



# **Symantec Data Loss Prevention v14.0.1 Backup Guide**

Prepared By  
**Sequaretek IT Solution Pvt. Ltd.**



## Table of Contents

Sr. No	Content	Page No
1	About backup and recovery on Windows	3
2	Recommendations	4
3	Calculating the total size of the backup on Windows	4
4	Calculating the size of database	5
5	Calculating the size of File System	7
6	Calculating the size of Server Configuration:	9
7	Creating backup directories on Windows	10
8	Performing a cold backup of the Oracle database on Windows	10
9	To generate a trace file of the control file	12
10	Collecting a list of files to be backed up	14
11	Creating a copy of the spfile on Windows	15
12	Shutting down the Symantec DLP system on Windows	16
13	Copying the database files to the backup location on Windows	18
14	Restarting the system on Windows	19
15	Backing up the server configuration files on Windows	20
16	Backing up files stored on the file system on Windows	20
17	The Windows recovery information worksheet	21



## About backup and recovery on Windows

Symantec recommends that administrators perform backups of their entire system.

Perform system backups in case the Symantec Data Loss Prevention system crashes and needs to be restored.

The system that should be backed up includes the Enforce Server, the detection servers, the database, and the incident attachment external storage directory, if present.

These backup procedures can be used for single-tier, two-tier, and three-tier installations.

The cold backup procedures for the Oracle database are for non-database Administrators who have no standard backup methods for databases.

Administrators should follow all of the backup instructions that are in this section in the order in which they are presented.

Administrators who would prefer to back up only part of their system must determine which subsets of the system backup instructions to follow.

Symantec recommends that your data storage administrator perform all backups of your incident attachment external storage directories.



## Recommendations:

1. Symantec recommends that administrators perform backups of their entire system.
2. Perform system backups regularly.
3. Complete system backups should be performed at the following times:
  - After installation
  - Before any system upgrades
  - Any time the system changes, such as when a Symantec Data Loss Prevention server is added to or removed from the system configuration

## Calculating the total size of the backup on Windows:

To calculate the total size of the backup

1 Enter the size of the database here: \_\_\_\_133.31 GB

2 Enter the size of the file system files here: \_\_\_\_426 MB + 22.3 MB  
(\SymantecDLP\Protect\plugins,\SymantecDLP\Protect\logs)

3 Enter the size of the server configuration files here: \_\_\_\_483 KB  
(\SymantecDLP\Protect\config)

4 Add the size of the database to the size of the configuration files and file system files for a total size here: \_\_\_\_134 GB Approx



## Calculating the size of the database:

1. Run SQL PLUS as Administrator

2. Perform the following Tasks

Connect to database as SYSDBA

```
SQL Plus
SQL*Plus: Release 11.2.0.4.0 Production on Thu Mar 31 12:00:43 2016
Copyright (c) 1982, 2013, Oracle. All rights reserved.
Enter user-name: sys as SYSDBA
Enter password:
Connected to:
Oracle Database 11g Release 11.2.0.4.0 - 64bit Production
SQL> _
```



## Run The Following Query

```
Administrator: Command Prompt - SQLPLUS
Enter user-name: sys as SYSDBA
Enter password:

Connected to:
Oracle Database 11g Release 11.2.0.4.0 - 64bit Production

SQL> SELECT ROUND(SUM(bytes)/1024/1024/1024, 4) GB
2 FROM (
3 SELECT SUM(bytes) bytes
4 FROM dba_data_files
5 UNION ALL
6 SELECT SUM(bytes) bytes
7 FROM dba_temp_files
8 UNION ALL
9 SELECT SUM(bytes) bytes
10 FROM v$log
11 );

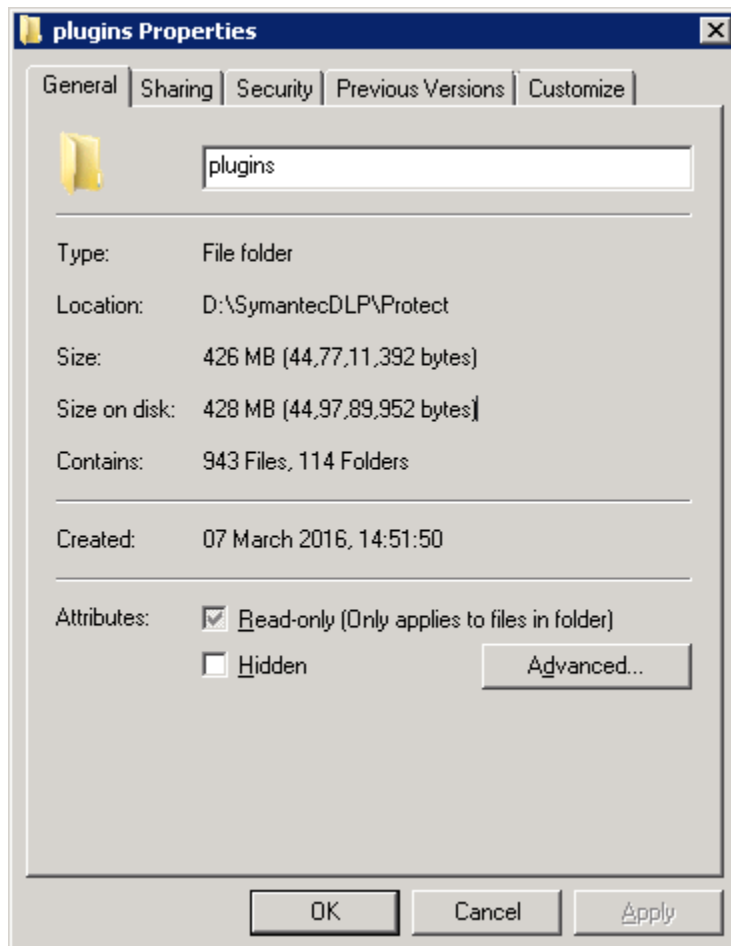
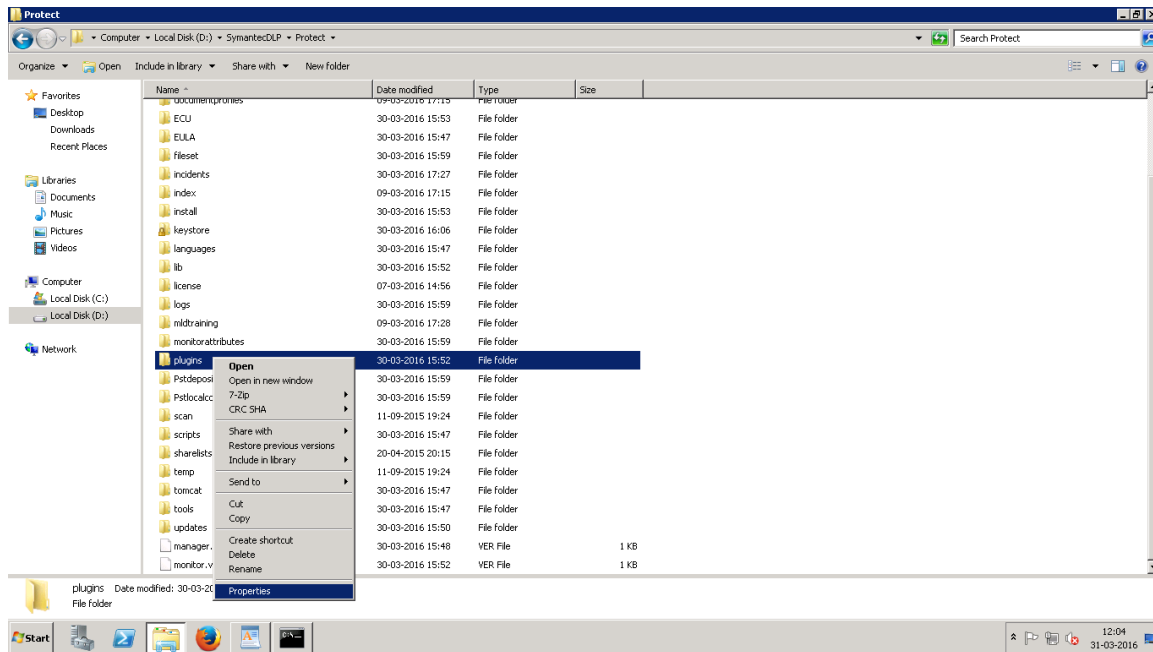
          GB
-----
133.3145

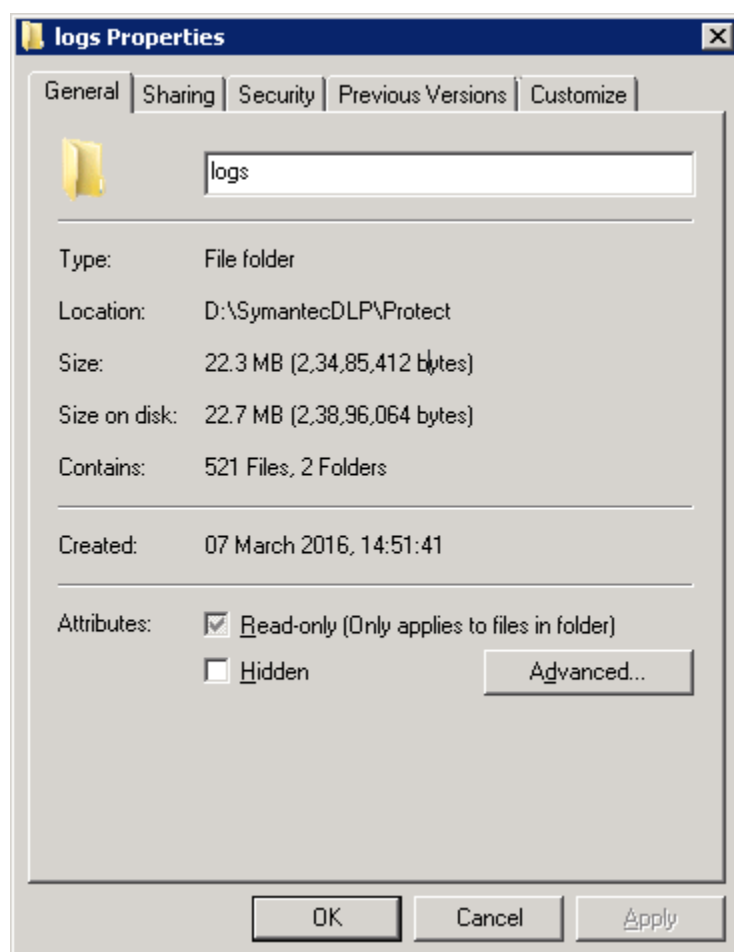
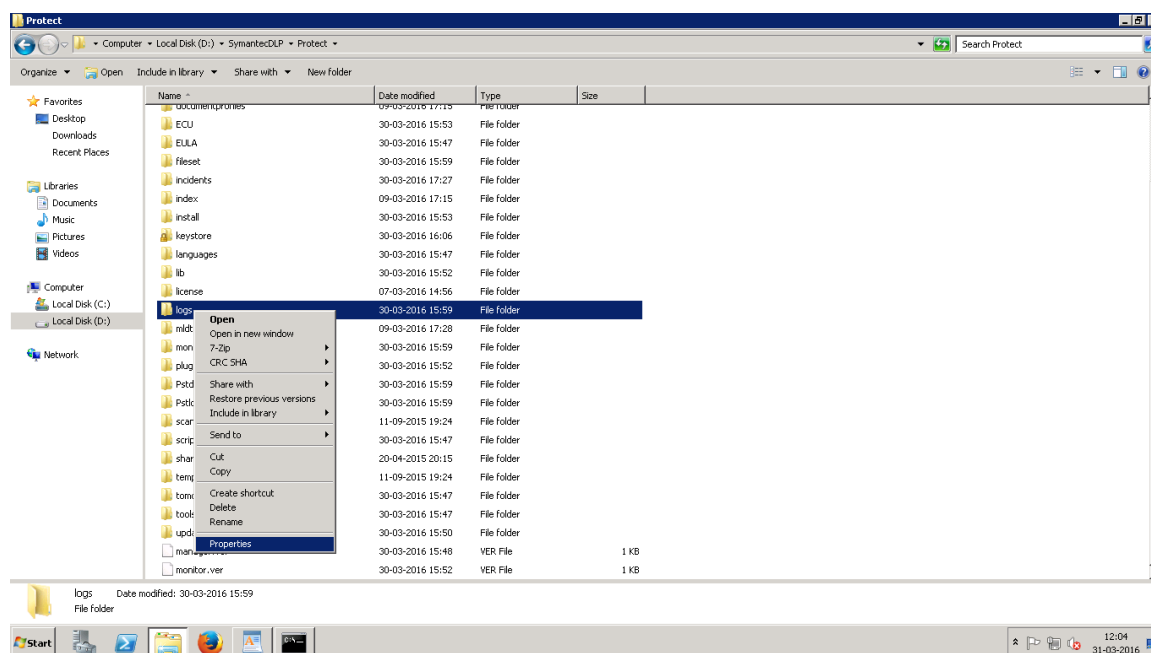
SQL> _
```

```
SELECT ROUND(SUM(bytes)/1024/1024/1024, 4) GB
FROM (
SELECT SUM(bytes) bytes
FROM dba_data_files
UNION ALL
SELECT SUM(bytes) bytes
FROM dba_temp_files
UNION ALL
SELECT SUM(bytes) bytes
FROM v$log
);
```



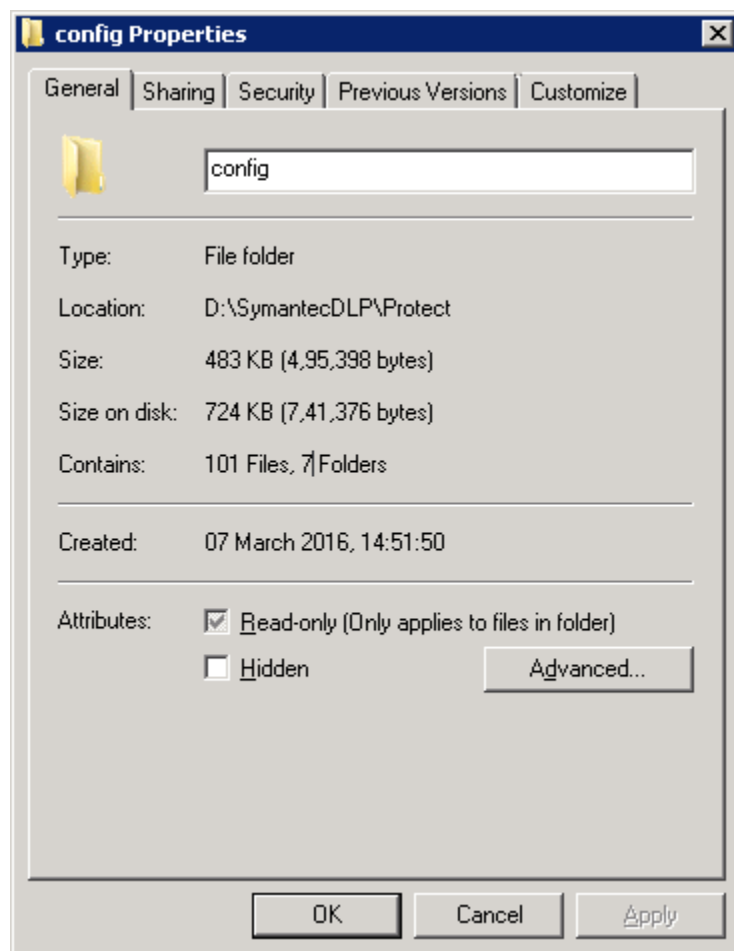
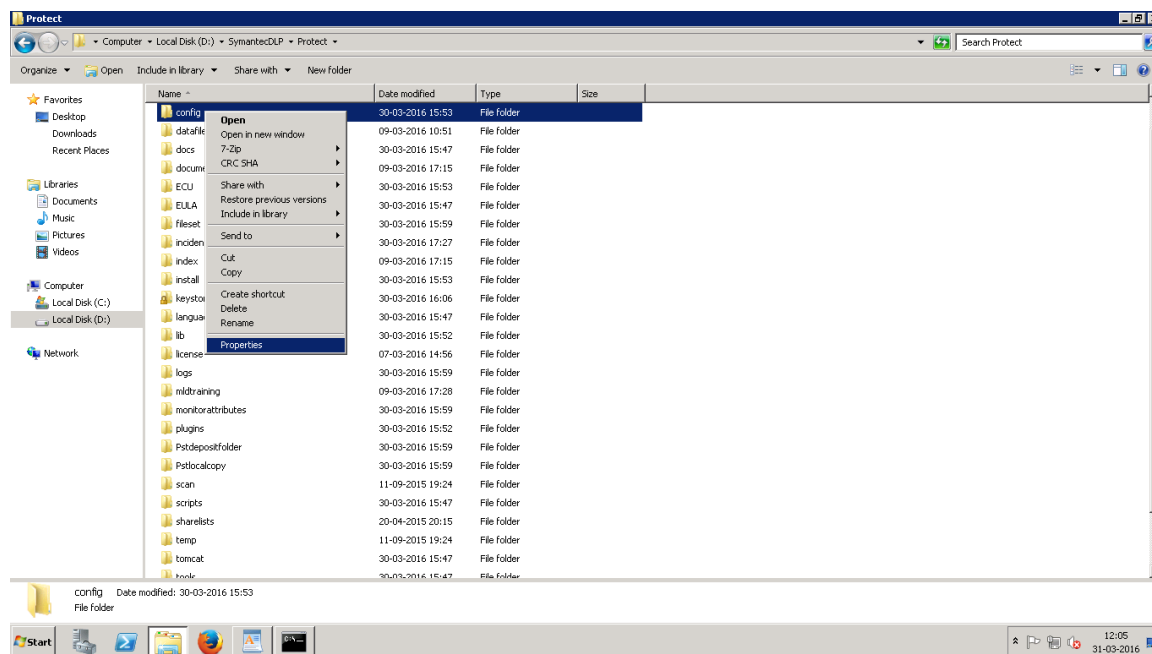
## Calculating the size of File System:







## Calculating the size of Server Configuration:





## Creating backup directories on Windows:

Create the following directories, preferably on a external storage device.  
To create the backup directory structure

1. Create a directory in which to store the backup files:

`\SymantecDLP_Backup_Files`

Remember that this directory should be created on a computer other than the one that hosts the database, the Enforce Server, or the detection servers.

2. Create the following subdirectories in which to store the backup files:

`\SymantecDLP_Backup_Files\File_System`

`\SymantecDLP_Backup_Files\Server_Configuration_Files`

`\SymantecDLP_Backup_Files\Database`

`\SymantecDLP_Backup_Files\Recovery_Aid`

## Performing a cold backup of the Oracle database on Windows

Cold backups are recommended primarily for non-database administrator users.

You perform a cold backup by

- Stopping the Symantec Data Loss Prevention system
- Shutting down the Oracle database
- Copying important files to a safe backup location



<b>Steps to perform a cold backup of the Oracle database</b>	
<b>Step 1</b>	Create recovery aid files.
<b>Step 2</b>	Collect a list of directories that should be backed up.
<b>Step 3</b>	Shut down all of the Symantec Data Loss Prevention and Oracle services.
<b>Step 4</b>	Copy the database files to the backup location.
<b>Step 5</b>	Restart the Oracle and Symantec Data Loss Prevention services.

You should create recovery aid files for use in recovery procedures. A trace file of the control file and a copy of the init.ora file are very helpful for database recoveries.

The trace file of the control file contains the names and locations of all of the data files.

The init.ora file contains the initialization parameters for Oracle, including the names and locations of the database control files.



## To generate a trace file of the control file

1. At the command prompt, enter **sqlplus /nolog**.
2. At the SQL> command prompt, to connect as the sysdba user, enter **connect sys/password@protect as sysdba** where password is the SYS password.
3. After receiving the Connected message, at the SQL> command prompt, enter:

```
alter database backup controlfile to trace as  
'C:\SymantecDLP_Backup_Files\Recovery_Aid\controlfile.trc';
```

Success is indicated by the message "Database altered."

With this command you are generating a copy of the backup control file and outputting this file to the \SymantecDLP\_Backup\_Files\Recovery\_Aid directory that you created previously.

4. Issue the following command to backup the init.ora file.

```
create pfile='C:\SymantecDLP_Backup_Files\Recovery_Aid\init.ora' from spfile;
```

exit;

5. Navigate to the C:\SymantecDLP\_Backup\_Files\Recovery\_Aid directory.  
You  
should see the controlfile.trc and init.ora files in this directory.

6. Rename the file controlfile.trc so that it can be easily identified.  
**controlfilebackupMMDDYY.trc**



```
Enter user-name: sys as sysdba
Enter password:
ERROR:
ORA-01017: invalid username/password; logon denied

Enter user-name: sys as sysdba
Enter password:

Connected to:
Oracle Database 11g Release 11.2.0.4.0 - 64bit Production
SQL> _
```

Connect To Database as sysdba

```
Administrator: Command Prompt - sqlplus
SQL> alter database backup controlfile to trace as
2 'C:\SymantecDLP_Backup_Files\Recovery_Aid\controlfile.trc';

Database altered.

SQL> _
```

Create trace File

```
Administrator: Command Prompt - sqlplus
SQL> create pfile='C:\SymantecDLP_Backup_Files\Recovery_Aid\init.ora' from spfile;

File created.

SQL> _
```

Create init.ora File



## Collecting a list of files to be backed up

You can create a list of files that need to be backed up. These lists are used in a later step.

To create a list of files for back up

1. Open SQL\*Plus using the following command:

```
sqlplus sys/<password> as sysdba
```

2. Enter the following SQL commands to create lists of files that must be backed up:

```
SELECT file_name FROM dba_data_files  
UNION  
SELECT file_name FROM dba_temp_files  
UNION  
SELECT name FROM v$controlfile  
UNION  
SELECT member FROM v$logfile;
```

3. Save the list of files returned by the query to use in the following procedures:

**C:\SymantecDLP\_Backup\_Files\Recovery\_Aid\oracle\_datafile\_directories.txt.**

4. Exit SQL\*Plus:

```
exit;
```



```
Administrator: Command Prompt - sqlplus

Connected to:
Oracle Database 11g Release 11.2.0.4.0 - 64bit Production

SQL> SELECT file_name FROM dba_data_files
2 UNION
3 SELECT file_name FROM dba_temp_files
4 UNION
5 SELECT name FROM v$controlfile
6 UNION
7 SELECT member FROM v$logfile;

FILE_NAME
-----
D:\ORACLE\ORADATA\PROTECT\CONTROL01.CTL
D:\ORACLE\ORADATA\PROTECT\CONTROL02.CTL
D:\ORACLE\ORADATA\PROTECT\CONTROL03.CTL
D:\ORACLE\ORADATA\PROTECT\DRSYS01.DBF
D:\ORACLE\ORADATA\PROTECT\LOB01.DBF
D:\ORACLE\ORADATA\PROTECT\LOB02.DBF
D:\ORACLE\ORADATA\PROTECT\LOB03.DBF
D:\ORACLE\ORADATA\PROTECT\REDO01.LOG
D:\ORACLE\ORADATA\PROTECT\REDO02.LOG
D:\ORACLE\ORADATA\PROTECT\REDO03.LOG
D:\ORACLE\ORADATA\PROTECT\SYSAUX01.DBF

FILE_NAME
-----
D:\ORACLE\ORADATA\PROTECT\SYSTEM01.DBF
D:\ORACLE\ORADATA\PROTECT\TEMP01.DBF
D:\ORACLE\ORADATA\PROTECT\UNDOTBS01.DBF
D:\ORACLE\ORADATA\PROTECT\USERS01.DBF
D:\ORACLE\ORADATA\PROTECT\USERS02.DBF
D:\ORACLE\ORADATA\PROTECT\USERS03.DBF

17 rows selected.

SQL> _
```

## Creating a copy of the spfile on Windows

After you generate a trace file of the control file, you must create a copy of the spfile.

Performing a cold backup of the Oracle database on Windows  
To create a copy of the spfile

1. In Oracle SQL\*Plus, at the SQL> command prompt, enter:  
**create pfile= 'C:\SymantecDLP\_Backup\_Files\Recovery\_Aid\inittemp.ora'**  
**from spfile;**
2. To exit Oracle SQL\*Plus, enter: **Exit**



```
Administrator: Command Prompt - sqlplus
SQL> create pfile='C:\SymantecDLP_Backup_Files\Recovery_Aid\inittemp.ora' from s
pfile;
File created.
SQL> _
```

## Shutting down the Symantec Data Loss Prevention system on Windows

To shut down the system

1. On the computer that hosts the Enforce Server, navigate to Start > All Programs > Administrative Tools > Services to open the Windows Services menu.
2. Open the Services menu and stop all running Symantec Data Loss Prevention services, which might include the following:

Vontu Update

Vontu Incident Persister (on the computers that also host the Enforce Server)

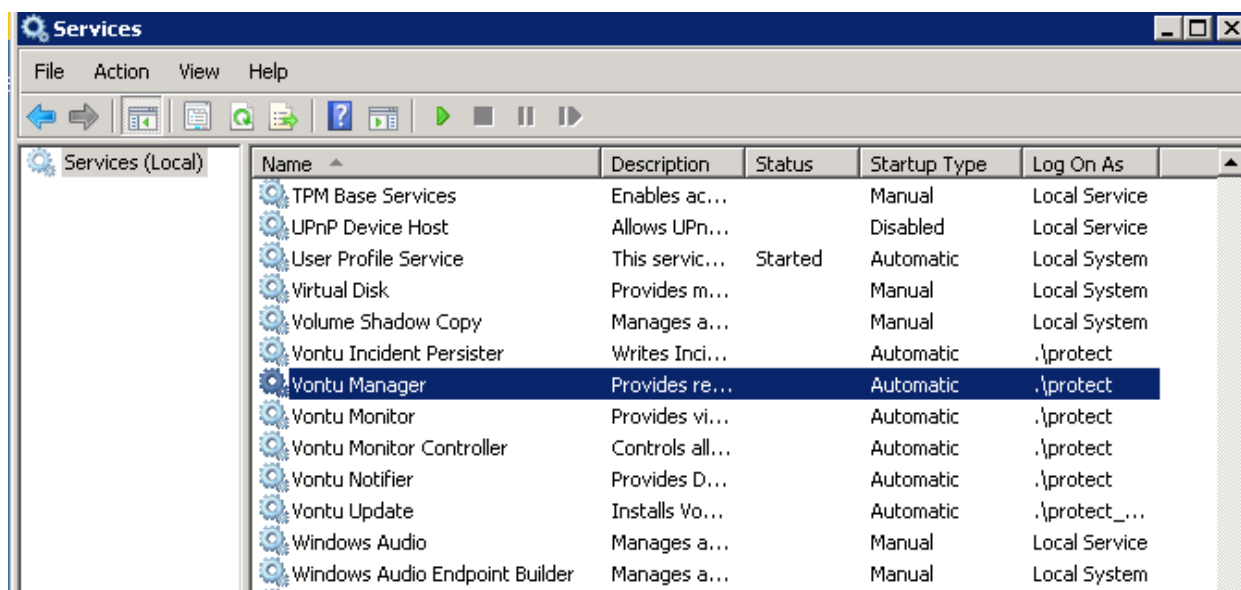
Vontu Manager (on the computers that also host the Enforce Server)

Vontu Monitor (on the computers that also host a detection server)

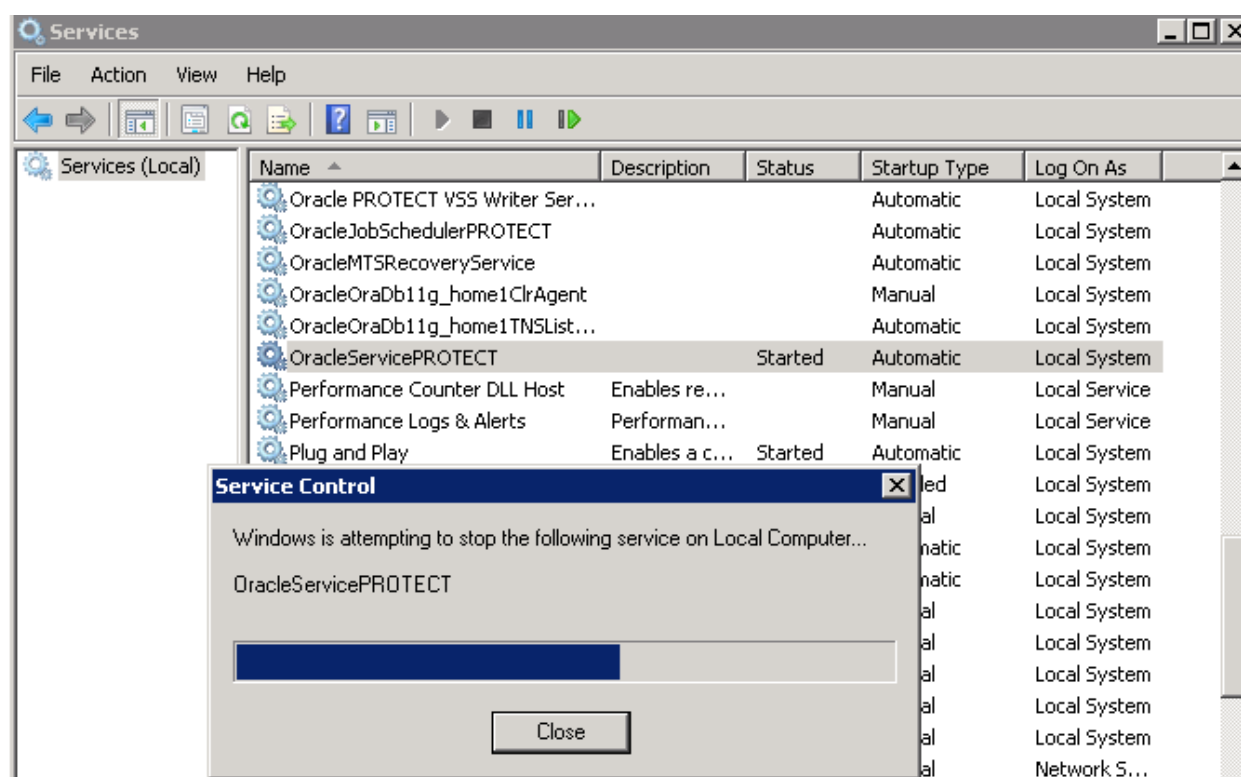
Vontu Monitor Controller (on the computers that also host the Enforce Server)

Vontu Notifier (on the computers that also host the Enforce Server)

3. On the computer that hosts the database, stop the OracleService  
databasename, where databasename is the Global Database Name and SID  
selected during installation.



### Stop All Vontu Services



### Stop All Oracle Services



## Copying the database files to the backup location on Windows

The database files that should be backed up include the files in the \protect directory and the database password file.

To copy the database files to the backup location

1. Make sure that the Oracle services are stopped.

If the Oracle services are not stopped, the backup files may be corrupt and unusable.

2. On the computer that hosts the database, copy the files from the list that you Collected in the procedure collecting a list of files to be backed up to the computer that hosts the backup files.

Copy the protect directory into the **c:\Symantec\_DLP\_Backup\_Files\Database** directory of the computer that hosts the backup files.

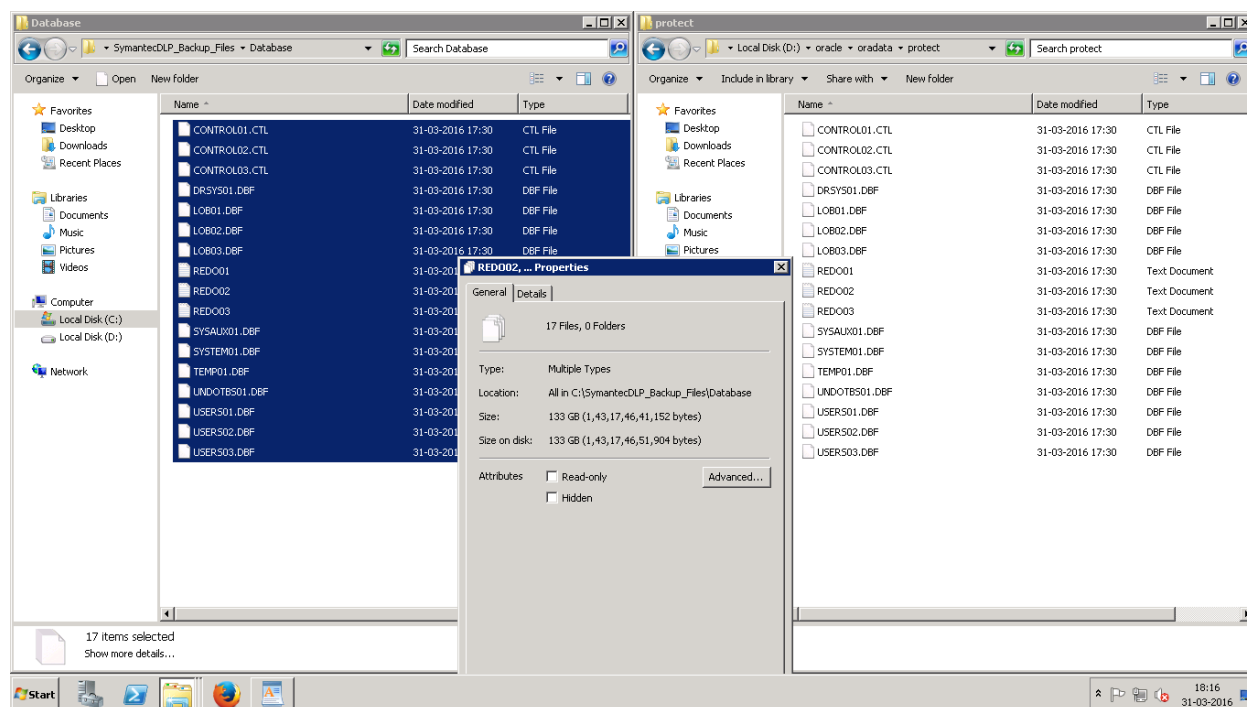
3. On the computer that hosts the database, select the

**%ORACLE\_HOME%\database\PWDprotect.ora** file and copy it into the **c:\Backup\_Files\Database** directory of the computer that hosts the backup files.

**OR**

Run the Database\_Files\_Backup.bat From Attachment to Backup All the Files.

Modify .bat File if required.



## Restarting the system on Windows

To restart the system

=> Start all of the Oracle services:  
OracleServiceDATABASENAME

=> On the computer that hosts the Enforce Server, start the Vontu Notifier service before starting other Symantec Data Loss Prevention services.

=> Start the remaining Symantec Data Loss Prevention services, which might include the following:

- Vontu Manager
- Vontu Monitor
- Vontu Incident Persister
- Vontu Update
- Vontu Monitor Controller



## Backing up the server configuration files on Windows

To back up the server configuration files

1. Select the **\SymantecDLP\Protect\config** directory.

Copy it to the

**\SymantecDLP\_Backup\_Files\Server\_Configuration\_Files** Directory on the computer that hosts the backup files.

**OR**

Run the Config\_Files\_Backup.bat as Administrator to Backup All Files in One Shot. You Can Modify This File According to your Environment.

## Backing up files stored on the file system on Windows

Some files that are stored on the file system for the Enforce Server and detection servers should be backed up whenever they are changed. These files include:

- => Custom configuration changes
- => System logs
- => Keystore file

Copy All Files and Folders from Following location and store it to **\SymantecDLP\_Backup\_Files\File\_System**

**\SymantecDLP\Protect\plugins\  
\SymantecDLP\Protect\logs\  
\SymantecDLP\Protect\tomcat\conf\keystore**

**OR**

Run the File\_System\_Backup.bat as Administrator to Backup All Files in One Shot. You Can Modify This File According to your Environment.



## The Windows recovery information worksheet

Modify Recovery Information Worksheet According to your setup.

Recovery Information Worksheet	
Backup file information	Example and locations
Name of the computer that hosts backup files	Backup_Server1_Gurgaon
Directory containing backup files	C:\SymantecDLP_Backup_Files
Subdirectory containing file system backup files	C:\SymantecDLP_Backup_Files\ File_System
Subdirectory containing Enforce and detection server configuration backup files	C:\SymantecDLP_Backup_Files\ Server_Configuration_Files
Subdirectory containing database backup files	C:\SymantecDLP_Backup_Files\Database
Subdirectory containing Database Recovery Aid files	C:\SymantecDLP_Backup_Files\Recovery_Aid

=> Print this page containing the Recovery Information Worksheet.

=> Store this worksheet in a secure location because it contains sensitive data.