# SCADA Gateway

# Installation and Configuration Manual

MNE-00020-03 · Issue 3 · May 2017

www.taitradio.com

## Contact Information

**Tait Communications**
**Corporate Head Office**

Tait Limited
P.O. Box 1645
Christchurch
New Zealand

For the address and telephone number of regional offices, refer to our website: www.taitradio.com

## Copyright and Trademarks

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

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

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

## Disclaimer

There are no warranties extended or granted by this document. Tait 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 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 Limited together with their international equivalents, pending patent or design applications, and registered trade marks: NZ409837, NZ409838, NZ415277, NZ415278, NZ524509, NZ530819, NZ534475, NZ547713, NZ577009, NZ579051, NZ579364, NZ586889, NZ593887, NZ610563, NZ615954, NZ700387, NZ708662, NZ710766, NZ711325 , NZ726313, AU2015215962, AU339127, AU339391, AU2016259281, AU2016902579, EU000915475-0001, EU000915475-0002, GB2532863, US14/834609 Div. no 1, US15/346518 Div. no 2, US15/350332, US15/387026 Div., US20150085799, US20150350090, US20160044572, US20160057051, US640974, US640977, US698339, US702666, US7758996, US7937661, US8902804, US9107231, US9504034.

This product may also be made under license under one or more of the following U.S. Patents: 5,146,497, 5,148,482, 5,164,986, 5,185,795, 5,185,796, 5,271,017, 5,377,229 and 5,502,767.

This product may also be made under license under one or more of the following patents:
- US7203207, AU2004246135, CA2527142, GB2418107, HK1082608, MY134526, US8306071
- US7339917, AU2004246136, CA2526926, GB2418812, MY134217
- US7499441, AU2005262626, CA2570441, GB2430333, JP4690397, NZ551231, KR100869043, RU2351080, BRP10512052, MXPA06015241
- US 7200129, AU2005226531, CA2558551, CN1930809, GB2429378, JP4351720, BRP10508671, NZ549124, KR848483, RU2321952

## Environmental Responsibilities

Tait 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.taitradio.com/weee. Please be environmentally responsible and dispose through the original supplier, or contact Tait Limited.

Tait Limited also complies with the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Directive in the European Union.

In China, we comply with the Measures for Administration of the Pollution Control of Electronic Information Products. We will comply with environmental requirements in other markets as they are introduced.

# Contents

**Preface** . . . . . **5**
Scope of Manual . . . . . 5
Document Conventions . . . . . 5
Alerts . . . . . 5
Associated Documentation . . . . . 5
Publication Record . . . . . 6

**1 Introduction** . . . . . **8**
1.1 Overview . . . . . 8
1.2 SCADA Gateway Components . . . . . 9
1.2.1 SCADA Gateway . . . . . 9
1.2.2 TD9300 Data Terminals . . . . . 9
1.3 Tait TN9300 DMR Trunked Network . . . . . 9

**2 Installation** . . . . . **10**
2.1 Before You Start . . . . . 10
2.1.1 High Availability . . . . . 11
2.2 Installing the SCADA Gateway on the DMR Node Controller . . . . . 11
2.2.1 CentOS . . . . . 11
2.2.2 Solaris . . . . . 12
2.3 Installing the License Files . . . . . 15
2.3.1 Obtaining the Host ID for Requesting the License File . . . . . 15
2.3.2 Uploading the license . . . . . 16
2.4 Recovering the DMR Node . . . . . 16
2.4.1 CentOS . . . . . 16
2.4.2 Solaris . . . . . 16
2.5 Creating Your Custom ‘ssh’ Login Script . . . . . 17
2.6 Creating Your Custom Web Login Script . . . . . 18

**3 Configuration** . . . . . **19**
3.1 Configuring the DMR Node Controller . . . . . 19
3.2 Logging on to the SCADA Gateway WebUI . . . . . 22
3.3 Configuring a Primary SCADA Gateway . . . . . 23
3.3.1 Creating a Division . . . . . 23
3.3.2 Adding TD9300 Data Terminals . . . . . 23
3.3.3 Configuring the SCADA Gateway . . . . . 24
3.3.4 Setting up the SCADA Gateway for High Availability . . . . . 25
3.4 Configuring a Secondary SCADA Gateway . . . . . 26
3.4.1 Configuring the SCADA Gateway . . . . . 26
3.4.2 Setting up the SCADA Gateway for High Availability . . . . . 26


© Tait Limited May 2017

3.4.3 Synchronizing the Secondary SCADA Gateway Database . . . . . 27

**4 Administrating the SCADA Gateway . . . . . 28**

4.1 Logging on to the SCADA Gateway . . . . . 28

4.2 Logging on to the SCADA Gateway as ‘root’ . . . . . 28

4.3 Self-Signed SSL Certificates . . . . . 29

4.3.1 Firefox Users . . . . . 29

4.3.2 Internet Explorer Users . . . . . 31

4.3.3 Chrome Users. . . . . 33

4.4 Using the Certificate from a Certification Authority (CA) . . . . . 34

4.5 Changing the ‘root’ and ‘taitnet’ Passwords . . . . . 35

4.6 Stopping/Starting the SCADA Gateway Software. . . . . 36

4.7 Changing to a Local Time Zone. . . . . 36

4.7.1 CentOS. . . . . 36

4.7.2 Solaris . . . . . 37

4.8 SCADA Gateway Resource File . . . . . 38

**5 Uploading SCADA Gateway Firmware. . . . . 41**

5.1 Uploading a New Firmware Version . . . . . 41

5.2 Upgrading the SCADA Gateway to a New Firmware Version . . . . . 41

5.3 Reverting to an Earlier Firmware Version . . . . . 42

**6 Backing up/Restoring Configuration Files . . . . . 43**

6.1 Manual Backup. . . . . 43

6.2 Restoring a Backup File . . . . . 43

**Appendix 1: Transferring an ISO Image to a USB Flash Drive. . . . . 45**

1.1 Using Rufus . . . . . 45

1.2 Using Win32DiskImager . . . . . 48

**Appendix 2: Adding an Alternate Interface in CentOS . . . . . 51**

**Tait Software License Agreement . . . . . 52**


© Tait Limited May 2017

# Preface

## Scope of Manual

This SCADA Gateway Installation and Configuration Manual provides information on installing and configuring a SCADA gateway in a Tait DMR Tier 3 trunked network when operating with the Q9391NC software version 2.04 or later.

## Document Conventions

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`**

## Alerts

Please follow exactly any instruction that appears in the text as an alert. An alert provides necessary safety information as well as instruction in the proper use of the product. This manual uses the following types of alert:

**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.

## Associated Documentation

TD9300 Data Terminal Installation and Configuration Manual (MNE-00003-**xx**).

TN9300 DMR System Manual (MNB-00003-xx).

The characters **xx** represent the issue number of the documentation.

Always get the latest issue of a manual from the Tait support website. Also available on the website are software release notes, and technical notes (TNs) which provide technical details not yet in the manuals, or solve any problems that may have arisen.


© Tait Limited May 2017

# Publication Record

| Issue | Publication Date | Description |
|---|---|---|
| 1 | June 2015 | First release. SCADA gateway version 1.00. |
| 2 | December 2016 | Updated for SCADA gateway version 1.04 and later<br>■ Section 1.3 Tait TN9300 DMR Trunked Network updated<br>■ Section 2.1 Before You Start updated<br>■ Section 2.2 Installing the SCADA Gateway on the DMR Node Controller updated<br>■ Section 2.3.1 Obtaining the Host ID for Requesting the License File updated<br>■ Section 2.4 Recovering the DMR Node updated<br>■ Section 2.4 Recovering the DMR Node updated<br>■ Section 2.6 Creating Your Custom Web Login Script updated<br>■ Section 3.1 Configuring the DMR Node Controller updated<br>■ Section 3.3 Configuring a Primary SCADA Gateway updated<br>■ Section 3.3.4 Setting up the SCADA Gateway for High Availability added<br>■ Section 3.4 Configuring a Secondary SCADA Gateway added<br>■ Section 4.4 Using the Certificate from a Certification Authority (CA) updated<br>■ Section 4.6 Stopping/Starting the SCADA Gateway Software updated<br>■ Section 4.8 SCADA Gateway Resource File added<br>■ Section 6 Backing up/Restoring Configuration Files updated<br>■ Appendix 2:Adding an Alternate Interface in CentOS updated |


© Tait Limited May 2017

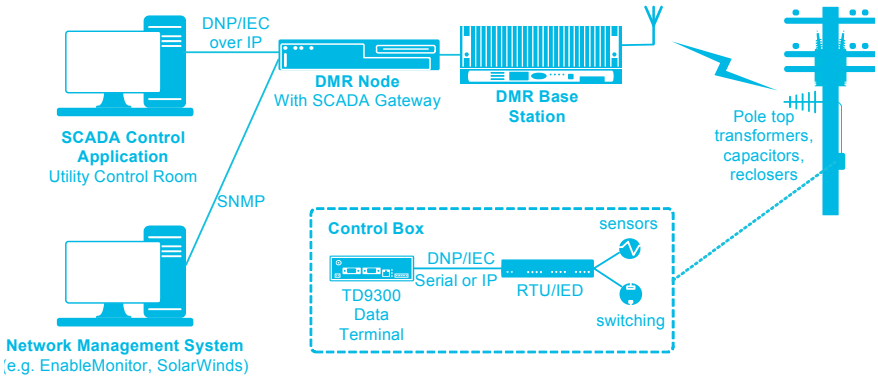
| Issue | Publication Date | Description |
|---|---|---|
| 3 | May 2017 | Updated for SCADA gateway version 1.06 and later<br>■ Terminology: ‘Dip line’ changed to ‘DIP connection’ throughout<br>■ Section 2.2.2 Solaris updated<br>■ Section 3.2 Logging on to the SCADA Gateway WebUI added<br>■ Section 3.3.3 Configuring the SCADA Gateway updated<br>■ Section 4.5 Changing the ‘root’ and ‘taitnet’ Passwords updated<br>■ Section 4.7 Changing to a Local Time Zone added |


© Tait Limited May 2017

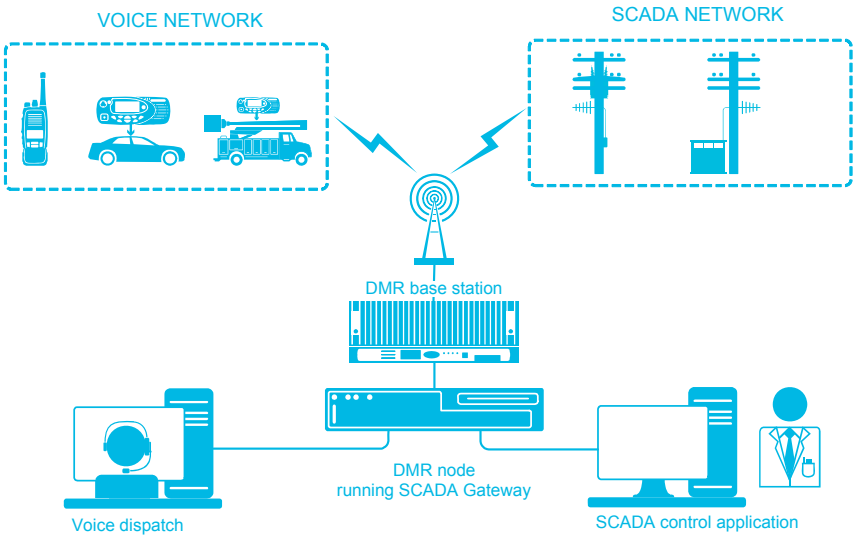
# 1 Introduction

## 1.1 Overview

The Tait SCADA gateway solution delivers reliable, scalable and secure two-way wireless communications between a SCADA control system and the outstation devices on electricity distribution networks. Built on the Tait DMR Tier 3 trunked network, a SCADA gateway and TD9300 Data Terminals are added that pass messages between the SCADA control system and remote outstation devices (RTUs). In this way, the power distribution network can be monitored so that faults can be quickly identified and resolved.




A Tait DMR network with a SCADA gateway provides a dual-purpose network that handles voice for communication with mobile field workers as well as data for monitoring and controlling outstation devices.





© Tait Limited May 2017

## 1.2 SCADA Gateway Components

### 1.2.1 SCADA Gateway

The Tait SCADA gateway provides the interface between the SCADA control system and the DMR network. Its primary function is to control the transfer of messages from the SCADA control system to SCADA outstation devices. As it has detailed knowledge of the current network load, it can queue and prioritize SCADA messages to and from the SCADA outstation devices, ensuring reliable communications under both normal and fault conditions.

The SCADA gateway application is normally co-located on the DMR control node, but can be installed on its own server.

The SCADA gateway supports DNP3 over Ethernet and IEC 60870-5-104 protocols for linking to SCADA control systems.

### 1.2.2 TD9300 Data Terminals

TD9300 data terminals connect over the DMR network to exchange DMR control channel and packet data messages with the SCADA gateway. They forward received messages to their SCADA outstation device (or RTU).

The data terminals support both serial and Ethernet SCADA interfaces to the SCADA outstation device, including

- DNP over TCP/IP, UDP and RS232
- IEC 60870-5-101
- IEC 60870-5-104

## 1.3 Tait TN9300 DMR Trunked Network

The Tait TN9300 DMR Trunked network is a wide-area trunked radio communications network that follows the Digital Mobile Radio open standard. It consists of one or more nodes controlling the operation of the network together with a number of sites, each consisting of several base stations within a local area network. An IP backbone links the nodes and sites together.

The base stations provide the RF interface to the mobiles, portables and Data Terminals that use the network. For more information, see the System Overview for Tait TN9300 DMR Trunked Networks.


© Tait Limited May 2017

# 2 Installation

The SCADA gateway application runs on the CentOS operating system.

The SCADA gateway can be deployed using either the Kontron CG2300 server, the Dell R230/R220, the Aleutia R50, or as a virtual machine on a Sun Netra X3-2 server. (Note that the Sun Netra X3-2 server is no longer available for new deployments (replaced by Kontron CG2300) but is still supported for deploying the SCADA gateway to operating DMR networks.)

The SCADA gateway application can run on the same server as the DMR node or on a standalone server. If deployed on a Sun Netra X3-2 server with the Solaris operating system then the SCADA gateway application is run in a virtual machine hosted in Solaris. If deployed with a CentOS DMR node then the SCADA gateway application is installed alongside the DMR node application.

Depending on network size and redundancy requirements, it may be advantageous to run the SCADA gateway on its own server hardware, separate from the DMR node. In this case, it is recommended that the same model or type of server hardware is used for both DMR node and SCADA gateway to simplify and provide the same level of management.

Refer to the TN9300 Node Controller Installation Manual (MNB-00001-xx) for information pertaining to the DMR system.

Installation is designed to occur without having to take the DMR node offline, and with no disruption to service. However, recovery and safety measures are also provided, in the unlikely event issues arise with the installation.

## 2.1 Before You Start

Ensure that you have the following before beginning the installation:

- host name of the node controller
- IP address of the node controller
- IP address plan for the DMR network
- IP address plan for the SCADA gateway (and TD9300 data terminals)
- IP address of the router/gateway
- sufficient DIP licenses
- PuTTy (www.putty.org)
- SCADA Gateway Installation CD


© Tait Limited May 2017

SCADA gateway license(s) can be obtained only after the SCADA gateway software has been installed.

### 2.1.1 High Availability

When installing an HA system, the following rules should be applied:

1. The Active IP address for the SCADA gateways should be different from the Active IP address for the DMR nodes.
2. The SCADA gateway(s) should access the active IP address of the DMR HA nodes regardless of whether or not they are co-hosted.
3. A co-hosted DMR node and SCADA gateway may use the same IP address (e.g. the `eth0` primary address), but it is recommended to either configure a static IP address on a separate NIC e.g. `eth1`, or a sub interface e.g. `eth0:2`. (See Appendix 2: Adding an Alternate Interface in CentOS)

   The DMR node always uses `eth0` and `eth0:1`, so the SCADA gateway must use the alternative interface. The interface name e.g. `eth0:2` or `eth1` is configured in the file `/home/taitnet/scadagw/scadagw.cfg` with key `NetworkDevice`.

## 2.2 Installing the SCADA Gateway on the DMR Node Controller

### 2.2.1 CentOS

Refer to the TN9300 Node Controller Installation Manual (MNB-00001-xx) for instructions on installing CentOS and the DMR node, if required.

1. Install CentOS.
2. Install DMR node.
3. Install the SCADA gateway:
   a. The installer is provided in an iso image `Q9361RH6_<version number>.iso`
   b. Create a USB flash drive containing the SCADA gateway installer as described in Appendix 1: Transferring an ISO Image to a USB Flash Drive.
4. Insert the USB drive.
5. As root user, enter the following

```
# cd /cdrom
# ./install
```


© Tait Limited May 2017

**Notice** The Dell R230 server can only be booted up by a USB type 3.0 flash drive. When installing software on a Dell R230, 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 for CD/DVD ROM installation instructions.

### 2.2.2 Solaris

**DMR**

1. Back up the DMR node controller database.
2. Ensure the databases on the DMR switching node(s) and control node are synchronized.
3. Ensure the DMR node firmware is up to date with a version compatible with the SCADA gateway (DMR node version 2.06 or later).
4. Insert the SCADA Gateway Installation CD.
5. Use an SSH terminal application (PuTTY) to connect to the IP address of the DMR node, using `taitnet` and `tait` as the default username and password.
6. Switch to root by entering:
   **`su`**
   **`k1w1`**
7. To mount the CD, enter:
   **`mount -F hsfs /dev/dsk/c1t0d0s0 /cdrom`**

   If this does not work, the device name may be different, in which case the following procedure will enable you to ascertain the correct device name:

   a. Enter **`iostat -En`** to list all the devices and look for the CD/DVD drive (this will be similar to `Product: DV-W28SS-V` or `Product: CD/DVDW`). See sample below:
   ```
   iostat -En
   c1t4d0 Soft Errors:0 Hard Errors:0 Transport Errors:0
   Vendor: TEAC Product: DV-W28SS-V  Revision: 1.0B
   Serial No:
   Size: 1.13GB <1132068864 bytes>
   Media Error :0 Device Not Ready: 0 No Device: 0
   Recoverable: 0
   Illegal Request: 3 Predictive Failure Analysis: 0
   ```
   b. Use the corresponding device name and add s0, as follows:
   **`mount -F hsfs /dev/dsk/c1t4d0s0 /cdrom`**
8. Change the current working directory by entering:
   **`cd /cdrom`** (press Enter)
   **`ls`** (press Enter)


© Tait Limited May 2017

a. If you can find the following sub-directories, then please proceed to step 9:

```
README
installvm
startup
vmnetconf
app packages
vbox
waitforvmtoboot
installapp
rebootvm
vm
```

b. If `cdrom0` is the only sub-directory you can observe, please enter:

**`cd /cdrom/cdrom0`** (press Enter)

9. Find the network interface that will be used for the Virtual Machine; type:

   **`ifconfig -a`**

   Look at the result and find the network interface which contains the node's IP address.

   In the following example the IP address of the DMR node controller is 172.29.0.101, and this is assigned to the network interface called e1000g0:

   ```
   lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTI-
   CAST,IPv4,VIRTUAL> mtu 8232 index 1
   inet 127.0.0.1 netmask
   e1000g0: flags=1000843<UP,BROADCAST,RUNNING,MUL-
   TICAST,IPv4> mtu 1500 index 2
   inet 172.29.0.101 netmask fffff000 broadcast
   172.29.0.255
   ```

10. Install virtual box and the virtual machine.

    Making sure you are still logged on as the root user, type the following:

    **`./installvm <network-interface>`**

    Replace <*network-interface*> with the identifier found in Step 9; the install script will display progress information during the installation process; it will take a couple of minutes to run.

    For our example configuration this would be:

    ```
    ./installvm e1000g0
    ```

11. Configure networking on the Virtual Machine.

    The IP address, netmask, and default gateway assigned for the SCADA gateway are needed.

**Do not use the same IP address for the DMR node controller and the SCADA gateway.**


© Tait Limited May 2017

Netmask and default gateway MUST be the same as that used by the DMR node controller.

Enter the following:

**./vmnetconf <*ip-address*> <*netmask*> <*default-gateway*>**

The Virtual Machine will automatically reboot after applying the required changes.

Test if address assignments are successful by pinging the Virtual Machine from the DMR node controller.

Enter:

**ping <*SCADAGateway-ip-address*>**

A succesful ping will return:

`<SCADAGateway-ip-address> is alive`

12. Look up the filename of the SCADA gateway software:

    **cd /cdrom/app**

    **ls -l**

    The SCADA gateway software is contained in an iso image with a filename similar to `Q9361RH6_01.04.02.423330.iso` (the numbers at the end of the file name are the version number).

13. To install the SCADA gateway software on the Virtual Machine, enter the following, using the filename acquired above:

    **cd ..**

    **./installapp app/<*filename*>**

**DMR**

14. Check the DMR node controller is operating correctly by making calls, checking log and alarm files etc.

**SCADA Gateway**

15. Check the SCADA gateway is running as follows:

16. Access the SCADA gateway WebUI by entering:

    **https://<*SCADAGateway-ip-address*>**

    or

    **https://<*SCADAGateway-ip-address*>:17443** for gateway v1.04 or higher

17. Log on using the following login credentials:

    username: `taitnet`
    password: `tait`

**Ejecting the CD**

1. Use an SSH terminal application to connect to the IP address of the DMR node, using `taitnet` and `tait` as the default username and password.


© Tait Limited May 2017

2. Switch to root user by entering[1]:

   **su**

   **k1w1**

3. Stop the volume management by entering:

   **/etc/init.d/volmgt stop**

4. Move out of the CDROM directory and unmount the DVD:

   a. If the DVD ROM directory is /cdrom:

      **cd / && umount /cdrom**

   b. If the DVD ROM directory is /cdrom/cdrom0:

      **cd / && umount /cdrom/cdrom0**

5. Start the volume management by entering:

   **/etc/init.d/volmgt start**

6. Eject the CD either by pressing the eject button on the DVD drive, or by using the following command:

   **eject cdrom**

## 2.3 Installing the License Files

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

License files can only be generated by Tait and each SCADA gateway must have its own unique license. If the SCADA gateway has been set up by Tait then an appropriate license file will have been installed. If not, then the following procedures should be followed to obtain a valid license file.

### 2.3.1 Obtaining the Host ID for Requesting the License File

To obtain the host ID:

1. Log on to the SCADA gateway. The host ID can be found in Settings > Local Parameters > Identity > Host ID.

2. Once you have provided the host ID and required features to Technical Support at Tait, you will be provided with a license file called `TN9300-3_<hostid>_xxxx.lic`. Rename and save the file as `license.dat` before uploading the license to the SCADA gateway.

---

1. See Section 4.5 Changing the ‘root’ and ‘taitnet’ Passwords for instructions on changing the root password.

### 2.3.2 Uploading the license

1. To install the license file on the SCADA gateway, go to the SCADA gateway web browser and select Settings > Local Parameters then click Edit.
2. At the License file field, click Upload > Choose file to select a license file, then click Open.
3. Once the license file has uploaded, the SCADA gateway will check if the license is valid.

## 2.4 Recovering the DMR Node

### 2.4.1 CentOS

**In the event issues with the operation of the DMR node are observed during installation, DO NOT uninstall the SCADA gateway, as this attempts to remove the taitnet user account from which the DMR node is run.**

To disable the SCADA gateway service, execute the following commands as root user:

```
# service scadagw stop
# rm -f /etc/rc0.d/K50scadagw
# rm -f /etc/rc2.d/K50scadagw
# rm -f /etc/rc3.d/S99scadagw
# rm -f /etc/init.d/scadagw
```

### 2.4.2 Solaris

In the event issues with the operation of the DMR node are observed during installation, it is essential that the node is taken back to a known working state to ensure minimum disruption to network service. The following steps detail how to achieve this.

1. If you have not already done so, insert the USB flash drive. (See Section 2.2 Installing the SCADA Gateway on the DMR Node Controller.)
   a. Once you are in the right sub-directory (`cdrom` or `cdrom0`), enter the following command:
      **`ls`**
   b. If you can see the file `installvm`, enter the following command:


© Tait Limited May 2017

```
./installvm clean
```

This will remove the Virtual Machine, and thus the SCADA gateway, and should place the node in the same state it was in prior to installation of the Communications Server

2. If Step 1 is unsuccessful, it is necessary to remove the Virtual Machine manually: use ssh to log into the node as user `taitnet`, and then:

   ```
   VBoxManage controlvm Q9361VM poweroff
   VBoxManage unregistervm Q9361VM –delete
   ```

   Now uninstall the startup script:

   ```
   rm -f /etc/rc3.d/S90vbox
   ```

   Now remove the virtual box software:

   ```
   VBoxManage extpack uninstall "Oracle VM VirtualBox Extension Pack"
   pkgrm -n -a /opt/VirtualBox/autoresponse SUNWvbox
   ```

3. If Step 2 is unsuccessful, in a multi node system, change a Switching Node mode to Control Node and contact Tait Technical Support to ascertain what steps to take.

## 2.5 Creating Your Custom 'ssh' Login Script

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

1. Locate (or write) a file with the login script required (see example below).

2. Copy this file to the `/etc` directory, and name it `issue`:

   ```
   # mv <path to login script> /etc/issue
   ```

3. Change the ownership and group of the file to `root`:

   ```
   # chown root:root /etc/issue
   ```

4. Check the ownership and permissions:

   ```
   # ls -l /etc/issue
   ```

5. If permissions are not `-rw-r--r--` make them so:

   ```
   # chmod 644 /etc/issue
   ```

**Sample login script**

"WARNING! THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS ONLY!

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


© Tait Limited May 2017

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

## 2.6 Creating Your Custom Web Login Script

It is recommended that you create a login script. This is the script that is displayed to the user when they log in from a web browser on your network.

1. Locate (or write) a file with the login script required.
2. Copy this file to the `/home/taitnet/scadagw/html` directory, and name it `index.html`:

   **# mv <*path to login script*> /home/taitnet/scadagw/html/index.html**


© Tait Limited May 2017

# 3 Configuration

Configure the DMR node for SCADA gateway operation first, before configuring the SCADA gateway itself.

## 3.1 Configuring the DMR Node Controller

For successful SCADA gateway operation on a DMR Network, the node must first be updated and configured with the correct firmware version and license keys.

This must be done before installing the components required to interface to the TD9300 data terminals and SCADA outstations.

ⓘ A different fleet identity is recommended for the SCADA gateway and TD9300 data terminals to keep them separate from the DMR voice subscribers. This will assist in channel partitioning at sites that are to be used for both DMR voice and SCADA gateway packet data calls.

1. Upgrade the node to the latest release required for SCADA gateway operation (version 02.06 and later).
2. Create a partition class for the following with an appropriate address range and call rights:
   - SCADA gateway packet data
   - DMR voice traffic
   a. Select Subscribers > Partition Classes and then click Add.
   b. Enter a name and optionally a comment about the partition class.
   c. Enter start and end addresses to define the range of radio addresses that can use the partitions assigned to this partition class.
   d. Select the call types that will be allowed to use the partitions assigned to the partition class.
   e. Under Access Level, select the call priority levels that will be allowed to use the partitions assigned to the partition class.
   f. Click Save.
3. To partition the sites as required, assign one traffic channel to accommodate voice + data and the remaining traffic channels as voice only:
   a. Select Network > Sites
   b. From the Site Status page, click the Partitions tab and then click Edit.
   c. To add a partition to the bottom of the list, click Add. To add a


© Tait Limited May 2017

partition elsewhere in the list, select the row that will be below the partition you wish to add and click Insert.

d. Select a partition class from the drop-down list. (This must have been previously created in Subscribers > Partition Classes, see Step 2).

e. In the Start and End boxes, enter the range of channel ID numbers for the channels that will belong to the partition.

f. Click Save.

4. Assign an appropriate service area for all TD9300 data terminals:

a. Select Subscribers > Unit Service Areas and then click Add.

b. Enter a name and optionally a comment about the unit service area.

c. Select one or more sites and then use the Service drop down list at the bottom of the table to select whether service is Allowed or Not Allowed for your selection.

d. Click Save.

**For system stability and traffic loading predictability it is recommend that the TD9300 data terminal service area be restricted to only the sites that it is allowed to use, as dictated by the coverage and traffic planning. For system resilience/reliability the service area for any individual TD9300 data terminal can be more than one site as long as the system design allows for it.**

5. Create two new unit profiles, one to assign to the SCADA master, and one to assign to all TD9300 data terminals:

a. Select Subscribers > Unit Profiles and then click Add.

b. Enter a name and optionally a comment about the unit profile.

c. Fill in the fields in the page to configure access, timers, supplementary data and call types (call types **must** include Packet data).

d. Click Save.

6. Add a new Fleet to assign to the SCADA gateway and data terminals:

Make sure that you assign sufficient numbers to allow for future expansion. Once a fleet is defined, it cannot be expanded. The only way to enlarge an existing fleet is to check that there is enough room first, delete the old fleet, then recreate it from scratch as a new, larger fleet.

a. Select Subscribers > Fleets and then click Add.

b. Enter a name and optionally a comment for the fleet.

c. Optionally enter the name of an administration group. If you do enter an administration group then only users in the same group will be able to view or edit the fleet and the units/groups that belong to it.


© Tait Limited May 2017

d. Enter a prefix number. The fleet will be part of this prefix.

e. If the network uses MPT1343 numbering, follow these steps:

- Enter the number of units and the number of groups for allocation to the fleet.
- Click Find Space. The node calculates values for the FIN and FGN fields
- If desired, you can edit the calculated values (these will be checked when you click Save).

f. If the network uses ANN numbering, follow these steps.

- Select the fleet size (Large, Small, or Mini).
- Click Find Space. The node calculates values for the L and R (rr) fields. (The node displays an error message if the ANN numbering model does not allow the fleet size you selected or if there is not enough room in the prefix.)
- If desired, you can edit the calculated values (these will be checked when you click Save).

When adding fleets to networks with ANN numbering, the FPP and MEP for a prefix must first be defined under Settings > ANN Fleet Parameters.

g. If the network uses MPT 1327 numbering, follow these steps:

- Enter the prefix.
- Enter the number of units and the number of groups for allocation to the fleet.
- Click Find Space. The node calculates values for the Base unit and Base group fields.
- If required, you can manually edit the calculated values (these will be checked when you click Save).

h. Click Save.

7. Add the DIP connection that will be used by the SCADA gateway / SCADA master:

This must match the allocation in the fleet and must match that programmed into the SCADA gateway.

a. Select Interfaces > DIP Connections and then click Add.

b. Enter a name and other details as required for the DIP connection. Note that the Maximum packet data size must be set to 1382.

c. Click Save.

A single DIP connection can service up to 20 simultaneous calls. If you predict that the SCADA system will need to make more than 20 simultaneous calls then more than one DIP connection will be needed in the DMR Node and more than one division will be needed in the SCADA gateway.


© Tait Limited May 2017

8. Add the DMR addresses of the TD9300 data terminals and the SCADA master DIP connection to the fleet created in Step 6.
   a. Select Subscribers > Fleets and then click the fleet that the data terminals will belong to.
   b. Click the Units tab and then click Add. The Add Unit page appears.
   c. Enter the terminal number. This must be a number that lies within the number range assigned to the fleet. If you add multiple terminals, they will be numbered starting from this number.
   d. Optionally add a comment to give more information about the terminal.
   e. Optionally enter the terminal's authentication key. This is the factory-programmed authentication key that is checked by the node to ensure that a terminal registering on the network is genuine. (Use the terminal's serial number as the authentication key.)
   f. If you want to add more than one terminal, enter the number of terminals into the Number of units to add box.
   g. Select a profile, and service area from the drop-down lists.
   h. Click Save.
9. Ensure the node is licensed for sufficient DIP calls (TNAS303).
10. Ensure the node is licensed for sufficient data calls (TNAS305).
11. In the event issues are encountered subsequent to installation, refer to Section 2.4 Recovering the DMR Node.

## 3.2 Logging on to the SCADA Gateway WebUI

For SCADA gateways running firmware versions up to 1.03, on your PC web browser enter the following:

**https://<*SCADAGateway-ip-address*>**

For SCADA gateways running firmware versions 1.04 and later, on your PC web browser enter the following:

**https://<*SCADAGateway-ip-address*>:17443**

In High Availability configurations, access to the WebUI is only allowed to the actual IP address for the SCADA gateway as specified in the Network Connection tab. Accessing the WebUI using the active SCADA gateway IP address will not work.

**Supported Browsers**

WebUI access has been tested on the following browsers, and are therefore recommended for use:

- Mozilla Firefox
- Google Chrome


© Tait Limited May 2017

- Internet Explorer (Version 7 and above)

## 3.3 Configuring a Primary SCADA Gateway

Use this section to configure a primary SCADA gateway. The primary SCADA gateway is the gateway with the highest High Availability priority (lowest priority number) in the network.

### 3.3.1 Creating a Division

1. Log on to the SCADA gateway WebUI using the following login credentials:

   username: `taitnet`
   password: `tait`

2. Select Network > Divisions and click Add.
3. Enter the name and DIP address of your SCADA gateway.
4. Click Save.

### 3.3.2 Adding TD9300 Data Terminals

ⓘ The SCADA gateway mode must be set to Online and the Gateway state must be Active prior to adding data terminals.

1. Select the Configuration tab (Network > Divisions, then select division to which to add terminals).
2. Click Add.
3. Enter the Radio Address of the TD9300 data terminal.
4. Select the division to which it belongs from the drop down menu.
5. Select the Tx rate. Normally it will be Full
6. Leave the Preemption disabled option unchecked. This should only ever be enabled during a patch upgrade of the data terminal.
7. Enter the port number on the SCADA gateway that the SCADA master will use to communicate with the RTUs via the data terminal.
8. Enter an encryption password, if required.
9. Enter the routable IP addresses that can be reached via this data terminal. A netmask can also be included as part of the IP address, e.g. 10.100.2.0/24.


© Tait Limited May 2017

10. Select the SCADA protocol that is in use from the drop down menu, and enter the SCADA address of the RTU to which the TD9300 data terminal is connected. If only IP is being used, select None.

11. In the Port field, enter the TCP port number.

12. Click Save.

13. Repeat Step 2 to Step 12 as required.

### 3.3.3 Configuring the SCADA Gateway

1. Select Settings > Local Parameters and click Edit.

2. In the General area, enter the name of the SCADA gateway.

3. In the Network Connection area, enter the IP address of the SCADA gateway, and the same subnet mask and default gateway IP addresses as entered on the DMR Node WebUI under Settings > Local Parameters > Network Connections.

4. In the Network Checks area, enter the IP addresses of up to two network elements to run checks that the SCADA gateway is connected to them. At least one entry is required. For example, enter the IP address of the Ethernet switch to which the SCADA Gateway is connected.

5. In the Node Connection area, add the DMR network node IP addresses as required.

6. In the SNMP area, click on 'click to download' if MIBs are required, and optionally enter the SNMP community string and the IP addresses for up to two recipients of SNMP traps.

7. In the NTP area, enter the IP address of the NTP source if required.

8. Configure Logging as required:
   a. Select the logging level from the drop-down menu.
   b. Enter up to two IP addresses for external syslog collection.
   c. Select the Syslog protocol from the drop-down menu.
   d. Select the level of alarms to be sent to the syslogger(s) from the Syslog severity drop-down menu.

9. In the License area, click the Upload button to select a license file to upload.

10. Click Save.

11. Select Settings > Network Parameters and click Edit.

12. Edit the Timers area as required, or accept the default settings.


© Tait Limited May 2017

a. Response delay is the time, in milliseconds, that the gateway should wait for a response to a message from a data terminal, or its connected equipment, to reply to a request.

b. Queue message timeout is the length of time a message will be queued before timing out when the gateway is busy.

13. In the SCADA area, select the protocol to use and the default port number to be monitored for communications from all/any data terminals.

14. In the IP area, enter the range of the IP addresses of the RTUs in CIDR format, under Remote IP Network. The IP address range entered should include all IP addresses entered as 'routable IP addresses' in the TD9300 data terminal configuration. If multiple ranges are required, enter them as a space separated list.

15. Click Save.

16. Select Settings > DMR Site Parameters and click Add.

17. For each DMR site as required, add the site ID and maximum number of concurrent call setup attempts allowed at that site.

18. Click Save.

### 3.3.4 Setting up the SCADA Gateway for High Availability

1. The different SCADA gateways that need to communicate need to be added to the Gateways list, including the localhost.

   a. Select Network > Gateways and click Add.

   b. Enter the Name, an optional Comment and the IP address of this SCADA gateway and click Save.

   c. Repeat steps 1 and 2 for each SCADA gateway in the network.

2. Assign the HA Active IP address and the SCADA gateway HA Priority.

   a. Select Settings > Local Parameters and click Edit.

   b. Under the High Availability section enter the assigned Priority and Active SCADA gateway IP address for this gateway (priority 1 is the highest priority) and click Save.

   c. The gateway needs to be rebooted to apply the changes. To reboot the gateway, connect to it by SSH and login as root (see Section 4.1 and Section 4.2). Issue the command **`reboot`**.

ⓘ If the SCADA gateway is running on a CentOS DMR node this will also reboot the DMR node.


© Tait Limited May 2017

## 3.4 Configuring a Secondary SCADA Gateway

Use this section to configure a secondary SCADA gateway. The primary SCADA gateway must already be configured and online.

### 3.4.1 Configuring the SCADA Gateway

1. Select Settings > Local Parameters and click Edit.
2. In the General area, enter the name of the SCADA gateway.
3. In the Network Connection area, enter the IP address of the SCADA gateway, and the same subnet mask and default gateway IP addresses as entered on the DMR Node WebUI under Settings > Local Parameters > Network Connections.
4. In the SNMP area, click on 'click to download' if MIBs are required, and optionally enter the SNMP community string and the IP addresses for up to two recipients of SNMP traps.
5. In the NTP area, enter the IP address of the NTP source if required.
6. Configure Logging as required:
   a. Select the logging level from the drop-down menu.
   b. Enter up to two IP addresses for external syslog collection.
   c. Select the Syslog protocol from the drop-down menu.
   d. Select the level of alarms to be sent to the syslogger(s) from the Syslog severity drop-down menu.
7. In the License area, click the Upload button to select a license file to upload.
8. Click Save.

### 3.4.2 Setting up the SCADA Gateway for High Availability

1. The different SCADA gateways that need to communicate need to be added to the Gateways list, including the localhost.
   a. Select Network > Gateways and click Add.
   b. Enter the Name, an optional Comment and the IP address of this SCADA gateway and click Save.
   c. Repeat steps 1 and 2 for each SCADA gateway in the network.
2. Assign the HA Active IP address and the SCADA gateway HA Priority.
   a. Select Settings > Local Parameters and click Edit.
   b. Under the High Availability section enter the assigned Priority and Active SCADA gateway IP address for this gateway (priority 1 is the highest priority) and click Save.


© Tait Limited May 2017

c. The gateway needs to be rebooted to apply the changes. To reboot the gateway, connect to it by SSH and login as root (see Section 4.1 and Section 4.2). Issue the command **`reboot`**.

ⓘ If the SCADA gateway is running on a CentOS DMR node this will also reboot the DMR node.

### 3.4.3 Synchronizing the Secondary SCADA Gateway Database

1. Select Settings > Local Parameters and click Edit.
2. Set the mode to Online.
3. The State displayed in the status bar should be Standby.
4. Select Network > Gateways to confirm that the Gateways list contains the Active SCADA gateway and that the Connection Uptime is incrementing. The Database Synchronized column is likely to show No for the Active gateway.
5. Select Settings > Local Parameters and click Edit.
6. Set the mode to Program.
7. Wait until the State displayed in the status bar shows Offline.
8. Select Settings > Local Parameters and click Edit.
9. Set the mode to Online.
10. The State displayed in the status bar should be Standby.
11. Select Network > Gateways to confirm that the Gateways list contains the Active SCADA gateway and that the Connection Uptime is incrementing. The Database Synchronized column should now show Yes for the Active gateway.


© Tait Limited May 2017

# 4 Administrating the SCADA Gateway

The SCADA gateway runs on CentOS or the Solaris operating system (which is a variant of UNIX), depending on your server type. This chapter tells you how to carry out basic maintenance and operational tasks by logging onto the SCADA gateway and using the operating system command line interface.

Note that, whilst still supported, Solaris-based servers are no longer available.

## 4.1 Logging on to the SCADA Gateway

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

1. Use an SSH terminal application to connect to the IP address of the SCADA 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 SCADA gateway using the default command shell (bash).

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

## 4.2 Logging on to the SCADA Gateway as ‘root’

Some tasks can only be carried out if you are logged in as root. To do this 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.


© Tait Limited May 2017

## 4.3 Self-Signed SSL Certificates

When your browser connects to the SCADA 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.

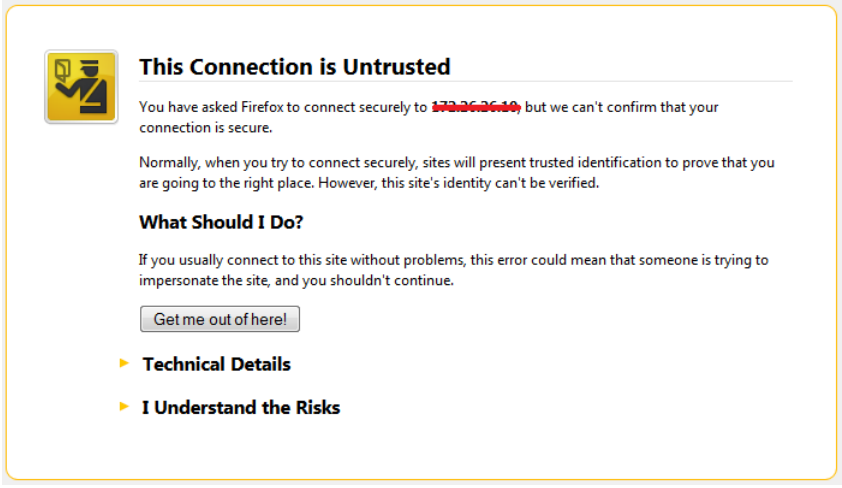
The SCADA gateway creates a self-signed certificate when the SCADA gateway or its firmware is installed. Your browser raises a security warning because the security certificate was not issued by a trusted Certification Authority. The browser has a way of letting you override or bypass the security warning,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

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 SCADA gateway changes. If the SCADA gateway's IP address is changed, simply repeat the certification procedure.

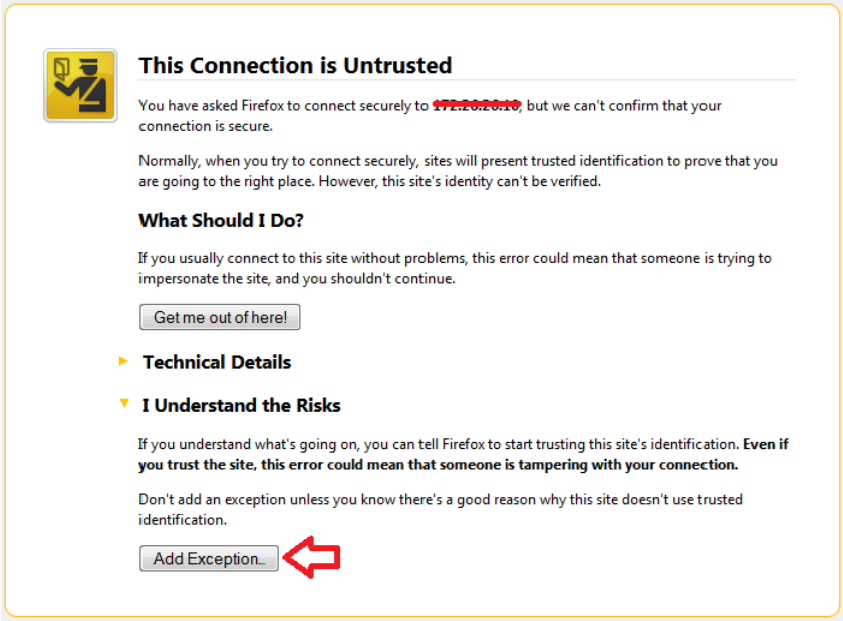
For more information, refer to http://support.microsoft.com/kb/931850 (Internet Explorer) or search for "security certificate" in your browser's Help.

### 4.3.1 Firefox Users

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



1. Click ‘I Understand the Risks’.




2. Click ‘Add Exception’.

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

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


© Tait Limited May 2017

### 4.3.2 Internet Explorer Users

**Windows 8 and Internet Explorer**

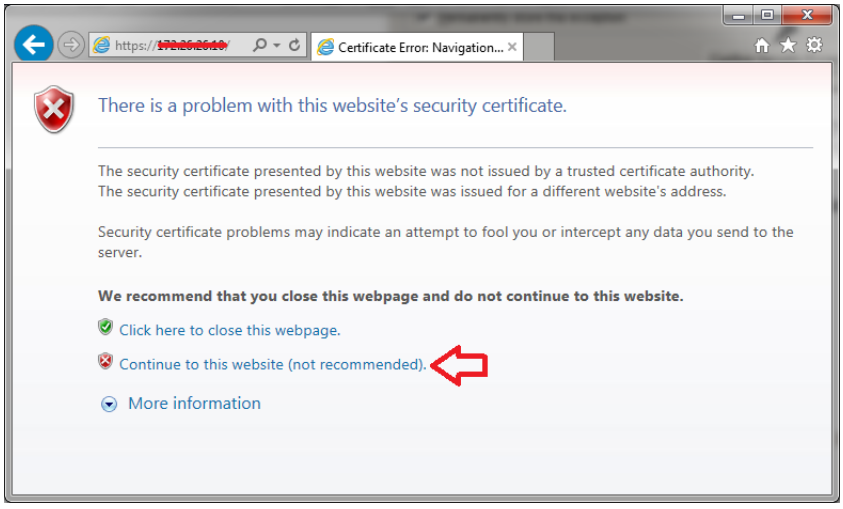
For Windows 8, before following the procedure listed below for installing the certificate, you should make the SCADA gateway a trusted site:

1. Open Internet Options from the Control Panel.
2. Select the Security tab.
3. Click ‘Trusted sites’ then click the Sites button.
4. Add the SCADA gateway’s IP address to Trusted Sites.
5. Apply and close Internet Options.
6. Open Internet Explorer then follow the process.

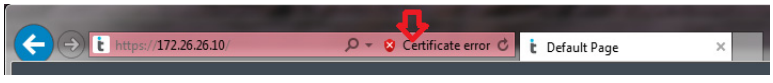
After installing the certificate, the SCADA gateway’s IP address can be removed from your Trusted Sites list.

**Installing the Certificate**

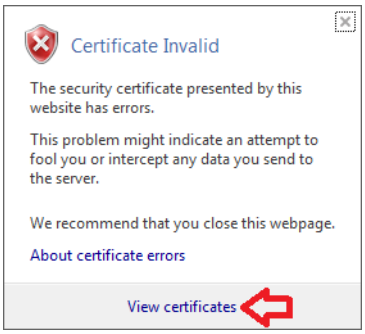
If Internet Explorer is used, the following window appears when the user tries to access the SCADA gateway WebUI for the first time:



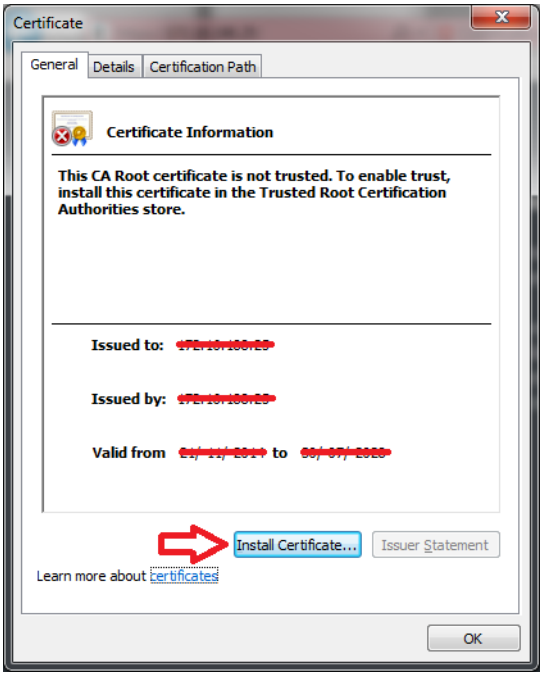

1. Click ‘Continue to this website (not recommended)’. A notification appears at the top of the browser window:



2. Click ‘Certificate error’. The following screen is displayed:




3. Click ‘View certificates’. The Certificate popup with General tab is displayed:




4. Click ‘Install Certificate...’ and then follow the Certificate Import Wizard to install the certificate. Proceed to the end without changing the default values. When the Security Warning window appears, click Yes.

**Windows 7 and Internet Explorer**

When using Windows 7, step 4 of the procedure for Internet Explorer will not remove the Certificate error. Replace step 4 with the following:

1. Click ‘Install Certificate’. In the Certificate Import Wizard click Next.

2. Select ‘Place all certificates in the following store’ and click Browse.

3. Select ‘Trusted Root Certification Authorities’ and click OK.

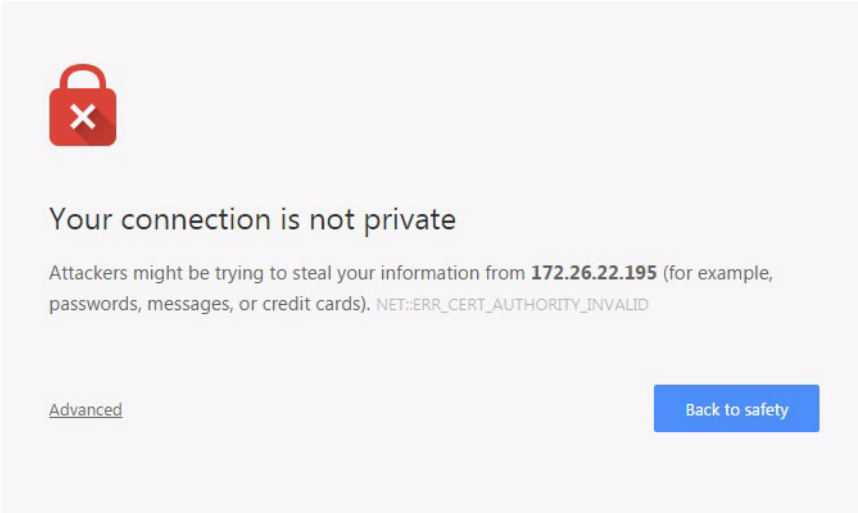

© Tait Limited May 2017

4. Click Next and Finish. When the Security Warning window appears, click Yes.

Internet Explorer must be restarted before the changes take effect. The security certificate is added to a specific computer name. If you add the certificate to the computer, but then access the SCADA gateway WebUI by entering the active SCADA gateway address or name, the certificate error message will appear again.

### 4.3.3 Chrome Users

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




1. Click on Advanced.
2. Click on Proceed to <*SCADA 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 SCADA gateway is accessed. The only way to create a permanent solution is to perform the steps required to create the security certificate using Internet Explorer. Chrome will use the certificates generated by Internet Explorer.

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

By default, the SCADA 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 SCADA 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.

If the CA requires a Certificate Signing request (CSR), this can be generated as follows:

(In the following instructions, the hostname assigned to the SCADA gateway is assumed to be `scadagw-1.orgname.com`.)

1. Connect to the SCADA gateway via SSH as the taitnet user (see Section 4.1).

2. Enter the following command to generate the CSR file based on the server's existing private key file:

   ```
   openall req -new -key /home/taitnet/scadagw/ssl/
   server.key -out /home/taitnet/scadagw/logs/
   scadagw-1.orgname.com.csr
   ```

3. There are various prompts for information. The most critical item is the common name. This **must** match the web address used to access the server, i.e. if the WebUI is accessible via `https://scadagw-1.orgname.com:17443`, then the common name should be entered as `scadagw-1.orgname.com`

4. The CSR is now available for download from the SCADA gateway WebUI. Select Files > Logs, and clicking on the required filename to download it.

5. Send the CSR to the CA and they will return a certificate (.crt) file that can be uploaded to the server.

6. Once the CSR file has been downloaded it can be deleted from Files > Logs. Simply check the box at the beginning of the CSR file's row and click Delete.


© Tait Limited May 2017

Assuming that the server certificate file to be uploaded is called `server-scadagw1.crt`, and the associated private key file is called `server-scadagw1.key` (if a CSR file was generated and submitted to the CA then there will not be a key file), to load a new certificate and associated private key file:

1. Select Files > Backups on the SCADA gateway WebUI and click Upload.
2. Click Choose File.
3. Select the `server-scadagw1.crt` file to upload and click Open.
4. An upload progress window will be displayed. Once the upload is complete the file will be listed on the Files > Firmware page.
5. To upload the private key (if required), perform Steps 1 to 4 for the `server-scadagw1.key` file.
6. Connect to the SCADA gateway via ssh as the taitnet user (see Section 4.1).
7. Move the certificate file to the correct place using the following command:

   **`mv /home/taitnet/scadagw/backups/server-scadagw1.crt /home/taitnet/scadagw/ssl/server.crt`**

8. Press `y` when prompted to overwrite the existing file.
9. Move the private key file (if required) to the correct place using the following command:

   **`mv /home/taitnet/scadagw/backups/server-scadagw1.key /home/taitnet/scadagw/ssl/server.key`**

10. Press `y` when prompted to overwrite the existing file.
11. Restart the SCADA gateway (see Section 4.6).

## 4.5 Changing the ‘root’ and ‘taitnet’ Passwords

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

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

**`passwd`**

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

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

## 4.6 Stopping/Starting the SCADA Gateway Software

Login to the SCADA gateway as the root user. To stop the SCADA gateway enter:

```
service scadagw stop
```

To start the SCADA gateway enter:

```
service scadagw start
```

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

```
service scadagw restart
```

## 4.7 Changing to a Local Time Zone

### 4.7.1 CentOS

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

For first time installation and configuration the time zone can be set during the installation of CentOS (see the relevant section of Section 2.2 Installing the SCADA Gateway on the DMR Node Controller).

To change existing systems to a local time zone you must perform the following procedure:

1. SSH to the SCADA gateway and execute the following as root:
   a. Select the required time zone name from `/usr/share/zoneinfo`
   b. Copy the required time zone file to `/etc/localtime` by typing

      ```
      cp /usr/share/zoneinfo/<required timezone> /etc/localtime
      ```

2. Check the date/time by executing the date command:

   ```
   date
   ```

   This should display the correct date and time for the newly set timezone (see example in step 3). If not login as root, then:

   **EITHER**


© Tait Limited May 2017

a. Correct the date and time using the date command where `<datetime>` is a string of numbers representing the month, day, hour, minute and second, for example `date 10061424.40` sets the date to October 6, 2:24:40 pm:

**`date <datetime>`**

**OR**

b. If using an NTP server, use the `ntpdate` command, where `<server>` is the IP address of a contactable local NTP server:

**`ntpdate <server>`**

This command checks the NTP server time, and sets the local server time (when run as root).

3. Login to the WebUI and check that the date/time is now being correctly displayed as per the following example:

`Fri Jan 17 01:39:30 GMT 2014` (before changing time zone)

`Fri Jan 17 14:50:19 NZDT 2014` (after changing time zone)

The WebUI status bar shows the current time with UTC offset. For example:

`12:51:57 UTC+00:00` (the SCADA gateway local time is the same as UTC)

`12:51:57 UTC+13:00` (the SCADA gateway local time is 13 hours ahead of UTC)

### 4.7.2 Solaris

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

For first time installation and configuration the time zone can be set during the installation of Solaris 10 (see the relevant section of Section 2.2 Installing the SCADA Gateway on the DMR Node Controller).

To change existing systems to a local time zone you must perform the following procedure:

1. SSH to the SCADA gateway and execute the following as root:

a. Select the required time zone name from `/usr/share/lib/zoneinfo`

b. Change the permissions of `/etc/default/init` so that it is writable by root:

**`chmod 755 /etc/default/init`**

c. Edit the `/etc/default/init` file, so that a line starting with TZ= has the timezone name you require, e.g.:

**`TZ=NZ`**


© Tait Limited May 2017

d. Execute the commands (where `<name>` is the timezone name):

```
rtc -z <name>
rtc -c
```

2. Shutdown and restart the machine. The recommended command to shutdown and restart is:

```
shutdown -y -i6 -g0
```

(Note that `shutdown -y -i5 -g0` will shutdown the system, but will not restart it.)

3. Check the date/time by executing the date command:

```
date
```

This should display the correct date and time for the newly set time-zone (see example in step 4). If not login as root, then:

**EITHER**

a. Correct the date and time using the date command where `<datetime>` is a string of numbers representing the month, day, hour, minute and second, for example `date 10061424.40` sets the date to October 6, 2:24:40 pm:

```
date <datetime>
```

**OR**

b. If using an NTP server, use the `rdate` command, where `<server>` is the IP address of a contactable local NTP server:

```
rdate <server>
```

This command checks the NTP server time, and sets the local server time (when run as root).

4. Login to the WebUI and check that the date/time is now being correctly displayed as per the following example:

`Fri Jan 17 01:39:30 GMT 2014` (before changing time zone)

`Fri Jan 17 14:50:19 NZDT 2014` (after changing time zone)

The WebUI status bar shows the current time with UTC offset. For example:

`12:51:57 UTC+00:00` (the SCADA gateway local time is the same as UTC)

`12:51:57 UTC+13:00` (the SCADA gateway local time is 13 hours ahead of UTC)

## 4.8 SCADA Gateway Resource File

The SCADA gateway has a resource configuration file (`scadagw.cfg`), located in the `/home/taitnet/scadagw/` directory. This file contains some configuration parameters that cannot be changed on the WebUI. It is not recommended that they are changed unless Tait Technical Support has requested it.


© Tait Limited May 2017

**If changes are made to `scadagw.cfg` on one SCADA gateway it needs to be edited on all SCADA gateways in the network, and a backup of the settings should be taken after any edits.**

The release notes for a `scadagw` version should be checked for any changes to the settings included in this file.

1. Connect to the SCADA gateway using SSH (Section 4.1). Ensure you are logged in as the taitnet user (not root).
2. Save a backup of the `scadagw.cfg` file using the command:
   **`cp /home/taitnet/scadagw/scadagw.cfg /home/taitnet/scadagw/scadagw.cfg.backup`**
3. Make a copy of the `scadagw.cfg` file editing using the command:
   **`cp /home/taitnet/scadagw/scadagw.cfg /home/taitnet/scadagw/scadagw.cfg.edit`**
4. Edit the `scadagw.cfg` file using the command:
   **`nano /home/taitnet/scadagw/scadagw.cfg.edit`**
   This brings up the nano text editor. The cursor can be moved using the keyboard arrow keys. Text can be inserted and deleted using the keyboard.
5. Take care to not modify any lines of the file you do not intend to modify.
6. Settings in the file follow the format `<key>: <value>`.
7. Comments can be written in the file by putting a # character at the beginning of the line.
8. To exit the editor without saving use Ctrl+X and press **`n`** when prompted to save.
9. To save the changes use Ctrl+O to save and Ctrl+X to exit the editor.
10. If you are happy with the edits then copy the edits over the master file using the command:
    **`mv /home/taitnet/scadagw/scadagw.cfg.edit /home/taitnet/scadagw/scadagw.cfg`**
11. The SCADA gateway service must be restarted to apply the changes (Section 4.6).
12. Take a backup of the edited `scadagw.cfg` file.

The following parameters are ones that may be modified by the customer after consultation with Tait Technical Support.

**MaxCalls**

Sets the maximum number of call attempts the SCADA gateway will make on the DMR network. Set this to the lower of the DIP calls or Packet Data

Calls license values from the DMR Node, e.g. if the DMR node is licensed for 1 DIP call and 1 packet data call then **`MaxCalls: 1`** should be entered.

**NetworkDevice** Sets the network device for the SCADA gateway to use.

**LogAgeLimit** The number of seconds to keep log files for, Default = 1209600 (14 days).

**LogNumberLimit** The number of log files to allow before the oldest is deleted. Default = 99. On installs that have limited HDD space (VM installs using installers prior to v1.04) then this value needs to be set to 30 or lower.

**LogSizeLimit** Maximum size (approximate) for each individual log file. Default = 52428800 (50MB).

**Https.Port** The HTTPS port to use for the SCADA gateway web interface. v1.04 default = 17443. On standalone SCADA gateway machines (i.e. not co-hosted on the CentOS DMR Node, this can be set to HTTPS port 443.

**Glp.MaxQueueSize** In gateway versions later than v1.04 this setting controls the maximum message queue depth in the SCADA gateway. V1.04 default is 99 messages.


© Tait Limited May 2017

# 5 Uploading SCADA Gateway Firmware

From time to time you will need to upgrade the SCADA gateway firmware, which you can do online by uploading the firmware file. This will provide the benefits of receiving new features and software fixes.

ⓘ Refer to the Release Notes supplied with each new firmware release for any special instructions that might be required for that particular upgrade.

## 5.1 Uploading a New Firmware Version

1. Using a web browser, login to the SCADA gateway.
2. Select Files > Firmware Files.
3. Click Upload.
4. On the Upload firmware pop up click Choose File. The firmware file is named `Q9361GW_<version number>` (no file extension).
5. Navigate to the folder on your PC where the firmware file is located.
6. Select the file and then click Open.
7. A progress bar indicates how the upload is progressing.

## 5.2 Upgrading the SCADA Gateway to a New Firmware Version

1. Select Files > Firmware Files.
2. Select the correct firmware file from the list of uploaded firmware files.
3. Click Install.

ⓘ Before installation of the upgrade file takes place, it is first validated to ensure that it is compatible.

4. The SCADA gateway will automatically restart if the upgrade is successful. If the upgrade fails, it will report an error message and revert to the previous software version.


© Tait Limited May 2017

## 5.3 Reverting to an Earlier Firmware Version

The procedure in "Upgrading the SCADA Gateway to a New Firmware Version" can also be used to revert to a previous version of the firmware. When the SCADA gateway firmware is upgraded, the old firmware is not overwritten. Simply select the firmware version to which you wish to revert.

**IMPORTANT - On a CentOS DMR co-hosted installation do not attempt to downgrade from 01.04.02 to any earlier version.**


© Tait Limited May 2017

# 6 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, such as adding new data terminals, or editing configuration parameters.

The SCADA gateway and terminal configuration settings 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.

ⓘ The Backup and Restore functions back up and restore all settings, including the IP address for the device. It is recommended that a backup of each gateway in a network be taken and saved in a safe location and that the backups should only be restored to the gateway from which they were taken.

## 6.1 Manual Backup

1. Using a web browser, login to the SCADA gateway.
2. Select Files > Backups and then click Backup.
3. When an information message appears, click OK.
4. Give the gateway time to create the backup and then use a browser command to reload the page. This updates the display to show the file that has been created.
5. Click on the filename of the backup to download it and save it to a safe location

ⓘ The backup process saves the database settings for the SCADA gateway. It is also recommended to keep backups of the `licence.dat` file and the `scadagw.cfg` file in a safe place to make sure the gateway can be rebuilt if there is ever a need to do so.

## 6.2 Restoring a Backup File

1. Using a web browser, login to the SCADA gateway.
2. Select Files > Backups.
3. To load a backup from another location, click Upload. An Upload Database dialog will appear. Select `Choose File` to open the


© Tait Limited May 2017

selection dialog and open the backup to restore. Once the file is uploaded it will appear in the list of files available to restore.

4. Click the check box to select the row of the file and then click Restore and confirm.


© Tait Limited May 2017

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

ISO images can be transferred to a USB flash drive using either Win32DiskImager or another tool such as Rufus, both of which are documented here.

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.

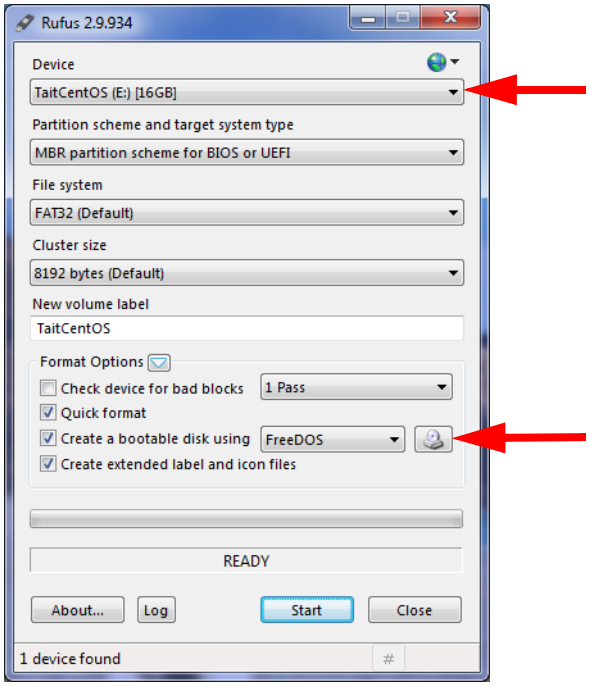
**Notice** The Dell R230 server can only be booted up by a USB type 3.0 flash drive. When installing software on a Dell R230, please make sure your flash drive is compliant. The internet can provide tips on how to recognise a USB 3.0 flash drive (e.g. sometimes it has a blue insert). If problems arise, please contact Tait Technical Support for CD/DVD ROM installation instructions.

## 1.1 Using Rufus

1. To create a USB flash drive with CentOS or SCADA gateway software, first download and install the Rufus application.
2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (CentOS will require at least an 8GB flash drive, and for the DMR application 1GB or greater is required.)


© Tait Limited May 2017

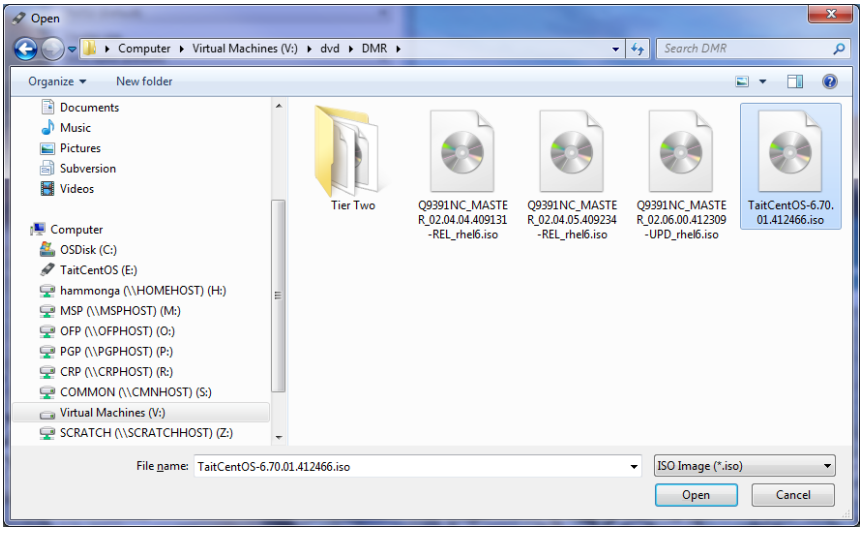
3. Run the Rufus program.




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.

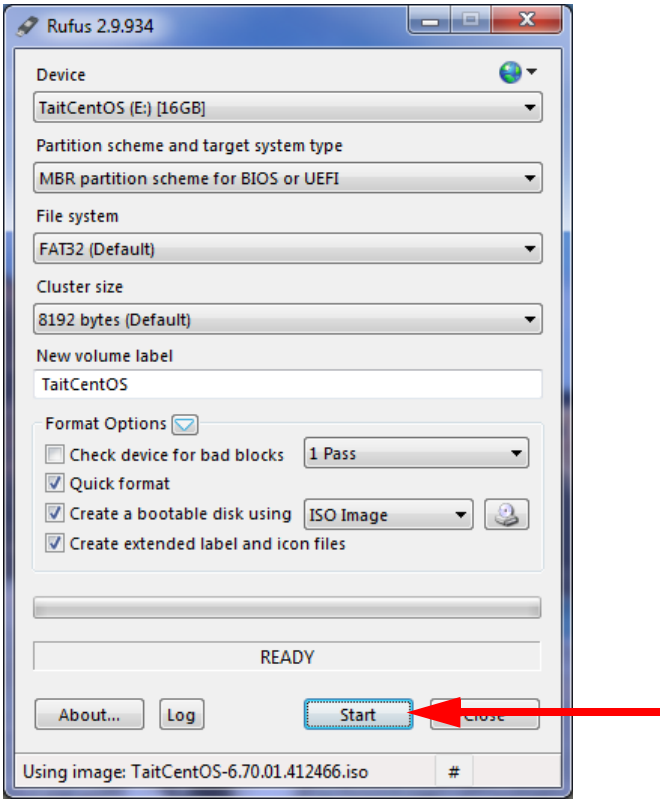
6. Select the ISO file and click Open, which takes you back to Rufus.





© Tait Limited May 2017

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

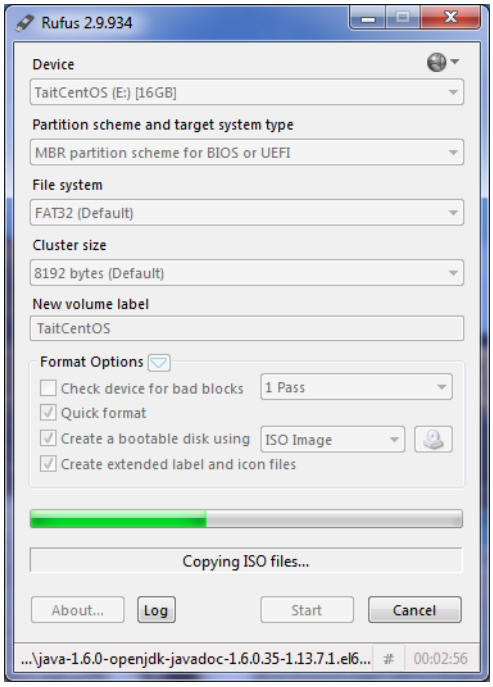



8. A dialog box will appear to confirm that a write operation is to be carried out. At this point double check that the correct device is being written to and then click OK.

   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.


© Tait Limited May 2017

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.

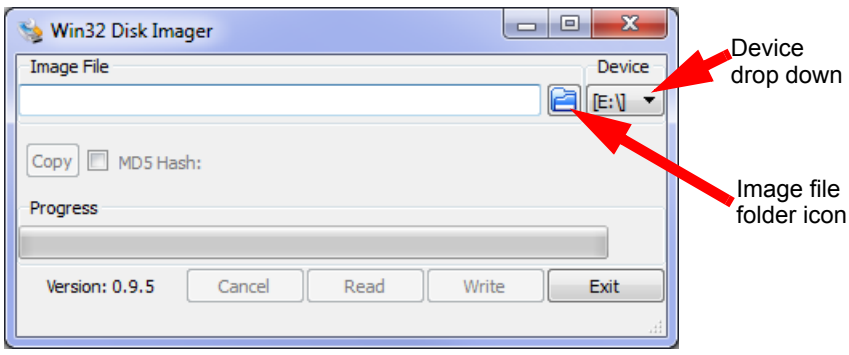
11. Remember to safely eject the USB flash drive before physically removing it from the PC.

## 1.2 Using Win32DiskImager

1. To create a USB flash drive with CentOS or SCADA gateway software, first download and install the Win32DiskImager application.

2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (CentOS will require at least an 8GB flash drive, and for the DMR application 1GB or greater is required.)

3. Run the Win32DiskImager program.



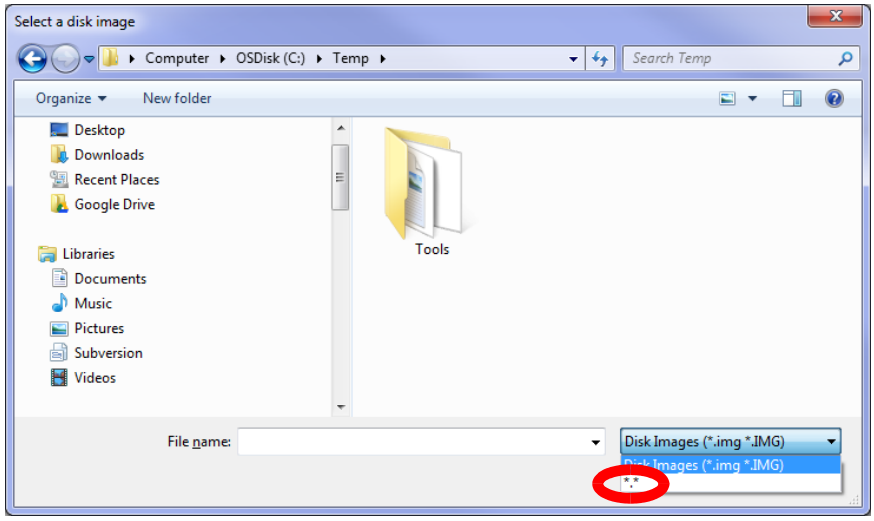


© Tait Limited May 2017

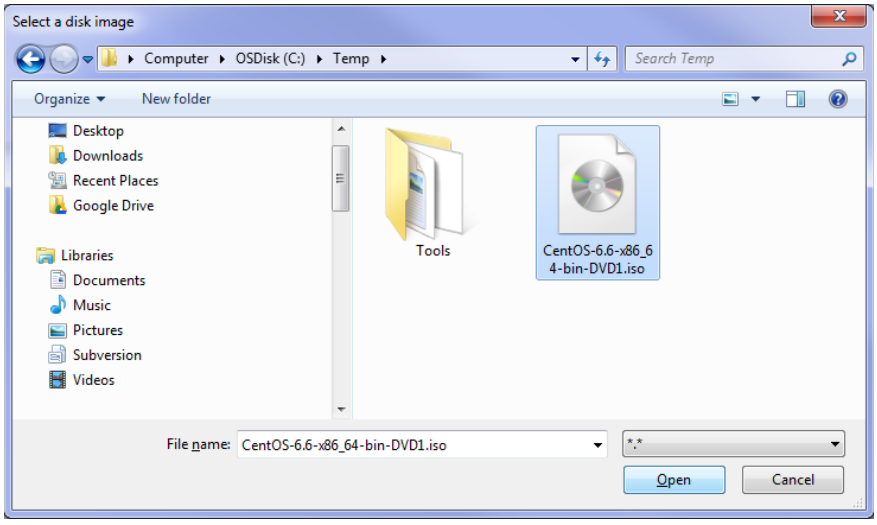
4. Check that the drive letter in the `Device` drop down list is the same as the USB flash drive. If you get this wrong, you could erase the wrong disk.

5. Click on the folder icon for the Image file.

6. Change the file filter from `Disk Images (*.img *.IMG)` to `*.*`



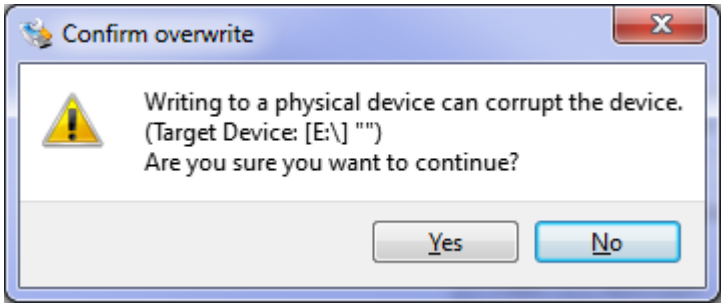

7. Select the desired iso file and click Open.



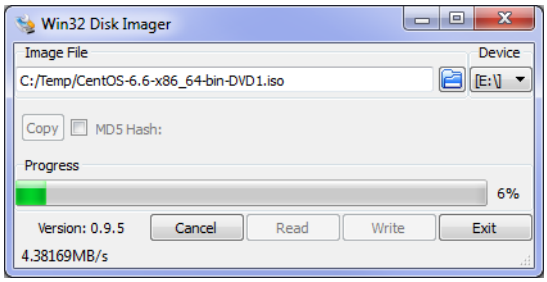

8. When ready to proceed, click Write.

© Tait Limited May 2017

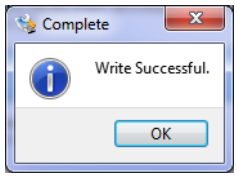
9. A `Confirm overwrite` dialog will appear which gives you a last chance to abort the process. Click Yes to continue.




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.


© Tait Limited May 2017

# Appendix 2: Adding an Alternate Interface in CentOS

CentOS uses configuration files for each interface to be configured. These configuration files are stored in `/etc/sysconfig/network-scripts/` with filenames `ifcfg-<interface>`, e.g. `ifcfg-eth0:2`.

To enable the sub-interface on the first Ethernet port (interface `eth0:2`) for the SCADA gateway:

1. Login as the root user: **`su -`**
2. Edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0:2` using the command **`nano /etc/sysconfig/network-scripts/ifcfg-eth0:2`**
3. Set or edit the following lines in the file:

   DEVICE=**eth0:2**
   ONBOOT=**yes**
   BOOTPROTO=**none**
   IPADDR=***<ip-address>***
   PREFIX=***<prefix>***
   GATEWAY=***<gateway-ip>***

4. Save the changes (**^O**) and exit from nano (**^X**).
5. Restart the network service to apply the changes by running the command **`service network restart`**


© Tait Limited May 2017

# Tait Software License Agreement

This Software License Agreement ("Agreement") is between you (“Licensee”) and Tait Limited (“Tait").

By using any of the Software items embedded and pre-loaded in the related Tait Designated Product, included on CD, downloaded from the Tait website, or provided in any other form, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, do not install or use any of the Software. If you install or use any of the Software, that will be deemed to be acceptance of the terms of this Agreement.

For good and valuable consideration, the parties agree as follows:

**Section 1 DEFINITIONS**

**“Confidential Information”** means all or any information supplied to or received by Licensee from Tait, whether before or after installation or use and whether directly or indirectly pertaining to the Software and Documentation supplied by Tait, including without limitation all information relating to the Designated Products, hardware, software; copyright, design registrations, trademarks; operations, processes, and related business affairs of Tait; and including any other goods or property supplied by Tait to Licensee pursuant to the terms of this Agreement.

**“Designated Products”** means products provided by Tait to Licensee with which or for which the Software and Documentation is licensed for use.

**“Documentation”** means product and software documentation that specifies technical and performance features and capabilities; user, operation, and training manuals for the Software; and all physical or electronic media upon which such information is provided.

**“Executable Code”** means Software in a form that can be run in a computer and typically refers to machine language, which is comprised of native instructions the computer carries out in hardware. Executable code may also refer to programs written in interpreted languages that require additional software to actually execute.

**“Intellectual Property Rights”** and **“Intellectual Property”** mean the following or their substantial equivalents or counterparts, recognized by or through action before any governmental authority in any jurisdiction throughout the world and including, but not limited to all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation; including any adaptations, corrections, de-compilations, disassemblies, emulations, enhancements fixes, modifications, translations and updates to or derivative works from, the Software or Documentation, whether made by Tait or another party, or any improvements that result from Tait processes or, provision of information services.

**“Licensee”** means any individual or entity that has accepted the terms of this License.

**“Open Source Software”** means software with freely obtainable source code and license for modification, or permission for free distribution.

**“Open Source Software License”** means the terms or conditions under which the Open Source Software is licensed.

**“Person”** means any individual, partnership, corporation, association, joint stock company, trust, joint venture, limited liability company, governmental authority, sole proprietorship, or other form of legal entity recognized by a governmental authority.

**“Security Vulnerability”** means any flaw or weakness in system security procedures, design, implementation, or internal controls that if exercised (accidentally triggered or intentionally exploited) could result in a security breach such that data is compromised, manipulated, or stolen, or a system is damaged.

**“Software”** (i) means proprietary software in executable code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Tait; and (iii) may contain one or more items of software owned by a third-party supplier. The term "Software" does not include any third-party software provided under separate license or not licensable under the terms of this Agreement.

**“Source Code”** means software expressed in human readable language necessary for understanding, maintaining, modifying, correcting, and enhancing any software referred to in this Agreement and includes all states of that software prior to its compilation into an executable programme.

**“Tait”** means Tait Limited and includes its Affiliates.

**Section 2 SCOPE**

This Agreement contains the terms and conditions of the license Tait is providing to Licensee, and of Licensee’s use of the Software and Documentation. Tait and Licensee enter into this Agreement in connection with Tait delivery of certain proprietary Software and/or products containing embedded or pre-loaded proprietary Software.

**Section 3 GRANT OF LICENSE**

3.1. Subject to the provisions of this Agreement and the payment of applicable license fees, Tait grants to Licensee a personal, limited, non-transferable (except as permitted in Section 7), and non-exclusive license to use the Software in executable code form, and the Documentation,


© Tait Limited May 2017

solely in connection with Licensee's use of the Designated Products for the useful life of the Designated Products. This Agreement does not grant any rights to source code.

3.2. If the Software licensed under this Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not in this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the any applicable Open Source Software Licenses, the terms and conditions of the Open Source Software Licenses will take precedence. For information about Open Source Components contained in Tait products and the related Open Source licenses, see:
http://support.taitradio.com/go/opensource

**Section 4 LIMITATIONS ON USE**

4.1. Licensee may use the Software only for Licensee's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited. Without limiting the general nature of these restrictions, Licensee will not make the Software available for use by third parties on a "time sharing," "application service provider," "service bureau" basis, or for any other similar commercial rental or sharing arrangement.

4.2. Licensee will not, and will not directly or indirectly allow or enable any third party to: (i) reverse engineer, disassemble, extract components, decompile, reprogram, or otherwise reduce the Software or any portion thereof to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party; (iv) grant any sublicense or other rights in the Software or Documentation to any third party; (v) take any action that would cause the Software or Documentation to be placed in the public domain; (vi) remove, or in any way alter or obscure any copyright notice or other notice of Tait or third-party licensor's proprietary rights; (vii) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by, any third party or on any machine except as expressly authorized by this Agreement; or (viii) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software by any means whatsoever other than what is permitted in this Agreement. Licensee may make one copy of the Software to be used solely for archival, back-up, or disaster recovery purposes; provided that Licensee may not operate that copy of the Software at the same time as the original Software is being operated. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

4.3. Unless otherwise authorized by Tait in writing, Licensee will not, and will not enable or allow any third party to: (i) install a copy of the Software on more than one unit of a Designated Product; or (ii) copy or transfer Software installed on one unit of a Designated Product to any other device. Licensee may temporarily transfer Software installed on a Designated Product to another device if the Designated Product is inoperable or malfunctioning. Temporary transfer of the Software to another device must be discontinued when the original Designated Product is returned to operation and the Software must be removed from the other device.

4.4. Licensee will maintain, during the term of this Agreement and for a period of two years thereafter, accurate records relating to this license grant to verify compliance with this Agreement. Tait, or a third party nominated by Tait, may inspect Licensee's premises, books and records, upon reasonable prior notice to Licensee, during Licensee's normal business hours and subject to Licensee's facility and security regulations. Tait is responsible for the payment of all expenses and costs of the inspection, provided that Licensee shall indemnify Tait for all costs (including audit costs and legal costs on a solicitor client basis) if Licensee has breached the terms of this Agreement. Any information obtained by Tait during the course of the inspection will be kept in strict confidence by Tait and used solely for the purpose of verifying Licensee's compliance with the terms of this Agreement.

**Section 5 OWNERSHIP AND TITLE**

Tait, its licensors, and its suppliers retain all of their Intellectual Property Rights in and to the Software and Documentation, in any form. No rights are granted to Licensee under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Agreement. All Intellectual Property developed, originated, or prepared by Tait in connection with providing the Software, Designated Products, Documentation, or related services, remains vested exclusively in Tait, and Licensee will not have any shared development or other Intellectual Property Rights.

**Section 6 LIMITED WARRANTY; DISCLAIMER OF WARRANTY**

6.1. The commencement date and the term of the Software warranty will be a period of one (1) year from Tait shipment of the Software. If Licensee is not in breach of any obligations under this Agreement, Tait warrants that the unmodified Software, when used properly and in accordance with the Documentation and this Agreement, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect has occurred will be determined solely by Tait. Tait does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. Tait makes


© Tait Limited May 2017

no representations or warranties with respect to any third-party software included in the Software.

6.2 Tait sole obligation to Licensee, and Licensee's exclusive remedy under this warranty, is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant, demonstrable program or documentation errors or Security Vulnerabilities. If Tait cannot correct the defect within a reasonable time, then at Tait option, Tait will replace the defective Software with functionally equivalent Software, license to Licensee substitute Software which will accomplish the same objective, or terminate the license and refund Licensee's paid license fee. If Tait investigation of the perceived defect reveals that no such defect in fact exists, Tait may recover its costs in respect of such investigation from Licensee.

6.3. Tait disclaims any and all other warranties relating to the Software or Documentation other than the express warranties set forth in this Section 6. Warranties in Section 6 are in lieu of all other warranties whether express or implied, oral or written, and including without limitation any and all implied warranties of condition, title, non-infringement, merchantability, or fitness for a particular purpose or use by Licensee (whether Tait knows, has reason to know, has been advised of, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, Tait disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

**Section 7 TRANSFERS**

7.1. Licensee will not transfer the Software or Documentation to any third party without specific prior written consent from Tait. Tait may withhold such consent or at its own discretion make the consent conditional upon the transferee paying applicable license fees and agreeing to be bound by this Agreement.

7.2. In the case of a value-added reseller or distributor of Tait Designated Products, the consent referred to in Section 7.1 may be contained in a Tait Reseller or Tait Distributor Agreement.

7.3. If the Designated Products are Tait vehicle-mounted mobile products or hand-carried portable radio products and Licensee transfers ownership of the Tait mobile or portable radio products to a third party, Licensee may assign its right to use the Software which is embedded in or furnished for use with the radio products and the related Documentation; provided that Licensee transfers all copies of the Software and Documentation to the transferee.

7.4. For the avoidance of any doubt, Section 7.3 excludes TaitNet Infrastructure, or the products listed at any time under network products at: http://www.taitradio.com.

7.5. If Licensee, as a contractor or subcontractor (integrator), is purchasing Tait Designated Products and licensing Software not for its own internal use but for end use only by a Customer, the Licensee may transfer such Software, but only if a) Licensee transfers all copies of such Software and the related Documentation to the transferee and b) Licensee has first obtained from its Customer (and, if Licensee is acting as a subcontractor, from the interim transferee(s) and from the ultimate end user sub license) an enforceable sublicense agreement that prohibits any other transfer and that contains restrictions substantially identical to the terms set forth in this Software License Agreement. Except as stated in the foregoing, Licensee and any transferee(s) authorised by this Section may not otherwise transfer or make available any Tait Software to any third party nor permit any party to do so. Licensee will, on request, make available evidence reasonably satisfactory to Tait demonstrating compliance with all the foregoing.

**Section 8 TERM AND TERMINATION**

8.1. Licensee's right to use the Software and Documentation will commence when the Designated Products are supplied by Tait to Licensee and will continue for the life of the Designated Products with which or for which the Software and Documentation are supplied, unless Licensee breaches this Agreement, in which case this Agreement and Licensee's right to use the Software and Documentation may be terminated immediately upon notice by Tait.

8.2. Within thirty (30) days after termination of this Agreement, Licensee must certify in writing to Tait that all copies of the Software have been removed or deleted from the Designated Products and that all copies of the Software and Documentation have been returned to Tait or destroyed by Licensee and are no longer in use by Licensee.

8.3. Licensee acknowledges that Tait made a considerable investment of resources in the development, marketing, and distribution of the Software and Documentation and that Licensee's breach of this Agreement will result in irreparable harm to Tait for which monetary damages would be inadequate. If Licensee breaches this Agreement, Tait may terminate this Agreement and be entitled to all available remedies at law or in equity including immediate injunctive relief and repossession of all non-embedded Software and associated Documentation. Licensee shall pay all Tait costs (on an indemnity basis) for the enforcement of the terms of this Agreement.

**Section 9 CONFIDENTIALITY**

Licensee acknowledges that the Software and Documentation contain proprietary and Confidential Information valuable to Tait and are Tait trade secrets, and Licensee agrees to respect the confidentiality of the information contained in the Software and Documentation.

**Section 10 LIMITATION OF LIABILITY**

10.1. In no circumstances shall Tait be under any liability to Licensee, or any other person whatsoever, whether in Tort (including negligence), Contract (except as expressly provided in this Agreement), Equity, under any Statute, or otherwise at law for any losses or damages whether general, special, exemplary, punitive, direct,


© Tait Limited May 2017

indirect, or consequential arising out of or in connection with any use or inability of using the Software.

10.2. Licensee's sole remedy against Tait will be limited to breach of contract and Tait sole and total liability for any such claim shall be limited at the option of Tait to the repair or replacement of the Software or the refund of the purchase price of the Software.

**Section 11 GENERAL**

11.1. COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.

11.2. COMPLIANCE WITH LAWS. Licensee acknowledges that the Software may be subject to the laws and regulations of the jurisdiction covering the supply of the Designated Products and will comply with all applicable laws and regulations, including export laws and regulations, of that country.

11.3. ASSIGNMENTS AND SUBCONTRACTING. Tait may assign its rights or subcontract its obligations under this Agreement, or encumber or sell its rights in any Software, without prior notice to, or consent of, Licensee.

11.4. GOVERNING LAW. This Agreement shall be subject to and construed in accordance with New Zealand law and disputes between the parties concerning the provisions hereof shall be determined by the New Zealand Courts of Law. Provided however Tait may at its election bring proceedings for breach of the terms hereof or for the enforcement of any judgment in relation to a breach of the terms hereof in any jurisdiction Tait considers fit for the purpose of ensuring compliance with the terms hereof or obtaining relief for breach of the terms hereof.

11.5. THIRD-PARTY BENEFICIARIES. This Agreement is entered into solely for the benefit of Tait and Licensee. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this Agreement. Notwithstanding the foregoing, any licensor or supplier of third-party software included in the Software will be a direct and intended third-party beneficiary of this Agreement.

11.6. SURVIVAL. Sections 4, 5, 6.3, 7, 8, 9, 10, and 11 survive the termination of this Agreement.

11.7. ORDER OF PRECEDENCE. In the event of inconsistencies between this Agreement and any other Agreement between the parties, the parties agree that, with respect to the specific subject matter of this Agreement, this Agreement prevails.

11.8. SECURITY. Tait uses reasonable means in the design and writing of its own Software and the acquisition of third-party Software in order to limit Security Vulnerabilities. While no software can be guaranteed to be free from Security Vulnerabilities, if a Security Vulnerability is discovered, Tait will take the steps specified in Section 6 of this Agreement.

11.9. EXPORT. Licensee will not transfer, directly or indirectly, any Designated Product, Documentation or Software furnished hereunder or the direct product of such Documentation or Software to any country for which New Zealand or any other applicable country requires an export license or other governmental approval without first obtaining such license or approval.

11.10. SEVERABILITY. In the event that any part or parts of this Agreement shall be held illegal or null and void by any court or administrative body of competent jurisdiction, such determination shall not affect the remaining terms which shall remain in full force and effect as if such part or parts held to be illegal or void had not been included in this Agreement. Tait may replace the invalid or unenforceable provision with a valid and enforceable provision that achieves the original intent and economic effect of this Agreement.

11.11. CONSUMER GUARANTEES. Licensee acknowledges that the licenses supplied in terms of this agreement are supplied to Licensee in business, and that the guarantees and other provisions of prevailing consumer protection legislation shall not apply.

11.12. WHOLE AGREEMENT. Licensee acknowledges that it has read this Agreement, understands it and agrees to be bound by its terms and conditions. Licensee also agrees that, subject only to the express terms of any other agreement between Tait and Licensee to the contrary, this is the complete and exclusive statement of the Agreement between it and Tait in relation to the Software. This Agreement supersedes any proposal or prior agreement, oral or written, and any other communications between Licensee and Tait relating to the Software and the Designated Products.


© Tait Limited May 2017