Infinera

Transcend Network Management System Server 18.10.3

Administrative Guidance for Common Criteria

Version 1.1
December 6th 2022

Table of Contents

Version History

Version	Date	Description
1.0	November 9th 2022	**Initial release for NIAP Checkout of TNMS Server V18.10.3.**
1.1	December 6th	**Added necessity for network connection**

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 Server only. The TNMS Client 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 Server 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 Server has been evaluated in a Red Hat Enterprise Linux 7.9 / CentOS 7.9 environment. The TNMS Server is primarily a Java application and features some native level libraries. For all components, the TNMS server is compiled with all necessary compilation flags to ensure that all required environmental protections are enabled by default and require no further configuration under Linux.

2.2 Other Hardware and Software resources

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

.

3 Prerequisites

3.1 Host Operating System

Red Hat Enterprise Linux 7.9 or CentOS 7.9 is to be installed on the recommended hardware

TNMS requires a Red Hat Enterprise Linux 7.9 or a CentOS 7.9 installation with **Server with GUI** as **Base Environment** and **KDE** as **Add-On for Selected Environment**.

The following additional packages should also be installed:

- `attr`
- `bc`
- `gcc`
- `gcc-c++`
- `ksh`
- `libaio-devel`
- `libzip`
- `ntp`
- `psmisc`

To ensure the protection of data at rest, LUKS - the platform encryption service – must be enabled during the installation of the host operating system.

3.1.1 Host Operating System Configuration

3.1.1.1 System Hosts

TNMS requires the proper configuration of the hosts file (/etc/hosts) in every Server machine. Each host file must also include a localhost entry. The configuration of *hosts* files also ensures the functionality of Hot Standby. The examples below outline two different scenarios **with** and **without** Hot Standby.

Note: The FQDN (Fully Qualified Domain Name) is displayed via `hostname --fqdn`

For networks **without** Hot Standby the hosts file must be configured as follows:

- `IP Address FQDN hostname loghost`

For networks **with** Hot Standby the hosts files must be configured as follows:

- On the Primary site Server hosts file:
  TNMS Primary Server: `IP Address FQDN hostname loghost`
  TNMS Secondary Server: `IP Address FQDN`

- On the Secondary site Server hosts file:
  TNMS Secondary Server: `IP Address FQDN hostname loghost`
  TNMS Primary Server: `IP Address FQDN`

3.1.1.2 Virtual Memory

The system configuration file (/etc/sysctl.conf) must be updated with the following settings:

```
vm.min_free_kbytes = 1048576

vm.swappiness = 1

vm.dirty_ratio = 15

vm.dirty_background_ratio = 3
```

The second parameter configures the system to only use swapping as a last resource, that is, the system will use paging when needed. The remaining parameters are OS-advised parameters.

3.1.1.3 NTP

Configure the Server as follows:

1. Edit configuration file /etc/ntp.conf.
   ```
   vi /etc/ntp.conf
   ```

2. Add the NTP server address and other NTP configurations to the ntp.conf file:
   ```
   'server aaa.bbb.ccc.ddd'
   ```

   Where "aaa.bbb.ccc.ddd" is the external NTP Server's IP.
   It is recommended to set two external NTP Servers, a Primary and a Backup.

3. Create the drift file:
   ```
   touch /var/lib/ntp/drift
   ```

4. Enable the NTP service
   ```
   systemctl enable ntpd
   ```

5. Check the NTP service status and start it if necessary:
   ```
   systemctl is-active ntpd
   systemctl start ntpd
   ```

3.1.1.4 Proxy Settings

If the environment variable http_proxy is configured in the operating system, make sure it is defined for all users using this syntax:

```
http_proxy=http://proxy.domain:3128
```

where `proxy.domain` is the name of the proxy server with the network domain.

3.1.1.5 ASLR

Ensure that ASLR has not been disabled by checking that the `randomize_va_space` option is set to 2 by using cat:

```
cat /proc/sys/kernel/randomize_va_space
```

If either 0 or 1 is returned instead of 2 set it to 2 by running:

```
echo 2 | tee /proc/sys/kernel/randomize_va_space
```

and then reboot the system.

3.2 Oracle Database

TNMS requires Oracle Database Server 18c Enterprise Edition with the partitioning option. The TNMS software prerequisites package includes an installation script to assist in the Oracle Database installation process. For compliance with the evaluated version of TNMS Server, the following additional requirements must be met during Oracle database installation:

- The Oracle database must be installed in the same host running TNMS Server.
- The database data installation directory (ORADATA) must reside under the /var/lib/oradata directory.

3.3 Software Pre-Requisites

TNMS Server is a Java application and requires a specific version of Java Runtime Environment to be installed in the Red Hat Enterprise Linux or CentOS Host:

- Amazon Corretto JDK 11.0.6.10.1 for Linux x64

The installation package may be obtained from Amazon AWS webpage. Download and install the JDK following the vendor’s instructions before installing TNMS Server.

4 TNMS Server User Guidance

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

4.1 TNMS Server Installation

Due to rpm file size limits, TNMS server is delivered as three separate rpm files. To install TNMS Server on a Red Hat Enterprise Linux or CentOS 7.9 Host, follow the following steps:

1. Log in the host as root.

2. Add the TNMS GPG public key included in the distribution to the rpm keyring. This is required for rpm to authenticate the TNMS installation files.

   ```
   rpm --import tnms-installer-zip-key.pub
   ```

3. Install TNMS Server on the host using rpm.

   ```
   rpm -ivh tnms-installer-z02-18.10.3-1904.el7.x86_64.rpm
   rpm -ivh tnms-installer-z01-18.10.3-1904.el7.x86_64.rpm
   rpm -ivh tnms-installer-zip-18.10.3-1904.el7.x86_64.rpm
   ```

   NOTE: TNMS Installation requires a minimum of 30 Gb of free disk space in the /var folder.

   The installation wizard will open in **Introduction** and the complete list of installation steps is displayed on the left pane.

4. Read the **License Agreement** and select *I accept the terms of the License Agreement*.

5. In **Installation Package** click **"TNMS Server and Mediation"**

6. In **Server Preparation: Transport Controller** leave the **"Enable connection to Transport Controller (TC)"** option disabled.

7. In **Server Preparation: Hardware Configuration** select your hardware configuration: **Small, Medium** or **Large** (see **Error! Reference source not found.**)

8. In **Server Preparation**, select items to customize:

   - Select the "Database Connection" and "Deployment Directories" option. These are mandatory steps.
   - The remaining option: "Users and Groups" is optional.

   a. If *Users and groups* is checked,
   In **Users and Groups** enter:

      - **TNMS User** Name (default is tnms)
        Checking **Create** enables *User ID*

      - **TNMS Group** (default is tnms).
        Checking **Create** enables *Group ID*

      - **SFTP User Name** (default is tnms_sftp).
        Checking **Create** enables *User ID*

      - Database User Name (database owner name. Default is oracle).

      - DBA Group Name (default is dba).

The User ID and Group ID values must be numeric.

Click Next.

b. If *Deployment Directories* is checked,
In **Deployment Directories** enter the path of the following folders (default paths are provided):

- **TNMS Installation Directory**
  If you choose a directory other than the default, the path cannot contain spaces. Throughout this document this folder will be referred to as <Installation_Folder>. Take note of the location of this folder for future reference.

- **TNMS Data Directory**
  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 <Data_Folder>. Take not of the location of this folder for future reference.

• **Database Installation Directory**
Enter the path where Oracle database software is installed.

• **Database Data Directory**
Enter the path where the database is located (ORADATA as defined in section 3.2 - Oracle Database). Backups will also be stored under subfolders of this folder.

9. In **Connection Configuration** (If you only have one IP configured in the host, this step is not displayed):

   Two selection boxes are displayed

   - Client Access:
     Select the IP Address through which the TNMS Server communicates with TNMS Clients.

   - Server Backend Access:
     This IP Address interface is used for serving other connected systems (TMF CORBA NBI, NMS and portals). These systems are not part of the evaluated configuration and will not be installed, so this configuration will have no effect.

10. In **Server Preparation: Database Migration** enter the required information for one of these options:

    • Build: creates a clean database
    • Migration: migrates an existing database.

11. In the **Server Preparation: Database** enter the required information for:

    - **Database IP Address**: Check the localhost checkbox.

    - **Database Port**: Port assigned to the database to communicate with TNMS (Default is 1521).

    - **Database User Name**: Name of the database user (Default is tnmsdba).
      Note 1: Special characters are not allowed when selecting a different user name for the Database.
      Note 2: If a standby server is deployed in the network, the same user name and password must be used for both the Primary and Secondary Servers. It is recommended that the same user name and password are used in all server machine installations in the network, ensuring database restoration in any machine. If a standby server is not deployed in the network, unique user name and passwords can be used for each server machine if required for security reasons.

    - **Database User Password**: Password for the database user that complies with the Password Complexity Rules. When FIPS mode is enabled, this must be at least 14 characters long.

    - **Re-enter Database User Password**: Re-enter the password.

    - **Database Name (SID)**: Name of the database that has been created during Oracle installation (by default it is TNMA.)

    - **Database User 'sys' Password**: Password defined during Oracle Installation for the default database administrator user SYS.

    - **Home Directory**: Oracle Database home directory (Default is opt/oracle/product/18c/db_1).

12. In **Server Preparation: Advisory Message**
    - Set Enable to display an advisory message before login.
    - Write the desired advisory message in the box.

This message will pop-up before a user's login. It is also possible to reconfigure this option after the installation process through TNMS system preferences.

13. In **Components: TNMS** select which managers to install. For the evaluated configuration you may only install the default selection:
    a. Ethernet Manager

   b. ASON Manager
   c. Optical Manager without IOC mode.
   d. Node Manager

14. In **Components: Northbound Interfaces** leave all options unchecked. Northbound interfaces are not part of the evaluated configuration.

15. In the **Components: Network Elements** select the NEs to install. For the evaluated configuration you may only select:

    a. MTERA (mandatory)
    b. UNO (optional)

    Note: UNO is a purely virtual Network Element that resides in TNMS database only. It may be used for simulating 3rd party network elements that TNMS does not actually manage.

16. *Only displayed if you selected to migrate your database*. In **Pre-migration Backup**, backup your current database to avoid data loss if any issue occurs during the migration.

17. The Pre-Installation Summary step summarizes all the previous settings. Click **Previous** to change any setting or **Install** to begin installation.

18. *Only displayed if you selected to migrate your database*. In **Post-migration Backup** backup your database after migration.

19. The results of the installation are presented in **Installation Results**. Click **Done** to finish the installation.

4.2 Post-Installation Steps

After running the installer, the following steps are required to setup TNMS Server.

Configure links to Java JREs:

1. Login as root

2. Create and go to directory `<Installation_Folder>/base/java`

3. Inside the new directory, create a link to the Java JRE:

```
ln -s jrex64 <JAVA 11 LOCATION>
```

Where,

- `<Installation_Folder>` is the base directory where TNMS will be installed

- `<JAVA 11 LOCATION>` is the full path to the installation folder of Amazon Corretto 11

4.3 Managing TNMS Server Services

To check the status of TNMS services, run as root:

```
<Installation_Folder>/system/admin/emsstarterdaemon.sh status
```

To start TNMS services, run:

```
<Installation_Folder>/system/admin/emsstarterdaemon.sh start
```

To stop TNMS services, run:

```
<Installation_Folder>/system/admin/emsstarterdaemon.sh stop
```

4.4 Enabling FIPS mode

TNMS Server cryptographic functions are provided by the “Bouncy Castle FIPS Java Provider v1.0.2.1” cryptographic engine embedded in the TNMS Server installation. After installing TNMS Server, FIPS mode must be enabled. This will ensure that the TNMS Server 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 Server.

To enable FIPS mode:

1. Stop TNMS Server

   ```
   <Installation_Folder>/system/admin/emsstarterdaemon.sh stop
   ```

2. Go to <Installation_Folder>/system/configuration

3. Run the script to enable fips:

   ```
   ./config_fips.sh enable
   ```

   Note: The command `config_fips.sh disable` will disable FIPS mode in TNMS Server and put it back in the general mode of operation.

4. Restart the TNMS Server

   ```
   <Installation_Folder>/system/admin/emsstarterdaemon.sh start
   ```

4.5 Managing Certificates and Keys

TNMS uses TLS to secure communication between TNMS Server and TNMS Client components (including Node Manager). TNMS Server is installed by default with a private key, a certificate (signed by a root Transcend_CA) and a root Transcend_CA certificate. TNMS Clients are installed by default with the root

Transcend_CA certificates as trust anchors. Both should be replaced with the customer's own private credentials, after TMNS installation.

TNMS includes the following optional extensions in its certificate validation process:

- Subject Alternative Name (SAN)
  TNMS validates the DNS Hostname or IP address if the certificate contains this extension. Otherwise, the Distinguished Name is used instead.

TNMS supports both ECDSA with NIST P-256 curve and RSA 2048-bit certificates.

TNMS Server does not rely on Java Runtime environment default key store. Instead, it uses its own key store. Management of the certificates and corresponding key pairs in the TNMS key store is done with the standard JRE `keytool` command.

4.5.1 Installing a new certificate

Note: Before you start, close all TNMS Clients. It's also recommended that you make a backup of the old key store file.

To replace TNMS Server credentials:

1. Login as root.

2. Change the directory to:
   `<Installation_Folder>/base/java/jrex64/bin`

3. Add a new certificate to the TNMS server keystore using the following command:
   ```
   keytool -importkeystore
   -destkeystore <keystore path>
   -deststorepass <keystore password>
   -destalias <alias>
   -srckeystore <pkcs#12 filename> -srcstoretype PKCS12
   -srcstorepass <pkcs#12 password>
   -srcalias <pkcs#12 alias>
   -srckeypass <pkcs#12 key password>
   -destkeypass <key password>
   -storetype BCFKS
   -provider
   org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
      -providerpath <provider path>
   ```

replacing the following parameters with their corresponding values:

- **`keystore path`**
  Path to TNMS Server key store:
  <Installation_Folder>/server/bicnet/configuration/bicnet_keystore.jks

- **keystore password**
  The key store password. Refer to TNMS Administration Guide for the default password.

- **key password**
  The private key password. Refer to TNMS Administration Guide for the default password.

- **alias**
  The alias used by TNMS to identify its credentials. Fixed to “bicnet”.

- **pkcs#12 filename**
  Path to the PKCS#12 file containing the credentials to be imported into TNMS.

- **pkcs#12 pass**
  Password used to protect the PKCS#12 file when it was created.

- **pkcs#12 alias**
  The alias used to identify the credentials when the PKCS#12 file was created.

- **pkcs#12 key password**
  Password used to protect the private key in PKCS#12 file when it was created.

- **provider path**
  Path to Bouncy Castle FIPS provider:
  <Product_Installation_Folder>/server/bicnet/modules/org/bouncycastle/bc-fips-1.0.2.1.jar

4. Restart TNMS services.

4.5.2 Listing certificates

Use the following command to view the certificate installed in TNMS Server:

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

replacing the following parameters with their corresponding values:

- **keystore path**
  Path to TNMS Server key store:
  <Installation_Folder>/server/bicnet/configuration/bicnet_keystore.jks

- **storepass**
  The key store password. Refer to TNMS Administration Guide for the default password.

- **provider path**

Path to Bouncy Castle FIPS provider:
<Product_Installation_Folder>/server/bicnet/modules/org/bouncycastle/bc-fips-1.0.2.1.jar

The output will show the installed certificate, identified by the "`bicnet`" alias and the corresponding SHA-256 fingerprint.

4.5.3 TLS Configuration

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

4.6 Firewall Configuration

TNMS Client will connect to TNMS Server through port 8443. This port needs to be opened in the server. The remaining ports may be closed for incoming connections.

The following iptables rules can be used to configure the Linux Host firewall. These rules will also accept ICMP packets and SSH connections to allow managing the server machine.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A INPUT -p tcp --dport 8443 -j ACCEPT
iptables -A INPUT -j REJECT
```

4.7 Checking the Installed Version

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

1. Go to <Installation_Folder>/system/admin

2. Run the NiapCheckVersion.sh script

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

4.8 Updating TNMS Server

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

1. Uninstall TNMS Server as described in section "4.10 - Uninstalling TNMS Server"

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 using *rpm -K <installation rpm files>*. TNMS GPG public key must be installed in the platform ("see 4.1 - TNMS Server Installation")

4. Install the new build of TNMS Server as described in section “4.1 - TNMS Server Installation”

5. Enable FIPS mode as described in section “4.4 - Enabling FIPS mode”

The TNMS server update is done through a clean reinstallation process. To verify if the TNMS Server update was successful, check the status of TNMS Server services as described in 4.3 - Managing TNMS Server Services. All services should have status RUNNING.

4.9 Changing TNMS database passwords

To change the passwords of the SYS user and database schemas after installation:

1. Log in to TNMS as Administrator.

2. Unassign the standby server, if configured.
   Open the **Standby server** window via **Main > Administration > System > Standby Server Configuration** and click **Unassign**.

3. Stop TNMS Server.
   Please refer to chapter 4.3 on how to stop TMNS Server.

4. Go to the changepassword directory:
   $SERVER_DIR/bin/changepassword.

5. Run the change_password.sh script

6. Enter the following (default database names are used below):
   a. Enter current user SYS password.
   b. Enter current TNMS schema password.
   c. If Node Manager is installed, enter current TNMS_NM schema password.
   d. Enter new user SYS password.
   e. Re-enter new user SYS password.
   f. Enter new TNMS schema password.
   g. Re-enter new TNMS schema password.
   h. Enter new TNMS_NM schema password.
   i. Re-enter new TNMS_NM schema password.

   NOTE 1: When defining the passwords during the normal installation process, the installer will set the TNMS_NM password to the same as TNMS password.

   NOTE 2: If FIPS mode is enabled, the TNMS and TNMS_NM passwords must be at least 14 characters long.

7. Start TNMS Server.

8. Reassign the standby server (if it was previously configured- see 3.8.5 of Assigning a Standby Server of the Administration Manual).

4.10 Uninstalling TNMS Server

Before uninstalling TNMS and in case you have a standby server assigned, you must first unassign it by doing as follows **in the active server**:

1. Select **Administration > System > Standby Server Configuration** and fill in the available fields.
   The address of the current standby server is filled in automatically.

2. Verify your input and click Unassign to start the procedure.
   The progress and result can be followed in the configuration steps, along with the elapsed time.

3. When the unassignment finishes, a notification pops up in the lower right corner with the status of the operation, either success or error. Alternatively, it is possible to check in System Event Log that the procedure has ended successfully.

If any error occurs, the logs can be checked in:

```
<Data_Folder>/trace/server/standby/[timestamp]/result.log
```

In the **standby server**, perform the following steps:

1. Go to the `$SERVER_DIR/bin/standby` and run the standby server executable file `standby-server.sh`

2. In the interactive menu select "**4. Start as Standalone.**"

To uninstall TNMS Server proceed as follows:

1. Login as root

2. Use rpm to uninstall TNMS Server (in the order presented below)

   ```
   rpm -e tnms-installer-zip-18.10.3-1904.el7.x86_64
   rpm -e tnms-installer-z01-18.10.3-1904.el7.x86_64
   rpm -e tnms-installer-z02-18.10.3-1904.el7.x86_64
   ```

3. Reboot the server to remove any temporary files left from the uninstallation process.

Note: The contents in the <*Data_Folder*> (default: /coriant) are also kept in the system. This folder contains log files. They may be manually deleted. Their deletion is optional.

4.11 Uninstalling the database

After uninstalling the TNMS Server it is needed to uninstall the database to remove files remaining on the TNMS server file system. The database can be removed with the following steps:

1. Change the permissions of the folder `/coriant/tnms/deinstall` to Oracle dba
   ```
   # chown -R oracle:dba *
   ```
   Remark: (default user / group is root root, and since the deinstall is done with Oracle user, it will not work)

2. Login as oracle user:
   ```
   # su – oracle
   ```

3. Run the uninstall by running (inside folder /coriant/tnms/deinstall)
   ```
   # ./deinstall
   ```
   The uninstaller begins.
   The uninstaller requests some confirmations, such as the database details. Accept the default by pressing **Enter** or change according to your environment.

4. When prompted for the Listener Name, enter **LISNER** and press **Enter**.

5. When prompted for the **Database SID** enter:

- **Small / Medium/Large (without Node Manager)** configuration - the name of the TNMS database (TNMS is the default name).

- **Large (with Node Manager)** configuration - the name of the TNMS database (TNMS is the default name) and the name of the Node Manager database (NMDB is the default and mandatory name), separated by a comma, for example **TNMS,NMDB**.
  Press **Enter**.

6. When prompted for TNMS database modification, enter “**n**” and press **Enter**. (The details of database(s) TNMS have been discovered automatically. Do you still want to modify the details of TNMS database(s)? [n]: n).

7. When prompted for continuation, enter “**y**” and press **Enter**. (Do you want to continue (y - yes, n - no)? [n]: y).

8. Under the “**Clean Operation Summary**”, after this message is displayed: Oracle Universal Installer cleanup was successful, follow the instructions in order to delete the remaining installation files.

9. Additionally, as root, delete the content of the ORADATA folders (/ora1, /ora2 and /ora3).

Additional remarks:

In some cases the deinstall tool may prompt for additional information. Answer as presented below:

- Specify the type of this database (1.Single Instance Database|2.Oracle Restart Enabled Database) [1]:

1

- Specify the diagnostic destination location of the database [/oradata/ora3/admin/TNMS/diag]:
  <Enter>

- Specify the storage type used by the Database ASM|FS []:
  FS

- Specify the list of directories if any database files exist on a shared file system. If 'TNMS' subdirectory is found, then it will be deleted. Otherwise, the specified directory will be deleted. Alternatively, you can specify list of database files with full path [ ]:
  <Enter>

- Specify the fast recovery area location, if it is configured on the file system. If "TNMS" subdirectory is found, then it will be deleted. []:
  <Enter>

4.12 TNMS Login

Make sure TNMS Server is up and running and log in to your TNMS Client. After a fresh installation, TNMS will have a default user ‘Administrator’ with a default password. You are forced to change the default password after the first login.

Note: If you are logging in after an update, users and passwords remain unchanged from the previous version.

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. The default user name is Administrator.

- Password
  Enter the password. Refer to TNMS Administration Manual document for the default Administrator password. If this is the first login after installation, you are requested to change the password, based on password complexity rules (see 4.15 - Changing the Password for a description of these rules).

If the 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.

4.13 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.

When creating or modifying a user, you can specify an inactivity timeout per user. If the **User inactivity timeout check box** is selected, the timeout defined for that user will override the inactivity timeout value defined in **System Preferences > Security Settings > General**. If the value is set to zero, there will be no timeout.

4.14 User and Security Management

The User and Security Management component in TNMS Server centralizes the functions of authentication and authorization in the system. All other software components rely on user and security management to ensure a secure TNMS system. User and security data stored in the TNMS database includes:

- Usernames/passwords
- User groups

User and security management supports the following main features:

User management

- Create, delete and modify user accounts and user groups.
- Activate/deactivate user accounts.
- Force a user to logoff.
- Unlock user accounts.
- View existing user accounts, login status and user groups they belong to
- Assign/unassign users accounts to user groups.
- View workspace settings, such as window size and positioning, filter and column settings.

Security management

- Configure security settings
    - Initial password change interval.
    - Inactivity duration.
    - Automatic deactivation/activation rules.
    - Display of the advisory message.
    - Set the advisory message.
    - Manage the password history.

4.15 Changing the Password

The first password change is performed in a popup window after the first login. This is also the case if the password has expired or has been forced to be changed by a TNMS administrator.

At any time, the password may be changed:

By the User:

1. Access **File > Change Password**
2. Enter the old password and the new password twice for confirmation

By a TNMS Administrator:

1. Access **Administration > User Management > User Modification**.
2. Enter the new password twice for confirmation.
3. Select the option to prevent the user from changing the password or make changing the password at next login mandatory.
4. Define the password expiration deadline (between 3 and 90 days).
   Note: In **System Preferences > Security Settings > General** tab set when you want to be warned of the password expiration date.

Password complexity rules

New passwords are validated by the system according to a set of rules:

- They must have at least 8 valid characters (see Table 3).
- Maximum length is 32 characters.

- It cannot contain:
    - Username
    - Reversed Username
    - Circular shifted version of the username (for example, 123abc / abc123)

- It cannot contain sequences of three or more characters of the user name or the previous password.

- It cannot contain more than three repeated characters of the same type, either lower or upper-case (for example aAaA).

- It cannot contain more than three consecutive characters in ascending or descendingorder, either lower or upper-case.

- It cannot contain a sequence of two or more repeated characters (for example a12b12).

- The password must be different from the last 5 passwords used.

- It cannot not begin nor end with a space.

- The password must include at least three of the following four specifications:
    - A lower case alpha character
    - An upper case alpha character
    - A numeric character
    - A special character.

Additionally, under **System Settings > Security > Password Rules** tab, the following rules can be optionally activated:

- Must not contain Employee First/Last Name
- Must not contain Employee Number
- Must not contain Date
- Must not contain Spaces.

4.16 DCN Management

The DCN, or Data Communications Network, refers to the network providing connectivity between TNMS Server and the Network Elements it manages. This section describes how to configure and manage the DCN in the TNMS Server evaluated configuration.

4.16.1 Enable SSH Strict Host Checking

SSH Strict Host Checking must be enabled in the evaluated configuration. When enabled, TNMS will validate the SSH host key when connecting to the Network Elements.

To enable SSH Strict Host Checking, enable the checkbox under **System Settings > DCN Manager > Strict Host Checking**

4.16.2 SSH Algorithms Configuration

SSH algorithms in TNMS Client are fixed and non-configurable. Similarly, SSH rekeying is always enabled and not configurable.

4.16.3 Adding Network Elements to TNMS

Adding a Mediator and Channels

Before adding Network Elements (NEs), you must setup the mediation and channels. A mediator is the TNMS server component that enables the connection of TNMS to specific NE types. A mediator can contain one or more mediation channels within which you can place one or more NEs. You can create channels to group the NEs according to your criteria, so you can manage them more efficiently.

In the evaluated configuration only the MVM mediator and mTera NE type are supported. This is configured during the installation process.

NOTE: UNO (Universal Network Objects) NEs and their respective mediation may also be optionally installed in the evaluated configuration. These are virtual NEs that can be configured and used to represent network elements which are not supported by TNMS and/or used to represent network services between third parties and TNMS networks. They exist in TNMS database only and there is no communication involved with UNO NEs.

To add an MVM mediator:

1. Open the DCN Management Window (**Network > DCN > Management**)
2. In the **DCN Tree**, right click on **TNMS** and select **New…**
3. In the **New Mediator** window, select **Multi-Vendor Mediator**
4. The property pages for the new mediator opens.
   a. Add or edit the **ID Name**
   b. Leave the **Primary IP** as default (127.0.0.1)
   c. Click **OK** to close the property pages.
5. In the **DCN Tree**, enable the checkbox next to the new mediator to activate it.

To add a channel:

1. Open the DCN Management Window (**Network > DCN > Management**)
2. In the **DCN Tree**, right click on the mediator under which the channel will be created, and select **New Channel…**

3. In the **New Channel** window, select **Multi-Vendor Channel**

4. The property pages for the new channel opens.
    a. Add or edit the **ID Name**
    b. Click **OK** to close the property pages.

5. In the **DCN Tree**, enable the checkbox next to the new channel to activate it.

To add an NE:

1. Open the DCN Management Window (**Network > DCN > Management**)

2. In the **DCN Tree**, right click on the channel under which the NE will be created, and select **New NE…**

3. In the **New NE** window, select the NE type and version (only mTera NE variants are supported in the evaluated configuration).

4. The property pages for the new mTera NE opens.
    a. In **General** tab:
        i. Add or edit the **ID Name**

    b. In **TL1 Settings** tab:
        i. Edit the **IP** address of the NE
        ii. Edit the **TID** (TL1 ID) of the NE
        iii. Enable the **Use secure connection checkbox**. This will configure TNMS to use SSH for this NE.
        iv. Set the **Port** to 3182
        v. Edit the **User name** and **Password** of the NE

    c. In **SSH Authentication** tab:
        i. In the **Authentication type** dropbox, select **PASSWORD** or **SSH_KEY**
        ii. If **SSH_KEY** authentication is selected:
            - Copy the SSH private key to the **Private Key** textbox (PEM format). The SSH Key should always be encrypted.
            - Edit the SSH private key passphrase in the **Passphrase** textbox.
        iii. If **PASSWORD** is selected:
            - TNMS will use the user name and password configured in the b).

    d. In **SSH Host Key** tab:
        i. Add the SSH **Host Key** of the NE. The format of the key is the same that is stored in the *ssh known_hosts* file.

    e. Click **OK** to close the property pages

5. In the DCN Tree, enable the checkbox next to the new NE to activate it. TNMS Server will connect and synchronize with the NE using the settings configured above.

SSH Supported Key Schemes

TNMS supports the following algorithms for Host Key and SSH Key based authentication:

- ssh-rsa, 2048 bits
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384