



NetBrain® Integrated Edition 10.1

System Upgrade Guide

Distributed Deployment

1. Upgrading System	4
1.1. Terminating System Tasks and Sessions	6
1.2. Stopping Server Services.....	6
1.3. Backing Up MongoDB Data	7
1.4. Upgrading MongoDB.....	9
1.5. Upgrading Elasticsearch.....	11
1.6. Upgrading License Agent.....	14
1.7. Upgrading Redis.....	16
1.7.1. Installing Redis on Linux	16
1.8. Upgrading RabbitMQ.....	21
1.8.1. Installing RabbitMQ on Linux.....	22
1.9. Installing Service Monitor Agent	27
1.9.1. Installing Service Monitor Agent on Linux.....	28
1.9.2. Installing Service Monitor Agent on Windows.....	31
1.10. Upgrading Web/Web API Server	34
1.11. Upgrading Worker Server	41
1.12. Installing Task Engine	47
1.13. Installing Front Server Controller.....	51
1.14. Upgrading Front Server.....	56
1.14.1. Installing Front Server.....	56
1.14.2. Uninstalling Proxy Server.....	62
1.15. Unbinding Perpetual License	62
1.16. Activating Subscription License.....	63
1.17. Verifying Upgrade Results.....	64

1.18.	Allocating Tenants to Front Server Controller.....	66
1.19.	Adding a Front Server for a Tenant	68
1.20.	Registering a Front Server	69
1.21.	Upgrading External Authentication	72
1.22.	Upgrading Email Settings.....	73
1.23.	Configuring Auto Upgrade Settings.....	73
1.24.	Customizing MongoDB Disk Alert Rules	84
1.25.	Tuning Live Access	85
1.26.	Scheduling Benchmark Task	86
3.	Appendix: Editing a File with VI Editor	87
4.	Appendix: Offline Installing Third-party Dependencies	88
4.	Appendix: Restoring MongoDB Data	90
5.	Appendix: Dumping MongoDB Data	92
6.	Appendix: Restoring Dumped MongoDB Data.....	93
7.	Appendix: Interactive Pre-Installation of Service Monitor Agent.....	94
8.	Appendix: Generating SSL Certificate.....	95

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.

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

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 Front 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 MongoDB](#)
5. [Upgrade Elasticsearch](#)
6. [Upgrade License Agent](#)
7. [Upgrade Redis](#)
8. [Upgrade RabbitMQ](#)
9. [Upgrade Web/Web API Server](#)
10. [Upgrade Worker Server](#)
11. [Install Task Engine](#)
12. [Install Front Server Controller](#)
13. [Upgrade Front Server](#)
14. [Install Service Monitor Agent](#)
15. [Unbind Perpetual License](#)
16. [Activate Subscription License](#)
17. [Verify Upgrade Results](#)

18. [Allocate Tenants to Front Server Controller](#)
19. [Add a Front Server to a Tenant](#)
20. [Register a Front Server](#)
21. [Upgrade External Authentication](#)
22. [Upgrade Email Settings](#)
23. [Customize MongoDB Disk Alert Rules](#)
24. [Tune Live Access](#)
25. [Schedule Benchmark Task](#)

Network Connectivity Requirements

Source	Destination	Protocol *) and Port Number **)
Thin Client	Web Server Web API Server	HTTP/HTTPS (80/443)
Service Monitor Agent	Web API Server	HTTP/HTTPS (80/443)
Web API Server	Knowledge Cloud Domain (https://knowledgecloud.netbraintech.com/)	HTTPS (443)
Web API Server Worker Server Task Engine Front Server Controller	MongoDB RabbitMQ	TCP 27017 TCP 5672
Web API Server Worker Server	Elasticsearch License Agent	TCP 9200 TCP 27654
Web API Server Worker Server Front Server Controller	Redis	TCP 6379 (non-ssl)
Worker Server Task Engine Front Server	Front Server Controller	TCP 9095
Front Server	Live Network	ICMP/SNMP/Telnet/SSH/REST API
Front Server	Ansible Agent (add-on)	TCP 9098
MongoDB License Agent	Web API Server	TCP 9099 ***)

Source	Destination	Protocol *) and Port Number **)
Elasticsearch		
Redis		
RabbitMQ		
Web Server		
Worker Server		
Task Engine		
Front Server		
Front Server Controller		
Web API Server	RabbitMQ	TCP 15672 ***)

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 for 10.1.

1.1. Terminating System Tasks and Sessions

1. Log into System Management page.
2. Navigate to **Current Users** tab, click **End Session** to terminate any active sessions.
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 servers 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 (Proxy) Server	proxyserverie
Task Engine	N/A
Front Server Controller	N/A

2. Disable the **Cron** task on the MongoDB. 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 MongoDB 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
```

```
*/1 * * * * /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.

```
#*/1 * * * * /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 `service mongodnetbrain stop` 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 `service mongodnetbrain start` command to start the MongoDB service.

1.4. Upgrading MongoDB

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with MongoDB and it 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 it has 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 them online
- **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded your 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 installation or 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.

Note: Upgrading the Linux operating system from v7.x to v8.x is **NOT** supported once the installation or upgrade of NetBrain Workstation v10 is completed. Refer to [Linux System Upgrade Instructions Online](#) or [Linux System Upgrade](#)

[Instructions Offline](#) for workaround solution to upgrade Linux operating system from v7.x to v8.x prior to the installation of or upgrade to NetBrain Workstation v10.

Upgrading MongoDB

1. Log in to the Linux server as the **root** user.

Note: It is highly recommended to install **numactl** on the Linux Server to optimize MongoDB performance. Run the `rpm -qa | grep numactl` command to check whether **numactl** has already been installed. If it has not been installed yet and the Linux server has access to the Internet, run the `yum install numactl` command to install it online.

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. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.

4. Download the installation package.

- **Option 1:** If the Linux server has no access to the Internet, obtain the **mongodb-linux-x86_64-rhel-4.0.28-10.1.tar.gz** file from NetBrain and upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
- **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/mongodb-linux-x86_64-rhel-4.0.28-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to directly download the **mongodb-linux-x86_64-rhel-4.0.28-10.1.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf mongodb-linux-x86_64-rhel-4.0.28-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

```
[root@centos netbraintemp10.1]# tar -zxvf mongodb-linux-x86_64-rhel-4.0.28-10.1.tar.gz
MongoDB/
MongoDB/config/
...
MongoDB/upgrade/upgrade_single_node/upgrade.sh
```

6. Run the `cd MongoDB` command to navigate to the **MongoDB** directory.

7. Enter the MongoDB username and password with the interactive command line.

```
INFO: 2022-02-10 17-54-52.734: MongoDB configuration file: /home/mongod.conf
Unit mongod.service could not be found.
The service of mongodnetbrain is running.
Please enter the MongoDB username: mongodb
Please enter the MongoDB password:
Successfully connected to MongoDB.
```

8. Run the `systemctl start mongodnetbrain` command to restart the MongoDB service.
9. Run the `./upgrade.sh` command under the **MongoDB** directory.

Note: Ensure MongoDB service is up and running before executing the `./upgrade.sh` command.

Note: If the default username and password were changed during the installation of MongoDB, you must enter these customized values during the upgrade.

Note: Before upgrading this component, Service Monitor Agent will be upgraded to the latest version. You'll need to use the interactive command line to install it. See [Appendix: Interactive Pre-Installation of Service Monitor Agent](#) for more details.

9. After the MongoDB Server is successfully upgraded, run the `systemctl status mongod` command to check its service status.

```
[root@localhost ~]# systemctl status mongod
mongod.service - MongoDB service
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-07-13 15:16:45 EDT; 1min 1s ago
     Process: 3025 ExecStop=/usr/bin/pkill mongod (code=exited, status=0/SUCCESS)
     Process: 3029 ExecStart=/bin/mongod -f /etc/mongodb/mongod.conf (code=exited, status=0/SUCCESS)
   Main PID: 3031 (mongod)
   Memory: 181.4M (limit: 6.8G)
   ...
```

1.5. Upgrading Elasticsearch

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with Elasticsearch and it 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 it has 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 them online
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded the 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 installation or 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, do not 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.

Note: Upgrading the Linux operating system from v7.x to v8.x is **NOT** supported once the installation or upgrade of NetBrain Workstation v10 is completed. Refer to [Linux System Upgrade Instructions Online](#) or [Linux System Upgrade Instructions Offline](#) for workaround solution to upgrade Linux operating system from v7.x to v8.x prior to the installation of or upgrade to NetBrain Workstation v10.

Upgrading Elasticsearch

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**.
3. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **elasticsearch-linux-x86_64-rhel-6.8.23-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.1** directory to directly download the **elasticsearch-linux-x86_64-rhel-6.8.23-10.1.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf elasticsearch-linux-x86_64-rhel-6.8.23-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

```
[root@centos netbraintemp10.1]# tar -zxvf elasticsearch-linux-x86_64-rhel-6.8.23-10.1.tar.gz
Elasticsearch/
Elasticsearch/config/
...
Elasticsearch/upgrade.sh
```

6. Run the `cd Elasticsearch` command to navigate to the **Elasticsearch** directory.
7. Run the `./upgrade.sh` command under the **Elasticsearch** directory.

Note: If the default username and password were changed during the installation of Elasticsearch, you must enter these customized values during the upgrade.

8. After the Elasticsearch is successfully upgraded, run the `systemctl status elasticsearch` command to check its service status.

```
[root@localhost ~]# systemctl status elasticsearch
elasticsearch.service - Elasticsearch
Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2020-07-13 15:28:12 EDT; 1min 15s ago
Docs: http://www.elastic.co
Main PID: 7751 (java)
Memory: 4.2G
```

9. Run the `curl -s -XGET --user <username:password> http://<IP address>:<port>` command to check the current version of Elasticsearch.

Note: If you enabled SSL, please use the `curl --tlsv1.2 -k -s -XGET --user <username:password> https://<IP address>:<port>` command instead.

Example:

```
[root@localhost Elasticsearch]# curl -s -XGET --user admin:admin http://10.10.3.142:9200
{
  "name" : "node1",
  "cluster_name" : "elastic-search-cluster",
  "cluster_uuid" : "OctFIL44T--5mArFA93r-A",
  "version" : {
    "number" : "6.8.23",
    "build_flavor" : "oss",
    "build_type" : "rpm",
    "build_hash" : "56c6e48",
    "build_date" : "2019-04-29T09:05:50.290371Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.3",
```

```

    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}

```

1.6. Upgrading License Agent

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with License Agent and it 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 it has 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 them online
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded the 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 installation or 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, do not 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.

Note: Upgrading the Linux operating system from v7.x to v8.x is **NOT** supported once the installation or upgrade of NetBrain Workstation v10 is completed. Refer to [Linux System Upgrade Instructions Online](#) or [Linux System Upgrade Instructions Offline](#) for workaround solution to upgrade Linux operating system from v7.x to v8.x prior to the installation of or upgrade to NetBrain Workstation v10.

Upgrading License Agent

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**.
3. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.

4. Download the installation package.

- **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-licenseagent-linux-x86_64-rhel-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
- **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.1** directory to directly download the file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf netbrain-licenseagent-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-licenseagent-linux-x86_64-rhel-10.1.tar.gz
License/
License/config/
License/config/install_licenseagent.conf
License/config/setup.conf
...
License/upgrade.sh
```

6. Run the `cd License` command to navigate to the **License** directory.

7. Run the `./upgrade.sh` command under the **License** directory.

- 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 License Agent.

```
[root@localhost License]# ./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: Creating upgrading log...
INFO: Dependent Package:
INFO: Component Name: License Agent
INFO: RPM name: netbrainlicense
INFO: RPM package list:
INFO: Starting to check system
...
INFO: Successfully installed License Agent. Service is running.
INFO: Backing up uninstall.sh SUCCEEDED.
INFO: Upgrading License Agent SUCCEEDED.
```

8. After the License Agent is successfully upgraded, run the `systemctl status netbrainlicense` command to check its service status.

```
[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 Mon 2020-07-13 15:35:39 EDT; 4min 11s ago
     Main PID: 10668 (licensed)
    CGroup: /system.slice/netbrainlicense.service
            └─10668 /usr/bin/netbrainlicense/licensed -f /etc/netbrainlicense/licensed.conf

Jul 13 15:35:39 netbrain_data_server systemd[1]: Starting NetBrain license agent service...
Jul 13 15:35:39 netbrain_data_server systemd[1]: Started NetBrain license agent service.
```

1.7. Upgrading Redis

Complete the following steps to upgrade Redis:

1. [Installing Redis on Linux](#)
2. [Uninstalling Redis on Windows](#)

1.7.1. Installing Redis on Linux

Pre-Installation Task

- Ensure you have upgraded the 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 installation or 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, do not 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.

Note: Upgrading the Linux operating system from v7.x to v8.x is **NOT** supported once the installation or upgrade of NetBrain Workstation v10 is completed. Refer to [Linux System Upgrade Instructions Online](#) or [Linux System Upgrade Instructions Offline](#) for workaround solution to upgrade Linux operating system from v7.x to v8.x prior to the installation of or upgrade to NetBrain Workstation v10.

Installing Redis on Linux

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**.
3. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **redis-linux-x86_64-rhel-6.2.6-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/redis-linux-x86_64-rhel-6.2.6-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to directly download the **redis-linux-x86_64-rhel-6.2.6-10.1.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf redis-linux-x86_64-rhel-6.2.6-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

```
[root@localhost netbraintemp10.1]# tar -zxvf redis-linux-x86_64-rhel-6.2.6-10.1.tar.gz
redis/
redis/config/
...
redis/config/setup.conf
...
redis/install.sh
...
```

6. Run the `cd redis/config/` command to navigate to the **config** directory.

7. Modify the [parameters](#) in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, see [Appendix: Editing a File with VI Editor](#) for more details.

```
[root@localhost config]# vi setup.conf
#Redis configuration file

#Note: Entries other than the password
can only contain letters or numbers, and should start with a letter.

#Account info.
#Password should not contain: {}[]:","|<>@&^%\\ or a space. The password should be the same
in all nodes if the mode is a cluster.
Password=Admin1.#

# Mode use 'standalone' if single installation, use 'cluster' if HA mode
Mode=standalone

# Port is used to start the redis service on specified port. We use default port 6379.
# Please enter the same Port for all nodes that belong to the same cluster
Port=6379

# Data Path is used to store redis files. Default path /var/lib/redis.
DataPath=/var/lib/redis

# Log Path is used to store redis log files. Default path /var/log/redis.
LogPath=/var/log/redis

# Role (NodeRole can only be 'master', 'slave' 'sentinel' or 'dr-sentinel')
# sentinel - start the redis in sentinel mode so that it can monitor a cluster
# dr-sentinel - start the redis in sentinel mode so that it can monitor a DR cluster for a
multi-DC on same node where you have redis already installed

NodeRole=master
#Master Node (Master Node can support ip address, hostname or FQDN and is used if the Mode is
cluster)
MasterNode=
# Sentinel Port is used to start the redis sentinel service on specified port. We use default
port 6380.
# For a multi-DC DR cluster there will be 2 instances of sentinel on same arbiter node so user
should change this value to default port 6381
or any other port which is not used by other service.
# Please enter the same sentinelPort for all nodes that belong to the same cluster
SentinelPort=6380

# Resource limitation. It can only be 'yes' or 'no'
ResourceLimit=no
# CPU Limit. It should end with %. Range is 1% to 100%
CPULimit=100%
#Memory Limit. It should end with %. Range is 1% to 100%
MemmmoryLimit=100%

# TLS. It can only be 'yes' or 'no'
UseSSL=no
Certificate=/etc/ssl/cert.pem
```

```
PrivateKey=/etc/ssl/key.pem
CertAuth=/etc/ssl/cacert.pem
```

8. Run the `cd ..` command to navigate to the **redis** directory.
9. Run the `./install.sh` script under the **redis** directory to install Redis.

```
[root@localhost redis]# ./install.sh
INFO: Checking root
INFO: Checking date
INFO: Starting to check Linux OS info
INFO: Starting to check required CPU
INFO: Starting to check minimum memory
INFO: Creating installation log file SUCCEEDED
INFO: Starting to check crontab
INFO: Component Name: Redis
INFO: RPM name: redis
INFO: Service name: redis
INFO: RPM package list: redis-6.2.6-1.x86_64.rpm
INFO: Config path: /etc/redis
INFO: Preprocessing SUCCEEDED
INFO: Starting to check system
INFO: Collecting system information SUCCEEDED.
INFO: Starting to check if rpm exists
INFO: Starting to check systemd
INFO: System checking SUCCEEDED
...
redis.service - Redis
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-07-14 00:38:49 EST; 37min ago
     Main PID: 36704 (redis-server)
        Memory: 1.2M
      CGroup: /system.slice/redis.service
              56299 /sbin/redis-server *:6379
...
INFO: Checking redis Status
INFO: Verification SUCCEEDED
INFO: Backup uninstall.sh SUCCEEDED
INFO: Backup fix_releaseinfo.json SUCCEEDED
INFO: Successfully installed Redis
```

10. Run the `systemctl status redis` command to verify whether its service starts successfully.

```
[root@localhost ~]# systemctl status redis
redis.service - Redis
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-07-13 15:47:04 EDT; 10min ago
     Main PID: 13240 (redis-server)
        Memory: 1.8M
...

```

Note: When your disk space is insufficient for large amounts of logs, you can modify the log settings in the **redis.conf** file under the **/etc/logrotate** directory.

Parameters


The following table describes the parameters that can be configured when installing Redis.

Parameter	Default Value	Description
Password	Admin1.#	Specify the admin password used to connect to Redis. Note: The password cannot contain any of the following special characters, and its length cannot exceed 64 characters. <code>{ } [] : " , ' < > @ & ^ % \</code> and spaces
Mode	standalone	Set whether to enable cluster deployment. Keep the default value for a standalone deployment.
Port	6379	Specify the port number that the master Redis node listens to.
DataPath	/var/lib/redis/	Specify the storage path for all data files of Redis.
LogPath	/var/log/redis/	Specify the storage path for all log files of Redis.
NodeRole	master	Set the role for the current node. Available options are master , slave , sentinel and dr-sentinel . Keep the default value for a standalone deployment.
MasterNode		This parameter is only required for cluster deployments.
SentinelPort	6380	The port number that the sentinel or dr-sentinel node listens to. Note: Use alternative port such as 6381 when deploying the dr-sentinel node.
ResourceLimit	no	Set whether to limit the system resource usage for Redis.
CPULimit	100%	The maximum CPU utilization of the machine that can be consumed by Redis.
MemoryLimit	100%	The maximum memory capacity of the machine that can be consumed by Redis.
UseSSL	no	Set whether to enable the encrypted connections to Redis by using SSL. Note: Redis itself does not support SSL. It uses stunnel as an SSL service agent. Stunnel will be automatically installed together with Redis.
Certificate	/etc/ssl/cert.pem	Specify the storage path for all the certificates and key files used for SSL authentication.

Parameter	Default Value	Description
		Note: It is required only if UseSSL is enabled.
PrivateKey	<code>/etc/ssl/key.pem</code>	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
CertAuth	<code>/etc/ssl/cacert.pem</code>	Specify the name of the SSL certificate chain or intermediate certificate (class 2 or class 3 certificate). Note: It is required only if UseSSL is enabled.

1.7.1.1. Uninstalling Redis on Windows

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 Redis (Cache) Server** app in the pane, and then select **Run as administrator** from the list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box pops up.
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.

1.8. Upgrading RabbitMQ

Complete the following steps to upgrade RabbitMQ:

1. [Installing RabbitMQ on Linux](#)

1.8.1.Installing RabbitMQ on Linux

Pre-Installation Task

- Ensure you have upgraded the 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 installation or 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, do not 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.

Note: Upgrading the Linux operating system from v7.x to v8.x is **NOT** supported once the installation or upgrade of NetBrain Workstation v10 is completed. Refer to [Linux System Upgrade Instructions Online](#) or [Linux System Upgrade Instructions Offline](#) for workaround solution to upgrade Linux operating system from v7.x to v8.x prior to the installation of or upgrade to NetBrain Workstation v10.

- 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**. Before you install the RabbitMQ, run the `rpm -qa|grep socat` and `rpm -qa|grep logrotate` commands to check whether they have been installed on the 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 [Offline Installing Third-party Dependencies](#) for more details.
- 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.

Note: If the Service Monitor Agent was not previously installed, it will be installed with RabbitMQ. You'll need to use the interactive command line to install it. See Installing MongoDB on Linux for more details. You can also install the Service Monitor Agent separately before installing RabbitMQ.

Installing RabbitMQ on Linux

Note: RabbitMQ has dependencies on the third-party package **socat** and **logrotate**. Before you install the RabbitMQ, run the `rpm -qa | grep socat` and `rpm -qa | grep logrotate` command to check whether **socat** and **logrotate** have been installed on the server. If it has not been installed, you can choose either option below to install the dependencies.

- **Online Install:** run the `yum -y install socat` and `yum -y install logrotate` command to install them online.

- **Offline Install:** see [Appendix: Offline Installing Third-party Dependencies](#) for more details.

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**
3. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **rabbitmq-linux-x86_64-rhel-3.8.19-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/rabbitmq-linux-x86_64-rhel-3.8.19-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to directly download the **rabbitmq-linux-x86_64-rhel-3.8.19-10.1.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf rabbitmq-linux-x86_64-rhel-3.8.19-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

```
[root@localhost netbraintemp10.1]# tar -zxvf rabbitmq-linux-x86_64-rhel-3.8.19-10.1.tar.gz
rabbitmq/
rabbitmq/config/
rabbitmq/config/setup.conf
...
rabbitmq/install.sh
...
```

6. Run the `cd rabbitmq/config` command to navigate to the **config** directory.

7. Modify the [parameters](#) in the **setup.conf** file and save the changes. For how to modify the configuration file, see [Appendix: Editing a File with VI Editor](#) for more details.

```
[root@centos config]# vi setup.conf
#RabbitMQ configuration file

#Account info
#The UserName or Password should not contain: {}[]:","|<>@&^%\\ or a space
#The length of UserName or Password should not be more than 64 characters
UserName=admin
Password=Admin1.#

# Mode (Mode can only be 'mirror' or 'standalone')
Mode=standalone

# A unique cluster string is used to join all cluster nodes. Each cluster node must have the
same cluster ID.
ClusterId=rabbitmqcluster

# The role of the current node in the cluster. One or two roles can be configured:
# master or slave.
NodeRole=master
# Must specify a resolvable hostname of the master node in either standalone or mirror mode.
MasterNode=localhost

# Resource limitation
ResourceLimit=no

# CPULimit and MemoryLimit should be ended by % and the range is from 1% to 100%
CPULimit=100%
MemoryLimit=100%

# TLS
UseSSL=no
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem

# Port --Please enter the same Port for all nodes that belong to the same cluster
Port=5672

# Log path
LogPath=/var/log/rabbitmq
```

8. Run the `cd ..` command to navigate to the **rabbitmq** directory.
9. Run the `./install.sh` script under the **rabbitmq** directory to install RabbitMQ.

```
[root@localhost rabbitmq]# ./install.sh
INFO: Start checking date
INFO: Start checking os
INFO: Start checking required CPU
INFO: Start checking minimum memory
INFO: Selinux-policy version: 3.13.1
INFO: Component Name: RabbitMQ
INFO: RPM name: rabbitmq-server
```



```

INFO: Service name: rabbitmq-server
INFO: RPM package list: erlang-23.2.1-1.el7.x86_64.rpm rabbitmq-server-3.8.19-1.el7.noarch.rpm
INFO: Installation path: /usr/lib/rabbitmq/
INFO: Config path: /etc/rabbitmq/
INFO: Preprocessing SUCCEEDED
...
Preparing... #####
Updating / installing...
rabbitmq-server-3.8.19-1.el7 #####
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission setting SUCCEEDED
Created symlink from /etc/systemd/system/multi-user.target.wants/rabbitmq-server.service to
/usr/lib/systemd/system/rabbitmq-server.service.
rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset:
disabled)
   Active: active (running) since Mon 2020-07-13 16:04:46 EDT; 8ms ago
 Main PID: 53927 (beam.smp)
   Status: "Initialized"
  Memory: 70.8M (limit: 15.5G)
...
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed RabbitMQ

```

10. Run the `systemctl status rabbitmq-server` command to verify whether its service starts successfully.

```

[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 Mon 2020-07-13 16:05:23 EDT; 13min ago
 Process: 19522 ExecStop=/usr/sbin/rabbitmqctl shutdown (code=exited, status=0/SUCCESS)
 Main PID: 19685 (beam.smp)
   Status: "Initialized"
  Memory: 74.5M
...

```

Parameters

The following table describes the parameters that can be configured when installing RabbitMQ.


Parameter	Default Value	Description
Username	admin	Specify the admin username used to connect to RabbitMQ. Note: The username and password cannot contain any of the following special characters, and its length cannot exceed 64 characters. <code>{ } [] : " , ' < > @ & ^ % \</code> and spaces
Password	Admin1.#	Specify the admin password used to connect to RabbitMQ.

Parameter	Default Value	Description
Mode	standalone	Set the RabbitMQ deployment Mode. Available options are standalone or mirror . Keep the default value standalone for a standalone deployment.
ClusterId	rabbitmqcluster	Specify the cluster id used by all nodes to join the cluster. This parameter is required only for cluster deployments.
NodeRole	master	Set the role for the current node. Available options are master or slave . Keep the default value for a standalone deployment.
MasterNode	localhost	This parameter is required for both standalone and cluster deployments. For standalone Mode, this parameter should be set as a resolvable hostname of the local server.
ResourceLimit	no	Set whether to limit the system resource usage for RabbitMQ.
CPUlimit	100%	Specify the maximum CPU utilization of the machine that can be consumed by RabbitMQ.
MemoryLimit	100%	Specify the maximum memory capacity of the machine that can be consumed by RabbitMQ.
UseSSL	no	<p>Set whether to enable the encrypted connections to RabbitMQ by using SSL.</p> <p>Tip: If UseSSL is set to yes, you can follow the steps below to modify the RabbitMQ Plugin config file after the service monitor is installed.</p> <ol style="list-style-type: none"> 1) Run the <code>vi /etc/netbrain/nbagent/check/rabbitmq.yaml</code> command to open the RabbitMQ Plugin config file. 2) Set the ssl value to true and save the changes. For how to modify the configuration file, see Editing a File with VI Editor for more details. <pre>[root@localhost check]# vi rabbitmq.yaml init_config: instances: - name: default managementPort: 15672, checkAvailableIntervalSeconds: 300 ssl: true collectQueues: equal: [] startWith: ['FullTextSearch', 'TaskManager', 'event_callback', 'RMClientCallbac k', 'ETL_Task'] endWith: ['IndexDriver']</pre>
Certificate	/etc/ssl/cert.p em	<p>Specify the storage path for all the certificates and key files used for SSL authentication.</p> <p>Note: It is required only if UseSSL is enabled.</p>

Parameter	Default Value	Description
PrivateKey	<code>/etc/ssl/key.pem</code>	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
Port	<code>5672</code>	Specify the port number that RabbitMQ service listens to.
LogPath	<code>/var/log/rabbitmq</code>	Specify the directory to save logs of RabbitMQ.

1.8.1.1. Uninstalling RabbitMQ on Windows

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 RabbitMQ (Message) Server** app in the pane, and then select **Run as administrator** from the drop-down list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box pops up.
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.

1.9. Installing Service Monitor Agent

Select one of the following ways to install the Service Monitor Agent on each NetBrain server, depending on its operating system:

- [Installing Service Monitor Agent on Linux](#)
- [Installing Service Monitor Agent on Windows](#)

1.9.1.Installing Service Monitor Agent on Linux

Pre-installation Tasks

- Service Monitor Agent will be installed with all Linux components and it 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 it has 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 [Offline Installing Third-party Dependencies](#) for more details.

Installing Service Monitor Agent on Linux

1. Log in to the Linux server as the **root** user.
2. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.
3. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-servicemonitoragent-linux-x86_64-rhel-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.1** directory to directly download the **netbrain-servicemonitoragent-linux-x86_64-rhel-10.1.tar.gz** file from NetBrain official download site.
4. Run the `tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-10.1.tar.gz` command under the **/opt/netbraintemp10.1** directory to extract installation files.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

```
[root@localhost netbraintemp10.1]# tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-10.1.tar.gz
ServiceMonitorAgent/
ServiceMonitorAgent/config/
ServiceMonitorAgent/config/setup.conf
...
ServiceMonitorAgent/install.sh
...
```

5. Run the `cd ServiceMonitorAgent/config` command to navigate to the **config** directory.
6. Modify the [parameters](#) in the **setup.conf** file located under the **config** directory according to your environment and save the changes. For how to modify the configuration file, refer to [Editing a File with VI Editor](#).

```
[root@localhost config]# vi setup.conf

# IE API Url, for example: http://ie.netbrain.com/ServicesAPI
# Attention please: /ServicesAPI is a fixed suffix
Server_Url=http://10.10.3.141/ServicesAPI

# Authentication Key to be used to communicate with Web API server.
# Note: please ensure this key must be the same as the API key created on Web API server.
Server_Key=Admin1.#

# LogPath is used to store log files for Servicemonitor.
# This directory must be at least a second level directory and used exclusively for this
purpose.
LogPath=/var/log/nbagent

# Whether to enable verifying Certificate Authority (CA): By default, it is disabled.
yes indicates enabled; no indicates disabled.
# Note: To enable the verifying CA, it is needed to change configuration of the Web Server.
CA_Verify=no

# CertAuth specifies the CA file source path. Below CA file will be copied to folder
/etc/ssl/netbrain/nbagent
CertAuth=/etc/ssl/cacert.pem
```

7. Run the `cd ..` command to navigate to the **ServiceMonitorAgent** directory.
8. Run the `./install.sh` script under the **ServiceMonitorAgent** directory to install the Service Monitor Agent.
 - 1) Read the License Agreement, and type **YES**.
 - 2) Type **I ACCEPT** to accept the License Agreement. The script starts to install Service Monitor Agent.

```
[root@localhost ServiceMonitorAgent]# ./install.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 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

Preprocessing SUCCEEDED
Starting to install Service Monitor Agent ...
```

```

Starting to system checking...
  Collecting system information...
...
  Collecting system information SUCCEEDED.
System checking SUCCEEDED.
Starting to configuration parameters checking...
Configuration parameters checking SUCCEEDED.
Start dependencies checking...
Dependencies checking SUCCEEDED.
...
Obtaining file:///usr/share/nbagent
Installing collected packages: agent
  Running setup.py develop for agent
Successfully installed agent
You are using pip version 18.1, however version 19.0.3 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Configuration parameters updating SUCCEEDED.
Starting to permission assigning...
Permission assigning SUCCEEDED.
Starting to daemon setting...
Daemon setting SUCCEEDED.
...
Successfully installed Service Monitor Agent. Service is running.
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed Service Monitor Agent.

```

9. Run the `systemctl status netbrainagent` command to verify whether its service starts successfully.

```

[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 Sat 2019-05-04 23:19:09 EDT; 5min ago
   Main PID: 4520 (python3)
   Memory: 73.5M
   ...

```

Parameters

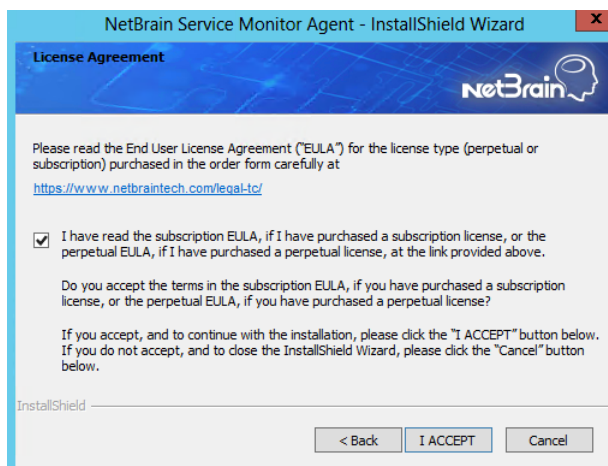
Parameter	Default Value	Description
Server_Url	<code>http://localhost/ServicesAPI</code>	The URL used to call the Web API service, <code>http://<IP address of NetBrain Web API Server>/ServicesAPI</code> . For example, http://10.10.3.141/ServicesAPI . Note: If SSL will be enabled with https binding created for the system website in IIS Manager, type https in the URL. Besides, if CA_Verify is enabled, hostname must be specified in the URL.
Server_Key	<code>Admin1.#</code>	The key used to authenticate the connections to your NetBrain Web API Server. Note: The Server_Key must be kept consistent with the key configured when you installed Web API Server.
LogPath	<code>/var/log/netbrain/nbagent</code>	The storage path for the log files of the Service Monitor Agent.

Parameter	Default Value	Description
		Note: At least 10GB free disk space is required.
CA_Verify	no	Set whether to authenticate the Certificate Authority (CA) of the certificates, which are used to enable SSL for the system website in IIS Manager. Note: It is required only if https is used in Server_Url .
CertAuth	/etc/ssl/cacert.pem	The storage path and file name of the root or class 2 CA file used for CA authentication. Note: It is required only if CA_Verify is enabled. Only the CA file in the Base-64 encoded X.509 (.CER) format is supported.

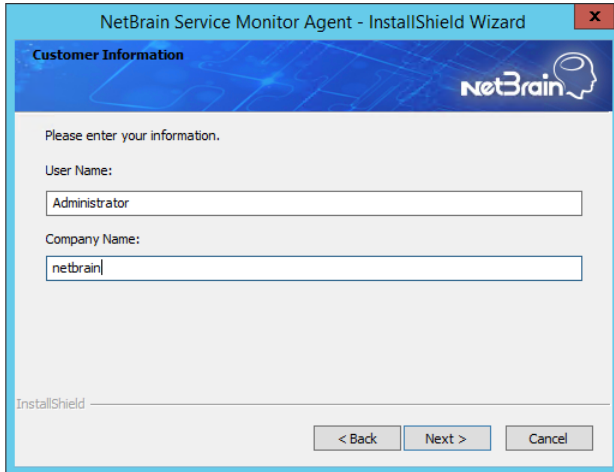
1.9.2.Installing Service Monitor Agent on Windows

Complete the following steps with administrative privileges.

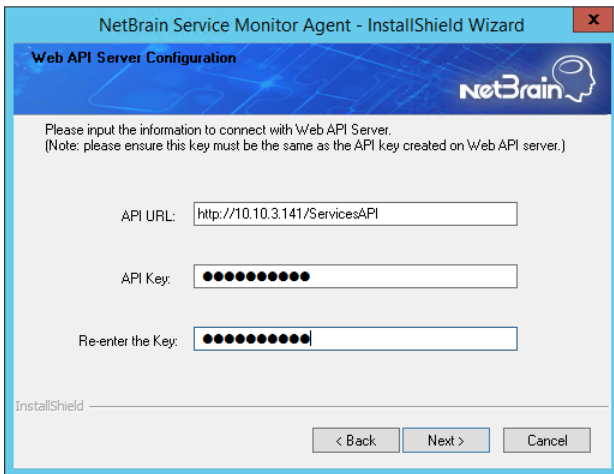
1. Download the **netbrain-servicemonitoragent-windows-x86_64-10.1.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-servicemonitoragent-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-servicemonitoragent-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) On the Welcome page, click **Next**.
 - 2) On the System Configuration page, review the system configuration summary and click **Next**.
 - 3) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA...** check box and then click **I ACCEPT**.



- 4) On the Customer Information page, enter your company name, and then click **Next**.



- 5) On the Destination Location page, click **Next** to install the Service Monitor Agent under the default path **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.
- 6) On the Web API Server Configuration page, enter the following information to connect to your NetBrain Web API Server, and then click **Next**.



- **API URL** — the URL used to call the Web API service, **http://<IP address of NetBrain Web API Server>/ServicesAPI**. For example, **http://10.10.3.141/ServicesAPI**.

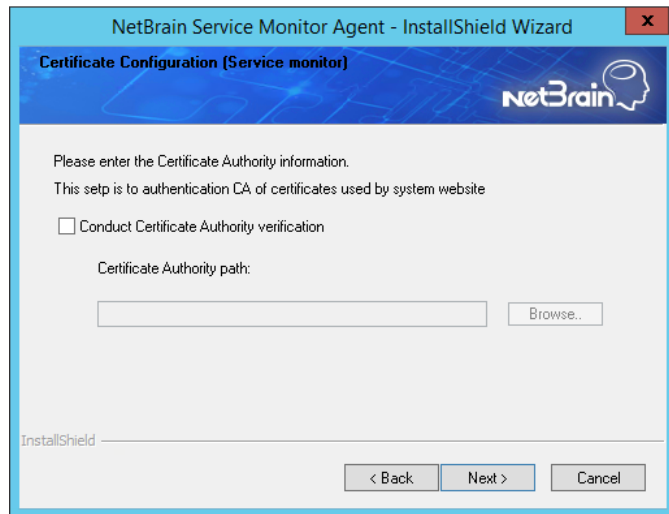
Note: If SSL is enabled with https binding created for the system website in IIS Manager, use **https** in the URL. Besides, if you want to authenticate the Certificate Authority of the SSL certificate used by the system website (to be completed in the next step), the hostname must be specified in the URL.

- **API Key** — the key used to authenticate the connections to Web API Server.

Note: The API Key must be kept consistent with the API Key configured when you install Web API Server.

- 7) This step is required only if **https** is used in **API URL**. Configure whether to authenticate the Certificate Authority (CA) of the certificates used to enable SSL for NetBrain website in IIS Manager, and then click

Next.



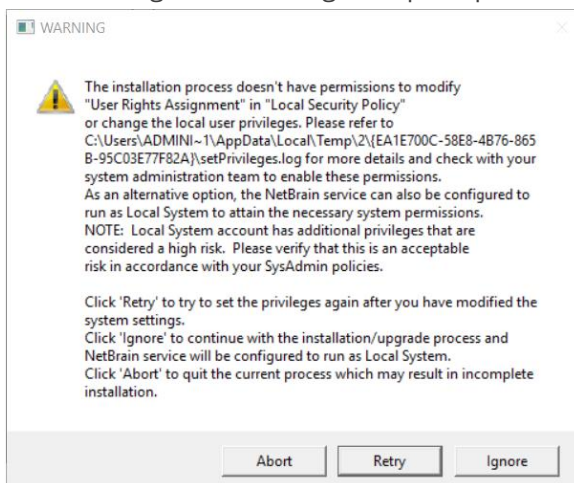
To authenticate CA:

- a) Select the **Conduct Certificate Authority verification** check box.
- b) Click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

8) Review the summary of the installation information and click **Install**.

- 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.

4. After NetBrain Service Monitor Agent is successfully installed, click **Finish** to complete the installation process and exit the Installation Wizard.

Tip: After the installation is completed, you can open the Task Manager and navigate to the **Services** panel to check whether **NetBrainAgent** is running.

1.10. Upgrading Web/Web API Server

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

Note: It is not allowed to upgrade multiple Web API Servers at the same time. Otherwise, it will cause DB data initializing failure.

Note: Service Monitor Agent needs to be installed prior to installing Web/Web API Server. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

Note: Uninstall NetBrain Update Server from the Windows Control Panel.

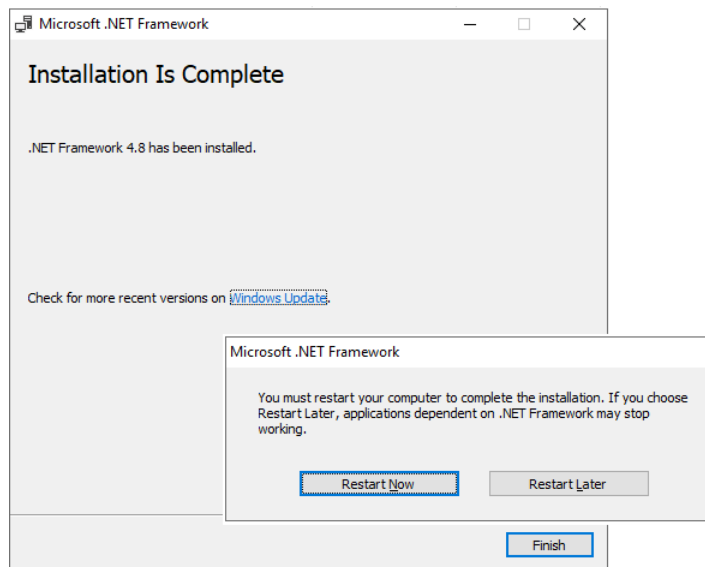
Complete the following steps to upgrade Web API Server and Web Server on the same machine with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-10.1.zip** and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to start the Installation Wizard.
4. Follow the Installation Wizard to complete the upgrade 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** first.

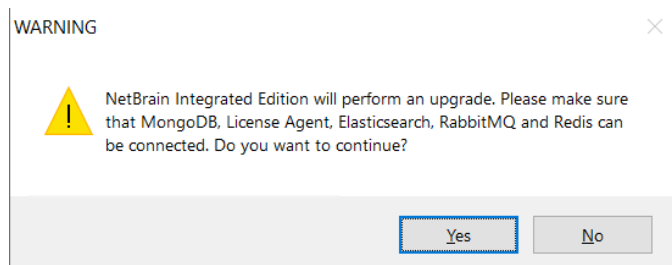
Note: Make sure the Windows update is of the latest. For Windows Server 2012, the update **KB2919442** and **KB2919355** must be installed before the .NET Framework 4.8 installation can start.

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.

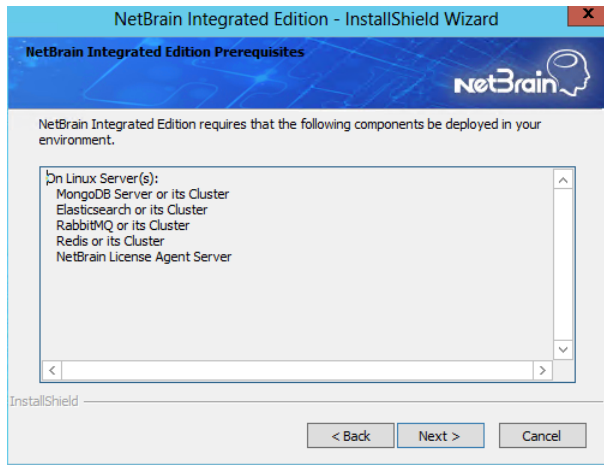


- 2) Stop the services of Web/Web API server manually before continuing the upgrade.
- 3) Click **Yes** in the dialog box to initiate the upgrade.

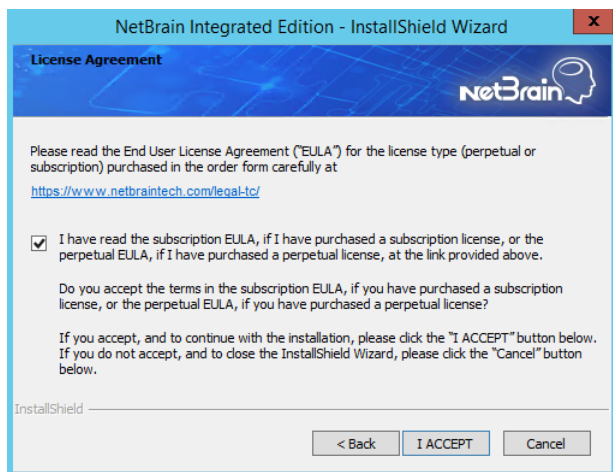


- 4) On the Welcome page, click **Next**.

- 5) On the NetBrain Integrated Edition Prerequisites page, read the components that must be set up in your environment beforehand and click **Next**.



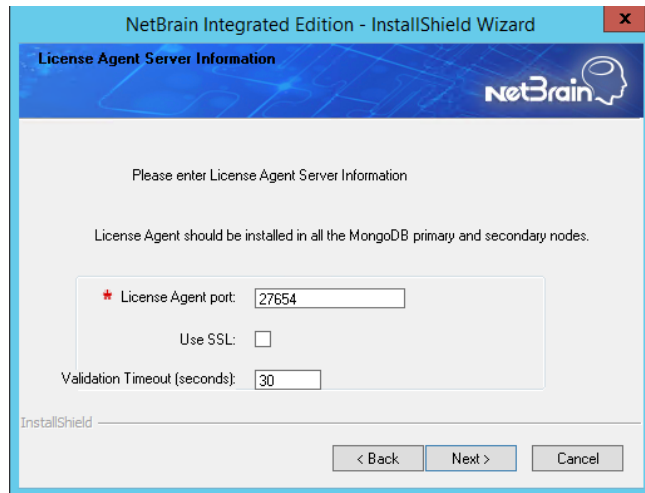
- 6) On the System Configuration page, review the system configuration summary and click **Next**.
- 7) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 8) On the Customer Information page, input your username and company name.
- 9) On the MongoDB Server Connection page, confirm the information and click **Next**.

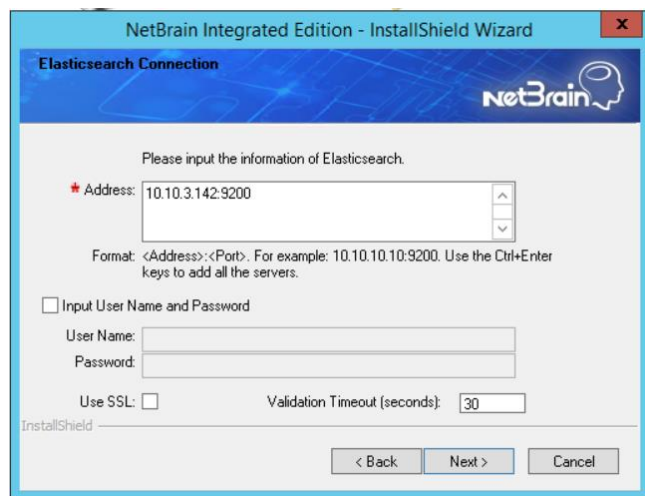


- 10) On the License Agent Server Information page, verify the information to connect to the License Agent, and then click **Next**.



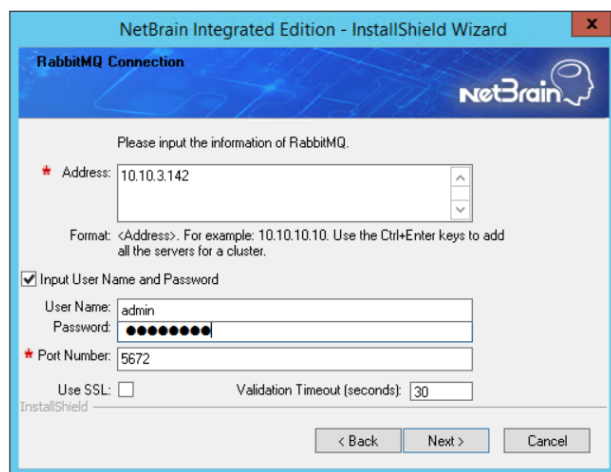
The screenshot shows the 'License Agent Server Information' page of the NetBrain Integrated Edition - InstallShield Wizard. The page has a blue header with the NetBrain logo. The main content area is white and contains the following text: 'Please enter License Agent Server Information', 'License Agent should be installed in all the MongoDB primary and secondary nodes.', and a form with three fields: 'License Agent port:' with a text box containing '27654', 'Use SSL:' with an unchecked checkbox, and 'Validation Timeout (seconds):' with a text box containing '30'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 11) On the Elasticsearch Connection page, confirm the information and click **Next**.



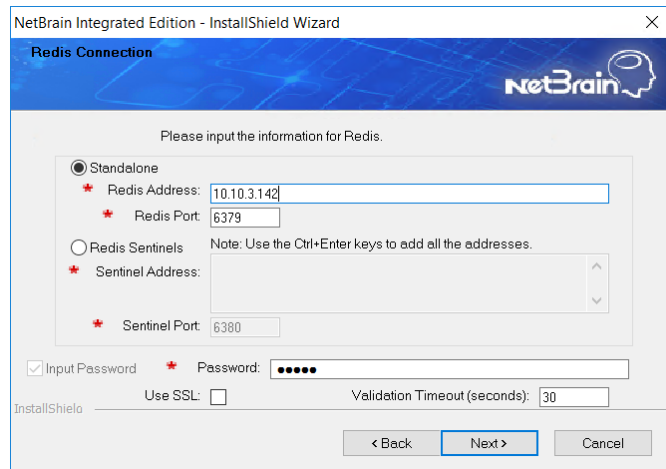
The screenshot shows the 'Elasticsearch Connection' page of the NetBrain Integrated Edition - InstallShield Wizard. The page has a blue header with the NetBrain logo. The main content area is white and contains the following text: 'Please input the information of Elasticsearch.', a form with an 'Address:' field containing '10.10.3.142:9200', a note 'Format: <Address>:<Port>. For example: 10.10.10.10:9200. Use the Ctrl+Enter keys to add all the servers.', an unchecked checkbox for 'Input User Name and Password', and fields for 'User Name:' and 'Password:'. Below these are 'Use SSL:' (unchecked) and 'Validation Timeout (seconds):' (30). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 12) On the RabbitMQ Connection page, enter the IP address, port, user name and password of the RabbitMQ, and then click **Next**.

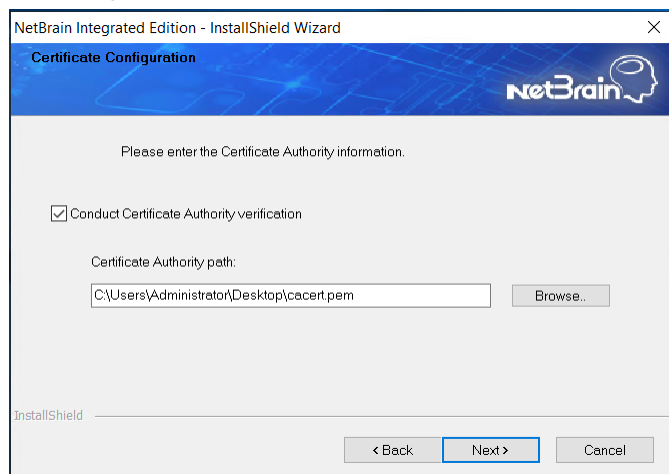


The screenshot shows the 'RabbitMQ Connection' page of the NetBrain Integrated Edition - InstallShield Wizard. The page has a blue header with the NetBrain logo. The main content area is white and contains the following text: 'Please input the information of RabbitMQ.', a form with an 'Address:' field containing '10.10.3.142', a note 'Format: <Address>. For example: 10.10.10.10. Use the Ctrl+Enter keys to add all the servers for a cluster.', a checked checkbox for 'Input User Name and Password', fields for 'User Name:' (admin) and 'Password:' (masked with dots), a 'Port Number:' field containing '5672', 'Use SSL:' (unchecked), and 'Validation Timeout (seconds):' (30). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 13) On the Redis Connection page, enter the IP address, port, and admin password of the Redis, and then click **Next**.



- 14) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) On the Certificate Configuration page, confirm the Certificate Authority (CA) of the SSL certificates used on these servers, and then click **Next**.



To authenticate CA:

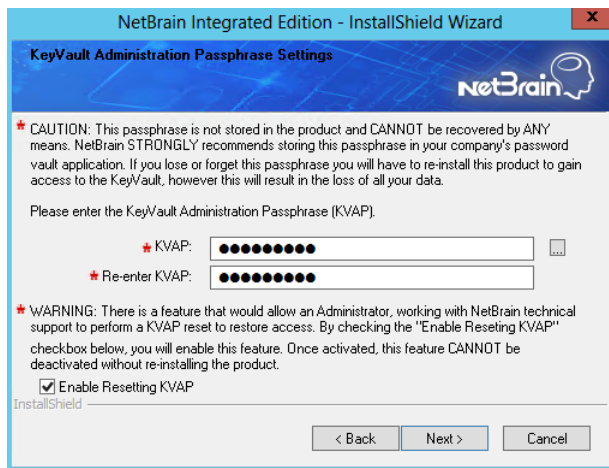
- Select the **Conduct Certificate Authority verification** check box.
- If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

- 15) 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**.

The screenshot shows the 'KeyVault Administration Passphrase Settings' window of the NetBrain Integrated Edition - InstallShield Wizard. It features a blue header with the NetBrain logo. A caution message states that the passphrase is not stored and cannot be recovered. Below this, there are two password input fields labeled 'KVAP:' and 'Re-enter KVAP:'. A warning message explains the 'Enable Resetting KVAP' checkbox, which allows for a KVAP reset. The checkbox is checked. At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons.

NetBrain Integrated Edition - InstallShield Wizard

KeyVault Administration Passphrase Settings

CAUTION: This passphrase is not stored in the product and CANNOT be recovered by ANY means. NetBrain STRONGLY recommends storing this passphrase in your company's password vault application. If you lose or forget this passphrase you will have to re-install this product to gain access to the KeyVault, however this will result in the loss of all your data.

Please enter the KeyVault Administration Passphrase (KVAP).

KVAP: [password field]

Re-enter KVAP: [password field]

WARNING: There is a feature that would allow an Administrator, working with NetBrain technical support to perform a KVAP reset to restore access. By checking the "Enable Resetting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.

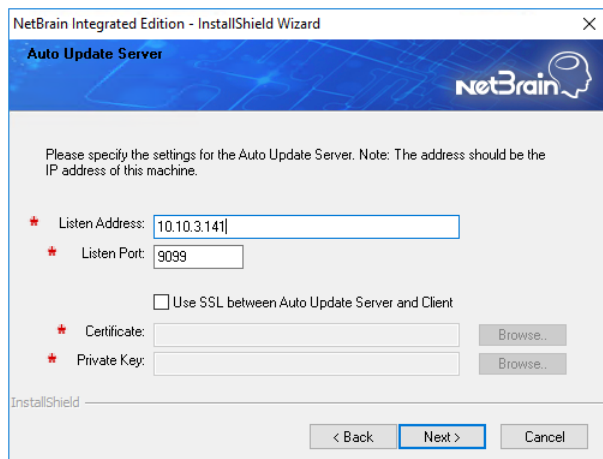
☒ Enable Resetting KVAP

< Back Next > Cancel

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 these servers. In case of losing the passphrase, keep the **Enable Resetting KVAP** check box selected so that NetBrain system admin can reset the passphrase at any time.

- 16) On the Auto Update Server page, verify the configuration summary and then click **Next**.

The screenshot shows the 'Auto Update Server' window of the NetBrain Integrated Edition - InstallShield Wizard. It features a blue header with the NetBrain logo. A note specifies that the listen address should be the IP address of the machine. There are input fields for 'Listen Address' (containing '10.10.3.141') and 'Listen Port' (containing '9099'). A checkbox for 'Use SSL between Auto Update Server and Client' is unchecked. Below these are fields for 'Certificate' and 'Private Key', each with a 'Browse...' button. At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons.

NetBrain Integrated Edition - InstallShield Wizard

Auto Update Server

Please specify the settings for the Auto Update Server. Note: The address should be the IP address of this machine.

Listen Address: 10.10.3.141

Listen Port: 9099

☐ Use SSL between Auto Update Server and Client

Certificate: [field] Browse...

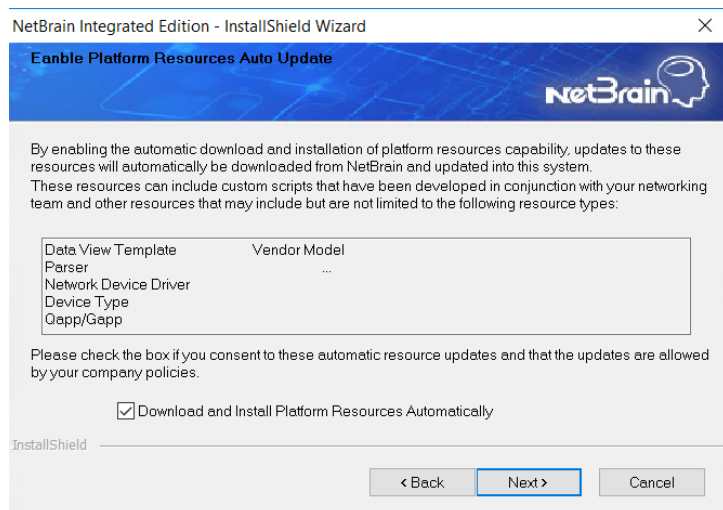
Private Key: [field] Browse...

< Back Next > Cancel

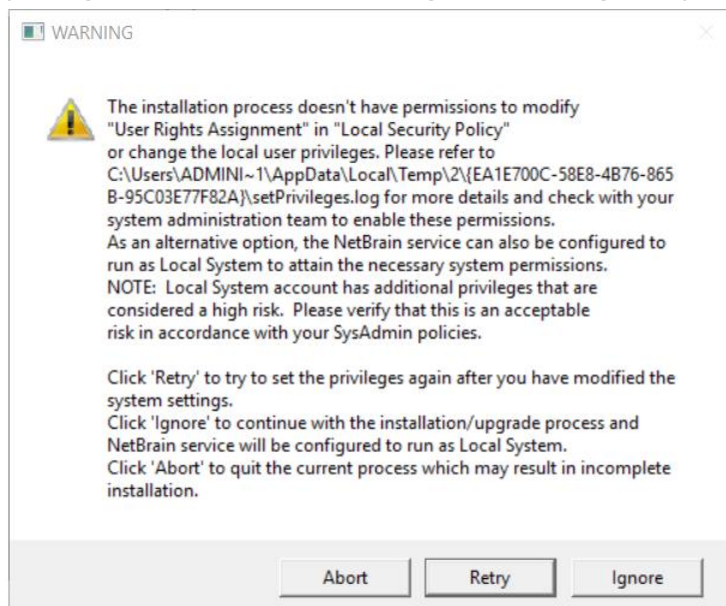
Note: The listen address is the address of Web API Server. It can only be the IP address of the machine.

Note: To enable the SSL between Auto Update Server and Client, select the Use SSL checkbox and upload the certificate file that contains the public key as well as the private key file in the respective fields below.

- 17) 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**.



- 18) Review the summary of the installation settings and click **Install**. The installation will take some time and it depends on the scale of your database.
- 19) (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 successfully upgrading the Web Server and Web API Server, click **Finish**.
6. Open the IIS Manager to check that the **Default Web Site** and **ServicesAPI** service exist.
7. Open the Task Manager to check that the **NetBrainKCProxy** service is running.

1.11. Upgrading Worker Server

Note: If you have deployed a Worker Server Cluster for load balancing, you can repeat the following steps to upgrade the Worker Servers on separate machines.

Note: Service Monitor Agent needs to be installed prior to installing Worker Server. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

Note: Make sure all cluster members have the same configurations for MongoDB, License Agent, Elasticsearch, RabbitMQ, and Redis. And your network configurations allow communications among them.

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.

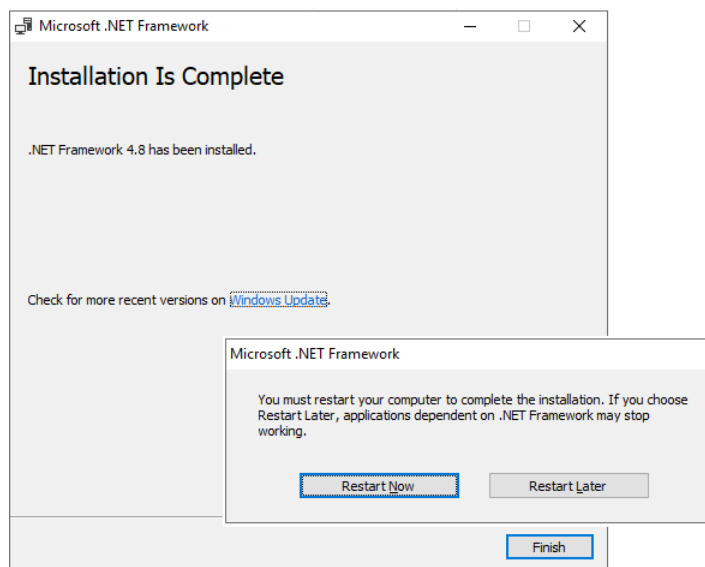
1. Download the **netbrain-ie-windows-x86_64-10.1.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to launch the Installation Wizard.
4. Follow the Installation Wizard to complete the upgrade 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** first.

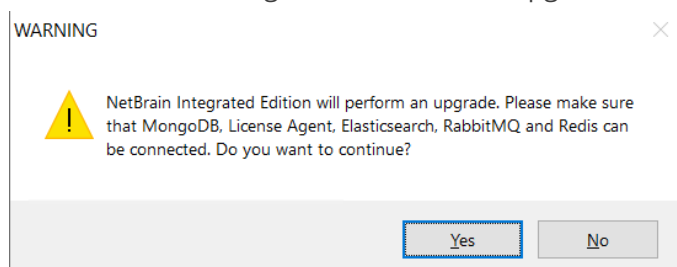
Note: Make sure the Windows update is of the latest. For Windows Server 2012, the update **KB2919442** and **KB2919355** must be installed before the .NET Framework 4.8 installation can start.

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.

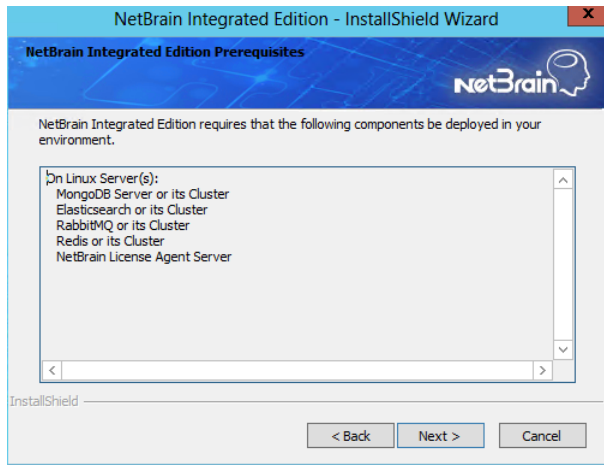


- 2) Stop the service of worker server manually before continuing the upgrade.
- 3) Click **Yes** in the dialog box to initiate the upgrade.

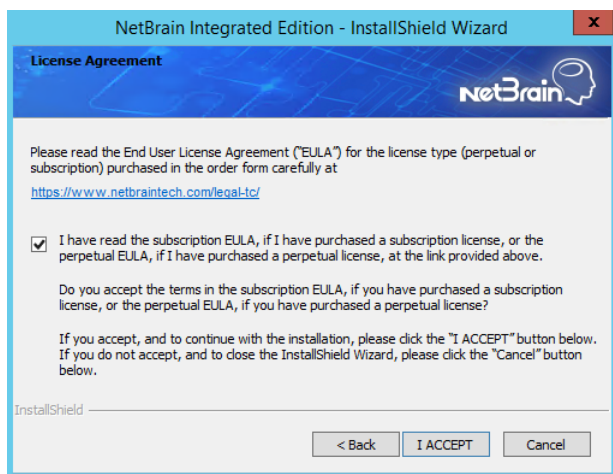


- 4) On the Welcome page, click **Next**.

- 5) On the NetBrain Integrated Edition Prerequisites page, read the components that must be set up in your environment beforehand 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 agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 8) On the Customer Information page, input your username and company name.

- 9) On the MongoDB Server Connection page, confirm the information and click **Next**.

The screenshot shows the 'MongoDB Server Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142:27017'.
- Format:** A label indicating the format is <Address>:<Port>, with an example '10.10.10.10:27017'.
- Input User Name and Password:** A checkbox that is unchecked.
- User Name:** A text box.
- Password:** A text box.
- Replica Set Name:** A text box containing 'rs'.
- Use SSL:** A checkbox that is unchecked.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 9) On the Elasticsearch Connection page, confirm the information and click **Next**.

The screenshot shows the 'Elasticsearch Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

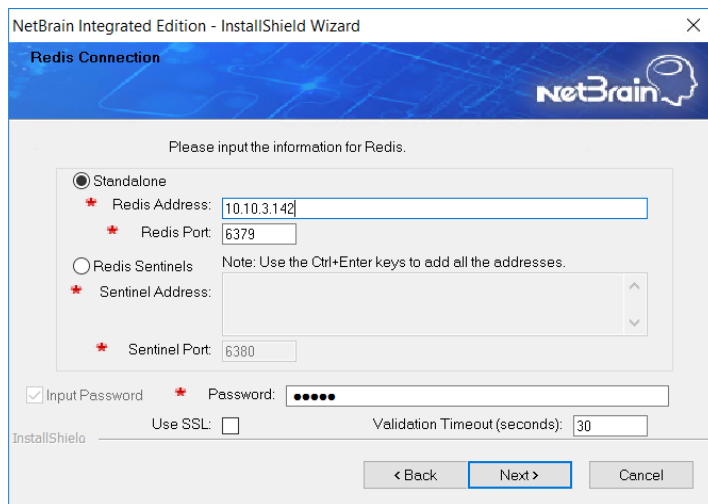
- Address:** A text box containing '10.10.3.142:9200'.
- Format:** A label indicating the format is <Address>:<Port>, with an example '10.10.10.10:9200'.
- Input User Name and Password:** A checkbox that is unchecked.
- User Name:** A text box.
- Password:** A text box.
- Use SSL:** A checkbox that is unchecked.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 10) On the RabbitMQ Connection page, enter the IP address, port, user name and password of RabbitMQ, and then click **Next**.

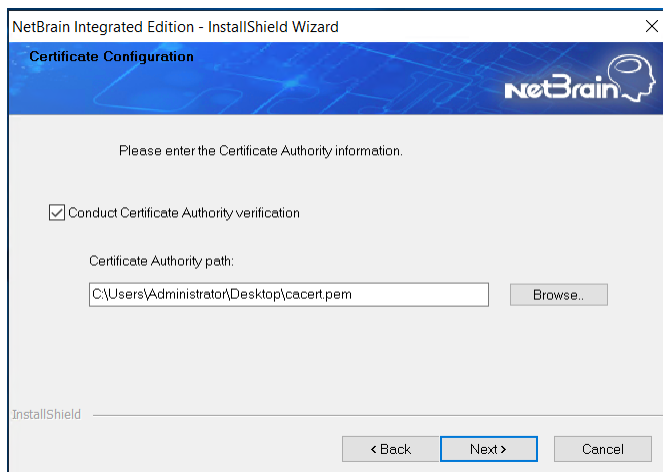
The screenshot shows the 'RabbitMQ Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142'.
- Format:** A label indicating the format is <Address>, with an example '10.10.10.10'.
- Input User Name and Password:** A checkbox that is checked.
- User Name:** A text box containing 'admin'.
- Password:** A text box with masked characters (dots).
- Port Number:** A text box containing '5672'.
- Use SSL:** A checkbox that is unchecked.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 11) On the Redis Connection page, enter the IP address, port, and admin password of the Redis, and then click **Next**.



- 12) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) On the Certificate Configuration page, confirm the Certificate Authority (CA) of the SSL certificates used on these servers, and then click **Next**.



To authenticate CA:

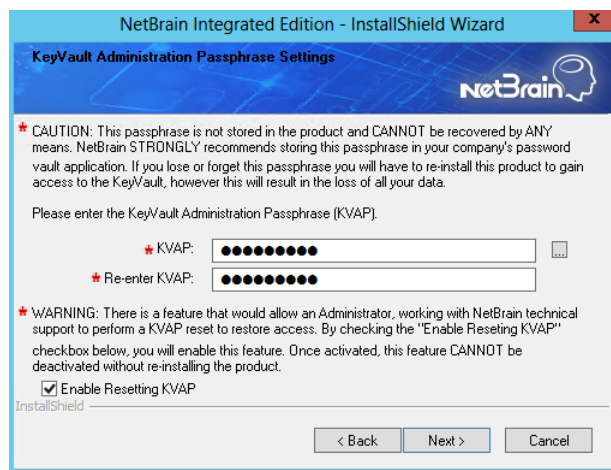
- Select the **Conduct Certificate Authority verification** check box.
- If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

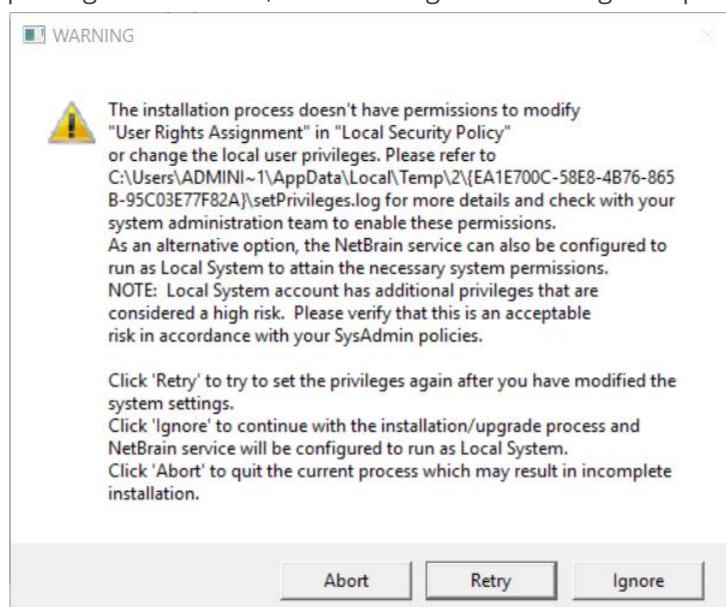
- 13) On the KeyVault Administration Passphrase Settings page, create a passphrase to initialize and manage the system KeyVault which contains all encryption keys to protect data security. Type it twice and click **Next**.



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, keep the **Enable Resetting KVAP** check box selected so that NetBrain system admin can reset the passphrase at any time.

- 14) Review the summary of the installation information and click **Install**.
- 15)(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 successfully upgrading the Worker Server on your machine, click **Finish**.
6. Open the Task Manager and navigate to the Services panel to check that the **NetBrainWorkerServer** service is running.
7. If you deployed a Worker Server Cluster for load balancing, repeat the above steps on other machines for an upgrade.

Note: Make sure all cluster members have the same configurations for MongoDB, License Agent, Elasticsearch, RabbitMQ, and Redis. And your network configurations allow communications among them.

1.12. Installing Task Engine

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

Note: Service Monitor Agent needs to be installed prior to installing Task Engine. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

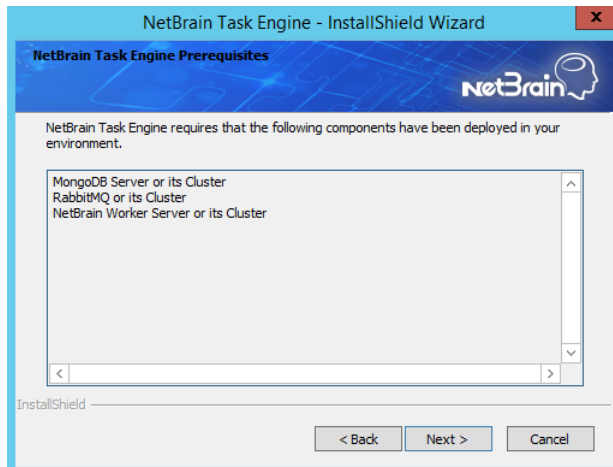
Depending on your network scale, you can deploy either a standalone Task Engine, or two for high availability.

Complete the following steps with administrative privileges.

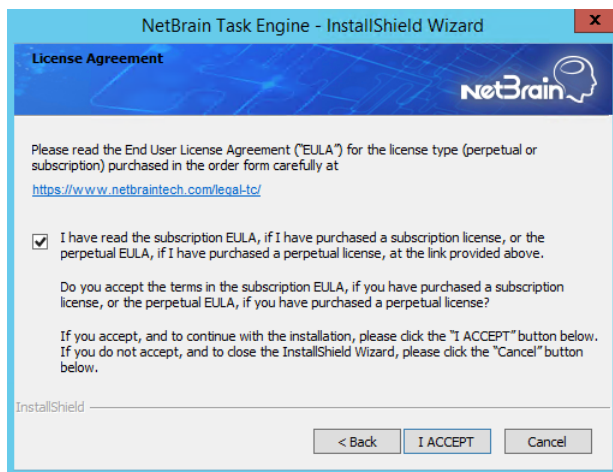
1. Download the **netbrain-taskengine-windows-x86_64-10.1.zip** file and save it in your local folder.

Note: Contact [NetBrain Support Team](#) to get the download link. The download link is case-sensitive.

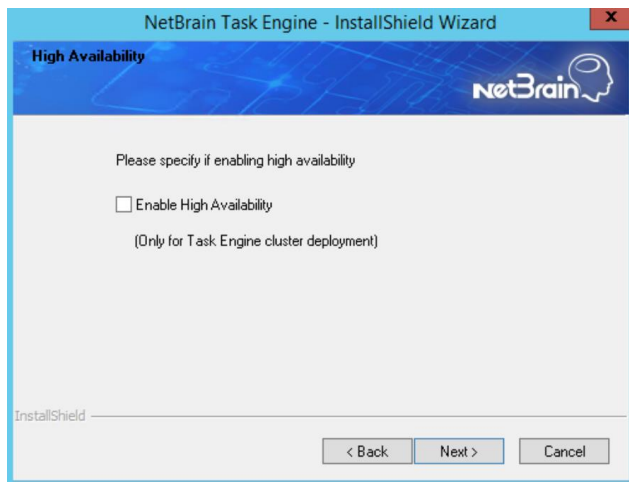
2. Extract installation files from the **netbrain-taskengine-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-taskengine-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) On the Welcome page, click **Next**.
 - 2) On the NetBrain Task Engine Prerequisites page, view the components that must be deployed beforehand in your environment and click **Next**.



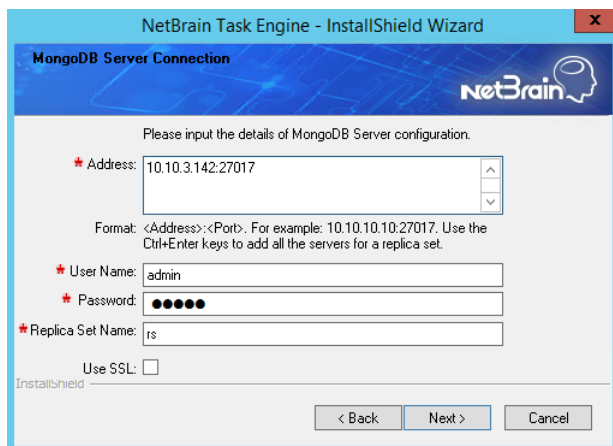
- 3) On the System Configuration page, review the system configuration summary and click **Next**.
- 4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA, ...** check box and then click **I ACCEPT**.



- 5) On the Customer Information page, input your username and company name, and then click **Next**.
- 6) On the Destination Location page, click **Next** to install the Task Engine under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.
- 7) On the High Availability page, leave the **Enable High Availability unchecked**, and then click **Next**.



- 8) On the MongoDB Server Connection page, enter the following information to connect to the MongoDB, and then click **Next**.



- **Address** — enter the IP address of MongoDB and the corresponding port number. By default, the port number is **27017**.

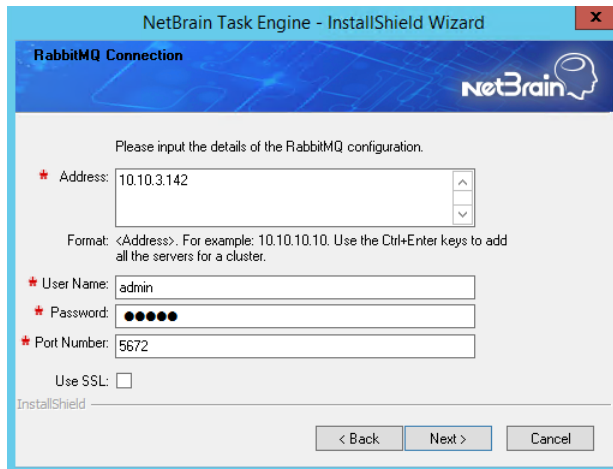
Tip: You can enter the fully qualified domain name (FQDN) of MongoDB if all NetBrain servers are managed in the same domain. For example, **test.netbraintech.com:27017**.

- **User Name** — enter the username that you created when installing MongoDB.
- **Password** — enter the password that you created when installing MongoDB.
- **Replica Set Name** — enter the replica set name of MongoDB. By default, it is **rs**.

Note: If you installed MongoDB by using MongoDB official installation package, you must also set up a replica set name. See the documentation <https://docs.mongodb.com/manual/tutorial/deploy-replica-set/> on MongoDB official website for reference.

- **Use SSL** — used to encrypt the connections to MongoDB with SSL. If SSL is enabled on MongoDB, select this check box; otherwise, leave it unchecked.

- 9) On the RabbitMQ Connection page, enter the following information to connect to RabbitMQ, and then click **Next**.

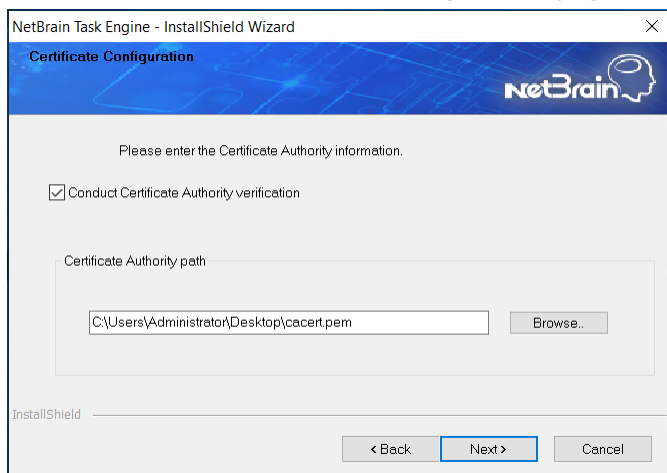


- **Address** — enter the IP address of RabbitMQ.

Tip: You can enter the FQDN of RabbitMQ if all NetBrain servers are managed in the same domain.

- **User Name** — enter the admin username that you created when installing RabbitMQ.
- **Password** — enter the admin password corresponding to the username that you created when installing RabbitMQ.
- **Port Number** — enter the port number used by RabbitMQ to communicate with Web API Server, Worker Server, and Task Engine. By default, it is **5672**.
- **Use SSL** — used to encrypt the connections to RabbitMQ with SSL. If SSL is enabled on RabbitMQ, select it; otherwise, leave it unchecked.

- 10) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB or RabbitMQ.) On the Certificate Configuration page, confirm the CA of SSL certificates, and then click **Next**.



To authenticate CA:

- a) Select the **Conduct Certificate Authority verification** check box.

- b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

11) Review the summary of the installation information and then click **Install**.

4. After successfully installing the Task Engine, click **Finish**.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainTaskEngine** service is running.

1.13. Installing Front Server Controller

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

Note: Service Monitor Agent needs to be installed prior to installing Front Server Controller. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

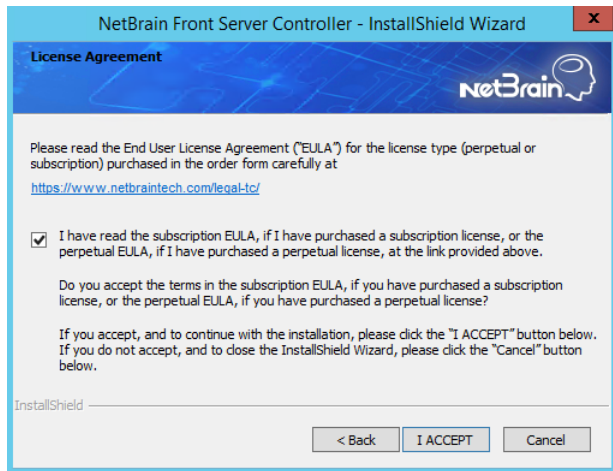
Complete the following steps with administrative privileges.

1. Download the **netbrain-frontservercontroller-windows-x86_64-10.1.zip** file and save it in your local folder.

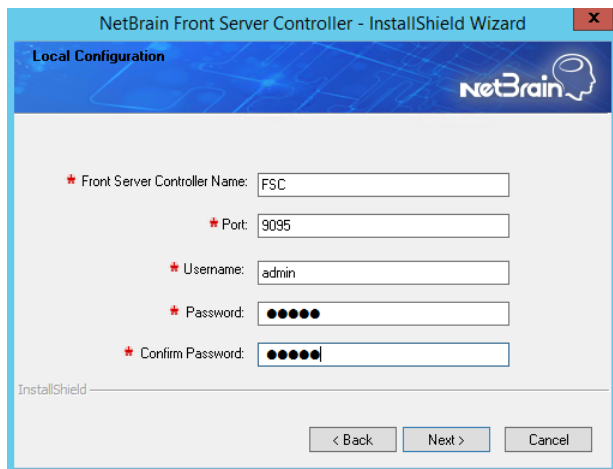
Note: Contact [NetBrain Support Team](#) to get the download link. The download link is case-sensitive.

2. Extract installation files from the **netbrain-frontservercontroller-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-frontservercontroller-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) On the Welcome page, click **Next**.
 - 2) On the System Configuration page, review the system configuration summary and click **Next**.

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



- 4) On the Customer Information page, input your username and company name, and then click **Next**.
- 5) On the Destination Location page, click **Next** to install the Front Server Controller under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.
- 6) On the Local Configuration page, configure the following information, and then click **Next**.



- **Front Server Controller Name** — create a name for the controller to authenticate the connections established from Worker Server.

Note: This field cannot contain any of the special characters: \ / : * ? " ' < > | . \$.

Note: Keep notes of **Front Server Controller Name** as well as **Port**, **Username**, and **Password** because they are required when you [allocate tenants to Front Server Controller](#) and [register a Front Server](#).

- **Port** — specify the port number used for the connections from Worker Server and Front Server. By default, it is **9095**.
- **Username** — create a username to authenticate the connections established from Worker Server.
- **Password** — create a password to authenticate the connections established from Worker Server.

- 7) (Required only if SSL has already been enabled) On the Local SSL Configuration page, confirm the certificate and private key for the Front Server Controller to establish encrypted connections with Worker Server and Front Server, and then click **Next**.

The screenshot shows the 'Local SSL Configuration' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Define SSL configuration to connect with Worker Server and Front Server.' There is a checkbox for 'Enable SSL' which is checked. Below this, there are two fields: 'Certificate' and 'Private Key', both with a red asterisk. The 'Certificate' field contains the path 'C:\Program Files\NetBrain\Front Server Controller\cc' and has a 'Browse...' button next to it. The 'Private Key' field also contains the same path and has a 'Browse...' button next to it. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 8) On the MongoDB Connection page, enter the following information to connect to MongoDB and then click **Next**.

The screenshot shows the 'MongoDB Configuration' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Please input the details of the MongoDB Server configuration.' There are four fields: 'Address' with a red asterisk, 'User name' with a red asterisk, 'Password' with a red asterisk, and 'Replica Set Name' with a red asterisk. The 'Address' field contains '10.10.3.142:27017' and has a dropdown arrow on the right. Below the 'Address' field, there is a note: 'Format: <Address>:<Port>. For example: 10.10.10.10:27017. Use the Ctrl+Enter keys to add all the servers for a replica set.' The 'User name' field contains 'admin'. The 'Password' field contains five dots. The 'Replica Set Name' field contains 'rs'. There is a checkbox for 'Use SSL' which is unchecked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- **Address** — enter the IP address of MongoDB and the corresponding port number. By default, the port number is **27017**.

Tip: You can enter the fully qualified domain name (FQDN) of MongoDB if all NetBrain servers are managed in the same domain. For example, **test.netbraintech.com:27017**.

- **User Name** — enter the username that you created when installing MongoDB.
- **Password** — enter the password that you created when installing MongoDB.
- **Replica Set Name** — enter the replica set name of MongoDB. By default, it is **rs**.
- **Use SSL** — used to encrypt the connections to MongoDB with SSL. If SSL is enabled on MongoDB, select this check box; otherwise, leave it unchecked.

- 9) On the RabbitMQ Connection page, enter the following information to connect RabbitMQ, and then click **Next**.

NetBrain Front Server Controller - InstallShield Wizard

RabbitMQ Connection

Please input the details of the RabbitMQ configuration.

* Address: 10.10.3.142

Format: <Address>. For example: 10.10.10.10. Use the Ctrl+Enter keys to add all the servers for a cluster.

* User name: admin

* Password: ●●●●●●

* Port Number: 5672

Use SSL: ☐

InstallShield

< Back Next > Cancel

- **Address** — enter the IP address of RabbitMQ.

Tip: You can enter the FQDN of RabbitMQ if all NetBrain servers are managed in the same domain.

- **User Name** — enter the admin username that you created when installing RabbitMQ.
- **Password** — enter the admin password corresponding to the username that you created when installing RabbitMQ.
- **Port Number** — enter the port number used by RabbitMQ to communicate with Web API Server, Worker Server, and Task Engine. By default, it is **5672**.
- **Use SSL** — used to encrypt the connections to RabbitMQ with SSL. If SSL is enabled on RabbitMQ, select it; otherwise, leave it unchecked.

- 10) On the Redis Connection page, enter the following information to connect to Redis, and then click **Next**.

NetBrain Front Server Controller - InstallShield Wizard

Redis Connection

Please input the information for Redis.

☒ Standalone

Redis Address: 10.10.3.142

Redis Port: 6379

☐ Redis Sentinels Note: Use the Ctrl+Enter keys to add all the addresses.

Sentinel Address:

Sentinel Port: 6380

Password:

Use SSL: ☐ Validation Timeout (seconds): 30

InstallShield

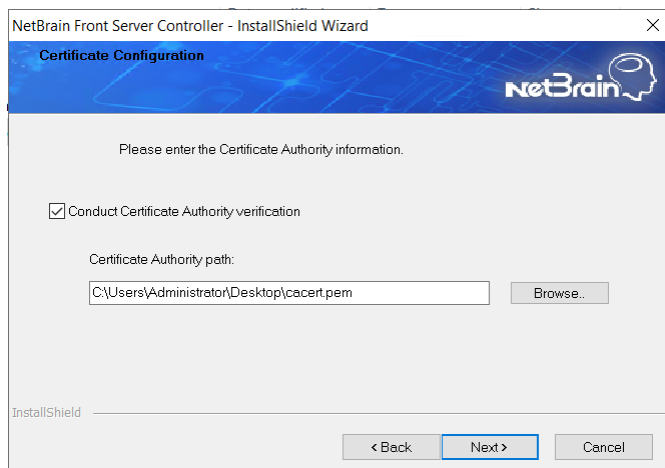
< Back Next > Cancel

- **Redis Address** — enter the IP address of Redis.

Tip: You can enter the FQDN of Redis if all NetBrain servers are managed in the same domain.

- **Password** — enter the admin password that you created when installing Redis.
- **Use SSL** — used to encrypt the connections to Redis with SSL. If SSL is enabled on Redis, select it; otherwise, leave it unchecked.
- **Redis Port** — enter the port number used by Redis to communicate with Web API Server, Worker Server, and Front Server Controller. By default, it is **6379**.
- **Redis Sentinels** — required only if you set up a Redis Cluster. Leave it unchecked.

11) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, RabbitMQ, or Redis). On the Certificate Configuration page, confirm the CA of SSL certificates on these servers, and then click **Next**.



To authenticate CA:

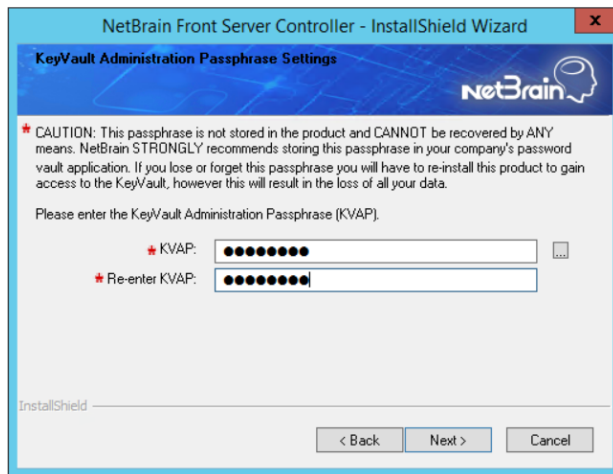
- a) Select the **Conduct Certificate Authority verification** check box.
- b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

12) On the KeyVault Administration Passphrase Settings page, enter the passphrase that you created when installing Web API Server twice and click **Next**.



- 13) Review the summary of the installation information and click **Install**.
4. After successfully installing the Front Server Controller, click **Finish**.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainFrontServerController** service is running.

1.14. Upgrading Front Server

Complete the following steps to upgrade Front Server:

1. [Installing Front Server](#)
2. [Uninstalling Proxy Server](#)

1.14.1. Installing Front Server

Each Front Server is recommended to manage 5,000 network nodes at most. Depending on your network scale, you can deploy either a standalone Front Server, or multiple Front Servers for load balancing.

Note: Ports 7778, 7086, and 29916 must be open for communications.

Select either of the following ways to install the Front Server, depending on your operating system:

- [Installing Front Server on Linux](#)
- [Installing Front Server on Windows](#)

1.14.1.1. Installing Front Server on Linux

Pre-Installation Task

Service Monitor Agent will be installed with Front Server and it 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 it has 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 [Offline Installing Third-party Dependencies](#) for more details.

Note: You can also [install the Service Monitor Agent](#) separately.

- Front Server has dependencies on several third-party packages. Before you install the Front Server, run the `rpm -qa|grep -E "glibc|libstdc++|libuuid|pam"` command to check whether these dependencies have been installed. If they have not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum install -y glibc libstdc++ libuuid pam` command to install these third-party packages online.
 - **Offline Install:** refer to [Offline Installing Third-party Dependencies](#) for more details.

Installing Front Server on Linux

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 Front Server installation package. For example, **netbraintemp10.1**.
3. Run the `cd /opt/netbraintemp10.1` command to navigate to the **/opt/netbraintemp10.1** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-frontserver-linux-x86_64-rhel-10.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.1** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.1** directory to directly download the **netbrain-frontserver-linux-x86_64-rhel-10.1.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf netbrain-frontserver-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-frontserver-linux-x86_64-rhel-10.1.tar.gz
FrontServer/
FrontServer/config/

FrontServer/install.sh
...
```

6. Run the `cd FrontServer/config` command to navigate to the **config** directory.
7. Modify the value of DataPath (based on your environment) in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, refer to [Editing a File with VI Editor](#).

```
[root@localhost config]# vi setup.conf
#DataPath is used to store data and log files for Front server. This directory must be at least
a second level directory and used exclusively for this purpose.
DataPath=/usr/lib/netbrain/frontserver
#The PostgreSQL port must be between 1025 and 32767.
Port=5432
#Password should not contain: {}[]:","|<>@&^%\ or a space.

This password is used by front server to connect to PostgreSQL.
Password=Admin1.#
# To disable the Service Monitor Agent installation, set the 'DisableSM=1'
# The default value of 'DisableSM' is 0 which means Service Monitor Agent
# will be installed with FrontServer if it has not yet been installed.
DisableSM=0
```

8. Run the `cd ..` command to navigate to the **FrontServer** directory and run the `./install.sh` script under the **FrontServer** directory to install the Front Server.

- 1) Read the License Agreement, and type **YES**.
- 2) Type **I ACCEPT** to accept the License Agreement. The script starts to install the Front Server.

```
[root@localhost FrontServer]# ./install.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 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: Starting to check Linux OS info...
INFO: Starting to check required CPU...
INFO: Starting to check minimum memory...
...
INFO: Creating application databases and update PostgreSQL user SUCCEEDED
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed Front Server.
```

Note: The Front Server service will not be automatically started until it is successfully registered. You cannot [register a Front Server](#) immediately until [adding the Front Server to a Tenant](#).

Note: Disk space check will be performed to ensure the requirement of minimum 180G free disk space is met.

Note: If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See [Upgrading MongoDB](#) for more details.

9. To install more Front Servers for load balancing, repeat the above installation steps on separate machines.
10. Run the `systemctl status netbrainfrontserver` command to check the service status of each node.

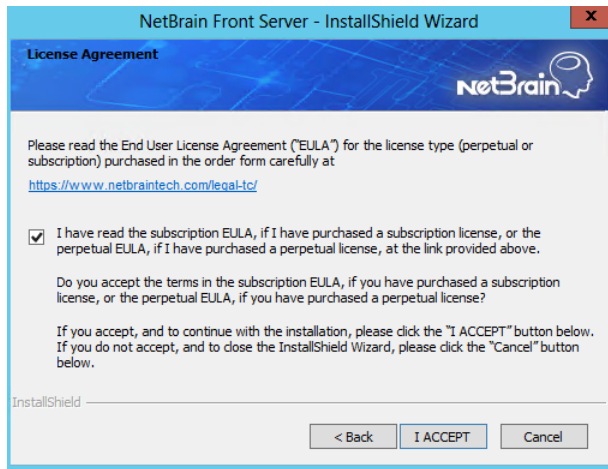
1.14.1.2. Installing Front Server on Windows

Note: Service Monitor Agent needs to be installed prior to installing Front Server. Refer to [Installing Service Monitor Agent on Windows](#) for more detailed steps.

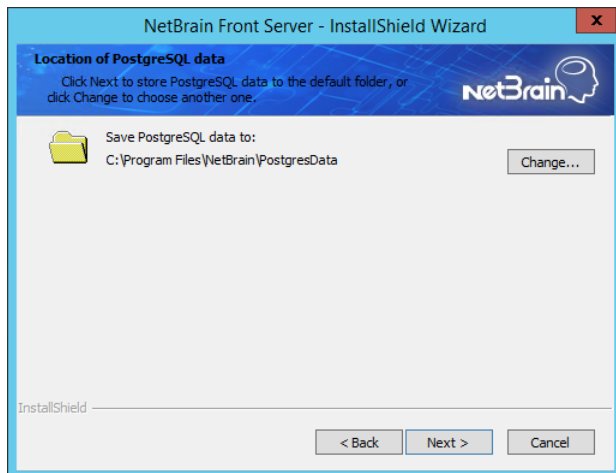
Complete the following steps with administrative privileges.

1. Download the **netbrain-frontserver-windows-x86_64-10.1.zip** file by using the download link provided in the email and save it in your local folder.
2. Extract installation files from the **netbrain-frontserver-windows-x86_64-10.1.zip** file.
3. Right-click the **netbrain-frontserver-windows-x86_64-10.1.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) On the Welcome page, click **Next**.
 - 2) On the System Configuration page, review the system configuration summary and click **Next**.

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

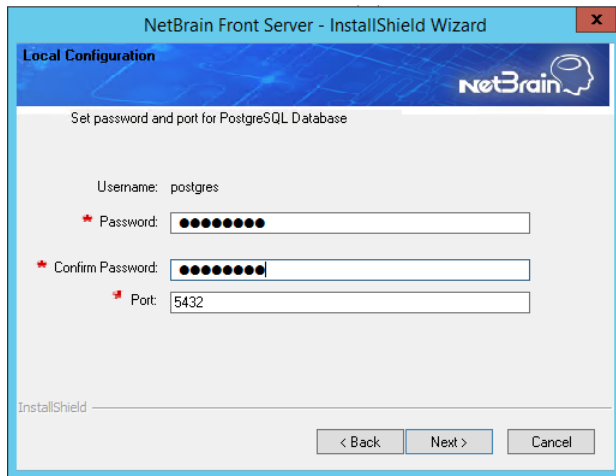


- 4) On the Customer Information page, enter your company name, and then click **Next**.
- 5) On the Destination Location page, click **Next** to install the Front Server under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.
- 6) On the Location of PostgreSQL data page, click Next to store the PostgreSQL data to the default directory **C:\Program Files\NetBrain\PostgresData**. If you want to restore it under another location, click **Change**.



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

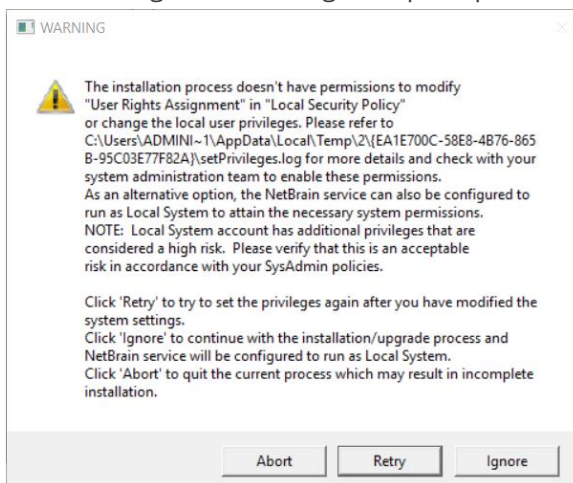
7) On the Local Configuration page, set password and port for PostgreSQL database.



The image shows a screenshot of the 'NetBrain Front Server - InstallShield Wizard' window, specifically the 'Local Configuration' tab. The window has a blue header with the NetBrain logo. Below the header, the text 'Set password and port for PostgreSQL Database' is displayed. There are four input fields: 'Username' with the value 'postgres', 'Password' (masked with dots), 'Confirm Password' (masked with dots), and 'Port' with the value '5432'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8) Review the summary of the current installation settings and click **Install**.

- 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.


4. After the Front Server is successfully installed, click **Finish** to complete the installation process and exit the Installation Wizard. Close the pop-up registration program.

Note: The Front Server service will not be automatically started until the Front Server is added to a tenant and successfully registered. See [Adding a Front Server to a Tenant](#) and [Registering the Front Server](#) for more details.

5. To install more Front Servers for load balancing, repeat the above installation steps on separate machines.

1.14.2. 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.

1.15. Unbinding Perpetual License

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Web Server>/admin.html** to log in to the System Management page.

Note: In order to minimize the issue caused by insufficient privilege, it's strongly recommended to use the local "admin" account to log in to the System Management page.

2. Click **OK** on a pop-up notification dialog.
3. Click **Unbind**.

4. Validate your perpetual license information and unbind it from NetBrain License Server.

- 1) Select **Online** and click **Next**.
- 2) Enter your license password and click **Unbind**.
- 3) Click **Yes** on a notification dialog box.

Note: If your NetBrain Web/Web API Server is not allowed to access the Internet, you can unbind the license from your local machine first, and then send the unbind file to [NetBrain Support Team](#).


- 1) Select **Via Email** and click **Next**.
- 2) Enter your email address and click **Unbind**. The **netbrain.Unbind** file will be generated and downloaded to your local disk.
- 3) Send an email to [NetBrain Support Team](#) with the file attached. NetBrain support team will help remove your license information from NetBrain License Server.

1.16. 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.

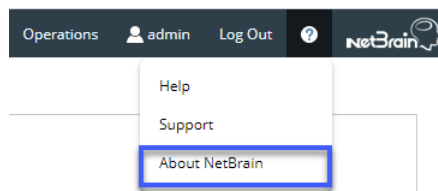
To browse the license information, navigate to **License > Current License Term**. See [License Information](#) for more details.

1.17. 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.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

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.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

- 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("2022-02-09T01:05:18.018Z") } } }
```

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

Note: System Update feature heavily relies on all the NetBrain servers and service metrics, therefore it is required to ensure all the NetBrain servers and component metrics can be viewed in the Service Monitor page.

1.18. 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.

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**.

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

- 3) Click **Test** to verify whether the Web API 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							

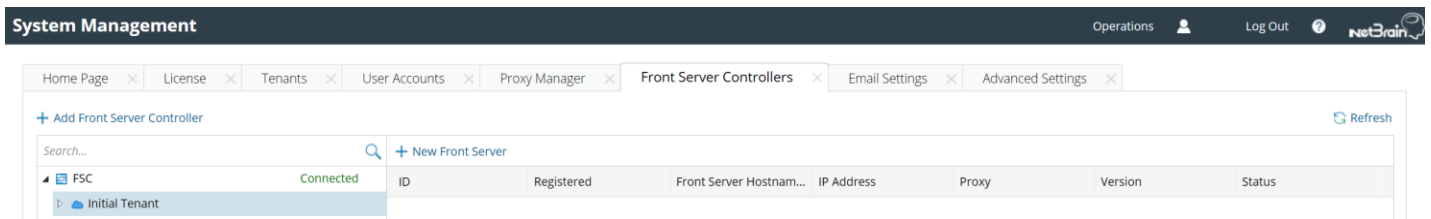
Front Server Controller Settings

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

Field	Description
Name	The name of the Front Server Controller created when you install the Front Server Controller.
Hostname or IP Address	Enter the IP address of Front Server Controller.
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 when you install the Front Server Controller to authenticate the connections from Worker Server.
Password	The password created on the NetBrain Front Server Controller page when installing the Front Server Controller.
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.

1.19. Adding a Front Server for a Tenant

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



2. Enter the following properties of the Front Server.

Add 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:

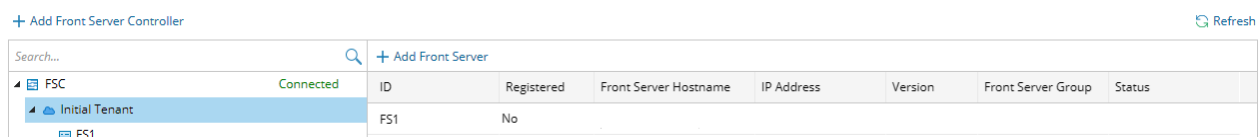
Proxy:

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

- **Front Server ID** — create an ID for identifying the Front Server.
- **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](#).

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



1.20. Registering a Front Server


Select either of the following ways to register the Front Server, depending on the operating system of your machine:

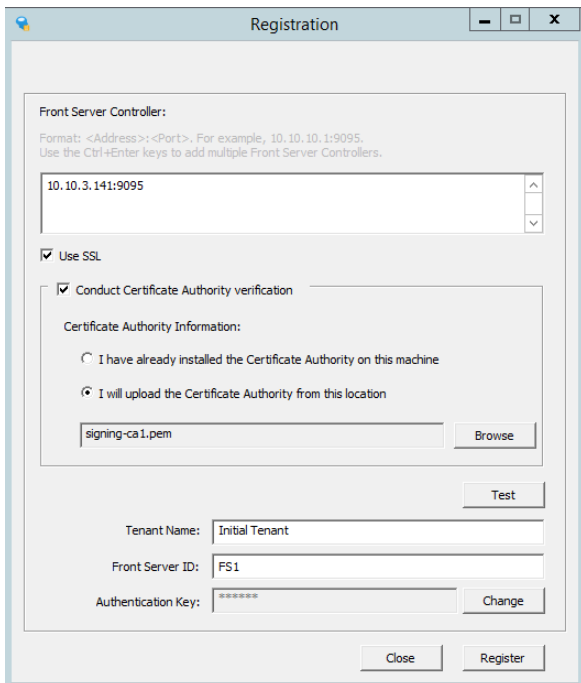
- [Registering Front Server on Windows](#)
- [Registering Front Server on Linux](#)

Registering a Front Server on Windows

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 Windows 'Registration' dialog box. It contains the following fields and options:

- Front Server Controller:** A text box with '10.10.3.141:9095' entered. Above it is a format hint: 'Format: <Address>:<Port>. For example, 10.10.10.1:9095. Use the Ctrl+Enter keys to add multiple Front Server Controllers.'
- ☒ **Use SSL**
- ☒ **Conduct Certificate Authority verification**
- Certificate Authority Information:**
 - ☐ I have already installed the Certificate Authority on this machine
 - ☒ I will upload the Certificate Authority from this location
 - A text box with 'signing-ca1.pem' and a 'Browse' button.
- A 'Test' button.
- Tenant Name:** A text box with 'Initial Tenant'.
- Front Server ID:** A text box with 'FS1'.
- Authentication Key:** A text box with '*****' and a 'Change' button.
- 'Close' and 'Register' buttons at the bottom.

- 1) Enter the following information about the Front Server Controller.
 - **Hostname or IP address** — the IP address or FQDN of Front Server Controller 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.

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

+ Add Front Server Controller Refresh

Search...

FSC

Initial Tenant

FS1

Connected

Connected

Connected

ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status
FS1	YES	WIN-M2CQ6EJO685	10.10.3.141	8.0		Connected

Legend: FSC Front Server Controller Front Server Controller Group Initial Tenant Tenant FS1 Front Server (Registered) Front Server (Unregistered)

Registering a Front Server on Linux

1. On the machine where the Front Server is installed, run the `cd /usr/lib/netbrain/frontserver/conf` command to navigate to the **conf** directory.
2. Modify the following [parameters](#) in the **register_frontserver.conf** file located under the **conf** directory and save the changes. For how to modify the configuration file, see [Appendix: Editing a File with VI Editor](#) for more details.

```
[root@localhost conf]# vi register_frontserver.conf
# Enter <hostname or IP address>:<port> of the Front Server Controller. For example,
```

```
192.168.1.1:9095
# Use a semicolon to separate multiple Front Server Controllers.
Front Server Controller =10.10.3.141:9095

# Define the SSL settings. "no" indicates disable; "yes" indicates enable
Enable SSL = Yes

# If "Conduct SSL certificate authority" is enabled, please enter the full path of the
certificate file
Conduct SSL Certificate Authority = Yes
SSL Certificate Path = /root/test.pem

# Define the front server that got registered
Tenant Name =Initial Tenant
Front Server ID =FS1
```

3. Run the `cd ../bin` command to navigate to the **bin** directory.
4. Run the `./registration` command under the **bin** directory, and input the Authentication Key and press the **Enter** key.

```
[root@localhost bin]# ./registration
Loading configuration files...
Authentication Key:
Stopping Front Server Service...
Registering Front Server...
Successfully registered to the tenant "Initial Tenant".
10.10.3.141: active.

Succeeded to start up front server service.
```

5. Run the `service netbrainfrontserver status` command to verify whether the service of the Front Server starts successfully.

```
[root@localhost FrontServer]# service netbrainfrontserver status
Redirecting to /bin/systemctl status netbrainfrontserver.service
netbrainfrontserver.service - netbrain front server daemon
Loaded: loaded (/usr/lib/systemd/system/netbrainfrontserver.service)
Active: active (running)
```

Parameters

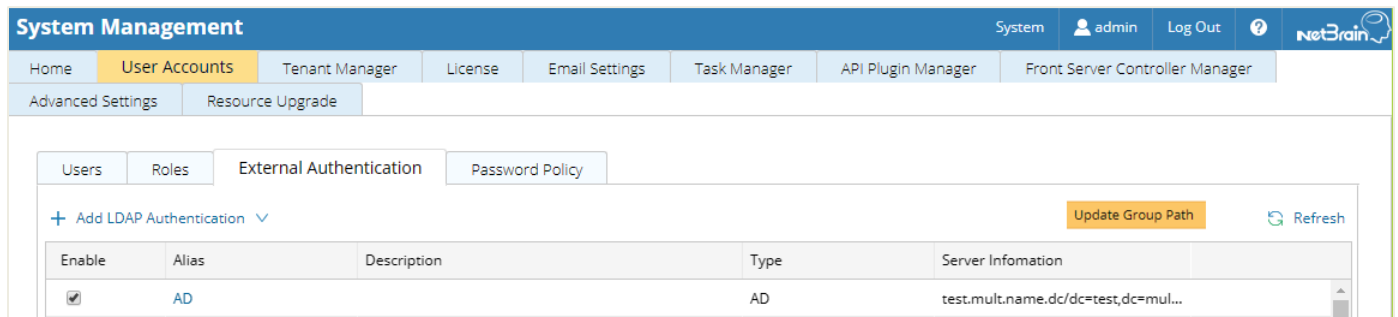
Parameter	Default Value	Description
Front Server Controller		<p>The hostname, IP address, or FQDN of the Front Server Controller and the port number.</p> <p>If you want to register a Front Server Controller group, use a semicolon to separate multiple Front Server Controllers.</p>

Parameter	Default Value	Description
Enable SSL	No	Set whether to encrypt the connections to Front Server Controller with SSL. If SSL is enabled on the Front Server Controller, type Yes ; otherwise, leave the default value as it is. Note: Type Yes only if you enabled SSL on MongoDB.
Conduct SSL Certificate Authority	No	Set whether to authenticate the Certificate Authority (CA) of SSL certificates on the Front Server Controller. If you want to authenticate the Certificate Authority, type Yes .
SSL Certificate Path		The full storage path and certificate name. Note: Only the certificate in the Base-64 encoded X.509 PEM format is supported. Note: Please ensure that the user netbrain can access the certificate file.
Tenant Name	Initial Tenant	The name of the tenant that this Front Server will serve.
Front Server ID	FS1	The ID created when you add this Front Server to a tenant.
Authentication Key		The authentication key created when you add this Front Server to a tenant.

1.21. Upgrading External Authentication

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

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



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

1.22. Upgrading Email Settings

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

The screenshot shows the 'System Management' interface with the 'Email Settings' tab selected. The 'Email Server Settings' sub-tab is active. The page contains the following fields and controls:

- Enable Email Server Settings:** A checked checkbox with a 'Fetch Last Setting' link to its right.
- SMTP Server:** A text input field containing '10.10.10.8'.
- SMTP Port:** A text input field containing '587'.
- Encryption:** A dropdown menu currently set to 'No'.
- Sender Email Address:** A text input field containing 'qaauto@netbrain.com'.
- Password:** A text input field showing masked characters '*****' with '(New Password)' text.
- Sender Email Frequency:** A text input field containing '5' with 'Minutes' and a help icon to its right.
- Email Signature:** A rich text editor with a toolbar (Normal, Bold, Italic, Underline, Link, Unlink, Bulleted List, Numbered List, Indent, Outdent, Undo, Redo) and a text area containing 'Please type here...'.
- Buttons:** 'Test' and 'Save' buttons at the bottom.
- Footer:** 'Activate Windows Go to Settings to activate Windows.' watermark.

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

1.23. 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.

1. [Check the Latest Version](#)
2. [Download Package from NetBrain Customer Portal](#)
3. [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.

System Management

License

Tenants

Proxy Manager

Front Server Controllers

Advanced Settings

System Update

Current Version: 10.1.0.0

☒ Automatically check the latest version
 Last checked on: 2/18/2022, 12:56:52 PM

Check Update Now

☒ Download and Install Platform Resources Automatically

Latest Available Version: N/A

Get Latest Version

Upload Latest Version

Schedule

[View Update History](#)

To Upgrade the system and resource, do as follows:

1. Click the **Check Update Now** button to see whether there is a new software or resource version available if your system is connected to the Internet. Ignore this step if your system is offline.
2. Click the **Get Latest Version** button to log in **NetBrain Customer Success Center** and download the software package. The package is created just for this system and cannot be used by other systems.
3. Click the **Upload Latest Version** button and upload the file downloaded at step 2.
4. Click the **Schedule** button to schedule the system update.

Note: If you need to cancel the system update after uploading the latest version, simply click the **Discard Uploaded Version** to cancel the update.

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,,]

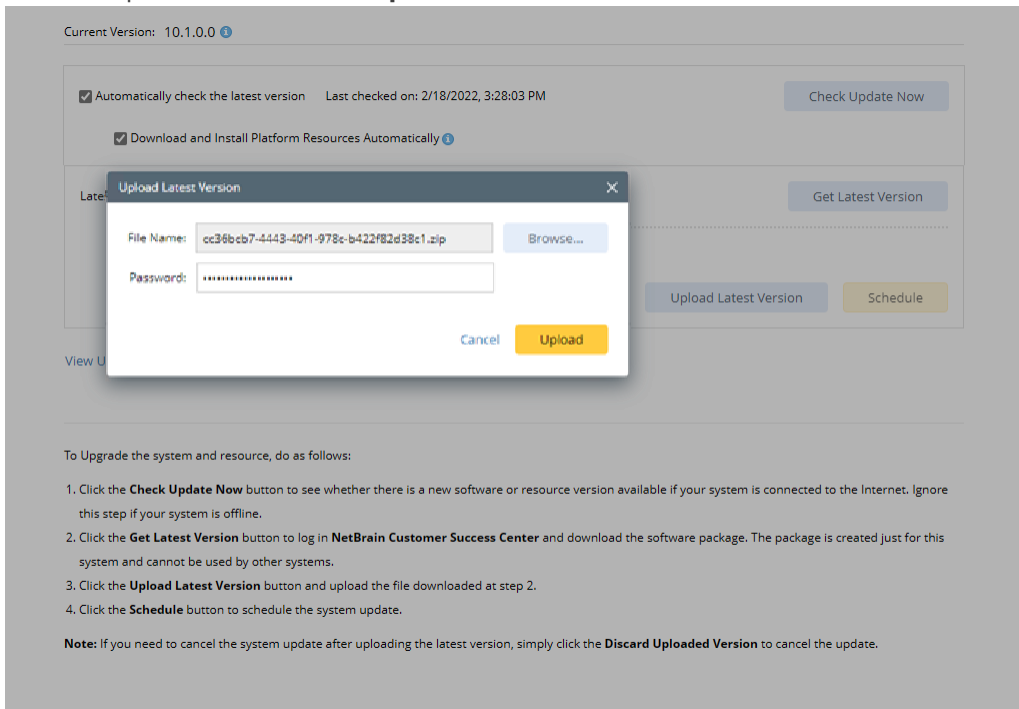
[Resource Package Link](#) Password: **mQyKB0bZPOKzpHEleCcK**

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**.

License Agreement

×

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

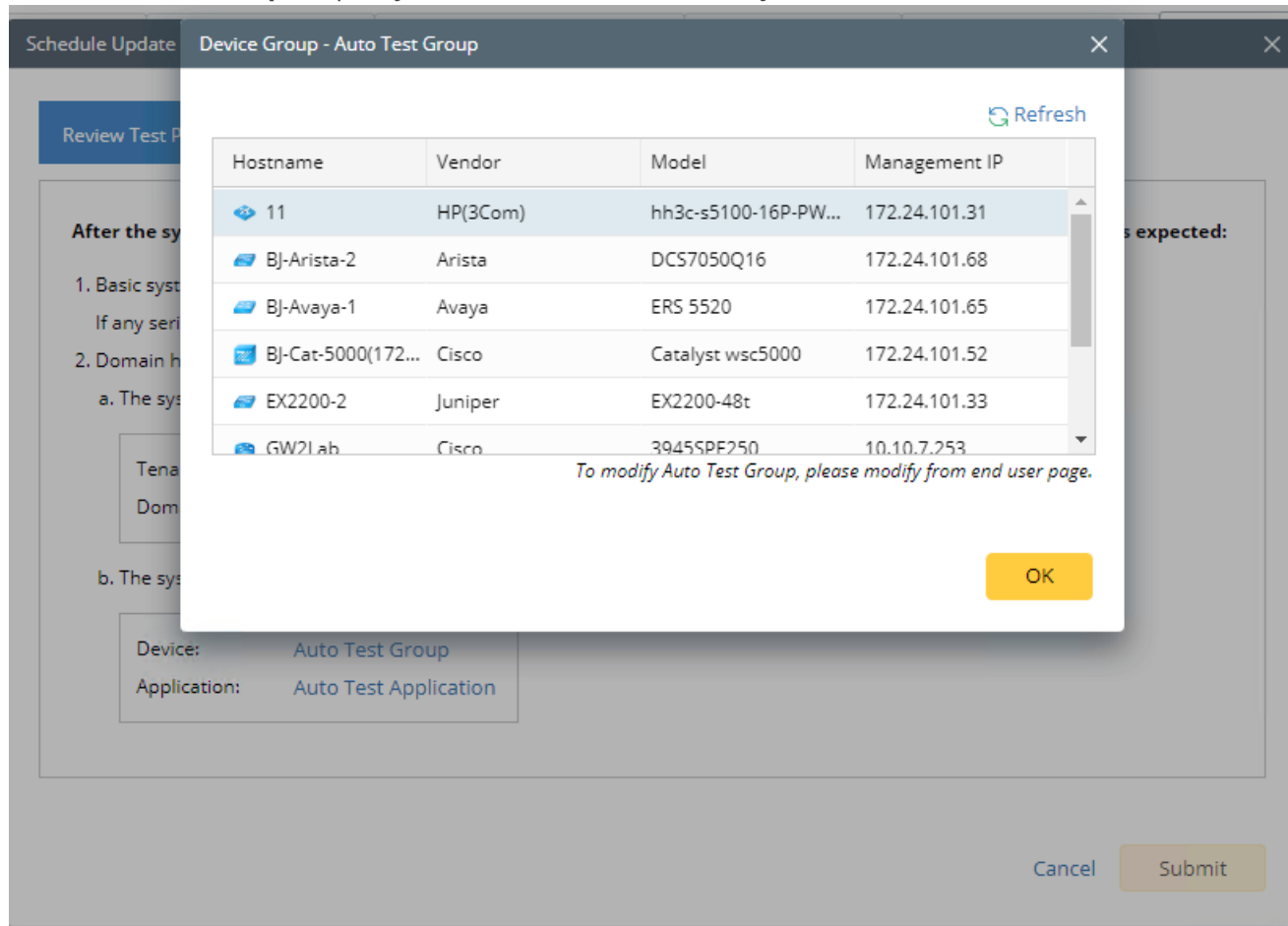
Cancel Submit

- 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).

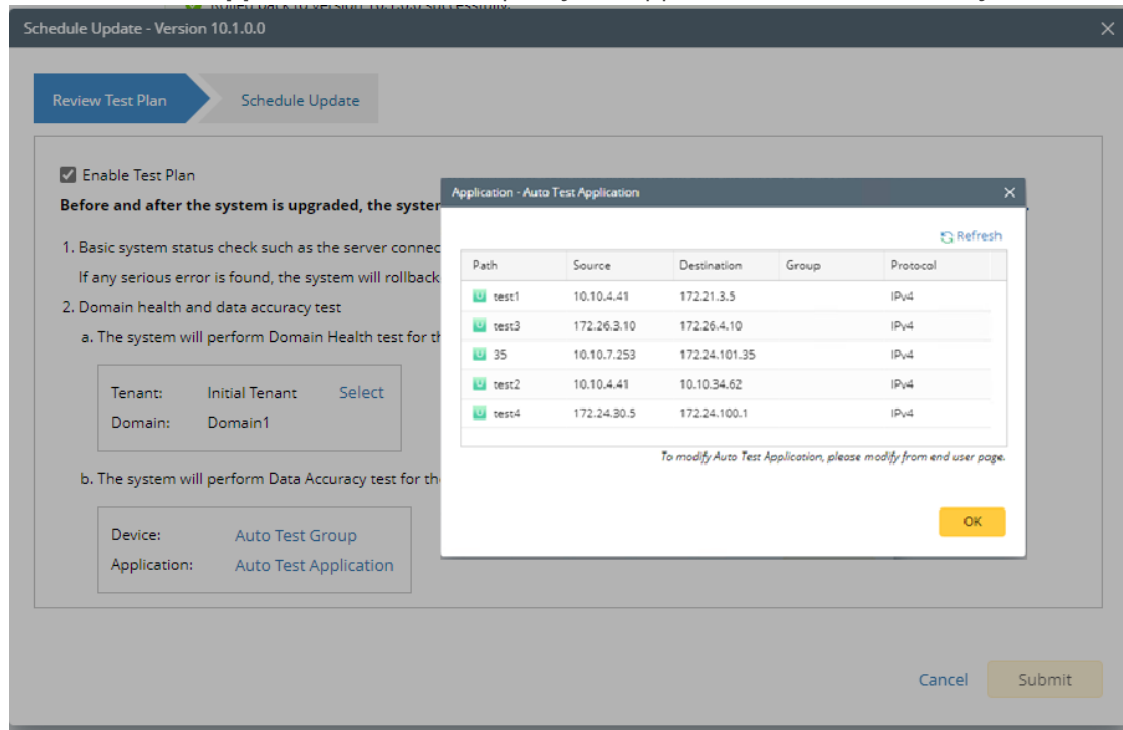
Note: If there is only one tenant and domain, the Initial Tenant will be automatically selected and you can directly proceed to step 2).

- 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.

Update History								
Upgrade From	Upgrade To	Updated Time	Executor	Action	Status	Release Note	Installation Log	Test Report
10.1.0.0 	10.1.0.0 	Mar 16, 2022, 11:32:11 PM	admin	Upgrade	Succeeded	Release Note	Installation Log	Test Results

1.24. Customizing MongoDB Disk Alert Rules

To proactively prevent the system database from data loss or even corruption, you can customize MongoDB, Front Server, and Elasticsearch disk alert rules with progressive quotas assigned. When the usage reaches the predefined threshold, specified users can be notified by both email alerts and system alerts.

1. In the System Management page, click the start menu > **Service Monitor**.

2. In the Service Monitor home page, click **Alert Rules** at the upper-right corner. The default settings are as follows.

Alert Rules

MongoDB:

- ☒ 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.

Front Server:

- ☒ When Front Server disk usage reaches % or only GB free space, send emails.

Elasticsearch:

- ☒ When Elasticsearch disk usage reaches % or only GB free space, send emails.

Server/Service:

- ☒ When a server is disconnected or a service is stopped, send email

Send Email Settings:

Send Email To : Cc :

Send Email Frequency : Hours

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

3. Change the settings based on your needs.
 - 1) Specify the disk usage threshold for different levels.

Note: To email alerts when a server is disconnected or a service is stopped, select the corresponding check box.

- 2) Enter the email address in the **Send Email To** or **CC** fields.


Note: Email alerts are enabled only when email addresses are added at least in one field. Use a colon or semicolon to separate multiple items.

- 3) Specify the frequency to send emails.
- 4) Click **OK** to save the configuration.


1.25. Tuning Live Access

To tune live access, complete the following steps:

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Web Server>/** to log in to your 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**.

1.26. Scheduling Benchmark Task

1. In the Domain Management page, click the  start menu > **Schedule Task**.
2. On the **Schedule Task > Schedule Discovery/Benchmark** tab, select the **Enable** check box for the **Basic System Benchmark** entry.

Note: A full benchmark must be performed by enabling the **L2 Topology** option under the **Build Topology** section of the **Additional Operation After Benchmark** tab.

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 10.1** 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.
```

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: 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.

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. If you have set up a MongoDB replica set for high availability, you only need to dump data from the primary node.

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 following command in one line and run it to dump the MongoDB data to the **/etc/mongodb_databk** directory.
 - For IEv7.x, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip -out <filepath>` command.
 - For IEv8.0, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --authenticationMechanism SCRAM-SHA-256 --gzip -out <filepath>` command.

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: Interactive Pre-Installation of Service Monitor Agent

Service Monitor Agent will be pre-installed with MongoDB, Elasticsearch, License Agent, Redis, RabbitMQ and Front Server if it was not previously installed.

In such scenario, you'll be prompted to configure the following parameters before the installation or upgrade of the above components takes place:

```
INFO: Starting to check configuration parameters...
Configuring Service Monitor Agent ...
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 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/
Please enter the API Key to be used to communicate with application server which must be the same
as the one created on Web API server:
Please re-enter API key to confirm:
Please enter a log path for NetBrain Service Monitor Agent
[/var/log/netbrain/nbagent]: /log/nbagent
NetBrain Web API service URL: http://10.10.3.141/ServicesAPI
API key: *****
NetBrain Service Monitor Agent LogPath: /log/nbagent
Certificate Authority verification: no
Do you want to continue using these parameters? [yes]
...
```

Note: The log path for Service Monitor Agent must have at least 10G free space.

Note: If **https://** is used in the Web API Service URL, you will be asked whether to enable the Certificate Authority verification and input the Certificate Authority file if enabled.

8. Appendix: Generating SSL Certificate

1. Run PowerShell as an administrator.

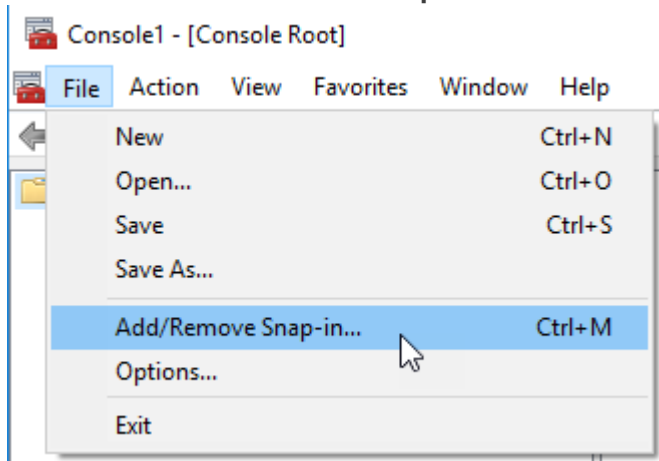
2. Run the following command to create the certificate:

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

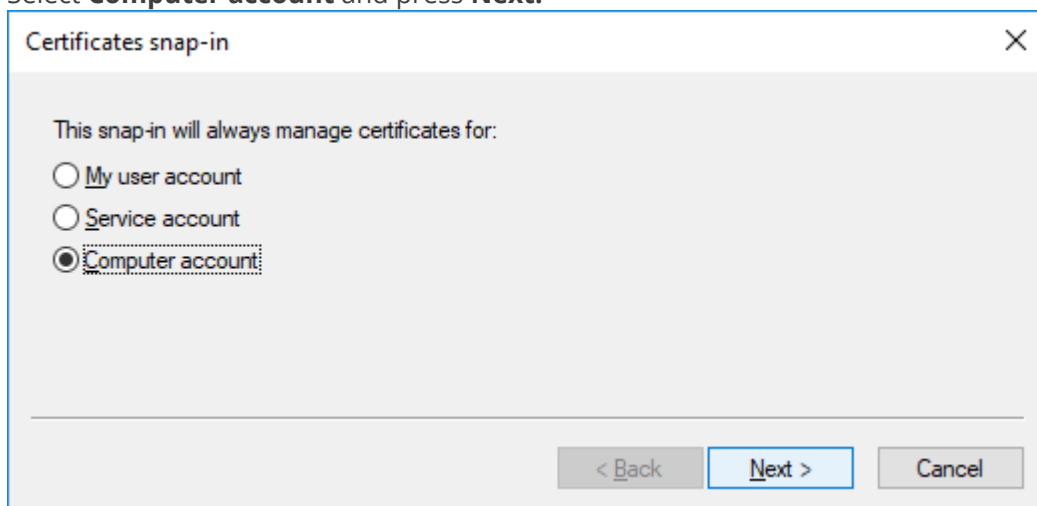
Tip: You can use the Tab key to help you input location, and hostname command for your computer name.

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

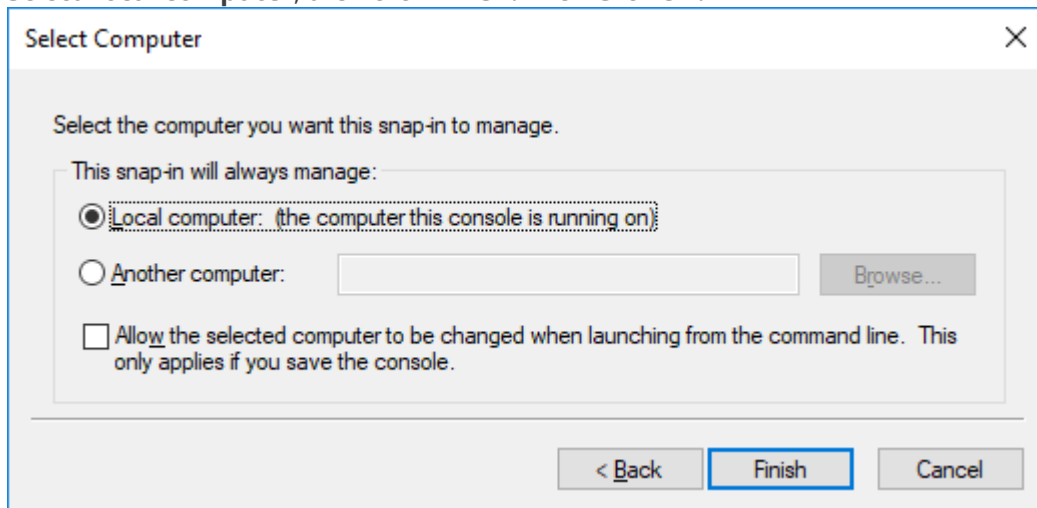
4. Select **File > Add or Remove Snap-ins**.



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**.