Cambium Networks™

Installation Guide

PTP 820 NMS
System Release R25A00

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

Contents

List of Figures

List of Tables

About This User Guide

This guide contains the following chapters:

- Chapter 1: About PTP 820 NMS
- Chapter 2: PTP 820 NMS Installation
- Chapter 3: PTP 820 NMS Installation
- Chapter 4: PTP 820 NMS Server High Availability Setup

Contacting Cambium Networks

Support website:	https://support.cambiumnetworks.com
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	support@cambiumnetworks.com
Repair enquiries:	rma@cambiumnetworks.com
Telephone number list:	https://www.cambiumnetworks.com/contact-us/
Address:	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Purpose

Cambium's PTP 820 Network Management System (NMS) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the support website.
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PTP products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor.

Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium PTP 820 Networks systems and equipment provide security parameters that can be configured by the operator based on their operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances, Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

Caution

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.

Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to http://www.cambiumnetworks.com/support

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Chapter 1: About PTP 820 NMS

Cambium PTP 820 NMS is a comprehensive Network Management System offering centralized operation and maintenance capability for a range of network elements.

Cambium PTP 820 NMS offers full range management of network elements. It can perform configuration, fault, performance and security management. PTP 820 NMS is the user interface to transmission and access products and the key issue for the system is to present management networks in the simplest possible manner. The software has network auto-discovery and uses the configuration data in the network elements to automatically build the managed network. The various elements and their attributes may be accessed using the intuitively graphical presentation of the element and its components. PTP 820 NMS has a continuously updated display of network status and network events are reported from the elements using notifications. An extensive database and context sensitive help facilities enable the user to analyze and report network events.

PTP 820 NMS provides the following network management functionality:

- Fault Management
- Configuration Management
- Performance Monitoring
- Security Management
- Graphical User Interface with Internationalization
- Network Topology using Perspectives and Domains
- Automatic Network Element Discovery
- HW and SW Inventory
- Software Download jobs
- Northbound interface to higher order OSS
- Report Generator

Functionality is maintained during network growth, with solutions covering the entire range of radio networks from a single hop to nationwide multi-technology networks. High availability and reliability is obtained through various redundancy schemes.

PTP 820 NMS functionality

The PTP 820 NMS is scalable both in size and functionality. The NMS Server is the basis for any PTP 820 NMS system, providing basic functionality within the Fault, Configuration, Performance and Security (FCPS) management areas. The NMS Server is by itself an advanced tool for the user to perform operations and monitor network elements for the whole operational network in real time. The flexible client/server architecture gives the operators easy access to all network elements and full control of the system from many different locations.

By selecting among a set of optional features, the PTP 820 NMS system can be enhanced and tailored to each operator's individual needs and requirements. With all optional features installed, PTP 820 NMS system provides the operator with an advanced and sophisticated network management system that will highly increase the efficiency of operations and maintenance in the network.

For easy integration to external higher-level management systems, a Northbound SNMP interface can be provided.

Installation Guide

The PTP 820 NMS Installation Guide can provide you with help about **PTP 820 NMS Installation** and how to configure the application. For detailed information regarding how to use PTP 820 NMS, including system management information, please see the PTP 820 NMS User Guide.

More information

If you cannot find the answer to your question in the installation Guide, contact Cambium support team (see **Contacting Cambium Networks** for contact details).

Chapter 2: PTP 820 NMS Components and Setup Deployments

PTP 820 NMS Components

A PTP 820 NMS System contains the following components, sub-components and complementary applications:

- CLI Reports module

  Generates reports executed by a CLI command.
- PTP 820 NMS Client

  client application that connects to the PTP 820 NMS Server and provides a GUI interface for network management. Can be installed on a separate machine.
- PTP 820 NMS Server
- Server application. PTP 820 NMS SNMP

  Northbound interface to higher-level network management (HLM) systems.
- System Manager

  database configuration and maintenance tool.
  System Manager is part of every PTP 820 NMS Server installation. It is mandatory to install System Manager also on the SQL database server in order to enable on demand or automatic backup and restore of the PTP 820 NMS database.
- A dedicated SQL database (PostgreSQL or Oracle)
- A dedicated Elasticsearch database, also referred to as an ES cluster

  The ES cluster is composed of ES nodes which are installed on every machine where System Manager is installed. The number of ES nodes is defined by the number of machines required in a specific PTP 820 NMS setup. ES cluster data is replicated 1:1 on every ES node in real time.

  PTP 820 NMS utilizes the ES database to store large volumes of data such as Performance Measurements (KPIs) collected from devices.

PTP 820 NMS Setup Deployments

The PTP 820 NMS system can be installed in various configurations, from the simplest which is 1+0 Standalone, to the most complex called 2+2 HA, which is suitable for high performance and high availability. The possible setup deployments include:

- 1+0 Standalone
- 1+0 Split
- 1+1 High Availability (1+1 HA)
- 2+2 High Availability (2+2 HA)
- 1+1 Server High Availability

Note

For Windows deployments, it is highly recommended to use a Windows Domain, especially where more than two Windows instances are used, such as in High Availability setups. The domain does not have to be the same domain as the user's private company domain; it can be a separate private domain in which all Windows instances related to PTP 820 NMS are members of the domain.

Machines IPs or hostname allocation

All the computers on which NMS Server, SQL database and Elasticsearch nodes are installed must have Static IPs, whether or not hostnames are used during SQL database and Elasticsearch configuration.

If Hostname addressing is used for Elasticsearch configuration and the IP address of an Elasticsearch Node is changed, 'Cluster Configuration' must be performed again in order to reconfigure the Elasticsearch configuration with the new IP address.

Communications between the PTP 820 NMS Server, SQL database and Elasticsearch nodes must be done over the same Network Domain, and each component must be able to reach the other components using the same network interface.

Operating System Restrictions

All the computers on which PTP 820 NMS Components are installed must have the same type of operating system (OS), either Windows or Linux. There are two exceptions:

- The PTP 820 NMS Client can be installed on a Windows OS only
- The PTP 820 NMS SQL database in a 1+1 Server High Availability setup can be installed on any OS

1+0 Standalone

A setup in which one machine, either physical or virtual, is required. The PTP 820 NMS Server and the dedicated SQL database are hosted by this machine. This machine also hosts an ES node that is required for ES cluster.

1+0 Split

A setup in which two machines, either physical or virtual, are required. The PTP 820 NMS Server is hosted by one machine and the dedicated SQL database user/schema is hosted on the second machine. Each of the two machines hosts an ES node required for the ES cluster.

1+1 High Availability

A setup in which two machines, either physical or virtual, are required. Each of the two machines hosts a PTP 820 NMS Server and a dedicated SQL database. Each of the two machines also hosts an ES node required for the ES cluster.

The two Servers, called mates, are configured so that one is the Primary server, and the other is the Secondary server.
The SQL databases are also configured so that one is the Active Database, and the other is the Failover Database.

Switchover policy in 1+1 High Availability

At any given time only one of the two PTP 820 NMS Servers is Active and the other is on Standby, and both are connected to the Active SQL Database. The Active Server can both read from and write to the SQL database, while the Standby Server can only read from the SQL database. Only the Active Server is connected to the ES cluster.
Clients are always connected to the Active Server.

The designated Primary Server remains the Active Server until it is stopped by a user or shuts down because of an error. Once the Primary Server shuts down, the Secondary Server takes over, becoming the Active Server. This operation is called Server Switch.

The designated Primary Database remains Active until it is stopped by a user or shuts down because of an error. Once the Primary Database shuts down, the Failover Database takes over, becoming the Active Database. This operation is called Database Switch.

If one of the machine is stopped by a user or fails, the ES cluster will still be reachable by the remaining Active Server, but will contain only one ES node.

Note that Server Switch is independent of Database Switch. Both switches occur at the same time only if both the Active Server and the Active Database shut down simultaneously.

2+2 High Availability

A setup in which four machines, physical or virtual, are required. Two machines host a PTP 820 NMS Server (one each), and two additional machines host an SQL database (one each). Each of the four machines hosts an ES node required for the ES cluster. The two Servers, called mates, are configured so that one is the Primary server, and the other is the Secondary server. The SQL databases on the other two machines are also configured so that one is the Active SQL Database, and the other is the Failover SQL Database.

Switchover policy in 2+2 High Availability

At any given time only one of the two PTP 820 NMS Servers is Active and the other is on Standby, and both are connected to the Active SQL Database. The Active Server can both read from and write to the database, while the Standby Server can only read from the database. Only the Active Server is connected to the ES cluster.
clients are always connected to the Active Server.

The designated Primary Server remains the Active Server until it is stopped by a user or shuts down because of an error. Once the Primary Server shuts down, the Secondary Server takes over, becoming the Active Server. This operation is called Server Switch.

The designated Primary Database remains Active until it is stopped by a user or shuts down because of an error. Once the Primary Database shuts down, the Failover Database takes over, becoming the Active Database. This operation is called Database Switch.

If one of the machines is stopped by a user or fails, the ES cluster will still be reachable by the remaining Active Server, but will contain only three ES nodes.

Note that Server Switch is independent of Database Switch. Both switches occur at the same time only if both the Active Server and the Active Database shut down simultaneously.

1+1 Server High Availability

A setup in which two machines, physical or virtual, are required. In this setup, the SQL database is not managed by System Manager, so it's not counted as part of the setup. The database type can be any of those supported by PTP 820 NMS and can be installed on any operating system.

Only the machines that host the PTP 820 NMS Servers also host an ES node required for the ES cluster, so the ES cluster contains two ES nodes.

In a 1+1 Server High Availability setup, only PTP 820 NMS Server high availability is managed by the PTP 820 NMS System Manager; database high availability remains the responsibility of the user.

Chapter 3: PTP 820 NMS Installation

This chapter describes how to discover, manage, monitor and update NE (Network Elements). It also explains user management, GUI handling and NMS configuration. This chapter consists of the following sections:

- PTP 820 NMS Installation on Windows
- PTP 820 NMS Installation on Solaris
- Post Installation
- Database Installation
- External Documents

Installation Packages

PTP 820 NMS Server and System Manager must be installed on the same OS type – either Windows or Linux. Therefore the PTP 820 NMS Server and PTP 820 NMS SQL Database must be installed on the same OS type1.

The available installation packages include:

Install Package	Package Contents
Server Node	CLI Reports, GUI Client, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch Node
Client Node (Windows only)	GUI Client, CLI Reports, PolyTopoImport
Database Node	System Manager, Elasticsearch Node

Elasticsearch Installation

The PTP 820 NMS Installer automatically installs an Elasticsearch node on every machine on which it installs the PTP 820 NMS System Manager. Elasticsearch is a distributed database, consisting of a cluster, local data nodes and a shared central repository.

As a prerequisite to PTP 820 NMS installation, you must create a local data folder for each node and a shared central repository for the cluster.

Note

You can configure the Elasticsearch cluster without a snapshot repository. If you do so:

- Scheduled database backup and scheduled Elasticsearch backup will not be available.
- Manual full database backups and manual Elasticsearch database backups may take longer.

  A configuration without a snapshot repository path is intended only for 1+0 Split, 1+1 Server HA and 1+1 HA setups where the PTP 820 NMS components are installed on different administrative domains; in all other cases, we recommend using a snapshot repository.

1) The operating system restrictions applying to a remote database installation are required only if System Manager is needed on the remote machine. If System Manager is not needed, the remote database can be installed on any type of operating system.

	Note that configuring the Elasticsearch cluster without a snapshot repository is applicable only for the following setups: 1+0 Split, 1+1 Server High Availability, 1+1 High Availability. For 1+0 Standalone and 2+2 High Availability setups, the Snapshot Repository is mandatory.

Creating Elasticsearch Folders

1. Node data path: On each machine on which PTP 820 NMS or System Manager will be installed, create an empty local folder with an identical path and file name, such as: C:\ES_DATA. This is the location where the local Elasticsearch node will save its data. You will need to provide this information in the Data Path field of the Cluster Configuration wizard during PTP 820 NMS Server configuration.
2. Cluster Snapshot Repository Path: Create a single central location, reachable by all machines on which PTP 820 NMS Server or System Manager will be installed, such as a shared folder within the company, for example: `\\fsro1\NMS\ES_Repo`. This will serve as the central Elasticsearch repository, in which the ES cluster creates its own backups. You will need to provide this information in the **Snapshot Repository Path** field of the Cluster Configuration wizard during PTP 820 NMS Server configuration.
3. If cluster snapshot repository redundancy is required, you can optionally create a second central location, reachable by all machines on which PTP 820 NMS Server or System Manager will be installed, such as a shared folder within the company, for example: `\\fsro1\NMS\ES_Repo_2`. You will need to provide this information in the Snapshot Repository Path #2 field of the Cluster Configuration wizard during PTP 820 NMS Server configuration.
4. Keep in mind that for Windows-based deployments, the use of Windows Domain and Active Directory facilitates the secured reachability of the ES repositories.
5. For Linux-based deployments, when mounting the repository paths into the PTP 820 NMS Server machine, make sure to add the following line in the `/etc/fstab` file, on the PTP 820 NMS machine:

   ```
   <host_repo_IP>:</host_path_to_folder> </local_mount_point> nfs
   rw,soft,timeo=10,retry=2 0 0
   ```

   This will cause the mounted path to timeout much faster in case the repository host machine is shut down.
6. Make sure that the Elasticsearch Repository folder is shared with either:
   - The machines (specified by their host ID) on which the PTP 820 NMS ES cluster nodes are installed – applicable for Windows if PTP 820 NMS services are started by 'Local System' (this is the default startup configuration).
   - The domain users used to start PTP 820 NMS services – applicable to Linux (always), and for Windows if PTP 820 NMS services are configured to be executed not by 'Local System' but by a specific system user.

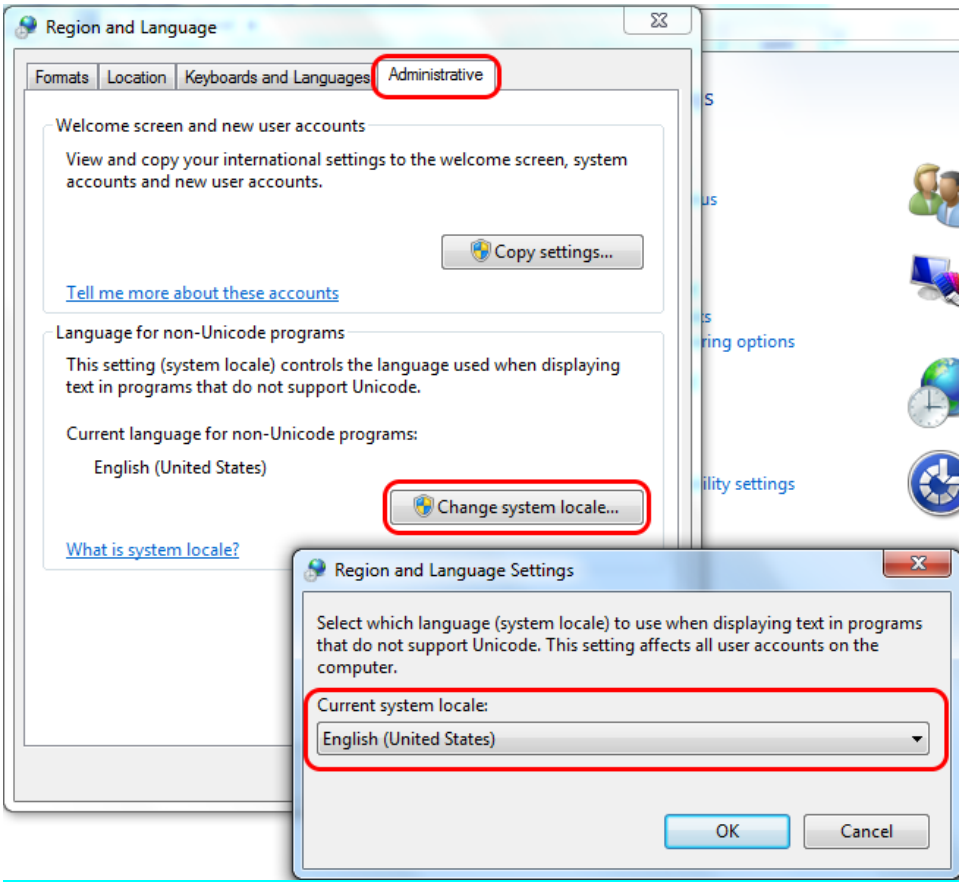
Database Installation

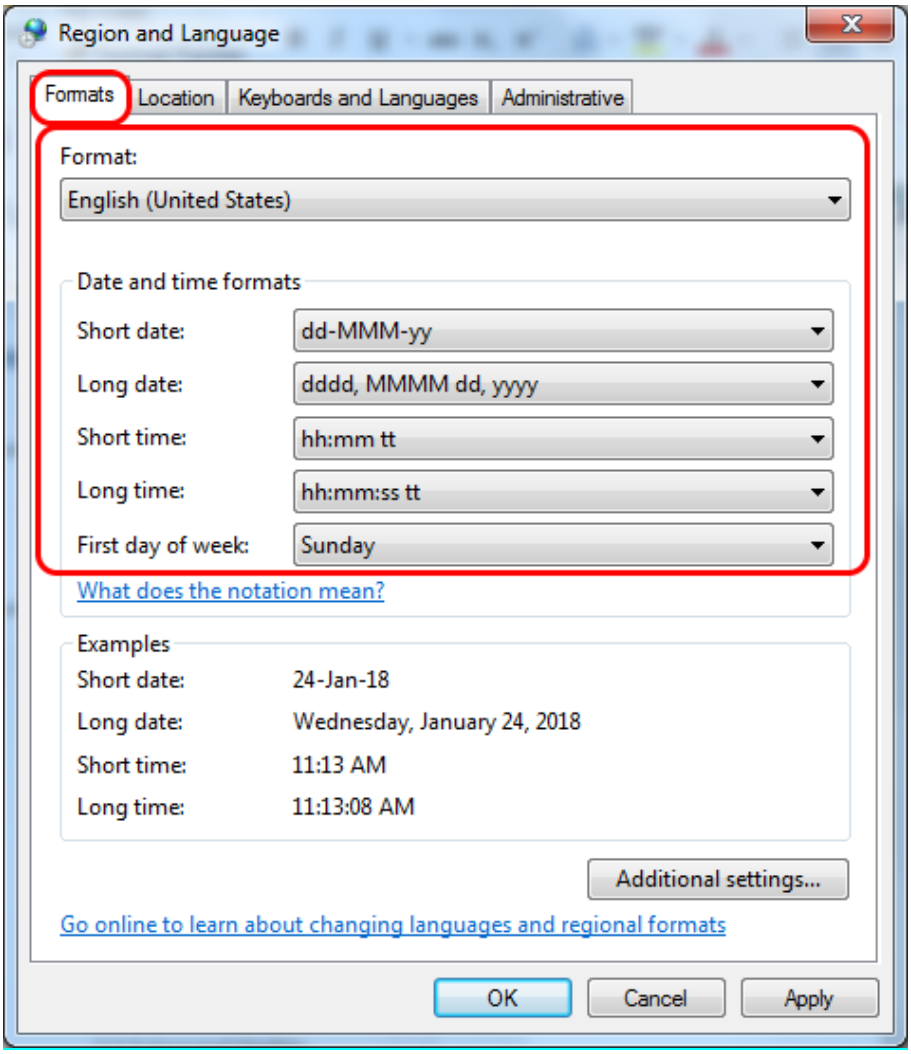
requires an Oracle or PostgreSQL database to be installed and available for use. Please refer to PostgreSQL documentation for instructions how to install PostgreSQL. Please refer to Oracle documentation for instructions how to install Oracle.

Please note that **System Manager** must be installed on the database server. Installation of System Manager is only supported for Windows and Solaris platform. Even though it might be possible to connect to a database on an unsupported platform, some essential features, like backup of database using System Manager, are not supported. We recommend using a system supporting use of System Manager, but if that is not possible, you should set up backup routines for the database manually.

Language and Date/Time format requirements for Windows

If you are installing the database on a Windows machine, make sure the Windows language format and date and time formats are as shown in the figure below.





Oracle

For the supported version of Oracle, refer to the System Requirements document.

When installing Oracle, keep in mind the following:

- Make sure to install Oracle using USA local English
- If you are installing an Oracle 12c database, it is important to set it up as a single tenant database configuration and not as a multitenant container database (CDB). That is, the option **Create as Container Database** must be unchecked, as shown below.

Oracle Recommendations

The following Oracle recommendations are suggestions, they are not mandatory.

Configuring large redo logs

Oracle best practices recommend having no more than 4 log switches per hour, therefore we recommend configuring larger redo logs (1 Gigabyte each).

Multiplexing of redo logs and control files

This is an Oracle-recommended best practice and consists of having at least two copies of a given file on different storage devices, such as different disks or RAID arrays. Unlike RAID mirroring, this process is managed by Oracle and is particularly useful for recovery, such as in the case of a media failure.

Installing as an Oracle dedicated server

Oracle can be installed in either dedicated or shared mode. We recommend the dedicated mode, because the Oracle Multithreaded Server (MTS, aka Shared Server) was specifically designed in Oracle 7 when RAM was expensive and there were multiple restrictions related to 32-bit access. In shared mode, a shared server process can service multiple user processes, while in dedicated mode, each user process has a dedicated server process.

Extending the AWR retention period

Oracle recommends that you adjust the AWR retention period to at least a month. You can also extend the period to one business cycle so you can compare data across time frames such as the close of the fiscal quarter.

Separating data files

According to Oracle OFA (Optimal Flexible Architecture), it is recommended to have separate mount points (for separate storage arrays) for binaries and data. Data itself can be split along multiple storage arrays in order to support file multiplexing and distribute I/O operations to avoid bottlenecks.

Creating an additional Oracle custom DBA user

	**Note:** This section applies to Oracle 12.

You may wish to add a new Oracle custom DBA user, in addition to the default DBA user (system). This user can be used instead of the system user when setting up the database from System Manager.

To create a new Oracle custom DBA user:

1 Create a script that includes the following commands. Call the script, for example, CUSTOM_DBA_USER.sql.

```
CREATE USER <user_name> IDENTIFIED BY <password>;

GRANT SELECT ON sys.user$ TO <user_name>;
GRANT CREATE SESSION TO <user_name>;
GRANT SELECT ON sys.v_$session TO <user_name>;
GRANT SELECT ON sys.v_$transaction TO <user_name>;
GRANT SELECT ON sys.v_$rollname TO <user_name>;

GRANT SELECT ON sys.v_$parameter TO <user_name>;
GRANT SELECT ON sys.v_$instance TO <user_name>;
GRANT datapump_exp_full_database TO <user_name>;
GRANT datapump_imp_full_database TO <user_name>;
COMMIT;
```

2 In a DB IDE (such as SQL Developer, SQuirrel or SQL*Plus), log in as "system as sysdba" or "sys as sysdba".

3 Run the commands in the CUSTOM_DBA_USER.sql file.

For example, in a Solaris server run:

```
#su - oracle
$ sqlplus / as sysdba
Sqlplus> start <FULL PATH TO SCRIPT>/CUSTOM_DBA_USER.sql
```

The script will create a user with the username and password you specified, and will grant that user rights on various tables, parameters and instances. It will also grant the user the rights to use Oracle's datapump mechanism for import and export, enabling Backup and Restore of the database.

	Note: Instead of creating a new Oracle admin user, you can grant an existing Oracle system user, the required privileges needed to administrate the Oracle database. The required privileges are the ones listed in step (1) of this section.

Oracle post installation

Database administrator user privileges

In order to be able to run the wizards that can be found in the Database Task view in the PTP 820 NMS System Manager on an Oracle database, you need to create database users with sufficient privileges to perform the tasks. The required privileges are listed in Creating an additional Oracle custom DBA user.

Oracle 12c - Adding missing admin privileges to the existing SYSTEM user

In Oracle 12c, instead of creating a new Oracle admin user, you can grant an existing Oracle system user all the required privileges needed to administrate the PTP 820 NMS Oracle database. To do so:

1 Launch an Oracle database utility such as SQLPLUS and log into the Oracle database with SYSDBA privileges.

For example, in SQLPLUS, enter the following in the command prompt:

```
sqlplus SYSTEM AS SYSDBA/password@sid.
```

2 Grant to an existing SYSTEM user the required admin privileges by running the following:

```
GRANT SELECT ON SYS.USER$ to system;

Commit;
```

Altering system settings for large-scale setups

To improve overall system performance in large-scale setups, you need to make some changes in parameter settings after installing Oracle, to make it work optimally with .

Run the following commands on the machine on which you installed the Oracle database:

```
alter system set open_cursors=3000 scope=memory;

alter system set optimizer_mode=first_rows;

alter system set processes=600 scope=both sid='*';
```

For large setup installations with more than 10000 devices it is recommended to check that the pga_aggregated_limit has a value of 64G; if it does not, set it by running the following command:

```
ALTER SYSTEM SET pga_aggregate_limit=64G SCOPE=BOTH;
```

PostgreSQL

For the supported version of PostgreSQL, refer to the *System Requirements* document.

During database installation make sure to use database encoding method UTF8 or ASCII. If the PTP 820 NMS setup requires High Availability, make sure that both databases are using the same encoding method.
Instructions for how to set the encoding method can be found on the Postgres support site.

PTP 820 NMS System Manager must be installed on every machine where databases are installed; otherwise the following PTP 820 NMS features will not be available:

- SQL Database Backup and SQL Database Restore will not be available
- Configuration of 1+1 HA or 2+2 HA setups will not be possible

Migrating from PostgreSQL 14.7 to PostgreSQL 17.4

Starting from R25A00, works with PostgreSQL 17.4. If you had installed with PostgreSQL 14.7 (starting from R23B00), you need to migrate to PostgreSQL 17.4, as detailed below.

The migration process detailed below consists of uninstalling the PTP 820 NMS server (whose version is prior to R25A00), as well as uninstalling the PostgreSQL version 14.7; then installing PostgreSQL version 17.4 and finally installing the new PTP 820 NMS server (version R25A00 or above).

	**Note:** Any PTP 820 NMS server upgrade between PTP 820 NMS server versions that use different Postgres versions, entails uninstalling and re-installing the PTP 820 NMS server.

1 Perform a back-up of the current active schema using the PostgreSQL **14.7** version, as follows:
   i Open System Manager.
   ii Select **Database tasks** > **Backup User/Schema**. Take care to save the schema's credentials securely for reuse during upgrade.
   iii Perform a backup of the active schema.
   iv Copy the backup from its location (by default, this is C:\NgNMS\backup\database), and paste it into another folder which you will use for the restore operation.
2 Uninstall the server.
   Make sure the devices backup folder is available at the location configured in the config_folder_location.properties file.
3 Uninstall PostgreSQL version **14.7** and delete the folder in which it was installed.
4 Install PostgreSQL version **17.4**.
5 Perform post-installation as described in PostgreSQL post installation.
   Restart the Postgres service via Task Manager on Windows.
6 Install PTP 820 NMS version R25A00 or above, taking care to perform the following:
   I. In the System Manager's **Initial Setup** wizard, create a new schema with the same user name/password as the schema backed up in step (1)(iii).
   II. For versions 19A00 and 20A00, take care to uncheck the **Start NMS Server** checkbox.
7 In the newly created schema, use System Manager's Restore User/Schema Wizard to restore from file the schema backed up in step (1)(iii). Do not start the server – make sure to uncheck the **Start NMS Server** checkbox.
8 In System Manager, perform a user/schema upgrade of the restored schema. Go to Database **Tasks > Upgrade User/Schema** and upgrade the restored schema.

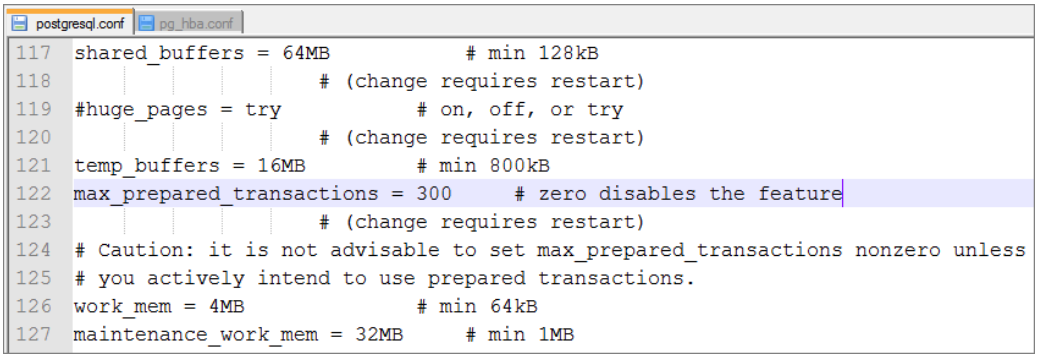
PostgreSQL post installation

After installing PostgreSQL you need to change several parameter settings to make it work optimally with . The parameter changes in the postgresql.conf file are mandatory. The changes in the pg_hba.conf file is optional.

Configuring postgresql.conf

1 Navigate to the location of the postgresql.conf file. By default, it is located under <Postgres installation folder>\data.

2 Open the **postgresql.conf** file in a text editor.



3 For each parameter appearing in the following table, make sure the parameter is enabled by removing the #, and set its value according to the table.

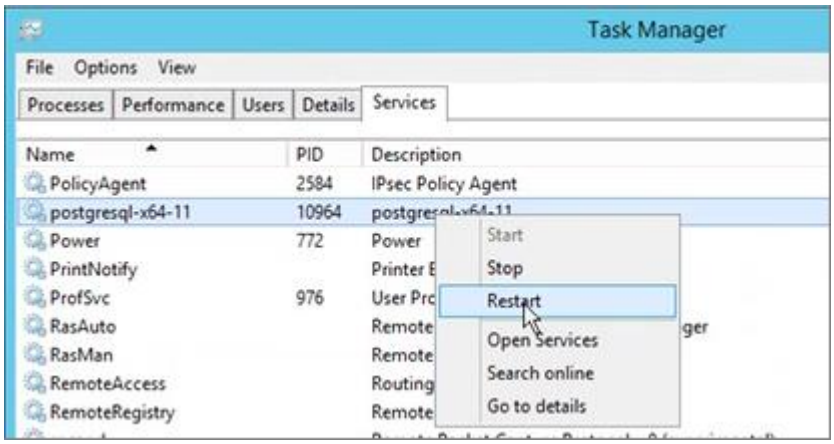
The following table contains required minimum values for running with PostgreSQL:

Parameter name	Setups with 1-1000 devices	Setups with >1000 devices Windows| Solaris	
checkpoint_completion_target	0.5	0.7	
checkpoint_timeout	5 min	5 min	
effective_cache_size	4 GB	8 GB	18 GB
maintenance_work_mem	64 MB	1023 MB	
max_connections	250 500 in Server High Availability setups	500 1000 in Server High Availability setups	
max_prepared_transactions	300 600 in Server High Availability setups	600 1100 in Server High Availability setups	
max_wal_size	1 GB	5 GB	
shared_buffers	128 MB	2 GB	6 GB
temp_buffers	16 MB	16 MB	

Parameter name	Setups with 1-1000 devices	Setups with >1000 devices Windows| Solaris
wal_buffers	-1	1
work_mem	4 MB	8 MB

4 Save the file changes and exit the text editor.

5 Restart the PostgreSQL service to ensure all parameter values are correctly updated. In Windows, launch Task Manager, select the **Services** tab and restart the PostgreSQL service:



Configuring pg_hba.conf

If you plan to install the server on a machine that is not the one on which the PostgreSQL server is installed, or in a Server or Database High Availability configuration, you have to enable access in the host based authentication configuration, as follows:

1 Navigate to the lcoation of the pg_hba.conf file. By default, it is located under <Postgres installation folder>\data

2 Open the **pg_hba.conf** file in a text editor.

3 Add an entry with the IP-address and subnet mask of the client that shall be allowed access to the database server.

- In a 1+1 High Availability or 2+2 High Availability setup, add the IP address of the Primary server and the IP address of the Secondary server.

For example:

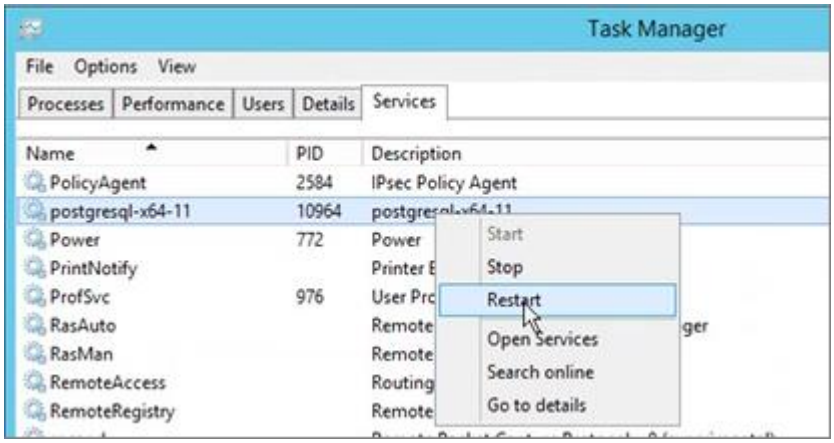
```
host  all   all   10.10.66.10/32   md5
host  all   all   10.10.66.11/32   md5
host  all   all   10.10.66.12/32   md5
host  all   all   10.10.66.13/32   md5
```

Where 10.10.66.10 is the IP address of the Active database machine, 10.10.66.11 is the IP address of the Failover database machine, 10.10.66.12 is the IP address of the Primary Active server, and 10.10.66.13 is the IP address of the Secondary Standby server.

More details on this are given in the PostgreSQL online help.

4 Save the file changes and exit the text editor.

5 Restart the PostgreSQL service to ensure all parameter values are correctly updated. In Windows, launch Task Manager, select the **Services** tab and restart the PostgreSQL service:



Installation on Windows

Server Pre-Installation for Windows

Server host name

The server host name should not contain '_' (underscore).

Creating a dedicated Windows user for PTP 820 NMS

On a Windows machine, installation must be performed by a dedicated Windows user with Administrator permissions. The same user should be used for running PTP 820 NMS itself. This user must be created prior to PTP 820 NMS installation.

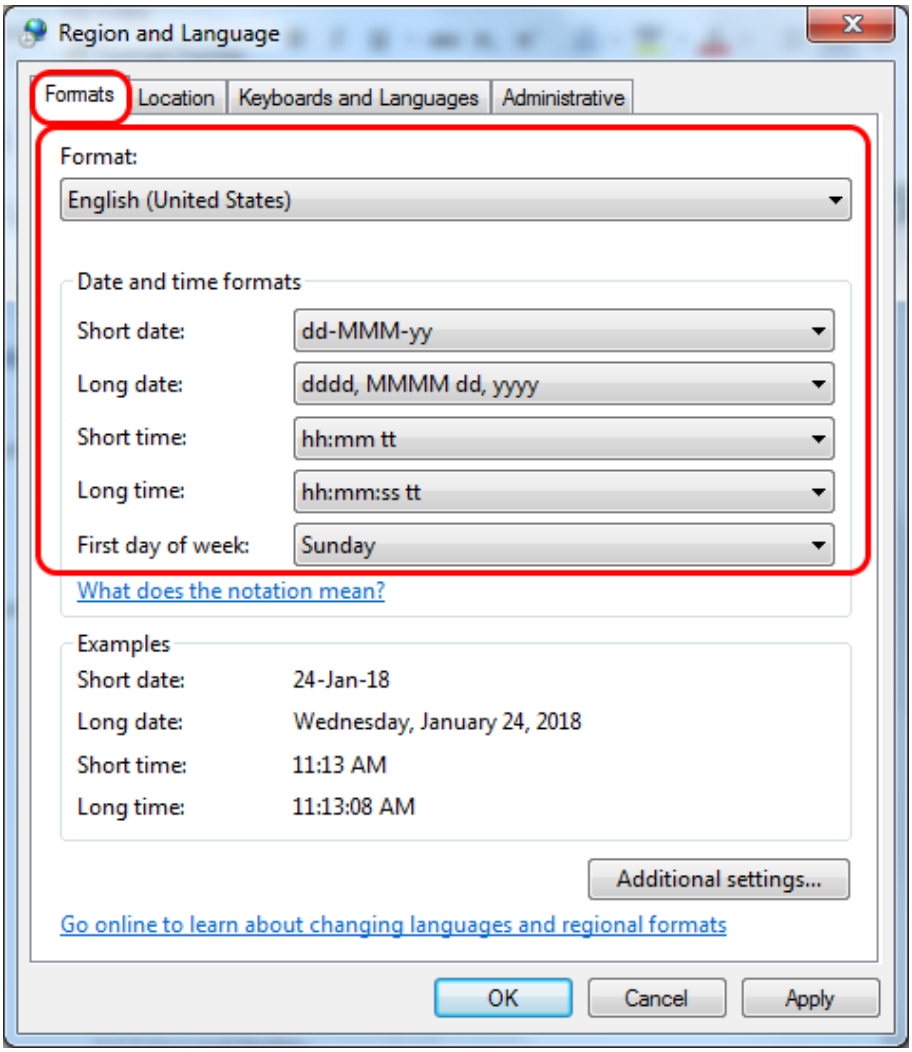
Users running the PTP 820 NMS client must have access to the folder C:\Program Files\PTP 820 NMS\GUI_Client.

Region and Language requirements

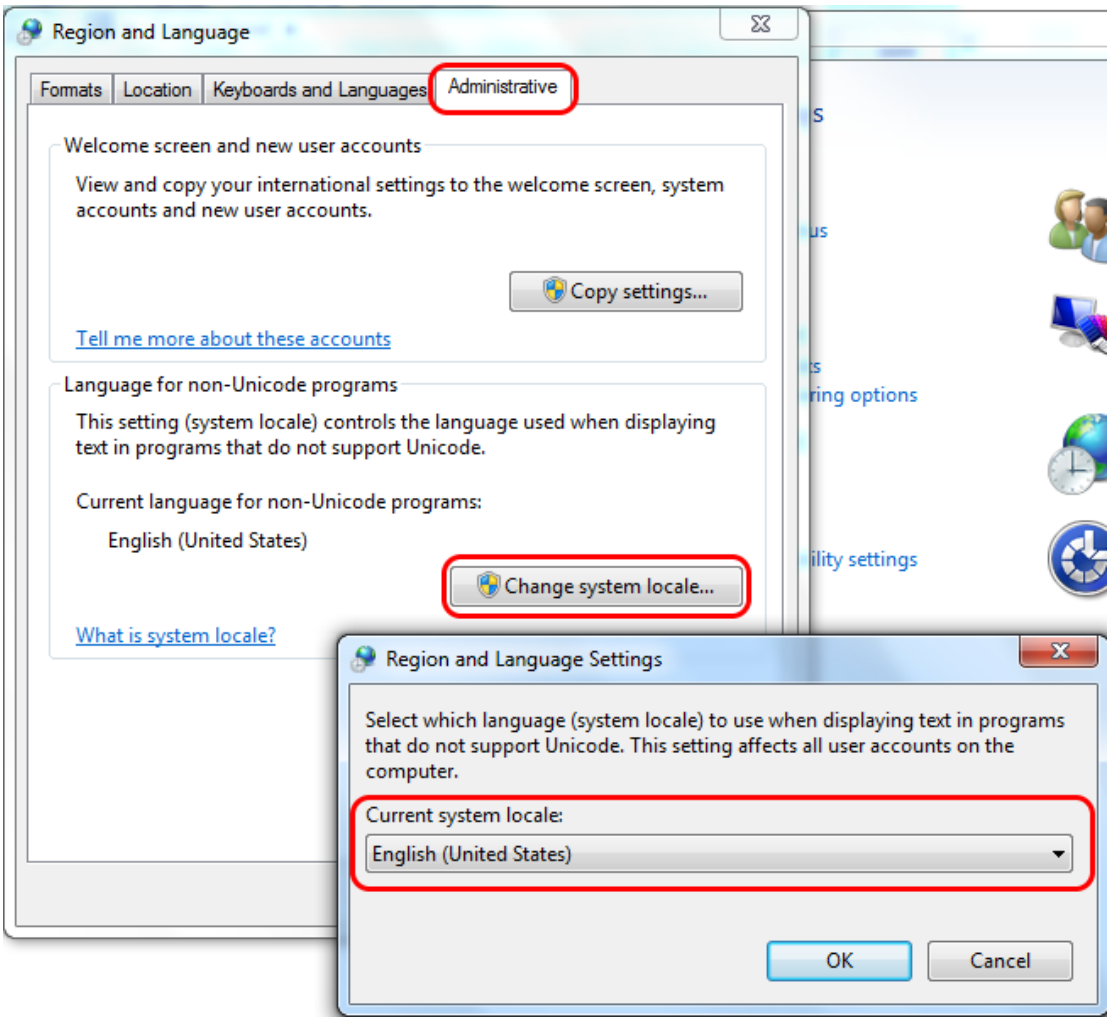
The language of the operating system and database on which is installed must be English (United States). This refers to all components and applications in the package (Server, Client, System Manager, etc.).

When installing on a Windows machine, make sure to set the following:

1 Set the Windows language **Format** and **Date and time formats** as shown in the figure below.

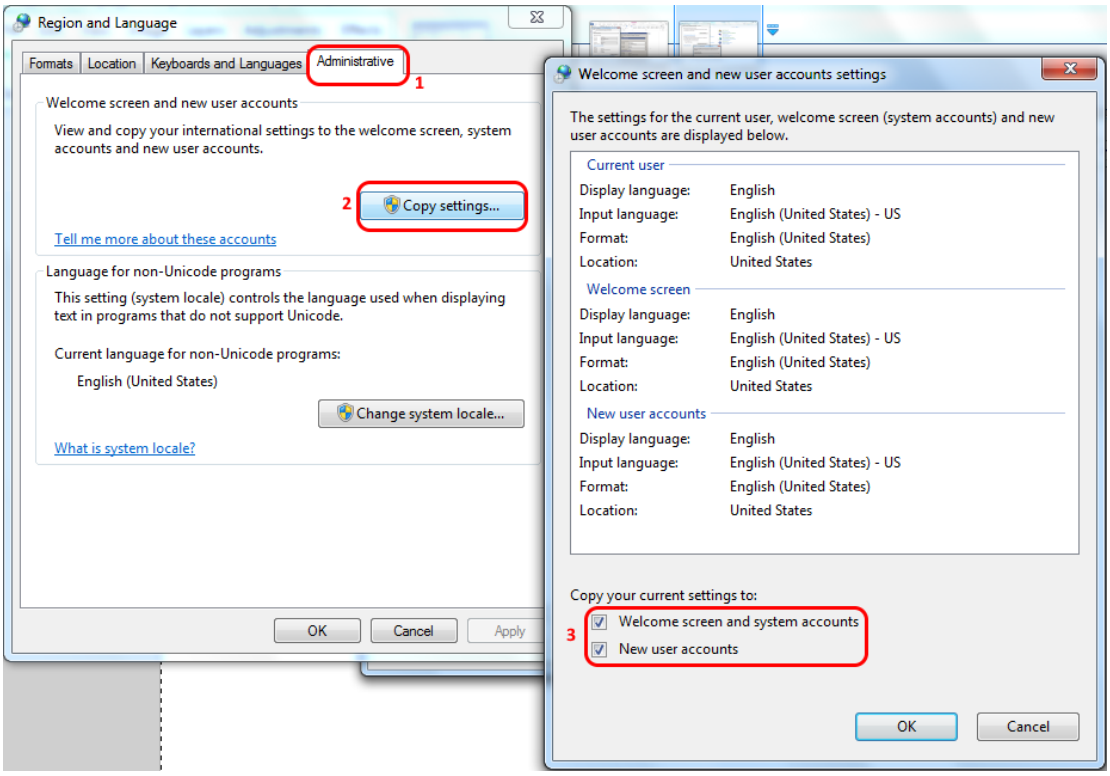

Region and Language
Formats
Location
Keyboards and Languages
Administrative
Format:
English (United States)
Date and time formats
Short date:
dd-MMM-yy
Long date:
dddd, MMMM dd, yyyy
Short time:
hh:mm tt
Long time:
hh:mm:ss tt
First day of week:
Sunday
What does the notation mean?
Examples
Short date:
24-Jan-18
Long date:
Wednesday, January 24, 2018
Short time:
11:13 AM
Long time:
11:13:08 AM
Additional settings...
Go online to learn about changing languages and regional formats
OK
Cancel
Apply

2 Set the **System Locale** to **English (United States)**.



3 Copy the Current User settings (by selecting the corresponding checkboxes), to the:

- **Welcome Screen and system accounts**
- **New user accounts**



Elasticsearch Folders

Make sure that Elasticsearch Folders are created as described in Creating Elasticsearch Folders.

Power Plan Settings for Windows

To improve overall system performance in large-scale setups using Windows , it is recommended to set the server's power plan (in **Control Panel** > **All Control Panel Items** > **Power Options**) to **High Performance**.

Java Installation

1 We recommend removing all Oracle Java installations from the computer on which you will install (client and/or server). If you installed previously, we also recommend removing the environmental variables used by it, such as **NMS_JAVA_HOME**.

2 Download OpenJDK, version **jdk8u222-b10**.

3 Install OpenJDK.

4 Edit the **NMS_JAVA_HOME_8** environment variable to point to the OpenJDK version:

C:\Program Files\AdoptOpenJDK\jdk-8.0.222.10-hotspot

(The path might be different depending on the Java installation folder.)

5 Edit the **JAVA_HOME** environment variable to point to the OpenJDK version:

C:\Program Files\AdoptOpenJDK\jdk-8.0.222.10-hotspot

(The path might be different depending on the Java installation folder.)

6 Edit the **PATH** environment variable by appending to its front, the path to the OpenJDK version:

C:\Program Files\AdoptOpenJDK\jdk-8.0.222.10-hotspot\bin

(The path might be different depending on the Java installation folder.)

7 Restart the computer.

Prepare Database

Server requires a database to work. Make sure that a database server is installed and reachable from the computer on which you want to install server.

The database server can be installed on the same computer as the PTP 820 NMS.

Server – refer to the *PTP 820 NMS System Requirements* document for guidance – or it can be installed on a separate computer.

If the database server is running on a different computer than the Server, the Firewall settings on the database server may have to be modified (i.e. open the port used for communication with the database server).

Oracle and PostgreSQL database servers are supported – see the System Requirements document for information about supported database editions.

Server Installation for Windows

The following section guides you through installation on Windows platform.

Note: This section requires that the steps for Server Pre-Installation for Windows already have been completed.

If you wish to upgrade an existing PTP 820 NMS installation, refer to Performing an upgrade in Windows.

Install Sets for Windows

This section guides you through installation on a Windows platform.

PTP 820 NMS Installation Packages for Windows

The available Windows installation packages include:

Install Unit	Explanation
Server Node	CLI Reports, GUI Client, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch
Client Node	GUI Client, CLI Reports, PolyTopoImport
Database Node	System Manager, Elasticsearch

Install Sets

Install Set	Explanation
Client	Client only.
CLI Reports	Generates reports executed by a CLI command
PTP 820 NMS Server	Server application.
GUI Client	Client only. client application that connects to the PTP 820 NMS Server and provides a GUI interface for network management. Can be installed on a separate machine.
PolyTopoImport	PolyView Topology Importer. Enables exporting discovered elements and subnetworks from PolyView NMS into a file and then importing them, while preserving their hierarchy, into as managed elements in administrative domains
System Manager	Database configuration and maintenance tool.

	System Manager is part of every PTP 820 NMS Server installation. It is recommended to install System Manager also on the database server in order to enable automatic backup and restore of the PTP 820 NMS Database.
Elasticsearch	A complementary database in which PTP 820 NMS stores large volumes of data such as Performance Measurements (KPIs) collected from devices.

Install Modes

There are two possible modes of installation:

- New Installation
- Upgrade Installation

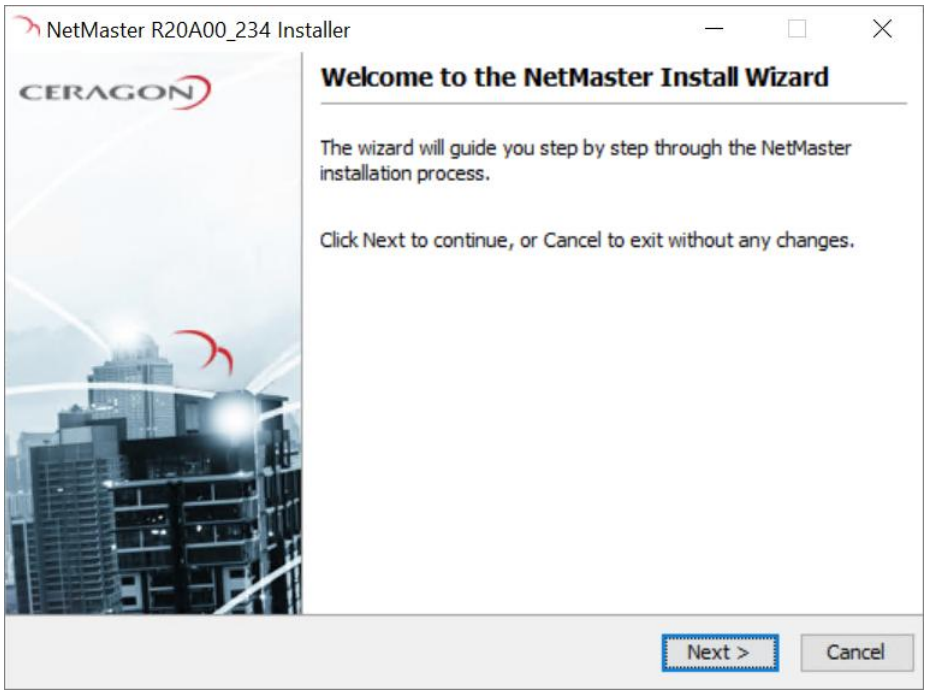
New PTP 820 NMS Installation for Windows

You may cancel the installation at any step until the Install wizard starts installing the files.

1. Right click the installation zip file PTP 820 NMS_*<major version number>*_*<minor version number>*_windows.zip to extract the single .exe file.
2. Double-click the PTP 820 NMS_*<major version number>*_*<minor version number>*_windows.exe file to launch the install wizard.
3. If a security warning appears, requesting permission to run the installer, click **Yes**.

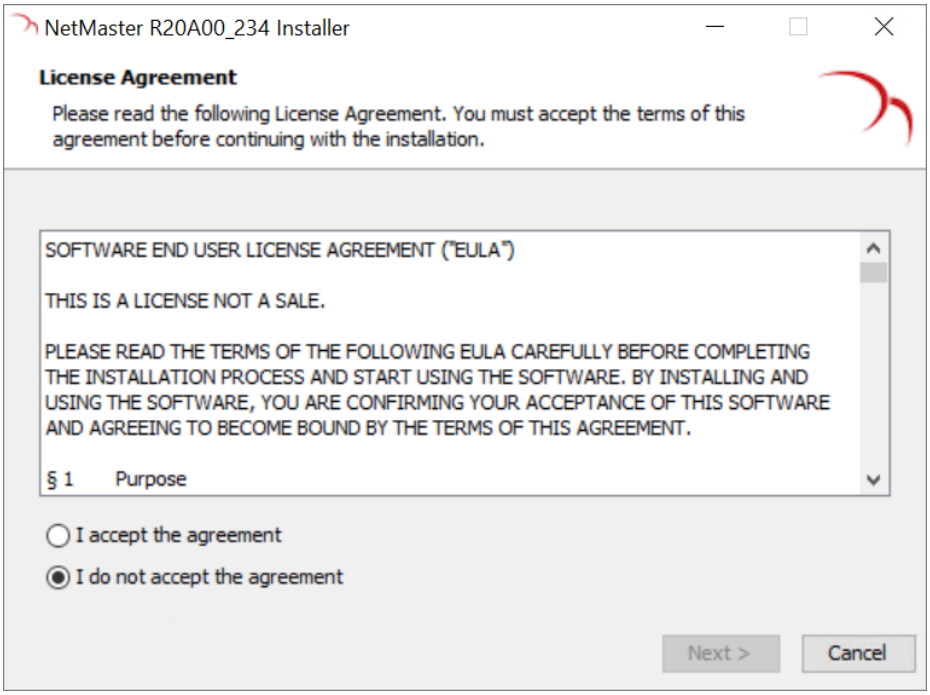
   A message appears, informing you the install wizard is being prepared.
   The Welcome page of the **PTP 820 NMS** Install Wizard appears.

4. In the Welcome page, click **Next** to initiate installation.



The License Agreement page appears.

5. In the License Agreement page, if you accept the agreement, select the **I accept the agreement** option and then click **Next** to continue.

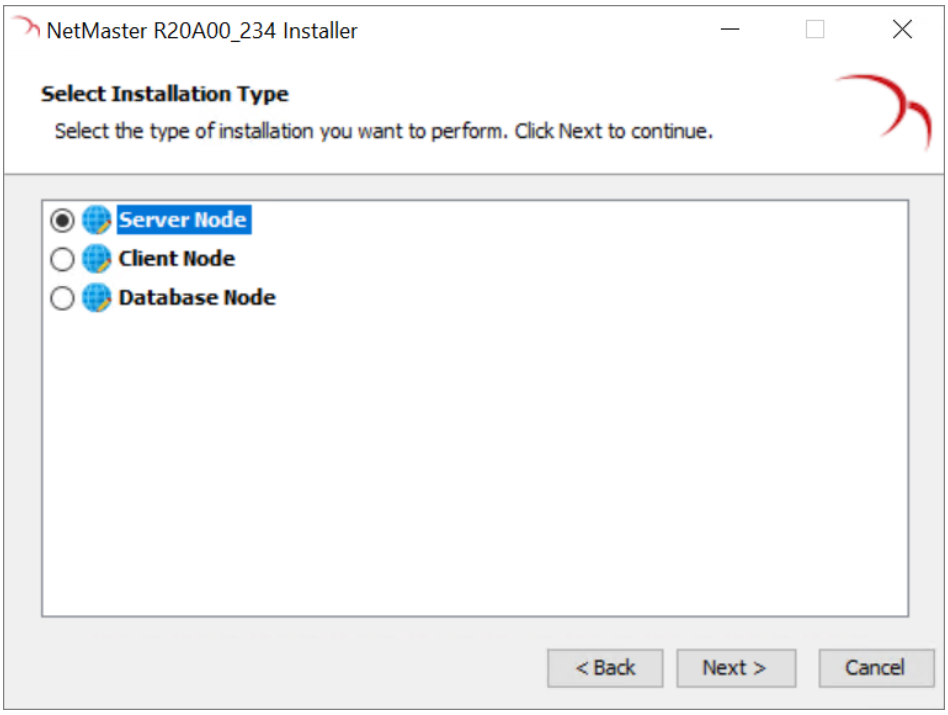


The select Installation Type page appears.

6. In the Select Installation Type page, select the installation type, and then click **Next**.

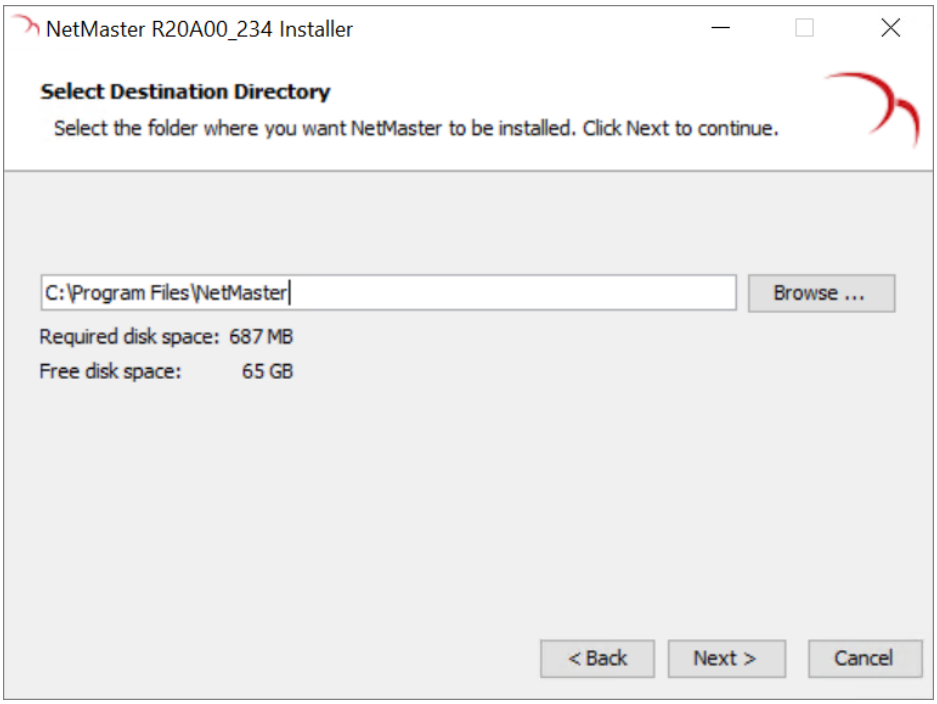
   There are three types of installations. Each type includes a different mix of

   - **Server Node** – Includes: CLI Reports, GUI Client, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch
   - **Client Node** – Includes: GUI Client, CLI Reports, PolyTopoImport
   - **Database Node** – Includes: System Manager, Elasticsearch



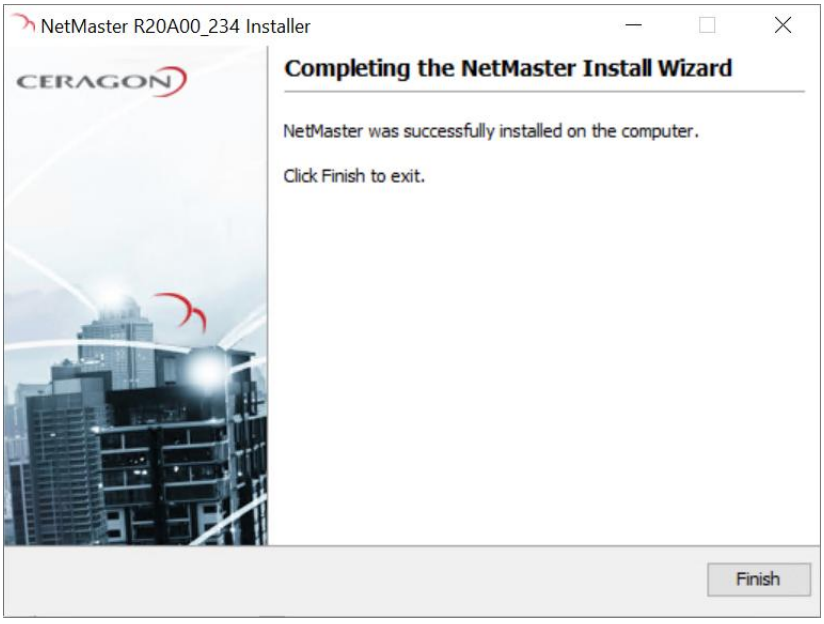
The Select Installation Directory page appears.

7. In the Select Installation Directory page, select the installation directory, and then click **Next**.

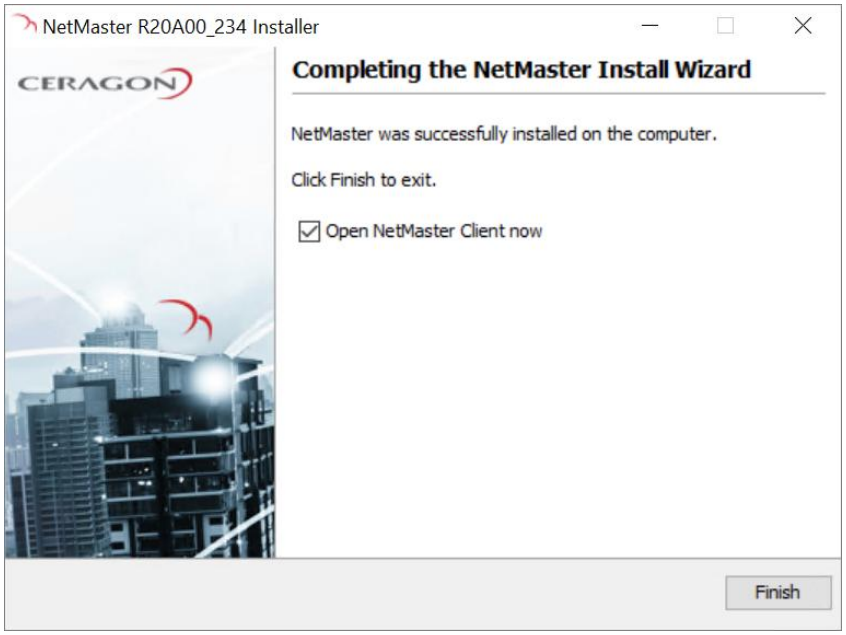


   - PTP 820 NMS installation begins. A progress bar appears, and messages inform you that installation is in progress.
   - When installation is complete, a Completing the PTP 820 NMS Install Wizard page appears, informing you that installation completed successfully.

8. If you are installing a **Database Node**, click **Finish**.

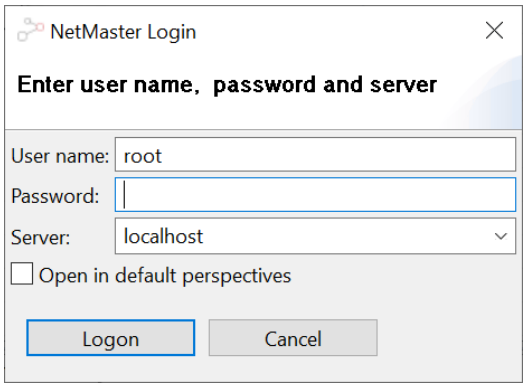


9. If you are installing a **Client Node**, an **Open PTP 820 NMS Client now** checkbox is by default selected.



If you leave **Open PTP 820 NMS Client now** selected, then upon clicking **Finish** the PTP 820 NMS Client application is launched, and a login window appears.

- Enter the initial authentication user credentials for a PTP 820 NMS Client administrator:
  Username: root
  Password: pw
- In **Server**, enter the IP address or network name of a PTP 820 NMS Server. You can enter **localhost** if the server is running on the same machine as the client.

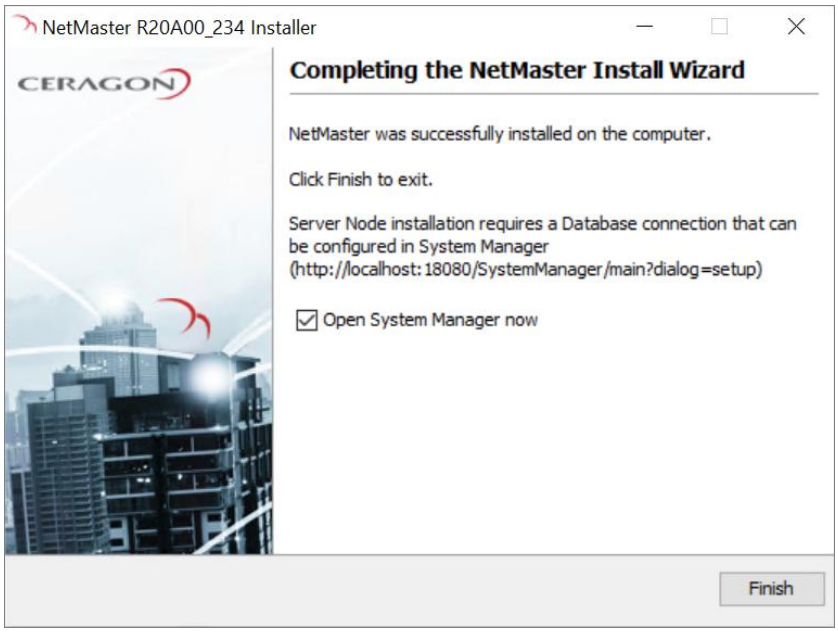


It is strongly recommended to change the password as soon as possible to prevent unauthorized access. You can do so in the **User Settings** Preference page of the PTP 820 NMS Client GUI.

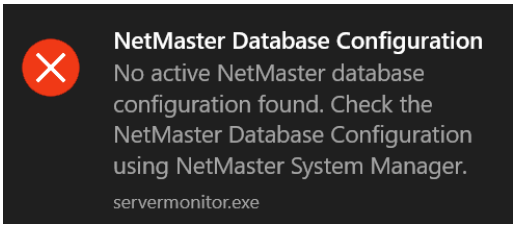
Note that you can launch the PTP 820 NMS Client anytime from:

C:\Program Files\PTP 820 NMS\GUI_client\Ngnms.exe, or from the shortcut accessible from the Start menu.

10. If you are installing a **Server Node**, an **Open System Manager now** checkbox is by default selected. Click **Finish**.



- First a message appears, informing you that no active PTP 820 NMS database configuration is found.



- Then System Manager is automatically launched so you can perform initial PTP 820 NMS Server setup.
  Follow the instructions in PTP 820 NMS Database and Cluster Configuration.

Upgrade PTP 820NMS Installation for Windows

Upgrade from legacy NetMaster releases is provided for up to two years after the release (see the *NetMaster Release Notes*). To upgrade from older versions, contact Ceragon Customer Support.

Before upgrading in Windows

- Make sure you install the Java version mentioned in the Java Installation sub-section of the PTP 820 NMS Server Pre-Installation for Windows section.
- Make sure that Elasticsearch folders exist, as described in Creating Elasticsearch Folders.
- All services must be stopped before installing the new version.
  This includes the Server, the System Manager, the SNMP Agent, and the PTP 820 NMS Elasticsearch service.
  In rare cases in which you do not manage to stop one of these services, you must reboot the machine and then verify these services are stopped.
- From R24B10, legacy devices are no longer supported by NetMaster except as OpenSNMP devices (see the NetMaster Release Notes for the full list of legacy devices). If you are managing legacy devices and wish to upgrade to R24B10 or above, you must unmanage the legacy devices prior to upgrading, and after upgrade is complete you can re-manage the legacy devices as OpenSNMP devices.

Upgrade Notes Related to R23A00 and Above

A change password wizard is triggered upon first login to System Manager following upgrade from a release earlier than R23A00.

Upgrade Notes Related to R23B00 and above

Starting with 23B00, the parent node under which the following folders are located, is by default C:\NgNMS for Windows:

- Scheduled reports. These are saved in the <folder_location>\reports folder
- Configuration files – Device configuration backups, stored in <IP-address-of-element> subfolders of the <folder_location>\BackupConfigurations folder
- Element Software files – Device software images, stored each in its own subfolder under the <folder_location>\SoftwareImages folder

Performing an upgrade in Windows

If the installed version is 20A00 or higher, upgrade is supported, and manual uninstallation is not required.

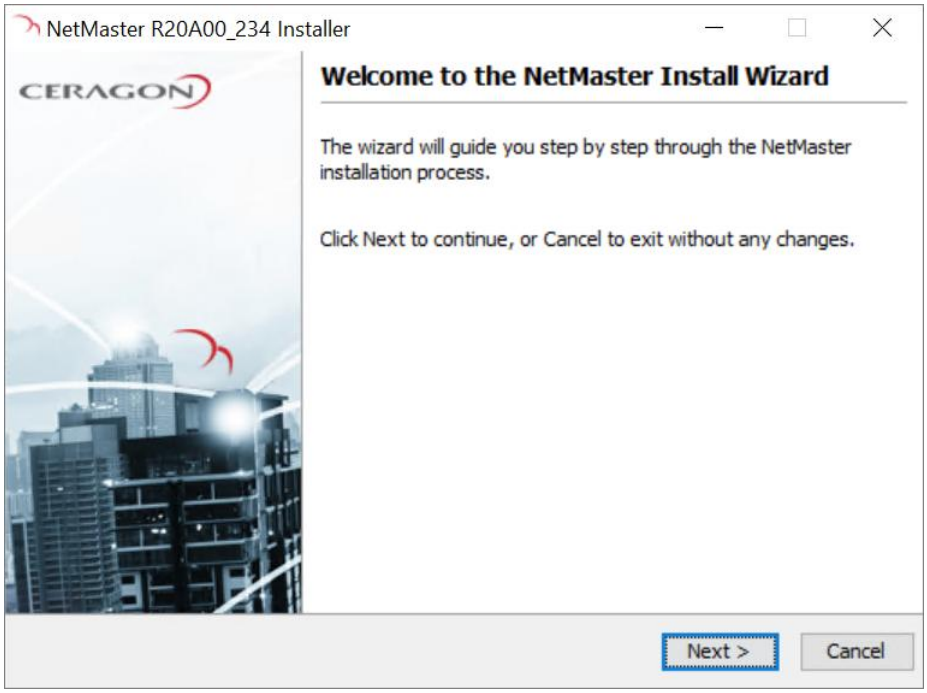
Perform the following:

1. Back up the active schema using System Manager, and store it in a different location. Store also the current database credentials.
2. Back up all the NetMaster file folders (scheduled reports folder, configuration backup files, element software files).
3. Uninstall the old version.
4. Make sure you comply with the Prerequisites in Server Pre-Installation for Windows.
5. Install the new version as described in New PTP 820 NMS Installation for Windows

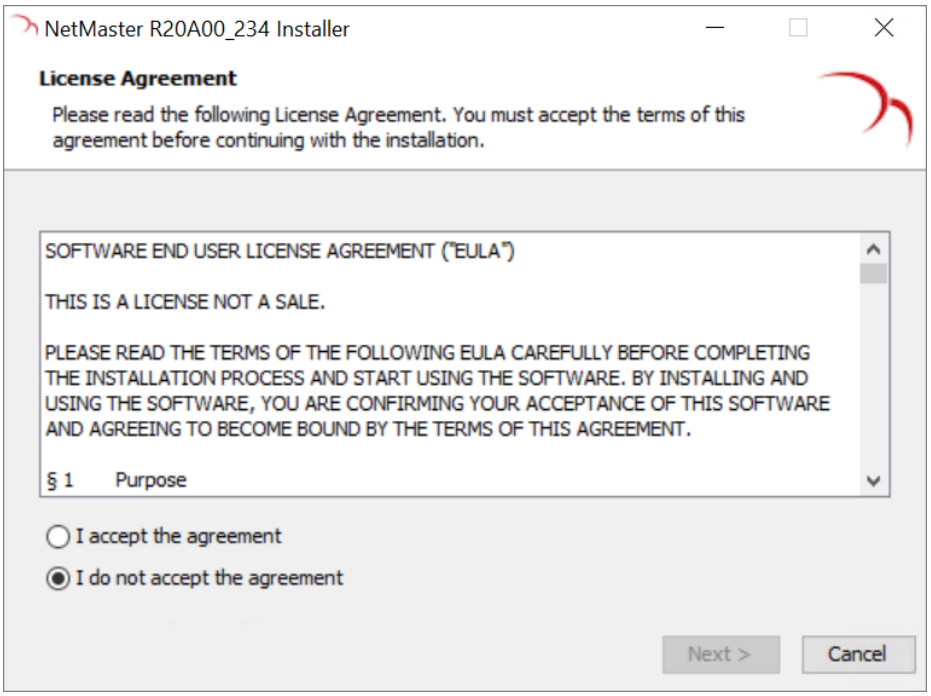
You may cancel the installation at any step until the Install wizard starts installing the files.

11. Right click the installation zip file PTP 820 NMS_<*major version number*>_<*minor version number*>_windows.zip to extract the single .exe file.
12. Double-click the PTP 820 NMS_<*major version number*>_<*minor version number*>_windows.exe file to launch the install wizard.
13. If a security warning appears, requesting permission to run the installer, click **Yes**.

    A message appears, informing you the install wizard is being prepared.
    The Welcome page of the **PTP 820 NMS** Install Wizard appears.
14. In the Welcome page, click **Next** to initiate installation.



    The License Agreement page appears.
15. In the License Agreement page, if you accept the agreement, select the **I accept the agreement** option and then click **Next** to continue.

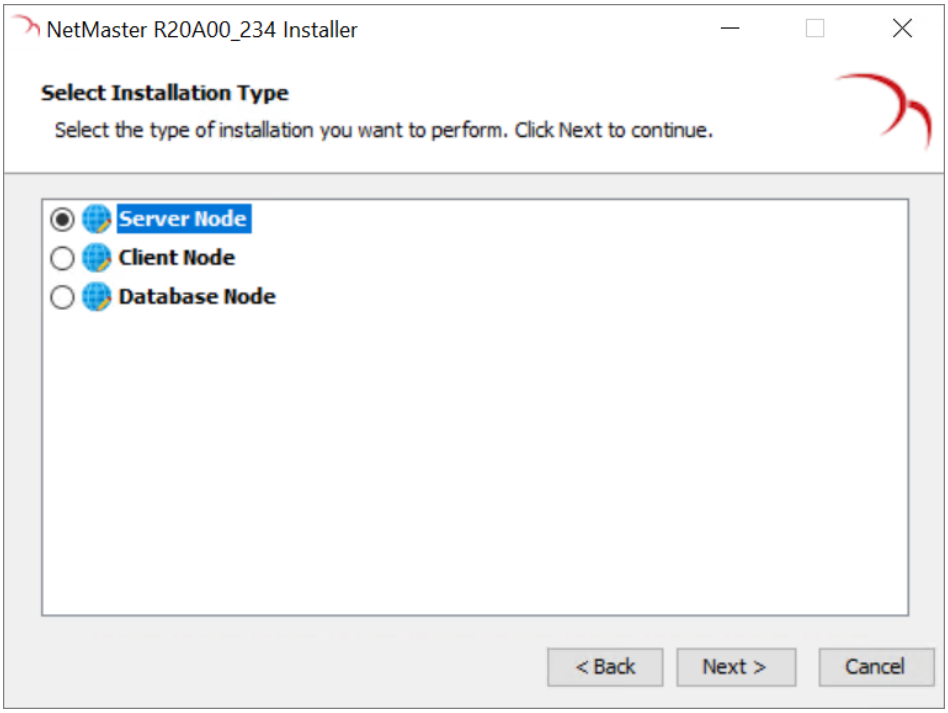


The select Installation Type page appears.

16. In the Select Installation Type page, select the installation type, and then click **Next**.

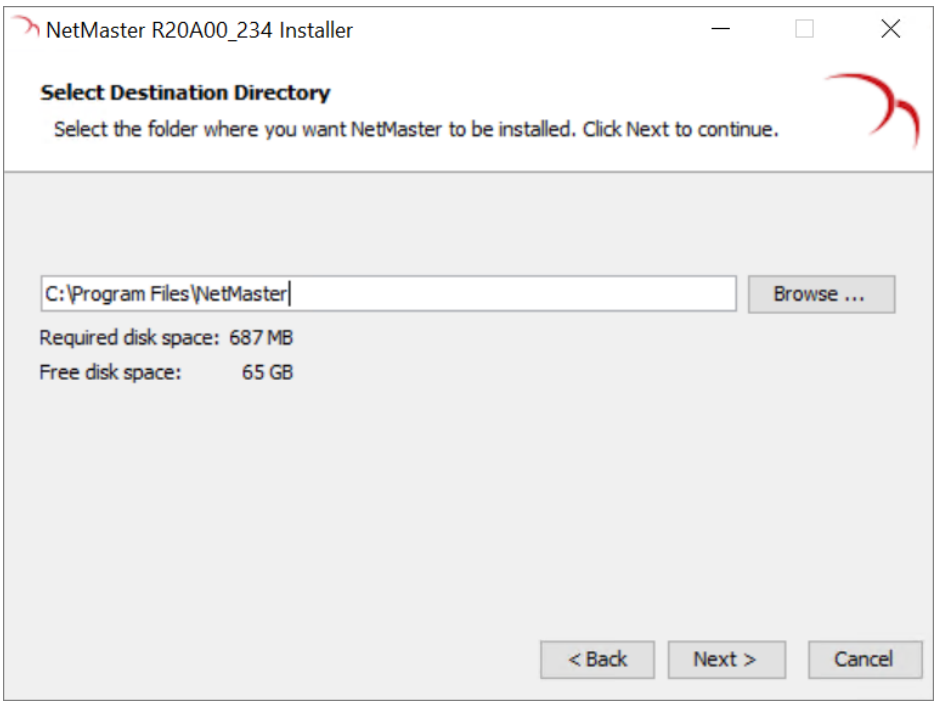
    There are three types of installations. Each type includes a different mix of

    - **Server Node** – Includes: CLI Reports, GUI Client, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch
    - **Client Node** – Includes: GUI Client, CLI Reports, PolyTopoImport
    - **Database Node** – Includes: System Manager, Elasticsearch



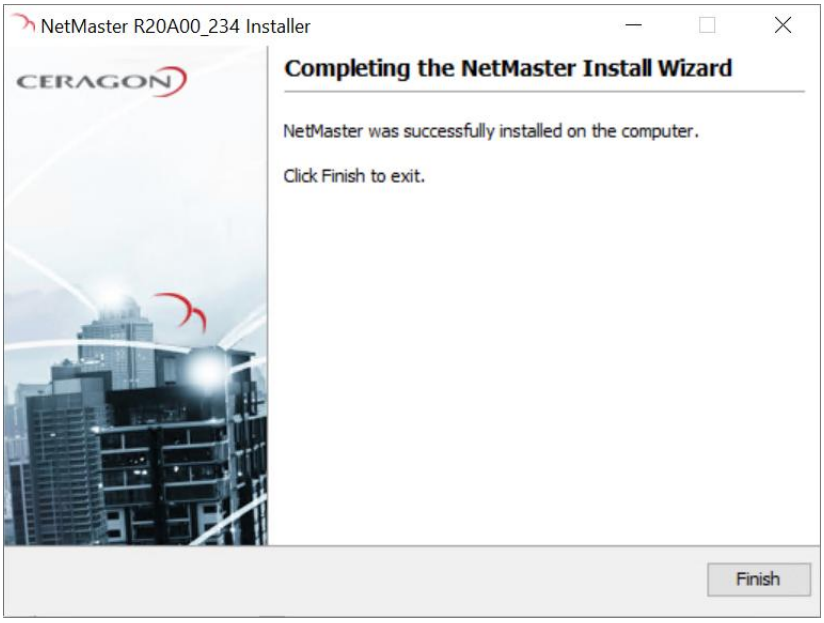
The Select Installation Directory page appears.

17. In the Select Installation Directory page, select the installation directory, and then click **Next**.

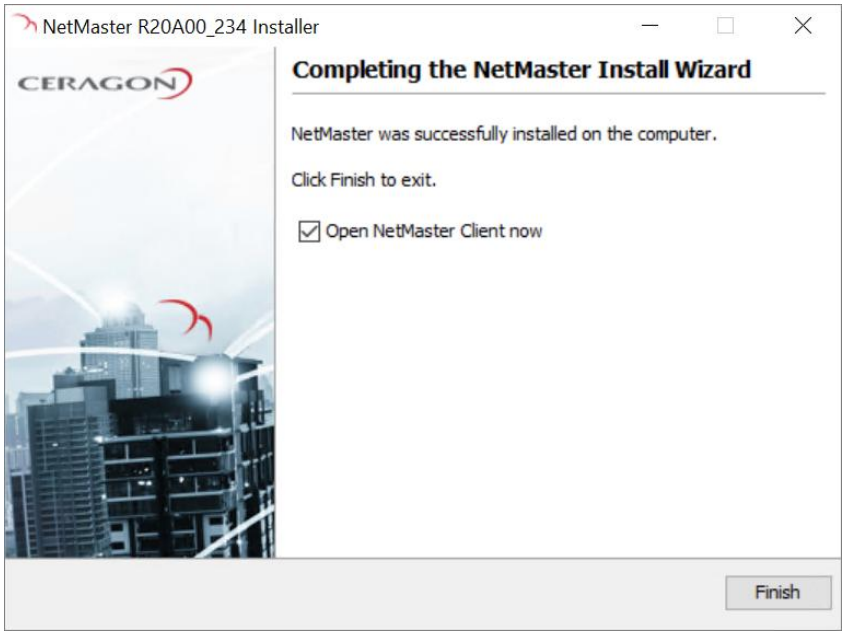


- PTP 820 NMS installation begins. A progress bar appears, and messages inform you that installation is in progress.
- When installation is complete, a Completing the PTP 820 NMS Install Wizard page appears, informing you that installation completed successfully.

18. If you are installing a **Database Node**, click **Finish**.

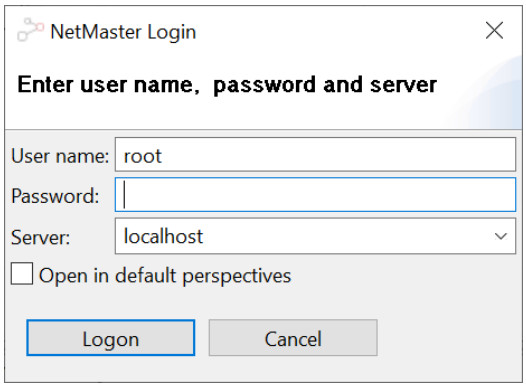


19. If you are installing a **Client Node**, an **Open PTP 820 NMS Client now** checkbox is by default selected.



If you leave **Open PTP 820 NMS Client now** selected, then upon clicking **Finish** the PTP 820 NMS Client application is launched, and a login window appears.

- Enter the initial authentication user credentials for a PTP 820 NMS Client administrator:
  Username: root
  Password: pw
- In **Server**, enter the IP address or network name of a PTP 820 NMS Server. You can enter **localhost** if the server is running on the same machine as the client.

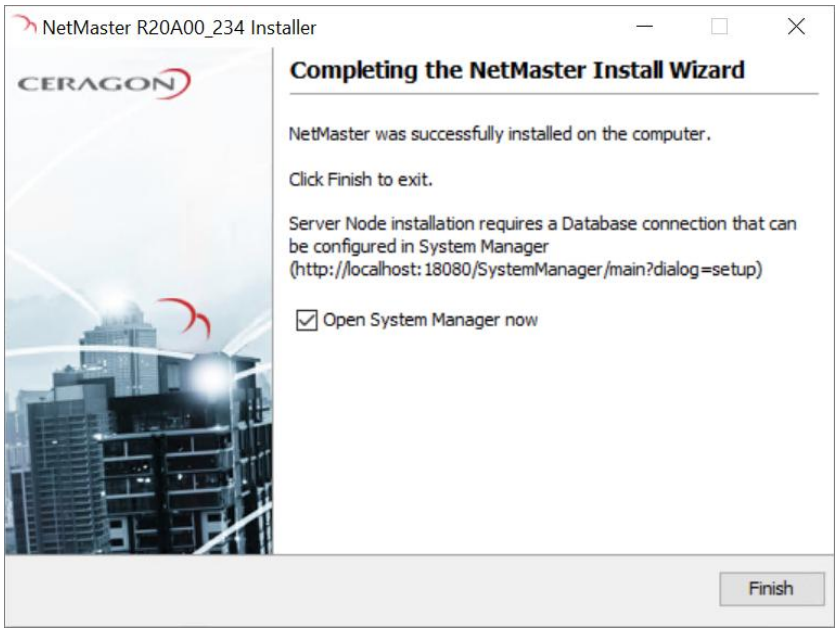


It is strongly recommended to change the password as soon as possible to prevent unauthorized access. You can do so in the **User Settings** Preference page of the PTP 820 NMS Client GUI.

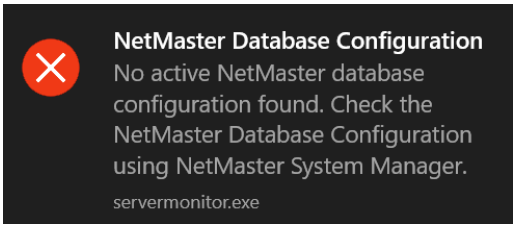
Note that you can launch the PTP 820 NMS Client anytime from:

C:\Program Files\PTP 820 NMS\GUI_client\Ngnms.exe, or from the shortcut accessible from the Start menu.

20. If you are installing a **Server Node**, an **Open System Manager now** checkbox is by default selected. Click **Finish**.

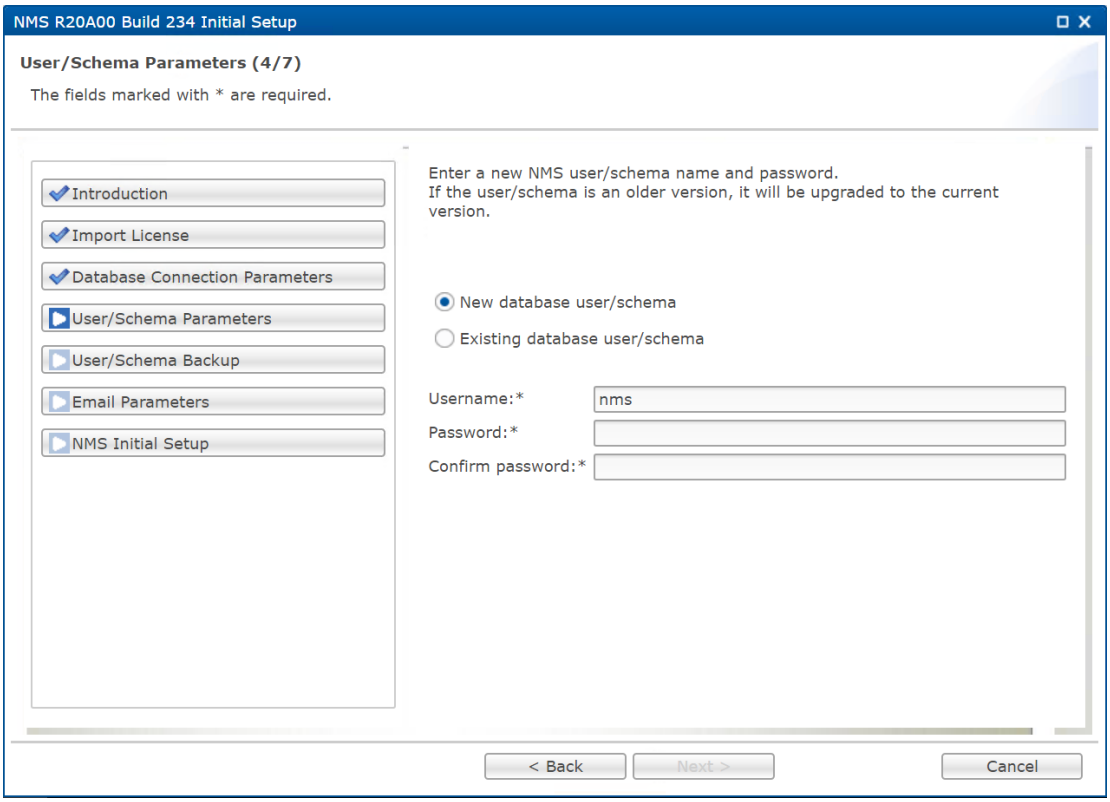


- First a message appears, informing you that no active PTP 820 NMS database configuration is found.



- Then System Manager is automatically launched so you can perform initial PTP 820 NMS Server setup.
  Follow the instructions in PTP 820 NMS Database and Cluster Configuration.

6. .
7. In System Manager, when the Initial Setup wizard is started, select **New database user/schema** and supply the credentials for that backed-up database. When you finish the wizard, do not start the server.



8. Perform Elasticsearch cluster configuration, as described in PTP 820 NMS Elasticsearch Cluster Configuration.
9. Use System Manager's **Restore User/Schema** wizard to restore from file the backup previously saved. When you finish the wizard, do not start the server.
10. Upgrade the schema from System Manager using the **Upgrade User/Schema** wizard. When specifying the database path you might need to change to the new version. Note that the **Database server address** must be an IPv4 address or IPv6 address or the machine hostname, and not **localhost** or **127.0.0.1** or **::1**.
    Note: Do not specify a mix of IPv4 and IPv6 addresses in System Manager. Use either only IPv4 or only IPv6 addresses.
11. Start the server.

Uninstall for Windows

To uninstall :

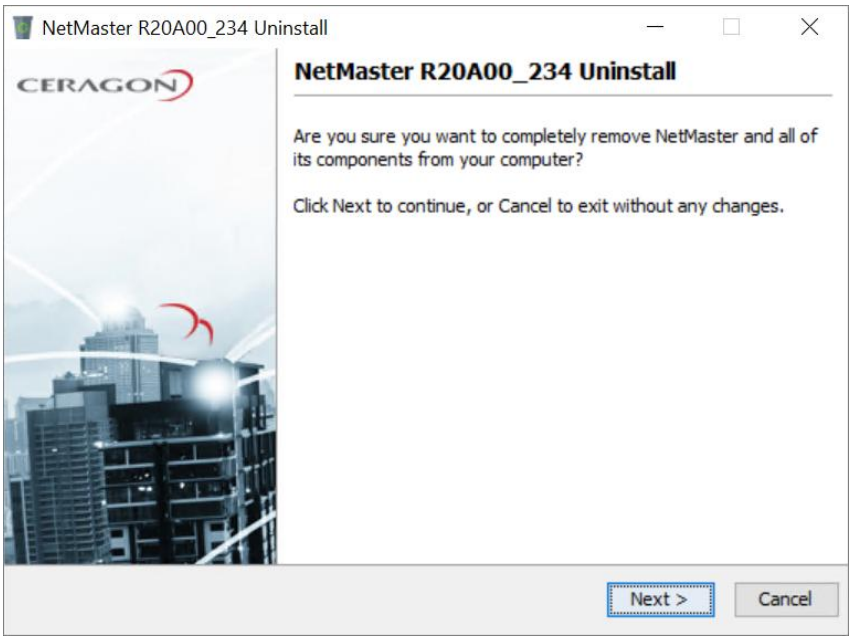
1. Uninstall PTP 820 NMS from the application, in either of the following ways:
   - Navigate to **Start** > **Settings**, search for **Apps & features**, select **PTP 820 NMS** in the list of apps, and click **Uninstall**.
   - Run the Uninstaller wizard as described in Running Windows Uninstaller Wizard.
2. Delete the PTP 820 NMS folder from the installation path (for example, C:\Program Files\PTP 820 NMS).
3. Delete the following folders from C:\Users\<domain_user>:

- .PTP 820 NMS Client
- .ngnms
- NgNMS

PTP 820 NMS Server Running Windows Uninstaller Wizard

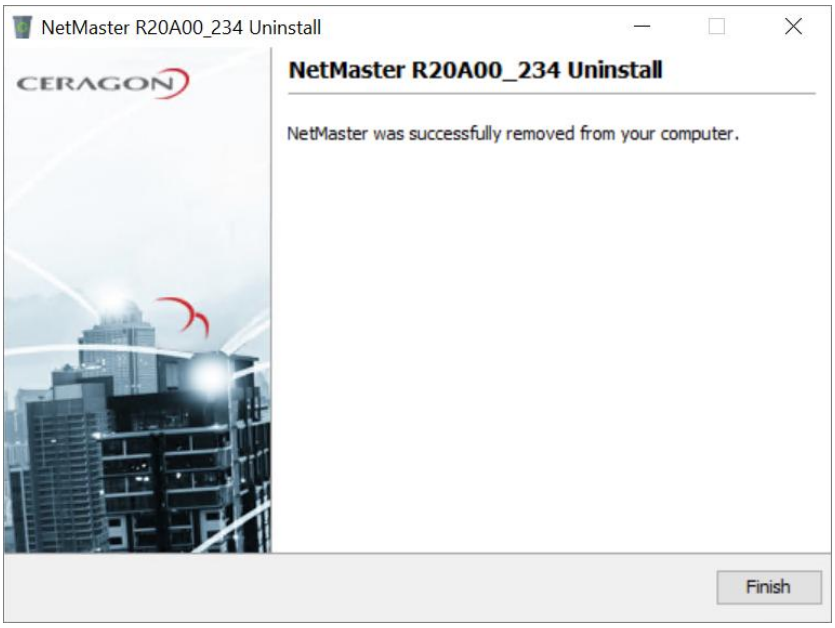
To run the Uninstaller wizard:

1. Run Uninstall_PTP 820 NMS.exe from the installation path (for example, C:\Program Files\PTP 820 NMS).
2. If a security warning appears, requesting permission to run the Uninstaller, click Yes.
3. The Uninstaller wizard appears, requesting uninstall confirmation. Click Next to confirm PTP 820 NMS removal.



A progress bar appears, reporting uninstall progress.

When uninstall is complete, a success message appears.



4. Click Finish to exit the PTP 820 NMS Uninstaller wizard.

Installation on Linux

PTP 820 NMS Server Pre-Installation for Linux

Server host name

The server host name should not contain '_' (underscore).

NetMaster Linux System Users

In the case of 1+1 HA and 2+2 HA deployments on Linux, the users under which NetMaster is installed, configured and run, must have the same username, user ID (UID) and group ID (GID) across all machines.

Region and Language requirements

The language of the operating system and database on which is installed must be English (United States).

Elasticsearch Folders

Make sure that Elasticsearch Folders are created as described in Creating Elasticsearch Folders.

Verify installation of required applications

Verify the **traceroute** and **systemctl** applications are installed, as follows:

1. Run the following command. If you receive an error, **traceroute** is not installed on the machine, so install the **traceroute** application.

traceroute -V

2. Run the following command. If you receive an error, **systemctl** is not installed on the machine, so install the **systemctl** application.

   systemctl –-version

Configure the Linux Server to work with both IPv4 and IPv6

1. Run the following command:

   grub2-editenv - list | grep kernelopt

   The output should be similar to the following:

   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap r d.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet ipv6.disable=1

2. Run the following command:

   grub2-editenv - set "<output>"

   where <output> is the output generated in the previous step, but without the last characters: ipv6.disable=1

3. Restart the Linux machine for the changes to be applied.

Install OpenJDK

1. Make sure you have internet access.
2. As root or sudo, run the following command, to list all the available Java packages:

   yum --showduplicates list java-1.8.0-openjdk

3. Install the required OpenJDK package, by running:

   yum install -y java-1.8.0-openjdk-1:1.8.0.242.b08-0.el8_1

4. Make sure the Java version is 1.8.0_242, by running the following command:

   $ java -version

   The output contains the version number, as follows:

   openjdk version "1.8.0_242"

   OpenJDK Runtime Environment (build 1.8.0_242-b08)

   OpenJDK 64-Bit Server VM (build 25.242-b08, mixed mode)

Set the Java Home variable

1. : Make sure you have internet access.
2. As root or sudo, run the following command, to list all the available Java packages:

   yum --showduplicates list java-1.8.0-openjdk

3. Install the required OpenJDK package, by running:

   yum install -y java-1.8.0-openjdk-1:1.8.0.322.b06-11.el8

4. Make sure the Java version is 1.8.0_242, by running the following command:

   $ java -version

The output should be:

openjdk version "1.8.0_242"

OpenJDK Runtime Environment (build 1.8.0_322-b06)

OpenJDK 64-Bit Server VM (build 25.322-b06, mixed mode)

5. Make sure the Java version is 1.8.0_322, by running the following command:

   $ java -version

   The output should be:

   openjdk version "1.8.0_322"

6. Find the folder where Java is installed, as follows:

   i. Run the following command:

      $ which java

      Suppose the output is:

      /usr/bin/java

   ii. Run the following command.

      $ ls -l /usr/bin/java

      Suppose the output is:

      /etc/alternatives/java

   iii. Run the following command.

      $ ls -l /etc/alternatives/java

      Suppose the output is:

      /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre/bin/java

      The folder where Java is installed (which we will set as the value of the NMS_JAVA_HOME_8 variable) is the final output, but without the last characters /bin/java:

      /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre

7. If you plan to run the PTP 820 NMS Installer as a root user, set the value of NMS_JAVA_HOME_8 as follows:

   i. Add to the file /root/.bashrc the following:

      export NMS_JAVA_HOME_8="/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre"

      where

      /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre

      is the folder where Java is installed, as discovered in (2)(iii).

   ii. For the change to take effect, either reopen the console or enter:

      source ~/.bashrc

   iii. Verify the variable is set by running the following, and verifying no error is received:

      printenv|grep java

1. If you plan to run the PTP 820 NMS Installer as a user with sudo permissions, you can do either of the following:

i. Add to the file /<sudo_user>/.bashrc the following:

export NMS_JAVA_HOME_8="/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre"

where

/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre

is the folder where Java is installed, as discovered in (2)(iii).

ii. For the change to take effect, either reopen the console or enter:

source ~/.bashrc

iii. Verify the variable is set by running the following, and verifying no error is received:

printenv|grep java

When executing the installer, follow the instructions in Execute the installer as sudo whose .bashrc includes NMS_JAVA_HOME_8

Specify the value of NMS_JAVA_HOME_8 when executing the installer , as described in Execute the installer as sudo and NMS_JAVA_HOME_8 defined at installation.
Note that if you choose this option, you will need to specify the value of NMS_JAVA_HOME_8 again upon each PTP 820 NMS uninstall and install. When executing the installer, follow the instructions.

Create a user to run PTP 820 NMS

On a Linux machine, installation must be performed by a root user or a user with sudo permissions, but PTP 820 NMS itself is run with a user whom you specify during installation.

The user who will run PTP 820 NMS must be created prior to PTP 820 NMS installation, as follows:

- Create a non-root user, and without a nologin option.
- Using a root user, execute the following command for the user who will run PTP 820 NMS:

  Loginctl enable-linger <user>

Configure PTP 820 NMS SNMP ports

PTP 820 NMS by default uses UDP port 162 to receive SNMP traps from the devices, and UDP port 161 to receive SNMP agent commands (if the Northbound interface SNMP Agent feature is enabled). However, Linux only permits a root user to listen to ports whose number is below 1024.

This poses a problem for PTP 820 NMS installations in which a non-root user runs PTP 820 NMS. In such a cases, you can either:

- Modify Linux settings to allow a non-root user to use ports 161 and 162.
  If you choose this option, do so prior to PTP 820 NMS Linux installation.
  Refer to Allowing non-root Linux user to use ports 161 and 162.
- Modify PTP 820 NMS to use ports higher than 1024.
  If you choose this option, do so after installing PTP 820 NMS.
  Refer to Changing UDP port 161 and UDP port 162.

Allowing non-root Linux user to use ports 161 and 162

To modify the Linux installation so that a non-root user can use ports 161 and 162, you need to set the capabilities of the JDK binary that executes PTP 820 NMS, by performing the following as root or sudo:

1. Run the following command to help you find the <absolute path to java>:
    1. Run the following command:

       $ which java

       Suppose the output is:

       /usr/bin/java
    2. Run the following command.

       $ ls -l /usr/bin/java

       Suppose the output is:

       /etc/alternatives/java
    3. Run the following command.

       $ ls -l /etc/alternatives/java

       The output is the absolute path to Java.
2. Suppose the absolute path to Java (that is, the output of Step (1) [iii]), is:

   /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre/bin/java

   Then run:

   etcap cap_net_bind_service+epi /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre/bin/java
3. Create a new file, as follows.

   touch /etc/ld.so.conf.d/java.conf

   Note: Make sure that the user who will run PTP 820 NMS has permission to read the folder: /etc/ld.so.conf.d
4. Search in the lib folder for a sub-folder with a processor name such as i386 or amd64 or another value depending on the machine used. Next, copy the path:

   /<absolute path to java>/jre/lib/<processor>/jli
5. Paste the path into the file you created in Step 3.
6. Reboot the machine.
7. Check that pathname from /etc/ld.so.conf.d/ was added to the trusted user path, by running:

   ldconfig -p | grep libjli

   The result should be similar to the following:

   libjli.so (libc6,x86-64) => /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre/lib/amd64/jli/libjli.so
8. Execute the following, and check that the version is shown:

   /<absolute path to java>/bin/java -version

Prepare Database

Server requires a database to work. Make sure that a database server is installed and reachable from the computer on which you want to install Server.

If the database server is running on a different computer than the Server, the firewall settings on the database server may have to be modified (i.e. open the port used for communication with the database server).

Supported databases are Oracle and PostgreSQL. See the System Requirements document for information about supported database editions.

Manage Maximum Number of Open Files on Linux

On a Linux system there are cases where the default number of files that a process can open, 1024, is not enough. In those cases, upon starting the process from systemctl the error “Too many open files” is received. To increase the number of files that a process can open:

1. Open the following file in a text editor:
   /etc/security/limits.conf
2. Add the following lines, then save and exit the file.
   <NMS_system_user> soft nofile 96000
   <NMS_system_user> hard nofile 96000
   <NMS_system_user> soft memlock unlimited
   <NMS_system_user> hard memlock unlimited
3. Open the following files in a text editor:
   /etc/systemd/user.conf
   /etc/systemd/system.conf
4. In both those files, add (or edit) the following lines, then save and exit the files.
   DefaultLimitNOFILE=65535
   DefaultLimitMEMLOCK=infinity
5. Open the following file in a text editor:
   /etc/sysctl.conf
6. Add (or edit) the following line, then save and exit the file.
   vm.max_map_count=262144

PTP 820 NMS Install Sets for Linux

This section guides you through installation on a Linux platform.

That the Client must be installed on a Windows platform, see PTP 820 NMS installation for Windows installation for Windows for details.

Note: This section requires that the steps for Pre Installation for Linux already have been completed.

PTP 820 NMS Installation Packages for Linux

The available Linux installation packages include:

Install Package	Package Contents
Server Node	CLI Reports, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch
Database Node	System Manager, Elasticsearch

Install Sets

Component	Explanation
CLI Reports	Generates reports executed by a CLI command.
PTP 820 NMS Server	Server application.
Northbound SNMP	Northbound interface to higher-order network management systems.
PolyTopoImport	PolyView Topology Importer. Enables exporting discovered elements and subnetworks from PolyView NMS into a file and then importing them, while preserving their hierarchy, into as managed elements in administrative domains.
System Manager	Database configuration and maintenance tool. System Manager is part of every PTP 820 NMS Server installation. It is recommended to install System Manager also on the database server in order to enable automatic backup and restore of the PTP 820 NMS Database.
Elasticsearch	A complementary database in which PTP 820 NMS stores large volumes of data such as Performance Measurements (KPIs) collected from devices.

Install Modes

There are two possible modes of installation:

- New Installation
- Upgrade Installation

New PTP 820 NMS Installation for Linux

Executing the installer

You can execute the installer in any of the following ways:

- Execute the installer as root

- Execute the installer as sudo whose .bashrc includes NMS_JAVA_HOME_8
- Execute the installer as sudo and NMS_JAVA_HOME_8 defined at installation

Note: The sudo user executing installation must have execute rights on the Java folder set in NMS_JAVA_HOME_8.

Execute the installer as root

1. Unpack the installer PTP 820 NMS-sol_R****.PTP 820 NMS_<major version number>_<minor version number>_linux.zip to a temporary folder and do the following:extract the .sh file.
2. Give the installer execution right by running:

   chmod +x <installer name>
3. Run the following command:

   ./PTP 820 NMS_<major version number>_<minor version number>_linux.sh

   A message appears, informing you the install wizard is being prepared. Follow the instructions in Running the installer for Linux.

Execute the installer as sudo whose .bashrc includes NMS_JAVA_HOME_8

1. Unpack the installer PTP 820 NMS_<major version number>_<minor version number>_linux.zip to extract the .sh file.
2. Run the following command:

   sudo chmod +x <installer name>
3. Run the following command:

   sudo -E <pathToInstaller>./PTP 820 NMS_<major version number>_<minor version number>_linux.sh

   where <pathToInstaller> is the path where the PTP 820 NMS Installer for Linux is located.

   A message appears, informing you the install wizard is being prepared. Follow the instructions in Running the installer for Linux.

Execute the installer as sudo and NMS_JAVA_HOME_8 defined at installation

1. Unpack the installer PTP 820 NMS_<major version number>_<minor version number>_linux.zip to extract the .sh file.
2. Run the following command:

   sudo chmod +x <installer name>
3. Run the following command:

   sudo NMS_JAVA_HOME_8="/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el8_1.x86_64/jre" <pathToInstaller>./PTP 820 NMS_<major version number>_<minor version number>_linux.sh

   where <pathToInstaller> is the path where the PTP 820 NMS Installer for Linux is located.

   A message appears, informing you the install wizard is being prepared. Follow the instructions in Running the installer for Linux.

Running the installer for Linux

On the Linux machine:

1. In the command prompt, type:

   ./PTP 820 NMS_R20B00_1_linux.sh

2. Type o and press the Enter key.

```
root@d:/tmp# ./NetMaster_R20B00_537_linux.sh
Starting Installer ...
This will install NetMaster on your computer.
OK [o, Enter], Cancel [c]
```

3. The License Agreement is shown. If you accept the agreement, press the Enter key until I accept the agreement is shown, then type 1 and press Enter.

```
I accept the agreement
Yes [1], No [2]
1
```

4. Select the type of installation you want to perform, and press Enter.

   There are three type of installations. Each type includes a different mix of components. The types and their components are:

   - Server Node – Includes: CLI Reports, GUI Client, Northbound SNMP, PolyTopoImport, PTP 820 NMS Server, System Manager, Elasticsearch
   - Client Node – Includes: GUI Client, CLI Reports, PolyTopoImport
   - Database Node – Includes: System Manager, Elasticsearch

```
Select the type of installation you want to perform.
Server Node [1, Enter]
Client Node [2]
Database Node [3]
1
```

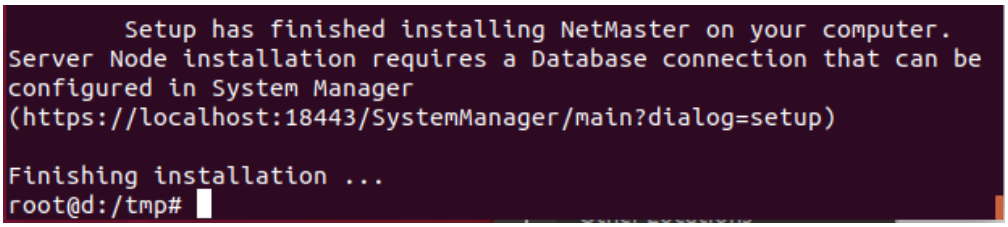
5. Select the user predefined in Create a user to run and press Enter.
   In the example shown below, user ‘d’ was previously created.

```
Select the user to be used for running NMS server.
d [1, Enter]
gdm [2]
gnome-initial-setup [3]
hplip [4]
speech-dispatcher [5]
sync [6]
tomcat [7]
vboxadd [8]
whoopsie [9]
1
```

6. Specify the folder where you want PTP 820 NMS to be installed. Press Enter to accept the recommended folder, or type another location and press Enter.

```
Specify the folder where you want NetMaster to be installed. Press
Enter if default folder is ok.
[/opt/NetMaster]
/usr/NetMaster
```

7. PTP 820 NMS installation begins. Wait until Finishing installation ... appears and the prompt is returned.



PTP 820 NMS installation is completed. To continue with the initial configuration of the PTP 820 NMS Server, follow the instructions in PTP 820 NMS Database and Cluster Configuration.

Upgrade PTP 820 NMS Installation for Linux

Before upgrading in Linux

- Make sure you install the Java version mentioned in the Java Installation sub-section of the PTP 820 NMS Server Pre-Installation for Linux section.
- Make sure that Elasticsearch folders exist, as described in Creating Elasticsearch Folders.
- All services must be stopped before installing the new version. This includes the Server, the System Manager, the SNMP Agent and the PTP 820 NMS Elasticsearch service.
- From R24B10, legacy devices are no longer supported by NetMaster except as OpenSNMP devices (see the NetMaster Release Notes for the full list of legacy devices). If you are managing legacy devices and wish to upgrade to R24B10 or above, you must unmanage the legacy devices prior to upgrading, and after upgrade is complete you can re-manage the legacy devices as OpenSNMP devices.

Upgrade Notes Related to R23A00 and Above

A change password wizard is triggered upon first login to System Manager following upgrade from a release earlier than R23A00.

Upgrade Notes Related to R23B00 and Above

Starting with R23B00, the parent node under which the following folders are located, is by default <same level as NetMaster installation folder>/NgNMS for Linux:

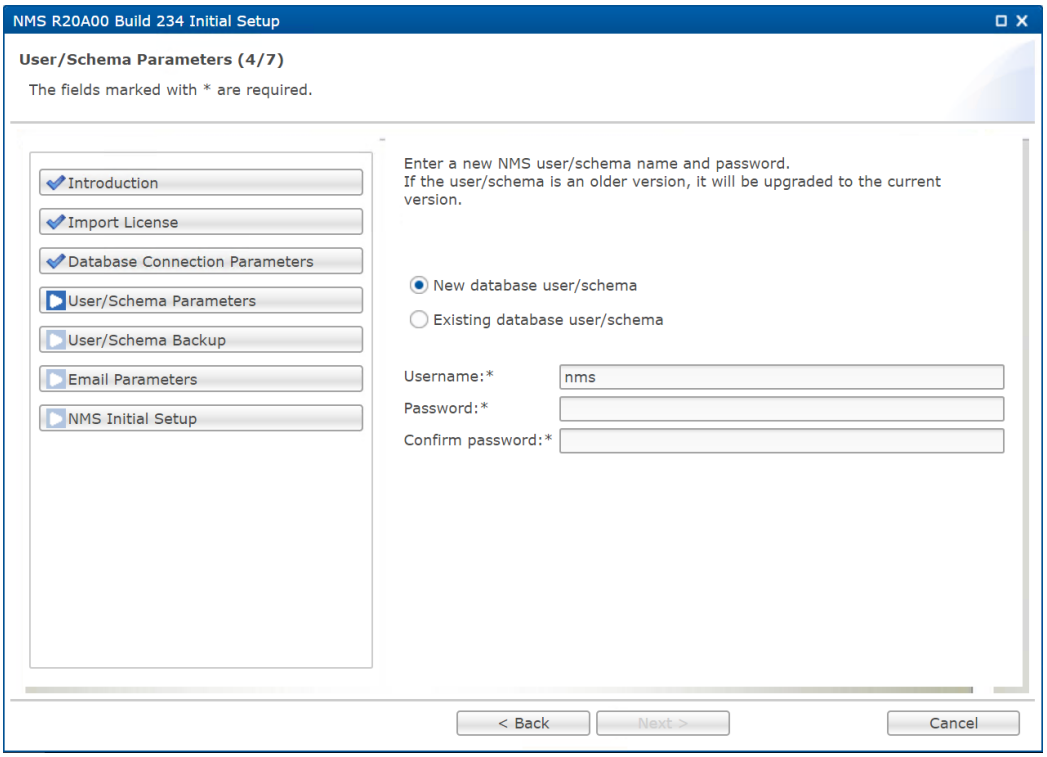
- Scheduled reports. These are saved in the <folder_location>\reports folder
- Configuration files – Device configuration backups, stored in <IP-address-of-element> subfolders of the <folder_location>\BackupConfigurations folder
- Element Software files – Device software images, stored each in its own subfolder under the <folder_location>\SoftwareImages folder

Performing an upgrade in Linux

Perform the following:

1. Back up the active schema using System Manager, and store it in a different location. Store also the current database credentials.

2. Back up all the NetMaster file folders (scheduled reports folder, configuration backup files, element software files).
3. Uninstall the old version.
4. Make sure you comply with the Prerequisites in NetMaster Server Pre-Installation for Linux.
5. Install the new version as described in New NetMaster Installation for Linux.
6. In System Manager, when the Initial Setup wizard is started, select **New database user/schema** and supply the credentials for that backed-up database. When you finish the wizard, do not start the server.



7. Perform Elasticsearch cluster configuration, as described in PTP 820 NMS Elasticsearch Cluster Configuration.
8. Use System Manager's **Restore User/Schema** wizard to restore from file the backup previously saved. When you finish the wizard, do not start the server.
9. Upgrade the schema from System Manager using the **Upgrade User/Schema** wizard. When specifying the database path you might need to change to the new version. Note that the **Database server address** must be an IPv4 address or IPv6 address or the machine hostname, and not **localhost** or **127.0.0.1** or **::1**.
   Note: Do not specify a mix of IPv4 and IPv6 addresses in System Manager. Use either only IPv4 or only IPv6 addresses.
10. Start the server.

Uninstall PTP 820 NMS for Linux

On the Linux machine, perform the following as root or sudo:

1. Give the uninstaller execution rights by running:

chmod +x /<install_path>/Uninstall_PTP 820 NMS

2. Run uninstaller:

   ./<install_path>/Uninstall_PTP 820 NMS

3. When prompted, confirm the uninstall.

PTP 820 NMS Database and Cluster Configuration

Immediately upon completing a new PTP 820 NMS Server Node installation (whether on Windows or Linux), perform initial setup of the SQL database and ES cluster, as described in:

- PTP 820 NMS Initial SQL Database Setup
- PTP 820 NMS Elasticsearch Cluster Configuration

PTP 820 NMS Initial SQL Database Setup

Following a new PTP 820 NMS Server Node installation (whether on Windows or Linux) perform initial setup of the SQL database as described in this section.

If you are setting up a High Availability setup, refer to PTP 820 NMS Initial SQL Database Setup.

1. In a Windows installation, System Manager launches automatically following installation. In a Linux installation, launch it manually by navigating to:

   https://<PTP 820 NMS Server address>:18443/SystemManager/main?dialog=setup

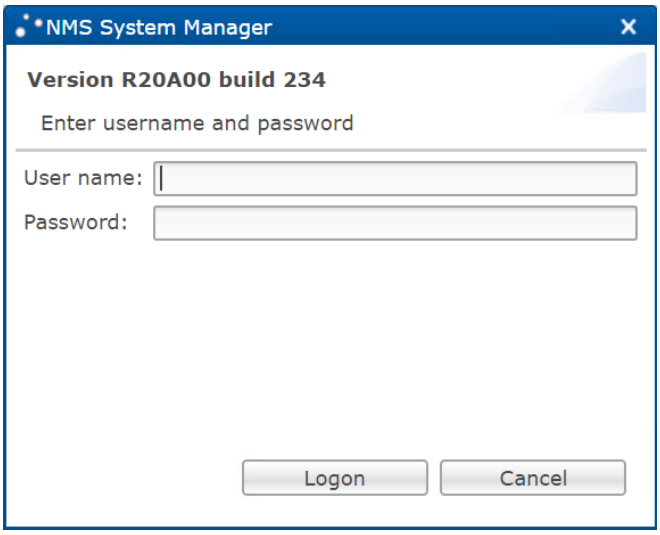
   where <PTP 820 NMS server Server address> is the address of the server on which PTP 820 NMS Server is running.

2. In the System Manager login dialog, enter the default root user credentials:

   Username: root

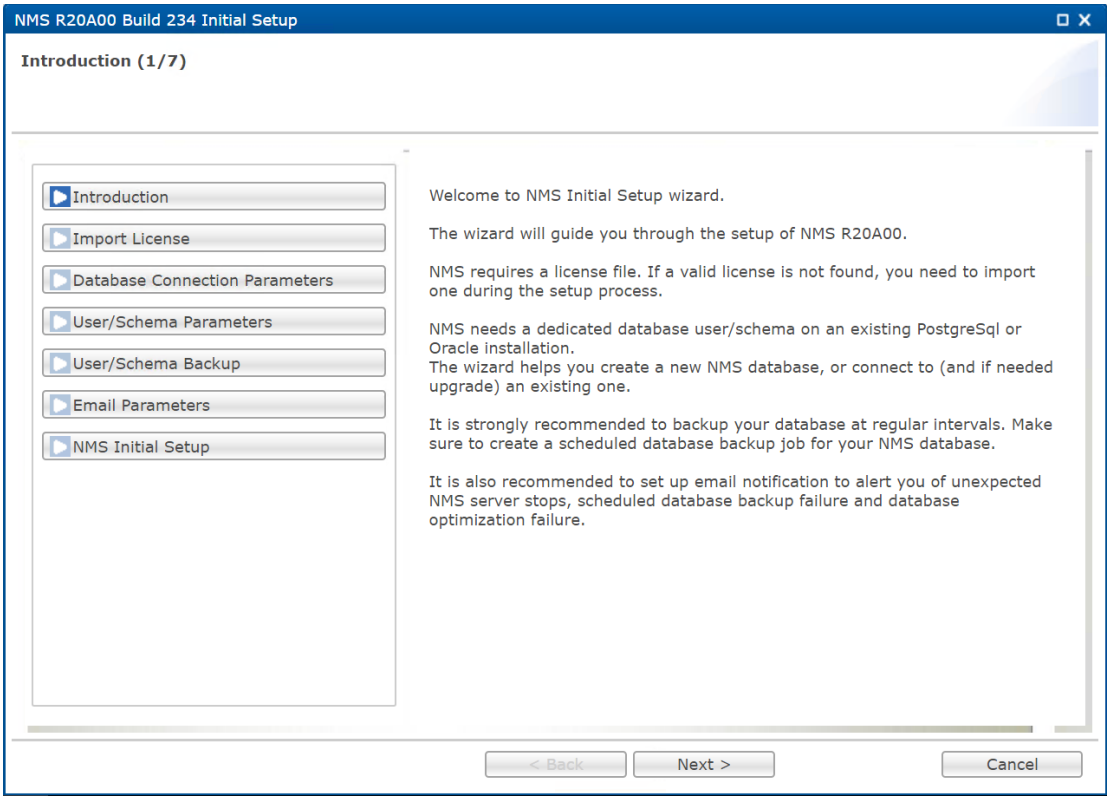
   Password: pw

   Upon first login following NetMaster installation or an upgrade from a release earlier than R23A00, a Change Password wizard appears for selecting a new password. Enter a password that complies with the following requirements: a minimum of 8 characters, of which at least one must be an uppercase letter, at least one must be a lowercase later, at least one must be a numeric character, and at least one must be a special character; the password may not contain the username; and the password may not be identical to the current password.



The NMS Initial Setup wizard appears, displaying the Introduction page.

3. In the Introduction page that appears, click Next.



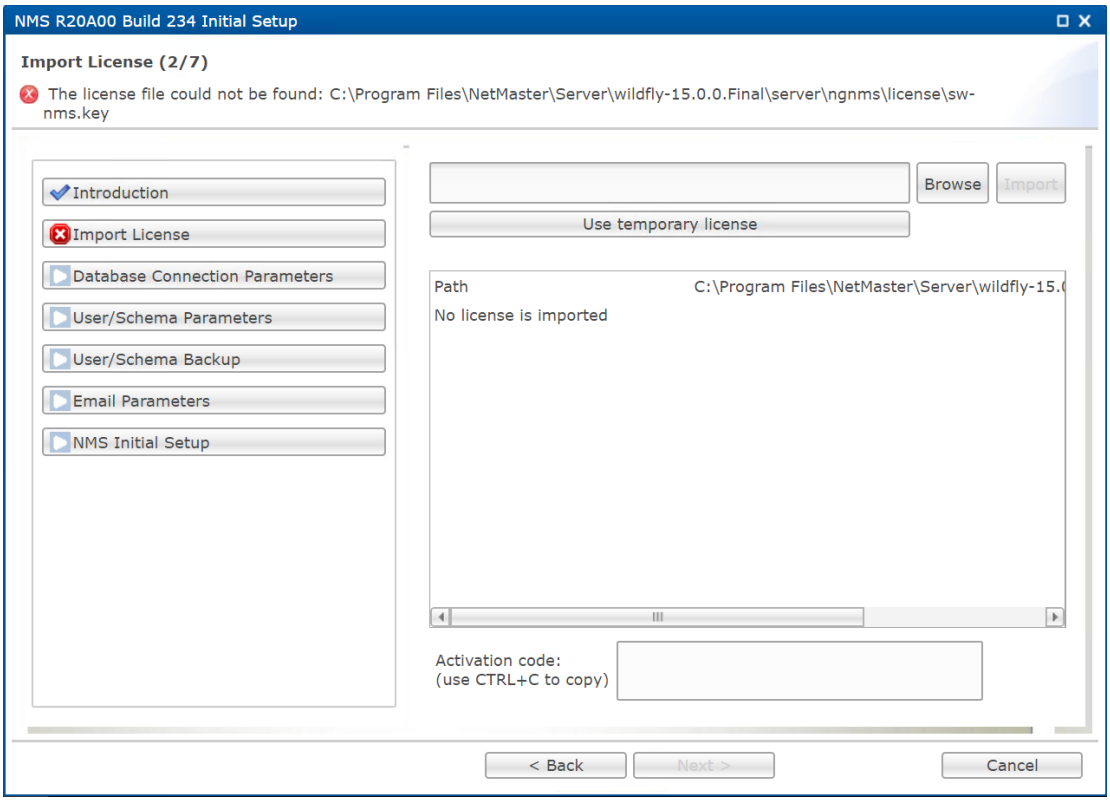
The Import License page appears.

4. In the Import License page that appears:

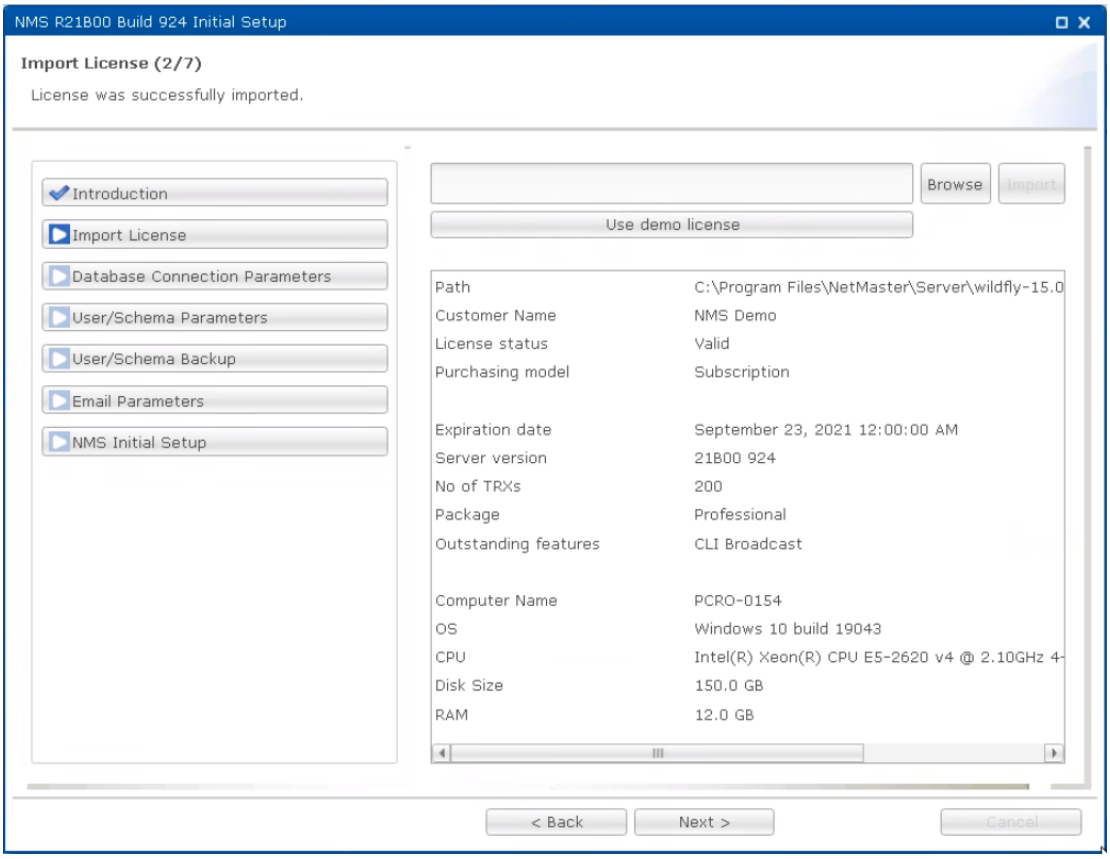
   i. Click Use Temporary License to load the temporary license file provided with the installation.

      In order to run PTP 820 NMS, it is necessary to have a license. For new installations, a temporary license file is provided with the installation.

The temporary license is valid for 30 days. During that time, contact Customer Support to obtain a permanent license.



The license details appear.



Click Next.

4. In the Database Connection Parameters page that appears, specify the details for connecting to a dedicated SQL database user/schema.

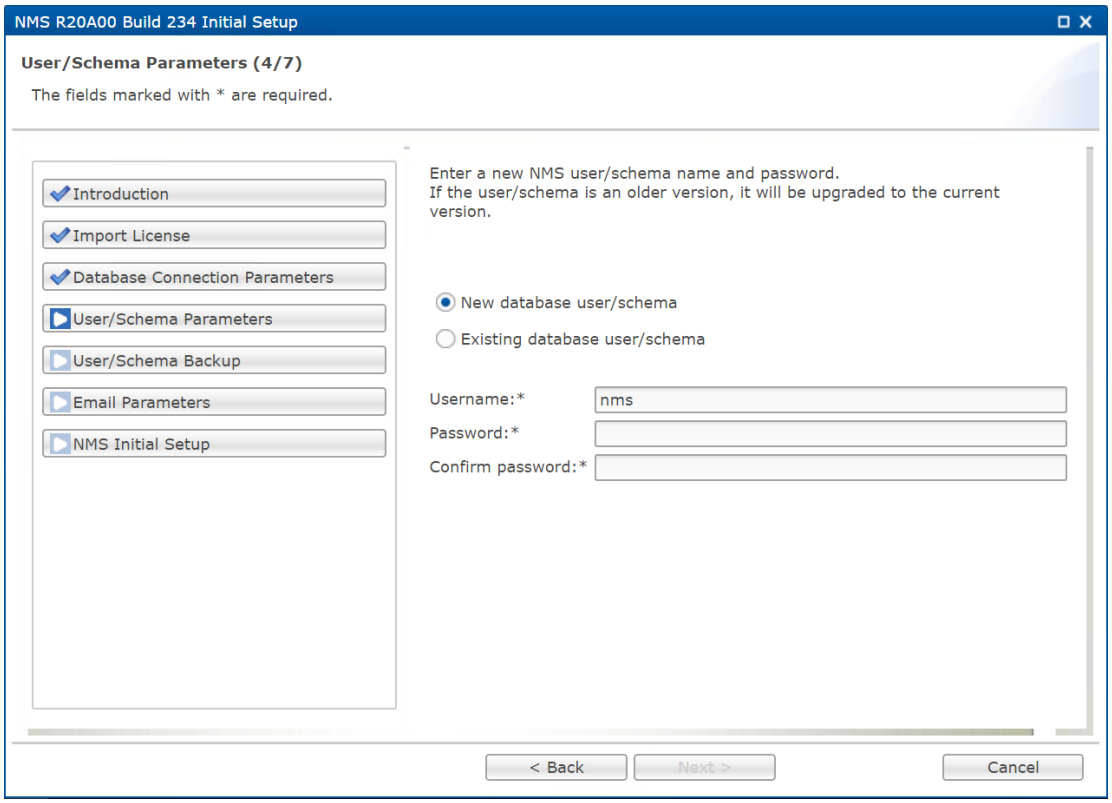
   Specify the following parameters:

Name	Explanation
Database instance name	Name of a database instance.
Database type	Either Oracle or PostgreSQL.
Database server address	IPv4 address or machine hostname of the database server, which can be reached by a remote connection. Note that the Loopback IP address (127.0.0.1) and 'localhost' are not allowed. **Note**: Do not specify a mix of IPv4 and IPv6 addresses in System Manager. Use either only IPv4 or only IPv6 addresses.
Database server port	TCP port for the database. Default value is 1521 for Oracle, 5432 for Postgres.
Username	The database system user needed to create the user/schema.

Password	Password for the database system user.

Click Next.

5. In the User/Schema Parameters page that appears, specify an Oracle or Postgres user/schema for .



Click Next.

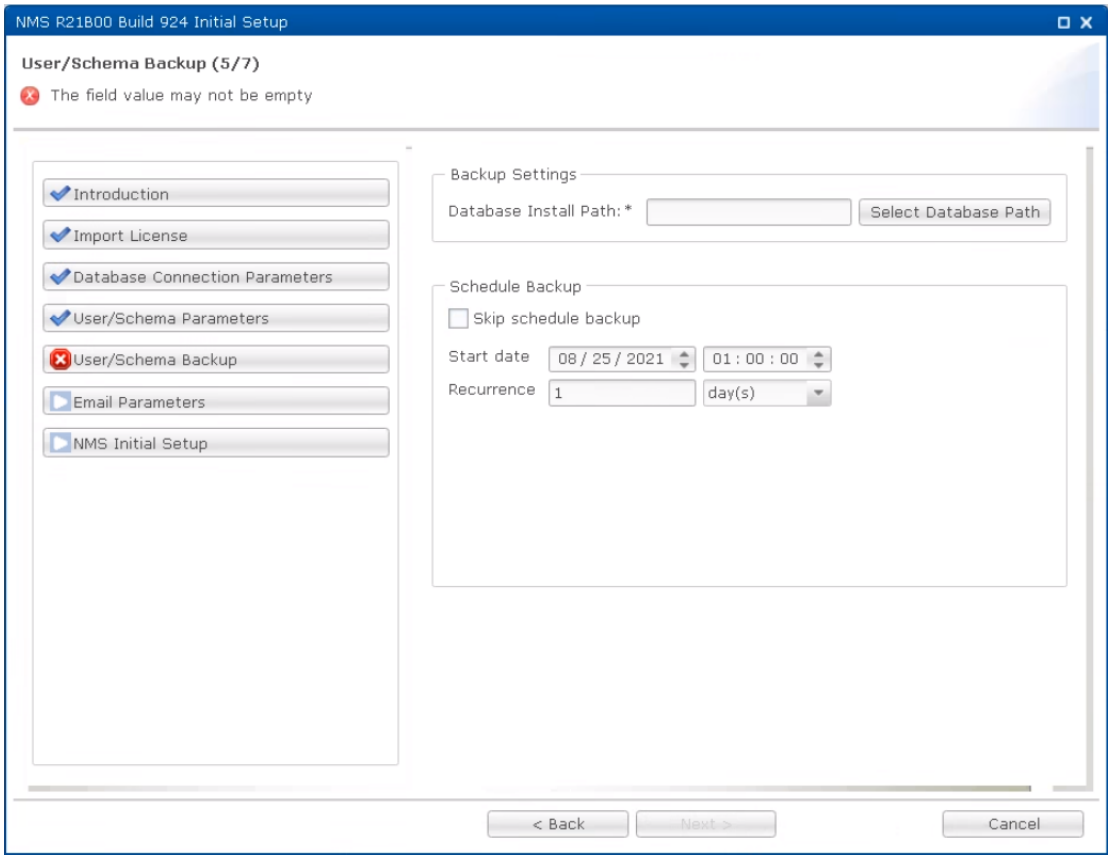
6. In the User/Schema Backup page that appears you can configure periodic backup of the PTP 820 NMS SQL database. That is the recommended option.

   The Database Install Path is the database server path to the tools that System Manager needs in order to run backup and restore operations. The tools in question are exp.exe and imp.exe for Oracle and pg_dump and pg_restore for Postgres.

- Click Select Database Path to allow System Manager to try to find the Database Install Path automatically:
- If System Manager fails to locate the correct path for you, you must supply the correct path yourself.
- You can check the Skip schedule backup check box if you don't want to set up periodic backup. You can schedule periodic backup later if desired by using the Backup Active User/Schema or Backup User/Schema wizards.
- To initiate periodic backup, leave the Skip schedule backup checkbox unchecked and adjust the start time and backup interval as desired. The backup files are zipped to reduce disk space consumption, but you should make sure to select a file system with enough free disk space to hold the backup files.

- You can change the backup file storage location on the server. It is also possible to configure the number of days to keep the scheduled database backups. Both settings are found in the Settings > Database view in System Manager.
- If periodic backup is enabled, it is recommended to also enable deletion of old backup files to prevent the file system from filling up.

User/schema backups are stored on the PTP 820 NMS Server machine. In a 1+1 High Availability or 2+2 High Availability setup, the Primary PTP 820 NMS Server will have its own backup and the Secondary PTP 820 NMS Server will have its own backup.



7. In the Email Parameters page you can set up System Manager to send email notification in case of:

- Periodic backup failure
- PTP 820 NMS server unexpected shutdown
- Database optimization failure

  In order to make use of the email notification feature, you need an SMTP server in your network.

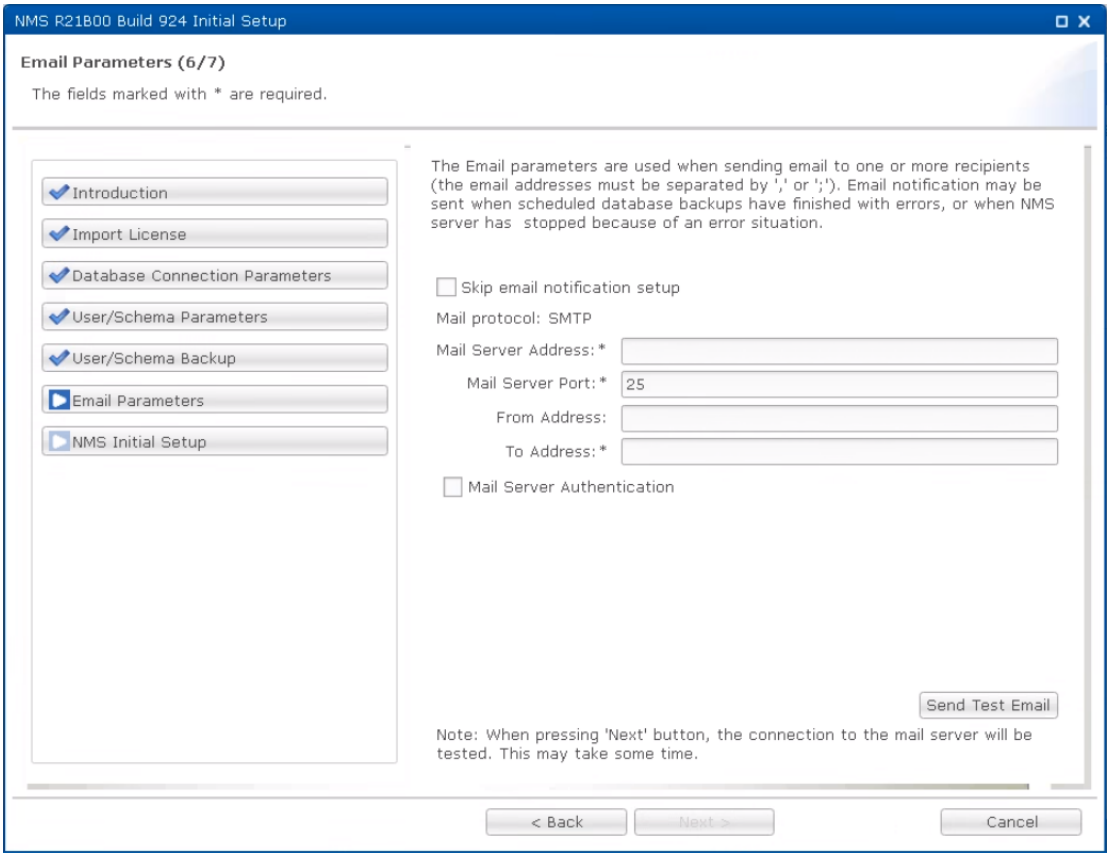
  If you don't want to make use of the email notification feature, you can check the Skip email notification setup check box.

  If you want email notification, you need to fill in the following settings:

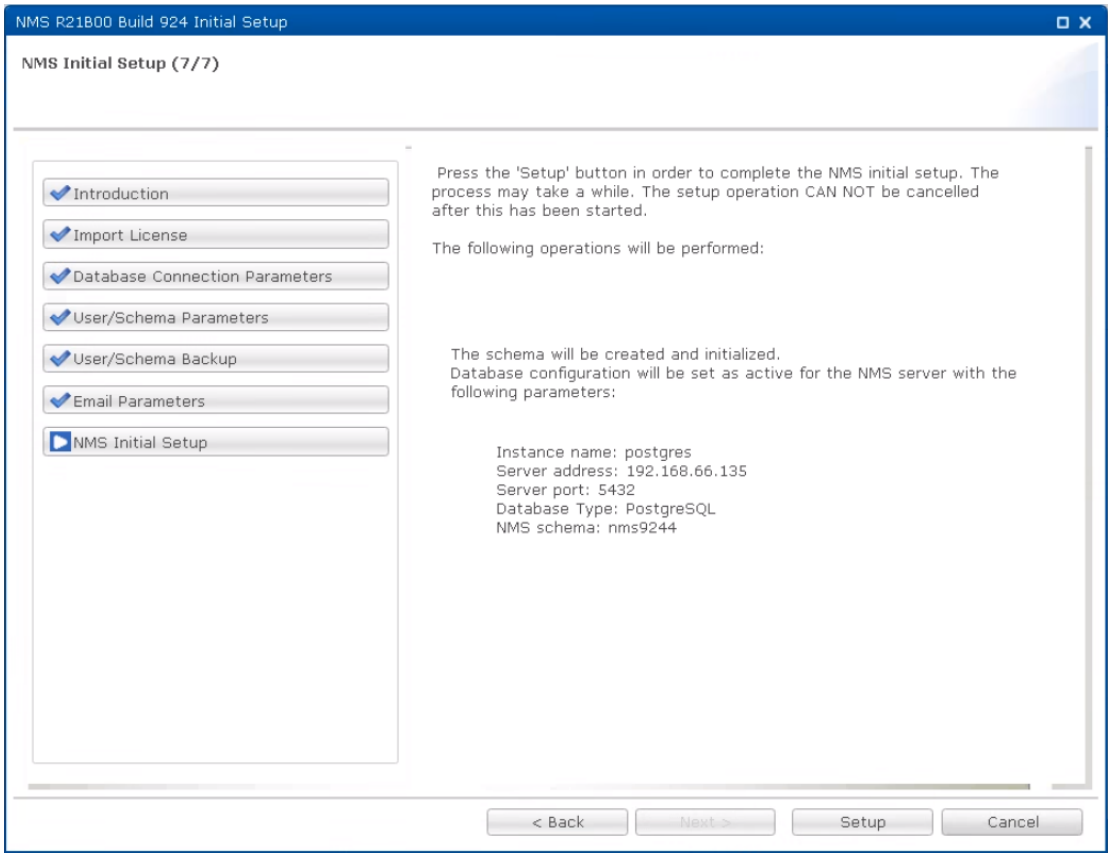
Name	Explanation
Mail Server Address	IPv4 address or machine hostname of your SMTP server.

Mail Server Port	SMTP port on your mail server. Default is 25.
From Address	The email address that will appear as the email sender. Be aware that no validation is performed whether this is a real email address or not.
To Address	Email recipient. May be a list of email addresses, separated by comma or semicolon.
Username	Username for Mail Server Authentication.
Password	Password for Mail Server Authentication.

Click Send Test Email to send a test email to verify that the email notification settings are correct.



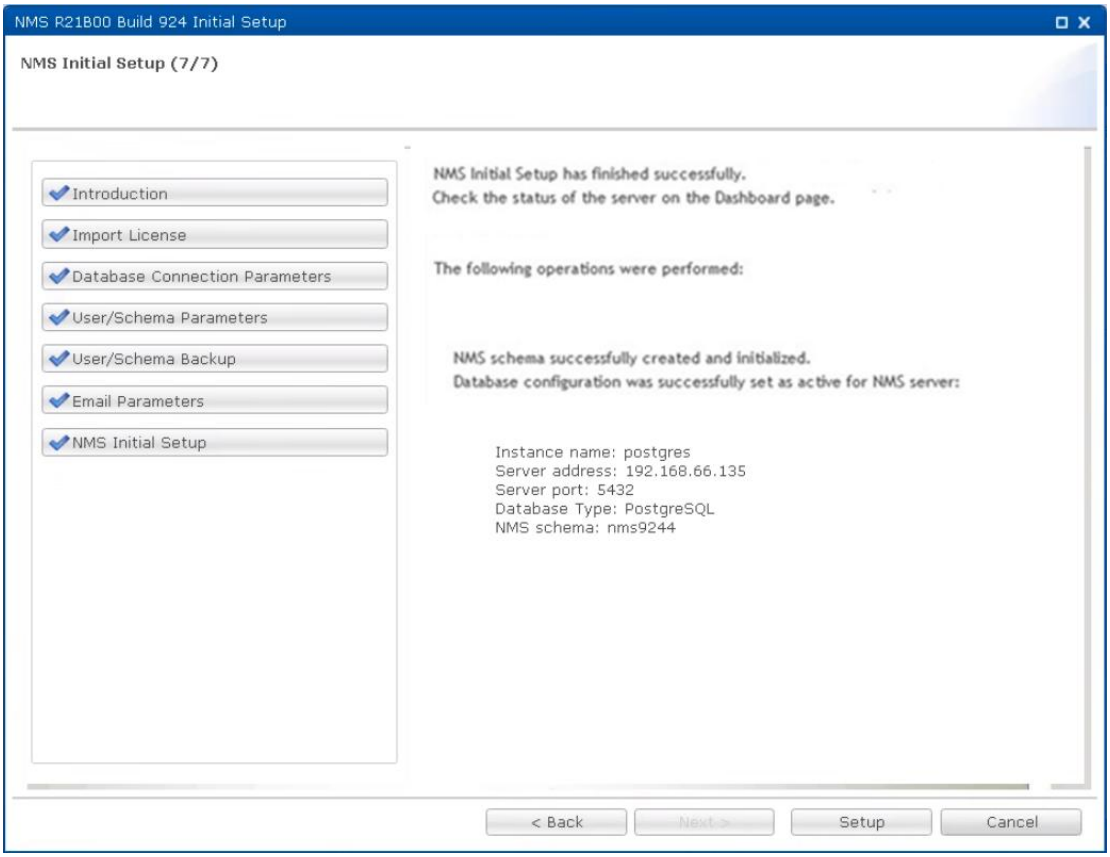
8. In the NMS Initial Setup page, review the operation list summary. Click Setup to initiate the setup process



A message appears, informing that setup is in process.

9. When setup is complete, a success message appears.

   Click Close to complete the PTP 820 NMS Initial Setup wizard.



You now need to perform Cluster Configuration in the System Manager's Dashboard view. Follow the instructions in PTP 820 NMS Elasticsearch Cluster Configuration.

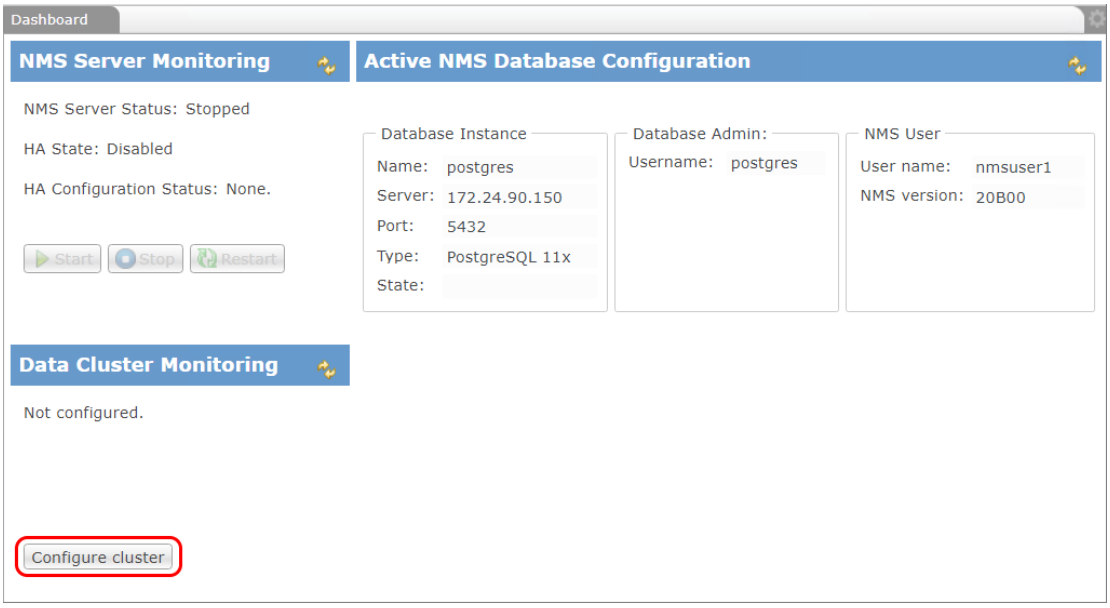
However, if you are configuring a high-availability setup, first complete PTP 820 NMS Server High Availability Setup configuration before configuring the Elasticsearch cluster.

PTP 820 NMS Elasticsearch Cluster Configuration

Following PTP 820 NMS Initial SQL Database Setup, you need to perform Elasticsearch cluster configuration. This must be done before you can start PTP 820 NMS.

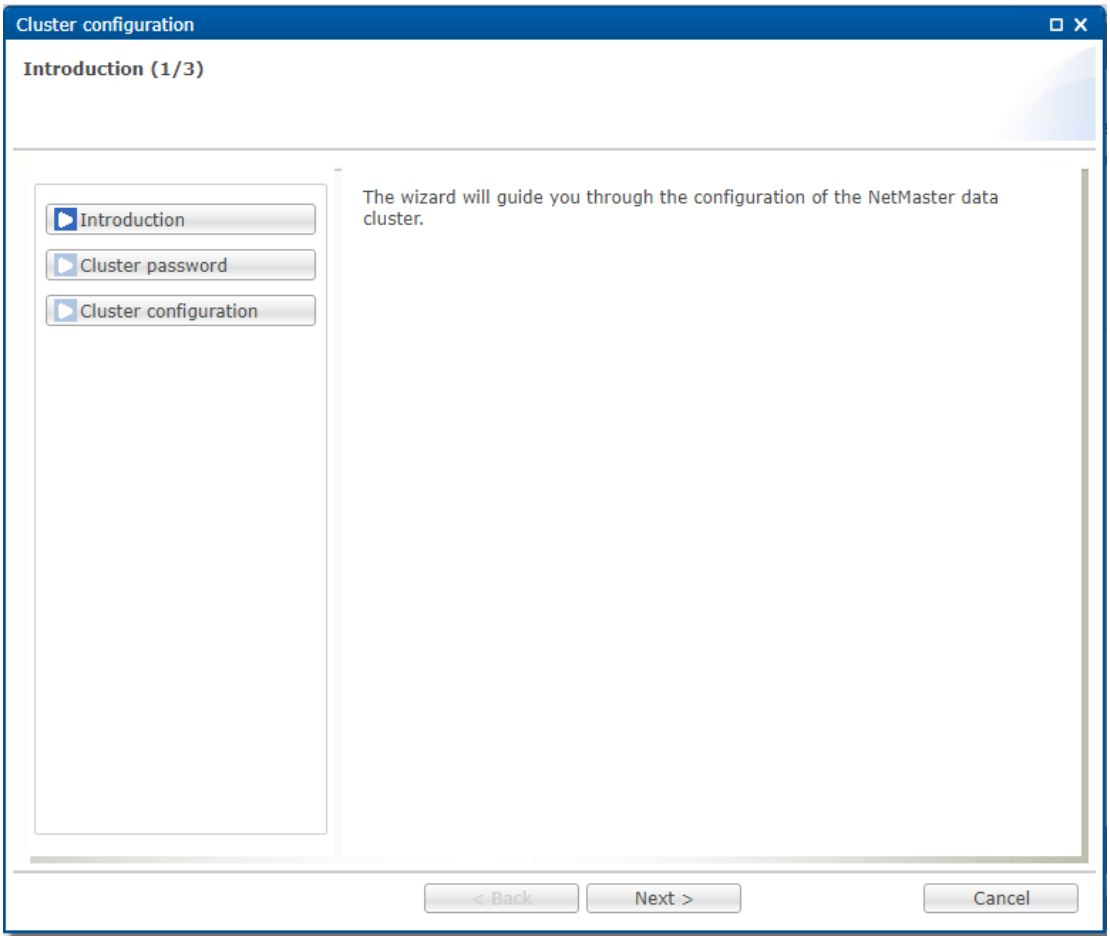
If you are configuring a high-availability setup, first complete PTP 820 NMS Server High Availability Setup configuration before configuring the Elasticsearch cluster.

1. In the System Manager Dashboard view, click Configure cluster.



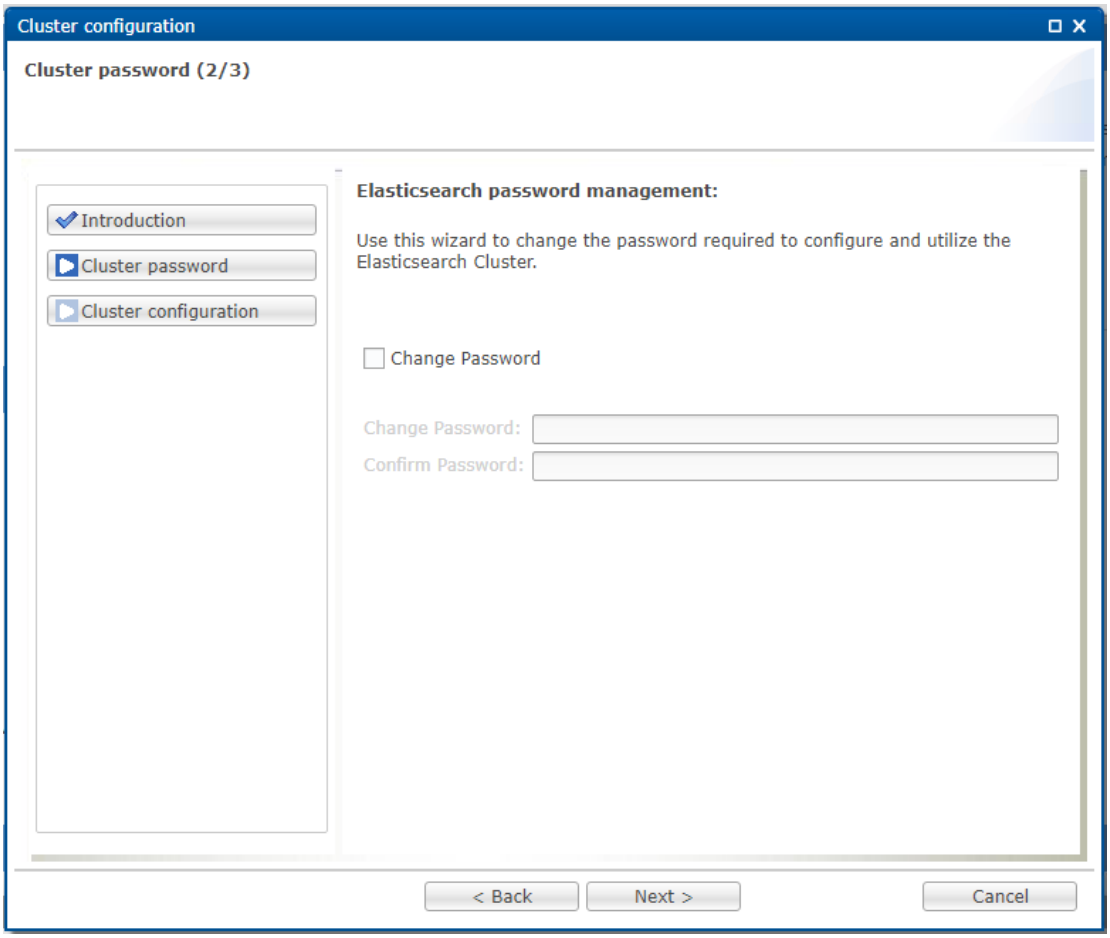
The Cluster Configuration wizard appears, displaying the Introduction page.

2. In the Introduction page, click Next.



The Cluster password page appears.

3. In the Cluster Password page, check Change Password if you want to change the default password used to connect to the Elasticsearch cluster.
   The default password is: pw
   If you do not want to change the password, leave the option unchecked and click Next.



   The Cluster Configuration page appears, listing the Elasticsearch cluster nodes that PTP 820 NMS automatically detected.

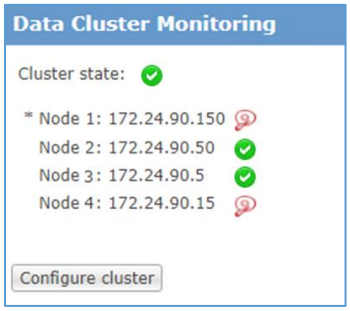
4. In the Cluster Configuration page, perform the following and then click Configure:
   - In Data Path, enter the local folder you created in Creating Elasticsearch Folders.
   - In Snapshot Repository Path, enter the repository path you created in Creating Elasticsearch Folders. Enter the path in a syntax that can be used identically by all machines participating in the PTP 820 NMS setup. For example: \\fsro1\NMS\ES_Repo.

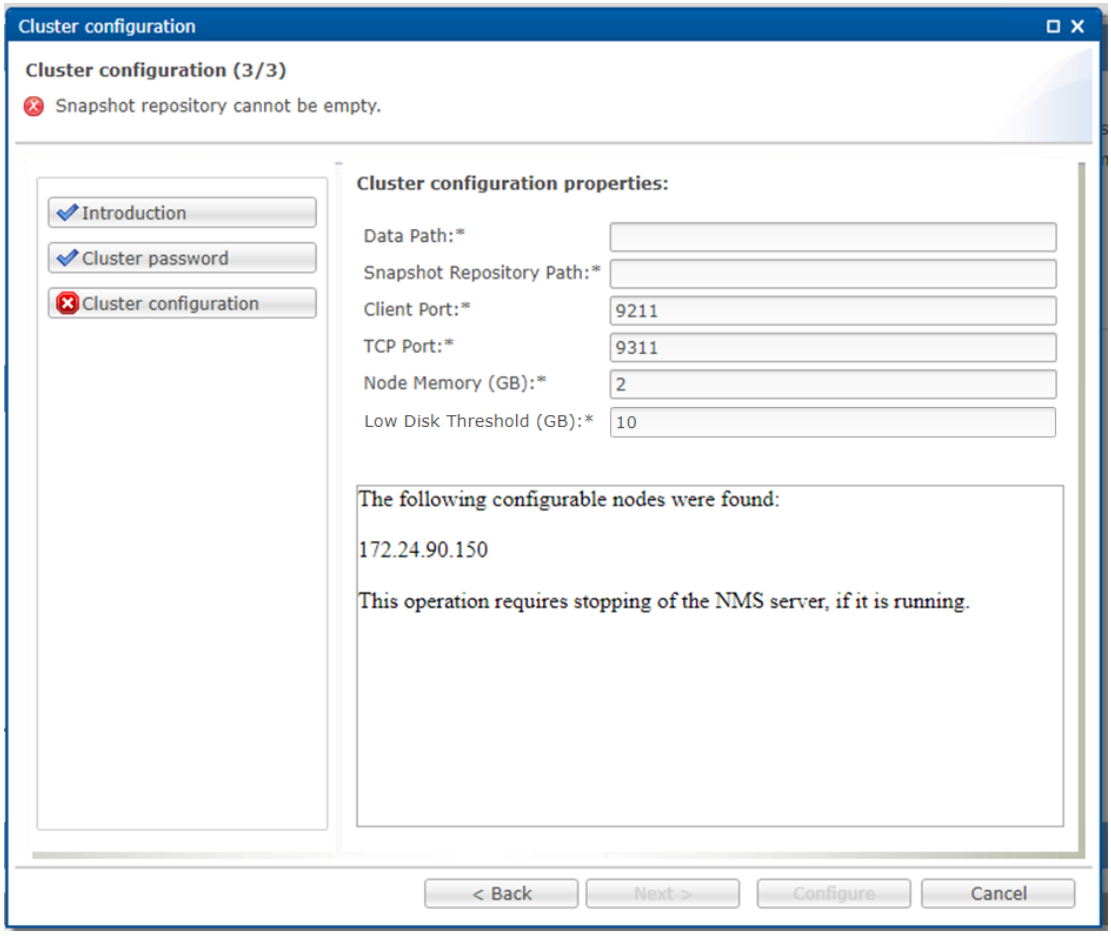
     Note: You can configure the Elasticsearch cluster without a snapshot repository. If you do so:
     - Scheduled database backup and scheduled Elasticsearch backup will not be available.
     - Manual full database backups and manual Elasticsearch database backups may take longer.
     - A configuration without a snapshot repository path is intended only for 1+0 Split, 1+1 Server HA and 1+1 HA setups where the PTP 820 NMS components are installed on

different administrative domains; in all other cases, we recommend using a snapshot repository.

- Note that configuring the Elasticsearch cluster without a snapshot repository is applicable only for the following setups: 1+0 Split, 1+1 Server High Availability, 1+1 High Availability. For 1+0 Standalone and 2+2 High Availability setups, the Snapshot Repository is mandatory.

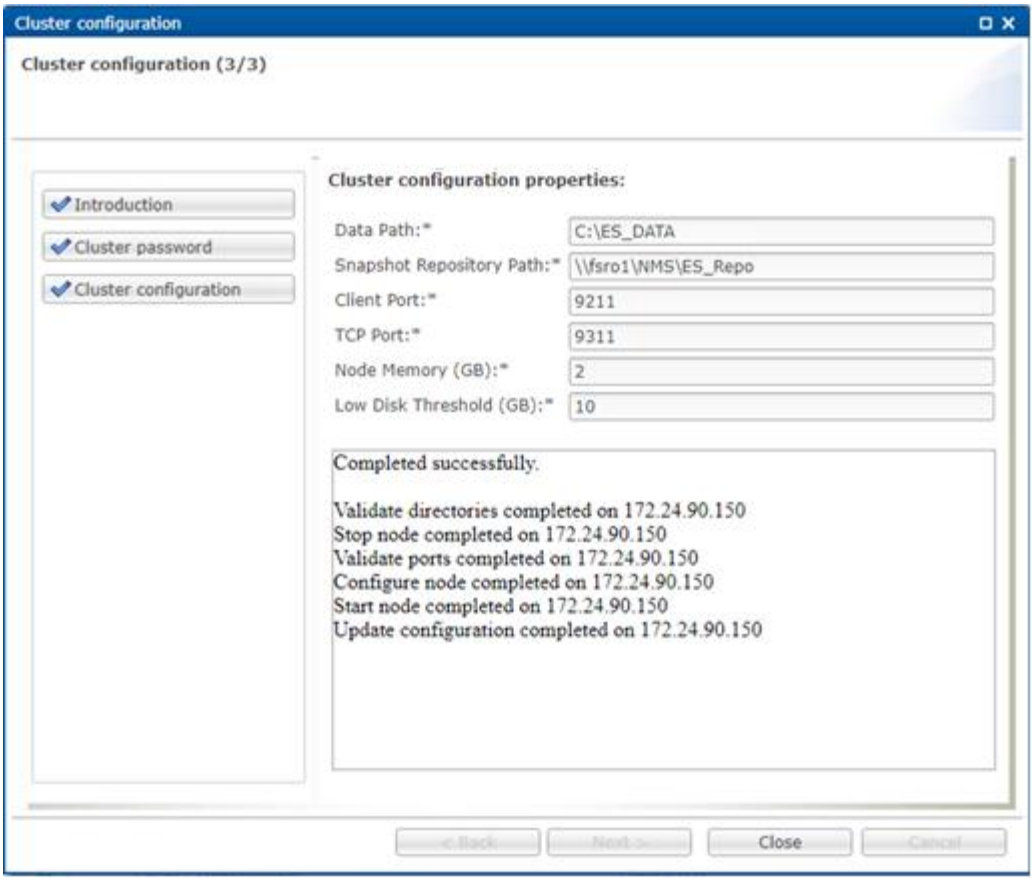
- Optionally, in Snapshot Repository Path #2, enter the second repository path you created in Creating Elasticsearch Folders for repository redundancy purposes. Enter the path in a syntax that can be used identically by all machines participating in the PTP 820 NMS setup. For example: \\fsro1\NMS\ES_Repo_2.
  If you do not wish to have a second (backup) repository path, leave this field empty.
- In Automatic Repo Switch Timer (min), enter the number of minutes that System Manager will wait if Repository 1 fails before switching to Repository 2. When Repository 1 recovers, System Manager will switch back to Repository 1 after a few seconds
  - The default value is 1 minute, the allowed range is between 1 - 1440 minutes.
- In Client Port, enter a port number for communication between the PTP 820 NMS Server and the Elasticsearch cluster. The default value is 9211.
- In TCP Port, enter a port number for communication between Elasticsearch cluster nodes. The default value is 9311.
- In Node Memory (GB), specify the RAM allocation for the node.
  - The default and minimal value is 2
  - The recommended value is 25% of the machine's RAM, but no more than 32 GB
- In Low Disk Threshold (GB), set a threshold value (the default value is 10). When this amount of disk space is left available on a machine that is part of the PTP 820 NMS setup, the Elasticsearch cluster stops allocating shards to that node, an alarm is triggered, and an indication appears in the Dashboard view, as shown below. The PTP 820 NMS Server may even stop functioning if more disk space is not allocated.



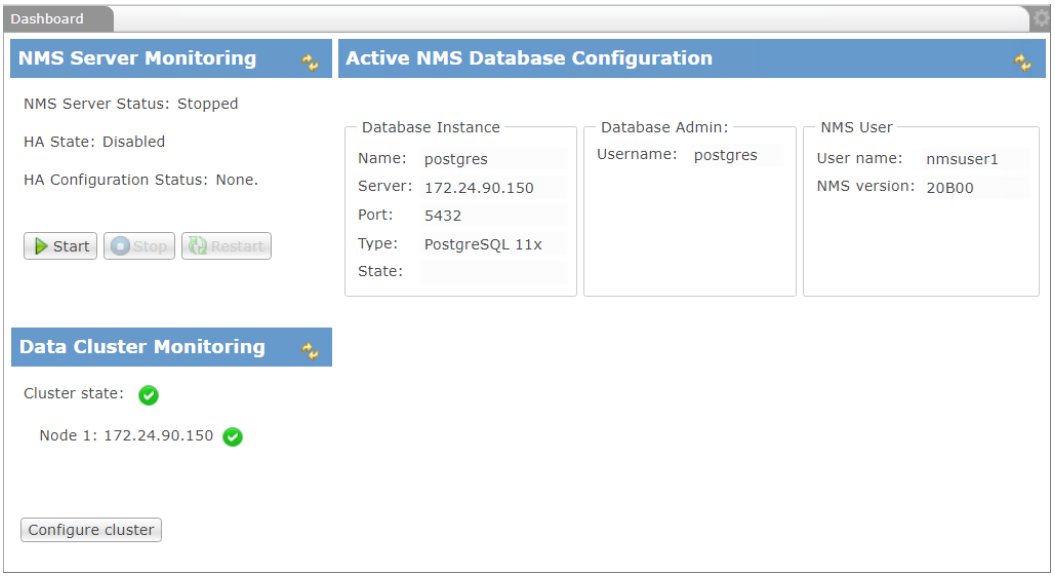


Progress messages appear, informing you that configuration is in process.

5. When cluster configuration is complete, a success message appears.
   Click Close to complete the Cluster Configuration wizard.



The System Manager Dashboard view appears, displaying the cluster state, and all configured cluster nodes.



6. After cluster configuration is completed, the Cluster State in the System Manager Dashboard might be red. Wait up to a minute for the Cluster State to refresh and become green.
7. Click Start  if you wish to start the PTP 820 NMS Server.

In a **Windows setup**: If Server is installed and configured, the server will be installed as an automatic Windows Service, with its own Server monitor in the systray. The Server monitor starts when installation is completed, and you are prompted whether to start the Server. If you don't want the Server to start automatically upon computer reboot, you can set the mode of the Service to manual in the Services applet in the Control Panel.

In a **Linux setup**: You can now install the Client. It must be installed on a Windows platform, see PTP 820 NMS installation for Windows for details.

After the server is started, the client can be accessed. For more details see Upgrading from versions prior to R13B00

The NetMaster license mechanism was changed in R21B00. Therefore, if you wish to upgrade a NetMaster version that is older than R13B00, you must first upgrade to a version between R13B00 and R21A00, and then upgrade to R21B00 or later.

Updating license following changes in computer properties

If you changed the name or the major OS version of the machine on which the NetMaster server is installed, you need to download your Server ID file after the change, and send it to Customer Support with a request for a new license.

Changing an existing license

You can change your existing license to fit your needs at any time. You can:

- Upgrade from a Basic package to a Professional package
- Add Outstanding features to a Basic or Professional package
- Upgrade the number of TRX
- Upgrade a Perpetual license to a new version
- Upgrade a Subscription license to a new time period

In all these cases, contact Customer Support for a new license.

Client GUI .

For details regarding specific post-installation configurations, see the Server Post installation steps.

See the PTP 820 NMS User Guide for more information about System Manager and how to use it.

PTP 820 NMS Server Post Installation

This section describes post installation steps for a Server installation.

Note

This section requires that the steps for Installation on Windows or Installation on Solaris already have been completed.

Note that for a new and upgrade installation, is not ready to run until System Manager's Initial Setup wizard is completed.

Configure PTP 820 NMS to work with IPv4 only or IPv6 only

If the machine hosting PTP 820 NMS is configured to work exclusively with IPv4 or exclusively with IPv6, you must set PTP 820 NMS accordingly.

1. Open the following file in a text editor:

   ```
   <PTP 820
   NMS installation>\Server\wildfly-15.0.0.Final\bin\ngNMSService.vmoptions
   ```

2. Perform one of the following:

   - To specify that PTP 820 NMS work exclusively with IPv4, set

     ```
     -Djava.net.preferIPv4Stack=true
     ```

   - To specify that PTP 820 NMS work exclusively with IPv6, set

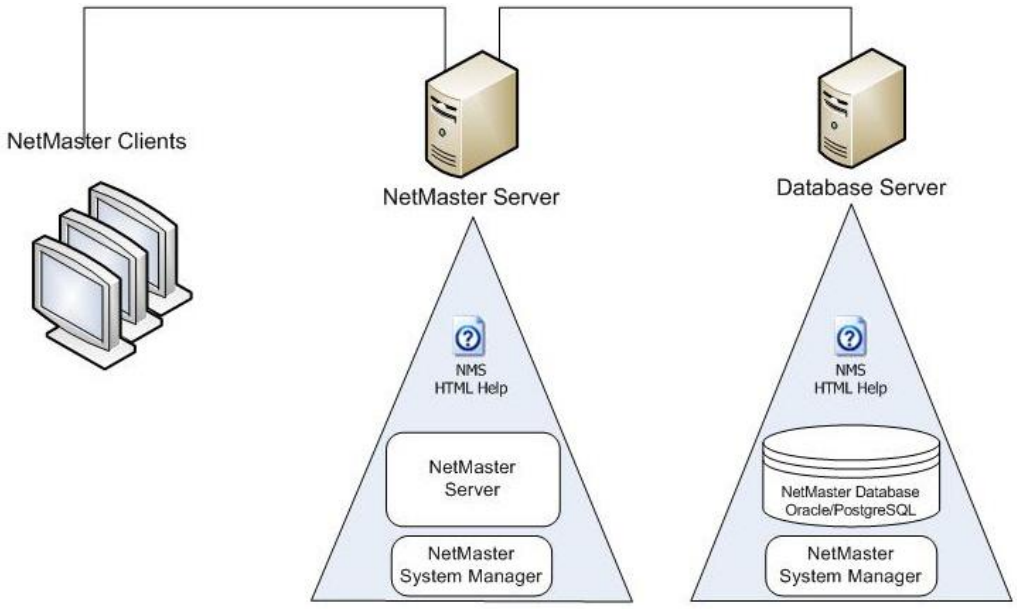
     ```
     -Djava.net.preferIPv4Stack=false
     ```

Database Backup and Restore

The System Manager tool is a component of the Server and Node package and the Database Node package. System provides the operators an easier and more flexible way to deal with some administrative tasks:

- Set up database connection
- Set up Elasticsearch cluster connection
- Upgrade old database to a new version
- Backup/restore database (requires System Manager on database server)
- Schedule database backup and database maintenance tasks
- Configure email notification
- Start and stop of Server

As database backup and restore operations MUST be run on the actual database server, you have to install System Manager as a standalone application on your database server if you want System Manager to handle database backup and restore for you.



A database export will then work like this:

1 User logs on to System Manager on the server and requests a database backup. (Or a periodic database backup job has just started.)

2 A request is sent to System Manager on the database server that runs a database backup job and stores the export file in the default folder C:\NgNMS\backup\database on the database server.

3 System Manager on the server then copies the newly created database export file from the database server and places it in the location specified in the Database view available from the System Manager Settings menu. The default location is C:\NgNMS\backup\database on the server.

Note: If System Manager is not installed on the database server, the database backup and restore feature in System Manager is not available.

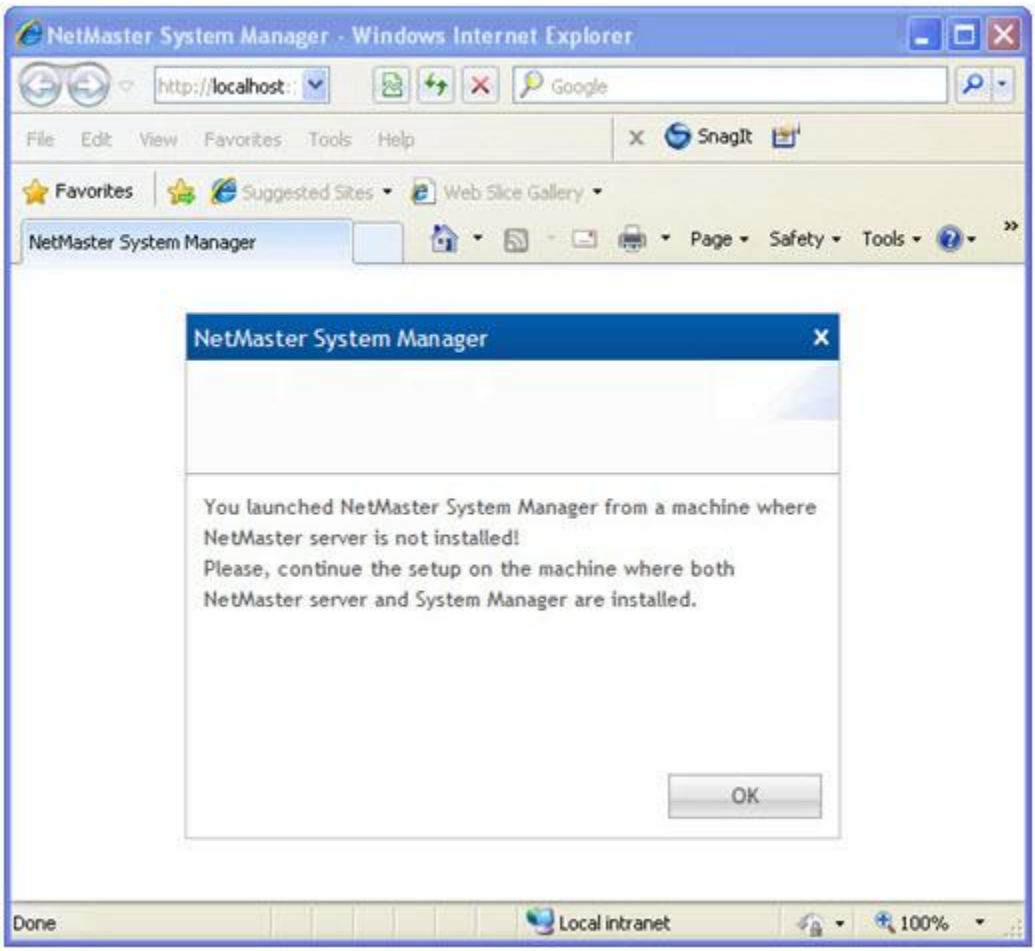
If the local computer has more than one network card, in order to let know to System Manager which IP can be used for remote connection with secondary System Manager please define own IP in C:\Program Files\PTP 820 NMS\SystemManager\sysman.properties

In the case of a backup done before an upgrade operation (started either from the Initial Setup Wizard or from the "Upgrade User/Schema" menu), the backup is kept only on the database server.

Configuration

If you open **System Manager** on a machine on which only a PTP 820 NMS Database Node is installed, the following information is shown:

Figure 1 System Manager



All configuration should in general take place using the System Manager that is installed on the server, and not on the Database Server.

However, note that database backups will by default be saved in a folder on the same drive as the database installation folder. As the database backups occupy too large amounts of space on the storage drive, it might be helpful to change the database folder to a location on a different drive. On a system with standalone Database Server, this must be done manually.

Firewall settings

Configure the following port exceptions in the firewalls according to your needs.

Towards the server

The following is configured on the inbound firewall of the machine hosting the server.

Table 1 Towards the PTP 820 NMS server

Port	Description
TCP 8080	Master port for several types of communication
TCP 61616	Used by client to connect to an enterprise messaging queue that runs within , used to push events to the client about changes in services.
UDP 162 (or as configured by the user in System Manager)	SNMP Trap Port Default port is 162, but can be set to a different port in the **Snmp Trap Port Number** field in System Manager's **NMS Server** view
UDP 161	SNMP get/set when SNMP Agent is used

Towards the NE

The following is configured on the outbound firewall of the machine hosting the server.

Table 2 Towards the NE

Port	Description
TCP 80	HTTP – Hypertext Transfer Protocol
TCP 443	HTTPS – Hypertext Transfer Protocol Secure
UDP 161	SNMP get/set

Towards the server if FTP is used

The following is configured on the inbound firewall of the machine hosting the FTP server.

Table 3 Towards the server if FTP is used

Port	Description
TCP 20	FTP - File Transfer Protocol [default data]
TCP 21	FTP - File Transfer Protocol [Control]

Towards the server if SFTP is used

The following is configured on the inbound firewall of the machine hosting the SFTP server.

Table 4 Towards the PTP 820 NMS server if SFTP is used

Port	Description
TCP 20	SFTP – Secure File Transfer Protocol [default data]
TCP 22	SFTP – Secure File Transfer Protocol [Control]

Note: For SFTP usage, it is required to use SSH software, such as OpenSSH, that supports the ability to change the root directory.

Note: For SFTP on a Windows OS, it is recommended to use the SolarWinds SFTP server 1.0.4.9 (freeware).

Towards the server if RADIUS or TACACS+ is used

The following is configured on the inbound firewall of the machine hosting the RADIUS or TACACS+ server.

Table 5 Towards the PTP 820 NMS server if RADIUS or TACACS+ is used

Port	Description
TCP 49	TACACS+ Protocol
UDP: 1812 & 1813 or UDP: 1645 & 1646	RADIUS Protocol

Towards the database machine

The following is configured on the inbound firewall of the machine hosting the database.

Table 6 Towards the PTP 820 NMS database machine

Port	Description
TCP 1521	Oracle Database server
TCP 5432	Postgres SQL Database server

Towards the System Manager installation

The following is configured on the inbound firewall of the machine hosting the System Manager.

Table 7 Towards the System Manager installation

Port	Description
TCP 1521	Oracle Database server
TCP 5432	Postgres SQL Database server

TCP 9211	Communication between PTP 820 NMS and Elasticsearch cluster
TCP 9311	Communication between Elasticsearch cluster nodes
TCP 18005	Shutdown port
TCP 18080	Connector port
TCP 18443	Redirect port

For Windows Firewall, these ports can be opened as follows:

1 Open the Windows Firewall in the Windows Control Panel

2 In the **General** tab, make sure that **On (recommended)** is selected and that **Don't allow exceptions** is not checked.

3 In the **Exceptions** tab, click **Add Port**. Repeat for all ports to allow.

   i Type the name, e.g. "nms_server_port".

   ii Type the port number, e.g. "8443".

   iii Make sure that TCP is selected.

   iv If you want to limit the IP addresses that are allowed to connect using this port, click the **Change scope** button:

   - Select **Custom list** and specify the IP-addresses of all GUI Client computers, or
   - Select **My network (subnet) only** to only allow GUI Clients within your local subnet.
   - Click **OK**.

4 Click **OK**.

5 In the **Advanced** tab, make sure that the network connection your computer is using is enabled (checked) in the **Network Connection Settings** list.

For other firewalls, different procedures may be required.

Reserving ports

Reserving ports on the machine hosting the server

The following ports need to be left empty on the machine hosting the server so that the application can bind to them.

Table 8 Reserving ports on the machine hosting the server

Port	Description
UDP 162 (or as configured by the user in System Manager)	SNMP Trap Port Default port is 162, but can be set to a different port in the **Snmp Trap Port Number** field in System Manager's **NMS Server** view.

UDP 1621	SNMPv1 and SNMPv2c internal trap port. In use on the server machine when either SNMPv1 or SNMPv2c traps are received from the device on the SNMP trap port (default: 162). This port does not need to be opened on the firewall.
UDP 1622	SNMPv3 internal trap port, in use on the server machine when SNMPv3 traps are received from the device on the SNMP trap port (default: 162). This port does not need to be opened on the firewall.
TCP 4712	Socket for TX Recovery Manager
TCP 4713	Socket for TX Status Manager
TCP 8080	Master port for several types of communication
TCP 8443	Socket for HTTPS communication
TCP 8009	Socket for AJP (web proxy)
TCP 9211	Communication between PTP 820 NMS and Elasticsearch cluster
TCP 9311	Communication between Elasticsearch cluster nodes
TCP 9990	Socket for HTTP Management Console
TCP 9993	Socket for HTTPS Management Console
TCP 8787	Java remote debug port
TCP 61616	Used by the client to connect to an enterprise messaging queue that runs within , used to push events to the client about changes in services.

Reserving ports on the machine hosting the System Manager

The following ports need to be left empty on the machine hosting the System Manager so that the application can bind to them.

Table 9 Reserving ports on the machine hosting the System Manager

Port	Description
TCP 18005	Shutdown port
TCP 18010	AJP connector port
TCP 18443	Connector port
TCP 18443	Redirect port
TCP 9211	Communication between PTP 820 NMS and Elasticsearch cluster
TCP 9311	Communication between Elasticsearch cluster nodes

Changing TCP ports in 8443

The 8080 TCP port is the default port that the server exposes to clients (GUI, CLI reports, NIF Agent). This port needs to be added to the firewall setting (see Firewall settings).

If you wish to configure to use other ports instead, you can change the default settings, and specify which TCP ports should perform the functions instead.

The following table lists the modules that make use of this port, and describes in which configuration files and fields the port is defined.

Note that before changing the port, all modules relating to the port must first be stopped.

Table 10 modules

Module	File	Path to File	Field/Location in file	Default Port
Polytopo import	config.properties	<Install_path>\PTP 820 NMS\PolyTopoImport\conf	topo.import.port	8080
NIF Agent	loginfo.properties	<Install_path>\PTP 820 NMS\Northbound SNMP\bin\conf	serverurl	8080
Server	standalone-ngnms.xml	<Install_path>\PTP 820 NMS\Server\wildfly-15.0.0.Final\standalone\configuration	<socket-binding name="http" port="${jboss.http.port:8080}"/>	8080
Client	NGnms.ini	<Install_path>\PTP 820 NMS\GUI_Client	nms_server_port	8080
CLI Reports	jboss.properties	<Install_path>\PTP 820 NMS\CLI_Reports\conf	server_port	8080
System Manager	wrapper.conf	<Install_path>\PTP 820 NMS\SystemManager\Tomcat-6.0.18-win\conf	wrapper.java.additional.7=-Deserver_port=	8080

Changing UDP port 161 and UDP port 162

In both Windows and Linux installations:

- PTP 820 NMS's default SNMP Trap port is UDP 162. You can specify a different port in the Snmp Trap Port Number field in System Manager's NMS Server view.
- PTP 820 NMS's default SNMP Agent port is UDP 161. You can specify a different port by accessing the file: <PTP 820 NMS installation>/Northbound_SNMP/bin/ngNIFService.vmoptions, and in a text editor changing the port number in the line:

  ```
  -Dlistening.port=161
  ```

  Then save the changes and restart the SNMP Agent service from the system tray icon.

Managing Windows Services and Server Monitor

The PTP 820 NMS services include:

- ngNMSService – PTP 820 NMS Server

- ngNIFService – PTP 820 NMS SNMP Agent
- ngSysMgr – PTP 820 NMS System Manager
- ngNMSElastic – PTP 820 NMS Elasticsearch service

At the end of an installation on Windows platform, the Server is installed as a Windows service and a Server Monitor application is automatically started (look for the systray icon ). If you don't want the Server to start automatically upon computer reboot, you can set the mode of the Service to **Manual** in the *Services* applet in the *Control Panel*.

A service and a monitor are available also for the PTP 820 NMS SNMP Agent, if it is started (look for the systray icon ). For more details see the *PTP 820 NMS User Guide*.

Managing Linux Services

The PTP 820 NMS services include:

- ngNMSService – PTP 820 NMS Server
- ngNIFService – PTP 820 NMS SNMP Agent
- ngSysMgr – PTP 820 NMS System Manager
- ngNMSElastic – PTP 820 NMS Elasticsearch service

The following are useful service-related commands, and:

- To find all services, whether running or not:

```
systemctl --all | grep <service>
```

- To find running services only:

```
systemctl | grep running | grep <service>
```

- To find not-running services only:

```
systemctl --all | grep inactive | grep <service>
```

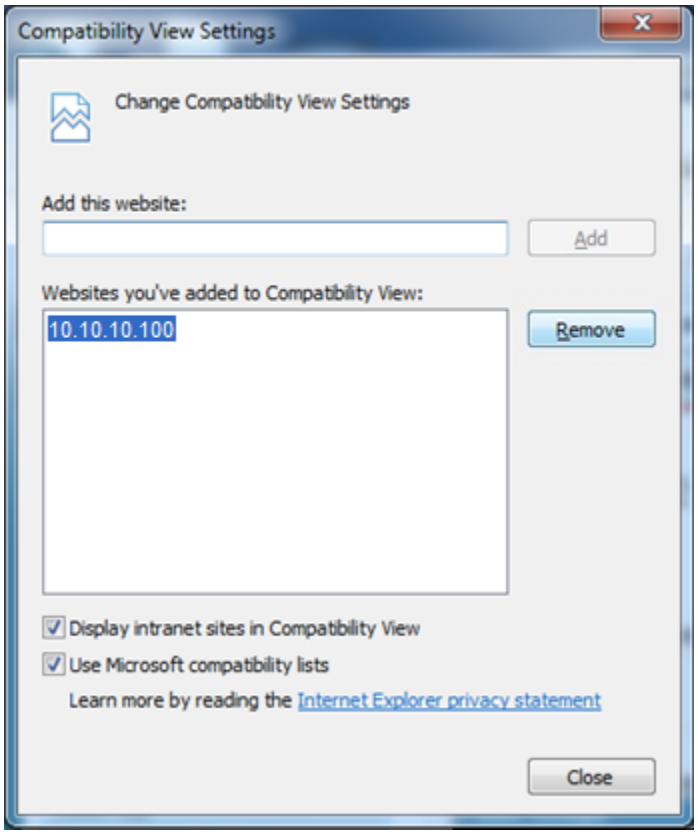
To check status or to stop/start/restart PTP 820 NMS related services use the following commands. They can be used only by the user allowed to run PTP 820 NMS that was selected in step 5 of Running the installer for Linux:

```
systemctl status --user <service>

systemctl start --user <service>

systemctl stop --user <service>

systemctl restart --user <service>
```

Enable System Manager in Internet Explorer

To enable System Manager to open with Internet Explorer 11 following the completion of a installation or upgrade, do the following:

- In Internet Explorer 11, add localhost, or the site where you installed the System Manager, to the Compatibility View. See the example below.



Server Recommended Settings

is predefined with default server settings for Maximum Connection Pool Size, Maximum Thread Pool Size, and Maximum Heap Size. These settings should be tuned on servers managing large networks. The following table presents the recommended settings for various network sizes:

Table 11 PTP 820 NMS Server Recommended Settings

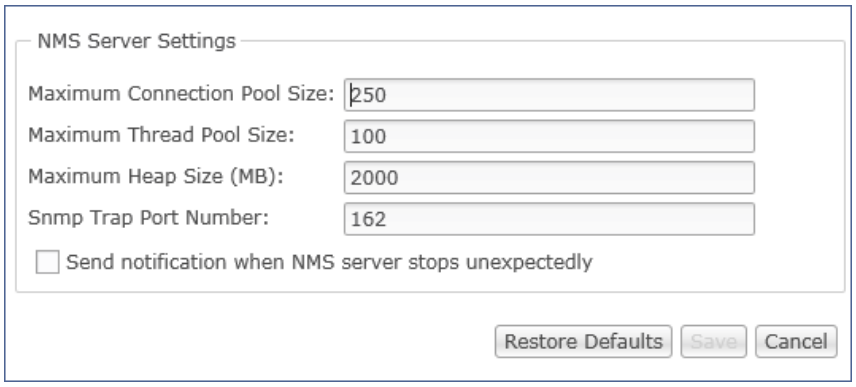
Network size	Max Connection Pool Size	Max Thread Pool Size	Heap Size
1000 NEs	250	100	3000
2000 NEs	300	130	5000
4000 NEs	500	250	10000
10000 – 20000 NEs	500	300	20000

To change these settings:

1 In the System Manager: open the Settings menu and click **PTP 820 NMS Server**.

2 Change the value for Maximum Connection Pool Size, Maximum Thread Pool Size, and Maximum Heap Size according to the values in the table above.
Note that the maximum allowed heap size is highly dependent on available memory on the server.

Figure 2 NMS Server Settings



3 Restart Server.

- If the server fails to start, reset the values, as above, using lower values than the ones suggested.
- If the server starts successfully, leave the server running or increase the values even further until server start failing. Then use the last values it successfully started with.

Server should now have an optimal configuration.

license

In order to run , it is necessary to have a suitable license.

For full details regarding the available license types and options, see the NetMaster Licensing Model section in the NetMaster User Guide.

License installation for a new installation

Following completion of installation, System Manager is automatically launched and opens the **NMS Initial Setup** wizard, beginning with License Import. Note that License Import can also be performed from the System Manager's **Import License** wizard.

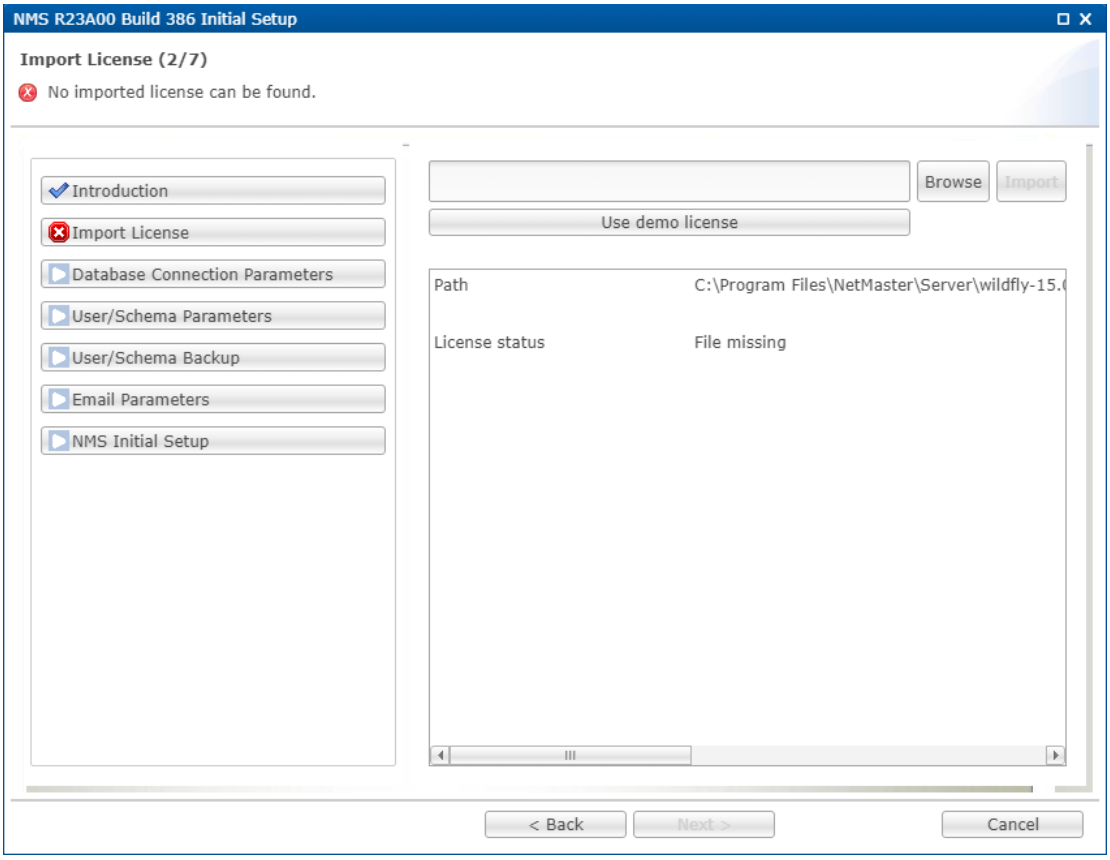
Note: For a full explanation of System Manager, see the *PTP 820 NMS User Guide*.

To install a license:

1 In the System Manager's **Database** tab, run the **NMS Initial Setup** wizard. Or in the System Manager's **License Administration** tab, run the **Import License** wizard.

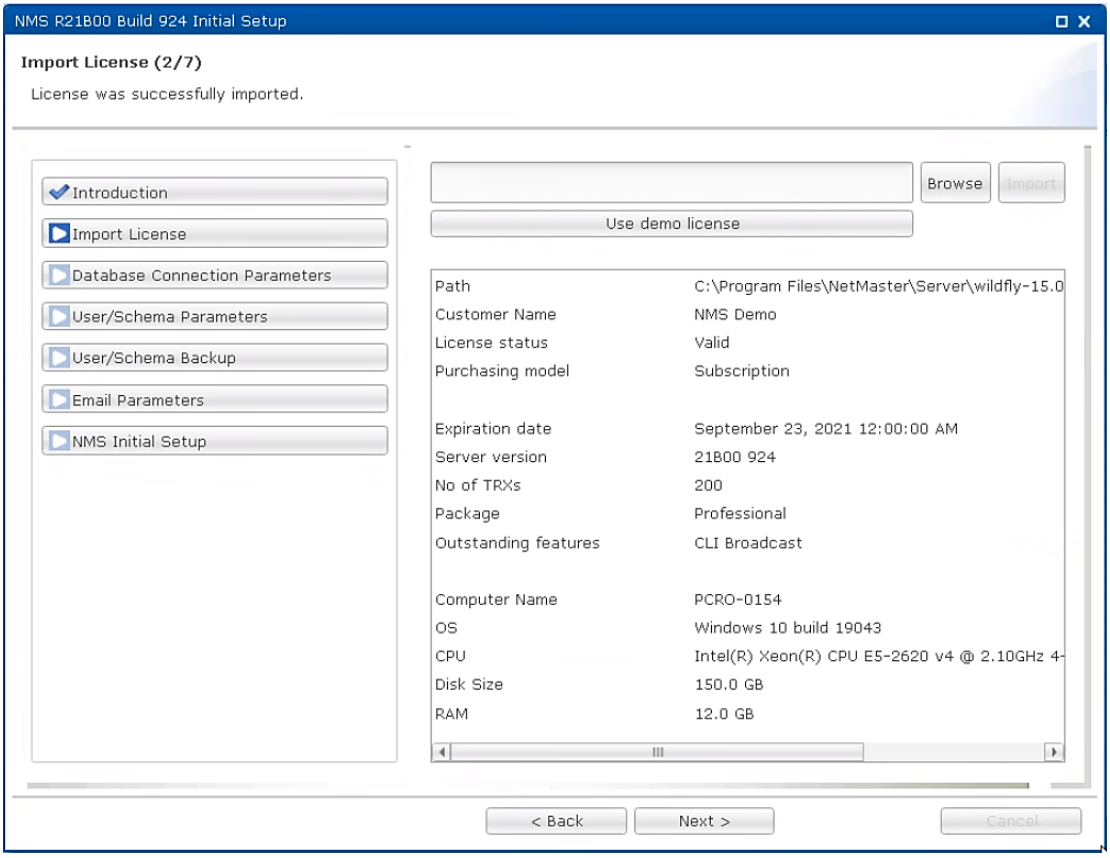
2 In the **Import License** window, click **Use Temporary License** to load the temporary license file provided with the installation.

Figure 3 Import License window



3 A temporary license, which will expire in 30 days, is loaded.
Copy the Activation key, appearing at the bottom of the Wizard's Import License window. You will need to provide it when requesting a permanent license.

Note: At any point, you can view your Activation key in the System Manager's License Administration tab.

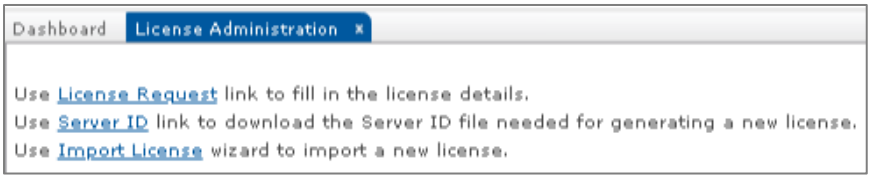


4 Follow the instructions to complete the wizard.

5 To obtain your own NetMaster license, access the **License** > **License Administration** view in System Manager, and:

   i Click **License Request** and fill in the license request details.

   ii Click **Server ID** and send the downloaded file to Customer Service with a request to generate a NetMaster license for you.



6 When you receive your own NetMaster license, run the **Import License** wizard to **Import** the license. This can be done via System Manager even after the demo license expired.

Upgrading from versions prior to R13B00

The NetMaster license mechanism was changed in R21B00. Therefore, if you wish to upgrade a NetMaster version that is older than R13B00, you must first upgrade to a version between R13B00 and R21A00, and then upgrade to R21B00 or later.

Updating license following changes in computer properties

If you changed the name or the major OS version of the machine on which the NetMaster server is installed, you need to download your Server ID file after the change, and send it to Customer Support with a request for a new license.

Changing an existing license

You can change your existing license to fit your needs at any time. You can:

- Upgrade from a Basic package to a Professional package
- Add Outstanding features to a Basic or Professional package
- Upgrade the number of TRX
- Upgrade a Perpetual license to a new version
- Upgrade a Subscription license to a new time period

In all these cases, contact Customer Support for a new license.

Client GUI

Start the Client by double-clicking Ngnms.exe, located in <Netmaster installation>/GUI_Client.

A Login window will be displayed where the authentication credentials and the server host name must be entered.

The authentication credentials for the root administrator are:

User name: **root**

Password: **pw**

Note: It is strongly recommended to change the password of the root account immediately after the first login to prevent unauthorized access. To change the password, open the User Settings preferences menu.

The next step is now to discover your network, as described in the *PTP 820 NMS NMS User Guide*.

Client memory allocation

The client by default is allocated 2GB of RAM. In large setups, follow these directives:

- For setups with over 5,000 devices, increase the memory allocation by an extra 1GB of RAM for each additional 5,000 devices. That is:
    - For a setup with 10,000 devices, allocate a total of 3GB of memory
    - For a setup with 15,000 devices, allocate a total of 4GB of memory
    - For a setup with 20,000 devices, allocate a total of 5GB of memory

- It is recommended to limit the number of devices managed by a single client to 10,000 (5,000 is preferable) to avoid delays in screen update.

To change the memory allocation of the client:

1. Open the file Ngnmns.ini located in <PTP 820 NMS Instalation>/GUI_Client.
2. Replace -Xmx2048m with the appropriate value. For example:
   - -Xmx3062m (to allocate 3GB)
   - -Xmx4096 (to allocate 4GB)
3. Save the changes.

The new memory settings will go into effect when you restart the client.

Changing HTTPS Certificates

The PTP 820 NMS components and sub-components (Server, Client, System Manager, Elasticsearch) communicate over an encrypted HTTPS communication channel. If you wish to generate your own certificates for communication, perform the following.

Prerequisites

1. Make sure the Java development kit is installed and the environment paths are defined. Refer to:
   - For a Windows installation: Java Installation
   - For a Linux installation: Install OpenJDK and Set the Java Home variable.
2. Create a folder, anywhere on disk, where the two certificates will be created. For example: C:\Sandbox\SSL_Cert.
3. Stop PTP 820 NMS Client, PTP 820 NMS Server, PTP 820 NMS System Manager and SNMP Agent Service.

Create an application.keystore certificate

1. Open a CMD window.
2. Run:

   ```
   cd <certificates_folder>
   ```

   For example: cd C:\Sandbox\SSL_Cert
3. Run:

   ```
   keytool -genkey -v -keystore application.keystore -alias [your_alias_name] -keyalg RSA -keysize 2048 -validity [number_of_days]
   ```

   For example:

   ```
   keytool -genkey -v -keystore application.keystore -alias server -keyalg RSA -keysize 2048 -validity 10000
   ```

   where validity [number_of_days] specifies how many days the certificate is valid. The permitted range is 1 – 365000 days.
4. When prompted, enter a password for the **application.keystore** certificate.

5. When prompted, enter responses to questions.
6. Enter a key password for [your_alias_name]. This can be the same password you entered in step (4), or a different one.

An **application.keystore** certificate file is created in the folder you specified in step (2).

Export the application.keystore certificate

1. Run:

```
keytool -exportcert -keystore applicaton.keystore -alias [your_alias_name] -
file [your_crt_name]
```

For example:

```
keytool -exportcert -keystore application.keystore -alias server -
file  wildfly.crt
```

2. Enter the **application.keystore** password chosen in step (4) of Create an application.keystore certificate.

   A certificate file with the <your_crt_name> you specified in the previous step (for example, **wildfly.crt**), is created in the folder you specified in step (2) of Create an application.keystore certificate.

Importing the certificate into the client.truststore

1 Copy the **application.keystore** file and certificate file to the <NetMaster_Install_Path>\Resources folder on the NetMaster server machine. Replace the existing files if needed.

2 Open CMD in <NetMaster_Install_Path>\Resources and run:

```
keytool -import -file <your_crt_name> -alias <your_alias_name> -keystore
client.truststore
```

For example:

```
keytool -import -file wildfly.crt -alias server -keystore
client.truststore
```

The command triggers a prompt for a password. Enter password (this is the default value).

Note: If you wish to change the default password, run the following command and provide the new password.

```
keytool -storepasswd -keystore client.truststore
```

3 Optionally, delete the certificate file from the <NetMaster_Install_Path>\Resources folder.

Updating NetMaster to use the new certificates

1 Update the **client.truststore** password for all client components. That is, update:

```
-Djavax.net.ssl.trustStorePassword = <password created in step (2) of
Importing a certificate into the client.trustore>
```

In the following files:

<NetMaster_Install_Path>/GUI_Client/Ngnms.ini
<NetMaster_Install_Path>/CLI_Reports/pmreport.vmoptions
<NetMaster_Install_Path>/CLI_Reports/alarmreport.vmoptions
<NetMaster_Install_Path>/CLI_Reports/inreport.vmoptions
<NetMaster_Install_Path>/Northbound_SNMP/bin/ngNIFService.vmoptions
<NetMaster_Install_Path>/SystemManager/tomcat/bin/ngSysMgr.vmoptions
<NetMaster_Install_Path>/Server/ServerMonitor/servermonitor.vmoptions

2 Update passwords for Server component in the following file:

<NetMaster_Install_Path>/Server/wildfly-15.0.0.Final/bin/ngNMSService.vmoptions

That is, search for the following sequences and update the passwords as follows:

```
-Djavax.net.ssl.trustStore=C:\\Program Files\\NetMaster\\Resources\\client.truststore

-Djavax.net.ssl.trustStorePassword=<password created in step (2) of Importing a certificate into the client.trustore>

-Djavax.net.ssl.keyStore=C:\\Program Files\\NetMaster\\Resources\\application.keystore

-Djavax.net.ssl.keyStorePassword=<password chosen in step (4) of Create an application.keystore certificate>
```

3 Update the keystore-password, alias, and key-password for all Server components. That is:

i Identify the following block:

```
<server-identities>
  <ssl>
    <keystore path="application.keystore" relative-to="jboss.server.config.dir" key
store-password="password" alias="server" key-password="password" generate-self-si
gned-certificate-host="localhost"/>
  </ssl>
</server-identities>
```

ii In each of the following files:

<NetMaster_Install_Path>\Server\wildfly-15.0.0.Final\standalone\configuration\standalone-ngnms.xml
<NetMaster_Install_Path>\Server\wildfly-15.0.0.Final\standalone\configuration\standalone-ngnms-template.xml

iii And in both files, update:

- keystore-password – with the value specified in step (4) of Create an application.keystore certificate
- alias – with the value specified in step (3) of Create an application.keystore certificate
- key-password – with the value specified in step (4) of Create an application.keystore certificate

4 Update the keystore-password, alias, and key-password for all System Manager components. That is:

i In the following file:

<NetMaster_Install_Path>\SystemManager\tomcat\conf\server.xml

ii Identify the following block:

```
<Connector port="18443" protocol="org.apache.coyote.http11.Http11NioProtocol"
        maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
        keystoreFile="../../Resources/application.keystore" keystorePass="password"
        clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.3"
        ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
            TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
            TLS_RSA_WITH_AES_256_GCM_SHA384,
            TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"/>
```

iii Replace it with the following block:

```
<Connector port="18443" protocol="org.apache.coyote.http11.Http11NioProtocol"
        maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
        keystoreFile="../../Resources/application.keystore" keystorePass="password"
        clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.3"
        ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
            TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
            TLS_RSA_WITH_AES_256_GCM_SHA384,
            TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
        keyAlias="server" keyPass="password"/>
```

iv And update:

- keystorePass – with the value specified in step (4) of Create an application.keystore certificate
- keyAlias – with the value specified in step (3) of Create an application.keystore certificate
- keyPass – with the value specified in step (4) of Create an application.keystore certificate

5 Update the keystore password for all Elasticsearch nodes. That is:

i In the following file:

<NetMaster_Install_Path>\SystemManager\elasticsearch\config\elasticsearch.yml

ii Identify the following lines:

```
xpack.security.transport.ssl.keystore.password: "password"
xpack.security.http.ssl.keystore.password: "password"
```

iii And update the password with the one specified in step (4) of Create an application.keystore certificate.

iv In the same file, identify the following lines:

```
xpack.security.transport.ssl.keystore.key_password: "password"
xpack.security.http.ssl.keystore.key_password: "password"
```

iv And update the password with the one specified in step (4) of Create an application.keystore certificate.

6 Start System Manager and the SNMP Agent service and execute again cluster configuration, as described in PTP 820 NMS Elasticsearch Cluster Configuration.

7 Start the NetMaster Client and NetMaster Server applications.

Changing HTTPS Certificates to CA-Signed Certificates for Communication between NetMaster Components

The NetMaster components and sub-components (Server, Client, System Manager, Elasticsearch) communicate over an encrypted HTTPS communication channel. If you wish to use CA-signed certificates for communication, perform the following.

Prerequisites:

- Make sure you have a PFX file and the corresponding PFX key password.
- Use only numbers and letters in the PFX key, application.keystore and client.truststore passwords.
- Stop all NetMaster-related services: NetMaster Client, NetMaster Server, NetMaster System Manager, SNMP Agent service, and Elasticsearch service.

Change application.keystore password to be identical to PFX Key password

1 Paste the PFX file into the `<NetMaster_Install_Path>\Resources` folder on the NetMaster server machine.

2 Open CMD in `<NetMaster_Install_Path>\Resources` and run the following command as an admin:

```
keytool -storepasswd -keystore application.keystore
```

3 At the prompt, enter the current password of **application.keystore**, which is by default 'password'.

4 At the prompt, enter as the new password, the same password as the PFX key password.

Import PFX to Keystore

1 Run:

```
keytool -importkeystore -srckeystore <name of the pfx file>.pfx -srcstoretype pkcs12 -destkeystore application.keystore
```

For example:

```
keytool -importkeystore -srckeystore pfxfile.pfx -srcstoretype pkcs12 -destkeystore application.keystore
```

2 At the prompt, enter the source keystore password and destination keystore password. For each of them, enter the same password as the PFX key password.

Remove default certificate from keystore

Run the following command in order to remove the default or self-signed certificate from **application.keystore**:

```
keytool -delete -alias server -keystore application.keystore -storepass "<password from step 1>"
```

Take care to enclose the application.keystore password in quotation marks "". For example:

```
keytool -delete -alias server -keystore application.keystore -storepass "password1"
```

Find the alias of the imported PFX file

1 Perform either of the following:

- Review the output of the command you ran to **Import PFX to Keystore.**

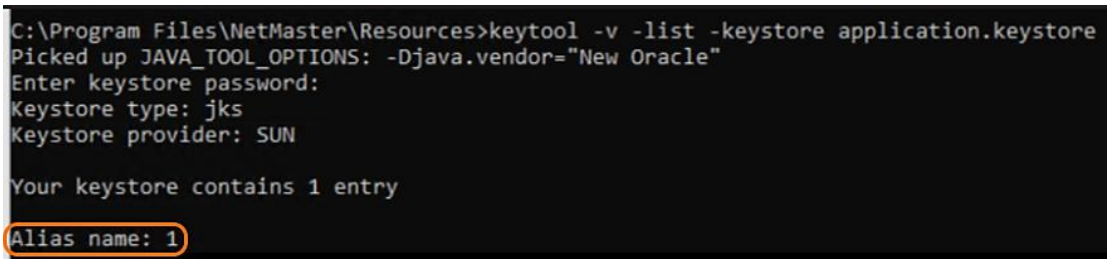
  Or

- Run the following command to display the information related to the files in the application.keystore:

  ```
  keytool -v -list -keystore application.keystore
  ```

  When prompted, enter the password for the **application.keystore**.

2 Find the alias in the output:



Export certificate from keystore

1 Run the following command to export the certificate (.crt) from the keystore:

```
keytool -exportcert -keystore application.keystore -alias <alias name> -file <certificate_name>.crt
```

For example:

```
keytool -exportcert -keystore application.keystore -alias cert_alias -file ca.crt
```

2 When prompted, enter the password for the **application.keystore**.

Add the exported certificate to the truststore

1 Run the following command to import the certificate to the **client.truststore**:

```
keytool -import -file <name of the certificate>.crt -alias <alias name> -keystore client.truststore
```

For example:

```
keytool -import -file ca.crt -alias cert_alias -keystore client.truststore
```

2 When prompted, enter the password for the **client.truststore**. The default password is: 'password'.

Note: The default **client.truststore** password is 'password'. If you wish to change the default password, refer to Changing the client.truststore password – Optional

Changing the client.truststore password – Optional

The default client.truststore password is 'password'. If you wish to change the client.truststore password, perform the following.

Run the following command and provide the new password.

```
keytool -storepasswd -keystore client.truststore
```

If you changed the **client.truststore** password, update it in the following files:

<NetMaster_Install_Path>/GUI_Client/Ngnms.ini
<NetMaster_Install_Path>/CLI_Reports/pmreport.vmoptions
<NetMaster_Install_Path>/CLI_Reports/alarmreport.vmoptions
<NetMaster_Install_Path>/CLI_Reports/inreport.vmoptions
<NetMaster_Install_Path>/Northbound_SNMP/bin/ngNIFService.vmoptions
<NetMaster_Install_Path>/SystemManager/tomcat/bin/ngSysMgr.vmoptions
<NetMaster_Install_Path>/Server/ServerMonitor/servermonitor.vmoptions
<NetMaster_Install_Path>/Server/wildfly-15.0.0.Final/bin/ngNMSService.vmoptions

To update the password, search for the following sequence and update it with the proper password:

```
-Djavax.net.ssl.trustStorePassword = <truststore_password>
```

Delete the certificate and PFX files

Delete the certificate and PFX files from the following folder:

<NetMaster_Install_Path>\Resources

Updating NetMaster to use the new certificates

1 Update **application.keystore** for Elasticsearch:

   i Delete the existing **application.keystore** from:

   <NetMaster_Install_Path>\SystemManager\elasticsearch\config

   ii Copy the new **application.keystore** from:

   <NetMaster_Install_Path>\Resources

   iii Paste the new **application.keystore** into:

   <NetMaster_Install_Path>\SystemManager\elasticsearch\config

2 If you changed the **client.truststore** password, then update it for Client components in the following files:

To update the password, search for the following sequence and update it with the proper password:

```
-Djavax.net.ssl.trustStorePassword = <truststore_password>
```

3 Update **client.truststore** passwords for the Server component in the following file:
<NetMaster_Install_Path>/Server/wildfly-15.0.0.Final/bin/ngNMSService.vmoptions

To update the passwords, search for the following sequence and update the **client.truststore** and **application.keystore** passwords as follows:

```
-Djavax.net.ssl.trustStore=C:\\Program
Files\\NetMaster\\Resources\\client.truststore

-Djavax.net.ssl.trustStorePassword=<truststore_password>

-Djavax.net.ssl.keyStore=C:\\Program
Files\\NetMaster\\Resources\\application.keystore

-Djavax.net.ssl.keyStorePassword=<password from step 1>"
```

4 Update passwords and alias for the Server component in the following two files:

<NetMaster_Install_Path>\Server\wildfly-15.0.0.Final\standalone\configuration\standalone-ngnms.xml

<NetMaster_Install_Path>\Server\wildfly-15.0.0.Final\standalone\configuration\standalone-ngnms-template.xml

To update, search for the following sequence

```
<server-identities>

<ssl><keystore path="../../Resources/application.keystore" relative-
to="jboss.home.dir" keystore-password="password1" alias="Server" key-
password="password1" generate-self-signed-certificate-host="localhost"/>

</ssl>

</server-identities>
```

Then update it as follows:

keystore-password = "<password_from_step_1_substep_4>"
alias = "<your_alias_name_from_step_4_substep_2>"
key-password = "<password_from_step_1_substep_4>"

5 Update passwords and alias for the System Manager component in the following file:
<NetMaster_Install_Path>\SystemManager\tomcat\conf\server.xml

To update, identify the following sequence:

```
"<Connector port="18443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
keystoreFile="../../Resources/application.keystore" keystorePass="password"
clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.3"
ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"/>"
```

Replace it with:

```
"<Connector port="18443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    keystoreFile="../../Resources/application.keystore" keystorePass= <password>"
    clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.3"
    ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
        TLS_RSA_WITH_AES_256_GCM_SHA384,
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
    keyAlias="<alias>" keyPass="<password>"/>"
```

Then update it as follows:

```
keystorePass = "<password_from_step_1_substep_4>"
keyAlias = "<your_alias_name_from_step 4_substep_2>"
keyPass = "<password_from_step_1_substep_4>"
```

6 Update password for all Elasticsearch nodes in the following file:
`<NetMaster_Install_Path>\SystemManager\elasticsearch\config\elasticsearch.yml`

To update, search for the following sequences and update the password with the one used in step 1 substep_4:

```
xpack.security.transport.ssl.keystore.password:
"<password from step 1 substep 4>"

xpack.security.http.ssl.keystore.password: "<password from step 1 substep 4>"

xpack.security.transport.ssl.keystore.key_password:
"<password from step 1 substep 4>"

xpack.security.http.ssl.keystore.key_password:
"<password from step 1 substep 4>"
```

7 Start System Manager and the SNMP Agent service and execute again cluster configuration, as described in PTP 820 NMS Elasticsearch Cluster Configuration

8 Start the NetMaster Client and NetMaster Server applications.

CA Certificate updates for Client node installations

After all the changes for certificates defined above have been made on the machine where the server is installed, copy the Resources folder from the machine where the server is installed to the machine where the client is installed, at the following path: <NetMaster_Install_Path>\NetMaster\Resources.

Changing HTTPS Certificates for High Availability Setups

The NetMaster components and sub-components (Server, Client, System Manager, Elasticsearch) communicate over an encrypted HTTPS communication channel. If you wish to use CA-signed

certificates in a High Availability Setup where each machine has its own certificate, perform the following.

Prerequisites:

- In order for the browser to validate the certificate used in System Manager, the certificate provided must also include an additional field, called SAN (Subject Alternative Name) which should be populated with the FQDN or IP of the machine.
- Make sure you have a PFX file and the corresponding PFX key password.
- Along with the certificate, request the public of the signer (issued directly by the root CA)
- Use only numbers and letters in the PFX key, application.keystore and client.truststore passwords.
- Stop all NetMaster-related services: NetMaster Client, NetMaster Server, NetMaster System Manager, SNMP Agent service, and Elasticsearch service.

Perform standalone configuration

For each server, follow the procedure in Changing HTTPS Certificates to CA-Signed Certificates for Communication between NetMaster Components.

Update client.truststore for multiple nodes

Update **client.truststore** for multiple nodes by performing the following for each of the server:

The entries to add are:

```
xpack.security.transport.ssl.truststore.path: "client.truststore"

xpack.security.transport.ssl.truststore.password: "<client.store
password>"
```

Note: The default **client.truststore** password.

Managing IP-10 devices using HTTPS on Linux

Because IP-10 devices use TLS 1 and Red Hat Linux does not have it enabled by default, you must run the following command on the Linux machine on which NetMaster is installed, and then restart the machine:

```
update-crypto-policies --set LEGACY
```

In addition, a known issue related to using JDK_412 is that the TLS protocol used for communicating specifically with IP-10 over HTTPS is, by default, in the disabled Algorithms list of the new java installation.

To re-enable HTTPS communication with IP-10 devices when using JDK_412 , in the `java.security` file located in `/conf/security` under your `JAVA_HOME`, remove the TLS protocol entry from the `jdk.tls.disabledAlgorithms` list and add it to the `jdk.tls.legacyAlgorithms` list, and then restart the NetMaster server.

Enabling the SNMP Agent

The PTP 820 NMS SNMP agent makes it possible for any SNMP based management system to perform inventory and fault management of any managed network element.

SNMP Agent configuration consists of creating an SNMP Agent user, creating a High-Level Manager, and starting the SNMP Agent Service. For more information, refer to *Configuring Northbound Interface SNMP* in the *NetMaster User Guide*.

Configuring FTP/SFTP servers on Linux

Enabling FTP functionality

1. Check whether the **vsftpd** package is installed, by running:

```
rpm -q vsftpd
```

2. If vsftpd is not installed, install it using the dnf or yum commands:

```
dnf install vsftpd
```

3. After installation, open `/etc/vsftpd/vsftpd.conf` and edit the file with the following parameters:

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
listen_ipv6=NO
pam_service_name=vsftpd
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
user_sub_token=ftpuser
local_root=/home/ftpuser
chroot_local_user=YES
allow_writeable_chroot=YES
```

4. Perform the following:
   - If the server you are using has IPv6 configured, start the **vsftpd** daemon:

```
systemctl enable vsftpd
systemctl start vsftpd
```

- Otherwise, change parameter settings as follows, and then start the daemon:
  - Change listen=NO to listen=YES
  - Change listen_ipv6=YES to listen_ipv6=NO

5. Create a new file in /etc using the command: touch vsftpd.userlist and add in it the FTP user (ftpuser).
6. Create the FTP user and make sure you add correct privileges (707) to its home directory so that file transfer from PTP 820 NMS will work:

```
useradd -m -c "FTP_user" -s /bin/bash ftpuser -d /home/ftpuser
passwd <ftpuser_password>
echo "ftpuser" | tee -a /etc/vsftpd.userlist
mkdir -p /home/ftpuser
chown ftpuser:ftpuser /home/ftpuser
cd /home
chmod -R 0707 ftpuser
```

7. Create /home/ftpuser/nmsbackup and /home/ftpuser/nmsswdownload with the proper permissions:

```
mkdir /home/ftpuser/nmsbackup
chmod 757 /home/ftpuser/nmsbackup
mkdir /home/ftpuser/nmsswdownload
chmod 757 /home/ftpuser/nmsswdownload
```

Enabling SFTP functionality

1. SFTP uses the OpenSSH server daemon. To use SFTP, verify that the **sshd** service is running:

```
systemctl status sshd
```

2. Create an SFTP user:

```
useradd sftp
passwd sftp
```

This will create a user with a home directory in `/home/sftp`.

3. Restrict SFTP user access only to its home directory by adding the following five lines in the `/etc/ssh/sshd_config` file. The first line you add must be at the beginning at the line, the next four lines must be preceded by a tab:

```
Match User sftp
    X11Forwarding no
    AllowTcpForwarding no
    ForceCommand internal-sftp
```

```
    ChrootDirectory %h
```

4. Set the ownership of the user home directory to root:

```
chown root:root /home/sftp
```

5. Allow other users to read and execute in this folder:

```
chmod 755 /home/sftp
```

6. Create `/home/sftp/nmsbackup` and `/home/sftp/nmsswdownload` with the proper permissions:

```
mkdir /home/sftp/nmsbackup

chmod 757 /home/sftp/nmsbackup

mkdir /home/sftp/nmsswdownload

chmod 757 /home/sftp/nmsswdownload
```

7. Make sure that in `/etc/ssh/sshd_config`, the `UsePAM` is set to `yes`.
8. Preserve the default Unix umask by making sure that the following line exists in the `/etc/pam.d/sshd` file:

```
session optional pam_umask.so umask=0022
```

9. Restart the sshd service:

```
systemctl restart sshd
```

Managing Maximum Number of Open Files on Linux

On a Linux system there are cases where the default number of files that a process can open, 1024, is not enough. In those cases, upon starting the process from **systemctl** the error “Too many open files” is received. To increase the number of files that a process can open:

1. Open the following file in a text editor:

```
/etc/security/limits.conf
```

2. Add the following lines, then save and exit the file.

```
<NMS_system_user>          soft    nofile          96000

<NMS_system_user>          hard    nofile          96000

<NMS_system_user>          soft    memlock         unlimited

<NMS_system_user>          hard    memlock         unlimited
```

3. Open the following files in a text editor:

```
/etc/systemd/user.conf

/etc/systemd/system.conf
```

4. In both those files, add (or edit) the following lines, then save and exit the files.

```
DefaultLimitNOFILE=65535

DefaultLimitMEMLOCK=infinity
```

5. Open the following file in a text editor:

```
/etc/sysctl.conf
```

6. Add (or edit) the following line, then save and exit the file.

```
vm.max_map_count=262144
```

Increasing the ARP table on Linux

High-load deployments that support thousands of devices with frequent polling and full performance counters collection, require increasing the Linux ARP table to support many connections. To increase the Linux ARP table:

1. Open the following file in a text editor:

   ```
   /etc/sysctl.conf
   ```

2. Edit the values of the following parameters, or add them if they are missing. The values shown below are the recommended values for deployments with 20,000 managed devices.

   a. For deployments where devices are managed using IPv4:

   ```
   net.ipv4.neigh.default.gc_thresh1 = 16384
   net.ipv4.neigh.default.gc_thresh2 = 32768
   net.ipv4.neigh.default.gc_thresh3 = 65536
   ```

   b. For deployments where devices are managed using IPv6:

   ```
   net.ipv6.neigh.default.gc_thresh1 = 16384
   net.ipv6.neigh.default.gc_thresh2 = 32768
   net.ipv6.neigh.default.gc_thresh3 = 65536
   ```

3. Save the file changes and exit the text editor.
4. In the Linux CMD terminal run the following command in order to load the new configuration:

   ```
   sysctl -p
   ```

   The values for thresh1, thresh2 and thresh3 should be correlated with the number of managed devices.

Maintenance issues

Server generates various log files. These files tend to grow large when managing networks with many elements and heavy traffic.

Delete old server log files

Locate your log file directory and remove all files older than three months:

Installation directory:

```
<PTP 820 NMS installation>\Server\wildfly-15.0.0.Final\server\ngnms\log
```

Example for Windows:

```
C:\Program Files\PTP 820 NMS\Server\wildfly-15.0.0.Final\server\ngnms\log
```

Delete old System Manager log files

Navigate to the System Manager log file directory and remove all files older than three months.

System Manager log file directory:

```
<PTP 820 NMS installation>\SystemManager\tomcat\sysman_logs
```

Example for Windows:

```
C:\Program Files\PTP 820 NMS\SystemManager\tomcat\sysman_logs
```

Backup important files and folders

A full system recovery is likely to take less time if these files and folders are backed up regularly:

- License file for :
  `<PTP 820 NMS installation>\Server\wildfly-15.0.0.Final\server\ngnms\license\sw-nms.key`
- Database server connection parameters and other settings (also copy sub folders):
  `<PTP 820 NMS installation>\SystemManager\conf\*`
- Database backup files. Can be stored on user configurable folders.
  Default folder for Windows is: `C:\NgNMS\backup\database`
  Default folder for Solaris is: `/usr/PTP 820 NMS/backup/database`

Chapter 4: PTP 820 NMS Server High Availability Setup

Server High Availability setup is intended to ensure continuous operation.

The PTP 820 NMS High Availability setups include:

- 1+1 High Availability (1+1 HA). In this setup, the SQL database must be PostgreSQL
- 2+2 High Availability (2+2 HA). In this setup, the SQL database must be PostgreSQL
- 1+1 Server High Availability (1+1 Server HA). In this setup, the SQL database may be either Postgres or Oracle. For Oracle, the RAC feature may be used, as described in Multiple RDBMS using Oracle RAC.

Note: Many of the tasks detailed in the following sub-sections are performed in System Manager. See the *PTP 820 NMS User Guide* for a detailed explanation of System Manager and how to use it.

Prerequisites to configuring Server a High Availability

Make sure you meet the following prerequisites before configuring any high availability setup, whether 1+1 High Availability, 2+2 High Availability, or 1+1 Server High Availability:

:

- You must obtain a license with a server High Availability feature for each of the two servers.
- The license settings on both servers must be **identical**.
- The Operating System on both servers must be identical: either both Solaris or both Windows.
- The version to be installed on both servers must be identical.
- Both servers must use the same user/schema.
- Both servers should be set up as Trap Managers.
- Northbound interface should be configured for both servers. In both servers, the NG NMS SNMP Agent service should be set (in the operating system's Services) to start automatically upon a server restart.
- Ensure that the UTC time on both servers is the same.

- For Linux setups, verify that rsync is installed, by running the rpm -q rsync command. If the message package rsync is not installed appears, run the yum install rsync command as root to install **rsync**.

PTP 820 NMS Configuring Server High Availability

The following section explains how to configure a PTP 820 NMS 1+1 High Availability or 2+2 High Availability setup. These kinds of setups rely on a Postgres Database. For a high availability setup that relies on Oracle Database see: Multiple RDBMS using Oracle RAC.

Installing SQL Database

Install the database on the servers intended as Primary and Failover, as described in Database Installation.

Reminder:

- In a 1+1 HA setup, the databases are collocated with the PTP 820 NMS Servers.
- In a 2+2 HA setup, the databases must be installed on two other machines, distinct from the machines hosting the PTP 820 NMS Servers.

Installing PTP 820 NMS

After meeting the Prerequisites to configuring Server a High Availability, install PTP 820 NMS on the servers intended as Primary and Secondary, as described in New PTP 820 NMS Installation for Windows and New PTP 820 NMS Installation for Linux.

Reminder:

- In a 1+1 HA setup, the PTP 820 NMS Servers are collocated with the SQL databases.
- In a 2+2 HA setup, the PTP 820 NMS Servers must be installed on two other machines, distinct from machines hosting the SQL database machines.

Creating the SQL Database Active and Failover User/Schemas

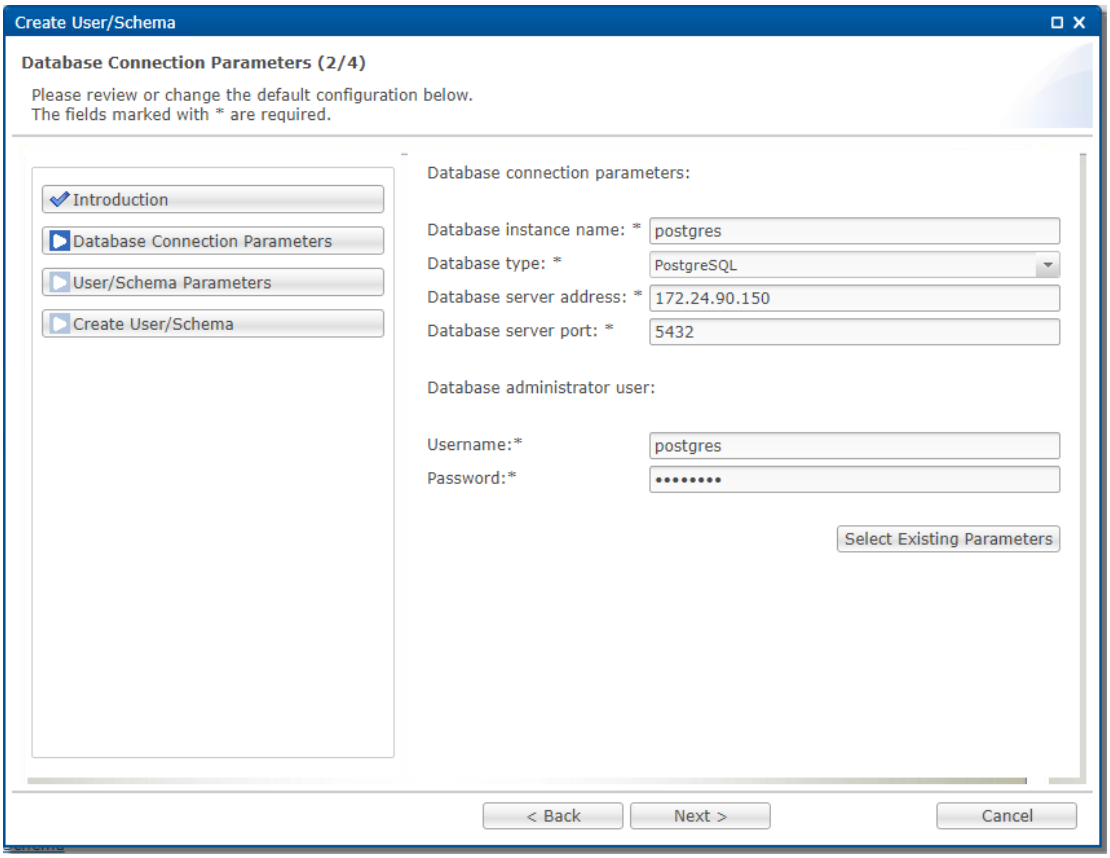
Using the System Manager of the Primary PTP 820 NMS Server, create two database user/schemas: one schema on the designated Primary Database and one schema on the designated Failover Database.

The schemas must have different names. We recommend names that indicate the designated role:

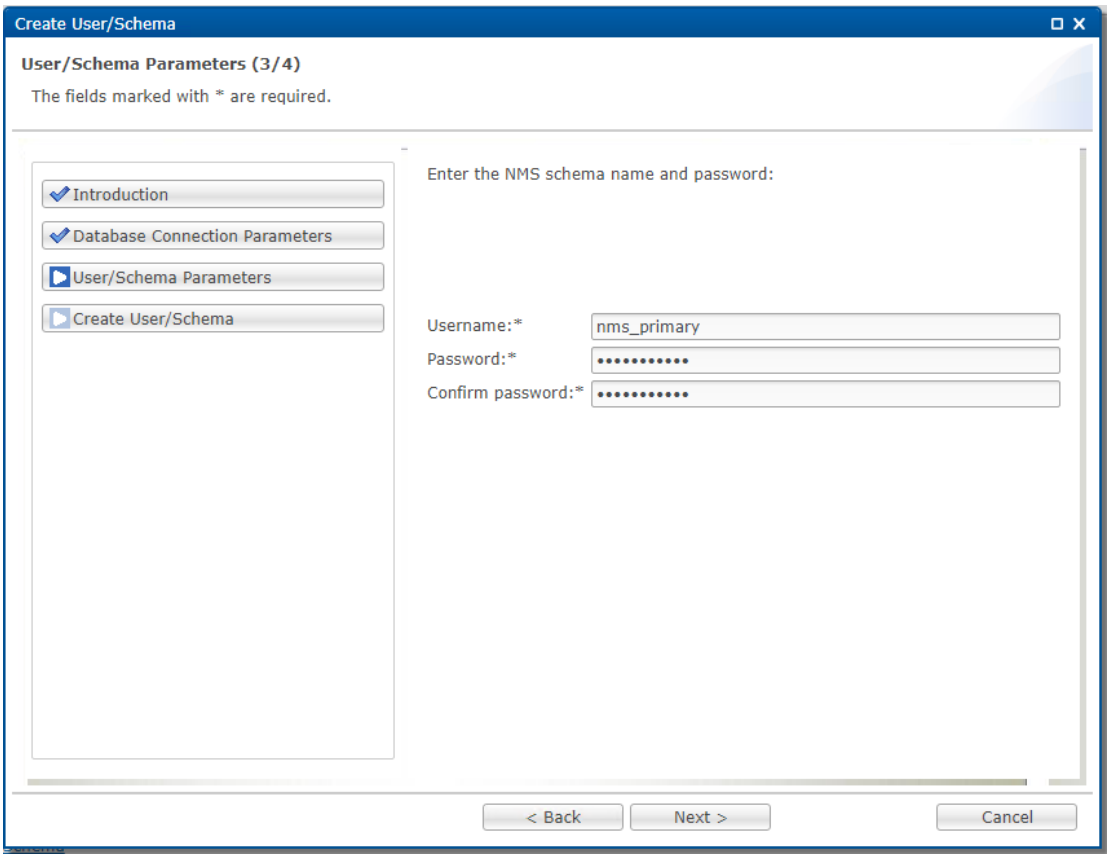
- For primary: <some_name>_primary
- For failover: <some_name>_failover

1. Create the designated primary user/schema as follows:
   i. In System Manager, go to Database Tasks > Create User/Schema.
   ii. In the Database Connection Parameters page:
   - In a 1+1 HA Setup, the Database server address must be the IPv4 address or machine hostname of the Primary (Active) PTP 820 NMS Server.
   - In a 2+2 HA Setup, the Database server address must be the IPv4 address or machine hostname of the machine designated as the primary database machine.

     Make sure that the mate server, SQL database and Elasticsearch nodes can all be reached using the same network interface.



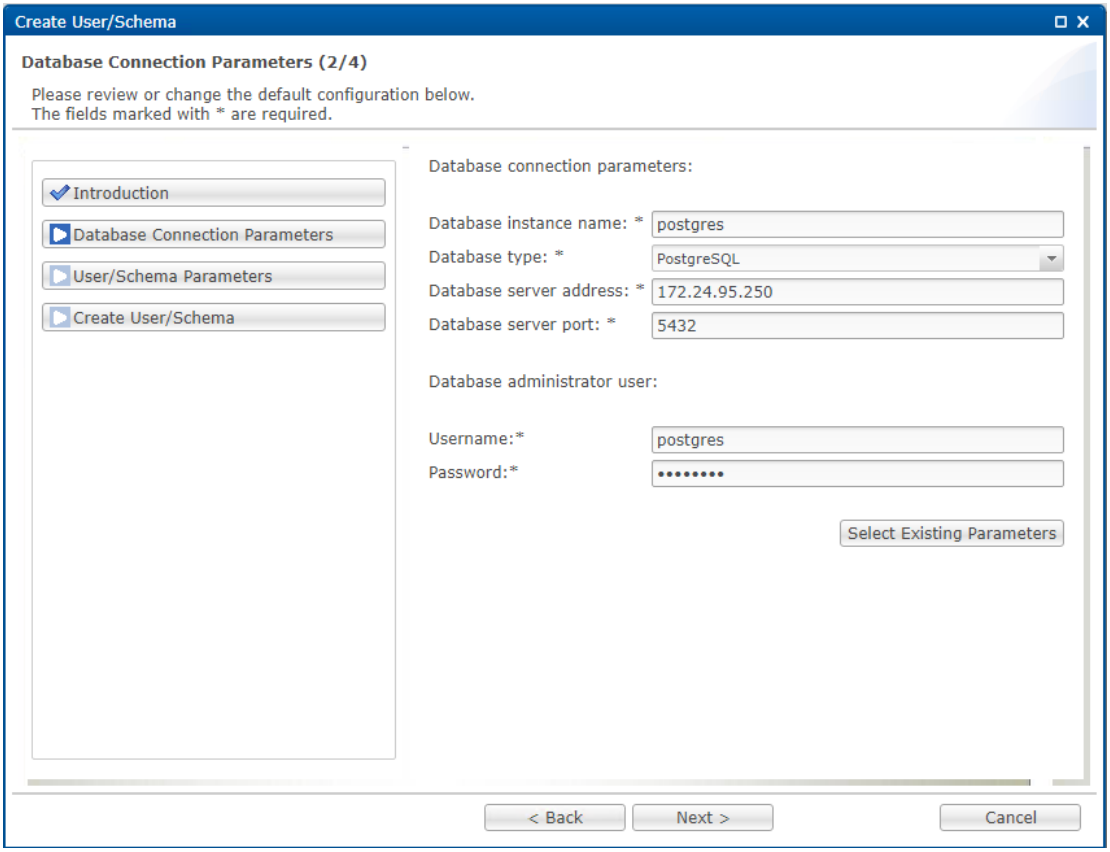
iii. In the User/Schema Parameters page, specify the username and the password for the primary database user/schema.



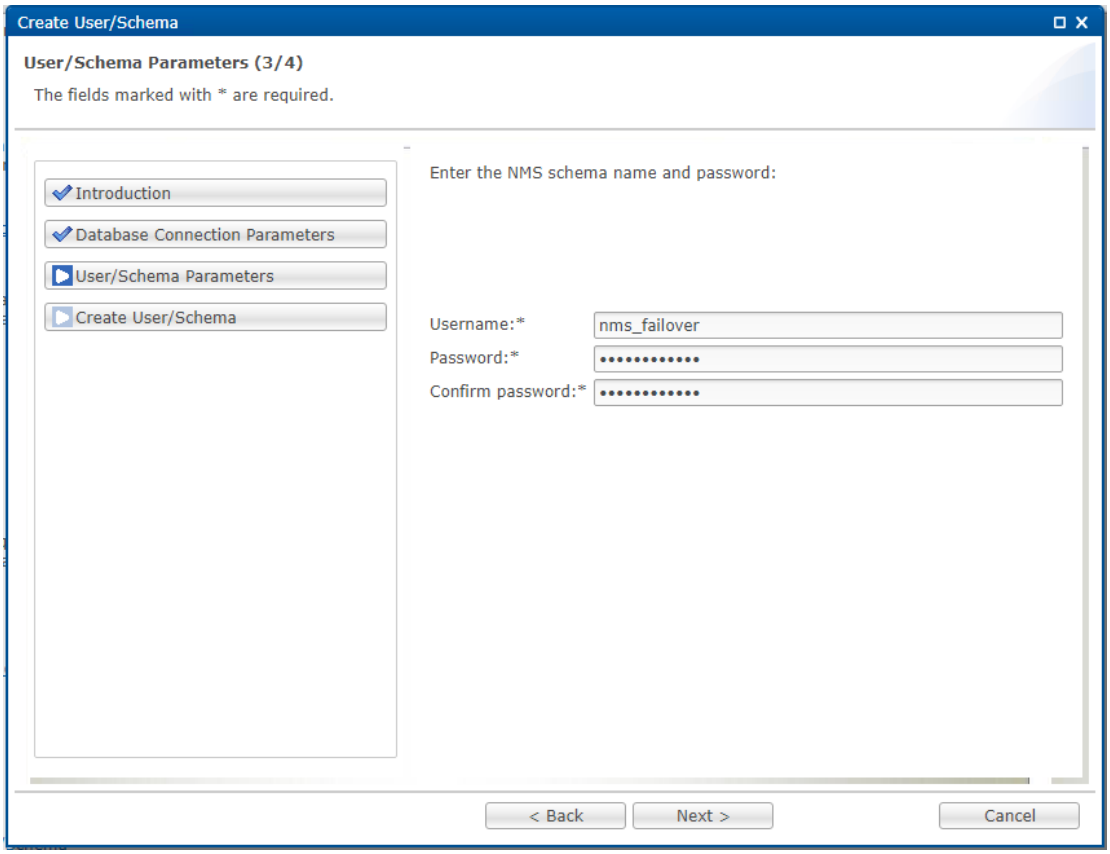
iv. Finish and exit the wizard.

2. Create the designated failover user/schema:
   - In System Manager, go to Database Tasks > Create User/Schema.
   - In the Database Connection Parameters page - In a 1+1 HA Setup, the Database server address must be the IPv4 address or machine hostname of the Secondary (Standby) PTP 820 NMS Server.
   - In a 2+2 HA Setup, the Database server address must be the IPv4 address or machine hostname of the machine designated as the failover database machine.

   Make sure that the mate server, SQL database and Elasticsearch nodes can all be reached using the same network interface.



3. In the User/Schema Parameters page, specify the username and the password for the failover database user/schema.



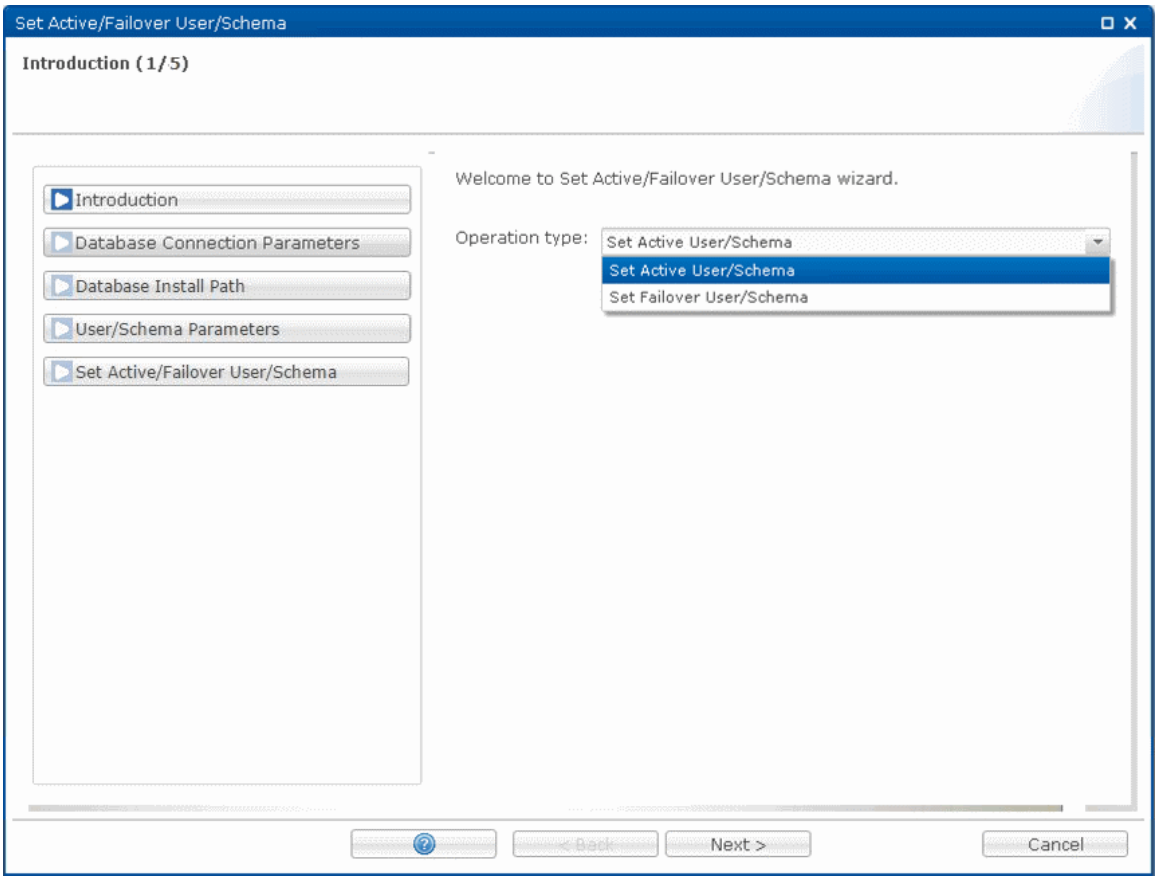
4. Finish and exit the wizard.

Defining the SQL Active and Failover user/schema for Primary PTP 820 NMS Server

On the System Manager of the Primary Server, define the Active Database, as follows:

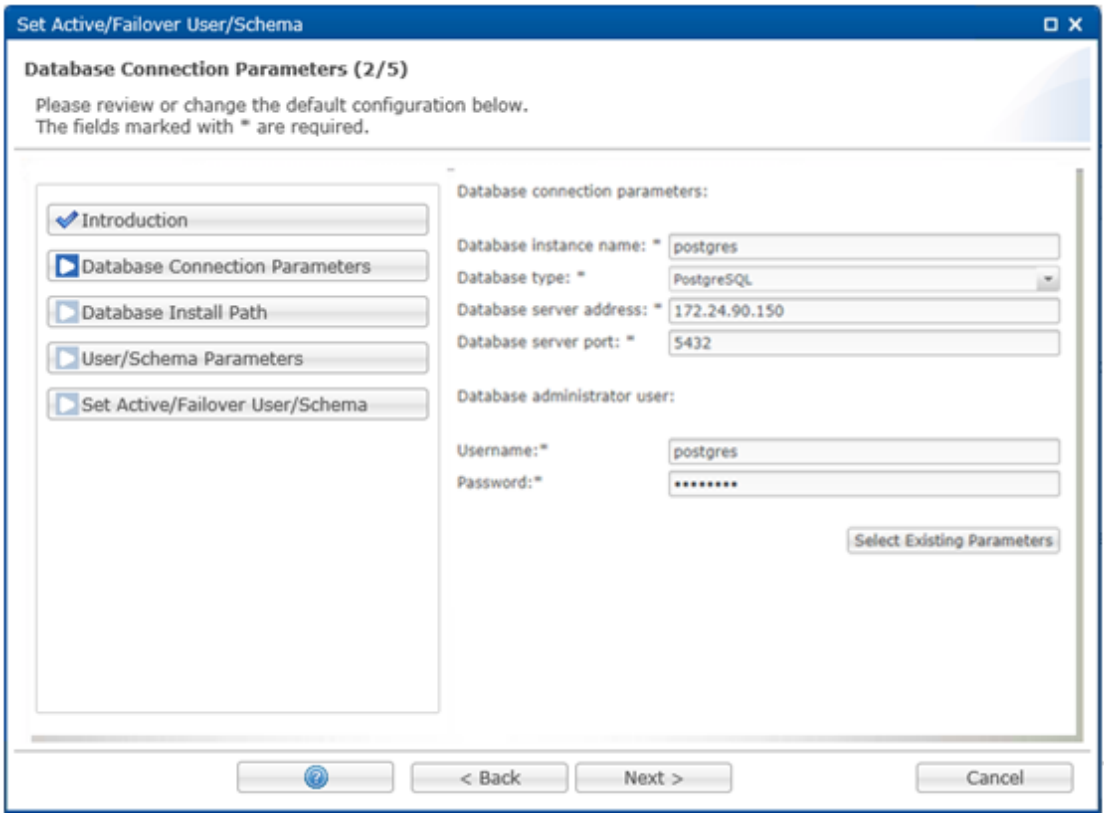
i. In System Manager, go to Database Tasks > Set Active/Failover User/Schema.

ii. In the Introduction page of the Set Active/Failover User/Schema wizard, set Operation type to Set Active User/Schema.

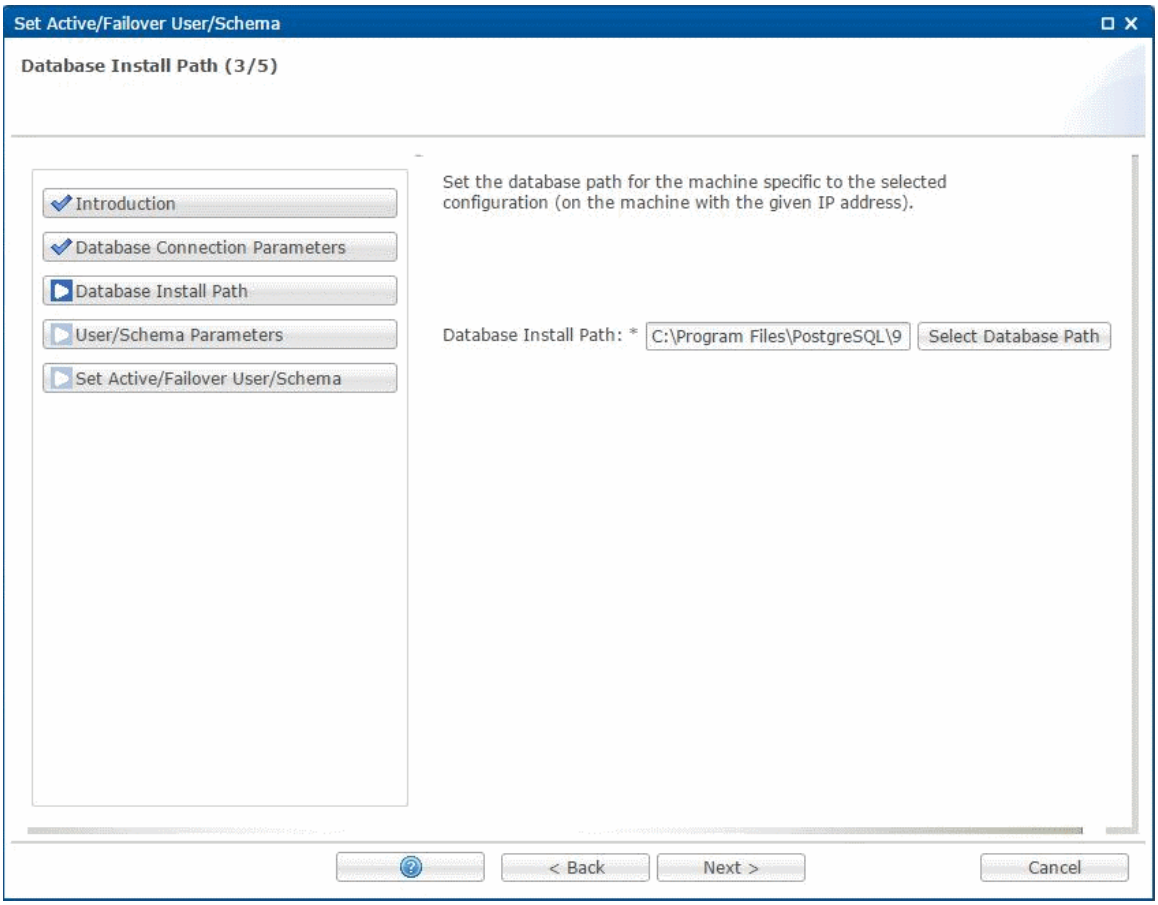


iii. In the Database Connection Parameters page, make sure the Database server address of the active database is entered as an IPv4 address or machine hostname (and not localhost or 127.0.0.1).

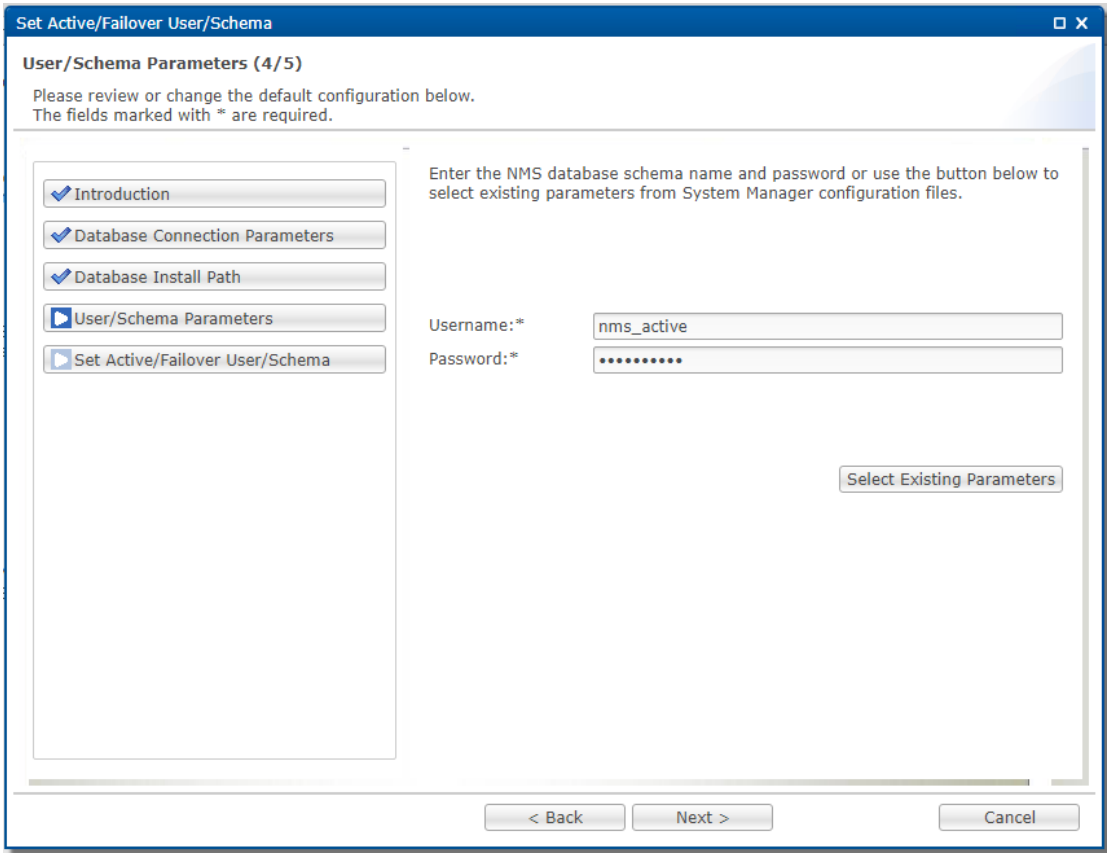
- In a 1+1 HA Setup, the Database server address must be the IPv4 address or machine hostname of the Primary (Active) PTP 820 NMS Server.
- In a 2+2 HA Setup, the Database server address must be the IPv4 address or machine hostname of the machine designated as the primary database machine.



In the Database Install Path page, specify the active database installation folder.



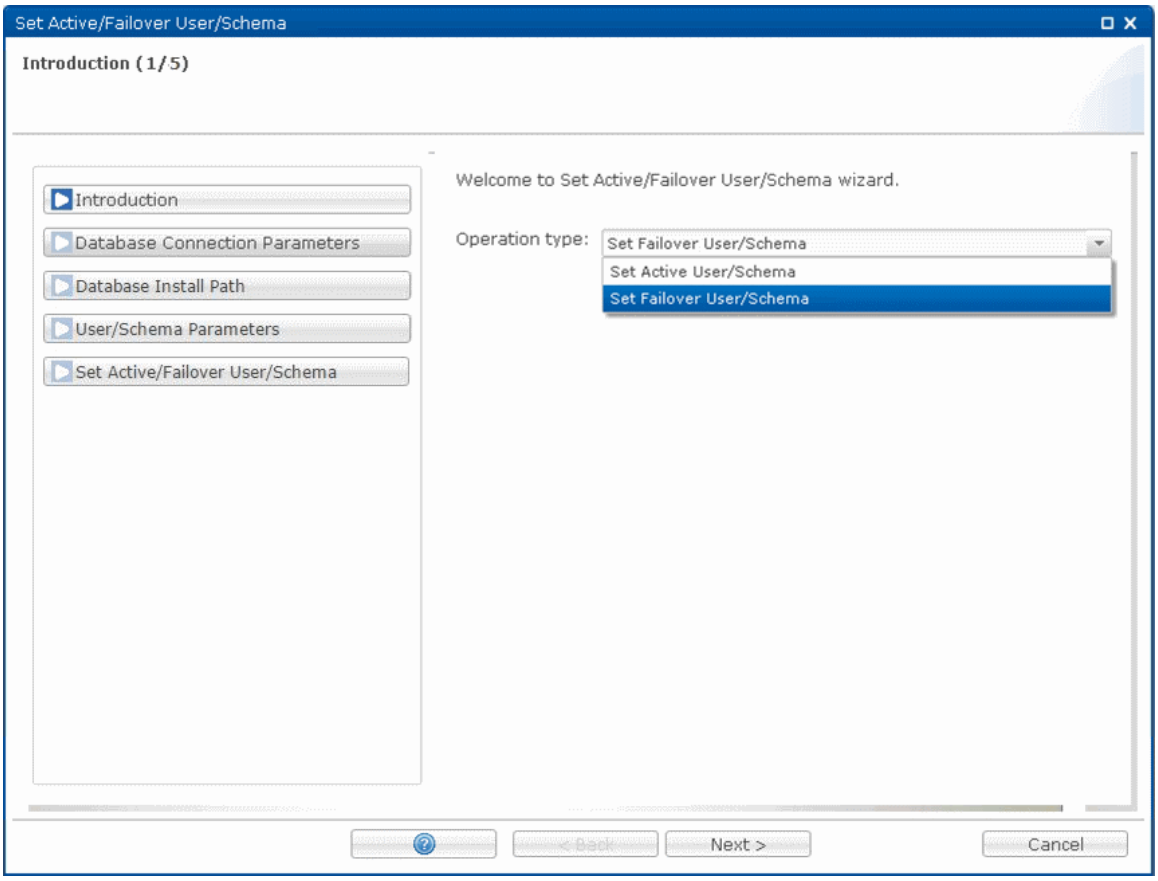
5. In the User/Schema Parameters page, provide the username and password for the designated primary user/schema.



On the System Manager of the Primary Server, define the failover database, as follows:

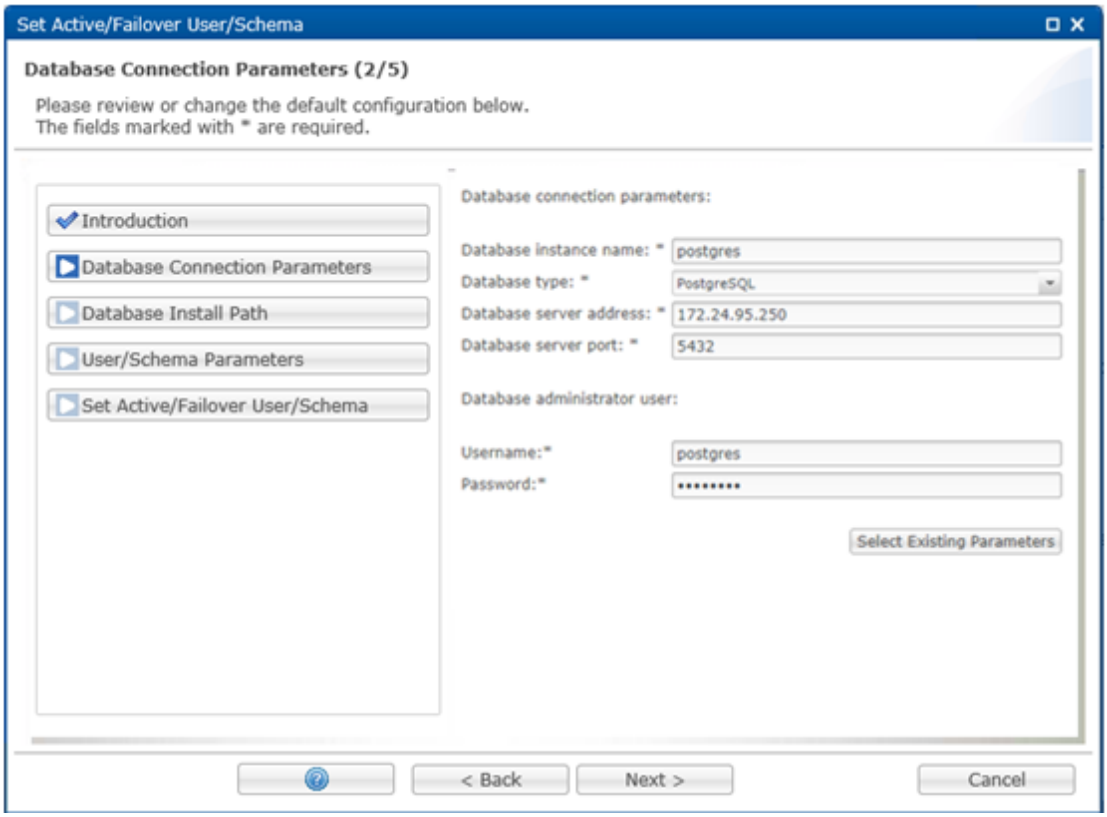
i. In System Manager, go to Database Tasks > Set Active/Failover User/Schema.

ii. In the Introduction page of the Set Active/Failover User/Schema wizard, set Operation type to Set Failover User/Schema.

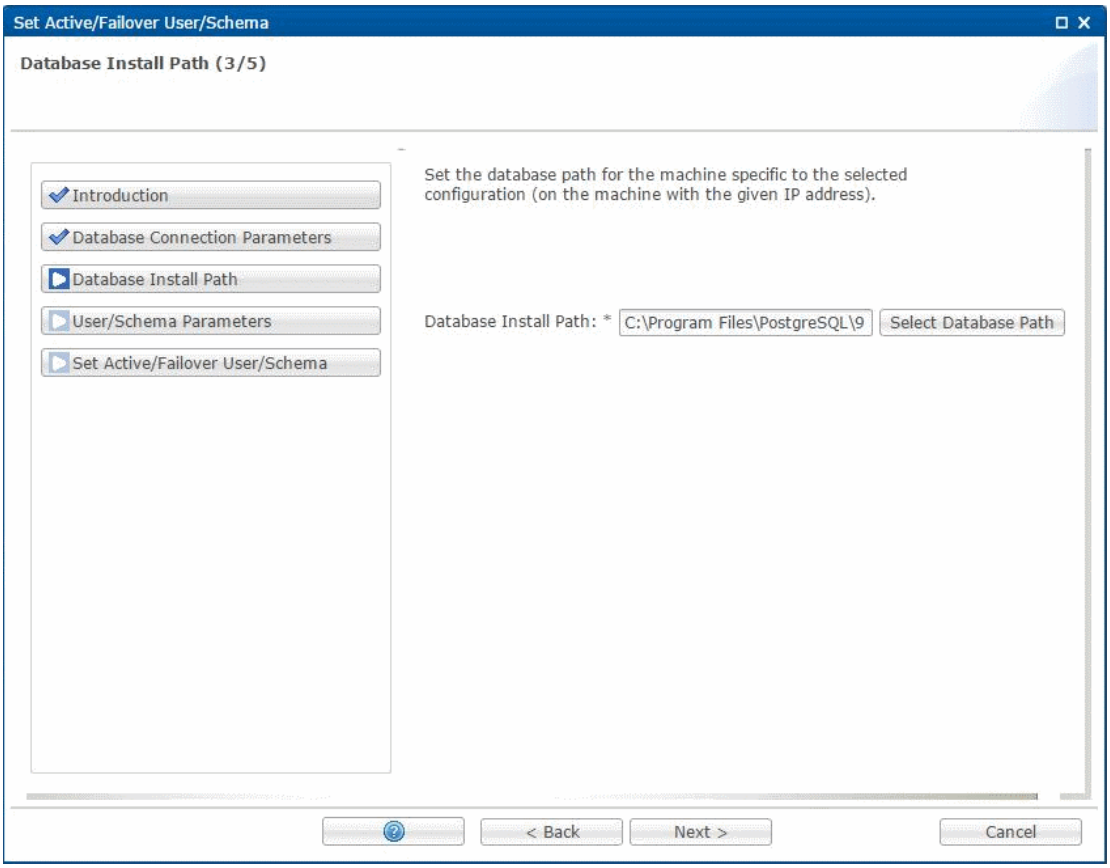


iii. In the Database Connection Parameters page, make sure the Database server address of the failover database is entered as an IPv4 address or machine hostname (and not localhost or 127.0.0.1).

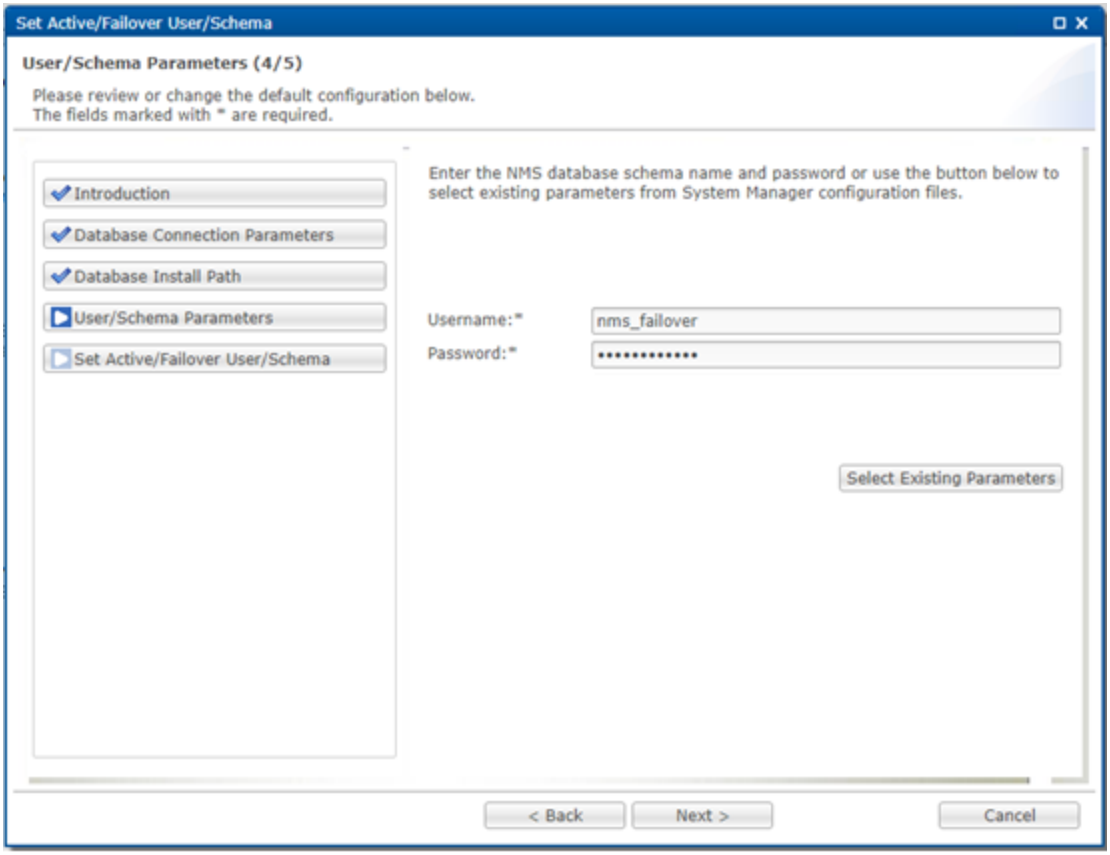
- In a 1+1 HA Setup, the Database server address must be the IPv4 address or machine hostname of Secondary (Standby) PTP 820 NMS Server.
- In a 2+2 HA Setup, the Database server address must be the IPv4 address or machine hostname of the machine designated as the failover database machine.



iv. In the Database Install Path page, specify the failover database installation folder.



v. In the User/Schema Parameters page, provide the username and password for the designated failover user/schema.



Defining the SQL Active and Failover user/schema for Secondary PTP 820 NMS Server

On the System Manager of the Secondary Server, define the Active and Failover user/schema in the same way as described in Defining the SQL Active and Failover user/schema for Primary PTP 820 NMS Server.

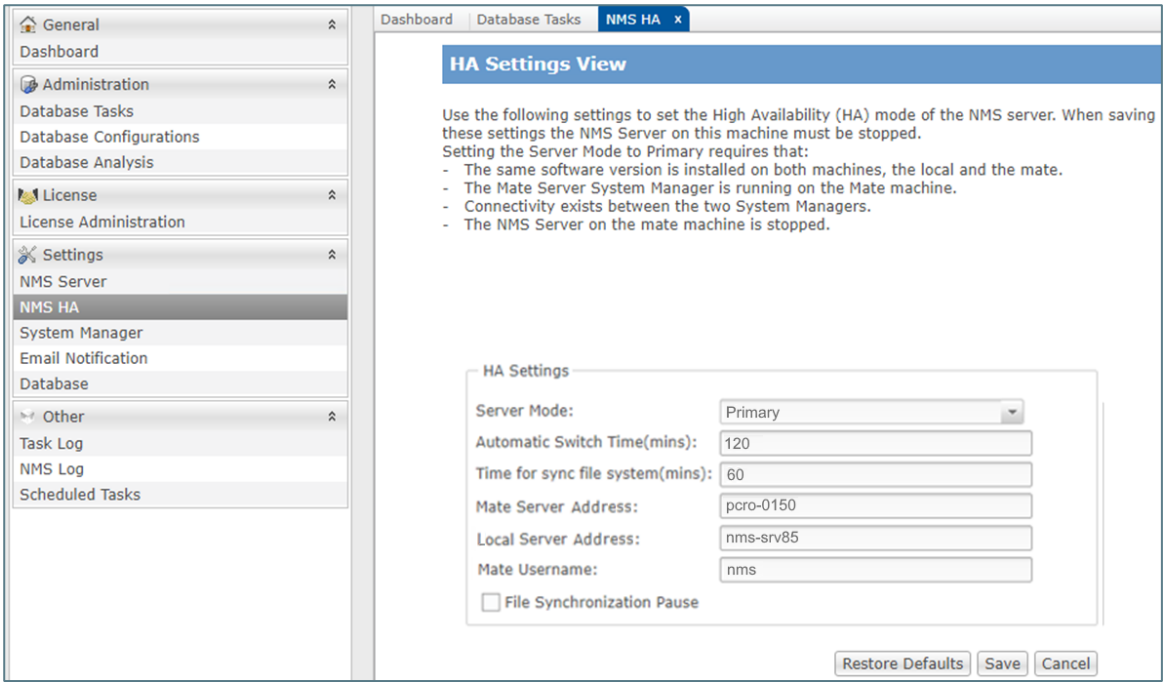
Enabling Server High Availability

After performing Defining the SQL Active and Failover user/schema for Primary PTP 820 NMS Server and Defining the SQL Active and Failover user/schema for Secondary PTP 820 NMS Server, configure server High Availability as follows:

1. Ensure there is connectivity between all System Managers.
2. Configure secure communications between the machine hosting the Primary PTP 820 NMS Server and the machine hosting the Secondary PTP 820 NMS Server, as described in Setting up secure communications between the two mate machines. This will enable file synchronization for server High Availability.
3. In the NMS HA View of the Primary server's System Manager:
   i. Set the Server Mode to Primary.
   ii. Optionally change the default settings of the Automatic Switch Time and Time for sync file system fields.

iii. Specify the IPv4 address or machine hostname of the Secondary server in the Mate Server IP field.

iv. Specify a domain username of the mate server in the Mate Username field.



4. In the NMS HA View of the Primary server's System Manager, click Save.

   If the HA configuration completes successfully, no error messages appear, and the Save button is greyed out.

   If the following error is displayed in the dashboard: Something went wrong during mate verification, this indicates that there is a problem/inconsistency with the configuration between the two servers. In that case, verify the following at the Secondary server:

   - Connectivity with the mate
   - Connectivity with DB

5. In the Dashboard View of the Primary server's System Manager, verify that HA Configuration Status is Configuration saved. Note:
   - In the Dashboard View of the Primary server, the HA State will be Active.
   - In the Dashboard View of the Secondary server, the HA State will be Standby.

Performing PTP 820 NMS Elasticsearch Cluster Configuration

Following the definition of SQL Active/Failover User/Schemas for the Primary and Secondary server and Enabling Server High Availability, you need to perform Elasticsearch cluster configuration as described in PTP 820 NMS Elasticsearch Cluster Configuration.

Setting up secure communications between the two mate machines

For file synchronization to work between the two mate machines, set up a secure communication tunnel as described in this section.

The following sub-sections describe how to configure secure file synchronization on Windows and on Linux. On Windows we utilize Robocopy with SMB encryption, and on Linux we utilize rsync with SSH.

During synchronization, all -related files under the NgNMS folder are copied to the other server under the same folder hierarchy.

- In Windows, the folder path is c:\NgNMS
- In Linux, the folder path is /usr/NgNMS

PTP 820 NMS related files have unique names. Any user files that are not uniquely named may be overwritten.

Securing communications between mates on Windows

Perform the following on both servers:

1. Optionally configure the files folder to be synchronized at the location configured in the config_folder_location.properties file (refer to Setting the device Backup Configuration and Software Images repository folder). The default is C:\NgNMS.
2. Open Server Manager and select File and Storage Services.
3. Choose Shares.
4. Right click in the white space and choose New Share; then choose SMB Share - Quick; then press Next.
5. In the wizard enter in Type a custom path the local path of the folder (default C:\NgNMS); then press Next.
6. In Share name enter the name of the folder; then press Next.
7. Select the checkbox Encrypt data access in order to use SMB Encryption; then press Next.
8. Define the permissions as needed so that the remote machine can reach the local folder; then press Next.
9. Click Create.

Securing communications between mates on Linux

Configure SSH to work without a password

Configure SSH to work between the two mates without a password, as follows:

1. For each user under which PTP 820 NMS runs on the primary and secondary servers, generate a pair of RSA private and public keys. The keys must be generated without a password. To do so, run the following command in a terminal:

   ```
   ssh-keygen -t rsa
   ```

   The command generates two files:

   - A private key saved in /home/%user%/.ssh/id_rsa where %user% is set to the logged in user; for example: /home/LimitedUser/.ssh/id_rsa
   - A public key saved in /home/%user%/.ssh/id_rsa.pub where %user% is set to the logged in user; for example: /home/LimitedUser/.ssh/id_rsa.pub

2. On each machine, perform the following to access the other machine using SSH without a password:
   i. Login on the other computer
   ii. Perform either of the following:

   Create the following file: /home/%user%/.ssh/authorized_keys, and add to authorized_keys only the public key from the first machine.

   OR

   Run the command ssh-copy-id %user%@%ip%, where user and IP are the credentials from the other machine. For example: ssh-copy-id user1@192.168.1.10.
   When prompted, enter the password of the user.

   iii. Verify that when running the following, you are logged in automatically without being required to provide a password:

   ssh %user%@%host%

   For example:

   ssh User1@192.168.1.10

3. If any of the mate machines has SFTP installed, change the default SSH port 22 to another unused port in each mate machine's SSH_config and SSHD_config files (standard busy ports can be found in: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers). Both mates must use the same SSH port number.

Working with non-default backup folders

If you wish to save backups in folders that are not the default PTP 820 NMS backup folder, make sure that the user under which PTP 820 NMS runs, which by default is the one giving the synchronization command, has write and read permissions to the non-default backup folders.

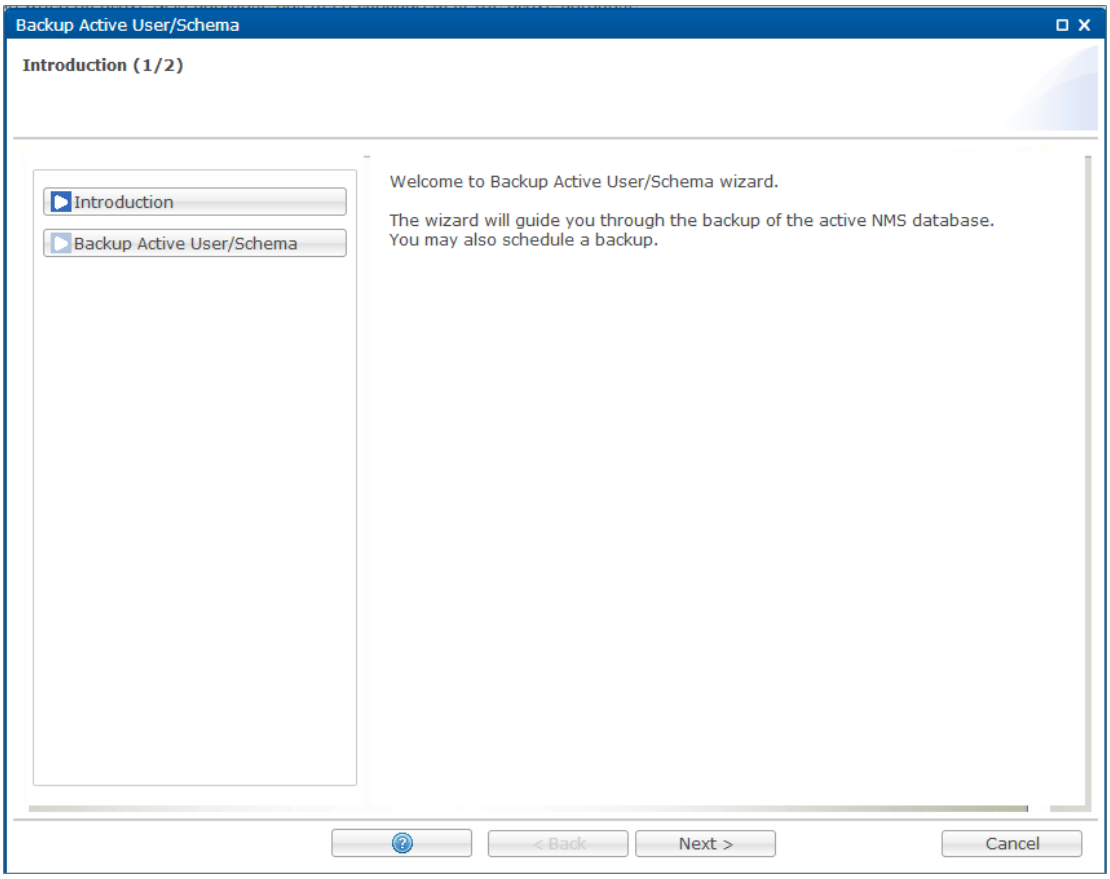
Schedule a Backup of the Active Database in High Availability setup

This section describes the steps required for scheduling an automatic backup of the Active database. Active database backup is a separate task than the database replication and provides extra protection in case of failures.

In a 1+1 HA or 2+2 HA setup, it is recommended that each PTP 820 NMS Server (both the Primary and the Secondary) create backups of the Active database only, but at different times of the day. knows which is the Active database at any given moment – either the Primary or the Secondary database.

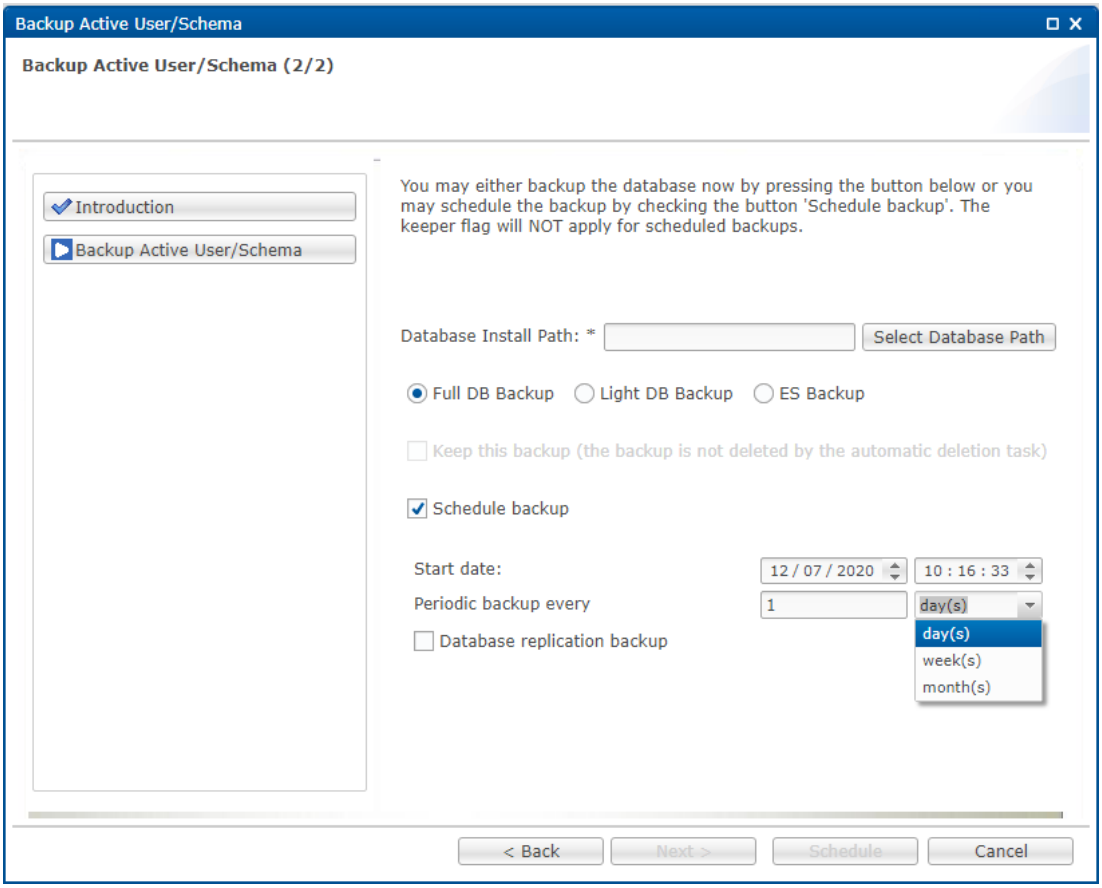
Note: For a setup with a large database, see the database backup recommendations in Database High Availability – performance considerations.

1. On the System Manager of the Primary server, create a scheduled Active database backup, as follows:
   i. In the Introduction page of the Backup Active User/Schema wizard, click Next.



ii. In the Backup Active User/Schema page, enter the database installation path, select the Schedule Backup checkbox, set the Start date and time as well as the frequency of the periodic backup, and click Schedule.

Note: Do not select the Database Replication backup checkbox, because you are now not setting the Replication frequency for the Database High Availability function.



iii. Repeat the above steps on the Secondary PTP 820 NMS Server, but schedule the backup for a different time.

Keep in mind:

- It is recommended to run the Backup task first and then the Replication task.
- Make sure that there is a large enough time interval between the Backup task and the Replication task in order to avoid tasks overlaps. In large setups (over 5K NEs), at least 4 hours between the tasks is recommended.

Defining the Database Replication Frequency

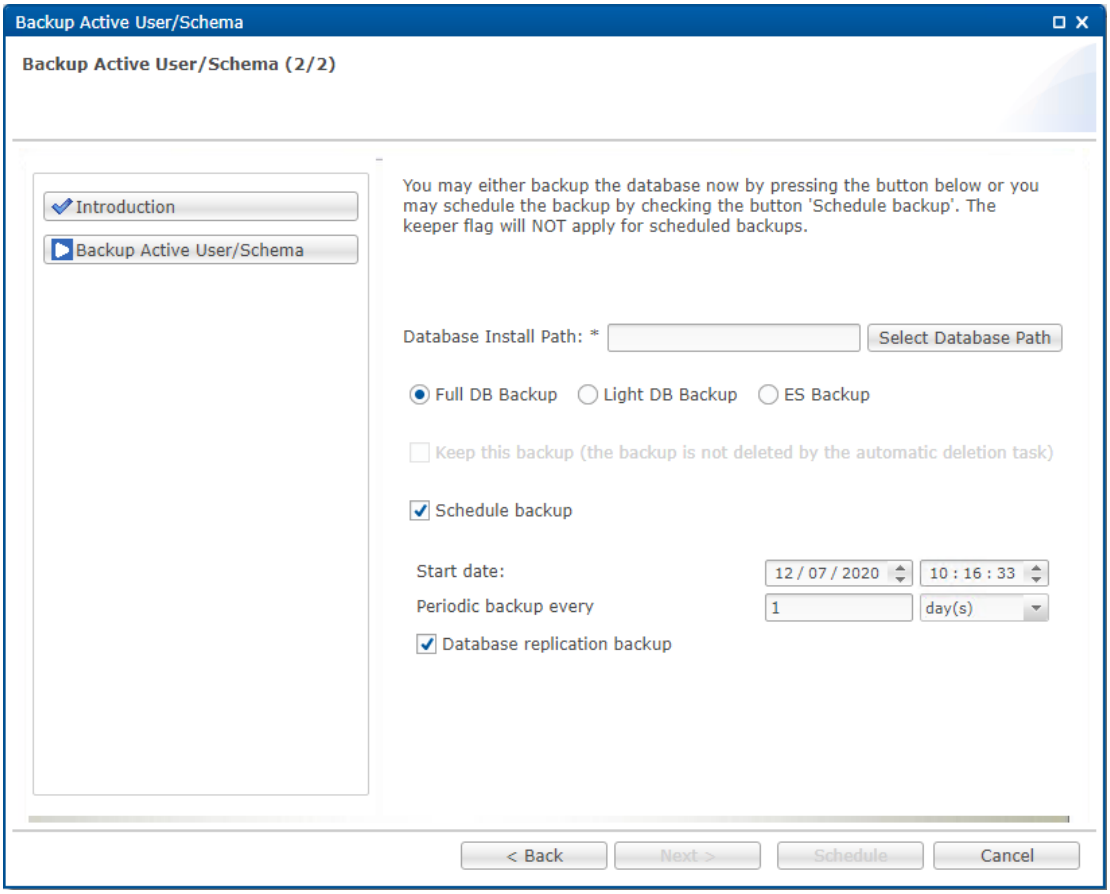
On the System Manager of the server, set the database replication frequency as described in this section. Note that replication is always made from the currently Active database to the current Failover database.

Note: The procedure described in this section must be performed identically in the System Manager of each of the two mate servers. The reason is that although replication is performed only on the Primary server, following a switchover the Secondary server becomes the Primary server. For a setup with a large database, see the database replication recommendations in PTP 820 NMS High Availability setup – performance consideration.

1. In the Backup Active User/Schema page of the Backup Active User/Schema wizard:

i. Select the Schedule Backup checkbox, and set the Start date and time, as well as the frequency of the periodic backup. The frequency settings apply also to database replications.

ii. Select the Database Replication backup checkbox. The replication frequency you set will apply to the database that is the active database at the time replication occurs.



PTP 820 NMS High Availability setup – performance considerations

For large setups having a large database, the Schedule a Backup of the Active Database in High Availability setup and Defining the Database Replication Frequency operations should NOT be scheduled during nighttime, so as not to affect the nightly poll.

We recommend setting the following schedule:

- Backup Active database on Primary (Active) Server – set to 8:00 daily
- Replicate Active database – set to 14:00 daily
- Backup Active database on Secondary (Stand-by) Server – set to 16:00 daily

Upgrading a High Availability setup

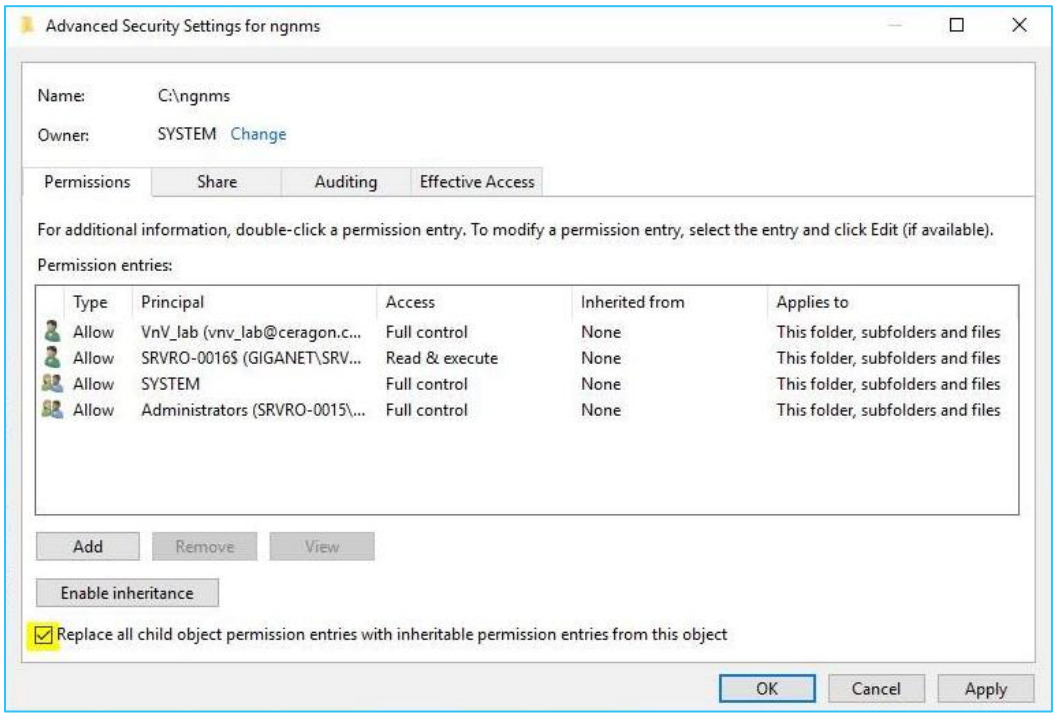
This section applies to 1+1 High Availability and 2+2 High Availability setups.

Both servers participating in a 1+1 High Availability or 2+2 High Availability setup must run the same software version. Therefore, to upgrade the versions of two servers in a High Availability configuration, you must perform the following:

1. In both servers, follow the instructions listed in Before upgrading in Windows or Before upgrading in Linux.
2. Stop both servers.
3. Upgrade to the new version on the Secondary server, by following the instructions in Performing an upgrade in Windows or Performing an upgrade in Linux.

   In System Manager's Initial Setup wizard, make sure to provide the details for accessing the existing Active database; followed by setting up the existing Failover database.
4. From System Manager on the Secondary server, perform Upgrade User/Schema for the Failover database.
5. Upgrade to the new version on the Primary server, by following the instructions in Performing an upgrade in Windows or Performing an upgrade in Linux.

   In System Manager's Initial Setup wizard, make sure to provide the details for accessing the same existing Active database followed by setting up the existing Failover database you specified for the Secondary Server (in the previous Step 3). The databases will not be upgraded, since this was already done.
6. Configure Server High Availability as described in **Enabling Server High Availability**.
7. Execute Cluster Configuration as described in PTP 820 NMS Elasticsearch Cluster Configuration.
8. Due to the new file synchronization implementation in R21A00, when upgrading from PTP 820 NMS versions older than 21A00, the following changes must be performed on the NgNMS folder:
   - Remove the deny permissions that are added automatically on the folder by Cygwin.
   - Apply permissions on all subfolders of the NgNMS folder as well, by checking the checkbox shown in yellow below.



Because Cygwin is no longer used, you can remove it from the two server machines by following the steps provided on the official Cygwin website's FAQ section.

9. Start the Primary server.
10. Start the Secondary server.

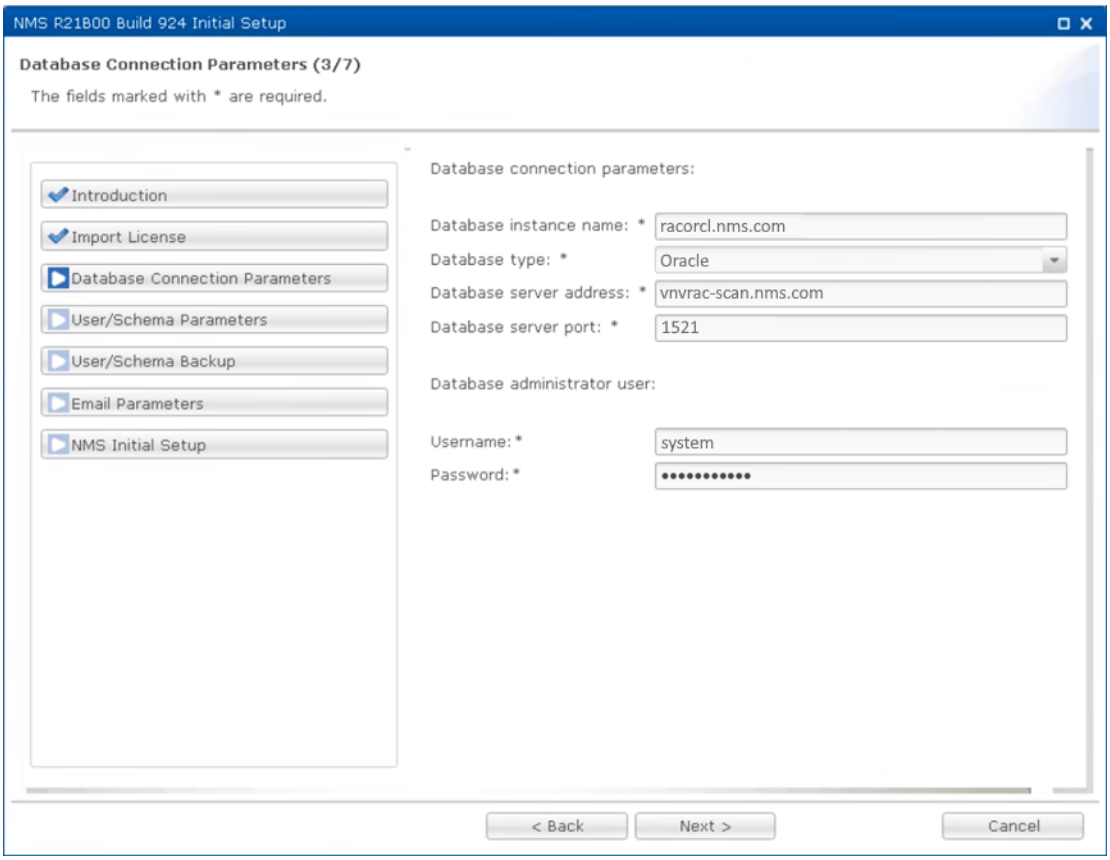
Multiple RDBMS using Oracle RAC

Oracle RAC 12 is not supported.

When installing each of the two servers which will participate in a server High Availability setup, do the following:

1. In the Database Connection Parameters page of the Initial Setup wizard:
   i. Set the Database instance name to the Service Name configured for RAC.
   ii. Set the Database type to Oracle.
   iii. In the Database server address field, instead of entering an address, enter the DNS address of the RAC instances (all the nodes on which RAC is installed are configured in the DNS).

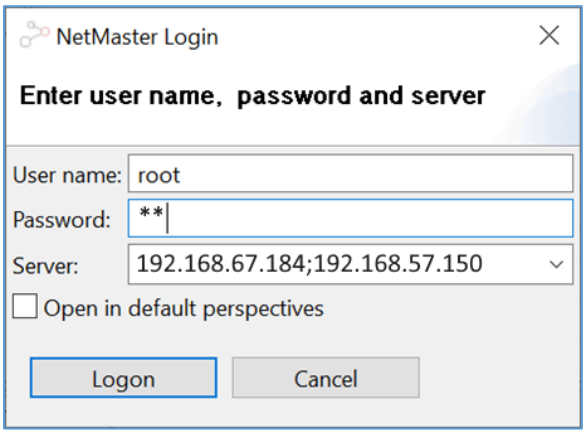
   The rest of the settings are the same as for regular databases.



2. After setup is complete, Click Close to complete the PTP 820 NMS Initial Setup wizard.

Starting the Primary and Secondary Servers

1. Start the Primary and Secondary servers, by clicking Start in the Dashboard View of their System Managers. You must start the Primary server first, and wait until it is up and running before starting the Secondary server.
   In any case where you need to start both the Primary and Secondary servers, you must start the Primary server first, and wait until it is up and running before starting the Secondary server.
2. When logging in, enter in the Server field the addresses of both the Primary and the Secondary servers, separated by a semicolon.



Note: Make sure to configure backup of the Primary and Secondary servers, in System Manager, at different, non-overlapping times.

Chapter 5: Abbreviations

A	
AD	Administrative domains
AJP	Apache JServ Protocol
ASCII	American Standard Code for Information Interchange

C	
CDB	Container Database
CLI	Command Line Interface

D	
DBA	Database administrator
DNS	Domain Name System

E	
EJB	Enterprise Java Beans
ES	Elasticsearch

F	
FCPS	Fault, Configuration, Performance and Security
FTP	File Transfer Protocol

G	
GUI	Graphical User Interface

H	
HA	High Availability

HTTP	Hypertext Transfer Protocol
HTTPS	Secured Hypertext Transfer Protocol

I	
IDE	Integrated Development Environment
IP	Internet Protocol

J	
JDK	Java Development Kit
JNDI	Java Name and Directory Interface
JRE	Java Runtime Environment
JRMP	Java Remote Method Protocol

N	
NE	Network Element
NIC	Network Interface Controller
NMS	Network Management System

O	
OSS	Operations Support System

R	
RAC	Oracle Real Application Cluster
RAM	Read-only Memory
RDBMS	Relational Database Management System
RSA	Rivest–Shamir–Adleman cryptosystem for public-key encryption

S	
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol

T	
TCP	Transmission Control Protocol

U	
UDP	User Diagram Protocol
UTC	Coordinated Universal Time

W	
Wildfly	Java application server