Tait EnableMonitor

Getting Started Guide

MNE-00001-13 · Issue 13 · June 2020

Contact Information

Tait Communications
Corporate Head Office

Tait International 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

Disclaimer

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

Enquiries and Comments

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

Updates of Manual and Equipment

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

Intellectual Property Rights

This product may be protected by one or more patents or designs of Tait International Limited together with their international equivalents, pending patent or design applications, and registered trade marks: NZ 409837, NZ 409838, NZ 415277, NZ 415278, NZ 508806, NZ 530819, NZ 534475, NZ 547713, NZ 577009, NZ 579051, NZ 579364, NZ 586889, NZ 610563, NZ 615954, NZ 700387, NZ 708662, NZ 710766, NZ 711325 , NZ 726313, NZ 733434, NZ 593887, AU 2015215962, AU 339127, AU 339391, AU 2016259281, AU 2016902579, AU 2017204526, EU 000915475-0001, EU 000915475-0002, GB 1518031.8, GB 1710543.8, GB 2532863, US 14/834609 Div. no 1, US 15/346518 Div.no 2, US 15/350332, US 15/387026 Div., US 29/614639, US 62/713910, US 62/729478, US 62/730107, US 62/767041, US 62/781642, US 62/778238, US 9794940 Div. no 1, US 20150085799, US 20160044572, US 20160057051, US 20170142646, US 20170055267 Div. no 2, US 20180006844, US 640974, US 640977, US 698339, US 702666, US 7758996, US 8902804, US 9107231, US 9504034, US 9559967.

Environmental Responsibilities

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

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

Tait International 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

Scope of Manual

Tait Communications has created a Network Management System (NMS), Tait EnableMonitor, to assist network administrators and managers to ensure that their Tait MPT-IP, DMR, or Tait and Airbus DS Communications P25 networks are running smoothly and at maximum efficiency.

Tait EnableMonitor is based on an award-winning off-the-shelf tool called OpManager from ManageEngine. Tait EnableMonitor offers a variety of at-a-glance views of the current status of any or all parts of your network, as well as reports detailing the health and availability of your network resources.

This manual is part of the documentation set for Tait Enable. This manual provides information on Tait EnableMonitor, and its intended audience is system administrators and IT personnel only.

This document describes Tait EnableMonitor version 12.3.

Document Conventions

“Select Maps > Add Business View” means “click Maps on the menu bar, then click Add Business View on the list of commands that pops up”. “Monitor > Module Details > Reciter” means “click the Monitor icon on the toolbar, then in the navigation pane find the Module Details group, and select Reciter from it”.

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:

Notice This alert is used to highlight information that is required to ensure procedures are performed correctly. Incorrectly performed procedures could result in equipment damage or malfunction.

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

Publication Record

Issue	Publication Date	Description
13	June 2020	■ Added alternative v3.24 (or 2.24 and later) TN9300 traps ■ Updated section “Upgrading from Tait EnableMonitor version 12.3 to 12.4” ■ Updated section “Disabling and Enabling SSL (HTTPS)” ■ Updated section “Automatically Refreshing the Tait EnableMonitor View” ■ Updated menu paths for various actions
12	June 2019	■ Updated section “1.5 Upgrading from Tait EnableMonitor version 11.6 to 12.3”
11	September 2018	■ EnableMonitor changed to Tait EnableMonitor
10	July 2018	■ Updated to Tait International Limited throughout ■ Updated to version 12.3 throughout ■ Removed 30 Day Trial Version text ■ Added packages that need to be followed when upgrading from Tait EnableMonitor version 11.6 to 12.3 ■ Minor updates throughout
9	June 2017	■ Added support for OpManager v12 and updated document for the new interface ■ Removed “Switching Between the New and Old Interfaces” section ■ Added TN9500 traps ■ Updated TN9300 traps ■ Added SCADA Gateway traps

1 Installing Tait EnableMonitor

1.1 Overview

Tait EnableMonitor can be delivered either as:

- a total package- a complete bundled hardware and software solution, configured and installed for ease of use
- a software bundle recommended for operation on servers running Windows Server 2008 or 2012 Release 2

Notice It is the customer's responsibility to ensure that relevant Windows security updates are installed. In the unlikely event that an update causes a problem with Tait EnableMonitor, contact your regional Tait office.

Tait EnableReport is an additional solution that operates with Tait EnableMonitor.

1.2 Total Package

1. Set up your server, connect to power and internet.
2. Power up and log on to Windows using `Administrator` as the username and `K1w1k1w1`[1] as the password.
3. Select the Tait EnableMonitor application from your program list.
4. Open a web browser and enter **`https://localhost/`** in the address bar.

Log on to Tait EnableMonitor using `admin` as the username and `admin` as the password.[2]

5. Proceed to Section 2 Setting Up Tait EnableMonitor.

1. Prior to 2014, password was `TaitAdmin`.
2. Tait products are deployed with weak default passwords. It is the responsibility of the customer to change these to strong passwords.

1.3 Software Only

Licenses

Depending on the size of your system, Tait EnableMonitor has two license types:

- Essential - 1 server, up to 1000 interfaces
- Enterprise - 2 to 10 servers, over 1000 interfaces

Licensing Options	Essential - 250, 500 or 1000 Interfaces	Enterprise - up to 50,000 Interfaces
Processor	Quad-core 2.5 GHz or more	Dual Quad-core 3.5 GHz
Memory	16 GB	32 GB
Free hard disk space	10 GB	40 GB
NIC	10 Mbps	100 Mbps
Video display resolution	1024 x 768 or higher	1024 x 768 or higher

The Enterprise license software package contains two versions of the Tait EnableMonitor application. The Central application is to be installed only on your main server, and the Probe application is to be installed on all other servers running Tait EnableMonitor. The Central and Probe applications cannot be installed on the same server.

Operating Systems Supported

Windows Server 2008 Release 2 64-bit
Windows Server 2012 Release 2 64-bit

Recommended Browsers

Microsoft Internet Explorer version 11 or above
Google Chrome version 47 or above

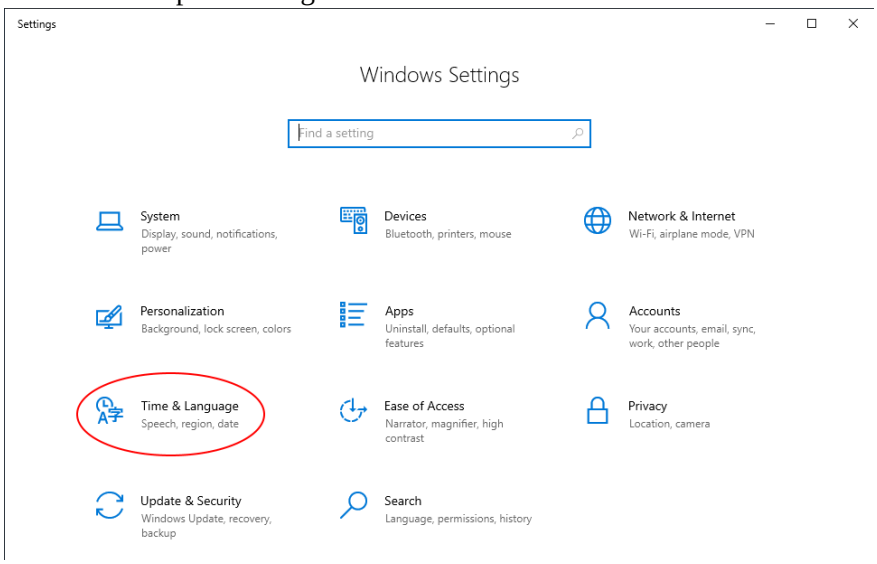
1.4 Essential Installation

The following procedure details the steps required for first-time installation of Tait EnableMonitor.

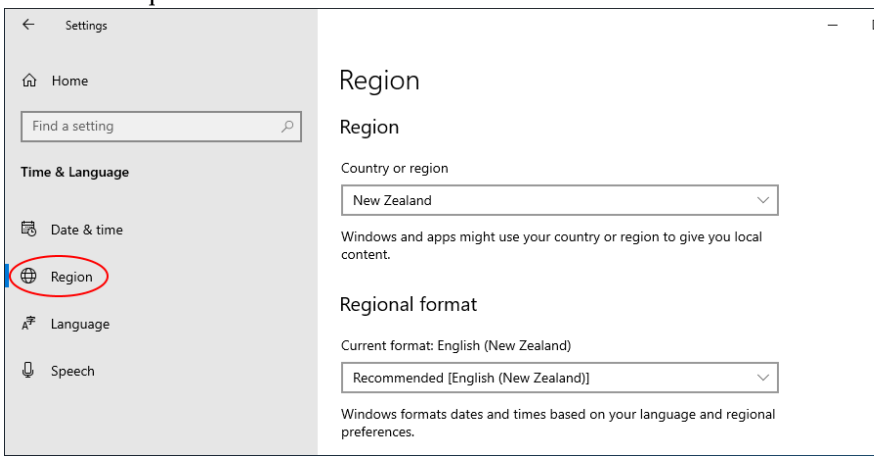
If you already have Tait EnableMonitor 12.3 installed, go to "Upgrading from Tait EnableMonitor version 12.3 to 12.4" on page 14.

Notice Please note that these instructions must be followed in the specified order. Any deviation from this order may result in unexpected behavior.

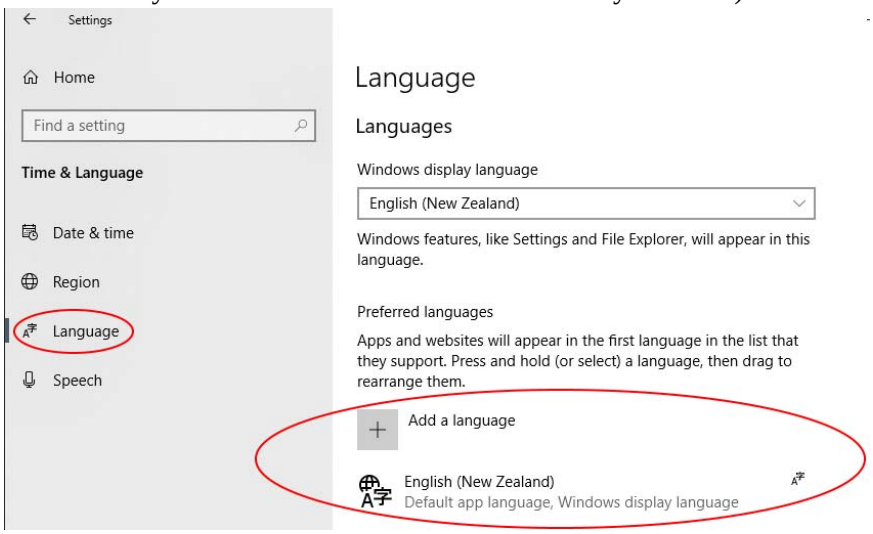
1. Select Settings > Time & Language to check Windows parameters for the specified region:



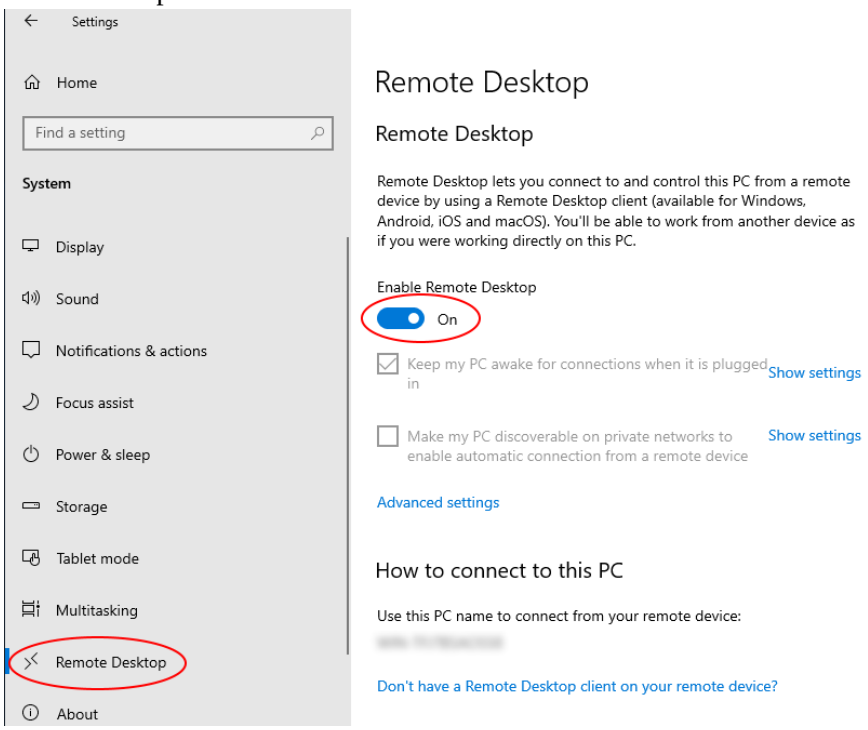
- Select Region and update Region and/or Regional format if required:



- Select Language (you may need to Add a Language or Options > Keyboard if the desired one is not currently installed):



2. Select Settings > System > Remote Desktop to allow remote desktop:



3. Install the Chrome web browser if required (Internet Explorer is pre-installed with Windows). Link is as follows:
   - `https://www.google.com/chrome/`

4. Install Adobe Reader, required for User Guides, from `http://get.adobe.com/reader/`

   Ensure the Optional Offers checkbox is unticked before clicking 'Download Acrobat Reader'.

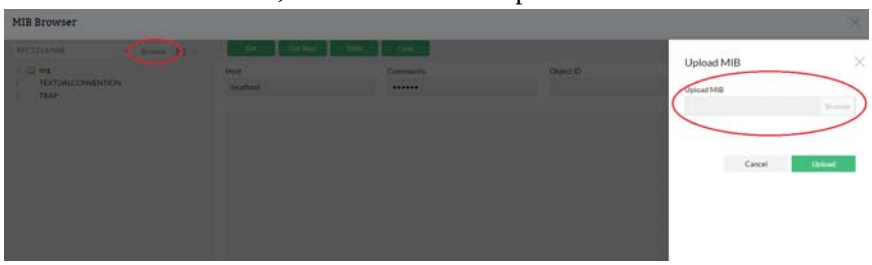
5. Install OpManager 12.4 standalone 64-bit.

6. Click Yes to accept the EULA.
7. Select a language and click Next.
8. Click Next (Default destination).
9. Click Next (Use Port 8060).
10. Click Skip.
11. Click Next (Standalone or Primary Server).
12. Click Next (POSTGRESQL).
13. If an antivirus software warning appears, click OK.
14. Click Finish.
15. Browse `localhost:8060` to check that OpManager is working, then install the dependencies packages:
    - Microsoft .NET Framework 4.0 (dotNetFx40_Full_x86_x64 version 4)
      `http://www.microsoft.com/en-us/download/details.aspx?id=17718`
    - Microsoft Visual C++ 2010 64-bit
      `http://www.microsoft.com/en-us/download/details.aspx?id=14632`
    - NTP Client version dkwin-3-06-99-12 May 8, 2012
      `http://www.meinberg.de/english/sw/ntp.htm#ntp_nt_stable`
      (Use `K1w1k1w1` as the password for NTP.)
16. Run the Tait EnableMonitor configuration package from the product DVD. The file name will be similar to the following: `Tait EnableMonitor <version>.msi`

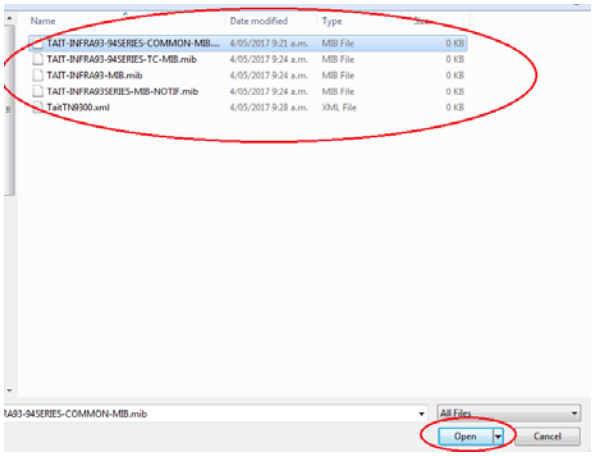
Important If the Tait EnableMonitor configuration package fails to install, restart the Manage Engine OpManager service and run the installer again.

17. Restart the ManageEngine OpManager service.
18. Wait for OpManager to start (this could take up to 5 minutes).
19. Open a web browser and enter **`https://localhost/`** in the address bar. Ignore any security warnings.
20. Logon to Enable Monitor with User: **`admin`** and Password: **`admin`**.
21. Optionally upload MIB files (MIBs required for the Tait solutions are already included):
    a. Navigate to Settings > Tools > MIB Browser.

b. Click Browse, then click on the Upload MIB field as before.



c. Upload the required MIB files by selecting a file and clicking Open (files will have to be done one at a time).



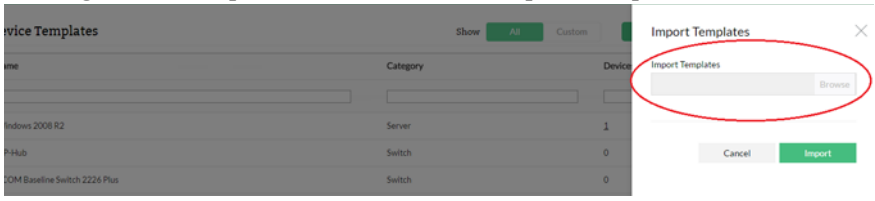
d. Click Upload.

22. Optionally upload Template files:

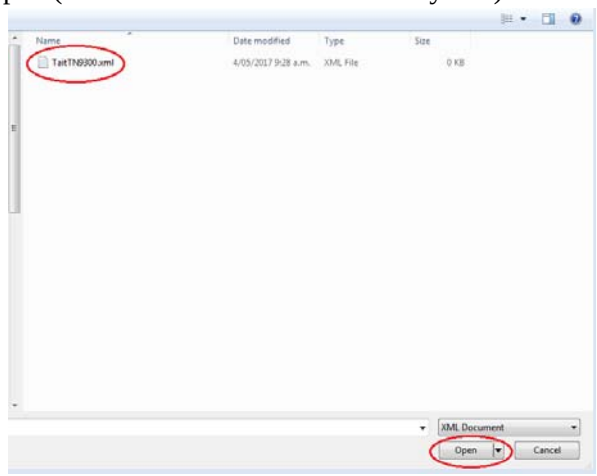
e. Navigate to Settings > Configuration > Device Template.

f. Delete any existing templates for the ones to be uploaded (in this example we are uploading the Tait TN9300 template) by clicking next to the existing template entry

g. Select Import, then click on the Import Templates field.



h. Upload the required Template files by selecting a file and clicking Open (files will have to be done one by one).



23. Click Import.

24. The installation is now complete.

    Remove any temporary files from the desktop.

    Set the home page for any installed web browsers to `https://localhost/`

1.5 Upgrading from Tait EnableMonitor version 12.3 to 12.4

Notice Please note that these instructions must be followed in the specified order. Any deviation from this order may result in unexpected behavior.

Notice Steps 1-9 will need to be followed for each of the upgrade packages:

- AdventNet_ManageEngine_OpManager_12_0_SP-4_0_0_6.ppm
- AdventNet_ManageEngine_OpManager_12_0_SP-4_1_9_6.ppm

1. Stop the ManageEngine OpManager service.
2. Run `C:\ManageEngine\OpManager\bin\UpdateManager.bat`
3. Browse to the location of the upgrade files.
4. Open the OpManager upgrade package.
5. Run the upgrade process by clicking “Install...”

6. Complete the install process with UpdateManager.
7. Click Close.
8. Exit UpdateManager.
9. Start the ManageEngine OpManager service.
10. Repeat steps 1 - 9 for the remaining upgrade packages.
11. Restart the ManageEngine OpManager service.

Notice During an upgrade, the device templates may be modified to include the latest modifications, but they will not be applied to the existing devices. The existing devices will keep their current set of performance monitors and WMI monitors. If you want the modifications to be applied to your existing devices, you will need to apply the changes as follows:

a. Go to Settings > Monitoring > Device Templates.

b. Select the template you wish to update.

c. Click Save and Associate.

d. Select the devices to update and click Apply & Overwrite.

1.6 Enterprise Installation

The procedure for installing an Enterprise license package is the same as the Essential Installation, with the following minor variations.

- you must select Central when installing Tait EnableMonitor on your main server
- you must select Probe when installing Tait EnableMonitor on any other servers

Notice During the Probe installation the location of the Central server is required, so it is imperative that the Central server is installed before creating a Probe.

1.7 Updating the Configuration Package

The following procedure details the steps required to update Tait EnableMonitor with a configuration package change.

1. Open Windows Explorer

2. Run the latest Tait EnableMonitor configuration package. You will be prompted to log in at administrator level.

3. Restart the OpManager service.

Notice During an upgrade, the device templates may be modified to include the latest modifications, but they will not be applied to the existing devices. The existing devices will keep their current set of performance monitors and WMI monitors. If you want the modifications to be applied to your existing devices, you will need to apply the changes as follows:

   a. From the Admin tab select Device Templates.

   b. Select the template you wish to update, click Apply.

   c. Select the devices to update and click Apply, then click Overwrite.

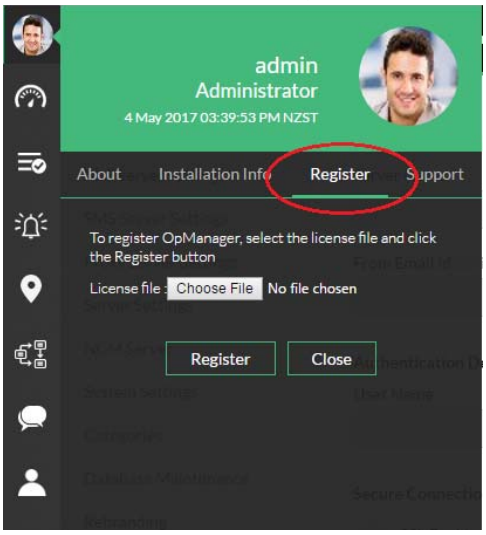
1.8 Installing the License File

The license file is an `xml` file provided by Tait.

1. Ensure that the EnableMonitor Server is running.

2. Login to the EnableMonitor Web Client.

3. To register the license click on User, then select Register.



4. Click Choose File and navigate to the license file.

5. Click Open

6. Click Register.

If you are applying the registered license after expiry of the evaluation license, then do the following:

1. Start the EnableMonitor Server. You will see the message ‘Trial Period has Expired’.
2. Click OK to enter the License details.
3. Browse and select the Registered License file provided to you and click Next.
4. Verify the licensing details displayed and click Finish.

It is important that you apply the correct license to your system:

- For a standalone system, you need an ESSENTIAL license
- For a distributed system with a central server and probes, you need an ENTERPRISE license

The system will not check if you have applied the right license.

2 Setting Up Tait EnableMonitor

2.1 Overview

With Tait EnableMonitor, you can monitor the health of your radio network at a glance, from an overall view of the entire network down to dashboard views of each individual element, including the status of the network link elements. You can specify the equipment parameters to monitor as performance indicators, and you can set up email or SMS notifications for specific alarms. It is also possible to use a control relay to set off flashing lights or a siren for major alarms.

As well as the real time views of your network, Tait EnableMonitor also offers a range of reports so that you can monitor any changes in performance indicators over a period of time.

To get started, Tait EnableMonitor needs the following information:

- a list of categories of network elements (such as router, controller, basestation)
- MIB files for your network elements, i.e.`TAIT-INFRA93SERIES-MIB.mib`
- device templates, i.e. Tait TN9300 (containing information about the actual items in your network, such as the category and the monitoring interval assigned to each one)

Tait EnableMonitor has already been pre-configured with the details of a wide range of possible network elements (both Tait and third-party equipment), so these steps may not need to be done.

Once Tait EnableMonitor has the above information, the following steps can be taken:

- create credentials for your network elements (these are the protocol types and passwords Tait EnableMonitor may need to be able to access them)
- provide your network elements' IP addresses so that Tait EnableMonitor can 'discover' all the devices on your network
- create multiple business views of each part of your network (i.e. by site, and/or as a whole) and create the links between the different devices
- create an actual Google map with the physical location of your network elements
- create log in details for your users, with the appropriate access levels

Details on how to do this are supplied in the following sections, as well as information on how to further customize Tait EnableMonitor, if required.

This guide has been written purely to provide information on how to get Tait EnableMonitor up and running for your network. It does not cover information on how to respond to alarms or other events that may take place on your network.

2.2 Creating and Assigning Credentials

Tait EnableMonitor accesses your remote devices using the SNMP, CLI, or WMI protocols. The credentials for your remote devices, such as the password/snmp community, port etc., may differ for different device types. Pre-configuring a set of credentials in Tait EnableMonitor helps with applying them to multiple devices at a time, saving a lot of manual effort.

2.2.1 Creating a Set of Credentials

1. Go to Settings > Discovery > Credentials.
2. Click Add Credential.
3. Select the Monitor radio button.
4. Configure the following parameters and click Save to add the credentials:

   Credential Type: Select the relevant protocol.

   - SNMP v1/v2 - SNMPv1 and SNMPv2 are community based security models. Enter the credential name and description. Configure the correct Read and Write community, SNMP Port, SNMP Timeout (in seconds) and SNMP Retries.
   - SNMP v3 - SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters:

     a.Name: Enter the name of the credential.

     b.Description: Enter a brief description about the credential.

     c.User Name: Enter the name of the user (principal) on behalf of whom the message is being exchanged.

     d.Context Name: An SNMP context name or “context” in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The “context name” is an octet string, which has at least one management

information.

e.Authentication: Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/ privacy keys in SNMPv3 applications.

f.Encryption: Select any of the encryption protocols either DES or AES-128 and enter the password. Note: You can only configure Encryption after configuring Authentication.

g.SNMP Port: Enter the SNMP port number, Time Out and Retries.

- Windows/WMI - If you select WMI as the credential type, configure the Domain Name, the user name, and the password. Example:- TestDomain\TestUser. Also enter the credential name and description.

  This applies to the EnableProtect KMF server. The WMI credentials have to be set up to monitor the EnableProtect KMF. Enter your domain\username (for example, `TEL\Administrator`) and a corresponding password. For more information, please refer to the KMF system Administration Manual.

- Telnet/SSH - Enter the credential name. Select either the Telnet or SSH protocol from the protocol drop down menu. Configure the port number and time out interval. For Telnet/SSH, make sure you configure the correct login prompt, command prompt, and password prompt besides the user name and password to access the device.

- VMware - Enter the credential name. Provide the HTTPS Username and Password of the Host. Enter the HTTPS web service port number and timeout interval for the connection between the Host and Tait EnableMonitor server.

The SNMP credentials created are used during the initial discovery and classification. Tait EnableMonitor uses these credentials to classify and add the devices into Tait EnableMonitor.

2.3 Discovering Your Devices

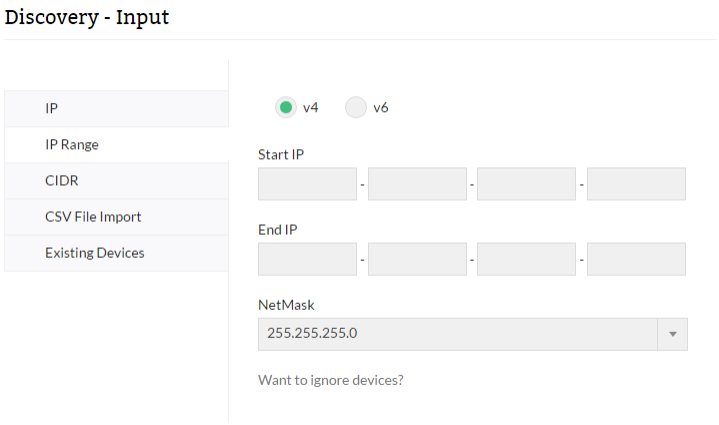
You can discover devices on a network by either specifying a range of IP addresses or the entire network.

Tait EnableMonitor uses ICMP/Nmap to discover the devices on a network.

2.3.1 Discover a Range

To discover devices from a selected range specify the start and end IP address and select the netmask for the devices to be discovered within that range.

1. Go to Settings > Discovery > Discovery.
2. Click IP Range.



3. Select either v4 or v6 radio button to specify the IP protocol revision used.
4. Start IP: Specify the IP address of the device in the range from where Tait EnableMonitor should start discovery.
5. End IP: Specify the IP address at the end of the range that Tait EnableMonitor should discover.
6. Netmask: Select the correct netmask.
7. Click Next.
8. Discovery Credentials: Select the Credentials to be used for discovery.
9. Click Next.
10. Discovery Rules: Select the Rules that will be used for discovery.
11. Click Next.
12. Discovery Interface: Select the interface options for discovery. These settings will differ depending on your network configuration.
13. Click Next.
14. Schedule when the discovery will be executed.
15. Click Next.
16. Optionally configure and include an Email notification for the discovery report.

17. Click Next.
18. Review the discovery summary and click either Save and Execute to execute the discovery task, or Save.

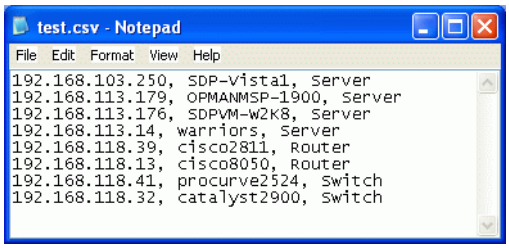
2.3.2 Discover a Complete Network

1. Use CIDR: Select this option to discover an entire network.
2. Network IP: Specify the Network IP to be discovered.
3. Click Next.
4. Discovery Credentials: Select the Credentials to be used for discovery.
5. Click Next.
6. Discovery Rules: Select the Rules that will be used for discovery.
7. Click Next.
8. Discovery Interface: Select the interface options for discovery. These settings will differ depending on your network configuration.
9. Click Next.
10. Schedule when the discovery will be executed.
11. Click Next.
12. Optionally configure and include an Email notification for the discovery report.
13. Click Next.
14. Review the discovery summary and click either Save and Execute to execute the discovery task, or Save.

2.3.3 Discover by Importing from a File

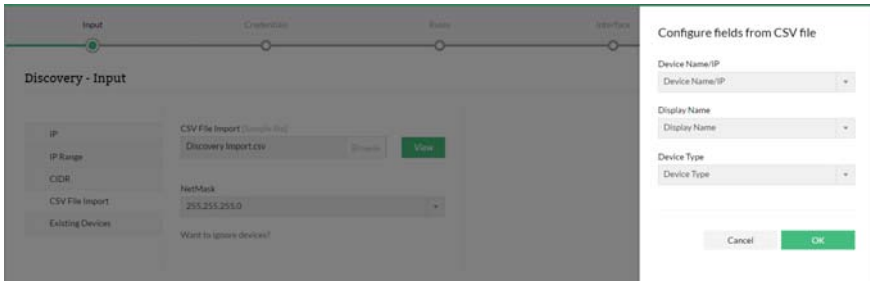
You can import a set of IP addresses for discovery from a csv file.

1. Create a csv file (as shown below) with the Device Name/IP address of the device, Display Name and Device Type.



2. Browse and select the CSV file from which you want the devices discovered and imported.

3. Select the Device Name/IP, Display Name and Device Type columns in the CSV file and click OK.



4. Discovery Credentials: Select the Credentials to be used for discovery.

5. Discovery Rules: Select the Rules that will be used for discovery.

6. Click Next.

7. Discovery Interface: Select the interface options for discovery. These settings will differ depending on your network configuration.

8. Click Next.

9. Schedule when the discovery will be executed.

10. Click Next.

11. Optionally configure and include an Email notification for the discovery report.

12. Click Next.

13. Review the discovery summary and click either Save and Execute to execute the discovery task, or Save.

2.3.4 Assigning Credentials

You can use the Quick Configuration Wizard to associate a credential to several devices at one go:

1. Go to Settings > Configuration > Quick Configuration Wizard.
2. Select ‘Credentials’ and click Next.
3. All of the available Credentials are listed. Select the Credential which you want to associate to your devices.
4. Select the devices to which you want to assign the credential from the column on the left and move them to the right.
5. Click Associate. The Credential is now associated to the selected devices.

2.4 Creating Your Business Maps

Click on Maps. The default maps are displayed Under Business Views, with options to add more maps.

2.4.1 Adding Views

1. Go to Maps > Business Views > Create New.
2. Configure a name for the business view.
3. Click Background and select a background image from those provided. Alternatively, download the background of your choice from the internet, taking into account any copyright requirements.

ⓘ To upload a downloaded background image click Choose File, select the file and click open, then click Upload.

4. Click Save.
5. From the available devices list, select the devices you want to be grouped in this business view, and drag them to the right, onto the map page. Tait device icons, as per the illustrated examples, are included with the Tait EnableMonitor package.

6. Once the devices are dropped on the map, select and drag-drop the devices to be placed in the required location on the map.

7. Click Save to create and save the map.

8. Click Exit to see the newly created business view. You will also find the availability dashboard for the devices in the business view.

2.4.2 Drawing a Link Between Devices

To represent the network diagram in the map, you can draw links between the devices in a business view. You can assign a meaningful name to the link and also configure it to change the color to indicate its status.

To draw a link, follow the steps given below:

1. Click the Add Link button (top middle).

2. From the map below, click the device from which you want to draw a link (the source device) and move the mouse to the destination device and click that device. A link properties dialog pops up.

3. Configure a display name for the link.

4. In the Get Status Form field, select any interface from either the source device or the destination device. The link will inherit the status of the interface that you choose here. For instance, if the source device goes down, and if you have selected an interface from that device, the link display will indicate that it is down.

5. Select the thickness of the link.

6. Click Apply.

7. Click Save on the top left to save the changes (when the map has saved there is no prompt or advisory to say it has been saved).

2.4.3 Modifying Business Views

You can edit the business views created:

1. Access the business view either from the Maps tab or from the list of views under the Home tab.

2. Click the Edit icon to modify the view properties.

3. After editing the view, for example by adding/removing links, adding more devices to the view, adding shortcuts on the view, or changing the background, click the Save button on the left to save your changes.

2.4.4 Adding Shortcuts

You can add shortcut icons to business views that help you to drill down through the network. This helps you to easily navigate to a view from another view when objects are grouped based on their geographical location.

You must have created at least two business views to be able to add a shortcut from one view to another.

Here are the steps to add shortcuts on the business views:

1. Go to the business view and click the Edit option in the right top corner of the view.
2. Click the Add Shortcut button at the top. A shortcut properties dialog pops up.
3. Configure a name for the shortcut in the Shortcut Name field.
4. From the Open Submap list-box, select the map which should be opened when you click the shortcut.
5. Select the icon to be used for the shortcut from the Default Icons or select from the Custom Icon combo-box.
6. Click Done for the shortcut to be added.

2.4.5 Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents unnecessary status checks made to the dependent devices.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

To configure the dependency for devices, follow the steps given below:

1. Go to Settings > Monitoring > Quick Configuration Wizard.
2. Click Device Dependencies.
3. Select the category of the device, Router or Switch, on which the dependency is to be configured. The devices managed under the chosen directory are listed. Choose a device and click Next.
4. Choose how you want to associate the device dependency. Select from:
   - Assign to all devices in the Category
   - Assign to all devices in the Businessview

- Manually group devices

5. Click Associate.

Configuring dependencies in individual devices

You can also configure dependencies for a single device from the device snapshot page. Follow these steps:

1. Go to the Inventory page.
2. Click on the device that you want to configure.
3. Click Full View ( ).
4. Click .
5. Click Edit device details.
6. From the Uplink Dependency list, select the device on which it is dependent.
7. Click Save.

Tait EnableMonitor stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.

2.5 Creating a Network Map with Google

You can integrate Google Maps with this application, and place your devices on the maps according to their geographic distribution.

See the OpManager online help for further details.

An Internet connection is required to access Google maps. A commercial licence for Google Maps is required if you wish to use this feature.

2.5.1 Adding Devices on the Google Map

1. Zoom in/out the map and double-click on the location where you want to place a discovered device.
2. A device list box pops up allowing you to select a device to be placed in that location.
3. Select the device and click on Add.
4. Add the required devices on to the map by double-clicking on their locations.
5. You can also add the devices to the map from the device snapshot page:

a. Go to the device snapshot page.
b. Click on Add to Google Map link in the page to add the device to the map.

2.5.2 Viewing Device Details from Google Map

1. Click on the device balloons on the Google Map to see a popup.
2. Click the device name/IP address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

2.5.3 Deleting Devices from Google Map

1. Click on the device balloons on the Google Map to see a popup.
2. Click the Delete link on this popup to delete the device from the map.

2.6 Creating Users

You can create users in Tait EnableMonitor and provide required privileges to them. The option to create users is available only for the admin login account or those accounts which have 'Full Control' privilege. To add a user:

1. Go to Settings > General Settings > User Management.
2. Click Add User.

3. Configure the following on the User Details tab:
   a. Role:
      Administrator - provides the user with full control of the system
      Operator - provides the user with read-only permissions
   b. User Type:
      Local Authentication
      Radius Authentication
      AD Authentication

c. Contact Details

Email ID - email address for the user

Phone Number - phone number for the user

Mobile Number - mobile number for the user

d. Login Details:

Password - a password for the user

Re-type Password - re-type the password for confirmation

e. Time Zone - a time zone for NetFlow reports

4. Click Next.

5. On the Scope tab, configure the user's access to the following:

Monitor - provide the user access to All Devices or Selected Business Views.

NetFlow - provide the user with access to specific NetFlow groups.

NCM - provide the user with access to specific NCN groups.

Firewall - provide the user with access to specific Firewall devices.

6. Click Save.

7. Logout and try logging in as the new user and check the privileges.

Password security

To create really secure passwords, they should be at least 8 characters long, and contain both upper and lower case letters as well as numbers.

You should create at least two Full Control accounts under the names of different people for your system administrators, and then delete the default `admin` login once this has been done. Each user (whether an administrator or read-only user) must have their own user account. Usernames and passwords must not be shared.

It is considered bad practice to retain default usernames and passwords, or to allow shared login authentication because it then becomes impossible to verify access.

2.7 Creating Email and SMS Alerts

Tait EnableMonitor allows you to send email and/or SMS alerts to network administrators when a fault is detected in a network device.

2.7.1 Configuring Mail Server Settings

By default, Tait EnableMonitor sends an email to the mail server specified in the email notification profile. To configure the SMTP server settings, and to provide secondary mail server settings if required, follow the steps given below:

1. Select Settings > General Settings > Mail Server Settings.
2. Enter the SMTP Server name, Port number and Time Out.
3. Configure the From and To Email ID fields.
4. Configure the Username and Password details, if your server requires authentication to send emails.
5. For SSL authentication, select the SSL Enabled check box, click browse to select the SSL certificate, then enter the password.
6. If you have a secondary mail server in your network, select Add a secondary mail server and provide the details. If the primary mail server should fail, Tait EnableMonitor will use the secondary mail server to send emails and SMS.

Verifying mail server configuration

To test your mail server settings enter the Email ID and click Test Mail. This email ID will be considered as the default To Email ID while creating Email and SMS notification profiles.

2.7.2 Creating Email Alert Profiles

To send an email to network administrators when a fault is detected in a network device, you need to set up notification profiles. Each network administrator should have a separate profile, especially if different administrators are responsible for different network devices, so that whenever a particular device has a fault, an email is sent to the person concerned.

To create an email alert profile, follow the steps given below:

1. Go to Settings > Notifications > Add Profile.
2. Select Email from the list.
3. Type valid To and From Email addresses.
4. Select the required alarm variables and other content, such as the subject, that will appear in the email alert. Click Next.
5. Select the fault criteria for which this profile will be notified. For instance, if you want this profile to be notified of a threshold violation, select ‘Threshold rule is violated’. Click Next.

6. Select the devices or the category of devices for which this profile should be associated.

   For example, if you want this profile to be notified of threshold violations in any of your servers, select the Server category from the combo-box. Click Next.

7. Select the scheduling options for the notification. You can configure when and how often the notification is triggered. Click Next.

8. Review the notification message and give the profile a name.

9. Click Save.

2.7.3 Configuring SMS Alerts

For Tait EnableMonitor to send SMS alerts to network administrators when a fault is detected in a network device, you need to set up notification profiles. Each network administrator should have a separate profile, especially if different administrators are responsible for different network devices, so that whenever a particular device has a fault, an SMS is sent to the person concerned.

To create an email-based SMS notification profile, follow the steps given below:

1. Configure the Mail Server Settings (see “Configuring Mail Server Settings” on page 30).

2. Go to Settings > Notifications > Add Profile.

3. Select Email based SMS.

4. Type valid To and From Email addresses.

5. Select the required alarm variables that you would like to see in the SMS alert. Click Next.

6. Select the fault criteria for which this profile will be notified. For instance, if you want this profile to be notified of a threshold violation, select ‘Threshold rule is violated’. Click Next.

7. Associate the profile to the required devices. This triggers alerts when faults occur. Click Next.

8. Select the scheduling options for the notification. You can configure when and how often the notification is triggered. Click Next.

9. Assign a meaningful name to this profile.

10. Click Save.

Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in Tait EnableMonitor. Whenever a new SMS

profile is created, the values of the primary SMTP server and the authentication details will be taken from your mail server settings. Refer to “Configuring Mail Server Settings” on page 30. If the primary SMTP server is not available, the secondary mail server will be used.

2.8 Final Step

Once your configuration is complete, it is recommended that you create a backup of all your data.

For information on how to back up and restore, go to “Dials” on page 70.

2.9 TN9400 Process Monitors

Once the Tait EnableMonitor installation procedure has been completed (Section 1) and you have customized the Tait EnableMonitor configuration for your TN9400 network (Section 2), use the following procedure to select your process monitors.

1. From your Business View (Inventory > Business Views), click on a device to display the snapshot page for that device.
2. From the Device Details tab, click Full View ( ) and then .
3. Click Edit device details.
4. Open the Type drop down list of available templates. Scroll down to select the template that applies to the device.
5. Click Save.
6. From the Monitor tab ( ), select Process Monitors and click to add the process monitors for the device. See the table of suggested monitors for each device type below.
7. Repeat this procedure for every device that is being monitored.

The following table lists the recommended process monitors to select:

Device	Process monitor
Common to all servers (including high availability)	■ httpd ■ monit ■ ntpd ■ snmpd ■ snmptrapd
High availability servers	■ heartbeat ■ drbd

Device	Process monitor
RFSS[1]	■ mysqld ■ Rlr (RlrService) ■ Rm (RmService) ■ Rnc (RncService)
Site Controllers[1]	Sc (ScService)
PSTN Gateways	Pstng (PstngService)

1. It is recommended that RFSS and Site Controllers be configured as HA servers

3 Using a Control Relay for Major Alarms

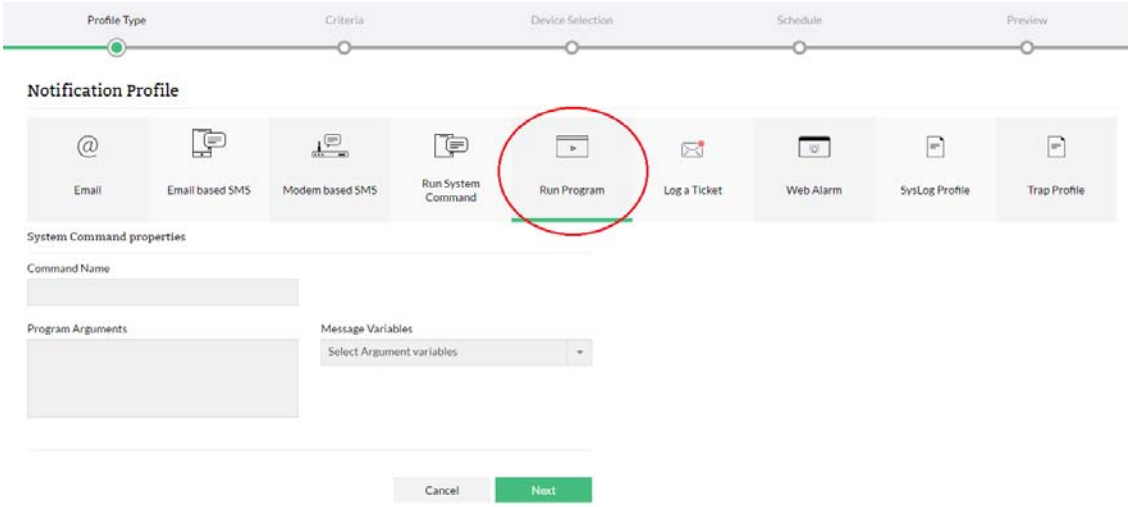
Critical major alarms generated by Tait EnableMonitor can be configured to activate a light, or sound an external siren, if required. To do this, the Tait EnableMonitor notification profile feature is used, together with (in this example) an Ontrak ADU208 I/O relay that is connected to the light/siren.

The number of notification profiles which can be created is limited to eight notification profiles, since there are only eight output ports available on the Ontrak ADU208 I/O relay.

The following sections describe the steps required to use the TaitRelayController utility through the notification profile in Tait EnableMonitor.

3.1 Creating Notification Profiles

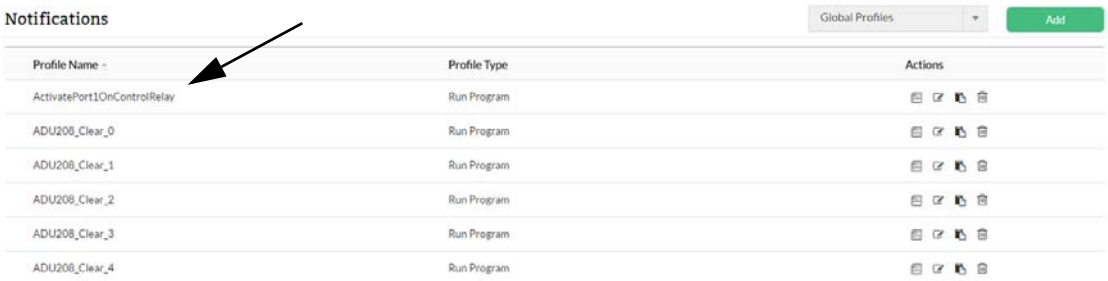
1. In Tait EnableMonitor go to Settings > Notifications > Add Profile.
2. Click Add.
3. Select Run Program



4. Enter the Command Name. This is the absolute path to the TaitRelayController utility. This utility has a command line parameter in the form:
`-w SKn (n=0...7)` to set (turn ON) an output port, or `-w RKn (n=0...7)` to reset (turn OFF) an output port.
5. If required, enter the program arguments. (e.g. **`-w SK1`**).

Selecting Message Variables from the list will enter them into the Program Arguments text box.

6. Click Next.
7. Select the fault criteria for which you need to be notified.
8. Click Next.
9. Select the Device(s) that the notification profile will be associated to.
10. Click Next.
11. Schedule the time (and date) the profile should be applied and click Next.
12. Review the notification profile settings and enter a profile name into the Give profile name to add field.
13. Click Save.
14. After saving the profile, it will appear in the Run Program list on the Notification Profiles window.



4 SNMP Traps

4.1 Overview

SNMP Traps are the messages received from SNMP devices about any faults that have occurred. They are alerts generated by the agents of a managed device, such as the elements of your network that have been declared to Tait EnableMonitor.

4.2 Processing SNMP Traps into Alarms

Tait EnableMonitor enables you to process the traps from the managed devices:

- When a trap is received from a managed device, the match criteria in the parser determines whether a specific trap matches the conditions specified in the trap processor. Once a matching trap is found, an alert is generated.
- The trap processor converts the cryptic trap message into a recognizable alarm message.
- Tait EnableMonitor is configured to process the traps that are not processed out-of-the-box as required, and convert them into alarms.
- Any traps that are not processed are listed under ‘Unsolicited Traps’.

When updating Tait EnableMonitor, SNMP traps can be automatically configured by selecting the “Automatically update trap processor details” check box. This check box will be selected by default.

4.2.1 Tools

The following actions can be done in Settings > Monitoring > SNMP Trap Processors:

- Edit: click on the name of the trap to edit
- Delete processor: delete the trap processor
- Search Processor: enter the start or end letters of the trap name to search for a trap. You can search by entering an OID too.

4.2.2 Adding to or Modifying the Trap Processor

1. Go to Settings > Monitoring > SNMP Trap Processors.
2. Click Add to add a new trap.

3. Click the TrapParser name or the Edit icon to modify an existing trap.

4. Configure/Modify the following properties:
   - Name: Configure a name for the new trap processor.
   - Description: Describe the trap.
   - Snmp Trap Version: Select the version (SNMP V1 or V2C/V3).
   - SNMP V1 Properties:
     - Generic Type: Cold Start, Link Up, Enterprise, etc. Select the appropriate type for the OID.
     - Specific Type: when the Generic Type is set to Enterprise, specify a specific trap ID
     - Enterprise OID: the corporation or organization from where the trap originated, such as .1.3.6.1.4.1.x SNMP V2C / V3
   - SNMP V2C/V3 Properties:
     - Trap OID: for devices with SNMP V2C/V3, select the trap OID from the MIB using the Select button
   - Severity: select the alarm severity (see “Recommended Trap Settings” on page 41)
   - Failure Component: this option is useful when you deal with a single trap OID that has multiple failure components. The VarBinds containing more details on the trap will have information on the failed components (entities like cpu, temperature etc). You can also match the entity by appending the VarBind number in this field to generate separate alarms for the failed components. For instance: $Source_trapName_trap_$5.
   - Source: Append the varbinds to be matched if required. This option is useful if the trap has been forwarded from another source.
   - Message: select the required message variables
   - Match Criteria: specify the following match conditions for further processing of traps:

     •Match Criteria: select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.

     •Rearm Criteria: similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.

5. Click Save for the configuration to take effect.

4.3 Loading Trap Parsers from a MIB

The following procedure describes how to load the traps from a MIB:

1. Select Settings > Monitoring > SNMP Trap Processors to display all of the configured processors.
2. On the right, click Load From Mibs.
3. From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are then listed.
4. Select the required trap variable(s), and click Save.

   A processor for the selected trap(s) is added, and is listed under SNMP Trap Processors.

Cisco traps are loaded by default.

4.4 Configuring the Trap Settings

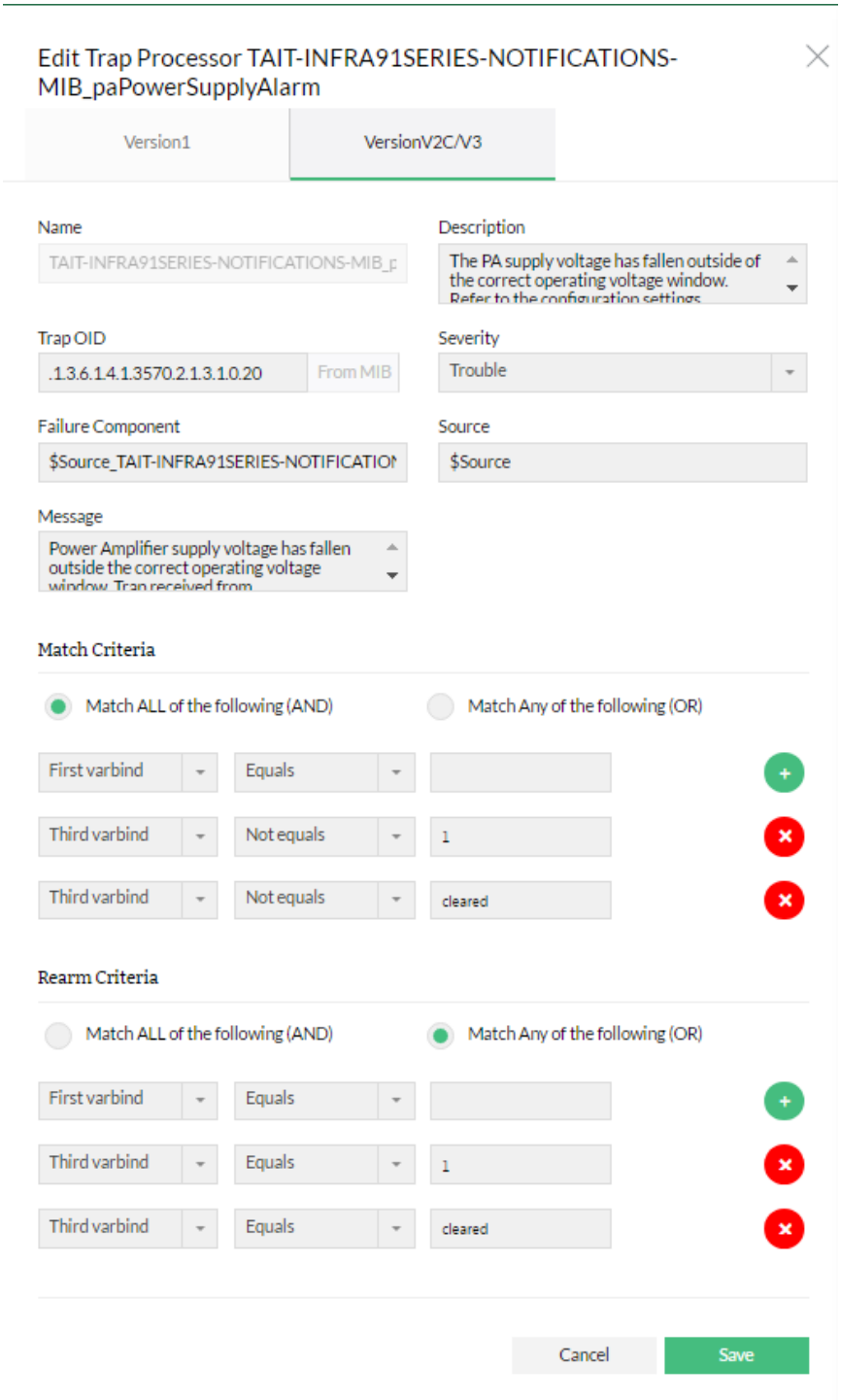
Each trap has an associated severity level that needs to be configured. Four levels are available:

- Critical
- Trouble
- Attention
- Clear

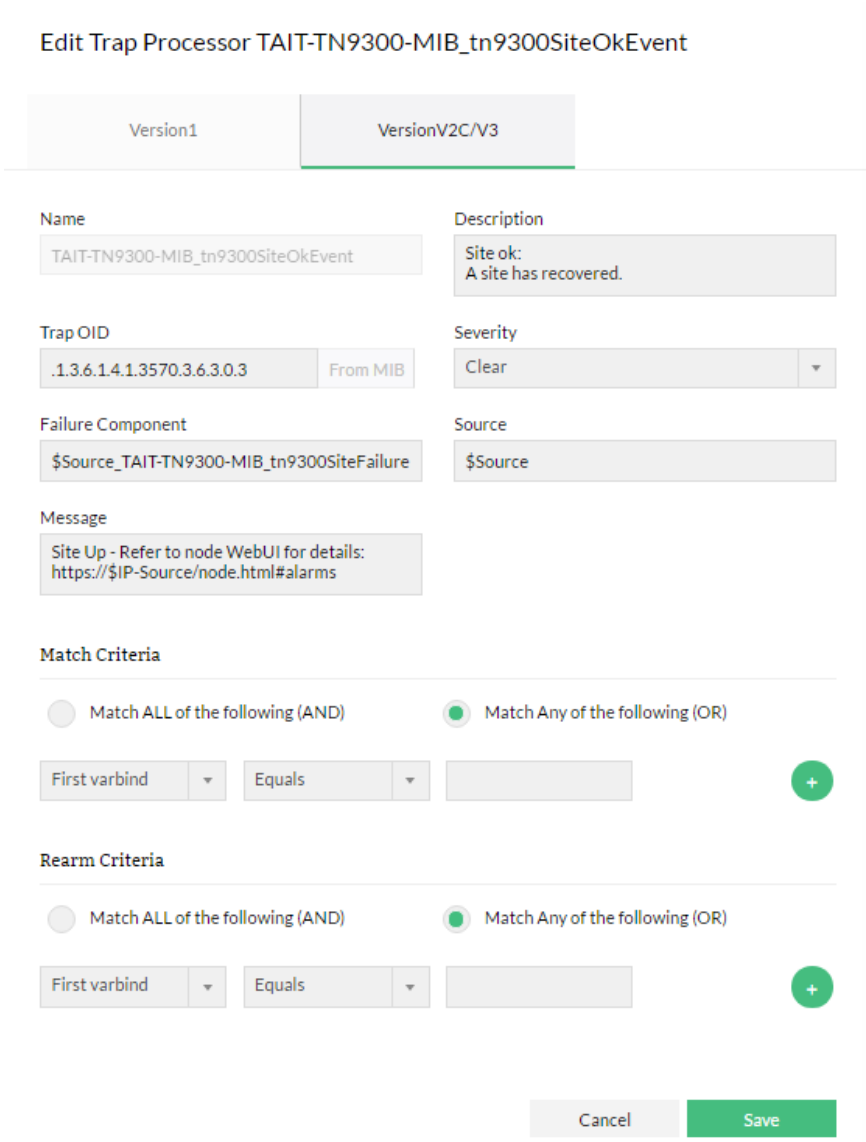
There are several types of trap, as follows:

1. A trap may include a variable indicating if it is an alarm or an event to clear an existing event. This variable needs to be identified and the expected values need to be specified to raise and/or clear the alarm.

   Use the Match Criteria and the Rearm Criteria and define the Severity appropriately.



2. A trap may be used to raise an alarm, with a separate trap used to clear the event. The trap clearing the alarm needs to know the alarm source trap.



Use the parameter called ‘Failure Component’ to program the clearing of the alarm. This is required when the cleared trap is different from the raised trap. Remember to define the Severity appropriately.

3. A trap may not be cleared automatically and the operator will need to acknowledge, clear and delete the alarm manually from the Active Alarms list.

4.5 Recommended Trap Settings

Notice Configuring SNMP Traps in the Agent:
If you have configured the SNMP Trap Processor in Tait EnableMonitor, but still cannot see the alarms based on these traps, you might need to check the SNMP agent configuration for the monitored devices.

We recommend updating the default severity settings to the settings listed in the following tables:

4.5.1 Tait Traps

Notice For EnableReport, TN9400 and EnableProtect KMF, go to the DELL website to download the DELL MIBs—in particular the DCMIB73_A00 package that contains the following files: `dellcm.mib` and `DELL-RAC-MIB.txt`. You will need to load the traps of these MIBs.

TN9300

If the TN9300 is installed on a Sun server, load the traps for files: SUN-PLATFORM-MIB.mib and SUN-HW-TRAP-MIB.mib.

From v3.24 (or 2.24) onwards, a new set of SNMP trap notification objects has been introduced as an alternative to the existing MIB for better clarification of trap events. The Trap version parameter has been added to Settings > Local Parameters > SNMP of the node WebUI to allow the user to select which version of notifications the Node should use. By default, the old notifications are selected for backwards compatibility with existing SNMP management tools.

Pre node version 3.24 (2.24) traps

This option uses the same set of traps included in controllers prior to version 3.24. In the MIB file, the traps used under the tn9300EventsV2 node would be numbered from 1 to 33.

For this version, the controller usually uses one trap to raise a condition and another to clear it. This can lead to confusion, and can make configuration complicated, as the SNMP monitoring tool needs to link the raising trap to the clearing trap for each event type.

The following TN9300 traps are from TAIT-TN9300-MIB:

Trap Name	Severity	Failure Component
TAIT-TN9300-MIB_tn9300 ChannelFailureEvent	Critical	
TAIT-TN9300-MIB_tn9300 ChannelJammedEvent	Trouble	

Trap Name	Severity	Failure Component
TAIT-TN9300-MIB_tn9300 ChannelMajorAlarmEvent	Trouble	
TAIT-TN9300-MIB_tn9300 ChannelMinorAlarmEvent	Attention	
TAIT-TN9300-MIB_tn9300 ChannelOkEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300ChannelMajorAlarmEvent_trap $Source_TAIT-TN9300-MIB_tn9300 ChannelMinorAlarmEvent_trap $Source_TAIT-TN9300-MIB_tn9300ChannelFailureEvent_trap)
TAIT-TN9300-MIB_tn9300 ChannelUnjammedEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300ChannelJammedEvent_trap)
TAIT-TN9300-MIB_tn9300 ControlChannelEvent	Attention	
TAIT-TN9300-MIB_tn9300 DipLinkDownEvent	Critical	
TAIT-TN9300-MIB_tn9300 DipLinkUpEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300DipLinkDownEvent_trap)
TAIT-TN9300-MIB_tn9300 LicenseCheckFailedEvent	Critical	
TAIT-TN9300-MIB_tn9300 LowDiskSpaceEvent	Attention	
TAIT-TN9300-MIB_tn9300 NetworkErrorEvent	Critical	
TAIT-TN9300-MIB_tn9300 NetworkGatewayDownEvent	Critical	
TAIT-TN9300-MIB_tn9300 NetworkGatewayUpEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300NetworkGatewayDownEvent_trap)
TAIT-TN9300-MIB_tn9300 NetworkUpEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300NetworkErrorEvent_trap)
TAIT-TN9300-MIB_tn9300 NodeActivationEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300NodeFailedEvent_trap)
TAIT-TN9300-MIB_tn9300 NodeFailedEvent	Critical	
TAIT-TN9300-MIB_tn9300 RemoteNodeDownEvent	Critical	
TAIT-TN9300-MIB_tn9300 RemoteNodeSyncFailedEvent	Critical	
TAIT-TN9300-MIB_tn9300 RemoteNodeSyncOkEvent	Clear	($Source_TAIT-TN9300-MIB_tn9300RemoteNodeSyncFailedEvent_trap)

Trap Name	Severity	Failure Component
TAIT-TN9300-MIB_tn9300 RemoteNodeUpEvent	Clear	($Source_TAIT-TN9300-MIB_ tn9300RemoteNodeDownEvent_ trap)
TAIT-TN9300_MIB_tn9300 SiteFailureEvent	Trouble	
TAIT-TN9300_MIB_tn9300 SiteOkEvent	Clear	($Source_TAIT-TN9300-MIB_ tn9300SiteFailureEvent_trap)
TAIT-TN9300_MIB_tn9300 SipLinkUpEvent	Clear	($Source_TAIT-TN9300-MIB_ tn9300SipLinkDownEvent_trap)
TAIT-TN9300_MIB_tn9300 SipLinkDownEvent	Critical	
TAIT-TN9300_MIB_tn9300 UnitStatusMessageEvent	Attention	
TAIT-TN9300-MIB_tn9300 AuthenticationOkEvent	Clear	($Source_TAIT-TN9300-MIB_ tn9300AuthenticationFailure Event_trap)
TAIT-TN9300-MIB_tn9300 AuthenticationFailureEvent	Trouble	
TAIT-TN9300-MIB_tn9300 UnitDeregisteredBySystemEvent	Attention	

Node version 3.24 (2.24) traps

This option uses a new set of traps that provides an alternative to how conditions are raised and cleared. In the MIB file, the traps used under the tn9300EventsV2 node would be numbered from 34 onwards. Note that new traps would only be available as part of this option.

For this version, the raising and clearing of conditions has been simplified by using only one trap for both, relying on the data included for further details. Variable bindings are a combination of the following (2, 3 and/or 4 may not be present for all):

1. Severity
2. State to determine whether a condition has been raised or cleared
3. Details of the object involved to locate it (site name, unit address, SIP/DIP line name, etc.)
4. Other useful information

The majority of traps are sent whenever a condition is raised or cleared. However, there are a few traps that are sent mainly as a single notification only (i.e. with no scenario to clear it). Such traps would not have the state included in its variable bindings.

The following TN9300 traps are from TAIT-TN9300-MIB:

Trap Name
TAIT-TN9300-MIB_tn9300BSStateEvent
TAIT-TN9300-MIB_tn9300ChannelJammedStateEvent
TAIT-TN9300-MIB_tn9300DipLinkStateEvent
TAIT-TN9300-MIB_tn9300BSMajorAlarmEvent
TAIT-TN9300-MIB_tn9300BSMinorAlarmEvent
TAIT-TN9300-MIB_tn9300NetworkGwConnEvent
TAIT-TN9300-MIB_tn9300NodeDiskSpaceEvent
TAIT-TN9300-MIB_tn9300NodeLicenseEvent
TAIT-TN9300-MIB_tn9300NodeNetworkStateEvent
TAIT-TN9300-MIB_tn9300NodeStateEvent
TAIT-TN9300-MIB_tn9300RemoteNodeStateEvent
TAIT-TN9300-MIB_tn9300RemoteNodeSyncEvent
TAIT-TN9300_MIB_tn9300SipLinkStateEvent
TAIT-TN9300-MIB_tn9300SiteControlChCountEvent
TAIT-TN9300_MIB_tn9300SiteStateEvent
TAIT-TN9300-MIB_tn9300UnitAuthenticationEvent
TAIT-TN9300_MIB_tn9300UnitRegTimeoutEvent
TAIT-TN9300_MIB_tn9300UnitStatusMsgEvent

TN9500

Load the traps for files: TAIT-TN9500-MIB.mib and DISMAN-EVENT-MIB.mib.

The following TN9500 traps are from TAIT-TN9500-MIB:

Trap Name	Severity	Failure Component/Message
TAIT-TN9500-MIB_tn9500 unifyNetworkGatewayStartupEvent	Attention	
TAIT-TN9500-MIB_tn9500 iniLinkUpEvent	Clear	($Source_TAIT-TN9500-MIB_ tn9500iniLinkDownEvent_trap)
TAIT-TN9500-MIB_tn9500 iniLinkDownEvent	Critical	
TAIT-TN9500-MIB_tn9500 inpLinkUpEvent	Clear	($Source_TAIT-TN9500-MIB_ tn9500inpLinkDownEvent_trap)
TAIT-TN9500-MIB_tn9500 inpLinkDownEvent	Critical	

Trap Name	Severity	Failure Component/Message
TAIT-TN9500-MIB_tn9500 e1SystemStartupEvent	Attention	
TAIT-TN9500-MIB_tn9500 e1t1redAlarmUpEvent	Clear	($Source_TAIT-TN9500-MIB_ tn9500e1t1redAlarmDownEvent_ trap)
TAIT-TN9500-MIB_tn9500 e1t1redAlarmDownEvent	Critical	
TAIT-TN9500-MIB_tn9500 e1t1yellowAlarmUpEvent	Clear	($Source_TAIT-TN9500-MIB_ tn9500e1t1yellowAlarmDownEvent_trap)
TAIT-TN9500-MIB_tn9500 e1t1yellowAlarmDownEvent	Attention	
TAIT-TN9500-MIB_tn9500 transcoderSystemStartupEvent	Attention	tn9500TranscoderState=$2 Example: “tn9500TranscoderState=operational” Match Criteria: Third varbind not equals operational Rearm Criteria: Third varbind equals operational
TAIT-TN9500-MIB_tn9500 transcoderWorkerErrorEvent	Critical	tn9500TranscoderAlarmState = $2 tn9500TranscoderState = $3 Example: “tn9500TranscoderAlarmState=cleared tn9500TranscoderState=operational” Match Criteria: Third varbind not equals cleared Rearm Criteria: Third varbind equals cleared
TAIT-TN9500-MIB_tn9500 transcoderLicenseInvalidEvent	Critical	tn9500TranscoderAlarmState = $2 tn9500TranscoderState = $3 Example: “tn9500TranscoderAlarmState=raised tn9500TranscoderState=noLicense” Match Criteria: Third varbind not equals cleared Rearm Criteria: Third varbind equals cleared

The TN9500 traps are from DISMAN-EVENT-MIB.

Trap Name	Severity	Message
mteTriggerFired	Attention (depending on the threshold)	The error is: $2, $5 = $6 Example: “The error is: DiskAlmostFull, dskPercent.1 = 94.”

EnableReport

The EnableReport traps are from DISMAN-EVENT-MIB.

Trap Name	Severity	Match/Ream Criteria
mteEventSetFailure	Attention	Match Criteria: Fifth varbind Not Equals 0 Rearm Criteria: Fifth varbind equals 0
mteTriggerFailure	Attention	Match Criteria: Fifth varbind Not Equals 0 Rearm Criteria: Fifth varbind equals 0
mteTriggerFalling	Attention (depending on the threshold)	
mteTriggerFired	Attention (depending on the threshold)	
mteTriggerRising	Attention (depending on the threshold)	

TB9300

The TB9300 traps are from TAIT-INFRA93SERIES-NOTIF-MIB. This MIB covers operation in all modes.

For each trap, configure:

- Match Criteria: Third varbind Not Equals 1 and third varbind Not Equals ‘cleared’
- Rearm Criteria: Third varbind Equals 1 or third varbind Equals ‘cleared’

Trap Name	Severity
paNoPADetectedAlarm	Trouble
paInvalidFirmwareAlarm	Critical
paInvalidCalibrationAlarm	Critical
paForwardPowerLowAlarm	Trouble
paPowerFoldbackAlarm	Critical
paReversePowerHighAlarm	Trouble

Trap Name	Severity
paShutdownImminentAlarm	Critical
paVSWRFaultAlarm	Trouble
paDriverCurrentHighAlarm	Trouble
paFinal1CurrentHighAlarm	Trouble
paFinal2CurrentHighAlarm	Trouble
paCurrentImbalanceAlarm	Trouble
paSupplyVoltageLowAlarm	Trouble
paSupplyVoltageHighAlarm	Trouble
paDriverTemperatureHighAlarm	Trouble
paFinal1TemperatureHighAlarm	Trouble
paFinal2TemperatureHighAlarm	Trouble
pmuNoPMUDetectedAlarm	Trouble
pmuInvalidFirmwareAlarm	Critical
pmuMainsFailureAlarm	Trouble
pmuSelfTestFailureAlarm	Trouble
pmuShutdownImminentAlarm	Critical
pmuTemperatureHighAlarm	Trouble
pmuBatteryProtectAlarm	Critical
pmuBatteryVoltageLowAlarm	Trouble
pmuBatteryVoltageHighAlarm	Trouble
pmuCurrentOutHighAlarm	Critical
pmuVoltageOutLowAlarm	Trouble
pmuVoltageOutHighAlarm	Trouble
systemAmbientTempLowAlarm	Trouble
systemAmbientTempHighAlarm	Trouble
systemExternalRefAbsentAlarm	Trouble
systemNetworkQosJitterAlarm	Trouble
systemNetworkQosLostPacketsAlarm	Trouble
systemFallbackControlled	Critical
systemDuplicateNodePriority	Trouble
rctInvalidChannelSelectedAlarm	Critical
rctOverTemperatureAlarm	Trouble
rctTxCalibrationInvalidAlarm	Critical
rctRxCalibrationInvalidAlarm	Critical

Trap Name	Severity
rctInvalidConfigurationAlarm	Critical
rct25MHzSynthOutOfLockAlarm	Critical
rct6144MHzSynthOutOfLockAlarm	Critical
rctTxFSynthOutOfLockAlarm	Critical
rctRxSynthOutOfLockAlarm	Trouble
customAlarm1Alarm	Attention
customAlarm2Alarm	Attention
customAlarm3Alarm	Attention
customAlarm4Alarm	Attention
customAlarm5Alarm	Attention
customAlarm6Alarm	Attention
customAlarm7Alarm	Attention
customAlarm8Alarm	Attention
customAlarm9Alarm	Attention
customAlarm10Alarm	Attention
customAlarm11Alarm	Attention
customAlarm12Alarm	Attention
fpFan1Alarm	Trouble
fpFan2Alarm	Trouble
fpFan3Alarm	Trouble
fpNoFPDetectedAlarm	Trouble
fpInvalidFirmwareAlarm	Trouble

TB9300 and TB9400

These traps are from NET-SNMP-AGENT-MIB:

Trap Name	Severity
nsNotifyStart	Attention
nsNotifyShutdown	Attention
nsNotifyRestart	Attention

TB9400

The TB9400 traps are from TAIT-INFRA94SERIES-NOTIF-MIB.

For each trap, configure:

- Match Criteria: Third varbind Not Equals 1 and third varbind Not Equals ‘cleared’
- Rearm Criteria: Third varbind Equals 1 or third varbind Equals

‘cleared’

Trap Name	Severity
paNoPADetectedAlarm	Trouble
paInvalidFirmwareAlarm	Critical
paInvalidCalibrationAlarm	Critical
paForwardPowerLowAlarm	Trouble
paPowerFoldbackAlarm	Critical
paReversePowerHighAlarm	Trouble
paShutdownImminentAlarm	Critical
paVSWRFaultAlarm	Trouble
paDriverCurrentHighAlarm	Trouble
paFinal1CurrentHighAlarm	Trouble
paFinal2CurrentHighAlarm	Trouble
paCurrentImbalanceAlarm	Trouble
paSupplyVoltageLowAlarm	Trouble
paSupplyVoltageHighAlarm	Trouble
paDriverTemperatureHighAlarm	Trouble
paFinal1TemperatureHighAlarm	Trouble
paFinal2TemperatureHighAlarm	Trouble
pmuNoPMUDetectedAlarm	Trouble
pmuInvalidFirmwareAlarm	Critical
pmuMainsFailureAlarm	Trouble
pmuSelfTestFailureAlarm	Trouble
pmuShutdownImminentAlarm	Critical
pmuTemperatureHighAlarm	Trouble
pmuBatteryProtectAlarm	Critical
pmuBatteryVoltageLowAlarm	Trouble
pmuBatteryVoltageHighAlarm	Trouble
pmuCurrentOutHighAlarm	Critical
pmuVoltageOutLowAlarm	Trouble
pmuVoltageOutHighAlarm	Trouble
systemAmbientTempLowAlarm	Trouble
systemAmbientTempHighAlarm	Trouble
systemExternalRefAbsentAlarm	Trouble
systemNetworkQosJitterAlarm	Trouble

Trap Name	Severity
systemNetworkQosLostPacketsAlarm	Trouble
system1PPSAbsentAlarm	Attention[1]
systemNetworkQosLatePacketsAlarm	Trouble
systemCartesianLoopUnstableAlarm	Critical
systemTxRCableAbsentAlarm	Critical
rctSimulcastSynchAlarm	Attention[1]
rctInvalidChannelSelectedAlarm	Critical
rctOverTemperatureAlarm	Trouble
rctTxCalibrationInvalidAlarm	Critical
rctRxCalibrationInvalidAlarm	Critical
rctInvalidConfigurationAlarm	Critical
rct25MHzSynthOutOfLockAlarm	Critical
rct6144MHzSynthOutOfLockAlarm	Critical
rctTxFSynthOutOfLockAlarm	Critical
rctRxSynthOutOfLockAlarm	Trouble
rctTxRSynthOutOfLockAlarm	Critical
customAlarm1Alarm	Attention
customAlarm2Alarm	Attention
customAlarm3Alarm	Attention
customAlarm4Alarm	Attention
customAlarm5Alarm	Attention
customAlarm6Alarm	Attention
customAlarm7Alarm	Attention
customAlarm8Alarm	Attention
customAlarm9Alarm	Attention
customAlarm10Alarm	Attention
customAlarm11Alarm	Attention
customAlarm12Alarm	Attention
fpFan1Alarm	Trouble
fpFan2Alarm	Trouble
fpFan3Alarm	Trouble
fpNoFPDetectedAlarm	Trouble
fpInvalidFirmwareAlarm	Trouble

1. Simulcast networks only.

TN8271	No traps available.

TB9100

The TB9100 traps are from TAIT-INFRA91SERIES-NOTIFICATIONS-MIB:

For all traps:

- Match Criteria: Third varbind Not Equals 1 and third varbind Not Equals ‘cleared’
- Rearm Criteria: Third varbind Equals 1 or third varbind Equals ‘cleared’

Trap Name	Severity
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_airTemperatureAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_configurationAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_customAlarm1	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_customAlarm2	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_customAlarm3	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_customAlarm4	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_fanAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_onePPSPulseAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paConfigurationAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paCurrentAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paPowerSupplyAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paTemperatureAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paTransmitterAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_paVswrAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuBatteryAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuConfigurationAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuMainsAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuPowerSupplyAlarm	Critical

Trap Name	Severity
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuShutDownAlarm	Trouble
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_pmuTemperatureAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_refFrequencyAlarm	Attention
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_simulcastAlarm	Critical
TAIT-INFRA91SERIES-NOTIFICATIONS-MIB_synthesizerStatus	Critical

SCADA Gateway (Host Machine)

The SCADA Gateway (Host Machine) traps are from TAIT-TN9361-MIB:

- For High Availability SCADA Gateway installations, $Source must be replaced with the 'Active IP' of the SCADA Gateway system, in the failure component and source. This is because the currently active SCADA Gateway Host Machine will be the $Source of the trap, but the desired device source for the trap is the Active IP address of the SCADA Gateway. For example:

  Failure component: 172.20.159.103_TAIT-TN9361-MIB_tn9361GatewayPacketsDropped_trap_@2

  Source: 172.20.159.103

Trap Name	Severity	Match/Rearm Criteria
TAIT-TN9361-MIB_tn9361 GatewayStartupEvent	Attention	
TAIT-TN9361-MIB_tn9361 GatewayStateChange	Critical	
TAIT-TN9361-MIB_tn9361 NetworkCheckAEvent	Attention	Match Criteria: Second varbind equals failed Rearm Criteria: Second varbind not equals failed

Trap Name	Severity	Match/Rearm Criteria
TAIT-TN9361-MIB_tn9361 NetworkCheckBEvent	Attention	Match Criteria: Second varbind equals failed Rearm Criteria: Second varbind not equals failed
TAIT-TN9361-MIB_tn9361 GatewayDiskSpaceEvent	Trouble	Match Criteria: Second varbind equals active AND second varbind not equals standby AND second varbind not equals program Rearm Criteria: Second varbind equals active OR second varbind equals standby OR second varbind equals program

SCADA Gateway (Gateway-Terminal Interface)

The SCADA Gateway (Gateway-Terminal Interface) traps are from TN9361-MIB:

For all traps:

- The OID of the third varbind in the trap message contains the specific terminal ID. Using the key @2=$2 in the trap message will display the specific terminal ID, with the value corresponding to that terminal.

  @2 can also be used in the failure component to provide a failure component per terminal.

- The DMR site the terminal is on is included as the fourth varbind, and can be printed in the trap message using the $3 key.

Trap Name	Severity	Failure Component	Match/Rearm Criteria
TAIT-TN9361-MIB_tn9361 GatewayMessagesDropped	Clear	($Source_TAIT-TN9361-MIB_tn9361GatewayMessagesDropped_trap_@2)	
TAIT-TN9361-MIB_tn9361 GatewayPacketsFailed	Clear	($Source_TAIT-TN9361-MIB_tn9361GatewayPacketsFailed_trap_@2)	
TAIT-TN9361-MIB_tn9361 GatewayPacketsRetried	Clear	($Source_TAIT-TN9361-MIB_tn9361GatewayPacketsRetried_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalCallFailedNotHome	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalCallFailedNotHome_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalCallFailedRadioBusy	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalCallFailedRadioBusy_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalCallFailedSystemBusy	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalCallFailedSystemBusy_trap_@2)	

Trap Name	Severity	Failure Component	Match/Rearm Criteria
TAIT-TN9361-MIB_tn9361 TerminalDiskSpaceEvent	Critical	($Source_TAIT-TN9361-MIB_tn9361TerminalDiskSpaceEvent_trap_@2)	Match Criteria: Second varbind not equals true Rearm Criteria: Second varbind equals true
TAIT-TN9361-MIB_tn9361 TerminalMoved	Attention	($Source_TAIT-TN9361-MIB_tn9361TerminalMoved_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalNoResponse	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalNoResponse_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalMessagesDropped	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalMessagesDropped_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalPacketsFailed	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalPacketsFailed_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalPacketsRetried	Clear	($Source_TAIT-TN9361-MIB_tn9361TerminalPacketsRetried_trap_@2)	
TAIT-TN9361-MIB_tn9361 TerminalRssiEvent	Attention	($Source_TAIT-TN9361-MIB_tn9361TerminalRssiEvent_trap_@2)	Match Criteria: Second varbind not equals true Rearm Criteria: Second varbind equals true
TAIT-TN9361-MIB_tn9361 TerminalStartupEvent	Attention	($Source_TAIT-TN9361-MIB_tn9361TerminalStartupEvent_trap_@2)	

Trap Name	Severity	Failure Component	Match/Rearm Criteria
TAIT-TN9361-MIB_tn9361 TerminalTemperatureEvent	Attention	($Source_TAIT-TN9361-MIB_tn9361TerminalTemperatureEvent_trap_@2)	Match Criteria: Second varbind not equals true Rearm Criteria: Second varbind equals true
TAIT-TN9361-MIB_tn9361 TerminalVoltageEvent	Attention	($Source_TAIT-TN9361-MIB_tn9361TerminalVoltageEvent_trap_@2)	Match Criteria: Second varbind not equals true Rearm Criteria: Second varbind equals true

4.5.2 SUN Platform

The SUN traps are from SUN-PLATFORM-MIB:

Trap Name	Severity	Match/Ream Criteria
SUN-PLATFORM-MIB_sunPlatAttributeChange Integer	Attention	
SUN-PLATFORM-MIB_sunPlatAttributeChangeOID	Attention	
SUN-PLATFORM-MIB_sunPlatAttributeChange String	Attention	
SUN-PLATFORM-MIB_sunPlatCommunications Alarm	Trouble	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatEnvironmentalAlarm	Trouble	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatEquipmentAlarm	Trouble	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatIndeterminateAlarm	Attention	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatObjectCreation	Attention	

Trap Name	Severity	Match/Ream Criteria
SUN-PLATFORM-MIB_sunPlatObjectDeletion	Attention	
SUN-PLATFORM-MIB_sunPlatProcessingError Alarm	Trouble	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatQualityOfService Alarm	Trouble	Match Criteria: Seventh varbind Not Equals 6 Rearm Criteria: Seventh varbind Equals 6
SUN-PLATFORM-MIB_sunPlatStateChange	Attention	

4.5.3 Zetron ACOM Traps

The Zetron ACOM traps are from ACOM-MIB:

Trap Name	Severity	Failure Component
ACOM-MIB_infoActiveNotif	Attention	
ACOM-MIB_infoClearNotif	Clear	($Source_ACOM-MIB_infoActiveNotif_trap)
ACOM-MIB_majorActiveNotif	Critical	
ACOM-MIB_majorClearNotif	Clear	($Source_ACOM-MIB_majorActiveNotif_trap)
ACOM-MIB_minorActiveNotif	Trouble	
ACOM-MIB_minorClearNotif	Clear	($Source_ACOM-MIB_minorActiveNotif_trap)
ACOM-MIB_rackAddedNotif	Attention	
ACOM-MIB_rackRemovedNotif	Attention	

4.5.4 AVTEC Scout

No traps available.

4.5.5 DPS Telecom

The DPS Telecom traps are from DPS-MIB-<...>:

Trap Name	Severity	Failure Component
dpsRTUcomFailed	Critical	
dpsRTUcomRestored	Clear	($Source_dpsRTUcomFailed_trap)

Trap Name	Severity	Failure Component
dpsRTUPointClr	Clear	($Source_dpsRTUPointSet)
dpsRTUPointSet	Attention (this could be changed by the user depending on the equipment monitored)	
dpsRTUsumPClr	Clear	($Source_dpsRTUsumPSet)
dpsRTUsumPSet	Attention (this could be changed by the user depending on the equipment monitored)	
NetGuardian420_Alarm_ IP_1	Attention (this could be changed by the user depending on the equipment monitored)	
NetGuardian420_Alarm_ IP_1_Clear	Clear	($Source_NetGuardian420_ Alarm_IP_1_trap)
NetGuardian420_Alarm_ IP_2	Attention (this could be changed by the user depending on the equipment monitored)	
NetGuardian420_Alarm_ IP_2_Clear	Clear	($Source_NetGuardian420_ Alarm_IP_2_trap)
NetGuardian420_Alarm_ IP_3	Attention (this could be changed by the user depending on the equipment monitored)	
NetGuardian420_Alarm_ IP_3_Clear	Clear	($Source_NetGuardian420_ Alarm_IP_3_trap)
NetGuardian420_Alarm_ IP_4	Attention (this could be changed by the user depending on the equipment monitored)	

Trap Name	Severity	Failure Component
NetGuardian420_Alarm_IP_4_Clear	Clear	($Source_NetGuardian420_Alarm_IP_4_trap)
NetGuardian420_Ext_Temp_Major	Critical	
NetGuardian420_Ext_Temp_Major_Clear	Clear	($Source_NetGuardian420_Ext_Temp_Major_trap)
NetGuardian420_Ext_Temp_Minor	Trouble	
NetGuardian420_Ext_Temp_Minor_Clear	Clear	($Source_NetGuardian420_Ext_Temp_Minor_trap)

4.5.6 MiMoMax NDL

The MiMoMax traps are from MIMOMAX-MIB::

Trap Name	Severity	Match/Ream Criteria
mwlHighTemperatureTrap	Trouble	
mwlLowSignalLevel	Trouble	
mwlLowVoltageTrap	Trouble	
mwlRFLinkStateTrap	Trouble	Match Criteria: First varbind Not Equals 1 Rearm Criteria: First varbind Equals 1

Trap Name	Severity	Match/Ream Criteria
mwlSubmuxTrap	Trouble	Match Criteria: First varbind Equals 1 OR (Match any of the Following) Second varbind Equals 1 OR Third varbind Equals 1 OR Fourth varbind Equals 1 OR Fifth varbind Equals 1 OR Sixth varbind Equals 1 OR Seventh varbind Equals 1 OR Eighth varbind Equals 1 OR Ninth varbind Equals 1 OR Tenth varbind Equals 1 OR Eleventh varbind Equals 1 OR Twelfth varbind Equals 1 OR Thirteenth varbind Equals 1 OR Fourteenth varbind Equals 1 OR Fifteenth varbind Equals 1 OR Sixteenth varbind Equals 1 OR Seventeenth varbind Equals 1 OR Eighteenth varbind Equals 1 OR Nineteenth varbind Equals 1 Rearm Criteria: First varbind Equals 0 AND (Match all of the Following) Second varbind Equals 0 AND Third varbind Equals 0 AND Fourth varbind Equals 0 AND Fifth varbind Equals 0 AND Sixth varbind Equals 0 AND Seventh varbind Equals 0 AND Eighth varbind Equals 0 AND Ninth varbind Equals 0 AND Tenth varbind Equals 0 AND Eleventh varbind Equals 0 AND Twelfth varbind Equals 0 AND ...
..\cont.		Thirteenth varbind Equals 0 AND Fourteenth varbind Equals 0 AND Fifteenth varbind Equals 0 AND Sixteenth varbind Equals 0 AND Seventeenth varbind Equals 0 AND R Eighteenth varbind Equals 0 AND Nineteenth varbind Equals0

4.5.7 MOXA Switches

The MOXA traps are from MOXA-<*model*>-MIB:

The traps on all the switches are similar.

Trap Name	Severity	Match/Ream Criteria
configChangeTrap	Attention	
power1Trap	Critical	
power2Trap	Critical	
poePDfailureRecoveryTrap	Critical	
poeportpowerfailTrap	Critical	
redundancyTopology ChangedTrap	Trouble	Match Criteria: First varbind Not Equals 1 Rearm Criteria: First varbind Equals 1
trafficOverloadTrap	Critical	
turboRingCouplingPort ChangedTrap	Trouble	Match Criteria: First varbind Not Equals 1 Rearm Criteria: First varbind Equals 1
turboRingMasterChanged Trap	Trouble	Match Criteria: First varbind Not Equals 1 Rearm Criteria: First varbind Equals 1

4.5.8 Airbus DS Communications MIBs

P25 Controllers

The P25 traps are from EADS-P25-BCSS-MIB, EADS-P25-IPDEVICE-MIB and EADS-P25-RFSS-NOTIF-MIB.

For all traps (except those with footnotes):

- Match Criteria: Fourth varbind Not Equals ‘cleared’
- Rearm Criteria: Fourth varbind Equals ‘cleared’

Trap Name	Severity
EADS-P25-BCSS-MIB_eadsP25AMSStateChange	Trouble[1]
EADS-P25-BCSS-MIB_eadsP25AMSStoragePurge	Attention
EADS-P25-BCSS-MIB_eadsP25BackupConfDataFilesInd	Attention
EADS-P25-BCSS-MIB_eadsP25BckSrvInaccessible	Attention
EADS-P25-BCSS-MIB_eadsP25CorruptFreqPlan	Attention
EADS-P25-BCSS-MIB_eadsP25DuplicateSuIpAddress	Critical
EADS-P25-BCSS-MIB_eadsP25FuncStateChange	Critical[2]
EADS-P25-BCSS-MIB_eadsP25InconsistentSuIpAddress	Attention
EADS-P25-BCSS-MIB_eadsP25MaintenanceMode	Trouble
EADS-P25-BCSS-MIB_eadsP25RepStateChange	Attention
EADS-P25-BCSS-MIB_eadsP25RestoreConfDataFilesInd	Attention[3]
EADS-P25-BCSS-MIB_eadsP25RfRepNoMorePdch	Critical
EADS-P25-BCSS-MIB_eadsP25SiteControllerState Change	Trouble[4]
EADS-P25-BCSS-MIB_eadsP25SoftDownloadEnd	Critical
EADS-P25-BCSS-MIB_eadsP25SoftDownloadError	Trouble
EADS-P25-BCSS-MIB_eadsP25TckFileDelNbDaysInd	Attention
EADS-P25-BCSS-MIB_eadsP25TckFileDelPartSizeInd	Attention
EADS-P25-BCSS-MIB_eadsP25UndeclaredSuIpAddress	Attention
EADS-P25-BCSS-MIB_eadsP25TkgRgrpAlert	Attention
EADS-P25-BCSS-MIB_eadsP25ChannelPartioningError	Trouble
EADS-P25-BCSS-MIB_eadsP25ChannelPartioning Warning	Attention
EADS-P25-IPDEVICE-MIB_eadsP25MaintenanceMode	Attention
EADS-P25-IPDEVICE-MIB_eadsP25SoftDownloadEnd	Attention
EADS-P25-IPDEVICE-MIB_eadsP25SoftDownloadError	Trouble
EADS-P25-RFSS-NOTIF-MIB_eadsP25LicenseAlert	Attention[5]

Trap Name	Severity
EADS-P25-RFSS-NOTIF-MIB_eadsP25LicenseNot Allowed	Attention
EADS-P25-RFSS-NOTIF-MIB_eadsP25UnknownRfss	Attention
EADS-P25-RFSS-NOTIF-MIB_eadsP25WgidRanges Overlap	Attention

1. Match Criteria: Seventh varbind Not Equals “aMSServConnected”
   Rearm Criteria: Seventh varbind Equals “aMSServConnected”
2. Match Criteria: Seventh varbind Not Equals “normal”
   Rearm Criteria: Seventh varbind Equals “normal”
3. Match Criteria: Seventh varbind Not Equals “OK”
   Rearm Criteria: Seventh varbind Equals “OK”
4. Match Criteria: Seventh varbind Not Equals “notIsolated”
   Rearm Criteria: Seventh varbind Equals “notIsolated”
5. Match Criteria: Seventh varbind Not Equals “LicenseOK”
   Rearm Criteria: Seventh varbind Equals “LicenseOK”

Tait Base Station MIB

The Tait base station (TB9100 and TB9400) traps are from EADS-P25-REPEATER-NOTIFICATIONS-MIB.

For all traps:

- Match Criteria: Third varbind Not Equals 1 and third varbind Not Equals ‘cleared’
- Rearm Criteria: Third varbind Equals 1 or third varbind Equals ‘cleared’

Trap Name	Severity
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25AirTemperaturealarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25batteryPMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Configurationalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25ConfigurationPAalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25ConfigurationPMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25CurrentPAalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm2	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm3	Critical

Trap Name	Severity
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm4	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25fanalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25MainsPMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25OnePPSpulsealarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25powerSupplyPAalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25powerSupplyPMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25RefFrequencyalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25ShutDownPMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25Simulcastalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25SWRalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25synthesizerstatus	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25temperaturePAalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25TemperaturePMUalarm	Critical
EADS-P25-REPEATER-NOTIFICATIONS-MIB_eadsP25TransmitterPAalarm	Critical
eadsP25synthesizerstatus	Trouble
eadsP25temperaturePAalarm	Trouble
eadsP25SWRalarm	Attention
eadsP25Simulcastalarm	Trouble
eadsP25TransmitterPAalarm	Attention
eadsP25TemperaturePMUalarm	Trouble
eadsP25Systemalarm	Trouble
eadsP25Frontpanelalarm	Attention

TB9400

The TB9400 traps are from EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB.

For all traps:

- Match Criteria: Third varbind Not Equals 1 and third varbind Not Equals ‘cleared’
- Rearm Criteria: Third varbind Equals 1 or third varbind Equals ‘cleared’

Trap Name	Severity
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25AirTemperaturealarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25batteryPMUalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Configurationalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25ConfigurationPAalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25ConfigurationPMUalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25CurrentPAalarm	Critical
EADS-P25-TB9400-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm2	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm3	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Customalarm4	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25fanalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25MainsPMUalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25OnePPSpulsealarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25powerSupplyPAalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25powerSupplyPMUalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25RefFrequencyalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25ShutDownPMUalarm	Critical

Trap Name	Severity
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25Simulcastalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25SWRalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25synthesizerstatus	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25temperaturePAalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25TemperaturePMUalarm	Critical
EADS-P25-TB9400-REPEATER-NOTIFICATIONS-MIB_eadsP25TransmitterPAalarm	Critical

4.5.9 RFI Traps

The RFI traps are from RFI-AXM-ALARM-MIB:

Trap Name	Severity	Match/Ream Criteria
RFI-AXM-ALARM-MIB_axmAlarm Event	Attention	Match Criteria: Sixth varbind Not Equals 1 Rearm Criteria: Sixth varbind Equals 1

4.5.10 Eventide

The Eventide trap is from EVENTIDE-SNMP-MIB.

Trap Name	Severity
EVENTIDE-SNMP-MIB_swAlertRaiseNotification	Critical

4.5.11 Omnitronics

The Omnitronics traps are from OMNI-MIB.

Trap Name	Severity
OMNI-MIB_errorTrap	Critical
OMNI-MIB_informationTrap	Attention
OMNI-MIB_ipr400AnalogInput1Trap	Trouble
OMNI-MIB_ipr400AnalogInput2Trap	Trouble
OMNI-MIB_ipr400AnalogInput3Trap	Trouble
OMNI-MIB_ipr400AnalogInput4Trap	Trouble

Trap Name	Severity
OMNI-MIB_ipr400AnalogInput5Trap	Trouble
OMNI-MIB_ipr400AnalogInput6Trap	Trouble
OMNI-MIB_ipr400AnalogInput7Trap	Trouble
OMNI-MIB_ipr400AnalogInput8Trap	Trouble
OMNI-MIB_ipr400DigitalInput1Trap	Trouble
OMNI-MIB_ipr400DigitalInput2Trap	Trouble
OMNI-MIB_ipr400TemperatureTrap	Critical
OMNI-MIB_ipr400VoltageTrap	Critical
OMNI-MIB_omniEventConfigChange	Attention
OMNI-MIB_omniEventError	Trouble
OMNI-MIB_omniEventInformation	Attention
OMNI-MIB_omniEventPushToTalkTimeout	Attention
OMNI-MIB_omniEventVoipLinkStatus	Attention
OMNI-MIB_omniEventVoipRxSeqErrPackets	Trouble
OMNI-MIB_omniEventVoipRxTooLatePackets	Trouble
OMNI-MIB_omniEventWarning	Attention
OMNI-MIB_warningTrap	Trouble

4.5.12 Valiant E1 or T1 Failover Switch

The Valiant E1 or T1 Failover Switch is connected to the TN9500 via E1 or T1 and SNMP. Because the Valiant E1 or T1 Failover Switch supports SNMP polling by one SNMP entity only, we do **not** recommend using Tait EnableMonitor to poll the TN9500. But the Valiant failover switch can be configured to send its traps to Tait EnableMonitor.

If the SNMP of the Valiant failover switch becomes unresponsive, restart the OAM card. The card works independently of the main system, so you can reset the card only by pressing the **Reset OAM** switch in front of the card. You don’t need to restart or unplug the power for the whole Valiant unit. Resetting the OAM card has no effect on the primary function of the main system, which is to provide failover switching.

The Valiant failover switch traps are defined in E1-QUAD-FAILOVER-S.MIB or T1-QUAD-FAILOVER-S.MIB. The example trap names below are from the E1 MIB file.

Trap Name	Severity
E1-QUAD-FAILOVER-S_switchAlarm	Attention
E1-QUAD-FAILOVER-S_switchStatusChange	Attention

4.6 Processing Unsolicited Traps

1. Select Alarms > Unsolicited Traps.
2. Click on Create Trap Processor corresponding to the trap message.
3. Type a name for TrapName.
4. Make sure that the status is enabled.
5. Select the Severity.
6. Click Add.

5 Dials

To change the dial for a device:

1. Stop the Tait EnableMonitor service.
2. Take a copy of `C:\Manage Engine\OpManager\conf\opmanager_snapshot_dial.xml`, then open it in a text editor.
3. Find the correct category (e.g. BaseStation).
4. Under each dial add a new line:
   `<PARAM pollKey="[performance monitor]" type="[type]"/>`
   where:
   - `[performance monitor]` is a performance monitor currently being monitored on the device (e.g. TB9400paTemperature Driver)
   - `[type]` is the type of device (e.g. Tait TB9400)

   for example:

   ```
   <PARAM pollKey="TB9400paTemperatureDriver"
   type="Tait TB9400"/>
   ```

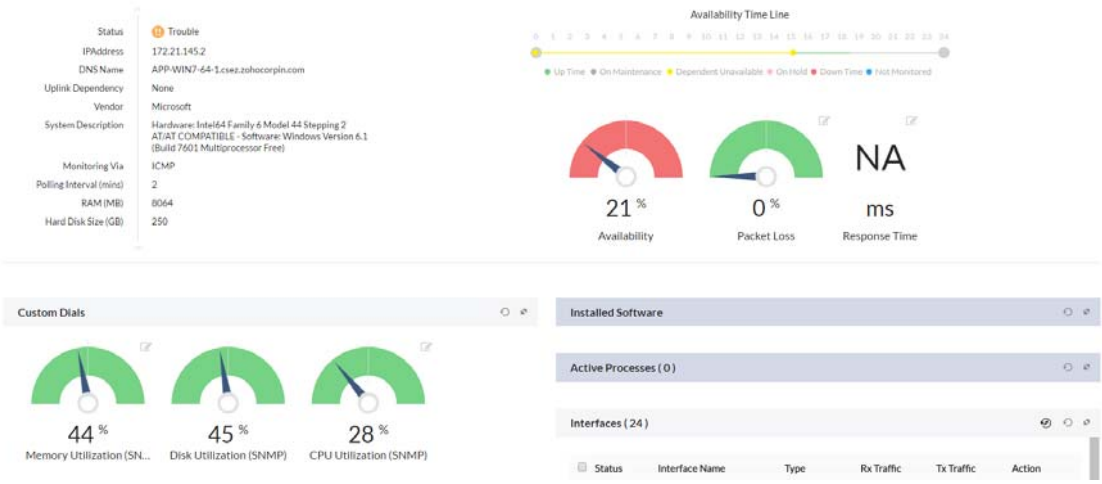
The quotation marks are required.

5. If the type of monitor is being changed, change the dial title as well:

   ```
   <DIAL dialType="[meter/number/pie]" display-
   Name="[New title]" name="[New title]" short-
   Key="[New title]" unit="[New units]">
   ```

6. Start the Tait EnableMonitor service.

A sample display of dials is as follows:



The following dials are available in Tait EnableMonitor:

Base Station

Base Station	Duty Cycle %	PA Temperature (^{o}C)	Trunking Mode
Default	TB9100paDuty CycleDuty5	TB9100pa TemperatureDriver	TB9100nwChanGrp TrunkingState
Tait - Airbus Base Station	eadsP25DutyCycle PADuty5	eadsP25Pa TemperatureDriver Temperature	eadsP25current Channelgrp TrunkingState
Tait TB8200	N/A	N/A	N/A
Tait TB9100	TB9100paDuty CycleDuty5	TB9100pa TemperatureDriver	TB9100nwChanGrp TrunkingState
Tait TB9300	N/A	N/A	N/A
Tait TB9400	N/A	TB9400pa TemperatureDriver	TB9400nwChanGrp TrunkingState

Controller

Controller	CPU Utilization (%)	Memory Utilization (%)	Disk Utilization (%)
Default	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait - Airbus	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait TN8271	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait TN9300	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait TN9400 PSTN RFSS	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait TN9400 PSTN Site Controller	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Tait TN9400 PSTN Gateway	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization

Gateway

Gateway	Input Level (dBm)	Output Level (dBm)	Lost Voice Packets
TN8271	InputLevel	OutputLevel	VDP packet lost

Linking

Linking	RSSI (dBm)	Tx Power (dBm)	Tx Temperature (^{o}C)
4RF Aprisa	aprisaXETerminal RSSI	aprisaXE TransmitterPower	aprisaXE Transmitter Temperature
Aviat Eclipse	Eclipse RSSI	Current Eclipse Forward Power	Eclipse Pwr Det Temperature
MiMoMax OPV2	RSSI Average	NA	Tx Temperature Average

Router

Router	CPU Utilization (%)	Memory Utilization (%)	Temperature (^{o}C)
Default	CPUUtilization	MemoryUtilization	CiscoTemperature
Cisco 2900 IS Series	RouterCPU Utilization	RouterMemory Utilization	CiscoTemperature
Cisco Device	RouterCPU Utilization	RouterMemory Utilization	NA

Server

Server	CPU Utilization (%)	Memory Utilization (%)	Disk Utilization (%)
Default	Win-CPUUtilization	Win-MemoryUtilization	DiskUtilization
Dell iDrac	NA	NA	NA
Solaris	Lin-CPUUtilization	Win-MemoryUtilization	Telnet-DiskUtilization

Switch

Switch	CPU Utilization (%)	Memory Utilization (%)	Backplane Utilization (%)
Default	CPUUtilization	MemoryUtilization	BackplaneUtilization
Cisco Catalyst 3750 Series	SwitchCPU Utilization	CiscoMemory Utilization	Backplane Utilization
DLink DES 3526 series	NA	NA	NA
DLink DES-1210-28	NA	NA	NA
DLink DES-3028	NA	NA	NA

Time Server

Time Server	Number Of Satellites	Temperature	NTP Status
Spectracom	Spectracom Number Of Satellites	NA	NTP Status Current
Tait T801	NA	NA	NA

6 Basic Administration

Although this guide is not an intended to provide instructions on how to operate Tait EnableMonitor, the following sections contain basic administrative information.

6.1 Status Icon Descriptions

Tait EnableMonitor uses the following color-coded status icons for you to easily monitor the health of your network:

Icon	Description
	Clear - there are no alarms for this device
	Attention - this means that there is some action that could be taken to prevent a problem
	Trouble - this means that this device is not functioning as it should and could be causing a problem on the network
	Critical - this means that this device has failed and needs immediate intervention
	Device down - this means that the device is out of action. It could be because the device has failed, or that it is offline for maintenance purposes.
	Unmanaged - this alarm has not been assigned to any particular technician

6.2 Accessing a Device's Application

If Tait EnableMonitor is reporting problems on a specific device, you may wish to access its application to check its configuration, or to monitor it directly:

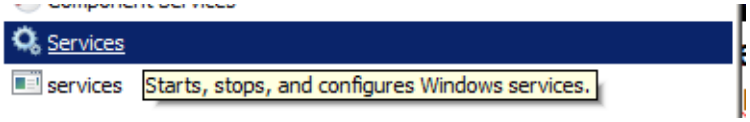
1. Select the device in question.
2. In the Device Details area, click on the Browse () icon, then select https to automatically open the product application's website in a new tab.

6.3 Backing Up and Restoring the Tait EnableMonitor Database

6.3.1 Stand-alone Configurations (Essential License)

1. Stop OpManager service:
   a. Click on the Start Window button:

   b. Enter **`Services`** in 'Search program and files' on the Enable Monitor Windows server:



   c. Launch Windows Services.
   d. Search for Manage Engine OpManager, select it, then click Stop.

2. Complete the backup (a) or restore (b) operation as required:
   a. Use the batch files `BackupDB.bat` for Windows (or `BackupDB.sh` for linux) to backup the database using the following command:

      `<OpManager Home>`[1]`\bin\backup\<batch file> -mode all`

      The advantage of using these batch files is that you can backup the database very quickly.

      `BackupDB.bat/sh` takes a backup of the entire database. If you want to take a backup of the configuration data alone, which would be very helpful when re-establishing the existing Tait EnableMonitor setup in another machine, but leaving out the performance data, use the following command:
      `<OpManager Home>\bin\backup\<batch file> -mode configdata`

   b. To restore the backed up data, go to `<OpManager Home>\bin\backup` directory and execute `RestoreDB.bat` (Windows) or `RestoreDB.sh` (Linux) with the backup file name as argument.
      Example: `RestoreDB.bat "C:\Backup_NOV19_2012_03_00_00_9200.zip"`

1. *OpManager Home* is `C:\Program Files\Manage Engine\OpManager` if the default path has not been changed.

3. Disable and then Enable SSL see “Disabling and Enabling SSL (HTTPS)” on page 76.

4. Start Enable Monitor service.

6.3.2 Distributed Configurations (Enterprise License)

1. Stop the Manage Engine OpManager Probe service on the Probe servers. (See above for detailed instructions.)

2. Complete the backup/restore operation on each probe (See above for detailed instructions.)

3. Disable SSL as explained in “Disabling and Enabling SSL (HTTPS)” on page 76.

4. Copy over the `\\OpManager Central home\conf\itom.truststore` to the `\\OpManager Probe home\conf` folder.

5. Enable SSL as explained in “Disabling and Enabling SSL (HTTPS)” on page 76.

6. Start the Manage Engine OpManager Probe service.

6.4 Clearing Control Relay Notifications Manually

An alarm on a device (Device A) has closed a relay on the control relay. Once the alarm is cleared, if the relay is still active, then the following steps should be taken:

1. Login to Tait EnableMonitor.

2. Manually run the Tait.RelayController.exe through the command prompt with the appropriate arguments.
(e.g. for port 2: Tait.RelayController.exe -w RK2)

6.5 Disabling and Enabling SSL (HTTPS)

6.5.1 Enabling SSL

1. Go to Settings > General Settings > Security Settings.

2. Click on the Secure Mode slider and then select the desired Certificate Type.

3. Confirm the selection with Generate, Create or Fetch, depending on the chosen Certificate Type.

4. Restart the Manage Engine OpManager service.

6.5.2 Disabling SSL

1. Go to Settings > General Settings > Security Settings.
2. Click on the Secure Mode slider and confirm the change.
3. Restart the Manage Engine OpManager service.

6.6 Accessing Tait EnableMonitor using the API

Tait EnableMonitor can be accessed using the API. Credentials are required to initially obtain the Tait EnableMonitor API key, but once obtained, API requests can be made without any further credential checks.

For details on using the API to access Tait EnableMonitor, refer the OpManager documentation (https://www.manageengine.com/network-monitoring/help/rest-api-opmanager.html).

6.7 Automatically Refreshing the Tait EnableMonitor View

1. Go to the Tait EnableMonitor Web-Client and click the cog icon in the top right corner of the screen.

2. Select Automatic Refresh from the drop-down menu.
3. Click Automatic Refresh.
4. Set the refresh timer.
5. Click Apply.

6.8 Removing Old Data From the Databases

1. Go to Settings > General Settings > Database Maintenance.
2. Configure the number of recent alarms to be maintained in the database. The Events Table (EVENT_<DATE>) cleanup will be based on the value configured in Detailed statistics (see below).
3.

a. Detailed Statistics - Configure the number of days data to be retained in the raw table (STATSDATA_<DATE>). This table contains the values at each poll. Default is 7 days. Note that maintaining the detailed statistics for over 15 days will impact performance.

b. Hourly Statistics - Data is archived every one hour and is stored in the STATSDATA_HOURLY table. Configure the number of days data to be retained. Default is 30 days.

c. Daily Statistics - Data is archived every day from the above table and is stored in STATSDATA_DAILY table. By default, the data for 365 days is stored here. Configure the required period.

4. Click Save for the Database Maintenance configuration to take effect.

6.9 Configuring Alarm Suppression

As part of the normal operation of a communications system, there may be planned outages. It is common practice to suppress alarms from affected devices for the period of the planned outage.

6.9.1 Turning Alarm Suppression On

1. To configure alarm suppression for multiple devices, go to Settings > Configuration > Quick Configuration Wizard.
2. Select the Alarm Suppression option.
3. Select the time period for which you want to suppress the alarms.
4. Select the Category of the devices for which you want to associate or manually select the devices.
5. Click Save.

ⓘ The option to select business views is also useful, if you have a business view for each site location.

6.9.2 Turning Alarm Suppression Off

1. Follow the steps above, to re-create the suppression rule, but select ‘Never’ as the period, with the same group of devices.
2. Click Save.

6.10 Improving Performance Monitoring

Depending on the network, devices and Tait EnableMonitor configurations, it may be possible that some performance parameter polls are missed. To avoid this issue, we recommend the following:

1. If a device has a lot of performance monitors that are polled at the same time, ensure that the SNMP timeout is correctly configured to give enough time for the device to answer, depending on the network configuration, its latency, its bandwidth and use. Select the credential from EnableMonitor Settings > Discovery > Credentials and increase the SNMP timeout to 10 or 20 seconds with at least 1 retry.

2. In each device template, make sure that there are no more than 10 parameters with the same polling value. This will avoid long SNMP GET BULK messages.

3. Note that setting multiple monitors to very low update times (i.e. less than 10 minutes) may cause performance problems.

4. If you still have missing performance monitors during polling, please contact Technical Support, who with ManageEngine support, can advise you on increasing the number of threads required for the polling. For example, in `C:\Manage Engine\OpManager\conf\threads.conf`, set datapoll to 20.

6.11 Interpreting Utilization Data

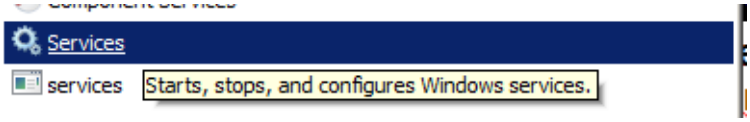
On a server running Linux, it is normal for the memory utilization dial (see "Dials" on page 70) of the controller, to display a high reading. This is because Linux utilizes RAM to speed up disk operations by using available memory for buffers and cache. If memory is required by programs or applications, Linux will free up this memory as needed.

Server RAM and CPU should be monitored, with an alert if the utilization nears 95-100%.

6.12 Uninstalling Tait EnableMonitor

1. Stop Tait EnableMonitor
   a. Click on the Start Window button:

   b. Enter **`Services`** in 'Search program and files' on the EnableMonitor Windows server:



   c. Launch the Windows services.
   d. Search for ManageEngine OpManager, select it then click Stop.
2. Open Windows Task Manager (Ctrl+Alt+Delete then click on Start Task Manager). In the processes list, check that java.exe and mysql.exe are stopped. If they are not, reboot the server.
3. Click on the Windows Start and Enter **`cmd`** in the Search programs and files field.
4. Enter **`netstat`** in the new window. Check that in the local address, there is no reference to an IPaddress:443. If there is, reboot the server.
5. Select Start > Programs > ManageEngine OpManager > Uninstall OpManager.
6. Check that the OpManager folder in `ManageEngine\OpManager` has been deleted, otherwise delete it.
7. Delete the `C:/Tait` directory and all the files it contains.

Appendix 1: Windows Interactive Services Detection

This appendix has been included as a work-around for a Windows problem that may be an irritant for some users.

The Interactive Services Detection feature of the Windows Server 2008 R2 is enabled if the following message keeps displaying: `A program running on this computer is trying to display a message.`

The Interactive Services Detection feature is for legacy applications (i.e. Internet Explorer) that detects if one of them is trying to interact with the Windows desktop. This feature can be disabled as follows:

1. Select Start > Control Panel and then double-click Administrative Tools.
2. Double-click Services.
3. Scroll down and double-click Interactive Services Detection.
4. On the General tab, change the Startup type to Manual or Disabled.
5. Click OK and restart the server.