# Oracle Plug-in 8.6

# User Guide

OSP·EVAULT

The software manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, the software manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the software manufacturer to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

The Agent, Agent Console, and Vault applications have the added encryption option of 128/256 bit AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS). See: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf for details.

The Agent and Vault applications have the added security feature of an over the wire encryption method.

# Document History

| Version | Date | Description |
|---|---|---|
| 1 | March 2018 | Initial guide provided. |

# Contents

# 1 Introduction to the Oracle Plug-in

To protect Oracle databases, install the Oracle Plug-in with the Windows Agent on the Oracle database server. You can then add and run backup jobs that specify which databases to back up, and where to save the backup data.

The Plug-in provides ARCHIVELOG-based, non-RMAN backups of whole online database instances. All non-temporary tablespaces and instance parameter files are automatically backed up. Full and partial databases are restored through normal user-managed Oracle recovery mechanisms.

Database passwords are encrypted for enhanced security over script-based methods.
For installation and configuration information, see the Windows Agent guide or Portal online help. For supported platform information, see the Windows Agent release notes.

## 1.1 Limitations

- Only local, single-instance, disk-based databases are backed up.
- Database clusters are not backed up.
- Raw devices are not backed up.
- Remote databases are not backed up.
- The database must run in ARCHIVELOG mode, and the user under which the backup is configured must have SYSDBA privileges.

# 2 Add an Oracle database backup job

After a Windows computer with the Oracle Plug-in is added in Portal, you can create a backup job for one or more Oracle databases. The backup job specifies which databases to back up, and where to save the backup data. You must also specify credentials for the Agent to use to connect to the Oracle server.

The Oracle Plug-in performs what Oracle Corporation deems an “inconsistent” whole database backup, requiring that the database be run in ARCHIVELOG mode. During a live backup, any changes to the database will be written to archived logs. The database administrator should ensure that the database is in ARCHIVELOG mode.

To ensure that archived log files do not take up too much disk space on your system, the Oracle Plug-in can delete archived redo logs after a successful backup. This functionality is available with the Oracle Plug-in for the Windows Agent or Linux Agent version 8.60 or later. If you specify that archived logs should be deleted after a backup, ensure that the logs are backed up using a Local System or Image job.

To back up the data, you can run the backup job manually, or schedule the backup job to run. See Run and schedule backups and synchronizations.

To add an Oracle database backup job:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered computers.

2. Find a computer with the Oracle Plug-in, and expand its view by clicking the computer row.

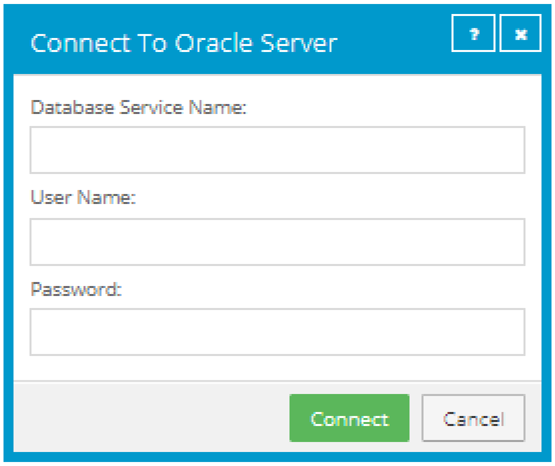
3. Click the **Jobs** tab.

   If a valid vault connection is not available for the computer, you cannot access the **Jobs** tab.

4. In the **Select Job Task** menu, click **Create New Oracle Job**.

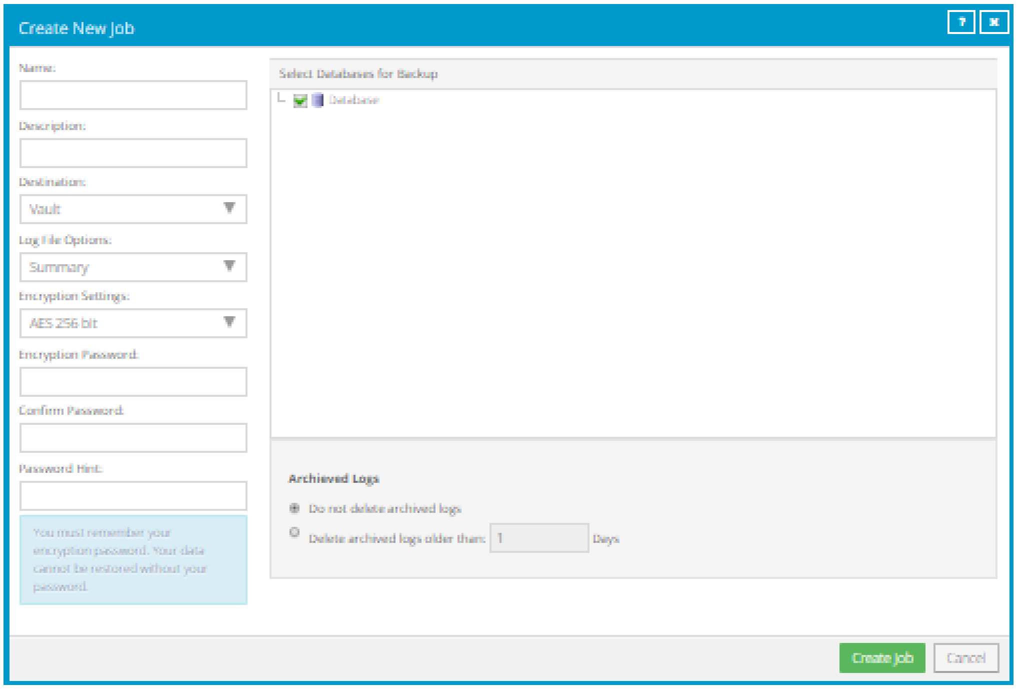
5. In the **Connect to Oracle Server** dialog box, specify the following information:

   - In the **Database Service Name** box, type the service name of the database that you want to back up.
   - In the **User Name** box, type the name of a user who has sysdba privileges.
   - In the **Password** box, type the password for the specified user.



6. Click **Connect**.
7. In the **Create New Job** dialog box, specify the following information:
   - In the **Name** box, type a name for the backup job.
   - In the **Description** box, optionally type a description for the backup job.
   - In the **Destination** list, select the vault where you want to save the backup data.

     A vault only appears in the list if it assigned to the user, or if the user added it on the computer's Vault Settings tab.
   - In the **Log File Options** list, select the level of detail for job logging.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods.
   - In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.



Create New Job

Name:

Description:

Destination: Vault

Log File Options: Summary

Encryption Settings: AES 256 bit

Encryption Password:

Confirm Password:

Password Hint:

You must remember your encryption password. Your data cannot be restored without your password.

Select Databases for Backup

☑ Database

Archieved Logs

● Do not delete archived logs

○ Delete archived logs older than: 1 Days

8. In the **Select Databases for Backup** box, select the database to back up.

9. Do one of the following:

   - To leave Oracle archived redo logs on the system, click **Do not delete archived logs.**

   - To delete Oracle archived redo logs after a successful backup, click **Delete archived logs older than […] days**. Enter the number of days after which archived logs can be deleted.

10. Click **Save**.

    The job is created, and the **View/Add Schedule** dialog box appears. Now you can create a schedule for running the backup. Click **Cancel** if you do not want to create a schedule at this time.

    For information about how to run and schedule the backup job, see Run and schedule backups and synchronizations.

# 3 Run and schedule backups and synchronizations

After a backup job is created, you can run it manually (ad-hoc) at any time and schedule it to run.

When running or scheduling a backup, you can specify the following settings:

- Retention type. The retention type specifies the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.
- Deferring. You can use deferring to prevent large backups from running at peak network times. When deferring is enabled, the backup job does not back up any new data after the specified amount of time and commits the safeset to the vault, even if some data in the job is not backed up. Changes to data that was previously backed up will be backed up, regardless of the specified amount of time.

  When the job runs again, the Agent checks for changes in data that was previously backed up, backs up those changes, and then backs up the remaining data.
- For computers with Windows or Linux Agent version 8.60 or later, you can specify whether scheduled backups should automatically retry if they do not run successfully. You can also specify how many times a scheduled backup should retry after a failed attempt, and specify the amount of time between retries. See Specify whether scheduled backups retry after a failure.
- When you schedule a job to run, you can also set the compression level for the data. The compression level optimizes the volume of data sent to the vault against the speed of processing. The default compression level is usually the optimal setting.

When a backup job first runs, all data selected in the job is backed up to the vault. This initial backup is called a “seed” backup. In subsequent backups, only data that has changed is backed up to the vault, unless a reseed is required (e.g., after a job’s encryption password has changed). In a reseed, all data selected in a backup job is sent to the vault again, even though it has already been backed up.

After running a backup, you can view logs to check whether the backup completed successfully.

In some cases, you must synchronize a backup job before you run it or restore data from the job. When you synchronize a job, the Agent checks which safesets for the job are online and available for restore. See Synchronize a job.

## 3.1 Schedule a backup

After creating a backup job, you can add one or more schedules for running the job automatically.

You can create complex schedules for a job by creating multiple schedules. For example, you can schedule a backup job to run at midnight every Friday, and schedule the job to run at 8 pm on the first day of every month.

If a job is scheduled to start at exactly the same time by multiple schedules, the job only runs once at the scheduled time. If the jobs have different retention types, the retention type of the schedule that is highest in the list is applied to the resulting safeset. For example, in the following screenshot, the job is scheduled to run at 12 AM each Saturday with the Weekly retention type, and every day at 12 AM with the Daily retention type. On Saturdays, the job runs only once at 12 AM. Because the schedule with the Weekly retention type is higher in the list than the schedule with the Daily retention type, the Weekly retention type is applied to the safeset.

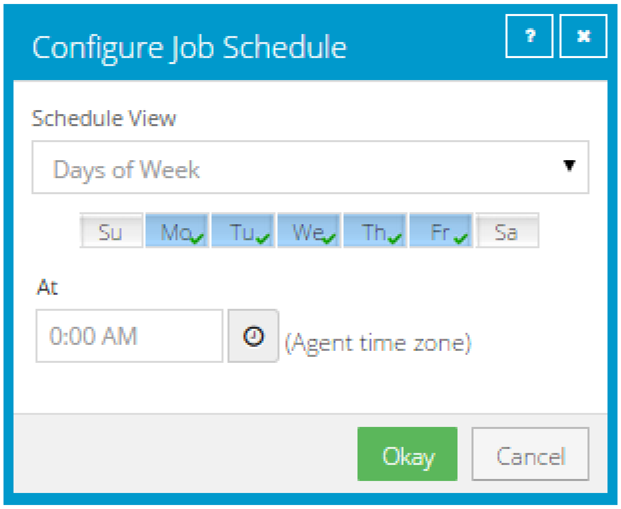
*Note:* If a job is scheduled to run at slightly different times, the Agent attempts to run the job according to each schedule. For example, if a job is scheduled to run at 11 PM by one schedule and 11:01 PM by another schedule, the Agent will attempt to run the job twice. Try to avoid overlapping schedules; problems can occur if a job is scheduled to run twice in a short period of time.

To schedule a backup:

1. Do one of the following:
   - On the navigation bar, click **Computers**. Find the computer with the backup job that you want to schedule, and click the computer row to expand its view. On the **Jobs** tab, find the job that you want to schedule. In its **Select Action** menu, click **View/Add Schedule**.
   - Create a new backup job. The **View/Add Schedule** dialog box appears when you save the job.
2. In the **View/Add Schedule** dialog box, click **Add Schedule**.

   A new row appears in the dialog box.
3. In the new schedule row, in the **Retention** list, click a retention type.
4. In the **Schedule** box, click the arrow.

   The **Configure Job Schedule** dialog box opens.
5. In the **Configure Job Schedule** dialog box, do one of the following:
   - To run the backup on specific days each week, select **Days of Week** in the **Schedule View** list. Select the days when you want to run the job. Then use the **At** field to specify the time when you want to run the job.



Configure Job Schedule

Schedule View

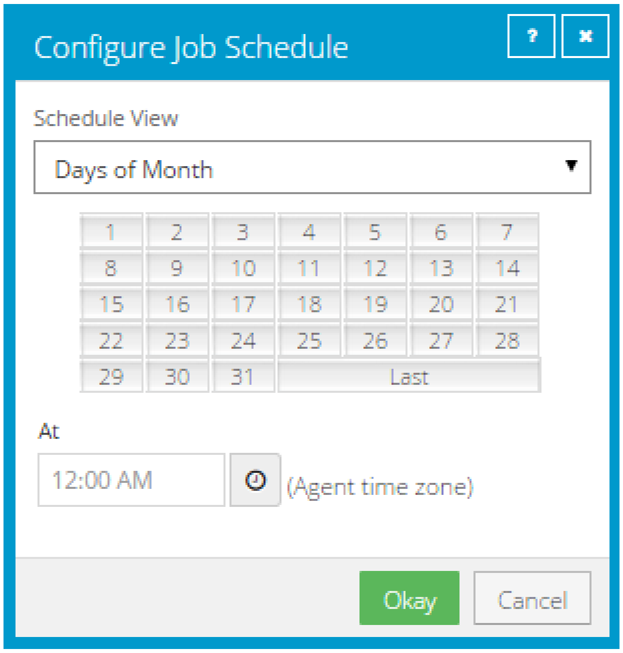
Days of Week

| Su | Mo ✓ | Tu ✓ | We ✓ | Th ✓ | Fr ✓ | Sa |
|---|---|---|---|---|---|---|

At

0:00 AM (Agent time zone)

- To run the backup on specific dates each month, select **Days of Month** in the **Schedule View** list. On the calendar, select the dates when you want to run the job. Then use the **At** field to specify the time when you want to run the job.



Configure Job Schedule

Schedule View

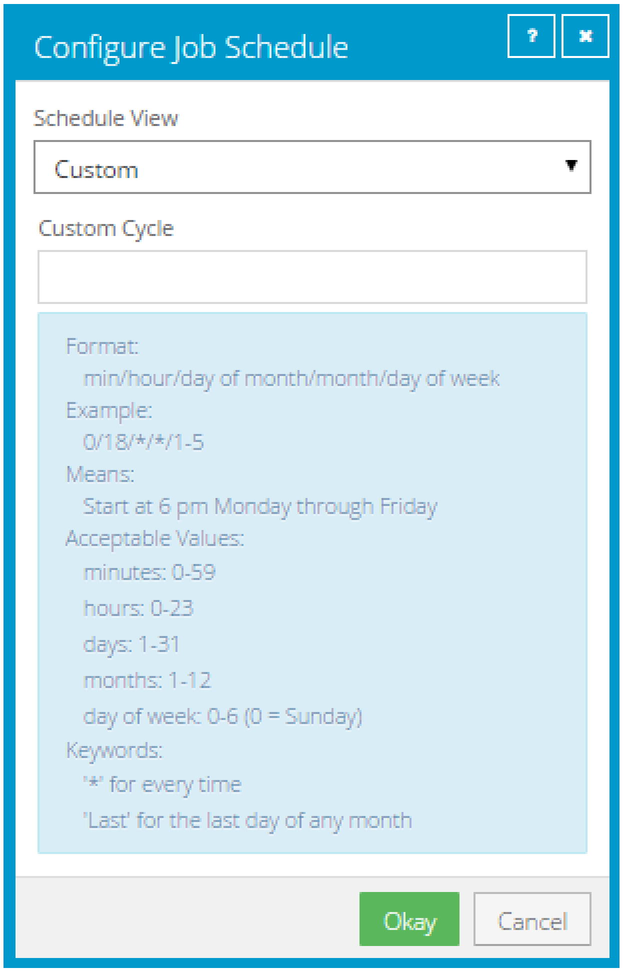
Days of Month

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | Last | | | |

At

12:00 AM (Agent time zone)

- To create a custom schedule, select **Custom** in the **Schedule View** list. In the **Custom Cycle** dialog box, enter a custom schedule. Be sure to follow the format and notation as described.



Schedule View: Custom

Custom Cycle

Format:
min/hour/day of month/month/day of week
Example:
0/18/*/*/1-5
Means:
Start at 6 pm Monday through Friday
Acceptable Values:
minutes: 0-59
hours: 0-23
days: 1-31
months: 1-12
day of week: 0-6 (0 = Sunday)
Keywords:
'*' for every time
'Last' for the last day of any month

6. Click **Okay**.

   The new schedule appears in the **Schedule** box.

7. In the **Compression** list, click a compression level for the backup data. Compression levels optimize the volume of data sent against the speed of processing.

8. Do one of the following:

   - To allow the backup job to run without a time limit, click **None** in the Deferring list.
   - To specify a maximum amount of time that the backup job can run, click **Minutes** or **Hours** in the **Deferring** list. In the adjacent box, type the maximum number of minutes or hours that the job can run.

   *Note:* When deferring is used, the backup job does not back up any new data after the specified amount of time, even if some data is not backed up. Changes to data that was previously backed up will be backed up, regardless of the amount of time specified.

9. To run the job on the specified schedule, select the **Enable** check box near the end of the row.

10. If an Automatic Retry for Scheduled Backups section appears at the bottom of the View / Add Schedule dialog box, you can specify whether scheduled backups should retry after a failed backup. See Specify whether scheduled backups retry after a failure.
11. Click **Save**.

## 3.2 Specify whether scheduled backups retry after a failure

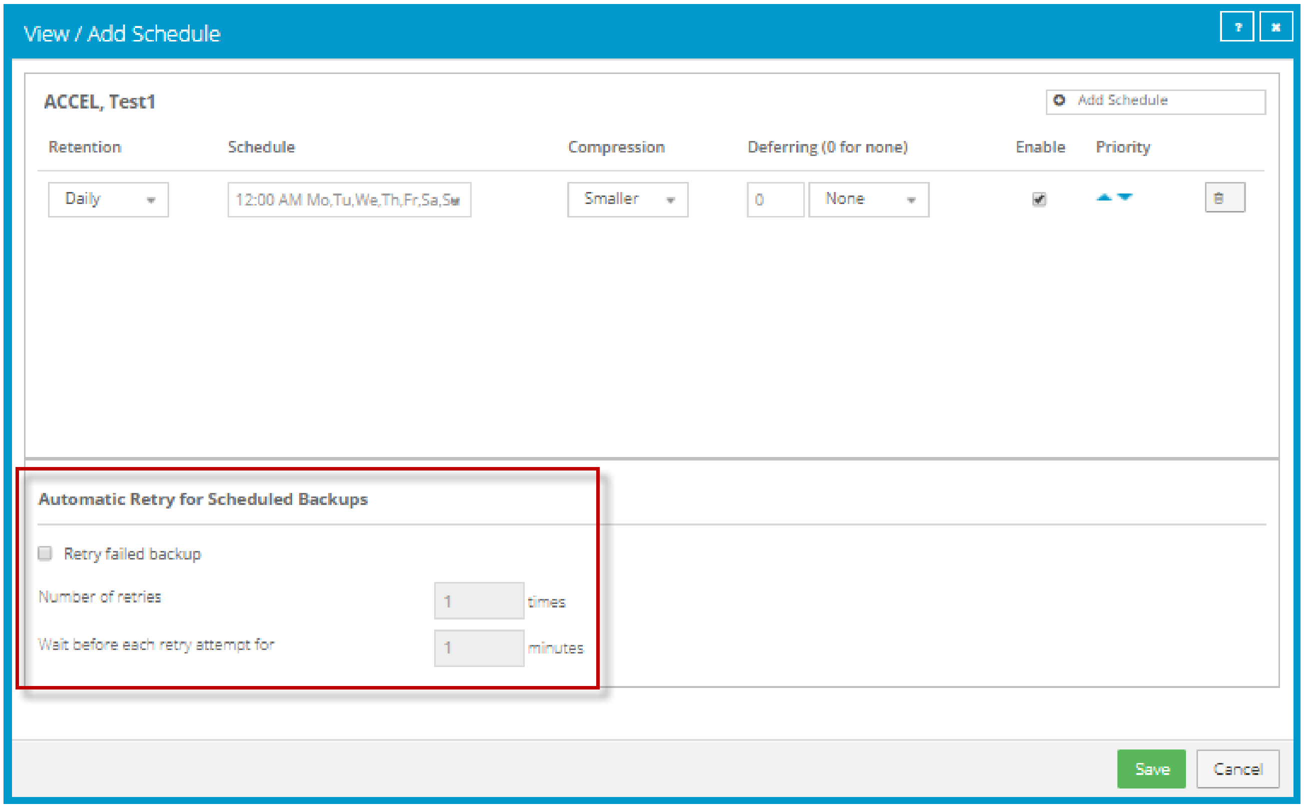
You can specify whether scheduled backups automatically retry if they do not run successfully.

You can also specify how many times a scheduled backup should retry after a failed attempt, and specify the amount of time between retries.

*Note:* Automatic retry settings only apply to scheduled backups. A backup will not retry automatically after a failed ad-hoc backup attempt.

To specify whether scheduled backups retry after a failure:

1. Do one of the following:
    - On the navigation bar, click **Computers**. Find the computer for specifying automatic retry settings, and click the computer row to expand its view. On the **Jobs** tab, in the **Select Action** menu for a job, click **View/Add Schedule**.
    - Create a new backup job. The **View/Add Schedule** dialog box appears when you save the job.
2. In the Automatic Retry for Scheduled Backups section, do one of the following:
    - To specify that scheduled backups should not retry after failed backup attempts, clear the **Retry failed job** check box.
    - To specify that scheduled backups should retry after failed backup attempts, select the **Retry failed job** check box. In the **Number of retries** box, enter the number of times the backup should try again**.** In the **Wait before each retry attempt for [ ] minutes** box, enter the number of minutes that the Agent should wait before the next backup attempt.



ACCEL, Test1

| Retention | Schedule | Compression | Deferring (0 for none) | | Enable | Priority |
|---|---|---|---|---|---|---|
| Daily | 12:00 AM Mo,Tu,We,Th,Fr,Sa,Su | Smaller | 0 | None | ☑ | ▲▼ |

Automatic Retry for Scheduled Backups

□ Retry failed backup

Number of retries 1 times

Wait before each retry attempt for 1 minutes

3. Click **Save**.

## 3.3 Run an ad-hoc backup

After a backup job is created, you can run the backup at any time, even if the job is scheduled to run at specific times.

To run an ad-hoc backup:

1. On the navigation bar, click **Computers**.

   A grid lists available computers.

2. Find the computer with the backup job that you want to run, and expand its view by clicking the computer row.

3. Click the **Jobs** tab.

4. Find the job that you want to run, and click **Run Job** in its **Select Action** menu.

   The **Run Job** dialog box shows the default settings for the backup.

   *Note:* Beginning at this point, you can click **Start Backup** to immediately start the job. If you prefer, you can change backup options before running the job.

5. In the **Retention Scheme** list, click a retention type.

The retention type specifies the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.

6. Click Start Backup.

   The **Process Details** dialog box shows the backup progress, and indicates when the backup is completed. Other recent job processes might also be listed in the dialog box. See View current process information for a job.

7. If you want to stop the backup, click **Stop**.

8. To close the **Process Details** dialog box, click **Close**.

## 3.4 Synchronize a job

When a backup job is synchronized, the Agent checks which safesets for the job are online and available for restore.

A job is synchronized automatically when you restore data from the job. You can also synchronize a job manually at any time. A manual synchronization is recommended or required in the following cases:

- Before running backup jobs on reregistered computers..
- Before restoring data from jobs that are backed up to a Satellite vault and replicated to the cloud or another vault.
- To rebuild a delta (.dta) file for a job. If an error message in a log file says that the delta mapping file is corrupt, delete the delta (.dta) file from the job folder on the protected computer and then synchronize the job to rebuild the delta file.

To synchronize a job:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered computers.

2. Find the computer with the job that you want to synchronize. Expand its view by clicking its row.

3. Click the **Jobs** tab.

4. Find the job that you want to synchronize, and click **Synchronize** in its **Select Action** menu.

   The **Process Details** dialog box shows the backup progress, and indicates when the backup is completed. Other recent job processes might also be listed in the dialog box. See View current process information for a job.

5. If you want to stop the backup, click **Stop**.

   To close the **Process Details** dialog box, click **Close**.

# 4 Restore Oracle databases

After backing up an Oracle database using the Oracle Plug-in, you can restore the database.

You might also need to recover the entire system, by performing a “bare metal restore” (installing the OS, applications, and then the full database (plus any transaction logs) onto a new system).

If there is an Oracle backup and a full-system backup:

1. Restore the system (putting back the contents of ORACLE_HOME – specifically the database installation). If you like, you can exclude the data files and archive logs that are backed up by the plug-in.
2. Restore the Oracle backup, and then copy the required components to the appropriate directories. Follow the standard user-managed Oracle recovery procedure from the Oracle backup and recovery guide (available from Oracle) that is appropriate for the operating system.

An Oracle restore process is performed by a Database Administrator. Briefly, the steps are:

- Shut down the database.
- Restore the files.
- If necessary, reset the control information for the database.
- Start and recover the database.
- Re-open the database for use.

The Plug-in does not do table-level restores.

To restore an Oracle database:

1. On the navigation bar, click **Computers**.

   A grid lists available computers.
2. Find the computer with the Oracle database that you want to restore, and expand its view by clicking the row for the computer.
3. Click the **Jobs** tab.
4. Find the job with the database that you want to restore, and click **Restore** in the **Select Action** menu for the job.

   The **Restore** dialog box shows the most recent safeset for the job.
5. To restore the database from an older safeset, or from SSI (safeset image) files, do one of the following:

   - To restore data from an older safeset, click the calendar button. 📅 In the calendar that appears, click the date of the safeset from which you want to restore. To the right of the calendar, click the specific safeset that you want to use.

- To restore data from SSI (safeset image) files on disk, select **Directory on disk** from the **Source Device** list. Click the folder button. 📂 In the **Select Folder** dialog box, select the directory where the files are located, and click **Okay**.

  SSI files are full backups exported from the vault or backed up to disk instead of to a vault. It can be quicker to save backup files on physical media and transport them to a location for a restore, than to restore data from a vault in a remote datacenter.

  *Note:* If SSI files were created by a backup to a directory on disk, you cannot restore from the SSI files until they have been imported into the vault and you have synchronized the Agent with the vault.

6. In the **Files to Restore** box, select the items that you want to restore.
7. Select a **Restore Destination** option.
   - To restore files and folders to the location where they were backed up, select **Restore files to their original location**.
   - To restore files and folders to a different location, select **Restore files to an alternate location**. Click the folder button. 📂 In the **Select Folder** dialog box, select the location where you want to restore, and click **Okay**.
8. Select a **File Overwrite** option. This option specifies how to restore a file to a location where there is a file with the same name.
   - To overwrite existing files with restored files, select **Overwrite existing files**.

     *Note:* If you try to restore multiple files with the same name to an alternate location and select **Overwrite existing files**, only the last file restored will remain. Other files with the same name will be overwritten.
   - To add a numeric extension (e.g., .0001) to a *restored* file name, select **Do not overwrite existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *restored* file name (e.g., “filename.txt.0001”).
   - To add a numeric extension (e.g., .0001) to an *existing* file name, select **Rename existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *existing* file name (e.g., “filename.txt.0001”). The name of the restored file continues to be “filename.txt”.
9. To change the log detail level or bandwidth settings, click **Advanced Restore Options**. Specify settings in the **Advanced Restore Options** dialog box, and click **Okay**. See Advanced restore options.
10. Click **Run Restore**.

    The **Process Details** dialog box shows the restore progress and indicates when the restore is completed. Other recent job processes might also be listed in the dialog box. See View current process information for a job.

11. To close the **Process Details** dialog box, click **Close**. If the restore is running, it will continue to run.

**Note:** For a full disaster recovery (in which the full database instance is restored), be careful when you recover the database because the plug-in does not back up TEMPORARY tablespaces.

## 4.1 Advanced restore options

When restoring data, you can specify the following options:

### Log Options

Select one of the following job logging levels from the list:

- **Files** — Provides the most detailed information, and is typically used for troubleshooting. Provides information about files that are backed up.
- **Directory** — Provides less detail than the Files logging level. Provides information about folders that are backed up.
- **Summary** — Provides high-level information, including the vault and Agent version, and backup sizes.
- **Minimal** — Provides high-level information, including the vault and Agent version.

Changing the logging level only affects log files that are created from that point and after. It does not affect previously-created log files.

### Performance Options

To use all available bandwidth for the restore, select **Use all available bandwidth**.

Bandwidth throttling settings specify the amount of bandwidth consumed by an Agent for backups. For example, you might want to restrict the amount of bandwidth used for daytime backups so that online users are not affected, and allow unlimited bandwidth usage at night so that scheduled backups run as fast as possible.

Bandwidth settings include:

- Maximum bandwidth (upper limit), in megabits per second, to be consumed by the Agent for all backups and restores
- Period of time during the day that throttling is in effect. Only one time window can be specified. Outside the window, no throttling takes place.
- Days of the week that throttling is in effect

If the bandwidth throttling time period begins when a backup is underway, the maximum bandwidth is applied dynamically to the running backup. Similarly, if the bandwidth throttling time period ends when a backup is running, bandwidth throttling is ended for the backup.

If you edit an Agent’s bandwidth settings while a backup is running, the new Agent settings do not affect the backup that is running. Bandwidth settings are applied when a backup starts, and are not applied to backups that are already running.

# 5 Monitor computers, jobs and processes

You can monitor backups, restores and protected computers using the following Portal features:

- Computer page. The Computer page shows status information for protected computers and their jobs. See View computer and job status information. You can also access logs for unconfigured computers from this page. See View an unconfigured computers logs.
- Process Details dialog box. This dialog box shows information about all running, queued and recently-completed processes for a job. See View current process information for a job.
- Email notifications. To make it easier to monitor backups, users can receive emails when backups finish or fail. See Monitor backups using email notifications.
- Process logs and safeset information. Process logs indicate whether each backup and restore completed successfully, and provide information about any problems that occurred. You can also view information about the safeset created by a specific backup. See View a jobs process logs and safeset information.
- Monitor page. The Monitor page shows the most recent backup status for each job, and allows you to navigate to the computer and job for each backup. See View and export recent backup statuses.

## 5.1 View computer and job status information

On the Computer page in Portal, you can view status information for protected computers and their jobs.

To view computer and job status information:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered Agents.

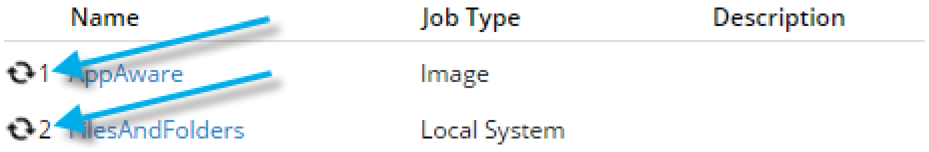
   The **Availability** column indicates whether each Agent is online or offline. Online computers are in contact with Portal, while offline computers are not currently available. A computer can be offline if it is turned off, if the Agent has been uninstalled from the system, or if the system has been lost.

   The **Status** column shows the status of each computer. Possible statuses include:

   - ✓ OK — Indicates that all jobs on the computer ran without errors or warnings.
   - ! OK with warnings — Indicates that one or more of the computer’s jobs completed with warnings.
   - ! Attention — Indicates that one or more of the computer’s jobs failed or completed with errors.
   - ⊘ Unconfigured — Indicates that no jobs have been created for the computer.
2. Find the Agent for which you want to view logs, and click the row to expand its view.

3. View the **Jobs** tab.

   If a backup or restore is running for a job, an “In Progress” symbol ⟳ appears beside the job name, along with the number of processes that are running.

   | Name | Job Type | Description |
   |---|---|---|
   | ⟳1 AppAware | Image | |
   | ⟳2 FilesAndFolders | Local System | |

   If you click the symbol, the **Process Details** dialog box shows information about running, queued and recently-completed processes for the job. See View current process information for a job.

   The **Last Backup Status** column shows the result of the last backup attempt for each job. Possible statuses include:

   - ✓ Completed — Indicates that the last backup completed successfully, and a safeset was created.
   - ❗ Completed with warnings — Indicates that the last backup completed and a safeset was created, but problems occurred during the backup. For example, a warning could indicate that a file or volume that was selected in the backup job was not available for backup.
   - ❗ Deferred — Indicates that the last backup was deferred. A safeset was created, but not all data that was selected was backed up.

     Deferring is used to prevent large backups from running at peak network times. When deferring is enabled, a backup job does not back up any new data after a specified amount of time.
   - ⊘ Never Run — Indicates that the backup job has never run.
   - ❗ Missed — Indicates that the job has not run for 7 days.
   - ❗ Completed with errors — Indicates that the backup completed and a safeset is available for restore, but problems occurred.
   - ❗ Failed — Indicates that the backup failed and no safeset was created.
   - ❗ Cancelled

   To view logs for a job, click the job status. For more information, see View a jobs process logs and safeset information.

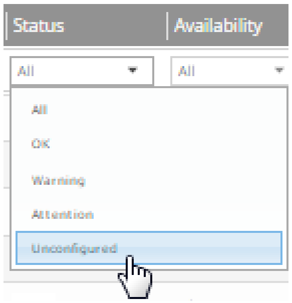
## 5.2 View an unconfigured computer’s logs

You can view logs for unconfigured computers. Unconfigured computers do not have any backup jobs.

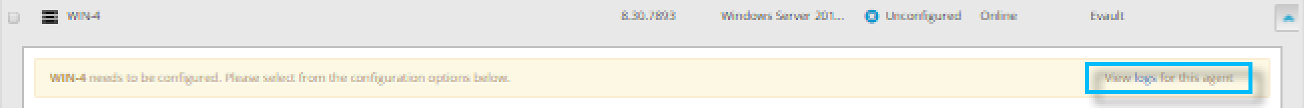
To view an unconfigured computer’s logs:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered computers. To only show unconfigured computers, click “Unconfigured” in the **Status** filter.



2. Find the unconfigured computer, and expand its view by clicking the computer row.

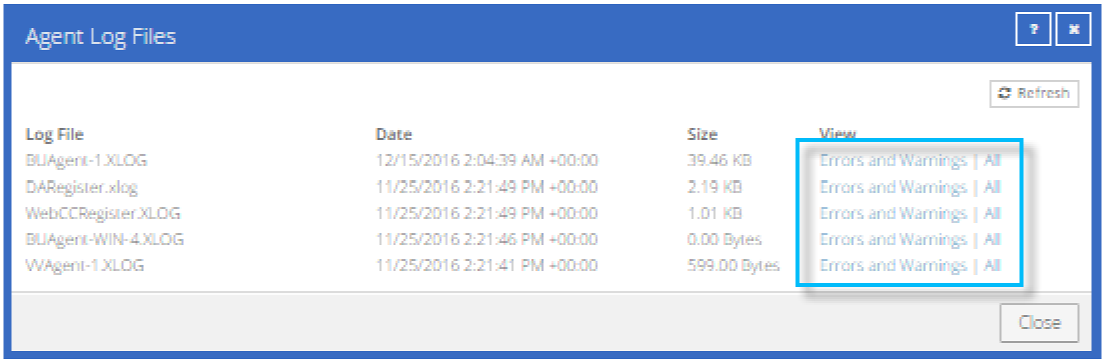


| | | | | | |
|---|---|---|---|---|---|
| WIN-4 | 8.30.7893 | Windows Server 201... | Unconfigured | Online | Evault |

**WIN-4** needs to be configured. Please select from the configuration options below.

3. Click the **logs** link for the unconfigured computer.

   The Agent Log Files window shows a list of logs for the computers. Links to the logs appear at the right side of the window.



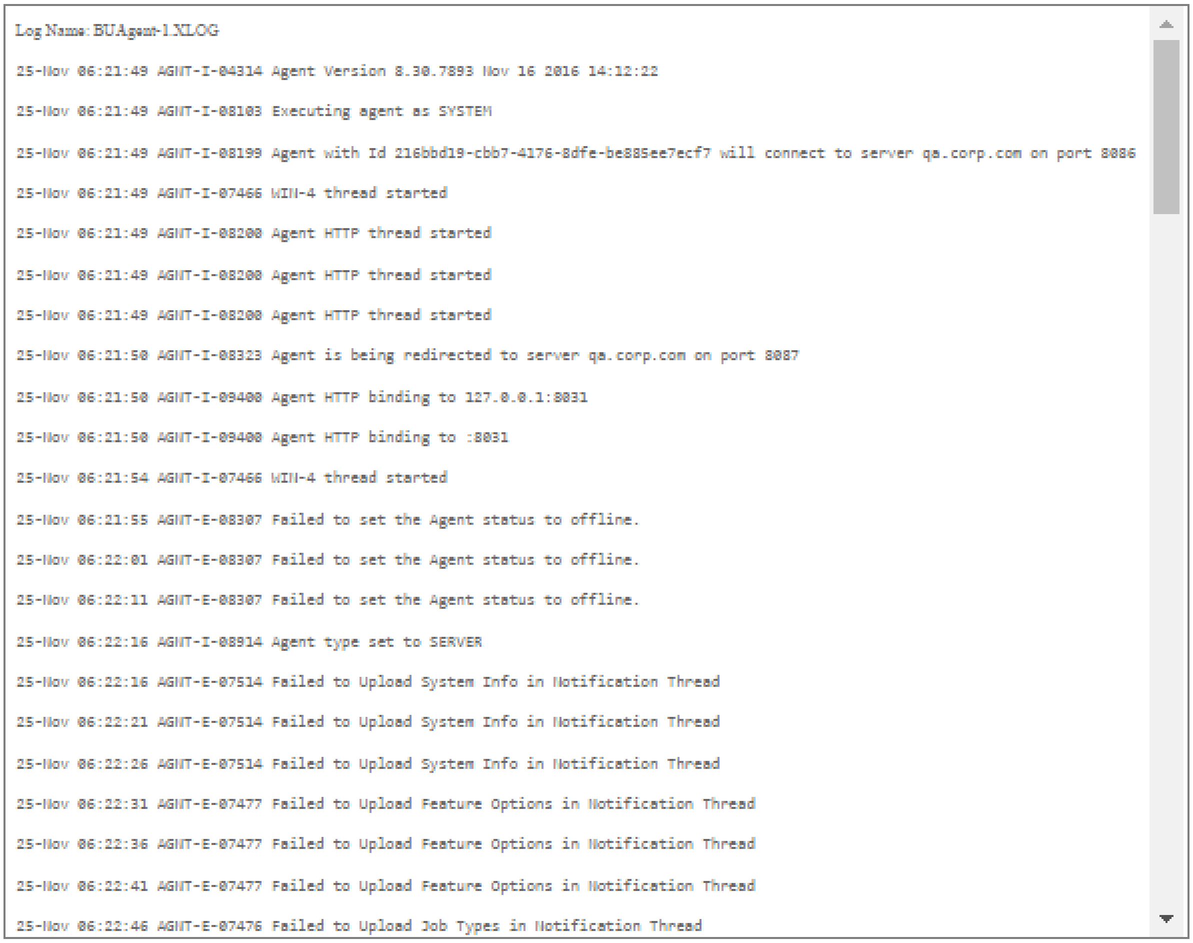
Agent Log Files

| Log File | Date | Size | View |
|---|---|---|---|
| BUAgent-1.XLOG | 12/15/2016 2:04:39 AM +00:00 | 39.46 KB | Errors and Warnings \| All |
| DARegister.xlog | 11/25/2016 2:21:49 PM +00:00 | 2.19 KB | Errors and Warnings \| All |
| WebCCRegister.XLOG | 11/25/2016 2:21:49 PM +00:00 | 1.01 KB | Errors and Warnings \| All |
| BUAgent-WIN-4.XLOG | 11/25/2016 2:21:46 PM +00:00 | 0.00 Bytes | Errors and Warnings \| All |
| VVAgent-1.XLOG | 11/25/2016 2:21:41 PM +00:00 | 599.00 Bytes | Errors and Warnings \| All |

4. Do one of the following:

   - To only view errors and warnings in a log, click **Errors and Warnings** for the log.
   - To view an entire log, click **All** for the log.

   The log appears in a new browser tab.



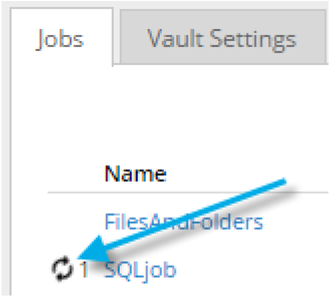
```
Log Name: BUAgent-1.XLOG

25-Nov 06:21:49 AGNT-I-04314 Agent Version 8.30.7893 Nov 16 2016 14:12:22

25-Nov 06:21:49 AGNT-I-08103 Executing agent as SYSTEM

25-Nov 06:21:49 AGNT-I-08199 Agent with Id 216bbd19-cbb7-4176-8dfe-be885ee7ecf7 will connect to server qa.corp.com on port 8086

25-Nov 06:21:49 AGNT-I-07466 WIN-4 thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:50 AGNT-I-08323 Agent is being redirected to server qa.corp.com on port 8087

25-Nov 06:21:50 AGNT-I-09400 Agent HTTP binding to 127.0.0.1:8031

25-Nov 06:21:50 AGNT-I-09400 Agent HTTP binding to :8031

25-Nov 06:21:54 AGNT-I-07466 WIN-4 thread started

25-Nov 06:21:55 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:01 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:11 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:16 AGNT-I-08914 Agent type set to SERVER

25-Nov 06:22:16 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:21 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:26 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:31 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:36 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:41 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:46 AGNT-E-07476 Failed to Upload Job Types in Notification Thread
```

## 5.3 View current process information for a job

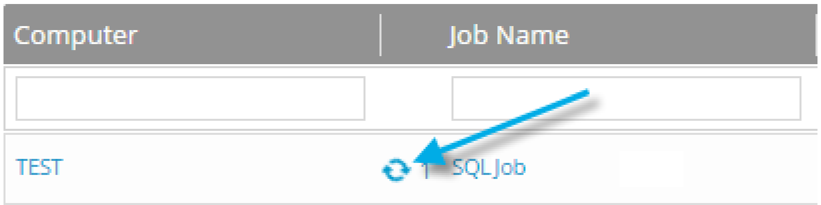
In the Process Details dialog box, you can view information about running, queued and recently-completed processes for a job. Processes include backups, restores and synchronizations. Process information is typically deleted within an hour after the process ends.

To view current process information for a job:

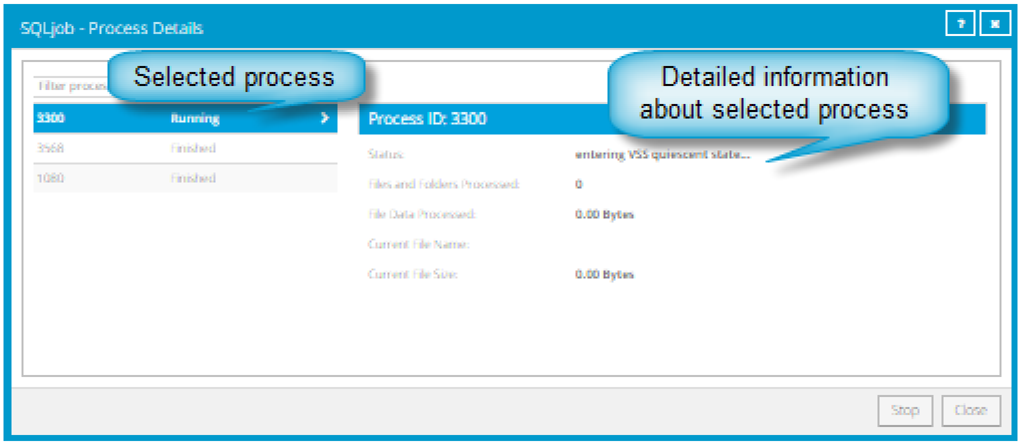
1. Do one of the following:
   - On the Computers page, on the Jobs tab, start a backup, restore or synchronization.
   - On the Computers page, on the Jobs tab, click the “In Progress” symbol beside the job name.



- On the Monitor page, click the “In Progress” symbol ⟳ beside the job name.



The **Process Details** dialog box lists processes that are running, queued and recently completed for the job. Detailed information is shown for the process that is selected on the left side of the dialog box.



| | |
|---|---|
| 3300 | Running |
| 3568 | Finished |
| 1080 | Finished |

Process ID: 3300

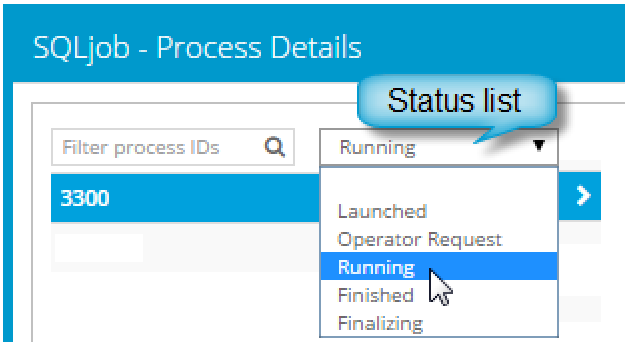
Status: entering VSS quiescent state...
Files and Folders Processed: 0
File Data Processed: 0.00 Bytes
Current File Name:
Current File Size: 0.00 Bytes

2. To view information about a different process, click the process on the left side of the dialog box.

   Detailed information for the process is shown at the right side of the dialog box.

3. To show only some processes in the dialog box, do one of the following in the status list:

   - To only show queued processes, click **Launched**.
   - To only show processes that are waiting for user action, click **Operator Request**.
   - To only show processes that are in progress, click **Running**.
   - To only show completed processes, click **Finished**.
   - To only show processes that are finishing, click **Finalizing**.



## 5.4 Monitor backups using email notifications

To make it easier to monitor backups, users can receive emails when backups finish or fail. Admin users and regular users in Portal can set up email notifications for a computer. See Set up email notifications for backups on a computer.

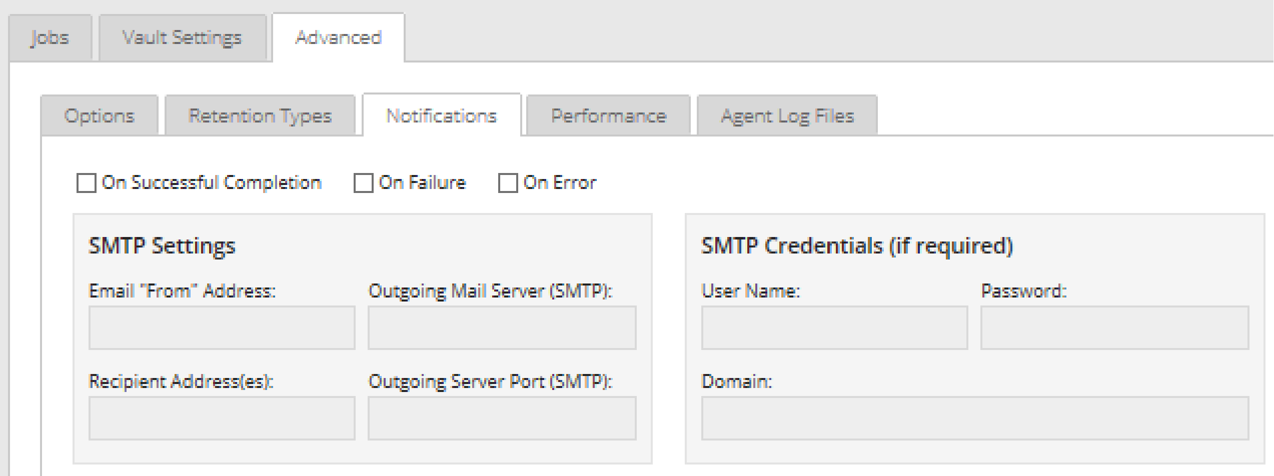
In some Portal instances, email notifications are configured centrally for , instead of separately for each computer. See Set up email notifications for backups on multiple computers.

### 5.4.1 Set up email notifications for backups on a computer

To set up email notifications for a computer:

1. On the navigation bar, click **Computers**.
2. Find the Agent for which you want to configure email notifications, and click the row to expand its view.
3. On the **Advanced** tab, click the **Notifications** tab.

   If the **Notifications** tab appears, but a policy is assigned to the Agent, you cannot change values on the **Notifications** tab. Instead, notifications can only be modified in the policy.



   Select one or more of the following checkboxes:

- **On failure**. If selected, users receive an email notification when a backup or restore fails. If a backup fails, you cannot recover any files from the backup.
- **On error**. If selected, users receive an email notification when a backup or restore completes with errors in the log file. You cannot recover files that are backed up with errors, but you can restore other files from the backup (safeset).
- **On successful completion.** If selected, users receive an email notification when a backup or restore completes successfully. You can recover files from a backup that completes, even if there are warnings in the log file.

Email notifications are sent separately for each backup and restore. For example, if three backup jobs fail on a computer and **On failure** is selected for the computer, three notification emails are sent.

If users will receive email notifications after backups and restores, specify the following email notification information:

| | |
|---|---|
| Email "From" Address | Email address from which email notifications will be sent. |
| Outgoing Mail Server (SMTP) | Network address of the SMTP that will send the email. |
| Recipient Address(es) | Email notification recipient email addresses, separated by commas. These should be real, valid email addresses. If one or more is not valid, the transmission to those addresses will fail, and errors will appear in the log files. |
| Outgoing Server Port (SMTP) | Port number for sending email notifications. |
| SMTP Credentials | If required, SMTP username, domain, and password. |

4. Click **Save**.

## 5.4.2 Set up email notifications for backups on multiple computers

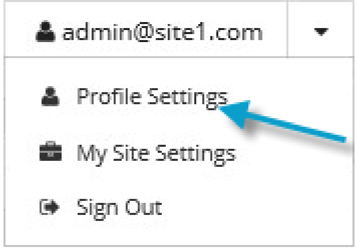
By default in some Portal instances, Admin users receive emails when backups fail, or are cancelled, deferred, missed or completed. Admin users can select backup statuses for which they want to receive email notifications. These email notifications are sent for , instead of separately for each computer.

For other computers, and in Portal instances where Admin users do not automatically receive email notifications, notifications must be configured separately for each computer. See Set up email notifications for backups on a computer.

To set up email notifications for backups on multiple computers:

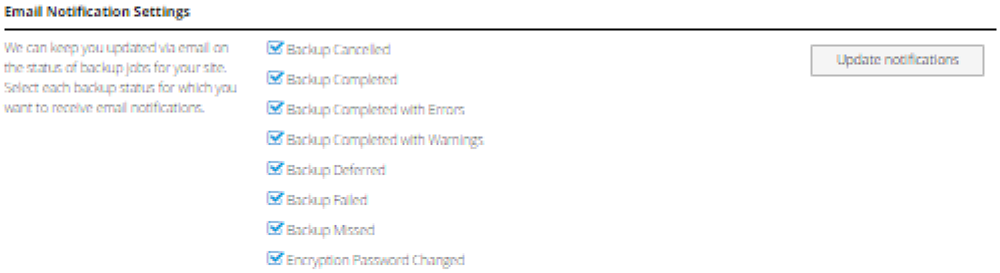
1. When signed in as an Admin user, click your email address at the top right of the Portal page.

   The user menu appears.



2. Click **Profile Settings**.

   Your user profile appears. If your profile includes an Email Notification Settings section with a list of backup events (e.g., Backup Canceled, Backup Completed), you can select events for which you want to receive emails.



**Email Notification Settings**

We can keep you updated via email on the status of backup jobs for your site. Select each backup status for which you want to receive email notifications.

☑ Backup Cancelled<br>
☑ Backup Completed<br>
☑ Backup Completed with Errors<br>
☑ Backup Completed with Warnings<br>
☑ Backup Deferred<br>
☑ Backup Failed<br>
☑ Backup Missed<br>
☑ Encryption Password Changed

   If Email Notifications Settings do not appear, you must set up notifications separately for each computer. See Set up email notifications for backups on a computer.

3. In the Email Notification Settings list, select any of the following events for which you want to receive emails:

   - Backup Cancelled
   - Backup Completed
   - Backup Completed with Errors
   - Backup Completed with Warnings
   - Backup Deferred
   - Backup Failed
   - Backup Missed

4. Click **Update notifications**.

## 5.5 View a job's process logs and safeset information

To determine whether a backup or restore completed successfully, or to determine why a process failed, you can view a job's process logs.

You can also view information about safesets created for the job. A safeset is an instance of backup data on the vault. For most Agents, one safeset is created by each successful backup.

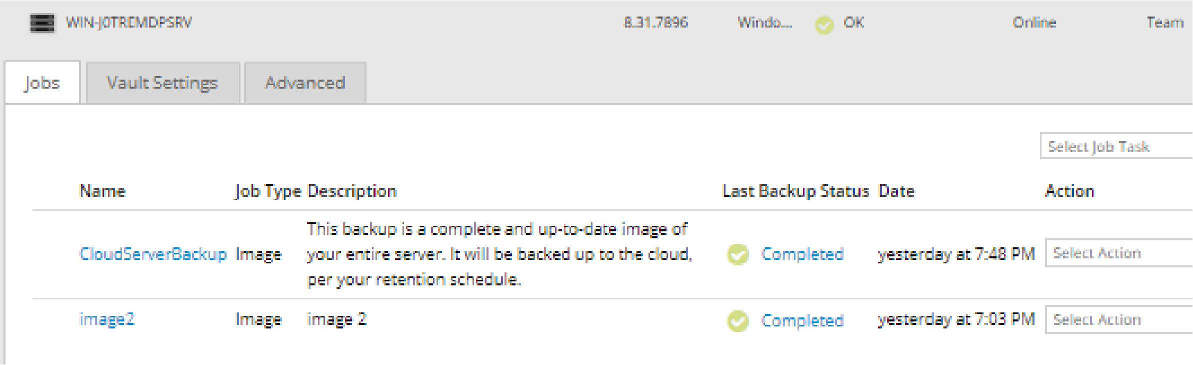
To view a job’s process logs and safeset information:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered Agents.

2. Find the Agent for which you want to view logs, and click the row to expand its view.

   On the **Jobs** tab, the **Last Backup Status** column shows the status of each backup job.



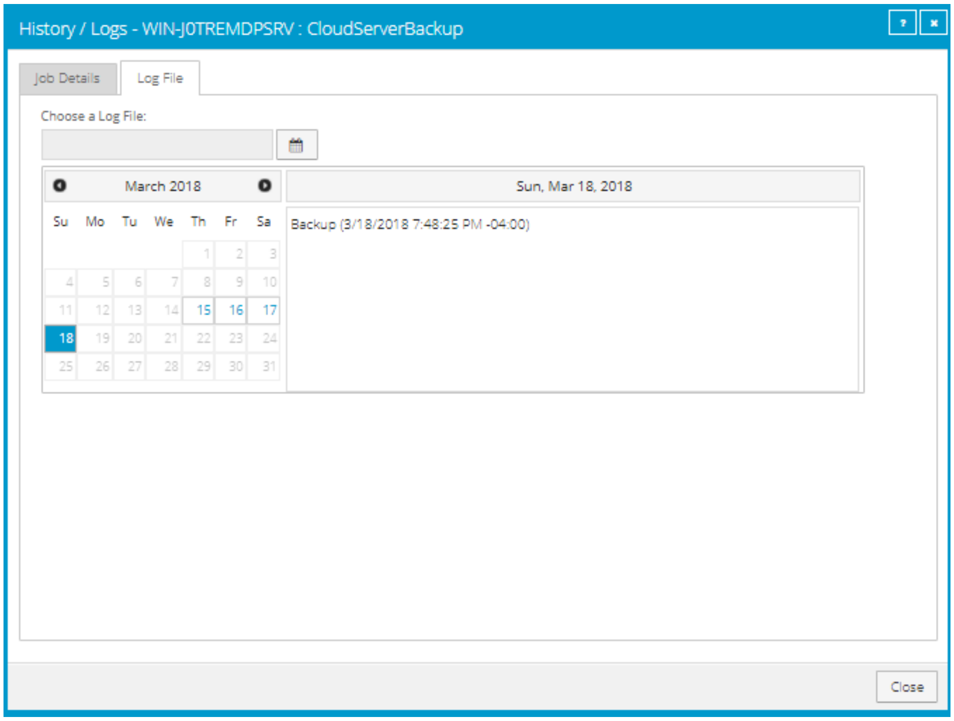
| WIN-J0TREMDPSRV | 8.31.7896 | Windo... | OK | Online | Team |
|---|---|---|---|---|---|

| Name | Job Type | Description | Last Backup Status | Date | Action |
|---|---|---|---|---|---|
| CloudServerBackup | Image | This backup is a complete and up-to-date image of your entire server. It will be backed up to the cloud, per your retention schedule. | Completed | yesterday at 7:48 PM | Select Action |
| image2 | Image | image 2 | Completed | yesterday at 7:03 PM | Select Action |

3. To view log files for a job, do one of the following:

   - In the job’s **Select Action** menu, click **History / Logs**.
   - In the **Last Backup Status** column, click the job status.

   The **History / Logs** window lists the most recent backups, restores and synchronizations on the computer.

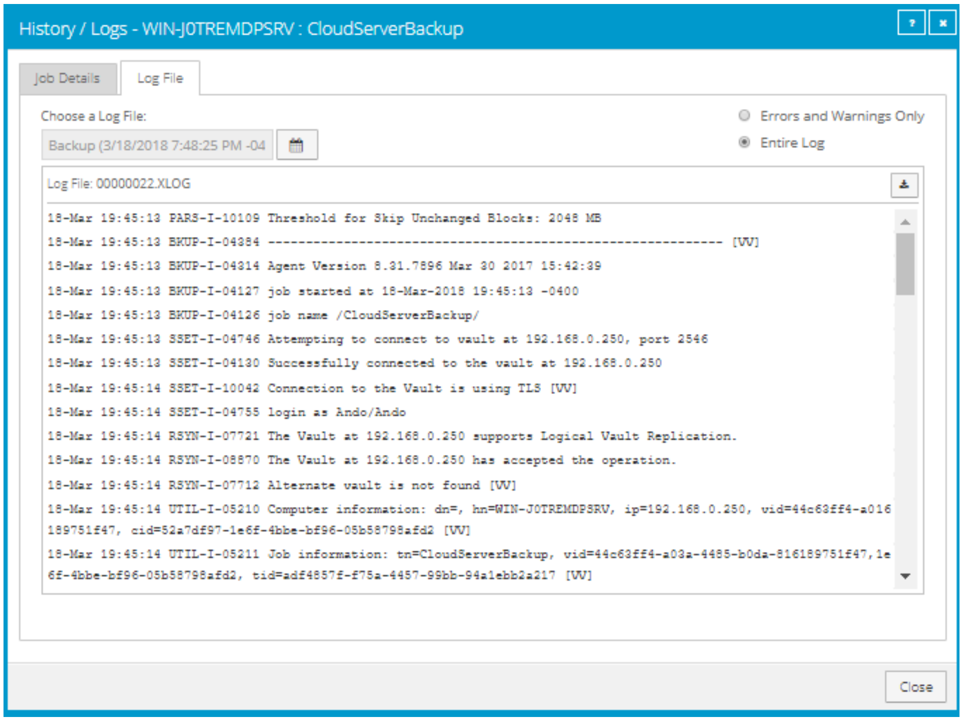


History / Logs - WIN-J0TREMDPSRV : CloudServerBackup

Backup (3/18/2018 7:48:25 PM -04:00)

4. To view processes for a different day, click the calendar button. 📅 In the calendar that appears, click the date of the log that you want to view. In the list of processes on the selected date, click the process for which you want to view the log.

   The **History / Logs** window shows the selected log.



Choose a Log File: Backup (3/18/2018 7:48:25 PM -04

○ Errors and Warnings Only
● Entire Log

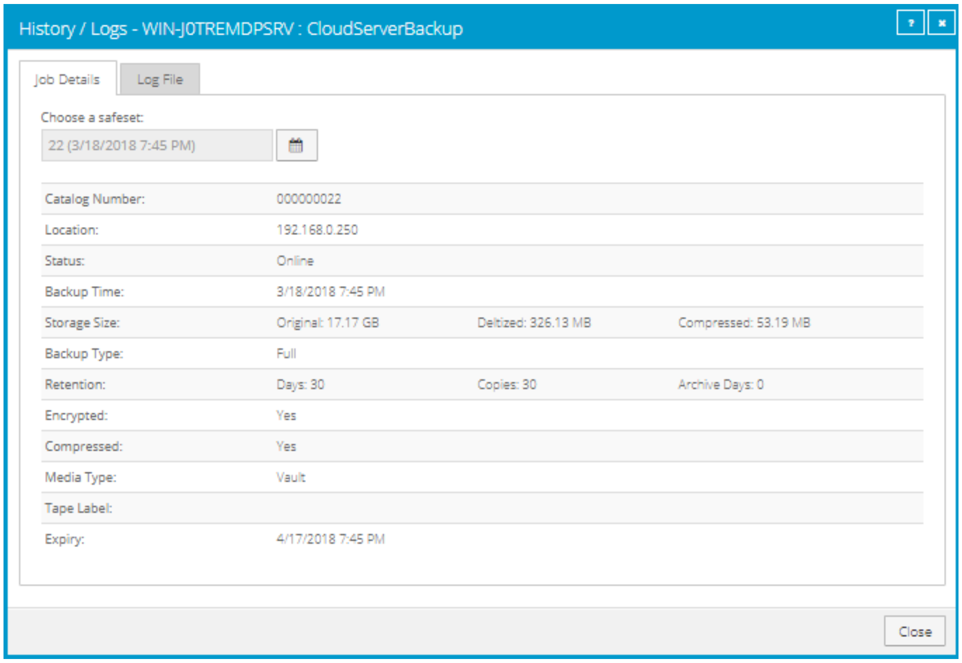
Log File: 00000022.XLOG

```
18-Mar 19:45:13 PARS-I-10109 Threshold for Skip Unchanged Blocks: 2048 MB
18-Mar 19:45:13 BKUP-I-04384 ------------------------------------------------------------ [VV]
18-Mar 19:45:13 BKUP-I-04314 Agent Version 8.31.7896 Mar 30 2017 15:42:39
18-Mar 19:45:13 BKUP-I-04127 job started at 18-Mar-2018 19:45:13 -0400
18-Mar 19:45:13 BKUP-I-04126 job name /CloudServerBackup/
18-Mar 19:45:13 SSET-I-04746 Attempting to connect to vault at 192.168.0.250, port 2546
18-Mar 19:45:13 SSET-I-04130 Successfully connected to the vault at 192.168.0.250
18-Mar 19:45:14 SSET-I-10042 Connection to the Vault is using TLS [VV]
18-Mar 19:45:14 SSET-I-04755 login as Ando/Ando
18-Mar 19:45:14 RSYN-I-07721 The Vault at 192.168.0.250 supports Logical Vault Replication.
18-Mar 19:45:14 RSYN-I-08870 The Vault at 192.168.0.250 has accepted the operation.
18-Mar 19:45:14 RSYN-I-07712 Alternate vault is not found [VV]
18-Mar 19:45:14 UTIL-I-05210 Computer information: dn=, hn=WIN-J0TREMDPSRV, ip=192.168.0.250, vid=44c63ff4-a016
189751f47, cid=52a7df97-1e6f-4bbe-bf96-05b58798afd2 [VV]
18-Mar 19:45:14 UTIL-I-05211 Job information: tn=CloudServerBackup, vid=44c63ff4-a03a-4485-b0da-816189751f47,1e
6f-4bbe-bf96-05b58798afd2, tid=adf4857f-f75a-4457-99bb-94a1ebb2a217 [VV]
```

5. To only show errors and warnings in the log, click the **Errors and Warnings Only** option at the top right of the window.

6. To view safeset information for a particular backup, click the **Job Details** tab. The tab shows safeset information for the job's most recent backup.

   To view information for a different safeset, click the calendar button. 📅 In the calendar that appears, click the date of the backup for which you want to view information. In the list of backups on the selected date, click the backup for which you want to view information. The tab shows safeset information for the selected backup.



Choose a safeset: 22 (3/18/2018 7:45 PM)

| | | | |
|---|---|---|---|
| Catalog Number: | 000000022 | | |
| Location: | 192.168.0.250 | | |
| Status: | Online | | |
| Backup Time: | 3/18/2018 7:45 PM | | |
| Storage Size: | Original: 17.17 GB | Deltized: 326.13 MB | Compressed: 53.19 MB |
| Backup Type: | Full | | |
| Retention: | Days: 30 | Copies: 30 | Archive Days: 0 |
| Encrypted: | Yes | | |
| Compressed: | Yes | | |
| Media Type: | Vault | | |
| Tape Label: | | | |
| Expiry: | 4/17/2018 7:45 PM | | |

## 5.6 View and export recent backup statuses

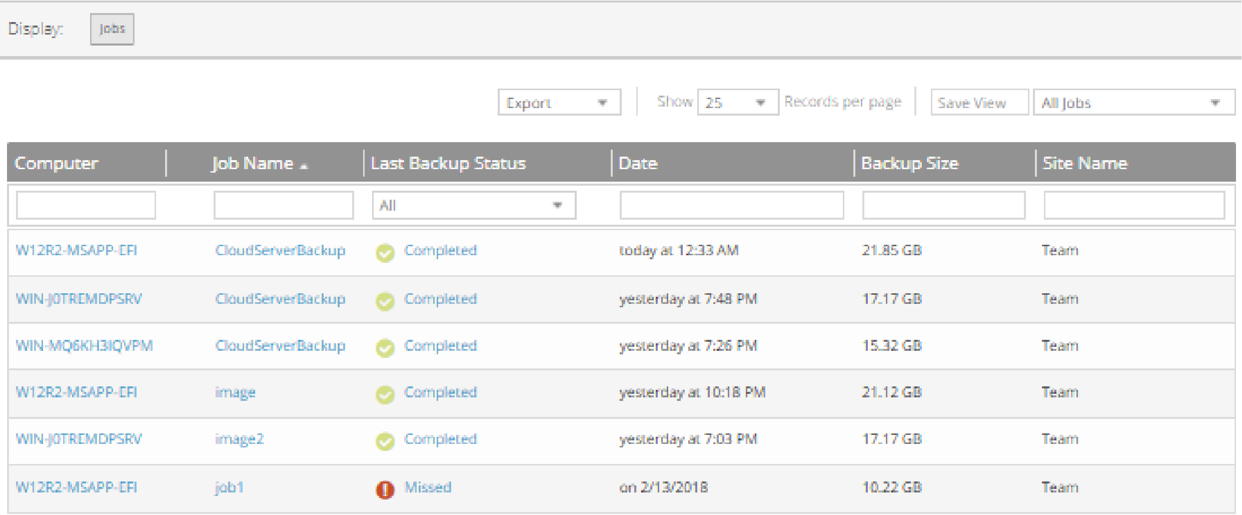
You can view recent backup statuses for computers on the Monitor page in Portal. You can also export the information in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format.

From the Monitor page, you can navigate to related information on the Computers page or in the Logs window.

To view and export recent backup statuses:

1. On the navigation bar, click **Monitor**.

   The Monitor page shows recent backup statuses for jobs in your site.

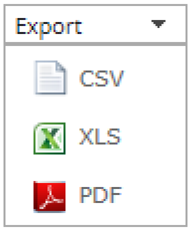


Show 25 Records per page; All Jobs

| Computer | Job Name | Last Backup Status | Date | Backup Size | Site Name |
|---|---|---|---|---|---|
| | | All | | | |
| W12R2-MSAPP-EFI | CloudServerBackup | ✓ Completed | today at 12:33 AM | 21.85 GB | Team |
| WIN-J0TREMDPSRV | CloudServerBackup | ✓ Completed | yesterday at 7:48 PM | 17.17 GB | Team |
| WIN-MQ6KH3IQVPM | CloudServerBackup | ✓ Completed | yesterday at 7:26 PM | 15.32 GB | Team |
| W12R2-MSAPP-EFI | image | ✓ Completed | yesterday at 10:18 PM | 21.12 GB | Team |
| WIN-J0TREMDPSRV | image2 | ✓ Completed | yesterday at 7:03 PM | 17.17 GB | Team |
| W12R2-MSAPP-EFI | job1 | ! Missed | on 2/13/2018 | 10.22 GB | Team |

2. To change which backup statuses appear on the page, click the views list at the top of the page, and then click the view that you want to apply.
3. To view information for a job or computer on the Computers page, click the name of an online computer or job.
4. To view the job's logs in the History/Logs window, click the job's last backup status.
5. To export backup status information from the page, click the **Export** box. In the list that appears, click one of the following formats for the exported data file:

   - CSV (comma-separated values)
   - XLS (Microsoft Excel)
   - PDF (Adobe Acrobat)

   The data file is downloaded to your computer in the specified format.