

SQL Server Plug-in 8.7

User Guide

© Copyright Owner 2018. All Rights Reserved.

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.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval System or translated into any language including computer language, in any form or by any means electronic, mechanic, magnetic, optical, chemical or otherwise without prior written permission.

All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

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.

"Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright (C) 2001-2006 Robert A. van Engelen, Genivia inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

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	December 2018	Initial guide provided for SQL Server Plug-in 8.7x.

Contents

1	Introduction to the SQL Server Plug-in	3
1.1	Required permissions.....	3
2	Add a SQL Server Plug-in backup job	4
3	Protect SQL Server databases in AlwaysOn Availability Groups.....	8
4	Protect SQL Server clusters	9
5	Run and schedule backups and synchronizations.....	10
5.1	Schedule a backup.....	11
5.2	Specify whether scheduled backups retry after a failure	15
5.3	Run an ad-hoc backup.....	16
5.4	Synchronize a job	17
6	Restore SQL Server databases.....	19
6.1	Restore databases directly to SQL Server	19
6.2	Restore SQL Server databases to flat files.....	21
6.3	Restore a SQL Server master database	22
6.4	Restore SQL Server database files or objects from Image backups	23
6.5	Restore databases in AlwaysOn Availability Groups.....	25
7	Restore items from a SQL Server or SharePoint database	26
8	Delete jobs and computers, and delete data from vaults	28
8.1	Delete a backup job without deleting data from vaults.....	28
8.2	Delete a backup job and delete job data from vaults	29
8.3	Cancel a scheduled job data deletion	32
8.4	Delete a computer without deleting data from vaults	33
8.5	Delete an online computer and delete computer data from vaults	34
8.6	Cancel a scheduled computer data deletion.....	36
9	Monitor computers, jobs and processes.....	38
9.1	View computer and job status information	38
9.2	View an unconfigured computer's logs.....	40

9.3	View current process information for a job	41
9.4	Monitor backups using email notifications	43
9.5	View a job's process logs and safeset information	45
9.6	View and export recent backup statuses	48

1 Introduction to the SQL Server Plug-in

To protect Microsoft SQL Server databases, install the SQL Server Plug-in with the Windows Agent on the machine where SQL Server is running. You can then add and run backup jobs that specify which SQL Server databases to back up and where to save the backup data.

The SQL Server Plug-in can back up databases that span volumes, databases that have Transparent Data Encryption (TDE) enabled and databases in AlwaysOn Availability Groups. The Plug-in can also back up BLOB data from filestream-enabled databases. You can run full database backups, full database with transaction logs backups or transaction log only backups.

Note: You can only back up transaction logs for databases that use the full or bulk-logged recovery model.

When installed with the Cluster Support Plug-in, the SQL Server Plug-in can protect databases on SQL Server clusters. For more information about the Cluster Support Plug-in, see the Portal help or Windows Agent guide.

After a SQL Server database is backed up, you can restore the database to the SQL Server instance where it was backed up, to a different instance or to flat files on disk. In a single pass, the Plug-in can restore a database from a full backup and transaction log backups to its state at a selected point in time.

You can also use the SQL Server Plug-in to back up Microsoft SharePoint databases. You can restore entire SharePoint databases or restore individual SharePoint items (e.g., site collections, web sites, lists, documents) using the SQL Server Plug-in and the Granular Restore for Microsoft SharePoint application.

For installation and configuration information, see the Windows Agent guide or Portal online help. For supported platform information, see the Windows Agent release notes.

Note: You can also back up SQL Server databases using the Windows Agent and Image Plug-in version 7.5 or later. For more information, see the Image Plug-in guide or Portal online help.

1.1 Required permissions

In addition to permissions required for the Windows Agent, the account specified during the Agent and SQL Server Plug-in installation must have the public server role to perform full SQL Server backups.

The account must have the "sysadmin" role to perform transaction log backups.

2 Add a SQL Server Plug-in backup job

After a Windows computer with the SQL Server Plug-in is added and configured in Portal, you can create a backup job for one or more databases in a SQL Server instance. The backup job specifies which database or databases to back up, and where to save the backup data. A SQL Server Plug-in job cannot include databases from multiple SQL Server instances.

You can also back up a SharePoint database with a SQL Server Plug-in job.

When you create a SQL Server database backup job, you must specify Windows administrator or SQL Server administrator credentials that allow the Agent to connect to the instance where you are backing up databases.

To back up the data, you can run the backup job manually or schedule the job to run. When scheduling or running a job, you can specify whether to back up the database, the transaction logs, or both. See [Run and schedule backups and synchronizations](#).

From the backup, you can restore an entire database. You can also use a Granular Restore application to restore specific items from the database. See [Restore items from a SQL Server or SharePoint database](#).

To add a SQL Server database backup job:

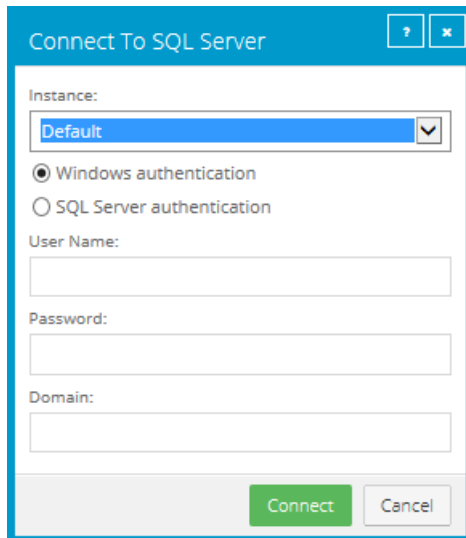
1. On the navigation bar, click **Computers**.

The Computers page shows registered computers.

2. Find a Windows computer with the SQL Server 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. For information about adding a vault connection, see the Portal help.

4. In the **Select Job Task** menu, click **Create New SQL Server Job**.
5. In the **Connect to SQL Server** dialog box, specify the following information:
 - In the **Instance** list, select the SQL Server instance where you want to back up databases.
 - To connect to the instance using a Windows administrator account, select **Windows authentication**.
 - To connect to the instance using a SQL Server administrator account, select **SQL Server authentication**.
 - In the **User Name** box, type the user name for connecting to the instance.
 - In the **Password** box, type the password of the specified user.
 - If you selected Windows authentication, in the **Domain** box, type the domain of the specified account.



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.

8. In the **Select Databases for Backup** box, do one or more of the following to add databases to the backup job:

- To add specific databases to the backup job, select the check box for each database, and then click **Include**. The included databases appear in the **Backup Set** box.
- To back up all databases in the selected SQL Server instance, select the check box for the instance, and then click **Include**. The included instances appear in the **Backup Set** box.

Note: When the job runs, newly-added databases in the selected instance are automatically backed up.

- To back up databases with names that match a filter when the job runs, select the check box for the SQL Server instance, and then click **Include**. An inclusion record with an asterisk (*) appears in the **Backup Set** box.

In the **Database Filter** box, enter the names of databases to include. Separate multiple names with commas, and use asterisks (*) and question marks (?) as wildcard characters. For example, to back up databases with names that end with “Management” or include the word “database” followed by a single character, enter the following filter: *management, database?

Note: Filters are applied when the backup job runs. New databases that match the specified filters are automatically backed up when the job runs.

Note: Filters are not case-sensitive.


9. To exclude databases from the backup job, do one or more of the following in the **Select Databases for Backup** box:

- To exclude specific databases from the backup job, select the check box for each database, and then click **Exclude**. The excluded databases appear in the **Backup Set** box.
- To exclude databases with names that match a filter when the backup job runs, select the check box for the SQL Server instance, and then click **Exclude**. A record with an asterisk (*) appears in the **Backup Set** box.

In the **Database Filter** box, enter the names of databases to exclude. Separate multiple names with commas, and use asterisks (*) and question marks (?) as wildcard characters. For example, to exclude databases if their names begin with “M”, enter the following filter: m*

Note: Filters are applied when the backup job runs. New databases that match the specified filters are automatically excluded when the backup job runs.

Note: Filters are not case-sensitive.

10. To remove an inclusion or exclusion record from the **Backup Set** box, click the Delete button beside the record. 
11. Click **Apply Now** to consolidate and simplify records in the **Backup Set** box, if changes need to be applied.
12. Click **Create Job**.

The job is created, and the **View/Add Schedule** dialog box appears. You can now create a schedule for running the backup. See [Run and schedule backups and synchronizations](#).

Click **Cancel** if you do not want to create a schedule at this time.

3 Protect SQL Server databases in AlwaysOn Availability Groups

You can protect SQL Server databases in AlwaysOn Availability Groups using the Windows Agent and SQL Server Plug-in.

If you back up a database in a secondary replica, a copy-only backup of the database is performed. Copy-only backups do not affect the sequence of conventional SQL Server backups. Microsoft only supports copy-only backups of secondary databases (see <http://msdn.microsoft.com/en-us/library/hh245119.aspx>).

Note: If a backup job includes secondary databases and databases that are not in a secondary replica, a copy-only backup will be performed for all databases in the job. Do not include a secondary database in the same job as a standalone database.

To protect SQL Server databases in AlwaysOn Availability Groups, do one of the following:

- Install the Windows Agent and plug-in on the server where the primary replica is hosted. You can run a full backup of the primary databases, followed by full or transaction log backups. If the primary replica becomes a secondary replica after a failover, the Agent automatically runs copy-only database backups instead of full backups. Transaction log backups remain the same.
- Install the Windows Agent and plug-in on a server where a secondary replica is hosted. This backup strategy offloads backup processing to a non-primary server. You can run a copy-only backup of the secondary database, followed by copy-only or transaction log backups. If the secondary replica becomes the primary replica after a failover, the Agent automatically runs full backups instead of copy-only backups. Transaction log backups remain the same.

Note: If the availability mode of the secondary replica is asynchronous-commit, transaction logs on the secondary database could lag behind the primary replica database. If the secondary database is being backed up, data loss could occur.

- Install the Windows Agent and plug-in on the primary replica server and on secondary replica servers. This strategy ensures that backups continue even if one of the replicas is down. You can run a full backup on the primary replica, followed by full or transaction log backups. You can also run copy-only backups on the secondary replicas, followed by copy-only or transaction log backups.

If a SQL database in an AlwaysOn Availability Group is hosted on a SQL Server Failover Cluster Instance, install the Agent, SQL Server Plug-in and Cluster Plug-in on each physical node, and configure jobs on the virtual node. Full backups will run if the database is a primary database, and copy-only backups will run if the database is a secondary database.

For information about restoring SQL Server databases in AlwaysOn Availability Groups, see [Restore databases in AlwaysOn Availability Groups](#).

4 Protect SQL Server clusters

To protect a SQL Server cluster, you must install the Windows Agent with the Cluster Support Plug-in and SQL Server Plug-in on each node in the cluster. In Portal, you can then register a virtual server for the SQL Server role in Portal and create and run backup jobs on the virtual server. Backup jobs on a virtual server are automatically directed to the active cluster node and will not reseed after a failover.

To fully protect a SQL Server cluster, you must back up:

- the quorum disk
- each physical node in the cluster
- cluster volumes
- the SQL Server databases to provide point-in-time database recovery.

When a cluster is fully protected, you can recover the cluster if components are lost, are corrupted or fail.

For detailed information, see Windows cluster information in the Portal online help or the Windows Agent guide.

5 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.

If a SQL Server Plug-in backup job is deferred while a database is being backed up, the backup for that database is incomplete and the database cannot be restored. However, you can restore databases that were completely backed up in the job before the job was deferred. If the backup is deferred while a SharePoint database is being backed up, the backup is incomplete and you cannot restore items from the database.

Note: Backups to SSI files on disk cannot be deferred.

- For a SQL Server Plug-in backup job, you can specify whether to back up the database, the transaction logs, or both. Frequent transaction log backups are recommended for databases with a high level of activity.

Note: After a transaction log backup, logs are marked for truncation. If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.

Note: Transaction logs can only be backed up for databases that use the full or bulk-logged recovery model.

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](#).

5.1 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.

When scheduling multiple SQL Server database jobs in the same instance, it is good practice to schedule the jobs so that their running times do not overlap. Simultaneous backups are supported, but are not recommended.

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. In particular, avoid overlapping schedules for SQL Server database jobs in the same instance. Simultaneous backups in the same SQL Server instance are supported but are not recommended.

Retention	Backup Type	Schedule	Compression	Deferring (0 for none)	Enable	Priority	
Weekly	Full with	12:00 AM Sa	Better	0	None	<input checked="" type="checkbox"/>	▲ ▼
Daily	Full with	12:00 AM Su,Mo,Tu,We,Th,Fr,Sa	Better	0	None	<input checked="" type="checkbox"/>	▲ ▼

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**.

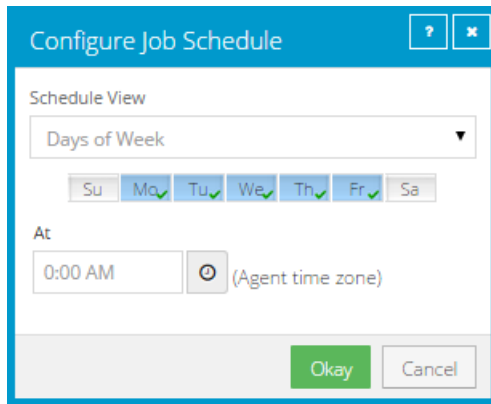
A new row appears in the dialog box.

3. In the new schedule row, in the **Retention** list, click a retention type.
4. Do one of the following in the **Backup Type** list:
 - To back up each database from the point in time when the backup starts, click **Full**.
 - To back up each database and its transaction logs from the point in time when the backup starts, click **Full with transaction logs**.
 - To back up the database transaction logs only from the point in time when the backup starts, click **Transaction logs only**. When **Transaction Logs only** is selected, the entire database and its transaction logs will be backed up when the job first runs. In subsequent backups, only the transaction logs will be backed up.

Note: After a transaction log backup, logs are marked for truncation. If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.

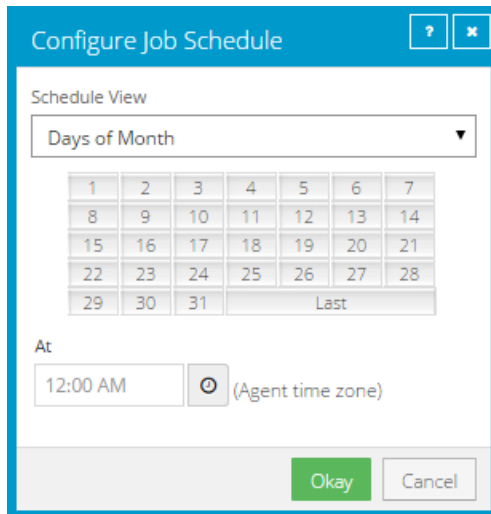
Note: Transaction logs can only be backed up for databases that use the full or bulk-logged recovery model.

5. In the **Schedule** box, click the arrow.
The **Configure Job Schedule** dialog box opens.
6. 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.



The screenshot shows the 'Configure Job Schedule' dialog box with the 'Schedule View' dropdown set to 'Days of Week'. Below the dropdown, there are seven buttons representing the days of the week: Su, Mo, Tu, We, Th, Fr, and Sa. The buttons for Mo, Tu, We, Th, and Fr are highlighted in blue and have a small green checkmark in the bottom right corner, indicating they are selected. The 'At' field is set to '0:00 AM' and has a clock icon and '(Agent time zone)' next to it. At the bottom, there are 'Okay' and 'Cancel' buttons.

- 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.

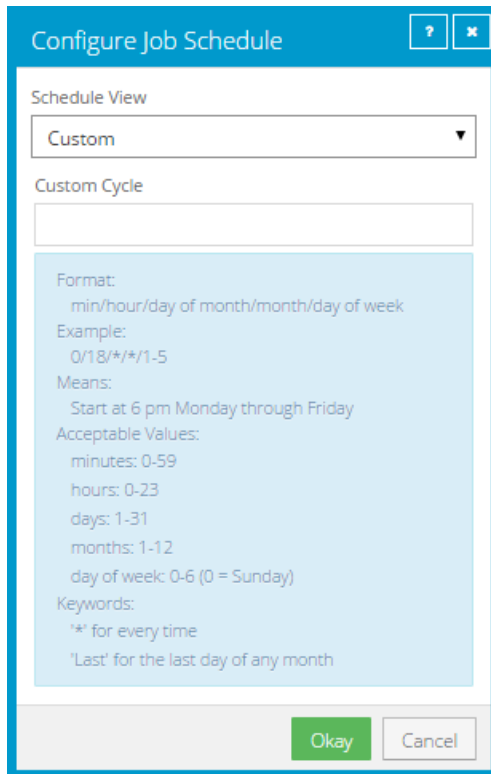


The screenshot shows the 'Configure Job Schedule' dialog box with the 'Schedule View' dropdown set to 'Days of Month'. Below the dropdown is a calendar grid with the following dates:

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			

The 'At' field is set to '12:00 AM' and has a clock icon and '(Agent time zone)' next to it. At the bottom, there are 'Okay' and 'Cancel' buttons.

- 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.



7. Click **Okay**.

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

8. 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.
9. 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.

10. To run the job on the specified schedule, select the **Enable** check box near the end of the row.
11. If there is more than one schedule row, you can use the **Priority** arrows to change the order of the schedule rows. Schedules higher in the list have a higher priority than schedules lower in the list.

If a job is scheduled to run at the same time by multiple schedules, the job only runs once at the scheduled time. If the schedules have different retention types, the job only runs with the retention type of the schedule that is highest in the list.

12. 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](#).
13. Click **Save**.

5.2 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.

The screenshot shows the 'View / Add Schedule' dialog box for a backup job named 'PROTECTEDSERVER, CloudServerBackup'. The dialog has a table with columns: Retention, Schedule, Compression, Deferring (0 for none), Enable, and Priority. There are two rows of backup schedules. Below the table, the 'Automatic Retry for Scheduled Backups' section is highlighted with a red box. It contains a checked checkbox for 'Retry failed backup', a 'Number of retries' input field with the value '1', and a 'Wait before each retry attempt for' input field with the value '1' and the unit 'minutes'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

3. Click **Save**.

5.3 Run an ad-hoc backup

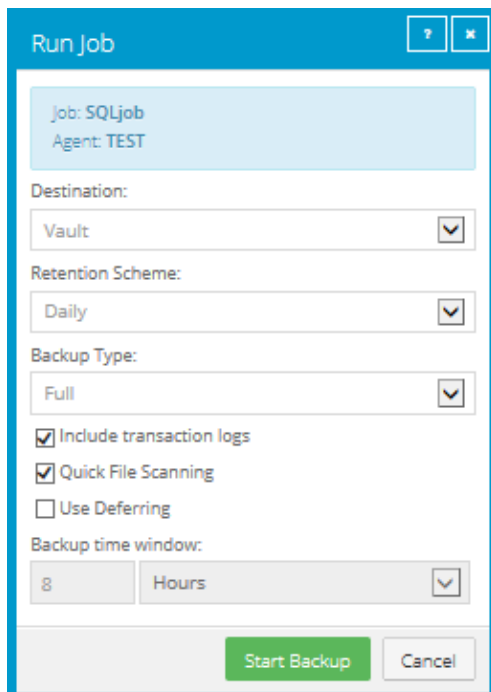
After a backup job is created, you can run the backup at any time, even if the job is scheduled to run at specific times. When running an ad-hoc backup, you can back up the data to a vault or to SSI files (safeset image) on disk.

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.



The screenshot shows a 'Run Job' dialog box with the following settings:

- Job: SQLjob
- Agent: TEST
- Destination: Vault
- Retention Scheme: Daily
- Backup Type: Full
- Include transaction logs
- Quick File Scanning
- Use Deferring
- Backup time window: 8 Hours
- Buttons: Start Backup, Cancel

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. Do one of the following:

- To back up the database, click **Full**. To also back up the database's transaction logs, select **Include transaction logs**.
- To back up transaction logs only, click **Transaction Log**. When **Transaction Log** is selected, the database and its transaction logs will be backed up when the backup first runs. In subsequent backups, only the transaction logs will be backed up.

Note: After a transaction log backup, logs are marked for truncation. If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.

Note: Transaction logs can only be backed up for databases that use the full or bulk-logged recovery model.

7. To enable Quick File Scanning, select the **Quick File Scanning** check box.

Quick File Scanning (QFS) reduces the amount of data read during the backup process. Any file streams that have not changed since the last backup are skipped. Without QFS, files are read in their entirety. Note that changes in delta-file format might cause QFS to be temporarily disabled during the first backup following an upgrade. This could cause this first backup to take longer than usual.

8. Do one of the following:

- To allow the backup job to run without a time limit, clear the **Use Deferring** check box.
- To specify a maximum amount of time that the backup job can run, select the **Use Deferring** check box. From the **Backup time window** list, select **Minutes** or **Hours**. 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 backup time window.

Note: The **Use Deferring** check box is not available if you are backing up data to SSI (safeset image) files on disk.

9. 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](#).

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

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

5.4 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. You must also enter the encryption passwords for the computer's existing backup jobs. .
- 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**.

6 Restore SQL Server databases

After backing up SQL Server databases using the SQL Server Plug-in, you can restore databases directly to a SQL Server instance, or restore databases to flat files. See [Restore databases directly to SQL Server](#) or [Restore SQL Server databases to flat files](#).

When restoring a SQL Server database in an Always On Availability Group, you must always restore the database to the primary replica. See [Restore databases in AlwaysOn Availability Groups](#).

6.1 Restore databases directly to SQL Server

After backing up SQL Server databases using the SQL Server Plug-in, you can restore databases directly to a SQL Server instance.

If transaction logs have been backed up using an alternative method (e.g., native SQL Server backup), you can restore a database in the restoring state so that you can apply transaction logs to the database after the restore.

You must specify a Windows or SQL Server administrator account for connecting to SQL Server during a restore.

After restoring a SQL Server 2016 database that is stretched to Microsoft Azure, you must run a stored procedure (`sys.sp_rda_reauthorize_db`) to reconnect the local restored database to the remote Azure data. See “Restore the connection between the SQL Server database and the remote Azure database” on the Microsoft Developer Network website: <https://msdn.microsoft.com/en-us/library/mt733205.aspx#reconnect>

To restore a database directly to SQL Server:



1. On the navigation bar, click **Computers**.
A grid lists available computers.
2. Find the computer with the SQL Server database backup 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. In the job’s **Select Action** menu, click **Restore**.
5. In the **Choose how to restore** dialog box, select **Restore database to a SQL Server instance**.
6. In the **Instance** list, click the SQL Server instance where you want to restore the database.
7. Do one of the following:
 - To connect to the instance using a Windows administrator account, select **Windows authentication**. Enter the user name, password, and domain in the appropriate fields.

- To connect to the instance using a SQL Server administrator account, select **SQL Server authentication**. Enter the user name and password in the appropriate fields.

8. Click **Continue**.

The **SQL Server Restore** dialog box shows the most recent safeset for the job.


9. To restore data 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.

10. In the **Database Selection** box, select the check box for each database that you want to restore.

11. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 

12. Do one of the following:

- To restore one or more databases with their original names, select **Original Database Names**.
- To restore one database with a new name, select **Alternate Database Name**. In the field that appears, enter the new name for the restored database.

Note: You can only restore one database if **Alternate Database Name** is selected.


13. Do one of the following:

- To overwrite the existing database if you restore a database with the same name as the existing database, select **Overwrite existing databases**.
- To fail the restore if a database with the same name already exists, clear **Overwrite existing databases**.

If **Overwrite existing databases** is not selected, and you are restoring multiple databases, the restore fails for all databases if even one database has the same name as an existing database.

14. To restore the database in restoring state, select **Restore using No Recovery option**.

If this option is selected, and transaction logs have been backed up using an alternative method (e.g., native SQL Server backup), you can apply transaction logs to the database after it has been restored.

15. To specify an alternate location for database files, select **Alternate Path**. Click the folder button. 
In the **Select Folder** dialog box, select the alternate file location, and click **Okay**.

Note: The alternate file location is only used if the original location for database files is not available.

16. To change the log detail level, bandwidth throttling setting or hard recovery option, click **Advanced Restore Options**. In the dialog box, do one or more of the following:
 - In the **Log Level Detail** list, select the level of detail for job logging.
 - Select or clear the **Use all available bandwidth** option.
17. 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](#).

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

6.2 Restore SQL Server databases to flat files



After backing up SQL Server databases using the SQL Server Plug-in, you can restore a SQL Server database to flat files. SQL Server tools can then be used to bring the data into a database.

To restore a SQL Server database to flat files:

1. On the navigation bar, click **Computers**.
A grid lists available computers.
2. Find the computer with the SQL Server database backup 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 you want to restore, and click **Restore** in the **Select Action** menu for the job.
5. In the **Choose how to restore** dialog box, select **Restore to folder**.
6. Click **Continue**.



The **SQL Server Restore** dialog box shows the most recent safeset for the job.

7. To restore data 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.

8. In the **Database Selection** box, select the check box for each database that you want to restore.
9. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 
10. Under **Restore Destination**, enter a path for the destination, or click the folder button.  In the **Select Folder** dialog box, select the location where you want to restore, and click **Okay**.
11. To change the log detail level, bandwidth throttling setting or hard recovery option, click **Advanced Restore Options**. In the dialog box, do one or more of the following:
 - In the **Log Level Detail** list, select the level of detail for job logging.
 - Select or clear the **Use all available bandwidth** option.
12. 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](#).

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

6.3 Restore a SQL Server master database

In a SQL Server instance, a master database contains information about all other databases and configuration information for the instance. The master database must be restored by itself while the instance is offline.

Other system databases (i.e., msdb and model) can be restored while the SQL Server instance is online, and do not require a special restore procedure.

To restore a SQL Server master database:

1. Stop the SQL Server services on the machine where you want to restore the master database.
2. Manually copy the existing master database files (master.mdf and mastlog.ldf) to another location so they will not be overwritten.

These copies can be used to roll back the database if a problem occurs with the restored master database.

3. Restore the master database files (master.mdf and mastlog.ldf) from a SQL Server Plug-in backup or application-aware Image Plug-in backup. See [Restore SQL Server databases to flat files](#) or [Restore SQL Server database files or objects from Image backups](#).
4. Manually copy the master database files to the original location of the master database files (with replace).
5. Restart all SQL Server services.

6.4 Restore SQL Server database files or objects from Image backups

After backing up SQL Server databases using Image Plug-in version 7.5 or later, you can restore database files, tables and objects from the application-consistent backups.

To restore database files from Image Plug-in backups, you must mount a safeset as a drive on the computer where you want to restore database files. You can then restore files using Windows Explorer or tables and other objects using the Granular Restore for Microsoft Exchange and SQL application.



To restore SQL Server database files or objects from an Image Plug-in backup:

1. On the navigation bar, click **Computers**.
A grid lists available computers.
2. Find the computer with the SQL Server database backup created using the Image Plug-in, and expand its view by clicking the row for the computer.
3. Click the **Jobs** tab.
4. Find the job with the database you want to restore, and click **Restore** in the **Select Action** menu for the job.

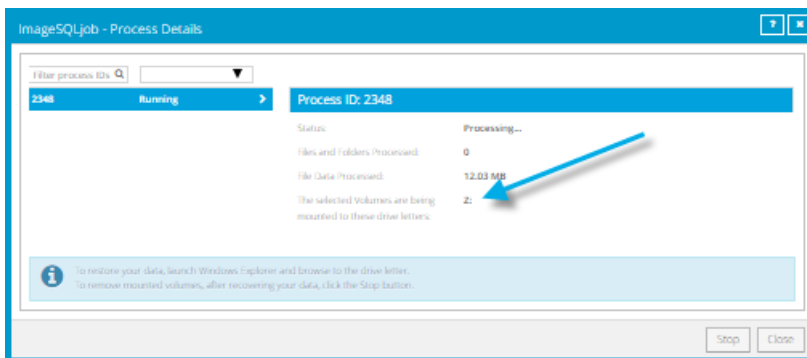
The **Choose how to restore** dialog box appears.

5. Select **Individual File or Folders**.
6. Click **Continue**.

The **Restore** dialog box shows the most recent safeset for the job.

7. 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.
8. In the **Idle Time** text box, enter the number of minutes of inactivity after which the share should automatically stop. This value can range from 2 to 180.
9. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 
10. In the **Volume to Restore** column, select each backed-up volume from which you want to restore files and folders.
11. In the **Volume Mount Drive Letter** column, choose the drive letter for mounting each volume.
12. Click **Mount Volumes**.
13. If a confirmation message appears, read the message, and then click **Continue**.

The **Process Details** dialog box appears. When each volume is mounted, the drive letter is shown at the right side of the dialog box.



14. Do one of the following:
 - To restore SQL Server databases, use Windows Explorer to browse to the location of the database files and copy the database files (.mdf and .ldf) that you want to restore. If a *databaseName_mod* folder exists, copy the *databaseName_mod* folder as well. You can then attach the database in Microsoft SQL Server.
 - To restore SQL Server database tables or objects, launch the Granular Restore for Microsoft Exchange and SQL application on a SQL Server system. In the Granular Restore application, choose **File > Open**, drill down into the volume to choose the .mdf file, then select and restore your data. For more information, see documentation for the Granular Restore for Microsoft Exchange and SQL application.
15. When you are done restoring database files, click **Stop** to remove the mounted drives.

If you do not click **Stop**, the drive will be unmounted automatically after the number of minutes of inactivity specified in the **Idle Time** box. See Step [8](#).

6.5 Restore databases in AlwaysOn Availability Groups

You must always restore a SQL Server database to the primary replica in an AlwaysOn Availability Group. If a Windows Agent and plug-in are not installed on the primary replica server, you must fail over to a server where the Agent and plug-in are installed before restoring the database.

After restoring a database to the primary replica and adding the database back into the AlwaysOn Availability Group, it will be replicated to the secondary replicas. To reduce the amount of replication traffic after a restore, you can run a “Restore from another computer” on any secondary replica server where the Windows Agent and plug-in are installed.

For information about backing up databases in AlwaysOn Availability Groups, see [Protect SQL Server databases in AlwaysOn Availability Groups](#).

To restore a primary database in an AlwaysOn Availability Group:

1. If the Agent and plug-in are not installed on the primary replica server, fail over to the secondary database instance where the Agent is installed.
The formerly secondary replica where you backed up the database becomes the primary replica.
2. Remove the primary database from the AlwaysOn Availability Group.
3. Delete the database from all secondary replicas.
4. Restore the primary database to the original database name using the Overwrite Existing Databases option.
5. Add the restored primary database to the AlwaysOn Availability Group using the Full Synchronization option.

After restoring a SQL Server database to the primary replica, to reduce the amount of required replication traffic, you can restore the database to secondary replica servers.

To restore a secondary database in an AlwaysOn Availability Group:

1. If you did not delete the database from all secondary replicas when restoring the primary database (see Step 3 in the previous procedure), remove the secondary database from the AlwaysOn Availability Group.
2. On a secondary replica server where the Agent and plug-in are installed, restore the database by running a Restore From Another Computer using the No Recovery option.
3. Add the restored secondary database to the AlwaysOn Availability Group using the Join option.

7 Restore items from a SQL Server or SharePoint database

If a Microsoft SharePoint database is backed up using the SQL Server Plug-in, you can restore items such as site collections, websites, lists and documents from the backup.

If a Microsoft SQL Server database is backed up using the SQL Server Plug-in or Image Plug-in, you can restore specific tables and objects from the backup.

To restore items from a database backup, you must first use Portal to expose the safeset as a shared resource. You can then use a Granular Restore application to find and restore items from the backup. To restore items from a SharePoint database backup, use Granular Restore for Microsoft SharePoint. To restore items from a SQL Server database backup, use Granular Restore for Microsoft Exchange and SQL. For more information, or to obtain a Granular Restore application, contact your service provider.

To restore items from a SQL Server or SharePoint database:

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



A grid lists available computers.

2. Find the computer with the safeset with SharePoint or SQL Server data that you want to restore, and expand its view by clicking the computer row.
3. Click the **Jobs** tab.
4. Find the job with the SharePoint data that you want to restore, and click **Restore** in the **Select Action** menu for the job.


The **Choose how to restore** dialog box appears.

5. Select **Restore items to a SharePoint or SQL Server database**, and click **Continue**.

The **SQL Server Restore** dialog box shows the most recent safeset for the job.

6. 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.
7. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 
8. In the **Idle Time** box, enter the number of minutes of inactivity after which the share should automatically stop. The value can range from 2 to 180 minutes.
9. Select or clear the **Use all available bandwidth** option.
10. Click **Share**.

The **Process Details** dialog box shows the status of the share process. When the share is available, the share path appears at the right side of the dialog box.

11. Click the Copy Path to Clipboard button.  The path is now available for you to paste into the Granular Restore application.
12. Do one of the following:
 - To restore SharePoint items, launch the Granular Restore for Microsoft SharePoint application on a SharePoint system.
 - To restore SQL Server database items, launch the Granular Restore for Microsoft Exchange and SQL application on a SQL Server system.
13. Paste the path for the SQL safeset share into the Granular Restore application.
14. Select and restore your data. For more information, see documentation for the Granular Restore application.
15. When you no longer need to share the safeset, click **Stop**.

When you click **Stop** or the share idle time is reached, the **Process Details** dialog box indicates that the share is no longer available.

8 Delete jobs and computers, and delete data from vaults

Regular users and Admin users can delete backup jobs from Portal without deleting associated data from vaults. See [Delete a backup job without deleting data from vaults](#). Admin users can delete computers from Portal without deleting associated data from vaults. See [Delete a computer without deleting data from vaults](#).

In a Portal instance where the data deletion feature is enabled, Admin users can also:

- Delete backup jobs from Portal and submit requests to delete the job data from vaults. See [Delete a backup job and delete job data from vaults](#).
- Delete online computers from Portal and submit requests to delete the computer data from vaults. See [Delete an online computer and delete computer data from vaults](#).

After an Admin user submits a request to delete job or computer data from vaults, there is a 72-hour waiting period before the data is deleted. During this waiting period, Admin users in the site can cancel the data deletion. See [Cancel a scheduled job data deletion](#) and [Cancel a scheduled computer data deletion](#).

8.1 Delete a backup job without deleting data from vaults

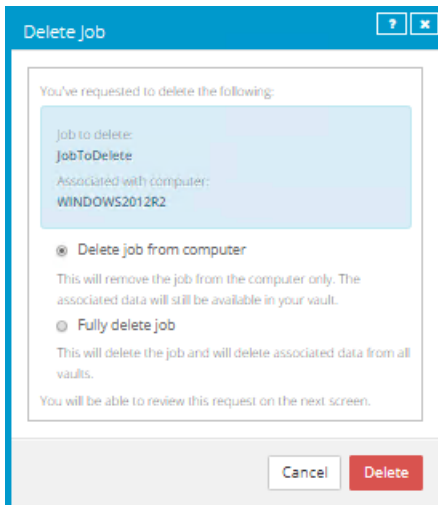
Regular users and admin users can delete backup jobs from online computers without deleting the job data from vaults. If a job is deleted from Portal in this way, the data can still be restored using the *Restore from Another Computer* procedure.

In a Portal instance where the data deletion feature is enabled, Admin users can submit requests to delete job data from vaults when they delete jobs from Portal. See [Delete a backup job and delete job data from vaults](#).

To delete a backup job without deleting data from vaults:

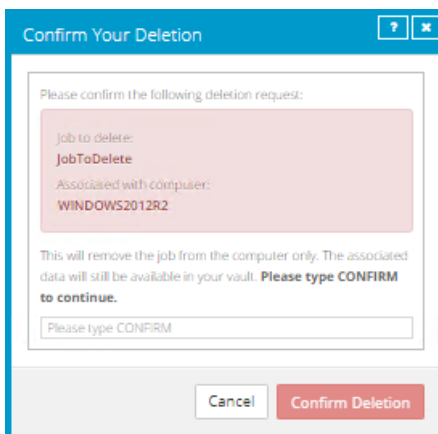
1. On the navigation bar, click **Computers**.
The Computers page shows registered computers.
2. Find the online Agent with the job that you want to delete, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. In the **Select Action** menu of the job that you want to delete, click **Delete Job**.
5. If you are signed in as an Admin user in a Portal instance where the data deletion feature is enabled, a Delete Job dialog box appears.

To delete the backup job without deleting data from vaults, click **Delete job from computer** and then click **Delete**.



Note: The Delete Job dialog box does not appear if you cannot delete backup data in vaults because your Portal instance does not support vault data deletion or you are signed in as a regular user.

A confirmation dialog box asks you to confirm the deletion request.



6. In the text box, type **CONFIRM**.

Note: You must type **CONFIRM** in capital letters.

7. Click **Confirm Deletion**.

8.2 Delete a backup job and delete job data from vaults

In a Portal instance where the data deletion feature is enabled, Admin users can delete backup jobs and request that data for the jobs be deleted from all vaults. The data deletion is scheduled for 72 hours after the request is made and an email notification is sent to Admin users in the site and to Super users.

During the 72-hour waiting period before job data is deleted, Admin users can cancel scheduled job data deletions in their sites. See [Cancel a scheduled job data deletion](#).

If a scheduled job data deletion is not canceled during the 72-hour waiting period, the job is deleted from Portal, the deletion request is sent to vaults and job data is automatically deleted from associated vaults. If

data for a job cannot be deleted for some reason, an email notification is sent to a vault administrator. The vault administrator can then manually delete the data.

WARNING: Job data deletion is permanent. After the data is deleted from vaults, it cannot be recovered or restored.

To delete a backup job and delete job data from vaults:

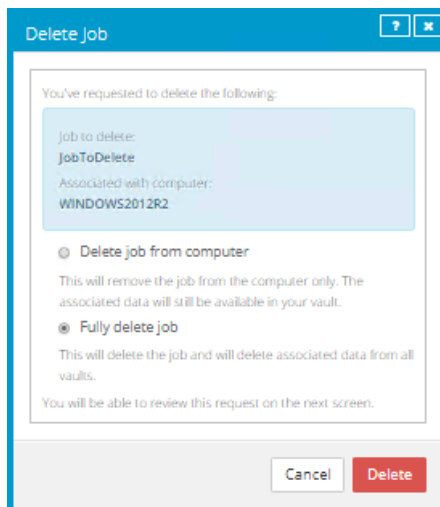
1. When signed in as an Admin user, click **Computers** on the navigation bar.

The Computers page shows registered computers.

2. Find the Agent with the job that you want to delete, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. In the **Select Action** menu of the job that you want to delete, click **Delete Job**.

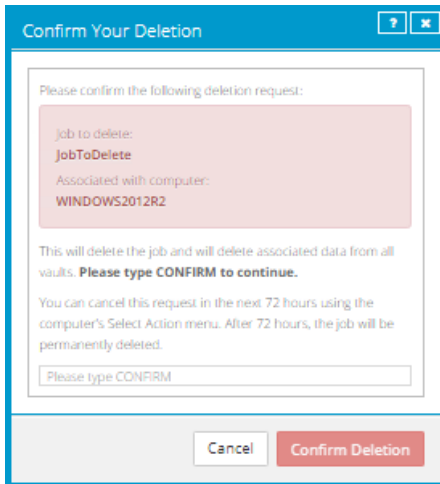
A Delete Job dialog box appears if the data deletion feature is enabled in your Portal instance.

Note: If the Delete Job dialog box does not appear, you cannot request that data for the job be deleted from vaults. You can only delete the job from Portal. See [Delete a backup job without deleting data from vaults](#).



5. Select **Fully delete job**, and then click **Delete**.

A confirmation dialog box asks you to confirm the deletion request.

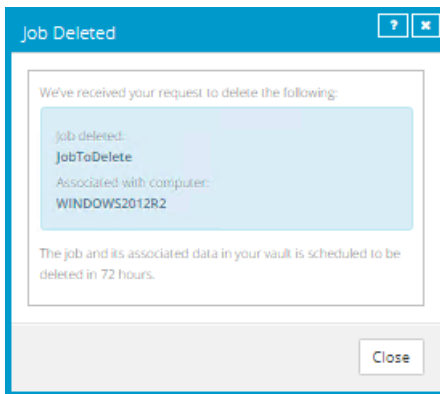


8. In the text box, type **CONFIRM**.

Note: You must type **CONFIRM** in capital letters.

9. Click **Confirm Deletion**.

A Job Deleted dialog box states that the job and associated data in your vaults is scheduled to be deleted.



10. Click **Close**.

The Last Backup Status column shows *Scheduled For Deletion* for the job. The Date column shows the date when the job will be deleted from Portal and job data will be deleted from vaults. Within a day of the scheduled deletion, the Date column will also show the time when the job and its data will be deleted.

An email is sent to Admin users in the site and to Super users to indicate that the job deletion has been scheduled.

JobToDelete	Local System	Scheduled For Deletion on 8/10/2018	Select Action
-------------	--------------	-------------------------------------	---------------

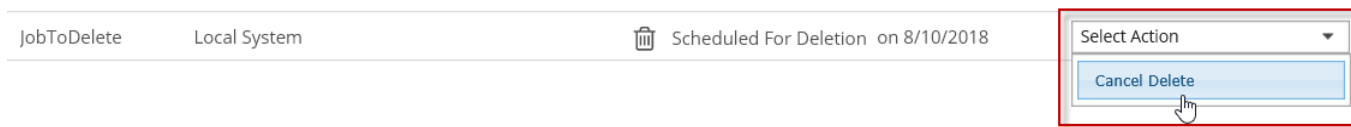
8.3 Cancel a scheduled job data deletion

In a Portal instance where the data deletion feature is enabled, Admin users can delete a backup job and request that data for the job be deleted from all vaults. The data deletion is scheduled for 72 hours after the request is made and an email notification is sent to Admin users in the site and to Super users.

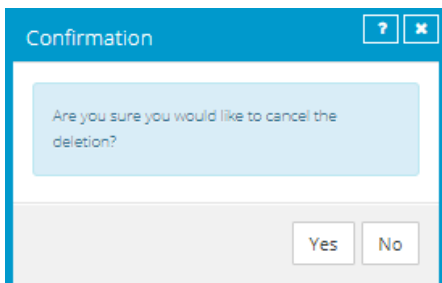
During the 72-hour period before a job is deleted from Portal and the job data is deleted from vaults, Admin users in the site can cancel the data deletion. If a scheduled data deletion is canceled, an email notification is sent to Admin users in the site and to Super users.

To cancel a scheduled job data deletion:

1. When signed in as an Admin user, click **Computers** on the navigation bar.
The Computers page shows registered computers.
2. Find the Agent with the scheduled job data deletion that you want to cancel, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. In the Select Action menu of the job that is scheduled for deletion, click **Cancel Delete**.



A confirmation dialog box asks whether you want to cancel the deletion.



5. Click **Yes**.

Values in the Last Backup Status and Date columns for the job revert to the values that appeared before the job was scheduled for deletion.

An email is sent to Admin users in the site and to Super users to indicate that the scheduled job deletion has been canceled.



8.4 Delete a computer without deleting data from vaults

Admin users can delete computers from Portal without deleting the computer data from vaults. If a computer is deleted from Portal in this way, the data can still be restored using the *Restore from Another Computer* procedure. You can delete both online and offline computers from Portal without deleting data from vaults.

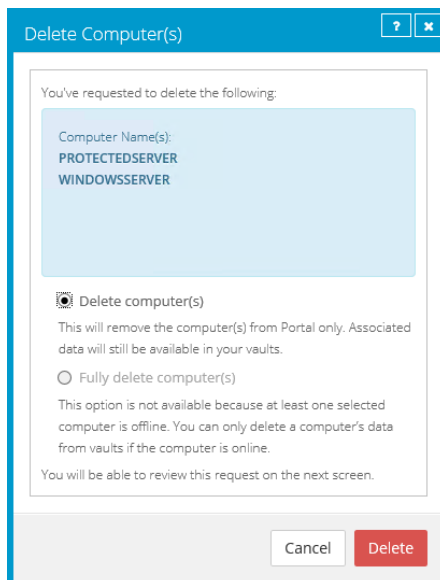
To delete a computer without deleting data from vaults:

1. When signed in as an Admin user, click **Computers** on the navigation bar.

The Computers page shows registered computers.

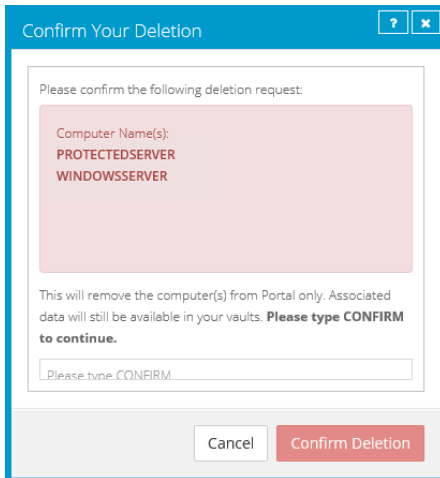
2. Select the check box for each computer that you want to delete.
3. In the **Actions** list, click **Delete Selected Computer(s)**.
4. If the data deletion feature is enabled in your Portal instance, a Delete Computer(s) dialog box appears.

To delete the computer without deleting data from vaults, click **Delete computer(s)** and then click **Delete**.



Note: The Delete Computer(s) dialog box only appears if your Portal instance supports vault data deletion.

A confirmation dialog box asks you to confirm the deletion request.



5. In the text box, type **CONFIRM**.

Note: You must type **CONFIRM** in capital letters.

6. Click **Confirm Deletion**.
7. In the confirmation dialog box, click **Yes**.
8. In the Success dialog box, click **Okay**.

8.5 Delete an online computer and delete computer data from vaults

In a Portal instance where the data deletion feature is enabled, Admin users can delete online computers and request that data for the computers be deleted from all vaults. The data deletion is scheduled for 72 hours after the request is made and an email notification is sent to Admin users in the site and to Super users.

Note: You cannot delete data from vaults for offline computers, but you can delete offline computers from Portal. See [Delete a computer without deleting data from vaults](#).

During the 72-hour waiting period before computer data is deleted, Admin users can cancel scheduled computer data deletions in their sites. See [Cancel a scheduled computer data deletion](#).

If a scheduled computer data deletion is not canceled during the 72-hour waiting period, the computer is deleted from Portal, the deletion request is sent to vaults and job data is automatically deleted from associated vaults. If data for a computer cannot be deleted for some reason, an email notification is sent to a vault administrator. The vault administrator can then manually delete the data.

WARNING: Computer data deletion is permanent. After the data is deleted from vaults, it cannot be recovered or restored.

To delete an online computer and delete computer data from vaults:

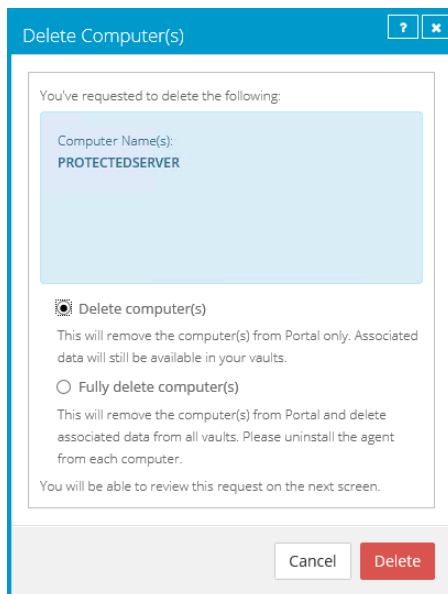
1. When signed in as an Admin user, click **Computers** on the navigation bar.

The Computers page shows registered computers.

2. Select the check box for each online computer that you want to delete.
3. In the **Actions** list, click **Delete Selected Computer(s)**.

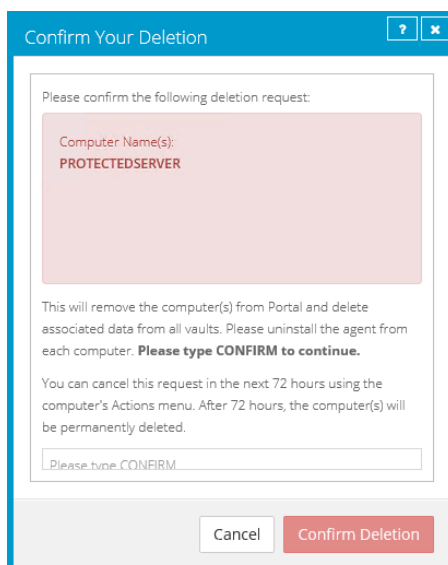
A Delete Computer(s) dialog box appears if the data deletion feature is enabled in your Portal instance. The **Fully delete computer(s)** option is available if no offline computers are selected.

Note: If the Delete Computer(s) dialog box does not appear or the **Fully delete computer(s)** option is not available, you cannot request that data for the selected computers be deleted from vaults. You can only delete the selected computers from Portal. See [Delete a computer without deleting data from vaults](#).



4. Select **Fully delete computer(s)**, and then click **Delete**.

A confirmation dialog box asks you to confirm the deletion request.

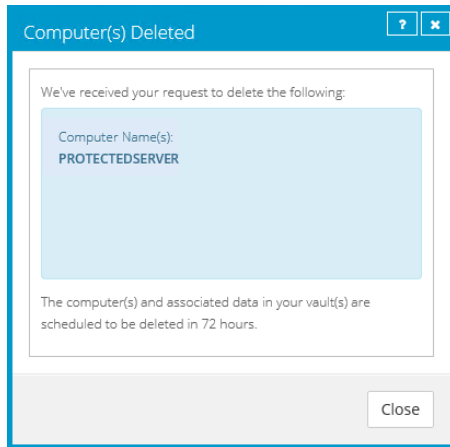


- In the text box, type **CONFIRM**.

Note: You must type **CONFIRM** in capital letters.

- Click **Confirm Deletion**.

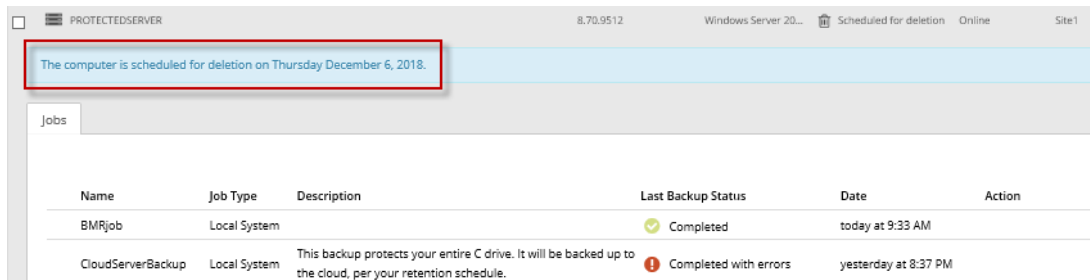
A Computer(s) Deleted dialog box states that the computer(s) and associated data in your vault(s) are scheduled to be deleted.



- Click **Close**.

The Status column shows *Scheduled for deletion* for the computer(s). If you expand the computer, a message indicates when the computer is scheduled to be deleted.

You cannot add, edit, run, schedule or delete jobs for a computer that is scheduled for deletion. Existing backup jobs continue to run as scheduled until the computer is deleted.



8.6 Cancel a scheduled computer data deletion

In a Portal instance where the data deletion feature is enabled, Admin users can delete an offline computer and request that data for the computer be deleted from all vaults. The data deletion is scheduled for 72 hours after the request is made and an email notification is sent to Admin users in the site and to Super users.

During the 72-hour period before a computer is deleted from Portal and the computer data is deleted from vaults, Admin users in the site can cancel the data deletion. If a scheduled data deletion is canceled, an email notification is sent to Admin users in the site and to Super users.

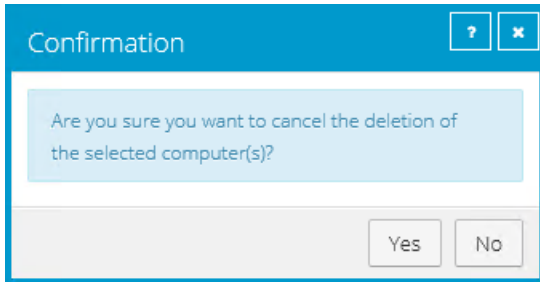
To cancel a scheduled computer data deletion:

1. When signed in as an Admin user, click **Computers** on the navigation bar.

The Computers page shows registered computers.

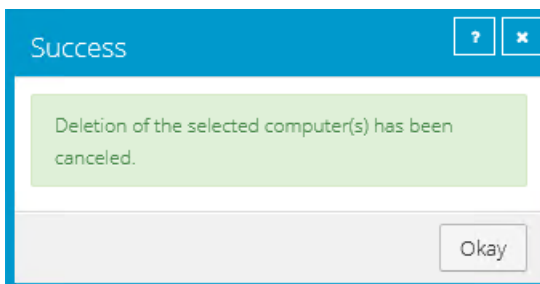
2. Select the check box for each Agent for which you want to cancel the scheduled data deletion.

A confirmation dialog box asks whether you want to cancel the deletion.



3. Click **Yes**.

A Success dialog box appears.



4. Click **Okay**.

The value in the Status column for each computer reverts to the value that appeared before the computer was scheduled for deletion.

An email is sent to Admin users in the site and to Super users to indicate that the scheduled computer deletion has been canceled.

9 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](#).

9.1 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. Typically, this status indicates that not all of the data was backed up.
-  Failed — Indicates that the backup failed and no safeset was created.
-  Cancelled
-  Scheduled for Deletion — Indicates that the job is scheduled to be deleted from Portal and job data is scheduled to be deleted from all vaults on the date shown in the Date column. This backup status is only possible in Portal instances where the data deletion feature is enabled.

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

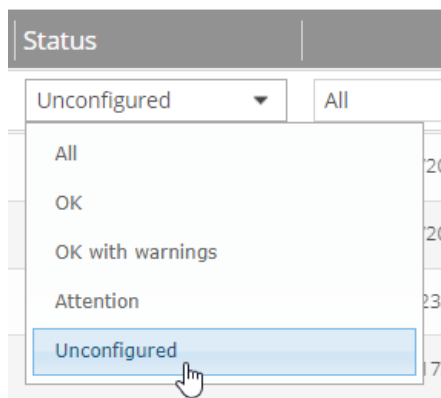
9.2 View an unconfigured computer's logs

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

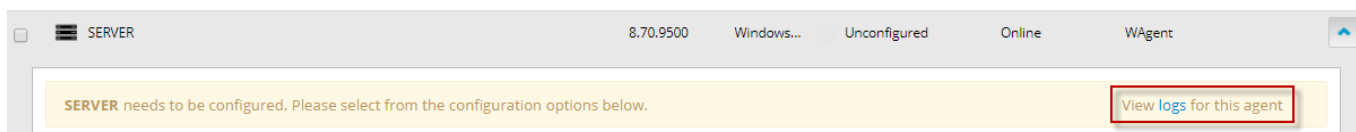
To view an unconfigured computer's logs:

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

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

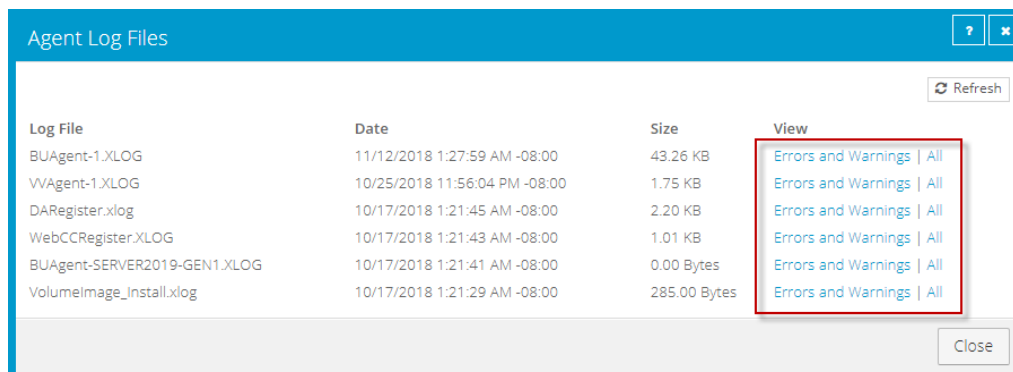


2. Find an unconfigured computer that is online, and expand its view by clicking the computer row.



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.



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.

```


LogName: BUAgent-1.XLOG
25-Nov 06:21:49 AGIIT-I-04314 Agent Version 8.30.7893 Nov 16 2016 14:12:22
25-Nov 06:21:49 AGIIT-I-08103 Executing agent as SYSTEM
25-Nov 06:21:49 AGIIT-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 AGIIT-I-07466 WII-4 thread started
25-Nov 06:21:49 AGIIT-I-08200 Agent HTTP thread started
25-Nov 06:21:49 AGIIT-I-08200 Agent HTTP thread started
25-Nov 06:21:49 AGIIT-I-08200 Agent HTTP thread started
25-Nov 06:21:50 AGIIT-I-08323 Agent is being redirected to server qa.corp.com on port 8087
25-Nov 06:21:50 AGIIT-I-09400 Agent HTTP binding to 127.0.0.1:8031
25-Nov 06:21:50 AGIIT-I-09400 Agent HTTP binding to :8031
25-Nov 06:21:54 AGIIT-I-07466 WII-4 thread started
25-Nov 06:21:55 AGIIT-E-08307 Failed to set the Agent status to offline.
25-Nov 06:22:01 AGIIT-E-08307 Failed to set the Agent status to offline.
25-Nov 06:22:11 AGIIT-E-08307 Failed to set the Agent status to offline.
25-Nov 06:22:16 AGIIT-I-08914 Agent type set to SERVER
25-Nov 06:22:16 AGIIT-E-07514 Failed to Upload System Info in Notification Thread
25-Nov 06:22:21 AGIIT-E-07514 Failed to Upload System Info in Notification Thread
25-Nov 06:22:26 AGIIT-E-07514 Failed to Upload System Info in Notification Thread
25-Nov 06:22:31 AGIIT-E-07477 Failed to Upload Feature Options in Notification Thread
25-Nov 06:22:36 AGIIT-E-07477 Failed to Upload Feature Options in Notification Thread
25-Nov 06:22:41 AGIIT-E-07477 Failed to Upload Feature Options in Notification Thread
25-Nov 06:22:46 AGIIT-E-07476 Failed to Upload Job Types in Notification Thread

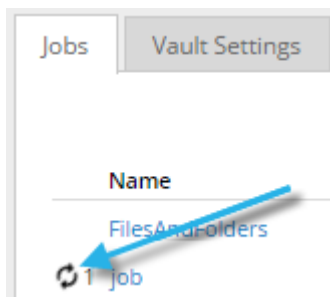
```

9.3 View current process information for a job

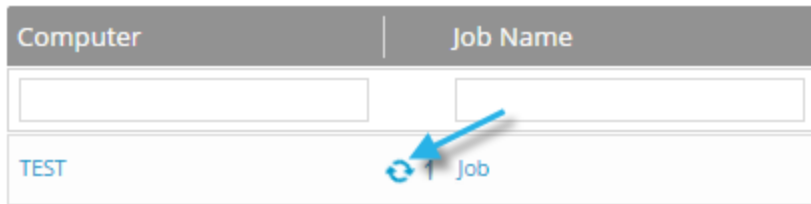
In the Process Details dialog box, you can view information about running, queued and recently-completed processes for a job. Processes include backups, restores and synchronizations. Process information is typically deleted within an hour after the process ends.

To view current process information for a job:

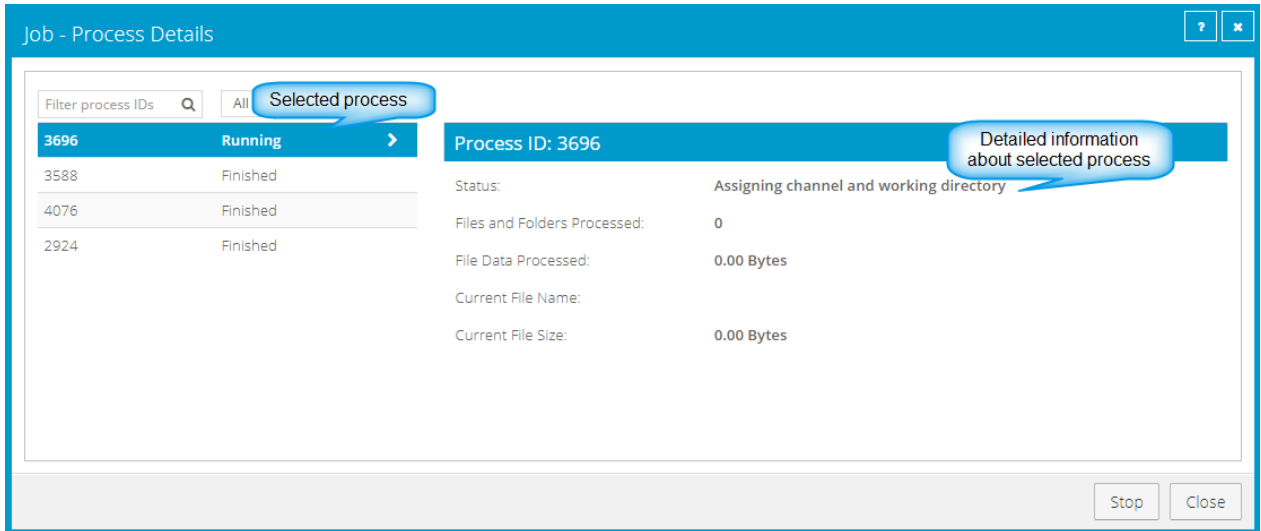
- Do one of the following:
 - On the Computers page, on the Jobs tab, start a backup, restore or synchronization.
 - On the Computers page, on the Jobs tab, click the “In Progress” symbol  beside the job name.



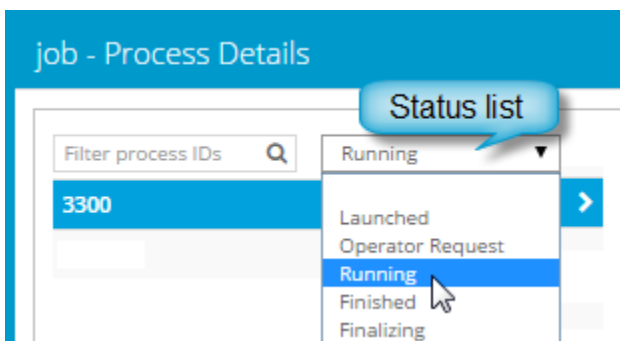
- On the Monitor page, click the “In Progress” symbol  beside the job name.



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.



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**.



9.4 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 Windows systems with Agent version 8.0 or later, instead of separately for each computer. See [Set up email notifications for backups on multiple computers](#).

9.4.1 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.

The screenshot shows the 'Advanced' configuration page for an agent. The 'Notifications' sub-tab is selected, showing three checkboxes: 'On Successful Completion', 'On Failure', and 'On Error'. Below these are two main sections: 'SMTP Settings' and 'SMTP Credentials (if required)'. The 'SMTP Settings' section includes fields for 'Email "From" Address', 'Outgoing Mail Server (SMTP)', 'Recipient Address(es)', and 'Outgoing Server Port (SMTP)'. The 'SMTP Credentials (if required)' section includes fields for 'User Name', 'Password', and 'Domain'.

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**.

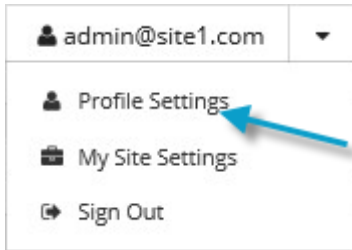
9.4.2 Set up email notifications for backups on multiple computers

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 Windows systems with Agent version 8.0 or later, 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
- Backup Completed
- Backup Completed with Errors
- Backup Completed with Warnings
- Backup Deferred
- Backup Failed
- Backup Missed
- Encryption Password Changed

Update notifications

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**.

9.5 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.

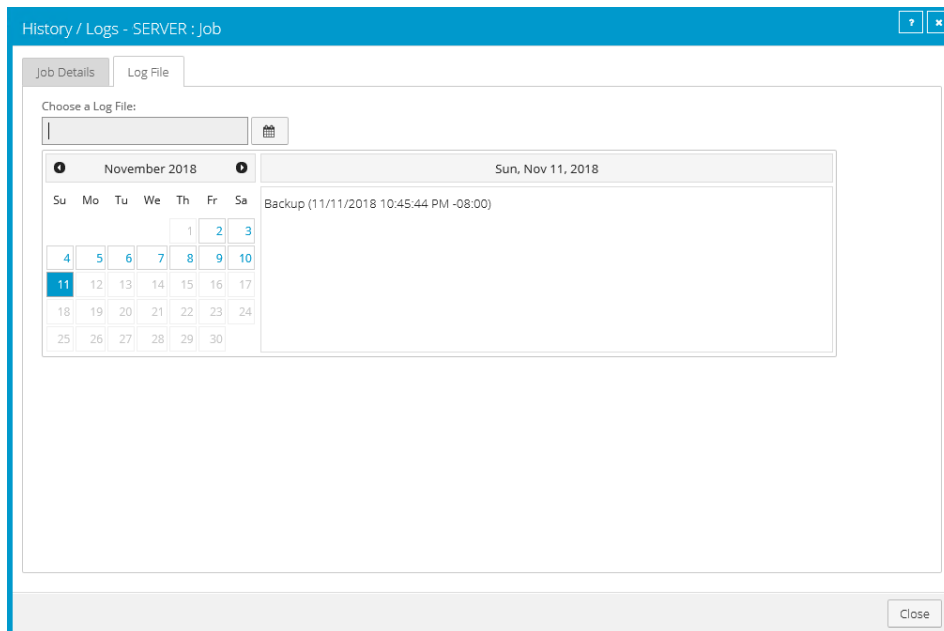
On the **Jobs** tab, the **Last Backup Status** column shows the status of each backup job.

Name	Job Type	Description	Last Backup Status	Date	Action
BMRjob	Local System		Completed	today at 9:31 AM	Select Action
CloudServerBackup	Local System	This backup protects your entire C drive. It will be backed up to the cloud, per your retention schedule.	Completed	yesterday at 7:32 PM	Select Action
Job	Local System		Completed with warnings	yesterday at 10:45 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.

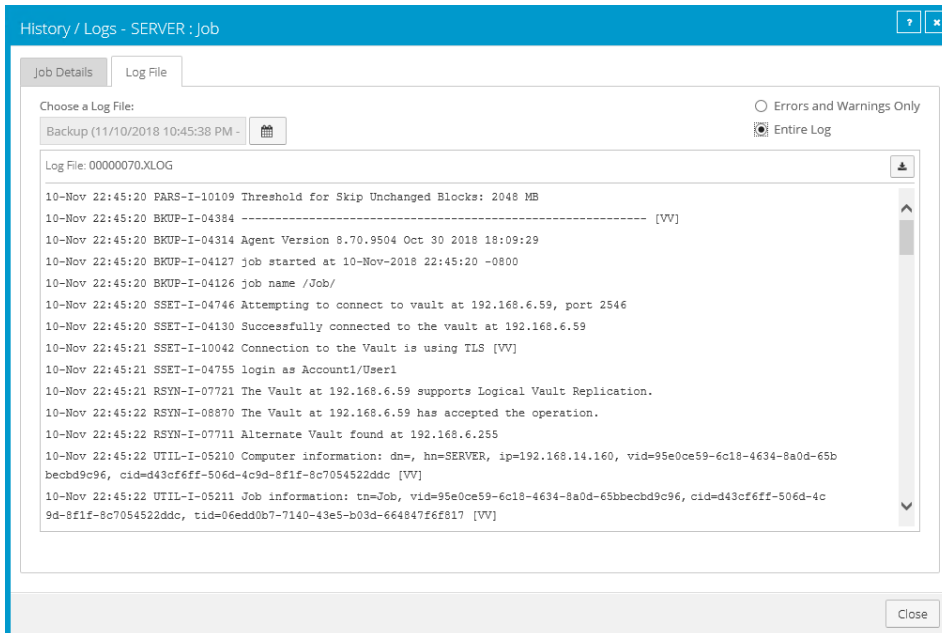
The **History / Logs** window lists the most recent backups, restores and synchronizations on the computer.



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.

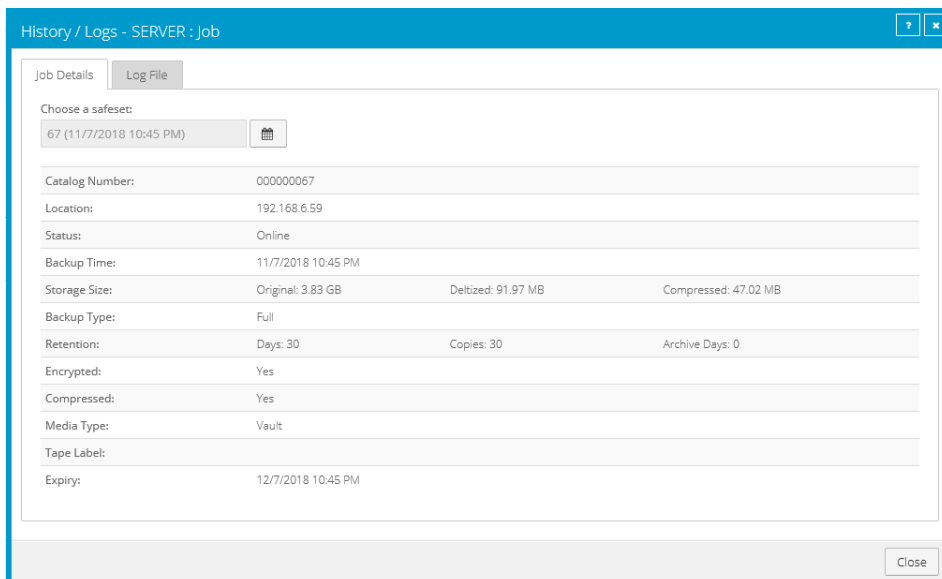
- In the list of processes on the selected date, click the process for which you want to view the log.

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



- To only show errors and warnings in the log, click the **Errors and Warnings Only** option at the top right of the window.
- To view safeset information for a particular backup, click the **Job Details** tab. The tab shows safeset information for the job's most recent vault backup.

To view information for a different safeset, click the calendar icon. 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.



9.6 View and export recent backup statuses

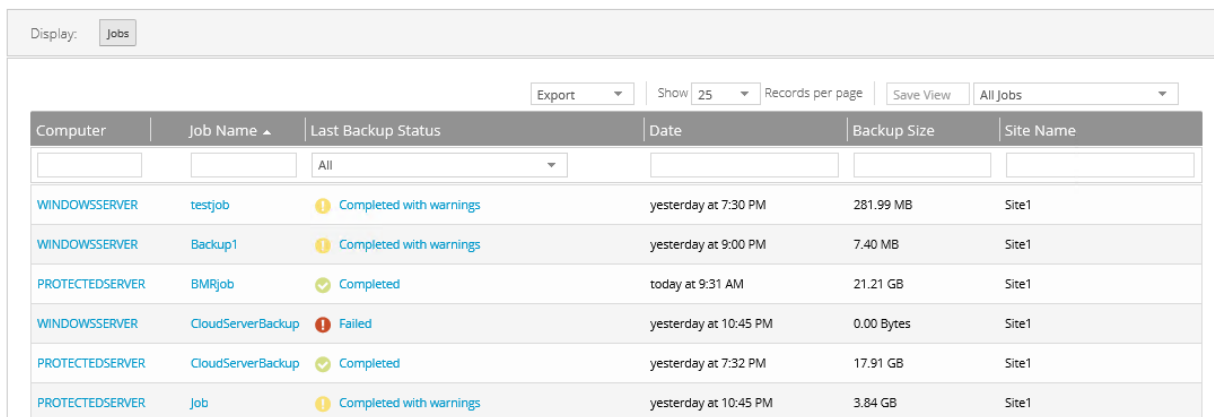
You can view recent backup statuses for computers on the Monitor page in Portal. You can also export the information in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format.

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:

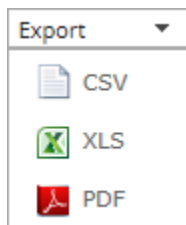
1. On the navigation bar, click **Monitor**.

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



Computer	Job Name	Last Backup Status	Date	Backup Size	Site Name
WINDOWSSERVER	testjob	Completed with warnings	yesterday at 7:30 PM	281.99 MB	Site1
WINDOWSSERVER	Backup1	Completed with warnings	yesterday at 9:00 PM	7.40 MB	Site1
PROTECTEDSERVER	BMRjob	Completed	today at 9:31 AM	21.21 GB	Site1
WINDOWSSERVER	CloudServerBackup	Failed	yesterday at 10:45 PM	0.00 Bytes	Site1
PROTECTEDSERVER	CloudServerBackup	Completed	yesterday at 7:32 PM	17.91 GB	Site1
PROTECTEDSERVER	Job	Completed with warnings	yesterday at 10:45 PM	3.84 GB	Site1

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.