

# Tait TN9500 Inter-Network Gateway

## Installation and Configuration Manual

MNB-00008-11 · Issue 11 · September 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 manual is the property of Tait International Limited. All rights reserved. This manual 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 words TAIT, TAITNET and the TAIT logo are registered 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>6</b>
Scope of Manual .....	6
Document Conventions .....	6
Associated Documents .....	7
Publication Record .....	8
<b>1 Introduction</b> .....	<b>10</b>
1.1 TN9500 Inter-Network Gateway and Network Linking .....	10
1.2 TN9500 Inter-Network Gateway and Migration .....	10
1.3 Maximum Capability .....	10
1.4 Overview .....	11
1.4.1 Installation and Operation .....	11
1.4.2 Maintenance and Monitoring .....	11
<b>2 Operating the TN9500 Inter-Network Gateway</b> .....	<b>13</b>
2.1 Logging on to the TN9500 Inter-Network Gateway Using SSH .....	13
2.1.1 Logging into a Container Using SSH (Tait Ubuntu only) .....	13
2.2 Logging on to the TN9500 Inter-Network Gateway as ‘root’ .....	14
2.2.1 TaitCentOS Users .....	14
2.2.2 Tait Ubuntu Users .....	14
2.3 Logging on to the TN9500 Inter-Network Gateway WebUI .....	15
2.3.1 From the WebUI Home Page .....	15
2.3.2 From the TaitNet Administration Application .....	16
2.4 Installing License Files .....	16
2.4.1 Checking That the License File is Correct .....	16
2.4.2 Obtaining the Hostid .....	17
2.4.3 Obtaining the license.dat File .....	17
2.4.4 Installing the TN9500 Inter-Network Gateway’s License File .....	17
2.4.5 Licensed Features .....	17
2.5 Self-Signed SSL Certificates .....	19
2.5.1 Firefox Users .....	19
2.5.2 Chrome Users .....	21
2.5.3 Internet Explorer and Microsoft Edge Users .....	21
2.6 Using the Certificate from a Certification Authority (CA) .....	22
2.7 Changing Passwords .....	22
2.7.1 Changing the ‘root’ and ‘taitnet’ Passwords .....	22
2.7.2 Changing the iDRAC Password .....	23
2.8 Performing an Operating System Restart .....	23

2.9	Stopping/Starting the TN9500 Inter-Network Gateway Software .....	24
2.10	Powering Down the TN9500 Inter-Network Gateway .....	25
2.11	Changing to a Local Time Zone .....	25
<b>3</b>	<b>Basic Configuration.....</b>	<b>26</b>
3.1	Network Time Protocol (NTP) .....	26
3.2	SNMP .....	26
3.3	Syslog .....	27
3.4	E1/T1 .....	27
3.4.1	E1/T1 Troubleshooting .....	28
3.4.2	Configuring the Digium Card for E1 or T1 Use .....	29
3.4.3	Loopback Dongles for Unused Spans .....	29
3.5	a-law/ $\mu$ -law Companding Algorithm .....	30
3.6	Users .....	31
3.6.1	Centralized Authentication .....	31
3.6.2	Local Users .....	31
3.7	Linking Multiple MPT-IP/DMR Trunked Networks .....	32
3.7.1	Node Configuration Overview .....	32
3.7.2	MPT-IP/DMR Control Node Configuration .....	32
3.7.3	TN9500 Gateway Configuration .....	33
3.7.4	Forwarding Group Calls .....	33
3.8	External Sites .....	35
3.8.1	External Site Overview .....	36
3.8.2	Configuration Procedure .....	37
3.9	High Availability .....	41
3.9.1	Tait Ubuntu Requirements .....	41
3.9.2	Tait Ubuntu Configuration Procedure .....	41
3.9.3	Tait CentOS Requirements .....	42
3.9.4	TaitCentOS Configuration Procedure .....	42
3.9.5	Additional Information .....	43
3.10	PTToX Connector Configuration .....	47
<b>4</b>	<b>Backing up/Restoring Configuration Files .....</b>	<b>48</b>
4.1	Manual backup .....	48
4.2	Restoring .....	48
<b>5</b>	<b>TN9500 Inter-Network Gateway Information .....</b>	<b>50</b>
5.1	IP Protocols and Default Ports .....	50
5.1.1	IP Protocols .....	50
5.1.2	IP Default Ports .....	51
5.1.3	QoS/DSCP .....	53
5.2	System Events and Alarms .....	53

5.2.1	System Events . . . . .	53
5.2.2	Alarm Types . . . . .	54
5.3	Registration Records . . . . .	55
5.4	TN9500 Inter-Network Gateway Call Records. . . . .	57
5.4.1	Call Records File Format . . . . .	57
5.4.2	Call Types . . . . .	59
5.4.3	Call End Reasons . . . . .	60
5.4.4	Call Close Reasons . . . . .	61
5.4.5	Call Handler IDs . . . . .	63
5.5	TN9500 Inter-Network Gateway Status Monitoring. . . . .	63
5.6	Log Files . . . . .	64
5.6.1	Installation and Upgrade Logs . . . . .	64
<b>Appendix 1 . . . . .</b>		<b>67</b>
A.1	Transferring an ISO Image to a USB Flash Drive . . . . .	67
A.1.1	Using Rufus for TaitCentOS . . . . .	67
A.1.2	Using Rufus for Tait Ubuntu. . . . .	70
A.1.3	Using dd for Tait Ubuntu on Linux. . . . .	71
A.1.4	Using Win32DiskImager (TaitCentOS Only). . . . .	71
<b>Appendix 2 . . . . .</b>		<b>75</b>
B.1	Deploying PTTToX in a DMR Trunked Network. . . . .	75
B.1.1	TN9300 DMR Trunked Node Controller Configuration . . . . .	75
B.1.2	Install TN9500 and PTTToX Connector Applications . . . . .	76
B.1.3	Administration Application Configuration . . . . .	76
B.1.4	Tait PTTToX Connector Configuration. . . . .	77
B.1.5	TN9500 Configuration . . . . .	77

# Preface

---

## Scope of Manual

This Tait TN9500 Inter-Network Gateway Installation and Configuration Manual provides installation, configuration and monitoring information for the Tait Inter-Network Gateway, also known as the TN9500 gateway, or TN9500.

## 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 is 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	MPT	MPT-IP	DMR
TaitNet MPT1327 System Manual	MNA-00019	✓		
T1541 Installation Manual	MNA-00007	✓		
T1541 Operations Manual	MNA-00008	✓		
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		✓	✓
Tait Core Networks Installation and Configuration Manual	MNB-00012		✓	✓
Tait TN9300 DMR Trunked System Manual	MNB-00003			✓
Migrating TaitNet MPT Networks using the TN9500 System Manual	MNB-00009	✓	✓	✓
Tait TN9500 Inter-Network Gateway Installation and Configuration Manual	MNB-00008	✓	✓	✓

Technical Notes are also published from time to time on the Tait Partner Portal 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
11	September 2023	Updated for TN9500 release 1.24 and later <ul style="list-style-type: none"> <li>■ <a href="#">G.711 Connector</a> licenses updated</li> </ul>
10	June 2023	Updated for TN9500 release 1.22 and later <ul style="list-style-type: none"> <li>■ <a href="#">G.711 Connector</a> now supports HA</li> </ul>
9	December 2022	Updated for TN9500 release 1.20 and later <ul style="list-style-type: none"> <li>■ Dell R250 replaces the R240 throughout</li> <li>■ Sintrones SBOX-2621 replaces the SBOX-2620 throughout</li> <li>■ Tait Ubuntu information added throughout</li> <li>■ <a href="#">Section 1.2 TN9500 Inter-Network Gateway and Migration</a> updated</li> <li>■ <a href="#">Section 1.3 Maximum Capability</a> updated</li> <li>■ <a href="#">Section 3.7 Linking Multiple MPT-IP/DMR Trunked Networks</a> updated</li> </ul>
8	December 2021	Updated for TN9500 release 1.18 and later <ul style="list-style-type: none"> <li>■ PTTToX connector removed from TN9500 installation package</li> <li>■ <a href="#">Section 1.3 Maximum Capability</a> updated</li> <li>■ G.711 connector licenses added to <a href="#">Section 2.4.5 Licensed Features</a></li> </ul>
7	June 2021	Updated for TN9500 release 1.16 and later <ul style="list-style-type: none"> <li>■ <a href="#">Section 2.2 Configuring BIOS and iDRAC Settings</a> updated</li> <li>■ Footnote added to <a href="#">Section 2.1 Installation</a></li> <li>■ PTTToX added to <a href="#">Section 2.4.5 Licensed Features</a></li> <li>■ <a href="#">Section 3.10 PTTToX Connector Configuration</a> updated</li> <li>■ <a href="#">Appendix 2 Deploying PTTToX in a DMR Trunked Network</a> added</li> </ul>
6	December 2020	Updated for TN9500 release 1.14 and later <ul style="list-style-type: none"> <li>■ <a href="#">Section 3.9 High Availability</a> updated</li> <li>■ <a href="#">Section 3.10 PTTToX Connector Configuration</a> added</li> <li>■ <a href="#">Section 5.4.1 Call Records File Format</a> updated</li> </ul>



Version	Publication date	Amended sections and pages
5	September 2020	<p>Updated for TN9500 release 1.12 and later</p> <ul style="list-style-type: none"> <li>■ Updated for the Dell R240</li> <li>■ <a href="#">Section 2.3 Installing TaitCentOS for the First Time</a> updated to include TaitCentOS 7</li> <li>■ <a href="#">Section 2.4 Changing the Default IP Address Using the Network Configuration Tool</a> updated to include TaitCentOS 7</li> <li>■ <a href="#">Section 2.4.4 Installing the TN9500 Inter-Network Gateway's License File</a> updated</li> <li>■ <a href="#">Section 2.11 Changing to a Local Time Zone</a> updated</li> <li>■ <a href="#">Section 3.7.2 MPT-IP/DMR Control Node Configuration</a> updated</li> <li>■ <a href="#">Section 3.7.3 TN9500 Gateway Configuration</a> updated</li> <li>■ <a href="#">Section 5.1.3 QoS/DSCP</a> added</li> </ul>
4	May 2019	<p>Updated for TN9500 release 1.08 and later</p> <ul style="list-style-type: none"> <li>■ <a href="#">Section 1.3 Maximum Capability</a> added</li> <li>■ <a href="#">Section 2.1.2 Equipment Required</a> updated</li> <li>■ <a href="#">Section 2.3 Installing TaitCentOS for the First Time</a> updated</li> <li>■ <a href="#">Section 3.4 E1/T1</a> updated</li> <li>■ <a href="#">Section 3.7.4 Forwarding Group Calls</a> updated</li> <li>■ Instructions for changing the Valiant IP address added to <a href="#">Section 3.9.3 Additional Information</a></li> <li>■ SNMP monitoring added to <a href="#">Section 3.9.3 Additional Information</a></li> </ul>
3	September 2018	<p>Updated for TN9500 release 1.06 and later</p> <ul style="list-style-type: none"> <li>■ <a href="#">Section 3.4 E1/T1</a> updated</li> <li>■ <a href="#">Section 3.8 External Sites</a> added</li> <li>■ <a href="#">Section 3.9.3 Additional Information</a> updated</li> </ul>
2	December 2017	Updated for release 1.04 and later
01	March 2017	First release for TN9500 gateway v1.00

# 1 Introduction

---

## 1.1 TN9500 Inter-Network Gateway and Network Linking

The TN9500 gateway can be used to create DMR trunked or MPT-IP wide area networks by linking together networks of the same type.

See [Section 3.7 Linking Multiple MPT-IP/DMR Trunked Networks](#) for further information.

## 1.2 TN9500 Inter-Network Gateway and Migration

Tait has designed a migration strategy for those network users that would like to replace their analog networks with enhanced capacity IP-based digital networks without losing connectivity during the migration process.

The TN9500 gateway is capable of connecting multiple combinations of networks (TaitNet MPT, TaitNet MPT-IP and Tait TN9300 DMR trunked) together, allowing calls to be made seamlessly between the different networks. Only one TN9500 gateway is required for migration.

- ⓘ The TN9500 gateway running on the Tait Ubuntu operating system does not support connections to TaitNet MPT networks.

## 1.3 Maximum Capability

- ⓘ A maximum of five networks (or four nodes and a PTTToX Connector) can be connected together by a single TN9500 gateway.

The TN9500 gateway can support a maximum of one hundred concurrent talk paths.

This means that if for example, a TN9500 gateway is used to link five networks together, and all of the networks will be included in a call, then the maximum number of concurrent calls that can take place is twenty (5 networks x 20 calls = 100 talk paths).

At this highest usage rate, call performance cannot be guaranteed.

- ⓘ The TN9500 gateway subscriber limit is 5000.

## 1.4 Overview

This manual describes the full installation and operation process of the TN9500 as listed below, followed by maintenance and monitoring information.

### 1.4.1 Installation and Operation

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

1. Configuring the servers for their BIOS and iDRAC monitoring and troubleshooting access (refer to ‘Section 2 BIOS and iDRAC Settings’ of the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx)).
2. Installing the operating system (TaitCentOS or Tait Ubuntu) and the Tait Administration application (refer to ‘Section 5 Installing TaitCentOS’ or ‘Section 6 Installing Tait Ubuntu’ of the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx)).
3. Installing the TN9500 gateway application from the administration application (refer to ‘Section 8 Installing the Tait Packages Using TaitCentOS’ or ‘Section 9 Installing the Tait Packages Using Tait Ubuntu’ of the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx)).
4. Configuring security features, such as the access banner (refer to ‘Section 10.4 Creating Your Custom’ssh’ Login Script’ of the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx)) and SSL certificate selection (section 2.5). (Additional IP setting information for the firewall is available in section 5.1.)
5. Accessing the TN9500 gateway interface (section 2.3).
6. Installing the TN9500 licenses to enable the required TN9500 gateway features (section 2.4).
7. Final configuration of the Tait radio networks to be linked (section 3).
8. At this stage, the TN9500 gateway is ready to be configured. Please use the online help to assist with configuring the TN9500 gateway via the web interface.

### 1.4.2 Maintenance and Monitoring

Maintenance and monitoring information can be found in the following sections:

- How to perform regular backups of the TN9500 gateway application and administration application (section 4). This section also explains restoring backups in case of an event.
- System event and alarm files can be used for monitoring and diagnostic


purposes (alarm types listed in section 5.2).

- Registration record files can be used for monitoring and diagnostic purposes (section 5.3).
- Call record files can be used for monitoring and diagnostic purposes (section 5.4).
- Log files can be used for monitoring and diagnostic purposes (section 5.6).

# 2 Operating the TN9500 Inter-Network Gateway

---

The TN9500 gateway can run on the TaitCentOS or Tait Ubuntu operating systems. This chapter tells you how to carry out basic maintenance and operational tasks by logging onto the TN9500 gateway and using the operating system's command line interface and/or WebUI.

 The TN9500 gateway running on the Tait Ubuntu operating system does not support connections to TaitNet MPT networks.

## 2.1 Logging on to the TN9500 Inter-Network Gateway Using SSH

You can connect to the TN9500 gateway using an SSH terminal application.

1. Use an SSH terminal application to connect to the IP address of the TN9500 gateway.

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.

You should now be logged on to the TN9500 gateway using the default command shell (`bash`).

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

### 2.1.1 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	IMAGE	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	"/entrypoint.sh 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 the TN9500 Inter-Network container, enter:  

```
docker exec -it tait_ing bash
```
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 ing
```

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.

## 2.2 Logging on to the TN9500 Inter-Network Gateway as 'root'

### 2.2.1 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 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.

### 2.2.2 Tait Ubuntu Users

1. Logon as user `taitnet` as described in Section 2.1 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
```


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

## 2.3 Logging on to the TN9500 Inter-Network Gateway WebUI

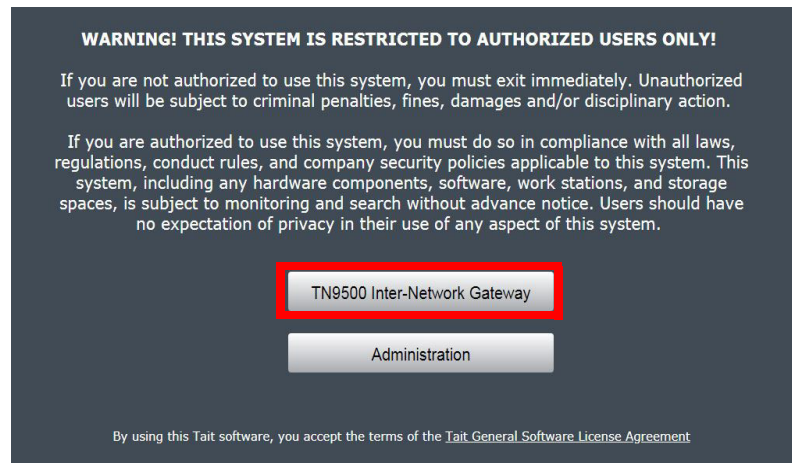
### 2.3.1 From the WebUI Home Page

1. Open the PC browser and enter the IP address of the TN9500 gateway.

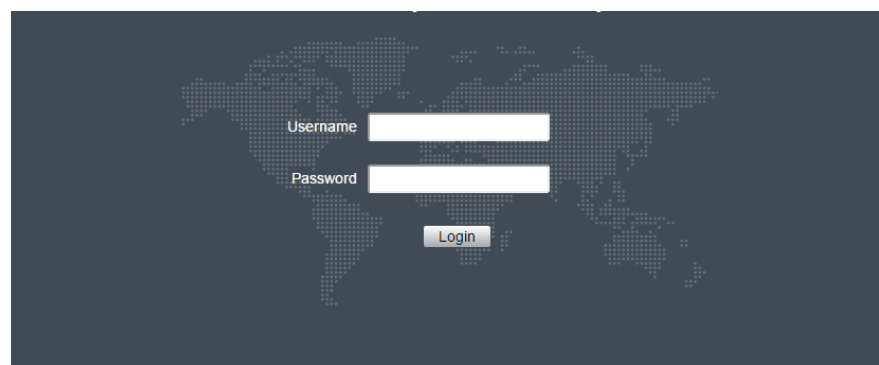
 The TN9500 uses secure HTTP by default (HTTPS). You may need to prepend your IP address with HTTPS:// in your browser to access the WebUI.

 In case of proxy errors, refer to the 'Migrating TaitNet MPT Networks using the TN9500 System Manual' (MNB-00009) for information on IP ports.

2. Tait Ubuntu users - go to the next step.  
TaitCentOS users only - select TN9500 Inter-Network Gateway.

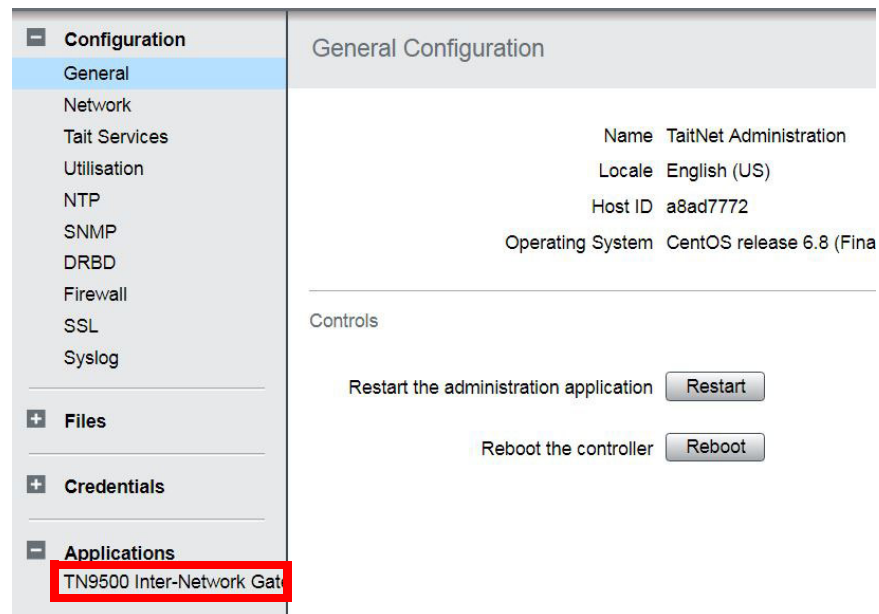


3. Log in using `taidnet` as the username and `taid` as the password.



## 2.3.2 From the TaitNet Administration Application

1. Select Applications > TN9500 Inter-Network Gateway from the menu.



## 2.4 Installing License Files

A TN9500 gateway must have a valid license file installed before it can operate.

License files can only be generated by Tait and each TN9500 gateway must have its own unique license. If the TN9500 gateway has been set up by Tait then an appropriate license file will have been installed.

### 2.4.1 Checking That the License File is Correct

1. On the TN9500 Inter-Network gateway WebUI, select Settings > License to display license information.
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 TN9500 gateway from scratch, a new license file will be required.

To get a license file, Tait must be supplied with the hostid of the server that the TN9500 gateway will be installed on (see below), and a list of the features required (see [Section 2.4.5 Licensed Features](#)).



## 2.4.2 Obtaining the Hostid

A license request file, which contains the hostid, can be downloaded via a link on the Settings > License page in the TN9500 gateway WebUI.

The hostid can also be found on the Configuration > General page in the Administration application WebUI.

## 2.4.3 Obtaining the `license.dat` File

Once you have provided the hostid and required features to Tait, you will be provided a license file called `license.dat` for the TN9500 gateway.

If you are getting multiple licenses, you may combine the license files into one file that can be installed on all the TN9500 gateways. 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 TN9500 gateway will only use the line in the license information that matches its hostid.

## 2.4.4 Installing the TN9500 Inter-Network Gateway's License File

1. On the TN9500 gateway WebUI, select Settings > License then click Upload.
2. Click Choose File, then navigate to the license file, select it and click Open.
3. Once the license file has uploaded, the TN9500 gateway will check if the license is valid.

You can also manually copy the license file to the TN9500 gateway application directory (`/home/taitnet/ing`) on the TN9500 gateway by using SCP. We do not recommend this. If you do manually upload the license file, you will need to restart the TN9500 gateway.

## 2.4.5 Licensed Features

The TN9500 can be licensed for the following features:

License Code	License Type	Notes
TNAS701	TaitNet MPT-IP, TN9300 DMR or PTTToX Inter Node connection license <sup>1</sup>	One per network required
TNAS702	TaitNet MPT Inter Node connection license	One required for each T1541 node in the MPT network

License Code	License Type	Notes
TNAS703	TN9500 with High Availability (HA)	A second gateway can be installed as a standby that can take over if the primary gateway fails. One license required per gateway.
TNAS704	Transcoding block of 1 license	For transcoding from G711 (MPT) to AMBE (DMR) <sup>2</sup> .  A license is required for each simultaneous call required, i.e. two TNAS704 licenses plus two TNAS705 licenses enables up to 42 calls at a time.
TNAS705	Transcoding block of 20 licenses	

1. Note that PTTToX inter node connections are only supported for single DMR networks. PTTToX to MPT-IP or TaitNet MPT is not supported.
2. When transcoders are used for calls between an MPT (TaitNet MPT or TaitNet MPT-IP) network and a Tait DMR network, if the licensed limit is reached and new calls are made, the TN9500 will queue the calls until a licensed transcoder is available. It is important to buy the correct number of transcoding licenses to avoid unnecessary call delays.

## G.711 Connector

The G.711 connector is licensed for the following features:

License Code	License Type
TNAS800	G.711 transcoder license (quantities vary from 1 to 100)
TNAS801	High availability option
TNAS802 <sup>1</sup>	Non-AMBE connections

1. If this feature is enabled, the maximum number of Non-AMBE connections allowed is 100 less the number of TNAS800 licenses.

The G.711 connector application can be co-located on a TN9300 node, a TN8291 node, or a TN9500 server:

- If co-located on the TN9500, the total number of transcoders allowed depends on the other functions operating on the platform:
  - TNAS800 can be a maximum of 100 or
  - TNAS800 + TNAS704 + TNAS705 can be a maximum of 100
- If co-located on the TN9300 or TN8291, TNAS800 can be a maximum of 100

## 2.5 Self-Signed SSL Certificates

When your browser connects to the TN9500 gateway's WebUI 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.

The TN9500 gateway creates a self-signed certificate when the TN9500 gateway or its 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.

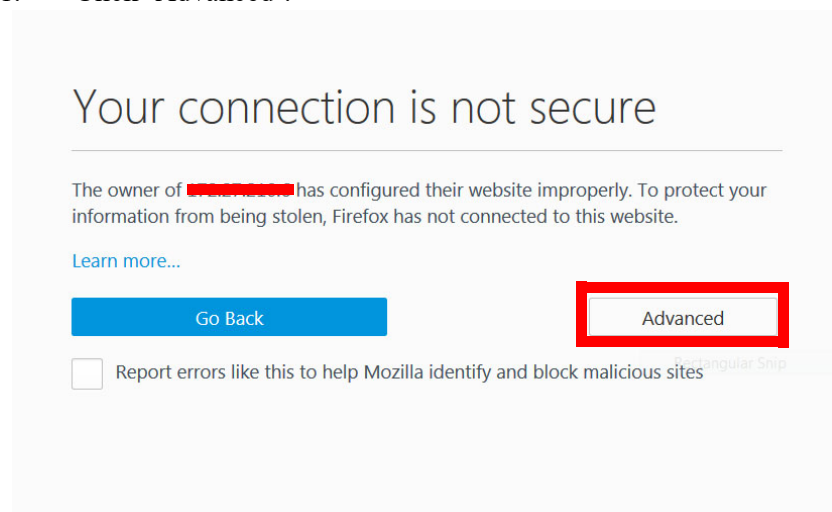
You can be confident that you are not connecting to a rogue website pretending to be your TN9500 gateway, so follow the procedure below to tell the browser that the security certificate is OK. The browser then stores the security certificate and will not raise a warning on subsequent connections, unless the IP address of the TN9500 gateway changes. If the TN9500 gateway's IP address is changed, simply repeat the certification procedure.

For more information, refer to <http://support.microsoft.com/kb/931850> or search for "security certificate" in your browser's Help.

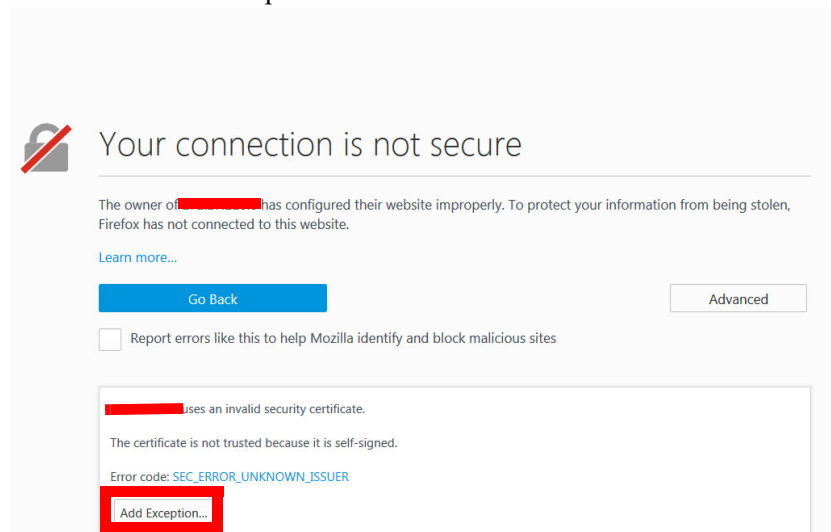
### 2.5.1 Firefox Users

If Firefox is used, the following window appears when the user tries to access the TN9500 gateway WebUI for the first time:

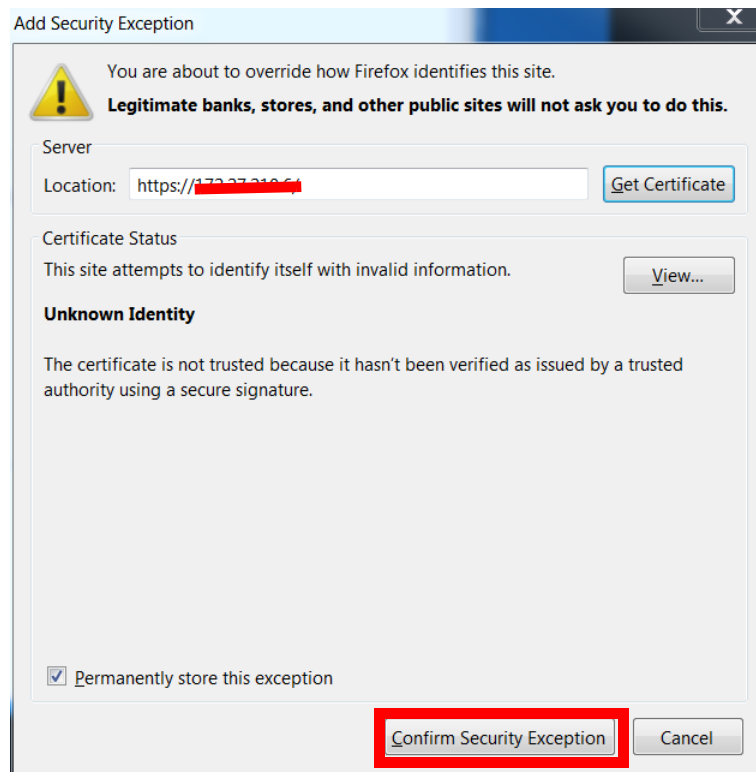
1. Click 'Advanced'.



2. Click 'Add Exception'.



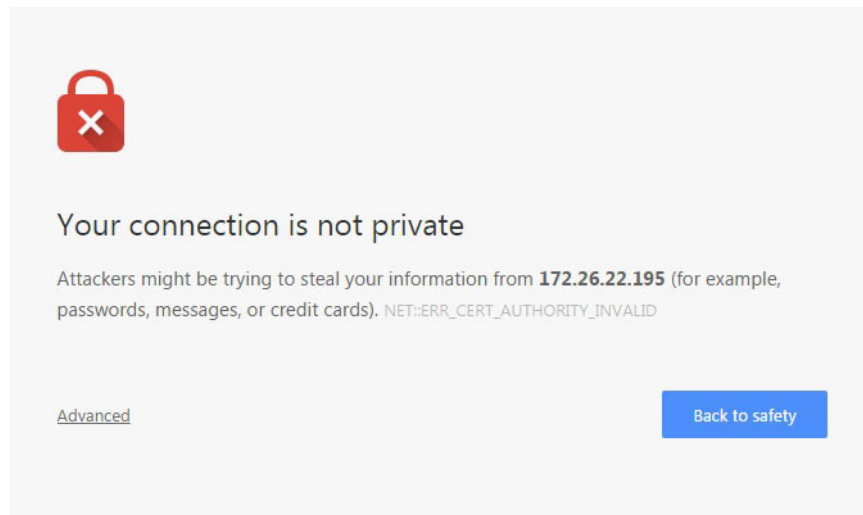
3. The Location field includes details specific to your TN9500 gateway. Without changing the default values, click 'Confirm Security Exception'.




4. A secure connection to the TN9500 gateway WebUI will be enabled in the browser.

## 2.5.2 Chrome Users

If Chrome is used, the following window appears when the user tries to access the TN9500 gateway WebUI for the first time:



1. Click on Advanced.
2. Click on Proceed to <TN9500 gateway WebUI IP address> (Unsafe).
3. Click Continue and log on as normal.

 This is only a temporary solution, that has to be repeated each time the TN9500 gateway is accessed.

## 2.5.3 Internet Explorer and Microsoft Edge Users

The TN9500 WebUI does not support Internet Explorer or Microsoft Edge.

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

By default, the TN9500 gateway 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 WebUI. 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 TN9500 gateway 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.

## 2.7 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)
- taitnet: tait (on the node WebUI)
- iDRAC:
  - admin: K1w1k1w1

### 2.7.1 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 to know the passwords to provide support. If you change the passwords, please ensure that you do not forget them.

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.

## 2.7.2 Changing the iDRAC Password

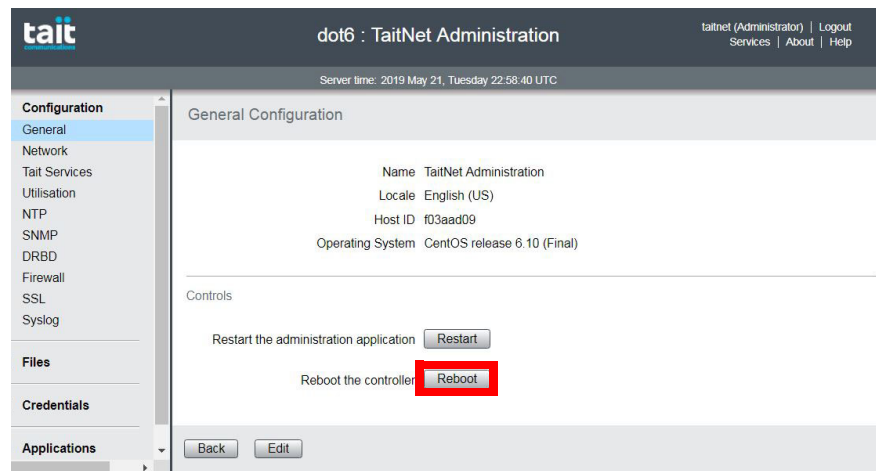
1. Connect a monitor, keyboard and mouse to the front of the Dell server.
2. Boot the server and wait for the Dell logo screen to appear during the early boot stages, then press the F2 key when 4 options appear in the top right corner of the Dell logo screen.  
After a period of approximately 1 minute, 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`.

## 2.8 Performing an Operating System Restart

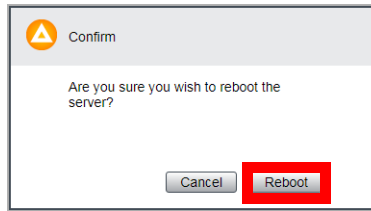
To perform a full reboot of the TN9500 gateway, login as root and enter the following:

```
reboot
```

Alternatively, log in to the Administration application's Configuration > General page, and click Reboot.



You will be asked to confirm the Reboot command.

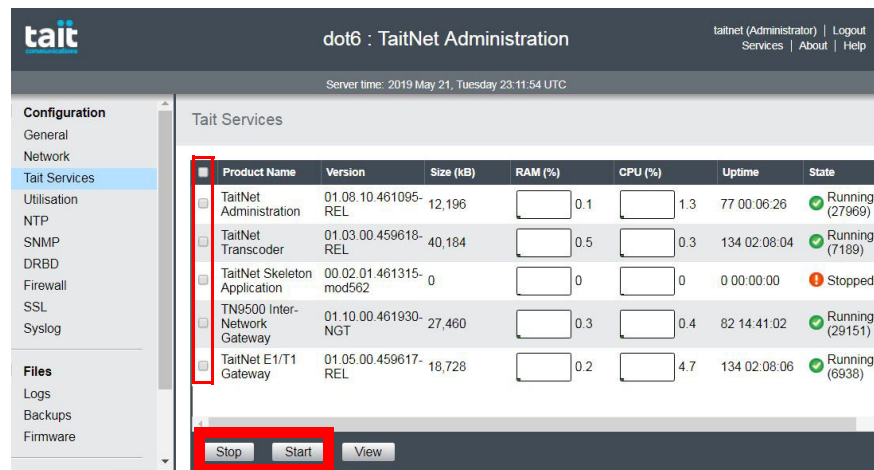


It can take up to 5 minutes for the TN9500 gateway to shut down and restart. The TN9500 gateway software will automatically start after the server reboots.

Connect to the WebUI to confirm the TN9500 gateway has started.

## 2.9 Stopping/Starting the TN9500 Inter-Network Gateway Software

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.



For TaitCentOS users, the following also applies:

Alternatively, you could login to the TN9500 gateway as root (see [Section 2.2 Logging on to the TN9500 Inter-Network Gateway as 'root'](#)). To stop the TN9500 gateway enter:

```
taitnet-services stop
```

To start the TN9500 gateway enter:

```
taitnet-services start
```

If the TN9500 gateway is running or the software is hung, you can restart it by entering:

```
taitnet-services restart
```



## 2.10 Powering Down the TN9500 Inter-Network Gateway



**The TN9500 gateway should always be powered down in a controlled fashion. You should always stop the TN9500 gateway software first, and you should never remove the power from the TN9500 gateway unless it is powered off.**

**Failure to follow this advice may lead to corrupt system files which will prevent the TN9500 gateway operating.**

You may need to power down the TN9500 gateway, 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 TN9500 gateway hardware, simply press the power button. The button is on the front panel of the Dell R250.
- If you are shutting the machine down remotely, ssh to the TN9500 gateway and switch to the root user. Enter the following:

```
poweroff
```

## 2.11 Changing to a Local Time Zone

- ① 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 WebUI without a UTC offset.

The one exception is the status bar that is always displayed across the top of the WebUI. It now has a time-date field in the middle that displays the current time and UTC offset of the TN9500 gateway in full date format as follows (for example):

```
Tuesday, 2014 February 11 12:51:57 UTC+00:00 (the  
TN9500 gateway local time is the same as UTC)
```

```
Tuesday, 2014 February 11 12:51:57 UTC+13:00 (the  
TN9500 gateway local time is 13 hours ahead of UTC)
```

## 3 Basic Configuration

---

The following basic configuration procedures are done from the TaitNet Administration application, and are indispensable to successful server and application operations.

### 3.1 Network Time Protocol (NTP)

1. Using a web browser, login to the Administration application (see the System Manual for details).
2. Select Configuration > NTP.
3. Select Edit.
4. Enter the IP addresses of up to three NTP servers.
5. Press Save.
6. Press Start to begin the NTP daemon service.
7. Pressing Synchronize will check the status of the synchronization of this server with at least one of the NTP servers specified.
8. Use the status area to monitor the state of the NTP service.

### 3.2 SNMP

The TN9500 gateway can be monitored via its own MIBs (e.g. status) and the 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, the TN9500 gateway can also use traps from DISMAN-EVENT-MIB (in particular `dismanEventMIBNotifications => mteTriggerFired` OID 1.3.6.1.2.1.88.2.0.1).

1. Using a web browser, login to the Administration application (see the System Manual for details).
2. Select Configuration > SNMP.
3. Select Edit.
4. Add or change the Read-only community string 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.

### 3.3 Syslog

1. Using a web browser, login to the Administration application (see the System Manual for details).
2. Select Configuration > Syslog.
3. Click Edit.
4. Enter the IP addresses of up to two external syslog collectors.
5. Select the protocol to use for the formatting of the syslog messages.
6. 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.

 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.

7. Click Save.


### 3.4 E1/T1

When used to connect to a TaitNet MPT network, the TN9500 gateway will need an E1/T1 card as part of its hardware configuration.

The E1/T1 card is the TE435F, manufactured by Digium. The manual for the card can be found at:

<https://www.digium.com/sites/digium/files/quad-span-digital-card-user-manual.pdf>

The Digium card is configured with default values (for example, a line length of 133 feet). Use the Digium manual to assist with making any changes. In addition, the card does not provide timing by default, as is usually expected in Tait networks.

 The Digium card is set to the following line coding and framing types by default:

- E1: HDB3 Line coding, CRC4 Framing type
- T1: B8ZS Line coding, ESF Framing type

- i** The following commands have to be used with caution. They should only be used if they are completely understood. They are generally only to be used when changing default parameters to load back into the card, or if the OS has been reinstalled, in which case the card will need to be reinitialised.

To perform the following procedures, first log on to the TN9500 server with root privileges.

1. To remove the driver from the kernel, enter the following:

```
service tait_e1_gateway stop
modprobe -r wcte43x
```

2. To add the driver back into the kernel, enter the following:

```
modprobe wcte43x
dahdi_cfg -vv
configure_e1 (or configure_t1)
service tait_e1_gateway start
```

- i** Although the service is named `tait_e1_gateway`, it is for both E1 and T1 operations.

3. The card now needs to be configured. Refer to [Section 3.4.2 Configuring the Digium Card for E1 or T1 Use](#) for configuration instructions.

### 3.4.1 E1/T1 Troubleshooting

If voice quality issues are perceived between the MPT-IP (or DMR) and the TaitNet MPT network, you may want to check that the Digium card has been synchronized with the DAS E1/T1 card.

To do this, use the following command on the TN9500 prompt when logged as root:

```
dahdi_test
```

The `dahdi_test` command is used to test if the DAHDI timer provides a timely response. It runs a timing test in a loop and prints the result of each loop. The test is as follows:


It reads 8192 bytes from the DAHDI timer device (`/dev/dahdi/pseudo`). This should take exactly 8000 ms. It uses calls to `gettimeofday(2)` before and after the read to check that exactly 8000ms have passed.

- Values of 100% and 99.99% Are considered a definite pass.
- Values of 99.98% and 99.97% are OK as well.
- Values <98% may infer that the card is faulty. Contact Tait for further information.

### 3.4.2 Configuring the Digium Card for E1 or T1 Use

The TN9500 gateway's Digium TE435F card, used for E1/T1 connection, must be configured according to card type:

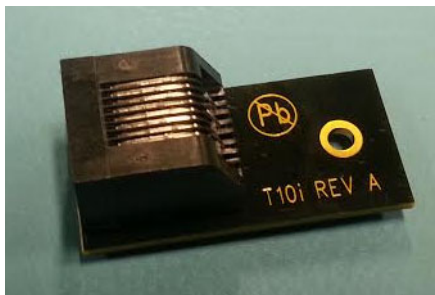
1. Log in to the TN9500 server with root privileges, using SSH (see [Section 2.2 Logging on to the TN9500 Inter-Network Gateway as 'root'](#)). (Note that the following commands work from any repository.)
2. To configure the Digium card for T1, enter:  
`#configure_t1`
3. Conversely, to configure the Digium card for E1, enter:  
`#configure_e1`

 The `configure_t1` and `configure_e1` commands will only work on a server that has the TN9500 gateway software installed (not just the Administration application).

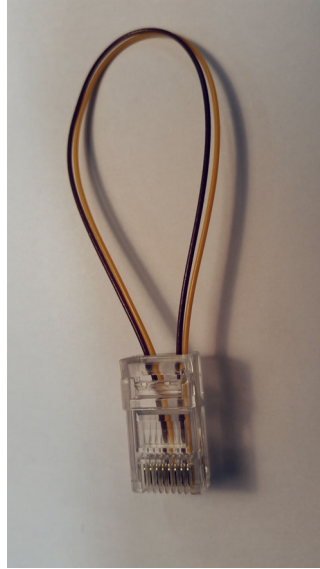
Running the `configure_t1` and `configure_e1` commands may produce some error messages related to modules being in use. This is normal if the E1/T1 gateway service is already running.

### 3.4.3 Loopback Dongles for Unused Spans

Any physical ports (spans) on the Digium card that are not going to be connected or used must be properly terminated with loopbacks to avoid spurious alarms. The TN9500 server is supplied with a Digium loopback dongle to be used when a port is not in use. See diagram below.



More loopback dongles can be made, if required as in the following diagram:



To make a loopback:


1. Connect pin 1 to pin 4.
2. Connect pin 2 to pin 5.

### 3.5 a-law/ $\mu$ -law Companding Algorithm

TaitNet MPT networks may be configured for a-law or  $\mu$ -law. This corresponds to the algorithm for digitizing the analog signals.

The TN9500 supports  $\mu$ -law by default, but can be configured for a-law by adding the following line to the `tait_e1_gateway.cfg` file (located in the `/home/taitnet/tait_e1_gateway` folder):

```
encoding.alaw_support: true
```

 The `tait_e1_gateway.cfg` file is for both E1 and T1 configurations.

If you are unsure if your MPT network is configured for a-law or  $\mu$ -law refer to the T1561 DAS Installation Manual.

## 3.6 Users

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 TN9500 gateway.

- ① It is recommended that local users should not be created if centralized authentication is used on your server.

### 3.6.1 Centralized 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.

- ① Any changes made to the authentication settings will result in all currently logged on remotely-authenticated users being logged out.
- ① If the RADIUS protocol is selected, the RADIUS configuration settings made in the Administration application will apply to the TN9500 gateway too. If the LDAP protocol is selected, LDAP configuration settings must be made in **both** the Administration application and the TN9500 gateway.


1. Log on to the Administration application.
2. Select Credentials > Authentication and click Edit.
3. Select LDAP or RADIUS as required from the Remote drop down menu.
4. Enter LDAP or RADIUS server details as required.
5. Click Save.
6. If the LDAP protocol is selected, log on the TN9500 gateway and follow steps 2 to 5.

### 3.6.2 Local Users

1. Log on to the Administration application.
2. Select Credentials > Users and click Add. (To add a user you must have the Administrator access level.)
3. 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: \* ' ' " \ ( ) & | ! = ~ < > , ;

4. 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.
5. Optionally enter a comment.
6. Select the appropriate access level for the user.

 Non-administrator users of other TaitNet applications only, such as the TN9500 gateway, should have their access level set to Disabled. It will be enabled from within the relevant TaitNet application.

## 3.7 Linking Multiple MPT-IP/DMR Trunked Networks

The TN9500 gateway can be used to link a maximum of up to five DMR trunked networks together, or four networks and a PTTToX Connector. This also applies to MPT-IP networks.


### 3.7.1 Node Configuration Overview

- Each node must be configured with the same fleet information, including the radios that are to operate across all the networks.
- Each node needs to be configured to use NTP (in Settings > Local Parameters).
- Start creating the sites and subscribers.

See the Online Help for the node and TM9300/TP9300 radio programming applications for configuration information.

### 3.7.2 MPT-IP/DMR Control Node Configuration

1. On the MPT-IP/DMR control node, select Interfaces > Inter-network Connections and click Add.
2. Enter a name for the new connection (e.g. TN9500).
3. Enter a username and password of your choice.
4. Enable the 'Invite without SDP' parameter if the MPT-IP/DMR controller is v3.34 or later, and will use the reliable provisional scheme. This scheme can be used for synchronizing calls set up in TN9500 gateway-connected networks.


 For this feature to work, it must also be enabled on the TN9500 gateway.

5. Click Save.




### 3.7.3 TN9500 Gateway Configuration

1. Log on to the TN9500 gateway WebUI.
2. Select Networks > Connections and click Add.
3. Create a network connection using the same username and password as in Step 3 above.
4. Create a list of the network nodes in order of priority, starting with the control node, or for those HA systems utilizing an active IP address, add only the active node IP address.
5. Enable the 'Invite without SDP' parameter if the MPT-IP/DMR controller is v3.34 or later, and will use the reliable provisional scheme. This scheme can be used for synchronizing calls set up in TN9500 gateway-connected networks.

 For this feature to work, it must also be enabled on the relevant MPT-IP/DMR controllers.

6. Click Save.
7. The new connection should be displayed with a status of OK.

 After the connection has been established, the TN9500 gateway and the respective nodes need to be synchronized. This is done automatically, and may take up to 15 minutes. It is recommended that the system not be used during synchronization. The TN9500 gateway will display Synchronizing in the status bar (below the page header). Calls may fail during this period.

Tait recommends that the MPT-IP/DMR network be tested in isolation before connecting it to another via the TN9500 gateway in order to verify that it is operating correctly (e.g. using the correct IP bandwidth allocations, as documented in the Migrating TaitNet MPT Networks using the TN9500 System Manual).

From the radios' perspective, the dialing scheme chosen must be the same as the dialing scheme of the network. The network type on the TM9300/TP9300 radio must be DMR/MPT (Trunked Features > Network Settings > Trunked Networks).

### 3.7.4 Forwarding Group Calls

For group calls to be forwarded to the TN9500:

1. Log on to the MPT-IP/DMR controller, select Subscribers > Group Service Area and then click Add.
2. Enter a name and optionally a comment about the group service area.

3. In the Service Area table, select one or more sites (on the current controller) and then use the Service drop down list at the bottom of the table to select the type of group call service that the selected site(s) will provide. See Viewing or Editing a Group Service Area for details about the service options.
4. In the Service Network table, select one or more external connected networks and then use the Service drop down list at the bottom of the table to select Allowed so that group calls will be allowed at the external network if a channel is available there.
5. Click Save.

Example:

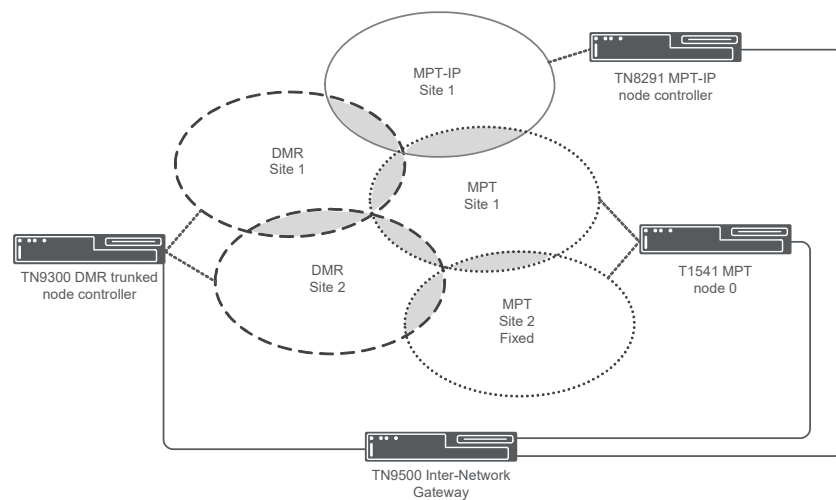
- Node 1 and Node 2 are connected via the TN9500 gateway.
- Group GA is set up on both Node 1 and Node 2
  - On both nodes, GA is configured to use a group service area that lists the other node in the Service Networks table with Allowed as the service type.
- Group GB is set up on both Node 1 and Node 2
  - On both nodes, GB is configured to use a group service area that lists the other node in the Service Networks table with Not Allowed as the service type.
- Two radios, U1 and U2, are both configured to belong to both group GA and GB.
- When radios U1 and U2 are registered on Node 2:
  - If a radio on Node 1 makes a call to group GA, the call is forwarded through the TN9500, and radios U1 and U2 will receive it.
  - If a radio on Node 1 makes a call to group GB, the call is not forwarded through the TN9500, so radios U1 and U2 will not receive it.

## 3.8 External Sites

There are three types of adjacent site, of which two are external:

- Local - the site belongs to the same network
- External inter-network - the site belongs to another network, and is updated dynamically as it may have dual control channels or rotating control channels. Also recommended to be used to mitigate channel failures at remote network sites.
- External fixed - the site belongs to another network, and has a fixed control channel RF number and syscode, or it is a cell extender site

Setting up external sites will involve configuring them on your TN9500 Inter-Network Gateway, and the networks that are connected through the gateway, be they DMR networks, MPT-IP or TaitNet MPT networks.



In this diagram, the following configurations are required:

- MPT-IP node controller:
  - The MPT-IP Site 1 Adjacent Sites table would have two entries:
    - DMR Site 1 configured as an external inter-network site
    - MPT Site 1 configured as an external inter-network site
- DMR node controller:
  - The DMR Site 1 Adjacent Sites table would have three entries:
    - MPT-IP Site 1 configured as an external inter-network site
    - MPT Site 1 configured as an external inter-network site
    - DMR Site 2 configured as a local site
  - The DMR Site 2 Adjacent Sites table would have three entries:
    - DMR Site 1 configured as a local site
    - MPT Site 1 configured as an external inter-network site
    - MPT Site 2 configured as an external fixed site

- MPT node 0:

The TN9500 is configured in the NMT as a node with three sites:

- MPT-IP Site 1
- DMR Site 1
- DMR Site 2

MPT Site 1 has four adjacent sites (note that configuring the external inter-network sites as adjacent sites on the NMT will allow for their control channel RF channel number and syscode information to be updated automatically):

- MPT-IP Site 1 is configured as an adjacent site
- DMR Site 1 is configured as an adjacent site
- DMR Site 2 is configured as an adjacent site
- MPT Site 2 is configured as an adjacent site

MPT Site 2 has two adjacent sites (note that configuring the external inter-network site as an adjacent site on the NMT will allow for its control channel RF channel number and syscode information to be updated automatically):

- MPT Site 1 is configured as an adjacent site
- DMR Site 2 is configured as an adjacent site

- TN9500 gateway

The table in the DMR/MPT-IP tab would have five entries:

- MPT-IP Site 1 would be configured as a dynamic external site
- DMR Site 1 would be configured as a dynamic external site
- DMR Site 2 would be configured as a dynamic external site
- MPT Site 1 would be configured as a dynamic external site
- MPT Site 2 would be configured as a fixed external site

The table in the MPT tab would have three entries:

- MPT-IP Site 1 would be configured as a dynamic external site (or as fixed if required)
- DMR Site 1 would be configured as a dynamic external site (or as fixed if required)
- DMR Site 2 would be configured as a dynamic external site (or as fixed if required)

### 3.8.1 External Site Overview

The external site feature enables radios to move seamlessly from one site on one network to an adjacent site on another network. The external adjacent site will belong to an external DMR, MPT-IP or TaitNet MPT network (connected via a TN9500 gateway). The current network will broadcast information to the radios about this external site (control channel RF number and syscode) to enable the radios to vote between the site it is on and the external inter-network site.

In DMR and MPT-IP networks, it is recommended that, for optimal performance, a maximum of twenty adjacent sites (this includes internal sites and external fixed sites as well as external inter-network sites) be configured per site.

In TaitNet MPT networks (where a TN9500 gateway is configured as a node and the external inter-network sites are configured as TN9500 sites), up to thirty inter-network adjacent sites can be configured. Of these thirty sites, a maximum of twenty adjacencies can be set up on a single site.

Only the sites nearest in geographic location to the current control channel should be configured as adjacent, in order to maintain acceptable performance during site re-selection.

### 3.8.2 Configuration Procedure

Before you begin, you will need to know the site aliases of the DMR/MPT-IP sites that are to be configured as external sites. On your DMR/MPT-IP WebUI, select Network > Sites, click the name of a site, then click on the Configuration tab to find the site alias.

For MPT sites, you will need to know the site name. Note that when entered on the TN9500, any spaces in the name must be removed.

#### TN9500


1. Log in to the WebUI of the TN9500 Inter-Network Gateway.
2. To add external sites to DMR/MPT-IP networks, select Network > External Sites > DMR/MPT-IP tab.
3. Select Add to add an external site. The Add DMR/MPT-IP External Site page is displayed.
4. Enter the site alias. Note that for an MPT site, for ease of site identification, enter the site's actual name, but with any spaces removed.
5. If MPT is selected as the network type, then two additional fields will be displayed. Enter the site ID and node ID of the MPT site.
6. Click Save to save this external site.
7. To add external sites to MPT networks, select Network > External Sites > MPT tab.
8. Select Add to add an external site. The Add MPT External Site page is displayed.

9. Enter the site ID and alias, and select the type from the drop down box. Options are Dynamic or Fixed.  
Note that the site ID must be the same as the site ID assigned to this site on the NMT (i.e. the order the sites are added must be the same as the order the sites are added in the NMT).
10. If the type of external site selected is Fixed, then the primary control RF channel number and syscode must also be entered, and optionally, the secondary control RF channel number and syscode where required for sites with dual control channels.
11. Click Save to save this external site.

## DMR/MPT-IP

The inter-network protocol (INP) is used to communicate external inter-network adjacent site information (using the site alias) from the DMR/MPT-IP network to the TN9500 gateway, when the dynamic adjacency feature has been enabled. If the site information (site alias, control channel RF number, syscode) changes, the TN9500 gateway will receive the updated control channel parameters.

Adjacent sites can be internal network sites, external inter-network sites, or external fixed sites. The current site's control channel will regularly send Vote Now messages (at the period specified by the Vote now interval parameter) asking radios to compare its signal strength with that of one of the specified adjacent sites. At the next period interval, the next site in the adjacent sites table is voted on. This is repeated in a circular fashion with all the sites in the table.

 For optimum results, a maximum of twenty adjacent sites per site is recommended.

1. Log in to the WebUI of the current network control node.
2. Select Settings > Network Parameters, and in the Features area, ensure that Dynamic adjacency is enabled. This will allow for the exchange of external inter-network adjacent site information between the node and the TN9500 gateway.
3. Click Save.
4. Select Network > Sites, click the name of a site, and then click the Voting Parameters tab to display voting configuration settings for the site.
5. Click Edit to add or update Voting Parameters and Adjacent Sites.
6. DMR networks only; MPT-IP networks do not use site priority. In the Voting Parameters area, enter a site priority for the current site. Options from the drop down menu are: No priority, Highest priority, Priority 2 to Priority 6, and Lowest priority.

Each site has an assigned priority, and the vote now messages contain the priority of both the current site and the site to be voted on.

Radio units can be configured whether to use the priority field or not. When enabled, radio units will use the site with the highest site priority so long as the site signal strength is above the radio's programmed L0 level.

- ① Using the site priority may result in a radio roaming to a site with a weaker signal strength than the currently registered site.
- 7. Enter the vote now interval and adjacent site info interval. These represent the time between broadcasts of vote now and adjacent site information messages from this site to the radios at the site.
- ① The adjacent site information broadcasts contain the same information as the vote now broadcast messages, however radios will not leave the control channel to perform a hunt upon reception of these. The purpose of the adjacent site information broadcasts is so that terminals can build up an internal hunt list, and prioritize which channels are more important should they lose contact with their currently registered site.
- 8. Click Add to add an adjacent site to the end of the table.
- 9. To insert an adjacent site in the list, click in a row and then click Insert. A new row is added above the selected row.
- 10. In the Type field, select External: Inter-network.
- 11. Enter the alias of the adjacent site. Note that for MPT sites, this is the site name with any spaces removed.
- 12. Enter the Priority of the adjacent site.
- 13. Click OK.
- 14. Click Save.

#### **TaitNet MPT**

The inter-node interface (INI) is used to communicate external inter-network adjacent site information (using the NMT site ID) from the MPT network to the TN9500 gateway. If the site information (site ID, control channel RF number or syscode) changes, the TN9500 gateway will receive the updated control channel parameters.

The TN9500 gateway is configured on the NMT as a node, and the external DMR/MPT-IP sites are configured as TN9500 sites.

1. Log in to the NMT.
2. From the main window, select Configuration > Network, to display the Network Configuration window.
3. To add the TN9500 gateway (as a node) press the Add button to display the Add Node window.

4. In the Node Number box, enter a number for the TN9500. It must be a number between 0 and 31. It is recommended that you use the highest number possible (i.e. 31) to distinguish the TN9500 from other network nodes.
5. In the Node Name box, enter a suitable name for the TN9500.
6. In the Primary Node IP Address box, enter the IP address of the TN9500.
7. In the Node Mnemonic box, optionally enter a short version of the TN9500 name, this will be displayed on various windows (for example, the DAS Monitor window), instead of the node's full name.
8. To enter the sites, click on the cells in the Sites table and enter the name and mnemonic (if required) for each external site configured on the TN9500. Note that the site ID must be the same on both the NMT and the TN9500, i.e. they must be entered in the same order.
9. Click on the Active column for each site, to enable it.
10. Press Apply to save your changes then Close to close the window.
11. The external inter-network sites added in step 8 can now be configured as adjacent sites for the MPT network's sites as required.
12. For each site, select *Site* > Configuration (where *Site* is the MPT site) and select the Adjacent Site tab.
13. In the Vote Now area, enable vote now broadcasts, by checking the box, and enter the required vote now broadcast interval for the between vote now messages being transmitted.
14. In the Adjacent Sites table, click in the Site area and select the adjacent sites as required from the pop-up node/site menu that appears. For each entry, select Vote as the voting mode.
15. Click Apply to save your changes then Close when finished entering adjacent sites for the selected site.
16. Select other sites as required until all external inter-network sites have been added as adjacent sites to the relevant MPT sites.



## 3.9 High Availability

To enable the TN9500 gateway for high availability, the primary (or active) and standby TN9500 gateways must be on the same subnet. The active IP address to be used by them must also be on the same subnet.

### 3.9.1 Tait Ubuntu Requirements

- Two TN9500 gateway servers
- Three IP addresses on the same subnet (an individual IP address for each server and one to be used by both as the active IP address)

### 3.9.2 Tait Ubuntu Configuration Procedure

#### Administration Application

In the containerized version, the Active IP address is configured in the Tait Administration Application for each containerized application running on that server as follows:

1. Log in to the Administration Application on the primary server.
2. Select Configuration > Tait Services.
3. Select the TN9500 Inter-Network Gateway service and click Edit to enter the Active IP address to be used.
4. Click Save.

#### TN9500 Gateway Application

In the containerized version, the high availability Priority, Network check A, Network check B, and the Peers IP Address is configured in the TN9500 Inter-Network Gateway application, as follows:

1. Log in to the primary (active) TN9500 gateway server.
2. Select Settings > High Availability.
3. In the General area, enter 1 as the Priority (where 1 is the highest priority).
4. Enter the Active IP address to be used. This is the IP address that the gateway will use when it is functioning as the active gateway. It will also be used by all connected network equipment.
5. For Network check A, enter the IP address of a network element that you wish to check that the gateway is able to connect to. This could be the IP address of the gateway of the LAN to which the gateway belongs.
6. For Network check B, enter the IP address of a second network element that you wish to check that the gateway is able to connect to. This could be the IP address of the INP node controller (MPT-IP or DMR node).

7. In the Peers area IP address field, enter the IP address of the second (standby) gateway and click Add.
8. Click Save.
9. Now log in to the standby TN9500 gateway.
10. Select Settings > High Availability.
11. In the General area, enter 2 as the Priority.
12. Enter the same Active IP address and Network check A and B addresses as for the primary (active) gateway.
13. In the Peers area IP address field, enter the IP address of the primary (active) gateway and click Add.
14. Click Save.

### 3.9.3 Tait CentOS Requirements

- Two TN9500 gateway servers
- Three IP addresses on the same subnet (an individual IP address for each server and one to be used by both as the active IP address)
- If a TaitNet MPT network is to be connected to the high availability TN9500 gateways, then a failover switch is required for successful switching of E1/T1 links. Tait recommends a Valiant E1 or T1 variant.

### 3.9.4 TaitCentOS Configuration Procedure

1. Log in to the WebUI of the primary (active) TN9500 gateway server.
2. Select Settings > High Availability.
3. In the General area, enter 1 as the Priority (where 1 is the highest priority).
4. Enter the Active IP address to be used. This is the IP address that the gateway will use when it is functioning as the active gateway. It will also be used by all connected network equipment. On the NMT, the active IP address of the gateway is used when defining the internode links of the T1541.
5. For Network check A, enter the IP address of a network element that you wish to check that the gateway is able to connect to. This could be the IP address of the gateway of the LAN to which the gateway belongs.
6. For Network check B, enter the IP address of a second network element that you wish to check that the gateway is able to connect to. This could be the IP address of the INP node controller (MPT-IP or DMR node).

7. If a TaitNet MPT network is connected to the high availability TN9500 gateways, then the Valiant E1/T1 Switch parameters must be configured. Enter the IP address of the Valiant failover switch and select the physical port on the switch to which the gateway is connected. In the event of a gateway failure, the switch will redirect the E1/T1 audio to the new active gateway.  
  
If the equipment port is set to Disabled, switchover will not take place in the event of a gateway failure.  
  
If the Valiant E1/T1 Switch is configured and enabled, a community string is required (see "[SNMP read-only community string](#)" in [Section 3.9.5 Additional Information](#)).
8. In the Peers area IP address field, enter the IP address of the second (standby) gateway and click Add.
9. Click Save.
10. Now log in to the WebUI of the standby TN9500 gateway.
11. Select Settings > High Availability.
12. In the General area, enter 2 as the Priority.
13. Enter the same Active IP address and Network check A and B addresses as for the primary (active) gateway.
14. If a TaitNet MPT network is connected to the high availability TN9500 gateways, then the Valiant E1/T1 Switch parameters must be configured. Enter the IP address of the Valiant failover switch and select the physical port on the switch to which the gateway is connected. The IP address will be the same as that entered in step 7, but the port will be different.  
  
If the Valiant E1/T1 Switch is configured and enabled, a community string is required (see "[SNMP read-only community string](#)" in [Section 3.9.5 Additional Information](#)).
15. In the Peers area IP address field, enter the IP address of the primary (active) gateway and click Add.
16. Click Save.

### 3.9.5 Additional Information

#### Network Check A and B

The TN9500 gateway will ping the network check addresses once every 2 seconds. When only one network check address has been entered and that connection fails, the gateway state will become 'Failed' and an alarm will be generated. If two network check addresses have been entered, the gateway will remain online and 'OK' if one connection has failed, but if both connections fail, the gateway state will become 'Failed' and an alarm will be generated.

If the active gateway in a high availability network moves to a 'Failed' state, then the standby gateway will take over. If the failed gateway automatically recovers when the network has been restored, it will become the standby gateway if another gateway became active.

If a Valiant E1 or T1 failover switch is operating, then the state of the E1/T1 spans will also be taken into account when deciding if switchover to the standby gateway is required.


### Synchronization

If the active and standby TN9500 gateway databases are not synchronized:

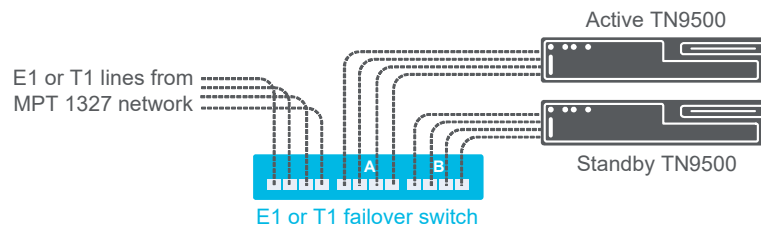
1. Log in to the standby TN9500 gateway.
2. Select Settings > General.
3. Click Edit.
4. Under Mode, select Synchronize.
5. Wait for the mode to change automatically from Synchronize to Offline, then select Online. The standby gateway databases will now be synchronized with the active gateway.

### Valiant E1/T1 Switch

As the E1/T1 connections are static links, a failover switch is required when high availability gateways are used with a TaitNet MPT network. The failover switch enables the switch over of E1/T1 lines between gateways.

-  There are two variants of failover switch from Valiant: the E1 failover switch and the T1 failover switch.

If the Valiant E1/T1 failover switch has been configured in the WebUIs of the primary and standby TN9500 gateways, it will be used by the handover algorithm if the active gateway fails and operation is switched to the standby gateway.



To configure the Valiant failover switch, program the IP address as described in the Valiant manual, or below.

The factory default IP address of the Valiant is 192.168.1.101. To change this, do the following:

1. Log in to the Valiant using `superuser` as both the username and password.

2. To put the system into Operation and Maintenance (OAM) mode for configuration purposes, at the prompt enter the following command:  
**\$\$config/oam**
3. To change the IP address, at the prompt enter the following command:  
**ipaddr=<IP address>**  
(Where <IP address> is the new IP address.)
4. To return to normal mode, at the prompt enter the following command:  
**\$\$exit**  
or to end the session and exit from the system, at the prompt enter the following command:  
**exit**

The default parameters of the Valiant do not need to be changed as the switchover is managed from the TN9500 gateway.

- i** Note that during the actual hardware installation of the Valiant E1/T1 failover switch, to avoid audio issues with the TaitNet MPT system, the cables must be connected according to the number of the ports. E.g. the cable from A1 on the Valiant must connect to Port1 on the TN9500, A2 must connect to Port2, and so on. Use a straight cable between the Valiant and the DAS, and a crossed cable between the Valiant and the TN9500. Using a crossed cable between the TN9500 and the Valiant allows the SNMP polling to show 'remote alarm' (cable connected but alarm received) rather than 'loss of signal' (cable disconnected).

#### **SNMP read-only community string**

The TN9500 gateway has the ability to check the status of the Valiant E1 or T1 failover switch by using SNMP polls. Enter the community name that must be included in SNMP 'get' requests. There is no maximum length. However, SNMP uses UDP as a transport protocol, so the only limitation would be data packet length. The following characters can be used in the string: ( ) . \* / - : \_ ? = @ , & % \$

- i** This may be different from the community string on the TN9500 gateway.

#### **Troubleshooting**

If the TN9500 gateway HA state (Settings > High Availability > General) is:

- unknown:  
check if the TN9500 gateway is running
- offline:  
change the mode of the TN9500 gateway to online
- standby:  
the other TN9500 gateway is active
- failed:

the E1/T1 links have failed or the ethernet has failed (Network check A and B have both failed)

- a. To fix the E1/T1 links, first put the TN9500 gateway into Offline mode (Settings > General > Mode) then into Online mode. This will put the TN9500 gateway on standby. Inspect the E1/T1 links for any failures and restore them, otherwise the next time this gateway becomes active it will end up in the failed state again.
- b. To fix IP connectivity, restore the IP network and ping to check. The status will change to standby.

If failure of the E1/T1 connections have caused the TN9500 gateway to enter the failed state, but you still want the gateway to operate, we recommend that you backup the database and delete all the E1/T1 configurations before putting the gateway online again.

**Handover** During the handover period (when the standby gateway becomes active) all calls through the gateway are stopped.

Handover timings are as follows (approximate times only):

- IP re-routing - twenty seconds
- E1/T1 failover switching - ten seconds
- Processing registrations on the newly active gateway for all connected networks - up to twenty minutes (depending on the number of registered radios on the whole system)

**Restoring Databases** It is recommended that, if required, the database restore is first done on the standby TN9500 gateway. Then the active TN9500 gateway should be set to offline or to synchronize mode to synchronize its database to the restored one.

**Disabling Filtering of RTP Packets** The TN9500 blocks RTP packets by default if the source ID is set to zero. This avoids passing noise between systems, usually as a result of using acknowledged group calls. However, in some instances, valid audio can be blocked. To disable filtering, add the following line to the `/ing/tait_ing.cfg` file:

```
packet-switch.allow-no-source-id-in-ais-packets:1
```

A restart is required for this option to take effect.

**SNMP Monitoring of Valiant** The TN9500 gateway has the ability to check the status of the Valiant E1 or T1 failover switch by using SNMP polls:

1. Select Settings > High Availability and click Edit.
2. In the Valiant E1/T1 Switch area, enter a community name in the SNMP read-only community string field. This is the community name that must be included in SNMP 'get' requests. There is no maximum length. However, SNMP uses UDP as a transport

protocol, so the only limitation would be data packet length. The following characters can be used in the string: ( ) . \* / - : \_ ? = @ , & % \$

3. Click Save.

## 3.10 PTTToX Connector Configuration

The TN9500 can be used to link TaitNet PTTToX to a DMR system.<sup>1</sup>

**i** If one connection is made to a PTTToX Connector, then only one other connection is supported and that must be to a DMR Trunked network.

1. Login to the TN9500.
2. To add a PTTToX connector, select Networks > Connections and click Add.
3. Enter a suitable name for the PTTToX connector.
4. Populate the following fields as follows:
  - Network Type: select PTTToX
  - Username: **admin** (this is fixed internally in the PTTToX Connector)
  - Password: **ta**it (this is fixed internally in the PTTToX Connector)
  - IP address: **172.51.1.1**
5. To verify the connection, check its status on Networks > Connections, and to verify that radio registrations come through, check Networks > Registrations.

For information on how to configure a DMR network for PTTToX, refer to [Appendix 2 Deploying PTTToX in a DMR Trunked Network](#).

**i** The recommended maximum number of concurrent PTTToX calls is 40 when the PTTToX connector is running on a Dell R250 or Kontron CG2400 server. On a Sintrones SBOX-2621, the recommended maximum is 39.

---

1. Note that PTTToX inter node connections are only supported for single DMR networks. PTTToX to MPT-IP or TaitNet MPT is not supported.

# 4 Backing up/Restoring Configuration Files


---

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

The Administration application and TN9500 gateway configurations 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.


## 4.1 Manual backup

1. Using a web browser, login to the Administration application (see the System Manual for details).
2. Select Files > Backups.
3. Select Backup.

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

## 4.2 Restoring

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

 Restoring backups from the previous TN9500 Gateway firmware (version 1.2.03) release is supported by version 1.4.03.

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 WebUI
- administration database (admin) - contains information about users that have been manually configured via the WebUI

The following database is backed up by the TN9500 gateway:

- inter-network gateway database (ing) - main application database containing all the settings configured by the host administrator



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.

# 5 TN9500 Inter-Network Gateway Information

---

## 5.1 IP Protocols and Default Ports

The TN9500 gateway is used to connect networks together. This section describes the IP protocols and IP ports used by default.

IP bandwidth information is totally dependent on the networks connected by the TN9500 gateway. It is advised that you check the relevant network system manuals (MPT Migration System Manual, TaitNet MPT System Manual, TaitNet MPT-IP System Manual and/or the DMR Trunked System Manual) for further information.

### 5.1.1 IP Protocols

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

The following table lists the ports and their usage.

Type	Usage	Ports/Protocols
HA peer protocol	TN9500 to/from TN9500	UDP/TCP 14060
ICMP	NMS and management PC to node controllers, network gateways, base stations, switches and routers	ICMP
InterNode Interface protocol (INI)	TN9500 to/from T1541 nodes	UDP/TCP 9047
InterNetwork Protocol (INP)	TN9500 to/from MPT-IP/DMR control nodes	UDP/TCP 5060
Network Management Terminal (NMT)	Communications to TaitNet MPT network NMS	TCP 9012
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

Type	Usage	Ports/Protocols
Real Time Protocol (RTP)	TN9500 to/from node controllers	UDP varies
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
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 5.1.2 IP Default Ports</a>

## 5.1.2 IP Default Ports

Each application has a resource configuration file (extension `.cfg`). This file provides some limited configuration parameters that cannot be changed when logged on to the TN9500 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 various Tait applications. 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:

- UseHttp: 0 (for HTTPS) or 1 (for HTTP)
- http\_port: 80
- https\_port: 1443

- watchdog\_server\_port: 9083
- watchdog\_application\_port: 9084

#### **TN9500 Gateway**

The configuration file for the TN9500 gateway is `/home/taitnet/ing/tait_ing.cfg` and the default port settings are:

- UseHttp: 0 (for HTTPS) or 1 (for HTTP)
- http\_port: 14080
- https\_port: 14443
- TaitNet\_NMT\_communication\_port: 9012 (this cannot be modified)
- watchdog\_server\_port: 14010
- watchdog\_application\_port: 14011
- watchdog\_packet\_switcher\_port: 14012

#### **E1/T1 Gateway**

The configuration file for the E1/T1 gateway is `/home/taitnet/tait_e1_gateway/tait_e1_gateway.cfg` and the default port settings are:

- UseHttp: 0 (for HTTPS) or 1 (for HTTP)
- http\_port: 15080
- https\_port: 15443
- watchdog\_server\_port: 15010
- watchdog\_application\_port: 15011

#### **Transcoder**

The configuration file for the transcoder is `/home/taitnet/transcoder/tait_transcoder.cfg` and the default port settings are:

- UseHttp: 0 (for HTTPS) or 1 (for HTTP)
- http\_port: 16080
- https\_port: 16443
- watchdog\_server\_port: 16010
- watchdog\_application\_port: 15011
- The watchdog worker ports range from `watchdog_application_port + 1` to `watchdog_application_port + 4`

All the above ports belong to the user port range as defined by RFC6335. If use is required over internet you may need to register them with IANA or they may already be used by other assigned applications and may need to be modified.

In addition, the applications use the following internal ports (however they cannot be used by the operating system, where they have been disabled):

- TN9500 gateway: 51000-51099
- E1/T1: 50000-50099
- Transcoder: 52000-52099

### 5.1.3 QoS/DSCP

DSCP (Differentiated Services Code Point) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks. It can, for example, be used to provide low-latency to critical network traffic such as voice or streaming media whilst providing simple, best-effort service to non-critical services such as web traffic or file transfers.

Currently the TN9500 gateway supports fixed DSCP configurations for the following network traffic.

Type	Protocol	DSCP	Meaning
Voice	RTP	46	Expedited Forwarding (EF) which is recommended as this will provide low-loss, low latency traffic
Control	INI, SIP (AIS)	26	Assured Forwarding (AF) which is recommended as it will give assurance of delivery under prescribed conditions
Management	HTTP, SNMP	0	Best effort delivery.

## 5.2 System Events and Alarms

System events and alarms are displayed in the TN9500 gateway's Networks > Events page.

### 5.2.1 System Events

The following table lists the possible system events. Their severity is based on syslog levels.

Syslog Level	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions

Syslog Level	Description
5	Notice: normal but significant condition
6	Informational: informational messages

## 5.2.2 Alarm Types

The following table lists the alarm types. Each alarm record is preceded with a timestamp consisting of the time at which the system event occurred. (Timestamp format: YYYY-MM-DDTHH:mm:ss.micros + offset)

Type	Name	Source (integer)	Source Name	Notes
1 <sup>1</sup>	tn9500-startupinfo	0		reason=reason for startup
	e1SystemStartupEvent	0		
2 <sup>1</sup>	tn9500-shutdown	0		reason=reason for shutdown
3 <sup>2</sup>	mpt-ini-connection-down-alarm-raised	Node number	Node IP address	
	e1t1redAlarmUpEvent	E1/T1 span #	E1/T1 span #	
4 <sup>1</sup>	mpt-ini-connection-down-alarm-cleared	Node number	Node IP address	
	e1t1redAlarmDownEvent	E1/T1 span #	E1/T1 span #	
5 <sup>2</sup>	mptip-network-down-alarm-raised	Network ID	Network name	
6 <sup>1</sup>	mptip-network-down-alarm-cleared	Network ID	Network name	
7 <sup>2</sup>	dmr-network-down-alarm-raised	Network ID	Network name	
	e1t1yellowAlarmUpEvent	E1/T1 span #	E1/T1 span #	
8 <sup>1</sup>	dmr-network-down-alarm-cleared	Network ID	Network name	
	e1t1yellowAlarmDownEvent	E1/T1 span #	E1/T1 span #	

Type	Name	Source (integer)	Source Name	Notes
14	ha-state-changed	N/A (0)	N/A	0: Unknown 1: Offline 2: Active 3: Standby 4: Synchronize 5: Failed
15	peer-manager-sync-status-changed	N/A (0)	N/A	0: Unknown 1: mismatch 2: OK

1. Alarm severity: Informational
2. Alarm severity: Alert

## 5.3 Registration Records

Select Network > Registrations page to display recent registration events.

Registration records show:

- registration or deregistration requests received from a remote network
- registration or deregistration requests sent to a remote network

Registration record files are saved in comma separated file format (.csv) under /home/taitnet/ing/registrations

Select Files > Logs to download Registration.csv files that list successful registrations (Registration Records). Failed registration records (i.e. if an out of date registration notification comes in from TaitNet MPT it is dropped by the registration manager and recorded in the TN9500 internal log file.

### Csv Files

The first line in the csv file contains the headings for the columns, and the subsequent lines contain the values for each call record as follows:

Column Name	Contents
address-mpt1327	prefix/ident with leading zeroes (%03d/%04d) so that excel does not convert them to dates)
address-dmr	DMR address with leading zeroes (%08d)
received-time	YYYYMMDDTHHmmSS+OSET
record-type	REG_RCV or DEREG_RCV or REG_SENT or DEREG_SENT
source-network-type	INP or INI <sup>1</sup>
source-inp-network-id	1-20 or empty

Column Name	Contents
source-inp-network-name	name (stripped of commas and double quotes) or empty
source-ini-node-number	0-31 or empty
<b>The following fields will only contain data for REG_SENT and DEREG_SENT records:</b>	
sent-time	YYYYMMDDTHHmmSS+OSET or empty
destination-network-type	INP or INI or empty
destination-inp-network-id	1-20 or empty
destination-inp-network-name	name (stripped of commas and double quotes) or empty
destination-inp-status-code	The SIP status code response to the registration request.
destination-ini-node-number	0-31 or empty

1. INP - Inter Network Protocol, used for DMR and MPT-IP networks  
INI - Inter Node Interface, used for TaitNet MPT networks

## Examples

Subscriber 5/1 registers on INI node 1:

```
005/0001,00040961,20161108T094729+1300,REG_RCV,INI,,,1,,,,,
```

Notification is sent to AIS network (ID = 1, name = "Test Network"):

```
005/
0001,00040961,20161108T094729+1300,REG_SENT,INI,,,1,20161108
T094659+1300,INP,1,Test Network,200,
```

Subscriber 5/24 registers on AIS network (ID = 1, name = "Test Network"):

```
005/0024,00040984,20161108T094730+1300,REG_RCV,INP,1,Test
Network,,,,,
```

Notification sent to INI node 0:

```
005/0024,00040984,20161108T094730+1300,REG_SENT,INP,1,Test
Network,,20161108T094702+1300,INI,,,1
```



## 5.4 TN9500 Inter-Network Gateway Call Records

Note that The TN9500 does not send its own call records to the TaitNet MPT NMT.

TaitNet MPT NMT call records shows the call records that are internal to the TaitNet MPT system and the call records for events originating on the MPT system and sent to the TN9500 gateway (but not the events sent to the MPT system from the TN9500).

### 5.4.1 Call Records File Format

Call record files are saved in both comma separated file format (.csv) and pure text file (.txt) under /home/taitnet/ing/callrecords

To download a call record file, in the TN9500 gateway WebUI, select Files > Call Records and click on the file name to download it.

#### Csv Files

The first line in the csv file contains the headings for the columns, and the subsequent lines contain the values for each call record as follows:

Column name	Description
uuid	A string of 36 characters that uniquely identifies a call. Sample: 46467d72-01fd-5a52-99fa-2942e5c15d1e
call_id	A sequence number used for diagnostics
date_time	A string containing the date and time the call was created. The format is: YYYYMMDDThhmmssZ, where T and Z are the characters T and Z.
a_party	The calling party address encoded as an integer
b_party	The called party address encoded as an integer
a_party_mpt1327	The calling party address in extended MPT 1327 format (prefix/ident). In MPT 1327 the prefix is restricted to the range 0-127. The extended format allows prefix in the range 0-4196.
a_party_fleet	The calling party address in fleet format
b_party_mpt1327	The calling party address in extended MPT 1327 format (prefix/ident). In MPT 1327 the prefix is restricted to the range 0-127. The extended format allows prefix in the range 0-4196.
b_party_fleet	The called party address in fleet format
a_fleet_id	The fleet ID for the calling party
b_fleet_id	The fleet ID for the called party

Column name	Description
call_type	Refer to the table in <a href="#">Section 5.4.2 Call Types</a> for a complete list of call types
call_priority	The priority of the call: 0 - Normal 1 - Priority 1 2 - Priority 2 3 - Priority 3 4 - Emergency (1, 2 and 3 are DMR priorities only, in MPT and MPT-IP they are all priority level calls.)
on_air_time	The time in seconds that this call was on air. Note that for SDM calls this actually displays the size of the SDM. For data calls that use only the control channel (UDTs), on_air_time is the number of codewords used to transmit the data, plus 1 (for the header codeword). For status calls, where the status information is carried in a field within the header codeword, on_air_time is always 1.
queue_time	The time in seconds that this call was queued
answer_time	The time in seconds before this call was answered
end_reason	Refer to the table in <a href="#">Section 5.4.3 Call End Reasons</a> for a complete list of call end reasons
handler_id	Refer to the table in <a href="#">Section 5.4.5 Call Handler IDs</a> for a complete list of call handler IDs
line_id	For handlers with multiple lines, this represents the line ID
supplemental_info	Any supplementary information. For a base station, this is the RF channel number. For DIP, this is the DIP sequence number.
call_flags	A bit field representing additional state information for the call: PRIORITY 0x00000002 The PRIORITY bit is set if the call is a high priority call. EMERGENCY 0x00000004 The EMERGENCY bit is set if the call is an emergency priority call. LOCAL 0x00008000 <sup>1</sup> The LOCAL bit is set if the call is local to the site and includes no other end points or sites. OUTGOING 0x00010000 The OUTGOING bit is defined if the site or end point for this call record receives the call. This is the inverse of the ORIGINATING bit. ORIGINATING 0x00020000 The ORIGINATING bit is set if the call originated from the site or end point for this call record. <b>ENCRYPTED_OVER 0x0000400000000000</b> The PTT over was encrypted.

1. For PTT overs, the LOCAL flag actually indicates if it is the called or calling party transmitting. i.e. if the local flag is set, it means called party.

## Txt files

The text files show each call record entry in the following format:

```
DateTime: 20170309T013401Z
UUID: 86d7ed15-01d8-ec5e-8009-79e4fe366cfa CallID: 334
From: 0/510 (00000510) To: 0/484 (00000484) Digits:
OnAirTime: 00000000 QueueTime: 000 AnswerTime: 002
CallType: M CallPriority: 0 CallFlags: 20000 EndReason: 1207
HandlerID: 9001 HandlerType: DMR HandlerName: DMRT3_FT LineID: 001
(000)
```

The calling or called party ID for a phone call can be PSTNI, PABXI or DUMMYI, but these special idents are defined on DMR and MPT-IP networks.

PSTNI and PABXI are used to indicate that the call is to/from a network with a phone interface. Normally PSTNI indicates that the network is connected to an external phone, and PABXI indicates that the network is connected to an internal PABX.

DUMMYI is used when the calling party is not known. (I.e. if a PTT is from a T1541 MPT node in a group call, the ING does not know the actual source address of the PTT, so the ING will display DUMMYI for the A party address in the PTT call records.)

	DMR (DMR ident)	MPT-IP (MPT ident)
<b>PSTNI</b>	16776896 (0x0xFFFE0)	8101
<b>PABXI</b>	16776897 (0x0xFFFE1)	8102
<b>DUMMYI</b>	0	0

## 5.4.2 Call Types

The following table lists the possible call types and characters representing those call types.

Type	Description
I	Individual voice and self test
G	Group voice
b	Broadcast
N	Individual packet data
n	Group packet data
M	Individual short data message
m	Group short data message
P	Short data poll

Type	Description
S	Individual status message
s	Group status message
T	Call diversion
g	Regroup
y	Supplementary data
R	Registration
a	Authentication
x	Cancel call
u	individual unit presence check
F	Force registration
Y	Stun unit
L	Revive unit
B	Bar unit

### 5.4.3 Call End Reasons

This field contains a numeric code giving a detailed reason why the call ended or failed. It is used to help diagnose configuration and equipment faults.

The following table lists the number and name of each TN9500 gateway generated call end reason and provides descriptions of them. Refer to the System Manuals for DMR, MPT-IP and MPT for the call end reasons raised by those network types.

No.	TN9500 Call End Reason	Corresponding Call Type(s)	Corresponding TaitNet MPT Call End Reason
2000	Unknown The gateway was unable to identify why the call ended or failed.	Unknown	Unknown
2001	Poll rejected The unit poll was rejected by the gateway.	Kill, Revive, Stun, Regroup, ESN, Bar	Site unsupported call type
2002	Non-prescribed data rejected The sent NPD message was rejected by the gateway.	Non-prescribed data calls	Data calls disabled OR Intersite data call failure

No.	TN9500 Call End Reason	Corresponding Call Type(s)	Corresponding TaitNet MPT Call End Reason
2003	Diversion rejected The diversion request was rejected by the gateway.	Diversion request	Site diversion request not supported
2004	Unsupported call type The call type is unsupported by the gateway.	N/A (generic)	Site unsupported call type
2005	Message size exceeded limit for called site The message exceeded the called site's maximum message size.	N/A	Site error
2006	Gateway message content out of range The message content is out of the remote network's supported range	N/A (generic)	Site error

#### 5.4.4 Call Close Reasons

This field contains a numeric code giving a detailed reason why the call closed.

The following table lists the number and name of each call close reason and provides descriptions of them.

No.	Reason and description:	
	Taitnet MPT Connection	Inter-network Connection
0	<b>TE BUSY</b> The called terminal equipment is already in a call at the time of the call request	
1	<b>SYSTEM BUSY</b> The network is overloaded or has problems	<b>TE BUSY</b> The called party is busy
2	<b>NO ANSWER</b> The called party does not answer	<b>SYSTEM BUSY</b> The system is too busy for this call
3	<b>NOT FOUND</b> The ident of the called party is valid but it is either not registered or the node could not route the call	<b>REJECTED</b> The called party rejected the call
4	<b>COMPLETE</b> The call was completed	<b>NOT HOME</b> The called party could not be found

No.	Reason and description:	
	Taitnet MPT Connection	Inter-network Connection
5	<b>PREEMPTED</b> The call was cleared down to make a channel available for a priority or emergency call	<b>COMPLETE</b> Cleared, completed, accepted
6	<b>TIMEOUT</b> The call exceeded the current maximum call duration or the maximum allowable call setup time	<b>CALL BACK</b> Queued in the radio for callback
7	<b>INACTIVE</b> One or more of the parties was inactive. The inactivity timer expired.	<b>INVALID</b> Call rights / service type failure
8	<b>CALLBACK</b> The call to a line dispatcher terminal was put in the callback queue	<b>PREEMPT</b> The call link wants to preempt the call
9	<b>UNSUPPORTED REQUEST</b> The call could not be processed because the system does not support it, for example, sending a status call to a PSTN port	<b>AMALGAMATED</b> Call has been amalgamated into a group call
10	<b>INVALID CALL</b> The call failed the system's validation check, for example, because the caller did not have rights to make the call or because the caller was outside the assigned service area	
11	<b>CONVERT TO LOCAL</b> The network could not process the call and sent it back to the originating site to process	<b>DIP CALL AMALGAMATED</b> DIP call has been amalgamated into a group call
12	<b>NO ROUTE</b> Internode routing failed	
13	<b>FORCE CLOSE</b> A group call was closed by a party other than the calling party	
14	<b>INCLUDE COMPLETE</b> The call was successfully amalgamated into another call	
15	<b>UNKNOWN</b> The close reason is unknown	
99		<b>UNKNOWN</b> The close reason is unknown

## 5.4.5 Call Handler IDs

Each link in a call is stored as a call record. The handler ID number identifies the link type, as follows:

- Site: Site ID
- SIP lines: 1000 + SIP line ID
- DIP connections: 2000 + DIP connection ID
- MPT gateway: 4000 + MPT gateway line ID
- Conventional connections: 5000 + Conventional connection ID
- AIS connections: 9000 + AIS connection ID
- INI node: 9100 + TaitNet MPT node ID



Note that ID is the allocated number as displayed in the ID column on the relevant WebUI page.

## 5.5 TN9500 Inter-Network Gateway Status Monitoring

The WebUI Status bar below the page header provides a snapshot of the current status of the TN9500 gateway.

As well as the current time and date, the following information is displayed:

### State

This is the status of the TN9500 gateway.

State	Description
Degraded	The gateway's performance is degraded, at least one, but not all of the connections may be down
Down	The gateway is not working, or high availability may have failed
Initializing	The gateway is in the process of starting up
Invalid license	Either: The gateway has a missing or invalid license. Or: The number of connected nodes exceeds the number defined in the license file.
Offline	The gateway has been taken offline. It is unable to communicate with nodes
OK	The gateway is in its normal operating mode

State	Description
Processing registrations	The gateway is processing registration information from the connected networks. <b>Note:</b> Processing registrations from newly connected networks can take a significant amount of time. During this time calls and other registration events may not work correctly until the process is complete.
Standby	The gateway is operating as a high availability standby gateway
Synchronizing	A high availability TN9500 gateway is synchronizing its database with its peer

**Connections** Tells you how many connections are up and how many are down.

**E1/T1** The status of the E1/T1 cards, if present. Status types of Initializing, Down, Degraded or OK are as described above.

## 5.6 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, ing for the internet network gateway, e1\_gateway for the driver looking after the E1/T1 interfaces, and transcoder for the vocoder. 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 WebUI under Files > Logs (in both the Administration application and TN9500 gateway WebUI) by clicking on an individual log file name.

### 5.6.1 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.

#### **TN9500 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

`taitnet-tn9500-ing-install.log`

This log file is created by the `taitnet-tn9500-ing` RPM and contains information on the installation status of the `taitnet-tn9500-ing` package. Any future downgrades and upgrades are appended to this log.

`taitnet-e1-gateway-install.log`

This log file is created by the `taitnet-e1-gateway` RPM and contains information on the installation status of the `taitnet-e1-gateway` package. This file contains logging information for T1 where applicable. Any future downgrades and upgrades are appended to this log.

`taitnet-transcoder-install.log`

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

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

`upgrade_<YYYYMMDD>.log`

This log file contains information on the upgrade status of the selected package (TN9500 gateway or Administration application for example). Any future downgrades and upgrades are appended to this log for the day.

`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.

# Appendix 1

---

## A.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.

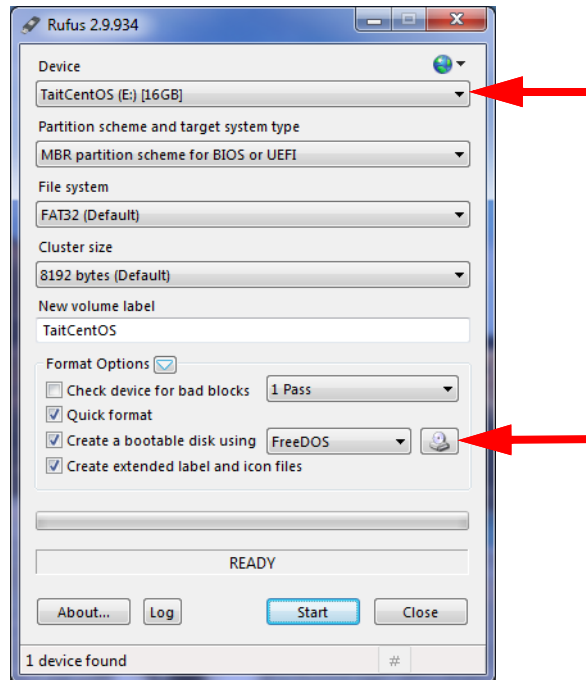
The advantage of Rufus over Win32DiskImager is that when the USB flash drive has been written to, the USB flash drive is still able to be read from and written to under Windows. This allows the user to add any additional scripts, configuration files etc. to the USB flash drive.

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

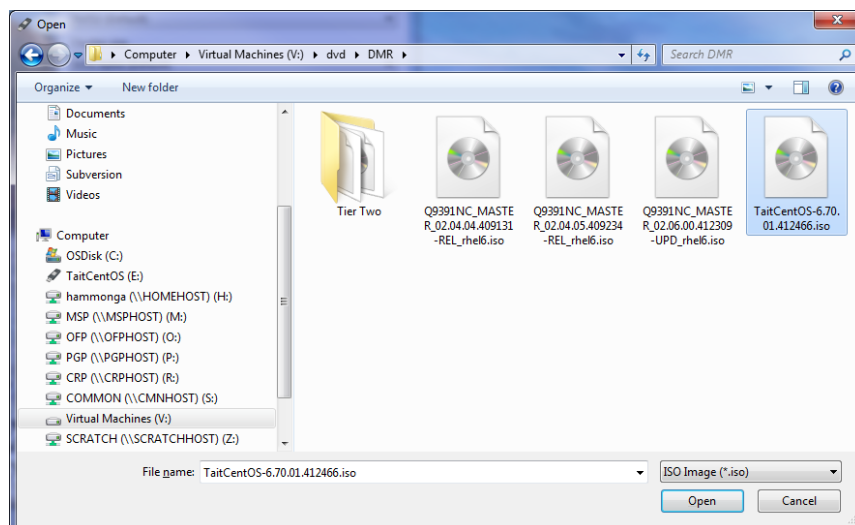
### A.1.1 Using Rufus for TaitCentOS

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 TaitCentOS version, 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.)

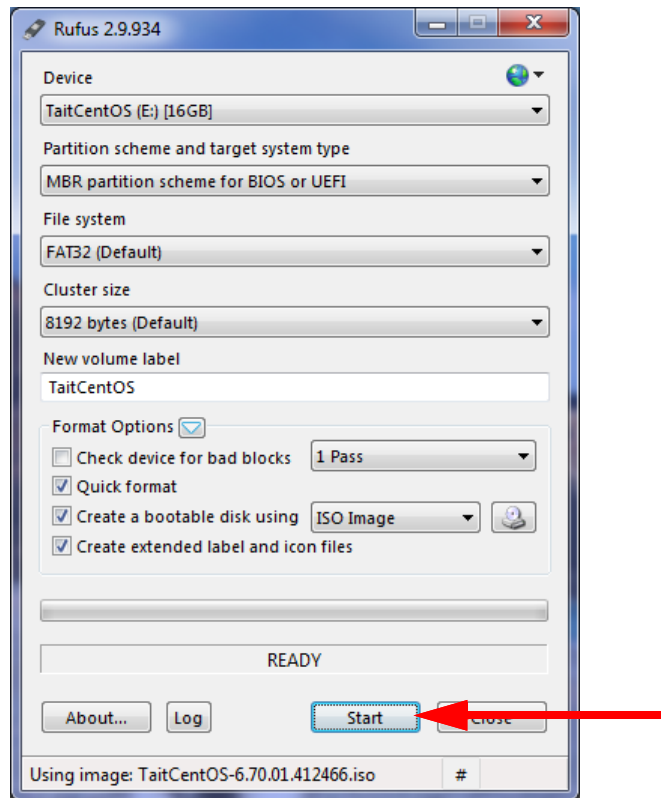
3. Run the Rufus program.



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.

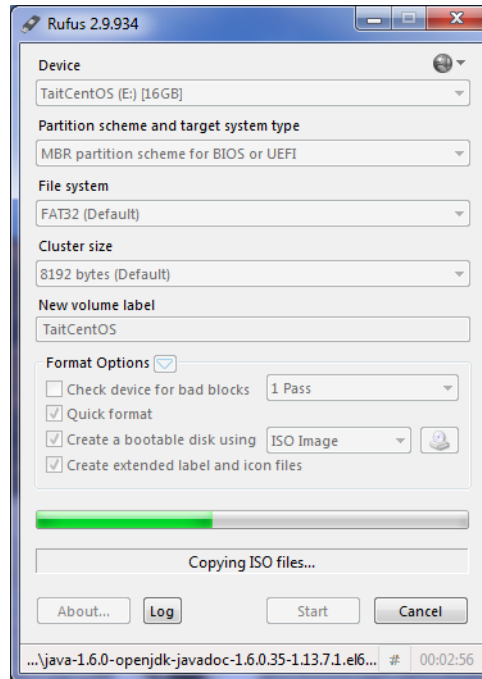


7. When ready to start the writing process, click Start.



8. 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.

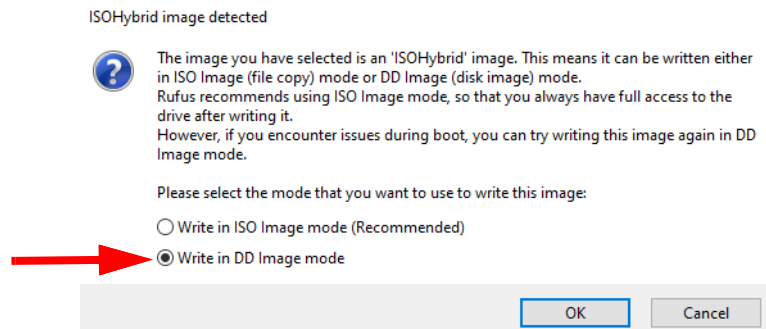
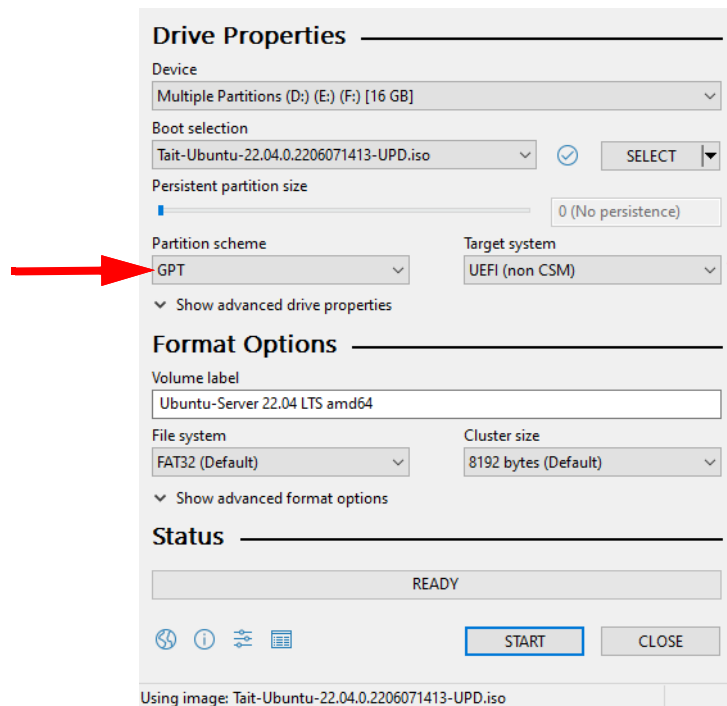
9. The progress of the USB flash drive write is displayed as follows:



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

## A.1.2 Using Rufus for Tait Ubuntu

1. To create a bootable USB flash drive with Tait Ubuntu, 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 Tait Ubuntu version (i.e. not a commercial Ubuntu package), to ensure that the correct customization and configuration settings are installed.
2. 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 screen shots below).



### A.1.3 Using dd for Tait Ubuntu on Linux

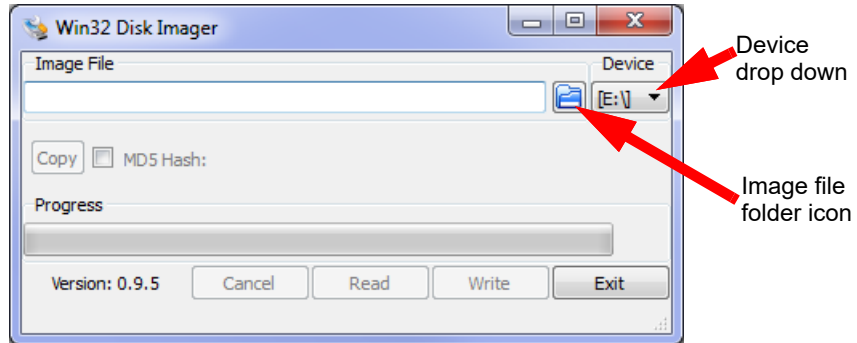
1. If you are using a Linux desktop, you can run the following command as root to flash the downloaded ISO image to a USB drive:  

```
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.

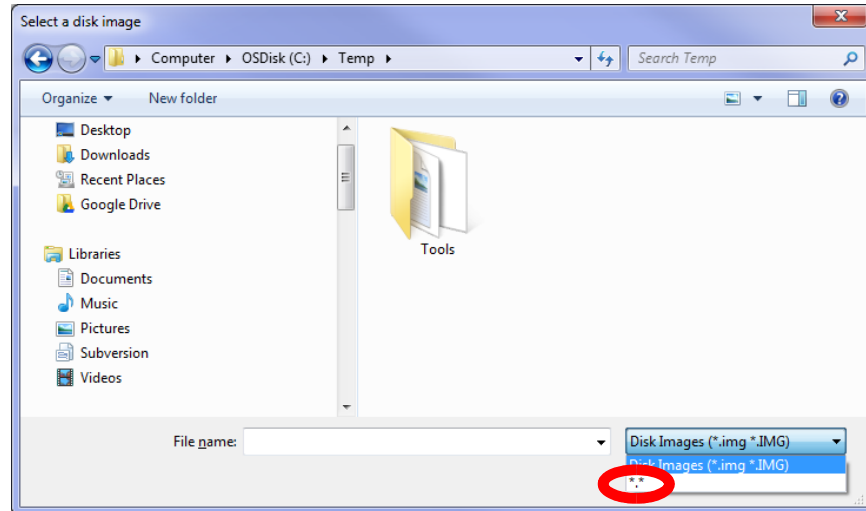
### A.1.4 Using Win32DiskImager (TaitCentOS Only)

1. To create a USB flash drive with TaitCentOS or node controller software, first download and install the Win32DiskImager application.

- ① Only install the TaitCentOS, 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.

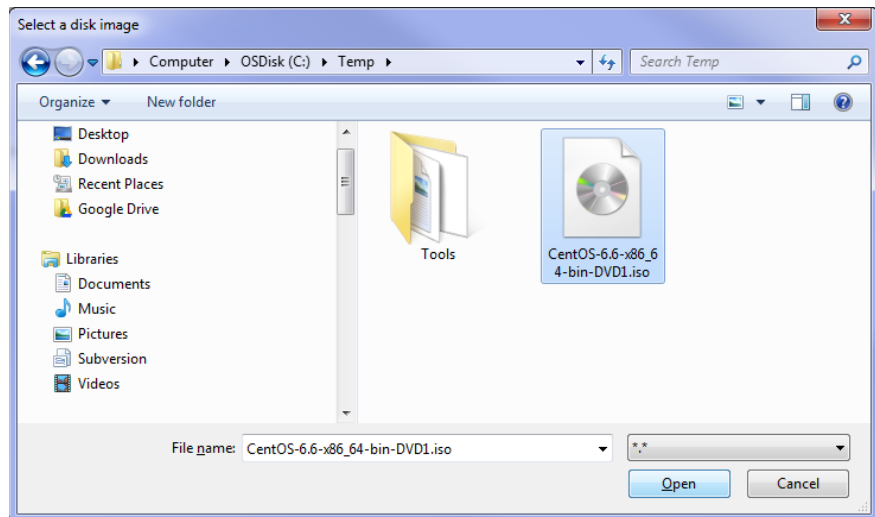


- 4. Check that the drive letter in the Device drop down list is the same as the USB flash drive. If you get this wrong, you could erase the wrong disk.
- 5. Click on the folder icon for the Image file.
- 6. Change the file filter from Disk Images (\*.img \*.IMG) to \*.\*.

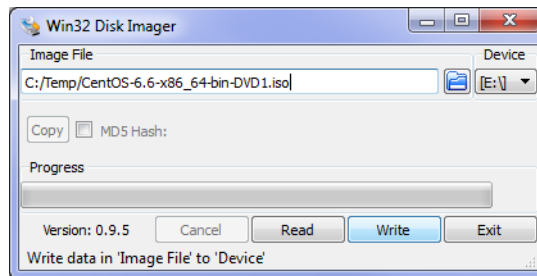




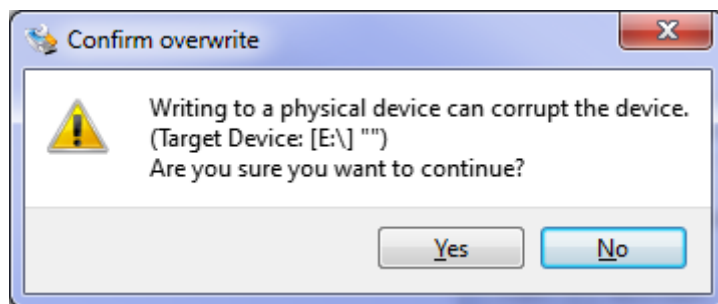
7. Select the desired iso file and click Open.



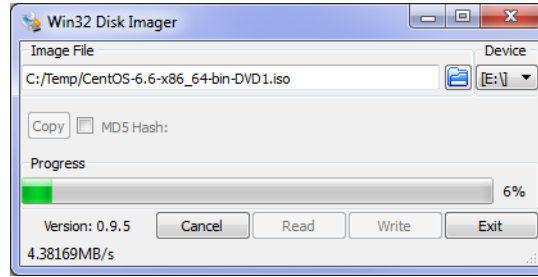
8. When ready to proceed, click Write.



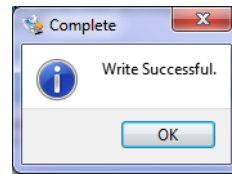
9. A Confirm overwrite dialog will appear which gives you a last chance to abort the process. Click Yes to continue.



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

---

## B.1 Deploying PTTToX in a DMR Trunked Network

This section provides a description of the steps required to configure a DMR trunked network for PTTToX.

The following applications will need to be installed/configured:

- TN9300 DMR trunked node controller
- Administration application
- Tait PTTToX connector
- TN9500 inter-network gateway

For information on installing/configuring the other parts of PTTToX, refer to the Tait PTTToX System Manual (MNE-00040-xx).

- ① The recommended maximum number of concurrent PTTToX calls is 40 when the PTTToX connector is running on a Dell R250 or Kontron CG2400 server. On a Sintrones SBOX-2621, the recommended maximum is 39.

### B.1.1 TN9300 DMR Trunked Node Controller Configuration

For installation information, refer to the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx).

- ① With TN9500 version 1.16.00 and PTTToX Connector version 1.08.18, the maximum fleet database size in the DMR Node is 1000 units.

#### Preparation and Configuration

1. Log in to the node WebUI.
2. Select Settings > License to ensure that an inter-network connections license (TNAS311) is present. If not, refer to the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx).
3. Select Telephony > SIP Groups, and create a SIP Group for the TN9500 PTTToX.
4. Select Interfaces > Inter-network Connections and create a connection to the TN9500 that is connecting to PTTToX.
  - In the Validation area, enter the same username and password used in the TN9500 to which this connection is being made.
  - In the Client area, select the SIP group created in Step 3, and ensure that the Invite without SDP parameter is disabled (i.e. unchecked).

5. Select Subscribers > Group Service Areas and add the TN9500.
6. For location services/AVL to work when the Tait AXIOM Mobile vehicle is not in DMR mode, the following items also need to be configured:
  - Select Subscribers > Fleets > Units to add a unit that will be allocated for AVL. Note down its DMR number.
  - Select Settings > Network Parameters and in the Features area, enter the DMR number noted above as the AVL monitor address.
7. For AVL to operate via the TN9500 using the DMR configured AVL monitoring address, the following entry should be added to the TN9300 node configuration file (`tait_dmrnc.cfg`):  

```
inp.allow_avl_registration:1
```

### B.1.2 Install TN9500 and PTTToX Connector Applications

To install the TN9500 and the PTTToX Connector applications, refer to 'Section 8 Installing the Tait Packages Using TaitCentOS' or 'Section 9 Installing the Tait Packages Using Tait Ubuntu' of the Tait Core Networks Installation and Configuration Manual (MNB-00012-xx).

### B.1.3 Administration Application Configuration

1. Log in to the Administration application.
2. Select Configuration > Network. In the Network Interface Card area, click the arrow in the Name dropdown box and select the third interface (the first two, br-xxx and docker 0, must not be changed). This is the physical interface that should be changed to the permanent IP address of the server, as follows:
  - Set the desired permanent IP address, Netmask, and Gateway IP address for this server.
  - In the General area, change the hostname to include TN9500 PTTToX.
  - Click Save. A reboot will now be required for the changes to take effect.
3. Select Configuration > NTP to set the time. The time must be the same as the DMR node.
4. Start the NTP service and check for connection.

## B.1.4 Tait PTTToX Connector Configuration

1. Log in to the PTTToX Connector application WebUI. You can browse to the PTTToX Connector application from the Administration application's Tait Services page.
2. Select General > Settings and click Edit.
3. In the Identity area, add the name of your PTTToX Connector. This will be displayed in the page header, together with the server name, for identification purposes.



**The fields in the Service area are required for connection to the PTTToX Cloud service.**

**They will be provided by Tait Services at the time of system deployment and are specific to your deployment. They should not be changed.**

**Please contact Tait Technical Support if more information is required.**

4. For Location reporting, enter the DMR unit number that was created for AVL in Step 6 of "[TN9300 DMR Trunked Node Controller Configuration](#)" on page 75.
5. The Location format has to match the format programmed into the terminals under Data Parameters > Location in the Terminals programming application.
6. Click Save.
7. Disable and enable PTTToX. Use the button in the Controls area of General > Settings to do this.



The connection from the TN9500 will not come up until the PTTToX connector has a connection to the PTTToX Core. Contact Tait Technical Support if further assistance is required.

## B.1.5 TN9500 Configuration



If one connection is made to a PTTToX Connector, then only one other connection is supported and that must be to a DMR Trunked network.

1. Log in to the TN9500 inter-network gateway application WebUI.
2. Select Settings > General and assign a name to the gateway.
3. Select Networks > Connections and click Add to create a connection to the DMR node, using the same username and password entered in Step 4 of "[TN9300 DMR Trunked Node Controller Configuration](#)" on page 75.

- ⓘ Make sure the Invite without SDP parameter is disabled.
4. Select Networks > Connections and click Add to create a connection to the PTTToX Connector. Populate the following fields as follows:
    - Network Type: select PTTToX
    - Username: **admin** (this is fixed internally in the PTTToX Connector)
    - Password: **tait** (this is fixed internally in the PTTToX Connector)
    - IP address: **172.51.1.1**
  5. To verify the connection, check its status on Networks > Connections, and to verify that radio registrations come through, check Networks > Registrations.
- ⓘ The connection from the PTTToX Connector will not come up until the connector has a connection to the PTTToX Core. Contact Tait Technical Support if further assistance is required.