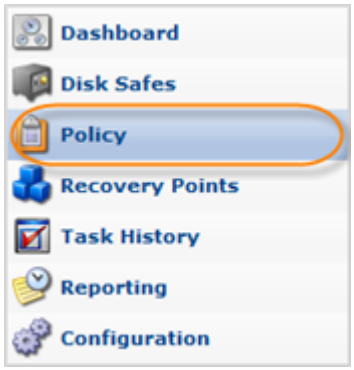
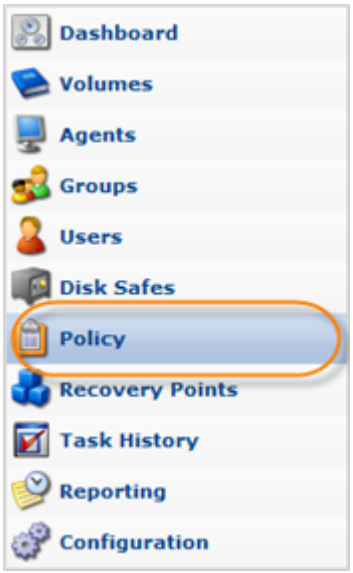
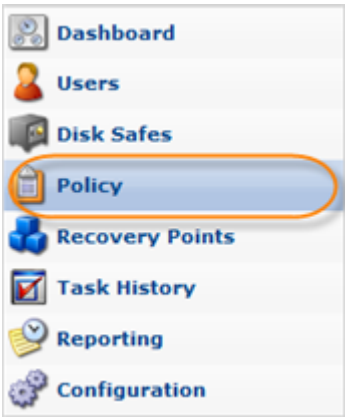
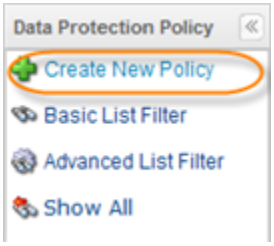
Creating Policies

Follow the instructions below to add a Data Protection Policy in CDP.

1. Click on "Policy" in the Main Menu to open the "Policies" screen.

Standard Edition	Enterprise Edition	Advanced Edition
		

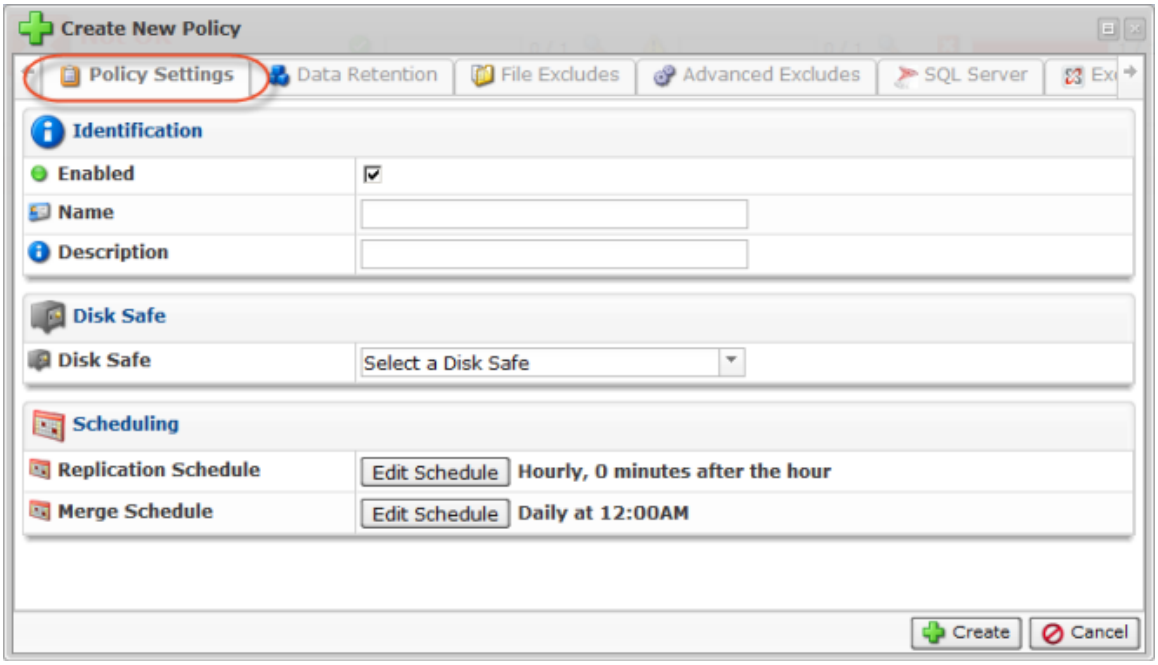
2. In the Policy menu, click on "Create New Policy."



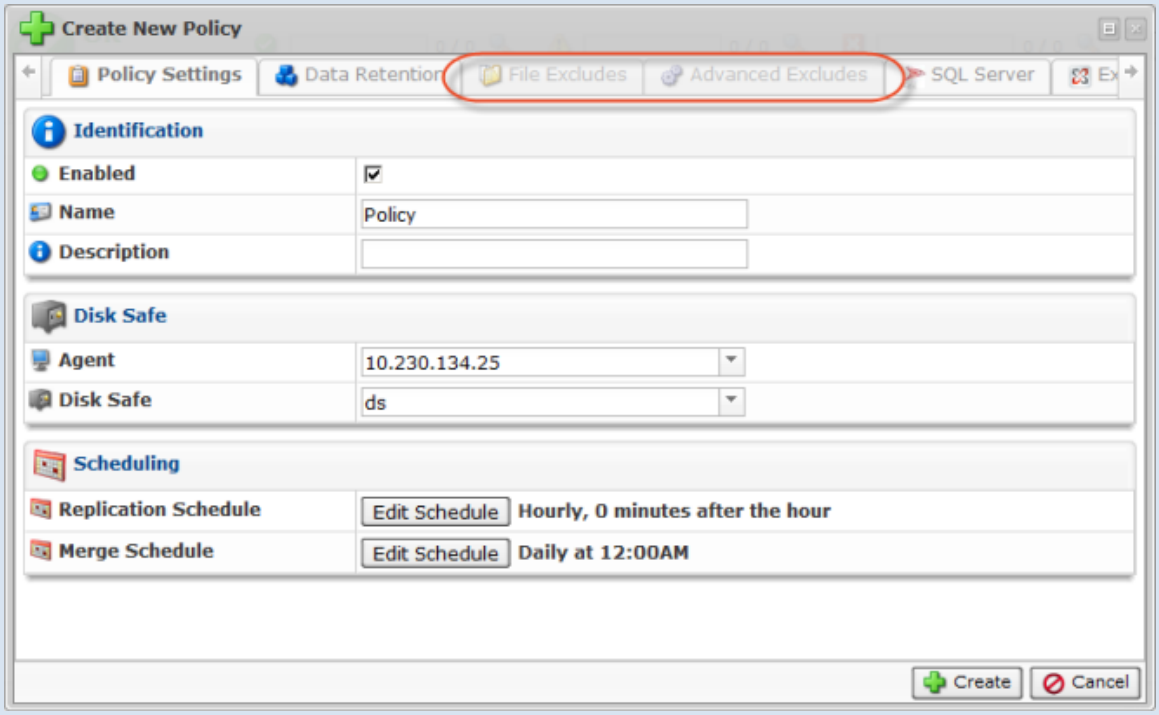
3. The "Create New Policy" window will open. It contains the following tabs:

- Policy Settings
- Data Retention
- File Excludes
- Advanced Excludes
- SQL Server
- Exchange
- MySQL
- Control Panels

- Advanced Policy Settings



Note
Depending on the limits defined for the Disk Safe to which the current Policy is assigned, some of the tabs might be disabled. See Creating Disk Safes.



4. Define the following settings specific to the new Policy:

"Policy Settings" Tab | "Data Retention" Tab | "File Excludes" Tab | "Advanced Excludes" Tab | "SQL Server" Tab | "Exchange" Tab | "MySQL" Tab | "Control Panels" Tab | "Advanced Policy Settings" Tab

"Policy Settings" Tab

This is the main tab for creating a Policy. The following options are available:

Identification

- Enabled - Select this check-box to enable the Policy. The Enabled Policy will run according to the schedule.
- Name - Enter a name you can use to identify this Policy among others in the Policies list.
- Description - Describe your Policy in detail. The description can be shown in the Policies list in the corresponding column.

Disk Safe

- Agent (Enterprise Edition) - From the drop-down menu, select an Agent whose data you are going to replicate. You will then be able to select a Disk Safe assigned to the Agent.
- Disk Safe - From the drop-down menu, select a Disk Safe in which to save the replicated data.

> **Note**
> The Policy will replicate data from the Devices assigned to the selected Disk Safe.

Scheduling

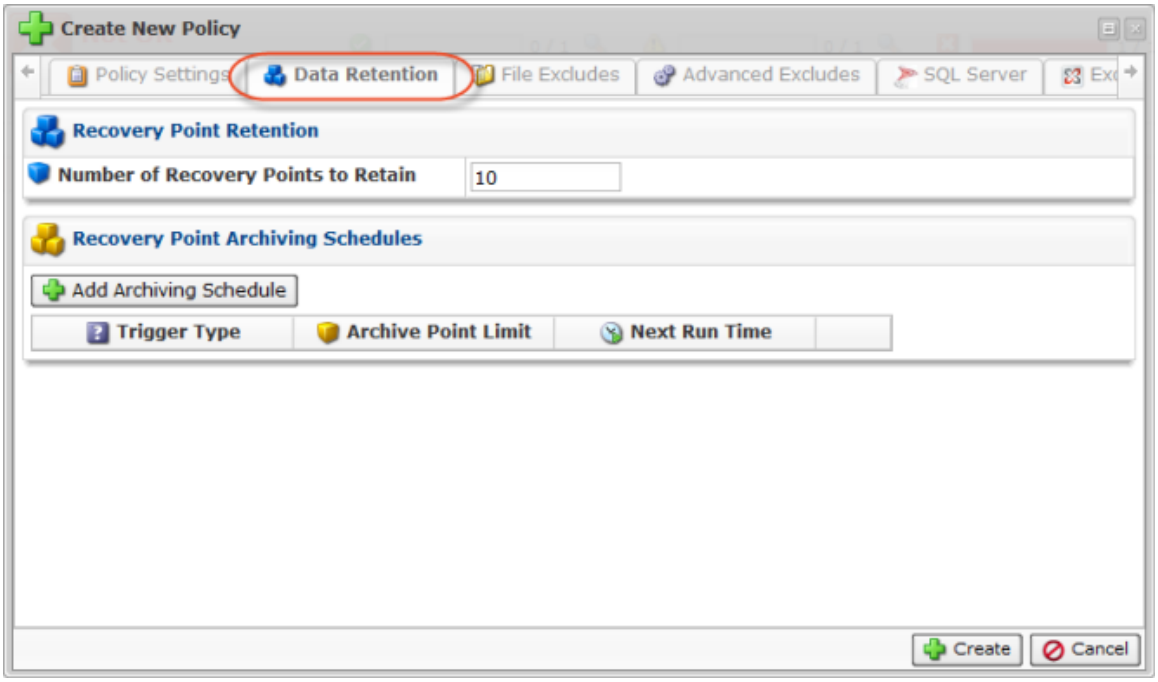
- Replication Schedule - Defines the schedule and recurrence for the new Policy (On Demand, Minutely, Hourly, Daily, Weekly, Monthly, or Yearly). See Scheduling the Recovery Points Replication.

> **Note**
> The lowest possible Replication frequency for all the Disk Safes assigned to a Volume is defined in "Volume properties" ("Volume properties" window › "Limits" tab › "Options" section › "Replication Limit" option).

- Merge Schedule - Defines the schedule and recurrence for Recovery Point merges (After Replication, Hourly, Daily, Weekly). See Scheduling Recovery Point Merges.

"Data Retention" Tab

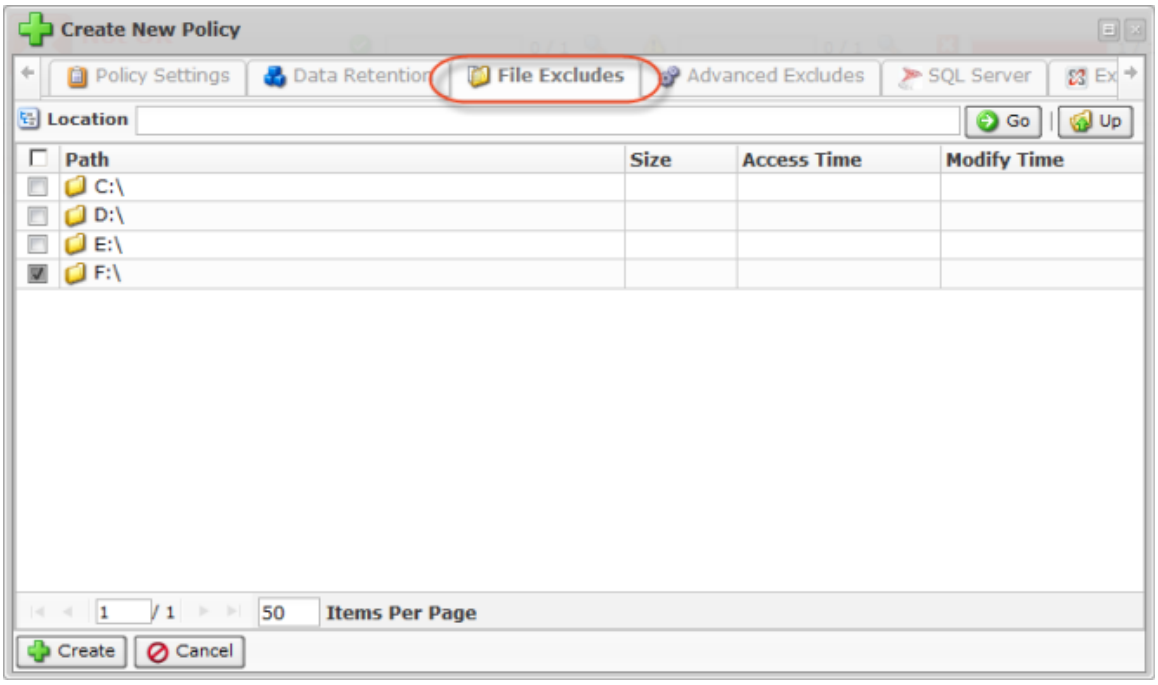
On this tab, you can set the Recovery Points Limit for the Policy and create an Archiving Schedule. See Creating Archiving Policies.



> **Note**
> The Recovery Point limit you set on this tab cannot be greater than the limit defined for the current Disk Safe. See Creating Disk Safes.

"File Excludes" Tab

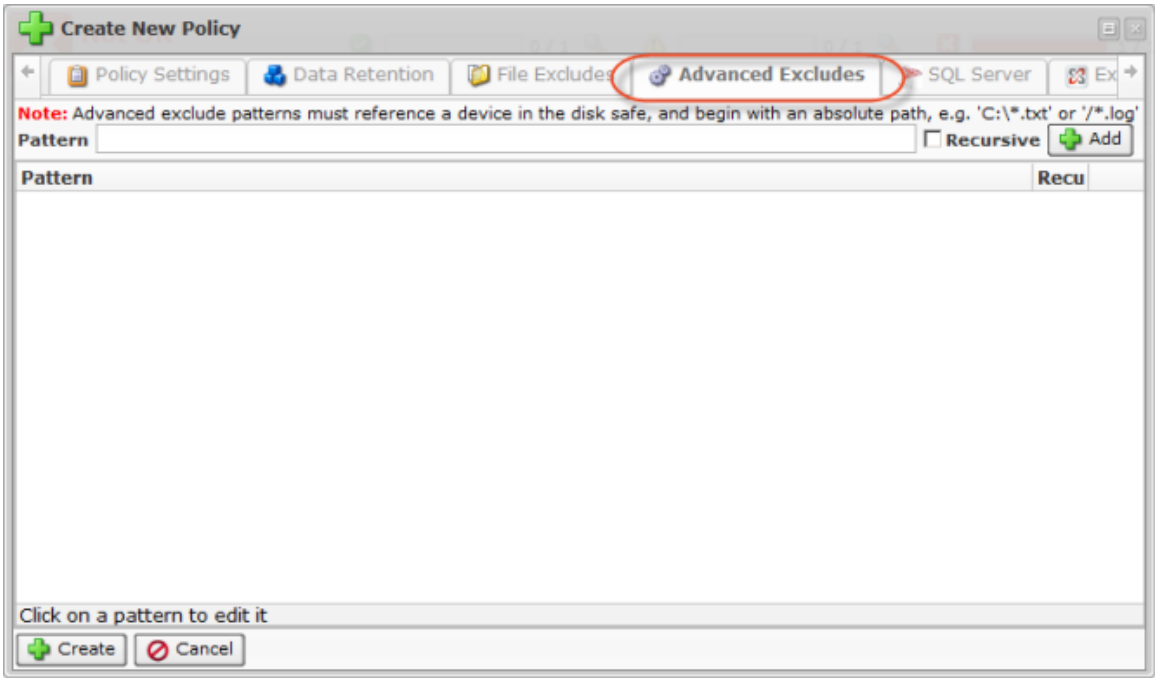
This tab allows you to manually exclude files and folders from the Replication.
See Excluding Files and Folders.



> **Note**
> In our example, the "F:\" disk is selected by default. This is due to the fact that a previously created Disk Safe is located there.

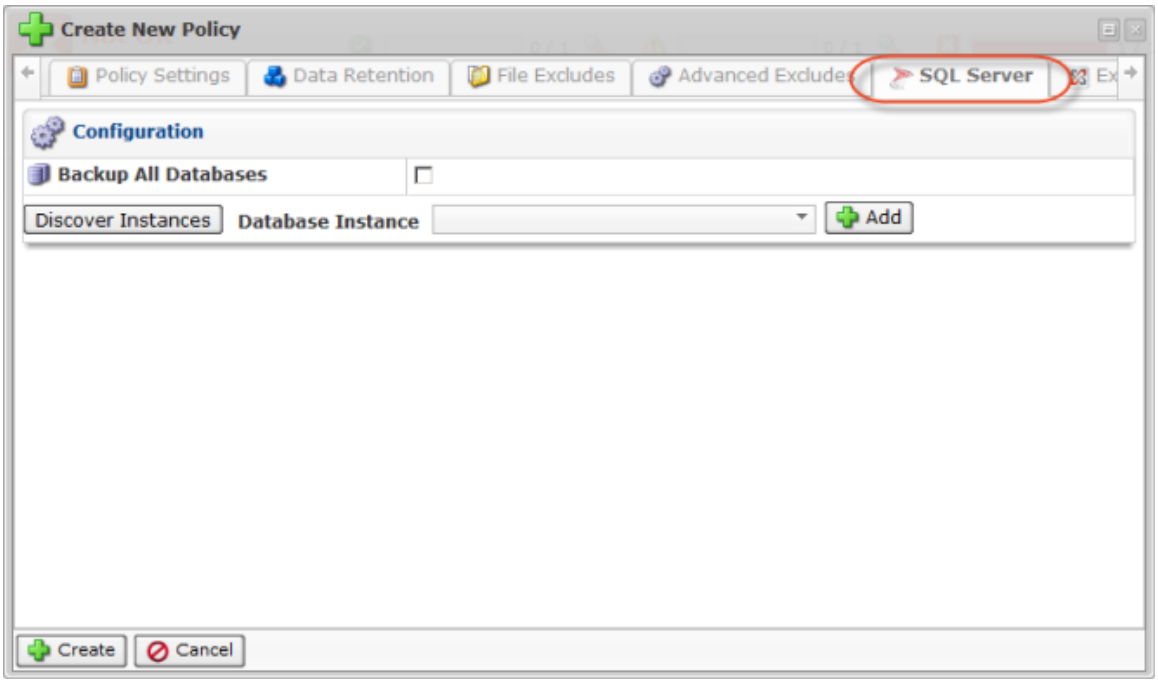
"Advanced Excludes" Tab

This tab allows you to define a pattern (mask) to exclude files from the Replication.
See Excluding Files and Folders.



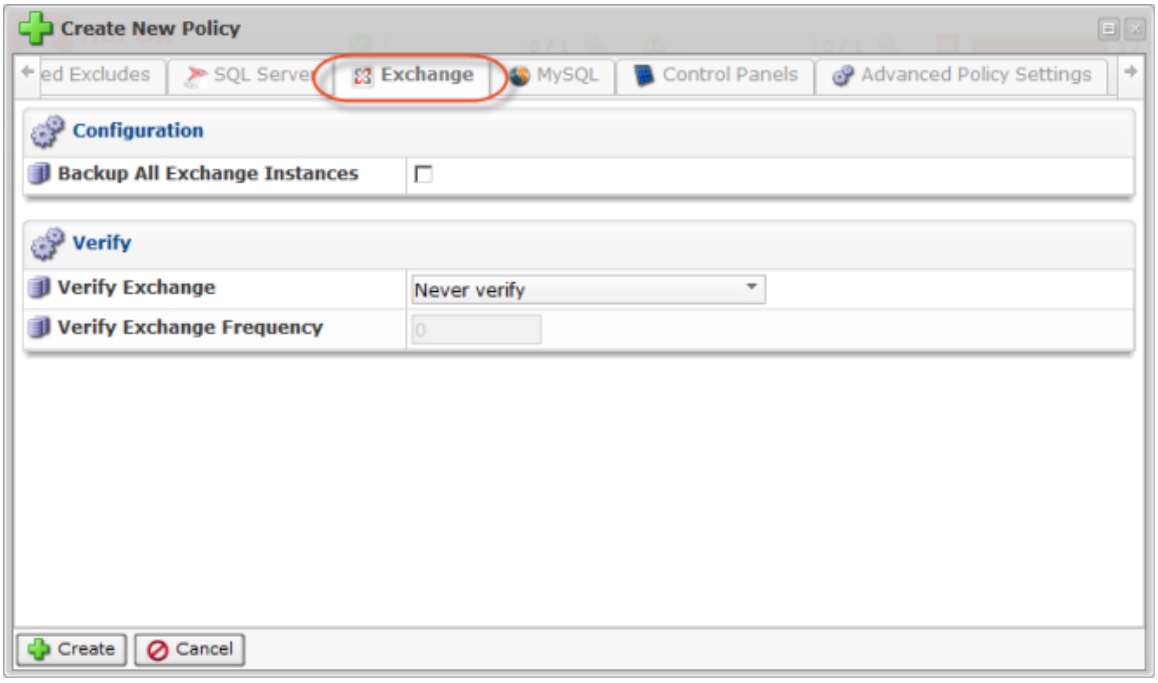
"SQL Server" Tab

This tab allows you to add Database Instances to the Policy.
See Adding a MySQL Instance to a Policy.



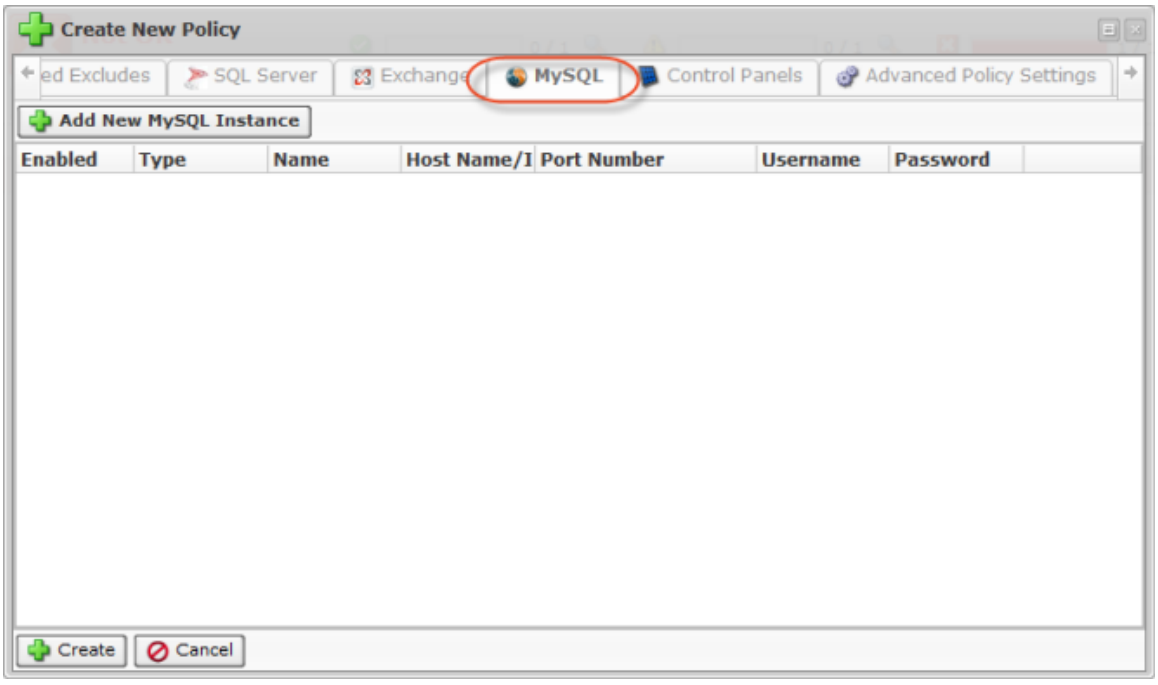
"Exchange" Tab

This tab allows you to configure an Exchange Instance for the Policy.
See Configuring an Exchange Instance.



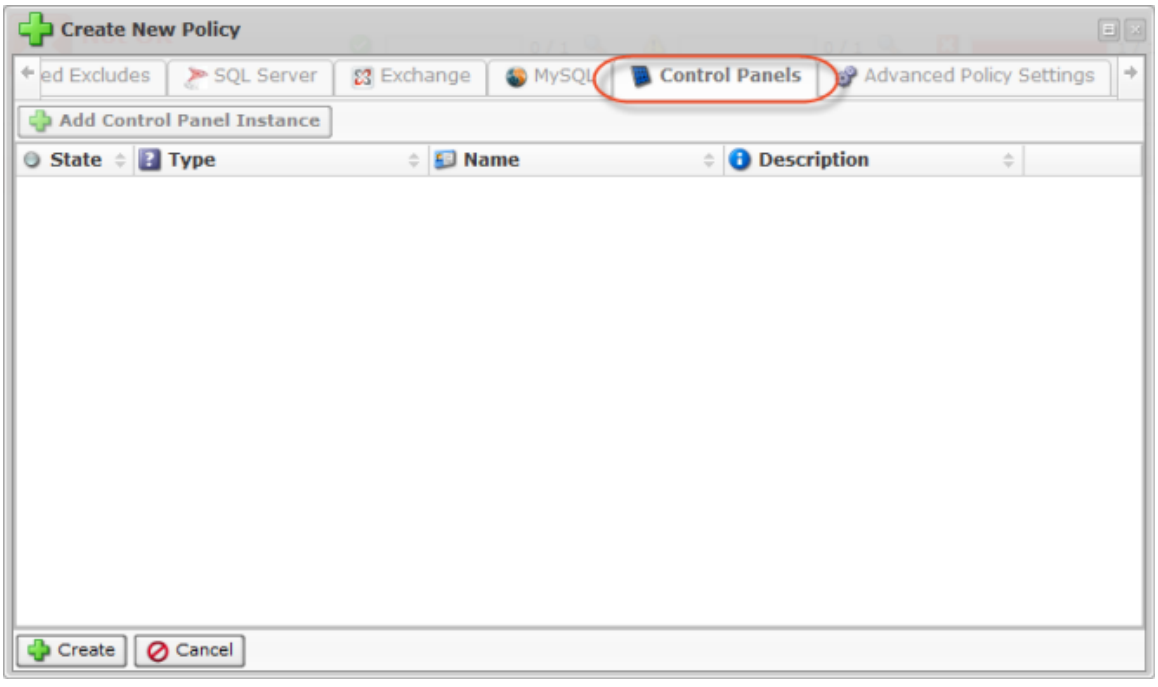
"MySQL" Tab

This tab allows you to add MySQL Instances to the Policy.
See Adding a MySQL Instance to a Policy.



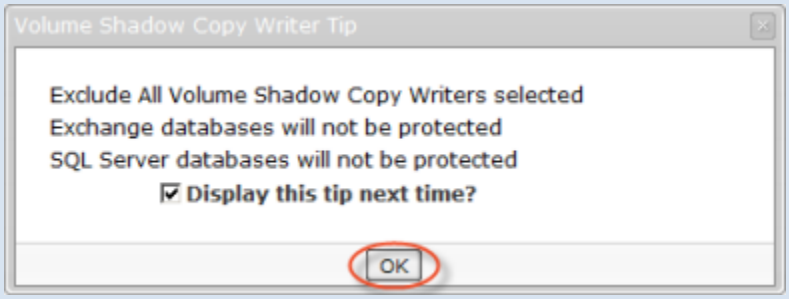
"Control Panels" Tab

This tab allows you to add a Control Panel Instance to the Policy.
See Adding Control Panel Instances.



"Advanced Policy Settings" Tab

- Force Full Block Scan - Optionally check this option to mandate the start of a Full Block Scan each time the Replication is performed. If the option is not selected, then an automatic Full Block Scan occurs only under certain conditions. A Full Block Scan compares the MD5 sum of all allocated blocks to perform the backup and synchronize CDP. Read more in 3 Stages of CDP 3 Replication (Technical Papers).
- Exclude All Volume Shadow Copy Writers - Optionally check this option if you temporarily want to exclude the Exchange and SQL Server databases from being backed up.

> Tip
> Once the "Exclude All Volume Shadow Copy Writers" option is checked, the following message will appear. Read the information and click the "OK" button.
>
> 
>

- Exclude Known Disk Safes (Standard and Advanced Editions) - This default option allows you to exclude the known Disk Safes from the Replication to avoid backing up the same data twice.
- Verify checksums server side - Optionally enable this option to ensure that no data is lost during transporting. If this option is activated, then the Server side uncompresses the data, unencrypts it if necessary, and compares block packet MD5 with data sent from the Agent. Verifying encrypted or unencrypted block checksums on the CDP Server allows you to triple-check the integrity of a backup.
- Specify Backing File Location (Linux only) - Optionally define a path that the mount point of a Device should use to store changed blocks. This option is useful to support backups of Devices with low free space. By default, the Linux snapshot driver stores changed blocks (needed to maintain snapshots) in the the free space of the file system on which it is performing a snapshot. When using a server with multiple disks, storing snapshots on a separate dedicated disk can help reduce the load during backup. The disk must have a file system and must be mounted.

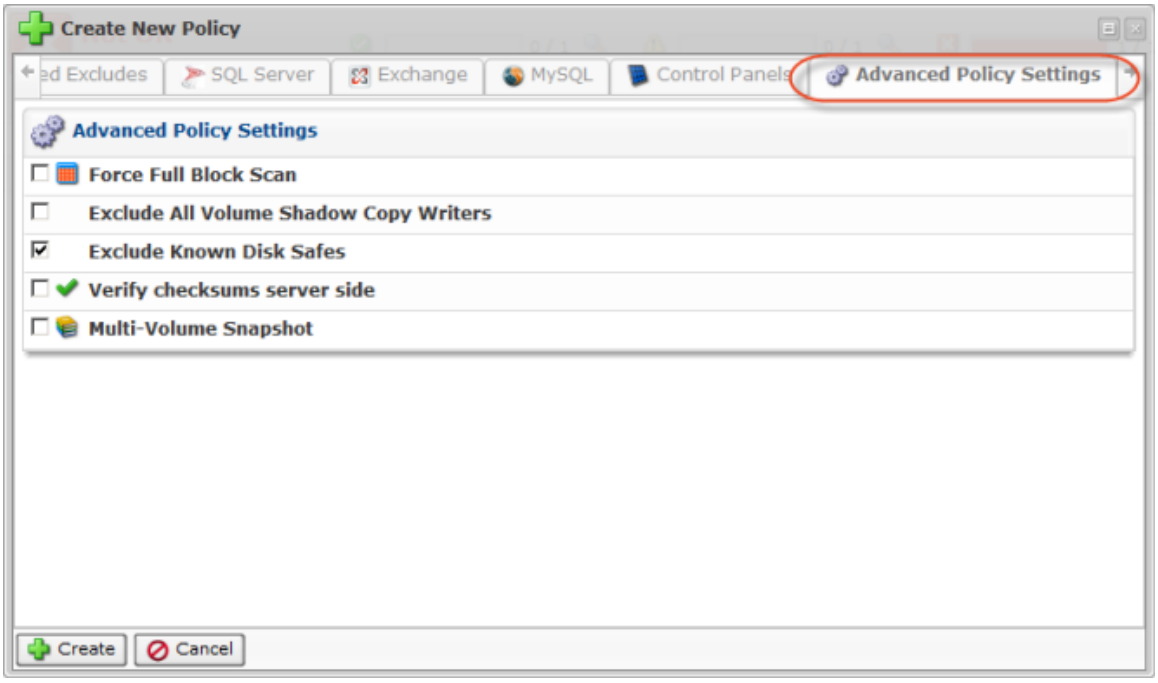
Example
Linux system:

Mount Point	Disk
/dev/sda1	/boot
/dev/sda3	/
/dev/sda4	/var

When /boot or /var is 99.99% full, the backups fail because there is no free space to maintain the snapshot.
Once the user inputs "/" into the "Backing File Location" field, the /dev/sda3 path will be used as the changed block storage location for all file systems.

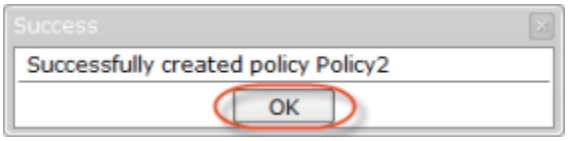
- Multi-Volume Snapshot - This option can be useful if the MS SQL Server has files across more than one Device. The check-box is hidden on Linux Policies and un-checked by default on new and upgraded Windows Policies.

Note
If the SQL Server has files across more than one Device, and the "Multi-Volume Snapshot" option is not selected, then the system displays an alert message.



5. Click on "Create" in the bottom of the window to add the Policy to the Policies list.

6. You will receive a notification that the creation of the Policy was successful. Click "OK."



> **Tip**
> The Task results can be sent via email as a Report. See Reporting.

7. The new Policy item appears in the Policies list. The properties are shown in the grid.

> **Tip**
> Click on an item in the Policies list to see the Policy details in the bottom pane.

You can find more information on how to use the "Policies" screen in Accessing Policies.

You can also create Policies using the "Policies" tab of the Agent "Details" Pane. This screen provides the same functionality as the main "Policies" screen. See more information in Accessing Agents.