Windows Agent 8.7

User Guide

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

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

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

Document History

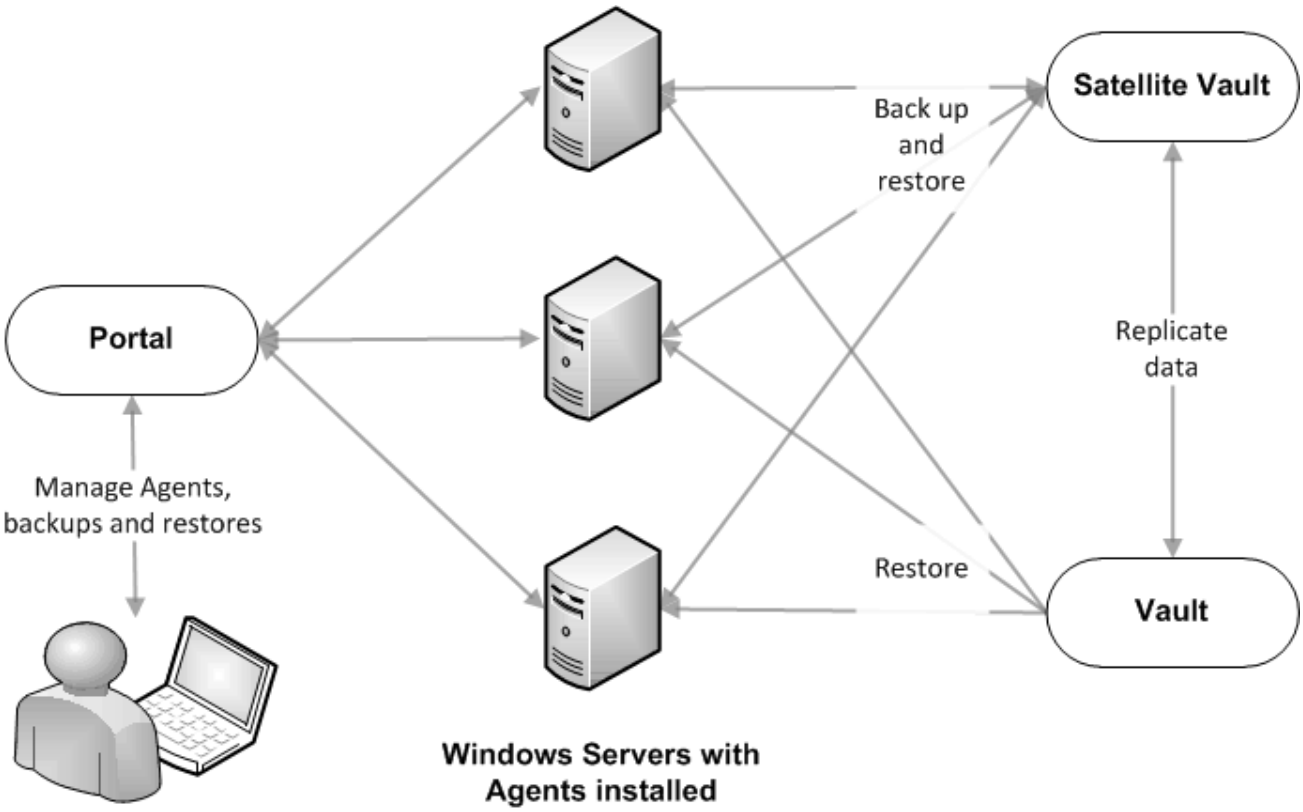
Version	Date	Description
1	December 2018	Initial guide provided for Windows Agent 8.7*x*.
2	March 2019	Updated Exchange Plug-in names in Windows Agent Plug-ins and Windows Agent feature parameters. Clarified cluster upgrade information in Upgrade the Windows Agent and plug-ins and added Upgrade Windows Agents in a cluster. Clarified BMR/system state restore information in Restore Windows data and Restore a domain controller.

Contents

1 Introduction to the Windows Agent

Agent for Microsoft Windows backs up data on Windows systems, and restores 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.



You can also use the legacy Windows CentralControl to manage the Agent and jobs. 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 is available as a 64-bit and a 32-bit application. You must install the appropriate Agent on each Windows system (i.e., 64-bit Agent for a 64-bit system; 32-bit Agent for a 32-bit system).

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.

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 and applications that can be installed with the Windows Agent, and indicates whether they can be installed with the 64-bit or 32-bit Windows Agent.

Note: Support ended for SharePoint Plug-in, Exchange MAPI and SQL Server VDI jobs as of Agent version 7.50. You must delete any jobs with these legacy types from the Agent before you can upgrade the Agent. If you upgrade an Agent with a legacy plug-in to version 7.50 or later, 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 an Agent to version 7.50 or later where the Agent Assistant is installed, the Agent Assistant will be removed from the system.

Plug-in or component	**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. Available with both the 64-bit and 32-bit Windows Agent.
Exchange Plug-in	Backs up and restores Exchange databases for versions later than Exchange 2007. You can also restore individual mailboxes and messages using this plug-in and the Granular Restore for Microsoft Exchange application. *Note:* In previous versions, this plug-in was called the Exchange 2010/2013/2016 DR Plug-in. Only available with the 64-bit Windows Agent.
Exchange Plug-in (Legacy)	Backs up and restores Exchange 2007 databases. You can also restore individual mailboxes and messages using this plug-in and the Granular Restore for Microsoft Exchange application. *Note:* In previous versions, this plug-in was called the Exchange 2007 DR Plug-in. This plug-in is for use with Exchange 2007 only. Only available with the 64-bit Windows Agent.

Plug-in or component	Description
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. Only available with the 64-bit Windows Agent.
Oracle Plug-in	Backs up and restores Oracle databases. Available with both the 64-bit and 32-bit Windows Agent.
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 2013 and 2010 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. Available with both the 64-bit Agent and the 32-bit Agent.

1.1.1 Image Plug-in

To back up Windows volumes as images, install the Image Plug-in with the 64-bit 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.

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. 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.*

Using Image Plug-in version 7.5 or later, you 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 file systems. The 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.

2 Install the Windows Agent and plug-ins

The Windows Agent is available as a 64-bit or 32-bit application. You must install the appropriate Agent for the system (i.e., 64-bit Agent for a 64-bit system; 32-bit Agent for a 32-bit system).

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

Important: This Windows Agent version provides support for automatic agent upgrades. You will not have to manually run an agent installation kit to upgrade this agent to later versions. Instead, when a new installer is available in Portal, the agent will download the installer and upgrade itself automatically.

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 the Agent, 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**.
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**.

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

     Note: 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 (64-bit or 32-bit). 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**.
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**.
    - To encrypt data using an external AES 256 encryption library that is provided with the Agent, click **Encrypt data using the external encryption library**. Some organizations require the external encryption library for audit purposes.

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

    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.

      Note: 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. The user must be an Admin user or regular user. Typically, the user name is an email address.

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

14. Click **Next**.
15. On the Ready to Install the Program page, click **Install**.

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

    The unconfigured Windows computer appears on the Computers page for the specified user, and for other Admin users in the user's site. To configure the computer, 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 to version 8.7*x* by manually running the Agent installation kit.

Important: Windows Agent 8.70 and later versions can be upgraded automatically. When a new installer is available in Portal, the agent will download the installer and upgrade 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.

Notes:

- 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 Agents in a Windows cluster.
- 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 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**.

   Note: 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**.

2.1.1 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.

2.2 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.

Note: 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.

Note: 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**.

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

     Note: 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**.

2.3 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 kit in silent mode.

Important: Windows Agent 8.70 and later versions can be upgraded automatically. When a new installer is available in Portal, the agent will download the installer and upgrade 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.

Notes:

- 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.
- 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:

```
installKitName /s /v"/qn [parameters] [featureParameters]" [/l"language"]
```

Where:

- *installKitName* is the name of the Windows Agent installation kit: Agent-Windows-x64-*x-xx-xxxx*.exe for 64-bit systems or Agent-Windows-*x-xx-xxxx*.exe for 32-bit systems. *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"

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.	

Parameter	Description	Default Value
REGISTERWITHWEBCC	Turns on/off registration of the Agent with Portal.	False
AMPNWADDRESS	If REGISTERWITHWEBCC is True, this field is required.	
AMPPASSWORD	If REGISTERWITHWEBCC is True, this field is required.	
AMPPORT		8086
AMPUSERNAME	If REGISTERWITHWEBCC is True, this field is required.	
EXTRACTMSI	Turns on/off extraction of the Microsoft Installer (MSI) package.	False
INTEGRATEDENCRYPTION	Specifies whether to use the optimized AES 256 data encryption method that is integrated with the Agent, or use an external encryption library. Available values are: • On – the Agent uses the internal, optimized AES 256 data encryption method • Off – the Agent uses the external encryption library *Note:* The data encryption method is used for data at rest. *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.	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.	

Windows Agent feature parameters

Feature Parameter	Description	Default Value
FEATURECLUSTER={On|Off}	Turns on/off installation of the Cluster Plug-in.	Off

Feature Parameter	Description	Default Value
`FEATUREEXCHANGE= {On|Off}`	Turns on/off installation of the Exchange Plug-in (Legacy). *Note:* In previous versions, this plug-in was called the Exchange 2007 DR Plug-in. This plug-in is for use with Exchange 2007 only. Only available with the 64-bit Windows Agent.	Off
`FEATUREEXCHANGE2010= {On|Off}`	Turns on/off installation of the Exchange Plug-in. *Note:* In previous versions, this plug-in was called the Exchange 2010/2013/2016 DR Plug-in. Only available with the 64-bit Windows Agent.	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. Only available with the 64-bit Windows Agent. *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 64-bit Agent in a different directory, run the following command:

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

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

To install the French version of the 32-bit Agent, run the following command:

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

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

To install the 64-bit Agent and register it with Portal, run a command similar to this:

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

To install the 64-bit Agent and the SQL Server Plug-in:

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

2.4 Windows Agent default ports

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

Agent Port	Communication	Protocol
Outbound: 8086, 8087	To Portal	TCP
Outbound: 2546	To vault	TCP
Outbound: 2548, 8031	To Windows CentralControl	TCP

2.5 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**.

2.6 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:

```
installKitName /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:

```
installKitName /s /x /v"/qn TOTALUNINSTALL=False"
```

installKitName is the name of the Windows Agent installation kit: Agent-Windows-x64-*x-xx-xxxx*.exe for 64-bit systems or Agent-Windows-*x-xx-xxxx*.exe for 32-bit systems. *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.

To protect a Windows cluster:

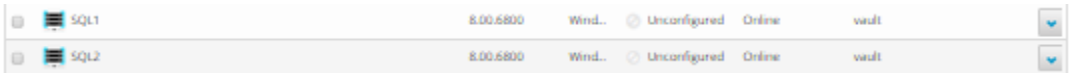
1. On each node in the Windows cluster, install the Windows Agent and the following plug-ins:
   - Cluster Support Plug-in
   - Image Plug-in (recommended)
   - SQL Server Plug-in (required for point-in-time database protection in a SQL Server cluster)

   See Install the Windows Agent and Plug-ins.

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

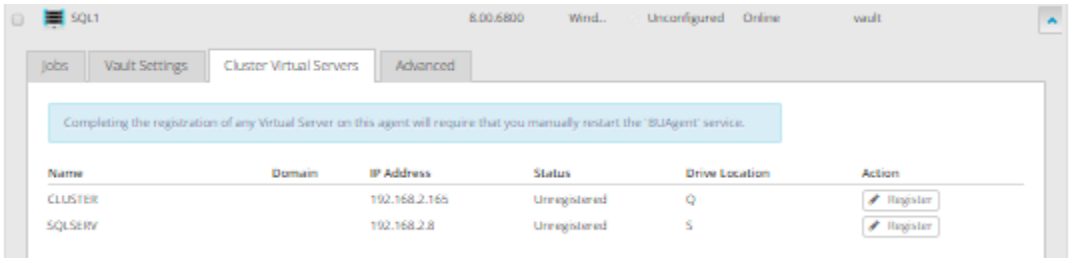
   We recommend specifying the Portal host name when you register an agent to Portal. If the Portal IP address changes in the future, DNS can handle the change and you will not have to manually register the agent to Portal again.
2. Sign in to Portal using the credentials that you used in Step 1.
3. In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

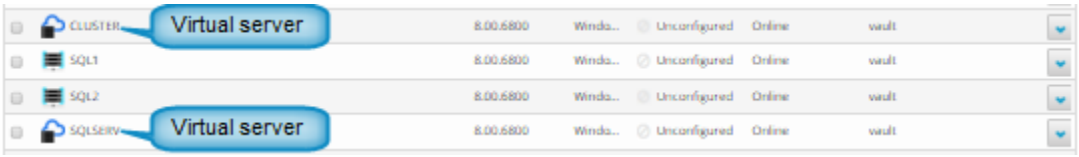


6. Click **Register** for the cluster core and for each role that you want to protect.

   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.

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 Agent 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 an Agent can back up data to or restore data from a vault, vault settings must be added for the Agent. 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 an Agent, 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 an Agent, 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 an Agent, Admin users can select any vault profile in the site. Regular users can only select vault profiles that are assigned to them.

In previous Portal versions, you could specify whether data is encrypted using AES encryption when it is transmitted to and from the vault. Over-the-wire encryption is now automatically enabled when you add vault settings or save existing vault settings.

When an E2 appliance reports a new IP address, the IP address is updated in Portal vault settings for Agents that are registered to the E2, and in the E2 vault profile. Agent versions 8.10 and later contact Portal to check for vault IP address changes. If a Super user or Admin user changes the name of an E2 vault profile, the name is updated automatically in vault settings for Agents that are registered to the E2.

To add vault settings:

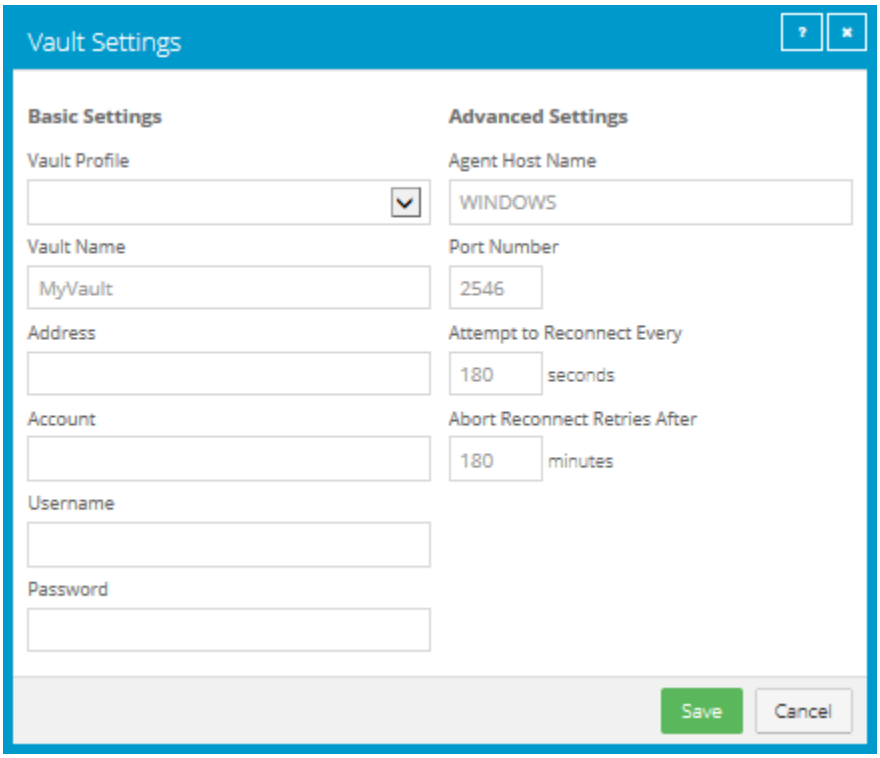
1. On the navigation bar, click **Computers**.

2. Find the Agent 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.
- **Abort Reconnect Retries After**. Specifies the number of times the Agent tries to reconnect to the vault, if the vault becomes unavailable during a backup or restore. If the Agent cannot connect to the vault successfully in the specified number of tries, the backup or restore fails.

6. Click **Save**.

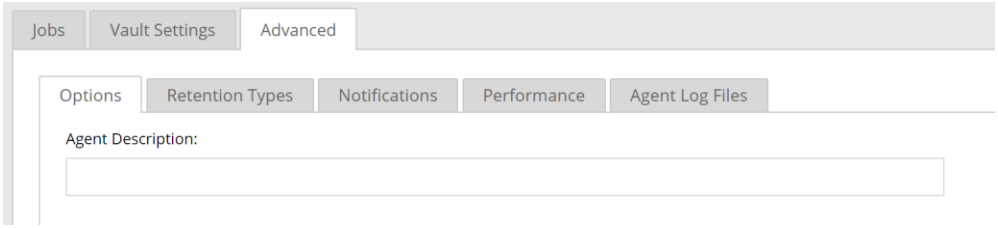
4.2 Add a description

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

To add a description:

1. On the navigation bar, click **Computers**.
2. Find the Agent 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 Agent.



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 an Agent where a policy is not assigned.

If a policy is assigned to an Agent, retention types cannot be added or modified on the Computers page. Instead, retention types can only be added or modified in the policy. See the Portal online help.

To add a retention type:

1. On the navigation bar, click **Computers**.
2. Find the Agent for which you want to add a retention type, and click the row to expand its view.

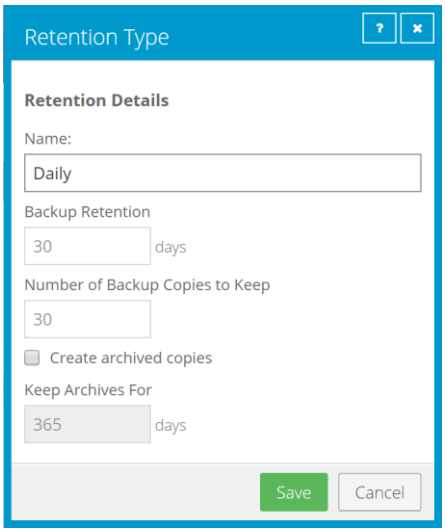
If the Configure Manually box appears, click **Configure Manually**. The Configure Manually box appears for some computers where a backup job has not been created.

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

   If a policy is assigned to the Agent, 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	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 throttling values are set at the computer (Agent) level, and apply to both backups and restores. If three jobs are running at the same time on the same computer, each job gets 1/3 of the specified maximum bandwidth.

Bandwidth settings include:

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

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

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

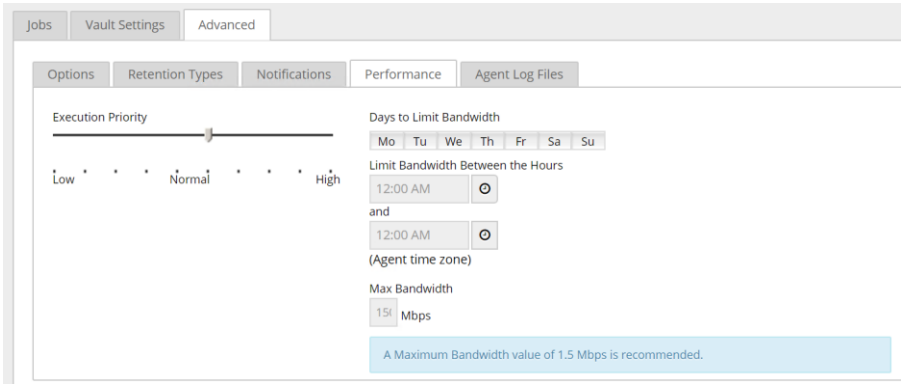
If a policy is assigned to a computer, bandwidth throttling settings cannot be modified on the Computers page. Instead, settings can only be added or modified in the policy. See the Portal online help.

To configure bandwidth throttling:

1. On the navigation bar, click **Computers**.
2. Find the Agent 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 Agent or protected environment, you cannot add or change values on the **Performance** tab. Instead, bandwidth settings can only be modified in the policy.



5 Add and manage Windows backup jobs

After a Windows computer is added in Portal, 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.

In a Windows backup job, you can select:

- Specific folders and files to back up
- 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.
- 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.

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.

5.1 Add a Windows 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.

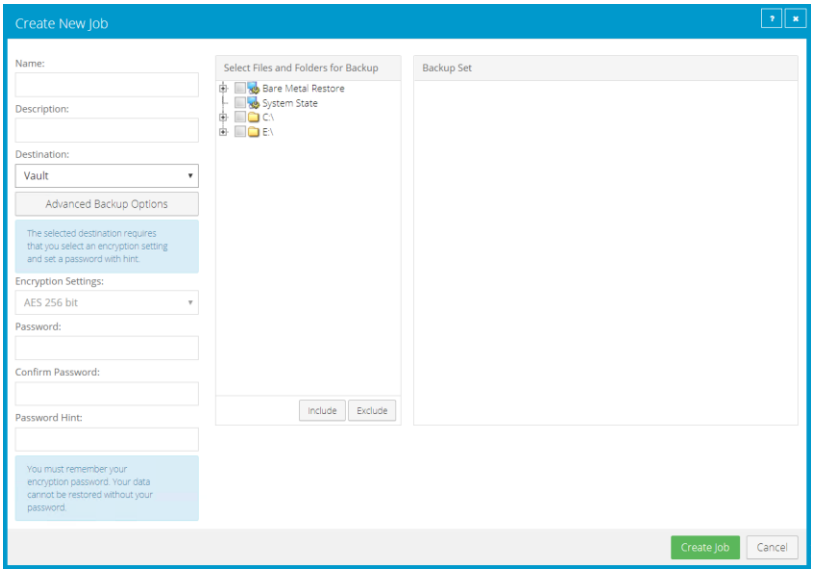
4. In the **Select Job Task** menu, click **Create New Local System Job**.

5. In the **Create New Job** dialog box, specify the following information:

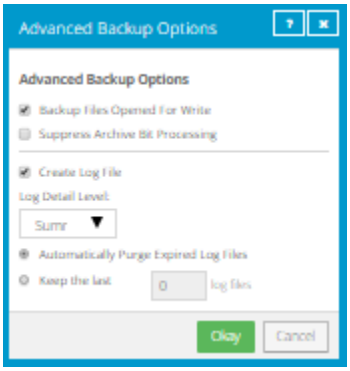
   - In the **Name** box, type a name for the backup job.
   - In the **Description** box, optionally type a description for the backup job.
   - In the **Destination** list, select the vault where you want to save the backup data.

     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 system files so that you can restore the system to its state at the time of the backup, select **System State**.
   - To back up volumes that are needed to boot up the system after a system recovery, select **Bare Metal Restore**.

     Note: 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.

- 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.

Click **Apply Now** to consolidate and simplify records in the **Backup Set** box, if changes need to be applied.

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

8. 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.

5.2 Add the first backup job for a Windows computer

Portal can automatically create a backup job for a Windows computer that does not have a backup job.

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 you can automatically create a backup job.

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.

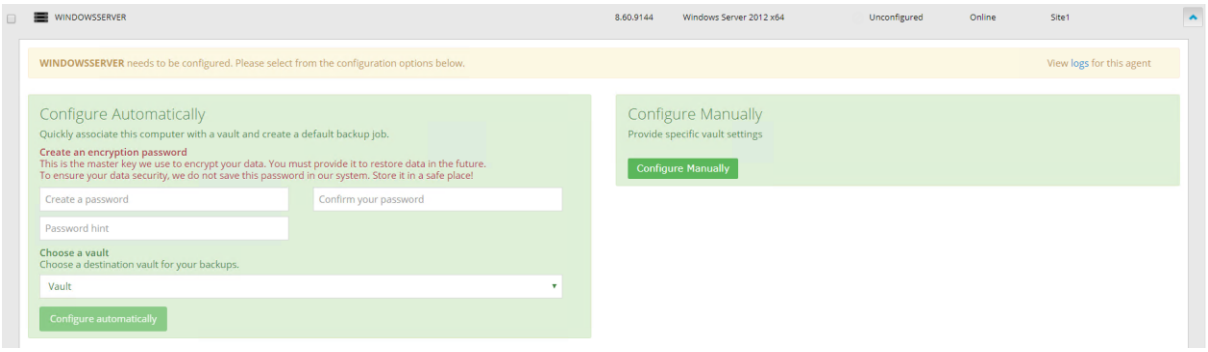
To add the first backup job for a Windows computer:

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 backup job has not been created for the computer, the Configure Manually box appears. If a backup job has not been created for the computer and at least one vault profile is available, the Configure Automatically box also appears.



3. Do one of the following:

   - To create a backup job manually, click **Configure Manually**. See Add a Windows backup job.
   - To automatically create a backup job for the computer, do the following:

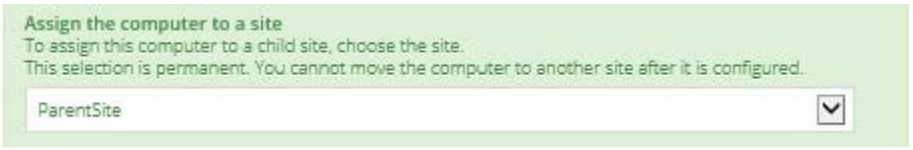
     i. In the **Create a password** and **Confirm your password** boxes, enter an encryption password.

     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.

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

     iii. 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.

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

     v. Click **Configure automatically**.

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

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

     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.

5.3 Add a UNC file backup job

After adding a Windows computer in Portal, 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.

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.

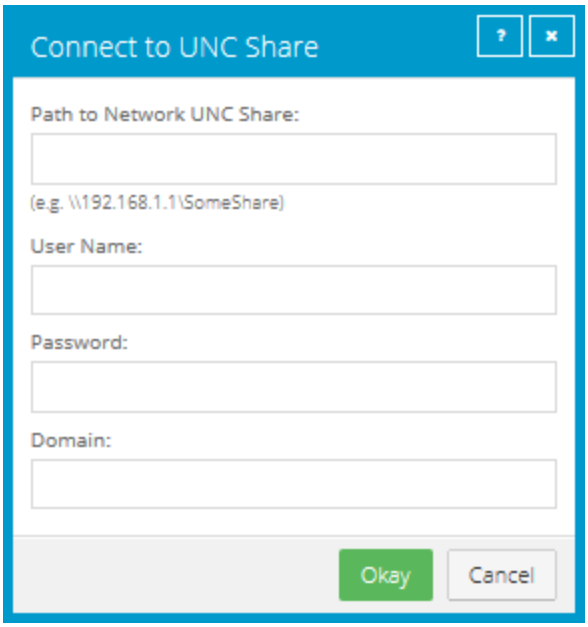
3. Click the **Jobs** tab.

   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.



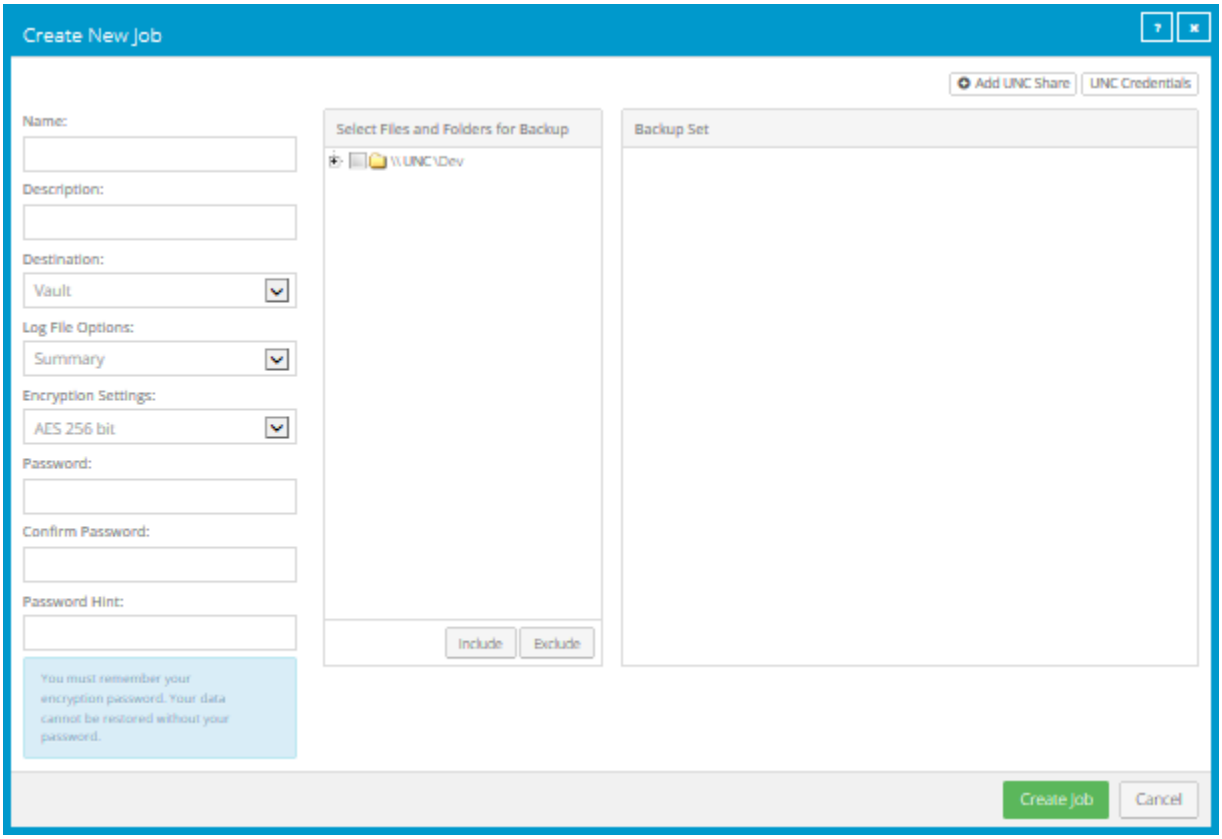
6. Click **Okay**.

   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.

   Click **Apply Now** to consolidate and simplify records in the **Backup Set** box, if changes need to be applied.

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.

5.3.1 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.

The following log file options are also available for some jobs:

- **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.

5.3.2 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.

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.

5.3.3 Advanced backup options

When you create or edit a 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.

5.3.4 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.
   - 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.
   - To back up the specified folder, but not its subdirectories, clear the **Recursive** check box.
   - To back up the folder’s subdirectories, select the **Recursive** check box.
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.

- 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. 

- 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 **Apply Now** to consolidate and simplify records in the **Backup Set** box, if changes need to be applied.

6. Click **Create Job** or **Save**.

5.4 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	Quorum disk	Image or local system job that backs up the

	the cluster core		quorum disk. See the *Image Plug-in Guide* 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 the *Image Plug-in Guide* 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 the *Image Plug-in Guide* 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 the *SQL Server Plug-in Guide.*

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

5.5 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.

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. Click **Save**.

6 Delete backup jobs and delete data from vaults

Regular users and Admin users can delete backup jobs from Portal without deleting the job data from vaults. See Delete a backup job without deleting data from vaults.

In a Portal instance where the data deletion feature is enabled, Admin users can delete backup jobs from Portal and submit requests to delete the job data from associated vaults. See Delete a backup job and delete job data from vaults. During the 72-hour waiting period before job data is deleted, Admin users can cancel scheduled data deletions in their sites. See Cancel a scheduled data deletion.

6.1 Delete a backup job without deleting data from vaults

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

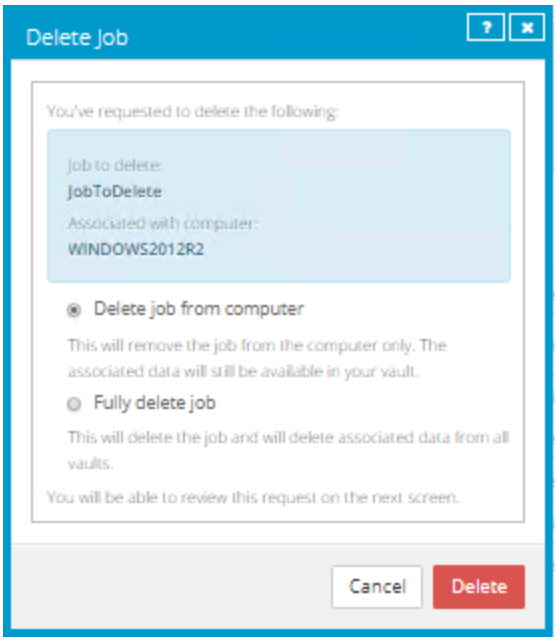
In a Portal instance where the data deletion feature is enabled, Admin users can also submit requests to delete job data from vaults when they delete jobs from Portal. See Delete a backup job and delete job data from vaults.

To delete a backup job:

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

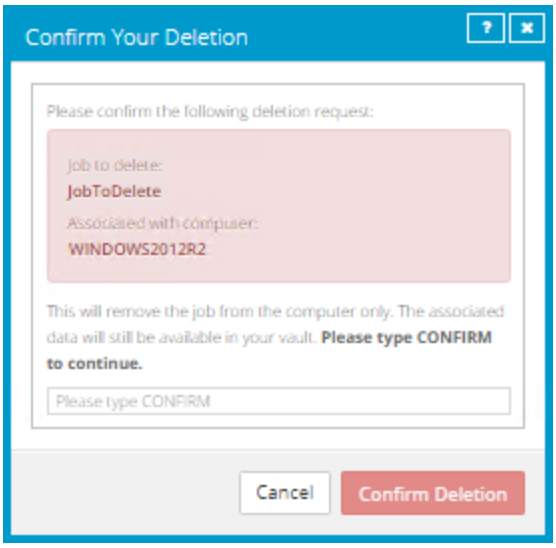
   The Computers page shows registered computers.
2. Find the Agent with the job that you want to delete, and expand its view by clicking its row.
3. Click the **Jobs** tab.
4. In the **Select Action** menu of the job that you want to delete, click **Delete Job**.
5. If you are signed in as an Admin user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

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



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

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



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

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

7. Click **Confirm Deletion**.

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 should be deleted from all vaults. The data deletion is scheduled for 72 hours after a request is made and an email notification is sent to Super users and Admin users for the site.

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

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

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

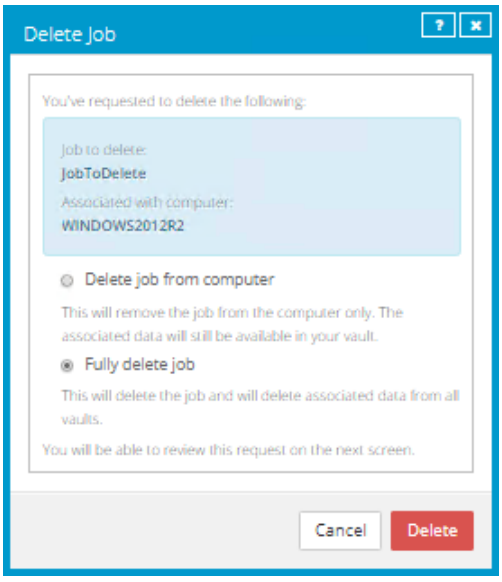
To delete a backup job and delete job data from vaults:

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

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

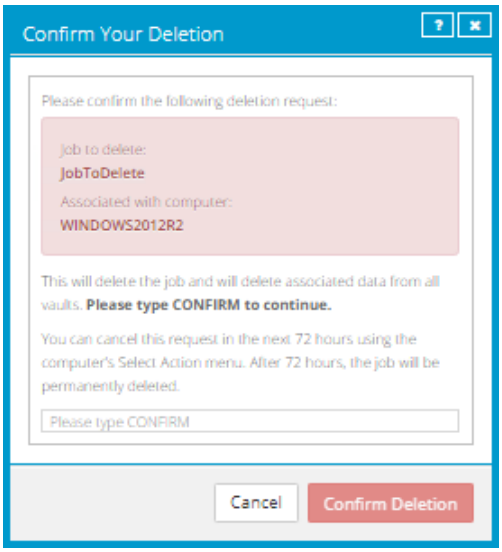
   A Delete Job dialog box appears if your Portal instance supports data deletion.

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



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

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

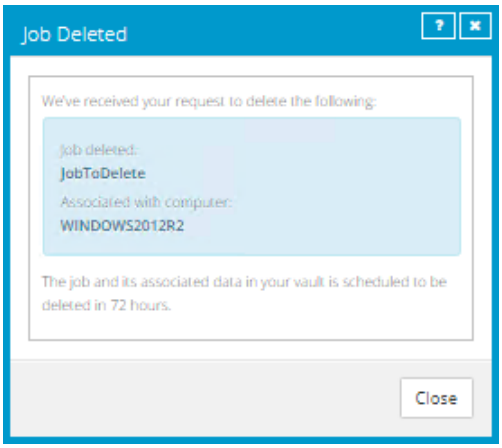


6. In the text box, type **CONFIRM.**

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

7. Click **Confirm Deletion**.

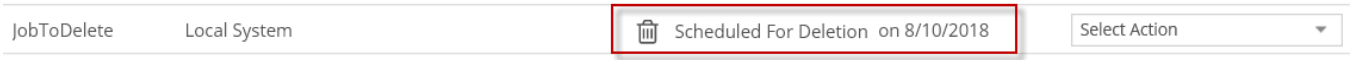
   A Job Deleted dialog box states that the job and its associated data in your vault is scheduled to be deleted.



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.

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



6.3 Cancel a scheduled data deletion

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

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

To cancel a scheduled data deletion:

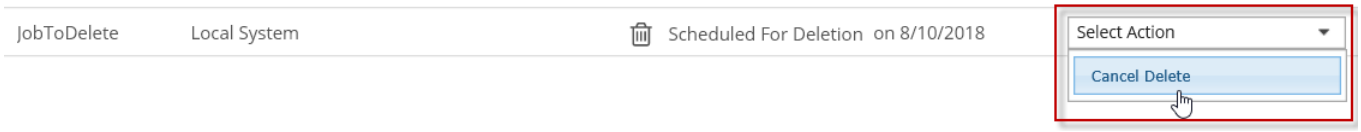
1. When signed in as an Admin user, click **Computers** on the navigation bar.

   The Computers page shows registered computers.

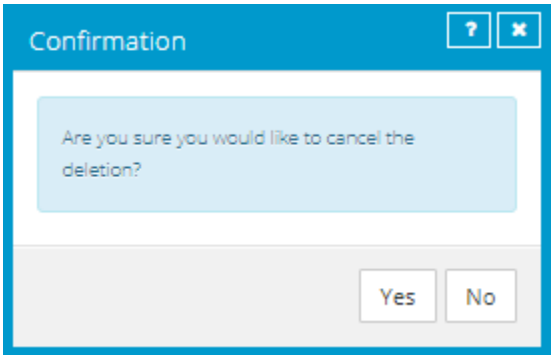
2. Find the Agent with scheduled data deletion that you want to cancel, and expand its view by clicking its row.

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 revert to the values that appeared before the job was scheduled for deletion.

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

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.

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

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

  When the job runs again, the Agent checks for changes in data that was previously backed up, backs up those changes, and then backs up the remaining data.

  If a backup job is deferred while an item (e.g., file) 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.

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

For computers with Windows or Linux Agent version 8.60 or later, you can specify whether scheduled backups should automatically retry if they do not run successfully. You can also specify how many times a scheduled backup should retry after a failed attempt, and specify the amount of time between retries. See Specify whether scheduled backups retry after a failure.

When you schedule a job to run, you can also set the compression level for the data. The compression level optimizes the volume of data sent to the vault against the speed of processing. The default compression level is usually the optimal setting.

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

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

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

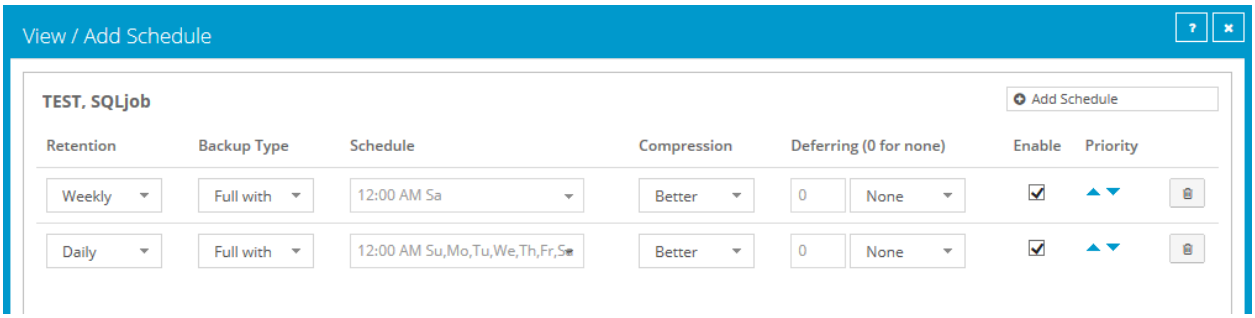
7.1 Schedule a backup

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

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

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

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



To schedule a backup:

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

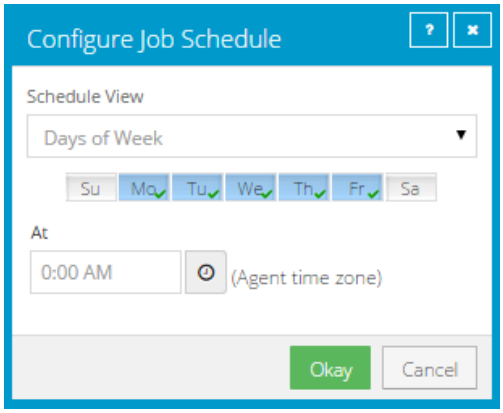
   A new row appears in the dialog box.
3. In the new schedule row, in the **Retention** list, click a retention type.

   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.
4. In the **Schedule** box, click the arrow.

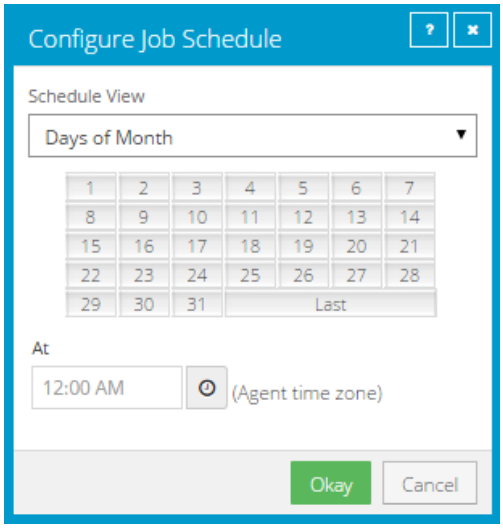
   The **Configure Job Schedule** dialog box opens.

5. In the **Configure Job Schedule** dialog box, do one of the following:

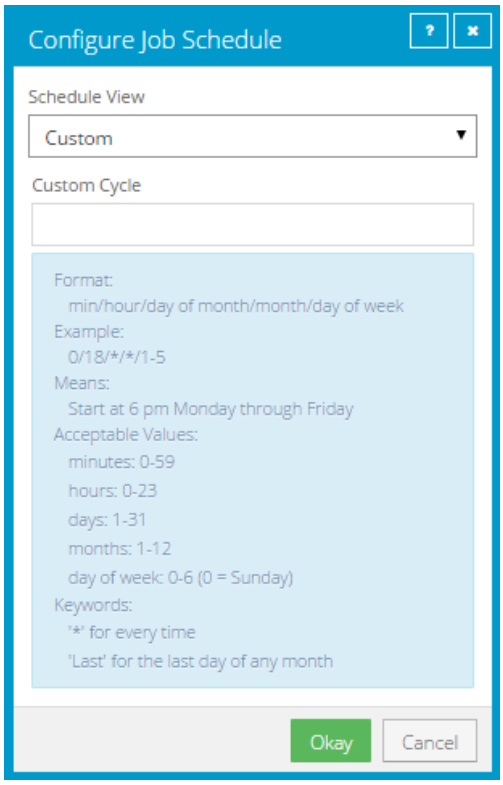
   - To run the backup on specific days each week, select **Days of Week** in the **Schedule View** list. Select the days when you want to run the job. Then use the **At** field to specify the time when you want to run the job.



   - 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.



6. Click **Okay**.

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

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

8. Do one of the following:

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

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

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

10. If 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.

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

7.2 Specify whether scheduled backups retry after a failure

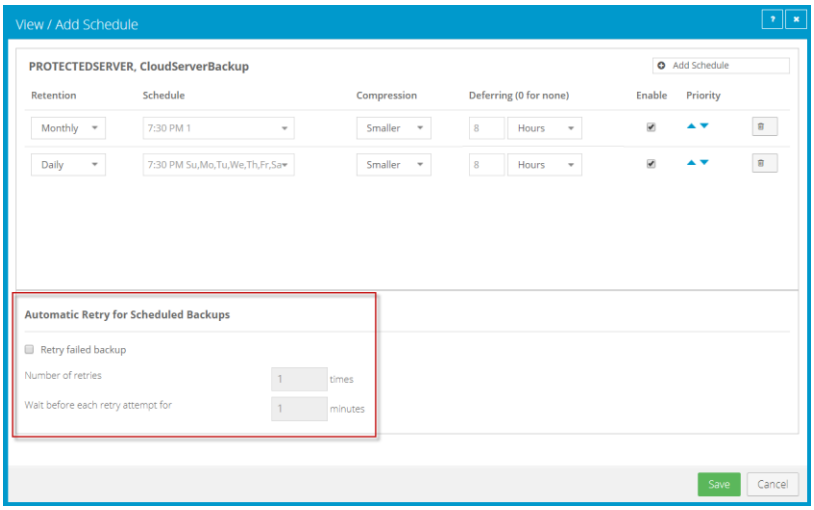
You can specify whether scheduled backups automatically retry if they do not run successfully.

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

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

To specify whether scheduled backups retry after a failure:

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



3. Click **Save**.

7.3 Run an ad-hoc backup

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

To run an ad-hoc backup:

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

   A grid lists available computers.

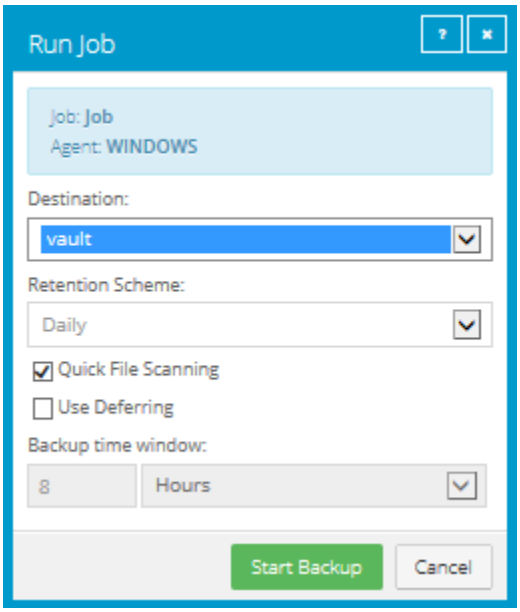
2. Find the computer with the backup job that you want to run, and expand its view by clicking the computer row.

3. Click the **Jobs** tab.

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

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

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



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

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

6. If the **Quick File Scanning** option is available, and you want to enable it, 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.

7. Do one of the following:
   - To allow the backup job to run without a time limit, clear the **Use Deferring** check box.
   - To specify a maximum amount of time that the backup job can run, select the **Use Deferring** check box. From the **Backup time window** list, select **Minutes** or **Hours**. In the adjacent box, type the maximum number of minutes or hours that the job can run.

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

   Note: The **Use Deferring** check box is not available if you are backing up data to SSI (safeset image) files on disk.
8. 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.
9. If you want to stop the backup, click **Stop**.
10. To close the **Process Details** dialog box, click **Close**.

7.4 Synchronize a job

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

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

- Before running backup jobs on reregistered computers. You must also enter the encryption passwords for the computer's existing backup jobs. See Restore data to a replacement computer.
- 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 Restore Windows data

After backing up data from a Windows computer, you can:

- Restore Windows files and folders
- Restore files from multiple UNC jobs

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

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.

8.1 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**.

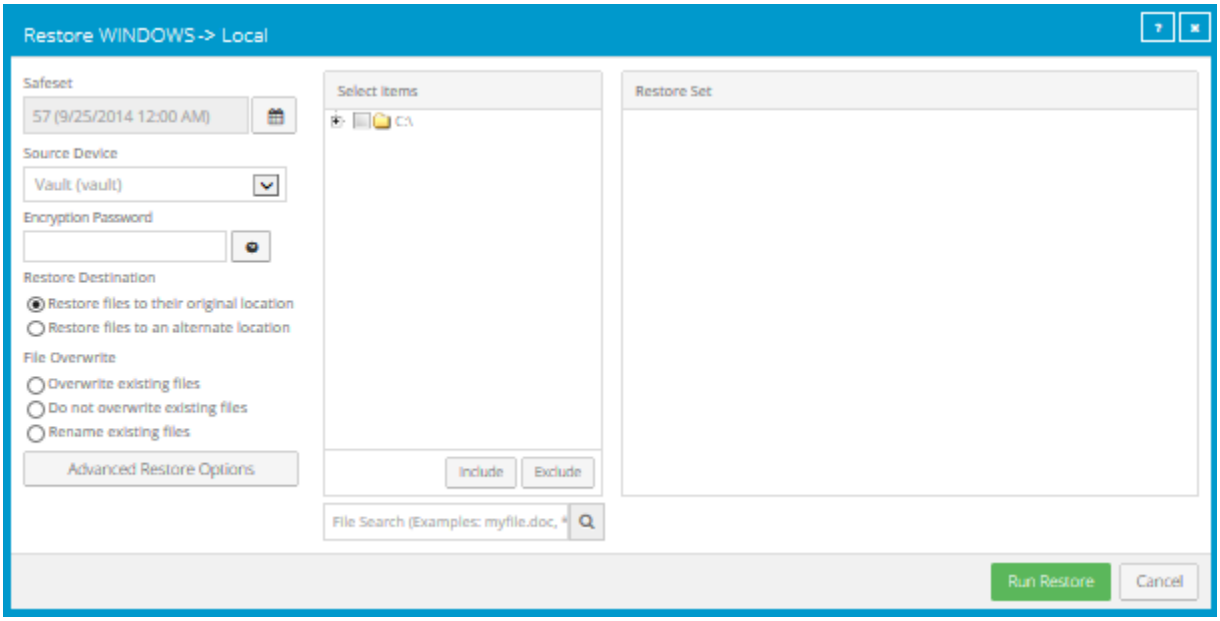
   A grid lists available computers.

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 shows the most recent safeset for the job.



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, 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 **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 an item (e.g., file, folder or symbolic link) to a location where there is an item with the same name.

   - To overwrite existing items with restored files, select **Overwrite existing files**.

     WARNING: Using Agent version 8.70, if you select **Overwrite existing files** and restore a file that has the same name as a folder in the restore location, the file will overwrite the folder and all of its contents.

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

   - To add a numeric extension (e.g., .0001) to a *restored* file name, select **Do not overwrite existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *restored* file name (e.g., “filename.txt.0001”).
   - To add a numeric extension (e.g., .0001) to an *existing* file name, select **Rename existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *existing* file name (e.g., “filename.txt.0001”). The name of the restored file continues to be “filename.txt”.

9. To change the 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.

    Click **Apply Now** to consolidate and simplify records in the **Restore Set** box, if changes need to be applied.
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.

8.1.1 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.

8.1.2 Restore a domain controller

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

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

8.2 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:

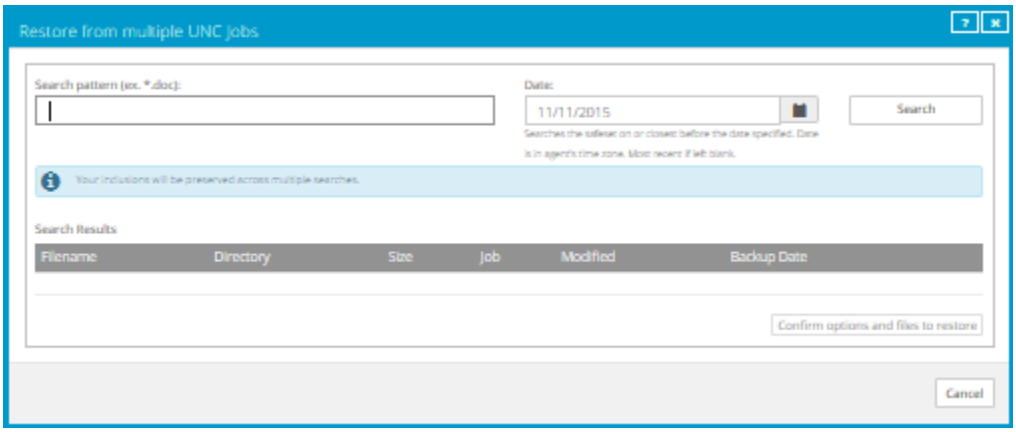
1. On the navigation bar, click **Computers**.

   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:

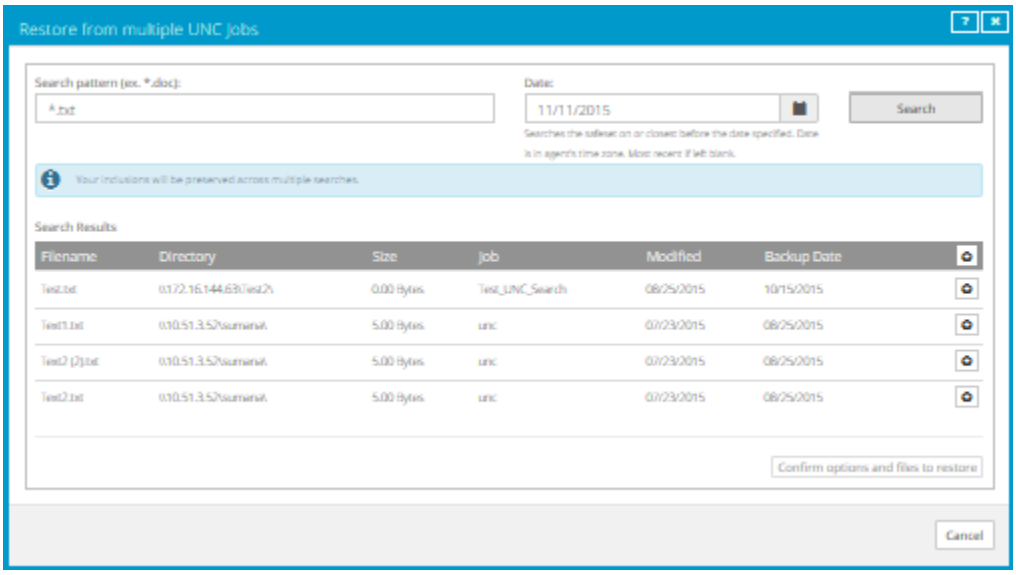
- To search for files in the most recent safeset for each UNC job, leave the **Date** box blank.
- To search for files in safesets with a specific date, click the calendar button. In the calendar that appears, click the date.

  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.

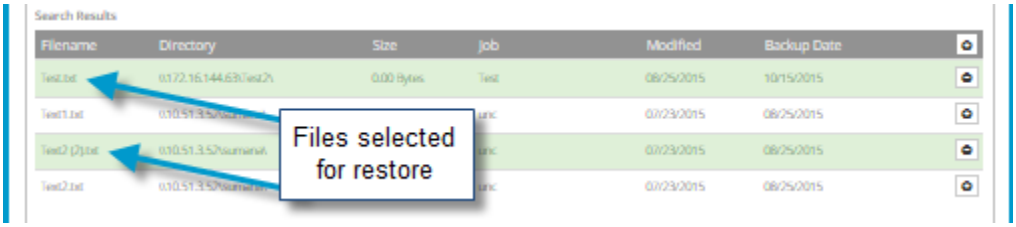
6. Click **Search**.

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



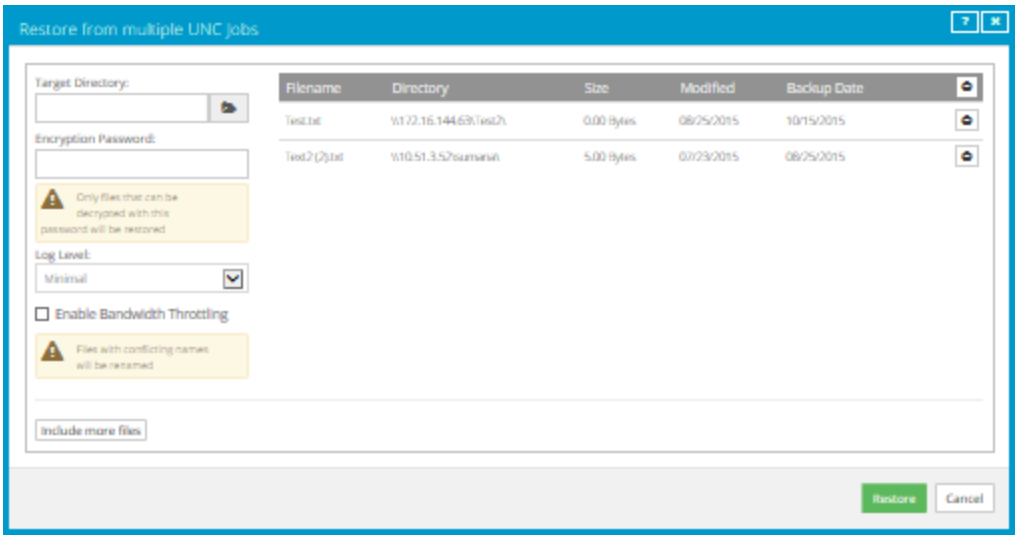
7. Do one of the following:
   - To restore specific files, click the **Include for restore** button for each file.
   - To restore all files in the list, click the **Include All** button at the top of the file list.

   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).

8.3 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 enter the encryption password for the computer's existing backup jobs and synchronize the jobs before they run successfully. See Synchronize a job.

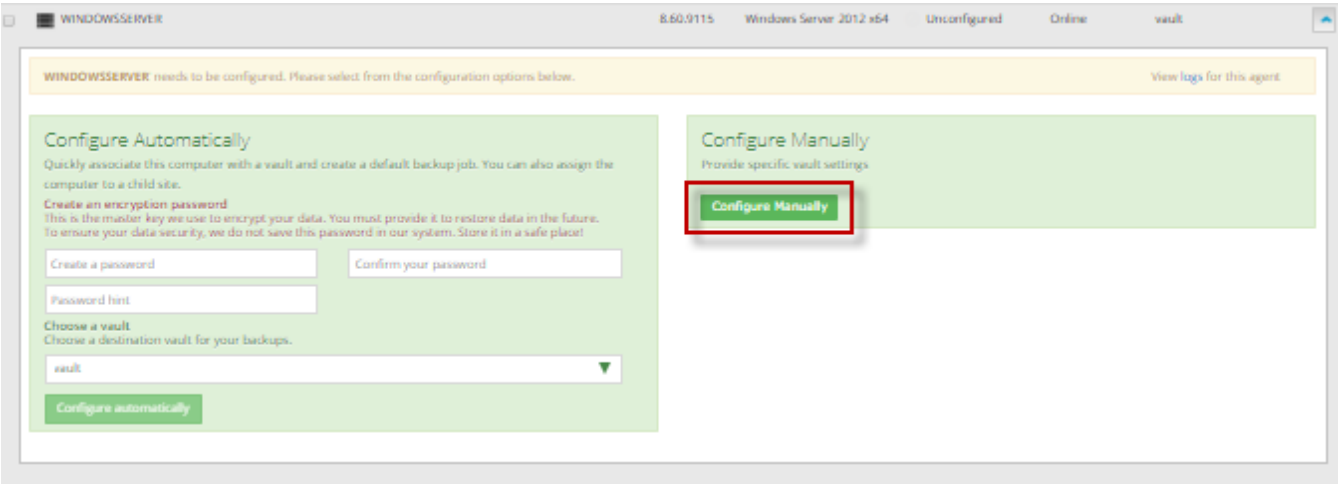
If you want to restore data to another computer without replacing the existing computer, you can restore data from another computer. See Restore data from another computer.

To restore data to a replacement computer:

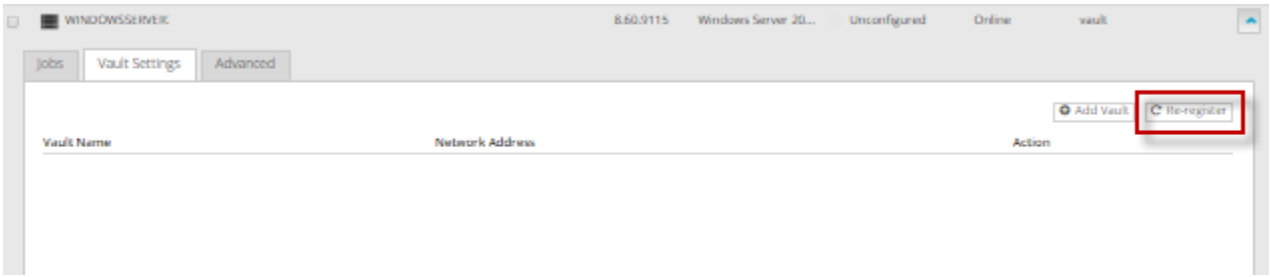
1. Download and install an Agent on the new or rebuilt computer.
2. On the navigation bar, click **Computers**.

   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.

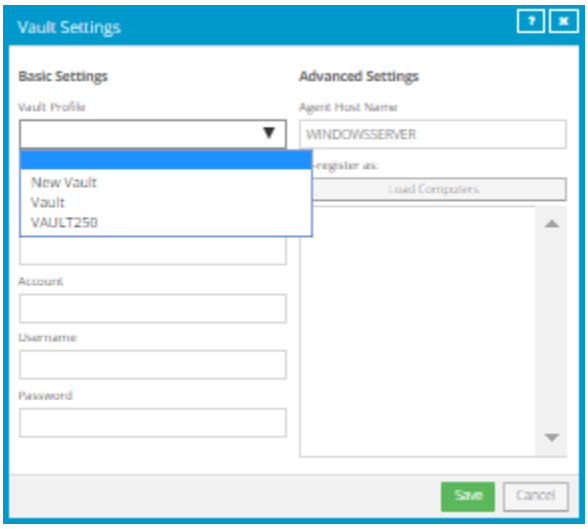
   If the following messages appear, a backup job has not been created for the computer. Click **Configure Manually**.



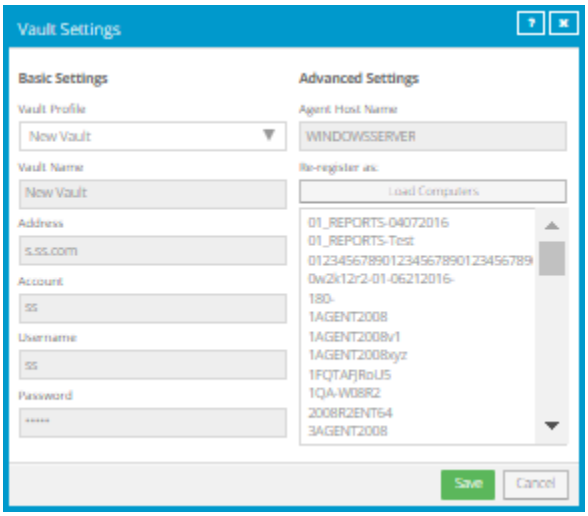
4. Click the **Vault Settings** tab.
5. Click **Re-register**.



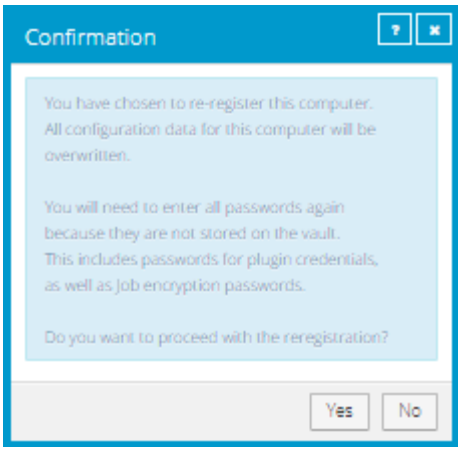
6. In the **Vault Settings** dialog box, in the **Vault Profile** list, select the vault where the backup from the original computer was stored.



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. After job information is downloaded, click the **Jobs** tab.
11. Find a job whose data you want to restore, and click **Restore** in the job's **Select Action** menu.

    During a restore, you must enter any passwords required for the job, including the encryption password. The remaining steps are the same as the steps for regular restores.

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

8.4 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.

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.

8.5 Advanced restore options

When restoring data, you can specify the following options:

Locked File Options

When restoring data from a local job, you can 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 from a local job, 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.

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.

Bandwidth throttling values are set at the computer (Agent) level, and apply to both backups and restores. If three jobs are running at the same time on the same computer, each job gets 1/3 of the specified maximum bandwidth.

Bandwidth settings include:

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

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

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

9 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.

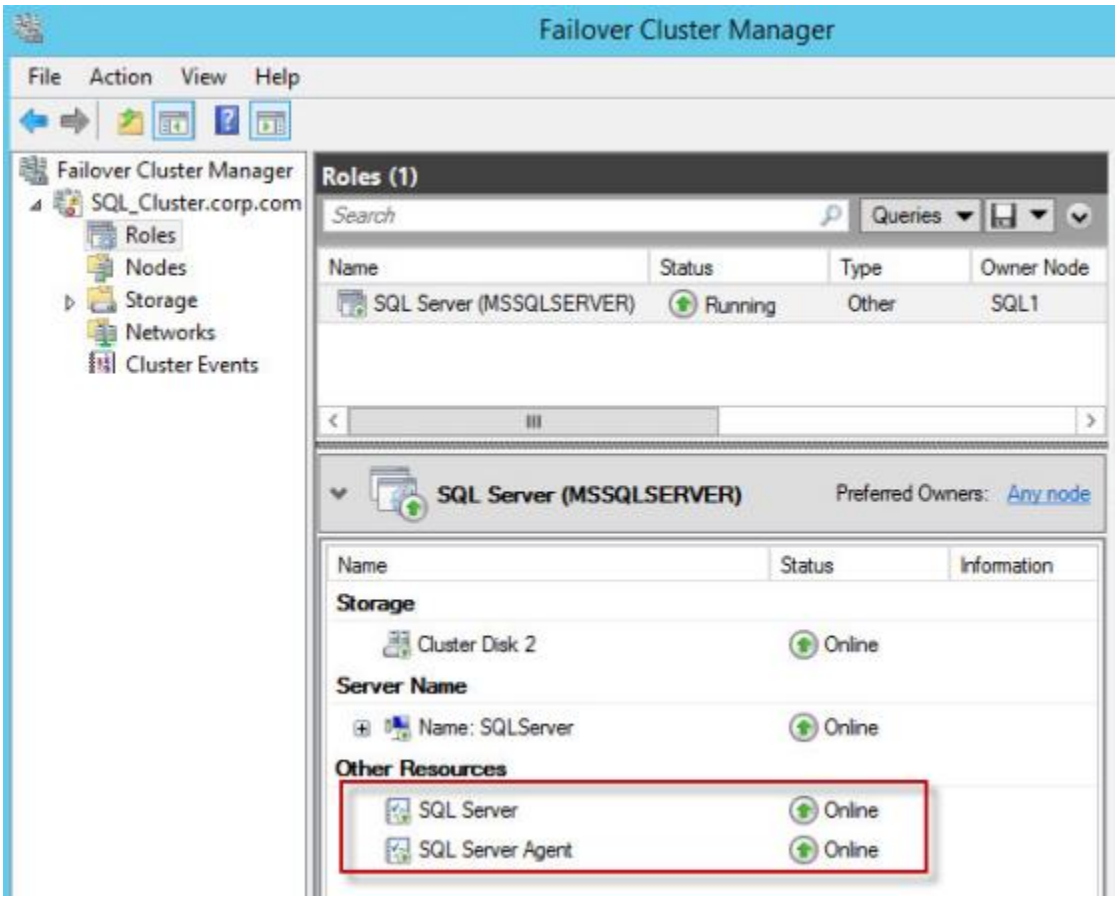
9.1 Recover volumes in a Windows cluster

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.

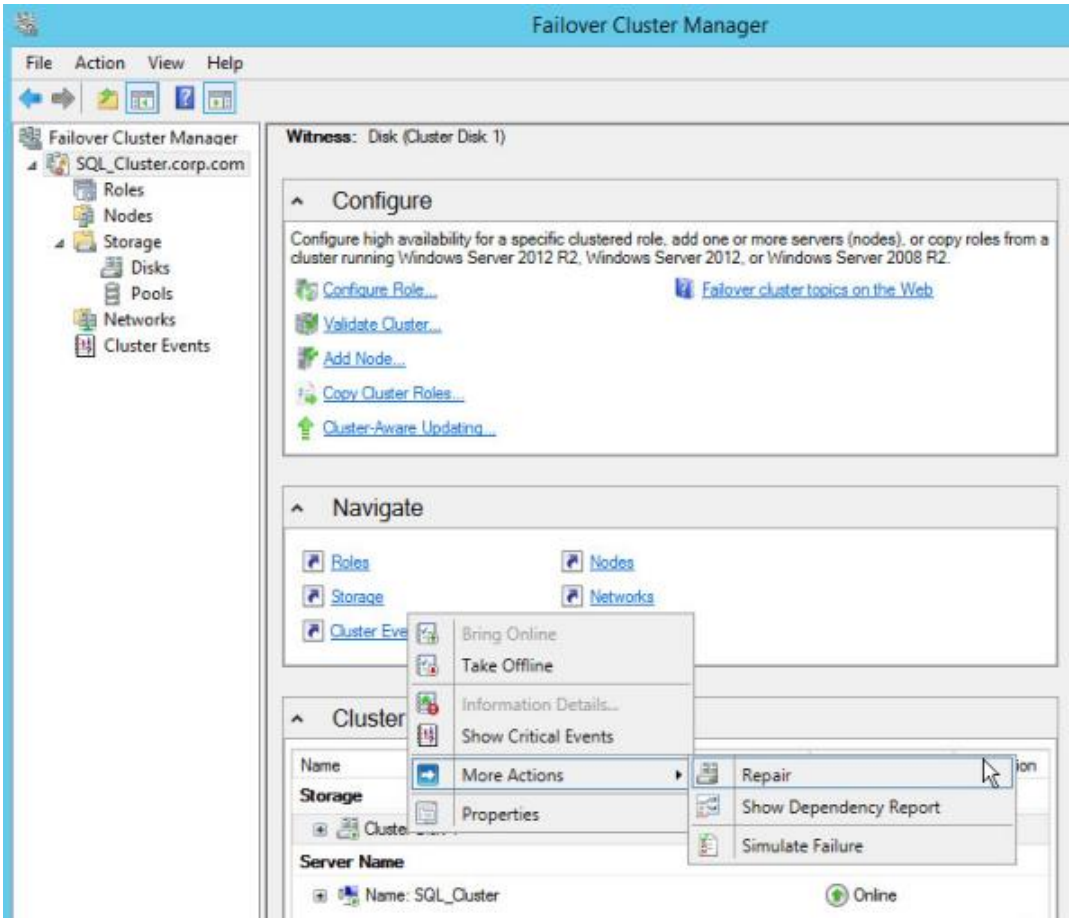
9.2 Recover the quorum disk in a Windows cluster

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).

9.3 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.

9.4 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.

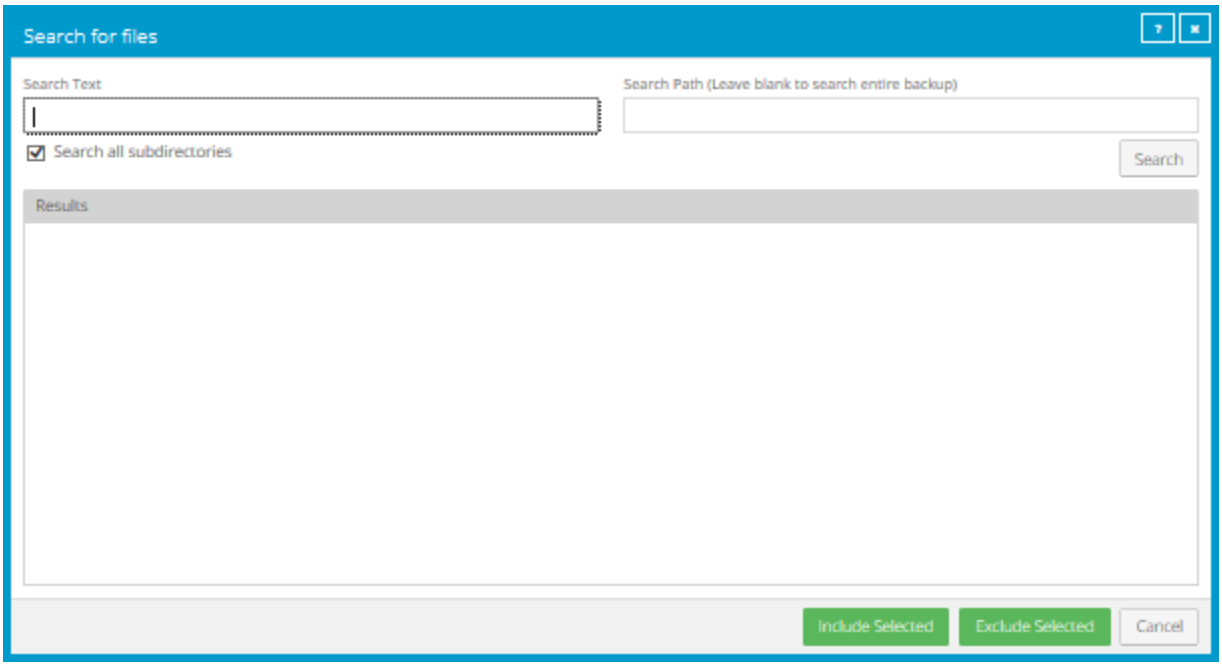
9.4.1 Search for files to restore

When you restore data from a backup job, 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**.

9.4.2 Filter subdirectories and files when restoring data

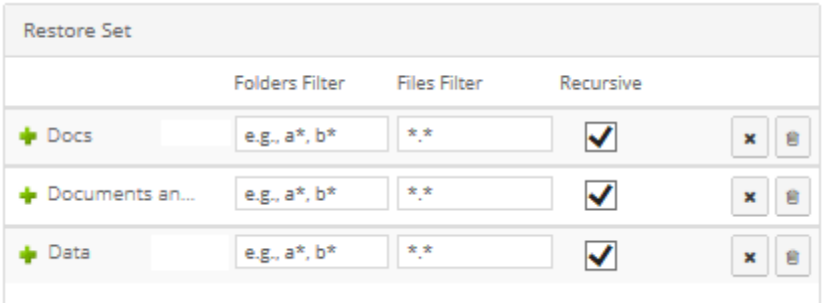
When you restore data from a backup job, you can specify folders and files to restore or not restore from the backup.

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 from a backup job, 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 **Apply Now** to consolidate and simplify records in the **Restore Set** box, if changes need to be applied.
6. Click **Run Restore**.

10 Monitor computers, jobs and processes

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

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

10.1 View computer and job status information

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

To view computer and job status information:

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

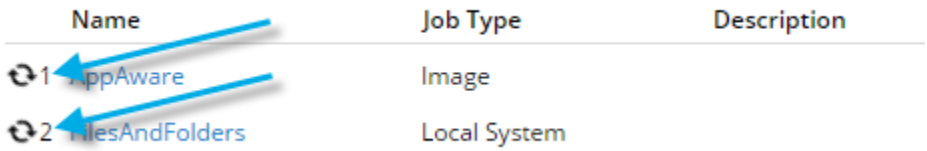
   The Computers page shows registered Agents.

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

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

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

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



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

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

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

  Deferring is used to prevent large backups from running at peak network times. When deferring is enabled, a backup job does not back up any new data after a specified amount of time.
- Never Run — Indicates that the backup job has never run.
- Missed — Indicates that the job has not run for 7 days.
- Completed with errors — Indicates that the backup completed and a safeset is available for restore, but problems occurred.
- Failed — Indicates that the backup failed and no safeset was created.
- Cancelled
- Scheduled for Deletion — Indicates that the job is scheduled to be deleted from Portal and job data is scheduled to be deleted from all vaults on the date shown in the Date column. This backup status is only possible in Portal instances where the data deletion feature is enabled.

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

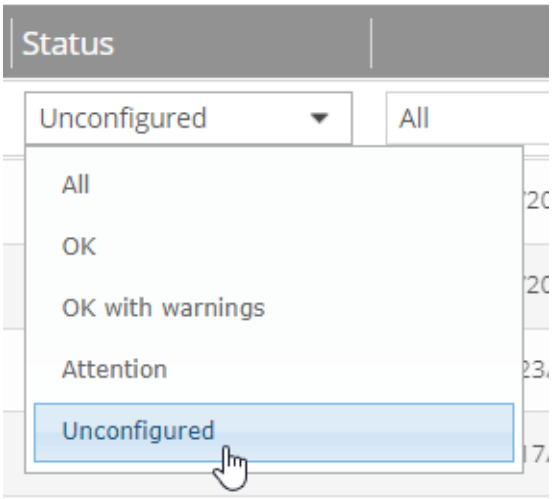
10.2 View an unconfigured computer's logs

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

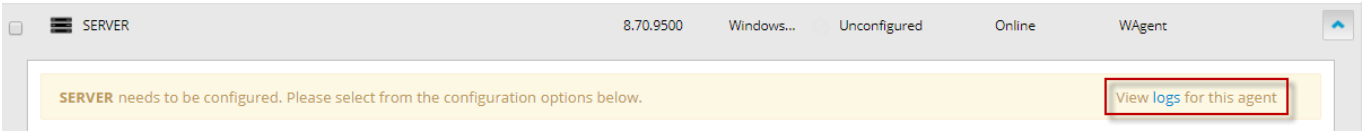
To view an unconfigured computer's logs:

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

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

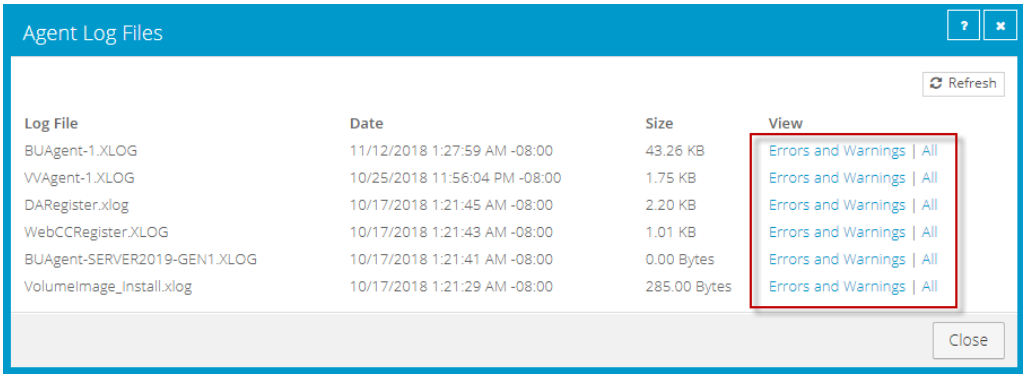


2. Find an unconfigured computer that is online, and expand its view by clicking the computer row.



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

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



4. Do one of the following:

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

- To view an entire log, click **All** for the log.

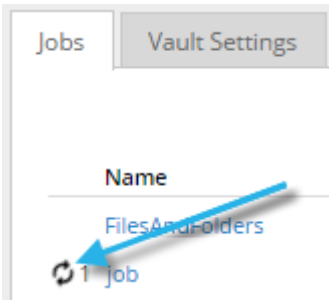
The log appears in a new browser tab.

10.3 View current process information for a job

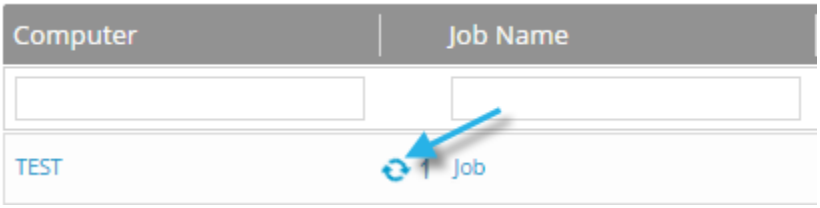
In the Process Details dialog box, you can view information about running, queued and recently-completed processes for a job. Processes include backups, restores and synchronizations. Process information is typically deleted within an hour after the process ends.

To view current process information for a job:

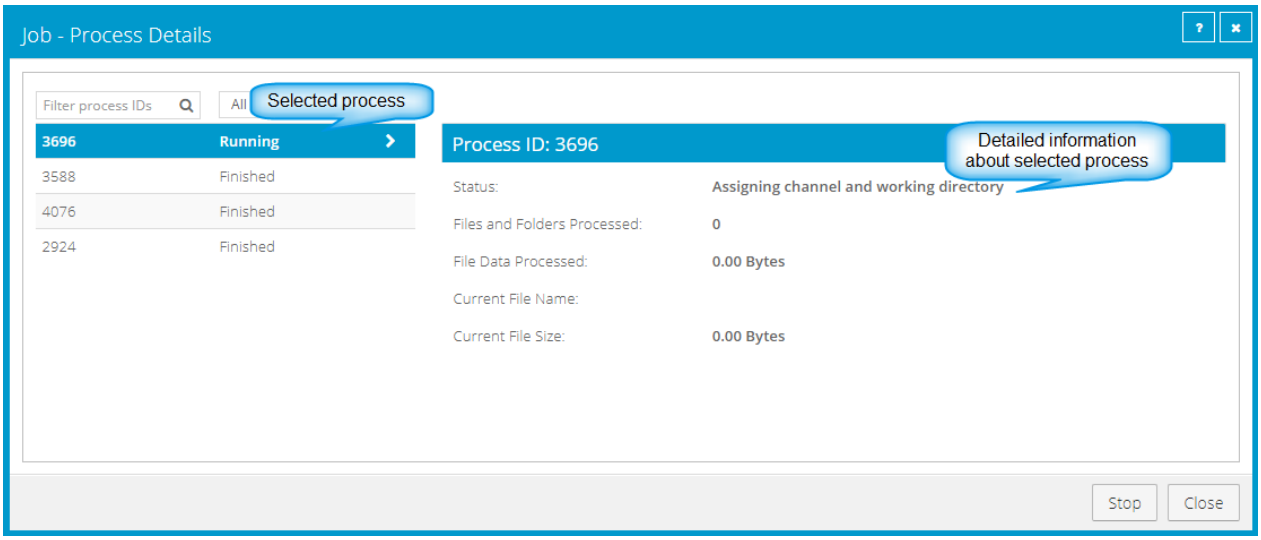
1. Do one of the following:
   - On the Computers page, on the Jobs tab, start a backup, restore or synchronization.
   - On the Computers page, on the Jobs tab, click the “In Progress” symbol beside the job name.



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



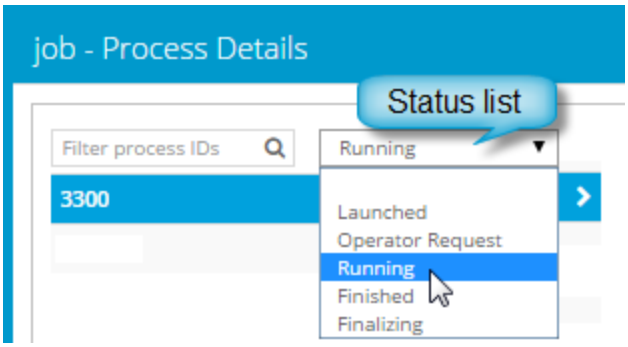
The **Process Details** dialog box lists processes that are running, queued and recently completed for the job. Detailed information is shown for the process that is selected on the left side of the dialog box.



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

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

3. To show only some processes in the dialog box, do one of the following in the status list:
   - To only show queued processes, click **Launched**.
   - To only show processes that are waiting for user action, click **Operator Request**.
   - To only show processes that are in progress, click **Running**.
   - To only show completed processes, click **Finished**.
   - To only show processes that are finishing, click **Finalizing**.



10.4 Monitor backups using email notifications

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

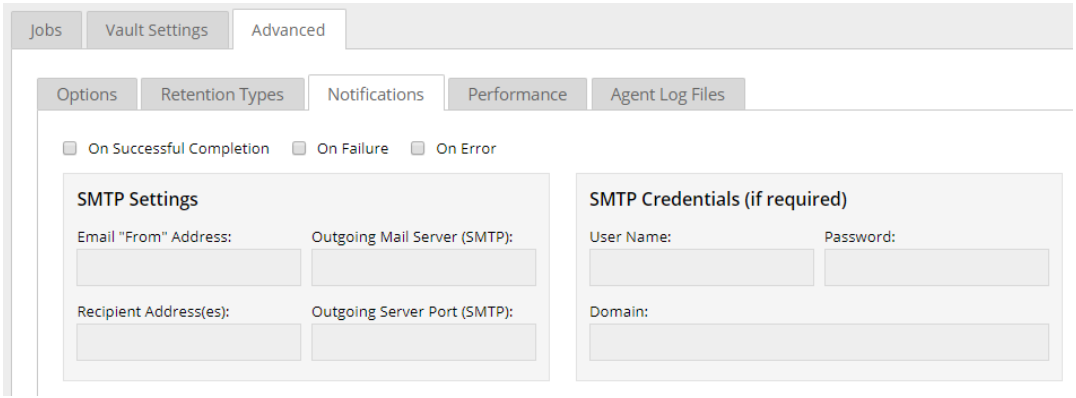
In some Portal instances, email notifications are configured centrally for Windows systems with Agent version 8.0 or later, instead of separately for each computer. See Set up email notifications for backups on multiple computers.

10.4.1 Set up email notifications for backups on a computer

To set up email notifications for a computer:

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

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



   Select one or more of the following checkboxes:

   - **On failure**. If selected, users receive an email notification when a backup or restore fails. If a backup fails, you cannot recover any files from the backup.

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

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

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

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

4. Click **Save**.

10.4.2 Set up email notifications for backups on multiple computers

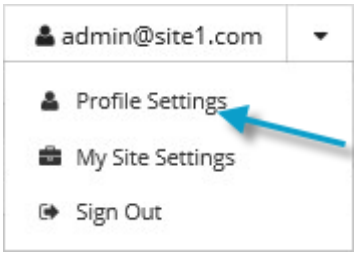
By default in some Portal instances, Admin users receive emails when backups fail, or are cancelled, deferred, missed or completed. Admin users can select backup statuses for which they want to receive email notifications. These email notifications are sent for Windows systems with Agent version 8.0 or later, instead of separately for each computer.

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

To set up email notifications for backups on multiple computers:

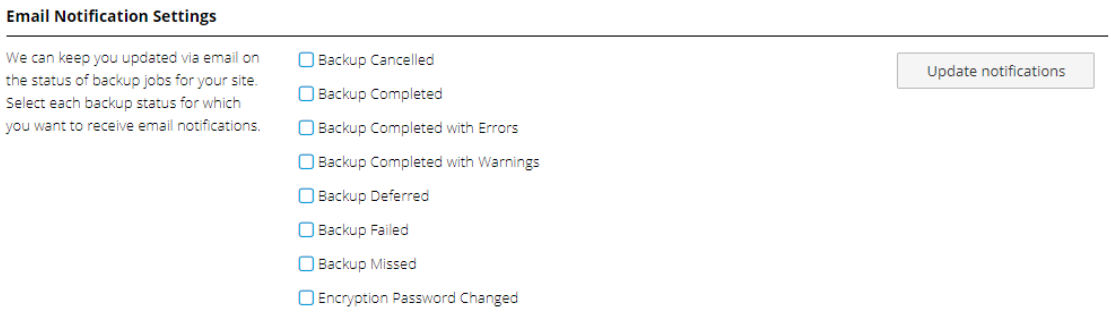
1. When signed in as an Admin user, click your email address at the top right of the Portal page.

   The user menu appears.



2. Click **Profile Settings**.

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



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

3. In the Email Notification Settings list, select any of the following events for which you want to receive emails:
   - Backup Cancelled
   - Backup Completed
   - Backup Completed with Errors
   - Backup Completed with Warnings
   - Backup Deferred
   - Backup Failed
   - Backup Missed
4. Click **Update notifications**.

10.5 View a job's process logs and safeset information

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

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

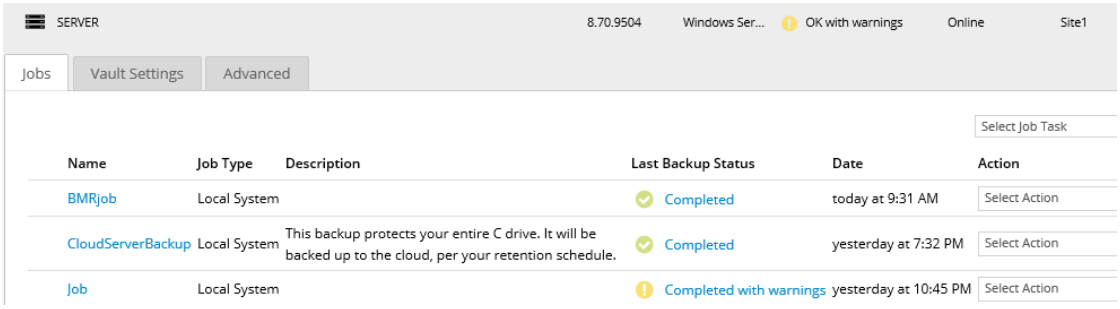
To view a job's process logs and safeset information:

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

   The Computers page shows registered Agents.

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

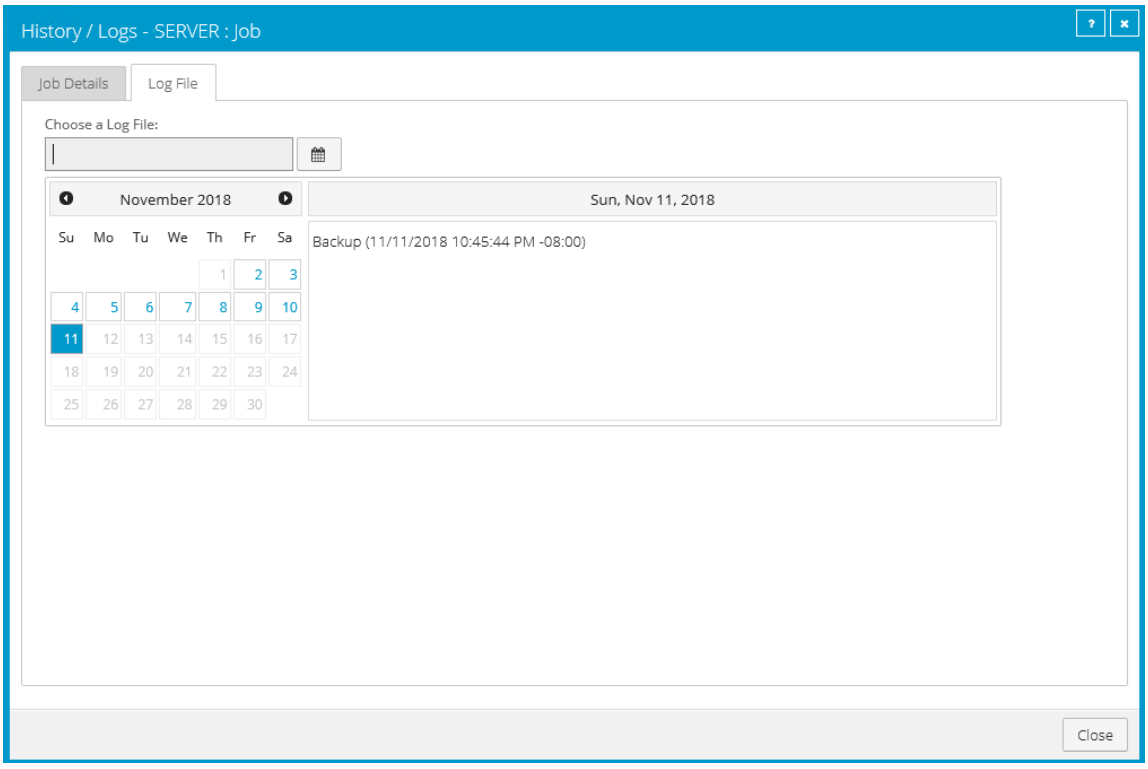
   On the **Jobs** tab, the **Last Backup Status** column shows the status of each backup job.



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

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

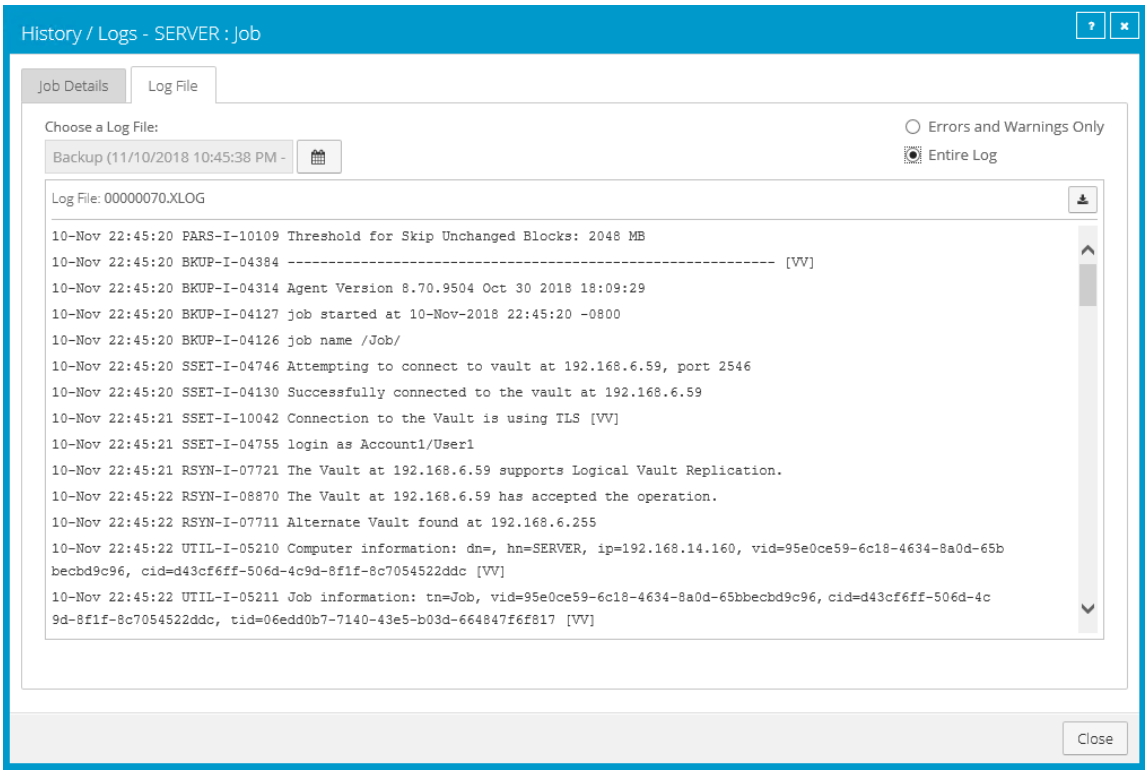
   The **History / Logs** window lists the most recent backups, restores and synchronizations on the computer.



4. To view processes for a different day, click the calendar button. In the calendar that appears, click the date of the log that you want to view.

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

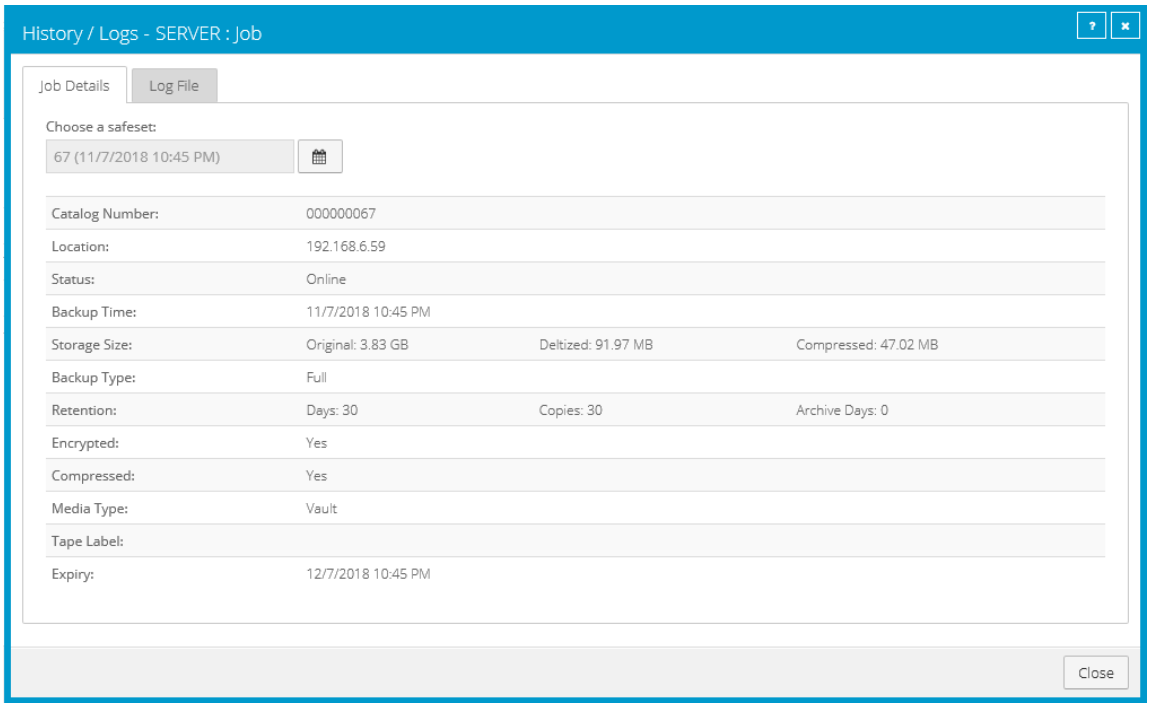
   The **History / Logs** window shows the selected log.



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.



10.6 View and export recent backup statuses

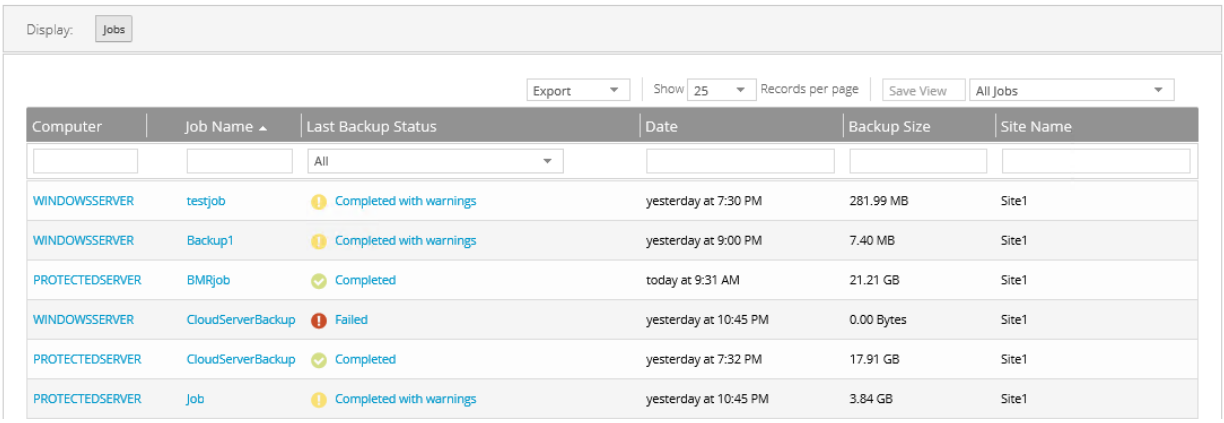
You can view recent backup statuses for computers on the Monitor page in Portal. You can also export the information in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format.

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

To view and export recent backup statuses:

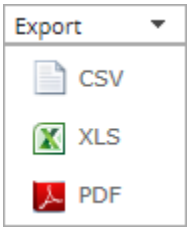
1. On the navigation bar, click **Monitor**.

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



2. To change which backup statuses appear on the page, click the views list at the top of the page, and then click the view that you want to apply.

3. To view information for a job or computer on the Computers page, click the name of an online computer or job.
4. To view the job's logs in the History/Logs window, click the job's last backup status.
5. To export backup status information from the page, click the **Export** box. In the list that appears, click one of the following formats for the exported data file:
   - CSV (comma-separated values)
   - XLS (Microsoft Excel)
   - PDF (Adobe Acrobat)



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