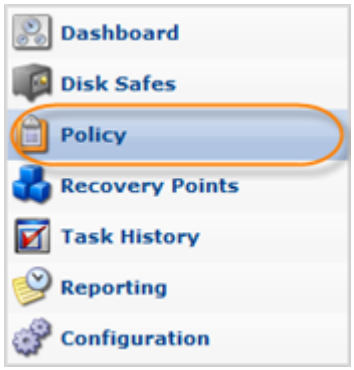
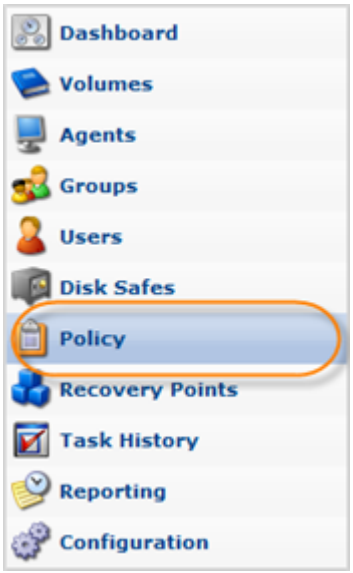
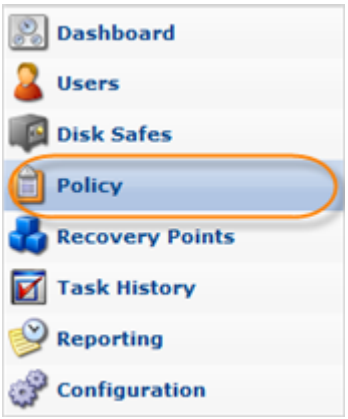
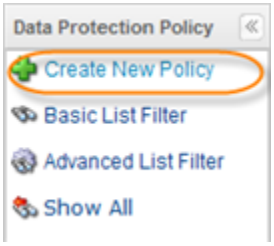
Creating Policies

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.

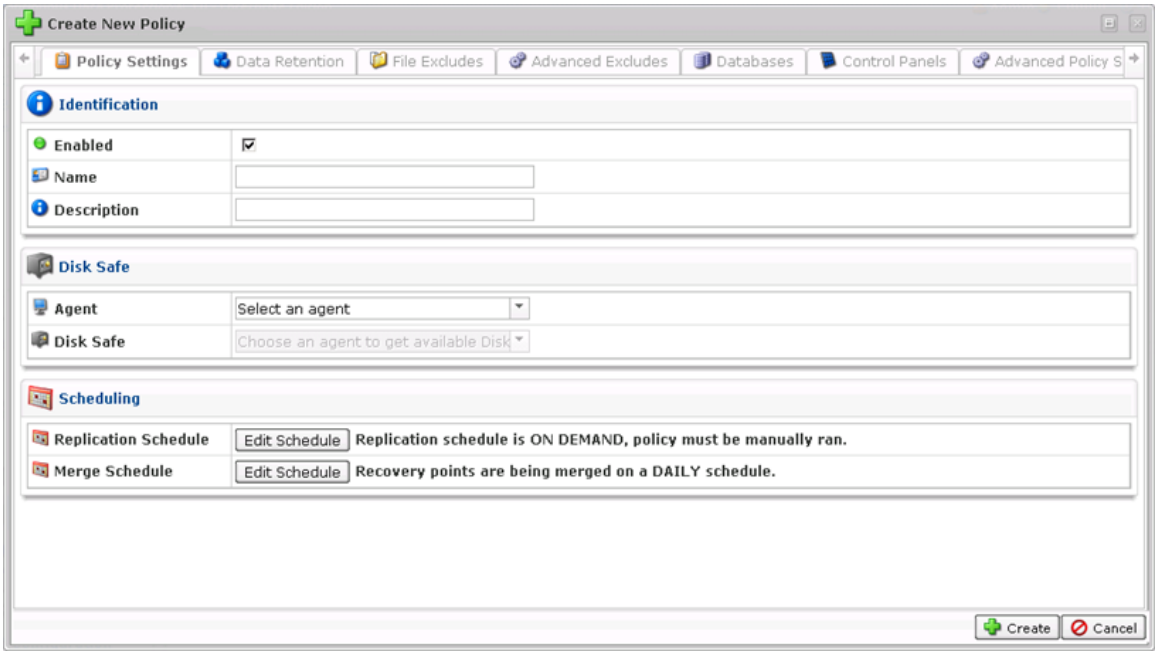
Standard Edition	Enterprise Edition	Advanced Edition
		

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



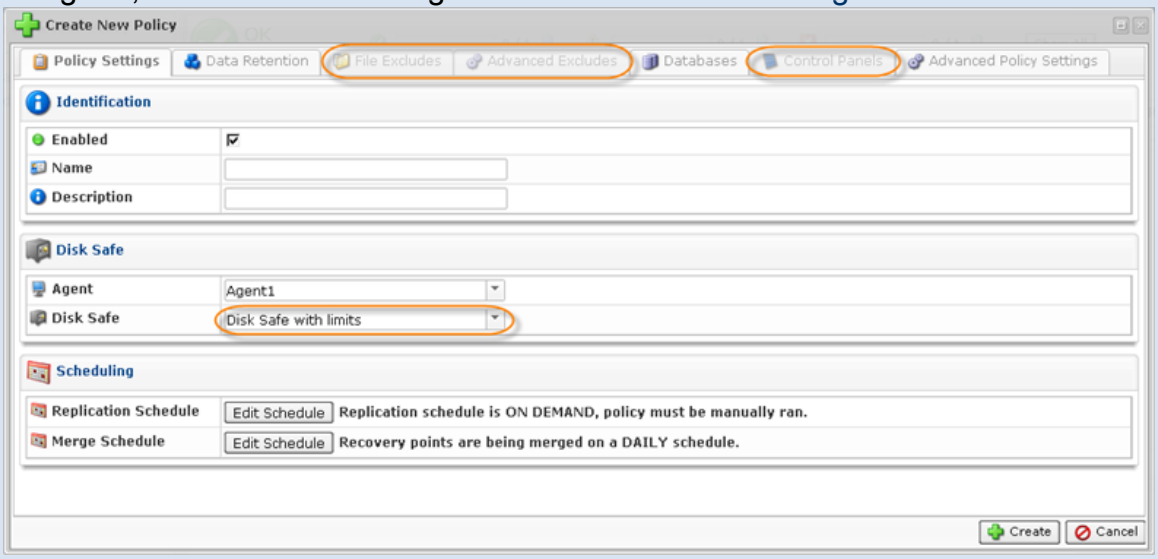
3. The "Create New Policy" window will open. It contains the following tabs:

- Policy Settings
- Data Retention
- File Excludes
- Advanced Excludes
- Databases
- 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#lim



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

Policy Settings Tab | Data Retention Tab | File Excludes Tab | Advanced Excludes Tab | Databases 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 checkbox 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 details. 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 for which data you are going to replicate. Then you will 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

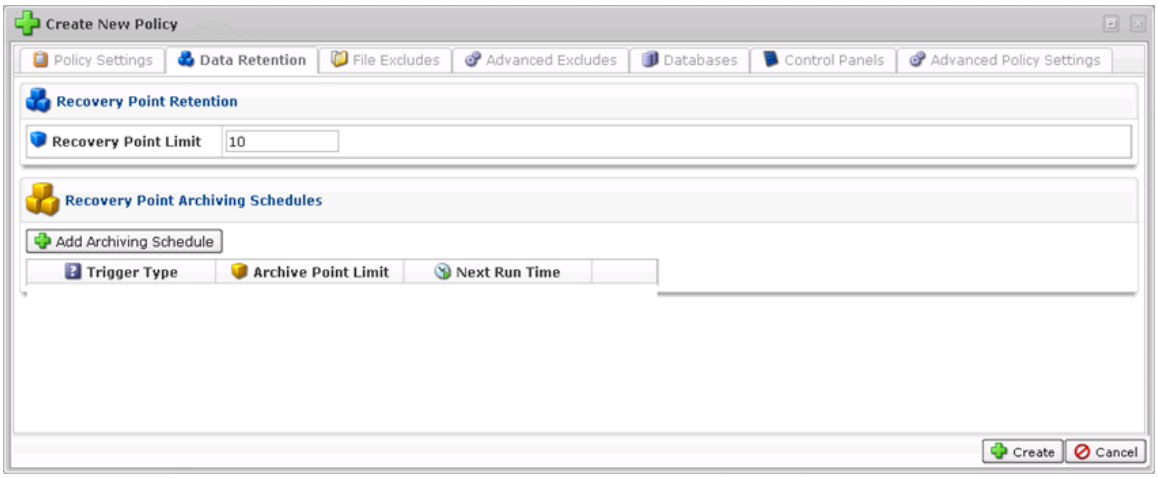
- Replication Schedule - Define the schedule and recurrence for the new Policy (On Demand, Minutely, Hourly, Daily, Weekly, Monthly, or Yearly). See Scheduling the Recovery Points Replication.

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

- Merge Schedule - Define the schedule and recurrence for the Recovery Points merge (After Replication, Hourly, Daily, Weekly). See Scheduling the Recovery Points Merge.

Data Retention Tab

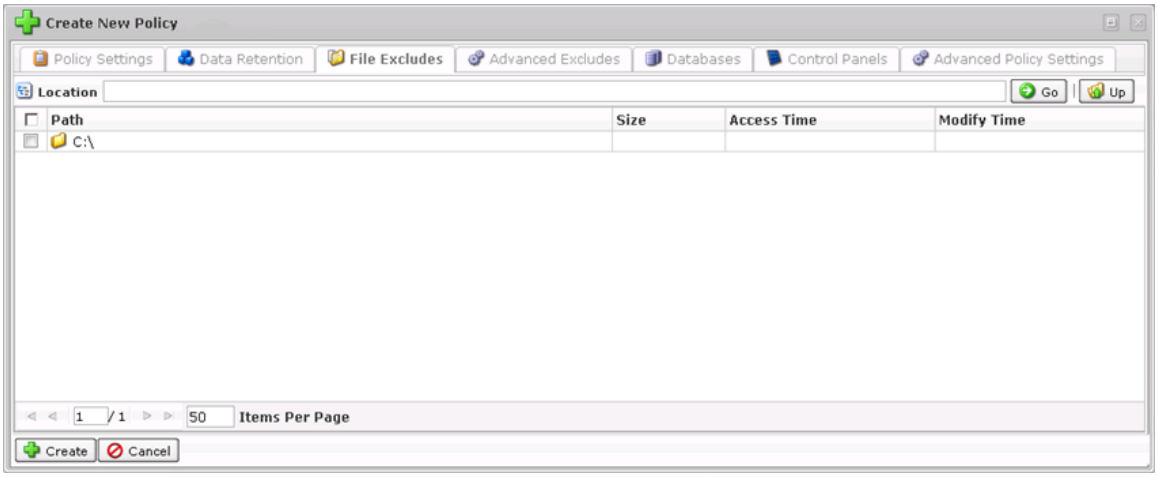
On this tab, you can set the Recovery Points Limit for the Policy and create an Archiving Schedule. See Creating Archiving Policies.



> **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#lim.

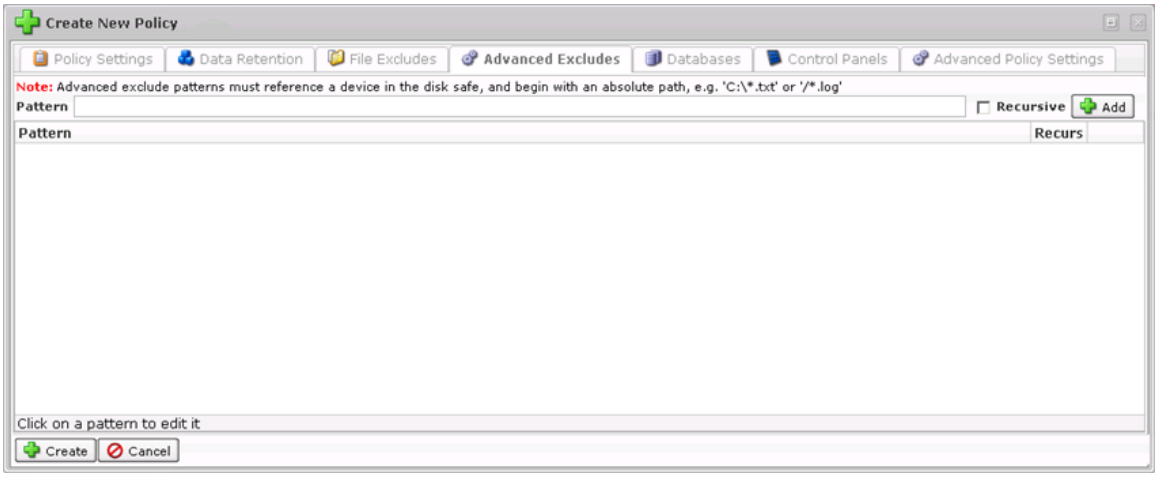
File Excludes Tab

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



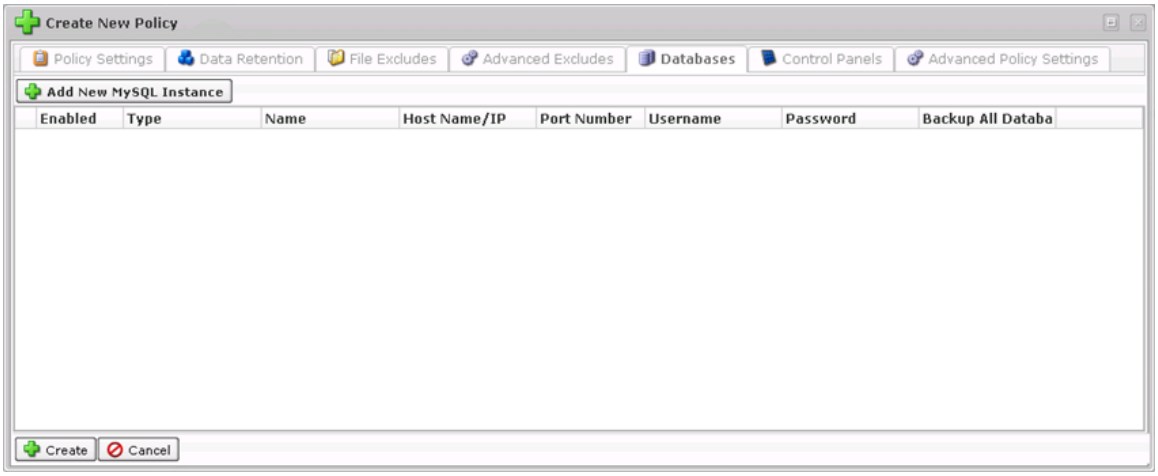
Advanced Excludes Tab

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



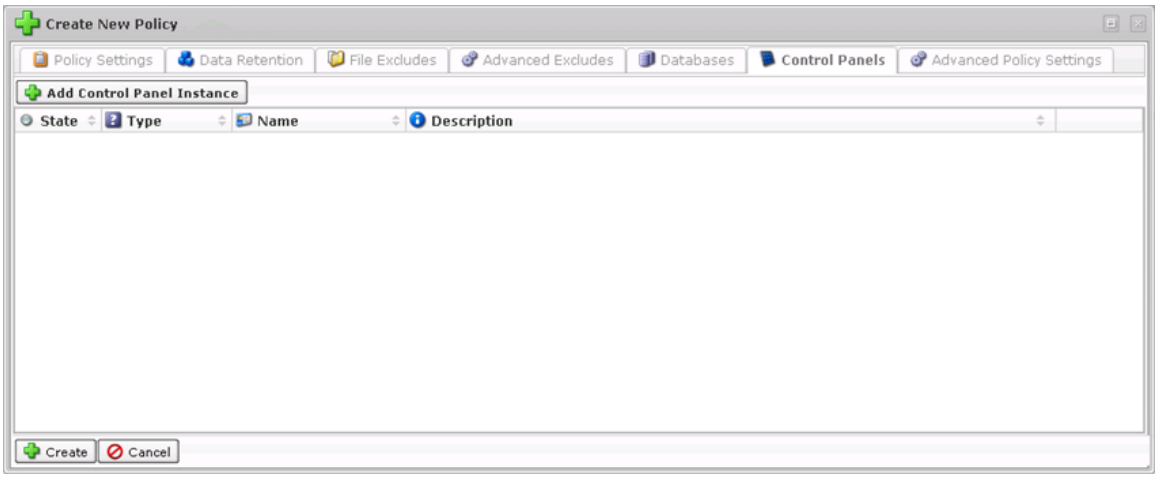
Databases Tab

This tab allows you to include MySQL databases in the replication policy.
See Adding MySQL Instance to the Policy.



Control Panels Tab

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



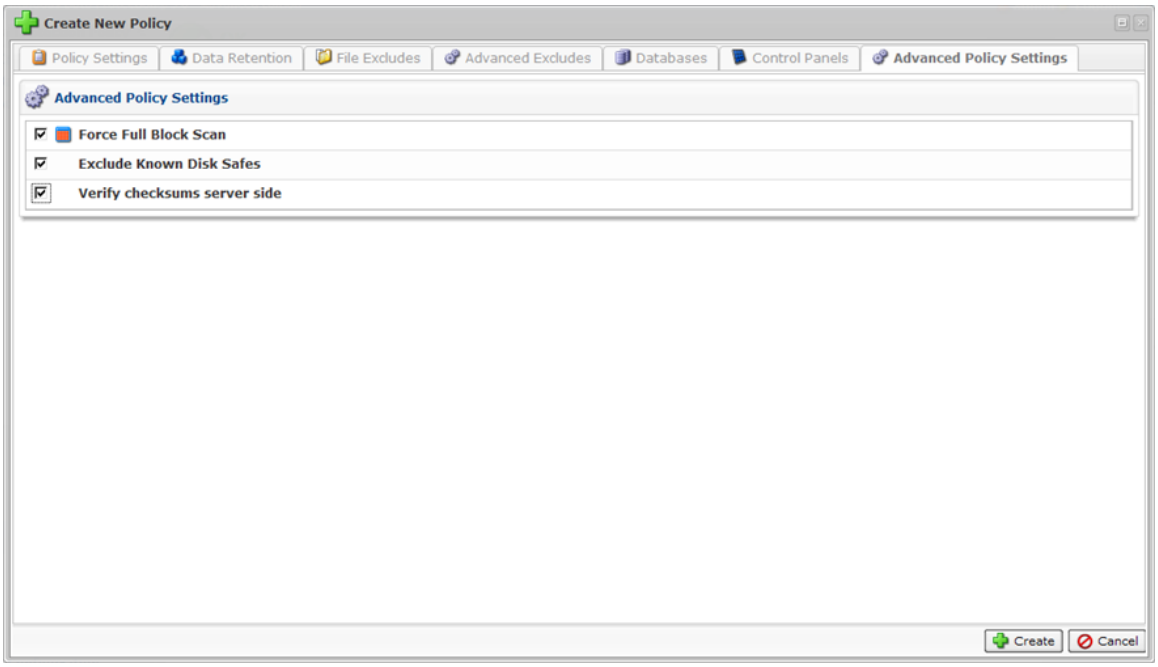
Advanced Policy Settings Tab

- 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 happens only under certain conditions. A full block scan compares the MD5 sum of all allocated blocks to perform the backup and get CDP back in synchronization. Read more in 3 Stages of CDP 3 Replication (Technical Papers).
- 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, unencrypts if necessary and compares block packet MD5 with data sent from Agent. Verifying encrypted or unencrypted block checksums on the CDP Server allows you to triple check the integrity of a backup.
- Exclude Known Disk Safes (Standard and Advanced Editions) - Optionally check this option to exclude the known Disk Safes from the replication to avoid backing up the same data twice.
- Specify Backing File Location (Linux only) - Optionally define a path which 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.

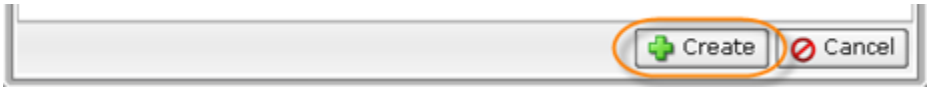
Example
Linux system:

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.



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.