CARBONITE™

Carbonite Server Backup Agent 7.5 for AIX

User Guide

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

Carbonite, Inc.
Two Avenue de Lafayette
Boston, MA 02111
www.carbonite.com

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 Carbonite Server Backup Agent, Carbonite Server Backup CentralControl, and Carbonite Server Backup Director applications have the encryption option of 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).

The Carbonite Server Backup Agents and Carbonite Server Backup Director applications also have the added security feature of an over the wire encryption method.

Document History

Version	**Date**	**Description**
1	June 2018	Initial guide provided for AIX Agent 7.5*x*.

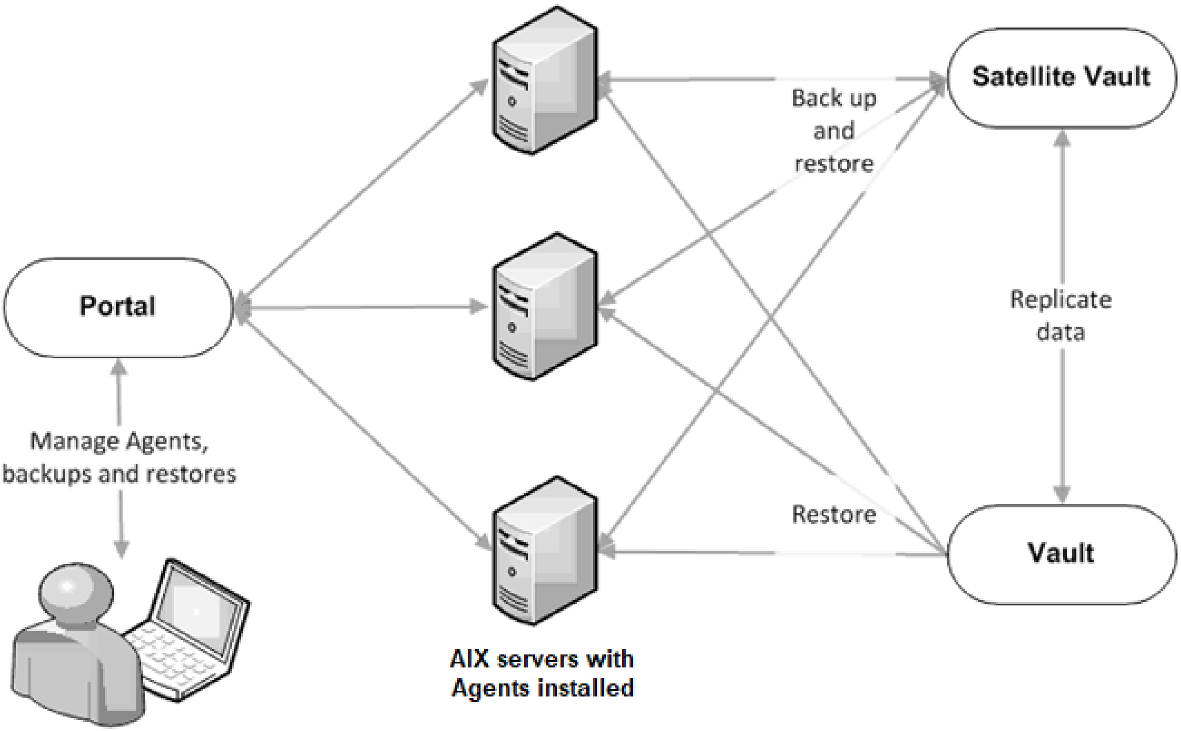
Contents

1 Introduction

Carbonite Server Backup Agent for AIX backs up data on AIX servers, and restores data from the backups.

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

Note: You can also use the legacy Windows CentralControl to manage the Agent and jobs.



The Agent includes support for:

- Workload Partitioning (WPAR)
- Trusted Execution (TE)
- Enhanced Role-Based Access Control (RBAC)

Workload Partitioning

You can install an Agent in a Workload Partition (WPAR), performing backup and restore operations in the WPAR as you would in a normal physical system. Also, an Agent instance running in a Global Environment can perform backup and restore operations in WPARs.

If you restore a WPAR within an ordinary directory (i.e., not at the WPAR root), the WPAR will restore as a directory.

Enhanced Role-Based Access Control (RBAC)

The AIX Agent can back up and restore the RBAC database.

Before you restore, make sure that the associated files (i.e., command files) and users exist on the system.

Trusted Execution (TE)

The AIX Agent can back up and restore the Trusted Signature Database (TSD). It can also back up trusted command files that are managed by the Trusted Execution environment.

To control trusted command files, use the `TSD_FILES_LOCK` option of the `trustchk` command:

- If TSD_FILES_LOCK is off, you can restore trusted command files. If the contents of a trusted command file have changed, the command will not run. This is because the integrity check that the TE environment performs at run time will have failed.
- If TSD_FILES_LOCK is on, all trusted command files are locked. You cannot modify them.

2 Install the AIX Agent

The Agent installation kit is provided as a tar.gz file. Only unzip this file on the machine where it will be installed. Unzipping the file on another type of machine can cause unpredictable results.

To install the AIX Agent, you must have root privileges.

The system must have sufficient disk space for the new installation, and for later job activities. The installation program will determine whether there is enough disk space for the installation to continue. If the available disk space is insufficient, the installation directory will roll back to its original state.

The Agent uses ports 808 and 8031. The default installation directory is /opt/BUAgent.

For supported AIX versions, see the AIX Agent release notes.

To install the Agent:

1. Download the AIX Agent tar.gz installation kit on the machine where you are installing the Agent.

2. Extract files from the installation package. To do so, run the following command:

   ```
   gzip -cd packageName.tar.gz | tar -xf-
   ```

   Where *packageName* is the name of the Agent installation kit.

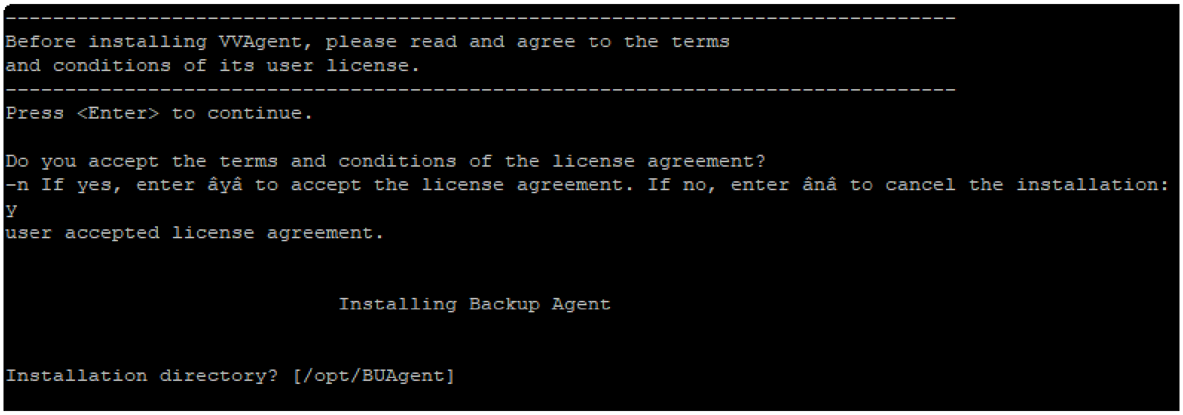
3. Change the directory to the extracted directory.

4. Run the following command to start the installation:

   ```
   ./install.sh
   ```

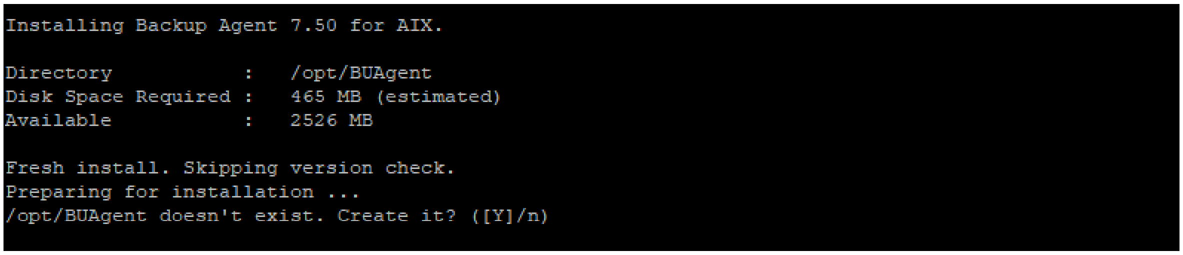
   For available options for this command, see Install the AIX Agent in silent mode.

5. Press **Enter**, and read the software license agreement. If you accept the terms and conditions of the license agreement, enter **Y** when prompted.



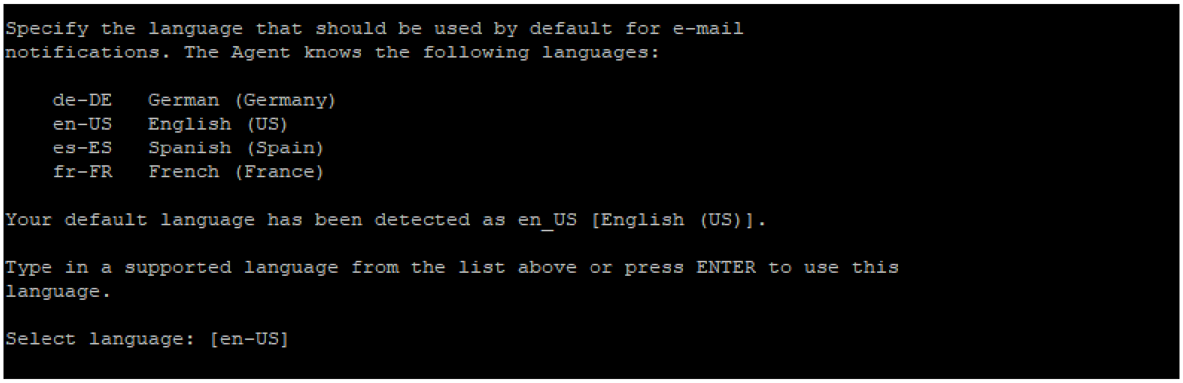
```
--------------------------------------------------------------------------------
Before installing VVAgent, please read and agree to the terms
and conditions of its user license.
--------------------------------------------------------------------------------
Press <Enter> to continue.

Do you accept the terms and conditions of the license agreement?
-n If yes, enter âyâ to accept the license agreement. If no, enter ânâ to cancel the installation:
y
user accepted license agreement.


                            Installing Backup Agent


Installation directory? [/opt/BUAgent]
```

6. Press **Enter** to accept the default installation directory.



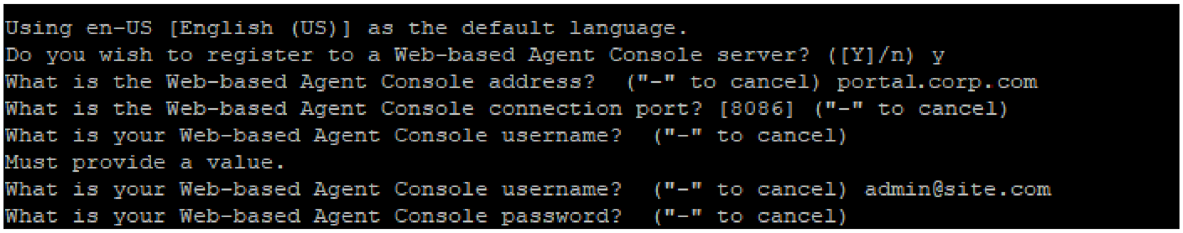
```
Installing Backup Agent 7.50 for AIX.

Directory           :   /opt/BUAgent
Disk Space Required :   465 MB (estimated)
Available           :   2526 MB

Fresh install. Skipping version check.
Preparing for installation ...
/opt/BUAgent doesn't exist. Create it? ([Y]/n)
```

7. Enter **Y** to create the BUAgent directory.
8. When prompted to select a language, enter the language for Agent log messages. The default language is English (en-US).



```
Specify the language that should be used by default for e-mail
notifications. The Agent knows the following languages:

    de-DE   German (Germany)
    en-US   English (US)
    es-ES   Spanish (Spain)
    fr-FR   French (France)

Your default language has been detected as en_US [English (US)].

Type in a supported language from the list above or press ENTER to use this
language.

Select language: [en-US]
```

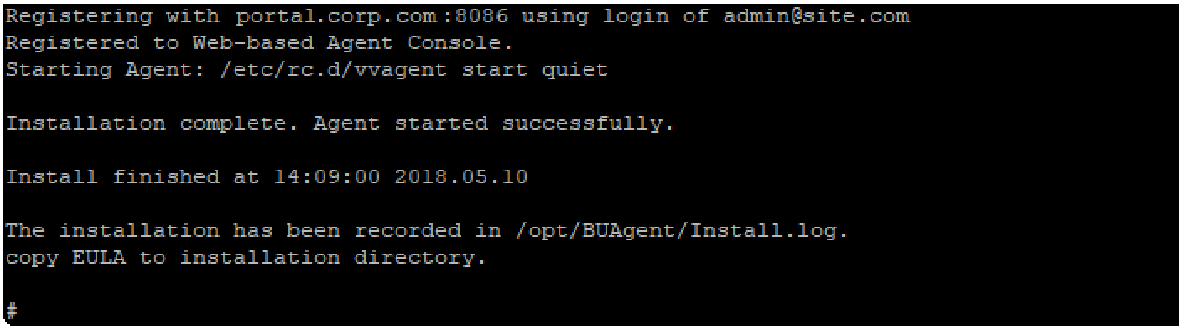
9. When prompted to register to a Web-based Agent Console server (Portal), enter **Y**.
10. At the Web-based Agent Console address prompt, enter the Portal address.
11. At the Web-based Agent Console connection port prompt, enter the Portal connection port. The default value is 8086.
12. At the Web-based Agent Console username prompt, enter the Portal username for registering the Agent.
13. At the Web-based Agent Console password prompt, enter the password for the Portal user specified in Step 12.



```
Using en-US [English (US)] as the default language.
Do you wish to register to a Web-based Agent Console server? ([Y]/n) y
What is the Web-based Agent Console address?  ("-" to cancel) portal.corp.com
What is the Web-based Agent Console connection port? [8086] ("-" to cancel)
What is your Web-based Agent Console username?  ("-" to cancel)
Must provide a value.
What is your Web-based Agent Console username?  ("-" to cancel) admin@site.com
What is your Web-based Agent Console password?  ("-" to cancel)
```

The installation proceeds. When complete, a message appears, and the Agent will be running.

After installation, the installation log (Install.log) is located in the installation directory.



```
Registering with portal.corp.com:8086 using login of admin@site.com
Registered to Web-based Agent Console.
Starting Agent: /etc/rc.d/vvagent start quiet

Installation complete. Agent started successfully.

Install finished at 14:09:00 2018.05.10

The installation has been recorded in /opt/BUAgent/Install.log.
copy EULA to installation directory.

#
```

2.1 Install the AIX Agent in silent mode

To install or upgrade the AIX Agent in silent mode, run the following command in the directory where the installation kit is located:

`install.sh` [*options*]

Where *options* are optional parameters for running the installation kit in silent mode. For a list of available options, see the following table.

AIX Agent installation parameters

Parameter	Description
`-shutdown | -s`	Force the Agent to shut down, if running.
`-force | -F`	Force the installation; skip the initial free space check.
`-defaults | -D`	Use the default values for installation.
`-force-defaults`	Force the installation using the defaults (assumes -s and -F).

`-web-registration=off`
`-W-`
	Turns off Portal registration.

`-web-registration=`*`registrationFile`*
`-W=`*`registrationFile`*
	Registers the Agent to Portal with the values found in a *registrationFile. registrationFile* is the path to and name of a file that contains Portal registration information (e.g., `−W=/tmp/registration.txt`). See AIX Agent registration options.

`-quiet | -Q`	Quiet install; does not echo output to the screen. If user interaction is required in quiet mode, the install will fail unless -force-defaults is specified.
`-log=NAME | -L=NAME`	Writes the installation log to the specified file NAME.

Parameter	Description
`-lang=NAME | -l=NAME`	Selects NAME as the language. Must begin with an ISO language code. May optionally be followed by a dash or underscore and an ISO country code (e.g., fr, fr-FR, and fr_FR are acceptable). Character set markers (e.g., UTF-8) are ignored. Languages that cannot be matched will report an error and the language will be defaulted to en-US [English (US)]. If not specified, the language will be guessed from your system value of "en_US.UTF-8".
`-backup=DIR | -B=DIR`	Backs up the current installation of the Agent to the specified directory.
`-verify | -V`	Verifies the integrity of the installation kit.
`-help`	Shows install.sh command options.

AIX Agent registration options

To provide Portal registration information during a silent installation, use the `-web-registration=`*`registrationFile`* parameter with the `install.sh` script. The registration file is a text file that contains the following information:

```
wccAddress=PortalAddress

wccPort=PortalConnectionPort # Defaults to 8086

wccLogin=PortalUserName

wccPassword=PortalPassword
```

Use the values provided by your administrator for the Portal address, port, username and password.

Note: You can only use the `-web-registration=`*`registrationFile`* parameter with the `install.sh` script. This parameter cannot be used with the `register` script.

2.2 Upgrade the AIX Agent

Before you upgrade the Agent, ensure that your system meets the minimum requirements for the new Agent version as described in the AIX Agent release notes.

During the upgrade, specify the installation directory of the AIX Agent that is currently installed. Otherwise, the upgrade will proceed as if it is a new installation.

When you upgrade the Agent, the installation directory does not change. The default Agent installation location for pre-version 7.5 AIX Agents was /usr/local/BUAgent. If you upgrade the Agent to version 7.5, the Agent will not be moved to the new default installation location (/opt/BUAgent).

After upgrading the Agent, we recommend running each of the Agent's backup jobs. This allows the Agent to upload new configuration information to the vault.

To upgrade the AIX Agent:

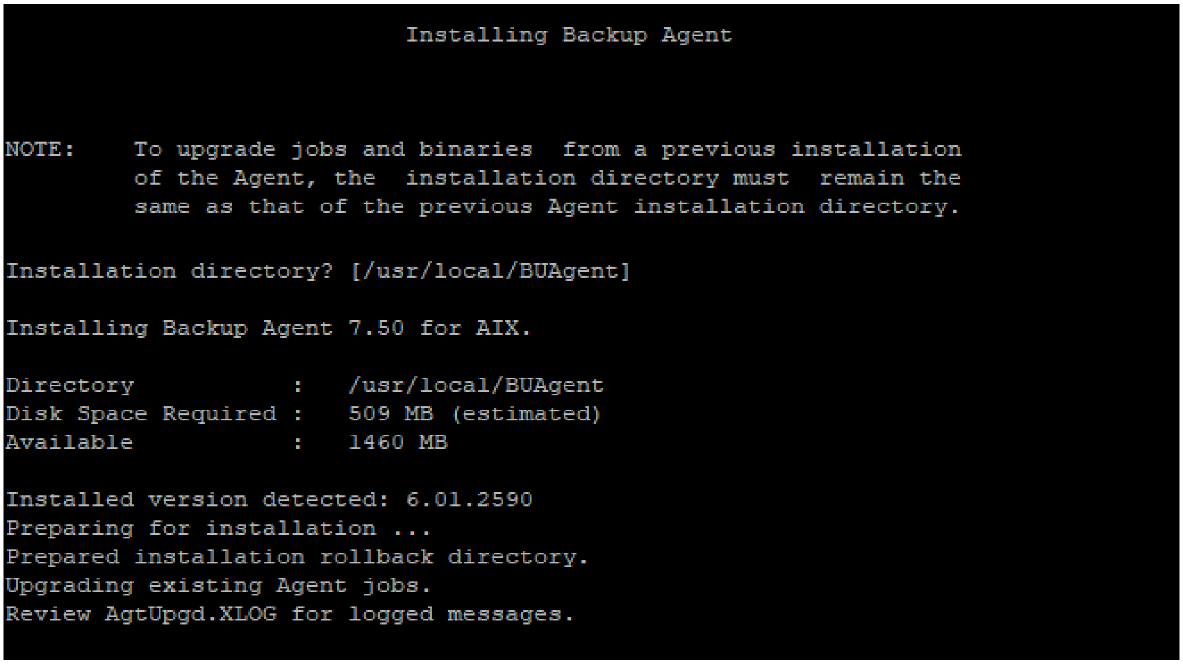
1. Download the AIX Agent tar.gz installation kit on the machine where you are installing the Agent.
2. Extract files from the installation package. To do so, run the following command:

   ```
   gzip -cd packageName.tar.gz | tar -xf-
   ```

   Where *packageName* is the name of the Agent installation kit.
3. Change the directory to the extracted directory.
4. Run the following command to start the upgrade:

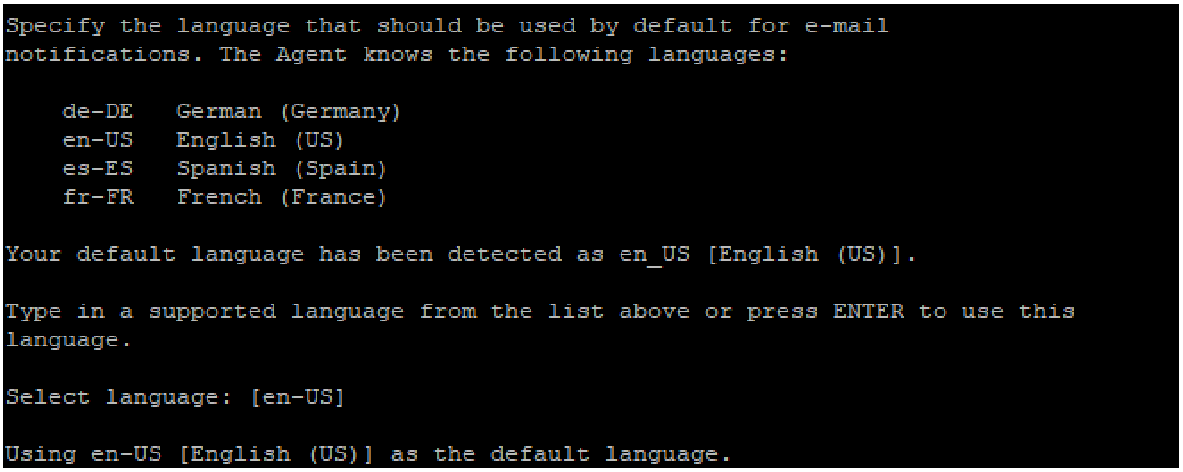
   ```
   ./install.sh
   ```
5. Press **Enter**, and read the software license agreement. If you accept the terms and conditions of the license agreement, enter **Y** when prompted.
6. If a message states that the Agent is still running, enter **Y** to stop it.
7. At the Installation directory prompt, enter the installation directory.

   IMPORTANT: Specify the installation directory of the Agent that is currently installed. Otherwise, the upgrade will proceed as if it is a new installation.



```
                            Installing Backup Agent


NOTE:    To upgrade jobs and binaries  from a previous installation
         of the Agent, the  installation directory must  remain the
         same as that of the previous Agent installation directory.

Installation directory? [/usr/local/BUAgent]

Installing Backup Agent 7.50 for AIX.

Directory           :   /usr/local/BUAgent
Disk Space Required :   509 MB (estimated)
Available           :   1460 MB

Installed version detected: 6.01.2590
Preparing for installation ...
Prepared installation rollback directory.
Upgrading existing Agent jobs.
Review AgtUpgd.XLOG for logged messages.
```

8. At the Select language prompt, enter the language for Agent messages. The default language is English [en-US].



```
Specify the language that should be used by default for e-mail
notifications. The Agent knows the following languages:

    de-DE   German (Germany)
    en-US   English (US)
    es-ES   Spanish (Spain)
    fr-FR   French (France)

Your default language has been detected as en_US [English (US)].

Type in a supported language from the list above or press ENTER to use this
language.

Select language: [en-US]

Using en-US [English (US)] as the default language.
```

9. If a message states that you are already registered to a Web-based Agent Console server, and asks whether you want to register as a new computer, do one of the following:

   - To change the Portal registration, enter **Y** and then enter the new Portal information.
   - To keep the same Portal registration, enter **N**.

   The upgrade proceeds. When complete, a message appears, and the Agent daemon will be running.

2.3 Change the Portal registration for an AIX Agent

When you install an AIX Agent, you can register the Agent to Portal. You can also change the Portal registration at any time.

The Agent is restarted when you change the Portal registration. You cannot change an Agent's Portal registration when a backup or restore is running.

To change the Portal registration for an AIX Agent:

1. In the directory where the Agent is installed, run the following command:

   ```
   ./register
   ```

2. If a message states that the Agent is already registered to a Web-based Agent Console server, enter **Y**.
3. At the Register to a Web-based Agent Console server prompt, enter **Y**.
4. At the Web-based Agent Console address prompt, enter the Portal address.
5. At the Web-based Agent Console connection port prompt, enter the Portal connection port. The default value is 8086.
6. At the Web-based Agent Console username prompt, enter the Portal username for registering the Agent.

   The Agent is restarted and the Portal registration is changed.

2.4 Change the language for AIX Agent log messages

When you install an AIX Agent, you can specify a language for Agent log messages. You can also change the Agent language at any time.

To change the language for AIX Agent log messages:

1. In the directory where the Agent is installed, run the following command:

   ```
   ./set_language
   ```

2. At the Select language prompt, enter one of the following values:
   - de – German
   - en – English
   - es – Spanish
   - fr – French

2.5 Uninstall the AIX Agent

To uninstall the AIX Agent:

1. In the directory where the Agent is installed, run the following command:

   ```
   ./uninstall.sh
   ```

2. If a message states that the Agent is still running, enter **Y** to stop the agent.
3. Do one of the following:
   - To remove the installation directory and all jobs, settings and logs, enter **Y**.
   - To leave the installation directory and all jobs, settings and logs, enter **N**. If you reinstall the Agent in the same directory, you can continue running these jobs.

3 Configure the Agent

After an AIX Agent is installed and registered with Carbonite Server Backup 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.

3.1 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.

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.

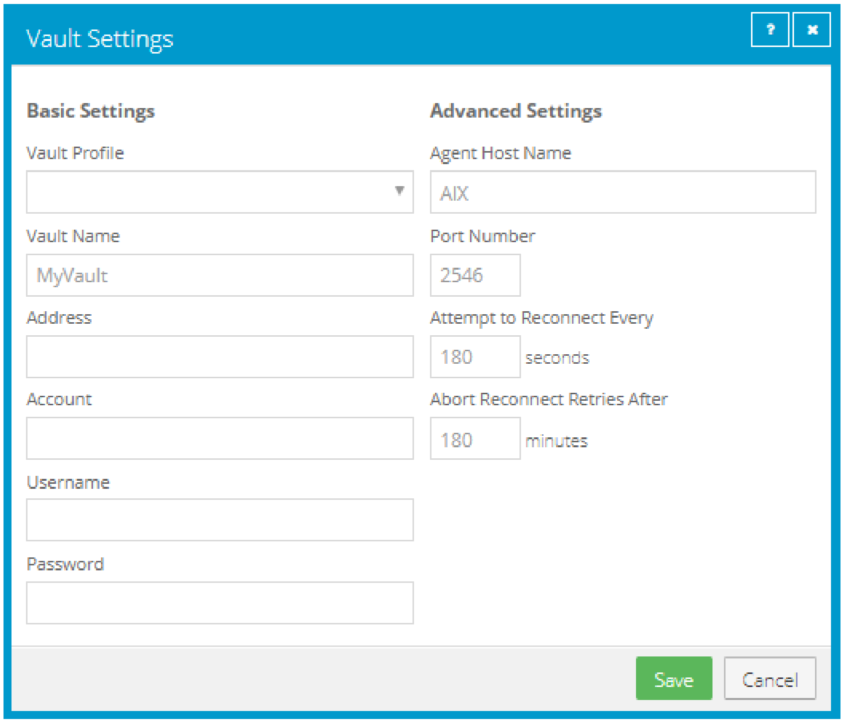
In the past, you could specify whether data is encrypted using AES encryption when it is transmitted to and from the vault. Over-the-wire encryption is now automatically enabled when you add vault settings or save existing vault settings.

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.



Basic Settings

Vault Profile:

Vault Name: MyVault

Address:

Account:

Username:

Password:

Advanced Settings

Agent Host Name: AIX

Port Number: 2546

Attempt to Reconnect Every: 180 seconds

Abort Reconnect Retries After: 180 minutes

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 IP 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**.

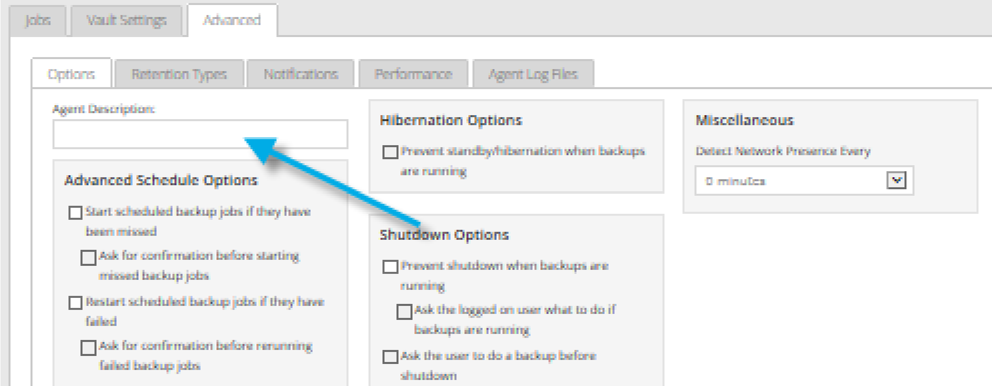
3.2 Add a description

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.



Agent Description:

Advanced Schedule Options

□ Start scheduled backup jobs if they have been missed

□ Ask for confirmation before starting missed backup jobs

□ Restart scheduled backup jobs if they have failed

□ Ask for confirmation before rerunning failed backup jobs

Hibernation Options

□ Prevent standby/hibernation when backups are running

Shutdown Options

□ Prevent shutdown when backups are running

□ Ask the logged on user what to do if backups are running

□ Ask the user to do a backup before shutdown

Miscellaneous

Detect Network Presence Every

0 minutes

5. Click **Save**.

3.3 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.

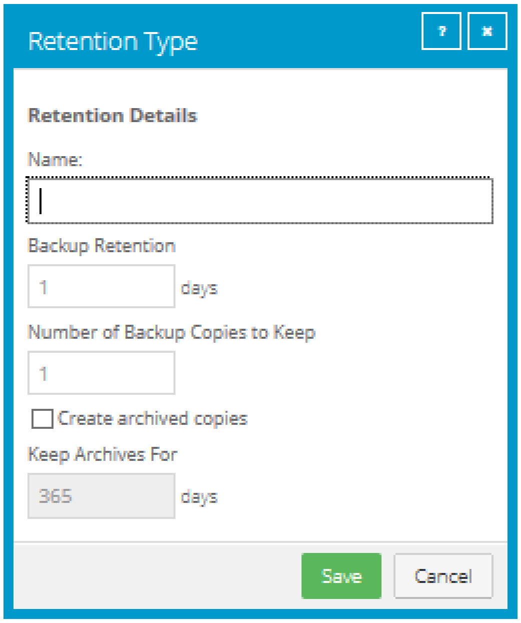
To add a retention type:

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.



Retention Type

Retention Details

Name:

Backup Retention

1 days

Number of Backup Copies to Keep

1

□ Create archived copies

Keep Archives For

365 days

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**.

3.4 Configure bandwidth throttling

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

Bandwidth settings include:

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

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

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

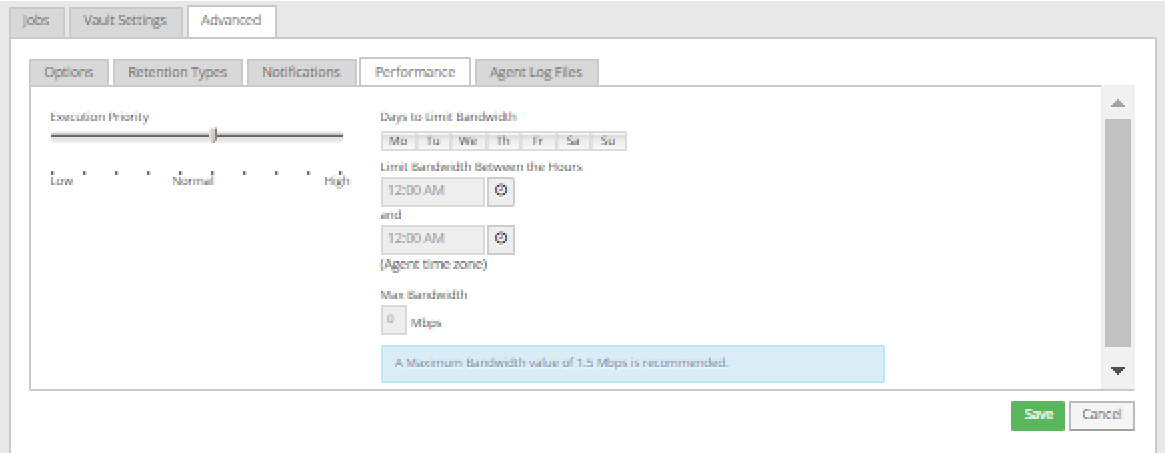
If a policy is assigned to a computer, bandwidth throttling settings cannot be modified on the Computers page. Instead, settings can only be added or modified in the policy.

To configure bandwidth throttling:

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



Execution Priority

Days to Limit Bandwidth

Limit Bandwidth Between the Hours

12:00 AM

and

12:00 AM

(Agent time zone)

Max Bandwidth

0 Mbps

A Maximum Bandwidth value of 1.5 Mbps is recommended.

4 Add an AIX backup job

After an AIX server is added in Portal, you can add backup jobs for the server. A backup job specifies which folders and files to back up, and where to save the data.

If an AIX server does not already have a backup job, and a valid vault profile is available, the system can automatically create a backup job. See Add an AIX backup job automatically.

You can also create a backup job for files and folders that are saved on mounted NFS shares. See Add an NFS backup job.

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

To add an AIX backup job:

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

   The Computers page shows registered computers.

2. Find an AIX system, and expand its view by clicking the computer row.

   If a Configure Manually box appears, click **Configure Manually** to continue adding the backup job.

   If a Configure Automatically box appears, the system can attempt to create a backup job automatically. See Add the first backup job for an AIX server.

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.

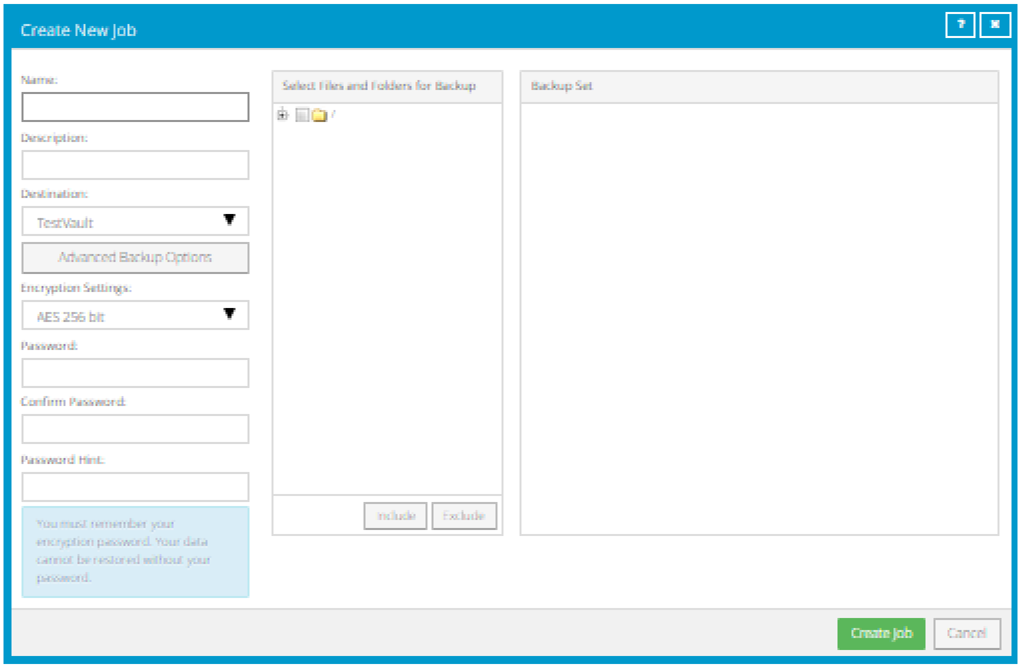
4. In the **Select Job Task** menu, click **Create New Local System Job**.

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.

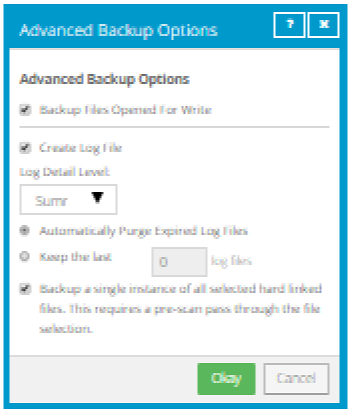


Destination: TestVault

Encryption Settings: AES 256 bit

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

6. To change log file or other backup options, click **Advanced Backup Options**. In the **Advanced Backup Options** dialog box, select options and then click **Okay**. For more information, see Log file options and Advanced backup options.



☑ Backup Files Opened For Write

☑ Create Log File

Log Detail Level: Summ

● Automatically Purge Expired Log Files

○ Keep the last 0 log files

☑ Backup a single instance of all selected hard linked files. This requires a pre-scan pass through the file selection.

7. 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 in and exclude from the backup:

   - 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. 🗑

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.

4.1 Add an AIX backup job automatically

If a backup job has not been created for an AIX server and a valid vault profile is available, Portal can automatically create a backup job for the server. For information about creating vault profiles and assigning them to users, see the Portal online help or Administration guide.

An automatically-created job backs up everything from the root, and is scheduled to run every night.

You can change the settings for an automatically-created job, if desired. For example, you can specify different directories to back up or change the schedule for running the job.

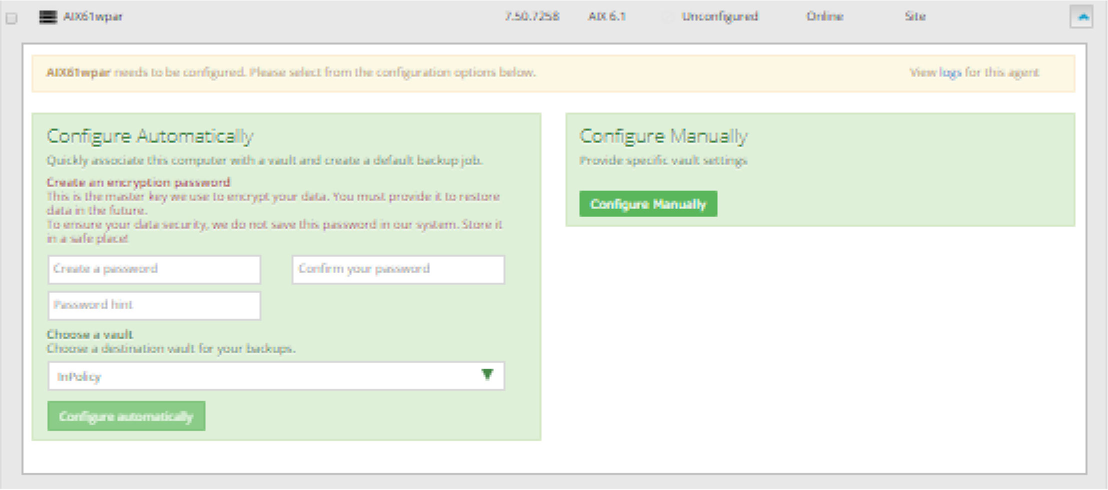
To add an AIX backup job automatically:

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

   The Computers page shows registered computers.

2. Find an AIX 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 for the user, the Configure Automatically box also appears.



AIX61wpar 7.50.7258 AIX 6.1 Unconfigured Online Site

AIX61wpar needs to be configured. Please select from the configuration options below. View logs for this agent

Configure Automatically

Quickly associate this computer with a vault and create a default backup job.

Create an encryption password
This is the master key we use to encrypt your data. You must provide it to restore data in the future.
To ensure your data security, we do not save this password in our system. Store it in a safe place!

Create a password | Confirm your password

Password hint

Choose a vault
Choose a destination vault for your backups.

InPolicy

Configure automatically

Configure Manually

Provide specific vault settings

Configure Manually

3. Do one of the following:

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

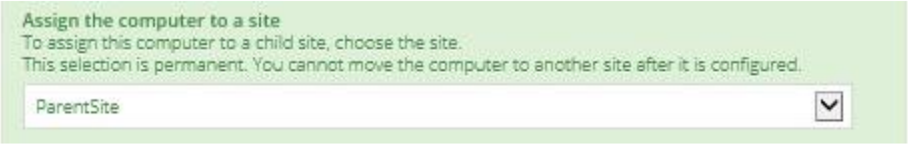
     i. In the **Create a password** and **Confirm your password** boxes, enter an encryption password.

        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.



Assign the computer to a site
To assign this computer to a child site, choose the site.
This selection is permanent. You cannot move the computer to another site after it is configured.

ParentSite

     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, click **Go to Agent.** A backup job appears for the computer.

If the automatic job configuration fails, do the following:

a. Click **Configure Manually**.

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

c. In the Vault Settings dialog box, enter vault information and credentials. See Add vault settings.

d. Create a backup job manually. See Add an AIX backup job.

4.2 Add an NFS backup job

After a system is added in Portal, you can create a backup job for files and folders that are saved on mounted NFS shares. The backup job specifies which folders and files to back up, and where to save the data.

NFS servers must share their exports in order to make them available to client systems. If you want to perform a mount-point backup or restore, the NFS server must be available, and it must provide sufficient privileges to your client system. Also, the NFS must be mounted on your client system at the time of the backup or restore.

Note: If you restore an NFS backup, and the NFS mount does not exist, the restore will proceed as if it were a local restore. It will put the data on the local disk (with a similar path that is local) without using a mount-point (NFS) path. It will not indicate a “failure”.

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

To add an NFS backup job:

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

   The Computers page shows registered computers.

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

3. Click the **Jobs** tab.

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

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

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

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

     A vault only appears in the list if it assigned to the user, or if the user added it on the computer’s Vault Settings tab.

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

6. In the **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 in and exclude from the backup:

   - 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. 🗑

7. 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.

4.2.1 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.

4.2.2 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.

4.2.3 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.

Back up a single instance of all selected hard linked files

A hard link is a reference, or pointer, to data on a storage volume. More than one hard link can be associated with the same data. Hard-linked files cannot cross disk boundaries and only exist on the same disk.

If the **Back up a single instance of all selected hard linked files** option is selected, only one copy of the data is backed up, along with all of the hard links. When the data is restored, both the data (with a new inode) and the hard links are restored. When this option is selected, a pre-scan process is required. The pre-scan reads through the file system, gets each inode and stores it in a map. The larger the file system, the more memory this map requires and the more time it takes to process. However, the resulting backup size is smaller.

If the **Back up a single instance of all selected hard linked files** option is not selected, the data is backed up separately for each hard link. When the data is restored, the hard-link relationship will not be re-established. Each file will be restored individually and applications depending on hard links may not be automatically restored. When this option is not selected, the backup is faster but the total backup size is larger.

4.2.4 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 .pl extension.

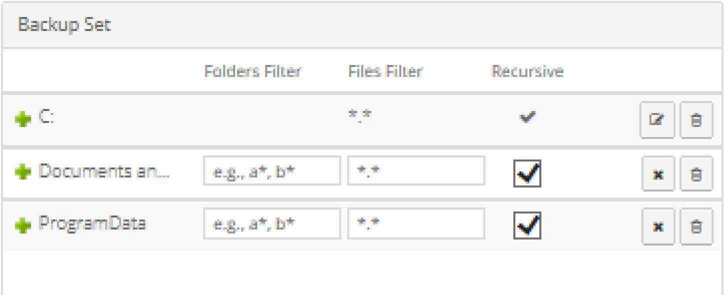
If you only want to exclude some subdirectories or files in a folder from a backup job, you can add filters to the exclusion record. For example, you could add a filter so that files in a folder are excluded from the backup if they have the .mpg extension.

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.



Backup Set

	Folders Filter	Files Filter	Recursive
C:		*.*	✓
Documents an...	e.g., a*, b*	*.*	☑
ProgramData	e.g., a*, b*	*.*	☑

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 .pl or .sh extension, enter the following filter: *.pl, *.sh

      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 exclude files from a backup if they have the .mpg or .gif extension, enter the following filter: *.mpg, *.gif

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

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

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

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

5.1 Schedule a backup

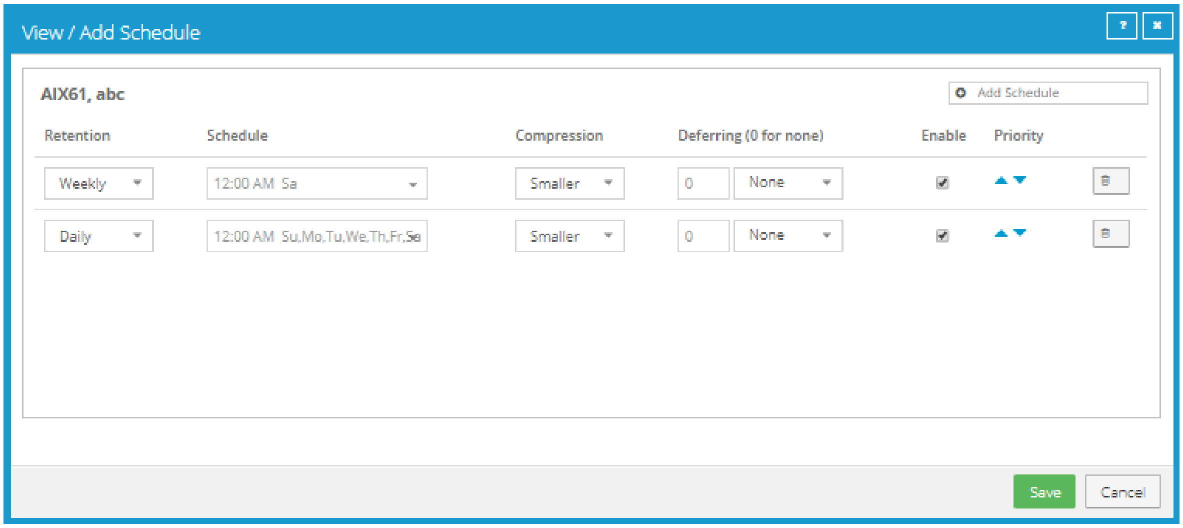
After creating a backup job, you can add one or more schedules for running the job automatically.

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

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.



AIX61, abc

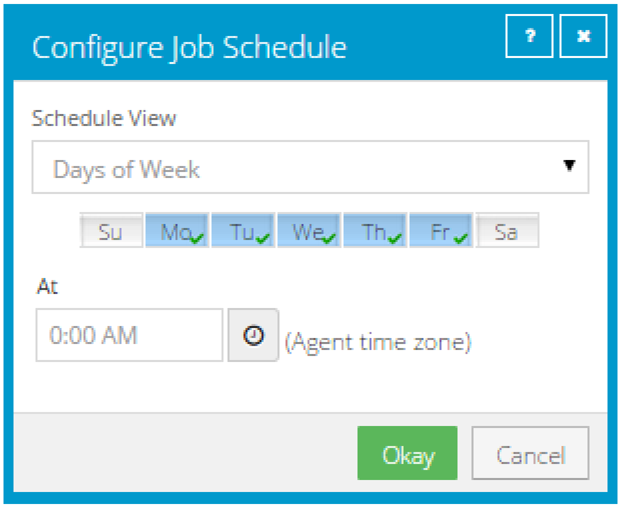
Retention	Schedule	Compression	Deferring (0 for none)		Enable	Priority
Weekly	12:00 AM Sa	Smaller	0	None	☑	▲▼
Daily	12:00 AM Su,Mo,Tu,We,Th,Fr,Sa	Smaller	0	None	☑	▲▼

To schedule a backup:

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

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

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



Configure Job Schedule

Schedule View

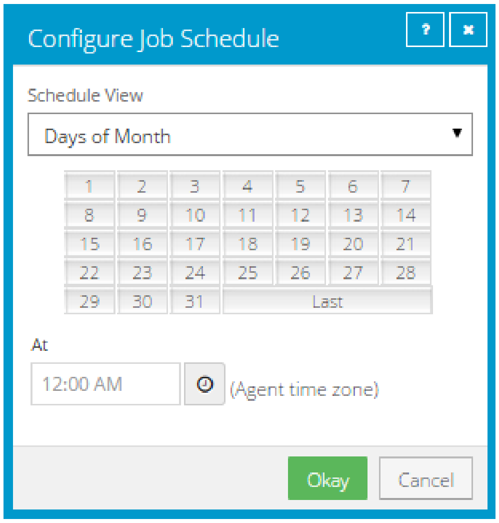
Days of Week

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

At

0:00 AM (Agent time zone)

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



Configure Job Schedule

Schedule View

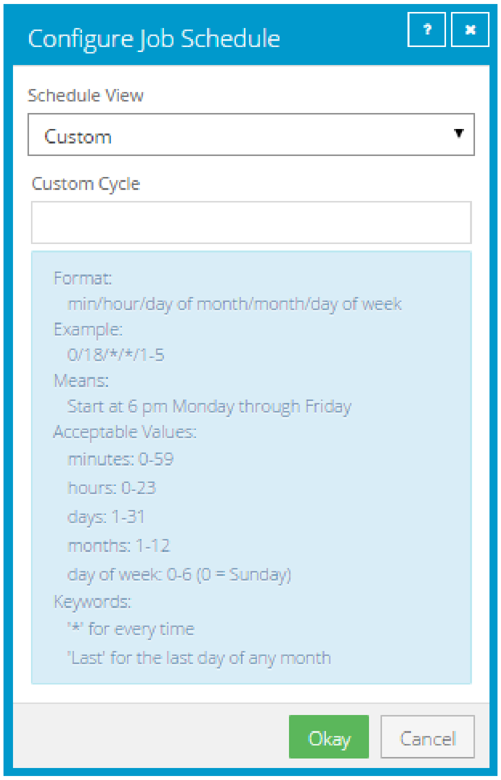
Days of Month

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

At

12:00 AM (Agent time zone)

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



Configure Job Schedule

Schedule View: Custom

Custom Cycle:

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

6. Click **Okay**.

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

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

8. Do one of the following:

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

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

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

10. If 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. Click **Save**.

5.2 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.

Note: The AIX operating system has a default file size limit of 1 GB. If you do not change the default file size limit, backing up a dataset over 1 GB to Directory On Disk may fail. To solve this problem, change the OS file size limit using commands such as the following:

```
ulimit -f unlimited
ulimit -f -H unlimited
chuser fsize=-1 fsize_hard=-1 root
```

To run an ad-hoc backup:

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

   A grid lists available computers.

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

3. Click the **Jobs** tab.

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

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

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

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

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

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

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

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

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

7. If you want to enable Quick File Scanning, select the **Quick File Scanning** check box.

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

8. Do one of the following:

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

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

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

9. Click Start Backup.

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

10. If you want to stop the backup, click **Stop**.
11. To close the **Process Details** dialog box, click **Close**.

5.3 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. 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**.

6 Restore AIX files and folders

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

When you restore a symbolic link, the modification date and time are set to the date and time of the restore (rather than the date and time of the symbolic link when it was backed up). A symbolic link (also called a symlink or soft link) is a special type of file that serves as a reference to another file or directory.

To restore AIX files and folders:

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

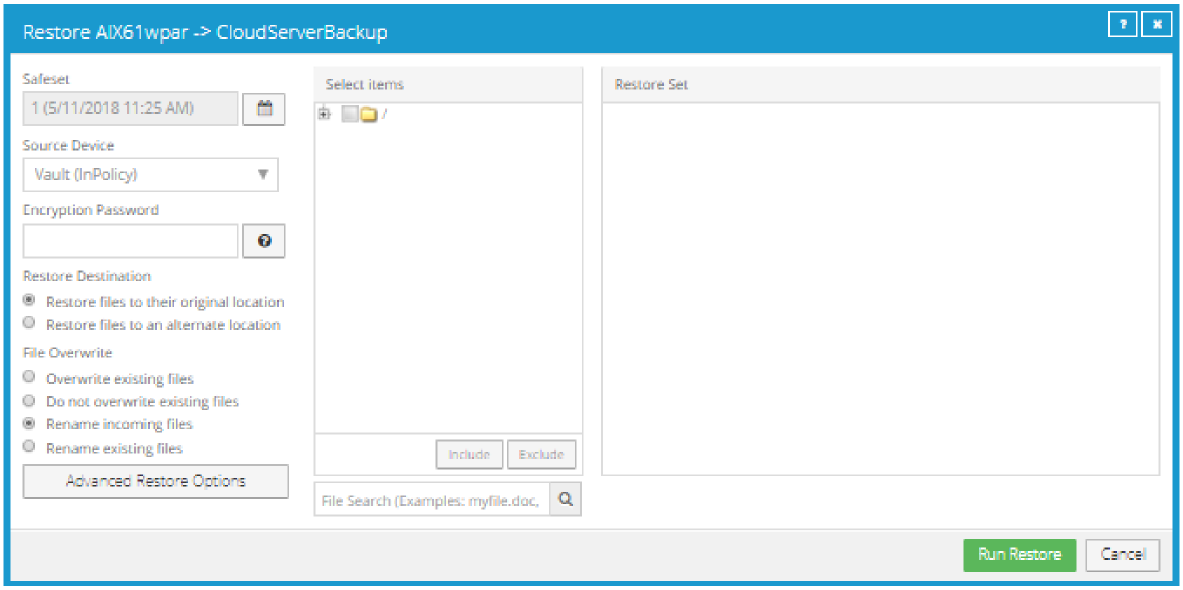
   A grid lists available computers.

2. Find the AIX 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.



Restore AIX61wpar -> CloudServerBackup

Safeset: 1 (5/11/2018 11:25 AM)

Source Device: Vault (InPolicy)

Encryption Password:

Restore Destination
● Restore files to their original location
○ Restore files to an alternate location

File Overwrite
○ Overwrite existing files
○ Do not overwrite existing files
● Rename incoming files
○ Rename existing files

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 a **File Overwrite** option. This option specifies how to restore a file to a location where there is a file with the same name.
   - To overwrite existing files with restored files, select **Overwrite existing files**.

     Note: If you try to restore multiple files with the same name to an alternate location and select **Overwrite existing files**, only the last file restored will remain. Other files with the same name will be overwritten.
   - To add a numeric extension (e.g., .0001) to a *restored* file name, select **Do not overwrite existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *restored* file name (e.g., “filename.txt.0001”).
   - To add a numeric extension (e.g., .0001) to an *existing* file name, select **Rename existing files**. For example, if you restore a file named “filename.txt” to a location where there is a file with the same name, an extension is added to the *existing* file name (e.g., “filename.txt.0001”). The name of the restored file continues to be “filename.txt”.
9. To change 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.

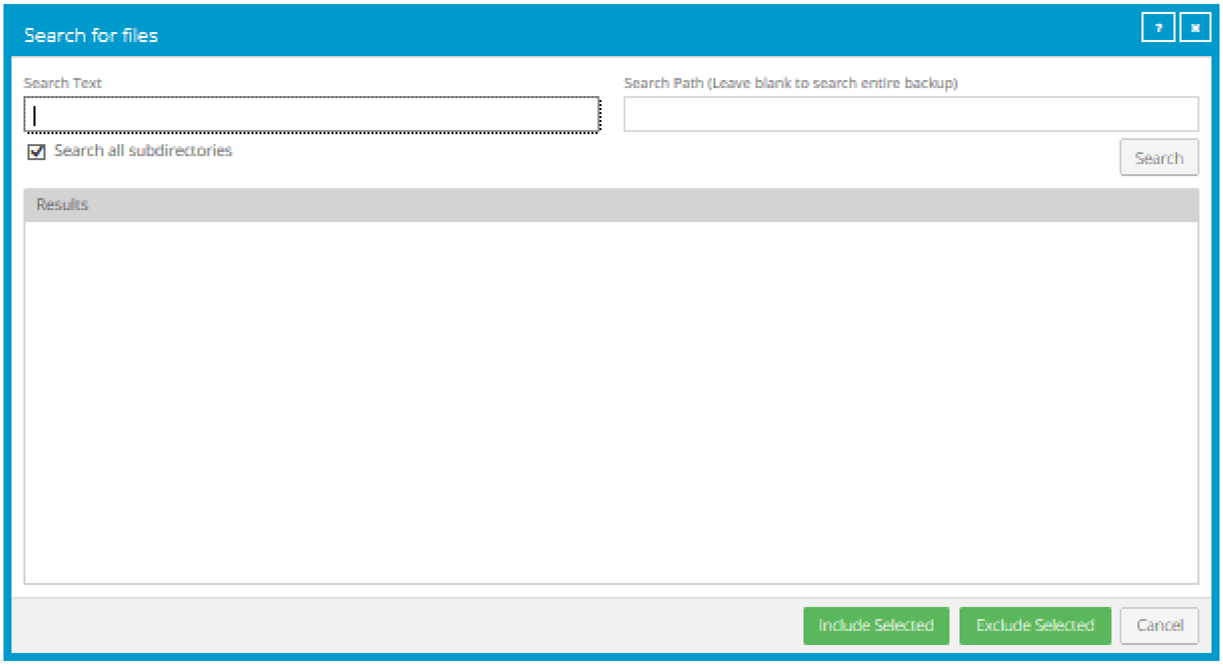
6.1.1 Search for files to restore

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**.

6.1.2 Filter subdirectories and files when restoring data

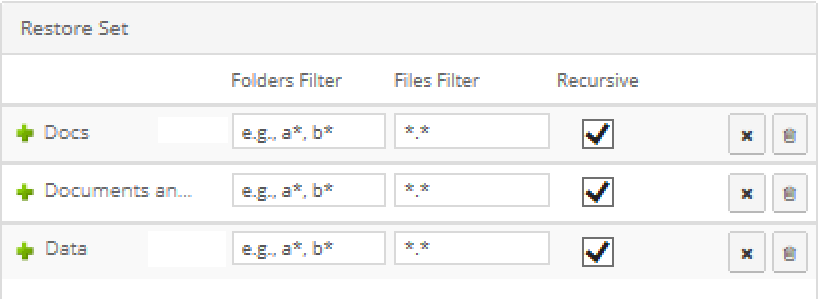
When you restore data from a backup job, you can specify folders and files to restore or not restore from the backup.

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 .pl 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 .sh extension.

To filter subdirectories and files when restoring data:

1. When restoring data from a backup job, view the **Restore Set** box.



Restore Set

	Folders Filter	Files Filter	Recursive
Docs	e.g., a*, b*	*.*	☑
Documents an...	e.g., a*, b*	*.*	☑
Data	e.g., a*, b*	*.*	☑

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 .pl extension, enter the following filter: *.pl

     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 .sh or .pl extension, enter the following filter: *.sh, *.pl

     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**.

6.2 Restore ACLs

You can back up and restore Access Control Lists (ACLs). ACLs control the access of users or groups to particular files. Similar to file permissions (e.g., owner, group, world), ACLs are tracked by the ID of the user/group. ACLs provide access-control granularity beyond regular file permissions. Unlike regular file permissions, ACLs are not always enabled.

This Agent version does not support ACLs on NFS filesystems and the /proc filesystem.

If you restore to the original system or a different system with the same AIX version, ACLs will be restored.

Since ACLs are associated with user and group IDs, you will observe the following if you restore to a different system:

- If the group, user names, and IDs on the restored system match those of the original system, the ACLs will be associated with the same user name as on original system.

- If the group, user names, and IDs on the restored system do not match those on the original system, the ACLs will be associated with a different user or group name compared to the original system.
- If the group or user name ID does not exist on the restored system, the ACLs will be associated with the user ID or group ID respectively. Therefore, browsing ACLs on these files will show user/group IDs as opposed to user/group names.

6.3 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.

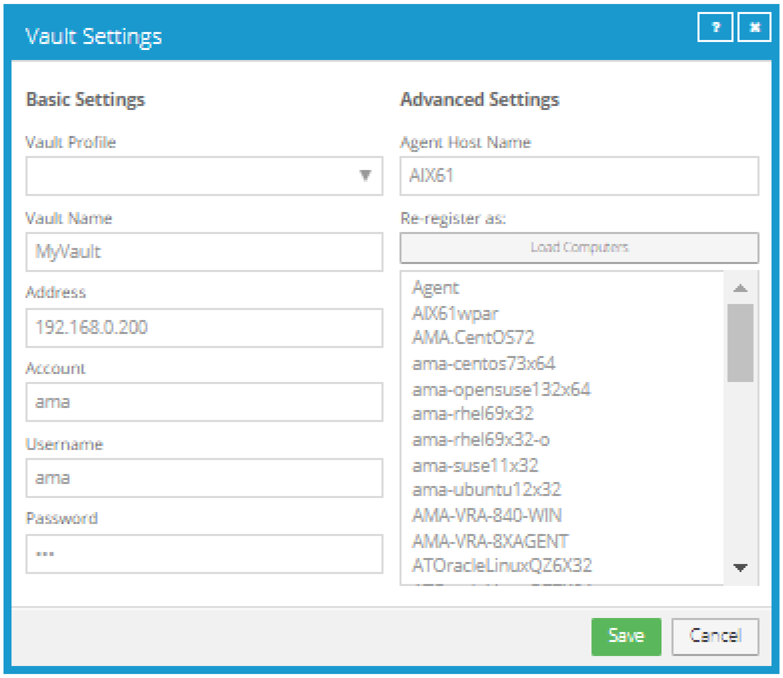
After you re-register a computer with a vault, you must synchronize existing backup jobs before they run successfully. See Synchronize a job.

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

To restore data to a replacement computer:

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

   A grid lists available computers.
3. Find the replacement computer to which you want to restore the data, and expand its view by clicking the computer row.
4. Click 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**.



Basic Settings

Vault Profile:

Vault Name: MyVault

Address: 192.168.0.200

Account: ama

Username: ama

Password: •••

Advanced Settings

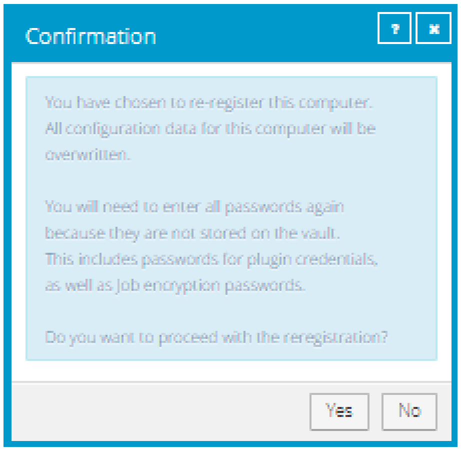
Agent Host Name: AIX61

Re-register as:

Agent
AIX61wpar
AMA.CentOS72
ama-centos73x64
ama-opensuse132x64
ama-rhel69x32
ama-rhel69x32-o
ama-suse11x32
ama-ubuntu12x32
AMA-VRA-840-WIN
AMA-VRA-8XAGENT
ATOracleLinuxQZ6X32

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**.



You have chosen to re-register this computer. All configuration data for this computer will be overwritten.

You will need to enter all passwords again because they are not stored on the vault. This includes passwords for plugin credentials, as well as job encryption passwords.

Do you want to proceed with the reregistration?

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 synchronize existing backup jobs before they run successfully. See Synchronize a job.

6.4 Restore data from another computer

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

The new computer 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

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.

6.5 Advanced restore options

When restoring data, you can specify the following options:

Locked File Options

When restoring data from a local job, you can 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. For example, you might want to restrict the amount of bandwidth used for daytime backups so that online users are not affected, and allow unlimited bandwidth usage at night so that scheduled backups run as fast as possible.

Bandwidth settings include:

- Maximum bandwidth (upper limit), in megabits per second, to be consumed by the Agent for all backups and restores

- Period of time during the day that throttling is in effect. Only one time window can be specified. Outside the window, no throttling takes place.
- Days of the week that throttling is in effect

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

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

7 System Recovery

The purpose of this chapter is to illustrate techniques for recovering a file system. The procedures provided describe the minimum resources and information required to rebuild the file system to its state at the last system backup.

The basic recovery procedure is:

1. Install the minimal operating system, including networking.
2. Install and configure the Agent.
3. Restore the backed-up system state, programs, and data using the Agent.
4. Perform post-recovery maintenance.
5. Verify the recovery.

7.1 Hardware Requirements

It is crucial for local storage on the system to be sufficient for a full recovery of programs, system state, and data. Otherwise the recovery will fail, and your system may be left in an indeterminate state.

If any configuration files for your operating system depend on specific identifiers of installed hardware (such as the MAC address of a network card), ensure that this information is noted, as the values may be different than when the system was backed up using the Agent.

7.2 Software Requirements

Ensure that the appropriate installation media is available. The minimum system software includes:

- Installation media identical to that installed on the original system.
- Any necessary OS patches to install the Agent.
- Agent installation media identical to that installed on the original system.

7.3 Recovery Steps

For successful AIX system recovery, the Technology Level (TL) of the target system must equal or surpass the TL of the source system.

7.3.1 Install the minimal operating system

Follow the instructions in your operating system manual and installation media to install a minimal operating system.

- When prompted to partition your drive(s), ensure that the partitions are large enough to restore to; they should be at least as large as the original partitions.
- If restoring over the network, TCP/IP network services must be installed and configured appropriately, and there must be a connection between the system and the backup vault.
- If restoring from a directory on disk, there must be sufficient disk space to handle all the restored data.

7.3.2 Install and configure the Agent

To install and configure the Agent:

1. Install the Agent according to the instructions in this guide.
2. Configure the Agent according to the instructions in this guide. It is important to reregister with the vault where the data was backed up.
3. Synchronize the job to ensure that local copies of job catalogs are created.

7.3.3 Restore the backed-up system

To restore the backed-up system:

1. Start a recovery according to the instructions in this guide.
2. Select the files you wish to restore. The Agent will restore most files to their original locations and protect against many known restore problems (for file systems mounted in their default locations), but some files may cause unpredictable results if restored. These files can generally be restored to alternative locations without problems.
3. Ensure that the files are not being restored to a file system that is mounted read-only.

When the recovery is complete, the process of verifying the integrity of the restore can commence.

7.3.4 Perform post-recovery maintenance

If any modifications to the configuration of the restored system are required after restore, these should be performed now. Known post-restore maintenance steps are noted below.

7.3.5 Verify the recovery

When the recovery procedure finishes, determine whether or not it is complete and correct. The listing and testing of the jobs should be performed as part of the systems recovery planning. The specific jobs to be performed for verification depend on the application environment and the system's importance.

Once the system is restored, the integrity of the recovery must be verified. The test can be as simple as placing a duplicate file in a different directory structure and testing for differences in the file. Then, confirm that the file can be opened using a known application and that you can send an e-mail to a known address. It can also be as complex as completing an SQL query on a known database set.

Whatever the test, both the list and the test itself must be planned and executed during normal system operation.

7.3.6 Troubleshooting a system recovery

If a system recovery fails, consider the following questions:

- Was the system restored using the same version of AIX?
- Were there differences in hardware or software settings that could have affected the recovery?
- Were errors reported in the error log file?
- Were all necessary drivers installed?
- Were the applicable AIX patches applied?
- Was there sufficient disk space for all of the restored data?
- Was the Technology Level (TL) of the target system lower than the TL of the source system? For successful AIX system restores, the TL of the target system must equal or surpass the TL of the source system.

8 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 Set up email notifications for backups on a computer.
- 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.

8.1 View computer and job status information

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

To view computer and job status information:

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

   The Computers page shows registered Agents.

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

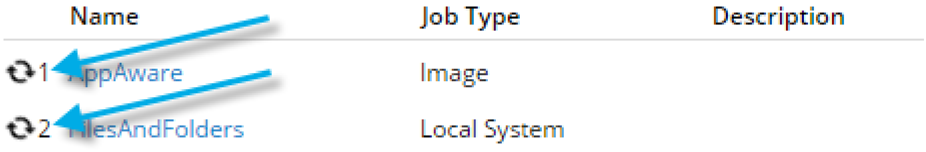
   The **Status** column shows the status of each computer. Possible statuses include:

   - ✓ OK — Indicates that all jobs on the computer ran without errors or warnings.
   - ! OK with warnings — Indicates that one or more of the computer’s jobs completed with warnings.
   - ❗ Attention — Indicates that one or more of the computer’s jobs failed or completed with errors.

- Unconfigured — Indicates that no jobs have been created for the computer.

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

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



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

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

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

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

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

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

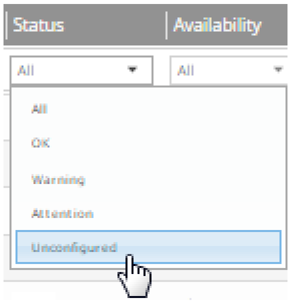
8.2 View an unconfigured computer’s logs

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

To view an unconfigured computer’s logs:

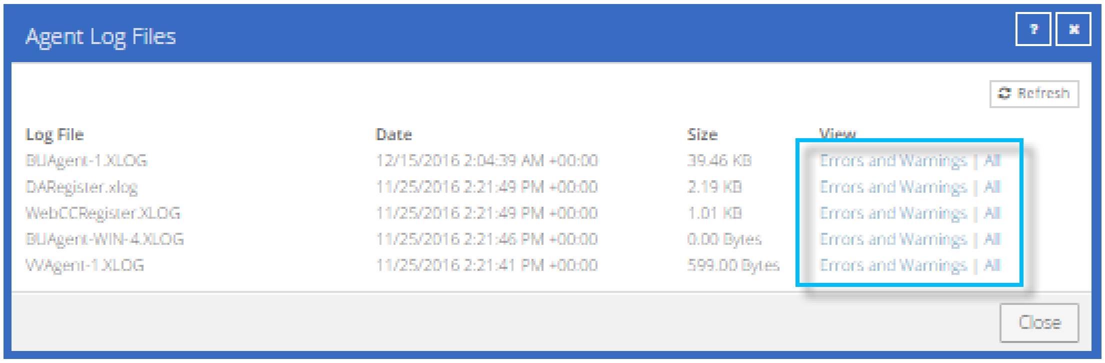
1. On the navigation bar, click **Computers**.

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

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

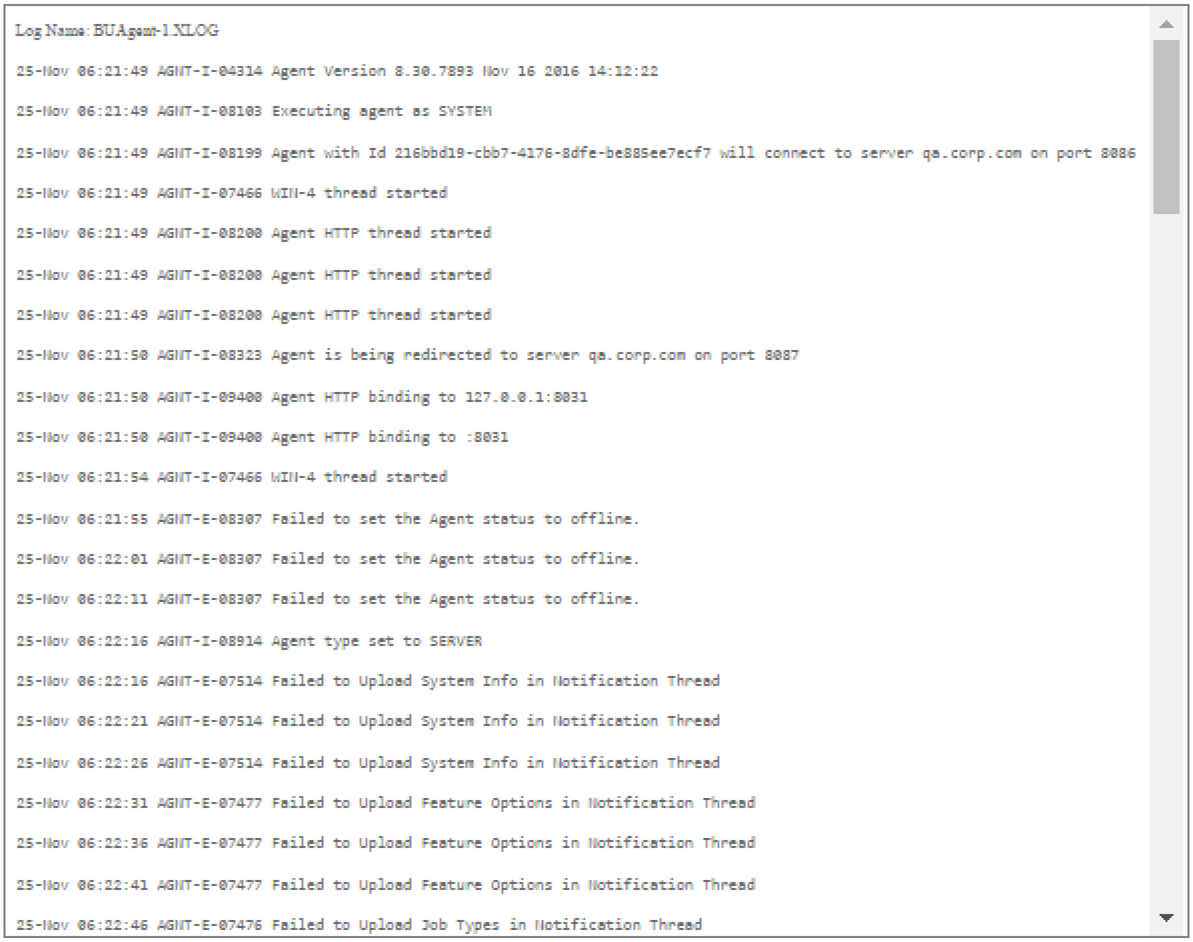
   

Log File	Date	Size	View
BUAgent-1.XLOG	12/15/2016 2:04:39 AM +00:00	39.46 KB	Errors and Warnings | All
DARegister.xlog	11/25/2016 2:21:49 PM +00:00	2.19 KB	Errors and Warnings | All
WebCCRegister.XLOG	11/25/2016 2:21:49 PM +00:00	1.01 KB	Errors and Warnings | All
BUAgent-WIN-4.XLOG	11/25/2016 2:21:46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

4. Do one of the following:

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

   The log appears in a new browser tab.



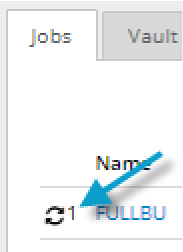
```
Log Name: BUAgent-1.XLOG

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.3 View current process information for a job

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

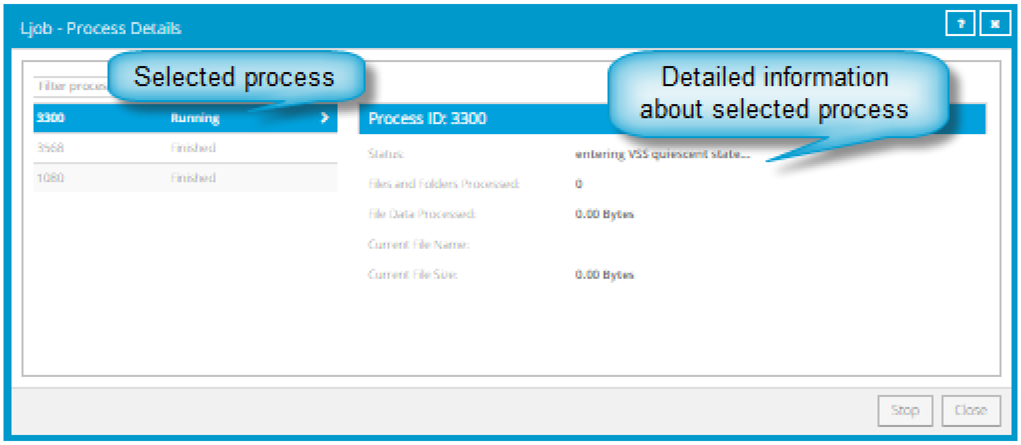
To view current process information for a job:

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



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

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



3300	Running
3568	Finished
1080	Finished

Process ID: 3300

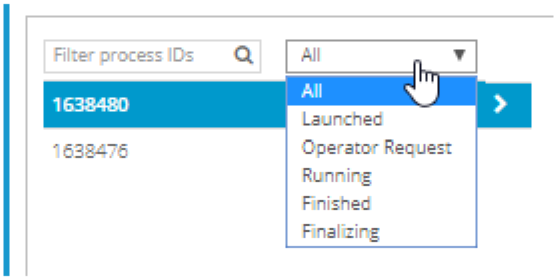
Status: entering VSS quiescent state...
Files and Folders Processed: 0
File Data Processed: 0.00 Bytes
Current File Name:
Current File Size: 0.00 Bytes

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

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

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

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



8.4 Set up email notifications for backups on a computer

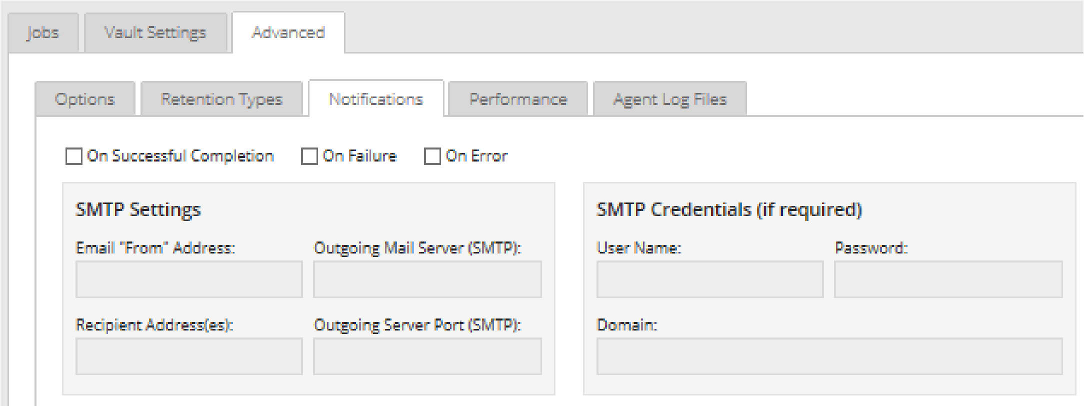
To make it easier to monitor backups, users can receive emails when backups finish or fail. Admin users and regular users in Portal can set up email notifications for a computer.

To set up email notifications for backups on 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.

Note: Email notifications can be sent using CRAM-MD5, AUTH LOGIN and AUTH PLAIN authentication.

4. Click **Save**.

8.5 View a job's process logs and safeset information

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

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

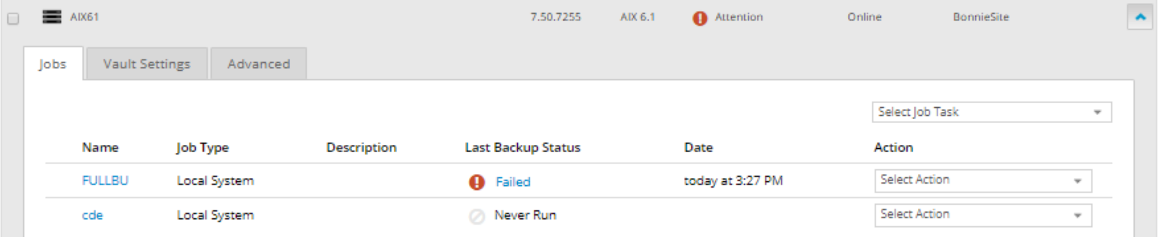
To view a job's process logs and safeset information:

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

   The Computers page shows registered Agents.

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

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

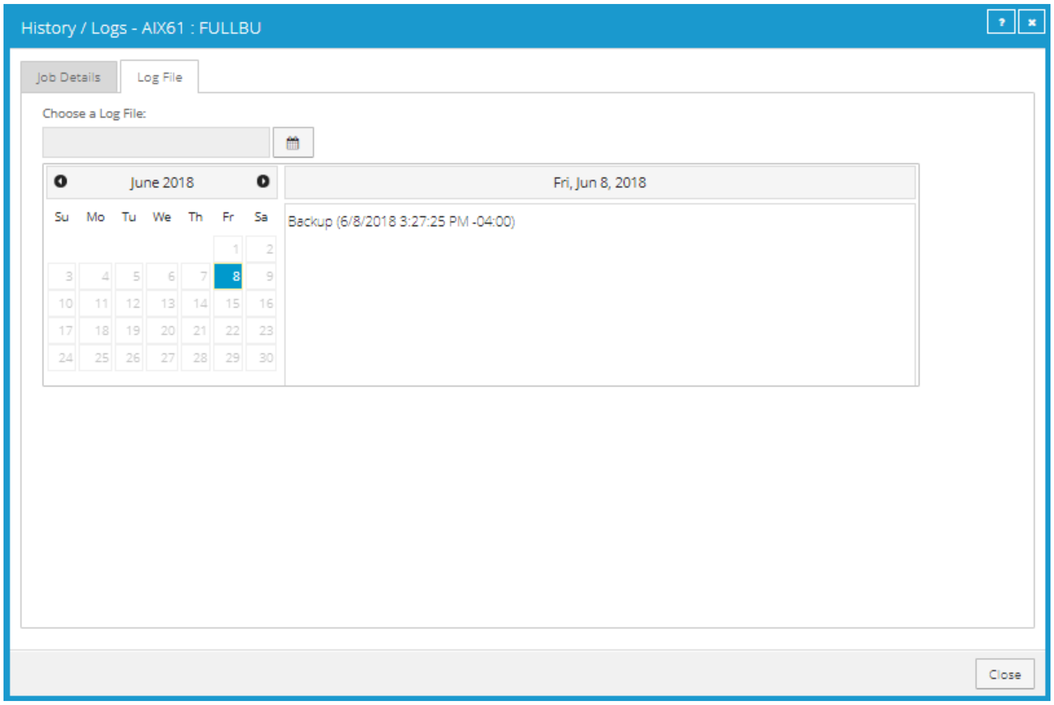


Name	Job Type	Description	Last Backup Status	Date	Action
FULLBU	Local System		Failed	today at 3:27 PM	Select Action
cde	Local System		Never Run		Select Action

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

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

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



Choose a Log File:

June 2018

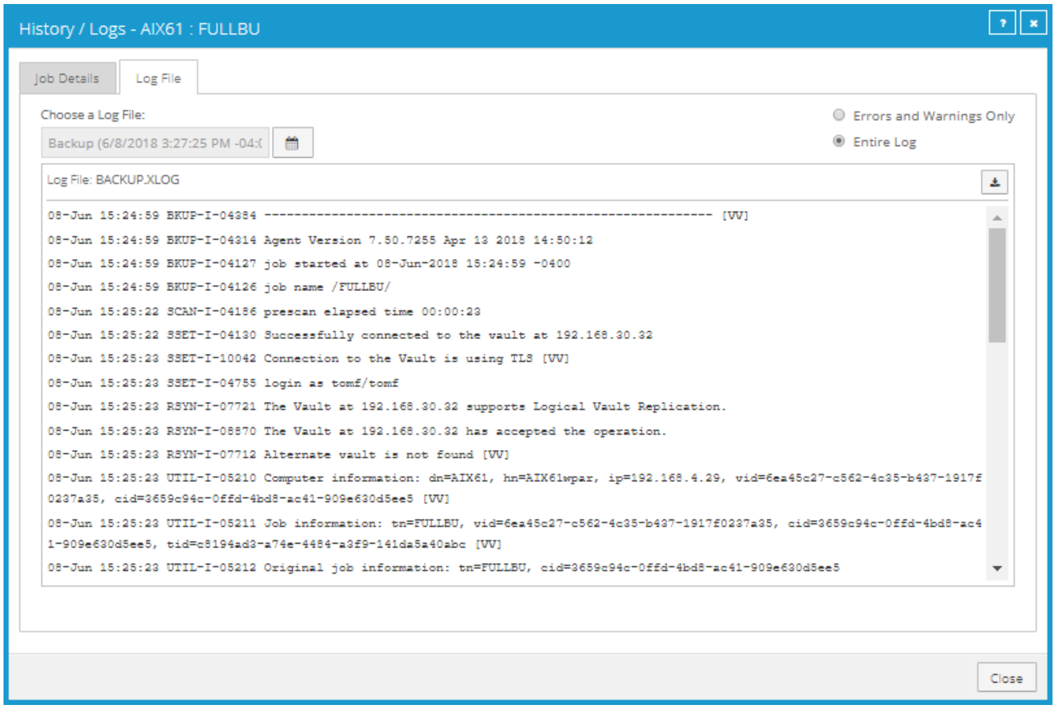
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Fri, Jun 8, 2018

Backup (6/8/2018 3:27:25 PM -04:00)

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

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



Choose a Log File: Backup (6/8/2018 3:27:25 PM -04:(

○ Errors and Warnings Only
● Entire Log

Log File: BACKUP.XLOG

```
08-Jun 15:24:59 BKUP-I-04384 ------------------------------------------------------------ [VV]
08-Jun 15:24:59 BKUP-I-04314 Agent Version 7.50.7255 Apr 13 2018 14:50:12
08-Jun 15:24:59 BKUP-I-04127 job started at 08-Jun-2018 15:24:59 -0400
08-Jun 15:24:59 BKUP-I-04126 job name /FULLBU/
08-Jun 15:25:22 SCAN-I-04186 prescan elapsed time 00:00:23
08-Jun 15:25:22 SSET-I-04130 Successfully connected to the vault at 192.168.30.32
08-Jun 15:25:23 SSET-I-10042 Connection to the Vault is using TLS [VV]
08-Jun 15:25:23 SSET-I-04755 login as tomf/tomf
08-Jun 15:25:23 RSYN-I-07721 The Vault at 192.168.30.32 supports Logical Vault Replication.
08-Jun 15:25:23 RSYN-I-08870 The Vault at 192.168.30.32 has accepted the operation.
08-Jun 15:25:23 RSYN-I-07712 Alternate vault is not found [VV]
08-Jun 15:25:23 UTIL-I-05210 Computer information: dn=AIX61, hn=AIX61wpar, ip=192.168.4.29, vid=6ea45c27-c562-4c35-b437-1917f
0237a35, cid=3659c94c-0ffd-4bd8-ac41-909e630d5ee5 [VV]
08-Jun 15:25:23 UTIL-I-05211 Job information: tn=FULLBU, vid=6ea45c27-c562-4c35-b437-1917f0237a35, cid=3659c94c-0ffd-4bd8-ac4
1-909e630d5ee5, tid=c8194ad3-a74e-4484-a3f9-141da5a40abc [VV]
08-Jun 15:25:23 UTIL-I-05212 Original job information: tn=FULLBU, cid=3659c94c-0ffd-4bd8-ac41-909e630d5ee5
```

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

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

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

8.6 View and export recent backup statuses

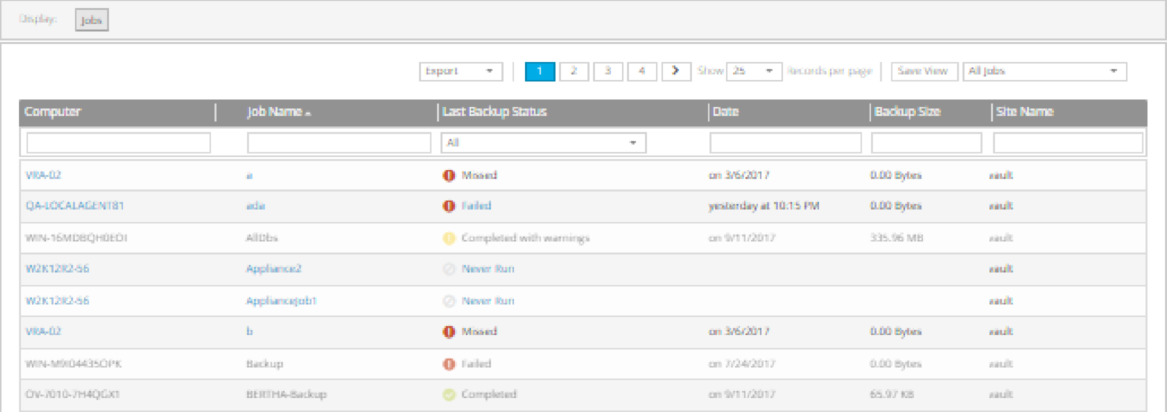
You can view recent backup statuses for computers on the Monitor page in Portal. You can also export the information in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format.

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

To view and export recent backup statuses:

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

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



Computer	Job Name	Last Backup Status	Date	Backup Size	Site Name
		All			
VRA-02	a	Missed	on 3/6/2017	0.00 Bytes	vault
QA-LOCALAGENT81	ada	Failed	yesterday at 10:15 PM	0.00 Bytes	vault
WIN-16MDBQH0EOI	AllDbs	Completed with warnings	on 9/11/2017	335.96 MB	vault
W2K12R2-56	Appliance2	Never Run			vault
W2K12R2-56	Appliancejob1	Never Run			vault
VRA-02	b	Missed	on 3/6/2017	0.00 Bytes	vault
WIN-M9D4435OPK	Backup	Failed	on 7/24/2017	0.00 Bytes	vault
OV-7010-7H4QGX1	BERTHA-Backup	Completed	on 9/11/2017	65.97 KB	vault

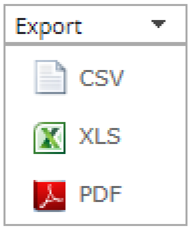
2. To change which backup statuses appear on the page, click the views list at the top of the page, and then click the view that you want to apply.

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)

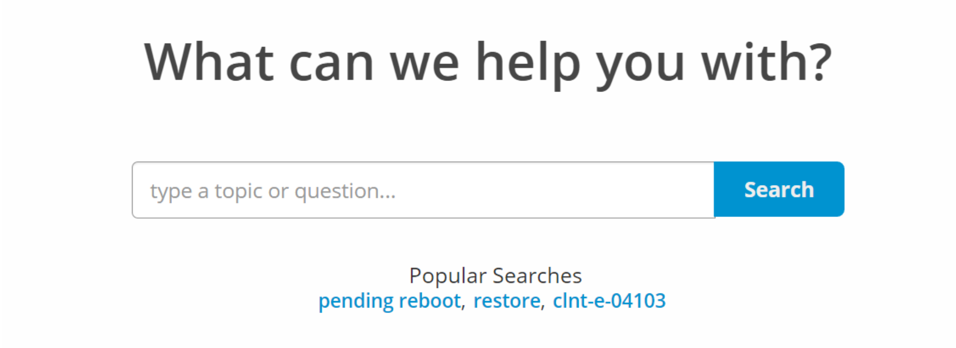


The data file is downloaded to your computer in the specified format.

9 Carbonite Server Backup Support

If you have a question about Carbonite Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any Carbonite Server Backup solutions you may need. We highly recommend searching here first for the quickest answers to your questions.

Knowledge Base: http://support.carbonite.com/evault

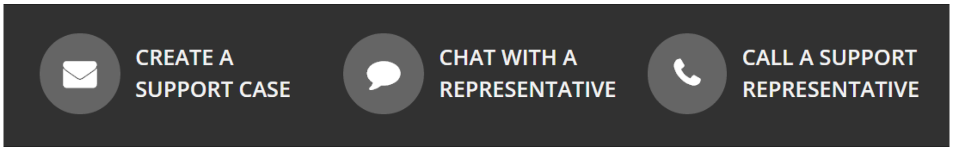


What can we help you with?

type a topic or question...
Search
Popular Searches
pending reboot, restore, clnt-e-04103

9.1 Contacting Carbonite

If you need live assistance from a qualified support agent, Carbonite Support is here for you 24 hours a day, 7 days a week (excluding US holidays). Please feel free to get in touch with us, and we'll help out any way we can! You can find the contact information for Carbonite Support in the Knowledge Base: http://support.carbonite.com/evault



Tip: When contacting Support with a technical issue, please have both the program's log files and the store you are having difficulty with ready.

To gather log files, click **File** menu and choose *Open log folder*. Compress the contents of the folder in a .zip file and attach it to your support request.

If the log archive and/or mail store exceeds 10 MB, you may not be able to send them as an email attachment. In that case, upload instructions will be provided to you upon request.