

Infinera

Transcend Network Management System
Client 18.10.3

Administrative Guidance for Common Criteria

Version 1.2
December 6th 2022

Table of Contents

1	INTRODUCTION	3
2	SYSTEM REQUIREMENTS	4
2.1	SUPPORTED OPERATING SYSTEMS	4
2.2	OTHER HARDWARE AND SOFTWARE RESOURCES	4
3	TNMS CLIENT USER GUIDANCE	5
3.1	SOFTWARE PRE-REQUISITES	5
3.2	TNMS CLIENT INSTALLATION	5
3.3	POST-INSTALLATION STEPS	6
3.4	ENABLING FIPS MODE	7
3.5	MANAGING ROOT CERTIFICATES	8
3.5.1	Installing a new root certificate	8
3.5.2	Listing root certificates	8
3.5.3	Deleting an existing root certificate	9
3.5.4	TLS Configuration	10
3.6	CHECKING THE INSTALLED VERSION	10
3.7	UNINSTALLING TNMS CLIENT	10
3.8	UPDATING TNMS CLIENT	11
3.9	TNMS LOGIN	11
3.10	TNMS LOGOUT	12

Version History

Version	Date	Description
1.0	November 9 th 2022	Initial release for NIAP Checkout of TNMS Client V18.10.3.
1.1	December 1 st 2022	Clarifications added for uninstall process and the necessity for network connection
1.2	December 6 th 2022	Moved misplaced information on uninstall process to correct section.

1 Introduction

The Transcend Network Management System (TNMS) is designed to provide end-to-end network and service management across multiple technologies and equipment vendors. The TNMS system has been developed with the following features:

- Network and service management with a broad feature set, from deep node-level troubleshooting to end-to-end service configuration and monitoring, across multiple technologies and equipment vendors for improved operational efficiency.
- An advanced graphical user interface providing overviews of the most relevant data and guidance through configuration steps.
- Flexible deployment configuration options that fit various needs of different network operators: from small networks to very large infrastructures, including support for virtualization and high availability.
- Clear user interfaces that provide user-friendly navigation and supporting responsive and efficient use.

The full TNMS system consists of a TNMS server and a TNMS client. This guidance document covers the TNMS Client only. The TNMS Server is not included as it is being evaluated separately. This document is provided as a supplement to the TNMS Customer Documentation provided with every TNMS installation and describes how to install and configure the TNMS Client Component as the evaluated configuration compliant with the Common Criteria for Information Technology Security Evaluation version 3.1.

2 System Requirements

2.1 Supported Operating Systems

TNMS Client has been evaluated in in a Microsoft Windows 10 (64 bit) environment. The TNMS client is primarily a Java application and features some native level libraries. For all components, the TNMS client is compiled with all necessary compilation flags to ensure that all required environmental protections are enabled by default and require no further configuration under Windows.

2.2 Other Hardware and Software resources

TNMS Client does not require access to any sensitive information repositories or special hardware resources other than network connectivity used to communicate with the TNMS Server or check for updates.

3 TNMS Client User Guidance

This section describes how to install and configure TNMS Client as the evaluated configuration compliant with the Common Criteria Evaluation.

3.1 Software Pre-Requisites

TNMS Client is a Java application and requires two specific versions of Java Runtime Environment to be installed in the Windows Host:

- Amazon Corretto JDK 11.0.6.10.1 for Windows x64
- Oracle Java JRE 8u201 for Windows x86

The installation packages may be obtained from Amazon AWS and Oracle Java webpages, respectively. Download and install both JDKs following the vendor's instructions before installing TNMS Client.

3.2 TNMS Client Installation

To install TNMS Client on a Windows 10 Host, follow the following steps:

1. Log in the operating system with a user that has administrative rights.
2. Right-click the installation file and select "Run as administrator"
The installation wizard opens in the Introduction window and the complete list of installation steps are displayed on the left pane.
3. Read the **License Agreement** and select *I accept the terms of the License Agreement*.
4. In **Installation Package** click "TNMS Client"
5. In **Components** Step 2:
 - a. Select **7191 Craft Station FP16.9.X** (optional, but recommended)
 - b. Unselect all other Craft Station options
6. In **Components** Step 3:
 - a. Unselect **Install L3 Applications**
7. In **Choose Install Folder** enter the path of the following folders, or accept the default paths:
 - a. TNMS Installation Folder
(Throughout the customer documentation this folder will be referred to as <Product_Installation_Folder>. Take note of the location of this folder for future reference.)
 - b. TNMS Data folder
Make sure that the TNMS data folder is empty. If not, backup and remove the data or select a different folder.
(Throughout the customer documentation this folder will be referred to as <Product_Data_Folder>. Take not of the location of this folder for future reference.)

c. LCT Installation folder

8. In **Folder Configuration: Client Login History** you may optionally change the default location of the *Client Login History* file to a custom location.
9. In **Folder Configuration** configure the options of the icons and shortcuts to be created during the installation.
10. A summary of the installation settings is provided in the **Pre-Installation Summary** step. If the settings are correct, click **Install** to start the installation.
11. The results of the installation are presented in **Installation Results**. Click **Done** to finish the installation.

Note: After installing TNMS Client, there may be some files left in the temporary file system. These files are no longer needed and should be removed manually:

- Delete the C:\Users\\AppData\Local\Temp\TempPUs folder and all its contents. <username> is the user that ran the installation process.

3.3 Post-Installation Steps

After running the installer, the following steps are required to setup TNMS Client and complete the installation process.

Configure links to Java JREs:

1. Open a Windows Command Prompt as Administrator
2. Go to <Product_Installation_Folder>\base\
e.g. `cd "c:\Program Files (x86)\Coriant\TNMS 18.10.3\base"`
3. Create a new directory named java
`mkdir java`
4. Inside the new directory, run the following commands:
`mklink /J jre64 <JAVA 11 LOCATION>`
`mklink /J jre8x86 <JAVA 8 LOCATION>`
`mklink /J jre86 <JAVA 8 LOCATION>`

Where,

- <JAVA 11 LOCATION> is the full path to the installation folder of Amazon Corretto 11
e.g. "C:\Program Files\Amazon Corretto\jdk11.0.6_10"
- <JAVA 8 LOCATION> is the full path to the installation folder of Oracle Java 8
e.g. "C:\Program Files (x86)\Java\jre1.8.0_201"

Move TNMS Client truststore to an approved location:

1. In Windows Explorer go to <Product_Installation_Folder>\client\
2. Move the file `client_truststore.jks` to a new directory
C:\ProgramData\Coriant
3. Open the file `jvm.options` with a text editor
4. Update the `-Djavax.net.ssl.trustStore` parameter with the new location of the truststore: "C:\\ProgramData\\Coriant\\client_truststore.jks"

Note that backslashes (\) in the path must be escaped (\\)

5. Save and close the file.

3.4 Enabling FIPS mode

TNMS Client cryptographic functions are provided by the "Bouncy Castle FIPS Java Provider v1.0.2.1" cryptographic engine embedded in the TNMS Client installation. After installing TNMS client, FIPS mode must be enabled. This will ensure that the TNMS Client cryptographic engine is running in FIPS approved mode of operation and in compliance with the Common Criteria Evaluation. The use of any other cryptographic engines, or configurations other than what is described in this section was not evaluated nor tested during the Common Criteria Evaluation of TNMS Client.

To enable FIPS mode:

1. Open a PowerShell Command Line with a user that has administrative rights.
2. Go to <Product_Installation_Folder>\client\bin
e.g. `cd 'C:\Program Files (x86)\Coriant\TNMS 18.10.3\client\bin\'`
3. Set the local execution policy to allow running scripts:
`Set-ExecutionPolicy RemoteSigned`
4. In the command line, run the script:
`config_fips.ps1 enable`

Note: The command `config_fips.ps1 disable` will disable FIPS mode in TNMS Client and put it back in the general mode of operation. General mode of operation is not compliant with the Common Criteria Evaluation.

3.5 Managing Root Certificates

TNMS Client does not rely on Java Runtime environment default trust store. Instead, it uses its own trust store. After installing or modifying the certificate chain in the TNMS Server, the root certificate must be installed in the TNMS Client trust store, so that TNMS can properly validate the trust chain.

Management of the root certificates and the TNMS trust store is done with the standard JRE `keytool` command. More than one certificate may be installed in TNMS Client's trust store. All installed certificates will be trusted.

3.5.1 Installing a new root certificate

Use the following command to install or replace a root certificate in TNMS Client:

```
keytool -import -trustcacerts -file <root certificate>
        -keystore <truststore path> -storepass <storepass>
        -alias <alias>
        -storetype BCFKS
        -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
        -providerpath <provider path>
```

replacing the following parameters with their corresponding values:

- **root certificate**
The path to the root certificate to install, in PEM format.
- **truststore path**
Path to TNMS Client trust store: `C:\ProgramData\Coriant\client_truststore.jks`
- **storepass**
The trust store password. Refer to TNMS Administration Guide for the default password.
- **alias**
A unique string identifying this root certificate. If the alias already exists in the trust store, it will replace the existing certificate with the new one being installed. Otherwise, a new entry will be created in the trust store.
- **provider path**
Path to Bouncy Castle FIPS provider:
`<Product_Installation_Folder>\client\lib\clib\bouncycastle\bc-fips-1.0.2.1.jar`

3.5.2 Listing root certificates

Use the following command to list all installed root certificates in TNMS Client:


```
keytool -list
  -keystore <truststore path> -storepass <storepass>
  -storetype BCFKS
  -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
  -providerpath <provider path>
```

replacing the following parameters with their corresponding values:

- **truststore path**
Path to TNMS Client trust store: C:\ProgramData\Coriant\client_truststore.jks
- **storepass**
The trust store password. Refer to TNMS Administration Guide for the default password.
- **provider path**
Path to Bouncy Castle FIPS provider:
<Product_Installation_Folder>\client\lib\clib\bouncycastle\bc-fips-1.0.2.1.jar

The output will show a list of all installed certificates, identified by their unique aliases and the corresponding SHA-256 fingerprint.

3.5.3 Deleting an existing root certificate

Use the following command to delete an existing certificate from TNMS Client:

```
keytool -delete
  -alias <alias>
  -keystore <truststore path> -storepass <storepass>
  -storetype BCFKS
  -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
  -providerpath <provider path>
```

replacing the following parameters with their corresponding values:

- **alias**
The alias string that identifies the certificate to be deleted.
- **truststore path**
Path to TNMS Client trust store: C:\ProgramData\Coriant\client_truststore.jks
- **storepass**
The trust store password. Refer to TNMS Administration Guide for the default password.
- **provider path**
Path to Bouncy Castle FIPS provider:
<Product_Installation_Folder>\client\lib\clib\bouncycastle\bc-fips-1.0.2.1.jar

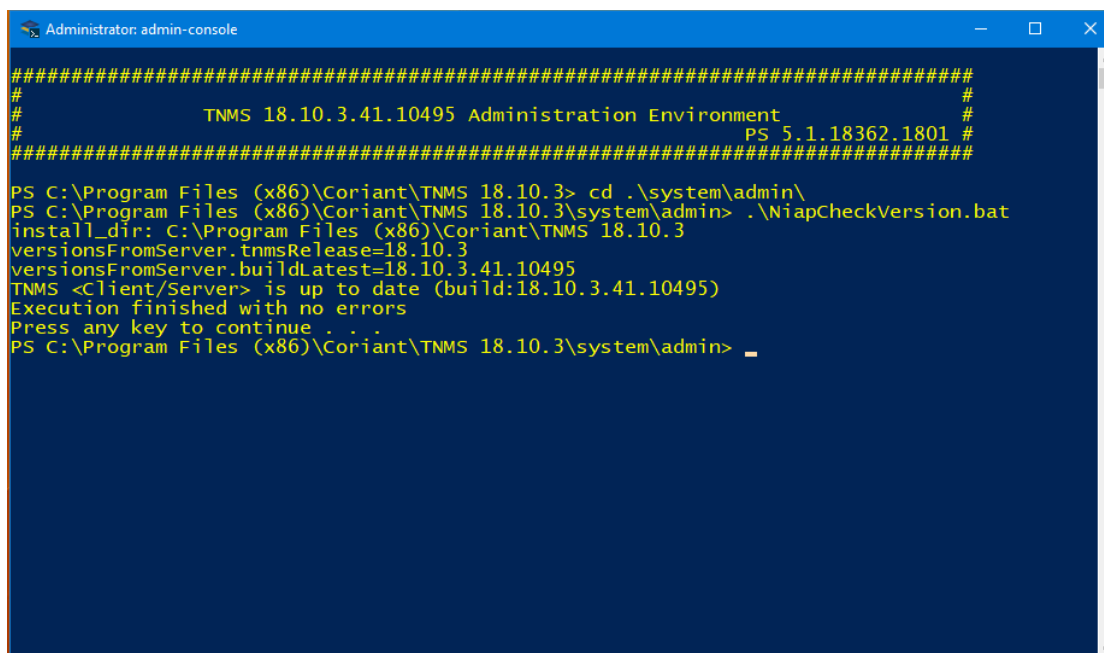
3.5.4 TLS Configuration

Other than setting the trusted root certificates, TLS settings in TNMS Client – such as supported cipher suites and key sizes - are fixed and not configurable by the user.

3.6 Checking the Installed Version

To check the TNMS Client installed version and verify if it is up to date:

1. In Windows Explorer go to <Product_Installation_Folder>\system\admin
2. Open the admin-console powershell shortcut
3. Run the NiapCheckVersion.bat tool



```
Administrator: admin-console
#####
#
#           TNMS 18.10.3.41.10495 Administration Environment           #
#                                           PS 5.1.18362.1801 #
#####
PS C:\Program Files (x86)\Coriant\TNMS 18.10.3> cd .\system\admin\
PS C:\Program Files (x86)\Coriant\TNMS 18.10.3\system\admin> .\NiapCheckVersion.bat
install_dir: C:\Program Files (x86)\Coriant\TNMS 18.10.3
versionsFromServer.tnmsRelease=18.10.3
versionsFromServer.buildLatest=18.10.3.41.10495
TNMS <Client/Server> is up to date (build:18.10.3.41.10495)
Execution finished with no errors
Press any key to continue . . .
PS C:\Program Files (x86)\Coriant\TNMS 18.10.3\system\admin> _
```

From the script output you can see the TNMS release, build number, and if you're running the latest build available.

3.7 Uninstalling TNMS Client

Uninstalling the TNMS Client is done from the **Windows Control Panel > Programs and Features**. Select the TNMS Client from the list and click uninstall. The Uninstall Wizard will open and uninstall TNMS.

The TNMS Client Uninstaller will keep some files in the system. To finish the installation process, the TNMS client truststore must be manually deleted:

Locate the TNMS client truststore at `C:\ProgramData\Coriant\client_truststore.jks` and manually delete the file.

Note: The contents in the <Product_Data_Folder> are also kept in the system. This folder contains log files. Their deletion is optional, however should be done in order to completely remove the TNMS Client from the system.

After the uninstallation wizard completes, the user will need to manually remove the uninstall script located at C:\Windows\SysWOW64\tnms_cleaner

3.8 Updating TNMS Client

If a new build is available, TNMS Client must be updated using a manual re-install process.

1. Uninstall TNMS client as described in section “3.8 – Uninstalling Updating TNMS Client”
2. Download the new build from Infinera’s Customer Service Portal (<https://support.infinera.com/>)
Note: This requires a customer account with Infinera with the support for the Transcend Network Management System product.
3. Verify the digital signature. This can be verified using the Windows platform.
 - a. Right Click on the installation file and select “Properties”
 - b. On the Properties Windows, select the “Digital Signatures” tab.
 - c. On the signature list you can check the “Name of Signer” attribute: www.infinera.com.
4. Install the new build of TNMS Client as described in section “3.2 - TNMS Client Installation”
5. Enable FIPS mode as described in section “3.4 - Enabling FIPS mode”

The TNMS client update is done through a clean reinstallation process. To verify if the TNMS Client update was successful, run the client and connect and login to a TNMS server as described in the next sections.

3.9 TNMS Login

Make sure TNMS Server is up and running and log in to your TNMS Client.

Press the spacebar or click login and fill in the following fields:

- Server name
Enter the server address either in <server IP address> or <FQDN> format.
- User name
Enter a valid user name.
- Password
Enter the password for the user name.

If the TNMS Server is unavailable the following error message is displayed:
“Login Failure. TNMS Server is not responsive.”

In this situation check for one of the following scenarios:

- The server is not reachable.
- Network connectivity.
- The server may not be running.
- You are trying to connect to a standby server instead of the active server.

3.10 TNMS Logout

To logout from TNMS Server you may:

- Select **File > Logout** or press the logout button from the toolbar.
- Close the TNMS client. TNMS will gracefully terminate the session.

TNMS Server will also automatically terminate sessions based on an inactivity timeout. This timeout value is globally configurable in the System Settings and/or can be set for each individual user.