Axcient Unified Management Console Quick Start Guide

AXCIENT™

axcient.com

NOTICE

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF AXCIENT, INC., AXCIENT MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE.

Axcient assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. This document contains information that is the property of Axcient, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Axcient.

The information contained in this document is subject to change without notice.

Axcient™, Uptiva™, RapidRestore™, SmartArchive™, SmartDR™, SmartCloudDR™, and ServerAlive™ are trademarks of Axcient, Inc.

All other trademarks and registered trademarks are the property of their respective holders.

TOC

Introduction

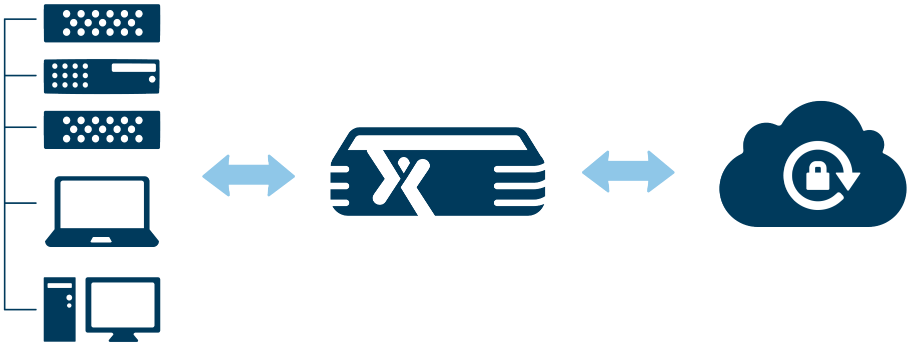
The Axcient data protection solution provides continuous data backup, business continuity, and rapid-recovery services. This protection is scalable, flexible and easy to administer, protecting data both locally and in the Cloud. The Axcient protection solution is minimally intrusive to install, maintain and operate and does not require the user to install agent software on systems in order for devices to be protected.

There are several steps the user will need to take to configure the Axcient protection solution:

1. Analyze the organization's data protection needs to determine what devices need to be protected and what data needs to be replicated. Additionally determine the data protection schedule, so that data can be backup up regularly without impeding on business operations.
2. Install the Axcient appliance at the target site. The Axcient appliance provides local backup and restore capabilities. Each Axcient appliance connects to the secure Axcient Cloud for offsite (disaster) capabilities.
3. Configure the Axcient appliance for optimal performance (as needed). Minimal configuration is require, but the user can customize settings for bandwidth throttling, web proxy, SNMP and other relevant parameters.
4. Add users who can perform administrative tasks (as needed). Default user accounts are provided, but the user can add additional users from the organization.
5. Identify the target devices (servers, desktops and laptop computers) and configure the Axcient appliance to access those devices.
6. Create the backup jobs. There are two types of backup jobs:
   - **File Backup** - Back up files and folders. The user can select any number of files on the device, from a single file to everything on all disks.
   - **Image Backup** - Backup a complete system image. This is a snapshot of the entire system which can be used to restore files, perform a Bare Metal Restore, or start a Failover Virtual Machine.
7. Monitor the Axcient appliance to ensure that devices are being properly protected. Axcient provides statistical and event reporting for this purpose.
8. Recover data or services as needed:
   - **File Restore** - Restore files from a file or image backup job.
   - **Bare Metal Restore** - Restore a complete system image to new hardware.
   - **Virtual Machine Failover (VM)** - Failover a server as a virtual machine on the Axcient appliance.
   - **Cloud Failover** - Failover a virtual office in the Axcient Cloud if the Axcient appliance is not available.

The following figure illustrates the Axcient architecture. The Axcient appliance copies data from the target devices and store it with the appliance. When scheduled, the appliance replicated the encrypted data to the Axcient Cloud for offsite storage and recovery when needed.

Figure 1 - Axcient Architecture



This guide describes how to quickly protect devices using the Axcient protection solution.

NOTE

See the Axcient Installation Guide for instructions on how to install the Axcient appliance at a target site. See the Axcient UMC User Guide for information about the Unified Management Console, including the topics listed above.

Add a Device

To add a device, do the following:

1. Log in to the Unified Management Console (UMC) of the appliance.
2. In the UMC Dashboard, click on the **devices** tab in the top navigation bar.
3. The Devices screen appears. Select the **add a device** option located on the left of the screen.
4. The Add a Device screen appears. Enter the appropriate information into the following fields and click the **Save** button to add the device:
   a. **Hostname or IP** - Enter the device's IP address or hostname.
   b. **Operating System** - Select the device operating system from the drop-down menu. The default is `AUTODETECT`, which should work in most cases.
   c. **Device Type** - Select the type of device (`SERVER`, `LAPTOP`, `DESKTOP`) from the drop-down menu.
   d. **Administrative username** - Enter the name of the user that has administrative privileges on the device.
   e. **Administrative password** - Enter the password for the user specified in the previous step.
   f. **Device alias** (optional) - Enter an alias for the device name. This name appears in the UMC displays.
   g. **Additional user assigned** (optional) - Select an additional user from the drop-down menu who can perform backup operations on this device. Otherwise, only the administrative user can perform operations.

When the device is added, an icon appears in the devices page for that device.

Create a Backup Job

Note: The following

To create a backup job, do the following:

1. On any page in the UMC, click on the **devices** tab in the top navigation bar.
2. The *Devices* screen appears. Click on the icon of a target device.
3. The Backup Jobs screen appears. Click on the **file backup** or **image backup** option in the left-hand navigation menu. If creating an **image backup**, skip to *Step 4*. If creating a **file backup**, do the following:
    a. Expand and locate target files and folders
    b. Select (click the box for) files to be backed up. Selecting a directory backs up all its files and directories. Selecting the top-level drive (such as C:) backs up everything on the drive.
    c. Determine whether files should be backup only locally, or both locally and in the Axcient Cloud. A solid box (one click) signifies both, while a half box (two clicks) signifies only locally.
    d. After specifying files to be backed up, click **next**.
4. The Schedule screen appears. Do the following:
    a. Verify the listed directories are the correct one(s) to be backed up.
    b. Enter a name for the backup job.
    c. Specify a backup type from the pull-down menu. The options are On Demand, Hourly, Daily, Weekly, Monthly or Yearly.
    d. Based on the option chose, additional fields will be presented which allow the user to further customize the backup schedule. Configure as needed or accept the defaults.
    e. Click the **save** button.

The backup request is recorded and saved. If it is an on-demand backup, the job will begin immediately. Other backup types will begin according to the configured schedule.

The user can start a backup job at any time by clicking the start button for that job in the *Idle Backups* section of the UMC Dashboard.