Hardening Document for Server

Security Configuration of Wyse Management Suite

May 2025
Rev. A04

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

This guide contains security hardening rules to secure your community servers that are deployed with Wyse Management Suite.

In database management, server hardening is the process of maximizing the security of database servers and eliminating database vulnerabilities. This document provides guidelines to restrict nonadministrators from accessing the database resources.

The audience for this guide is enterprise customers with administrator privileges.

2

Server hardening for MongoDB

This chapter contains security hardening rules to secure your MongoDB Enterprise servers 7.x that are deployed with Wyse Management Suite.

Topics:

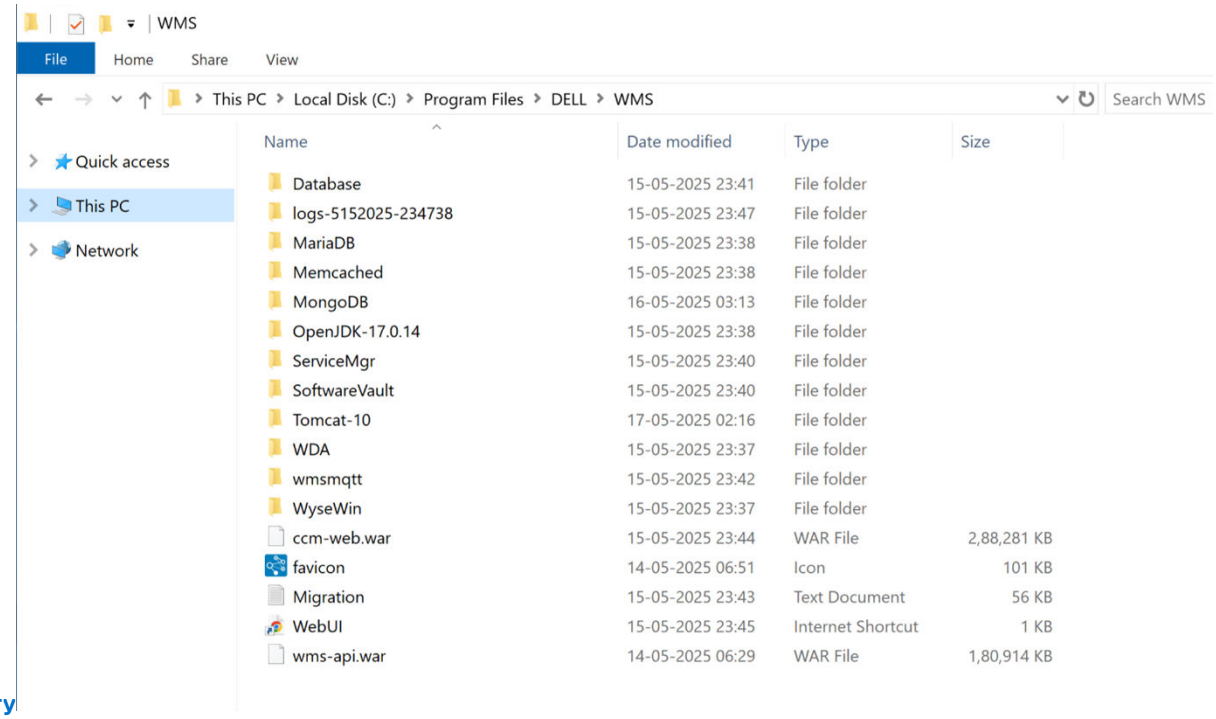
Restrict access to MongoDB resources

You must access the MongoDB service using an administrator account. If all users have access to the MongoDB service, they can access the configuration files and the data directories. Dell Technologies recommends restricting access to a service account and a user account that is used for Wyse Management Suite installation and configuration. You may restrict other local user access to Mongo DB resources. The following steps ensure that the MongoDB resources are not accessible to other users.

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the Wyse Management Suite installation directory.

Figure 1. Wyse Management Suite installation directory



3. Right-click **MongoDB** and click **Properties**.
   MongoDB Properties window is displayed.

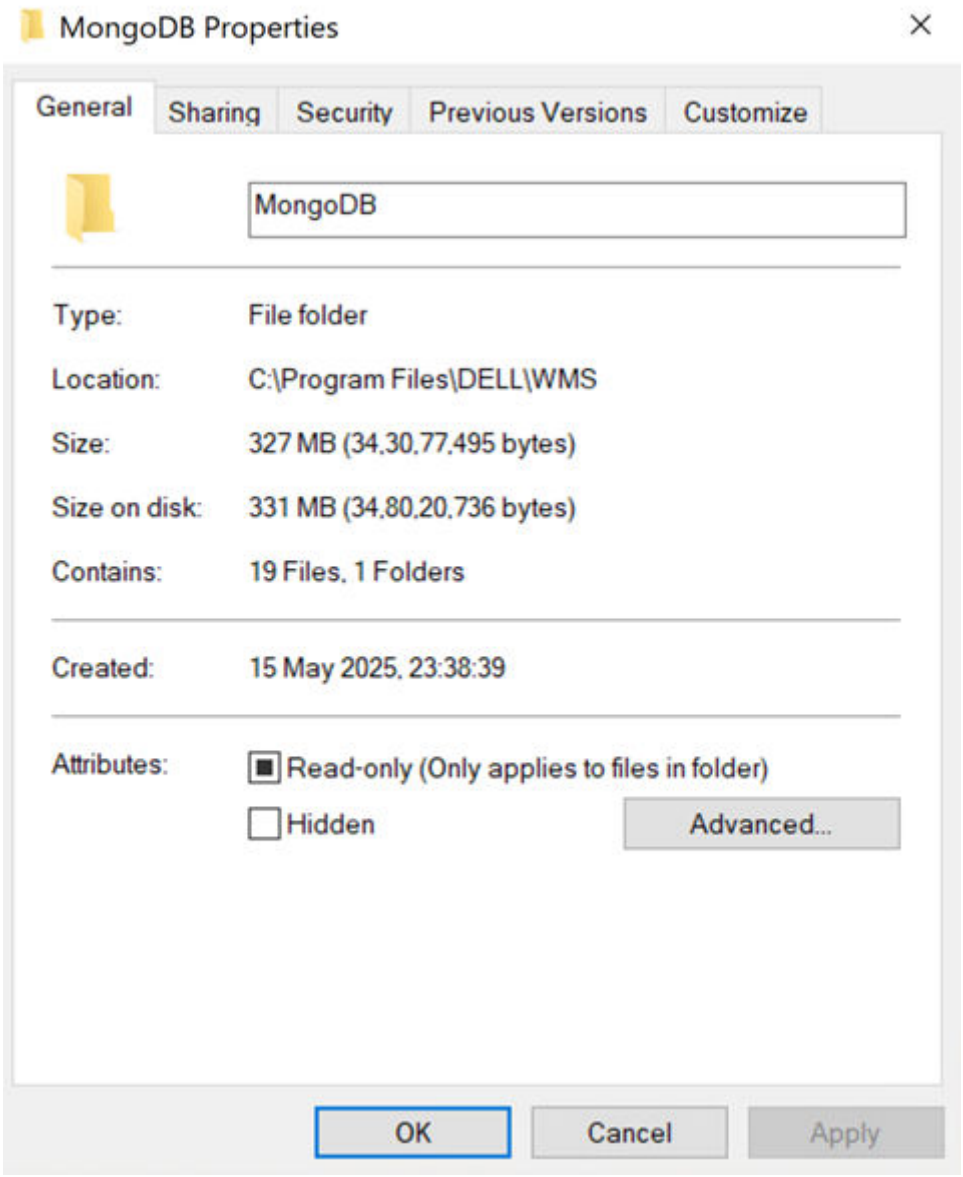


Figure 2. MongoDB properties

4. Go to the **Security** tab and click **Advanced**.

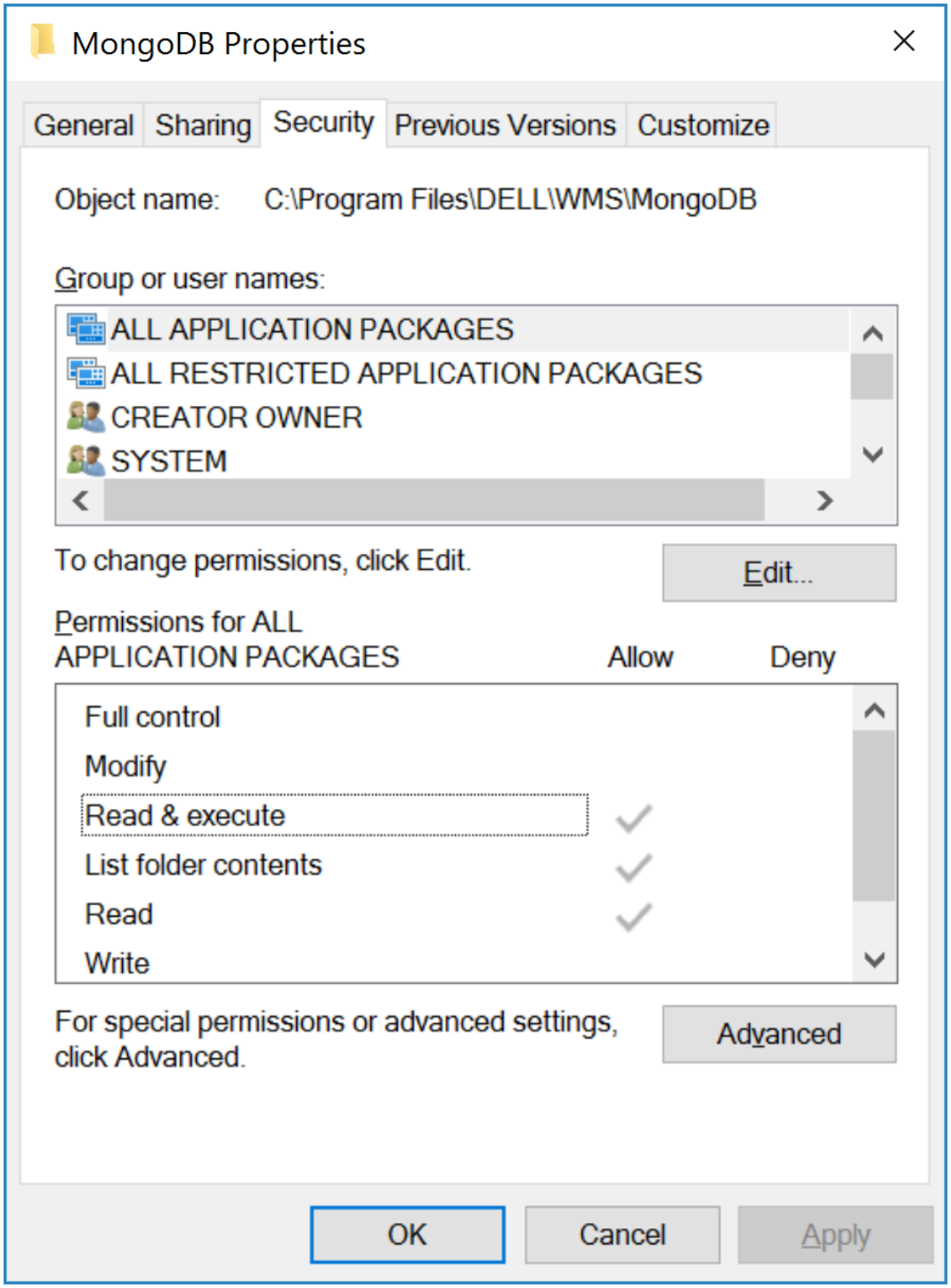


Figure 3. Security tab

Advanced Security Settings for MongoDB window is displayed.

5. Click **Disable inheritance**.
   The **Block Inheritance** window is displayed.

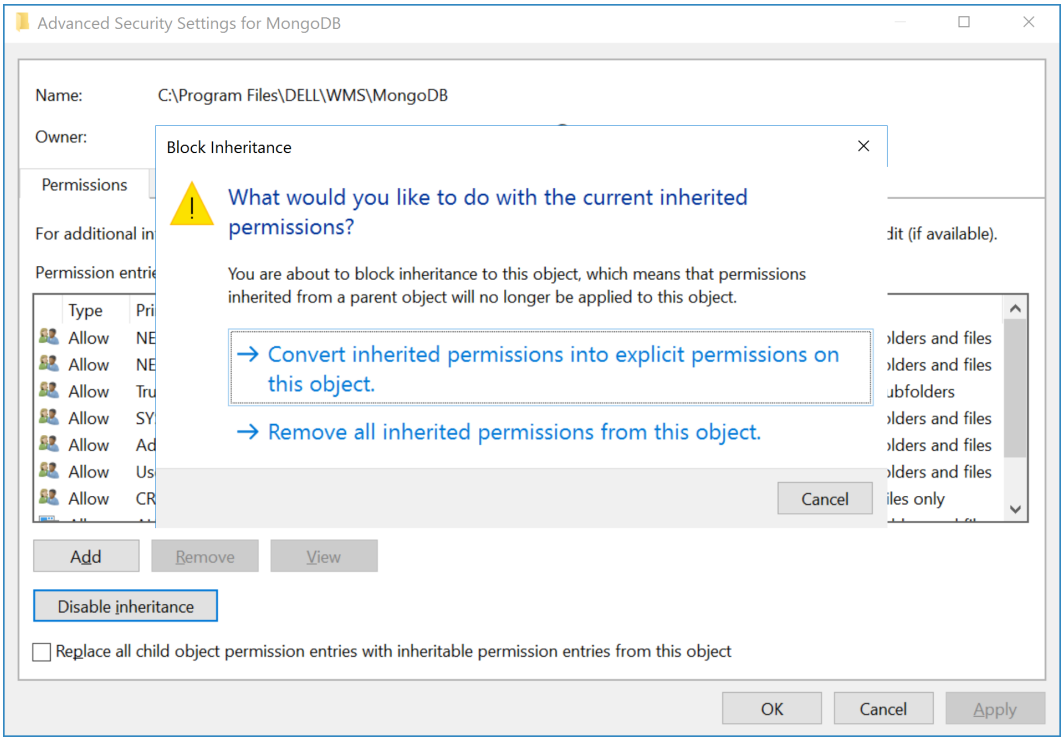


Figure 4. Block inheritance

NOTE: By default, inheritance is enabled which restricts the altering of permissions to the folder.

6. Click the **Convert inherited permissions into explicit permissions on this object** option, and click **OK**.
7. Click **Edit**, select the users that you want to remove access to the MongoDB service, and click **Remove**.

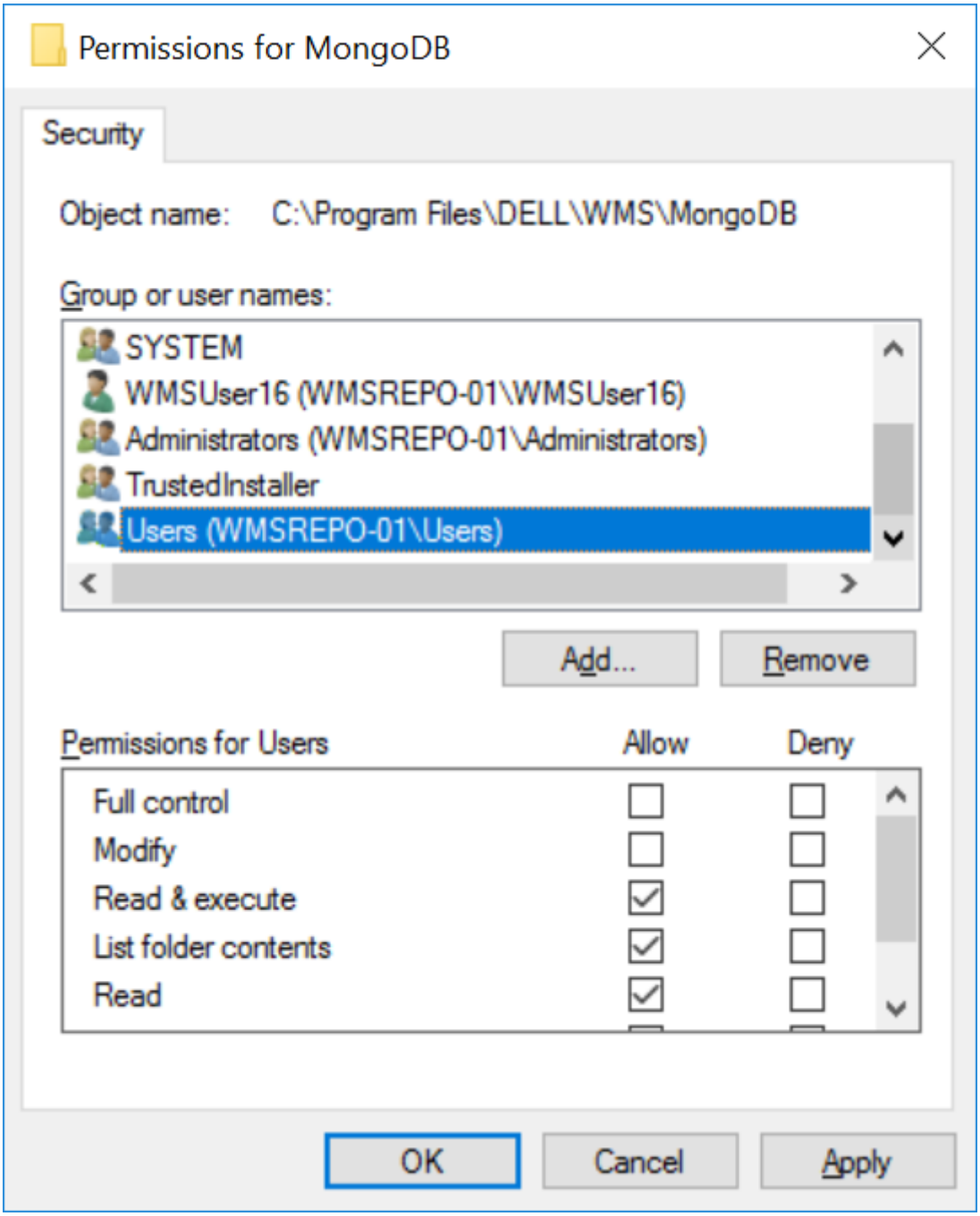


Figure 5. Remove user

8. Verify the changes by logging out from the server and logging in again using the removed user credentials. You must be denied access to the MongoDB folder—This step is optional.

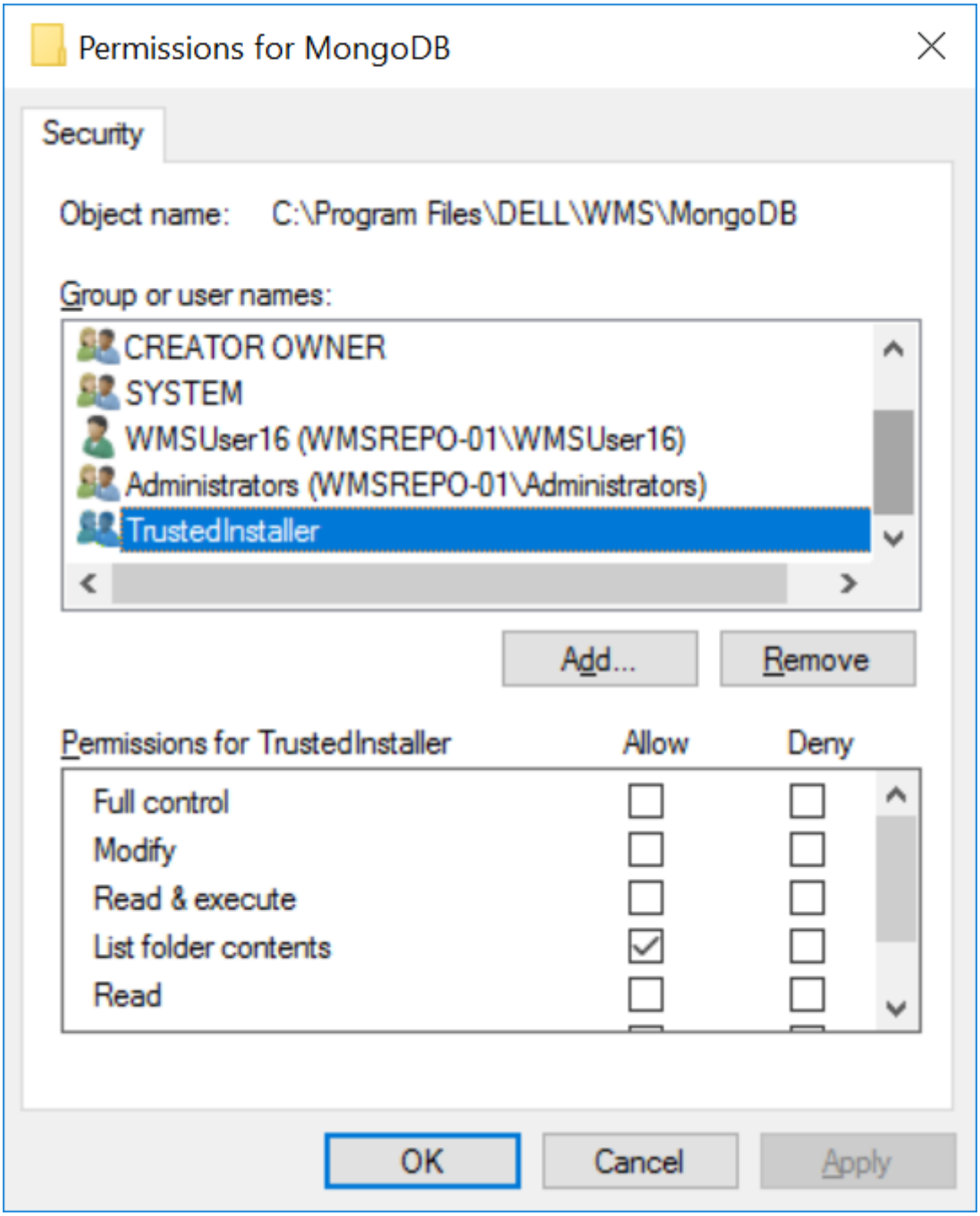


Figure 6. Verify the user deletion

If you log in with any other local user, the following screenshot is displayed.

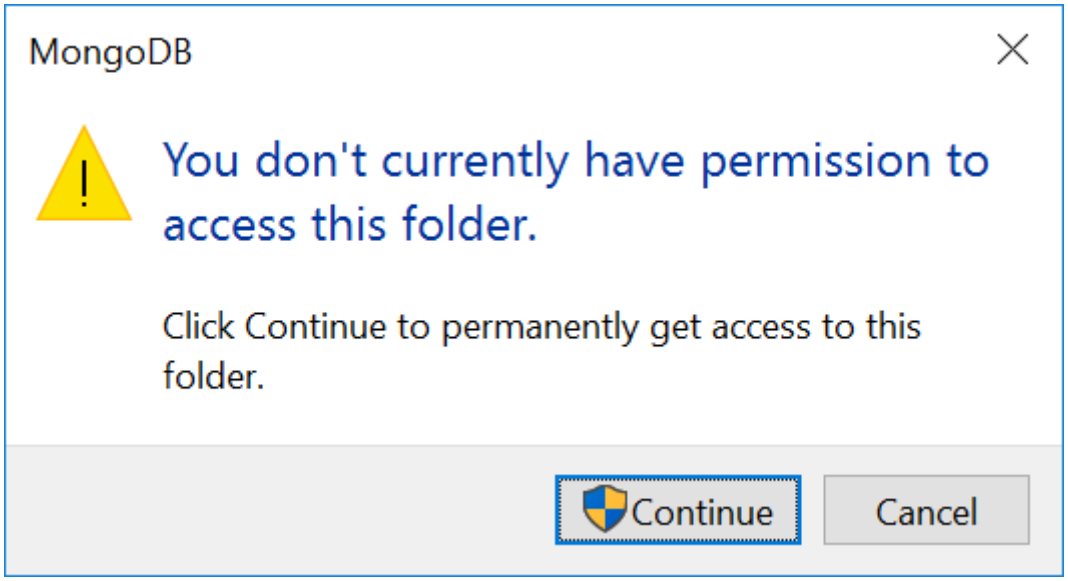


Figure 7. User restricted

Restrict access to MongoDB data directory

You must access the MongoDB data directory using an administrator account. If all users have access to the MongoDB data directory, they can access the configuration files and the data directories. Read and write permission must be set to only an administrator group, as these files are critical for the device to operate. The following steps ensure that the MongoDB resources are not accessible to other users.

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the MongoDB directory in the Wyse Management Suite installation directory.

Figure 8. Wyse Management Suite installation directory

3. Right-click **Mongo** and click **Properties**.
   MongoDB Properties window is displayed.
4. Go to the **Security** tab and click **Advanced**.

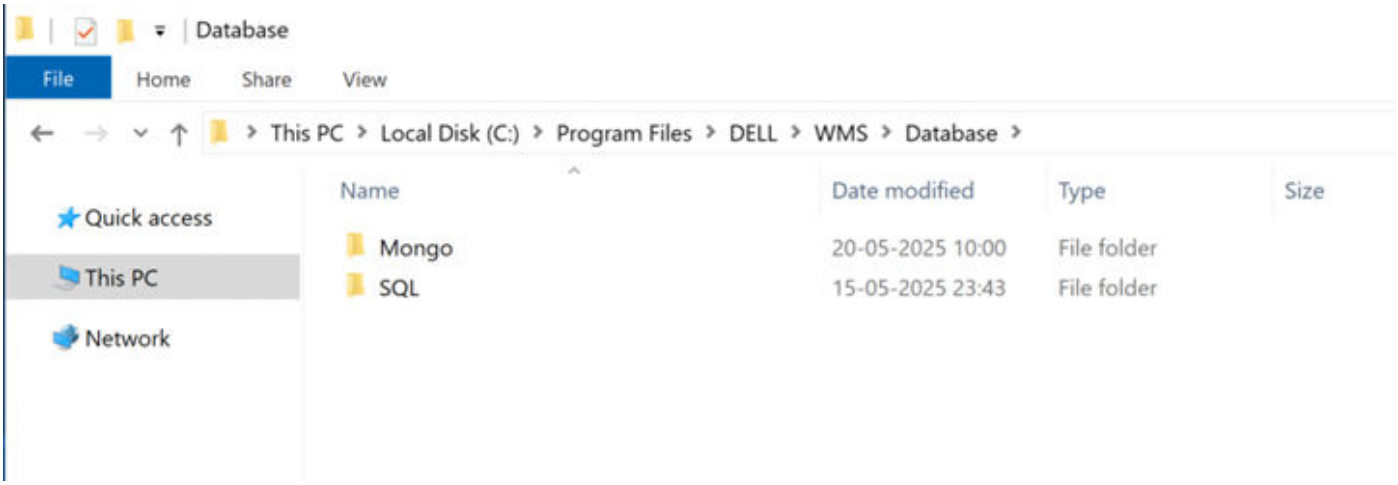


Figure 9. Security tab

Advanced Security Settings for MongoDB window is displayed.

5. Click **Disable inheritance**.
   The **Block Inheritance** window is displayed.

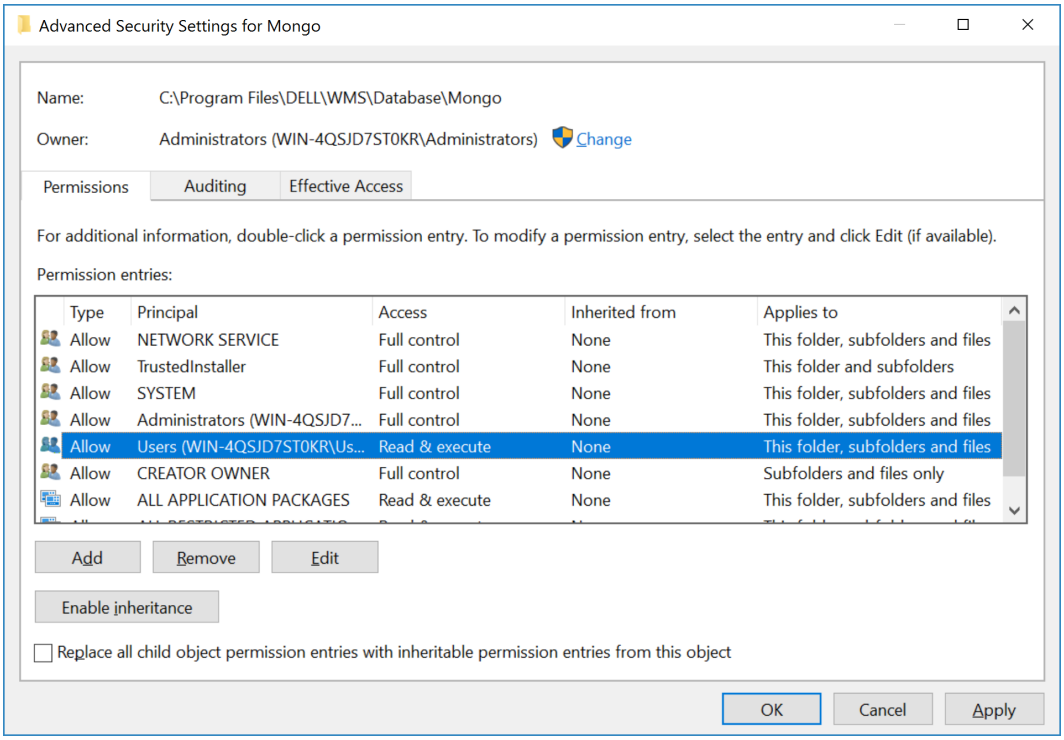


Figure 10. Disable Inheritance

NOTE: By default, inheritance is enabled which restricts the altering of permissions to the folder.

6. Click the **Convert inherited permissions into explicit permissions on this object** option.
7. Select the users that you want to remove access to the MongoDB service and click **Remove**.

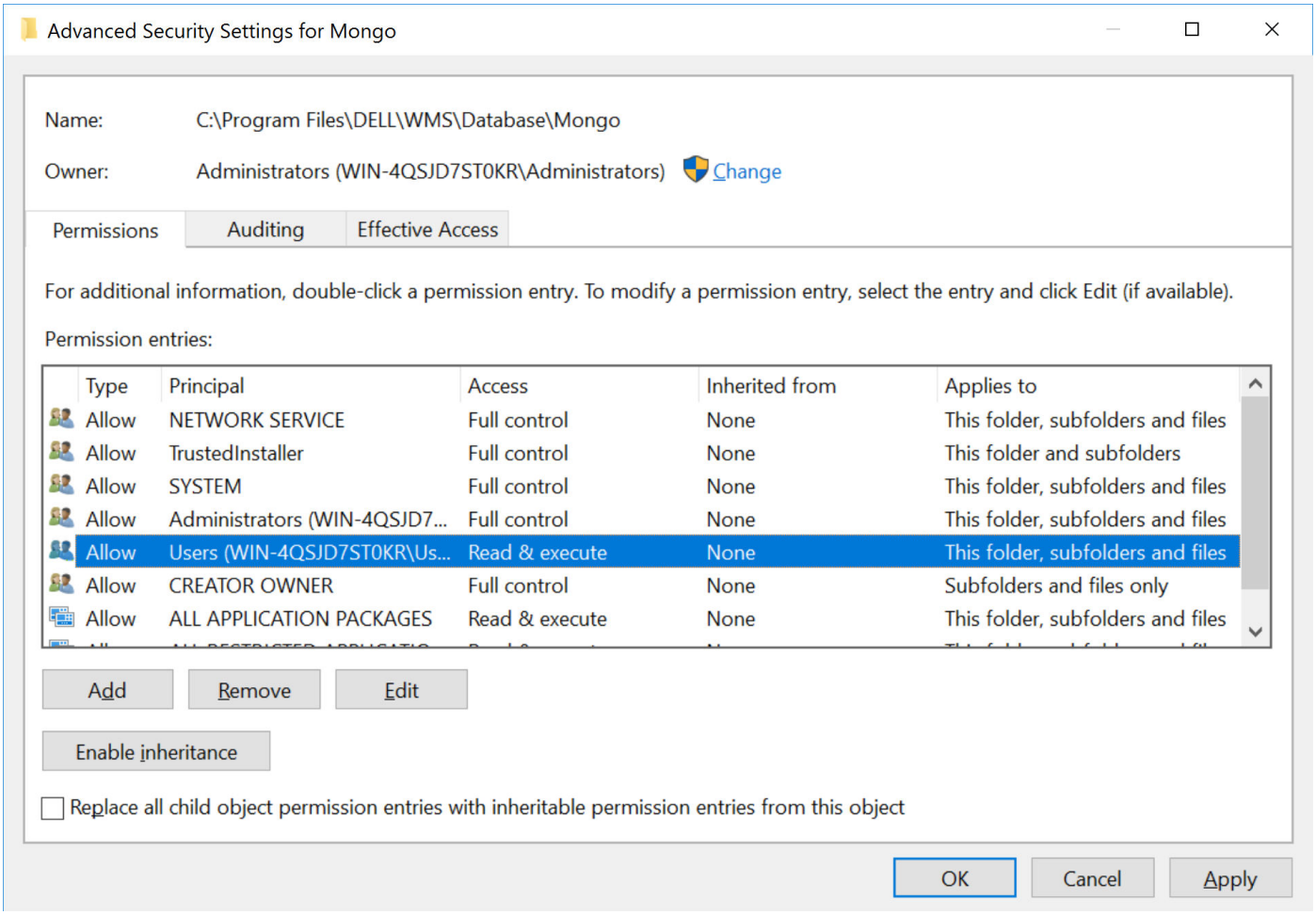


Figure 11. Remove users

8. Verify the changes by logging out from the server and logging in again using the removed user credentials. You must be denied access to the MongoDB folder—This step is optional.

Change the port number used by MongoDB

You can change the port number that is used by MongoDB and protect the database from an unauthorized access.

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the MongoDB folder in the Wyse Management Suite installation directory.

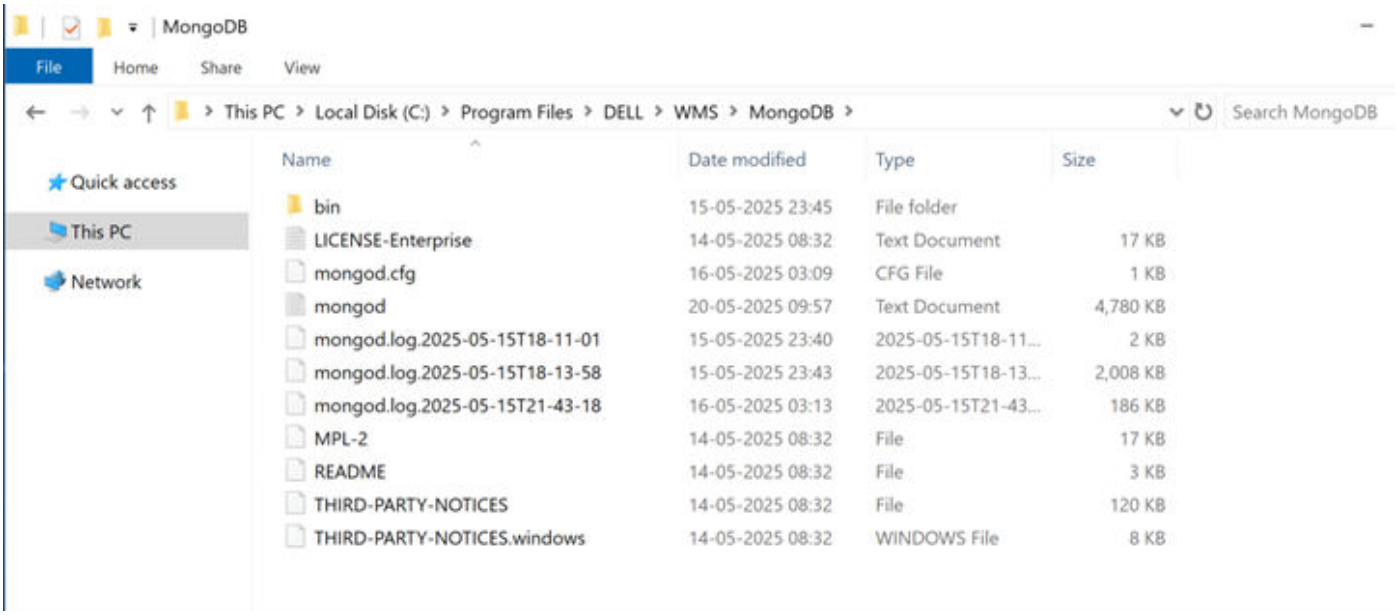


Figure 12. Wyse Management Suite installation directory

3. Open the `mongod.cfg` file and add the following command at the end of the configuration:

```
port=<new port number>
```

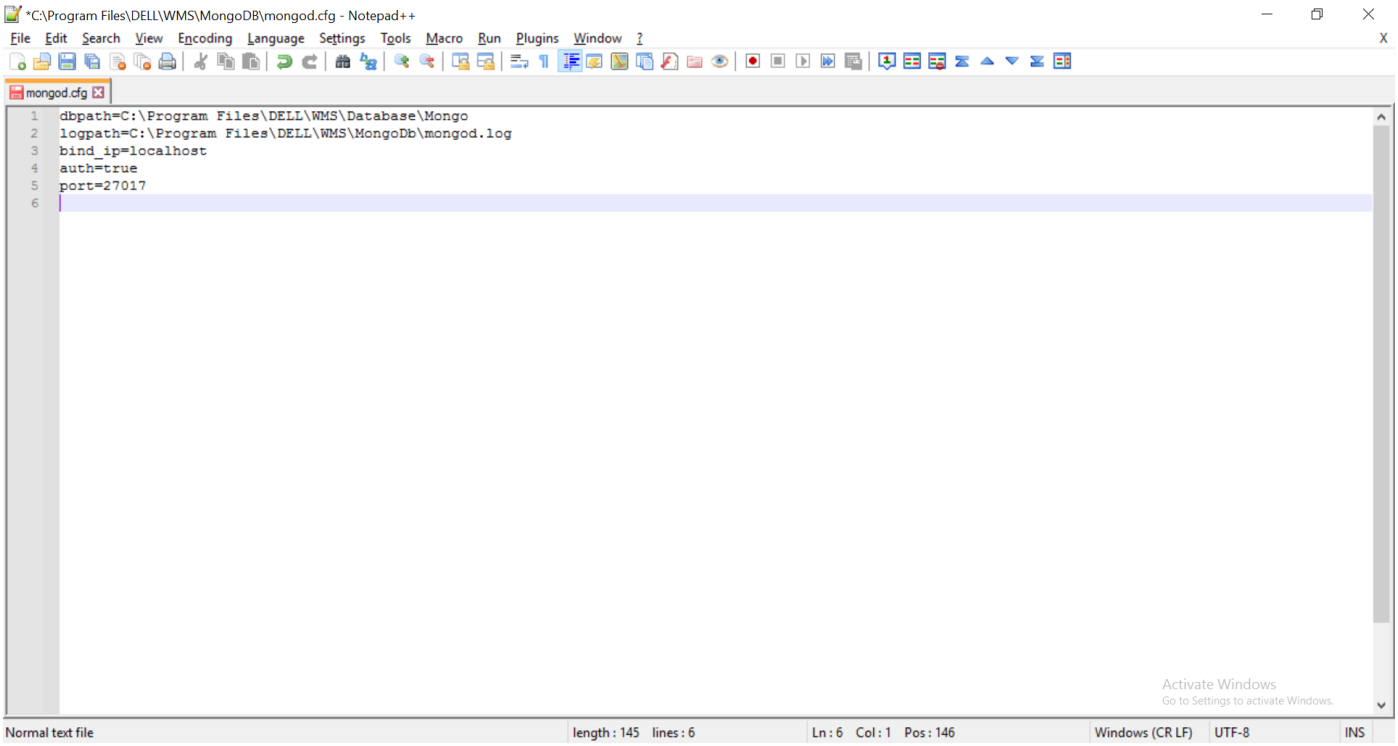


Figure 13. Change port number

The following are the default port numbers in MongoDB:

- 27017—The default port for Mongod and Mongos instances.
- 27018—The default port when you run with `--shardsvr` runtime operation.
- 27019—The default port when you run with `--configsvr` runtime operation.
- 28017—The default port for the web status page.

4. Go to **Start** > **Services**.
5. **Restart MongoDB** and **Tomcat Service**.

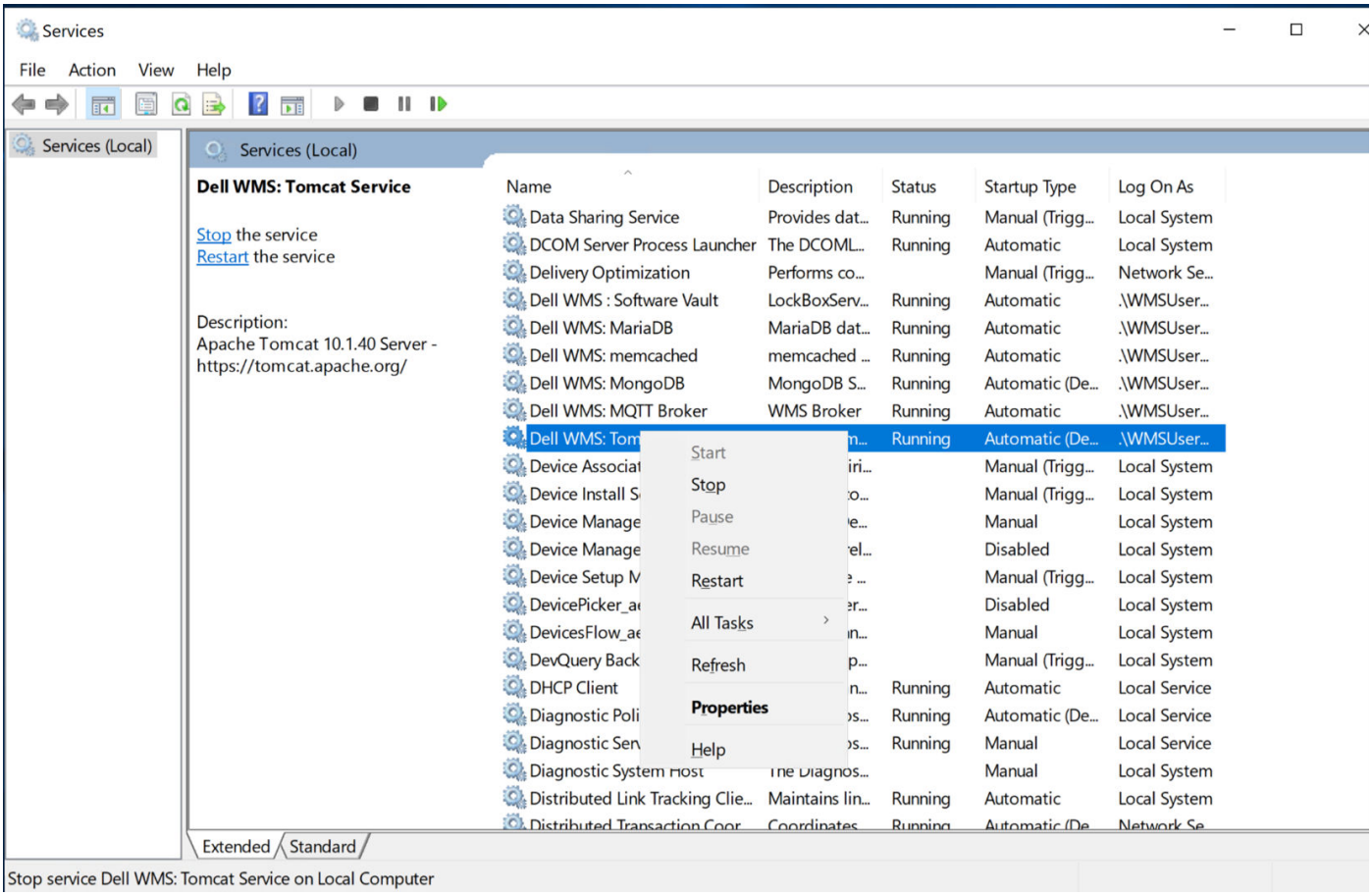


Figure 14. Restart MongoDB and Tomcat Service

NOTE: MongoDB port change and configuration file must have the same changed port entry. If not, the Wyse Management Suite server fails to load.

Change the new MongoDB port in the configuration file

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to `C:\Program Files\DELL\WMS\Tomcat-10\webapps\ccm-web\WEB-INF\classes` .

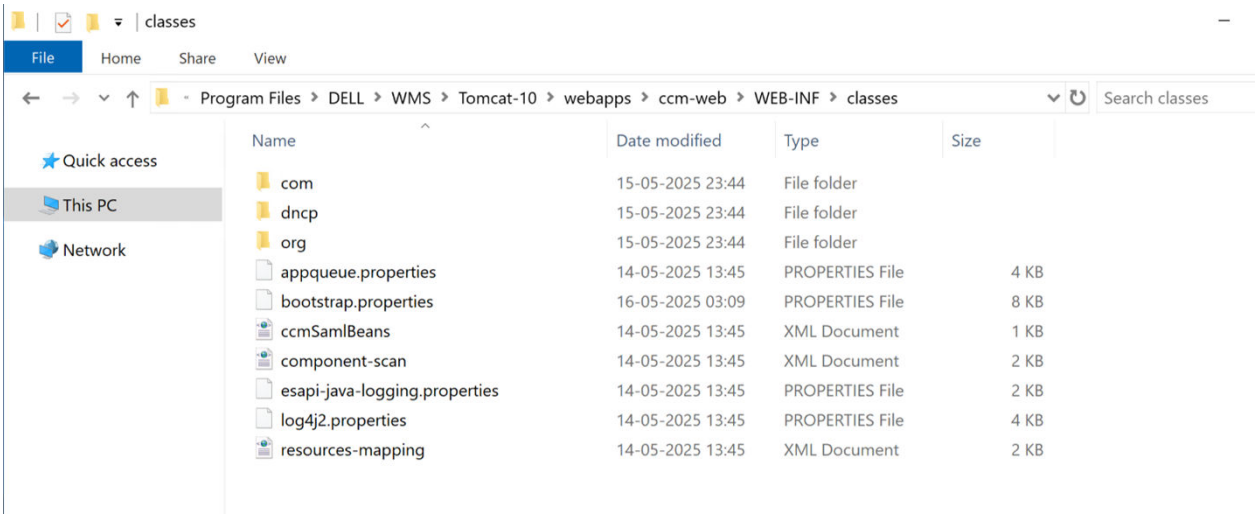


Figure 15. Configuration file directory

3. Open the `bootstrap.properties` file.
4. Update the following value with the new port number that is assigned to MongoDB in the file:

```
mongodb.Hostname=localhost\:<updated port number>
```

Figure 16. Updated port number

5. Save the file.
6. Go to **Start** > **Services**.
7. Right-click **Dell WMS: Tomcat Service** and click **Restart**.

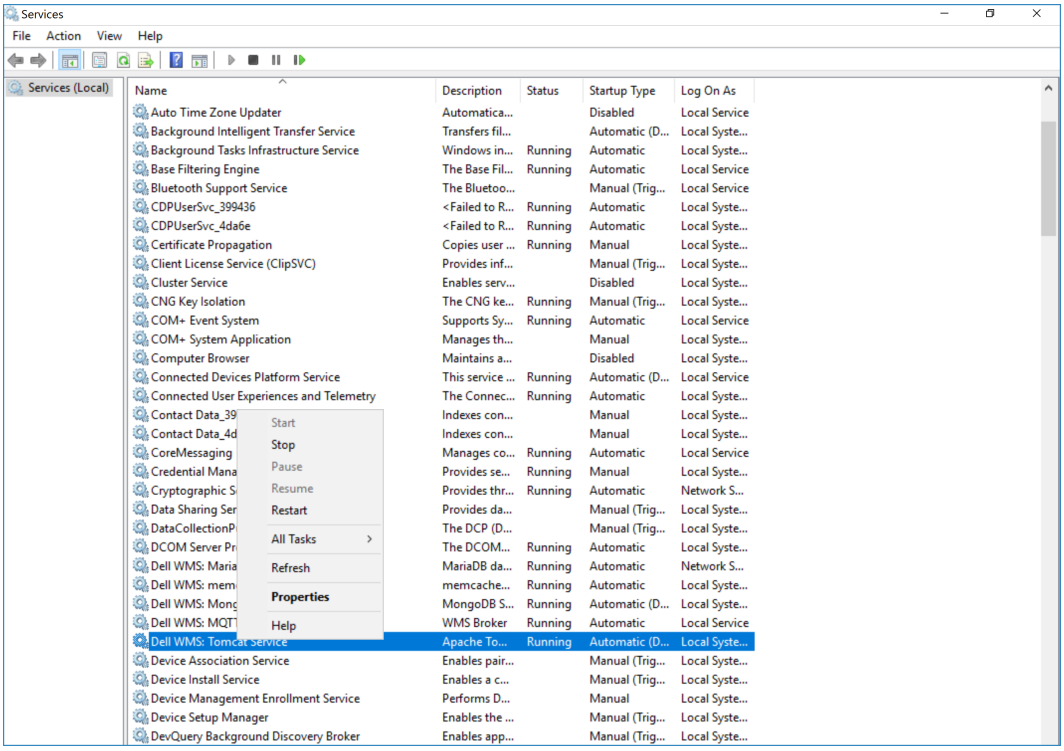


Figure 17. Restart Tomcat service

8. Log in to the Wyse Management Suite application.
   The port number is changed, and the application is loaded.

Configure MongoDB resources to capture system logs

If the MongoDB log configuration is set to silent or quiet, the logging of information does not work. You must configure the `SystemLog.quiet` option to log information such as connection events, authentication events, replication sync activities, and capture evidence if some harmful commands are run such as drop, dropIndexes, and so on.

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the MongoDB folder in the Wyse Management Suite installation directory.

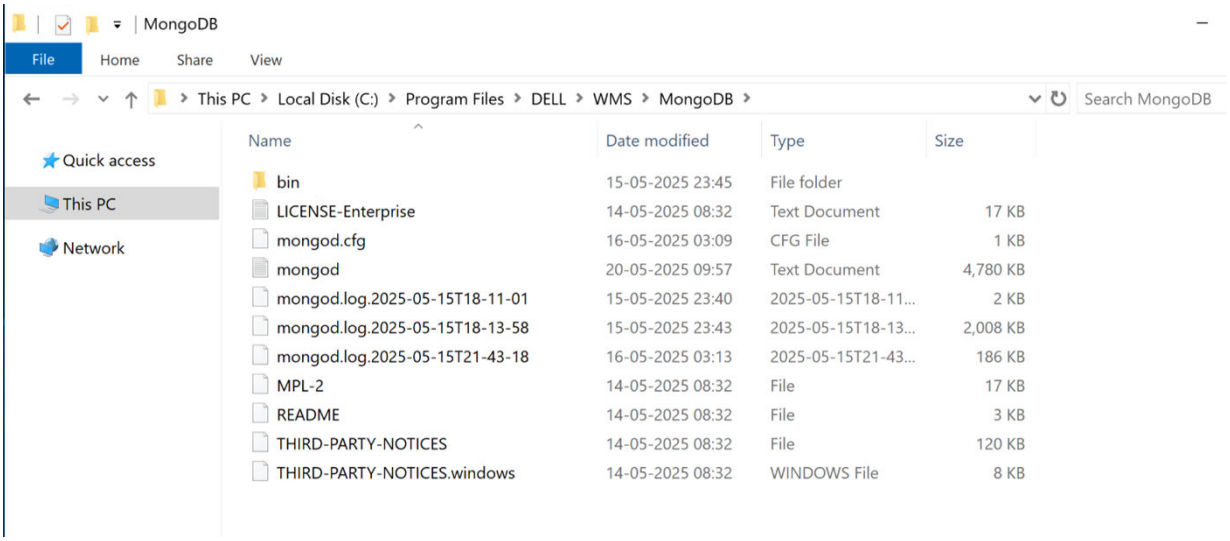


Figure 18. Wyse Management Suite installation directory

3. Open the `mongod.cfg` file and add the following commands at the end of the configuration:

```
#systemLog:
 quiet=false
```

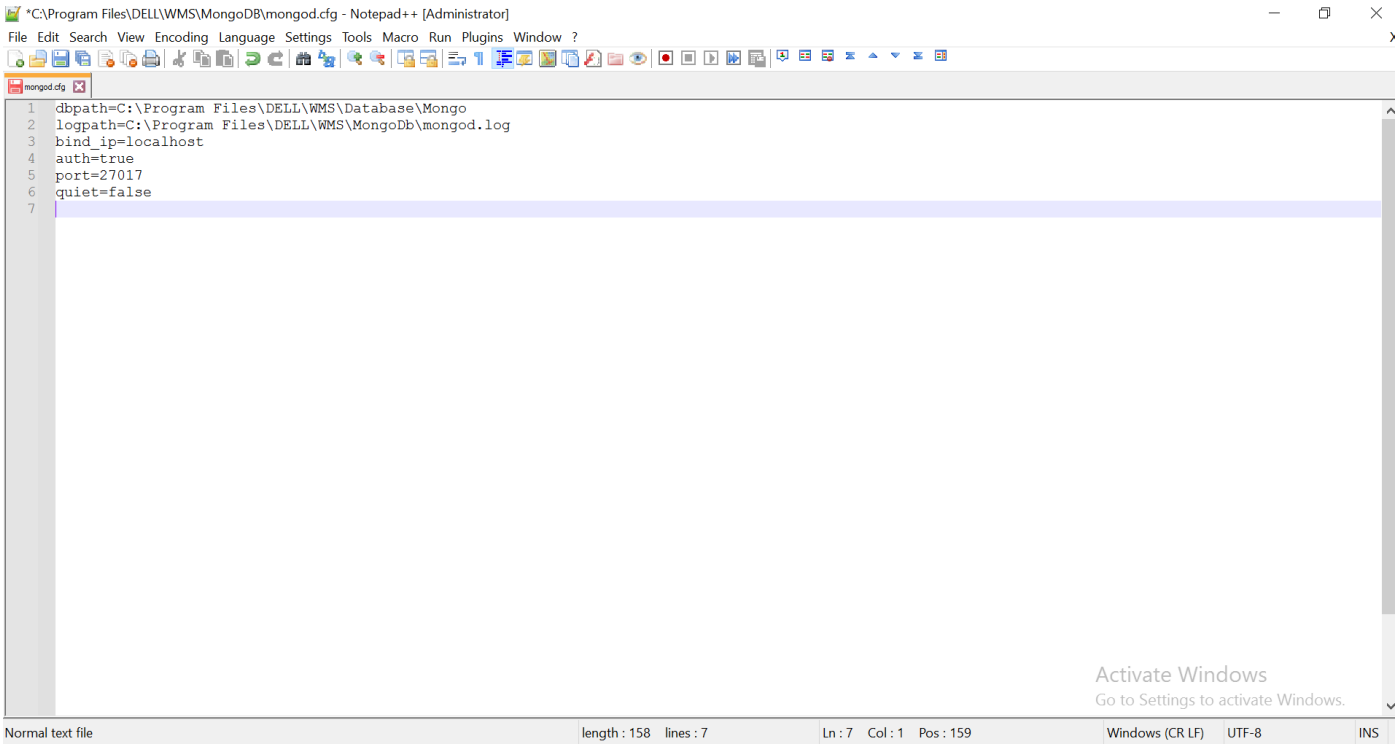


Figure 19. Configuration file

4. Go to **Start** > **Services**.
5. Restart **MongoDB** and **Tomcat Service**.

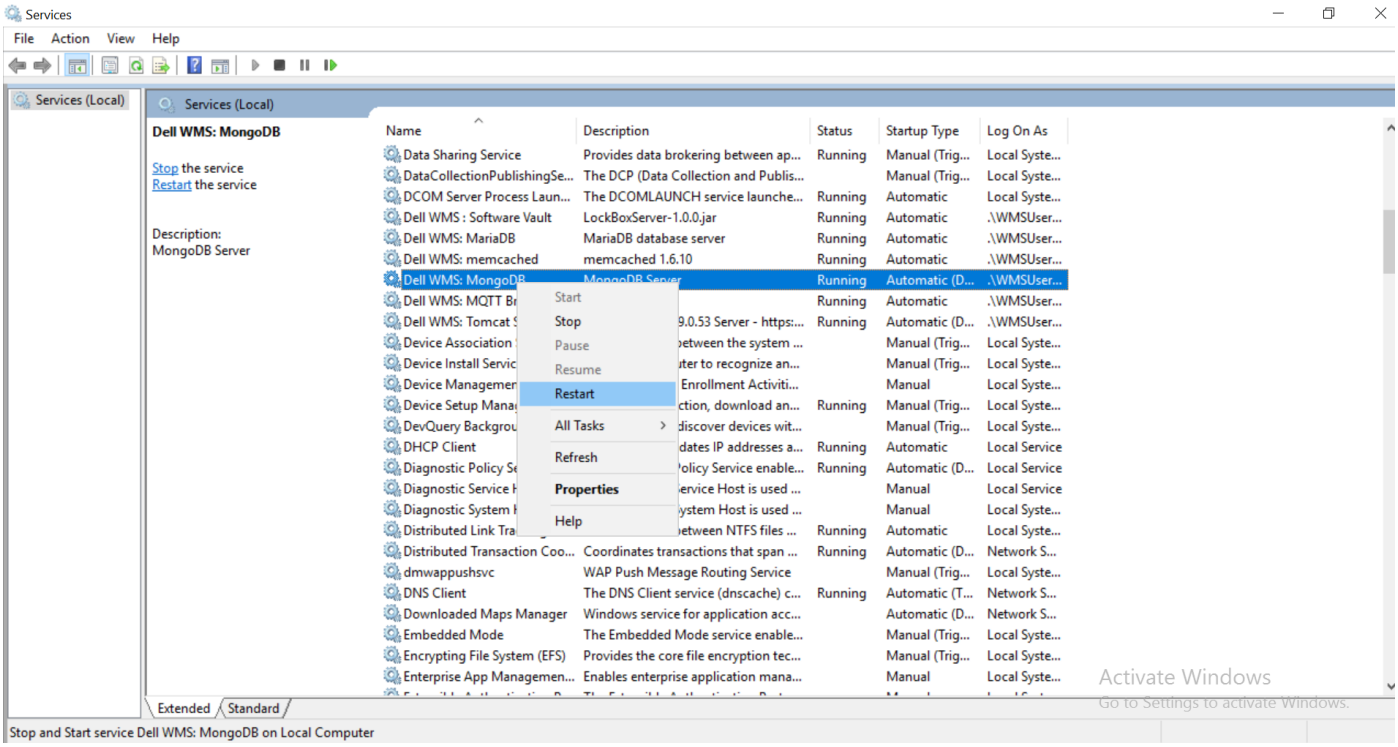


Figure 20. Restart MongoDB

3

Server hardening for MariaDB/MySQL

This chapter contains security hardening rules to secure your MariaDB and MySQL Community servers 10.x that are deployed with Wyse Management Suite.

Topics:

Restrict access to MariaDB or MySQL resources

You must access the MariaDB or MySQL service using an administrator account. If all users have access to the MariaDB or MySQL service, they can access the configuration files and the data directories. Dell Technologies recommends restricting access to a user account that is used for Wyse Management Suite installation and configuration. The following steps ensure that the MariaDB or MySQL resources are not accessible to other users.

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the Wyse Management Suite installation directory.

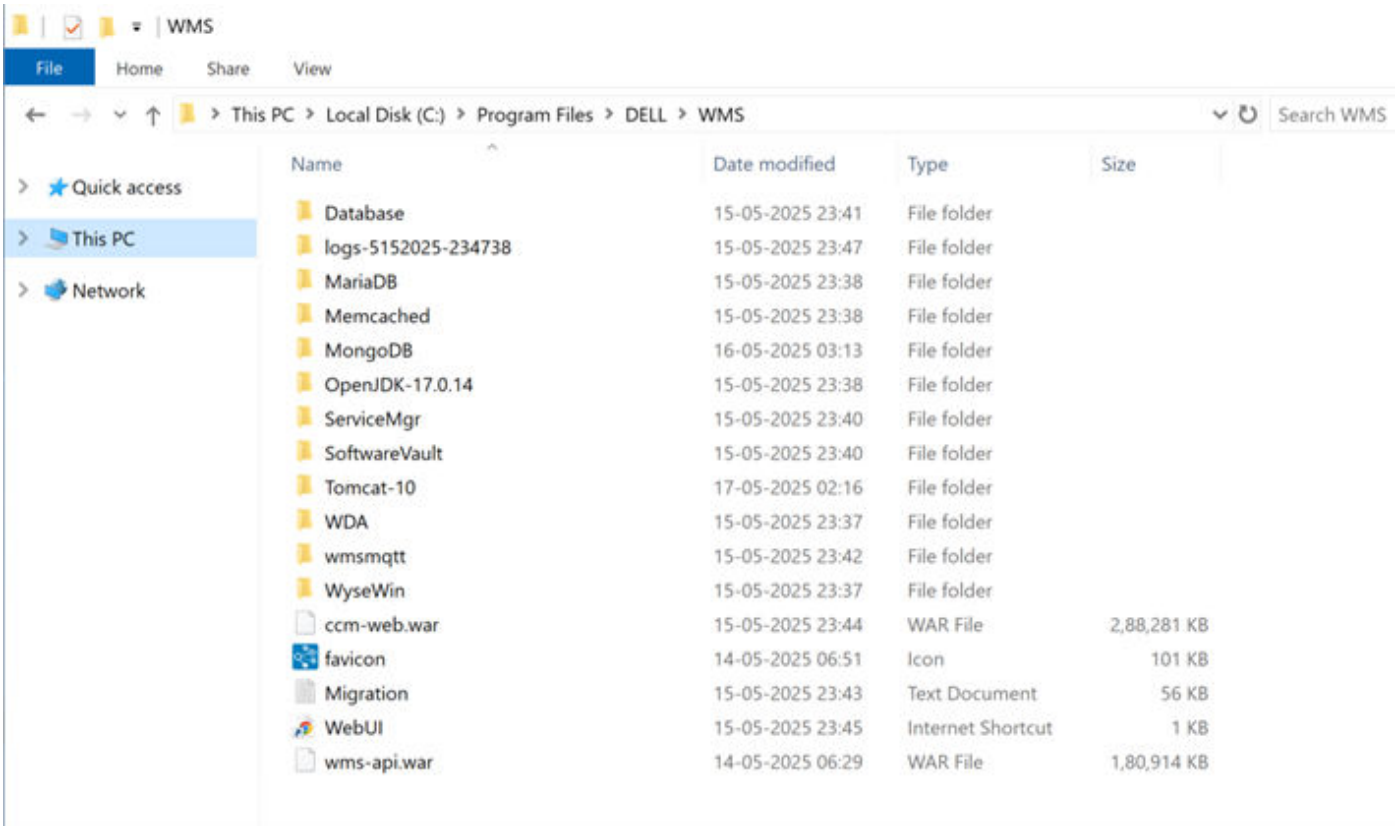


Figure 21. Wyse Management Suite installation directory

3. Right-click **MariaDB** and click **Properties**.
   MariaDB Properties window is displayed.

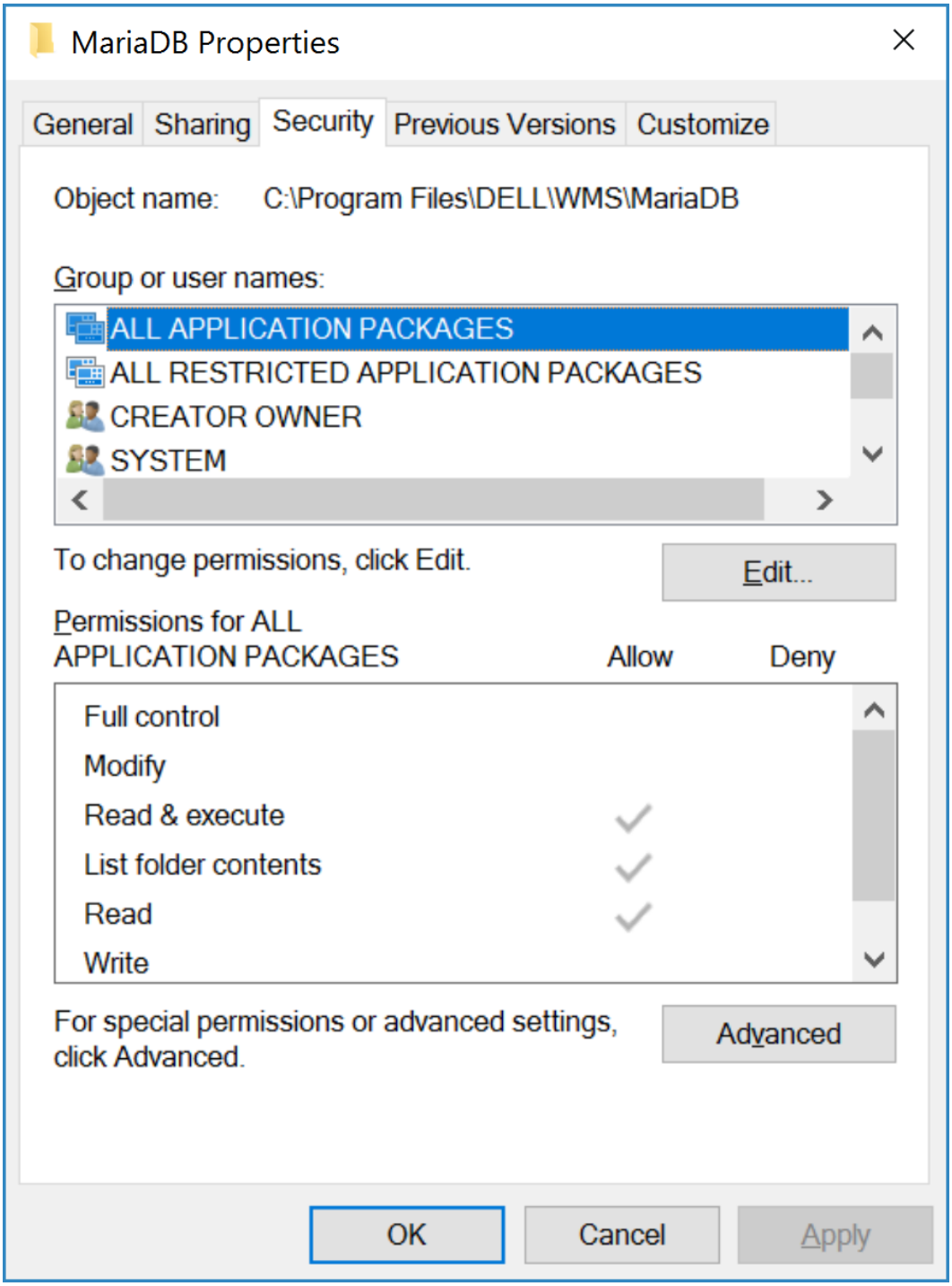


Figure 22. Security tab

4. Go to the **Security** tab and click **Advanced**.
   Advanced Security Settings for MariaDB window is displayed.
5. Click **Disable inheritance**.
   The **Block Inheritance** window is displayed.

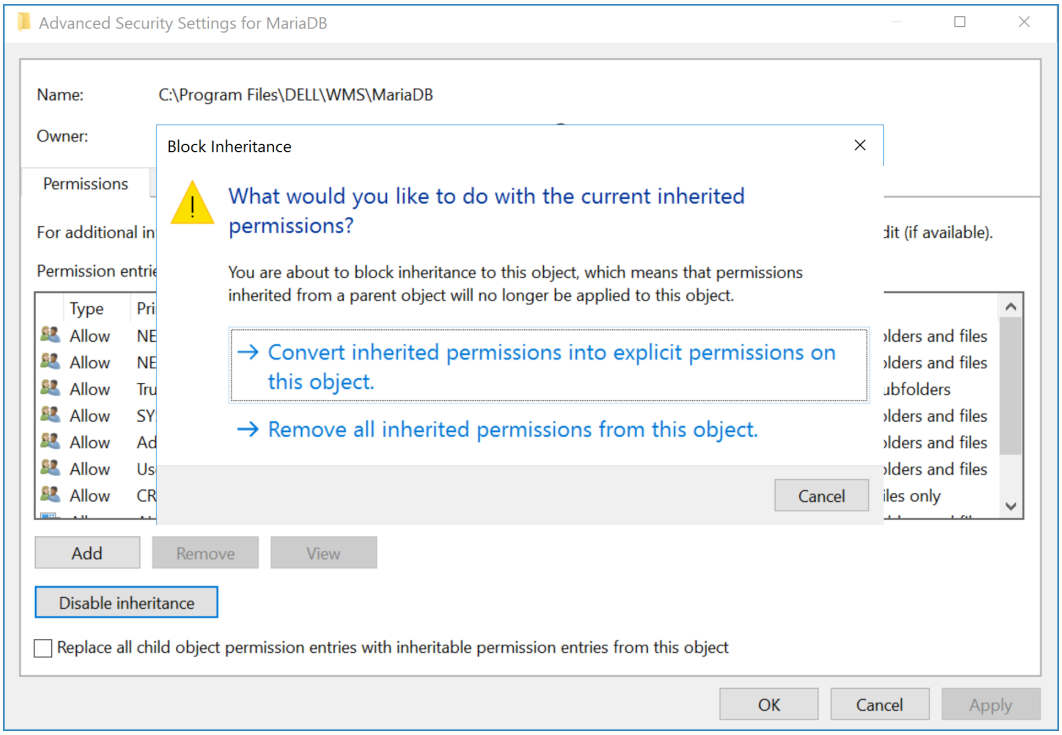


Figure 23. Block inheritance

NOTE: By default, inheritance is enabled which restricts the altering of permissions to the folder.

6. Click the **Convert inherited permissions into explicit permissions on this object** option, and click **OK**.
7. Go to the **Security** tab, click **Edit**, select the user that you want to remove access to the MariaDB service, and click **Remove**.

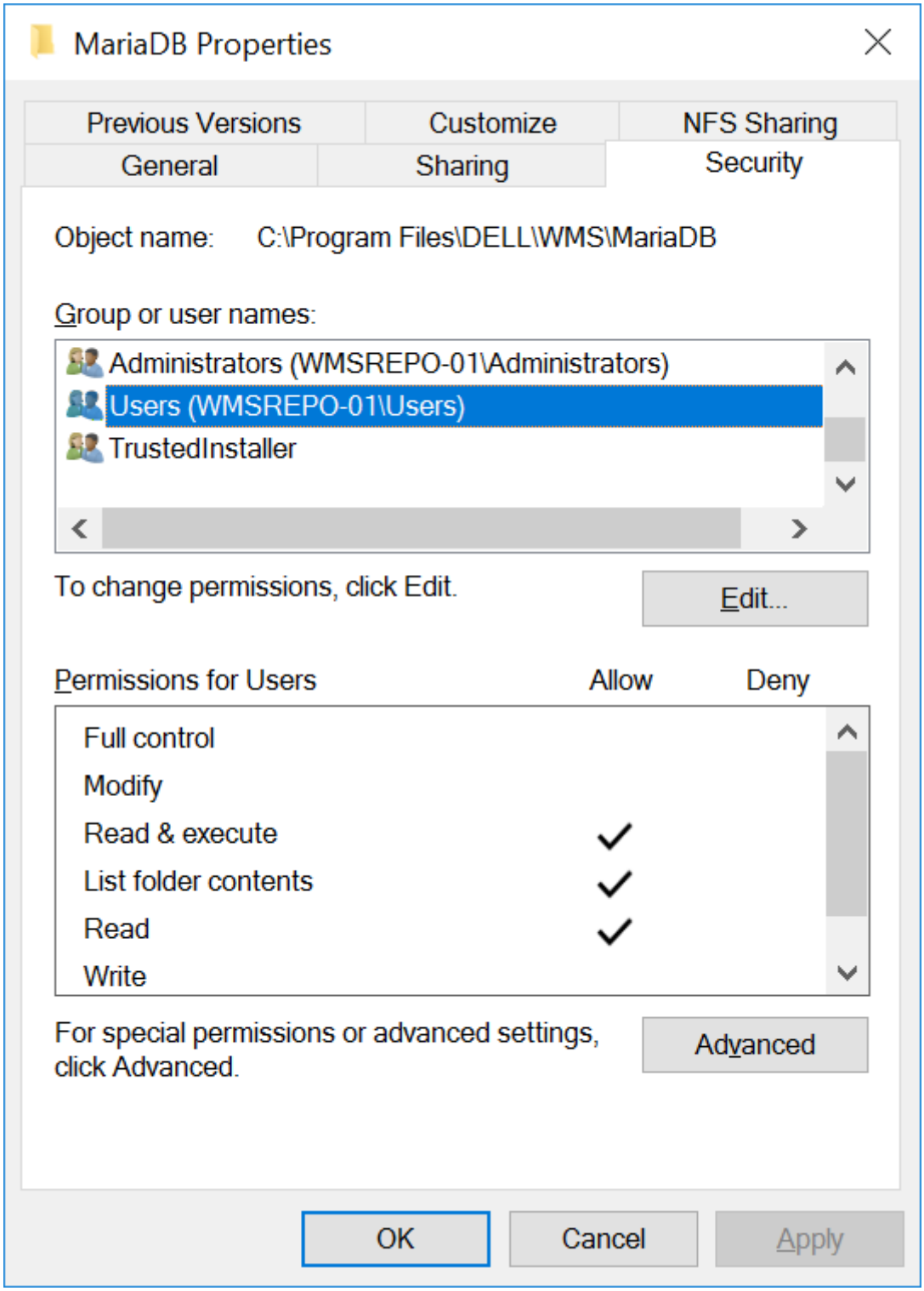


Figure 24. Remove users

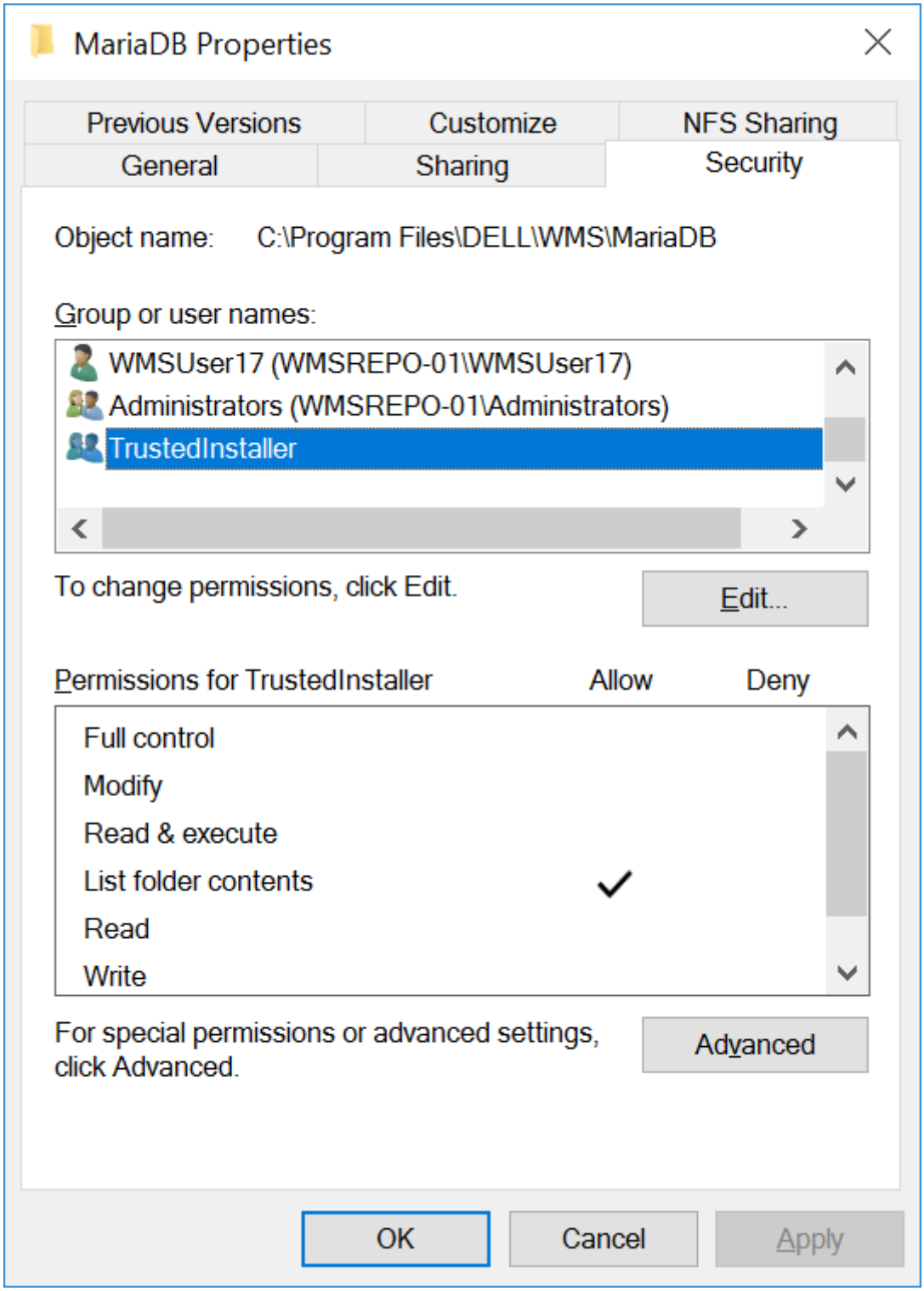


Figure 25. Select TrustedInstaller

If you log in with any other local user, the following screenshot is displayed.

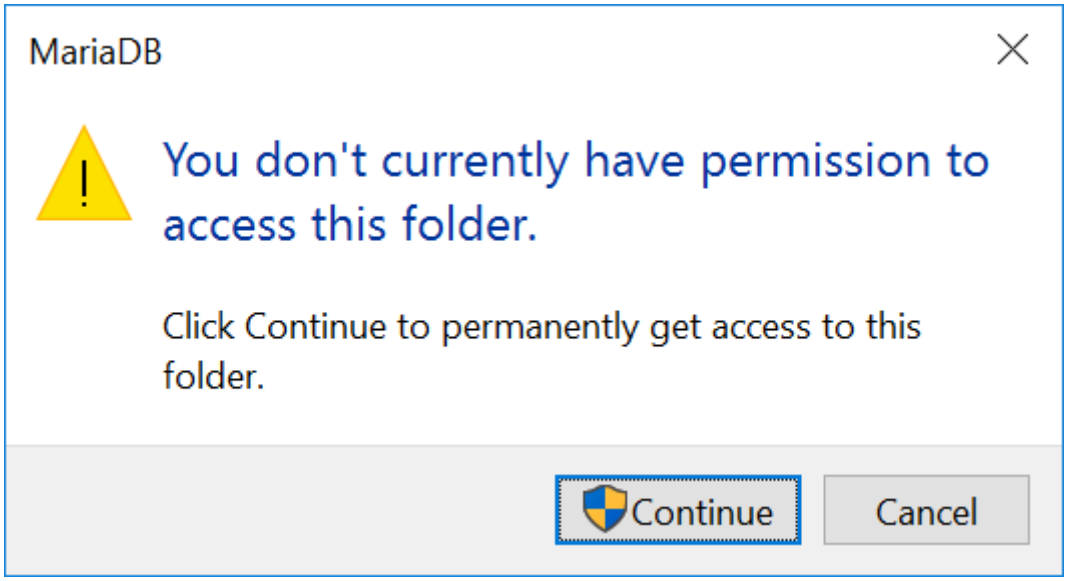


Figure 26. User restricted

8. Verify the changes by logging out from the server and logging in again using the removed user credentials. You must be denied access to the MariaDB folder—This step is optional.
9. Click **Enable inheritance**.

Restrict access to MariaDB or MySQL data directory

The data directory (datadir) contains the MySQL databases. If the access is restricted, other users cannot read data from the mysql.user table that contains passwords. You can also restrict access to a user who can manually create a file with a view definition.

Steps

1. Log in to the MariaDB shell.

   NOTE: The Stratus password is the password that was used for the database password during the Wyse Management Suite installation.

```
C:\Program Files\DELL\WMS\MariaDB\bin>mysql -u stratus -p
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 28
Server version: 10.2.29-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Figure 27. MariaDB shell

2. Switch to the stratus schema using the following command:

```
use stratus;
```

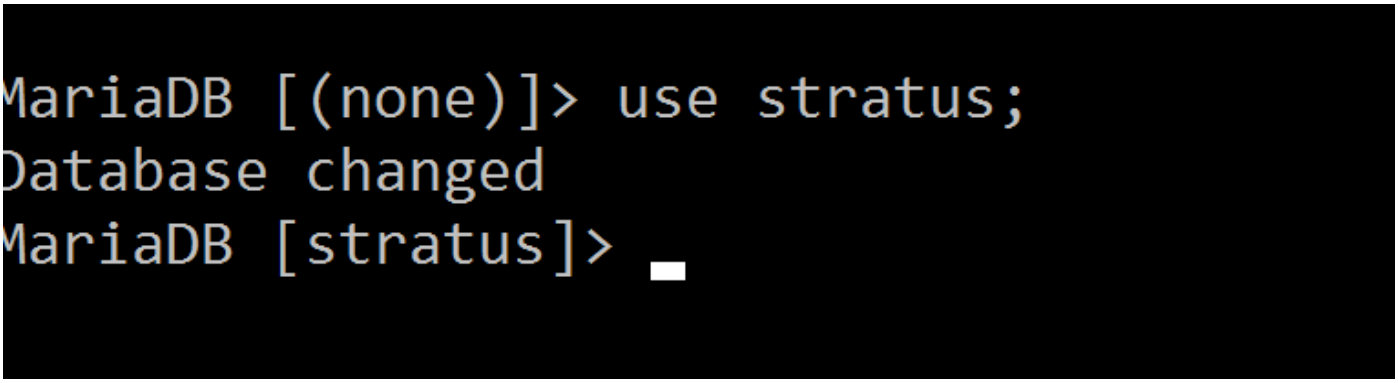


Figure 28. Switch schema

3. Run the following command to identify the data directory path:

```
--show variables where variable_name = 'datadir';
```

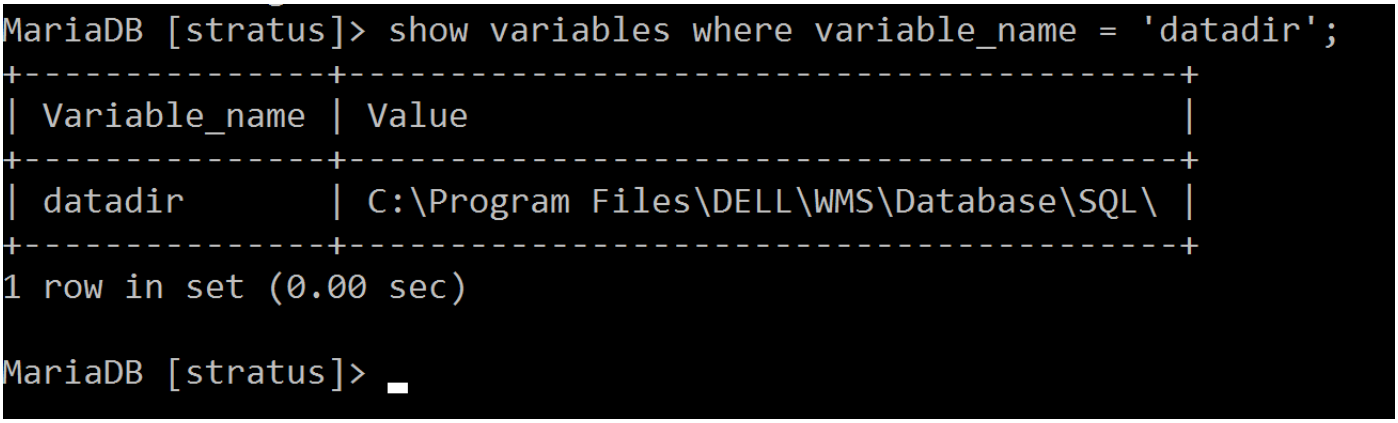


Figure 29. MariaDB data directory

4. Go to the data directory.
5. Right-click **SQL**, and click **Properties**.

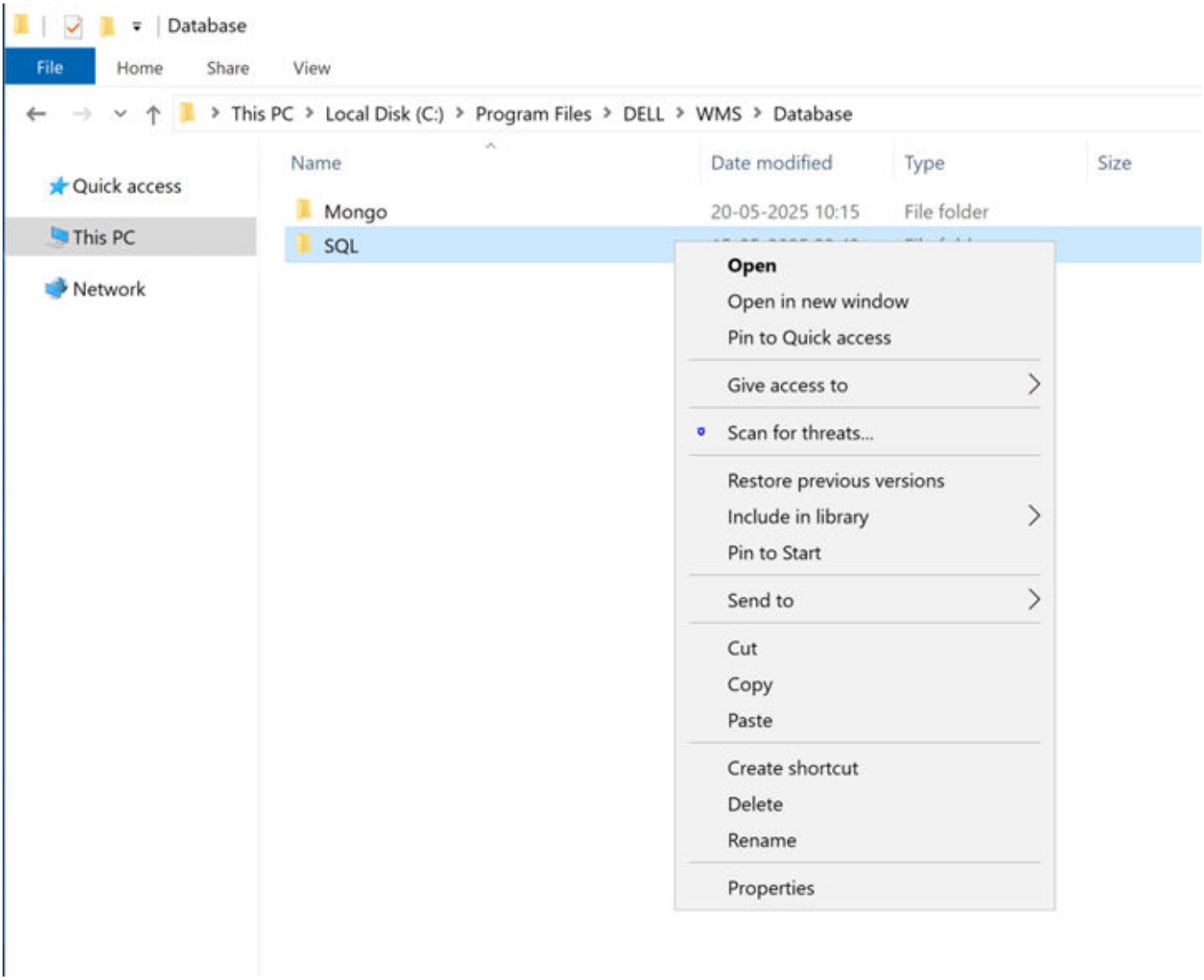


Figure 30. Properties

MariaDB Properties window is displayed.

6. Go to the **Security** tab and click **Advanced**.

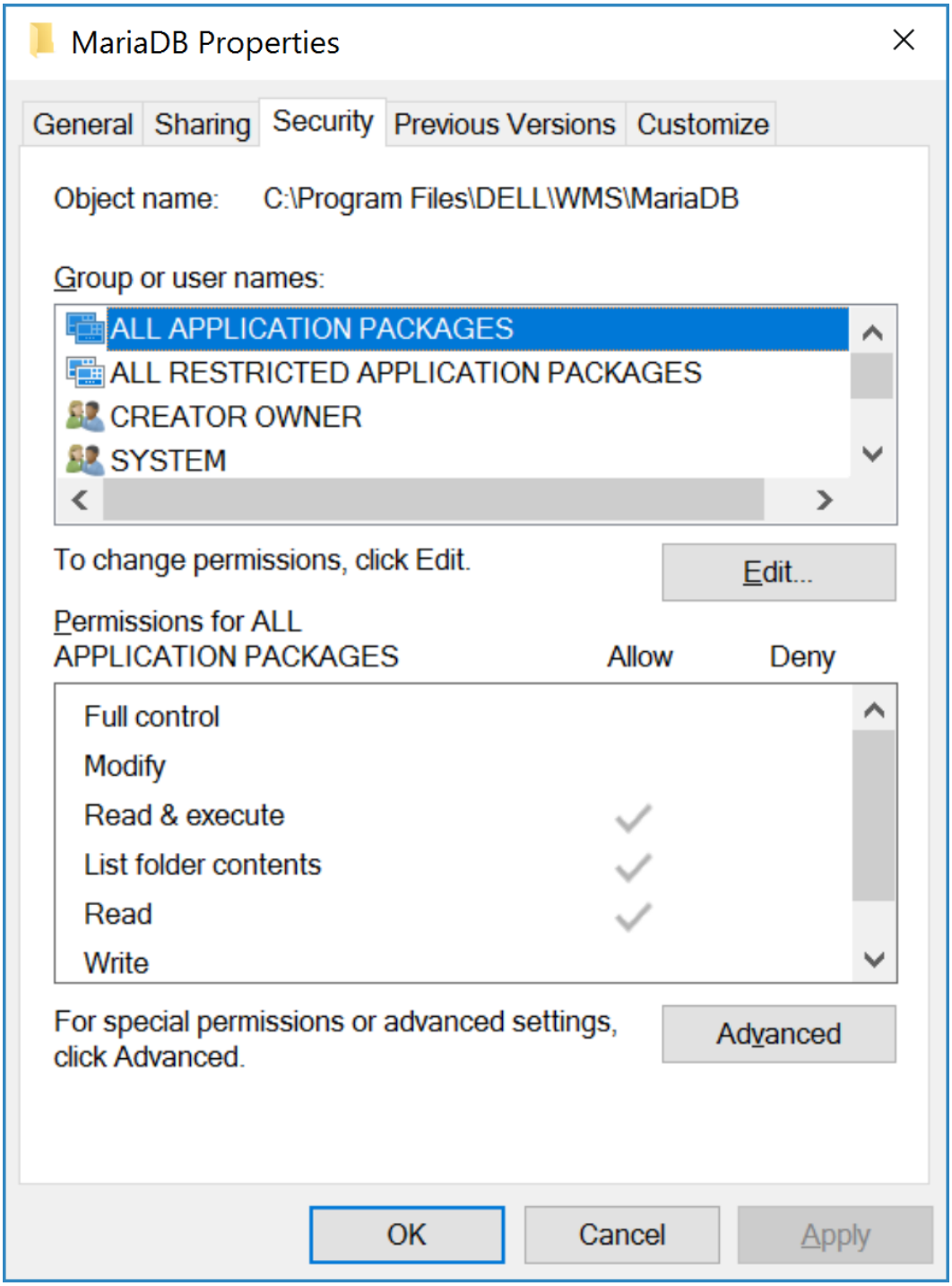


Figure 31. Security tab

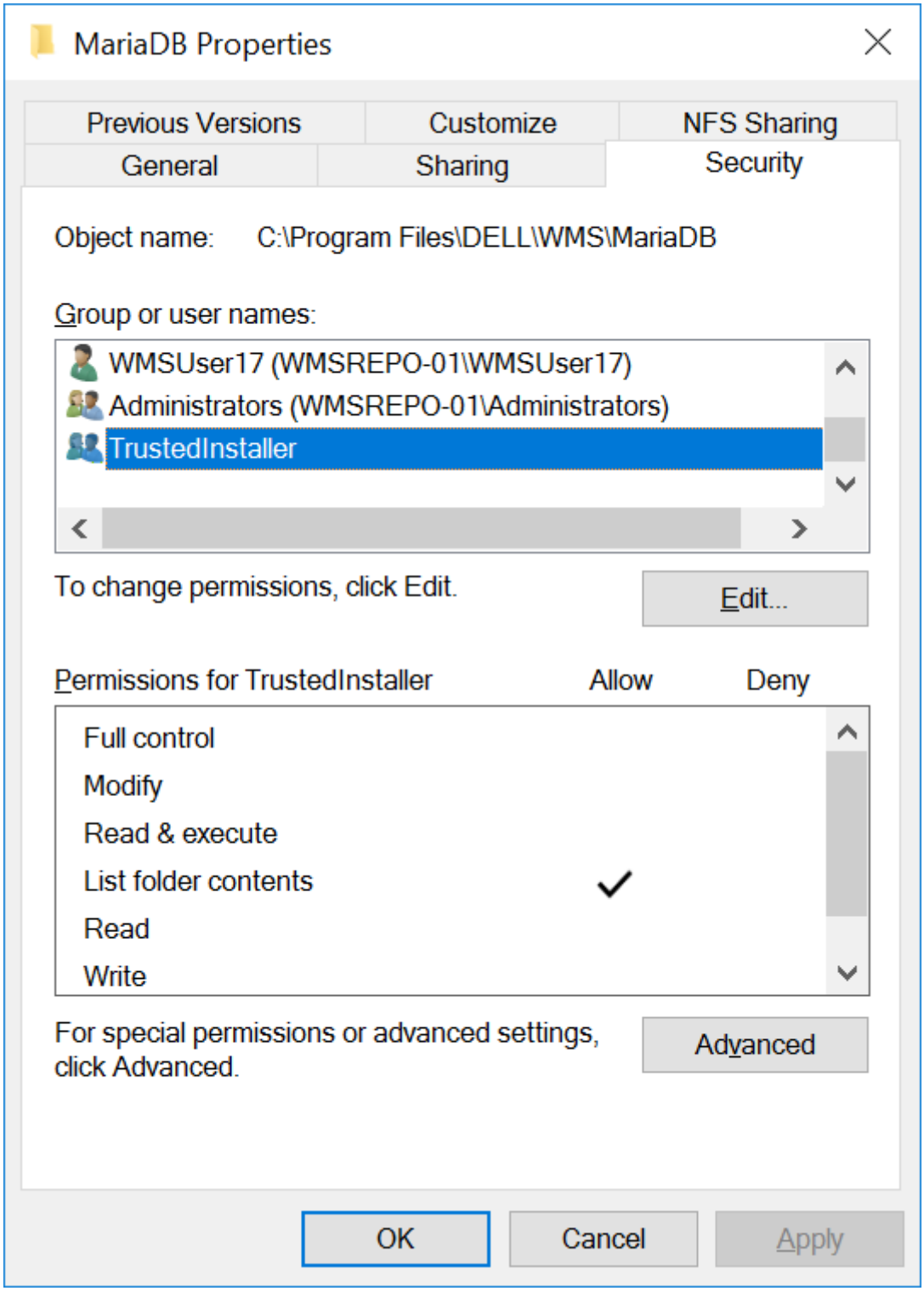


Figure 32. Select TrustedInstaller

NOTE: If the restricted user belongs to any other group, he has the group-related permissions. Revoke permissions as required.

7. Click the **Convert inherited permissions into explicit permissions on this object** option, and click **OK**.

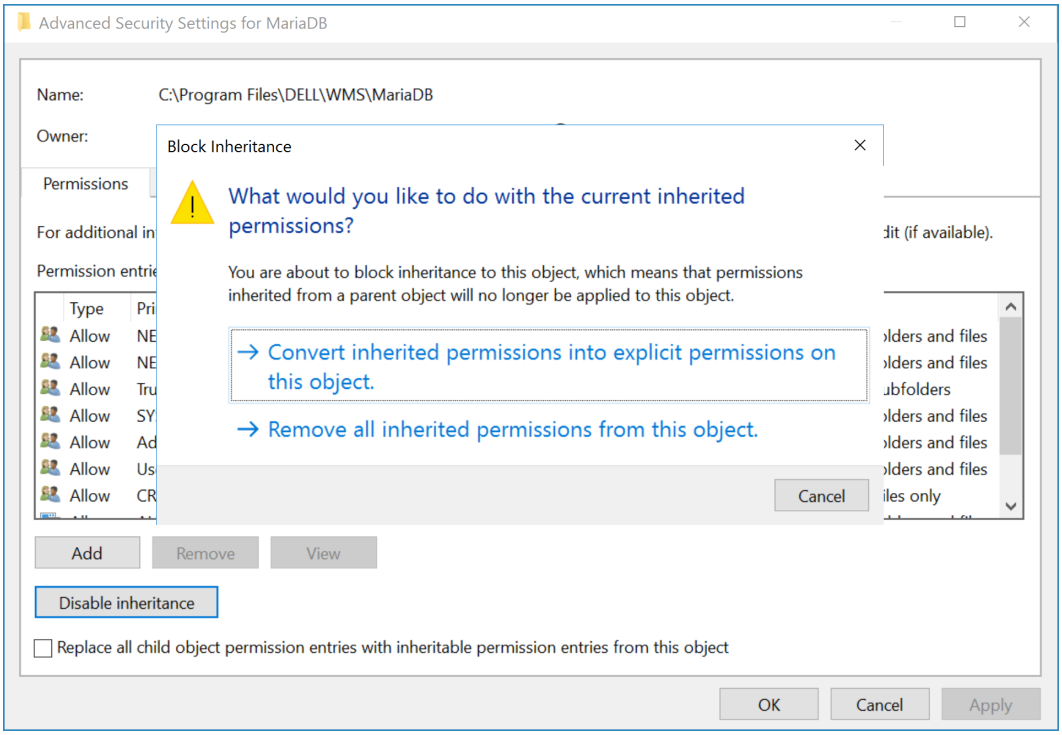


Figure 33. Block inheritance

8. Go to the **Security** tab, click **Edit**, select the user that you want to remove access to the MariaDB service, and click **Remove**.
9. Select the users that you want to remove access to the MariaDB service and click **Remove**.
   If you log in with any other local user, the following screenshot is displayed.

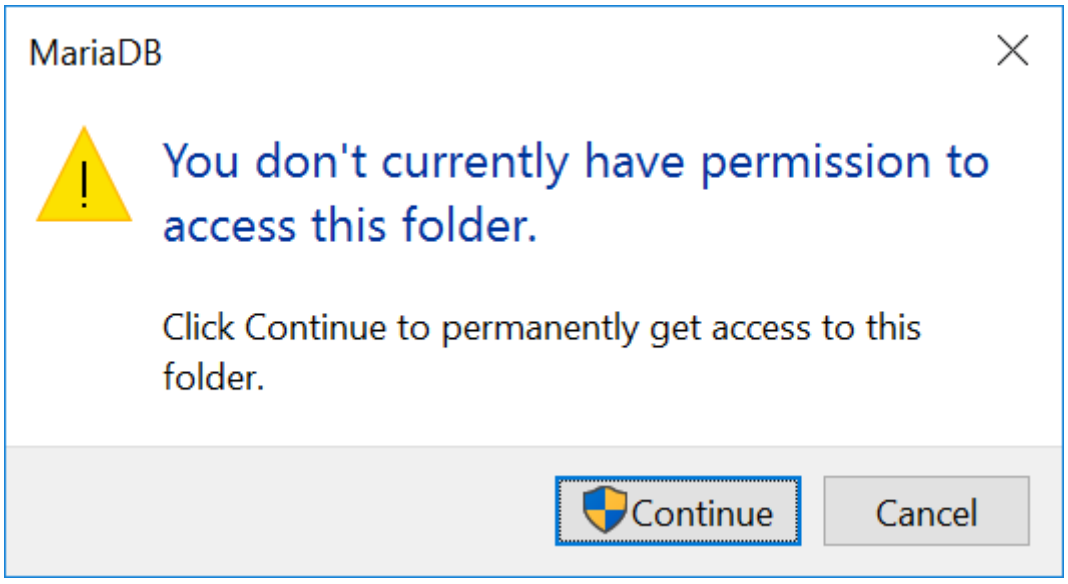


Figure 34. User restricted

Disable local_infile parameter

The local_infile parameter defines whether the files that are located in the MySQL client device can be loaded or selected using the LOAD DATA INFILE or SELECT local_file.

Steps

1. Log in to the MariaDB shell.

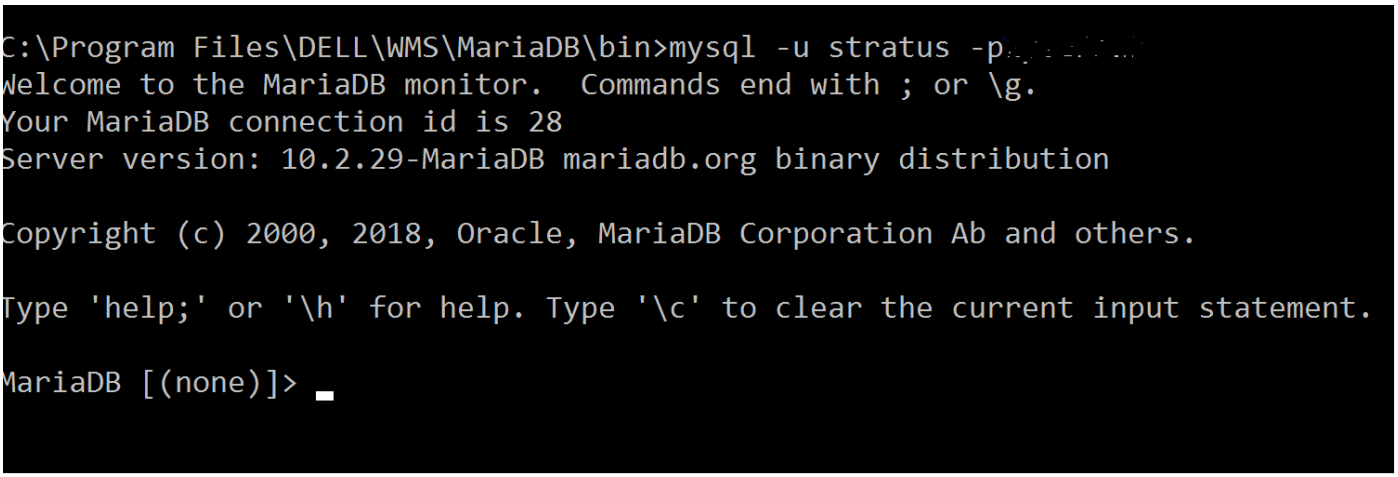


Figure 35. MariaDB shell

2. Switch to the stratus schema using the following command:

```
use stratus;
```

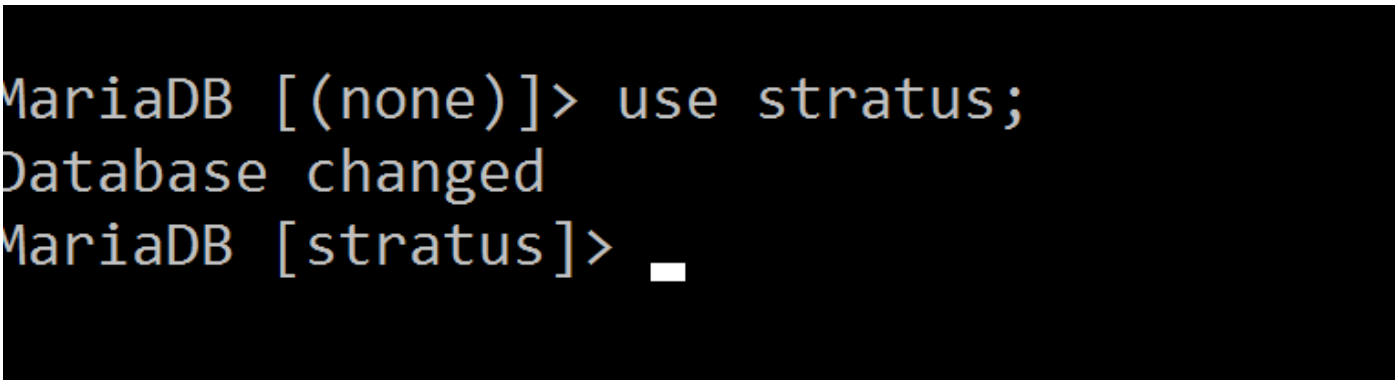


Figure 36. Stratus schema

3. Run the following command to identify the loca_infile value from the Wyse Management Suite schema:

```
SHOW VARIABLES WHERE Variable_name = 'local_infile';
```

```
MariaDB [stratus]> SHOW VARIABLES WHERE Variable_name = 'local_infile';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| local_infile  | ON    |
+---------------+-------+
1 row in set (0.00 sec)

MariaDB [stratus]>
```

Figure 37. Local infile value

4. Verify the `local_infile` value.
   If the value is ON, go to step 5.
5. Right-click **Dell WMS: MariaDB** and click **Properties**.
6. Go to the path mentioned in the **Path to executable** field.
7. Open the my.ini file and paste the following configuration after `[mysqld]`:

```
local-infile=0
```

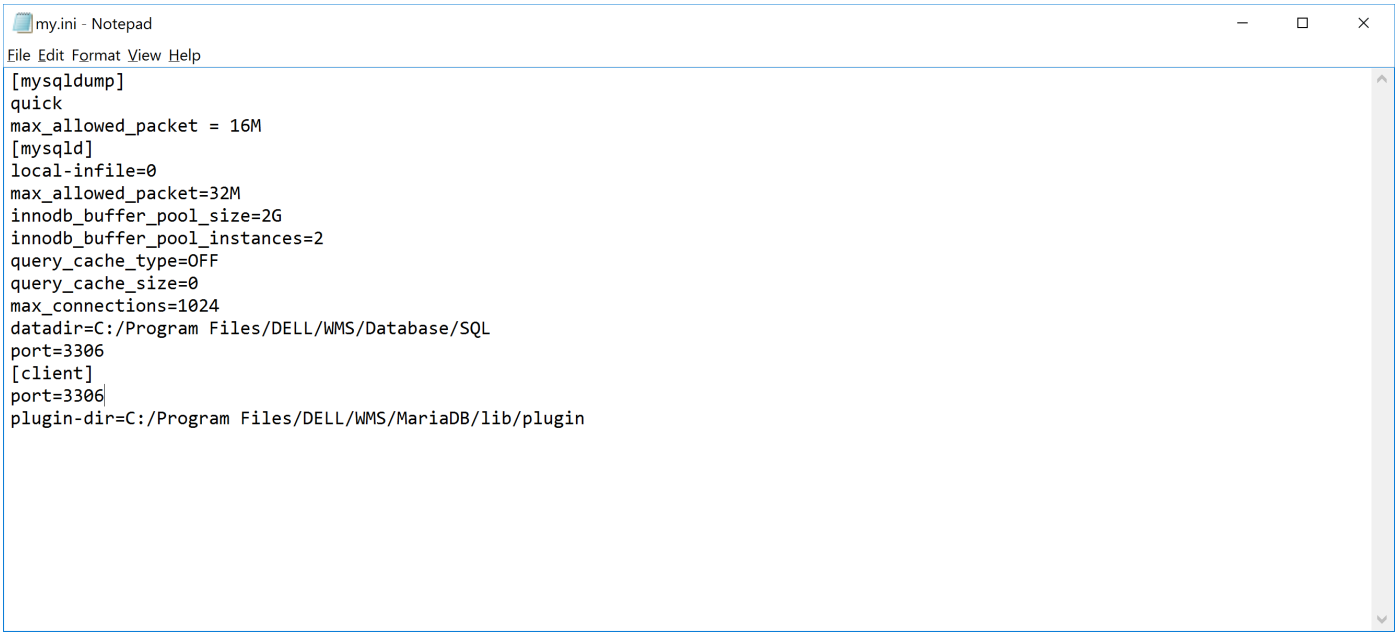


Figure 38. My.ini file

8. Go to **Start** > **Services** and right-click **Dell WMS: MariaDB**.

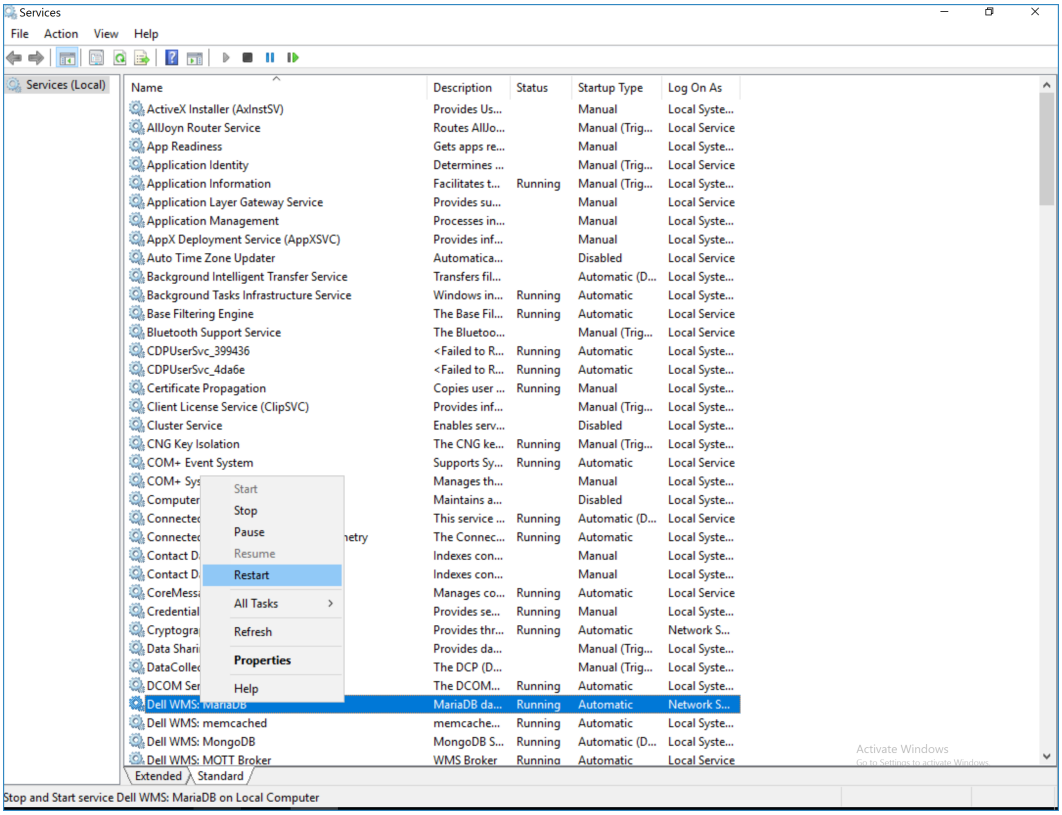


Figure 39. Restart MariaDB

9. Click **Restart**.
   When you restart the MariaDB services, you are prompted to restart Tomcat services.

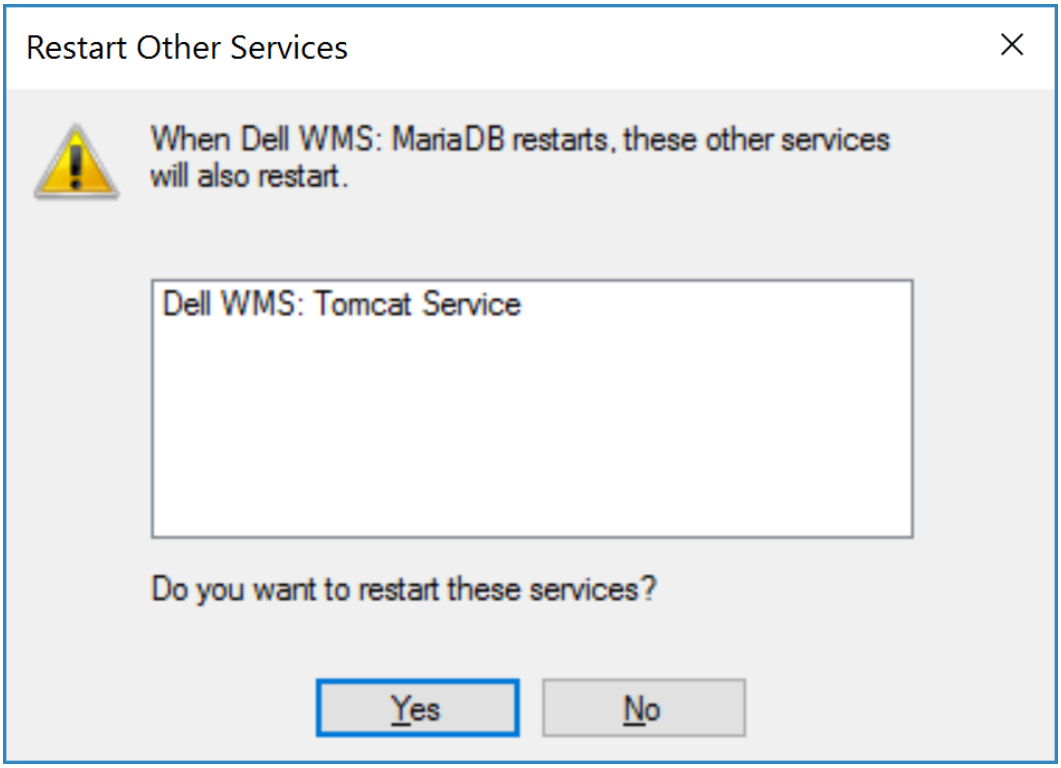


Figure 40. Restart Tomcat services

10. Click **Yes** in the **Restart Other Services** window.

Next steps

1. Log in to the MySQL shell.
2. Switch to the stratus schema using the following command:

```
--use stratus;
```

3. Run the following command to identify the loca_infile value from the Wyse Management Suite schema:

```
SHOW VARIABLES WHERE Variable_name = 'local_infile';
```

The `local_infile` value must be OFF instead of 0. In shell you cannot put 0 as value.

4

Server hardening for OpenJDK

This chapter contains security hardening rules to secure your OpenJDK Adoptium temurin 17.x that are deployed with Wyse Management Suite.

Topics:

Grant permissions

Steps

1. Go to the **conf** folder in the Tomcat installation directory after you install Wyse Management Suite and stop the tomcat service.

   The default **conf** folder location is `C:\Program Files\DELL\WMS\Tomcat-10`.

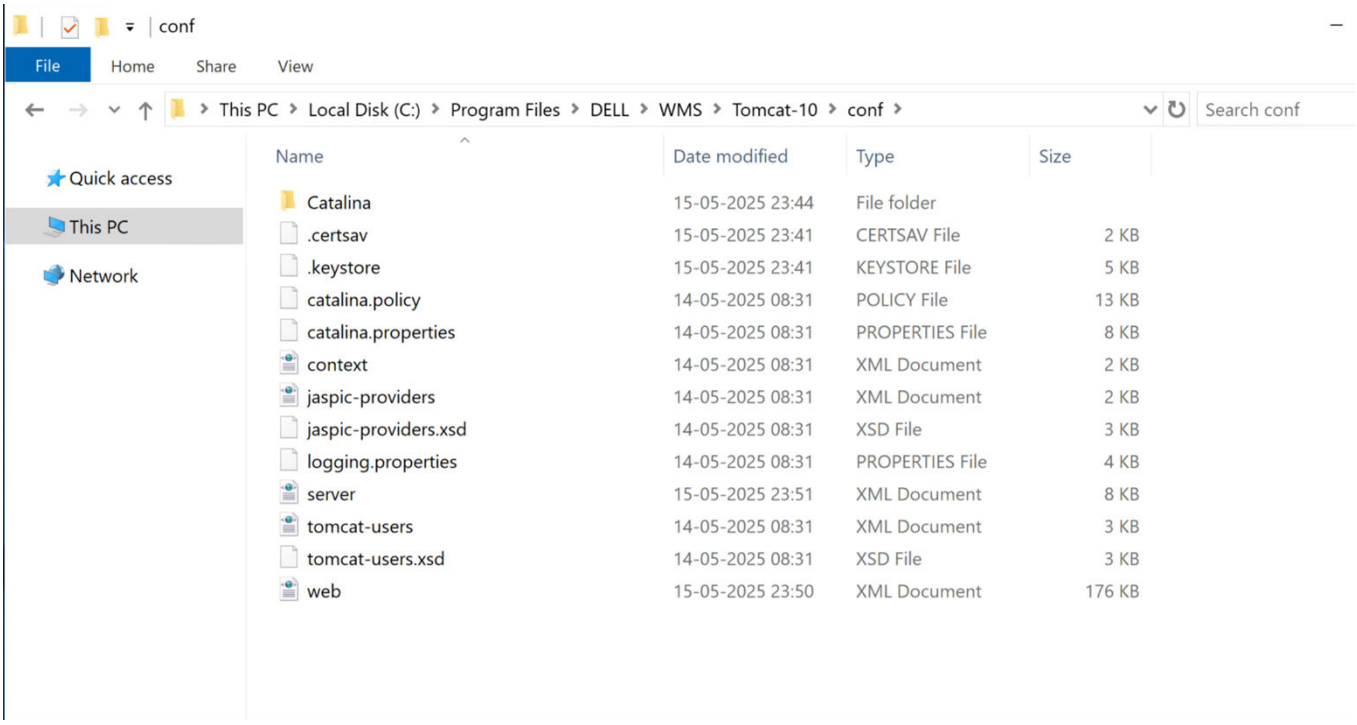


Figure 41. conf folder location

2. Right-click the **catalina.policy** file and open it in any editor.

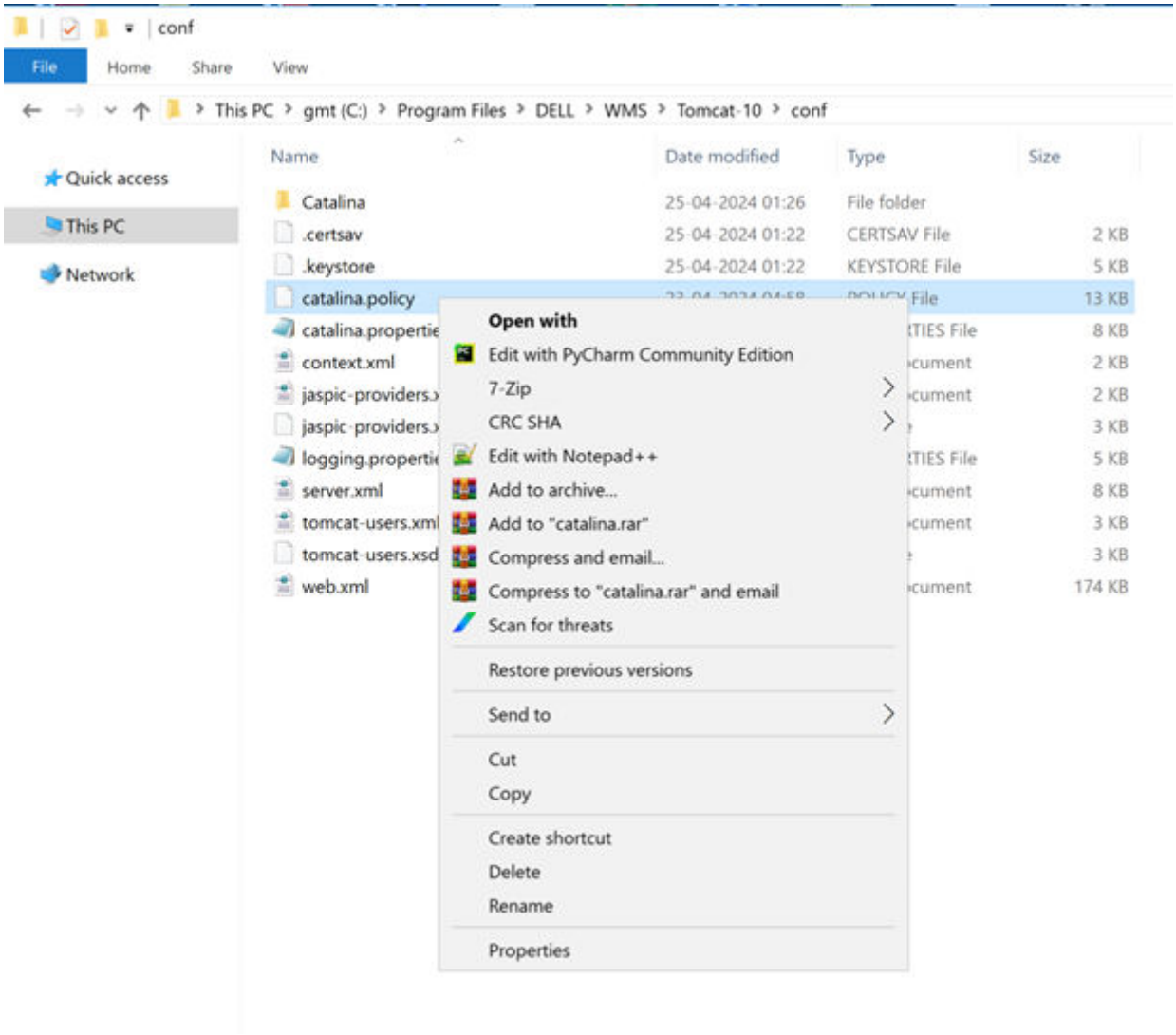


Figure 42. Right-click options

The default permissions are provided in the **catalina.policy** file.

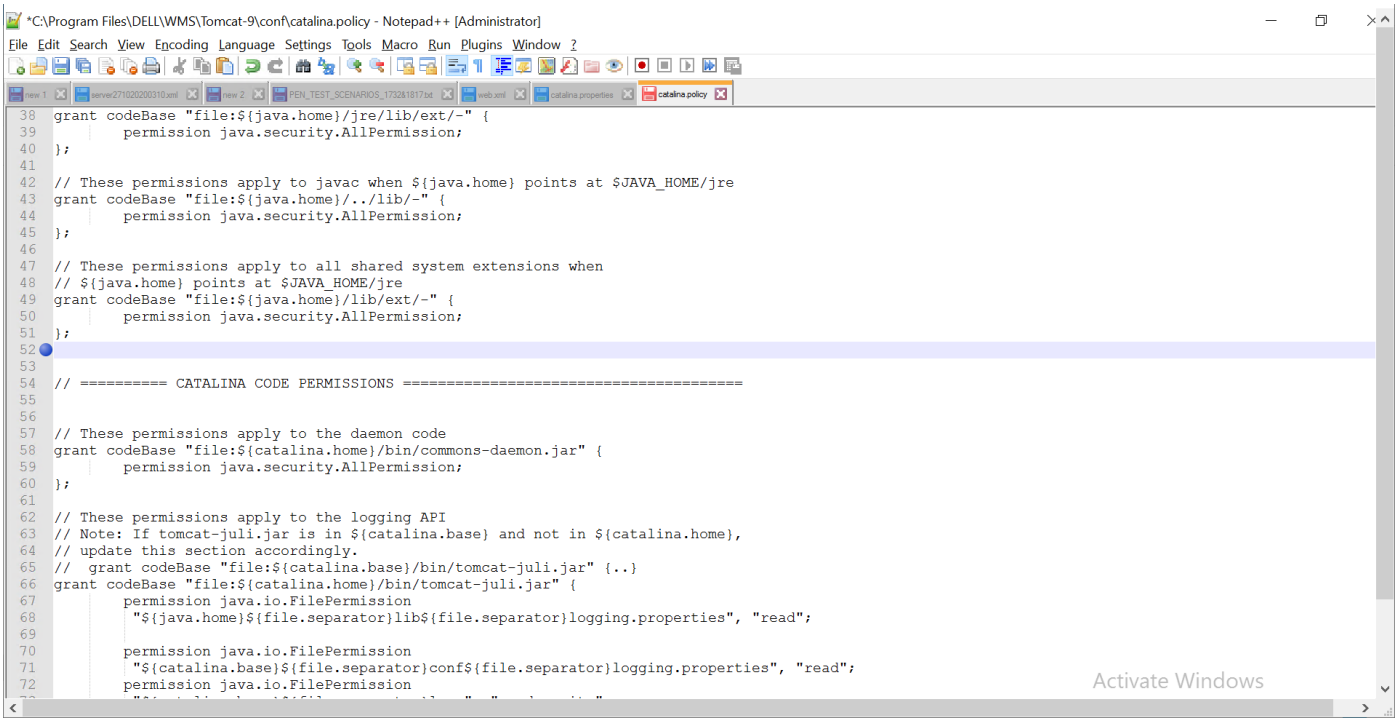


Figure 43. Default permissions

3. Update runtime permissions for packages `org.apache.tomcat.util.buf &` `org.apache.tomcat.util.descritptor.web` as mentioned in the below format:

```
permission java.lang.RuntimePermission
"accessClassInPackage.org.apache.tomcat.util.buf";
    permission java.lang.RuntimePermission
accessClassInPackage.org.apache.tomcat.util.descriptor.web";
```

- Use the following to grant permission to webapps to run the applications:

```
grant codeBase "file:${catalina.home}/webapps/-" { permission
java.security.AllPermission; };
```

- Use the following for JDK permissions:

```
grant { permission java.io.FilePermission "${java.home}${file.separator}conf$
{file.separator}security${file.separator}java.security", "read"; };
grant { permission java.io.FilePermission "${java.home}${file.separator}conf$
{file.separator}security${file.separator}java.policy",
"read,write,delete"; };
```

4. Save and close the editor.
   Restart Tomcat in secure mode to enable the configurations.

   NOTE: See Start Tomcat Service in secure mode if your Tomcat server is not running in secure mode. If Tomcat is already running in secure configuration mode, you can ignore the steps.

Start Tomcat Service in secure mode

Steps

1. Open the **Run** box, type **`services.msc`** and click **OK**.

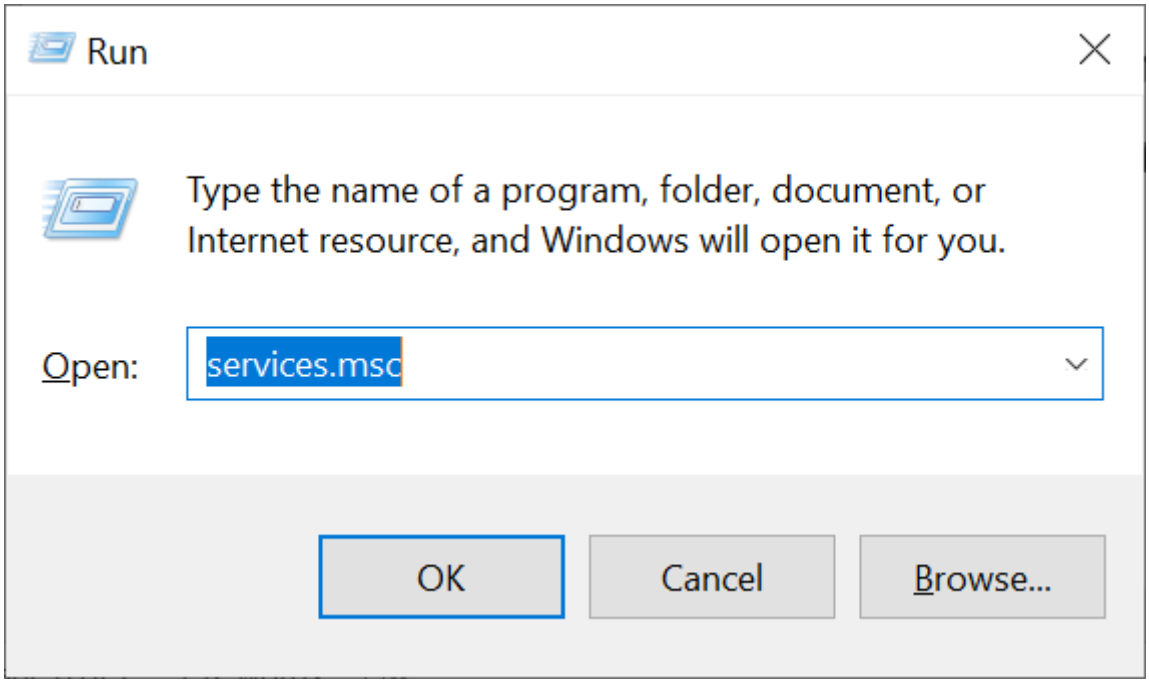


Figure 44. Run

The **Services** windows is displayed.

2. Right-click **Dell WMS: Tomcat Service** and click **Stop**.

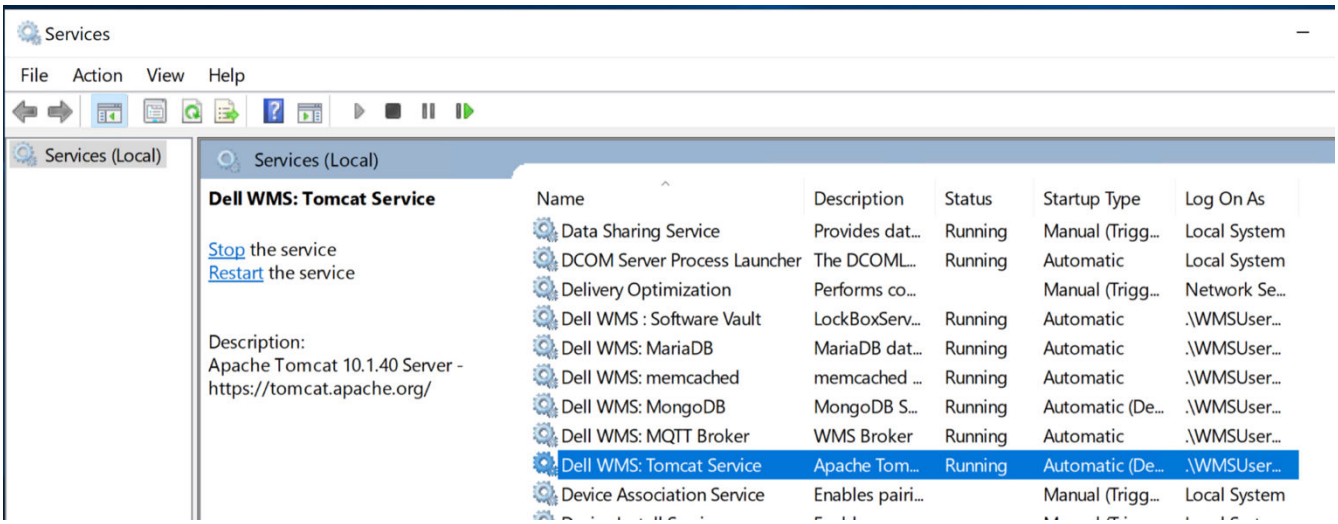


Figure 45. Services

3. Go to the Tomcat directory and open the **bin** folder.
   The default Tomcat directory location is `C:\Program Files\DELL\WMS\Tomcat-10`.

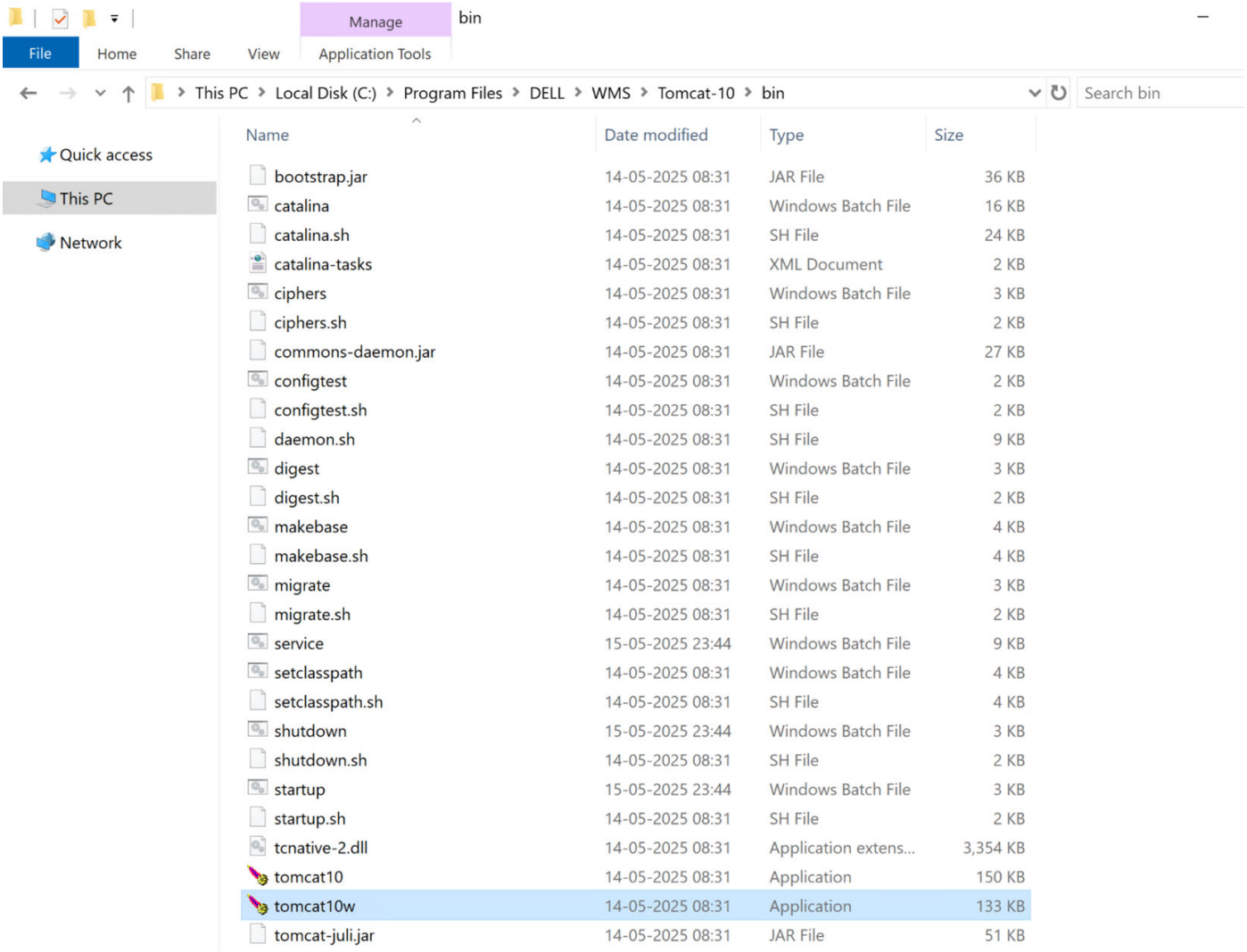


Figure 46. Tomcat directory

4. Double-click **Tomcat10w.exe**.
   The **Dell WMS: Tomcat Service Properties** window is displayed.
5. Go to the **Java** tab.
6. Add the following lines in the **Java Options** section:

```
-Djava.security.manager
-Djava.security.policy=C:\Program Files\DELL\WMS\Tomcat-10\conf\catalina.policy
```

NOTE: The path for **catalina.policy** is the default **conf** folder path of Tomcat after you install Wyse Management Suite in an on-premises environment.

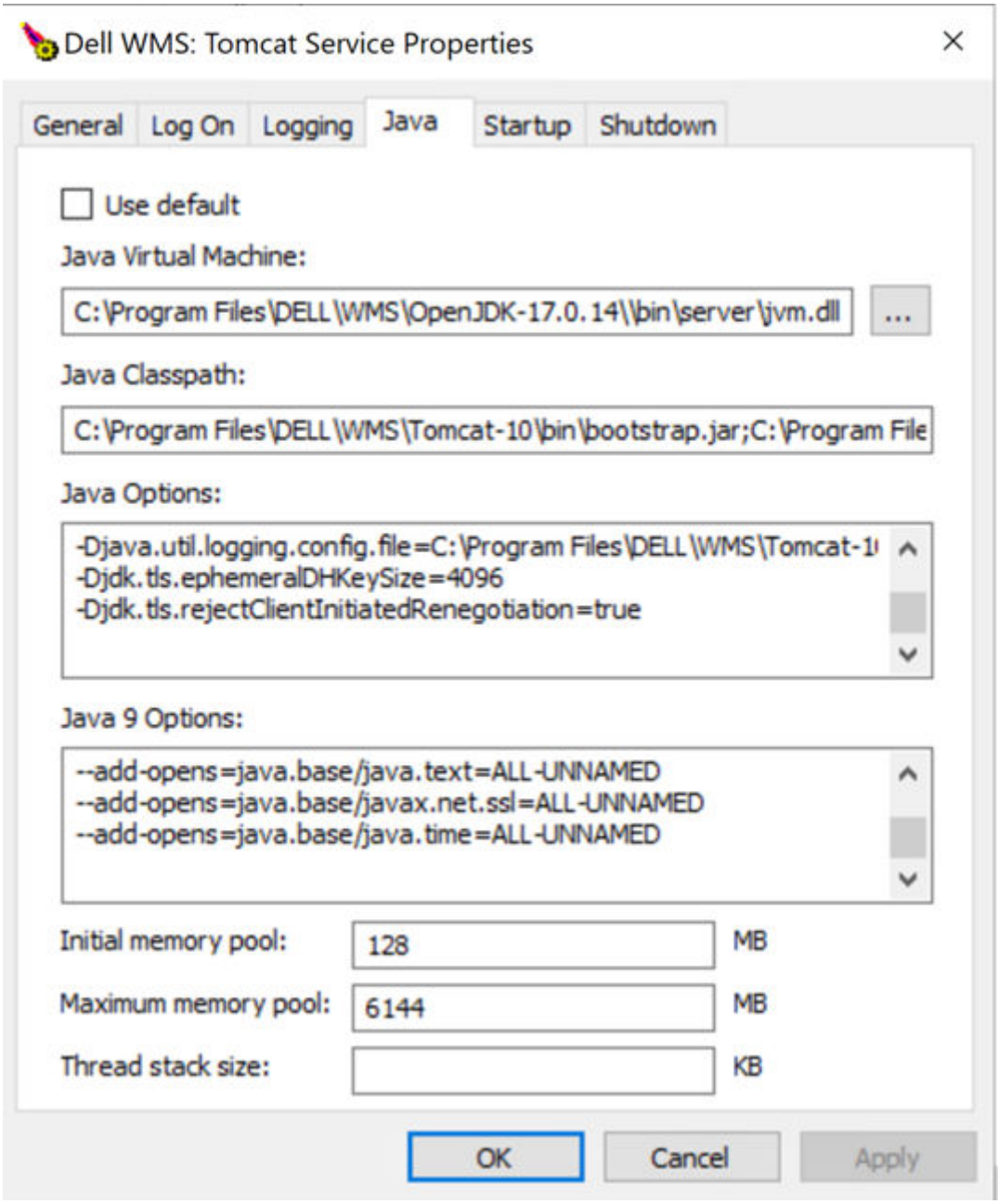


Figure 47. Java options

7. Click **Apply** and click **OK**.
8. Open the **Run** box, type **`services.msc`** and click **OK**.
9. Right-click **Dell WMS: Tomcat Service** and click **Start**.
   The Tomcat Service initiates.

Restrict access to OpenJDK resources

You must access the OpenJDK service using an administrator account. If all users have access to the OpenJDK service, they can access the configuration files and the data directories. Dell Technologies recommends restricting access to a user account that is used for Wyse Management Suite installation and configuration. The following steps ensure that the OpenJDK resources are not accessible to other users.

Steps

1. Log in to the server where Wyse Management Suite is installed.

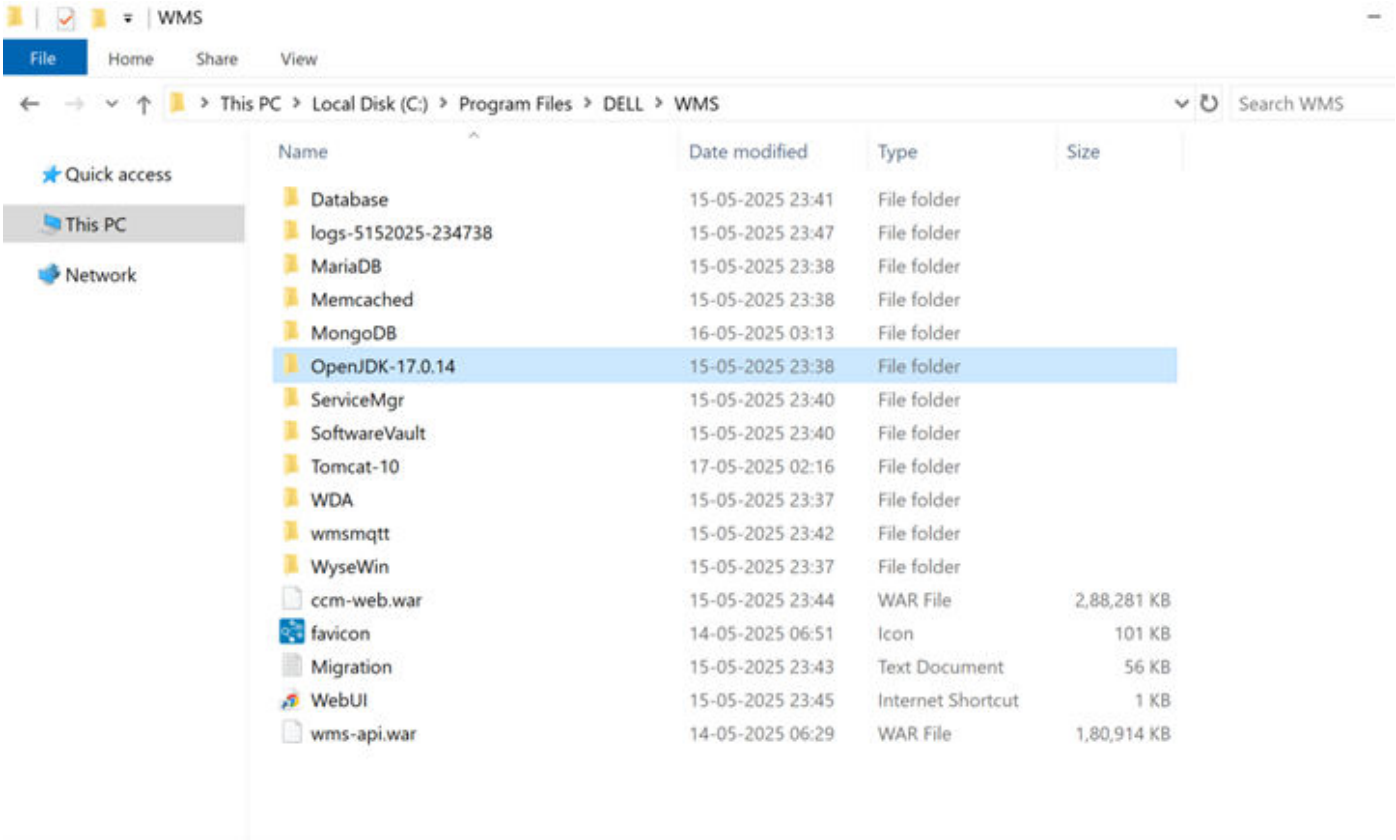


Figure 48. Wyse Management Suite installation directory

2. Go to the Wyse Management Suite installation directory.
3. Right-click **OpenJDK-17.x.x** and click **Properties**.
   OpenJDK-17.x.x Properties window is displayed.
4. Go to the **Security** tab and click **Advanced**.

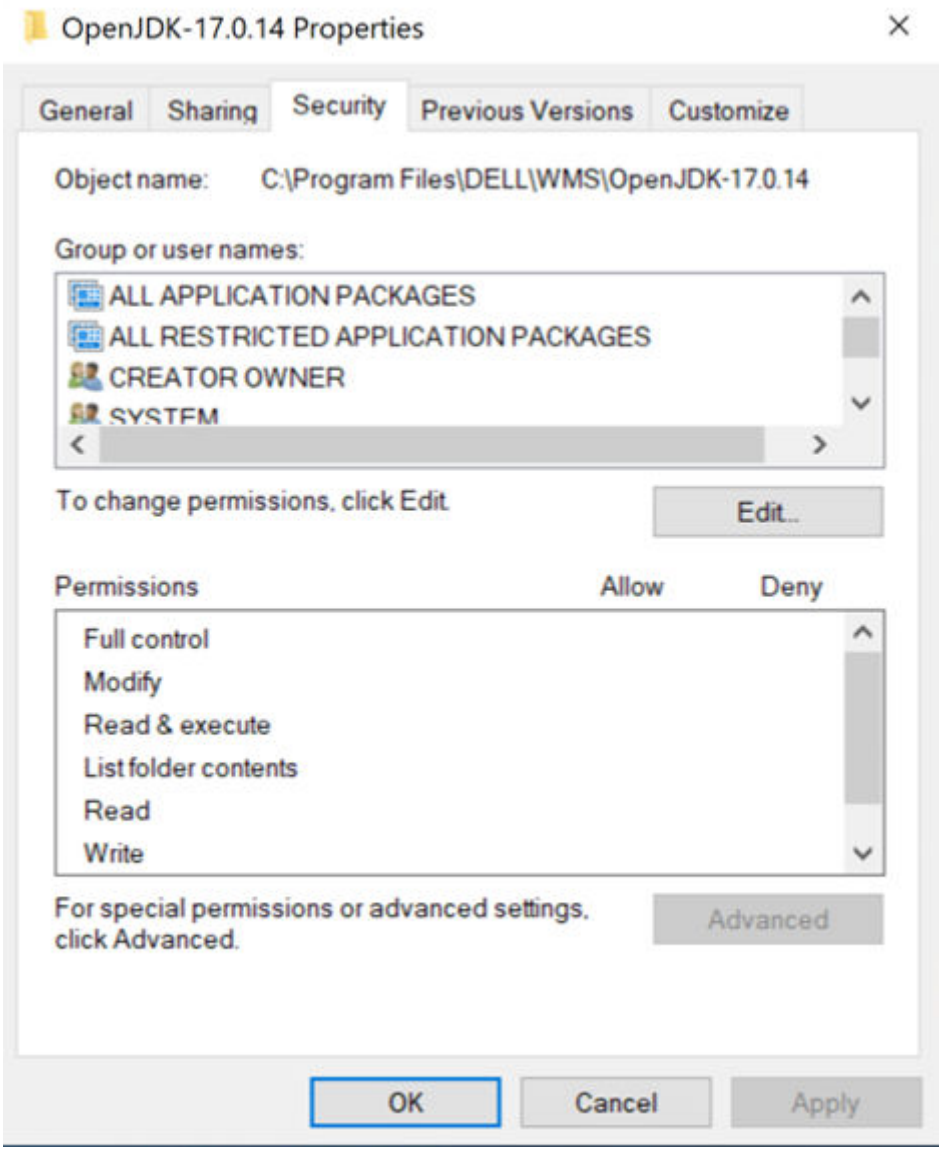


Figure 49. OpenJDK-17.x.x Properties

Advanced Security Settings for OpenJDK-17.x.x window is displayed.

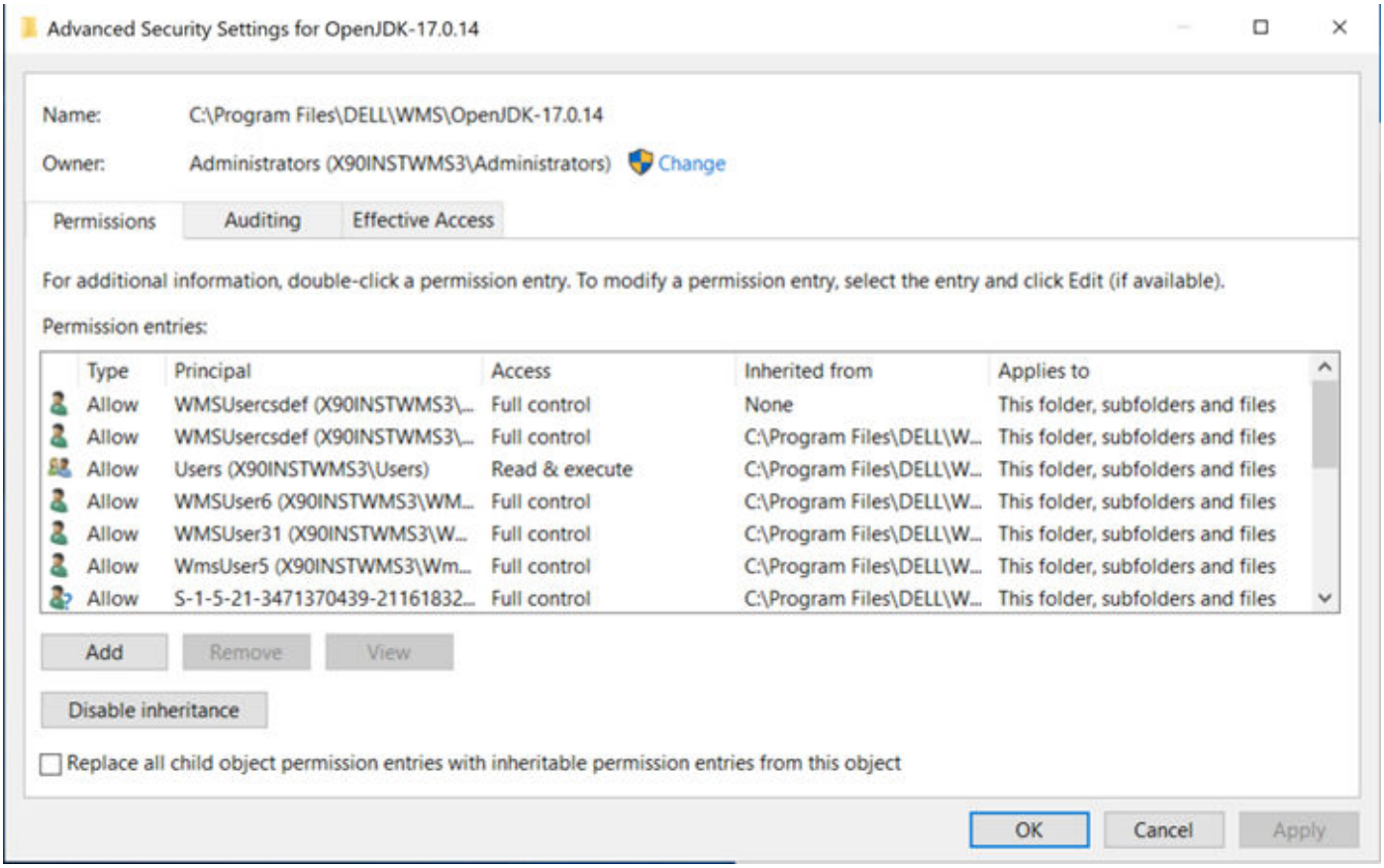


Figure 50. Advanced Security Settings for OpenJDK-17.x.x

5. Click **Disable inheritance**.
   The **Block Inheritance** window is displayed.

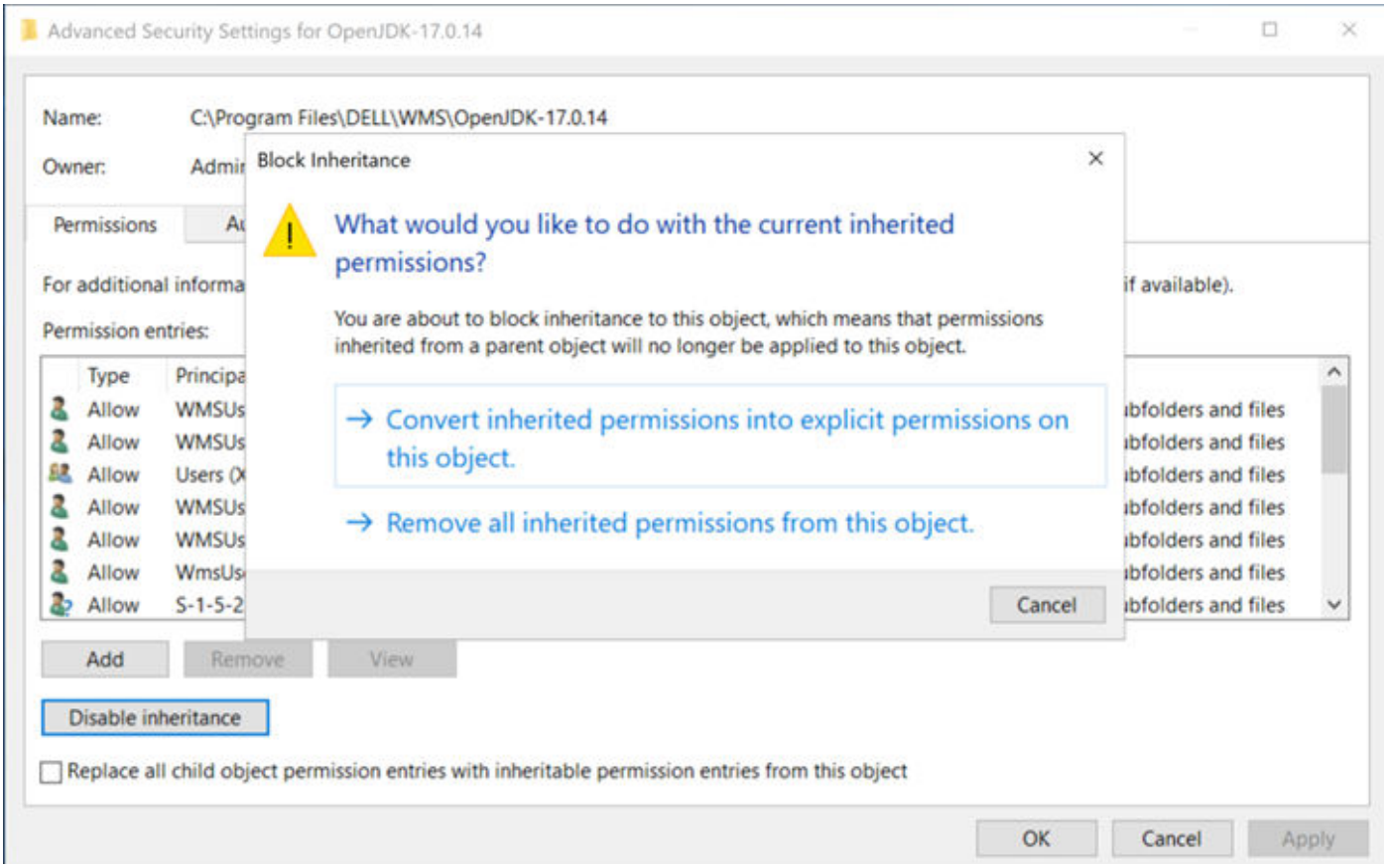


Figure 51. Block inheritance

NOTE: By default, inheritance is enabled which restricts the altering of permissions to the folder.

6. Click the **Convert inherited permissions into explicit permissions on this object** option.
7. Select the users that you want to remove access to the OpenJDK-17.x.x service and click **Remove**.

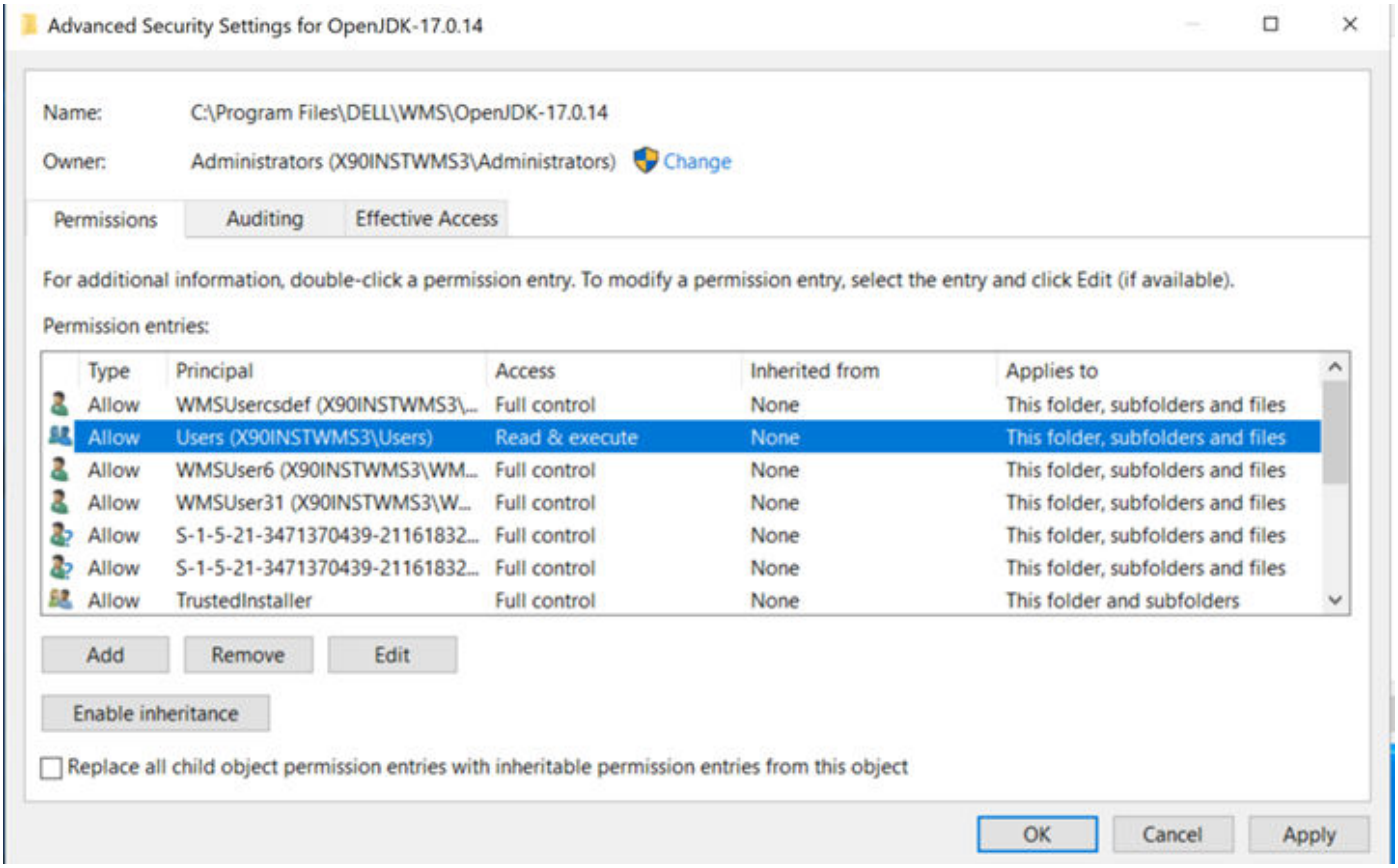


Figure 52. Remove user

8. Verify the changes by logging out from the server and logging in again using the removed user credentials. You must be denied access to the OpenJDK-17.x.x folder—This step is optional.

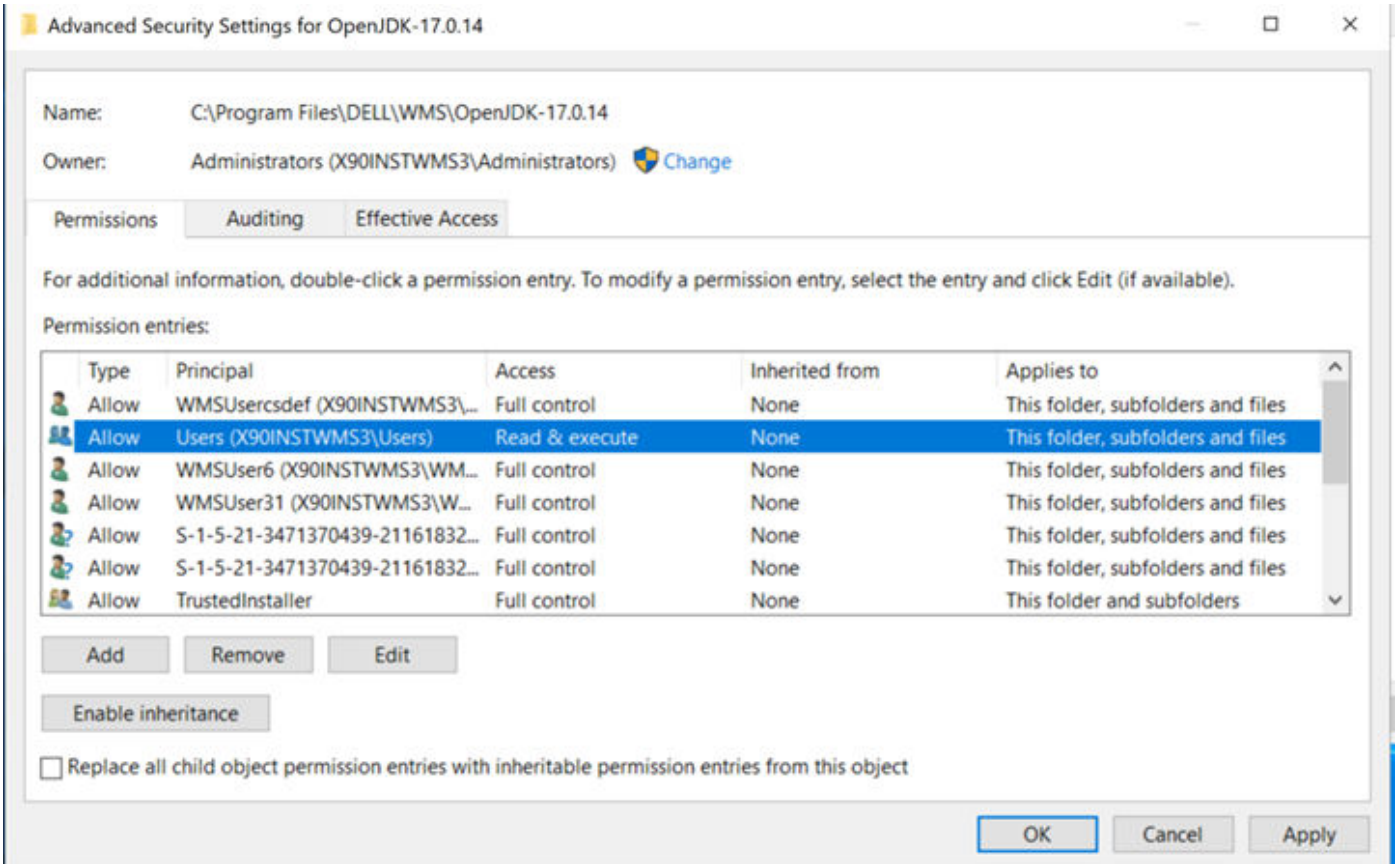


Figure 53. Verify the user deletion

5

Tomcat server hardening

Steps

1. Log in to the server where Wyse Management Suite is installed.
2. Go to the Wyse Management Suite installation directory and go to `\Tomcat-10\conf`.
   The default path is `C:\Program Files\DELL\WMS\Tomcat-10\conf`.

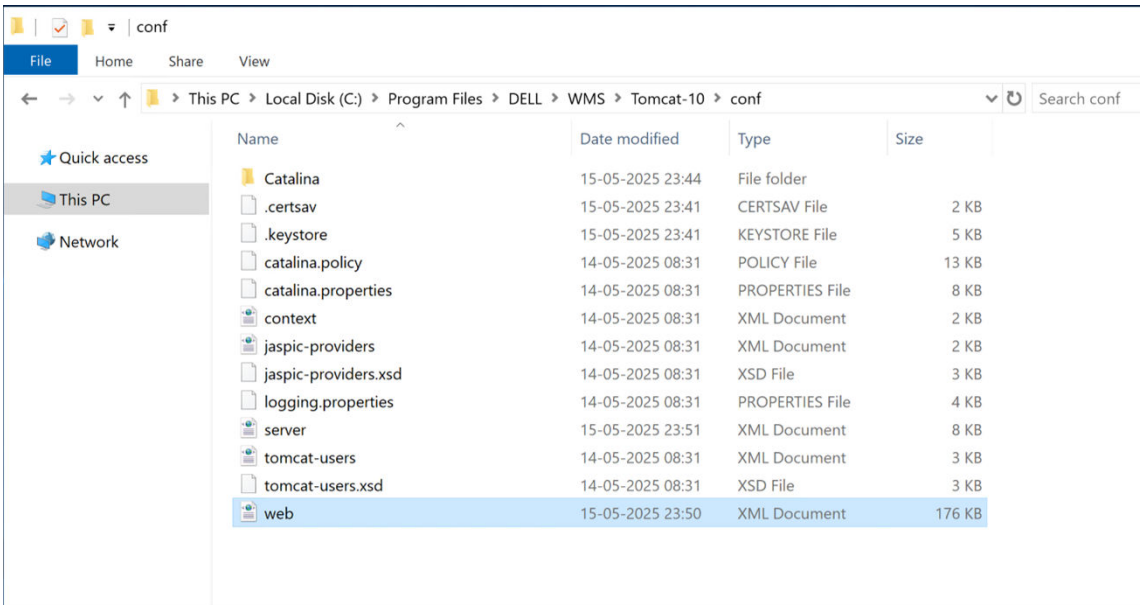


Figure 54. Tomcat Conf

3. Right-click the Web.xml file and edit the file.
4. Add the following code to the file and click **Save**.

```
<error-page>
<exception-type>java.lang.Throwable</exception-type>
<location>/error.jsp</location></error-page>
```

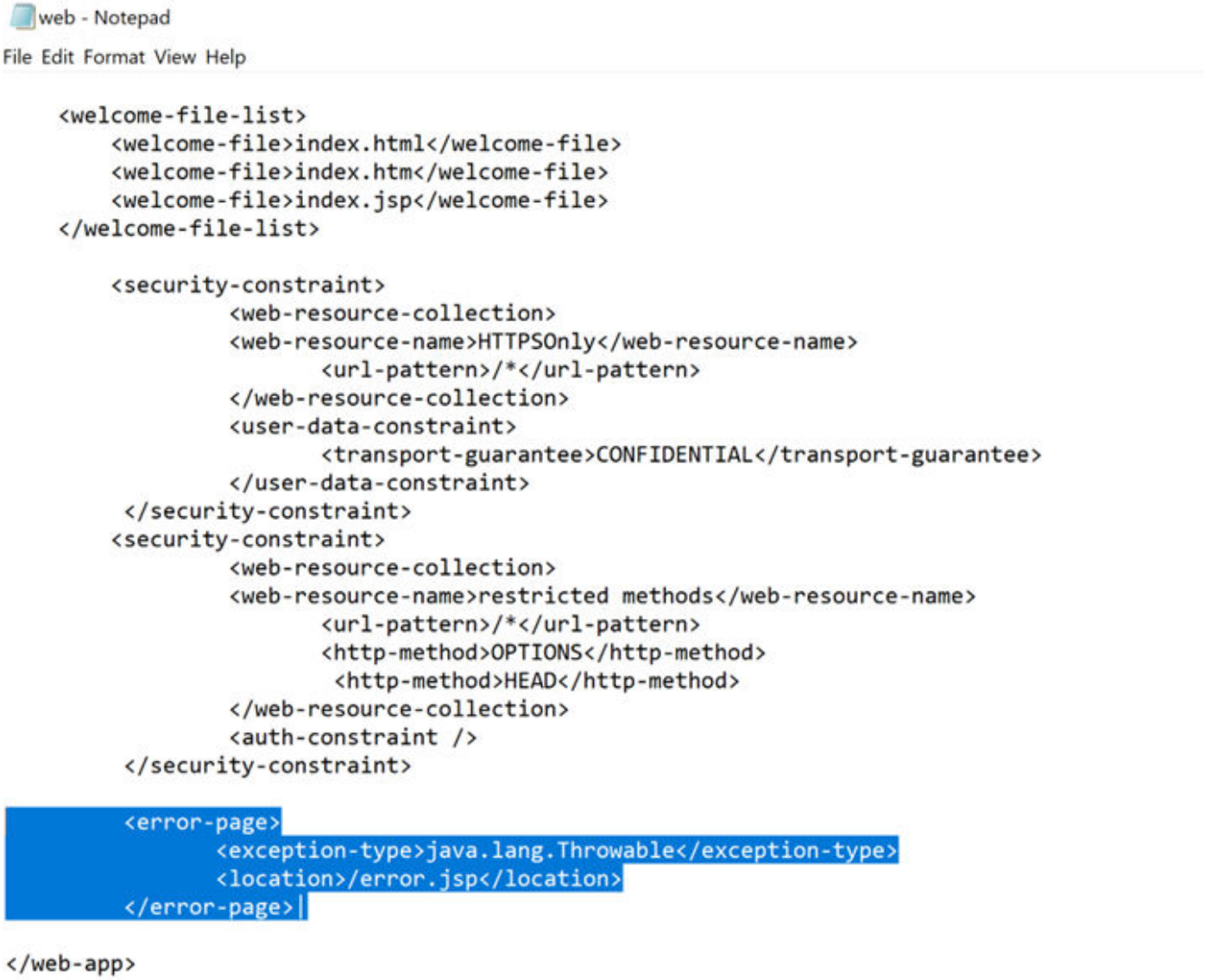


Figure 55. Error page code

5. Go to the Wyse Management Suite installation directory and go to `\Tomcat-10\conf`.
   The default path is `C:\Program Files\DELL\WMS\Tomcat-10\conf`.

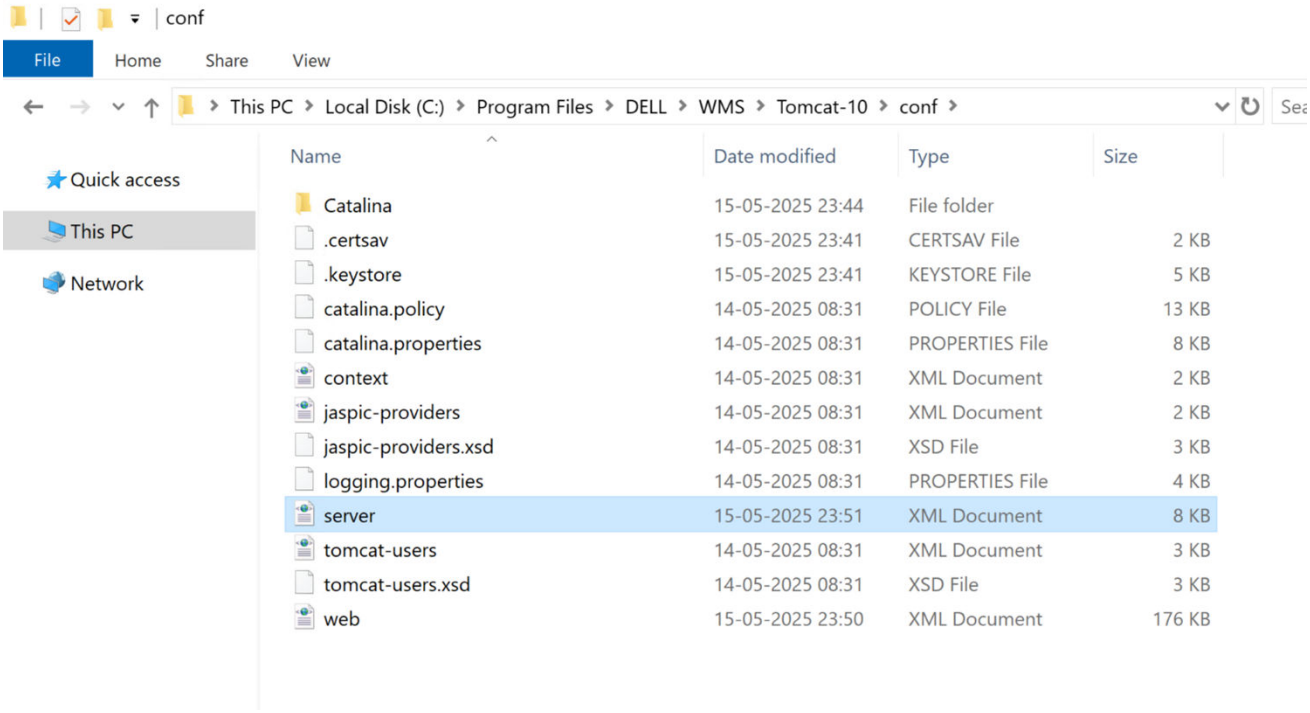


Figure 56. Server xml file

6. Right-click the Server.xml file and edit the file.
7. Update the <Server> tag to disable the shutdown port by setting it to **-1**.

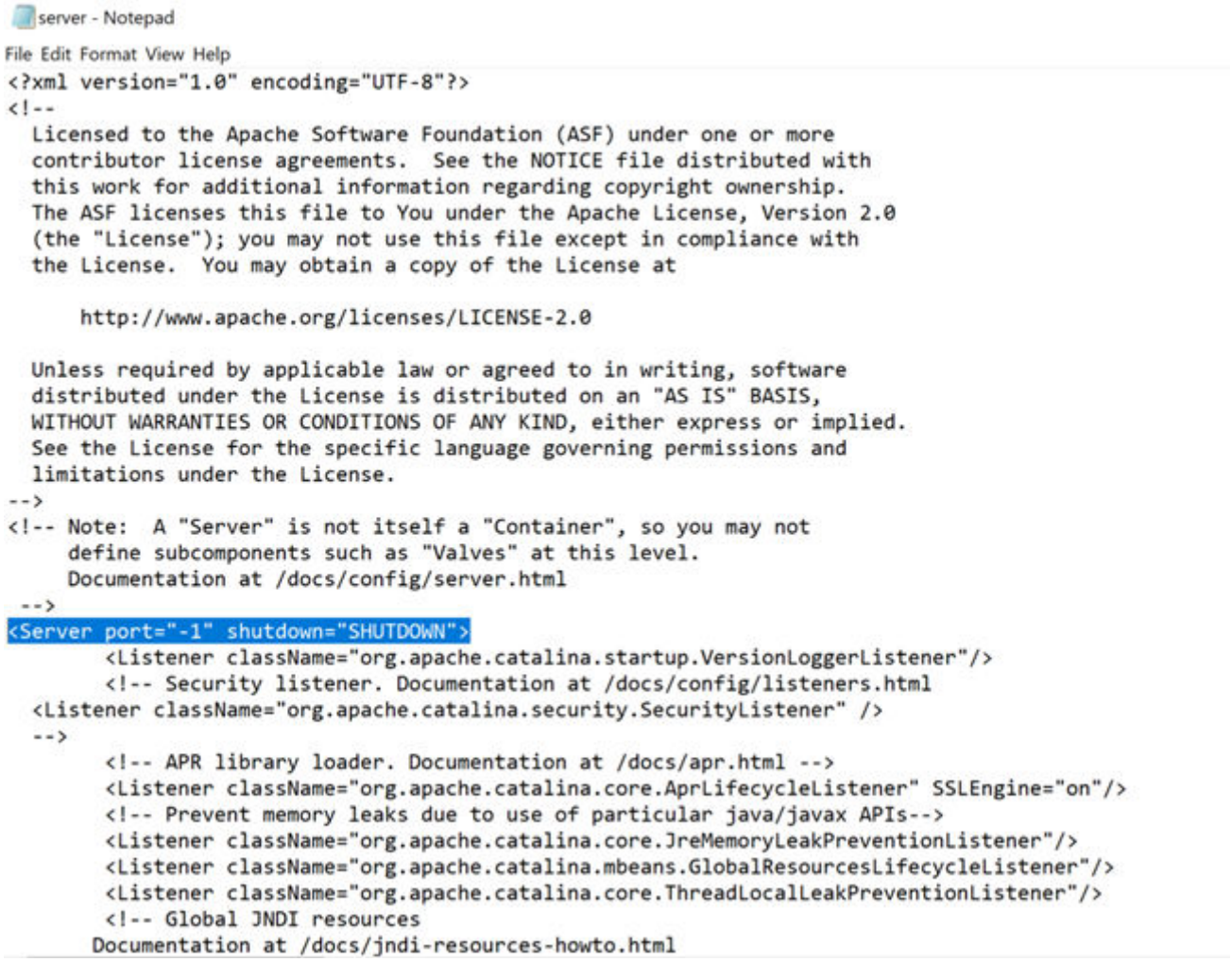


Figure 57. server code update

8. In the <Connector> tag, add the attribute **`allowTrace="false"`** and save the file.

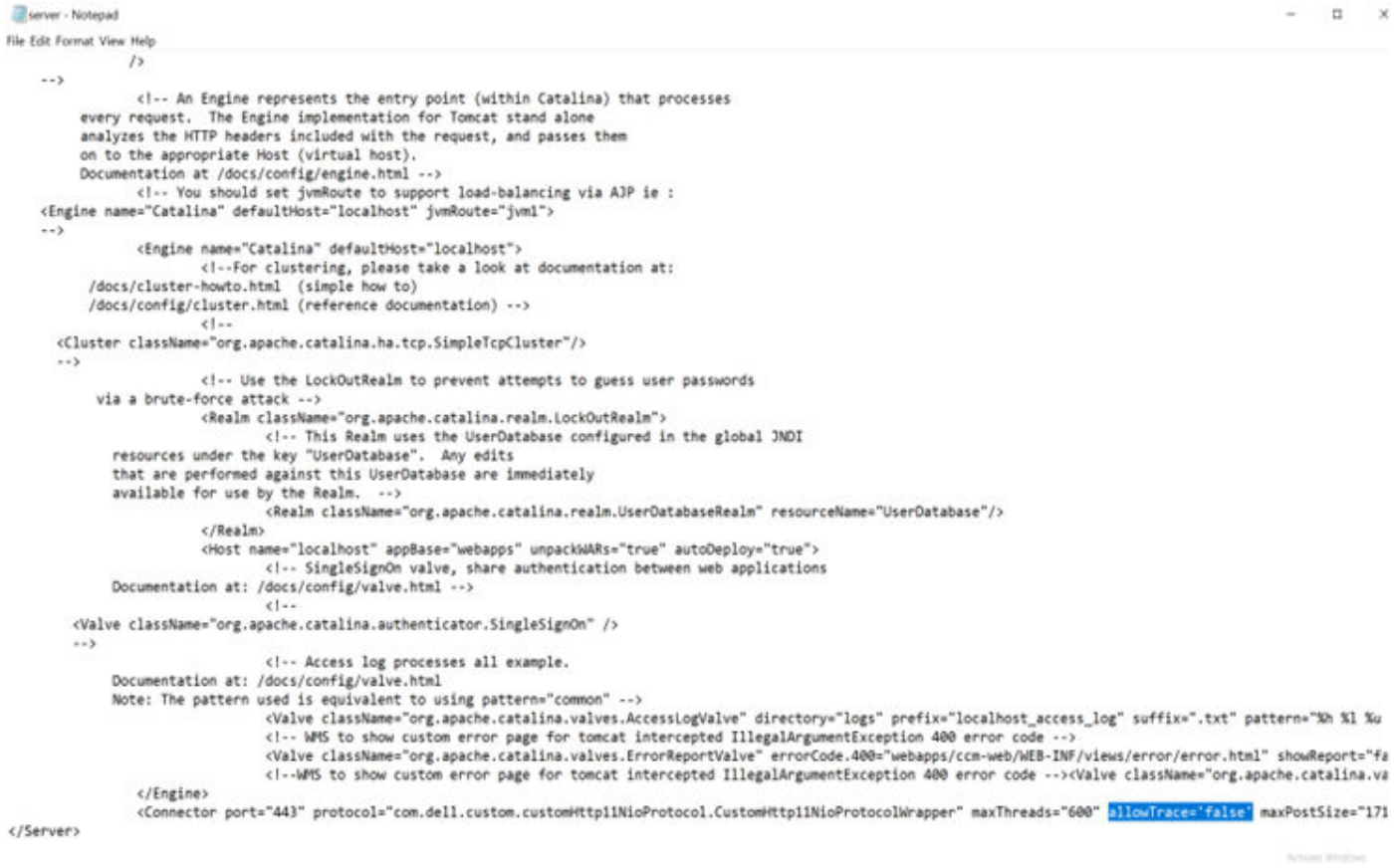


Figure 58. Updated server.xml file

NOTE: Ensure to update the value within the existing Connector tag and do not remove other required attributes.

9. Go to **Start** > **Services** and right-click **Dell WMS: Tomcat Service**.
10. Restart the service.

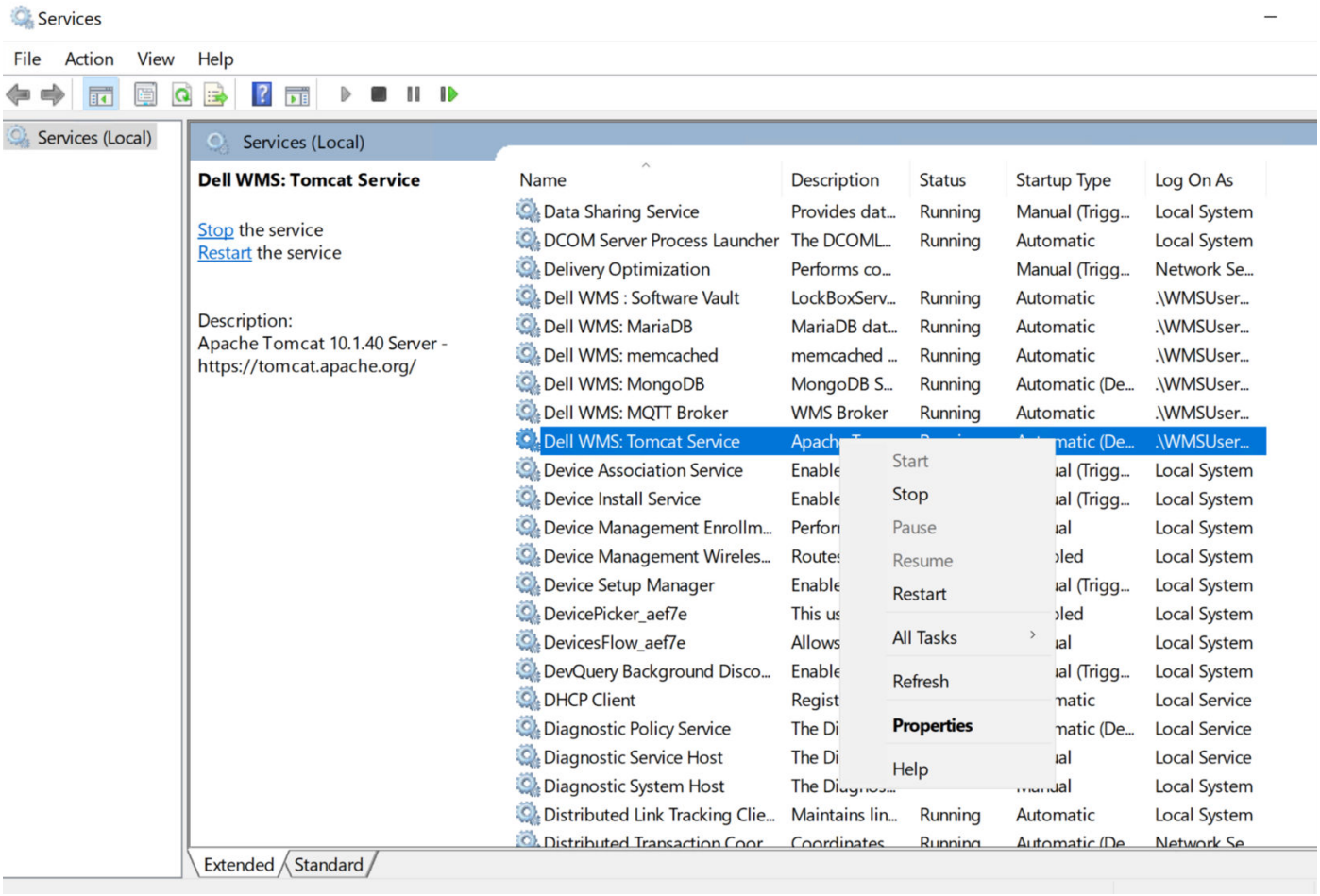


Figure 59. Restart the Tomcat service

NOTE: The Tomcat hardening updates are configured by default as part of Wyse Management Suite version 5.3 on-premises and Wyse Management Suite Repository version 5.3.

6

Server hardening for VNC

Due to vulnerabilities detected from the VNC application, the application deployment is restricted from Wyse Management Suite.