CARBONITE®
an opentext™ company

Carbonite Server Backup

Windows Agent and Plug-ins 9.3

User Guide

Carbonite LLC
251 Little Falls Drive
Wilmington, DE 19808
www.carbonite.com

Version History

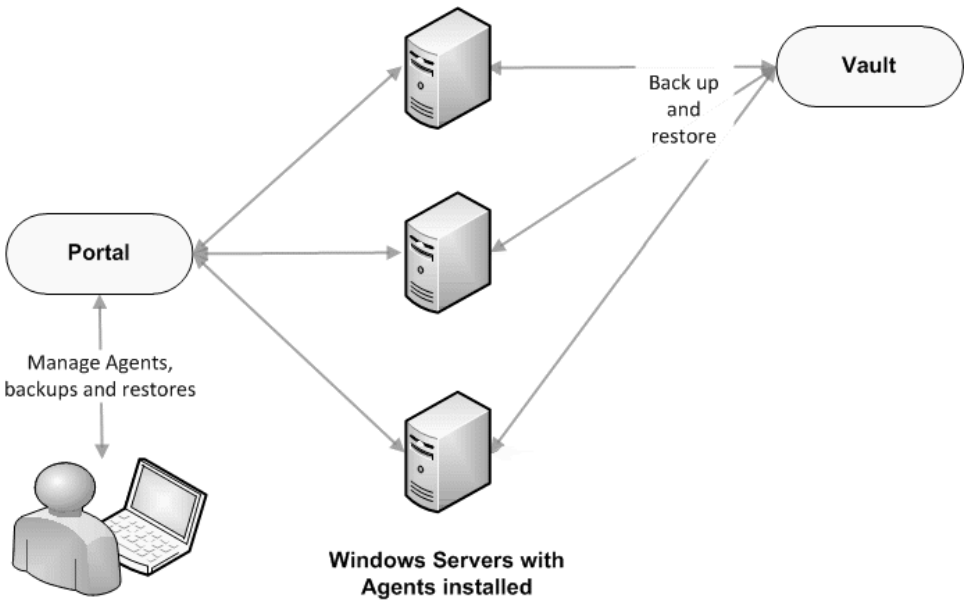
Version	Date	Description
1	April 2023	Initial guide for Windows Agent and Plug-ins 9.3*x*.

Contents

1 Introduction to the Windows Agent

Using the Windows Agent, you can back up data on Windows systems and restore data from the backups.

The agent is installed on Windows systems where you want to back up and restore data. As shown in the following diagram, you can use Portal to manage the agent and jobs, back up data to a secure vault, and restore data from the backups.



Note: This guide describes how to manage the agent and jobs using Portal. You can also use the legacy Windows CentralControl. However, if an agent is registered to Portal, the agent's vault settings are read-only in Windows CentralControl and you must use Portal to add and edit the vault settings.

The Windows Agent can back up:

- Files and folders on the Windows system.
- System files required for recovering the operating system, including registry and boot files.
- The entire system so that, in a disaster recovery situation, it can be restored to other hardware using System Restore.
- Files and folders on UNC shares.
- Data on Windows Storage Spaces.

  Note: The Agent does not back up or restore the configuration of Windows Storage Spaces. In a disaster recovery, you can configure storage spaces manually, and then restore data to the storage spaces.

For additional functionality, you can install plug-ins with the agent. See Windows Agent Plug-ins.

Beginning with Windows Agent 8.90, you can schedule a backup job to run multiple times per day, as often as hourly, when the agent backs up data to a Director version 8.60 or later vault. You can schedule a backup

job to run multiple times per day by creating an intra-daily schedule in Portal 8.88 or later. See Schedule a backup to run multiple times per day.

Beginning with Windows Agent 9.00, you can enable ransomware threat detection when you create or edit a Local System backup job in Portal 8.90 or later. When this option is enabled, the agent checks for potential ransomware threats when running the backup job. See Add a Windows backup job and Manage potential ransomware threats.

Beginning with Windows Agent 9.30 and Portal 9.30, Image and Local System backups can be triggered by system events on supported Windows desktop operating systems. Backups can be triggered, or start automatically, when a user logs on to the computer or when the computer starts to shut down. See Trigger backups when events occur on Windows desktop computers.

1.1 Windows Agent Plug-ins

When installing or upgrading a Windows Agent, you can install plug-ins with additional functionality. The following table lists and describes plug-ins that can be installed with the Windows Agent.

Plug-in	Description
Cluster Support Plug-in	Backs up and restores files and folders on shared cluster disks. The plug-in also works with the SQL Server Plug-in to protect SQL Server databases on Windows clusters, and the Image Plug-in to back up cluster volumes as images. Jobs are automatically redirected to the active node after a failover. For more information, see Protect a Windows cluster.
Exchange Plug-in	Backs up and restores Exchange databases. You can also restore individual mailboxes and messages using this plug-in and the Granular Restore for Microsoft Exchange application.
Exchange Plug-in (Legacy)	Legacy plug-in. Backs up and restores Exchange 2007 databases (no longer supported).
Image Plug-in	Backs up Windows volumes as images rather than backing up individual files and folders. You can restore complete volumes and specific files and folders from Image backups. You can also restore entire systems from Image backups using System Restore. Using Image Plug-in version 7.5 or later, you can create application-consistent SQL Server database backups and restore database files. For more information, see Image Plug-in. *Note:* You must use Portal to manage Image Plug-in backups and restores. This plug-in is not supported in the legacy Windows CentralControl.
Oracle Plug-in	Backs up and restores Oracle databases.

Plug-in	Description
SQL Server Plug-in	Backs up and restores SQL Server databases. The plug-in also works with the Cluster Support Plug-in to protect Microsoft SQL Server databases on Windows clusters. You can also use the SQL Server Plug-in to back up and restore SharePoint databases. You can restore individual SharePoint items (e.g., site collections, web sites, lists, documents) using this plug-in and the Granular Restore for Microsoft SharePoint application.

1.2 Image Plug-in

To back up Windows volumes as images, install the Image Plug-in with the Windows Agent. Unlike the Windows Agent, which enumerates and backs up individual files and folders during a backup, the Image Plug-in sequentially backs up all blocks on a volume. Because backups with the Image Plug-in require significantly less processing than backups with the Windows Agent, the time required for a backup can be significantly reduced. We recommend Image backup jobs over Local System backup jobs when backing up larger number of files on slow disks.

After the first "seed" backup of a volume, in which all data from the volume is sent to the vault, the Image Plug-in uses Changed Block Tracking to determine which blocks have changed. In subsequent Image backups, the plug-in only reads and backs up changed blocks to the vault.

When creating an Image backup job, you can select specific volumes to back up, or create a Bare Metal Restore (BMR) job that backs up all volumes, partitions, and data required for restoring a system to new hardware. You can also back up data on Windows Storage Spaces.

Note: The Image Plug-in is not supported with volumes created from Microsoft Storage Spaces Direct (S2D) storage pools.

Note: The Image Plug-in does not back up or restore the configuration of Windows Storage Spaces. In a disaster recovery, you can configure storage spaces manually, and then restore volumes to the storage spaces.

Note: The Image Plug-in is not supported on servers where Windows Offloaded Data Transfer (ODX) is enabled.

You can restore entire volumes and specific files and folders from Image backups. You can also use the System Restore application to restore systems from Image Plug-in BMR backups to new hardware. For more information, see the *System Restore User Guide*.

Beginning in version 7.5, the Image Plug-in can back up volumes with SQL Server database files. This option creates application-consistent database backups, so that separate SQL Server Plug-in jobs are not required. You can then mount these safesets, and restore database files from the backups.

You can use the Image Plug-in only on supported 64-bit Windows operating systems with the NTFS file system. The Image Plug-in is not supported with ReFS, FAT or FAT32 file systems (except for volumes that are required to start the system). To back up a system with the ReFS, FAT or FAT32 file system, use a

Windows Agent Local System job. The Image Plug-in supports both UEFI and BIOS, and MBR and GPT disks. For a complete list of supported platforms, see the Windows Agent release notes.

Image Plug-in Feature Summary

- Backs up volumes as images, which significantly reduces the amount of time required for a backup
- Backs up volumes from UEFI-based or BIOS-based systems. Restores volumes from UEFI-based system backups to UEFI-based systems, and restores volumes from BIOS-based system backups to UEFI-based or BIOS-based systems.
- Backs up system volumes, data volumes, or both in a single job
- Backs up and restores data on Windows Storage Spaces.

  Note: The Image Plug-in is not supported with volumes created from Microsoft Storage Spaces Direct (S2D) storage pools.

  Note: The Image Plug-in does not back up or restore the configuration of Windows Storage Spaces. In a disaster recovery, you can configure storage spaces manually, and then restore volumes to the storage spaces.
- Restores entire volumes to live volumes, or mounts a safeset so you can restore specific files and folders.
- Creates Bare Metal backups that can be restored using the System Restore application.
- Managed using Portal.

  You cannot manage Image Plug-in backups and restores using the legacy Windows CentralControl.

2 Install the Windows Agent and plug-ins

Beginning in version 9.20, the Windows Agent is only available as a 64-bit application; there is no 32-bit version of the agent. For supported platforms and system requirements, see the Windows Agent release notes.

Beginning with Windows Agent 8.90a and Portal 8.89, backups on Windows servers can be configured automatically based on job templates. If you install the Windows agent with a default encryption password and register the agent to a Portal child site where agent auto-configuration is enabled, a backup job and schedule can be created automatically. For more information, see Determine whether an agent has been configured automatically.

Note: Agent auto-configuration must be enabled in the child site when the agent first registers to Portal. If you enable auto-configuration after an agent is registered to Portal, the agent will not be configured automatically. To set up agent auto-configuration, see the *Portal Administration Guide* or Server Backup online help.

You can automate the deployment of the Windows agent across your organization using Active Directory Group Policy. For more information, see the *Agent for Microsoft Windows: Automating Agent Deployment* guide.

To install the Windows Agent and plug-ins:

1. Double-click the Windows Agent installation kit.

   The language selection dialog box appears.

2. In the language list, click the language for agent messages, and then click **OK**.

   The installation wizard starts.

3. On the Welcome page, click **Next**.
4. On the Support Information and Release Notes page, click **Next.**
5. On the License Agreement page, read the license agreement. Click **I accept the terms in the license agreement**, and then click **Next**.
6. On the Setup Type page, do one of the following:
   - To install the Agent only and use default settings, click **Typical**, and then click **Next**. Go to Step 13.
   - To install plug-ins and choose settings for the Agent, click **Custom**, and then click **Next**.

     Note: If you want the agent to be auto-configured, and are registering the agent to a Portal child site where an Image job template is selected, click **Custom** and select the Image Plug-in in Step 10.
7. On the Logon Credentials for Agent Services page, specify an account for running Agent services:

   Note: The account must be in the Administrators group and have the “Log on as a service” right.

- To run Agent services using the local system account, select **Use 'Local System' Account**.

  A local system account is required for restoring files and folders from Image backups.

  A local system account cannot be used to back up UNC files and folders.
- To automatically create an account for running Agent services, select **Create account automatically**.
- To run Agent services using a custom account, select **Use custom account**. In the **Username** and **Password** boxes, enter the custom account username and password.

8. Click **Next**.
9. On the Destination Folder page, do one of the following:
   - To install the Agent in the default location, click **Next**.
   - To install the Agent in another location, click **Change**. In the Change Current Destination Folder dialog box, browse to the new installation folder, or enter it in the **Folder name** box. Click **OK**. On the **Destination Folder** page, click **Next**.

   The Custom Setup page lists each Windows Agent component and plug-in that can be installed with the Agent that you are installing. For more information, see Windows Agent Plug-ins.

   The following icon appears for each component that will be installed: 

   The following icon appears for each component that will not be installed: 

   Note: The "Backup Agent" is the Windows Agent and is always selected and installed.
10. On the Custom Setup page, do the following:
    - For each component that you want to install, click the button to the left of the component name, and then click **This feature will be installed on local hard drive**.
    - For each component that you do not want to install, click the button to the left of the component name, and then click **This feature will not be available**.

      Note: If you want the agent to be auto-configured and are registering the agent to a Portal child site where an Image job template is selected, select the Image Plug-in.
11. Click **Next**.
12. On the Data Encryption Method page, do one of the following:
    - For best agent performance and to encrypt data using the optimized AES 256 encryption method that is integrated in the agent, click **Encrypt data using the integrated encryption method**, and then click **Next**.
    - To encrypt data using an external AES 256 encryption library that is provided with the agent, click **Encrypt data using the external encryption library**, and then click **Next**. Some organizations require the external encryption library for audit purposes.

    The data encryption method is used for data at rest.

IMPORTANT: The agent is only supported with the external encryption library that is provided with the agent. It has not been tested with other encryption libraries.

Note: You cannot change the data encryption method when you modify or repair the agent. You can only change the data encryption method when you install or upgrade the agent.

13. On the Register Agent with Portal page, specify the following information:
    - In the **Network Address** box, type the host name or IPV4 address of the Portal for managing the agent.

      We recommend specifying the Portal host name when you register an agent to Portal. If the Portal IP address changes in the future, DNS can handle the change and you will not have to manually register the agent to Portal again.
    - In the **Port** box, type the port number for communicating with the Portal. The default port is 8086.
    - In the **Username** box, type the name of the Portal user for the agent. Typically, the user name is an email address. The user must be an Admin user or regular user.

      If you want the agent to be auto-configured, the user must be in a child site where agent auto-configuration is enabled.
    - In the **Password** box, type the password of the specified Portal user.
14. Click **Next**.
15. On the Default Encryption Password page, do one of the following:
    - If you do not want the agent to be auto-configured, select **No** and then click **Next**.
    - To auto-configure the agent based on a job template, select **Yes**. In the **Password** and **Confirm Password** boxes, enter the data encryption password for the auto-configured backup job. Click **Next**.

      If you install Windows agent 8.90a or later with a default encryption password and register the agent to a Portal child site where agent auto-configuration is enabled, a backup job and schedule can be created automatically. For more information, see Determine whether an agent has been configured automatically.
16. On the Ready to Install the Program page, click **Install**.

    The Installing Agent page appears while the Agent is being installed.
17. On the InstallShield Wizard Completed page, click **Finish**.

    The Windows computer appears on the Computers page for the specified user, and for other Admin users in the user's site. If the agent is registered to a site where agent auto-configuration is enabled, wait for the agent to be configured. If the agent is not waiting for auto-configuration, you can add a backup job. See Add the first backup job for a Windows computer.

2.1 Upgrade the Windows agent and plug-ins

You can upgrade a Windows agent by manually running the agent installation kit. For supported upgrade paths and system requirements, see the Windows agent release notes.

IMPORTANT: Windows Agent 8.70 and later versions can be upgraded automatically. When automatic agent upgrades are set up in Portal, the agent downloads the installer and upgrades itself automatically. Agents can only be upgraded automatically on computers where Windows Agent version 8.70 or later is installed. Windows agents must be manually upgraded to version 8.70.

Note: Agents with the Cluster Plug-in cannot be upgraded automatically. You must upgrade these agents by running the installation kit, to ensure that all nodes in a cluster have the same agent version. See Upgrade Windows agents in a cluster.

Note: Support ended for SharePoint Plug-in, Exchange MAPI and SQL Server VDI jobs as of Agent version 7.50. You must delete jobs with these legacy types from a pre-version 7.50 agent before you can upgrade the agent. If you upgrade a pre-version 7.50 agent with a legacy plug-in, the plug-in will be removed. To restore from these legacy job types on the vault, install a version 7.34 or earlier agent with the appropriate plug-in, and use the *Restore from another computer* procedure.

Note: Support ended for the Agent Assistant as of Agent version 7.50. If you upgrade a pre-version 7.50 agent where the Agent Assistant is installed, the Agent Assistant will be removed from the system.

To upgrade the Windows agent and plug-ins:

1. Double-click the Windows Agent installation kit.

   A message box asks if you want to continue the Agent upgrade.

2. Click **Yes**.

3. On the Data Encryption Method page, do one of the following:

   - For best agent performance and to encrypt data using the optimized AES 256 encryption method that is integrated in the agent, click **Encrypt data using the integrated encryption method**, and then click **Next**.
   - To encrypt data using an external AES 256 encryption library that is provided with the agent, click **Encrypt data using the external encryption library**, and then click **Next**. Some organizations require the external encryption library for audit purposes.

   Note: The data encryption method is used for data at rest.

4. On the Portal registration page, do one of the following:

   - If the page states that the agent is already registered with Portal and you want to keep the same Portal registration information, select **Keep my current registration**, and then click **Next**.
   - If the page states that the agent is already registered with Portal and you want to change the Portal registration information, select **Change Registration**, and then click **Next**. On the Register Agent page, specify the Portal host name or IPV4 address, port number, username

and password. Click **Next**.

- If the page states that you can register the agent with Portal, specify the Portal host name or IPV4 address, port number, username and password. Click **Next**.

  We recommend specifying the Portal host name when you register an agent to Portal. If the Portal IP address changes in the future, DNS can handle the change and you will not have to manually register the agent to Portal again.

5. On the Resuming the Installshield Wizard page, click **Next**.
6. On the InstallShield Wizard Completed page, click **Finish**.

2.2 Upgrade Windows agents in a cluster

The same Windows Agent version should be installed on all nodes in a Windows cluster. Use the following upgrade procedure in a Windows cluster to avoid problems with mixed Agent versions.

Note: A Windows agent with the Cluster plug-in cannot be upgraded automatically. You must upgrade agents with the Cluster plug-in by running the installation kit.

To upgrade Windows agents in a cluster:

1. Ensure that no backups or restores are running.
2. Upgrade the agent on the active node in the cluster. See Upgrade the Windows agent and plug-ins.
3. Upgrade the agent on each passive node in the cluster. See Upgrade the Windows agent and plug-ins.

2.3 Modify a Windows agent installation

You can modify a Windows agent installation to change the credentials for running agent services, the plug-ins that are installed, or the Portal registration.

You cannot change the data encryption method (integrated encryption method or external encryption library) when you modify an agent. You can only change the data encryption method when you uninstall or upgrade the agent.

To change the language of an agent, uninstall the agent program files, and then reinstall the agent.

To modify a Windows agent installation:

1. Double-click the Windows Agent installation kit.
2. On the Welcome page, click **Next**.
3. On the Program Maintenance page, click **Modify**, and then click **Next**.
4. On the Logon Credentials for Agent Services page, do one of the following:
   - To continue using the same credentials for running Agent services, select **Leave unchanged**.
   - To run Agent services using the local system account, select **Use 'Local System' Account**.

A local system account is required for restoring files and folders from Image backups.

A local system account cannot be used to back up UNC files and folders.

- To automatically create an account for running Agent services, select **Create account automatically**.
- To run Agent services using a custom account, select **Use custom account**. In the **Username** and **Password** boxes, enter the custom account username and password.

Note: The account must be in the Administrators group and have the "Log on as a service" right.

5. Click **Next**.
6. On the Custom Setup page, do the following:
   - For each component that you want to install, click the button to the left of the component name, and then click **This feature will be installed on local hard drive**.
   - For each component that you do not want to install, click the button to the left of the component name, and then click **This feature will not be available**.
7. Click **Next**.
8. On the Portal registration page, do one of the following:
   - If the page states that the Agent is already registered with Portal and you want to keep the same Portal registration information, select **Keep my current registration**, and then click **Next**.
   - If the page states that the Agent is already registered with Portal and you want to change the Portal registration information, select **Change Registration**, and then click **Next**. On the Register Agent page, specify the Portal host name or IPV4 address, port number, username and password. Click **Next**.
   - If the page states that you can register the Agent with Portal, specify the Portal host name or IPV4 address, port number, username and password. Click **Next**.
9. On the Ready to Modify the Program page, click **Install**.
10. On the InstallShield Wizard Completed page, click **Finish**.

2.4 Install or upgrade the Windows agent and plug-ins in silent mode

You can install or upgrade the Windows agent and plug-ins by running the installation in silent mode.

Note: You can download agent installation kits from some Portal instances. However, you cannot install or upgrade the Windows agent in silent mode if the installation kit was downloaded from Portal.

Beginning with Windows Agent 8.90a and Portal 8.89, backups on Windows servers can be configured automatically based on job templates. If you install the Windows agent with a default encryption password and register the agent to a Portal child site where agent auto-configuration is enabled, a backup job and schedule can be created automatically. See Determine whether an agent has been configured automatically.

Note: Agent auto-configuration must be enabled in the child site when the agent first registers to Portal. If you enable auto-configuration after an agent is registered to Portal, the agent will not be configured automatically. To set up agent auto-configuration, see the *Portal Administration Guide* or Server Backup online help.

IMPORTANT: Windows Agent 8.70 and later versions can be upgraded automatically. When a new installer is available in Portal, the agent downloads the installer and upgrades itself automatically. Agents can only be upgraded automatically on computers where Agent version 8.70 or later is installed. Windows agents must be manually upgraded to version 8.70. Agents with the Cluster plug-in cannot be upgraded automatically. You must upgrade these agents manually, to ensure that all nodes in a cluster have the same agent version.

Note: Support ended for legacy Exchange MAPI, SQL Server VDI and SharePoint Plug-in jobs as of Agent version 7.50. Before upgrading an agent, you must delete jobs with these legacy types, or the upgrade will fail. If you upgrade an agent with a legacy plug-in to version 7.50 or later, the plug-in will be removed.

To install or upgrade the Windows agent and any plug-ins in silent mode, run the following command in the directory where the installation kit is located:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v"/qn [parameters] [featureParameters]"
[/l"language"]
```

Where:

- Agent-Windows-x64-*x-xx-xxxx*.exe is the name of the Windows Agent installation kit. *x-xx-xxxx* represents the Agent version number.
- *parameters* are optional parameters for running the installation kit in silent mode. For a list of available parameters, see Windows agent installation parameters.
- *featureParameters* are optional parameters for installing plug-ins and features in silent mode. See Windows Agent feature parameters.
- /l"*language*" is an optional parameter that specifies the language for the Agent. Available *language* values are:
    - 1033 – English (United States). This is the default value.
    - 1036 – French (Standard)
    - 1031 – German
    - 1034 – Spanish

For example, to install the French version of the agent, include the following parameter: /L"1036"

2.4.1 Windows agent installation parameters

Parameter	Description	Default Value
ACCOUNTTYPE	Possible values are LocalSystem, AutoCreate, and Custom.	LocalSystem
SERVICEACCOUNTNAME	If ACCOUNTTYPE is Custom, this field is required.	
SERVICEACCOUNTPASSWORD	If ACCOUNTTYPE is Custom, this field is required.	
REGISTERWITHWEBCC	Turns on/off registration of the agent with Portal.	False
AMPNWADDRESS	Host name or IPV4 address of the Portal for managing the agent. If REGISTERWITHWEBCC is True, this field is required.	
AMPPASSWORD	Password of the specified Portal user. If REGISTERWITHWEBCC is True, this field is required.	
AMPPORT	Port number for communicating with Portal.	8086
AMPUSERNAME	Portal user for the agent. The user must be an Admin user or regular user. If REGISTERWITHWEBCC is True, this field is required.	
DEFAULTJOBENCRYPTIONKEY	Data encryption password for automatically-configured backup jobs. Beginning with Windows Agent 8.90a and Portal 8.89, if you install the Windows agent with a default encryption password and register the agent to a child site where agent auto-configuration is enabled, a backup job and schedule can be created automatically. *Note:* This parameter is applicable for new installations, but not for upgrades. *Note:* Agent auto-configuration must be enabled in the child site when the agent first registers to Portal. If you enable auto-configuration after an agent is registered to Portal, the agent will not be configured automatically.	
EXTRACTMSI	Turns on/off extraction of the Microsoft Installer (MSI) package.	False

Parameter	Description	Default Value
INTEGRATEDENCRYPTION	Specifies whether to use the optimized AES 256 data encryption method that is integrated with the agent, or use the external AES 256 encryption library that is provided with the agent. Available values are: • On – the agent uses the internal, optimized AES 256 data encryption method • Off – the agent uses the external encryption library The data encryption method is used for data at rest. You cannot change the data encryption method when you modify or repair the agent. You can only change the data encryption method when you install or upgrade the agent.	On
KEEPAMPREGISTRATION	Set this property to True to retain the previous Portal registration.	True
MSIPATH	If EXTRACTMSI is True, this property denotes the location of the extracted MSI and MST files.	C:\
SILENTINSTALLDIR	Specifies an installation folder for the Agent. The installation folder must be enclosed in double quotation marks if there are spaces in the name or path.	

2.4.2 Windows Agent feature parameters

Feature Parameter	Description	Default Value
FEATURECLUSTER={On|Off}	Turns on/off installation of the Cluster Plug-in.	Off
FEATUREEXCHANGE= {On|Off}	Turns on/off installation of the Exchange Plug-in (Legacy).	Off
FEATUREEXCHANGE2010= {On|Off}	Turns on/off installation of the Exchange Plug-in.	Off
FEATUREORACLE={On|Off}	Turns on/off installation of the Oracle Plug-in.	Off
FEATURESQL={On|Off}	Turns on/off installation of the SQL Server Plug-in.	Off
FEATUREVOLUMEIMAGE= {On|Off}	Turns on/off installation of the Image Plug-in. *Note:* After the Image Plug-in is installed silently, the machine must be restarted before the Plug-in can use Changed Block Tracking (CBT) to identify data that has changed since a previous backup. Without CBT, the Agent reads all data when backing up a volume.	Off

For example, to install the Windows Agent in a different directory, run the following command:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v"/qn SILENTINSTALLDIR=\"C:\Program
Files\Acme Software\" "
```

Note: In each example shown, *x-xx-xxxx* represents the Agent version number.

To install the French version of the Agent, run the following command:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v"/qn" /l"1036"
```

where 1036 indicates that the French version of the Agent is installed.

To install the Windows Agent, register the agent to Portal, specify a default data encryption password, and install the Image Plug-in, run a command similar to this:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v"/qn REGISTERWITHWEBCC=True
AMPNWADDRESS=123.456.com AMPUSERNAME=user@test.com AMPPASSWORD=password
DEFAULTJOBENCRYPTIONKEY=encryptionpassword FEATUREVOLUMEIMAGE=On"
```

To install the Windows Agent and SQL Server Plug-in:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v" FEATURESQL=On /qn"
```

2.5 Windows Agent default ports

The following table shows default ports that must be open for Windows Agent to communicate with other systems:

Port	Communication	Protocol
Outbound: 8086, 8087	To Portal	TCP
Outbound: 443	To Portal (for automatic agent upgrades)	TCP
Outbound: 2546	To vault	TCP
Outbound: 8031	To Windows CentralControl	TCP
Inbound: 2548	From Windows CentralControl	TCP

2.6 Minimum Agent and plug-in permissions

Agent software requires sufficient permissions to back up and restore files. The following table lists the minimum permissions required for specific Agents and plug-ins.

Product	Required Permissions

Windows Agent	The account for running Agent services must: • belong to the Backup Operators group • have the “Log on as a service” right • have the “Replace a process level token” right To back up files and folders locally, the account must have read/write access to files and folders on the system. To back up files and folders in UNC locations, the account must have read/write permissions to the UNC locations, including security streams. Security streams might not work in some places unless the account is an Admin equivalent. If you are using Encrypting File System (EFS), additional permissions are required. After installing the Agent, you must change local security settings or the default domain policy. The service account must have the “Act as part of the operating system” right and the “Log on as a service” right. If the service account does not have the correct permissions, the service is denied access. ACLs for all subsequent files might not be backed up and error messages might appear in the log. *Note:* When you install, modify, repair or upgrade an Agent, the Agent installation kit sets or resets permissions on the Agent folder and all child items to full access for the Administrators and Backup Operators groups. Using the Modify option, the user can install Agent services under a local system account or another account that is created manually or automatically. For non-local system accounts, the created account is modified to be part of the Administrators group. If a user requires access to Agent services, the user should be included in the Administrators or Backup Operators group.
Exchange Plug-in	The account specified during the Windows Agent and Plug-in installation must belong to the following groups: • Exchange Organization Administrators • Group Policy Owners • Schema Admins • Enterprise Admins • Domain Admins
SQL Plug-in	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 and sysadmin role in order to perform full SQL Server backups and transaction log backups.

2.7 Uninstall the Windows agent and plug-ins

To uninstall the Windows agent and plug-ins:

1. Double-click the Windows Agent installation kit.
2. On the Welcome page, click **Next**.

3. On the Program Maintenance page, click **Remove**, and then click **Next**.
4. On the Uninstallation Type page, click **Total Install**, and then click **Next**.
5. On the Remove the program page, click **Remove**.
6. When the uninstallation is finished, click **Finish**.

2.7.1 Uninstall the Windows agent and plug-ins in silent mode

To uninstall the Windows agent and any plug-ins in silent mode and remove all of its configuration files, run the following command in the directory where the installation kit is located:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /x /v"/qn TOTALUNINSTALL=True"
```

To uninstall the Windows agent and any plug-ins in silent mode but leave its configuration files, run the following command in the directory where the installation kit is located:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /x /v"/qn TOTALUNINSTALL=False"
```

x-xx-xxxx represents the Agent version number.

3 Protect a Windows cluster

To protect a Windows cluster, install the Windows Agent and Cluster Support Plug-in on each node in the cluster. You can also install the Image Plug-in to back up Windows volumes as images, and install the SQL Server Plug-in to back up SQL Server databases.

When installing the Windows Agent and plug-ins on each cluster node, register the agent to Portal using the same user name and password. You can then sign in to Portal using these credentials and do the following:

- Register a virtual server for the cluster core and for each cluster role (e.g., file server, SQL Server) that you want to protect.
- Add the same vault setting for each virtual server.
- Create and run backup jobs on each virtual server. When a backup job runs on a virtual server, the job is automatically directed to the active cluster node and will not reseed after a failover. You can also create backup jobs on the cluster nodes. Jobs on a cluster node will not fail over when the cluster fails over. See Add backup jobs for a Windows cluster.

Note: Agents with the Cluster Plug-in cannot be upgraded automatically. You must upgrade these agents by running the installation kit, to ensure that all nodes in a cluster have the same agent version. See Upgrade Windows agents in a cluster.

To add a Windows cluster:

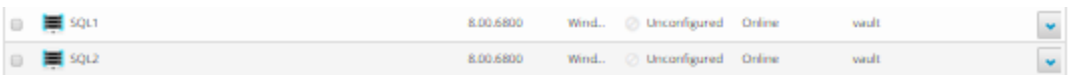
1. On each node in the Windows cluster, install the Windows Agent and the following plug-ins:
   - Cluster Support Plug-in
   - Image Plug-in (recommended)
   - SQL Server Plug-in (required for point-in-time database protection in a SQL Server cluster)

   See Install the Windows Agent and plug-ins.

   IMPORTANT: During the installation, register each agent to the same Portal instance using the same credentials.

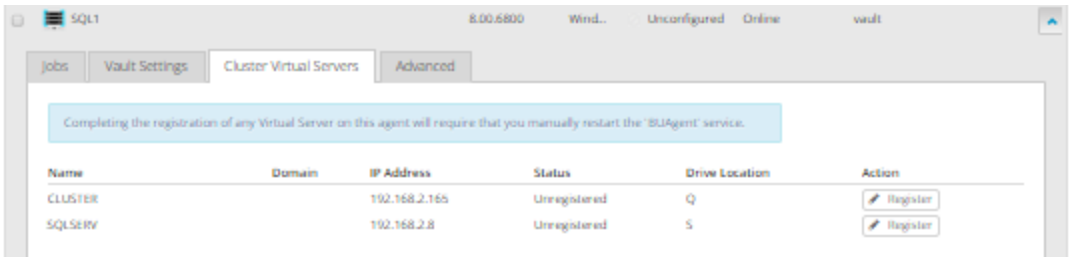
   We recommend specifying the Portal host name when you register an agent to Portal. If the Portal IP address changes in the future, DNS can handle the change and you will not have to manually register the agent to Portal again.
2. Sign in to Portal using the credentials that you used in Step 1.
3. In Portal, on the navigation bar, click **Computers**.

   The Computers page shows the registered cluster nodes.



4. Find the active cluster node, and expand its view by clicking its row. Click **Configure Manually**.
5. Click the **Cluster Virtual Servers** tab.

The tab lists the cluster core and each cluster resource (e.g., file server, SQL Server).

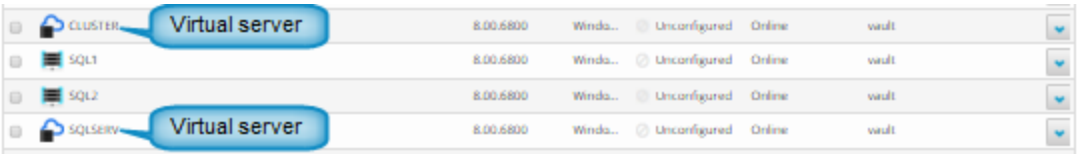


6. Click **Register** for the cluster core and for each role that you want to protect.

   A virtual server appears on the Computers page for the registered cluster core and each registered role. Initially, each virtual server is Offline.

7. On each cluster node, restart the BUAgent service.

   On the Computers page in Portal, each virtual server changes to Online.



8. In Portal, for each cluster node and virtual server, add the same vault setting. Each cluster node and virtual server must be registered to the same vault using the same credentials. See Add vault settings.

   You can then create and run jobs on the virtual server, and the jobs will run after a failover. You can also create and run jobs on each cluster node. See Add backup jobs for a Windows cluster.

3.1 Protect a SQL Server cluster

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.

4 Configure a Windows Agent

After a Windows Agent is installed and registered with Portal, you can configure settings for the agent. Settings include:

- Vault connections. Vault connections provide vault information and credentials so that the computer can back up data to and restore data from the vault. See Add vault settings.
- Description for the protected computer. The description appears for the agent on the Computers page in Portal. See Add a description.
- Retention types. Retention types specify how long backups are kept on the vault. See Add retention types.
- Amount of bandwidth consumed by backups. See Configure bandwidth throttling.
- Email notifications, so that users receive emails when backups complete, fail, or have errors. See Set up email notifications for backups on a computer.

4.1 Add vault settings

Before a computer can back up data to or restore data from a vault, vault settings must be added for the computer. Vault settings provide vault information, credentials, and agent connection information required for accessing a vault.

Note: If an agent is registered to Portal, the agent's vault settings are read-only in Windows CentralControl and you must use Portal to add and edit the vault settings.

When adding vault settings for a computer, Admin users and regular users can manually enter vault information, or select a vault profile with vault information and credentials.

If a policy is assigned to a computer, Admin users can select any vault profile from the policy. Regular users can only select policy vault profiles that are also assigned to them.

If a policy is not assigned to a computer, Admin users can select any vault profile in the site. Regular users can only select vault profiles that are assigned to them.

Over-the-wire encryption is automatically enabled when you add vault settings or save existing vault settings.

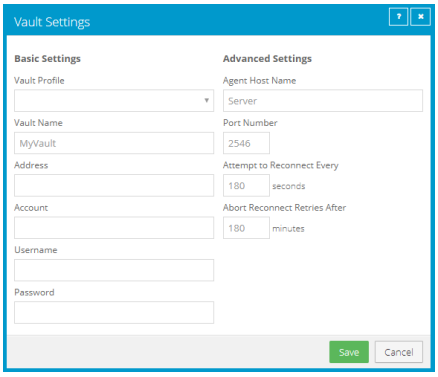
To add vault settings:

1. On the navigation bar in Portal, click **Computers**.
2. Find the computer for which you want to add vault settings, and click the computer row to expand its view.

   If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.

3. On the Vault Settings tab, click **Add Vault**.

   The Vault Settings dialog box appears.



4. Do one of the following:

   - In the **Vault Name** box, enter a name for the vault. In the **Address** box, enter the vault host name or IPV4 address. In the **Account**, **Username**, and **Password** boxes, enter an account and credentials for backing up data to and restoring data from the vault.

     Specifying the host name of the vault is recommended. This will allow DNS to handle IP address changes.

   - Click the **Vault Profile** box. If one or more vault profiles appear, click the vault profile that you want to add for the computer. Vault information and credentials are then populated in the Vault Settings dialog box.

     If a policy is assigned, the **Vault Profile** list includes vault profiles from the policy. If a policy is not assigned, the list includes vault profiles from the site. For a regular user, the list only includes vault profiles that are also assigned to the user.

5. (Optional) Change one or more of the following Advanced Settings for the vault connection:

   - **Agent Host Name**. Name to use for the computer on the vault.
   - **Port Number**. Port used to connect to the vault. The default port is 2546.
   - **Attempt to Reconnect Every**. Specifies the number of seconds after which the agent should try to connect to the vault if the vault becomes unavailable during a backup or restore. The value can be from 30 to 1800 seconds.
   - **Abort Reconnect Retries After**. Enter the number of minutes after which the agent should stop trying to reconnect to the vault if the vault becomes unavailable during a backup or restore. The value can be from 60 to 720 minutes. If the Agent cannot connect to the vault successfully in the specified time, the backup or restore fails.

6. Click **Save**.

4.2 Add a description

You can add a description for a computer in Portal. The description appears on the Computers page, and can help you find and identify a particular computer.

To add a description:

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

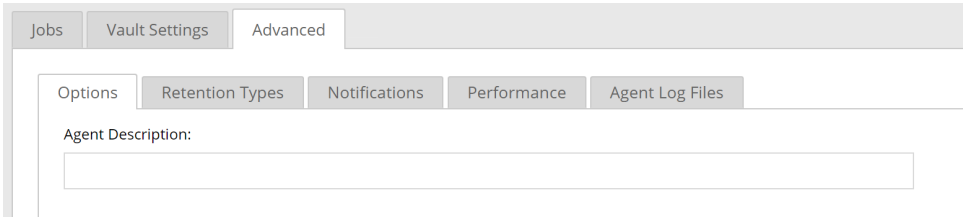
   The Computers page shows registered computers.

2. Find the computer for which you want to add a description, and click the row to expand its view.

   If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.

3. On the Advanced tab, click the **Options** tab.

4. In the Agent Description box, enter a description for the computer.



5. Click **Save**.

4.3 Add retention types

When you schedule or run a backup job, you must select a retention type for the resulting safeset. A 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.

Portal Admin users and regular users can add retention types for a computer where a policy is not assigned.

You cannot add, change or delete retention types for intra-daily schedules. For intra-daily schedules, you must choose one of two intra-daily retention types that are available beginning in Portal 8.88. See Schedule a backup to run multiple times per day.

If a policy is assigned to a computer, retention types cannot be added or modified on the Computers page. Instead, retention types can only be added or modified in the policy.

To add a retention type:

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

   The Computers page shows registered computers.

2. Find the computer for which you want to add a retention type, and click the row to expand its view.

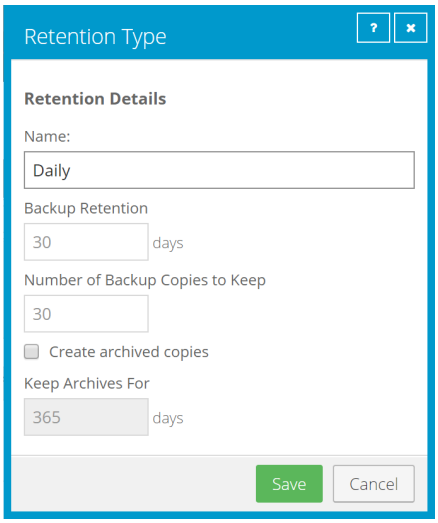
If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.

3. On the Advanced tab, click the **Retention Types** tab.

   If a policy is assigned to the computer, you cannot add or change values on the Retention Types tab. Instead, retention types can only be added or modified in the policy.

4. Click **Create Retention Type**.

   The Retention Type dialog box appears.



5. Complete the following fields:

Name	Specifies a name for the retention type.
Backup Retention	Specifies the number of days a safeset is kept on the vault. A safeset is deleted when its expiry date is reached. *Note:* Safesets are not deleted unless the specified number of copies online has also been exceeded.
Number of Backup Copies to Keep	Specifies how many safesets from a backup job are stored online. It functions in a first in/first out manner. Once the number of safesets is exceeded, the oldest safesets are automatically deleted until the actual number of safesets matches the definition. *Note:* Safesets are not deleted unless the specified number of days online has also been exceeded.
Create archived copies	Select this check box to create archived copies of safesets.

Keep Archives For	*Note:* If data archiving is disabled in your Portal instance, this value does not appear. Specifies how long the data is stored offline. Archive storage is used to store data offline for long periods of time. This data is not immediately accessible since it is stored remotely. A greater amount of time is required to restore from archive media. Typically, only long-term data archives are stored offline. The parameters for archived data are from 365 to 9999 days. Assuming that at least one successful backup has been completed for the job, there will never be less than one copy of its backup online. This is true even if all retention settings are zero, expiry conditions have been met, and the job definition is deleted from your system. Deleting the job does not affect data on the vault. Only your service provider can remove jobs and their associated data from the vault. This is a safeguard against accidental or malicious destruction of data.

6. Click **Save**.

4.4 Configure bandwidth throttling

Bandwidth throttling settings specify the amount of bandwidth consumed by an agent for backups and restores. 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 backups and restores. For example, if three jobs are running at the same time on the same computer, each job gets 1/3 of the specified maximum bandwidth.
- 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 a computer's bandwidth settings while a backup is running, the new 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.

If a policy is assigned to a computer, bandwidth throttling settings cannot be modified on the Computers page. Instead, settings can only be added or modified in the policy.

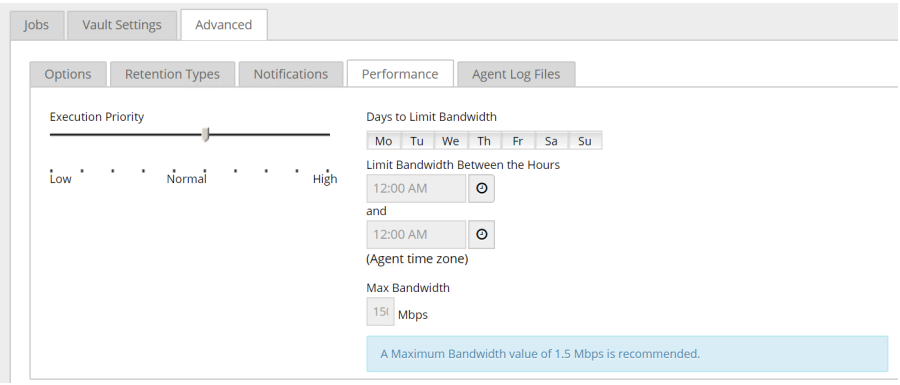
To configure bandwidth throttling:

1. On the navigation bar, click **Computers**.
2. Find the computer for which you want to configure bandwidth throttling, and click the row to expand its view.

   If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.
3. Click the **Advanced** tab, click the **Performance** tab, and then edit the bandwidth settings.

   If a policy is assigned to the computer, you cannot add or change values on the Performance tab. Instead, bandwidth settings can only be modified in the policy.

   Note: Depending on your Internet speed, the recommended maximum bandwidth value (1.5 Mbps) shown in Portal may be low. This is only a recommendation. You can specify a higher maximum bandwidth if your Internet speed will support it.



4. Click **Save**.

4.5 Set the data read error handling method for a Windows computer

For Windows computers with Agent version 8.70 or later, you can specify how the Agent handles data read VSS errors during backups.

When the agent encounters a data read VSS error that could result in missing data during a backup, the agent can log the error and stop the backup or log the error and continue the backup.

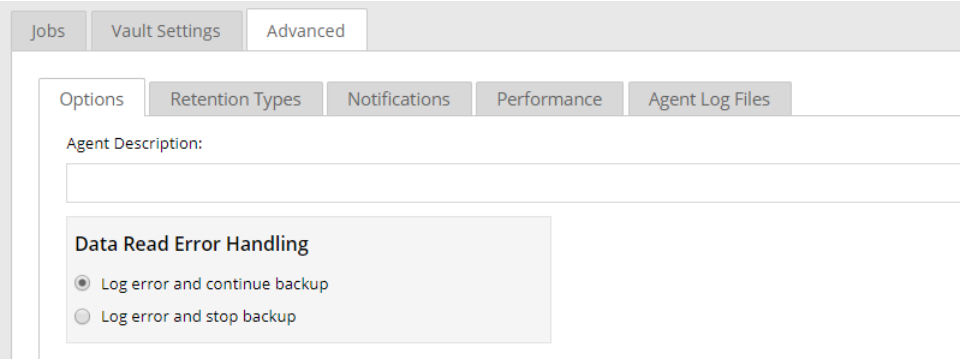
To set the data read error handling method for a Windows computer:

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

   The Computers page shows registered computers.
2. Find the computer for which you want to set the data read error handling method, and click the row to expand its view.

   If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.

3. On the Advanced tab, click the **Options** tab.



4. Specify how the Agent handles data read VSS errors that could result in missing data during backups:
   - To log the error and continue the backup, click **Log error and continue backup**.
   - To log the error and stop the backup, click **Log error and stop backup**.
5. Click **Save**.

5 Add and edit backup jobs

Before you can back up data, you must create a backup job. A backup job specifies which data to back up on a system, specifies where to save the data, and provides other backup settings.

You can create backup jobs that protect:

- Windows systems, files and clusters. See Add a Windows backup job, Add an Image backup job, Add the first backup job for a Windows computer, Add a UNC file backup job and Add backup jobs for a Windows cluster.
- Databases and application data. See Add a SQL Server database backup job, Add an Exchange backup job and Add an Oracle database backup job.

After creating a backup job, you can run the job manually and schedule the backup job to run. See Run and schedule backups and synchronizations. You can also edit settings in existing backup jobs. See Edit a backup job.

You can only create backup jobs for computers and environments that are online. Portal cannot communicate with computers that are offline. Computers might be offline if their Agent software is not running or has been uninstalled, if they have been shut down, or if they have no internet access.

5.1 Add a Windows backup job

When the Windows Agent is installed on a computer, you can create a backup job for the computer. The backup job specifies which drives, folder and files to back up, and the vault for saving the data.

Note: Beginning with Portal 8.89 and Windows Agent 8.90a, backups can be configured automatically on Windows servers based on job templates. When agent auto-configuration is set up in a Portal instance, you do not have to manually create a backup job and schedule for each Windows server. For more information, see Install the Windows Agent and plug-ins.

In a Windows backup job, you can select:

- Specific folders and files to back up
- The Bare Metal Restore (BMR) option, to back up volumes that are needed to boot up the system after a system recovery. In a disaster recovery situation, you can use the System Restore application to restore systems from BMR backups.

  Note: You can also create BMR backup jobs using the Image Plug-in. When you run an Image Plug-in BMR job, the Plug-in backs up required volumes as images, instead of enumerating and backing up individual files and folders on the volumes.

  Note: Encrypted volumes (BitLocker, TrueCrypt, etc.) are not supported in BMR jobs.
- The Entire Server option, available with Windows Agent 8.72 or later and Portal 8.87 or later. When this option is selected, the job backs up all non-removable volumes on the system, including volumes that are added after the job is created.

Beginning in Portal 8.89, the Bare Metal Restore option is automatically selected when you select the Entire Server option. This ensures that you can restore a protected server using the System Restore application, if required.

Note: When the Entire Server option is selected in a Local System job, you do not need to select files and folders to include. However, you can exclude specific files and folders from the job.

- The System State option, to back up files required for recovering the state of the operating system. System state backups typically include registry and boot files, the COM+ Class Registration Database, Windows system files and performance counters.

  IMPORTANT: Instead of system state backups, we recommend using Image backups with the Bare Metal Restore option on platforms where the Image Plug-in is supported.

Note: Do not include antivirus product installation directories or resource folders in backup jobs.

Note: Some files are filtered out automatically from a backup job. For example, files specified by the FilesNotToBackup and FilesNotToSnapshot registry keys might not be backed up, and the job folder is not backed up.

Beginning with Windows Agent 9.00 and Portal 8.90, you can enable ransomware threat detection when you add a Local System backup job. When this option is enabled, the agent checks for potential ransomware threats when running the backup job. If the Windows agent detects a potential threat, the resulting backup is identified as a potential threat throughout Portal so you can investigate and resolve the threat. See Manage potential ransomware threats.

Note: The agent does not check for potential ransomware threats in a seed backup or the first backup when threat detection is enabled in a job.

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

You can also back up Windows computers using the Image Plug-in. The Image Plug-in sequentially backs up all blocks on a volume instead of backing up specific files and folders. Because this process can require less processing than a traditional Windows backup job, the backup time can be significantly reduced. We recommend Image backup jobs over Local System backup jobs when backing up larger number of files on slow disks. See Add an Image backup job.

To add a Windows backup job:

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

   The Computers page shows registered computers.

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

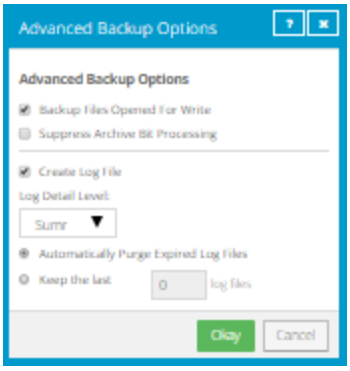
   If a backup job has not been created for the computer, the system can attempt to create a backup job automatically. See Add the first backup job for a Windows computer.

3. Click the **Jobs** tab.

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

4. In the **Select Job Task** menu, click **Create New Local System Job**.
5. 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.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.
6. To change log file settings or other backup options, click **Advanced Backup Options**. In the Advanced Backup Options dialog box, specify options and then click **Okay**. For more information, see Log file options and Advanced backup options.



7. In the **Select Files and Folders for Backup** box, do one or more of the following until the **Backup Set** box shows the drives, folders and files that you want to include and exclude in the backup job:
   - To back up all volumes on the system, including non-removable volumes that are added after the backup job is created, select the **Entire Server** option.

     Note: The Entire Server option is only available with Windows Agent 8.72 or later and Portal 8.87 or later.

     Note: Beginning in Portal 8.89, the Bare Metal Restore option is automatically selected when you select the Entire Server option.
   - To back up system files so that you can restore the system to its state at the time of the backup, select **System State**, and then click **Include**.

Note: Instead of system state backups, we recommend using Image backups with the Bare Metal Restore option on platforms where the Image Plug-in is supported.

- To back up volumes that are needed to boot up the system after a system recovery, select **Bare Metal Restore**, and then click **Include**.

  Bare Metal Restore (BMR) backups can be restored to new hardware using the System Restore application.

- To add one or more folders or files to the backup job, select the check box for each folder or file, and then click **Include**. The included folders or files appear in the **Backup Set** box. If you include a folder, the backup job includes all of the folder's subdirectories and files by default. If you do not want to back up all of the subdirectories and files, you can add filters. See Filter subdirectories and files in backup jobs.

  Note: When the Entire Server option is selected in a Local System job, you do not need to select files and folders to include. All files will be backed up unless you exclude specific files and folders from the job.

- To exclude one or more folders or files from the backup job, select the check box for each folder or file, and then click **Exclude**. The excluded folders or files appear in the **Backup Set** box. If you exclude a folder, all of the folder's subdirectories and files are excluded from the backup job by default. If you do not want to exclude all of the subdirectories and files, you can add filters. See Filter subdirectories and files in backup jobs.

- To remove an inclusion or exclusion record from the **Backup Set** box, click the Delete button beside the folder or file record.

8. Do one of the following:

   - To check for potential ransomware threats while running the job, select the **Enable Threat Detection** check box.

   - To disable ransomware threat detection, clear the **Enable Threat Detection** check box.

     IMPORTANT: If you disable threat detection for a job where it was enabled, any potential threat warnings for backups in the job will be cleared. Only disable threat detection for a job once all potential threats have been addressed. See Manage potential ransomware threats.

9. Click **Create Job**.

   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.

5.1.1 Advanced backup options

When you create or edit a Windows backup job, the following options are available in the Advanced Backup Options dialog box.

Back up files opened for write

If the **Backup files opened for write** option is selected, files are backed up if they are open for writing or shared reading during the backup. Files that are open for exclusive writes cannot be backed up.

When this option is selected, inconsistencies in the backup can occur if an open file is modified during the backup process.

Suppress archive bit processing

In some operating systems, an archive attribute is placed in a file when the file is created or modified. The archive attribute indicates that the file needs to be backed up.

If the **Suppress archive bit processing** option is selected, the Agent does not clear the archive attribute when it backs up a file. If you use other programs that rely on the archive attribute, make sure that the **Suppress archive bit processing** option is not selected.

If the **Suppress archive bit processing** option is not selected, the Agent clears the archive attribute when it backs up a file.

5.2 Add an Image backup job

When the Windows Agent and Image Plug-in are installed on a computer, you can create an Image backup job. The Image Plug-in sequentially backs up all blocks on a volume instead of backing up specific files and folders. Because this process can require less processing than a traditional Windows backup job, the backup time can be significantly reduced. We recommend Image backup jobs over Local System backup jobs when backing up larger number of files on slow disks.

In an Image backup job, you can select the following options:

- Specific volumes to back up.

  Note: Encrypted volumes (BitLocker, TrueCrypt, etc.) are not supported in Image jobs.

  Note: The Image Plug-in is not supported with volumes created from Microsoft Storage Spaces Direct (S2D) storage pools.

  Note: The Image Plug-in is not supported on servers where Windows Offloaded Data Transfer (ODX) is enabled.

- Bare Metal Restore (BMR). This option backs up volumes that are needed to boot up the system after a system recovery. A BMR backup includes the volume where the operating system is installed, and the EFI system partition (ESP) on a UEFI-based system or the volume with the master boot record (MBR) on a BIOS-based system. In a disaster recovery situation, you can use the System Restore application to restore systems from BMR backups.

Note: BMR backup jobs can also be created using the Windows Agent without the Image Plug-in. Regardless of how a BMR backup was created, you can restore the backup using the System Restore application.

- Volumes with SQL Server database files. This option creates application-consistent SQL Server database backups, so that separate SQL Server Plug-in jobs are not required. Image Plug-in version 7.5 or later is required for this functionality.
- The Entire Server option, available with Windows Agent 8.72 or later and Portal 8.87 or later. When this option is selected, the job backs up all non-removable volumes on the system, including volumes that are added after the job is created.

  Beginning in Portal 8.89, the Bare Metal Restore option is automatically selected when you select the Entire Server option. This ensures that you can restore a protected server using the System Restore application, if required.

Note: Some files are filtered out automatically from a backup job. For example, files specified by the FilesNotToBackup and FilesNotToSnapshot registry keys might not be backed up, and the job folder is not backed up.

After creating an Image backup job, you can run the job manually, and schedule the backup job to run. See Run and schedule backups and synchronizations.

In a seed backup, the Image Plug-in processes data for every block on a volume— even blocks that are empty. The amount of data reported in the backup log for a seed backup could be larger than the amount of data actually on the volumes.

Note: In some cases, a machine must be restarted before Changed Block Tracking (CBT) can identify data that has changed since a previous backup. For example, a machine must be restarted after the Image Plug-in is installed silently, a new volume is created, a new disk is added, or a disk is converted from basic to dynamic. Without CBT, the Agent reads all data on a volume before backing up the changed blocks.

Note: The Image Plug-in does not back up or restore the configuration of Windows Storage Spaces. In a disaster recovery, you can configure storage spaces manually, and then restore volumes to the storage spaces.

To add an Image backup job:

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

   The Computers page shows registered computers.

2. Find a Windows computer with the Image Plug-in, and click the computer row to expand its view.

   If a backup job has not been created for the computer, the system can attempt to create a backup job automatically. See Add the first backup job for a Windows computer.

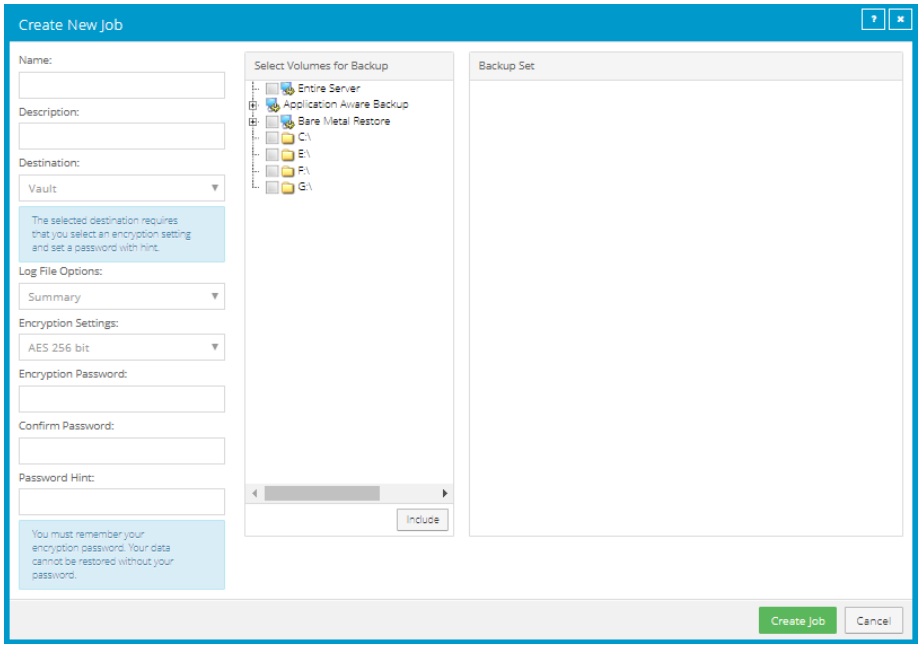
3. Click the **Jobs** tab.

   If a valid vault connection is not available for the computer, you cannot access the **Jobs** tab. You must add a vault connection before you can create a job. See Add vault settings.

4. In the **Select Job Task** menu, click **Create New Image Job**.
5. 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 more information, see Log file options.

     Note: For Image Plug-in jobs, the selected logging level does not affect the content of the logs.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.



6. In the **Select Volumes for Backup** box, do one of the following until the **Backup Set** box shows the volumes that you want to back up:
   - To back up all volumes on the system, including non-removable volumes that are added after the backup job is created, select the **Entire Server** option.

     Note: The Entire Server option is only available with Windows Agent 8.72 or later and Portal 8.87 or later.

Note: Beginning in Portal 8.89, the Bare Metal Restore option is automatically selected when you select the Entire Server option.

- To back up specific volumes, select the check box for each volume that you want to back up, and then click **Include**.
- To back up volumes that are needed to boot up the system after a system recovery, select the **Bare Metal Restore** check box, and then click **Include**.

  In addition to restoring systems from Bare Metal Restore (BMR) backups using the System Restore application, you can restore specific volumes, files, and folders from BMR backup jobs created using the Image Plug-in.
- To back up volumes with SQL Server database files, and create application-consistent SQL Server database backups, click **Application Aware Backup**, select the **SQL Volumes Protected** check box, and then click **Include**. The SQL Server Credentials dialog box appears. Enter the following credentials for connecting to SQL Server and then click **Okay**.
  - To connect to SQL Server using a Windows administrator account, select **Windows authentication**.
  - To connect to SQL Server 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.

    If you selected Windows authentication, to ensure that the Image Plug-in can protect SQL transaction logs, User Account Control (UAC) must be disabled on the system or the user must have explicit write permission to the folder where the Agent is installed and inherited permission to its subfolders.

7. 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. 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.

5.3 Add the first backup job for a Windows computer

Beginning with Portal 8.89 and Windows Agent 8.90a, backups can be configured automatically on Windows servers based on job templates. When agent auto-configuration is set up in a Portal site, you do not have to manually select a vault account and create a backup job and schedule for each Windows server. For more information, see Install the Windows Agent and plug-ins.

In Portal sites where agent auto-configuration is not available, Portal can create the first backup job for a Windows computer when you click a "Configure Automatically" button. The resulting job cannot be customized using a job template. For a computer where the Windows Agent is installed with the Image Plug-in, Portal automatically creates an Image BMR backup job that protects all volumes on the computer. For a computer where the Windows Agent is installed without the Image Plug-in, Portal automatically creates a job that backs up the C drive. Automatically-created jobs are scheduled to run every night. A valid vault profile must be available before a backup job can be created automatically.

Note: Some files are filtered out automatically from a backup job. For example, files specified by the FilesNotToBackup and FilesNotToSnapshot registry keys might not be backed up, and the job folder is not backed up.

After a job is created, you can change the job settings, if desired. For example, you can specify different folders to back up or change the schedule for running the job.

To add the first backup job for a Windows computer:

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

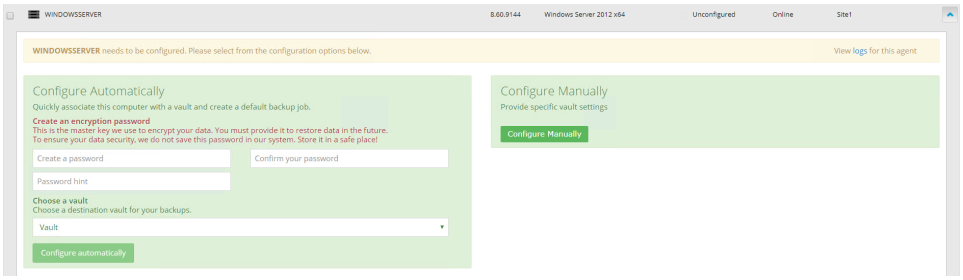
   The Computers page shows registered computers.

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

   If a Configure Manually button appears, a backup job has not been created for the computer. Other messages or buttons might also appear, as described in the following step.

3. Do one of the following:

   - If a "queued for automatic configuration" message appears for the computer, wait for the agent to be configured. Portal will attempt to configure backups on the server based on job templates in the next three minutes. See Determine whether an agent has been configured automatically.
   - To create a backup job manually, click **Configure Manually**. See Add a Windows backup job.
   - If a Configure Automatically button appears, Portal can automatically create a backup job for the computer.



Do the following:

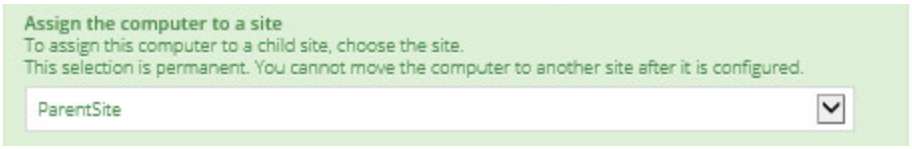
a. In the **Create a password** and **Confirm your password** boxes, enter an encryption password.

   Important: Your encryption password is required for restoring your data, so be sure to store it somewhere safe. If you forget the password, you will not be able to restore your data. The password is not maintained anywhere else and cannot be recovered.

b. In the **Password hint** box, enter a hint to help you remember the encryption password.

c. If the **Assign the computer to a site** list appears, choose a site for the computer.

   The site list appears if you are signed in as an Admin user in a parent site that has child sites, and the computer is currently in the parent site. The list includes the parent site if it has a vault profile, and all child sites. If the parent site name is in the list, it appears in bold followed by the word "Parent" in brackets.



d. If more than one vault is available, choose a vault from the **Choose a vault** list.

e. Click **Configure automatically**.

   If the configuration succeeds, a backup job appears for the computer.

   If the automatic job creation fails, do the following:

   i. Click **Configure Manually**.

   ii. On the Vault Settings tab, click **Add Vault**.

   iii. In the Vault Settings dialog box, enter vault information and credentials.

   iv. Create a backup job manually. See Add a Windows backup job.

5.4 Add a UNC file backup job

When the Windows Agent is installed on a computer, you can create a backup job that protects files and folders on UNC shares. The backup job specifies which folders and files to back up and where to save the data. You must also provide credentials for accessing the UNC share.

Note: The Agent cannot back up files and folders in a DFS namespace in a UNC job. Instead, create a separate UNC job for each server share without using the DFS namespace.

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 a UNC file backup job:

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

   The Computers page shows registered computers.

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

   If a backup job has not been created for the computer, the system can attempt to create a backup job automatically. However, this job only backs up local files. See Add the first backup job for a Windows computer.

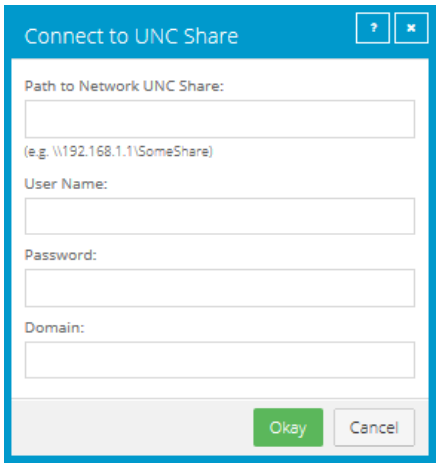
3. Click the **Jobs** tab.

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

4. In the **Select Job Task** list, click **Create New UNC Files Job**.

5. In the Connect to UNC Share dialog box, specify the following information:

   - In the **Path to Network UNC Share** box, type the name of the UNC share where you want to back up files (e.g., \\server\share).
   - In the **User Name** box, type the name of a user who has access to the UNC share.
   - In the **Password** box, type the password of the specified user.
   - In the **Domain** box, type the domain of the specified user account.

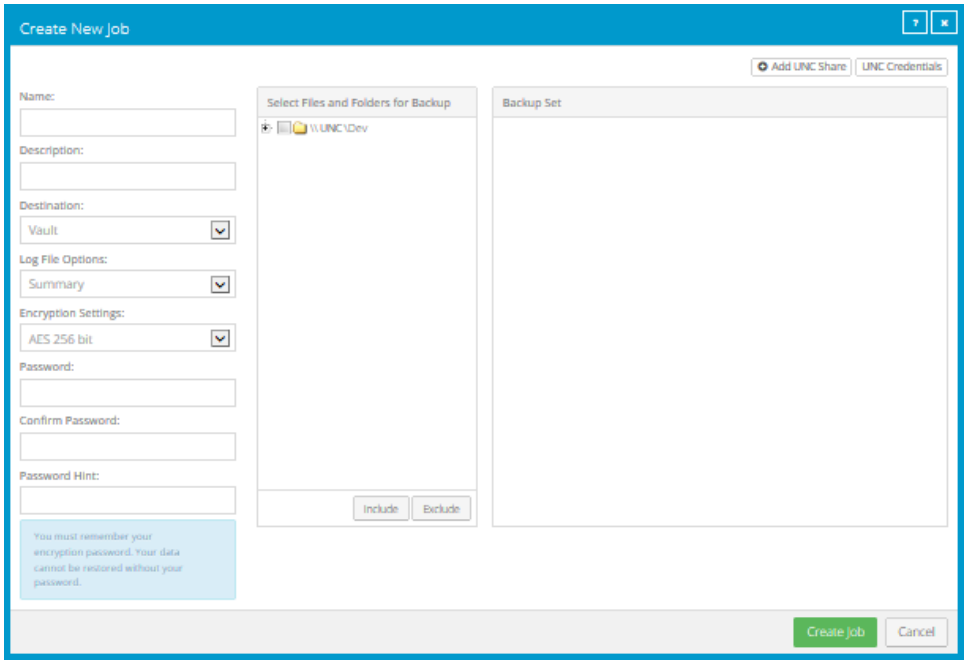
   

6. Click **Okay**.

The system validates the UNC path and credentials. If the UNC path or credentials are not valid, a message appears. You must reenter information in the dialog box and click **Okay** again.

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 more information, see Log file options.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - 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 Files and Folders for Backup** box, do one or more of the following until the **Backup Set** box shows the folders and files that you want to include or exclude:
   - To add one or more folders or files to the backup job, select the check box for each folder or file, and then click **Include**. The included folders or files appear in the **Backup Set** box. If you include a folder, the backup job includes all of the folder's subdirectories and files by default. If you do not want to back up all of the subdirectories and files, you can add filters. See Filter

subdirectories and files in backup jobs.

- To exclude one or more folders or files from the backup job, select the check box for each folder or file, and then click **Exclude**. The excluded folders or files appear in the **Backup Set** box. If you exclude a folder, all of the folder's subdirectories and files are excluded from the backup job by default. If you do not want to exclude all of the subdirectories and files, you can add filters. See Filter subdirectories and files in backup jobs.
- To remove an inclusion or exclusion record from the **Backup Set** box, click the Delete button beside the folder or file record.

9. Click **Create Job.**

   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.

5.5 Add backup jobs for a Windows cluster

After the Windows Agent and required plug-ins are installed on cluster nodes and added in Portal as described in Protect a Windows cluster, you can add backup jobs to protect the Windows failover cluster.

To fully protect a Windows cluster, you must back up:

- the quorum disk
- each physical node in the cluster
- cluster volumes

In a SQL Server cluster, you must also back up the SQL Server databases to provide point-in-time database recovery.

When a backup job runs on a virtual server, the job is automatically directed to the active cluster node. However, if failover occurs when a backup is in progress, the backup will fail and must be run again.

To add backup jobs for a Windows cluster:

1. In Portal, add the backup jobs shown in the following table:

Job	Computer where job is created	Cluster component protected	Job description
A	Virtual server for the cluster core	Quorum disk	Image or local system job that backs up the quorum disk. See Add an Image backup job or Add a Windows backup job.
B (one job for each cluster node)	Each node in the cluster	Physical nodes in the cluster	On each node in the cluster, a Bare Metal Restore (BMR) backup job created using the Image Plug-in or Windows Agent. See Add an Image backup job or Add a Windows backup job.
C (one job for each cluster role)	Virtual server for each cluster role	Cluster disks	On the virtual server for each cluster role (e.g., file server or SQL Server), an Image or local system job that backs up cluster disks for the role. See Add an Image backup job or Add a Windows backup job.
D (for SQL Server clusters only)	Virtual server for the SQL Server role	SQL Server databases	SQL Server Plug-in job that backs up all SQL Server databases. See Add a SQL Server Plug-in backup job.

2. Schedule the backup jobs to run in the order shown in Step 1.

5.6 Add a SQL Server database backup job

You can protect SQL Server databases using two types of backup jobs:

- SQL Server Plug-in backup jobs. Using the SQL Server Plug-in, you can back up one or more databases in a SQL Server instance. You can also back up SharePoint databases. See Add a SQL Server Plug-in backup job.
- Image Plug-in backup jobs. Using Image Plug-in version 7.5 or later, you can create application-consistent backups for databases in one or more SQL Server instances on a server. See Add an Image backup job.

You can back up SQL Server databases in AlwaysOn Availability Groups using either the SQL Server Plug-in or the Image Plug-in. See Protect SQL Server databases in AlwaysOn Availability Groups.

5.6.1 Add a SQL Server Plug-in backup job

When the Windows Agent and SQL Server Plug-in are installed on a computer, 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 with the SQL Server sysadmin role for 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.

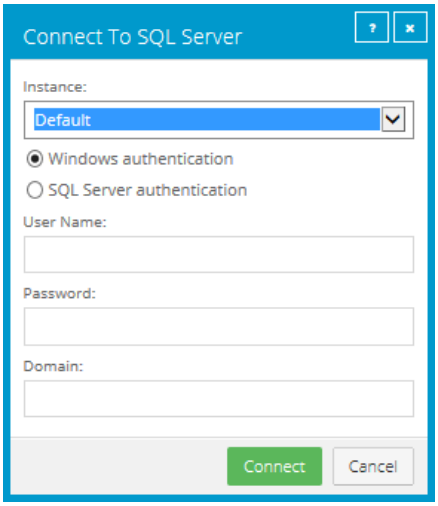
3. Click the **Jobs** tab.

   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:

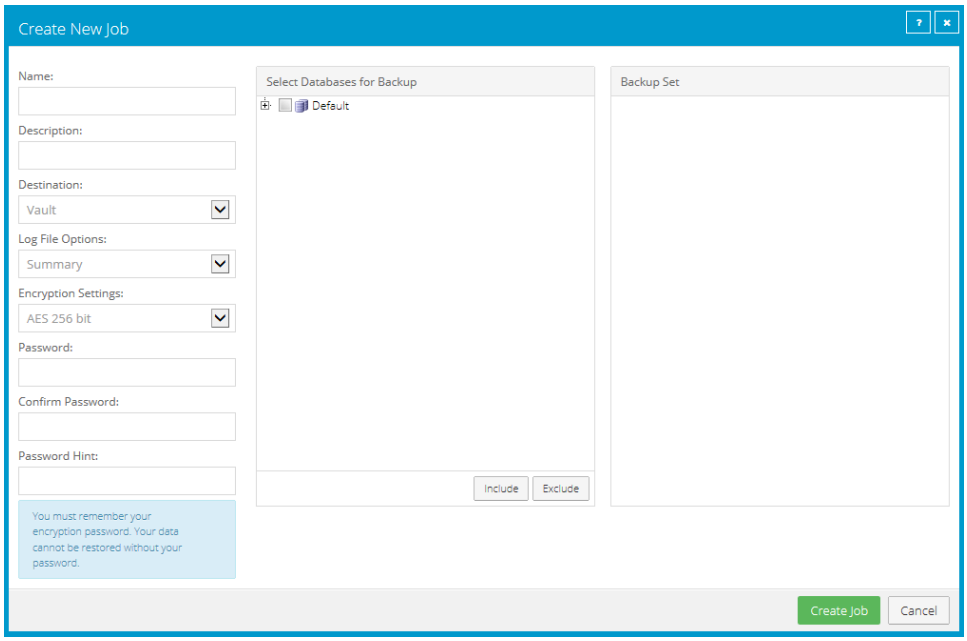
   - In the **Instance** list, select the SQL Server instance where you want to back up databases.
   - To connect to the instance using a Windows administrator account, select **Windows authentication**
   - To connect to the instance using a SQL Server administrator account, select **SQL Server authentication**.
   - 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 more information, see Log file options.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - 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.

     Note: If filter fields do not appear, you must upgrade the Agent on the computer to a version that supports database filtering.

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.

     Note: If filter fields do not appear, you must upgrade the Agent on the computer to a version that supports database filtering.

10. To remove an inclusion or exclusion record from the **Backup Set** box, click the Delete button beside the record.

11. 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.

5.6.2 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, or the Windows Agent and Image Plug-in version 7.5 or later.

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 https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/active-secondaries-backup-on-secondary-replicas-always-on-availability-groups).

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.

  If you use the SQL Server Plug-in, 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.

  If you use Image Plug-in version 7.5 or later, you can run application-consistent image backups of the volumes with database files. If the primary replica becomes a secondary replica after a failover, the Agent automatically runs copy-only backups.

- 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.

  If you use the SQL Server Plug-in, 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.

  If you use Image Plug-in version 7.5 or later, you can run application-consistent image backups of the volumes with secondary database files. The Agent automatically runs copy-only backups of secondary database files. If the secondary replica becomes the primary replica after a failover, the Agent automatically runs full backups instead of copy-only backups.

  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.

  If you use the SQL Server Plug-in, 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 you use Image Plug-in version 7.5 or later, you can run application-consistent image backups on both the primary replica server and the secondary replica server. The Agent automatically runs copy-only backups of secondary databases.

  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.

Note: Only GPT disks are supported for Image backups (including application-consistent Image backups of volumes with database files) in a cluster.

For information about restoring SQL Server databases in AlwaysOn Availability Groups, see Restore databases in AlwaysOn Availability Groups.

5.7 Add an Exchange backup job

When the Windows Agent and Exchange Plug-in are installed on a computer, you can create a backup job for one or more Microsoft Exchange databases. The backup job specifies which databases to back up, and where to save the backup data.

When running or scheduling an Exchange backup job, you can specify whether to run a Full or Incremental backup and whether to validate the Exchange data. See Run and schedule backups and synchronizations and Plan Full and Incremental Exchange backups.

After an Exchange backup job runs successfully, transaction logs for databases in the job are truncated so that the logs only contain changes that occurred after the backup.

When an Exchange server has multiple databases, you can put the databases into separate jobs and run the jobs simultaneously. Do not create parallel jobs for the same database or conflicts could prevent the jobs from completing successfully. Conflicts could also occur if you create backups using third-party applications or Agents on other Database Availability Group members.

When an Exchange backup job runs, databases in the job that are mounted or healthy are backed up. Other databases are skipped. If a database is skipped when a job runs but is mounted or healthy for the following run, the database backup does not reseed during the following run. However, if a database is skipped in two or more consecutive runs, the database backup reseeds during the next backup when the database is mounted or healthy. If no databases in a backup job are mounted or healthy when the job runs, the backup fails.

To add an Exchange backup job:

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

   The Computers page shows registered computers.

2. Find a Windows computer with the Exchange 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 more information, see the Portal online help or Windows Agent guide. See Add vault settings.

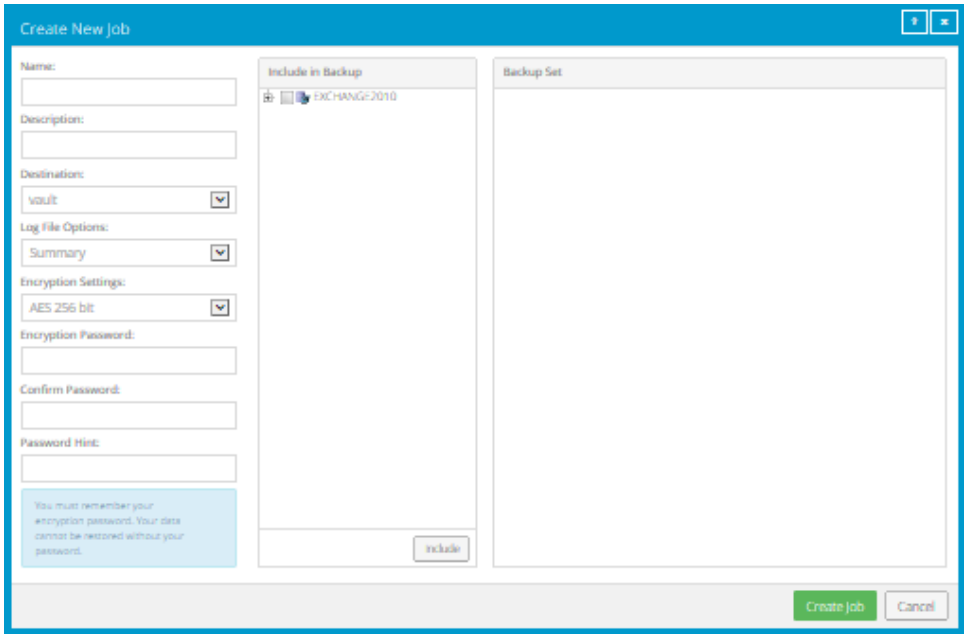
4. In the **Select Job Task** menu, click **Create New Exchange Server Job**.

5. 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 more information, see Log file options.
- For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
- In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.



6. In the **Include in Backup** box, do one of the following:
   - To add specific Exchange databases to the backup job, select the check box for each database, and then click **Include**.
   - To back up Exchange databases that match a filter when the job runs, select the check box for the server, and then click **Include**. An inclusion record appears in the **Backup Set** box.

     In the **Filter** box, enter the names of databases to back up. 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?

     Filters in a backup job are applied when the job runs. New databases that match the filters are automatically backed up when the job runs.
7. 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. 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.

5.8 Add an Oracle database backup job

When the Windows Agent and Oracle Plug-in are installed on a computer, 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.

The Oracle Plug-in backs up redo and archive logs that are created while the database backup job is running. For example, if an Oracle database backup job runs from 22:00 to 01:00 each day, the plug-in backs up redo and archive logs that are created between 22:00 and 01:00. To back up logs that are created after the Oracle database backup job runs, we recommend running a Local System or Image job at another time each day. Using the Local System or Image job, you will be able to recover the database to a point in time that is later than the time when the Oracle database backup job ran.

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 Windows 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**.

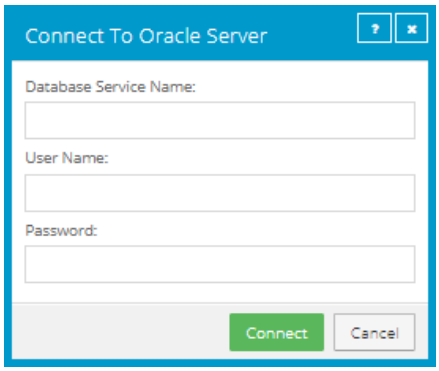
   The Computers page shows registered computers.

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.

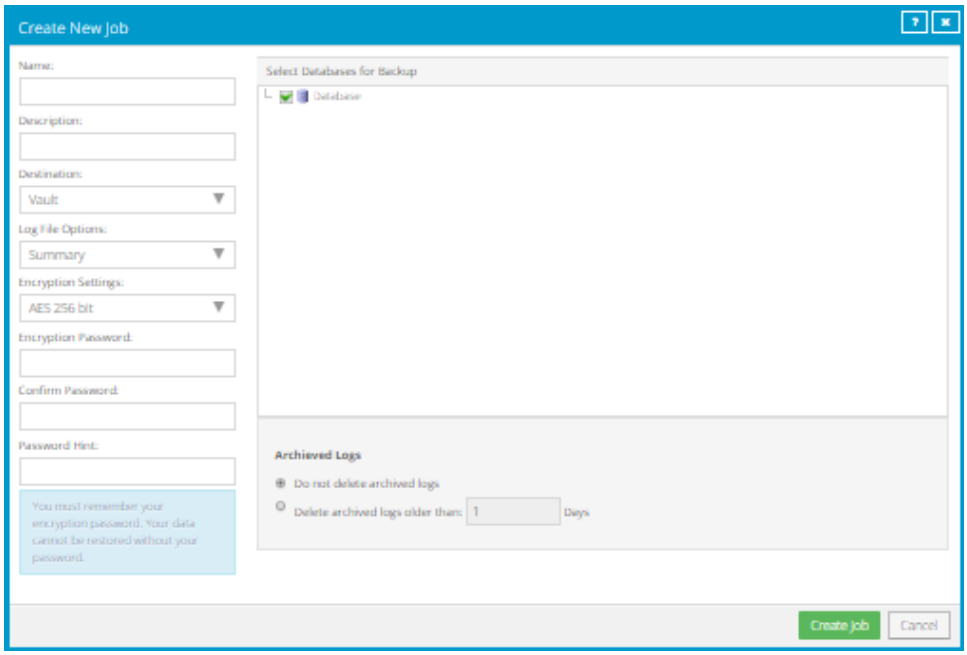
- In the **Password** box, type the password for the specified user.



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 more information, see Log file options.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - 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, 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.

5.9 Log file options

When you create or edit a backup job, you can specify the level of detail for job logging. 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.

Note: For Image Plug-in jobs, the selected logging level does not affect the content of the logs.

The following log file options are also available:

- **Create log file**. If this check box is selected, the system generates log files for each job. Log files can contain the start-connect-completion and disconnect times, file names (i.e., the names of the files that were copied during backup), and any processing errors.
- **Automatically purge expired log files**. If this check box is selected, the log file associated with a backup is automatically deleted when the backup has been deleted from the vault. Backups are typically deleted from the vault according to retention types. See Add retention types.
- **Keep the last *<number of>* log files**. Specifies the number of log files to keep for a backup job. When the specified number is reached, the oldest log file for a backup job will be deleted to make space for the newest one.

Note: You must choose either the **Automatically purge expired log files** option or the **Keep the last *<number of>* log files** option. When a backup job runs, log files are removed according to the specified option. Log files are not removed when a backup job is synchronized.

5.10 Encryption settings

Encryption settings specify the encryption type for backup data at rest on the vault. AES 256 bit encryption is the only encryption type available for new backup jobs.

If an existing job uses another encryption type (e.g., AES 128 bit, Blowfish, DES, Triple DES), you can continue to encrypt the job using that type. However, if you change the encryption type for an existing job, you cannot change the encryption type back to the original type. Only AES 256 bit will be available.

If you change encryption options for an existing job, it will force a new full backup (i.e., a reseed). The next backup will take longer than previous delta backups, and the amount of data stored on the vault will increase temporarily, depending on your retention settings.

Encryption password

You must enter a password for the encrypted backup data. The password is case-sensitive. To recover the data, you must provide the encryption password that was entered when the files were backed up.

You can also enter a password hint. When restoring data, you can view the password hint to remind you of the encryption password for this job. The password hint can include lowercase characters (a-z), uppercase characters (A-Z), international characters (Á-ÿ), numbers (0-9), spaces, and the following special characters: ! @ # $ % ^ & * ( ) _ - + = [ ] { } | ' " : ; , < . > ? ~ `

IMPORTANT: The encryption password is required for restoring the data, so be sure to store it somewhere safe. If you forget your password, you will not be able to restore your data. The password is not maintained anywhere else and cannot be recovered.

5.11 Filter subdirectories and files in backup jobs

When you include and exclude folders in a backup job, the folder's subdirectories and files are also included or excluded by default.

If you only want to back up some subdirectories or files in a folder, you can add filters to the inclusion record. For example, you could add a filter so that files in a folder are only backed up if they have the .doc or .docx extension.

If you only want to exclude some subdirectories or files in a folder from a backup job, you can add filters to the exclusion record. For example, you could add a filter so that files in a folder are only excluded from the backup if they have the .exe extension.

If a policy is assigned to a computer, you can add filters from the policy to a folder inclusion or exclusion record.

Filters in a backup job are applied when the job runs. New subdirectories and files that match the filters are automatically backed up or excluded when the job runs.

To filter subdirectories and files in a backup job:

1. When creating or editing a backup job, view the **Backup Set** box.

2. If editable fields do not appear for a folder inclusion or exclusion record where you want to filter subdirectories and files, click the **Edit** button in the folder row. 

3. In the **Backup Set** box, for each included folder where you want to include specific subdirectories or files, do one or more of the following:

   - To include specific subdirectories in the backup job, in the **Folders Filter** field, enter the names of subdirectories to include. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only include subdirectories in a backup if their names end with "-current" or start with "2015", enter the following filter: *-current, 2015*

     Note: Asterisks (*) are the only supported wildcards in filter fields.

- To include specific files in the backup job, in the **Files Filter** field, enter the names of files to include in the backup. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only include files in a backup if they have the .doc or .docx extension, enter the following filter: *.doc, *.docx

  Note: Asterisks (*) are the only supported wildcards in filter fields.

- To apply a file inclusion filter to the specified folder but not to its subdirectories, clear the **Recursive** check box.

  If a file filter is not applied to the inclusion, clearing the **Recursive** check box will have no effect. The specified folder and all of its content will be included.

- If a policy is assigned to the computer, to apply filters from the policy to the folder inclusion record, click the **Apply Policy Filters** button. 

4. In the **Backup Set** box, for each excluded folder where you want to exclude specific subdirectories or files, do one or more of the following:

   - To exclude specific subdirectories from the backup job, in the **Folders Filter** field, enter the names of subdirectories to exclude. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only exclude subdirectories from a backup if their names end with “-old” or start with “2001”, enter the following filter: *-old, 2001*

     Note: Asterisks (*) are the only supported wildcards in filter fields.

   - To exclude specific files from the backup job, in the **Files Filter** field, enter the names of files to exclude. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only exclude files from a backup if they have the .exe or .dll extension, enter the following filter: *.exe, *.dll

     Note: Asterisks (*) are the only supported wildcards in filter fields.

   - To apply a file exclusion filter to the specified folder but not to its subdirectories, clear the **Recursive** check box.

     If a file filter is not applied to the exclusion, clearing the **Recursive** check box will have no effect. The specified folder and all of its content will be excluded.

   - If a policy is assigned to the computer, to apply filters from the policy to the folder exclusion record, click the **Apply Policy Filters** button. 

5. Click **Create Job** or **Save**.

5.12 Edit a backup job

You can edit existing backup jobs to change the following settings:

- Items to back up
- Log file options

- Encryption settings. If you change the encryption method or password in a backup job, the job will reseed the next time it runs.
- Job description

For a SQL Server Plug-in backup job, you can also change the SQL Server instance where you want to back up databases and credentials for connecting to the instance.

Depending on backup job type, other options might appear in the Edit Job dialog box.

Note: You cannot change the name or destination of a job.

To edit a backup 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 edit, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. Do one of the following:
   - In the **Name** column, click the name of the job that you want to edit.
   - In the **Select Action** menu of the job that you want to edit, click **Edit Job**.

     The Edit Job dialog box shows the current job settings.
5. For a SQL Server Plug-in backup job, to change the SQL Server instance or credentials for connecting to the instance, click **Change Instance / Credentials**. In the Connect to SQL Server dialog box, select the SQL Server instance where you want to back up databases and specify credentials for connecting to the instance. Click **Connect**.
6. Do one or more of the following:
   - In the **Description** box, type a description for the backup job.
   - In the **Log File Options** list, select the level of detail for job logging.

     Note: For Image Plug-in jobs, the selected logging level does not affect the content of the logs.
   - In the **Encryption Settings** list, select the encryption method for the backup data. In most jobs, the encryption method is AES 256 bit. See Encryption settings. In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.
   - In the box that shows items for backup, select items to back up.
7. If other options are available, enable or disable the options as desired.

   IMPORTANT: If you disable threat detection for a Windows job where it was enabled, any potential threat flags for backups in the job will be cleared. Only disable threat detection for a job once all potential threats have been addressed.
8. Click **Save**.

6 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.

  When deleting job data from vaults, there is a 72-hour waiting period before the data deletion request is sent to vaults. This waiting period gives Admin users in the site an opportunity to cancel the data deletion, if required. See Cancel a scheduled job data deletion. During the waiting period, the job continues to run as scheduled.

- Delete computers from Portal and submit requests to delete the computer data from vaults. See Delete a computer and delete computer data from vaults.

  Note: Beginning in Portal 8.90, Admin users can submit requests to delete data from vaults for online or offline computers. In previous Portal versions, requests to delete data from vaults could only be submitted for online computers.

  When deleting computer data from vaults, there is a 72-hour waiting period before the data deletion request is sent to vaults. This waiting period gives Admin users in the site an opportunity to cancel the data deletion, if required. See Cancel a scheduled computer data deletion. During the waiting period, the computer's jobs continue to run as scheduled.

- Delete specific backups from vaults. This option is available beginning in Portal 8.90. See Delete specific backups from vaults.

  Backup deletion requests are submitted to vaults immediately; there is no waiting period before the data deletion request is sent to vaults. Because backup deletion requests are submitted immediately, backup deletion requests cannot be canceled.

6.1 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. Because the data remains in the vaults, you will be billed for it.

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 computer 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 **Remove job** 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.

6. In the confirmation dialog box, type **CONFIRM.**

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

7. Click **Confirm Deletion**.

6.2 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. After the data is deleted from the vaults, you will not be billed for it.

To protect against inadvertently deleting the wrong data, 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 waiting period, the job continues to run as scheduled.

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.

Note: Because the data is available for restore during the 72-hour waiting period, it will still be included in customer invoices. Usage reduction for invoicing purposes does not occur until the data is deleted.

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:

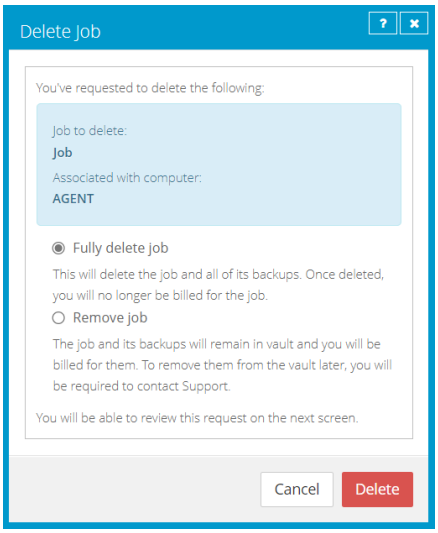
1. When signed in as an Admin user, click **Computers** on the navigation bar.

   The Computers page shows registered computers.

2. Find the computer 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**.

   IMPORTANT: To permanently delete unnecessary data from vaults and reduce billing, you must select **Fully delete job**. If you select **Delete job**, data will not be removed from vaults and your invoice will not be affected.

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

6. In the confirmation dialog box, type **CONFIRM.**

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

7. Click **Confirm Deletion**.

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

8. 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.

Beginning in Portal 9.10, when a job is scheduled for deletion, the **Scheduled for Deletion** status appears for every instance of the job in Portal. A job can appear for multiple computers if a computer was re-registered or the Restore from Another Computer workflow was used.

An email is sent to Admin users in the site and to Super users to indicate that the job deletion has been scheduled. During the 72-hour waiting period before data is deleted, you can cancel the deletion request. Because the data is available for restore during this period, it will still be included in customer invoices. Usage reduction for invoicing purposes does not occur until the data is deleted.

When data deletion is in progress for a job, the **Deletion in Progress** status appears for the job. Beginning in Portal 9.20, the **Scheduled for Deletion** status appears for every instance of the job in Portal.

When a job is deleted from vaults, the job is deleted from all computers where it appears.

6.3 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.

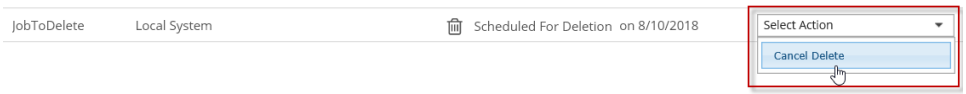
Beginning in Portal 9.10, when a job is scheduled for deletion, the **Scheduled for Deletion** status appears for every instance of the job in Portal. A job can appear for multiple computers if a computer was re-registered or the Restore from Another Computer workflow was used. An Admin user can cancel the deletion from any instance of the job.

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 computer 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.

6.4 Delete a computer without deleting data from vaults

Admin users can delete computers from Portal without deleting the computer data from vaults. You can delete both online and offline computers from Portal without deleting data from vaults. Because the data remains in the vaults, you will be billed for it.

If a computer is deleted from Portal in this way, the data can still be restored using the *Restore from Another Computer* procedure.

Note: When a computer is deleted from Portal, the agent is not removed from the computer where it is installed. To remove the agent from the computer, you must manually uninstall it.

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 **Remove computer(s) from Portal only** and then click **Delete**.

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

5. In the confirmation dialog 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**.

6.5 Delete a computer and delete computer data from vaults

In a Portal instance where the data deletion feature is enabled, Admin users can delete computers and request that data for the computers be deleted from all vaults. After the data is deleted from the vaults, you will not be billed for it.

Note: Beginning in Portal 8.90, Admin users can submit requests to delete data from vaults for online or offline computers. In previous Portal versions, requests to delete data from vaults could only be submitted for online computers.

To protect against inadvertently deleting the wrong data, the data deletion is scheduled for 72 hours after the request is made, an email notification is sent to Admin users in the site and to Super users, and the status of the computer in Portal changes to *Scheduled for deletion*. During the waiting period, the computer's jobs continue to run as scheduled.

During the 72-hour waiting period before a computer data deletion request is sent to vaults, Admin users in the site can cancel the scheduled computer data deletion. See Cancel a scheduled computer data deletion.

If a scheduled computer data deletion is not canceled during the 72-hour waiting period, 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. After the computer data is deleted from vaults, the computer is deleted from Portal.

Note: Because the data is available for restore during the 72-hour waiting period, it will still be included in customer invoices. Usage reduction for invoicing purposes does not occur until the data is deleted.

Note: When a computer is deleted from Portal, the agent is not removed from the computer where it is installed. To remove the agent from the computer, you must manually uninstall it.

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

To delete a computer and delete computer data from vaults:

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

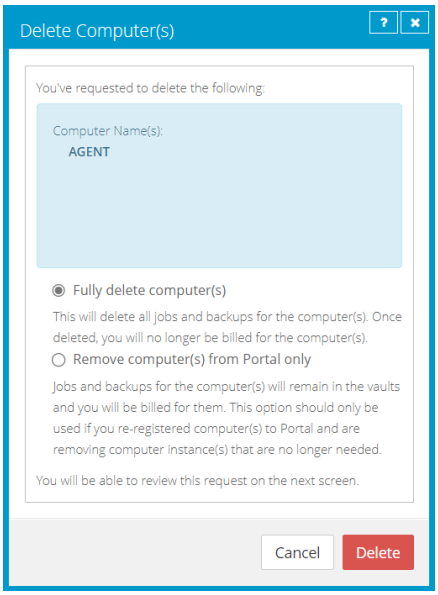
   The Computers page shows registered computers.

2. Select the check box for each 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.

   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**.

   IMPORTANT: To permanently delete unnecessary data from vaults and reduce billing, you must select **Fully delete computer(s)**. If you select **Delete computer(s)**, data will not be removed from vaults and your invoice will not be affected.

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

5. In the confirmation dialog box, type **CONFIRM**.

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

6. Click **Confirm Deletion**.

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

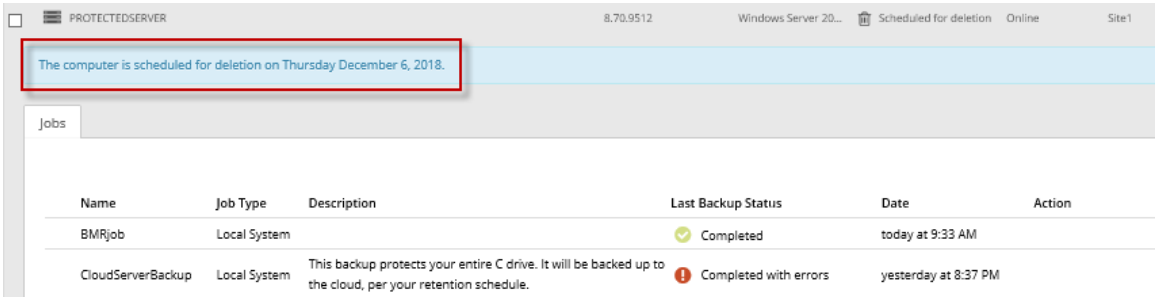
   A Computer(s) Deleted dialog box states that the computer(s) and associated data in your vault(s) are scheduled to be deleted.

7. 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.

   During the 72-hour period, you can cancel the deletion request. Because the data is available for restore during this period, it will still be included in customer invoices. Usage reduction for invoicing purposes does not occur until the data is 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.



6.6 Cancel a scheduled computer data deletion

In a Portal instance where the data deletion feature is enabled, Admin users can delete an online 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. See Delete a computer and delete computer data from vaults.

During the 72-hour period before a computer data deletion request is set to 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 computer for which you want to cancel the scheduled data deletion.

   The Status column shows *Scheduled for deletion* for each computer that is scheduled for deletion.

3. In the Actions list, click **Cancel Deletion of Selected Computers**.

   Note: If **Cancel Deletion of Select Computers** is not available, the data deletion request for a selected computer may have already been sent to vaults. To see when a computer was scheduled for deletion, expand the computer row.

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

4. Click **Yes**.

   A Success dialog box appears.

5. 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.

6.7 Delete specific backups from vaults

In a Portal instance where the data deletion feature is enabled, Admin users can request that specific backups (also known as safesets) be deleted from all vaults. When selecting backups to delete, Admin users can view information about each backup, including its date, retention settings, size, and whether it has a potential ransomware threat.

Backup deletion requests are submitted to vaults immediately and the data is automatically deleted from associated vaults. Because backup deletion requests are submitted immediately, backup deletion requests cannot be canceled.

When a backup deletion request is submitted, an email notification is sent to Admin users for the site and to Super users. A notification also appears in the Status Feed.

If a backup deletion request fails, an email notification is sent to a vault administrator whose email address is specified in Portal. The vault administrator can then manually delete the backup or backups from vaults.

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

To delete specific backups 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 computer with the backups 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 with backups that you want to delete, click **Delete Backup**.

   If the Delete backup option does not appear or a message states that the job is registered to a vault that does not support backup deletion, you cannot submit a request to automatically delete backups from vaults.

   A Delete Backup dialog box appears. The dialog box shows information about each backup, including its retention settings, size, and whether it has a potential ransomware threat. Backups that cannot be deleted (e.g., because a deletion request is scheduled for the job or computer) cannot be selected.

5. Select the check box for each backup that you want to delete, and then click **Delete**.

   Backups that cannot be deleted (e.g., because a deletion request is scheduled for the job or computer) cannot be selected.

   You cannot delete all available backups for a job. Instead, delete the entire job. See Delete a backup job and delete job data from vaults.

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

6. In the confirmation dialog box, type **CONFIRM** in the text box.

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

7. Click **Confirm Deletion**.

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

   A dialog box states that the backup data will be deleted from vaults.

8. Click **Close**.

7 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 on specific days of the week or month. See Run an ad-hoc backup and Schedule a backup.

To help you meet your recovery point objectives (RPOs), when Windows Agent 8.90 or later is backing up data to a Director version 8.60 or later vault, you can schedule a backup job to run multiple times per day, as often as hourly. See Schedule a backup to run multiple times per day.

Beginning with Portal 9.30 and Windows Agent 9.30, Image and Local System backups can also be triggered by system events on supported Windows desktop operating systems. See Trigger backups when events occur on Windows desktop computers.

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 remaining data.

  If a backup job is deferred while an item is being backed up, the backup for that item is incomplete and data from the item cannot be restored. However, you can restore items that were completely backed up in the job before the job was deferred.

  The following table describes deferral behavior for specific backup types:

Backup type	Behavior
System State	If the System State option is selected in a Windows backup job, the job cannot be deferred. If the agent tries to defer a job where System State data is being backed up, the backup fails.
Image Plug-in	In an Image Plug-in job, once a volume has been completely backed up, a backup for that volume cannot be deferred. When an Image Plug-in job runs, the agent backs up changes in any volumes that have been completely backed up and then starts to back up any remaining volumes. The backup can be deferred for any volume that was not previously backed up completely. If an Image Plug-in backup job is deferred while a volume is being backed up, the backup for the volume is incomplete and data from the volume cannot be restored. However, you can restore volumes, and files and folders from volumes in the job that were completely backed up.

SQL Server Plug-in	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.
Exchange Plug-in	Incremental backups for Exchange cannot be deferred, even if deferring is enabled. Deferring can be applied to full backups for Exchange.
To SSI files	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), be sure that only one tool is being used for truncating logs.

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

- For an application-aware Image Plug-in job, you can specify whether to truncate SQL Server database transaction logs.

  Note: If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.

- For an Exchange Plug-in backup job, you can specify whether to:
  - Run a Full or Incremental backup. When the Full backup type is selected, the database files, checkpoint file and transaction logs are backed up. When the Incremental backup type is selected, the database files, checkpoint file and transaction logs are backed up in the first "seed" backup, but only the checkpoint file and transaction logs are backed up in subsequent runs. For more information, see Plan Full and Incremental Exchange backups.
  - Validate Exchange data during the backup. When this option is selected, a utility checks the Exchange data during the backup. If data corruption is detected, the backup fails and the corruption is reported.

For computers with Windows 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 amount of data stored vs. the backup speed. 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 a backup runs, you can view logs to check whether the backup completed successfully. See View a job’s process logs and safeset information.

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.

7.1 Schedule a backup

After creating a backup job, you can add one or more schedules for running the job on specific days of the week or month. 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.

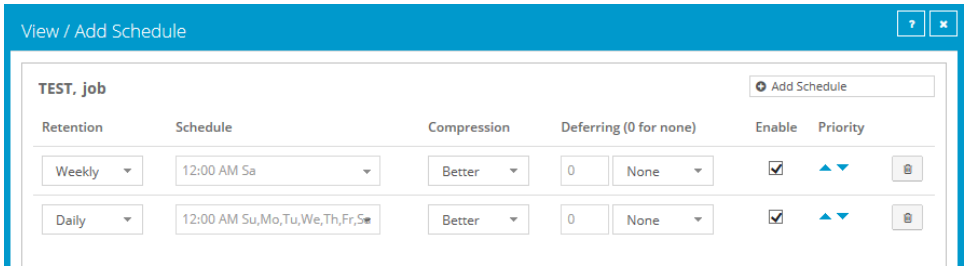
Note: Beginning in Portal 8.88, when Windows Agent 8.90 or later is backing up data to a Director version 8.60 or later vault, you can also schedule a backup job to run multiple times per day, as often as hourly. See Schedule a backup to run multiple times per day.

Note: Beginning with Portal 9.30 and Windows Agent 9.30, Image and Local System backups can also be triggered by system events on supported Windows desktop operating systems. See Trigger backups when events occur on Windows desktop computers.

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, and the retention type of the schedule that is higher in the schedule list is applied to the resulting safeset. For example, in the following screenshot, a job is scheduled to run at 12 AM on Saturdays by two schedules. 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 resulting 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.



When you schedule a backup, the View/Add Schedule dialog box shows the maximum number of restore points that could result from the job's current schedules and retention types. You can then change your schedules, if required. See Maximum number of restore points for a job.

To schedule a backup job to run at a specific time on specific days of the week or month:

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 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.

   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. See Add retention types.

   The 24-Hours and 48-Hours retention types are only available for intra-daily schedules. See Schedule a backup to run multiple times per day.
4. If the schedule is for a SQL Server Plug-in database backup job, 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.

     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), be sure that only one tool is being used for truncating logs.

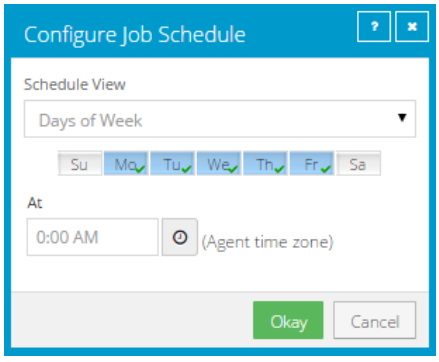
Note: Transaction logs can only be backed up for databases that use the full or bulk-logged recovery model.

6. If the schedule is for an Image Plug-in job that backs up volumes with SQL Server database files, do one of the following in the **SQL Application Settings** list:
   - To truncate database transaction logs after the backup, select **Truncate transaction logs**.
   - To run the backup without truncating logs, clear **Truncate transaction logs.**

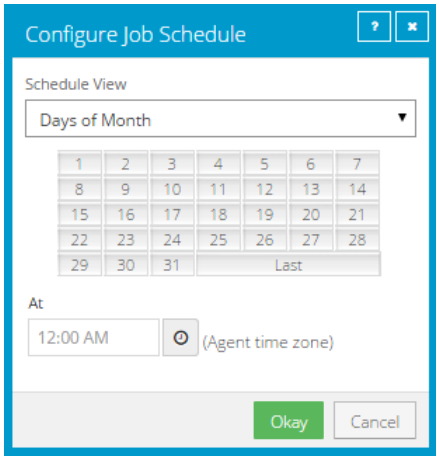
     Note: If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.
7. If the schedule is for an Exchange database backup job, do the following:
   - In the **Backup Type** list, do one of the following:
     - To only back up transaction logs and the checkpoint file after the first "seed" backup, click **Incremental**.
     - To back up the database files, checkpoint file and transaction logs, click **Full**.

     For more information, see Plan Full and Incremental Exchange backups.
   - To validate Exchange data during the backup, select **Validate Exchange database**.
8. In the **Schedule** box, click the arrow.

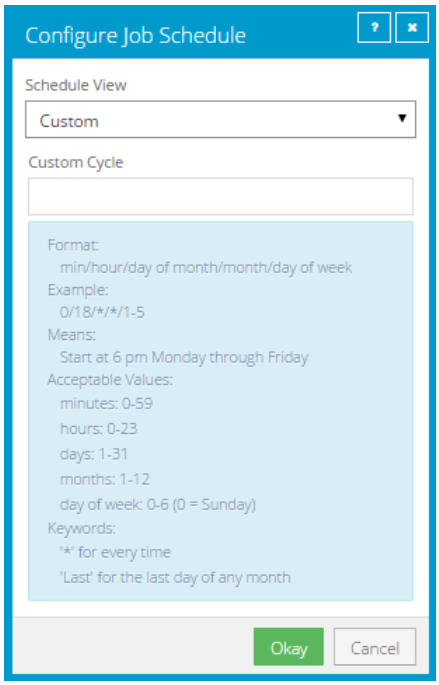
   The Configure Job Schedule dialog box opens.
9. In the Configure Job Schedule dialog box, do one of the following:
   - To run the backup on specific days each week, select **Days of Week** in the **Schedule View** list. Select the days when you want to run the job. Then use the **At** field to specify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

   - 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.



- 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.



Note: If **Intra-daily** appears in the **Schedule View** list, you can also schedule the backup to run multiple times each day. See Schedule a backup to run multiple times per day.

10. Click **Okay**.

    The new schedule appears in the Schedule box.

11. In the **Compression** list, click a compression level for the backup data. Compression levels optimize Compression levels optimize the amount of data stored vs. the backup speed.

12. 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.

      Note: Incremental backups for Exchange cannot be deferred, even if deferring is enabled. Deferring can be applied to full backups for Exchange.
13. To run the job on the specified schedule, select the **Enable** check box near the end of the row.
14. 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.
15. Check the number of restore points that could result from the job's schedules and retention policies. If you want to increase or decrease the number of restore points, change the schedules or retention types.

    The maximum number of restore points appears below the schedules in the View/Add Schedule dialog box. For more information, see Maximum number of restore points for a job.
16. If an Automatic Retry for Scheduled Backups section appears in 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.
17. If a Windows Event Backup Triggers section is available in the View / Add Schedule dialog box, you might be able to create a Windows event backup trigger. When a backup job has a trigger, the job runs automatically when a user logs on to the computer or the computer starts to shut down. See Trigger backups when events occur on Windows desktop computers.
18. Click **Save**.

7.2 Schedule a backup to run multiple times per day

Beginning in version 8.90, when the Windows Agent is backing up data to a Director version 8.60 or later vault, you can schedule the backup job to run multiple times per day by creating an intra-daily schedule using Portal 8.88 or later.

Note: To schedule a backup job to run on specific days of the week or month, see Schedule a backup.

Note: Beginning with Portal 9.30 and Windows Agent 9.30, Image and Local System backups can also be triggered by system events on supported Windows desktop operating systems. See Trigger backups when events occur on Windows desktop computers.

Each backup job can have one intra-daily schedule. If the job has other schedules, the intra-daily schedule has the lowest priority and is at the bottom of the schedule list. If a job is scheduled to start at exactly the same time by an intra-daily schedule and another schedule, the job only runs once and the retention type of the other schedule (e.g., daily or monthly) is applied to the resulting safeset.

When you create an intra-daily schedule for a backup job, you can choose one of two retention types:

- 24-Hours. With this retention type, each backup is kept for at least 24 hours and at least one backup with this retention type is stored online.
- 48-Hours. With this retention type, each backup is kept for at least 48 hours and at least one backup with this retention type is stored online.

Other retention types are not available for intra-daily schedules. You cannot add, change or delete retention types for intra-daily schedules.

When you schedule a backup, the View/Add Schedule dialog box shows the maximum number of restore points that could result from the job's current schedules and retention types. You can then change your schedules, if required. See Maximum number of restore points for a job.

To reduce schedule overloads, backups that are scheduled by intra-daily schedules are skipped in some cases. See Skipped backups.

To schedule a backup job to run multiple times per day:

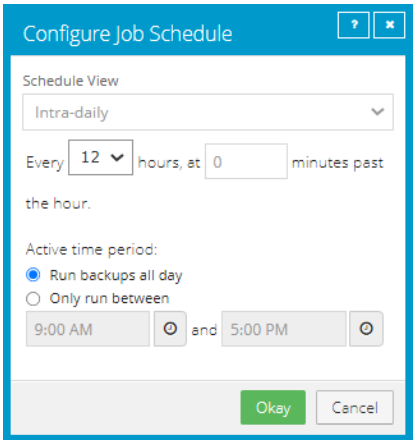
1. Do one of the following:
   - On the navigation bar, click **Computers**. Find the computer with the backup job that you want to schedule, and click the row to expand its view. On the Jobs tab, find the job that you want to schedule. In its **Select Action** menu, click **View/Add Schedule**.
   - 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, click the arrow in the **Schedule** box.

   IMPORTANT: To create an intra-daily schedule, you must select **Intra-daily** in the Schedule box before selecting a retention type.

4. In the Configure Job Schedule dialog box, do the following:

    a. In the **Schedule View** list, select **Intra-daily**.



    b. In the **Every *x* hours** list, click the frequency for running the job. You can schedule the job to run every 1, 2, 3, 4, 6, 8 or 12 hours.

    c. In the **at *y* minutes past the hour** box, type the number of minutes after the hour when you want to run the job. For example, enter 15 to run the job at 15 minutes past each hour when the job runs.

    d. In the Active time period area, do one of the following:

    - To run the job at the specified frequency for the full 24 hour period, click **Run backups all day**.
    - To run the job according to the intra-daily schedule for only part of each 24-hour day period, click **Only run between**. Click the first clock icon and specify the start of the time period for running backups at the specified frequency. Click the second clock icon and specify the end of the time period for running backups at the specified frequency.

    e. Click **Okay**.

    If the job has other schedules, the intra-daily schedule appears at the bottom of the schedule list and has the lowest priority. The priority of the intra-daily backup schedule cannot be changed.

5. In the **Retention** list, click one of the following retention types:

    - **24-Hours**. With this retention type, each backup is kept for at least 24 hours and at least one backup with this retention type is stored online.
    - **48-Hours**. With this retention type, each backup is kept for at least 48 hours and at least one backup with this retention type is stored online.

    Other retention types are not available for intra-daily schedules.

6. If the schedule is for a SQL Server Plug-in database backup job, 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.

     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), be sure that only one tool is being used for truncating logs.

     Note: Transaction logs can only be backed up for databases that use the full or bulk-logged recovery model.
7. If the schedule is for an Image Plug-in job that backs up volumes with SQL Server database files, do one of the following in the **SQL Application Settings** list:
   - To truncate database transaction logs after the backup, select **Truncate transaction logs**.
   - To run the backup without truncating logs, clear **Truncate transaction logs.**

     Note: If you also back up databases using another tool (e.g., native SQL Server backup), use only one tool for truncating logs.
8. If the schedule is for an Exchange database backup job, do the following:
   - In the **Backup Type** list, do one of the following:
     - To only back up transaction logs and the checkpoint file after the first “seed” backup, click **Incremental**.
     - To back up the database files, checkpoint file and transaction logs, click **Full**.

     For more information, see Plan Full and Incremental Exchange backups.
   - To validate Exchange data during the backup, select **Validate Exchange database**.
9. In the **Schedule** box, click the arrow.

   The Configure Job Schedule dialog box opens.
10. Click **Okay**.

    The new schedule appears in the Schedule box.
11. In the **Compression** list, click a compression level for the backup data. Compression levels optimize the amount of data stored vs. the backup speed.

12. 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. For deferral behavior for specific backup types, see Run and schedule backups and synchronizations.

      Note: Incremental backups for Exchange cannot be deferred, even if deferring is enabled. Deferring can be applied to full backups for Exchange.
13. To run the job on the specified schedule, select the **Enable** check box near the end of the row.
14. Check the number of restore points that could result from the job's schedules and retention policies. If you want to increase or decrease the number of restore points, change the schedules or retention types.

    The maximum number of restore points appears below the schedules in the View/Add Schedule dialog box. For more information, see Maximum number of restore points for a job.
15. In the Automatic Retry for Scheduled Backups section at the bottom of the View / Add Schedule dialog box, specify whether scheduled backups should retry after a failed backup. See Specify whether scheduled backups retry after a failure.
16. If a Windows Event Backup Triggers section is available in the View / Add Schedule dialog box, you might be able to create a Windows event backup trigger. When a backup job has a trigger, the job runs automatically when a user logs on to the computer or the computer starts to shut down. See Trigger backups when events occur on Windows desktop computers.
17. Click **Save**.

7.2.1 Skipped backups

Beginning in version 8.90, when the Windows Agent is backing up data to a Director version 8.60 or later vault, you can schedule the backup job to run multiple times per day, as often as hourly, by creating an intra-daily schedule using Portal 8.88 or later. See Schedule a backup to run multiple times per day.

To reduce schedule overloads when a backup job runs multiple times per day, backups are skipped when:

- An agent starts a backup that is scheduled by an intra-daily schedule, and a backup is already running for the job.

  Note: Windows Agent 8.72 also skips a backup if it is scheduled to run multiple times per day by a custom schedule and a backup is already running for the job.

- An agent contacts a Director version 8.60 or later vault to start a backup that is scheduled by an intra-daily schedule, and the vault is busy with high-priority maintenance for the job data.

Backups are not skipped if they are scheduled to run daily or less often, or are ad hoc (not scheduled). In these cases, if a backup is already running for the job, the new backup is queued and starts when the current backup is finished. If the vault is busy with high-priority maintenance for the job data, the new backup is delayed for five minutes. After this delay, the backup starts and interrupts any maintenance that is running for the job data.

If email notifications are configured centrally in a Portal instance, Admin users can receive an email when a backup is skipped. See Set up email notifications for backups on multiple computers. When the last backup status reported for a job was "Skipped", this Last Backup Status appears for the job on the Computers page and Monitor page. See View computer and job status information and View, export and email backup statuses on the Monitor page. The Daily Status report also shows skipped backups.

In some Portal instances, users can also see skipped rates and 48-hour backup status histories for jobs. See View skipped rates and backup status histories.

Best practices: Reducing the number of skipped backups

If you notice that some backups are skipped frequently, you can make changes to the backup job, backup schedule, or servers to ensure reliable backups. For example, you could:

- Reduce the frequency of the scheduled backups.
- Reduce the size of the job.
- On a Windows server, change from a Local System job to an Image job.
- Add system resources (e.g., RAM, CPU, Storage IO) on the server where the agent is running. While the resources on a server might be sufficient for backing up and restoring data periodically, the resources might not be sufficient to run backups multiple times per day.
- Add system resources to the vault server.

7.3 Maximum number of restore points for a job

Beginning in Portal version 8.88, when you schedule a backup job, the View/Add Schedule dialog box shows the maximum number of restore points that could result from the job's current schedules and retention types. The maximum number of restore points, or backups in the vault, is updated when you add or change a schedule row so you can understand the impact of your schedule changes and make additional changes, if required.

Note: Beginning in Portal 9.30, the "Maximum number of restore points" for a job is named "Maximum number of scheduled restore points". This value does not include ad hoc backups or backups that are started by Windows event backup triggers.

For example, if you schedule a backup to run daily and select the default Monthly retention type (which specifies that each backup is kept for 365 days), the maximum number of restore points shown in the View/Add Schedule dialog box is 365. If 365 restore points would use too much vault storage, you can

reduce the frequency of the backups or change the retention type. For example, you could change the retention type to the default Daily retention type, which specifies that each backup is kept for 30 days.

The maximum number of restore points includes backups created from Intra-daily, Days of Week and Days of Month schedules. The maximum number of restore points does not include restore points created using:

- Custom schedules for the job.
- Retention types that are no longer used. If a schedule was deleted or the retention for a job was changed, additional backups might remain in the vault.

  For example, if a job was scheduled to run daily using the default Daily retention type, but you delete that schedule and create a new schedule using another retention type, backups from the original daily schedule plus backups from the new schedule will be saved in the vault. However, backups from the original daily schedule would not be included in the Maximum number of restore points shown in the View/Add Schedule dialog box.

7.4 Specify whether scheduled backups retry after a failure

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

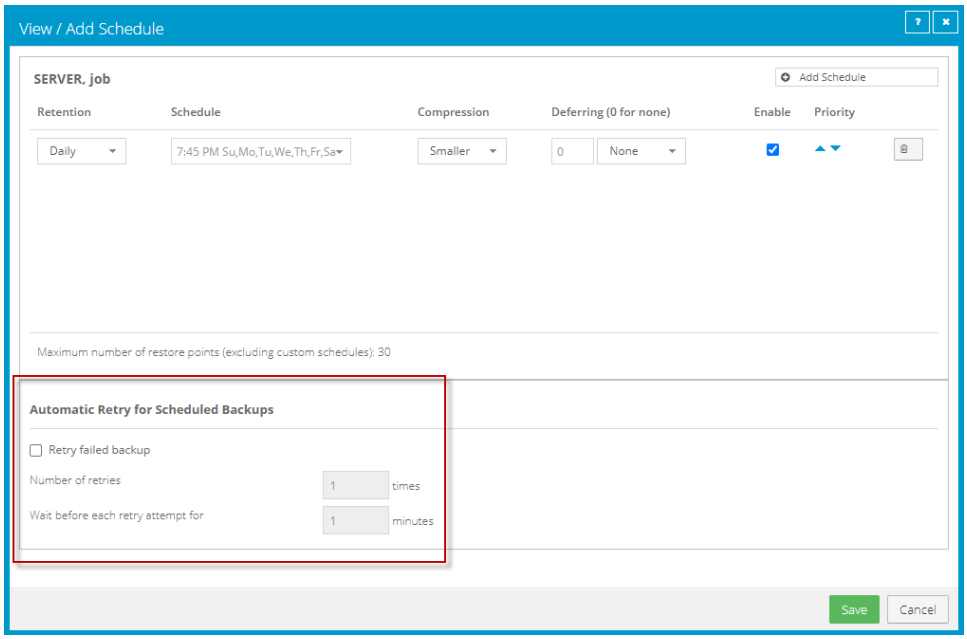
You can also specify how many times a scheduled backup should retry after a failed attempt, and specify the amount of time between retries.

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 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.



3. Click **Save**.

7.5 Trigger backups when events occur on Windows desktop computers

Beginning with Windows Agent 9.30 and Portal 9.30, Image and Local System backups can be triggered by system events on computers with supported Windows desktop operating systems.

On each computer, only one Image or Local System backup job can have a Windows event backup trigger. The backup trigger can be a:

- Log On trigger, where a backup starts automatically when a user logs on to the computer.

  or

- Shut Down trigger, where a backup starts automatically when the computer starts to shut down or restart.

  When you create a Shut Down trigger for a backup job on a computer, the agent automatically disables Fast Startup on the computer. If you re-enable Fast Startup on the computer, the agent will disable it. If you remove the trigger, the agent will not re-enable Fast Startup on the computer.

  When a computer has a Shut Down trigger, a message box appears on the computer when it starts to shut down or restart. The message box states that a backup is in progress and the system will shut down or restart after the backup is finished. The user then has the option to cancel the backup and shut down or restart the computer immediately. If the user does not cancel the backup, a "Shutting down" or "Restarting" message remains on the screen until the backup finishes and the computer shuts down or restarts. In rare cases (e.g., a seed backup), the computer might shut down before the backup is finished.

Note: If a user is connected to the computer using a remote connection, the user will not see a message box at shut down and will not be able to cancel the backup.

For each backup trigger, you can specify whether there should be at least 12 hours or 24 hours between triggered backups and specify a retention type for the resulting backups.

Triggered backups run in addition to scheduled and ad hoc backups for a computer. However:

- If a backup is triggered when a scheduled or ad hoc backup is running for the backup job, the triggered backup does not start. If the trigger is a Shut Down trigger, the computer shuts down or restarts after the scheduled or ad hoc backup finishes.
- If a scheduled or ad hoc backup starts while a triggered backup is running for the backup job, the incoming backup is queued or, if started by an intra-daily schedule, skipped.
- If a backup is triggered when a computer shuts down, and a scheduled or ad hoc backup for another backup job on the computer is already running, the computer might shut down before the scheduled or ad hoc backup is finished.

Backups cannot be triggered on computers with Windows Server operating systems.

To trigger a backup when an event occurs on a Windows desktop computer:

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

   IMPORTANT: Do not try to create a trigger on a computer that already has a backup trigger for a job; you will not be able to save your changes. Only one backup job on a computer can have a backup trigger.
2. In the View/Add Schedule dialog box, click **Windows Event Backup Triggers**.

   If a Windows Event Backup Triggers section does not appear in the dialog box or trigger options are disabled, you cannot create a trigger for the backup job. This can occur if the Windows Agent version does not support triggers or if the computer has a Windows Server operating system.
3. In the Windows Event Backup Triggers area, select the **Run backup on Windows Event** option.
4. In the **Event** list, do one of the following:
   - To run the backup job when a user logs on to the computer, click **Log On**.
   - To run the backup job when the computer starts to shut down, click **Shut Down**.

     Note: When you create a shut down trigger for a backup job on a computer, the agent disables Fast Startup on the computer. If you re-enable Fast Startup on the computer, the agent will

disable it. If you remove the trigger from the backup job, the agent will not re-enable Fast Startup on the computer.

5. In the **Retention** 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. See Add retention types.

   The 24-Hours and 48-Hours retention types are only available for intra-daily schedules. See Schedule a backup to run multiple times per day.

6. In the **Between triggered backups, wait at least** *x* **hours** list, do one of the following:

   - To wait at least 24 hours after a triggered backup on the computer before triggering another backup, click **24**.
   - To wait at least 12 hours after a triggered backup on the computer before triggering another backup, click **12**.

   The number of hours applies to any triggered backups on the computer. If you remove a trigger from one backup job and add a trigger to another backup job on the computer, the next triggered backup will not start until after the specified number of hours.

7. Click **Save**.

   If an error message states that another backup job on the computer has a Windows Event trigger, click **OK**. You cannot save the new trigger or any other changes that you made in the View/Add Schedule dialog box. Before you can create a trigger for this backup job, you must remove the trigger from the other backup job on the computer.

7.6 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.

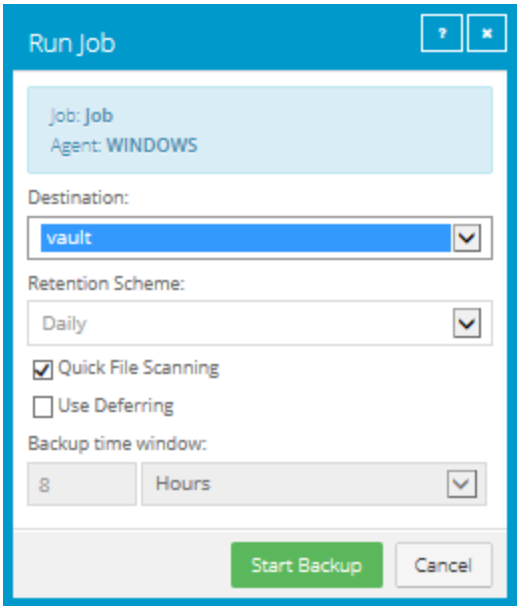
2. Find the computer with the backup job that you want to run, and expand its view by clicking the computer row.

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. To back up the data to the vault specified in the job, do not change the **Destination.**

   To back up the data to SSI (safeset image) files on disk, select **Directory on Disk** from the **Destination** list. Click the **Browse** button. In the Select Folder dialog box, choose the location where you want to save the SSI files, and click **Okay**.

   SSI files are full backups saved to disk instead of to a vault. Saving backup files on physical media and transporting them to a remote vault for importing can be quicker than backing up data directly to a vault in a remote datacenter.

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

6. 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.

7. If you are backing up a SQL Server database using the SQL Server Plug-in, 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.

     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), be sure that only one tool is being used for truncating logs.

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

8. If you are backing up volumes with SQL Server database files using the Image Plug-in, do one of the following:
   - To truncate database transaction logs after the backup, select **Truncate transaction logs**.
   - To run the backup without truncating logs, clear **Truncate transaction logs.**

   If you also back up databases with another tool (e.g., native SQL Server backup), use only one tool for truncating logs.
9. If you are backing up an Exchange database, do the following:
   - In the **Backup Type** list, do one of the following:
     - To only back up transaction logs and the checkpoint file after the first "seed" backup, click **Incremental**.
     - To back up the database files, checkpoint file and transaction logs, click **Full**.

       For more information, see Plan Full and Incremental Exchange backups.
   - To validate Exchange data during the backup, select **Validate Exchange database**.
10. 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.
11. 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: Incremental backups for Exchange cannot be deferred, even if deferring is enabled. Deferring can be applied to full backups for Exchange.
12. 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.
13. If you want to stop the backup, click **Stop**.
14. To close the Process Details dialog box, click **Close**.

7.7 Plan Full and Incremental Exchange backups

When you run or schedule an Exchange database backup job, you can specify whether to run a Full or Incremental backup. In a Full backup, the database files, checkpoint file and transaction logs are backed up. In an Incremental backup, only the transaction logs and checkpoint file are backed up after the first "seed" backup.

An Incremental backup takes less time to run than a Full backup. However, the time required to recover an Exchange database increases with the number of consecutive Incremental backups. To reduce the amount of time required for a recovery, we recommend performing a Full backup periodically. For example, you could schedule an Exchange backup job to run frequently with the Incremental backup type and periodically (e.g., once per week) with the Full backup type. As shown in the following table, the appropriate backup schedule can also depend on the Exchange database size and traffic.

Exchange database description	Sample backup schedule
Low traffic – approximately 250 users, 4 GB of data, 250 MB of daily data traffic	Full backup every second Saturday night; Incremental backup on other nights
Medium traffic – approximately 1000 users, 16 GB of data, 1 GB of daily data traffic	Full backup every Saturday night; Incremental backup on other nights
High traffic – approximately 4000 users, 64 GB of data, 4 GB of daily data traffic	Full backup every Wednesday and Saturday night; Incremental backup on other nights
High traffic – approximately 4000 users, 64 GB of data, 4 GB of daily data traffic, insufficient bandwidth for large backups during the week	Full backup every Saturday night (which could be deferred to Sunday, if required); Incremental backup on other nights

You should always perform a Full backup after database repair, defragmentation or recovery. These processes significantly change Exchange databases.

Exchange maintenance can affect how much data is transferred during a Full backup. If you run daily maintenance on your Exchange server, the database will change considerably each day. When performing a Full backup, these changes are incorporated into the safeset and will result in longer Full backup times.

When scheduling backup jobs, consider the maintenance window. Backup jobs have priority over mailbox database maintenance. If a backup job runs at the same time as maintenance processes, maintenance will be put on hold until the backup is finished. A maintenance window usually provides enough time for maintenance processes to finish after an Incremental backup, but a Full backup could prevent maintenance processes from running.

7.8 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 re-registered computers. You must also enter the encryption passwords for the computer's existing backup jobs.
- Before running existing backup jobs on computers that were restored using the System Restore application.
- 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**.

8 Resolve certificate failures and potential threats

Beginning in version 8.90, Windows agents can check vault TLS certificates when they try to connect to vaults. If an agent reports a certificate failure, you must investigate and resolve the certificate failure before backups and restores can continue. See Resolve certificate failures.

Beginning in version 9.00, the Windows agent can check for potential ransomware threats when running Local System jobs. If a Windows agent detects a potential threat, you must investigate and resolve the potential threat. See Manage potential ransomware threats.

8.1 Resolve certificate failures

If an agent reports a certificate failure, you must resolve the failure before backups and restores can continue. Certificate failures are summarized in the Current Snapshot on the Dashboard and shown on the Computers page in Portal. See Monitor backups and computers using the Current Snapshot and View computer and job status information. Agents can report certificate failures if they support certificate pinning, a security feature that is designed to ensure that agents are connecting to legitimate vaults.

A certificate failure can occur when a Windows agent tries to connect to a vault where the certificate pinning feature is enabled. Beginning with Windows Agent 8.90, when a Windows agent tries to connect to the vault (e.g., to run a backup or restore), it checks whether the public key of the vault's TLS certificate is the same as when the agent previously connected to the vault. If the public key of the vault certificate is different, the agent reports a certificate verification failure and will not connect to the vault.

Note: The certificate pinning security feature can be enabled in Director version 8.60 or later vaults.

If a certificate failure is reported, please contact your IT security staff or service provider to determine whether the certificate change was expected or whether further investigation is required.

If the certificate change was expected, follow the steps below to re-pin the certificate. When you re-pin a certificate, the agent securely records the new public key of the certificate.

To resolve certificate failures:

1. On the navigation bar, click **Computers**. The Computers page shows registered computers.
2. Select the check box for each computer with a certificate failure that you want to resolve.

   Note: Only select computers that have the Certificate failure status, or the Re-pin certificate action will not be available.
3. In the **Actions** list, click **Re-pin certificate**.
4. In the confirmation dialog box, click **Yes**.
5. In the Success message box, click **Okay**.

8.2 Manage potential ransomware threats

Beginning with Windows Agent 9.00 and Portal 8.90, you can enable threat detection when you create or edit a Local System backup job. When this option is enabled, the agent checks for potential ransomware

threats when running the backup job. See Add a Windows backup job.

Note: The agent does not check for potential ransomware threats in a seed backup or the first backup when threat detection is enabled in a job.

If an agent detects a potential ransomware threat, the job or backup is flagged in Portal. Potential threats are flagged:

- In the Current Snapshot on the Dashboard. See Monitor backups and computers using the Current Snapshot.
- On the Computers and Monitor pages. See View computer and job status information and View, export and email backup statuses on the Monitor page.
- In the Daily Status report.
- In email notifications to Admin users, if email notifications are configured centrally in a Portal instance. See Set up email notifications for potential ransomware threats.
- When you restore data or delete specific backups from a Local System backup job. See Restore Windows files and folders and Delete specific backups from vaults.

If a server has a potential threat, the Windows agent does not scan the server again during backups until the potential threat warning is cleared for the job.

When a potential threat is detected on a Windows server, you can sign in to the server in your environment and investigate whether it is infected with ransomware. An Admin user in Portal can then manage the threat:

- If the server is not infected or the ransomware threat has been addressed, an Admin user can clear the potential threat warning from the job.
- If the server is infected with ransomware, an Admin user can restore from a backup (also known as safeset) created before the attack. Backups with potential threats are identified in the Restore dialog box so you can choose a backup with no potential threat. After the restore, backups with potential ransomware threats remain in the vault and available for restore. To remove these backups (safesets), delete them from the vault and synchronize the job. See Delete specific backups from vaults and Synchronize a job. An Admin user can then clear the potential threat flag from the job.

To manage a potential ransomware threat:

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

   The Computers page shows registered computers.

2. Find the computer or environment with the potential threat, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. Find the job with the potential threat, and click **Manage Potential Threat** in its **Select Action** menu.

Note: The Manage Potential Threat option does not appear for a job that is restored from another computer. To manage a potential threat for a job, you must find the job on the original computer, if it exists, or re-register a new computer to the vault as the original computer. See Restore data to a replacement computer.

5. In the Manage Potential Threat box, do one of the following:
   - To restore from a backup before the potential ransomware threat was detected, select **Recover** and then click **Continue**. In the Restore dialog box, a calendar with a list of backups appears. "Potential Threat" appears beside any backup where a potential ransomware threat was detected. Select the backup (also known as safeset) from which you want to restore files, select restore options, and then click **Run Restore**. See Restore Windows files and folders.
   - *Note:* After a restore, backups with potential ransomware threats remain in the vault and available for restore. To remove these backups, delete them from the vault and synchronize the job. See Delete specific backups from vaults and Synchronize a job. An Admin user can clear the potential threat flag from the job.
   - If you investigated or addressed the potential threat and are sure that the server is not affected by ransomware, select **Clear Potential Threat Warning** and then click **Continue**. In the warning dialog box, click **Continue** to remove the potential threat flag from the job and all of its backups (safesets).

     Note: Clearing potential threat warnings will clear all existing threat warnings from the job and its backups (safesets). However, warning information will still be available in the log files.

9 Restore Windows data

After backing up Windows servers, you can:

- Restore Windows files and folders
- Restore files from multiple UNC jobs
- Restore Windows volumes from an Image backup
- Restore files and folders from an Image backup
- Recover a Windows cluster

You can also use the System Restore application to restore an entire system from a Bare Metal Restore (BMR) backup. A BMR backup includes the operating system, applications, system state and data. For more information, see Add a Windows backup job and the *System Restore Guide*.

Note: Although a BMR backup includes a computer's system state, you can only restore the system state from a BMR backup when you restore the entire computer using the System Restore application.

After backing up a Windows application or database, you can:

- Restore Exchange databases
- Restore Exchange mailboxes, messages and other objects
- Restore SQL Server databases
- Restore items from a SQL Server or SharePoint database
- Restore Oracle databases

To restore some or all of a computer's backed up data to another computer without replacing the original computer, see Restore data from another computer.

To register a new computer with the vault as if it were the old computer (i.e., re-register), see Restore data to a replacement computer. Re-registering a computer can be useful if you are replacing a system and want to migrate all data to a new computer (e.g., at the end of a lease or if hardware is failing).

9.1 Restore Windows files and folders

After backing up data from a Windows computer, you can restore files and folders from the backup.

To restore Windows files and folders:

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

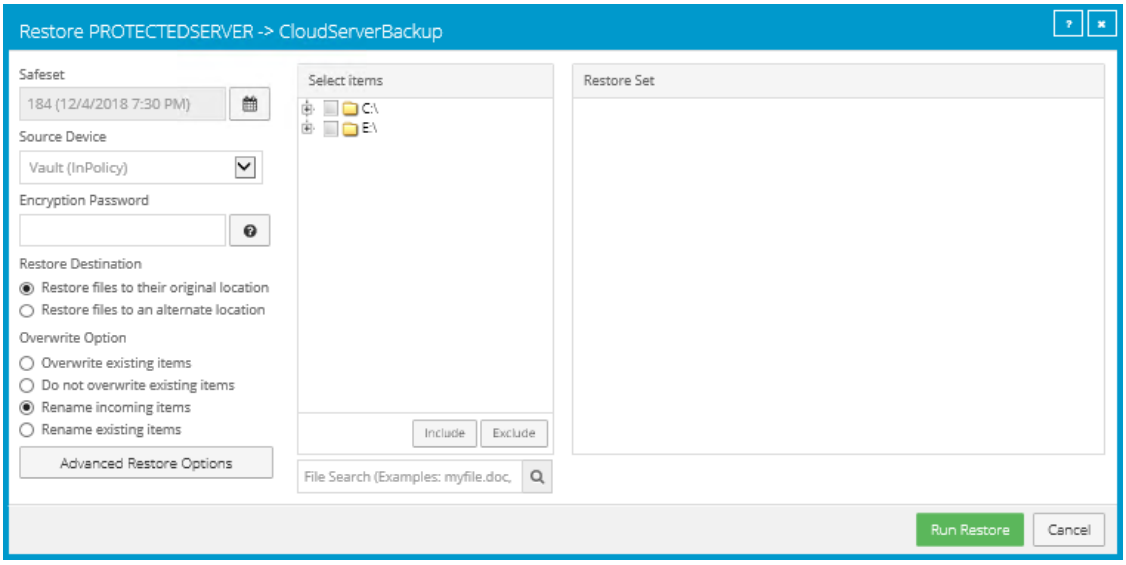
   A grid lists available computers.

2. Find the Windows computer with data that you want to restore, and expand its view by clicking the computer row.

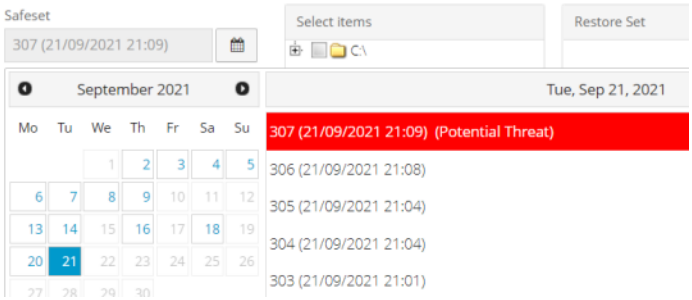
3. Click the Jobs tab.

4. Find the job with data that you want to restore, and click **Restore** in the job's **Select Action** menu.

   The Restore dialog box appears. If the job does not have a potential ransomware threat, the most recent safeset for the job appears in the Safeset box.



   If a potential ransomware threat was detected when running the job, a calendar with a list of backups appears. Any backup with a potential ransomware threat is highlighted in red and includes the words "Potential Threat" after the backup number and time.



5. 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, if a calendar with a list of backups does not already appear, click the calendar button. In the calendar, 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 **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 
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 an Overwrite Option. This option specifies how to restore a file, folder or symbolic link to a location where there is a file, folder or symbolic link with the same name.
   - To overwrite the existing item with the restored item, select **Overwrite existing items**.

     Note: If you try to restore multiple files with the same name to an alternate location and select **Overwrite existing items**, only the last file restored will remain. Other files with the same name will be overwritten.

     IMPORTANT: Using Agent version 8.70 or later, if you select **Overwrite existing items** and restore a file that has the same name as a folder in the restore location, the file will overwrite the folder. The folder and all of its contents will be removed.
   - To skip restoring the item that has the same name as an item in the destination location, select **Do not overwrite existing items**.
   - To add a numeric extension (e.g., .0001) to the **restored** item name, select **Rename incoming items**. 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 the **existing** item name, select **Rename existing items**. 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 is “filename.txt”.
9. To change the locked file, data streams, log detail level or bandwidth options, click **Advanced Restore Options**. Specify settings in the Advanced Restore Options dialog box, and click **Okay**. See Advanced restore options.

10. In the **Select Items** box, do one or more of the following until the **Restore Set** box shows the folders and files that you want to restore:
    - Select the check box for each folder and file that you want to restore, and then click **Include**. The **Restore Set** box shows the included folders and files. If you include a folder, all of the folder's subdirectories and files are restored by default. If you do not want to restore all of the subdirectories and files, you can add filters. See Filter subdirectories and files when restoring data.
    - To exclude one or more folders or files from the restore, select the check box for each folder or file, and then click **Exclude**. The **Restore Set** box shows the excluded folders and files. If you exclude a folder, all of the folder's subdirectories and files are excluded from the restore by default. If you do not want to exclude all of the subdirectories and files, you can add filters. See Filter subdirectories and files when restoring data.
    - To search for files to restore or exclude from the restore, click the **Search** button. In the **Search for files** box, enter search criteria and select files. See Search for files to restore. Click **Include Selected** or **Exclude Selected**. The Restore Set box shows the included or excluded files.
    - To remove an inclusion or exclusion record from the **Restore Set** box, click the Delete button beside the folder or file record.
11. 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.
12. To close the Process Details dialog box, click **Close**. If the restore is running, it will continue to run.

9.1.1 Restore NTFS hard links, symbolic links, mount points and junctions

When you restore files to their original locations and overwrite existing files, NTFS hard links, symbolic links, mount points and junctions are preserved. If you restore files to alternate locations or do not overwrite existing files, the links break.

Note: Remote hard links and mount points (e.g., UNC paths) are not supported.

When you restore junctions to their original locations, all link functionality is preserved. If you restore to an alternate location, the junction will revert to an empty directory. To recover to an alternate location, the junction must be explicitly selected for backup and will duplicate the contents of its target directory without preserving junction functionality.

Note: Remote/alternate junctions are not supported.

9.1.2 Restore a domain controller

You can restore a domain controller if the system was fully backed up using system state and system volume backups, or a Bare Metal Restore (BMR) backup. You can also restore a domain controller from a

Bare Metal Restore (BMR) backup using the System Restore application.

Note: A Windows Agent or BMR backup is not sufficient for an authoritative restore of Active Directory objects. For an authoritative restore, a System State backup with the Windows Agent is required. For more information, see Best-Practices-Backing-up-Domain-Controllers-or-Active-Directory.

When you have more than one domain controller, you must decide whether to perform an authoritative or non-authoritative restore before restarting the machine. For more information, see documentation from Microsoft.

9.2 Restore Windows volumes from an Image backup

After backing up volumes on a Windows computer using the Image Plug-in, you can restore volumes from the backup to selected live volumes (target volumes).

IMPORTANT: When you restore a volume from a backup, any data on the target volume will be lost.

A target volume must meet the following requirements:

- The target volume must be as large as or larger than the volume that was backed up.
- The Windows operating system cannot be installed on the target volume.
- The Windows Agent cannot be installed on the target volume.

To restore Windows volumes from an Image backup:

IMPORTANT: Before restoring volumes from an Image backup, stop any services on the system that are using the target volume (e.g., SQL Server or Exchange services). Restart the services after the restore is completed.

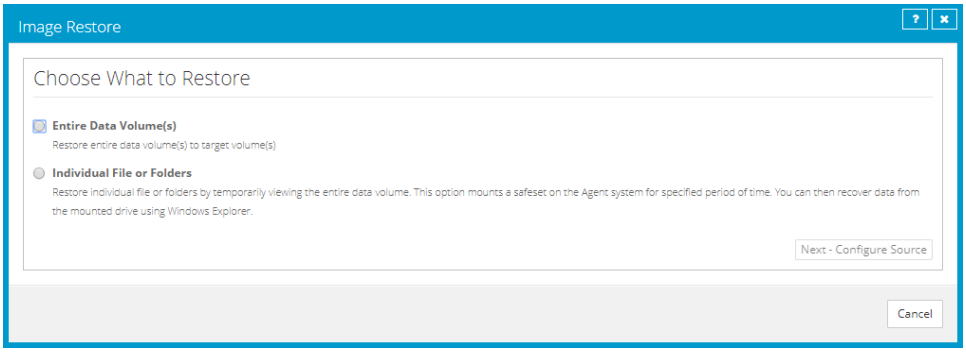
1. On the navigation bar, click **Computers**.

   A grid lists available computers.

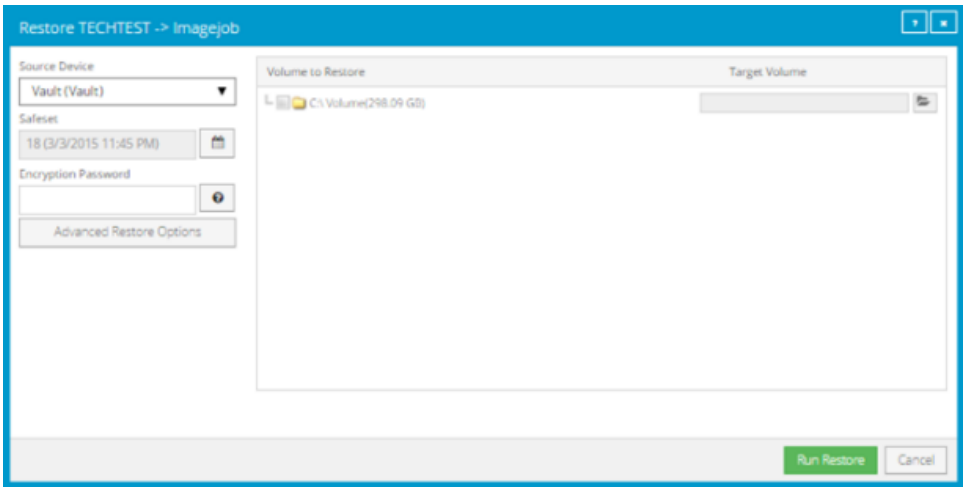
2. Find the Windows computer with the Image Plug-in, and expand its view by clicking the computer row.
3. Click the **Jobs** tab.
4. Find the Image backup job with volumes that you want to restore, and click **Restore** in the job's **Select Action** menu.

   You can restore volumes from regular or Bare Metal Restore backups created using the Image Plug-in.

5. In the Image Restore dialog box, select **Entire Data Volume(s)**, and then click **Continue**.



The Restore dialog box shows volumes that can be restored from the backup. The most recent safeset for the job appears in the **Safeset** box.



6. 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.

7. In the **Encryption Password** box, enter the encryption password. To view the password hint, click the **Hint** button.
8. To change the log detail level or bandwidth options, click **Advanced Restore Options**. Specify settings in the Advanced Restore Options dialog box, and click **Okay**. See Advanced restore options.
9. In the **Volume to Restore** column, select each volume that you want to restore.
10. For each selected volume, do the following to choose the live volume where it will be restored:

    IMPORTANT: Data on the selected volume will be lost when the backed-up volume is restored.

    a. Click the folder button.

       The Select Volume dialog box lists all live volumes on the computer. If you cannot restore the selected volume to a specific live volume (e.g., because the live volume is too small, contains the Windows operating system, or contains Windows Agent software), the volume is unavailable and cannot be clicked.

    b. Click the volume where you want to restore the backed up volume.

    c. Click **Okay**.
11. Click **Run Restore**.

    The Process Details dialog box shows the restore progress and indicates when the restore is completed. The target volume goes offline until the backed-up volume is restored.

    Other recent job processes might also be listed in the dialog box. See View current process information for a job.
12. To close the Process Details dialog box, click **Close**. If the restore is running, it will continue to run.

9.3 Restore files and folders from an Image backup

After backing up volumes from a Windows server using the Image Plug-in, you can restore individual files and folders from the backup.

To restore files and folders from an Image backup, you mount volumes from a safeset as drives on the computer where you want to restore files and folders. You can then browse the drives using Windows Explorer, and copy files and folders that you want to restore.

Note: To restore files and folders from Image backups, agent services must be running using the local system account. If the local system account did not have full permission to the files and folders during backup, you might not have permission to access files and folders during the restore. In this case, you can either:

- Restore the whole volume and grant appropriate permissions.
- Restore on a computer in the same domain using a domain account that has appropriate permissions.

Note: When SQL Server databases are backed up using Image Plug-in version 7.5 or later, you can also restore database files, tables and objects from the application-consistent backups.

To restore files and folders from an Image backup:

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

   A grid lists available computers.

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

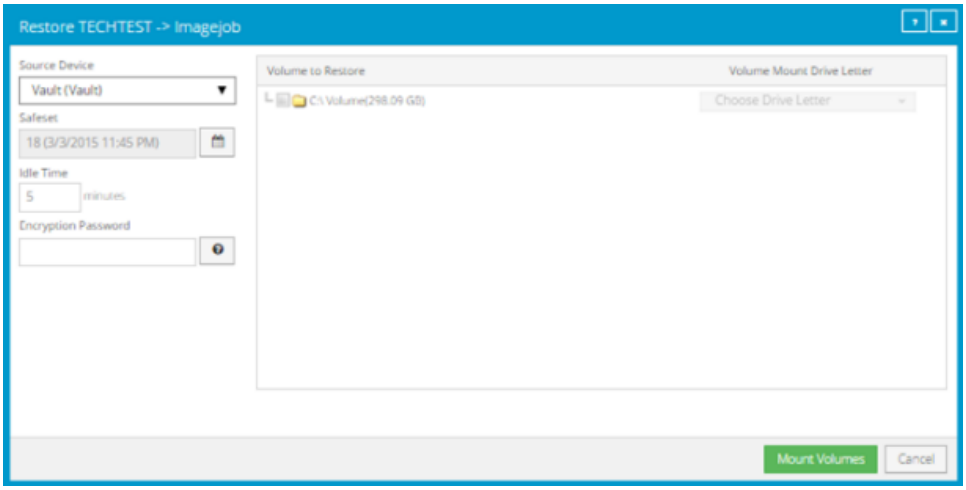
3. Click the **Jobs** tab.

4. Find the Image backup job with files and folders to restore, and click **Restore** in the job's **Select Action** menu.

   You can restore files and folders from any Image Plug-in job.

5. In the Image Restore dialog box, select **Individual File or Folders**, and then click **Next - Configure Source**.

   The Restore dialog box shows volumes that you can mount as drives. The most recent safeset for the job appears in the **Safeset** box.



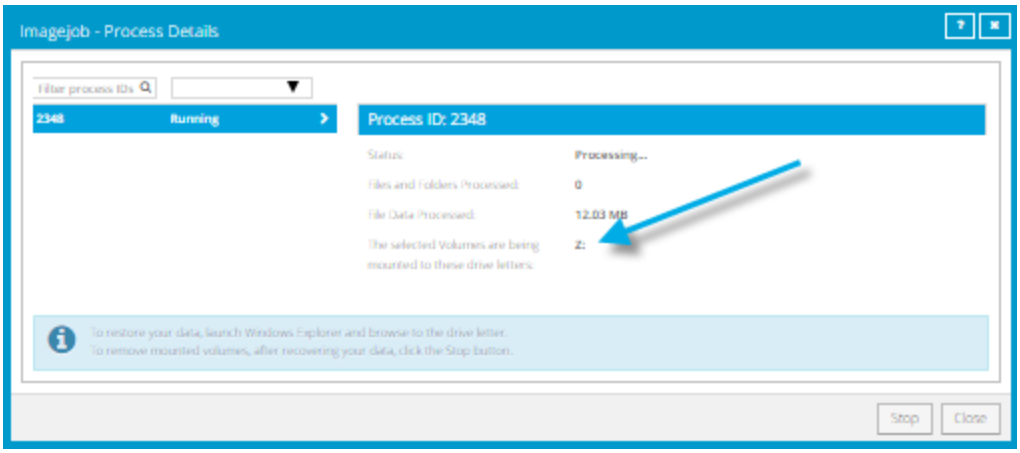
6. To restore data from an older safeset, click the calendar button. In the calendar that appears, click the date of the safeset from which you want to restore. To the right of the calendar, click the specific safeset that you want to use.

7. In the **Idle Time** box, enter the number of minutes of inactivity after which the shared drive will be unmounted automatically. The **Idle Time** can range from 2 to 180 minutes.

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

9. In the **Volume to Restore** column, select each backed-up volume from which you want to restore files and folders.
10. In the **Volume Mount Drive Letter** column, choose the drive letter for mounting each volume.
11. Click **Mount Volumes**.
12. 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.



13. Use Windows Explorer to navigate to the drive or drives and copy files and folders that you want to restore.
14. When you are done restoring files and folders, 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 7.

9.4 Restore files from multiple UNC jobs

When a Windows computer has more than one UNC backup job, you can search for and restore files from multiple UNC jobs at the same time. This functionality is available for computers where Windows Agent version 8.0 or later is installed.

You can restore files from UNC jobs to a local folder or to a UNC share. When you restore files to a UNC share, files are only restored from UNC jobs with credentials that have access to the share. If required, you can change the credentials in a UNC backup job until you have restored the files.

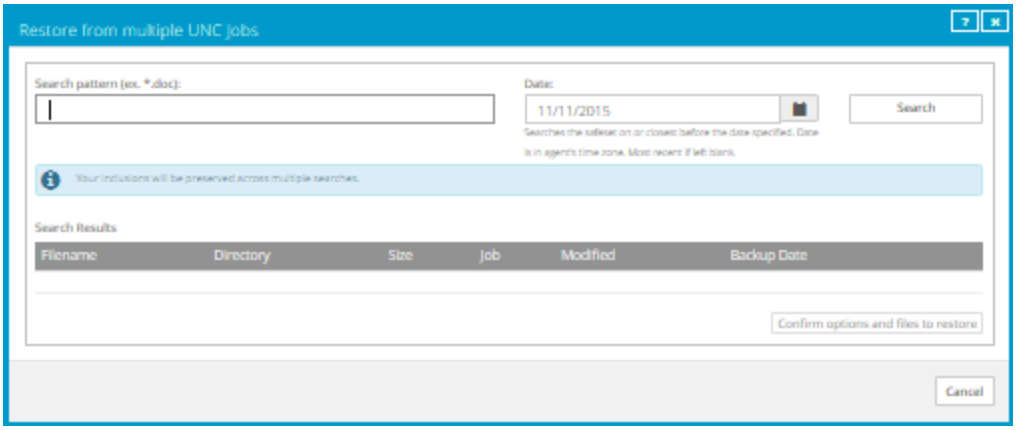
To restore files from multiple UNC jobs:

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

   A grid lists available computers.
2. Find a Windows computer with multiple UNC jobs, and expand its view by clicking the computer row.

3. In the **Select Job Task** menu, click **Restore from multiple UNC jobs**.

   The Restore from multiple UNC jobs dialog box appears.

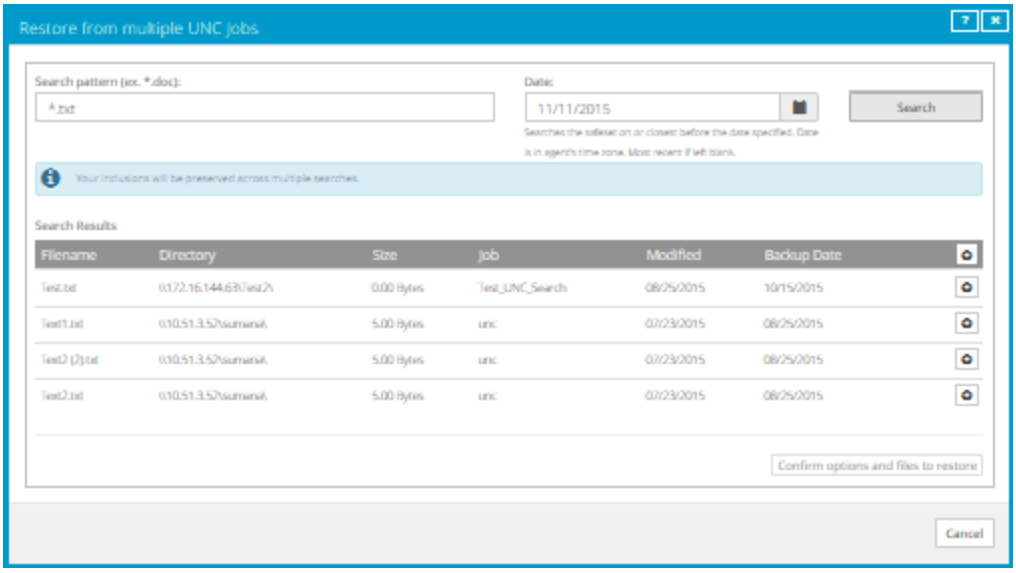


4. In the **Search Text** field, enter some or all of the name of a file that you want to restore. Use asterisks (*) and question marks (?) as wildcard characters. For example, to find all files with the .pdf extension, enter the following: *.pdf
5. Do one of the following:
   - To search for files in the most recent safeset for each UNC job, leave the **Date** box blank.
   - To search for files in safesets with a specific date, click the calendar button. In the calendar that appears, click the date.

     If a job does not have a safeset for the specified date, the system searches for files in the safeset with the date that is closest to and before the specified date.

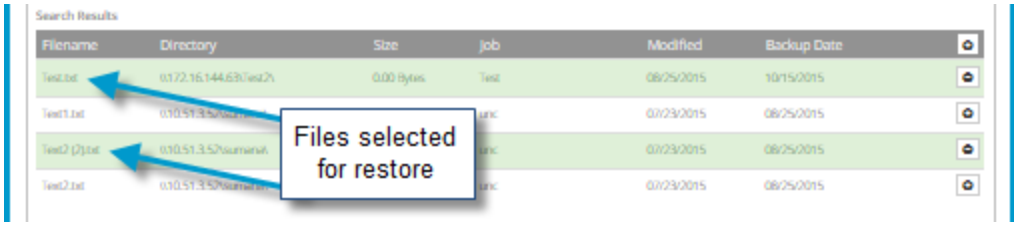
     If a job includes multiple safesets for the specified date, the system searches for files in the last safeset on the date.
6. Click **Search**.

   Files found in the safesets are listed in the lower part of the dialog box.



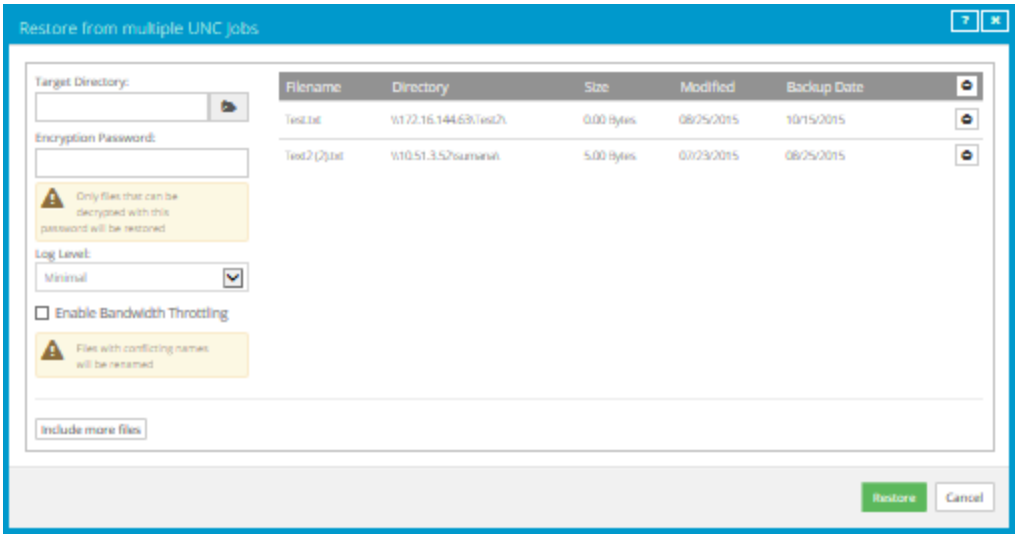
7. Do one of the following:
   - To restore specific files, click the **Include for restore** button for each file.
   - To restore all files in the list, click the **Include All** button at the top of the file list.

   After a file is selected for restore, the file is highlighted in the list.



8. To search for more files to restore, repeat Steps 4 to 7.
9. To view all files that are selected for restore, click **Confirm options and files to restore**.

   The Restore from multiple UNC jobs dialog box shows files that are selected for restore.



10. To select more files to restore, click **Include more files**. The Restore from multiple UNC jobs dialog box returns. Repeat Steps 4 to 9.
11. To restore the selected files, do the following:
    a. In the **Target Directory** box, do one of the following:
        - To select a local folder as the restore destination, click the **Browse** button. In the Select Folder dialog box, choose the folder and then click **Okay**.
        - To specify a local folder or UNC share as the restore destination, type the name of the folder or UNC share (e.g., \\server\share) where you want to restore files.

          If the destination is a UNC share, files will only be restored from jobs with credentials that have access to the share. If required, you can change credentials in a UNC backup job until you have restored the files.

          If the restore destination folder does not exist, it will be created during the restore.

    b. In the **Encryption Password** box, enter the encryption password.

       If you are restoring files from UNC jobs with different encryption passwords, files will only be restored from jobs with the password specified in this box.

    c. In the **Log Level** list, click the level of detail for logging. See Advanced restore options.

    d. To restrict the amount of bandwidth used, select the **Enable Bandwidth Throttling** check box. See Advanced restore options.

    e. Click **Restore**.

       The selected files are restored. If you restore a file with the same name as another file in the same location, a numeric extension (e.g., .0001) is added to the restored file name (e.g., filename.txt.0001).

9.5 Recover a Windows cluster

When a Windows cluster is protected as described in Add backup jobs for a Windows cluster, you can recover the cluster if components are lost, are corrupted or fail. The following table indicates how to recover a cluster after encountering specific issues.

Issue	Recovery Process	Jobs Used
Cluster disk data loss, corruption or failure	Restore volumes on the cluster disk. If the cluster disk failed or was corrupted, clean partition and volume formatting from the disk before restoring the data. See Recover volumes in a Windows cluster.	On the virtual server for each cluster role (e.g., file server or SQL Server role), an Image or local system job that backs up cluster disks for the role. See Job C in Add backup jobs for a Windows cluster.
Cluster quorum corruption, checkpoint loss, failure or rollback required	Create a new quorum disk. See Recover the quorum disk in a Windows cluster.	On the virtual server for the cluster core, an Image or local system job that backs up the quorum disk. See Job A in Add backup jobs for a Windows cluster.
Cluster node corruption or failure	Recover the cluster node using the System Restore application. See Recover a node in a Windows cluster.	On the cluster node, a Bare Metal Restore (BMR) backup job created using the Image Plug-in or Windows Agent. See Job B in Add backup jobs for a Windows cluster.
Complete cluster failure	Recover all components of the cluster. See Recover an entire Windows cluster.	Jobs B, A and C in Add backup jobs for a Windows cluster. In addition, for a SQL Server cluster, a SQL Server Plug-in job is required for point-in-time database recovery. The job is created on the virtual server for the SQL Server role. See Job D in Add backup jobs for a Windows cluster.

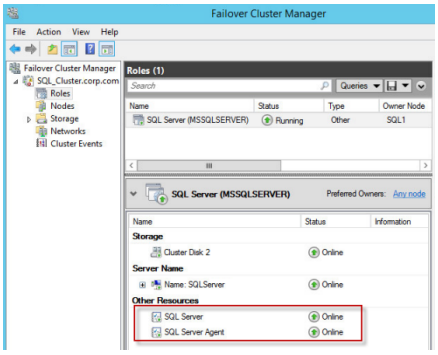
9.5.1 Recover volumes in a Windows cluster

If data has been lost from a cluster disk, or a cluster disk has become corrupted or failed, you can recover the cluster volumes.

Cluster volumes must be backed up using an Image or local system job on the virtual server for a cluster role (e.g., file server or SQL Server). See Job C in Add backup jobs for a Windows cluster.

To recover volumes in a Windows cluster:

1. If you are recovering volumes to a disk that became corrupted or failed, do the following:
    a. Remove the disk from the cluster.
    b. Clean partition and volume formatting from the disk using a tool such as diskpart.
    c. Add the disk back to the cluster.
2. Using the Failover Cluster Manager on any cluster node, stop the cluster resources. **Do not** stop the shared disk resource.



3. Using Portal, run a “Restore from another computer” on the cluster node where the disk is mounted. Restore the cluster volume or volumes from an Image or local system backup job on the virtual server for the SQL Server role (Job C in Add backup jobs for a Windows cluster). Restore volumes to their original locations.
4. Using the Failover Cluster Manager on any cluster node, start the SQL Server and SQL Server Agent cluster resources.
5. Using SQL Management Studio, ensure that the SQL Server database is running and operational.

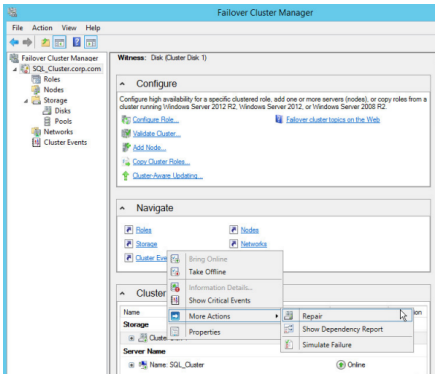
9.5.2 Recover the quorum disk in a Windows cluster

If the quorum disk in a Windows cluster is corrupted or fails, or if a rollback is required, you can create a new quorum disk and recover any required data.

Quorum disks are protected using an Image or local system job on the virtual server for the cluster core. See Job A in Add backup jobs for a Windows cluster.

To recover the quorum disk in a Windows cluster:

1. Connect a new disk to the cluster.
2. On one cluster node only, bring the disk online and initialize it. Partition the disk and assign the same drive letter that was previously assigned to the quorum disk.
3. In the Failover Cluster Manager on any cluster node, click the cluster name. Under **Cluster Core Resources**, right-click the quorum disk, click **More Actions** and then click **Repair**. Choose the newly formatted disk and click **OK**. Wait until the quorum disk is successfully repaired.



4. Bring the quorum disk online.
5. Ensure that the quorum disk is online and that there are no errors in the cluster logs.
6. If required, restore quorum data from the Image or local system job on the virtual server for the cluster core (Job A in Add backup jobs for a Windows cluster).

9.5.3 Recover a node in a Windows cluster

If a node in a Windows cluster is corrupted or fails, you can recover the node.

Each cluster node must be backed up using an Image or Windows Agent Bare Metal Restore (BMR) job on the node. See Job B in Add backup jobs for a Windows cluster.

To recover a node in a Windows cluster:

1. On a replacement machine that has similar hardware to the original cluster node, launch the System Restore application.

   For detailed procedures and information, see the *System Restore User Guide*.
2. Restore system volumes from a BMR backup of the original cluster node (Job B in Add backup jobs for a Windows cluster).
3. If required at the end of the restore, repair drivers on the system.
4. Reboot and then log in to the replacement node.
5. Configure network adaptors on the replacement node with the same network settings as the original node (i.e., same IP addresses and DNS entries).
6. If required, re-connect all cluster disks.
7. Open the Failover Cluster Manager and ensure that the restored node is up and running.
8. Fail over the SQL Server and SQL Server Agent cluster resources to the restored node to ensure that the restored node is functioning correctly.

9.5.4 Recover an entire Windows cluster

If all components of a Windows cluster fail and the cluster is protected as described in Add backup jobs for a Windows cluster, you can recover the cluster.

To recover an entire Windows cluster:

1. Recover one cluster node by doing the following:
    a. On a replacement machine that has similar hardware to one of the original cluster nodes, launch the System Restore application.

       For detailed procedures and information, see the *System Restore User Guide*.

    b. Restore system volumes from a BMR backup of the original cluster node (Job B in Add backup jobs for a Windows cluster).

    c. If required at the end of the restore, repair drivers on the system.

    d. Reboot and then log in to the replacement node.

    e. Configure network adaptors on the replacement node with the same network settings as the original node (i.e., same IP addresses and DNS entries).
2. On the restored cluster node, recreate the cluster disks. Format the disks and assign the original drive letters.
3. On the restored cluster node, stop the Cluster service. For a SQL Server cluster, also stop the SQL Server service.
4. If required, restore quorum data to its original location. Using Portal, run a "Restore from another computer" on the restored cluster node. Restore the quorum disk from an Image or local system backup job on the virtual server for the cluster core (Job A in Add backup jobs for a Windows cluster).
5. Restore cluster volumes to their original locations. Using Portal, run a "Restore from another computer" on the restored cluster node for each cluster role. Restore cluster volumes from an Image or local system backup job on the virtual server for each cluster role (Job C in Add backup jobs for a Windows cluster).
6. Start the cluster service.
7. Using the Failover Cluster Manager, connect to the cluster.
8. Start the cluster roles.
9. Repair the cluster disks and assign the original drive letters. Bring the cluster disks online.

   For more information about repairing cluster disks and bringing them online, see documentation from Microsoft.
10. For a SQL Server cluster, use Portal to run a "Restore from another computer" on the restored cluster node. Restore SQL Server databases from a SQL Server Plug-in job on the virtual server for the SQL Server role (Job D in Add backup jobs for a Windows cluster). Restore the databases to their original locations.

11. For each remaining cluster node, do the following:
    a. On a replacement machine that has similar hardware to the original cluster node, launch the System Restore application.

       For detailed procedures and information, see the *System Restore User Guide*.
    b. Restore system volumes from the BMR backup of the original cluster node (Job B in Add backup jobs for a Windows cluster).
    c. If required at the end of the restore, repair drivers on the system.
    d. Reboot the machine.
    e. Log in to the machine.
    f. Configure network adaptors with the same network settings as the original node (i.e., same IP addresses and DNS entries).
    g. If required, reconnect all cluster disks.

9.6 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, Restore SQL Server databases to files or Restore a SQL Server master database.

After backing up SQL Server databases using the Image Plug-in, you can restore database files from the safeset. See Restore SQL Server database files or objects from Image backups.

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.

9.6.1 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.

Note: If a database was backed up using the Image Plug-in, you must restore it using the Image Plug-in.

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.

     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.

      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 or bandwidth throttling setting, 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. See Advanced restore options.
    - Select or clear the **Use all available bandwidth** option. See Advanced restore options.
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.

9.6.2 Restore SQL Server databases to files

After backing up SQL Server databases using the SQL Server Plug-in, you can restore the databases to SQL database files (.mdf and .ldf files). You can then use SQL Server tools to attach the files to a SQL Server instance.

To restore a SQL Server database to 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.

     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 or bandwidth throttling setting, 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. See Advanced restore options.

- Select or clear the **Use all available bandwidth** option. See Advanced restore options.

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.

9.6.3 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 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.

9.6.4 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**.

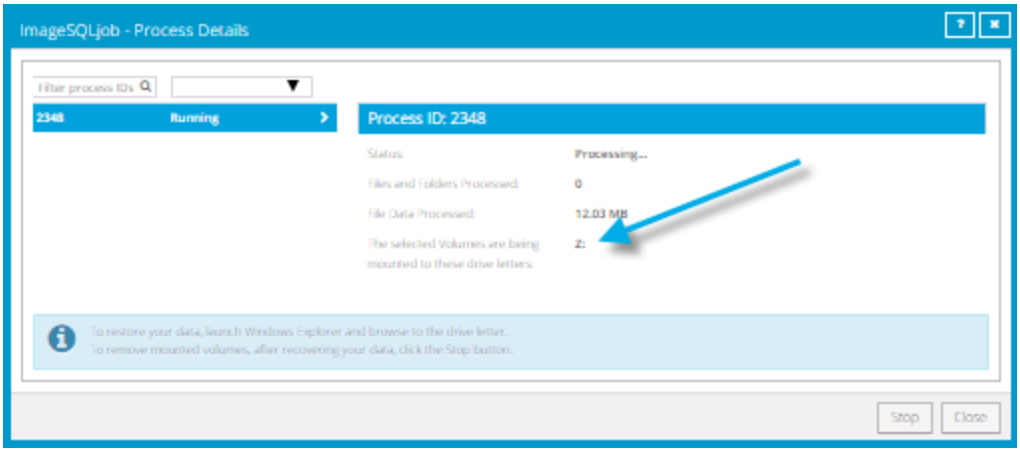
   A grid lists available computers.

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.

9.6.5 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.

9.7 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.

9.8 Restore Exchange databases

You can restore a Microsoft Exchange database to its original location or to an alternate Exchange database (e.g., a recovery database). To overwrite an existing database, the database must be unmounted and marked for overwrite.

When restoring an Exchange database, you can specify whether or not to replay transaction logs into the database and mount the database in Exchange. If this option is selected, the logs are rolled forward if they are in the original directory and no log files are missing or corrupt. If this option is not selected, transaction logs are restored to the system but are not replayed into the restored database. The Administrator must review the restored files and manually mount the database.

The process of restoring the database files to the system is recorded in the job logs. The process of replaying transaction logs into the database is recorded in the Windows Event Viewer.

For more information about Exchange restore strategies, see Exchange database restores and documentation from Microsoft.

To restore Exchange databases to flat files, see Restore Exchange databases to flat files.

To restore an Exchange database:

1. If you are restoring the database to its original location, delete all files (e.g., .edb, .log and .chk) in the folder where the original database files are located.

   Note: Do not delete the folder that has a GUID in its name (e.g., 523E7980-EA56-440-9ACB-AF0AE2CF1F0212…).

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

   A grid lists available computers.

3. Find the computer with the Exchange database you want to restore, and expand its view by clicking the computer row.
4. Click the **Jobs** tab.
5. Find the job whose Exchange database you want to restore, and click **Restore** in the **Select Action** menu for the job.
6. In the Choose What You Want to Restore dialog box, select **Exchange Databases**, and click **Okay**.

   The 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 **Items to Restore** box, select the check box for each database that you want to restore.
9. Select a Restore Destination option:

   - To restore data to the location where it was backed up, select **Restore files to their original location**.
   - To restore to an alternate Exchange database, select **Restore to an alternate Exchange database**. In the **Current Chosen Destination** box, click **Browse**. In the Select Folder dialog box, select the location where you want to restore, and click **Okay**.

10. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. 
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. See Advanced restore options.
    - Select or clear the **Use all available bandwidth** option. See Advanced restore options.
    - Select or clear the **Start Hard Recovery** option.

      If the **Start Hard Recovery** option is selected, transaction logs are replayed after the database is restored and the restored database is mounted by Exchange. Logs are also rolled forward if they are in the original directory and no log files are missing or corrupt.

      If the **Start Hard Recovery** option is not selected, transaction logs are restored to the system but are not replayed after the database is restored. The restored database is not mounted by Exchange. The Administrator must review the restored Exchange files and manually mount the database.

    Click **Okay**.
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.

9.8.1 Exchange database restores

You can only restore databases to the active copy in a Database Availability Group. If you restore to the replica copy, you will not be able to mount the database or make it active. You will need to copy the restored files to the active copy node in order to successfully mount (and take precedence over the other copies). You will also need to update each copy through the Exchange Management Console. For more information, see documentation from Microsoft.

If you are restoring to a new location and you want to mount the database, you must first create a recovery database through the Exchange Management Shell. For more information, see documentation from Microsoft.

To restore an Exchange database to an alternate location on a non-Exchange server, you must clear the **Start Hard Recovery** option.

If a database's transaction log files are missing or damaged, an incremental backup after the recovery will not succeed. Perform a full backup before you attempt another incremental backup.

9.8.2 Restore Exchange databases to flat files

On a computer where the Exchange Plug-in is installed, you can restore an Exchange database to flat files. The Eseutil utility can then be used to bring the data into a database.

To restore an Exchange database to flat files:

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

   A grid lists available computers.

2. Find the computer with the Exchange database 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 Exchange database that you want to restore, and click **Restore** in the **Select Action** menu for the job.
5. In the Choose What You Want to Restore dialog box, select **Restore to folder**, and click **Okay**.

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

6. 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.

     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.

7. In the **Files to Restore** box, select the check box for each database that you want to restore.
8. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the Hint button.
9. 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**.
10. To change the log detail level, bandwidth options 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. See Advanced restore options.
- Select or clear the **Use all available bandwidth** option. See Advanced restore options.
- Select or clear the **Start Hard Recovery** option.

  If the Start Hard Recovery option is selected, transaction logs are replayed after backup data is restored. The restored database is prepared for use by Exchange, and logs are rolled forward if they are in the original directory and no log files are missing or corrupt. These processes are recorded in the Windows Event viewer.

  If the Start Hard Recovery option is not selected, the database will not be available to Exchange after a restore. The Administrator must review the restored Exchange files and database and manually mount the database. For more information, see documentation from Microsoft.

Click **Okay**.

11. 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.

9.9 Restore Exchange mailboxes, messages and other objects

If a Microsoft Exchange database is backed up using the Exchange Plug-in, you can restore mailboxes, messages, and other objects from the backup.

To restore items from a Microsoft Exchange backup, you must first use Portal to expose the Exchange safeset as a shared resource. You can then use the Granular Restore for Microsoft Exchange and SQL application to find and restore mailboxes, messages and other Exchange objects.

For more information, or to obtain the Granular Restore for Microsoft Exchange and SQL application, contact your service provider.

To restore Exchange mailboxes, messages and other objects:

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

   A grid lists available computers.

2. Find the computer with Exchange objects that you want to restore, and expand its view by clicking the computer row.
3. Click the **Jobs** tab.
4. Find the job with Exchange objects (e.g., messages) that you want to restore, and click **Restore** in the **Select Action** menu for the job.

The Choose What You Want to Restore dialog box appears.

5. Select **Mailboxes, messages and other Exchange objects**, and click **Okay**.
6. In the Restore dialog box, choose a safeset from which to restore.
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.
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 to the safeset share is now available for you to paste into the Granular Restore application.
12. Launch the Granular Restore for Microsoft Exchange and SQL application. Paste the path to the Exchange safeset share into the Granular Restore application, and then select and restore your data. For more information, see the *Granular Restore for Microsoft Exchange and SQL User Guide.*
13. When you no longer need the safeset share, click **Stop**.

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

9.10 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.

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

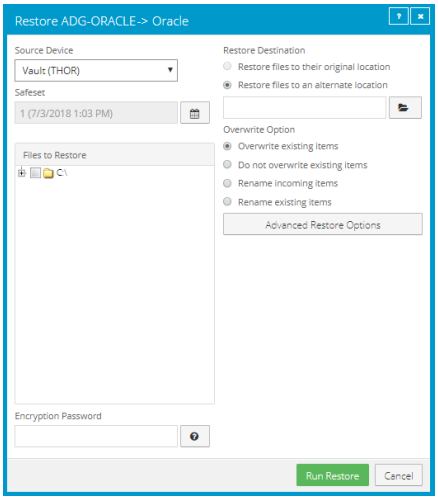
To restore an Oracle database:

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 an Overwrite Option. This option specifies how to restore an item (e.g., a file) to a location where there is an item with the same name.
   - To overwrite the existing item with the restored item, select **Overwrite existing items**.

     If you try to restore multiple files with the same name to an alternate location and select **Overwrite existing items**, only the last file restored will remain. Other files with the same name will be overwritten.

     IMPORTANT: Using Agent version 8.70 or later, if you select **Overwrite existing items** and restore a file that has the same name as a folder in the restore location, the file will overwrite the folder. The folder and all of its contents will be removed.
   - To skip restoring the item that has the same name as an item in the destination location, select **Do not overwrite existing items**.
   - To add a numeric extension (e.g., .0001) to the *restored* item name, select **Rename incoming items**. 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 the *existing* item name, select **Rename existing items**. 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 is “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.

9.11 Advanced restore options

When restoring data, you can specify the following options:

Locked File Options

When restoring data from a local job, you can specify whether to overwrite locked files with restored files with the same names. You can select one of the following options:

- **Yes, overwrite locked files** – Files on the system that are locked during the restore are overwritten by restored files when the system restarts. You must select this option for a system state or system volume restore.
- **No, do not overwrite locked files** – Files on the system that are locked during the restore are not overwritten by restored files with the same name.

Streams

When running a backup, information is collected from your files in various streams. Original data created by a user is called a data stream. Other information, such as security settings, data for other operating systems, file reference information and attributes, are stored in separate streams.

When restoring data, you can select one of the following options:

- **Restore all streams** – Restores all information streams. This option is recommended if you are restoring files to a system with an identical platform.
- **Restore data streams only** – For cross-platform restores, restores data streams only. This option ensures that conflicts do not arise as a result of system-specific information streams.

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.

Note: For Image Plug-in jobs, the selected logging level does not affect the content of the logs.

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 and restores. 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.

9.12 Filter subdirectories and files when restoring data

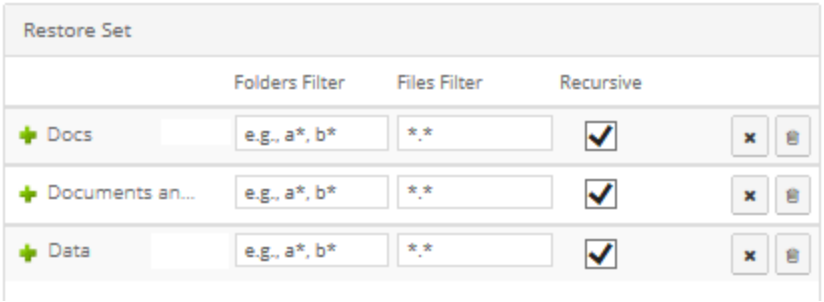
When you restore data, you can specify folders and files to restore or not restore from the backup.

By default, when you include a folder in a restore, the folder's subdirectories and files are also included. If you only want to restore some of a folder's subdirectories or files, you can add filters to the inclusion record. For example, you could add a filter so that files in a folder are only restored if they have the .doc or .docx extension.

By default, when you exclude a folder from a restore, the folder's subdirectories and files are also excluded. If you only want to exclude some of a folder's subdirectories or files, you can add filters to the exclusion record. For example, you could add a filter so that files in a folder are only excluded from the restore if they have the .exe extension.

To filter subdirectories and files when restoring data:

1. When restoring data, view the **Restore Set** box.



2. If editable fields do not appear for a folder inclusion or exclusion record where you want to filter subdirectories and fields, click the **Edit** button in the folder row.

3. In the **Restore Set** box, for each included folder where you want to include specific subdirectories or files, do one or more of the following:
   - To include specific subdirectories in the restore, in the **Folders Filter** field, enter the names of subdirectories to include. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only restore subdirectories if their names end with "-current" or start with "2015", enter the following filter: *-current, 2015*

     Note: Asterisks (*) are the only supported wildcards in filter fields.
   - To restore specific files, in the **Files Filter** field, enter the names of files to restore. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only restore files if they have the .doc or .docx extension, enter the following filter: *.doc, *.docx

     Note: Asterisks (*) are the only supported wildcards in filter fields.
   - To restore the specified folder, but not its subdirectories, clear the **Recursive** check box.
   - To restore the folder's subdirectories, select the **Recursive** check box.
4. In the **Restore Set** box, for each excluded folder where you want to exclude specific subdirectories or files, do one or more of the following:
   - To exclude specific subdirectories from the restore, in the **Folders Filter** field, enter the names of subdirectories to exclude. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only exclude subdirectories from a restore if their names end with "-old" or start with "2001", enter the following filter: *-old, 2001*

     Note: Asterisks (*) are the only supported wildcards in filter fields.
   - To exclude specific files from the restore, in the **Files Filter** field, enter the names of files to exclude. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to only exclude files from a restore if they have the .exe or .dll extension, enter the following filter: *.exe, *.dll

     Note: Asterisks (*) are the only supported wildcards in filter fields.
   - To exclude the specified folder, but not its subdirectories, clear the **Recursive** check box.
   - To exclude the folder's subdirectories, select the **Recursive** check box.
5. Click **Run Restore**.

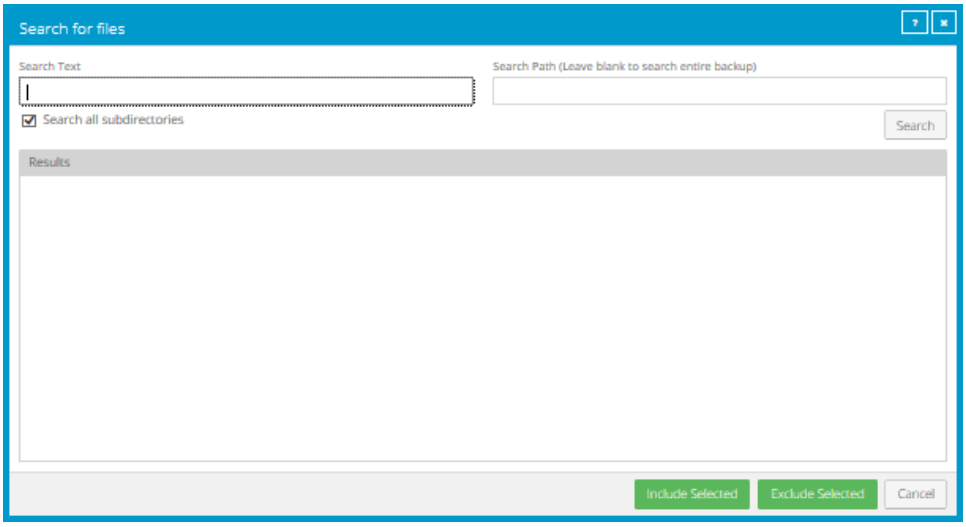
9.13 Search for files to restore

When you restore data, you can search for files to restore or exclude from the restore.

To search for files to restore:

1. In the Restore dialog box, click the **Search** button. 

   The Search for files dialog box appears.



2. In the **Search Text** box, enter the file name to search for. You can include asterisks (*) as wildcard characters.
3. To search for files in a specific folder in the backup, enter the path in the **Search Path** box.
4. To search for files only in the specified folder, clear the **Search all subdirectories** check box.
5. Click **Search**.

   The Results box lists files that match the search criteria.
6. In the **Results** box, select files to include or exclude. To select multiple consecutive items, press SHIFT while clicking the first and last items in the list. To select multiple items, press CTRL while clicking the items.
7. Do one of the following:
   - To restore the selected files, click **Include Selected**.
   - To exclude the selected files from the restore, click **Exclude Selected**.

9.14 Restore data to a replacement computer

If you are replacing a system and want to migrate all data to a new computer (e.g., at the end of a lease) or in a disaster recovery situation, you can re-register the new computer with the vault as the old computer, and restore data from the old computer's backups. If the old computer backed up data to multiple vaults, you can use Portal version 8.50 or later to re-register the new computer to multiple vaults.

After you re-register a computer with a vault, you must:

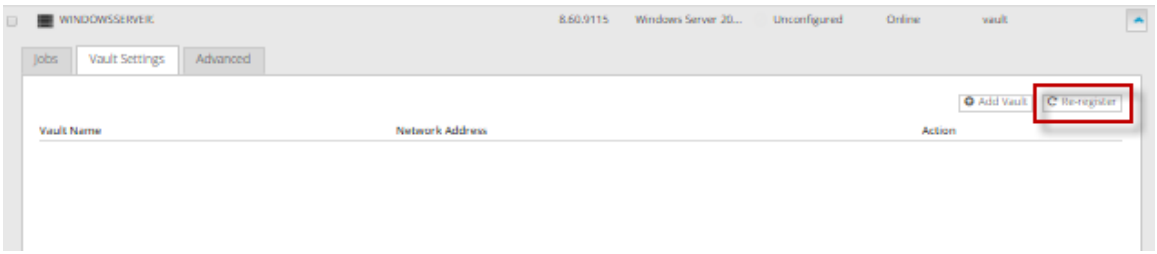
- Edit each existing backup job and enter the encryption password for the backup job.
- Synchronize the jobs before they run successfully. See Synchronize a job.

If you want to restore data to another computer without replacing the existing computer, you can restore data from another computer. See Restore data from another computer.

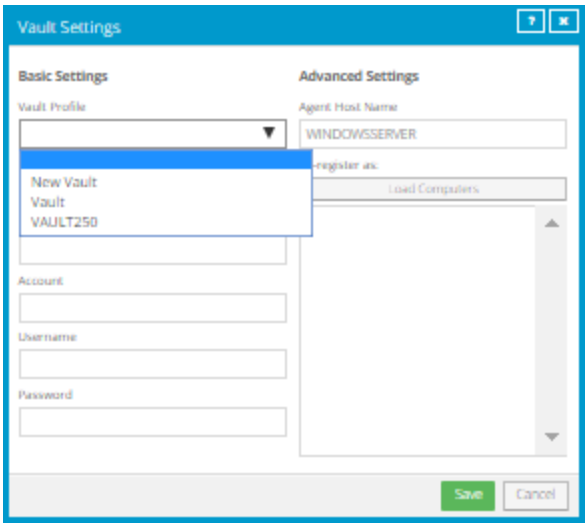
To restore data to a replacement computer:

1. Download and install an agent on the new or rebuilt computer.
2. On the navigation bar, click **Computers**.

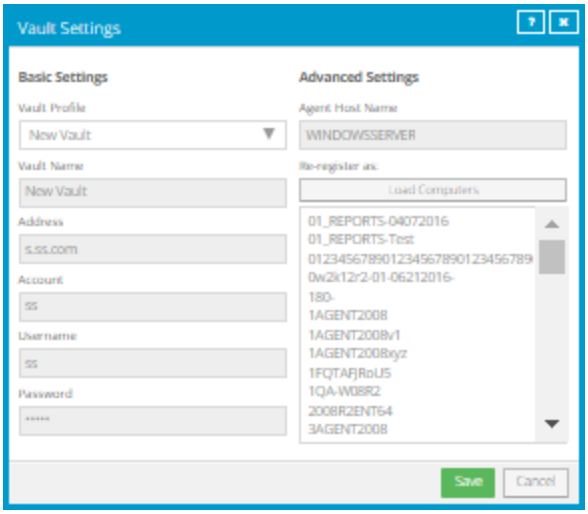
   A grid lists available computers.
3. Find the replacement computer to which you want to restore the data, and expand its view by clicking the computer row.
4. Click **Configure Manually**.
5. Click the Vault Settings tab.
6. Click **Re-register**.



6. In the Vault Settings dialog box, in the **Vault Profile** list, select the vault where the backup from the original computer was stored.



7. Click **Load Computers**.



8. In the list of computers, click the name of the computer where the data was backed up. Click **Save**.
9. In the confirmation dialog box, click **Yes**.
10. If the original computer backed up data to another vault, repeat Step 6 to Step 9 to download job information from the other vault.
11. After job information is downloaded, click the **Jobs** tab.

    You must enter any passwords required for the job, including the encryption password.
12. Find a job whose data you want to restore, and click **Restore** in the job's **Select Action** menu.

    The remaining steps are the same as the steps for regular restores.

    IMPORTANT: After you re-register a computer with the vault, you must enter the encryption passwords for the computer's backup jobs and synchronize the jobs before they run successfully. See Synchronize a job.

9.15 Restore data from another computer

You can restore some or all of a computer's backed up data to another (similar) computer.

To restore data from another computer, you can redirect data from a backup job on the vault to a different computer. If the data was backed up using a plug-in, the destination computer must have the same plug-in installed. If the data was backed up using the Exchange Plug-in, the destination computer must also have Microsoft Exchange installed. If the data was backed up using the SQL Plug-in, the destination computer must also have Microsoft SQL Server installed.

The new computer then downloads information from the vault so that the data can be restored on the new computer. For example:

- Computer A backs up data using Job A
- Computer B restores data from Job A (computer A's data) to Computer B

Alternatively, if you wish to perform a disaster recovery on the same or replacement computer, you can re-register a newly configured computer after installing an operating system and an agent on it. See Restore data to a replacement computer.

In some cases, where data streams are compatible, you may be able to restore to another computer with a similar (but not exactly the same) operating system. Different versions of the same operating system (e.g., Windows) are often compatible. Operating systems that share similar origins are also acceptable.

To restore data from another computer:

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

   A grid lists available computers.

2. Find the computer to which you want to restore the data, and expand its view by clicking the computer row.

3. In the **Job Tasks** menu, click **Restore from Another Computer**.

   The Restore From Another Computer dialog box opens.

4. In the **Vaults** list, select the vault where the backup is stored.

5. In the **Computers** list, select the computer with the backup from which you want to restore.

6. In the **Jobs** list, select the job from which you want to restore data.

7. Click **Okay**.

   Portal attempts to download information about the selected job. After the job information is downloaded, the job appears on the computer's Jobs tab. You can then continue restoring data as you would in a regular restore.

   If Portal cannot download information about the selected job, the restore cannot continue. This can occur if the vault cannot be reached, job information cannot be retrieved, or a required plug-in is not installed on the destination computer. Make sure that any required plug-in is installed on the destination computer before you try again.

10 Monitor computers, jobs and processes

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

- Current Snapshot. The Current Snapshot provides total numbers of backups and computers in various categories in your site, and allows you to navigate to more detailed information. See Monitor backups and computers using the Current Snapshot.
- Site Usage charts. In Portal instances that obtain data from billing systems, a Site Usage chart can show the amount of data backed up for a site in a billing period compared to a usage checkpoint amount. See Monitor storage usage using Site Usage charts and emailed alerts.
- Computers page. The Computers page shows status information for computers and their jobs. See View computer and job status information, View skipped rates and backup status histories and Determine whether an agent has been configured automatically. You can also access logs for unconfigured computers from this page. See View an unconfigured computer's 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. Admin users can also receive emails when job encryption passwords change and when potential ransomware threats are detected. See Set up email notifications for encryption password changes and Set up email notifications for potential ransomware threats.
- 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 job's 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, export and email backup statuses on the Monitor page and View skipped rates and backup status histories.

10.1 Monitor backups and computers using the Current Snapshot

In the Current Snapshot on the Dashboard, you can view total numbers of backup jobs and computers in your site in various categories. You can then navigate from these totals to view more detailed information about the jobs and computers.

To monitor backups and computers using the Current Snapshot:

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

   The Current Snapshot at the left side of the Dashboard shows the number of backup jobs and computers in the following categories:

- **Potential Threats** — Number of backup jobs where a potential ransomware threat was detected. See Manage potential ransomware threats. If a ransomware scan did not run successfully, the backup job could appear in the "Backups with Warnings" category. Please see the backup logs for more information.
- **Backups Requiring Attention** — Number of backup jobs where the last backup attempt failed, completed with errors, did not back up any files, reached a license limit, was cancelled or had a potential ransomware threat.
- **Missed Backups** — Number of backup jobs that have not run for seven days.
- **Backups With Warnings** — Number of backup jobs where the last backup attempt completed with warnings, was deferred, was deferred with warnings or was skipped. This category also includes backup jobs that have never run.
- **Computers Requiring Reboot** — Number of computers with a pending reboot.
- **Offline Computers** — Number of computers that are not currently in contact with Portal. A computer can be offline if it is turned off, if the Agent has been uninstalled from the system, or if the system no longer exists.
- **Computers Scheduled for Deletion** — Number of computers that are scheduled for deletion from Portal and from vaults. This category is only applicable to Portal instances where the data deletion feature is enabled.
- **Computers With Certificate Failures** — Number of computers reporting a certificate failure. See Resolve certificate failures.
- **Total Computers** — Total number of computers in the site.
- **Successful Backups** — Number of backup jobs where the last backup attempt completed without errors, warnings, or deferrals.
- **Jobs Scheduled for Deletion** — Number of jobs that are scheduled for deletion from Portal and from vaults. This category is only applicable to Portal instances where the data deletion feature is enabled.

2. To view computers in a particular site, click the sites box in the top right of the Current Snapshot box. In the menu, click the site that you want to view.

   Computers in the selected site appear on the Computers page.

3. To view information about backup jobs or computers in one of the categories, click the category.

   If you click **Potential Threats**, **Backups Requiring Attention**, **Missed Backups**, **Backups With Warnings** or **Successful Backups**, backup jobs in the category appear on the Monitor page.

   If you click **Computers Requiring Reboot**, **Offline Computers**, **Computers Scheduled For Deletion**, **Computers With Certificate Failures** or **Total Computers**, computers in the category appear on the Computers page.

10.2 View computer and job status information

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

To view computer and job status information:

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

   The Computers page shows registered computers.

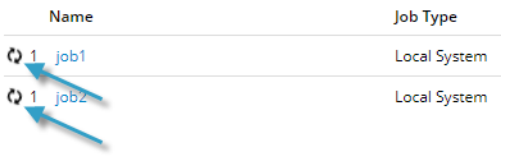
   The Availability column indicates whether each computer is online or offline. Online computers are in contact with Portal, while offline computers are not currently available. A computer can be offline if it is turned off, if the agent has been uninstalled from the system, or if the system has been lost.

   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.
   - Scheduled for deletion — Indicates that the computer is scheduled for deletion from Portal and from vaults. This status only appears in Portal instances where the data deletion feature is enabled.
   - Certificate failure — Indicates that the agent is reporting a certificate change.

2. Find the computer for which you want to view status information, and click the row to expand its view.
3. View the **Jobs** tab.

   If a backup or restore is running for a job, a Process Details symbol appears beside the job name, along with the number of processes that are running.



   If you click the Process Details symbol, the Process Details dialog box shows information about processes for the job. See View current process information for a job.

The **Last Backup Status** column shows the last backup status reported for each job. An agent reports a backup status to Portal each time it starts, skips or completes a backup. 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.
- Skipped — Indicates that a backup was skipped. Backups are sometimes skipped if they are scheduled to run multiple times per day. See Skipped backups.
- 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. This status can also indicate that a potential ransomware threat was detected.
- No Files backed up — Indicates that no files were backed up during the last backup attempt
- Failed — Indicates that the backup failed and no safeset was created.
- Cancelled — Indicates that the backup was 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. See Delete a backup job and delete job data from vaults.

If **Potential Threat** appears after the status in the Last Backup Status column, a potential ransomware threat was detected while running the backup job. See Manage potential ransomware threats.

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

10.3 Monitor storage usage using Site Usage charts and emailed alerts

For some sites in some Portal instances, Admin users can view a Site Usage chart on the Dashboard. This chart shows the amount of data backed up for computers in the site compared to a specified limit. This can help customers monitor their storage usage and avoid billing overages.

When this feature is enabled for a site, Admin users for the site also receive email alerts when the site's storage usage first reaches 50%, 75%, 90% and 100% of the specified limit. If a site's storage usage is above 50%, 75%, 90% or 100% of the specified limit at the start of a billing period, Admin users also receive an email alert at the start of the billing period. Admin users cannot opt out of usage email alerts when this feature is enabled.

Note: At the start of a billing period, Portal might show usage data and send email alerts for the previous billing period. Usage data and alerts are provided for the new billing period as soon as the data is available.

Site Usage charts and emailed alerts are available beginning in Portal 9.30 in some Portal instances that obtain data from billing systems. Admin users in a Parent site can enable this feature and specify a limit or "User Checkpoint" for eligible sites.

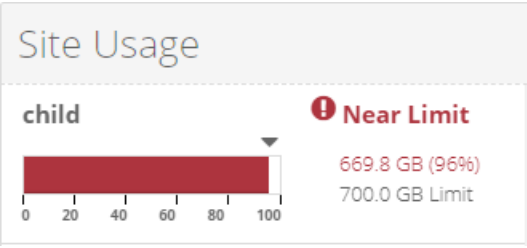
Support users can also view Site Usage charts.

To monitor storage usage using Site Usage charts:

1. Sign in to Portal as an Admin user.
2. On the navigation bar, click **Dashboard**.

   If usage tracking and alerting is enabled for your site, a Site Usage chart appears at the right side of the Dashboard. The chart shows the amount of data backed up for computers in the site in the current billing period as compared to the specified limit, or usage checkpoint amount. The amount of data backed up is the original size of the data before it was compressed.

   If you are viewing a parent site, a separate Site Usage chart could appear for the parent site and any child sites where this feature is enabled. If more than four charts appear, you can scroll through the charts.



   As described in the table below, the Site Usage chart color indicates how much data has been backed up in the current billing period compared to the specified limit, or usage checkpoint amount:

Chart color	Description
Green	The site's storage usage in the current billing period is less than 50% of the specified limit.
Yellow	The site's storage usage in the current billing period is between 50% and 75% of the specified limit.
Orange	The site's storage usage in the current billing period is between 75% and 90% of the specified limit. An orange warning message appears beside the chart in this case.
Red	The site's storage usage in the current billing period is more than 90% of the specified limit. A red warning message appears beside the chart in this case.

If a Site Usage chart does not appear, usage tracking and alerting might not be available for your site or in your Portal instance.

10.4 View skipped rates and backup status histories

When a Windows agent is backing up data to a Director version 8.60 or later vault, backups that are scheduled to run multiple times per day are skipped in some cases. To determine whether backups were skipped, users can view email notifications, the Computers page and Monitor page, and the Daily Status report. See Skipped backups.

In some Portal instances, users can also view the following skipped rate and backup status history information:

- Skipped rate for a job. If a backup was skipped for a job in the 48 hours before the most recent backup attempt, a skipped rate appears for the job on the Computers page and Monitor page. The skipped rate is the percentage of backups that were skipped in the 48 hours before the last backup attempt, and is calculated using the following formula:

  jobSkippedRate = *numberOfSkippedBackups* / *numberOfBackupAttempts*

  Where:

  - *numberOfSkippedBackups* is the number of backups that were skipped for the job during the 48 hours before the last backup attempt.
  - *numberOfBackupAttempts* is the total number of backup attempts for the job during the 48 hour period, including skipped, in-progress, deferred, canceled, failed and completed backups.

  If no backups were skipped for a job in the 48 hours before the last backup attempt, or if the last backup attempt occurred more than seven days ago, a skipped rate is not shown for the job.

- Skipped rate for a computer. If a skipped rate is reported for one or more jobs on a computer, the highest skipped rate on the computer appears on the Computers page.

- 48-hour backup status history for a job. If a skipped rate appears for a job on the Computers or Monitor page, you can view the job's backup history for the 48 hours before the last backup attempt. The status history shows the dates and times of backup attempts, and indicates the status of each backup attempt (e.g., skipped, in-progress, completed or failed). You can export the status history in comma-separated values (.csv), Microsoft Excel (.xls) or Adobe Acrobat (.pdf) format.

To view skipped rates and backup status histories, see View skipped rates and backup status histories on the Computers page and View skipped rates and backup status histories on the Monitor page.

10.4.1 View skipped rates and backup status histories on the Computers page

To prevent schedule overloads, backups that are scheduled to run multiple times per day are skipped in some cases. Users can obtain skipped backup information through email notifications, on the Computers page, and in the Daily Status report. See Skipped backups.

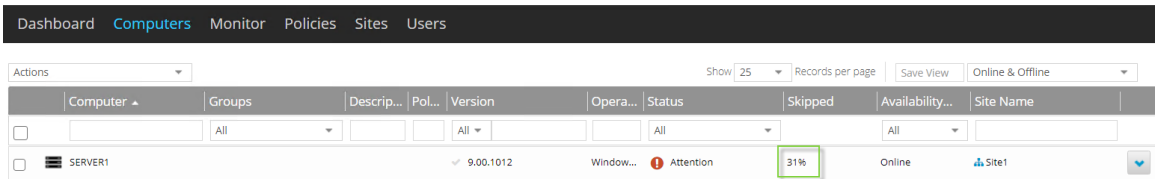
In some Portal instances, users can view skipped backup rates for jobs and computers on the Computers page, and view and export a job's backup status history for the 48 hours before the last backup attempt. For more information, see View skipped rates and backup status histories.

To view skipped rates and backup status histories on the Computers page:

1. Click **Computers** on the navigation bar.

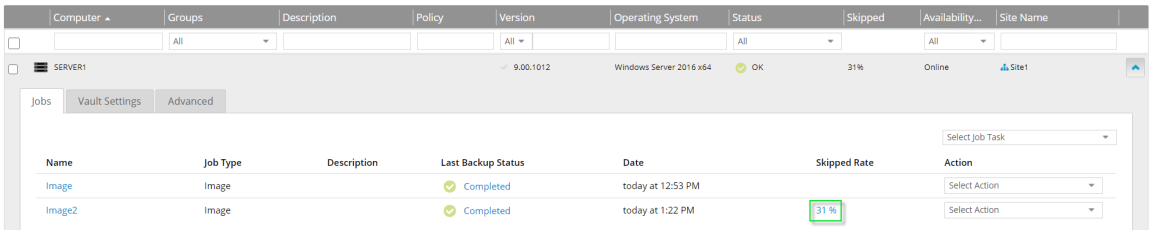
   A value appears in the Skipped column for any computer where at least one job has a skipped rate. If more than one job on a computer has a skipped rate, the highest skipped rate appears in the Skipped column.

   Note: If the Skipped column does not appear, skipped rates and 48-hour backup status histories are not available in your Portal instance.



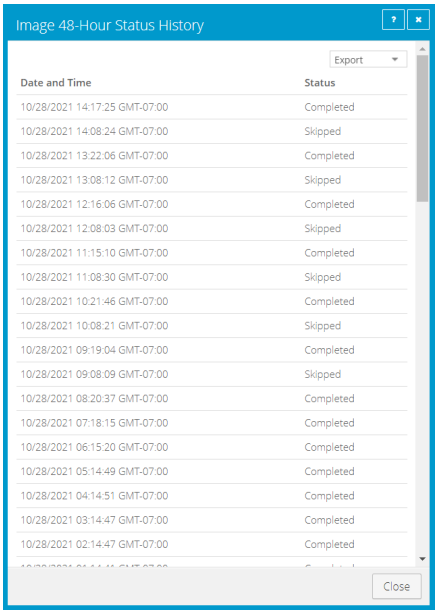
2. Find a computer with a value in the Skipped column, and click the computer row to expand its view.

   On the Jobs tab, a value appears in the Skipped Rate column for any job where a backup was skipped in the 48 hours before the last backup attempt, and the last backup attempt occurred in the last seven days.



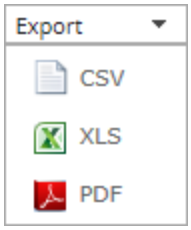
3. To see which backups were skipped in the 48 hours before the last backup attempt for a job, click the job's Skipped Rate value.

   The 48-Hour Status History for the job shows the date, time and status (e.g., skipped, in-progress, completed or failed) of each backup attempt.



   If you want to export the status history, click the **Export** box. In the list that appears, click one of the following formats for the exported data:

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



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

   Note: We recommend turning off macros in Microsoft Excel when using Portal, particularly if you export reports in XLS or CSV format and open these reports in Excel.

10.4.2 View skipped rates and backup status histories on the Monitor page

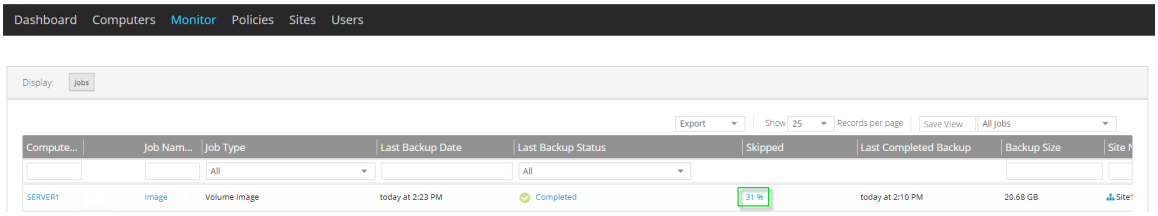
To prevent schedule overloads, backups that are scheduled to run multiple times per day are skipped in some cases. Users can obtain skipped backup information through email notifications, on the Computers page, and in the Daily Status report. See Skipped backups.

In some Portal instances, users can view skipped backup rates for jobs on the Monitor page, and view and export a job's backup status history for the 48 hours before the last backup attempt. For more information, see View skipped rates and backup status histories.

To view skipped rates and backup status histories on the Monitor page:

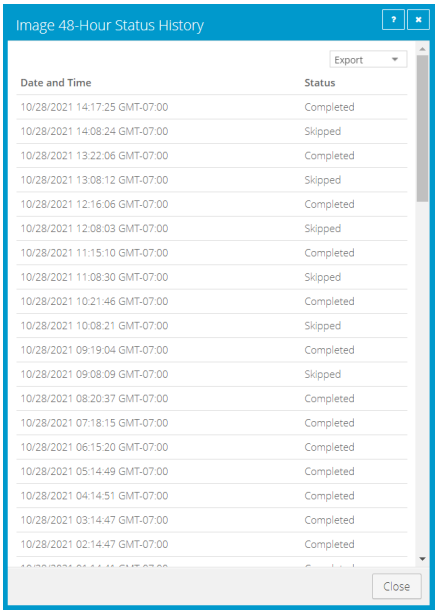
1. Click **Monitor** on the navigation bar.

   A value appears in the Skipped column for any job where a backup was skipped in the 48 hours before the last backup attempt, and the last backup attempt occurred in the last seven days.



2. To see which backups were skipped in the 48 hours before the last backup attempt for a job, click the job's Skipped value.

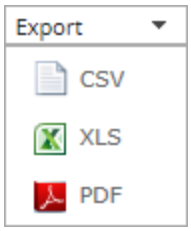
   The 48-Hour Status History for the job shows the date, time and status (e.g., skipped, in-progress, completed or failed) of each backup attempt.



   If you want to export the status history, click the **Export** box. In the list that appears, click one of the following formats for the exported data:

   - CSV (comma-separated values)
   - XLS (Microsoft Excel)

- PDF (Adobe Acrobat)



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

Note: We recommend turning off macros in Microsoft Excel when using Portal, particularly if you export reports in XLS or CSV format and open these reports in Excel.

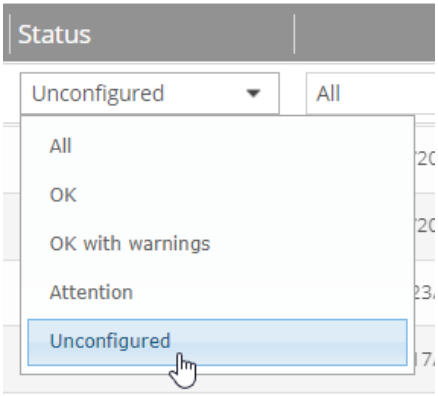
10.5 View an unconfigured computer's logs

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

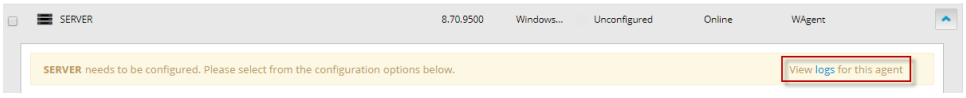
To view an unconfigured computer's logs:

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

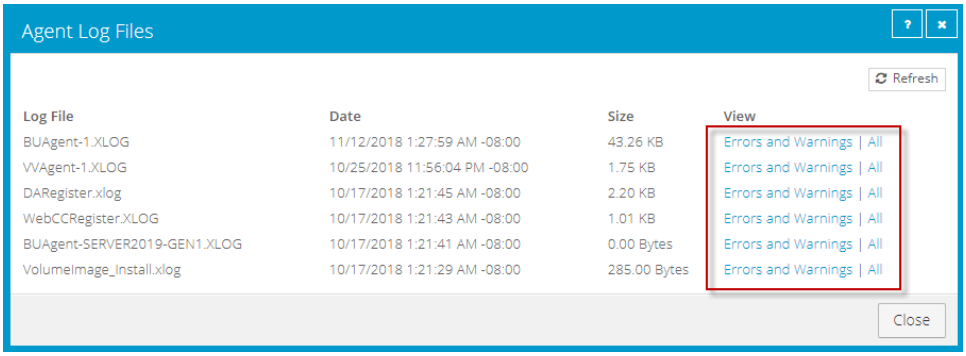
   The Computers page shows registered computers. To only show unconfigured computers, click "Unconfigured" in the **Status** filter.



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.

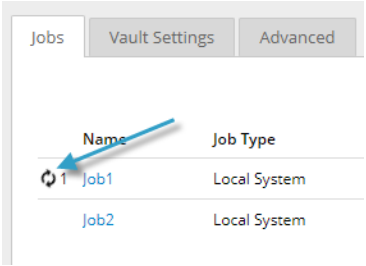
   The log appears in a new browser tab.

10.6 View current process information for a job

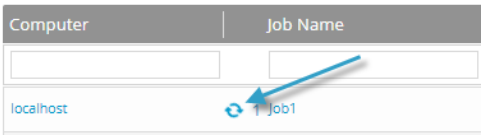
In the Process Details dialog box, you can view information about running, queued and recently-completed processes for a job. Processes include backups, restores, and synchronizations, and is typically deleted within an hour after the process ends.

To view current process information for a job:

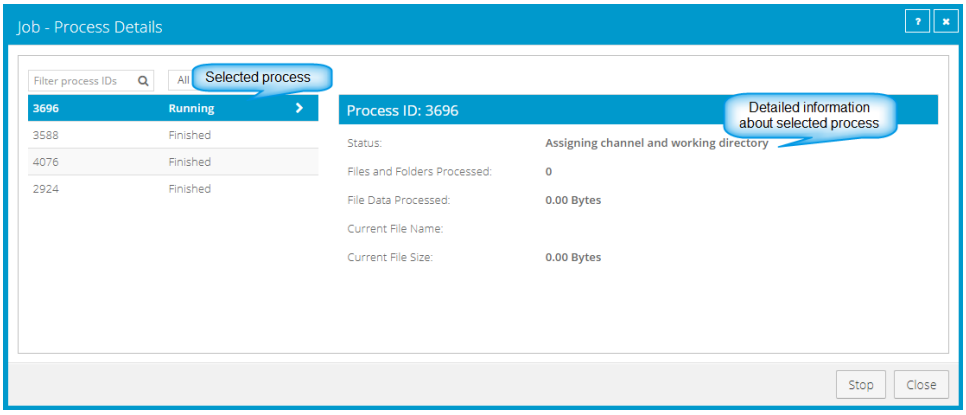
1. While a backup, restore, or synchronization is running, do one of the following:
   - On the Computers page, on the Jobs tab, click the Process Details symbol beside the job name.



   - On the Monitor page, click the Process Details symbol beside the job name.



   If you clicked a Process Details symbol, the Process Details dialog box lists backup, restore and synchronization 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.

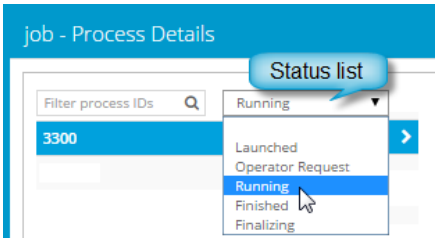


2. To view information about a different process, click the process or VM name on the left side of the dialog box.

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

3. If the Process Details dialog box lists backup, restore and synchronization processes for the job, do one of the following in the status list to show only some processes:

   - 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**.



10.7 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.

When email notifications are configured centrally in a Portal instance, admin users can also receive email notifications when the encryption password changes for a backup job or when a potential ransomware

threat is detected during a Windows backup. See Set up email notifications for encryption password changes and Set up email notifications for potential ransomware threats.

10.7.1 Set up email notifications for backups on a computer

To set up email notifications for a computer:

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

   The Computers page shows registered computers.

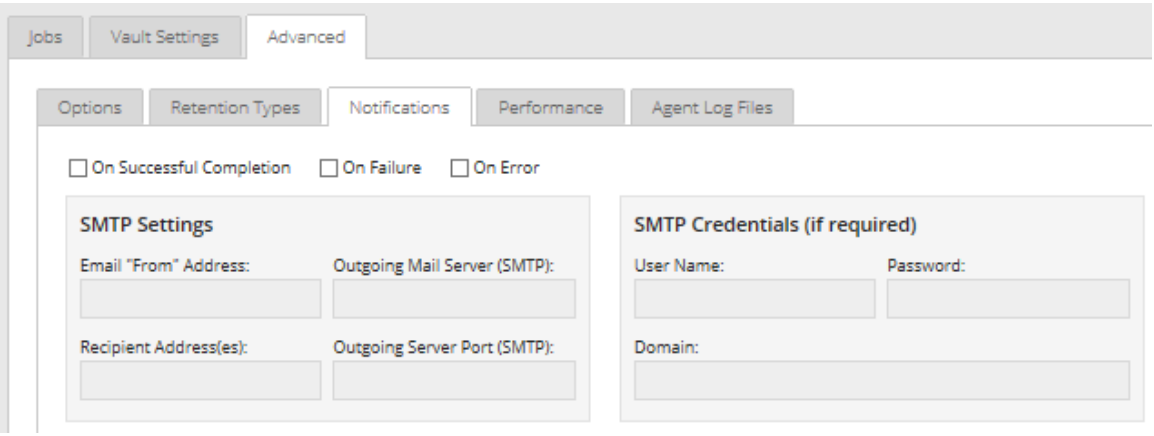
2. Find the computer for which you want to configure email notifications, and click the computer row to expand its view.

3. On the **Advanced** tab, click the **Notifications** tab.

   If the Notifications tab does not appear, email notifications for the computer's backups are configured centrally instead of for each computer. See Set up email notifications for backups on multiple computers.

   Note: If email notifications were set up for the computer before centrally-configured email notifications were enabled in the Portal instance, the Notifications tab can appear for the computer.

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



4. 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.

5. Click **Save**.

10.7.2 Set up email notifications for backups on multiple computers

By default in some Portal instances, Admin users receive emails when backups fail, or are canceled, deferred, missed, skipped or completed. Admin users can select backup statuses for which they want to receive email notifications.

When email notifications are configured centrally in a Portal instance, additional notification email addresses can be specified for each child site.

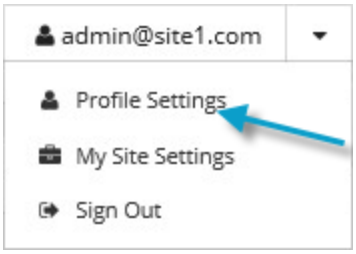
Note: Email notifications selected in Admin users' profile settings are only sent in English. Email notifications for child site email addresses are supported in multiple languages.

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, Backup Skipped), you can select events for which you want to receive emails.

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

   If an Encryption Password Changed option appears, you can choose to receive email notifications when encryption passwords change in your site.

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
   - Backup Skipped

     Note: Backups are sometimes skipped if they are scheduled to run hourly or multiple times per day. See Skipped backups.

4. Click **Update notifications**.

10.7.3 Set up email notifications for encryption password changes

In some sites, Admin users can choose to receive emails when job encryption passwords change.

Admin users in a parent site can receive emails when job encryption passwords change in the parent site and in its child sites. Admin users in a child site can receive emails when job encryption passwords change in the child site only.

Super users specify whether Admin users in a site can receive encryption password change emails.

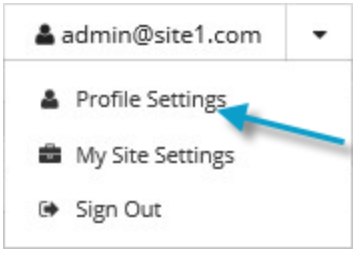
When email notifications are configured centrally in a Portal instance, additional notification email addresses can be specified for each child site.

Note: Email notifications selected in Admin users' profile settings are only sent in English. Email notifications for child site email addresses are supported in multiple languages.

To set up email notifications for encryption password changes:

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 an Encryption Password Changed option, you can choose to receive emails when encryption passwords change.

3. In the Email Notification Settings list, select the **Encryption Password Changed** option.
4. Click **Update notifications**.

10.7.4 Set up email notifications for potential ransomware threats

When email notifications are configured centrally in a Portal instance instead of separately for each computer, Admin users can receive emails when potential ransomware threats are detected on Windows servers. Threat detection can be enabled in Local System backup jobs, beginning with Windows Agent 9.00 and Portal 8.90. See Add a Windows backup job and Manage potential ransomware threats.

Admin users in a parent site can receive emails when potential threats are detected in the parent site and in its child sites. Admin users in a child site can receive emails when potential threats are detected in the child site.

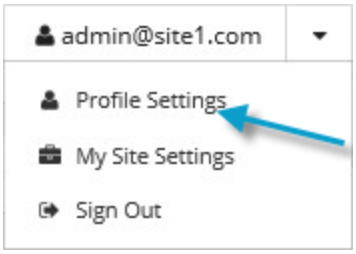
When email notifications are configured centrally in a Portal instance, additional notification email addresses can be specified for each child site.

Note: Email notifications selected in Admin users' profile settings are only sent in English. Email notifications for child site email addresses are supported in multiple languages.

To set up email notifications for potential ransomware threats:

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**.
3. In the Email Notification Settings list, select the **Potential Threats** option.
4. Click **Update notifications**.

10.8 View a job's process logs and safeset information

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

Note: When you run an Exchange database restore with the **Start Hard Recovery** option selected, the process of restoring database files is recorded in the process logs. The process of replaying transaction logs into the database is recorded in the Windows Event Viewer.

You can also view information about safesets created for the job. A safeset is an instance of backup data on the vault.

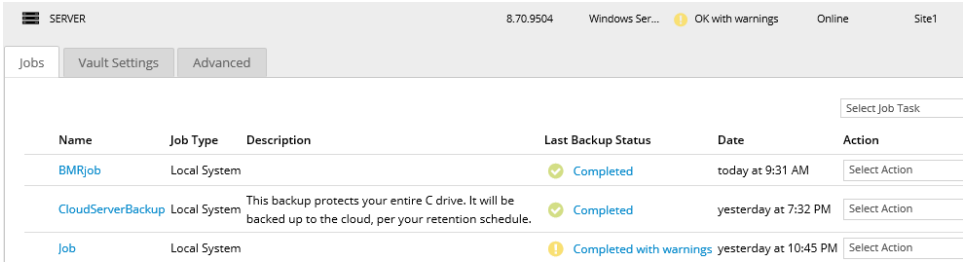
To view a job's process logs and safeset information:

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

   The Computers page shows registered computers.

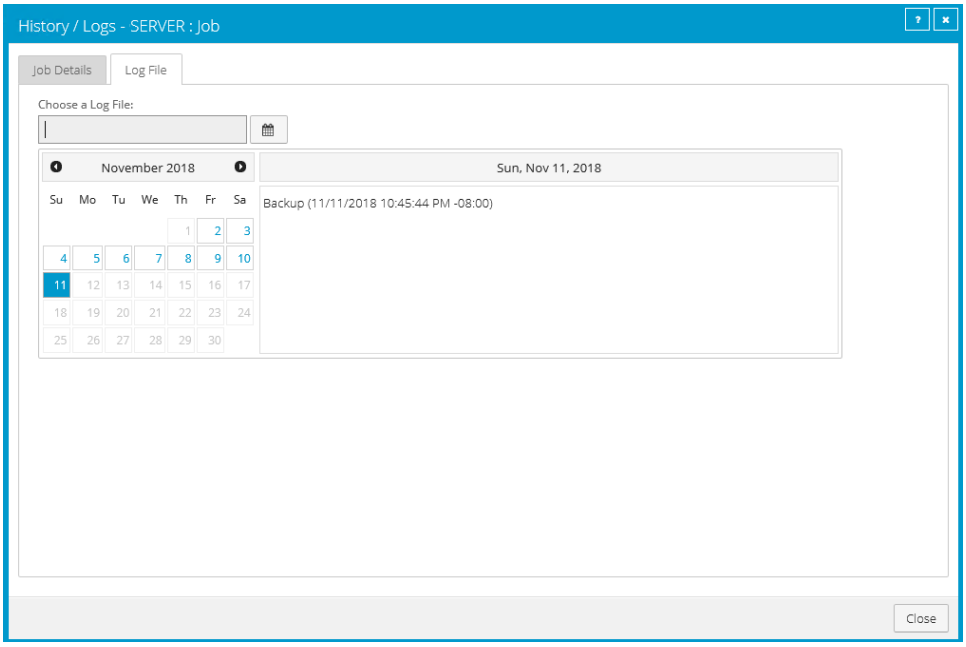
2. Find the computer for which you want to view logs, and click the row to expand its view.

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



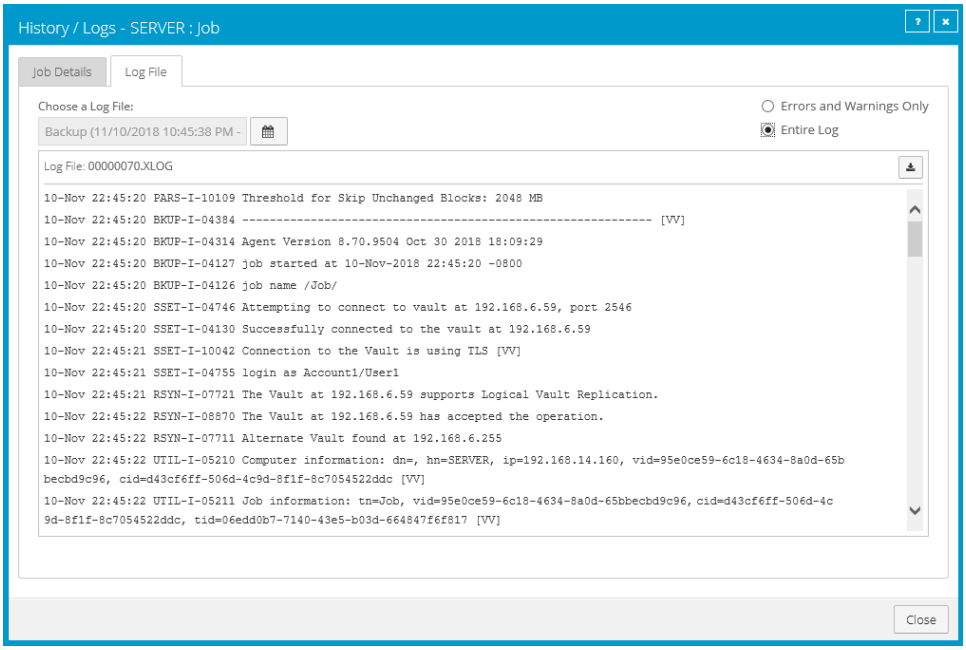
3. To view log files for a job, do one of the following:
   - In the job's **Select Action** menu, click **History / Logs**.
   - In the **Last Backup Status** column, click the job status.

   The History / Logs or Logs window lists the most recent backups, restores and other processes 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.
5. In the list of processes on the selected date, click the process for which you want to view the log.

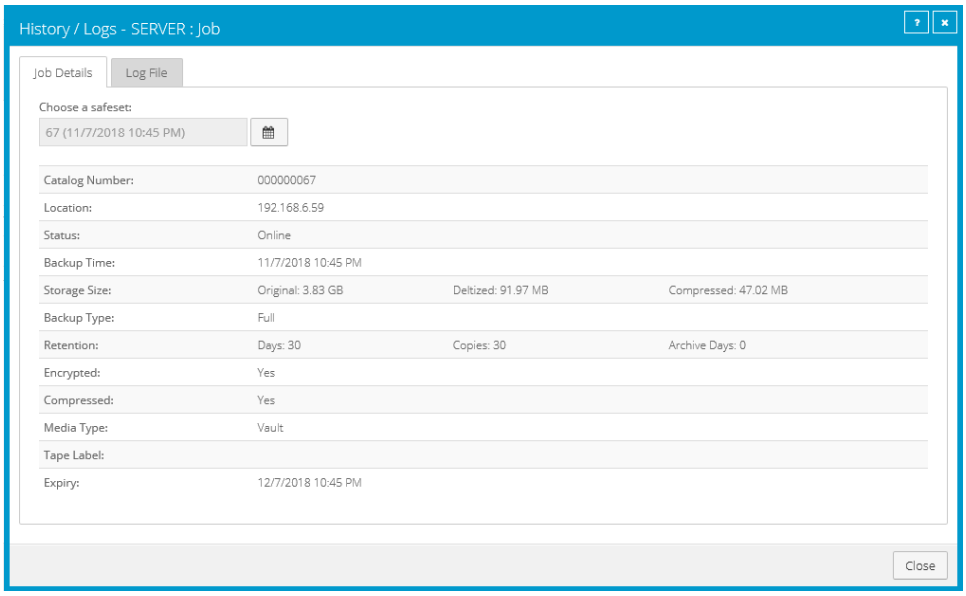
   The window shows the selected log.



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

7. 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.



10.9 View, export and email backup statuses on the Monitor page

You can view recent job backup statuses on the Monitor page in Portal and navigate to related information on the Computers page or in the Logs window.

You can export data from the Monitor page in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format. The exported data file (named "Job Monitor Export.csv", "Job Monitor Export.xls" or "Job Monitor Export.pdf") is downloaded to the user's computer.

Beginning in Portal 9.20, Admin users and Support users can email reports with data from the Monitor page. These Job Monitor Export reports can be:

- Emailed once to one or more recipients. To specify which job backup statuses appear in this report, you can select a view and filter data on the Monitor page.
- Scheduled to be emailed to one or more recipients on specified days at a specified time. To specify which job backup statuses appear in a scheduled report, you can filter data by any column except the Last Backup Date column. You can only schedule a report to be emailed from the All Jobs view on the Monitor page.

A Job Monitor Export report is emailed as an attachment in .csv, .xls or .pdf format (named "Job Monitor Export.csv", "Job Monitor Export.xls" or "Job Monitor Export.pdf"). Reports in .xls and .pdf format are formatted using the site's logo, color, and custom text.

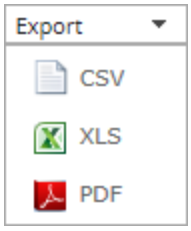
Note: We recommend turning off macros in Microsoft Excel when using Portal, particularly if you export or email information in .xls or .csv format and open these reports in Excel.

To view, export and email backup statuses on the Monitor page:

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

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

2. To change which job backup statuses appear, click a view or enter filter criteria.
3. To view information for a job or computer on the Computers page, click the name of a job or online computer.
4. To view a job's logs in the History/Logs window, click the job's last backup status.
5. To export job backup status data from the Monitor 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.
6. To email a Job Monitor Export report, do the following when signed in as an Admin or Support user:
   a. To specify which job backup statuses appear in the report, click a view or enter filter criteria.
   b. Click the **Email/Schedule** box. In the **Send Report** list that appears, click **Email Once**.
   c. In the Email Once dialog box, do the following:
      i. In the **To** box, type one or more email addresses for sending the report. Use commas to separate multiple email addresses.
      ii. In the **Subject** box, type a subject for the report email.
      iii. In the Attachment list, click one of the following formats for the emailed report:
         - CSV (comma-separated values)
         - Excel (Microsoft Excel)

- PDF (Adobe Acrobat)

d. Click **Okay**.

7. To schedule a Job Monitor Export report to be emailed, do the following when signed in as an Admin or Support user:

   a. To specify which job backup statuses appear in the scheduled report, enter filter criteria in any column except the Last Backup Date column.

      Note: You can only schedule a report to be emailed when the All Jobs view is selected on the Monitor page.

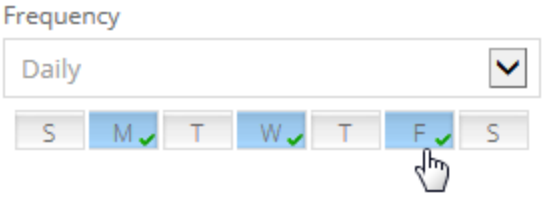
   b. Click the **Email/Schedule** box. In the **Send Report** list that appears, click **Schedule New Report**.

   c. In the Email/Schedule dialog box, do the following:

      - In the **To** box, type one or more email addresses for sending the report. Use commas to separate multiple email addresses.
      - In the **Report Name** box, type a name for the scheduled report. This name appears in the **Email/Schedule** list.
      - In the **Subject** box, type a subject for the email.
      - In the **Attachment** list, click one of the following formats for the emailed report:
        - CSV (comma-separated values)
        - Excel (Microsoft Excel)
        - PDF (Adobe Acrobat)

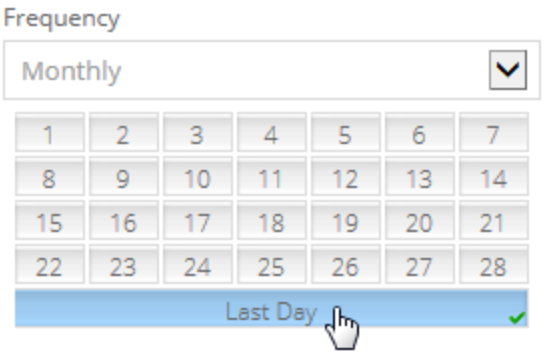
   d. Do one of the following:

      - To email the report on specific days each week, in the **Frequency** list, click **Daily**. In the day row, select the days when you want to email the report each week.



      - To email the report once each week, in the **Frequency** list, click **Weekly**. In the day row, select the day when you want to email the report each week.

- To email the report once each month, in the **Frequency** list, click **Monthly**. In the calendar, select the date when you want to email the report each month, or select **Last Day** to email the report on the last day of each month.



e. Using the **At** field, specify the time when you want to email the report on the specified days.

f. Click **Okay**.

10.10 Determine whether an agent has been configured automatically

Beginning with Portal 8.89 and Windows Agent 8.90a, backups can be configured automatically on Windows servers based on job templates. The Windows agent must be installed with a default encryption password and registered to a Portal site where agent auto-configuration is enabled.

When agent auto-configuration is enabled, Portal finds and auto-configures eligible Windows agents every three minutes. When an agent is successfully configured, a backup job for the Windows server is created that has:

- The name, description, settings and schedules specified by the job template selected for the child site.
- A randomly-assigned time for running backups with “Days of Week” and “Days of Month” schedules. By default, the time will be between 8 PM and 8 AM, but a different time window might be specified in your Portal instance.
- The vault profile selected for the child site.
- The default data encryption password specified when the agent was installed.

To determine whether an agent has been configured automatically, you can view the agent on the Computers page in Portal. If the agent has not been configured, an auto-configuration status message appears.

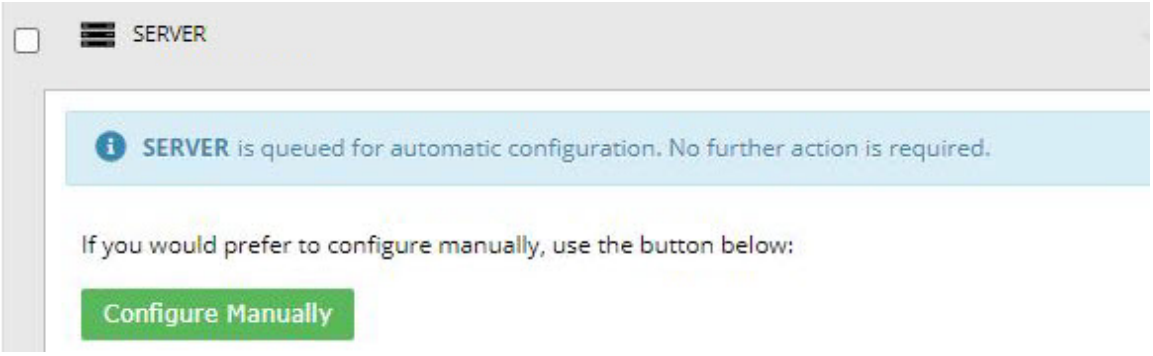
To determine whether an agent has been configured automatically:

1. Sign in to Portal as an Admin user in a child site where agent auto-configuration is enabled, or as a parent site Admin user who can manage the child site.
2. Do one of the following:
   - On the navigation bar, click **Computers**. On the Computers page, find the computer for which you want to view the auto-configuration status. Click the computer row to expand it.
   - On the navigation bar, click **Dashboard**. In the Notification Center, click **What's New**. In the center of the dashboard, find the notification of the computer and click its **Configure Now** link. The computer row is shown on the Computers page.

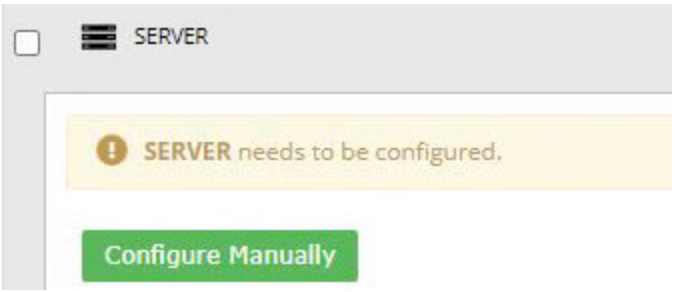
   Note: If the computer is unconfigured and offline, you cannot expand the computer row. An agent cannot be configured automatically if it is offline after it registers to Portal. If an agent stays offline for seven days after registering to Portal, backups cannot be automatically configured on the server. If the agent comes online after seven days, an "automatic configuration has failed" message appears for the agent.

   If a job appears in the computer row, the agent has been configured. If the agent was configured automatically, the job has the name, settings and schedule specified by the job template for the child site.

   If a "queued for automatic configuration" message appears in the computer row, the agent is waiting to be configured. Portal will attempt to configure the agent in the next three minutes.



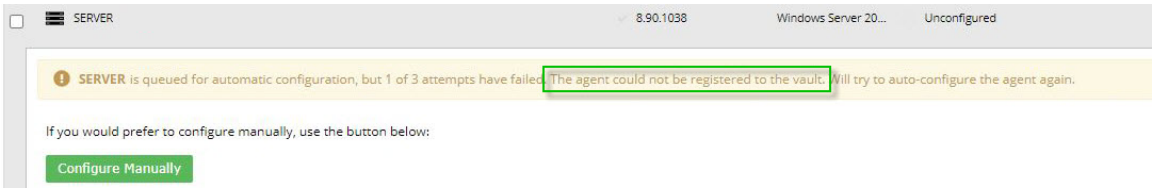
   If a "needs to be configured" message appears in the computer row, the agent is not eligible for auto-configuration and you must create a backup job manually. For more information, see Reasons that agents are not eligible for auto-configuration.



If a "queued for automatic configuration but *x* of 3 attempts have failed" message appears in the computer row, an auto-configuration attempt failed. Portal will attempt to configure the agent again in the next three minutes.

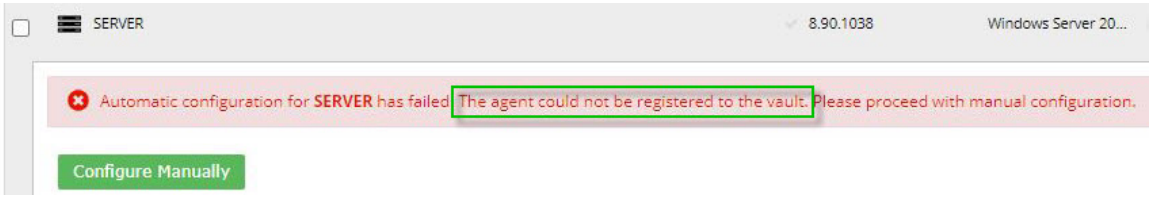
Note: Portal attempts to configure backups on a server three times after an agent is registered to Portal.

If error information is available, the second sentence of the message (shown in a green rectangle, below) describes the issue.



If an "automatic configuration has failed" message appears, three auto-configuration attempts failed. Please create a backup job manually.

If error information is available, the second sentence of the message (shown in a green rectangle, below) describes the issue.



10.10.1 Reasons that agents are not eligible for auto-configuration

If a "needs to be configured" message appears for an agent on the Computers page, the agent is not eligible for auto-configuration. This can occur if:

- The agent is not a Windows agent, or is a Windows agent version that is not supported for auto-configuration. Agent auto-configuration is supported with Windows Agent version 8.90a or later.
- An encryption password was not specified when the agent was installed. See Install the Windows Agent and plug-ins.

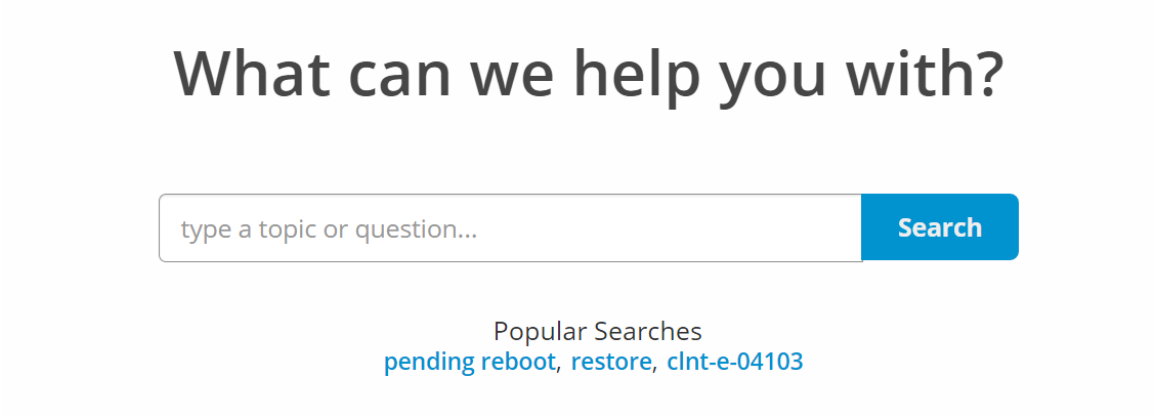
- An Image job template is selected for the child site, but the Image Plug-in is not installed with the agent.
- The agent has more than one vault registration (vault setting), or has a vault registration that does not match the vault profile selected for agent auto-configuration in the site.
- The agent has one or more backup jobs. This could occur if a backup job was manually configured before the Agent Configuration task ran in Portal.
- The agent is registered to a site where agent auto-configuration is not fully set up (e.g., a job template is not selected).

  IMPORTANT: Auto-configuration must be enabled in the child site when the agent first registers to Portal. An agent will not be automatically configured if you enable auto-configuration after the agent is registered to Portal.

11 Carbonite Server Backup Support

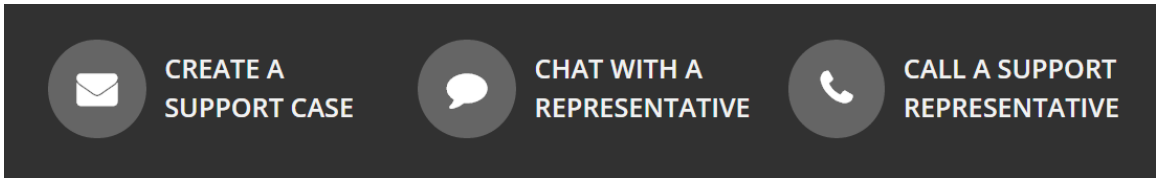
If you have a question about Carbonite Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any Carbonite Server Backup solutions you may need. We highly recommend searching here first for the quickest answers to your questions.

Knowledge Base: http://support.carbonite.com/evault



11.1 Contacting Carbonite

If you need live assistance from a qualified support agent, Carbonite Support is here for you 24 hours a day, 7 days a week (excluding US holidays). Please feel free to get in touch with us, and we'll help out any way we can! You can find the contact information for Carbonite Support in the Knowledge Base: http://support.carbonite.com/evault



Tip: When contacting Support with a technical issue, please have both the program's log files and the store you are having difficulty with ready.

Compress the program's log files in a .zip file and attach it to your support request.

If the log archive exceeds 10MB, you may not be able to send them as an email attachment. In that case, upload instructions will be provided to you upon request.