



NetBrain® Integrated Edition 10.1

System Upgrade Guide

Two-Server Deployment

Contents

1. Upgrading System	3
1.1. Terminating System Tasks and Sessions.....	4
1.2. Stopping Server Services	5
1.3. Backing Up MongoDB Data.....	6
1.4. Upgrading NetBrain Database Server	7
1.5. Upgrading NetBrain Application Server	14
1.5.1. Uninstalling Proxy Server.....	22
1.6. Activating Subscription License	22
1.7. Verifying Upgrade Results.....	23
1.8. Allocating Tenants to Front Server Controller	24
1.9. Adding a Front Server for a Tenant.....	26
1.10. Registering a Front Server.....	27
1.11. Upgrading External Authentication.....	29
1.12. Upgrading Email Settings	29
1.13. Configuring Auto Upgrade Settings	30
1.14. Customizing MongoDB Disk Alert Rules.....	40
1.15. Tuning Live Access	41
1.16. Scheduling Benchmark Task.....	41
2. Appendix: Offline Installing Third-party Dependencies.....	43
3. Appendix: Editing a File with VI Editor	45
4. Appendix: Restoring MongoDB Data.....	46
5. Appendix: Dumping MongoDB Data	48
6. Appendix: Restoring Dumped MongoDB Data.....	49
7. Appendix: Generating SSL Certificate.....	50

1. Upgrading System

The upgrade process ensures data integrity, which means that the data in the current system will be still available after upgrading. If you encounter any issues during the upgrade process, contact [NetBrain Support Team](#) for help.

Notes: Before upgrading your system, check its current version and the network connectivity requirements.

Note: In IEv10.1, upgrading the v7.* two-server deployment will unify all the usernames and passwords, including MongoDB, Elasticsearch, RabbitMQ and Redis together with the Web API authentication key for communication between Web API Server and Knowledge Cloud Proxy/Service Monitor Agents to be same as the previous defined MongoDB username and password. If different credentials are needed for any of above services, please refer to the upgrade guide for Distributed deployment mode.

Note: The Service Monitor Agent running on the Linux server(s) uses “netbrainadmin” user, and this user needs sudoers privilege to monitor other NetBrain components as well as to execute the system update tasks.

Note: For Linux servers, make sure each path of **/usr/lib**, **/usr/share**, and **/etc** has more than **10GB** free space to install the component files.

Note: There must be more than **180GB** free space for the Application Server PostgreSQL data path.

Note: If the Web API Server is installed on a Win 2012 R2 server with certificate binding to enable HTTPS, and the certificate does not meet the requirement of TLS1.2, users need to create and bind a new TLSv1.2 compatible certificate on Web API Server to provide HTTPS. Refer to [Appendix: Generating SSL Certificate](#).

Upgrade from IEv7.0b/b1

1. [Terminate System Tasks](#)
2. [Stop Server Services](#)
3. [Back Up MongoDB Data](#)
4. [Upgrade NetBrain Database Server](#)
5. [Upgrade NetBrain Application Server](#)
6. [Unbind Perpetual License](#)
7. [Activate Subscription License](#)
8. [Verify Upgrade Results](#)
9. [Allocate Tenants to Front Server Controller](#)
10. [Add a Front Server to a Tenant](#)
11. [Register NetBrain Front Server](#)
12. [Upgrade External Authentication](#)

13. [Upgrade Email Settings](#)
14. [Customize MongoDB Disk Alert Rules](#)
15. [Tune Live Access](#)
16. [Schedule Benchmark Task](#)

Network Connectivity Requirements

Source	Destination	Protocol ^{*)} and Port Number ^{**)}
Thin Client Service Monitor Agent	Application Server	HTTP/HTTPS (80/443)
Application Server	Database Server	TCP 5672/6379/9200/27017/27654/15672 ^{***)}
Application Server	Ansible Agent (add-on)	TCP 9098
Application Server	Live Network	ICMP/SNMP/Telnet/SSH/REST API
Database Server	Application Server	TCP 9099 ^{***)}

Note: ^{*)} If SSL was enabled for any component including MongoDB/ElasticSearch/Redis/RabbitMQ/License Agent/Front Server Controller/Ansible Agent/Auto Update Server (within Web API Server), the SSL protocol should be added to firewall rules to enable SSL connection between servers.

Note: ^{**)} The port numbers listed in this column are defaults only. The actual port numbers used during installation might be different.

Note: ^{***)} Ensure the newly added ports (9099 and 15672) are open for future system update of 10.1.

1.1. Terminating System Tasks and Sessions

1. Log into the System Management page.
2. Navigate to **Current Users** tab, click **End Session** to terminate any active session.
3. Select the **Task Manager** tab.
4. Select all running tasks and click **End Process**.

1.2. Stopping Server Services

To avoid any further dataset changes or data corruption while reinstalling MongoDB/Elasticsearch binary files or restoring MongoDB/Elasticsearch data, you must stop the following relevant services:

1. Log in to the Windows server where NetBrain Application Server is installed and stop the following services in the Task Manager.

- **W3SVC** (Web API Server service)
- **WAS** (Web API Server service)

NetBrain Components	Service Name in v7.0b/v7.0b1
Redis	RedisMaster
RabbitMQ	RabbitMQ
Worker Server	ResourceManager
Front Server	proxyserverie
Task Engine	N/A
Front Server Controller	N/A

2. Disable the **Cron** task on the Database Server. The **Cron** task is used to automatically pull up the MongoDB service timely when it is down.

- 1) Log in to the Linux server where the Database Server is installed as **root** user.
- 2) Open a command prompt and run the `crontab -e` command to edit the auto script.

```
[root@localhost ~]# crontab -e
```

```
*/* * * * * /bin/bash -c 'if /usr/sbin/service mongodnetbrain status|grep -q -E  
"(dead)|failed";  
then /usr/sbin/service mongodnetbrain start; fi' >/dev/null 2>&1
```

- 3) Add a pound sign (#) (highlighted) at the beginning of the auto script and save the changes. For how to edit the autoscript, see [Appendix: Editing a File with VI Editor](#) for more details.

```
#*//* * * * * /bin/bash -c 'if /usr/sbin/service mongodnetbrain status|grep -q -E  
"(dead)|failed";  
then /usr/sbin/service mongodnetbrain start; fi' >/dev/null 2>&1
```

1.3. Backing Up MongoDB Data

Before upgrading NetBrain Integrated Edition, it is highly recommended to back up all MongoDB data in case of any data loss or corruption during the upgrade process. The backup data will be used to restore data after MongoDB is reinstalled. See [Appendix: Restoring MongoDB Data](#) for more details.

In case that you don't want to stop the service of MongoDB or the volume of the MongoDB data is small, see [Appendix: Dumping MongoDB data](#) for another way to back up the data, and see [Appendix: Restoring Dumped MongoDB data](#) to restore the data.

The following section introduces how to use the `cp` command to copy underlying MongoDB data files directly for backup.

Notes:

- Make sure you have stopped [all relevant services](#) before backing up data.
- The backup data can only be used to restore the database on the same server.

1. Log in to the Linux server where the MongoDB node is installed as the **root** user.

2. Stop the service of MongoDB

1) Run the `systemctl stop mongodnetbrain` command to stop the MongoDB service.

Note: If you modified the MongoDB service name in the `install.conf` file during the MongoDB installation, you must replace the service name accordingly.

Tip: You can always confirm the MongoDB service name by executing the `crontab -l` command.

2) Run the `ps -ef|grep mongod` command to verify whether the **mongod** process is stopped.

```
[root@localhost ~]# ps -ef| grep mongod
root      15136 14237  0 10:42 pts/2    00:00:00 grep --color=auto mongod
```

Note: If the **mongod** process is stopped, the result should only contain one entry as shown above.

3. Run the following command to create a directory under the `/etc` directory to save the backup data.

Note: Ensure the backup directory (`/etc/mongodb_databk` in this example) has sufficient space to store the backup data.

```
[root@localhost ~]# mkdir /etc/mongodb_databk
```

4. Run the `cd /home/mongodb` command to navigate to the **/home/mongodb** directory.

Note: If you modified the following default directory to store all MongoDB data files during the MongoDB installation, you must use the new directory (available in **mongod.conf**) accordingly.

- For a freshly installed system, the default directory is **/usr/lib/mongodb**.

5. Run the `du -hs data` command under the **/usr/lib/mongodb** directory to check the total size of MongoDB backup data.

6. Run the `cp -a data /etc/mongodb_databk` command under the **/usr/lib/mongodb** directory to copy all MongoDB data files from the **data** directory to the **/etc/mongodb_databk** directory.

```
[root@localhost mongodb]# cp -a data /etc/mongodb_databk
```

7. Run the `cd /etc/mongodb_databk` command to navigate to the **/etc/mongodb_databk** directory.

8. Run the `ls -al` command under the **/etc/mongodb_databk** directory to browse the backup data.

```
[root@localhost mongodb_databk]# ls -al
total 136
drwxr-xr-x.  3 root root      18 Jun 6 22:49 .
drwxr-xr-x.  6 root root      79 Jun 6 22:48 ..
drwxr-xr-x.  4 netbrain netbrain 106496 Jun 6 22:49 data
```

9. Run the `systemctl start mongodnetbrain` command to start the MongoDB service.

1.4. Upgrading NetBrain Database Server

Pre-Upgrade Tasks

- Ensure you have upgraded your Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9, 64-bit**, **CentOS 7.5/7.6/7.7/7.8/7.9, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9, 64-bit** to avoid upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, don't restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

- For v7.0b OVA upgrade, it is required to assign minimum 8 core CPU to the database server.
- RabbitMQ has dependencies on the third-party package openssl (1.0.2k and above) and selinux-policy-target (3.13.1 and above). Before you install the RabbitMQ, run the `rpm -qa|grep openssl` and `rpm -qa|grep`

`selinux-policy-targeted` commands to check their version info. If the version number is less than the required one, you can run the `yum -y upgrade openssl` and `yum -y upgrade selinux-policy-targeted` commands to upgrade them online.

- Ensure the hostname of the Linux server must be resolvable by DNS or configured in `/etc/hosts` because RabbitMQ needs a resolvable hostname no matter whether it is a standalone server or a cluster.
- RabbitMQ has dependencies on the third-party package **socat** and **logrotate**. Run the `rpm -qa|grep socat` and `rpm -qa|grep logrotate` command to check whether **socat** and **logrotate** have been installed on this Linux server. If they have not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install socat` and `yum -y install logrotate` commands to install them online.
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Service Monitor Agent has dependencies on the third-party package **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If they have not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install it online.
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.

Upgrading NetBrain Database Server

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the `/opt` directory to place the installation package. For example, **netbraintemp10.1**.

Note: Don't place the installation package under any personal directories, such as `/root`.

3. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, upload the **netbrain-all-in-two-linux-x86_64-rhel-10.1.tar.gz** file to the `/opt/netbraintemp10.1` directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet and the **yum** service has been installed:
 - 1) Run the `yum -y install wget` command to install the `wget` command if it has not been installed.
 - 2) Run the `cd /opt/netbraintemp10.1` command to navigate to the `/opt/netbraintemp10.1` directory.
 - 3) Run the `wget <download link>` command under the `/opt/netbraintemp10.1` directory to download the **netbrain-all-in-two-linux-x86_64-rhel-10.1.tar.gz** file to this directory:

Note: The download link is case-sensitive.

4. Run the `tar -zxvf netbrain-all-in-two-linux-x86_64-rhel-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

```
[root@localhost netbraintemp10.1]# tar -zxvf netbrain-all-in-two-linux-x86_64-rhel-10.1.tar.gz
netbrain-all-in-two-linux-10.1/
netbrain-all-in-two-linux-10.1/config/
...
netbrain-all-in-two-linux-10.1/upgrade.sh
```

5. Run the `cd netbrain-all-in-two-linux-10.1` command to navigate to the **netbrain-all-in-two-linux-10.1** directory.
6. Run the `systemctl start mongodnetbrain` command to restart the MongoDB service.
7. Run the `./upgrade.sh` command under the **netbrain-all-in-two-linux-10.1** directory to install NetBrain Linux components.
 - 1) Read the license agreement, and then type **YES** and press the **Enter** key.
 - 2) Type **I ACCEPT** and press the **Enter** key to accept the license agreement. The script starts to check whether the system configuration of the Linux server meets the requirement, and all required dependent packages are installed for each Linux component.

```
[root@localhost netbrain-all-in-two-linux-10.1]# ./upgrade.sh
```

```
Please read the End User License Agreement ("EULA") for the license type (perpetual or
subscription) purchased in the order form at https://www.netbraintech.com/legal-tc/
carefully. I have read the subscription EULA, if I have purchased a subscription license, or
the perpetual EULA, if I have purchased a perpetual license, at the link provided above.
Please type "YES" if you have read the applicable EULA and understand its and understand its
contents, or "NO" if you have not read the applicable EULA. [YES/NO]: YES
```

```
Do you accept the terms in the subscription EULA, if you have purchased a subscription
license, or the perpetual EULA, if you have purchased a perpetual license? If you accept, and
to continue with the installation, please type "I Accept" to continue. If you do not accept,
and to quit the installation script, please type "CANCEL" to stop. [I ACCEPT/CANCEL]: I
```

```
ACCEPT
```

```
INFO: 2020-07-09 15-44-24.468: Creating upgrading log...
INFO: 2020-07-09 15-44-24.478: Starting to check system
INFO: 2020-07-09 15-44-25.762: Collecting system information SUCCEEDED.
INFO: 2020-07-09 15-44-25.766: Starting to check Linux OS info
INFO: 2020-07-09 15-44-25.782: ALL_COMPONENT_LIST=mongodb licenseagent elasticsearch rabbitmq
redis servicemonitoragent
INFO: 2020-07-09 15-44-26.541: Old version of MongoDB was installed. Upgrade is required.
INFO: 2020-07-09 15-44-26.736: Old version of Elasticsearch was installed. Upgrade is
required.
INFO: 2020-07-09 15-44-26.787: RabbitMQ was not installed. Fresh installation is required.
INFO: 2020-07-09 15-44-28.032: Redis was not installed. Fresh installation is required.
INFO: 2020-07-09 15-44-28.087: The service of Service Monitor Agent has not been installed on
```

```

this machine. Fresh installation is required.
INFO: 2020-07-09 15-44-28.092: Components to be upgraded: mongodb licenseagent elasticsearch
INFO: 2020-07-09 15-44-28.097: Components to be installed: rabbitmq redis servicemonitoragent
...
Getting rpm dependency list of rabbitmq...
Getting rpm dependency list of redis...
Getting rpm dependency list of servicemonitoragent...
Getting rpm dependency list of mongodb...
Getting rpm dependency list of licenseagent...
Getting rpm dependency list of elasticsearch...

```

3) Configure the following [parameters](#) one by one with an interactive command line.

```

Install NetBrain Linux components.
The values in brackets are the default values of the parameters. To keep the default value
for the
current parameter, press the Enter key.
Please enter the data path for NetBrain [/var/lib/netbrain]:
Please enter the log path for NetBrain [/var/log/netbrain]:
Please enter the IP address of this machine [10.10.3.142]:
Please enter the NetBrain Service Username: admin
Please enter the NetBrain Service Password:
INFO: conf=/opt/mongodb/mongod.conf
INFO: MongoDB configuration file exists.
INFO: The service of mongod is running.
INFO: Successfully connected to MongoDB.
Use SSL on NetBrain Services: no
Use customized server ports? [no]
Please enter the URL (must end with /) to call NetBrain Web API service for the Service
Monitor
[http(s)://<IP address or hostname of NetBrain Application Server>]: http://10.10.3.141/

```

Notes:

- Make sure the designated data path has more than **100GB** free space, and the designated log path has more than **50GB** free space. You can run the `df -h` command to check which directory has been mounted to a large disk.
- The certificate name specified in the path must strictly match with the one you uploaded.
- Here please input the MongoDB username and password as the NetBrain service username and password, and they will be used to change/initialize the credentials for Elasticsearch, RabbitMQ and Redis together with the API Key for Service Monitor Agent during upgrading. They will be used for validating the connections with:
 - MongoDB, Elasticsearch, RabbitMQ, and Redis when upgrading NetBrain Application Server
 - Front Server Controller when setting up the system
 - Service Monitor Agent when communicating with Web API Server

4) To continue the installation with the current configurations, press the **Enter** key. To change any configurations, type **no**.

```

Data path:                /var/lib
Log path:                  /var/log/netbrain
IP address:                10.10.3.142

```

```
Username:                admin
Password:                *****
Uses SSL:                no
Redis port:              6379
Rabbitmq port:           5672

NetBrain Web API service URL:  http://10.10.3.141/ServicesAPI

Do you want to continue using these parameters? [yes]
```

8. RabbitMQ, Redis and Service Monitor Agent will be installed; MongoDB, License Agent, and Elasticsearch will be upgraded. Then run the `reboot` command to restart the machine.
9. Run the following commands to check their service status separately after the server starts up.

- `systemctl status mongod`

```
[root@localhost ~]# systemctl status mongod
mongod.service - MongoDB service
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; vendor preset: disabled)
   Active: activating (start) since Tue 2020-07-07 13:23:24 EDT; 5min ago
   Control: 1143 (mongod)
   Memory: 243.4M (limit: 8.5G)
   ...
```

- `systemctl status netbrainlicense`

```
[root@localhost ~]# systemctl status netbrainlicense
netbrainlicense.service - NetBrain license agent service
   Loaded: loaded (/usr/lib/systemd/system/netbrainlicense.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-07 13:23:35 EDT; 9min ago
     Process: 1175 ExecStart=/usr/bin/netbrainlicense/licensed -f
             /etc/netbrainlicense/licensed.conf (code=exited, status=0/SUCCESS)
     Process: 1150 ExecStartPre=/bin/chmod o+r /sys/class/dmi/id/product_uuid (code=exited, status=0/SUCCESS)
    Main PID: 2111 (licensed)
     Memory: 17.6M
   ...
```

- `systemctl status elasticsearch`

```
[root@localhost ~]# systemctl status elasticsearch
elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-07 13:23:25 EDT; 12min ago
     Docs: http://www.elastic.co
    Main PID: 1153 (java)
     Memory: 4.5G
   ...
```

- `systemctl status rabbitmq-server`

```
[root@localhost ~]# systemctl status rabbitmq-server
rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-07 13:26:56 EDT; 9min ago
 Main PID: 1136 (beam.smp)
    Status: "Initialized"
   Memory: 131.2M
   ...
```

- **systemctl status redis**

```
[root@localhost ~]# systemctl status redis
redis.service - Redis
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-07 13:23:25 EDT; 14min ago
 Main PID: 1159 (redis-server)
   Memory: 7.3M
   ...
```

- **systemctl status netbrainagent**

```
[root@localhost ~]# systemctl status netbrainagent
netbrainagent.service - NetBrain Service Monitor Agent Daemon
   Loaded: loaded (/usr/lib/systemd/system/netbrainagent.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-07 13:23:24 EDT; 15min ago
 Main PID: 1144 (python3)
   Memory: 135.0M
   ...
```

10. Verify the upgraded MongoDB version. The version should be v4.0.28.

- 1) Log in to the Linux server where MongoDB is installed.
- 2) Open a command prompt and run the following command to connect to MongoDB.

```
mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --authenticationMechanism SCRAM-SHA-256
```

Example:

```
[root@localhost ~]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.28
connecting to: mongodb://10.10.3.142:27017/?authMechanism=SCRAM-SHA-256&authSource=admin&gssapiServiceName=mongodb
...
```

Tip: If SSL is enabled, run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates --authenticationMechanism SCRAM-SHA-256` command.

Parameters

Refer to the following table for the parameters of NetBrain Database Server.

Parameter	Default Value	Description
Data path	/var/lib/netbrain	The directory to save RabbitMQ & Redis data. You can press the Enter key to keep the default path or type a new one.
Log path	/var/log/netbrain	The directory to save RabbitMQ & Redis logs. You can press the Enter key to keep the default path or type a new one.
IP address of this machine	<current IP address automatically obtained from the machine>	The IP address of this server. It will be used for establishing connections with NetBrain Application Server. You can press the Enter key to keep the default value or type a new one.
NetBrain Service username		The existing admin username and password of your MongoDB in the previous version.
NetBrain Service password		
Certificate file path		The file name of the certificate file that contains the public key. Note: It is required only if Use SSL on NetBrain Services is enabled.
Private Key file path		The file name of the private key file. Note: It is required only if Use SSL on NetBrain Services is enabled.
Certificate Authority file path		The name and directory of the chain Certificate Authority (CA) file, which is used to authenticate the CA issuing the SSL certificates. Note: It is required only if Use SSL on NetBrain Services is enabled.
Use customized server ports?	no	Whether to customize a port number for RabbitMQ or Redis. To customize ports, type yes .
Rabbitmq port	5672	The port number that the RabbitMQ service listens to. Make sure the port is not used by other applications. Note: The value cannot be modified anymore after it is specified. Note: Keep notes of the customized port because it will be used for validating the connections with RabbitMQ.
Redis port	6379	The port number that the Redis service listens to. Make sure the port is not used by other applications. Note: The value cannot be modified anymore after it is specified.

Parameter	Default Value	Description
		Note: Keep notes of the customized port because it will be used for validating the connections with Redis.

1.5. Upgrading NetBrain Application Server

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

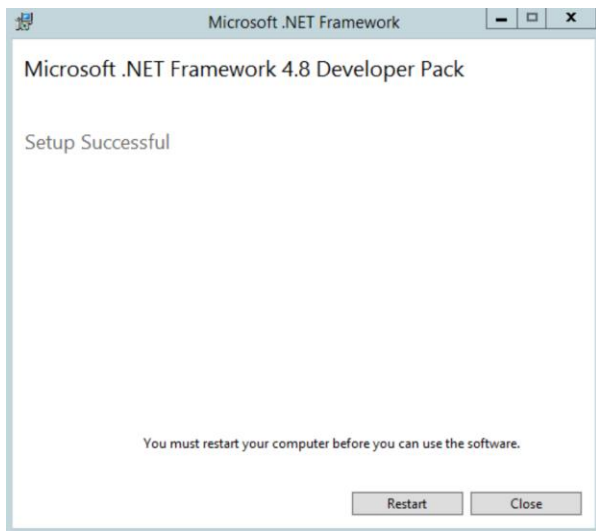
Complete the following steps with administrative privileges.

1. Download the **netbrain-all-in-two-windows-x86_64-10.1.zip** file and save it in your local folder.
2. Extract files from the **netbrain-all-in-two-windows-x86_64-10.1.zip** file.
3. Navigate to the **netbrain-all-in-two-windows-x86_64-10.1** folder, right-click the **netbrain-application-10.1.exe** file and then select **Run as administrator** to launch the Installation Wizard.
4. Follow the Installation Wizard to complete the installation step by step:
 - 1) If **.NET Framework 4.8** has not been pre-installed on this machine, the Installation Wizard will guide you through the installation of **.NET Framework 4.8**.

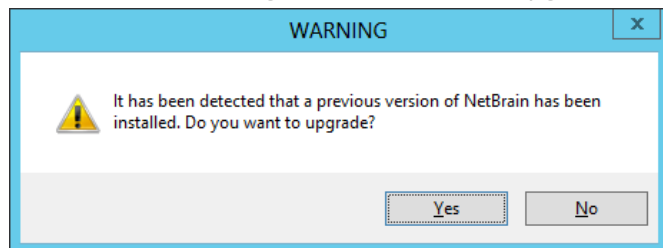
Note: Make sure the Windows update is of the latest. For Windows Server 2012, the update **KB2919442** and **KB2919355** must be installed before the .NET Framework 4.8 installation can start.

Note: Some running applications must be closed during the installation of .NET Framework 4.8, such as Server Manager.

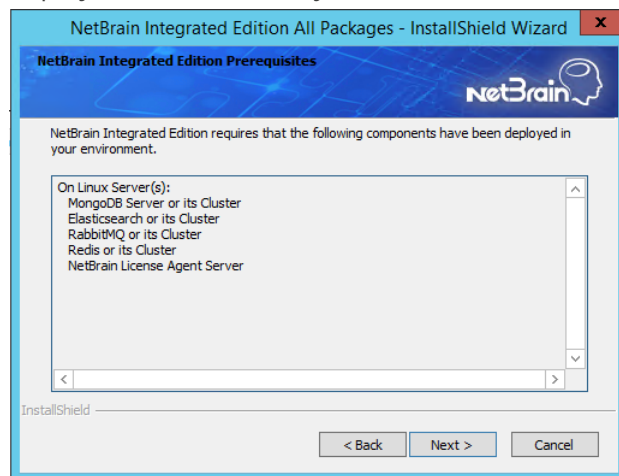
Note: After .NET Framework 4.8 is successfully installed, you must click **Restart** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, ensure the FIPS is disabled after restarting the machine. To disable the FIPS setting, modify the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry.



- 2) Stop all the NetBrain services on the Windows server manually before continuing the upgrade.
- 3) Click **Yes** in the dialog box to initiate the upgrade.

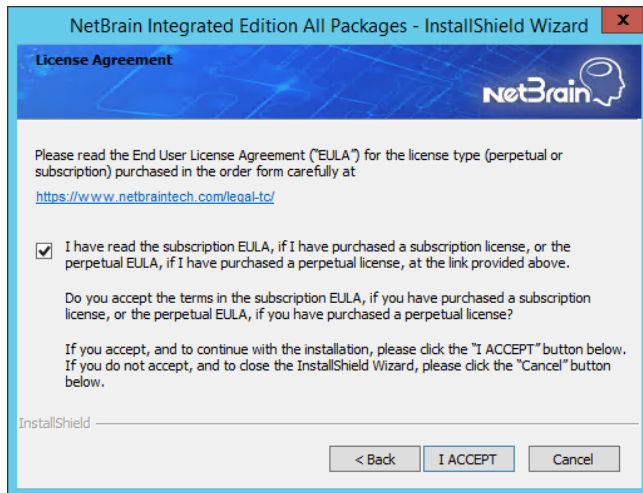


- 4) On the Welcome page, click **Next**.
- 5) On the NetBrain Integrated Edition Prerequisites page, read the list of Linux components that must be deployed beforehand in your environment and click **Next**.

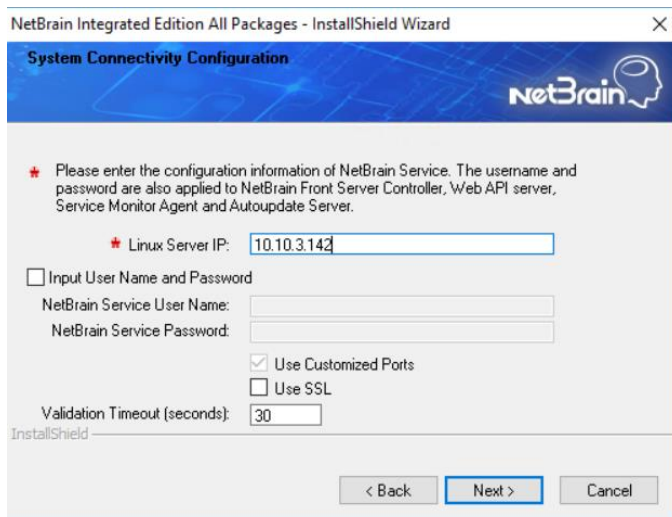


- 6) On the System Configuration page, review the system configuration summary and click **Next**.

- 7) On the License Agreement page, read the license agreement, and then select the **I have read the subscription EULA** check box and click **I ACCEPT**.



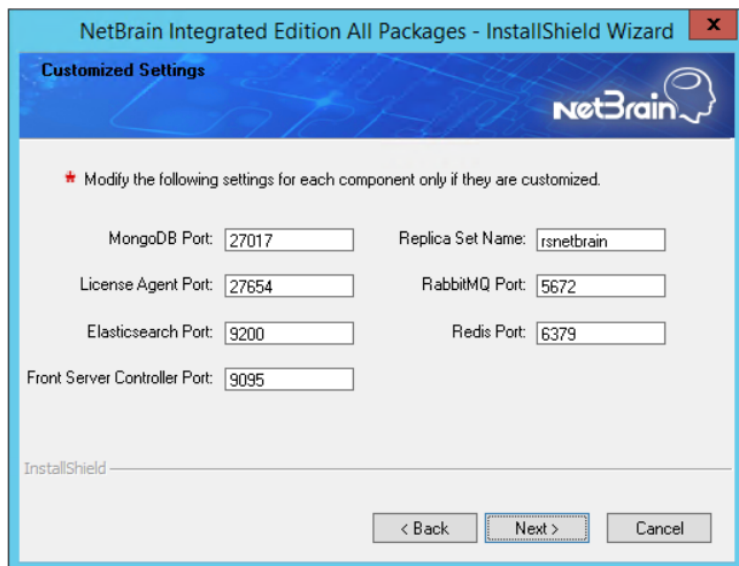
- 8) On the System Connectivity Configuration page, review the connection information to connect to NetBrain Database Server. Click **Next**.



Note: You can click the **Edit** button to modify the connection information after ensuring the **Use Customized Settings** is checked.

Tip: The **Use SSL** checkbox will inherit the SSL settings of your existing NetBrain Database Server.

- 9) On the Customized Settings page, enter the ports of RabbitMQ and Redis, and leave the others unchanged. Click **Next**.



NetBrain Integrated Edition All Packages - InstallShield Wizard

Customized Settings

★ Modify the following settings for each component only if they are customized.

MongoDB Port: Replica Set Name:

License Agent Port: RabbitMQ Port:

Elasticsearch Port: Redis Port:

Front Server Controller Port:

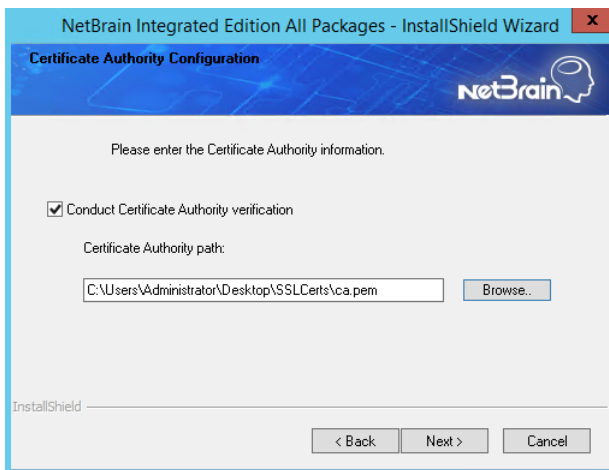
InstallShield

< Back Next > Cancel

NetBrain Application Server will use the specified credentials of NetBrain Database Server, including IP address, username, password, SSL settings, and port settings to validate the connectivity to MongoDB, License Agent, Elasticsearch, RabbitMQ, and Redis one by one.

10)(Required only if the **Use SSL** check box is selected) Configure the following SSL settings.

- a) On the Certificate Authority Configuration page, to validate the Certificate Authority (CA) of the SSL certificates used on NetBrain Database Server, select the **Conduct Certificate Authority verification** check box and click **Browse** to upload the chain certificate file. Click **Next**.



NetBrain Integrated Edition All Packages - InstallShield Wizard

Certificate Authority Configuration

Please enter the Certificate Authority information.

☒ Conduct Certificate Authority verification

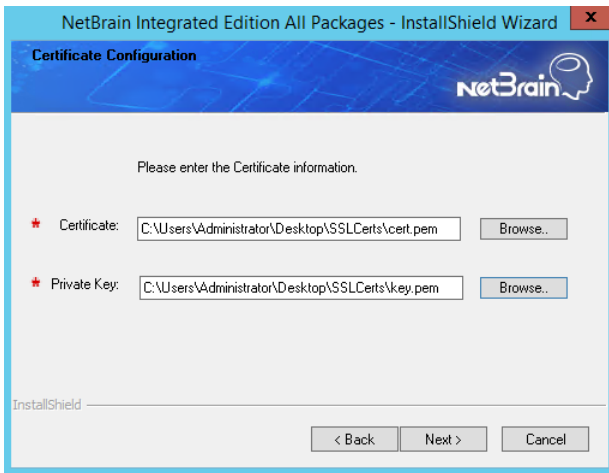
Certificate Authority path:

Browse..

InstallShield

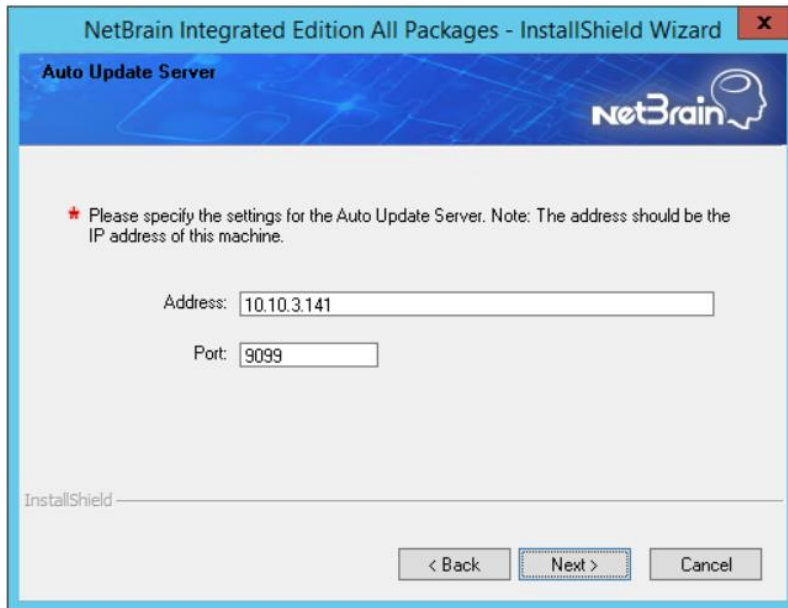
< Back Next > Cancel

- b) On the Certificate Configuration page, click **Browse** to upload the certificate file and private key file to enable SSL communications on Front Server Controller. Click **Next**.



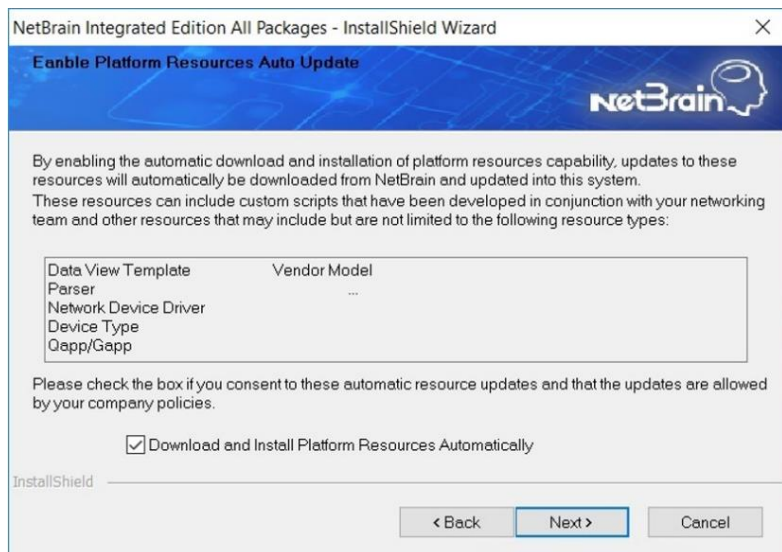
The screenshot shows the 'Certificate Configuration' window of the 'NetBrain Integrated Edition All Packages - InstallShield Wizard'. The window has a blue header with the NetBrain logo. Below the header, it says 'Please enter the Certificate information.' There are two fields: 'Certificate:' and 'Private Key:'. Both fields have text boxes containing file paths ('C:\Users\Administrator\Desktop\SSLCerts\cert.pem' and 'C:\Users\Administrator\Desktop\SSLCerts\key.pem' respectively) and a 'Browse...' button to the right of each text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted.

- 11) On the Auto Update Server page, enter the required information and click **Next**.

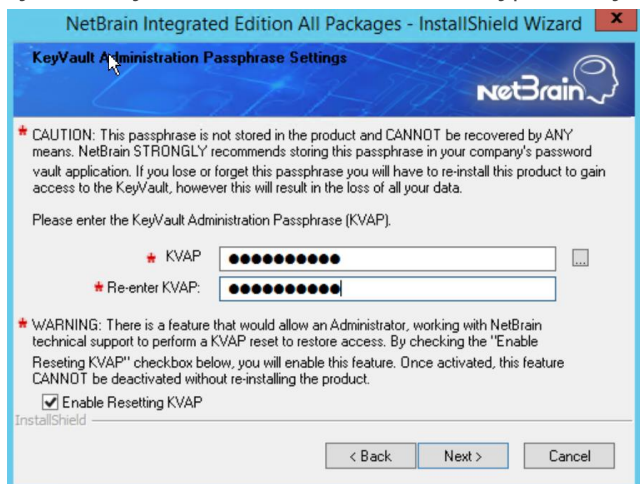


The screenshot shows the 'Auto Update Server' window of the 'NetBrain Integrated Edition All Packages - InstallShield Wizard'. The window has a blue header with the NetBrain logo. Below the header, it says 'Please specify the settings for the Auto Update Server. Note: The address should be the IP address of this machine.' There are two fields: 'Address:' and 'Port:'. The 'Address:' field has a text box containing '10.10.3.141'. The 'Port:' field has a text box containing '9099'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted.

- 12) On the Enable Platform Resources Auto Update page, if you want these resources to be downloaded automatically, check the Download and Install Platform Resources Automatically box. Click **Next**.



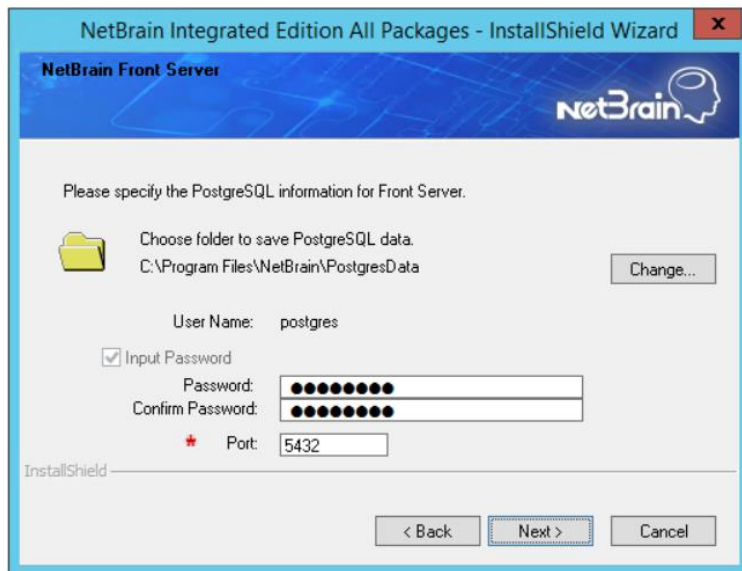
- 13) On the KeyVault Administration Passphrase Settings page, create a passphrase to initialize and manage the system KeyVault which contains all encryption keys to protect data security. Type it twice and click **Next**.



Tip: The passphrase must contain at least one uppercase letter, one lowercase letter, one number, and one special character, and the minimum permissible length is 8 characters. All special characters except for the quotation mark (") are allowed.

Note: Keep notes of the passphrase because it is required when you scale up or upgrade the Application Server. In case of losing the passphrase, select the **Enable Resetting KVAP** check box so that NetBrain system admin can reset the passphrase at any time.

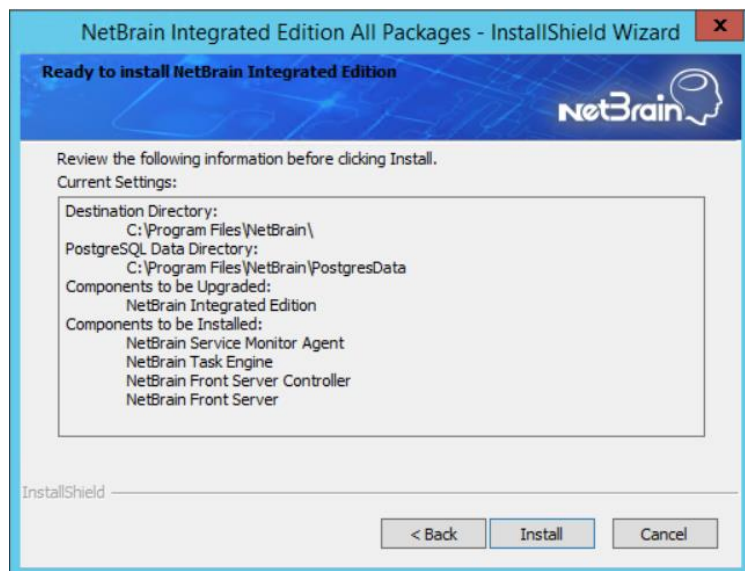
- 14) On the NetBrain Front Server page, create and confirm the password for PostgreSQL Database.



Note: The length of the password must be greater than 8 characters.

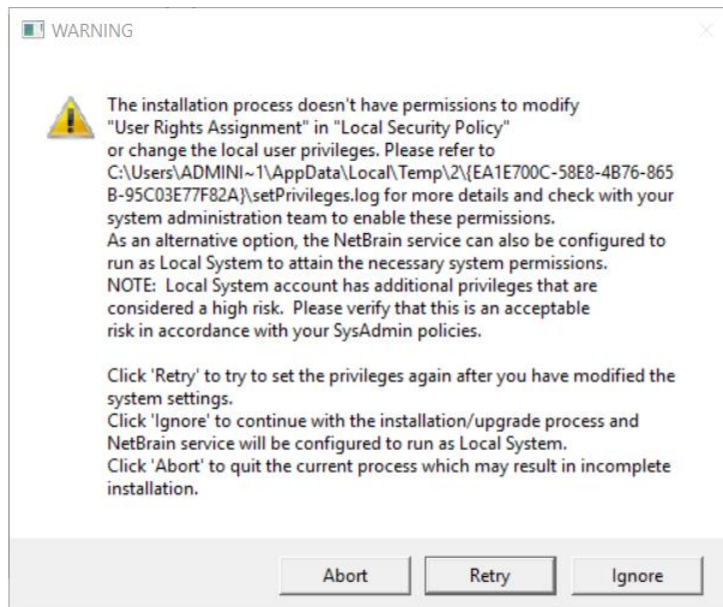
Note: Make sure the designated data folder has more than 180GB free space.

- 15) Review the server components to be installed and click **Install**. All the Windows components will be upgraded one by one. It will take a long while for all the components to be updated.



- 16)(Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user

privileges. Otherwise, the following error message will prompt when installing each Windows component.



- Click **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **Abort**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

5. After all the components are successfully upgraded, click **Finish** to complete the upgrading process and exit the Installation Wizard.
6. Open the Task Manager and navigate to the **Services** panel, you can find the following running NetBrain services.


Name	PID	Description	Status	Group
NetBrainAgent	5684	NetBrain Agent Service	Running	
NetBrainFrontServer		NetBrain Front Server Service	Stopped	
NetBrainFrontServerControl...	4152	NetBrain Front Server Controller ...	Running	
NetBrainKCProxy	4912	NetBrain KCProxy Service	Running	
NetBrainWorkerServer	3136	NetBrain Worker Server	Running	
NetBrainTaskEngine	2888	NetBrain Task Engine Service	Running	

Post-Upgrade Task

- [Uninstalling Proxy Server](#)


1.5.1. Uninstalling Proxy Server

Complete the following steps with administrative privileges. Take Windows Server 2012 R2 for example:

1. Click the Windows start menu and then click the  icon to open the **Apps** pane.
2. Right-click the **Uninstall NetBrain Proxy Server** app in the pane and select **Run as administrator** from the drop-down list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box prompts.
4. Select the **Delete all existing user data** check box to delete all registry information and files under its installation path, and click **Next**.
5. Click **Finish** to exit the Installation Wizard.

1.6. Activating Subscription License

1. In the System Management page, click **Activate** under the **License** tab. The activation wizard prompts.
2. Activate your subscription license:
 - 1) Select **Activate Subscription License** and click **Next**.
 - 2) Enter the license ID and activation key that you received from NetBrain, with your first name, last name, and email address.
 - 3) Select the activation method based on your situation.
 - **Online** (recommended) — click **Activate** to connect to NetBrain License Server and validate your license information immediately.

Note: If your NetBrain Web/Web API Server is not allowed to access the Internet, you can configure a proxy server. Click the  icon at the upper-right corner, select the **Use a proxy server to access the internet** check box and enter the required information.

- **Via Email** — validate your license information by sending an email to NetBrain.

Note: Only use this activation method when your NetBrain Web/Web API Server is not allowed to access the Internet.


- a) Follow the instructions to generate your license file. Attach the file to your email and send it to [NetBrain Support Team](#). After receiving your email, the NetBrain team will fill in the license information on NetBrain License Server and generate the corresponding activation file, and then send it back to you.
 - b) Click **Browse** to select the activation file that you received from NetBrain team, and then click **Activate**.
- 4) A message box will prompt you the subscription license has been activated successfully. Click **OK**.
 3. A confirmation dialog box prompts to ask you whether to generate an initial tenant. Click **Yes** and the initial tenant will be created automatically with all purchased nodes assigned.

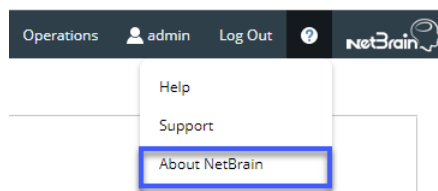
Note: If you want to create a tenant later, click **No**. See [Creating a Tenant](#) for more details.

1.7. Verifying Upgrade Results

1. Do the following steps to check the IE version in web browser:

Note: It is highly recommended to clear your web browser's cache before reloading the IE web page.

- 1) In the system Management page, click the  icon and select **About NetBrain** from the quick access toolbar.



- 2) Check the version information. The product version should be 10.1.

2. Do the following steps to check the system version in MongoDB:

- 1) Log in to the Linux server where MongoDB is installed.
- 2) Open a command prompt and run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --authenticationMechanism SCRAM-SHA-256` command to connect to MongoDB. The version should be v4.0.28.

Example:

```
[root@localhost ~]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.28
connecting to: mongodb://10.10.3.142:27017/?authMechanism=SCRAM-SHA-
256&authSource=admin&gssapiServiceName=mongodb
...
```

Tip: If SSL is enabled, run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates --authenticationMechanism SCRAM-SHA-256` command.

- 3) Run the `use NGSystem` command to switch to the **NGSystem** database.

```
rsnetbrain:PRIMARY> use NGSystem
switched to db NGSystem
```

- 4) Run the `db.SystemInfo.find({_id: "SystemVersion"})` command to check if the system version number is 10.1.1.

```
rsnetbrain:PRIMARY> db.SystemInfo.find({_id: "SystemVersion"})
{ "_id" : "SystemVersion", "version" : "10.1.1", "operateInfo" : { "opUser" : "NetBrain",
"opTime" :
  ISODate("2020-07-14T18:31:21.735") } } }
```

- 5) Run the `exit` command to exit the command prompt.

1.8. Allocating Tenants to Front Server Controller

1. In the System Management page, select the **Front Server Controllers** tab, and then click **Add Front Server Controller**.
2. In the **Add Front Server Controller** dialog, configure the settings for the Front Server Controller, and then allocate tenants to it.

- 1) Select the deployment mode, and then specify the basic information about the Front Server Controller. See [FSC Settings](#) for more details.

Add Front Server Controller

Deployment Mode: Standalone

Front Server Controller Settings:

Front Server Controller

*Name:

*Hostname or IP Address:

*Port:

*Username:

*Password:

Timeout: Seconds

Description:

SSL Settings

Allocated Tenants:

<input checked="" type="checkbox"/>	Tenant Name	Dedicated Front Server Controller
<input checked="" type="checkbox"/>	Initial Tenant	

Cancel Test OK

- **Standalone** — applicable to a single Front Server Controller deployment.
 - **Group** — applicable to a failover deployment of Front Server Controller.
- 2) Configure the SSL settings.
 - a) If SSL is enabled on Front Server Controller, select the **Use SSL** check box to encrypt the connections established from the Worker Server and Front Server with SSL. Otherwise, leave it unchecked.
 - b) To authenticate the Certificate Authority (CA) certificate on the Front Server Controller, select the **Conduct Certificate Authority verification** check box.
 - c) If CA has not been installed on the Worker Server and Task Engine, click **Browse** to upload the CA file, for example, **ca.pem**. Otherwise, click **I have already installed the Certificate Authority on Worker Server and Task Engine**.
- Note:** Only certificates in the **Base-64 encoded X.509 PEM** format are supported.
- 3) Click **Test** to verify whether the Worker Server can establish a connection to Front Server Controller with the configurations.
 - 4) In the **Allocated Tenants** area, select the target tenants to allocate them to the controller.
 - 5) Click **OK** to save the settings.

The Front Server Controller is added.

+ Add Front Server Controller		Refresh					
Search...	Front Server Control...	Hostname or IP ...	Port	Username	Description	Tenants	Status
FSC	Connected	FSC	10.10.3.141	9095	netbrain	Initial Tenant	Connected
Initial Tenant							

Front Server Controller Settings

The following items (except **Timeout** and **Description**) are required to be consistent with those configured during the installation of NetBrain Application Server.

Field	Description
Name	Keep the default value FSC as it is.
Hostname or IP Address	Enter the IP address of NetBrain Application Server.
Port	The port number created when you install the Front Server Controller for listening to the connections from Worker Server. By default, it is 9095 .
Username	The user name created for NetBrain service when installing NetBrain Database Server.
Password	The password created for NetBrain service when installing NetBrain Database Server.
Timeout	The maximum waiting time for establishing a connection from Worker Server to this Front Server Controller. By default, it is 5 seconds.
Description	The brief description to help you add more information about the Front Server Controller.

1.9. Adding a Front Server for a Tenant

1. In the Front Server Controller Manager, select the target tenant and click **Add Front Server**.

System Management

OperationsadminLog OutNetBrain

Home PageLicenseTenantsUser AccountsFront Server ControllersEmail SettingsAdvanced Settings

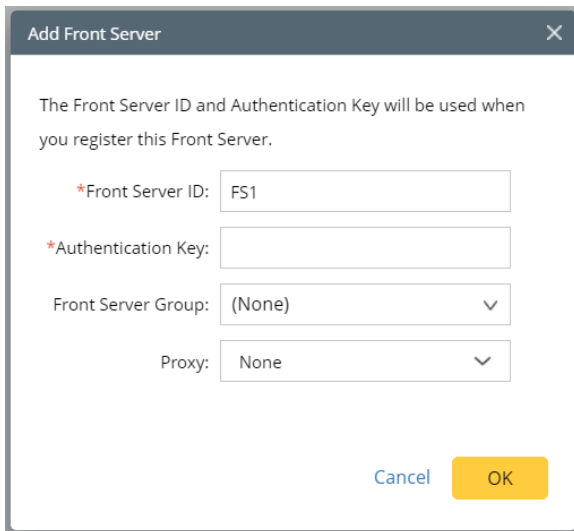
+ Add Front Server Controller

Refresh

Search...+ New Front Server

FSC	Connected	ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status
Initial Tenant								

2. Enter the following properties of the Front Server.



The Front Server ID and Authentication Key will be used when you register this Front Server.

*Front Server ID:

*Authentication Key:

Front Server Group:

Proxy:

[Cancel](#) [OK](#)

- **Front Server ID** — keep the default value **FS1** as it is.
- **Authentication Key** — create an authentication key for the Front Server.

Tip: Keep notes of the Authentication Key because it is required when you [register this Front Server](#).

- **Front Server Group** — assign the Front Server to a group for load balancing. It is only applicable when multiple Front Servers are added to one tenant, otherwise, leave it as default.

3. Click **OK**. The Front Server is added to the Front Server list.

+ Add Front Server Controller

Refresh

Search...

+ Add Front Server

FSC

Connected

Initial Tenant


FS1

ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status	
FS1	No						

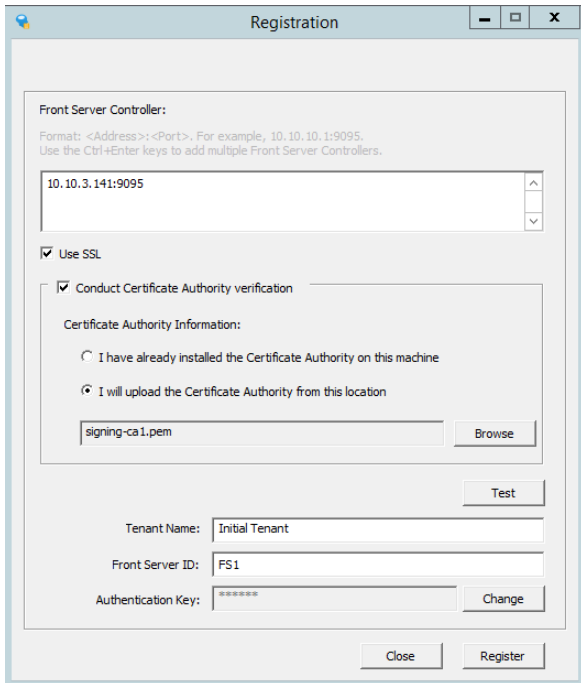
1.10. Registering a Front Server

Example: Register a Front Server on Windows Server 2012 R2.

Complete the following steps with administrative privileges.

1. On the machine where the Front Server is installed, click the Windows start menu and then click the  icon to open the **Apps** pane.
2. Under the **NetBrain** category, right-click **Registration** and then select **Run as administrator** from the drop-down list.

3. In the **Registration** dialog, complete the registration form.

The image shows a 'Registration' dialog box with a title bar containing a minimize, maximize, and close button. The main content area is titled 'Front Server Controller:' and includes a text box for the address and port, currently containing '10.10.3.141:9095'. Below this is a 'Use SSL' section with a checked checkbox. Underneath, there is a 'Conduct Certificate Authority verification' section with two radio buttons: 'I have already installed the Certificate Authority on this machine' (unchecked) and 'I will upload the Certificate Authority from this location' (checked). The second option is active, showing a text box with 'signing-ca1.pem' and a 'Browse' button. At the bottom of the dialog, there are fields for 'Tenant Name' (containing 'Initial Tenant'), 'Front Server ID' (containing 'FS1'), and 'Authentication Key' (containing seven asterisks). There are 'Test', 'Change', 'Close', and 'Register' buttons at the bottom.

- 1) Enter the following information about the Front Server Controller.

- **Hostname or IP address** — the IP address of NetBrain Application Server and the port number (defaults to 9095).

- 2) Configure the SSL settings.

- a) Select the **Use SSL** check box to encrypt the connections to Front Server Controller with SSL. If SSL is disabled on Front Server Controller, leave it unchecked and skip step b) to c).

Note: Select the **Use SSL** check box only if you enabled SSL on Front Server Controller.

- b) To authenticate the Certificate Authority (CA) of SSL certificates on Front Server, select the **Conduct Certificate Authority verification** check box.

- c) If the CA has not been installed on this machine, click **Browse** to upload the CA file, for example, **ca.pem**; otherwise, select **I have installed the Certificate Authority on this machine**.

Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

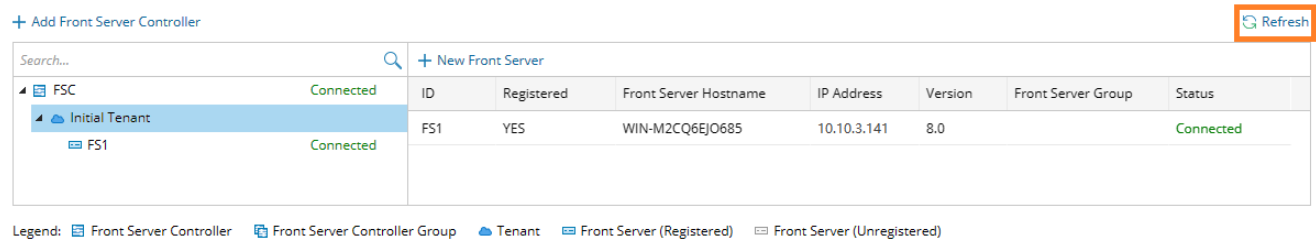
- 3) Click **Test** to verify whether this Front Server can establish a connection with Front Server Controller.

- 4) Keep all default values, and then enter the authentication key created when you add this Front Server to a tenant.

4. Click **Register**.

Tip: After registering the Front Server successfully, you can open the Task Manager and navigate to the **Services** panel to check whether the **NetBrainFrontServer** service is running.

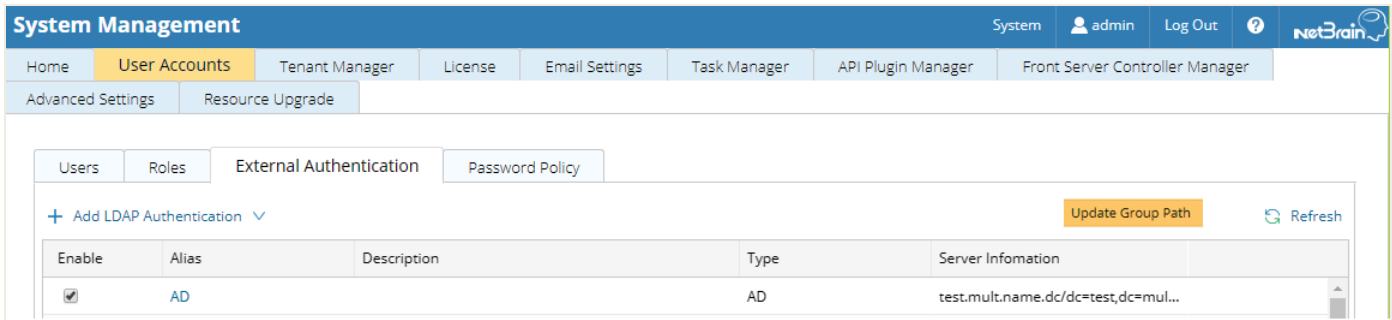
- Click **Close** after the registration is finished. The Front Server information in the Front Server Controller Manager will be synchronized by clicking **Refresh**.



1.11. Upgrading External Authentication

Note: Following steps only apply to AD/LDAP environments where group function is pre-configured.

- In the System Management page, click **User Accounts > External Authentication**.
- Click **Update Group Path**.



- When the group paths are successfully updated, a notification message is displayed in a dialog box. Click **OK**.

1.12. Upgrading Email Settings

- In the System Management page, click the **Email Settings** tab.
- Click **Save** under the **Email Server Settings** tab page.

- When the email settings are successfully upgraded, a notification message will be displayed in a dialog box. Click **OK**.

1.13. Configuring Auto Upgrade Settings

Knowledge Cloud (KC) manages both the framework components and the platform resources and allows NetBrain Workstation to automatically upgrade a patch or minor release. Besides replacing the files, the auto-upgrade process may restart services, execute the database upgrading, check the system health and roll back the release if the update fails.

Platform resources can be downloaded and installed automatically since NetBrain Workstation will be connected to KC through License Server. And for Framework resources, the software update package must be downloaded from NetBrain Customer Portal, manually uploaded into the system and then system updates need to be scheduled accordingly.

NetBrain Workstation Auto Upgrade flow consists of the following steps:

Note: Only user with System Management permissions can perform the following actions.


- [Check the Latest Version](#)
- [Download Package from NetBrain Customer Portal](#)
- [Upload Package to NetBrain Workstation](#)

4. [Schedule Update](#)
5. [View Update Status](#)
6. [View Update History](#)

Check the Latest Version

Follow the steps below to check the available releases from NetBrain:

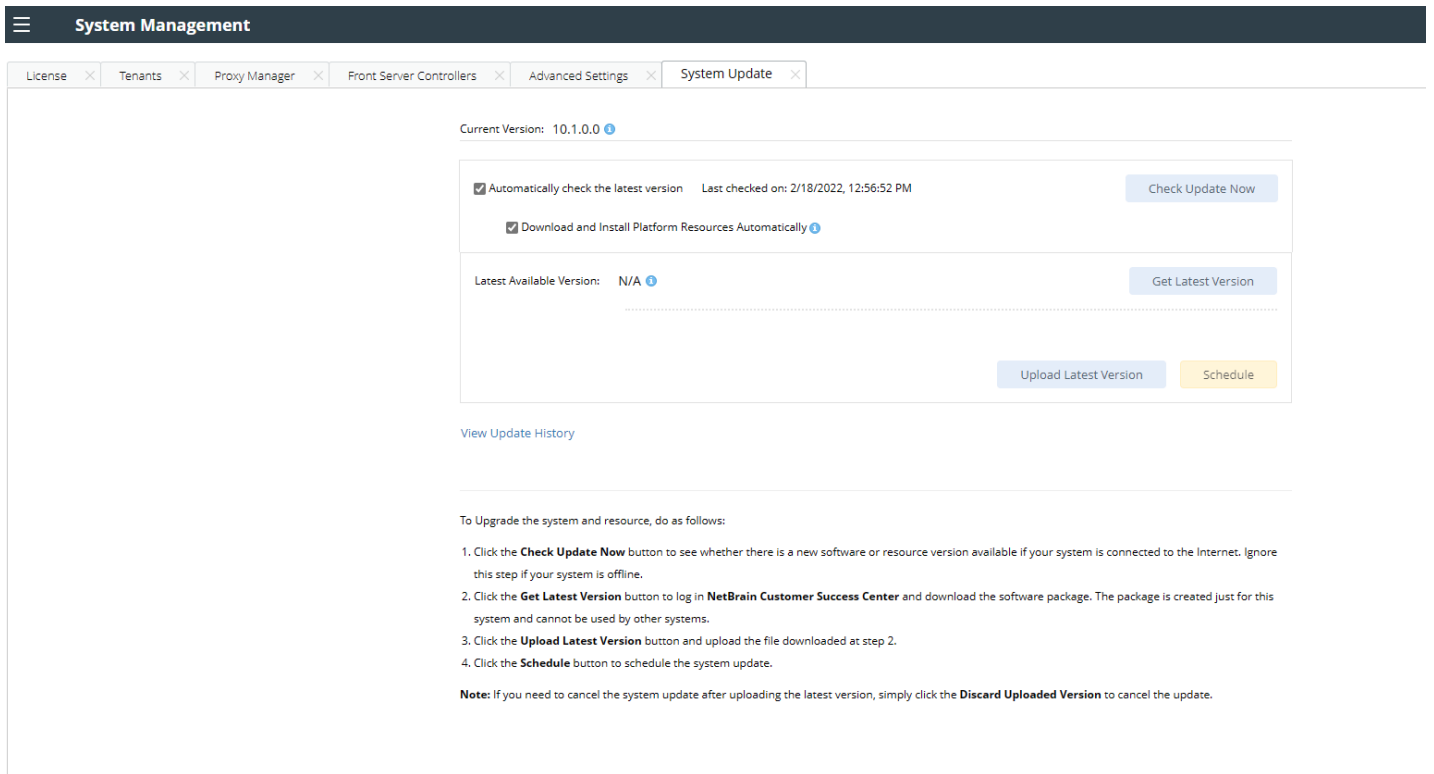
Note: The following steps only apply to the online auto upgrade procedures.

1. In the System Management page, click the  start menu > **System Update**.
2. By default, the **Automatically check the latest version** check box is enabled. You can click **Check Update Now** to see if there is a new version available.

Note: After the check box **Automatically check the latest version** is enabled, users with 'sys admin' role will receive auto notification via email when a new version becomes available.

Note: The Web API Server is required to have internet access with NetBrain public License Server in order to perform the function of **Automatically check the latest version** and **Check Update Now**.

Note: In order to download and install platform resources automatically, you need to enable the **Automatically check the latest version** check box, as well as the **Download and Install Platform Resources Automatically** check box.



3. When this check is enabled, NetBrain Workstation will check whether a minor release, a patch, a customized built-in, a customized resource or common platform resource updates have been published since the last time check (either auto or manual check). The latest available version will be displayed with the release note.
4. If the respective release or patch is available, after reviewing the Release Note, click **Get Latest Version** to [Download Package from NetBrain Customer Portal](#).

Download Package from NetBrain Customer Portal

Follow the steps below to download the system upgrade package from NetBrain Customer Portal:

1. Log into the NetBrain Customer Portal with your username and password.

Note: After clicking **Get Latest Version** in NetBrain Workstation, you will be redirected to the NetBrain Customer Portal. The portal account credentials are required by the web browser to grant access to the NetBrain Customer Portal.

2. Confirm the required info and click **Generate Package**.

Tip: Required info includes the License ID, Framework Version, Common Repo Version, Customized Built-in Resource Repo, Customized Resource Repo.

Tip: If you don't want to download framework components, enable the **Exclude Framework Patch** check box.

Resource Package

License ID

30320454

Current Framework Version

10.1.0.0

Current Common Repo

905abe93-7b6f-3939-97b5-2441944a08a1 |v0.0.1

Current Customized Built-in Resource Repo

N/A

Current Customized Resource Repo

N/A

Advanced Settings

☐ Exclude Framework Patch

☐ Include All Platform Resources

Generate Package

- Click **Resource Package Link** to download the package to your local drive.
- Keep note of the password for next step- [Upload Package to NetBrain Workstation](#).

Resource Package

License ID

30320454

Current Framework Version

10.1.0.0

Current Common Repo

905abe93-7b6f-3939-97b5-2441944a08a1 |v0.0.1

Current Customized Built-in Resource Repo

N/A

Current Customized Resource Repo

N/A

Advanced Settings

☐ Exclude Framework Patch

☐ Include All Platform Resources

Generate Package


Target Framework:10.1.0.9; Platform: [v0.0.1,,]

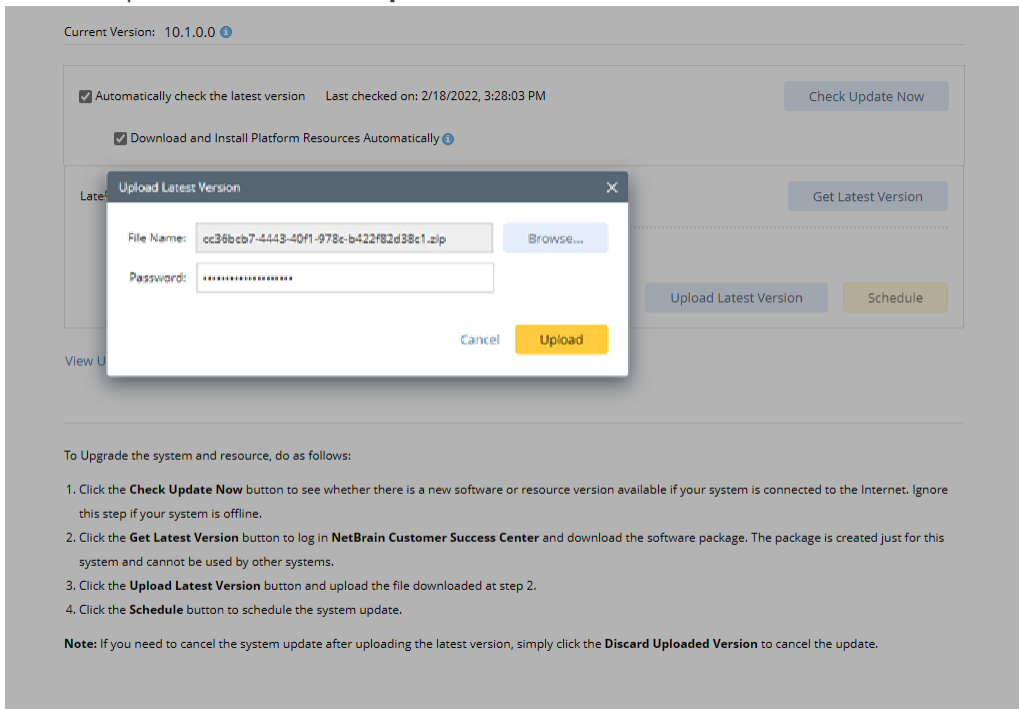
[Resource Package Link](#) Password: mQyKB0bZPOKzpHEleCcK

Attention: You will be asked to enter this password when you import this package to IE system for upgrade. Please save it somewhere.

Upload Package to NetBrain Workstation

Follow the steps below to upload the system upgrade package to NetBrain Workstation:


1. In the System Management page, the  start menu> **System Update**.
2. Click **Upload Latest Version**.
3. Click **Browse** and select the system upgrade package (.zip file).
4. Enter the password and click **Upload**.



Tip: With the **Discard Uploaded Version** button, you can discard the previous uploaded update package before it is scheduled and delete the system update task before the scheduled task is executed.

Schedule Update

Follow the steps below to schedule the system update:

1. Run [the system update pre-check tool](#) to verify the environment readiness for the auto-update.
2. In the System Management page, click the  start menu> **System Update**.
3. Click **Schedule**.
4. Review the license agreement, select the **I have read the subscription EULA** check box and click **I ACCEPT**.

Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at

<https://www.netbraintech.com/legal-tc/>

- ☐ I have read the subscription EULA, if I have purchased a subscription license, or the perpetual EULA, if I have purchased a perpetual license, at the link provided above.

Do you accept the terms in the subscription EULA, if you have purchased a subscription license, or the perpetual EULA, if you have purchased a perpetual license?

If you accept, and to continue with the installation, please click the **"I ACCEPT"** button below. If you do not accept, and to close the Wizard, please click the **"Cancel"** button below.

Cancel

I ACCEPT

5. **(Optional)** Check the **Enable Test Plan** checkbox.

Tip: You can leave the **Enable Test Plan** checkbox unchecked to skip the test plan.

Note: Only user with domain and tenant access will be granted permission to run the test plan.

Schedule Update - Version 10.1.0.0

Review Test Plan Schedule Update

☒ Enable Test Plan

Before and after the system is upgraded, the system will execute the following test plan to ensure that the system works properly.

1. Basic system status check such as the server connectivity, service status and key process.
If any serious error is found, the system will rollback the update
2. Domain health and data accuracy test
 - a. The system will perform Domain Health test for the following domain.

Tenant:	Initial Tenant	Select
Domain:	Domain1	
 - b. The system will perform Data Accuracy test for the following devices and applications.

Device:	Auto Test Group
Application:	Auto Test Application

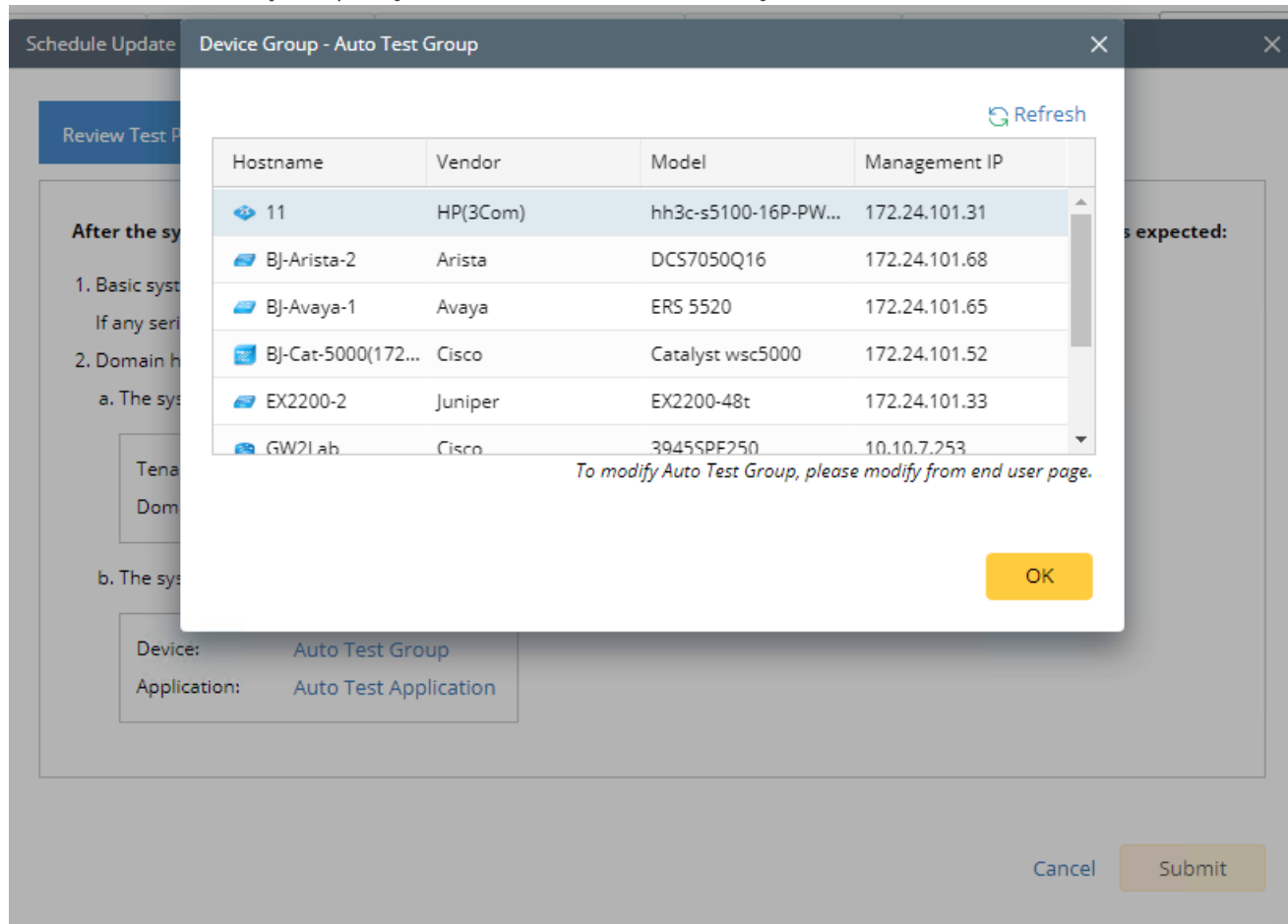
Cancel Submit

- 1) Click **Select** and specify the desired Tenant/Domain to perform Domain Health Check.

Note: If there are more than one tenant or domain, step 1) must be completed before proceeding to step 2).

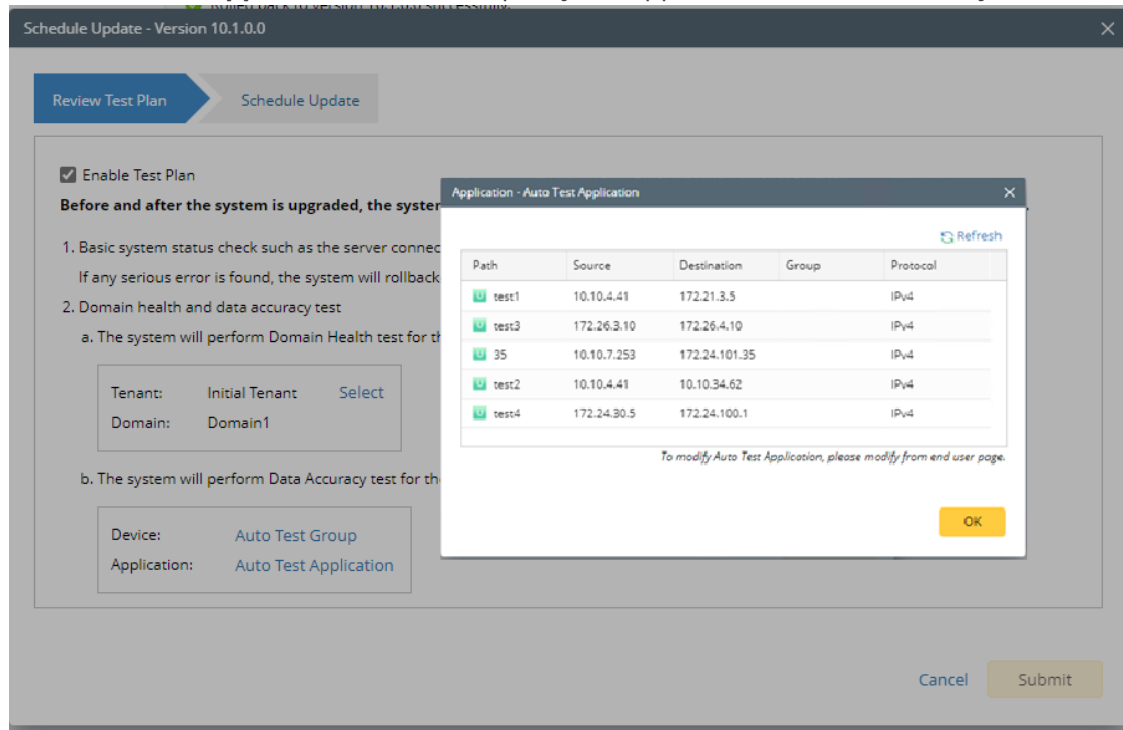
Note: If there is only one tenant and domain, the Initial Tenant will be automatically selected and you can directly proceed to step 2).

- 2) Click **Auto Test Group** to specify the devices for Data Accuracy Test.



Tip: The devices in the Auto Test Group are automatically selected according to the device type discovered by the system. You can also manually edit or delete any devices to suit your specific needs.

- 3) Click **Auto Test Application Folder** to specify the application for Data Accuracy Test.



Note: The last used Application Paths (up to 5 paths) will be automatically copied to the Auto Test Application Folder. You can also manually change the auto selected path in [Application Manager](#).

6. Set up the schedule to start the system update.

Schedule Update - Version 10.1.0.0

Review Test Plan Schedule Update

Select the Start Time and Time Zone you want to Update. Your web server time zone is "(UTC-05:00) Eastern Time (US & Canada)"

Update Start Time: 2022-02-18 03 : 41 PM Use Current Time

Time Zone: (UTC-05:00) Eastern Time (US & Cana... ▼

Cancel Submit

Tip: You can edit or remove the system update once it is scheduled.

7. Click **Submit** to apply the above settings.

Note: A confirmation message will prompt if the selected tenant/domain does not have application path, you can click Yes to dismiss the message and continue with the update process.

View Update Status


The possible status of auto update are as follows:

Stage of the Auto Update	Possible Status
Before the execution of Auto Update	<ul style="list-style-type: none">• Ready for schedule.• Ready for running.
During the execution of Auto Update	<ul style="list-style-type: none">• Running.

After the execution of Auto Update	<ul style="list-style-type: none"> • The system is successfully updated to the new version. • The system is successfully updated to the latest version, but the user performs a manual rollback and the rollback succeeds. • The system is successfully updated to the latest version, but the user performs a manual rollback and the rollback fails. • The update fails, and the system is rolled back to the old version. • The update fails at the beginning (due to insufficient disk space to perform auto-upgrade, unavailable component and etc.) and the roll back is not executed.
------------------------------------	---

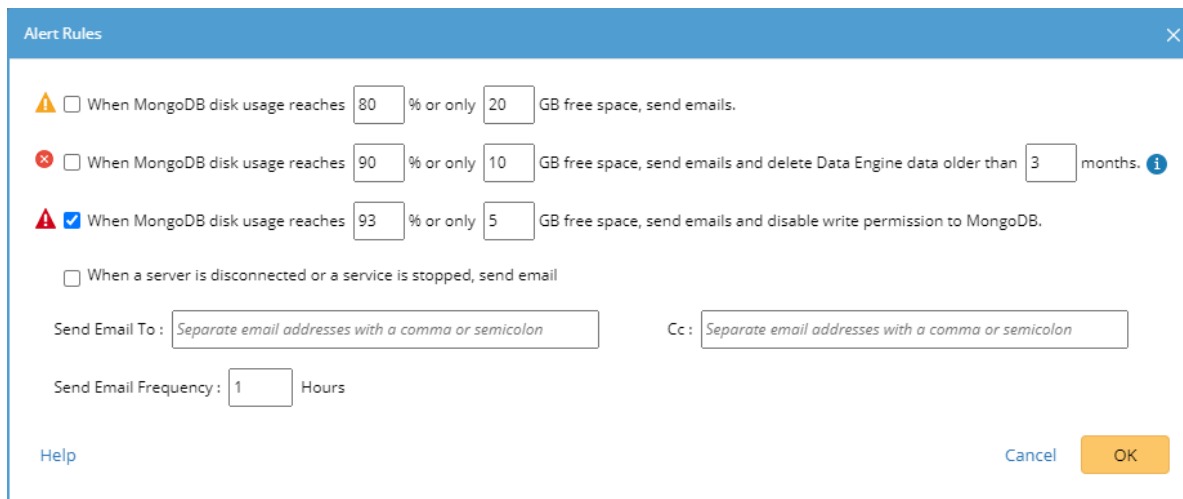
View Update History

Follow the steps below to view the update history:

1. In the System Management page, click the  start menu > **System Update**.
2. Click **View Update History**.

The update history only records the releases the system is scheduled to update with. The update history table provides the following information:

- **Update From:** the release number from which the system is updated.
- **Update To:** the release number to which the system is updated.
- **Update Time:** when the system finished the update.
- **Executor:** the person to schedule the update
- **Action:** upgrade or user roll back.
- **Status:** one of the statuses in [View Update Status](#).
- **Release Note:** the link of the release note.
- **Installation Log:** the link of the installation log.
- **Test Report:** the link of the test results.



The 'Alert Rules' window contains the following configuration options:

- ☐ When MongoDB disk usage reaches % or only GB free space, send emails.
- ☒ When MongoDB disk usage reaches % or only GB free space, send emails and delete Data Engine data older than months. ⓘ
- ☒ When MongoDB disk usage reaches % or only GB free space, send emails and disable write permission to MongoDB.
- ☐ When a server is disconnected or a service is stopped, send email


Send Email To : Cc :

Send Email Frequency : Hours



Buttons: Help, Cancel, OK

3. Click **OK**.

1.15. Tuning Live Access

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Application Server>/** to log in to each Domain.
2. Click the  start menu> **Tune Live Access**. The Tune Live Access tab opens with all devices in the domain listed.
3. Click **Start Tuning**.
4. When the tuning process is completed, a notification message is displayed. Click **OK**.

1.16. Scheduling Benchmark Task

1. In the Domain Management page, click the  start menu> > **Schedule Task**.
2. On the **Schedule Discovery/Benchmark** tab, select the **Enable** check box for the **Basic System Benchmark** entry.
3. Click the  icon to select the **Run Now** option from the drop-down list to run the benchmark task immediately.

Note: If you have multiple Front Servers, go to **Operations > Benchmark Tools > CheckPoint OPSEC Manager** to specify the target Front Server to access your CheckPoint firewalls and retrieve live data.

4. To recover the v7.0b/b1 benchmark data:

- 1) Download the [UpgradeDeviceData7.0To8.03.zip](#) file and save it to the **C:\Program Files\NetBrain\Worker Server** directory of your NetBrain Worker Server.

Note: If you changed the default installation directory for Worker Server, replace the above directory accordingly.

- 2) Extract the zip file under the **\NetBrain\Worker Server** folder and double-click the **UpgradeDeviceData7.0To8.0.exe** file under the **\NetBrain\Worker Server\DE 7.0 to 8.03** folder to execute the benchmark data recovery. A sample output is as follows:

```
begin to upgrade device data in domain <domain name>
end of upgrading device data in domain <domain name>
Press ENTER to continue.
```

2. Appendix: Offline Installing Third-party Dependencies

1. Download the dependency package from a server with the Internet access using one of the following download links according to the version of your Operating System:

- **CentOS7.5:** <http://download.netbraintech.com/dependencies-centos7.5.tar.gz>
- **CentOS7.6:** <http://download.netbraintech.com/dependencies-centos7.6.tar.gz>
- **CentOS7.7:** <http://download.netbraintech.com/dependencies-centos7.7.tar.gz>
- **CentOS7.8:** <http://download.netbraintech.com/dependencies-centos7.8.tar.gz>
- **CentOS7.9:** <http://download.netbraintech.com/dependencies-centos7.9.tar.gz>
- **CentOS8.2:** <http://download.netbraintech.com/dependencies-centos8.2.tar.gz>
- **CentOS8.3:** <http://download.netbraintech.com/dependencies-centos8.3.tar.gz>
- **CentOS8.4:** <http://download.netbraintech.com/dependencies-centos8.4.tar.gz>
- **CentOS8.5:** <http://download.netbraintech.com/dependencies-centos8.5.tar.gz>
- **RHEL7.5:** <http://download.netbraintech.com/dependencies-rhel7.5.tar.gz>
- **RHEL7.6:** <http://download.netbraintech.com/dependencies-rhel7.6.tar.gz>
- **RHEL7.7:** <http://download.netbraintech.com/dependencies-rhel7.7.tar.gz>
- **RHEL7.8:** <http://download.netbraintech.com/dependencies-rhel7.8.tar.gz>
- **RHEL7.9:** <http://download.netbraintech.com/dependencies-rhel7.9.tar.gz>
- **RHEL8.2:** <http://download.netbraintech.com/dependencies-rhel8.2.tar.gz>
- **RHEL8.3:** <http://download.netbraintech.com/dependencies-rhel8.3.tar.gz>
- **RHEL8.4:** <http://download.netbraintech.com/dependencies-rhel8.4.tar.gz>
- **RHEL8.5:** <http://download.netbraintech.com/dependencies-rhel8.5.tar.gz>
- **RHEL8.6:** <http://download.netbraintech.com/dependencies-rhel8.6.tar.gz>
- **OL7.7:** <http://download.netbraintech.com/dependencies-ol7.7.tar.gz>
- **OL7.8:** <http://download.netbraintech.com/dependencies-ol7.8.tar.gz>
- **OL7.9:** <http://download.netbraintech.com/dependencies-ol7.9.tar.gz>
- **OL8.2:** <http://download.netbraintech.com/dependencies-ol8.2.tar.gz>
- **OL8.3:** <http://download.netbraintech.com/dependencies-ol8.3.tar.gz>
- **OL8.4:** <http://download.netbraintech.com/dependencies-ol8.4.tar.gz>
- **OL8.5:** <http://download.netbraintech.com/dependencies-ol8.5.tar.gz>
- **OL8.6:** <http://download.netbraintech.com/dependencies-ol8.6.tar.gz>
- **Alma8.4:** <http://download.netbraintech.com/dependencies-almalinux8.4.tar.gz>

- **Alma8.5:** <http://download.netbraintech.com/dependencies-almalinux8.5.tar.gz>
- **Alma8.6:** <http://download.netbraintech.com/dependencies-almalinux8.6.tar.gz>
- **Rocky8.4:** <http://download.netbraintech.com/dependencies-rockylinux8.4.tar.gz>
- **Rocky8.5:** <http://download.netbraintech.com/dependencies-rockylinux8.5.tar.gz>
- **Rocky8.6:** <http://download.netbraintech.com/dependencies-rockylinux8.6.tar.gz>

2. Copy the downloaded dependency package to your Linux server.

3. Run the `tar -zxvf dependencies-<OS version>-8.0.tar.gz` command to decompress the package.

Tip: Possible values of **OS version** include: centos7.5; centos7.6; centos7.7; centos7.8; centos7.9; centos8.2; centos8.3; centos8.4; centos8.5; rhel7.5; rhel7.6; rhel7.7; rhel7.8; rhel7.9; rhel8.2; rhel8.3; rhel8.4; rhel8.5; rhel8.6; ol7.7; ol7.8; ol7.9; ol8.2; ol8.3; ol8.4; ol8.5; ol8.6; almalinux8.4; almalinux8.5; almalinux8.6; rockylinux8.4; rockylinux8.5; rockylinux8.6.

4. Run the `cd dependencies` command to navigate to the decompressed directory.

5. Run the `offline-install.sh` command to install the dependencies.

3. Appendix: Editing a File with VI Editor

The following steps illustrate how to edit a configuration file with the vi editor, which is the default text file editing tool of a Linux operating system.

1. Create a terminal and run the `cd` command at the command line to navigate to the directory where the configuration file is located.
2. Run the `vi <configuration file name>` command under the directory to show the configuration file.
3. Press the **Insert** or **I** key on your keyboard, and then move the cursor to the location where you want to edit.
4. Modify the file based on your needs, and then press the **Esc** key to exit the input mode.
5. Enter the `:wq!` command and press the **Enter** key to save the changes and exit the vi editor.

4. Appendix: Restoring MongoDB Data

Complete the following steps to restore the MongoDB data with the backup data if you encounter data loss or corruption during the upgrade process.

1. Log in to the Linux server where the MongoDB is installed as the **root** user.

2. Stop the MongoDB Service.

1) Run the `systemctl stop mongodnetbrain` command to stop the MongoDB service.

2) Run the `ps -ef|grep mongod` command to verify whether the **mongod** process is stopped.

```
[root@localhost ~]# ps -ef| grep mongod
root      15136 14237  0 10:42 pts/2    00:00:00 grep --color=auto mongod
```

Note: If the **mongod** process is stopped, the result should only contain one entry as shown above.

3. Restore the old data onto the MongoDB.

1) Run the `cd /usr/lib/mongodb` command to navigate to the **/usr/lib/mongodb** directory.

Note: If you modified the default directory to store all MongoDB data files during the MongoDB installation, you must use the new directory (available in the **mongod.conf** file) accordingly. For an upgraded system, e.g., upgraded from IEv7.x, the default directory is **/opt/mongodb**.

2) Run the `ls -al` command to browse all directories and files under the **/usr/lib/mongodb** directory.

```
[root@localhost mongodb]# ls -al
total 142
drwxr-xr-x. 5 netbrain netbrain  146 Oct 19 15:02 .
drwxr-xr-x. 4 root      root      42 Sep 19 14:41 ..
drwxr-xr-x. 4 root      root      42 Oct 19 15:03 data
drwxr-xr-x. 4 root      root     100 Oct 19 15: 03 log
-rwxr-xr-x. 2 netbrain netbrain 1004 Aug 25 17: 26 mongodb-keyfile
-rwxr-xr-x. 1 netbrain netbrain 1076 Oct 19 15:02 mongod.conf
```

3) Run the `rm -rf ./data` command to delete the **data** directory.

4) Run the `mv /etc/mongodb_databk/data` command under the **/usr/lib/mongodb** directory to move the data directory to the **/opt/mongodb** directory.

5) Run the `ls -al` command to browse all directories and files under the **/usr/lib/mongodb** directory.

```
[root@localhost mongodb]# ls -al
total 142
drwxr-xr-x. 5 netbrain netbrain  146 Oct 19 15:02 .
drwxr-xr-x. 4 root      root      42 Sep 19 14:41 ..
```

```
drwxr-xr-x. 4 root    root    86016 Oct 19 15: 03 data
drwxr-xr-x. 4 root    root      100 Oct 19 15: 03 log
-rwxr-xr-x. 2 netbrain netbrain 1004 Aug 25 17: 26 mongodb-keyfile
-rwxr-xr-x. 1 netbrain netbrain 1076 Oct 19 15:02 mongod.conf
-rwxr-xr-x. 1 netbrain netbrain 1147 Oct 19 14:51 mongod.conf2017|Oct|19|10:15:50
```

4. Run the `systemctl start mongodnetbrain` command to restart the MongoDB service.
5. Run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name>` command to connect to the node.

Example:

```
[root@localhost upgrade_replica_set]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.6
connecting to: mongodb://10.10.3.142:27017/?authMechanism=SCRAM-SHA-
256&authSource=admin&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("0315bda2-73f3-4304-9166-c008b9b06ce3") }
MongoDB server version: 4.0.6
...
rsnetbrain:PRIMARY>
```

Tip: If SSL is enabled, run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates` command.

5. Appendix: Dumping MongoDB Data

The built-in MongoDB command `mongodump` is a simple and efficient tool for backing up a small volume of MongoDB data. However, for a large volume of data, it is more time-consuming than using the `cp` command to copy data files from the MongoDB Server directly.

Note: Make sure the service of MongoDB is running when you run the `mongodump` command.

Note: The dumped data can be used to restore data in any server.

1. Log in to the Linux server where the MongoDB is installed as the **root** user.
2. Open a command prompt and run the following command to create a directory under the **/etc** directory to save the backup data.

```
[root@localhost ~]# mkdir /etc/mongodb_databk
```

3. Enter the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip -out <filepath>` command in one line and run it to dump the MongoDB data to the **/etc/mongodb_databk** directory.

Example:

```
[root@localhost ~]# mongodump --host 127.0.0.1:27017 -u mongodb -p mongodb  
--authenticationDatabase admin --gzip --out /etc/mongodb_databk
```

Tip: If SSL is enabled, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <dbname> --ssl --sslAllowInvalidCertificates --gzip -out <filepath>` commands.

4. Verify the backup result.
 - 1) Run the `cd /etc/mongodb_databk` command to navigate to the **/etc/mongodb_databk** directory.
 - 2) Run the `ls -al` command under the **mongodb_databk** directory to browse the backup data.

6. Appendix: Restoring Dumped MongoDB Data

Restore the dumped data by using the `mongorestore` command provided by MongoDB.

Note: Make sure the service of MongoDB is running when you run the `mongorestore` command.

Note: Make sure other relevant services are stopped.

Enter the `mongorestore --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip <filepath>` command in one line and run it to restore the dumped data onto the MongoDB Server:

Example:

```
[root@localhost ~]# mongorestore --host 127.0.0.1:27017 -u mongodb -p mongodb --  
authenticationDatabase admin --gzip /etc/mongodb_databk
```

Tip: If SSL is enabled, run the `mongorestore --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <dbname> --ssl --sslAllowInvalidCertificates --gzip <filepath>` commands.

7. Appendix: Generating SSL Certificate

1. Run PowerShell as an administrator.

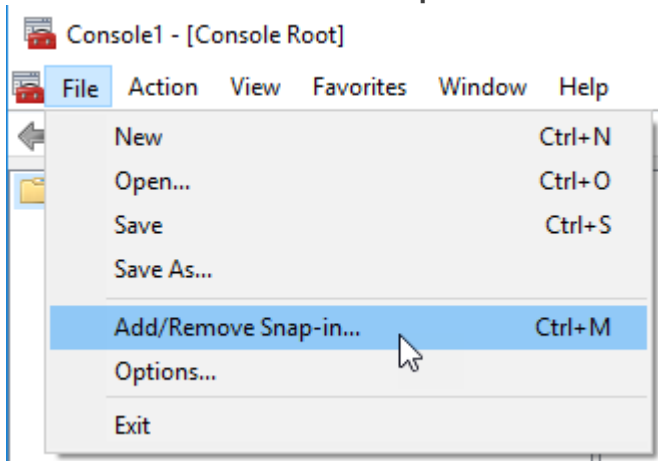
2. Run the following command to create the certificate:

```
New-SelfSignedCertificate -DnsName <Computer name> -CertStoreLocation  
"cert:\LocalMachine\My"
```

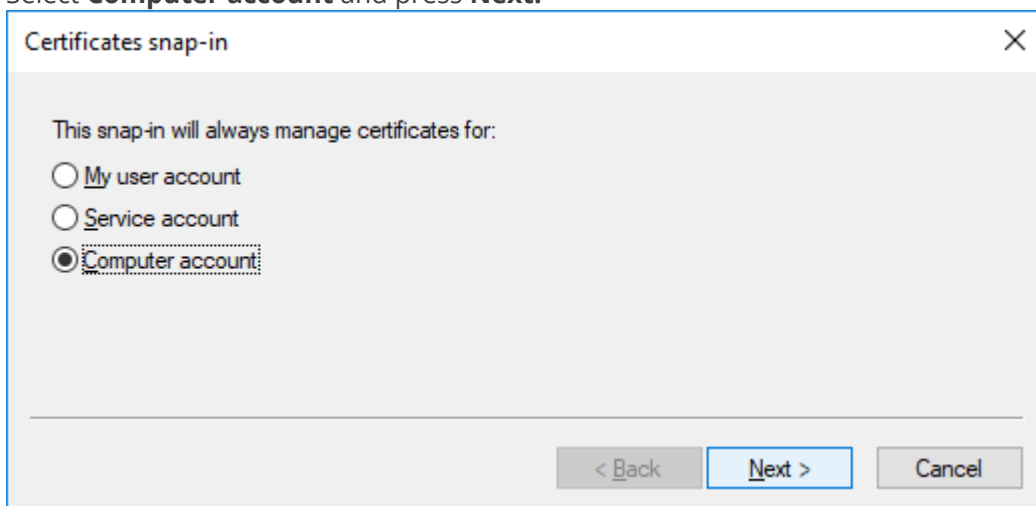
Tip: You can use the Tab key to help you input location, and hostname command for your computer name.

3. Next, you need to add the self-signed certificate as a trusted certificate authority.
Run `MMC -32` as an administrator.

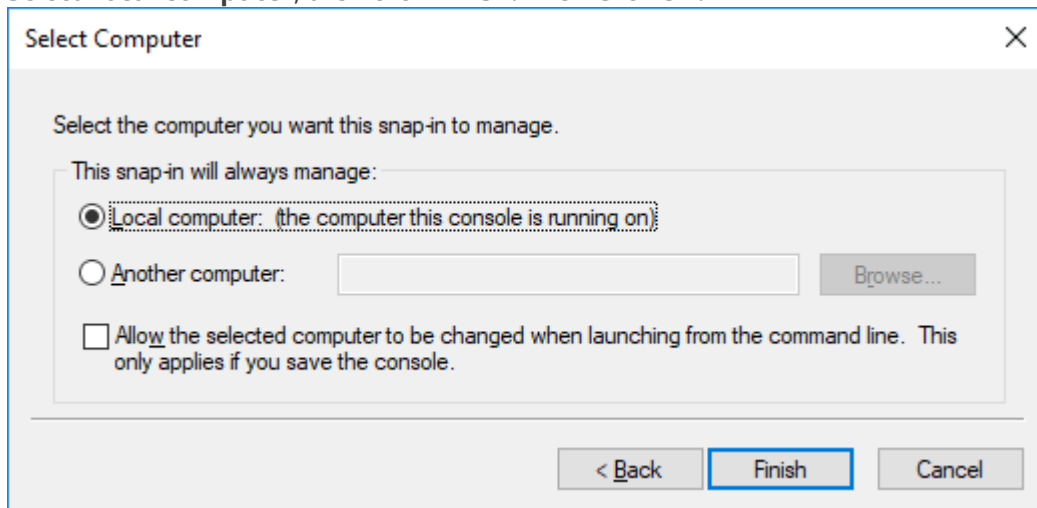
4. Select **File > Add or Remove Snap-ins**.



5. Select **Certificates** and then click **Add**.
6. Select **Computer account** and press **Next**.



7. Select **Local computer**, then click **Finish**. Then Click **OK**.



8. Find the certificate in **Personal > Certificates**.
9. Right-click the newly created certificate and then select **Properties**. Input the desired *Friendly Name* field for the certificate based upon what you are testing. Once completed, select the **Apply** button followed by **OK**.
10. You can copy the certificate to **Trusted Root Certificate Authorities**.