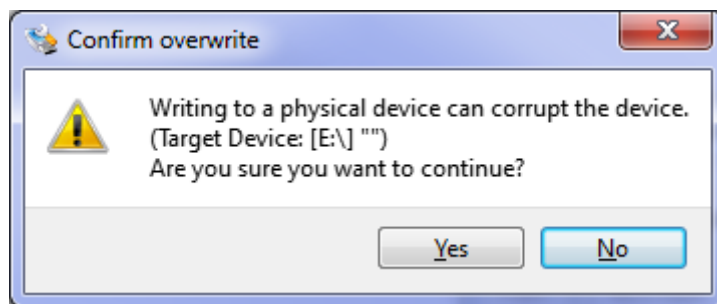
7. Select the desired iso file and click Open.



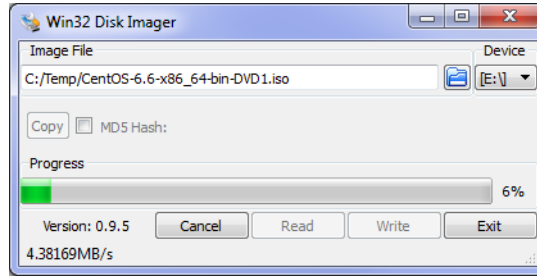
8. When ready to proceed, click Write.



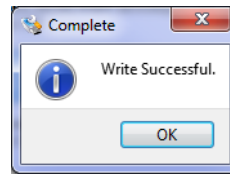
9. A Confirm overwrite dialog will appear which gives you a last chance to abort the process. Click Yes to continue.



10. The writing to the USB flash drive will begin and, depending on the quality/speed of the USB flash drive, this could take some time.



11. When the write has completed, a completion dialog will appear. Click OK.



12. Close the Win32DiskImager program.
13. Eject the USB flash drive by clicking the Safely Remove Hardware and Remove Media icon in the notification area, then clicking on the USB flash drive device.
14. Remove the USB flash drive from the PC.

# Appendix 2: Ethernet Bonding on TaitCentOS 7 DMR Networks

---

Support for Dual Ethernet connections via Ethernet bonding allows for provision of redundancy in case of an Ethernet switch failure or link failure, as the DMR node may connect to two independent switches.

Two interfaces may be configured to be part of one bond. This bond will have a single IP address which will be active on one of the two interfaces.

If the interface which has the active IP address fails, the other interface in the bond will become active and take over use of that IP address.

In the link based mode, the operating system monitors the link status between the NIC and the switch, and will react to changes in the link status. A failure of this link status will cause a failover to the second interface.


Ethernet Bonding is a standard feature of CentOS 7.

## A.1 Hardware Platform

Kontron CG2400 with PCI NIC card.

## A.2 Supported Redundant Configuration

Only link based configuration is supported for use with the Tait TN9300 DMR Node. When redundant operation is required, there will typically be multiple DMR node controllers specified to provide redundancy. Internode communication does not allow for node IP addresses to change during normal system operation.

 Testing performed with the Tait DMR node has been limited to the use of only two ports in a group/bond.

## A.3 Implementation

### A.3.1 Requirements

The Kontron CG2400 server should already have the operating system installed, and the DMR node installed and functional.

A valid and correct IP address and IP network configuration is required before beginning to configure IPMP or Ethernet bonding.

Root access is required for all configuration steps.

Console access via ILOM redirection is strongly recommended as the Ethernet interface may not be functional during configuration.

Both Ethernet port 0 and 1 should be connected to independent Ethernet switches.

### A.3.2 Switch Configuration


Ideally the Ethernet switch should activate the port very quickly, to minimise interruption when failover occurs. Failover can occur quickly enough that service interruption is minimal.

If using a Cisco switch, consider enabling portfast mode for the Spanning Tree configuration.


**Example:**

```
2960XL#configure terminal
2960XL(config)#interface fastethernet 0/12
2960XL(config-if)#spanning-tree portfast
2960XL(config-if)#end
2960XL#wr
```

### A.3.3 Enabling Ethernet Bonding

 Changing the node's IP address via the Administration Application WebUI does not work when bonding is enabled.

1. At the command line enter **ipconfig -a** and note the interface names for the bonding. In the example below, `enp1s0f0` and `enp1s0f1` will be used, along with mode `active-backup`.
2. Log in as root user and enter the commands as per the example below.

 Options for the mode below are:

- `802.ad`
- `balance-alb`
- `balance-tlb`
- `broadcast`
- `active-backup`
- `balance-rr`
- `balance-xor`

Tait uses either `802.ad` (LACP) or `active-backup`.

## Example

```
nmcli con add type bond ifname bond0 bond.options
"mode=active-backup,downdelay=5,miimon=100,updelay=10"
nmcli con add type ethernet ifname enpls0f0 master bond0
nmcli con add type ethernet ifname enpls0f1 master bond0
nmcli con mod bond-bond0 ipv4.method manual
ipv4.address 172.26.22.176/24 ipv4.gateway
172.26.22.254
nmcli con up bond-bond0
nmcli con up bond-slave-enpls0f0
nmcli con up bond-slave-enpls0f1
```

1. Edit `tait_dmrnc.cfg` to make `network_device: bond0` then restart the Node.

## A.3.4 Checking Ethernet Bonding

To run checks that ethernet bonding is set up correctly, enter the commands below. In the examples given, it is assumed that the Server IP address is 172.26.22.176, and the active IP address is 172.26.22.177.

```
[root@Kontron taitnet]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enpls0f0: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP>
mtu 1500 qdisc mq master bond0 state UP group default
qlen 1000
link/ether 00:1e:67:fc:80:d6 brd ff:ff:ff:ff:ff:ff
3: enpls0f1: <NO-CARRIER,BROADCAST,MULTICAST,SLAVE,UP>
mtu 1500 qdisc mq master bond0 state DOWN group default
qlen 1000
link/ether 00:1e:67:fc:80:d6 brd ff:ff:ff:ff:ff:ff
4: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu
1500 qdisc noqueue state UP group default qlen 1000
link/ether 00:1e:67:fc:80:d6 brd ff:ff:ff:ff:ff:ff
inet 172.26.22.176/24 brd 172.26.22.255 scope global
noprofixroute bond0
valid_lft forever preferred_lft forever
inet 172.26.22.177/24 scope global secondary bond0:1
valid_lft forever preferred_lft forever
inet6 fe80::8b65:dc79:9e59:6bbf/64 scope link
noprofixroute
valid_lft forever preferred_lft forever
```

Or:

```
[root@Kontron dmrnc]# nmcli con
NAME UUID TYPE DEVICE
bond-bond0 412f652b-397a-4a16-a667-f4dba888f824 bond
bond0
```

```
bond-slave-enpls0f0 81122bce-cee5-4f1d-bf88-  
fec5ade99f29 ethernet enpls0f0  
bond-slave-enpls0f1 6d04b3eb-66a0-4794-bdf4-  
22bd0f46e801 ethernet enpls0f1  
enpls0f0 a3a12b82-c951-4fc3-92ae-23af961b6c88 ethernet  
-  
Wired connection 1 ef67e414-25e1-3cc9-bdb5-a2b5ead8d8e9  
ethernet -
```

### A.3.5 Removing Ethernet Bonding

To remove ethernet bonding, enter the following commands:

```
nmcli con del bond-bond0 bond-slave-enpls0f0 bond-slave-  
enpls0f1  
ip link delete dev bond0
```